Math 115 Notes

Summer 2018

Alex Youcis

Contents

1 Lecture 1: Introduction

1.1 Preamble

Question 1.1

What are we doing?

The answer is that we are studying $\mathbb{Z}$:

Definition 1.1

The *integers* are the following set:

$$\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\} \tag{1}$$

Also, for future reference we recall that the *natural numbers*, denoted $\mathbb{N}$, is the set of non-negative

integers (so it contains 0). We denote by $\mathbb{N}^*$ the set of positive integers. The *rationals* are the set

$$\mathbb{Q} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\} \tag{2}$$

Two natural questions arise:

1. What structures does $\mathbb{Z}$ possess to study?
2. Why do we, as budding mathematicians, care about studying $\mathbb{Z}$?

The answers are intertwined. Namely, even though $\mathbb{Z}$ is an incredibly concrete object, it has structures that allow it to show up in essentially all areas of modern mathematics: logic, analysis, geometry/topology, algebra,.... Many of these we will see in this course. It is for this reason that $\mathbb{Z}$ serves as an excellent testing ground for many mathematical ideas: being simple enough to easily grasp, but universal enough to be significant.

As an example of the interactions between basic number theoretic questions and deep, widespread ideas of mathematics, we have the following result that people love to parade around:

Example 1.1

Basic question(Fermat): Is the sum of two n^{th} power (integers) ever an n^{th} power (integer)?

Answer(Wiles-Frey-Ribet-...): No if $n > 2$, except for silly examples like $0^5 + 3^5 = 3^5$.

Required immense amount of input from many areas of modern mathematics (geometry/topology, algebra, analysis,...) and is the culmination of hundreds of thousands of pages of mathematics.

This above example also underscores that while $\mathbb{Z}$ is interesting because of how many fields it intersects, by the same token one must accept the grim reality that questions in number theory are often brutally difficult and deep.

This is all nice and well, but the question still stands:

Question 1.2

Ok... but what are *we* doing?

This was a difficult to answer question for myself. For the reasons listed above, there are many, many directions one can take when giving a first course in number theory (even elementary number theory). That said, making this clarification is key. The varied nature of the techniques and ideas present in number theory often times makes it feel like a melange of random topics without a clear goal in mind. To avoid this feeling, it will be helpful to give us very specific goals for this course.

In particular, while $\mathbb{Z}$ is interesting because it has many interesting structures, our primary focus will be on the algebraic structure of $\mathbb{Z}$ and, more specifically the equational aspects of $\mathbb{Z}$. More specifically, we are interested in $(\mathbb{Z}, +, \cdot)$ ($\mathbb{Z}$ with addition and multiplication) and studying equations one can build from it.

1.2 The structure of $(\mathbb{Z}, +, \cdot)$

To understand the basic structure of $(\mathbb{Z}, +, \cdot)$ it's helpful to understand the operations $+$ and $\cdot$ individually.

1.2.1 The structure of $(\mathbb{Z}, +)$

The integers with addition are incredibly simple. In fact, they are 'generated' by a single number: 1. Namely, every $x \in \mathbb{Z}$ has a unique (minimal) expression in the form

$$x = \underbrace{1 + \cdots + 1}_{\text{Some number of times}} + \overbrace{-1 - \cdots - 1}^{\text{some number of times}} \tag{3}$$

This makes most questions about $(\mathbb{Z}, +)$ incredibly simple.

For example, equations in $(\mathbb{Z}, +)$ all look (essentially) like

$$a_1 x_1 + \cdots + a_n x_n = b \tag{4}$$

with $a_1, \ldots, a_n, b \in \mathbb{Z}$ constants and x_i are variables (in $\mathbb{Z}$). Such equations are not trivial to solve but, as we'll see next time, a judicious study of some of the most basic properties/constructions in $\mathbb{Z}$ swiftly leads to an algorithmic solution to when such equations have solutions, as well as ways of paramaterizing all solutions if they exist.

Example 1.2

The equation $3x + 5y + 7z = 1$ has infinitely many solutions in $\mathbb{Z}$.

Example 1.3

The equation $4x + 12y = 5$ has no solutions in $\mathbb{Z}$.

1.2.2 The structure of $(\mathbb{Z}, \cdot)$

The structure of the integers with multiplication is more complicated than the structure of $(\mathbb{Z}, +)$, but not overwhelmingly so. Instead of one 'generator' it has infinitely many. To explain this, it will be helpful to recall two basic definitions:

Definition 1.2

If $a, b \in \mathbb{Z}$ we say that a *divides* b, and denote it $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ca$.

Definition 1.3

An element $x \in \mathbb{Z}$ with $x > 1$ is called *prime* if $x \mid ab$ implies that $x \mid a$ or $x \mid b$.

Note that Definition 1.3 differs from how one usually thinks of primes. Namely, call an integer $x > 1$ *irreducible* if any factorization $x = ab$, with a and b elements of $\mathbb{N}^*$, has that $a = x$ or $b = x$. We will see in the next class that the above definition of prime agrees with the notion of irreducible.

Remark 1.1

The above distinction between prime and irreducible is a deceptively deep. In fact, the conflation of the notions of 'prime' and 'irreducible' in more general contexts led to a staggering amount of incorrect mathematics (e.g. Google the phrase 'Lamé's false proof') and the desire to clarify the differences

between the two phrases led to a surprising amount of modern mathematics (e.g. the whole field of ring theory in some sense).

The fundamental (pun intended) structural result concerning $(\mathbb{Z}, \cdot)$ is then the following:

Theorem 1.1: Fundamental Theorem of Arithmetic(FTA)

For every $x \in \mathbb{Z}$ with $x \neq 0$ there exists a unique factorization

$$x = (-1)^s 2^{e_2} 3^{e_3} 5^{e_5} \cdots p^{e_p} \cdots \tag{5}$$

where $s \in \{0, 1\}$, p ranges over the primes, $e_p \in \mathbb{N}$, and $e_p = 0$ for all but finitely many p.

In essence this says that -1 together with the primes 'generates' $\mathbb{Z}$ in terms of the multplication operator $\cdot$. The reason that we said $(\mathbb{Z}, \cdot)$ is infinitely generated then follows from the following classical result of Euclid:

Theorem 1.2: Euclid

There are infinitely many primes.

Or, even better,

Theorem 1.3: Euler

The sum $\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

Remark 1.2

For those who have taken some amount of algebra, Theorem 1.1 essentially says that $(\mathbb{Z}, \cdot)$, as a monoid, is $\mathbb{Z}/2\mathbb{Z}$ cross the free monoid on countably many generators.

Theorem 1.1 essentially makes all the equations in $(\mathbb{Z}, \cdot)$ fairly simple to solve. Namely, all such equations are (essentially) of the form

$$x_1^{m_1} \cdots x_n^{m_n} = b \tag{6}$$

with $n \in \mathbb{N}$, $m_1, \ldots, m_n \in \mathbb{N}$, and $b \in \mathbb{Z}$. Using Theorem 1.1 these equations have fairly simple algorithmic solutions.

Remark 1.3

There is no reason to expect that the algorithms to solve equations like (6) are going to be fast though since, in essence, they all will involve prime factorizing b.

For example:

Example 1.4

The equation $x^4y^{12} = 1024$ has no solution. Indeed, if we denote by $m_2(x)$ the power of 2 in the prime factorization of x, and $m_2(y)$ the power of 2 in the prime factorization of y, then since $1024 = 2^{10}$ we can use Theorem 1.1 to conclude that $4m_2(x) + 12m_2(y) = 10$. But, this is impossible since $m_2(x), m_2(y)$ are non-negative integers.

1.2.3 Putting the two together

Things when difficult when one wants to study $(\mathbb{Z}, \cdot, +)$ as a whole. To measure the difficulty of considering both operations simultaneously we can, as we did above, consider their equations, which we give special name. Before we do this though, recall that if $v \in \mathbb{N}^*$ then $\mathbb{Z}[x_1, \ldots, x_v]$ denotes the set of polynomials in the variables $x_1, \ldots, x_v$ with integer coefficients.

We then have the following definition:

Definition 1.4

A *Diophantine equation* is an equation of the form

$$f(x_1, \ldots, x_v) = 0 \tag{7}$$

where $v \in \mathbb{N}^*$ and $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_v]$. A *solution* to a Diophantine equation is a tuple $(a_1, \ldots, a_n)$ of integers such that $f(a_1, \ldots, a_n) = 0$. Let us denote the set of solutions to the Diophantine equation (7) by $X_f(\mathbb{Z})$.

In other words, Diophantine equations are just integer solutions to (multi-variable) integer polynomials.

Example 1.5

The equation $5x^2 - 2x + 1 = 0$ is a Diophantine equation.

Example 1.6

The equation $x^2 + y^2 - z^2 = 0$ is a Diophantine equation. It has infinitely many solutions (e.g. $(3, 4, 5)$).

Example 1.7

More generally the equation $x^n + y^n - z^n = 0$ (the so-called *Fermat equation*) is a Diophantine equation. It has no solutions if $n \geqslant 3$ except dumb ones (e.g. $5^7 + 0^7 - 5^7 = 0$) which is the aforementioned result from Example 1.1.

Example 1.8

The equation $x^2 + y^2 = 17$ is a Diophantine equation. It has solutions (e.g. $4^2 + 1^2 = 17$).

As we said before, to give one indication about why the study of $(\mathbb{Z}, +, \cdot)$ is so much harder than $(\mathbb{Z}, \cdot)$ and $(\mathbb{Z}, +)$ individually, we can compare the difficulty of solving their equations. For example, we saw that equations in $(\mathbb{Z}, \cdot)$ and $(\mathbb{Z}, +)$ were easy to solve. In comparison:

Theorem 1.4: Hilbert's tenth problem, Matiyasevich-Robinson-Davis-Putnam

There is no algorithm to determine whether or not a given Diophantine equation has a solution. More precisely, there is no algorithm that will take as input $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$ and output 0 if $X_f(\mathbb{Z}) = \varnothing$ and output 1 if $X_f(\mathbb{Z}) \neq \varnothing$.

Even with Theorem 1.4 being said, we can now roughly state the goal of this course as follows:

Goal 1.1: for the course (rough)

Develop basic techniques to analyze the existence of solutions to Diophantine equations (and, occasionally, develop algorithms to parameterize solutions).

Considering the difficulties mentioned in the solution to Fermat's equation (as in Example 1.1) and Theorem 1.4 it's shocking that unless we narrow the scope of our goal we will be categorically doomed. Thus, we will need to reign ourselves in a little bit.

To do this, let us first make the following definition:

Definition 1.5

Let $v \in \mathbb{N}^*$. An *integral v-ary quadratic form* is a polynomial of the following type:

$$q(x_1, \ldots, x_v) = \sum_{i,j=1}^{v} a_{i,j} x_i x_j \tag{8}$$

where $a_{i,j} \in \mathbb{Z}$.

In other words, one can think of quadratic forms as something like 'quadratic polynomials with integer coefficients in multiple variables'.

Example 1.9

The polynomial $q(x) = 7x^2$ is a unary quadratic form.

Example 1.10

The polynomial $q(x, y) = 4x^2 - 5xy + 2y^2$ is a binary quadratic form.

Example 1.11

The polynomial $q(x, y, z) = 4x^2 + 5xz - 8yz + 8z^2$ is a trinary quadratic form.

Example 1.12

Let $n \in \mathbb{Z}$. Let $q_n(x, y) := x^2 + ny^2$. Then, q_n is a binary quadratic form.

Let us then make the following definition:

Definition 1.6

Let $q(x_1, \ldots, x_v)$ be an integral v-ary quadratic form. We say that q *represents* the integer c if the Diophantine equation

$$q(x_1, \ldots, x_v) = c \tag{9}$$

has a solution.

So, we can then describe the more reasonable goal for this course as follows:

Goal 1.2: for the whole course

Study integral quadratic forms q with a focus on deciding which integers q represents—with an even more special interest in the case $v = 2$ (i.e. binary integral quadratic forms).

Let us give some sample theorems to help clarify the type of problems we'll be considering:

Theorem 1.5

Let p be an odd prime number. Then:

1. If $n = 1$ then p is represented by q_n if and only if $p = 4k + 1$ for some $k \in \mathbb{Z}$.
2. If $n = 2$ then p is represented by q_n if and only if $p = 8k + 1$ or $p = 3 + 8k$ for some $k \in \mathbb{Z}$.
3. If $n = 5$ then p is represented by q_n if and only if $p = 1 + 20k$ or $9 + 20k$ for some $k \in \mathbb{Z}$.

Theorem 1.6

Let p be a prime number. Then, the Diophantine equation $2x^2 + 2xy + 3y^2 = p$ has a solution if and only if p can be written in the form $3 + 20k$ or $7 + 20k$ for some $k \in \mathbb{Z}$.

Theorem 1.7: Legendre's theorem

Let $a, b, c \in \mathbb{Z}$. Then, whether $ax^2 + by^2 + cz^2 = 0$ has a non-zero solution can be determined algorithmically.

Theorem 1.8: Legendre's four square theorem

Let $n \in \mathbb{N}$. Then, the Diophantine equation $x^2 + y^2 + z^2 + w^2 = n$ has a solution.

Theorem 1.9: Legendre's three square theorem

Let $n \in \mathbb{N}$. Then, the Diophantine equation $x^2 + y^2 + z^2 = n$ has a solution if and only if n is not of the form $4^\ell(8k + 7)$ for $\ell \in \mathbb{N}$ and $k \in \mathbb{Z}$.

The above theorems are meant to seem both interesting, but also mysterious. For example, why can we deal with $x^2 + 5y^2$ but not $x^2 + 14y^2$? Why is the three square theorem so much more intricate than the four square theorem? By the end of course these questions will (hopefully) be satisfactorily answered for you. Keep these concrete questions in mind as we are developing the general machinery given in Goal 1.1.

1.3 Exercises

Exercise 1.1

Problem: Prove Theorem 1.1 assuming that prime is the same thing as irreducible.

Solution: Let us prove the existence first. Assume that $x > 0$. If x is prime we're not done. Else (as we'll prove next time!) we can factor $x = ab$ with $a, b \in \mathbb{Z}$, and $x > a, b > 0$. If a and b are both prime we're done. Else we can factorize them. This process must terminate since at every step the numbers are getting smaller and there are only finitely many integers in the interval $[0, x]$.

Let's now prove uniqueness. Suppose that

$$(-1)^s 2^{m_2} 3^{m_3} \cdots = (-1)^t 2^{n_2} 3^{n_3} \cdots \tag{10}$$

we need to prove that $s = t$ and $m_p = n_p$ for all primes p. Evidently $s = t$ since this is determined by the sign. Let's now prove that $m_p = n_p$ for all arbitrary, but fixed, primes p. We may assume without loss of generality that $m_p \geqslant n_p \geqslant 0$. Then, by dividing both sides by p^{n_p} if necessary, we may assume that $m_p \geqslant n_p = 0$. So, it suffices to show that this implies that $m_p = 0$. If $m_p > 0$ then p divides the left hand side of (10). Then, it must also divide the right hand side. But, by definition of primes this implies that it must divide one of the factors in the right hand side factorization. But, all the factors on the right hand side are of the form q^{n_q} with $n_q > 0$. If $q \neq p$ then $p \nmid q^{m_q}$ since, again by primality, this implies that $p \mid q$ which, since q is prime, implies that $q = p$ which is a contradiction. Since we assumed that $n_p > 0$ we know that p does not show up. Thus, p does not divide the right hand side, which is a contradiction.

Exercise 1.2

Problem: The goal of this exercise is to see why our definition of prime as in Definition 1.3 is the correct one (even though it's equivalent to the more naive definition of being unfactorizable). Namely, let's give a different situation where the more naive definition doesn't agree with the one from Definition

1.3 and then see that in this situation unique factorization doesn't hold.

Denote by $\mathbb{E}$ the set of even positive integers. Call an element $x \in \mathbb{E}$ *irreducible* if one cannot write $x = ab$ with $a, b \in \mathbb{E}$ and call it *prime* if $x \mid ab$, for $a, b \in \mathbb{E}$, implies that $x \mid a$ or $x \mid b$.

1. Show that every element of $\mathbb{E}$ has a factorization into irreducibles.
2. Show that 2, 6, and 18 are irreducible. Deduce that $\mathbb{E}$ does not have unique factorization into irreducibles.
3. What are the primes of $\mathbb{E}$?
4. Which elements of $\mathbb{E}$ have unique factorization into primes?

Solution:

1. The exact same argument that we used for the existence of prime factorization works. If x is not irreducible it factors. This process must terminate in finite time.
2. All of these numbers have a single factor of 2. Therefore, by Theorem 1.1, any factorization in $\mathbb{Z}$ would involve an odd term, and thus not be a factorization in $\mathbb{E}$. Since $18 \cdot 2 = 6 \cdot 6$ this shows that $\mathbb{E}$ doesn't have unique factorization into irreducibles.
3. The only primes in $\mathbb{E}$ are those of the form 2 and $2p$ with p an odd prime of $\mathbb{Z}$. To see that these are prime suppose that $2p \mid ab$ with $a, b \in \mathbb{E}$. Since p is a prime of $\mathbb{Z}$ we know that $p \mid a$ or $p \mid b$. Since a and b are both in $\mathbb{E}$ this implies that $2p \mid a$ or $2p \mid b$. Thus, $2p$ is prime. Suppose that $x \in \mathbb{E}$ is not of this form. We can then write it as $2^r p^s n^t$ where p is an odd prime, and $n > 1$ is a positive number with no factor of p. Note first that $r = 1$. Indeed, if $r > 1$ then we can factor x in $\mathbb{E}$ as $2 \cdot 2^{r-1} p^s n^t$ and since x divides neither of these factors it is not prime. Thus, $r = 1$. Note then that x divides $(2p^s)(2n^t)$ but doesn't divide either factor. Thus, x is not prime.
4. By the previous part it's clear that $x \in \mathbb{E}$ has a factorization into primes if and only if $x = 2^a p_1^{m_1} \cdots p_n^{m_n}$ where p_i are odd primes and $a > m_1 + \cdots + m_n$.

Exercise 1.3

Problem: Let $n = -7$. Is 11 represented by q_n?

Solution: It has no solutions! Not at all obvious. We'll see a solution to this in Example 5.13 by applying Example 5.7.

2 Lecture 2: Linear Diophantine equations, GCD, and the Euclidean algorithm

2.1 Setup

We start today with solving our first class of Diophantine equations and, as eluded to earlier, the only class of Diophantine equations which can be solved 'elementarily' (but not 'simply' since it will require some serious thinking!):

Definition 2.1

A *non-homogenous linear Diophantine equation* is a Diophantine equation of the form

$$a_1x_1 + \cdots + a_nx_n = c \tag{11}$$

where $n \in \mathbb{N}^*$ and $a_1, \ldots, a_n, c \in \mathbb{Z}$.

In other words, if we think of Diophantine equations as polynomials with integer coefficients, these are Diophantine equations whose polynomial has 'degree 1'.

Example 2.1

The Diophantine equation $3x + 5y - 2z = 12$ is an example of a non-homogenous linear Diophantine equation.

Our immediate goal, that will take this class and the next, is the following:

Goal 2.1

Give an algorithm to decide whether or not a given non-homogenous linear Diophantine equation has a solution and,if it does, have a solution give an algorithm to find all such solutions.

Again, while we will be able to complete this goal in two lectures, this problem is deceptively simple, and took mathematicians hundreds of years to fully understand.

In terms of 'real world' problems, non-homogenous linear Diophantine equations usually arise in the context of 'making exact change', as the following example illustrates:

Example 2.2

Your mother has 68,300 points on her supermarket rewards card and tells you to go to the store to buy as much beans, rice, and beef as you can. A can of beans costs 3,600 points, a bag of rice costs 6,000 points, and a package of beef costs 14,000 points. Can you spend all of your mom's points and avoid her ire?

It's clear that one can phrase this as to whether or not the non-homogenous linear Diophantine equation

$$3,600x + 6,000y + 14,200z = 68,300 \tag{12}$$

has a solution with x, y, z *positive* integers.

So, does it have a solution? The answer is no! Indeed, if $x, y, z, \in \mathbb{Z}$ (let alone if x, y, z were positive integers) satisfying (12) then since 200 divides the left hand side (since it clearly divides the coefficients) it would have to divide the right hand side, and it doesn't.

The fact that divisibility came up in the solution to the above problem is not a fluke. In fact, as we will see later, it has everything to do with solving (11).

2.2 Ideals and the division algorithm

Our goal today will be to give an abstract, simple way to partially fulfill the goal of Goal 2.1. The next class will then be spent explaining how to make things more concrete and fully fulfill Goal 2.1.

To motivate this abstract perspective, we wish to shift perspectives in the study of the equation (11). Namely, let's fix $a_1, \ldots, a_n$ as in the equation, but instead of fixing c and asking whether the equation has a solution let us, instead, flip the script and try to describe the whole set S of c's for which (11) has a solution.

Then, whether or not (11), for fixed c, has a solution will come down to a question of whether c is in S or not.

Remark 2.1

This shift in perspective from fixed c to varying c will be a theme throughout our course.

To put all of this in the correct framework, let us make the following definition:

Definition 2.2

A non-empty subset $I \subseteq \mathbb{Z}$ is called an *ideal* if it satisfies the following conditions:

1. If $x, y \in I$ then $x + y \in I$.
2. If $x \in I$ and $z \in \mathbb{Z}$ is arbitrary, then $zx \in I$.

Example 2.3

The set of even numbers is an ideal. Indeed, if x and y are even, then $x + y$ is even. If x is even and z is an arbitrary integer, then zx is even.

Example 2.4

The set of odd numbers is not an ideal. In fact, both properties of an ideal fail. For example, 1 is odd and 3 is odd but $4 = 1 + 3$ is not odd. Also, 3 is odd, and $2 \in \mathbb{Z}$, but $6 = 2 \cdot 3$ is not odd.

Example 2.5

The set $\{0\}$ is an ideal called the *zero ideal*.

In fact, here is a general method to make ideals:

Definition 2.3

Let $n \in \mathbb{N}^*$ and $a_1, \ldots, a_n \in \mathbb{Z}$. The *ideal generated by* $a_1, \ldots, a_n$, denoted $(a_1, \ldots, a_n)$, is the following subset of $\mathbb{Z}$:

$$(a_1, \ldots, a_n) := \{a_1 x_1 + \cdots + a_n x_n : x_1, \ldots, x_n \in \mathbb{Z}\} \tag{13}$$

Let us note then the following basic fact:

Lemma 2.1

Let $n \in \mathbb{N}^*$ and $a_1, \ldots, a_n \in \mathbb{Z}$. Then, $(a_1, \ldots, a_n)$ is an ideal.

Example 2.6

If $n = 1$, so we just have a single integer a, then (a) is just the set of multiples of a. So, for example, the ideal of even numbers from Example 2.3 is just the ideal (2).

Example 2.7

We claim that the ideal $(2, 3)$ is just all of $\mathbb{Z}$. Indeed, note that $3 - 2 = 1 \in (2, 3)$. But, since $(2, 3)$ is an ideal, this means that for any $z \in \mathbb{Z}$ we have that $z \cdot 1 = z \in (2, 3)$. Thus, $(2, 3) = \mathbb{Z}$.

The relevance of ideals to solving (11) now becomes clear. Namely, it's almost definitional that the ideal $(a_1, \ldots, a_n)$ is precisely the set of $c \in \mathbb{Z}$ such that (11) has a solution. Thus, a partial answer to Goal 2.1 will be to describe the sets $(a_1, \ldots, a_n)$ (it's not the full answer since we haven't given an algorithm to produce all the solutions).

Even though ideals look like incredibly scary objects, the fundamental result which typifies much of the basic properties of $\mathbb{Z}$ is the following:

Theorem 2.1

Let $I \subseteq \mathbb{Z}$ be a non-zero ideal. Let $d \in I$ be the smallest positive element of I. Then, $I = (d)$.

In other words, even though ideals seem like they could be arbitrarily crazy sets, they in fact all look like multiples of a fixed number. In particular, even though the ideal $(a_1, \ldots, a_n)$ looks like it needs n numbers (i.e. $a_1, \ldots, a_n$) to describe it, one only needs one number (more on this number later).

The proof of Theorem 2.1 is actually incredibly simple, and relies on the following 'trivial' result:

Theorem 2.2: Division algorithm

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then, there exists a unique $q \in \mathbb{Z}$ and a unique $r \in \mathbb{N}$ with $r < |b|$ such that

$$a = qb + r \tag{14}$$

We often call q in Theorem 2.2 the *quotient* of a by b and r the *remainder*. In words, this theorem says that while b might not divide a, in other words the equation $a = bx$ might not have a solution, there is always a 'best' approximate solution q and a bound on the error (i.e. a bound on how far q is from being an actual solution to $a = bx$).

Let's now see why Theorem 2.1 holds:

Proof 2.1: Theorem 2.1

Let I be an ideal, and let d be the smallest positive integer in I. Note then that for any other $x \in I$ one can use Theorem 2.2 to write $x = qd + r$ for some $q \in \mathbb{Z}$ and some $r \in \mathbb{N}$ with $r < d$. Now, since $d \in I$ we have that $-qd \in I$ by the second property of ideals and since $x \in I$ the first property of ideals this implies that $x + (-qd) \in I$. But, $x - qd = r$, so $r \in I$. If $r > 0$ then r would be a positive element

of I smaller than d, which is a contradiction. Thus, $r = 0$ and so $x = qd$. Thus, every element of I is a multiple of d and so $I \subseteq (d)$. But, evidently $(d) \subseteq I$. So, $I = (d)$ as desired.

In particular, from the above we know that given $a_1, \ldots, a_n \in \mathbb{Z}$ we know that the set of $c \in \mathbb{Z}$ such that (11) has a solution is precisely the multiples of some fixed integer d. Thus, to give a satisfactory description of the c for which (11) has a solution, it suffices to give a more concrete description of this integer d.

2.3 Divisibility and the GCD

As we noted after Example 2.2 the solution to whether it was possible to spend all your mom's points on beef, rice, and beans had something to do with the divisibility properties of the prices and the money you were given. This might key one off to the fact that maybe the d such that $(a_1, \ldots, a_n) = (d)$ has something to do with the divisibility properties of the a_i.

To flesh out this idea, let's make the following definition:

Definition 2.4

If $a \in \mathbb{Z}$ the *set of divisors* of a, denoted $\mathrm{Div}(a)$, is the set of $d \in \mathbb{Z}$ such that $d \mid a$. An element of $\mathrm{Div}(a)$ is called a *divisor* of x. Similarly, if $a_1, \ldots, a_n \in \mathbb{Z}$ then the set of *common divisors of* $a_1, \ldots, a_n$, denoted $\mathrm{Div}(a_1, \ldots, a_n)$, is the set of $d \in \mathbb{Z}$ such that $d \mid a_i$ for $i = 1, \ldots, n$. In other words:

$$\mathrm{Div}(a_1, \ldots, a_n) := \mathrm{Div}(a_1) \cap \cdots \cap \mathrm{Div}(a_n) \tag{15}$$

We call an element $d \in \mathrm{Div}(a_1, \ldots, a_n)$ a *common divisor* of $a_1, \ldots, a_n$.

Example 2.8

One has that $\mathrm{Div}(18) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9\}$.

Example 2.9

One has that $\mathrm{Div}(18, 15) = \{\pm 1, \pm 3\}$.

Example 2.10

One has that $\mathrm{Div}(12, 28, 20) = \{\pm 1, \pm 2, \pm 4\}$

Inspecting the above examples reveals the following pattern. In all the cases, there is a single element $d \in \mathrm{Div}(a_1, \ldots, a_n)$ such that $\mathrm{Div}(a_1, \ldots, a_n)$ is just $\mathrm{Div}(d)$. Let's try to formalize such an element as follows:

Definition 2.5

Let $n \in \mathbb{N}^*$ and $a_1, \ldots, a_n \in \mathbb{Z}$. The *greatest common divisor*, denoted by $\gcd(a_1, \ldots, a_n)$, is the unique positive divisor d of $a_1, \ldots, a_n$ with the property that if $d' \in \mathrm{Div}(a_1, \ldots, a_n)$ then $d' \mid d$.

In other words, the greatest common divisor of $a_1, \ldots, a_n$, is precisely a common divisor d such that the equality $\mathrm{Div}(a_1, \ldots, a_n) = \mathrm{Div}(d)$ holds.

It will be helpful to make the following definition:

Example 2.11

Let $n \in \mathbb{N}^*$ and $a_1, \ldots, a_n \in \mathbb{N}$. We say that the integers a_i are *coprime* if $\gcd(a_1, \ldots, a_n) = 1$ and we say that the a_i are *pairwise coprime* if $\gcd(a_i, a_j) = 1$ for all $i \neq j$.

Example 2.12

One has that $\gcd(18, 15) = 3$.

Example 2.13

The integers 12, 10, and 15 are coprime but not pairwise coprime.

Another description of the greatest common divisor is given as follows:

Lemma 2.2

Let $n \in \mathbb{N}^*$ and $a_1, \ldots, a_n \in \mathbb{N}$. Then, $\gcd(a_1, \ldots, a_n)$ is the largest positive common divisor of $a_1, \ldots, a_n$.

Now, while the above is all fine and good, there is a tiny, teensy-weensy issue: it's not obvious that the greatest common divisor exists. Why *should* there be always be a positive $d \in \mathrm{Div}(a_1, \ldots, a_n)$ such that $\mathrm{Div}(a_1, \ldots, a_n) = \mathrm{Div}(d)$?

The key is the following observation:

Theorem 2.3

Let $n \in \mathbb{N}^*$ and $a_1, \ldots, a_n \in \mathbb{Z}$. Then,

$$(a_1, \ldots, a_n) = (\gcd(a_1, \ldots, a_n)) \tag{16}$$

In other words, the d from Theorem 2.1 for $I = (a_1, \ldots, a_n)$ is precisely $\gcd(a_1, \ldots, a_n)$!

Proof 2.2: Theorem 2.3

We know from Theorem 2.1 that if d is the smallest positive integer in $(a_1, \ldots, a_n)$ that the equality $(a_1, \ldots, a_n) = (d)$ holds. Thus, it suffices to show that $d = \gcd(a_1, \ldots, a_n)$. Let's begin by observing that $d \in \mathrm{Div}(a_1, \ldots, a_n)$. Indeed, since each $a_i \in (a_1, \ldots, a_n) = (d)$ and (d) is the set of multiples of d we have that $d \mid a_i$ for all i. Next, we need to show that if $d' \mid a_i$ for all i, then $d' \mid d$. But, if $d' \mid a_i$ for all i, then for any $x_1, \ldots, x_n \in \mathbb{Z}$ we have that $d' \mid a_1 x_1 + \cdots + a_n x_n$. In particular, $d' \mid x$ for all $x \in (a_1, \ldots, a_n)$. Since $d \in (a_1, \ldots, a_n)$ this implies that $d' \mid d$. Thus, $d = \gcd(a_1, \ldots, a_n)$ as desired.

As a corollary, we get the following description of the solutions to (11):

Corollary 2.1

Let $n \in \mathbb{N}^*$ and $a_1, \ldots, a_n \in \mathbb{Z}$. Then, for $c \in \mathbb{Z}$ the Diophantine equation

$$a_1 x_1 + \cdots + a_n x_n = c \tag{17}$$

has a solution if and only if $\gcd(a_1, \ldots, a_n) \mid c$.

We also get the following useful corollary:

Corollary 2.2: Bezout's lemma

Let $a, b \in \mathbb{Z}$. Then, the Diophantine equation $ax + by = \gcd(a, b)$ has a solution.

Let us see some examples:

Example 2.14

The Diophantine equation $12x + 5y - 22z = 8$ has a solution. Indeed, $\gcd(12, 5, 22) = 1$ and $1 \mid 8$.

Example 2.15

The Diophantine equation $2x + 6y + 8z = 11$ has no solution since $\gcd(2, 6, 8) = 2$ and $2 \nmid 11$.

We can soup up Corollary 2.1 as follows:

Theorem 2.4

Let $a, b \in \mathbb{Z}$. Then, $ax + by = c$ has a solution if and only if $\gcd(a, b) \mid c$. Given a solution (x_0, y_0) to $ax + by = c$, all other solutions to the equation are of the form

$$\left(x_0 + m\frac{b}{\gcd(a,b)}, y_0 - m\frac{a}{\gcd(a,b)} \right) \tag{18}$$

for some $m \in \mathbb{Z}$.

Proof 2.3

Let us begin by verifying that all numbers of the form indicated in (18) are, in fact, solutions. By definition we know that

$$ax_0 + by_0 = c \tag{19}$$

then

$$\begin{aligned} a\left(x_0 + m\frac{b}{\gcd(a,b)}\right) + b\left(y_0 - m\frac{a}{\gcd(a,b)}\right) &= ax_0 + m\frac{ab}{\gcd(a,b)} + by_0 - m\frac{ab}{\gcd(a,b)} \\ &= c + 0 \\ &= c \end{aligned} \tag{20}$$

Moreover, suppose that (x_1, y_1) is another solution to $ax + by = c$. Note then that, by definition, we have that

$$ax_0 + by_0 = c = ax_1 + by_1 \tag{21}$$

thus

$$a(x_0 - x_1) = -b(y_1 - y_0) \tag{22}$$

and dividing through by $\gcd(a, b)$ gives

$$\frac{a}{\gcd(a,b)}(x_0 - x_1) = -\frac{b}{\gcd(a,b)}(y_1 - y_0) \tag{23}$$

But, since $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$ are coprime (see Exercise 2.1), we deduce that (23) implies that there exists some m such that $x_0 - x_1 = m\frac{b}{\gcd(a,b}$ and $y_1 - y_0 = -m\frac{a}{\gcd(a,b)}$. The conclusion follows.

The goal for next time will then be to describe an algorithm to produce an initial solution (x_0, y_0) as in Theorem 2.4. We also note that there are similar descriptions to Theorem 2.4 for more than two variables. They are no more conceptually difficult, but a little notationally cumbersome, so we don't discuss them here.

2.4 Exercises

Exercise 2.1

Problem: Use Corollary 2.2 to show that if $d := \gcd(a, b)$ then $\frac{a}{d}$ and $\frac{b}{d}$ are coprime.

Solution: By Corollary 2.2 we have that $ax + by = d$ has a solution, say (x_0, y_0). Note then that by dividing through by d we have that

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = 1 \tag{24}$$

But, this implies that $1 \in \left(\frac{a}{d}, \frac{b}{d}\right)$ which means, by Theorem 2.3, that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) \mid 1$ from where the conclusion follows.

Exercise 2.2

Problem: Let us now show that a positive $p \in \mathbb{Z}$ is prime (in the sense of Definition 1.3) if and only if it's irreducible (in the sense that $\mathrm{Div}(p) = \{\pm 1, \pm p\}$) using Corollary 2.2, and thus completing our proof of Theorem 1.1 carried out in Exercise 1.1:

1. Begin by showing that prime implies irreducible.
2. Suppose now that p is irreducible and that $p \mid ab$. We want to show that $p \mid a$ or $p \mid b$. Do this as follows:

(a) Assume that $p \nmid a$ and $p \nmid b$. Show that $\gcd(p, a) = \gcd(p, b) = 1$.

(b) Use Corollary 2.2 to deduce that there exists $x, y \in \mathbb{Z}$ such that $px + ay = 1$ and $x', y' \in \mathbb{Z}$ such that $px' + by' = 1$.

(c) Deduce that if $p \nmid a$ and $p \nmid b$ then $p \nmid ab$ (hint: multiply the two equations from (b)).

Solution:

1. Suppose that p is prime. Let $p = ab$ be any factorization of p. Since p is positive we may assume without loss of generality that a and b are positive. Since p is prime we have that $p \mid a$ or $p \mid b$. But, since $a, b \leqslant p$ this implies that $p = a$ or $p = b$. The conclusion follows.

2.

(a) If $p \nmid a$ then $\pm p \notin \mathrm{Div}(a)$. Since $\mathrm{Div}(p) = \{\pm 1, \pm p\}$ we conclude that $\mathrm{Div}(p) \cap \mathrm{Div}(a) = \{\pm 1\}$ so that evidently $\gcd(p, a) = 1$. The same holds for $\gcd(p, b) = 1$.

(b) This follows immediately from Corollary 2.2.

(c) Assume that $p \nmid a$ and $p \nmid b$. From (a) we know that this implies that $\gcd(a, p) = \gcd(b, p) = 1$. Thus, by (b) we can find $x, y, x', y' \in \mathbb{Z}$ such that $px + ay = 1 = px' + by'$. Thus,

$$1 = (px + ay)(px' + by') = p^2xx' + pbxy' + apyx' + abxy' \tag{25}$$

If $p \mid ab$, then p evidently divides all the summands on the right hand side of (25) and thus divides the left hand side, which is 1. This is impossible. Thus, $p \nmid ab$ as desired.

3 Lecture 3: Linear Diophantine equations, GCD, and the division algorithm (contd.)

We have now, in Theorem 2.4, give a full description of which $c \in \mathbb{Z}$ does the equation $ax + by = c$ have a solution to, and how to paramaterize all the solutions given an initial one (x_0, y_0). Thus, to fully fulfill Goal 2.1 we need only give an algorithm to produce such an initial solution (x_0, y_0) and that is the goal of today.

3.1 The Euclidean algorithm

To begin, let us note that if $ax + by = c$ has a solution, then $\gcd(a, b) \mid c$, say $c = \gcd(a, b)z$. Then, if we have an initial solution (x_0, y_0) to $ax + by = \gcd(a, b)$ then we get an initial solution (zx_0, zy_0) to $ax + by = c$. Thus, it really suffices to give an algorithm to find an initial solution to $ax + by = \gcd(a, b)$.

To do this, it will be helpful to make the following definition:

Definition 3.1

Let $a, b \in \mathbb{Z}$. Iteratively define a set of integers q_k and r_k for $k \geqslant -2$ as follows. Set $r_{-2} = a$ and $r-1 = b$. Then define r_k and q_k for $k \geqslant 0$ by applying the division algorithm

$$r_{k-2} = q_k r_{k-1} + r_k \tag{26}$$

where q_k is the quotient and r_k the remainder of dividing r_{k-2} by r_{k-1}.

Note that for all $k \geqslant -2$ we have that $r_k \geqslant 0$ and either $r_{k+1} \geqslant r_k$ with $r_{k+1} = r_k$ if and only if $r_k = 0$. In particular, we see that in finitely many steps r_k becomes zero. Define N as follows:

$$N := \max\{k : r_k > 0\} \tag{27}$$

So, in particular, we see that $r_{N+1} = 0$.

We then have the following beautiful claim:

Theorem 3.1: Euclidean algorithm

Let $a, b \in \mathbb{Z}$ and let r_N be defined as above. Then, $r_N = \gcd(a, b)$.

Proof 3.1

Let us begin by noting that for all $k \geqslant -2$ we have that $r_k \in (a, b)$. Indeed, this holds true $r_{-2} = a$ and $r_{-1} = b$ and equation (26) shows that $r_k \in (a, b)$ by applying Lemma 2.1. Thus, in particular, we see that $r_N \in (a, b)$.

We now claim that $r_N = \gcd(a, b)$. Let us write $d := \gcd(a, b)$. To do this we begin by showing that $d \mid r_N$. In fact, $d \mid r_k$ for all $k \geqslant -2$. This follows by induction since it holds for the base cases $k = -2$ and $k = -1$ and the inductive step is clear from (26). Conversely, we claim that $r_N \mid a$ and $r_N \mid b$. In fact, we claim that $r_N \mid r_k$ for all $k \geqslant -2$. But, this is just some sort of backwards induction. By assumption we know that the process terminated at N, we know that $r_{N-1} = q_N r_N$. This implies that $r_N \mid r_{N-1}$. But, we know that

$$r_{N-2} = q_{N-1} r_{N-1} + r_N \tag{28}$$

Since r_N divides both terms on the right, it divides the term on the left. Continuing this process iteratively shows that $r_N \mid r_k$ for all $k \geqslant -2$ and, in particular, r_N divides $r_{-2} = a$ and $r_{-1} = b$. In particular, $r_N \mid \gcd(a, b) = d$.
Since d and r_N are positive integers that divide each other, they are equal.

The above process is called the *Euclidean algorithm*. At first glance what it really does is give an algorithm to find $\gcd(a, b)$, but, in fact, by back substituting it also gives an algorithm to find an initial solution to the equation $ax + by = \gcd(a, b)$.

Let's do an example:

Example 3.1

Let's find $\gcd(1071, 462)$ and a solution to the equation $1071x + 462y = \gcd(1071, 462)$.

So, let us set $a = r_{-2} = 1071$ and $b = r_{-1} = 462$. The first step of the algorithm tells us that we should find the division of 1071 by 462 with remainder. One easily finds that

$$1071 = 2 \cdot 462 + 147 \tag{29}$$

thus $r_0 = 147$. Next, we need to find the division of 462 by 147. One quickly finds that

$$462 = 3 \cdot 147 + 21 \tag{30}$$

and so we set $r_1 = 21$. Next we need to find the division of 147 by 21, which one checks is

$$147 = 21 \cdot 7 + 0 \tag{31}$$

and thus the process has terminated. The last non-zero r_k was 21, so we deduce that $21 = \gcd(1071, 462)$. Moreover, we note that

$$\begin{gathered} 462 = 3 \cdot 147 + 21 \\ \Downarrow \\ 21 = 462 - 3 \cdot 147 \end{gathered} \tag{32}$$

and

$$\begin{aligned} 1071 &= 2 \cdot 463 + 147 \\ &\Downarrow \\ 147 &= 1071 - 2 \cdot 462 \end{aligned} \tag{33}$$

and combining these shows that

$$\begin{aligned} 21 &= 462 - 3 \cdot 147 \\ &= 462 - 3 \cdot (1071 - 2 \cdot 462) \\ &= 462 - 3 \cdot 1071 + 6 \cdot 147 \\ &= 7 \cdot 462 - 3 \cdot 1071 \end{aligned} \tag{34}$$

Thus, the equation $1071x + 462y = 21$ has the solution $x = -3$ and $y = 7$.

One can soup this up to work for more than two variables and so give an initial solution to any equation as in (11). To do this, one can perform the above process iteratively and using the following fact:

Lemma 3.1

Let $a, b, c \in \mathbb{Z}$. Then, $\gcd(a, b, c) = (\gcd(a, b), c)$.

Formalizing how to perform the Euclidean algorithm in more than 2 variables is then a simple, albeit notationally complicated, exercise and left to the reader.

3.2 Valuations and primes

Let us now try and understand greatest common divisors in terms of Theorem 1.1 which, thanks to Exercise 2.2, is now proven in full.

Before we do this, let us first make a notational convention. Namely, writing $2^{e_2}3^{e_3}\cdots$ every time we want to discuss the prime factorization of a number is way too cumbersome. It's infinitely nicer to consider these exponents as functions of the number being factored:

Definition 3.2

Let p be a prime. Then, the *p-adic valuation*, denoted v_p, is the function

$$v_p : \mathbb{Z} - \{0\} \to \mathbb{Z} \tag{35}$$

defined so that $v_p(x)$ is the largest power or p dividing x. Similarly, define the *sign valuation*, denoted v_{sign}, to be the function

$$v_{\text{sgn}} : \mathbb{Z} - \{0\} \to \{0, 1\} \tag{36}$$

defined as follows:

$$v_{\text{sgn}}(x) := \begin{cases} 0 & \text{if} \quad x > 0 \\ 1 & \text{if} \quad x < 0 \end{cases} \tag{37}$$

By definition, the p-adic valuation is made so that the following equation holds true

$$x = (-1)^{v_{\text{sgn}}(x)} \prod_p p^{v_p(x)} \tag{38}$$

and so, in particular, allows us to talk about the exponents in the prime factorization without making new symbols to represent them. In particular, one sees that one can interpret the mapping

$$x \mapsto (v_{\text{sgn}}(x), v_2(x), v_3(x), \ldots) \tag{39}$$

as giving a bijection

$$\mathbb{Z} \to \{0,1\} \times \mathbb{N}^{\oplus \aleph_0}, \tag{40}$$

where $\mathbb{N}^{\aleph_0}$ just means all tuples $(a_1, a_2, \ldots)$ of elements of $\mathbb{N}$ such that $a_i = 0$ for all but finitely many i. This bijection (at least if we add in $\{0,1\}$ modulo 2—see next lecture) translates multiplication in $\mathbb{Z}$ into addition in $\{0,1\} \times \mathbb{N}^{\oplus \aleph_0}$ (see Lemma 3.2 part (2)).

Example 3.2

One has that $v_2(34102000000) = 7$, $v_5(34102000000) = 6$, $v_{17}(34102000000) = 2$, $v_{59}(34102000000) = 1$ and $v_p(34102000000) = 0$ for all p different from $2, 5, 17$, and 59.

One has the following basic properties of v_p:

Lemma 3.2

Let p be a prime number and $a, b \in \mathbb{Z}$. Then:

1. $v_p(a) \geqslant 0$ with $v_p(a) = 0$ if and only if $p \nmid a$.
2. $v_p(ab) = v_p(a) + v_p(b)$.
3. Suppose that $a \neq -b$, then $v_p(a+b) \geqslant \min(v_p(a), v_p(b))$.

The relationship between the p-adic valuation and the notion of greatest common divisor is given as follows:

Lemma 3.3

Let p be a prime and $a, b \in \mathbb{Z}$. Then,

$$v_p(\gcd(a,b)) = \min(v_p(a), v_p(b)) \tag{41}$$

One can intrepret this as relation two orderings under the bijection (40) (the orderings being 'divides' and 'less than or equal to').

Spurred on by Lemma 3.3 one might wonder what operation in $(\mathbb{Z}, \cdot)$ corresponds to taking the maximum of two v_p's. The answer is as follows:

Definition 3.3

Let $a, b \in \mathbb{Z}$. The *least common multiple* of a and b, denoted $\mathrm{lcm}(a,b)$, is the smallest positive integer x such that $a \mid x$ and $b \mid x$.

One then has the following basic result mirroring Lemma 3.3:

Lemma 3.4

Let p be a prime and $a, b \in \mathbb{Z}$. Then,

$$v_p(\text{lcm}(a,b)) = \max\{v_p(a), v_p(b)\} \tag{42}$$

3.3 Exercises

Exercise 3.1

Problem: Let $a, b \in \mathbb{Z}$ be fixed. Show that for any fixed $z \in \mathbb{Z}$ one has that

$$\gcd(a,b) = \gcd(a+zb, b) \tag{43}$$

Solution: It suffices to show that $(a,b) = (a+zb,b)$ by Theorem 2.3. Clearly $(a+zb,b) \subseteq (a,b)$. Moreover, $a = (a+zb) + (-z)b$ and so $a, b \in (a+zb,b)$ so that $(a,b) \subseteq (a+zb,b)$.

Exercise 3.2

Problem: Show that $\dfrac{21n+4}{14n+3}$ is a reduced fraction.

Solution: One merely notes that being a reduced fraction means that $\gcd(21n+4, 14n+3) = 1$. That said, by Exercise 3.1

$$\gcd(21n+4, 14n+3) = \gcd(7n+1, 14n+3) = \gcd(7n+1, 1) = 1 \tag{44}$$

Exercise 3.3

Problem: Prove Lemma 3.1.

Solution: Let us note that $\gcd(\gcd(a,b),c)$ divides $\gcd(a,b)$ which, in turn, divides a and b. But, $\gcd(\gcd(a,b),c)$ also divides c. Thus, $\gcd(\gcd(a,b),c)$ divides a, b, and c and thus divides $\gcd(a,b,c)$. That said, $\gcd(a,b,c)$ divides a and b, and so divides $\gcd(a,b)$. But, $\gcd(a,b,c)$ also divides c. Thus, $\gcd(a,b,c)$ divides $\gcd(\gcd(a,b),c)$. The conclusion follows.

Exercise 3.4

Problem: Let $a, b \in \mathbb{Z}$. Prove Lemma 3.3, Lemma 3.4, and show that $|ab| = \gcd(a,b)\text{lcm}(a,b)$.

Solution: To prove Lemma 3.3 it suffices to show that

$$\gcd(a,b) = \prod_p p^{\min\{v_p(a), v_p(b)\}} \tag{45}$$

Since $\min\{v_p(a), v_p(b)\}$ is smaller than or equal to $v_p(a)$ and $v_p(b)$ it's clear from Lemma 3.2 (1) that the right hand side of (45) divides both a and b, and thus divides $\gcd(a,b)$ so that applying Lemma 3.2 (1) we see that $\min\{v_p(a), v_p(b)\} \leqslant v_p(\gcd(a,b))$.

That said, again applying Lemma 3.2 (1) we see that if $d \mid a$ and $d \mid b$ that $v_p(d) \leqslant v_p(a)$ and $v_p(d) \leqslant v_p(b)$ so that $v_p(d) \leqslant \min\{v_p(a), v_p(b)\}$. Applying this to $d = \gcd(a, b)$ shows that

$$v_p(\gcd(a, b)) \leqslant \min\{v_p(a), v_p(b)\} \tag{46}$$

The conclusion of Lemma 3.3 follows.

The proof of Lemma 3.4 is essentially verbatim with 'gcd' replaced by 'lcm' and 'min' replaced by 'max'.

To prove the last claim we merely note that it suffices to show that $v_p(ab) = v_p(\gcd(a, b)\mathrm{lcm}(a, b))$ by applying Theorem 1.1 and noting that

$$v_{\mathrm{sgn}}(|ab|) = v_{\mathrm{sgn}}(\gcd(a, b)\mathrm{lcm}(a, b)) = 1 \tag{47}$$

But, using Lemma 3.2 (2) this is equivalent to showing that

$$v_p(a) + v_p(b) = v_p(\gcd(a, b)) + v_p(\mathrm{lcm}(a, b)) \tag{48}$$

But, by the previous part of the exercise this is equivalent to showing that

$$v_p(a) + v_p(b) = \min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} \tag{49}$$

but this is obvious.

Exercise 3.5

Problem: Is it true that $v_p(a + b) = \min\{v_p(a), v_p(b)\}$ always?

Solution: No, it is not always true. For example, $v_3(3 + 6) = v_3(9) = 2$ but

$$\min\{v_3(3), v_3(6)\} = \min\{1, 1\} = 1 \tag{50}$$

Exercise 3.6

Let $a, b \in \mathbb{Z}$ and let c be a positive common divisor of a and b. Then, show that

$$\gcd(a, b) = c \gcd\left(\frac{a}{c}, \frac{b}{c}\right) \tag{51}$$

Solution: Let us merely note that since $ax + by = c\left(\frac{a}{c}x + \frac{b}{c}y\right)$ that (a, b) is precisely the set of c-multiples of elements of $\left(\frac{a}{c}, \frac{b}{c}\right)$. The claim then follows from Theorem 2.3.

4 Lecture 4: Congruences

4.1 Setup

In the last two lectures we (essentially) gave a full theory for non-homogenous linear Diophantine equations. We should then move on to the next logical step: quadratic Diophantine equations or, in other words, the

study of quadratic forms. But, as stated before, the study of quadratic forms is incredibly difficult and subtle and relies on a huge amount of techniques that, themself, rely on a non-trivial amount of foundational setup.

The most pivotal portion of this foundational setup will be started today, and the techniques developed using this setup will occupy us for quite some time.

4.2 Congruences: why we need them

We are about to do something drastic. We are about to, in some sense, forget all about $\mathbb{Z}$ and, instead, focus on a different set. Because our stated goals Goal 1.1 and Goal 1.2 have been so $\mathbb{Z}$-centric (in fact, we said that number theory is the study of $\mathbb{Z}$) we should justify why we are making this drastic change.

The rough idea is that $\mathbb{Z}$ is really complicated and so instead of attacking it straight on we should it replace it by another set/object that satisfies the following properties:

1. It faithfully models $\mathbb{Z}$.
2. It is simpler to deal with.

Let us attempt to be less cryptic (but still pretty cryptic). To say that a set/object X 'faithfully models $\mathbb{Z}$' we mean that X has the property that questions about about $\mathbb{Z}$ can be turned into questions about X (this is what is meant by 'models') and, moreover, if a statements about true in $\mathbb{Z}$ then its translated statement about X is also true (this is what is meant by 'faithful').

This is kind of confusing, so let's do an example of what is meant by this in a practical situation:

Example 4.1

Let us show that the Diophantine equation $x^2 - x = 2y + 1$ has no solution. To see this let's note that the right hand side is evidently odd. Is the left hand side ever odd? Well x, being an integer, is either odd or even. Let's consider these two cases separately:

- If it's even it looks like $2z$ in which case
$$x^2 - x = 4z^2 - 2z = 2(2z^2 - z) \tag{52}$$
so that the left hand side is even.
- If x is odd it looks like $2z + 1$ in which case
$$x^2 - x = (4z^2 + 4z + 1) - (2z + 1) = 2(2z^2 + z) \tag{53}$$
so that the left hand side is even again.

Thus, no matter what, the left hand side is even, so it could never equal the right hand side. Thus this equation has no solution.

In this case $\mathbb{Z}$ was modeled by the set $X := \{\text{even}, \text{odd}\}$. But, X is not just a set. It also has a good notion of addition:
$$\text{even} + \text{even} = \text{odd} + \text{odd} = \text{even}, \qquad \text{even} + \text{odd} = \text{odd} \tag{54}$$
and multiplication:
$$\text{even} \cdot \text{even} = \text{even} \cdot \text{odd} = \text{even}, \qquad \text{odd} \cdot \text{odd} = \text{odd} \tag{55}$$
Moreover, there is a natural map
$$\mathbb{Z} \to \{\text{even}, \text{odd}\} \tag{56}$$
which, if one thinks about, preserves addition and multiplication. Thus, if $x^2 - x = 2y + 1$ had a solution with $x, y \in \mathbb{Z}$ then by looking at it under the map in (56) one would obtain a solution to $x^2 - x = 2y + 1$ with $x, y \in X$ (here one should interpet 1 and 2 as their images under $\mathbb{Z} \to X$). One can then think of the

solution in Example 4.1 as being an overly complicated way to check that $x^2 - x = 2y + 1$ doesn't have a solution in X, and thus $x^2 - x = 2y + 1$ doesn't have a solution in $\mathbb{Z}$.

Thus, in some sense, we see that $X = \{\text{even}, \text{odd}\}$ fulfills the qualities desired to 'faithfully model $\mathbb{Z}$'. Namely, we had a way of turning problems about $\mathbb{Z}$ (Diophantine equations) into problems about X (equations in X) in such a way that if the problem had a solution in $\mathbb{Z}$ (i.e. if the Diophantine equation had a solution) so then did the problem in X (i.e. the problem in X had a solution).

But, note though that Example 4.1 also shows that even if some set X 'faithfully models $\mathbb{Z}$' it's not true that you can prove something about $\mathbb{Z}$ using X:

Example 4.2

The equation $x^2 - x = 4$ has no solution in $\mathbb{Z}$, but this is not detected in $X = \{\text{even}, \text{odd}\}$ since both sides are always even.

In general, if X faithfully models $\mathbb{Z}$ then the idea is that

$$\text{True in } \mathbb{Z} \implies \text{True in } X \tag{57}$$

but it is not necessarily true that the other direction holds. Thus, using X is a good way to disprove something in $\mathbb{Z}$ (if it doesn't hold in X it can't hold in $\mathbb{Z}$) but you, in general, cannot prove things in $\mathbb{Z}$ by proving things in X. Ways of trying to reverse the stream of information are generally quite deep.

The general idea of congruences is just a souping up of Example 4.1. Namely, note that whether a number is even or odd is, can be encoded by 0 or 1, depending on what its remainder (in the sense of Theorem 2.2) is when divided by 2. There is no reason that we cannot replace 2 here by any non-zero integer m.

Here's an example when $m = 3$:

Example 4.3

The equation $x^2 - 3y^2 = 2$ has no solution in $\mathbb{Z}$. We will prove this by thinking about the possible remainder values when dividing both sides of the equation by 3. Namely, x can either have remainder $0, 1$ or 2. Regardless of which of those three values it is its remainder when you square it is (check this!) 0 or 1. Thus, the term x^2 can only have remainders 0 or 1 when divided by 3. But, $3y^2 + 2$ will clearly always have remainder 2 when divided by 3. So, $x^2 = 3y^2 + 2$ cannot have a solution.

Now, if we really only care about the remainders of numbers when divided by m, we might as well identify two integers a and b if they have the same remainder when divided by m. But, this is equivalent to the statement that $m \mid a - b$. Thus, we make the following definition:

Definition 4.1

Let $m \in \mathbb{N}^*$. Then, a and b are said to be *equal modulo* m, written $a = b \mod m$ if $m \mid a - b$.

We then have the following obvious fact:

Lemma 4.1

If $a, b \in \mathbb{Z}$ and $a = b$ then $a = b \mod m$. Moreover, equality modulo m is preserved under addition, multiplication, subtraction, ... (e.g. if $a = b \mod m$ and $c = d \mod m$ then $a + c = b + d \mod m$).

One can think of equality modulo m as being a weaker notion of equality than normal, actual equality—equality modulo m is like normal equality up to some fudge factor (a multiple of m) we choose to ignore. In other words, equality modulo m is something like 'approximate equality'. As per usual, things are usually simpler to work with approximately than actually.

Let us now make the following definition that serves the role of $\{\text{even}, \text{odd}\}$ (the case of $m = 2$) for more general m:

Definition 4.2

Let $m \in \mathbb{N}^*$. The *integers modulo* m, denoted $\mathbb{Z}/m\mathbb{Z}$, is the set $0, 1, \ldots, m-1$.

Of course, we think of $\mathbb{Z}/m\mathbb{Z}$ as being the 'set of remainders' when dividing integers in $\mathbb{Z}$ by m. We then have an obvious surjection

$$r_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \tag{58}$$

that takes $a \in \mathbb{Z}$ to $r_m(a) \in \{0, \ldots, m-1\}$ where $r_m(a)$ is its remainder when divided by m. We call this the *reduction map* modulo m. Moreover, note that the reduction map preserves addition/subtraction and multiplication when $\mathbb{Z}/m\mathbb{Z}$ is given such operations by the following:

Definition 4.3

If $x, y \in \mathbb{Z}/m\mathbb{Z}$ then $x \pm_m y := r_m(x \pm y)$ where the addition/subtraction on the right hand side is taking place in $\mathbb{Z}$. Similarly, $x \cdot_m y := r_m(x \cdot y)$.

Example 4.4

If $m = 17$ then $8 +_{17} 11 = r_{17}(19) = 2$, $8 -_{17} 11 = r_{17}(-3) = 14$, and $8 \cdot_{11} 17 = r_{17}(88) = 3$.

In practice we will drop the subscript in $\pm_m$ and $\cdot_m$ since it will be clear from context that the addition/subtraction/multiplication is taking place in $\mathbb{Z}/m\mathbb{Z}$.

Lemma 4.2

The map $r_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ satisfies

1. $r_m(x \pm y) = r_m(x) \pm r_m(y)$
2. $r_m(xy) = r_m(x) r_m(y)$
3. $r_m(1) = 1$

We will, as per usual, denote by $-a$, for $a \in \mathbb{Z}/m\mathbb{Z}$, the additive inverse of a in $\mathbb{Z}/m\mathbb{Z}$. In particular, it's clear that $-a$ is $r_m(-a)$ which is $m - a$. Note that even though the integer $-a$ is not in $\{0, \ldots, m-1\}$ its residue is, and we will often times just leave $-a$ alone, not rewriting it as $m - a$. The reason for this is that $-a$ and, in particular -1, act precisely as one would expect a 'minus one' to act with respect to addition and multiplication. For example, $-a = -1 \cdot a$, $(-1)^2 = 1$, etc.

Remark 4.1

In general, we will tend to be somewhat sloppy in distinguishing between 'a up to equality modulo

m' and $r_m(a)$. So, for example, we might say something like the following: take $4, 8 \in \mathbb{Z}/11\mathbb{Z}$, then $4 \cdot 8 = 32 = 10 \mod 11$. In other words, we took the two elements $4, 8 \in \mathbb{Z}/11$, multiplied them in $\mathbb{Z}$, and then took the result modulo 11, in essence dropping the r_{11} from the equation (i.e. just writing 32 instead of $r_{11}(32)$).

Such issues can be really confusing at first. In fact, the yoga of switching between thinking of elements of $\mathbb{Z}/m\mathbb{Z}$ as general integers and 'up to equivalence modulo m' and literal elements of $\mathbb{Z}/m\mathbb{Z}$ is key to thinking fluidly about $\mathbb{Z}/m\mathbb{Z}$.

Let us now try to sync back up with our study of $\mathbb{Z}$ and, in particular, our study of Diophantine equations. Let us begin by making the following definition:

Definition 4.4

Let m and v be elements of $\mathbb{N}^*$. The set of *polynomials modulo m in v-variables*, denoted $\mathbb{Z}/m\mathbb{Z}[x_1, \ldots, x_v]$, is the of all polynomials in the variables $x_1, \ldots, x_v$ with coefficients in $\mathbb{Z}/m\mathbb{Z}$. In particular, two such polynomials are equal if and only if their coefficients are equal in $\mathbb{Z}/m\mathbb{Z}$. We add/subtract and multiply elements of $\mathbb{Z}/m\mathbb{Z}[x_1, \ldots, x_v]$ in the normal way, except addition/subtraction and multiplication of the coefficients takes place in $\mathbb{Z}/m\mathbb{Z}$.

Example 4.5

One has that $(1 + x)^2 = 1 + x^2$ as elements of $\mathbb{Z}/2\mathbb{Z}[x]$. Indeed,

$$(1 + x)^2 = 1 + 2x + x^2 = 1 + x^2 \tag{59}$$

where the last equality holds since $2 = 0$ in $\mathbb{Z}/2\mathbb{Z}$ so $2x = 0$.

With this, we can then make the following definition:

Definition 4.5

A *Diophantine equation modulo m* is a polynomial equation of the form

$$g(x_1, \ldots, x_v) = 0 \tag{60}$$

where $v \in \mathbb{N}^*$ and $g(x_1, \ldots, x_v) \in \mathbb{Z}/m\mathbb{Z}[x_1, \ldots, x_v]$. A *solution* to a Diophantine equation modulo m is a solution in $\mathbb{Z}/m\mathbb{Z}$. When we are dealing with a Diophantine equation modulo m for some m which we don't wish to specify, we will call the equation a *modulus Diophantine equation*.

Here are some examples of modulus Diophantine equations:

Example 4.6

Let $m = 5$. Then, we could take the Diophantine equation modulo 5 given by $g(x, y) = 0$ where $g(x, y) = 4x^2 + 3y^3 - 2$. A solution to this is $(x, y) = (1, 1)$.

Example 4.7

Let $m = 11$. Then, we could take the Diophantine equation modulo 11 given by $g(x) = 0$ where $g(x) = x^2 - 1$. This has only the solutions $x = 1$ and $x = 10$.

Example 4.8

Let $m = 6$. Then, we could take the Diophantine equation modulo 6 given by $g(x) = 0$ where $g(x) = x^2 - x$. This has four solutions given by $x = 0$, $x = 1$, and $x = 3$, and $x = 4$.

Remark 4.2

As Example 4.8 shows, one must be careful in manipulating modulus Diophantine equations—normal properties of polynomials, and their solutions, needn't hold. For example, in Example 4.8 we had a polynomial of degree 2 with 4 solutions, something not possible for equations over $\mathbb{Z}$. We will see more oddities concerning polynomials modulo m, together with some patches to these weirdness, in Lecture 9.

As in the case of Diophantine equations, the following definition will be very useful to eliminate notational clutter:

Definition 4.6

Let n and v be in $\mathbb{N}^*$ and let $g(x_1, \ldots, x_v) \in \mathbb{Z}/m\mathbb{Z}[x_1, \ldots, x_v]$. Let us denote by $X_g(\mathbb{Z}/m\mathbb{Z})$ the set of all solutions in $(\mathbb{Z}/m\mathbb{Z})^v$ of the modulus Diophantine equation $g(x_1, \ldots, x_v) = 0$.

Example 4.9

Let $m = 3$ and let $g(x, y) = x^2 + 2y^2 - 3$. Then

$$X_g(\mathbb{Z}/3\mathbb{Z}) = \{(0,0), (1,1), (2,1), (1,2), (2,2)\} \tag{61}$$

To connect modulus Diophantine equations to Diophantine equations the following definition is pivotal:

Definition 4.7

Let m and v be in $\mathbb{N}^*$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Then, the *reduction modulo* m of f, denoted $r_m(f)$, is the polynomial $g(x_1, \ldots, x_v)$ obtained by reducing all the coefficients of f modulo m (i.e. applying r_m to them).

Remark 4.3

In practice we will often times not be careful in writing $r_m(f)$ and, instead, just write f. It should always be clear from context (e.g. we are trying to solve an modulo m) when this occurs.

Example 4.10

If $m = 4$ and $f(x_1, x_2, x_3) = 7x_1^2 + 33x_2^8 - 44x_1x_2x_3$ then its reduction modulo 4 is just $3x_1^2 + x_2^8$ thought of as a polynomial with coefficients in $\mathbb{Z}/4\mathbb{Z}$.

We have the following basic fact concerning the reduction of polynomials modulo m:

Lemma 4.3

Let m and v be elements of $\mathbb{N}^*$. The reduction map

$$r_m : \mathbb{Z}[x_1, \ldots, x_v] \to \mathbb{Z}/m\mathbb{Z}[x_1, \ldots, x_v] \tag{62}$$

satisfies the following properties:

1. $r_m(f_1 \pm f_2) = r_m(f_1) \pm r_m(f_2)$.
2. $r_m(f_1 \cdot f_2) = r_m(f_1) \cdot r_m(f_2)$.
3. $r_m(1) = 1$.
4. $r_m(0) = 0$.

Let us make one final notational definition:

Definition 4.8

Let v and m be in $\mathbb{N}^*$. Then, given $\mathbf{a} = (a_1, \ldots, a_v) \in \mathbb{Z}^v$ the *reduction of* $\mathbf{a}$ *modulo* m, denoted either $r_m(\mathbf{a})$ or $\mathbf{a} \mod m$, is the element $(r_m(a_1), \ldots, r_m(a_v))$ in $(\mathbb{Z}/m\mathbb{Z})^v$.

In other words, the reduction of a tuple of integers modulo m is just obtained by reducing each of its entries modulo m individually.

The upshot of all of this is the following basic fact:

Theorem 4.1

Let v and m be in $\mathbb{N}^*$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Then, the map

$$r : \mathbb{Z}^v \to (\mathbb{Z}/m\mathbb{Z})^v \tag{63}$$

restricts to a map

$$X_f(\mathbb{Z}) \to X_{r_m(f)}(\mathbb{Z}/m\mathbb{Z}) \tag{64}$$

Remark 4.4

As in Remark 4.3 we will, in practice, be sloppy and write $X_f(\mathbb{Z}/m\mathbb{Z})$ instead of $X_{r_m(f)}(\mathbb{Z}/m\mathbb{Z})$.

The important corollary of Theorem 4.2 is the following:

Corollary 4.1

Let v and m be in $\mathbb{N}^*$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. If $X_f(\mathbb{Z})$ is non-empty, then so is $X_f(\mathbb{Z}/m\mathbb{Z})$. Phrased differently, $X_f(\mathbb{Z}/m\mathbb{Z}) = \varnothing$ implies that $X_f(\mathbb{Z}) = \varnothing$.

This is the correct framework in which to phrase the claim that $\mathbb{Z}/m\mathbb{Z}$ faithfully models $\mathbb{Z}$ in terms of Diophantine equations. For example, let's use this to much more elegantly explain our solution from Example 4.3:

Example 4.11

The Diophantine equation $x^2 - 3y^2 = 2$ has no solution. Indeed, let $f(x, y) := x^2 - 3y^2 - 2$. We want to show that $X_f(\mathbb{Z}) = \varnothing$. By Corollary 4.2 it suffices to show that $X_f(\mathbb{Z}/3\mathbb{Z}) = \varnothing$. Now, the reduction of $f(x, y)$ modulo 3 is just $g(x, y) = x^2 - 2$. Let us check by hand that this has no solution $(\mathbb{Z}/3\mathbb{Z})^2$. It suffices to check that $x^2 - 2$ has no solution in $\mathbb{Z}/3\mathbb{Z}$. But, one just checks that $0^2 = 0$, $1^2 = 1$, $2^2 = 4 = 1 \mod 3$. The conclusion follows.

So, in conclusion, we see that modulus Diophantine equations provide a very powerful tool to prove the non-existence of solutions to Diophantine equations. For this reason, we have the following goal:

Goal 4.1

Develop techniques to decide whether modulus Diophantine equations have solutions.

Once we have given a satisfactory partial answer to Goal 4.1 (satisfactory for this course—still woefully unsatisfactory in general) we will then move on to the deep question of statements mimicking the converse of Corollary 4.2. Namely, be careful to note that the converse of Corollary 4.2 is not true. Namely, it is certainly possible that $X_f(\mathbb{Z}) = \varnothing$ and $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ (e.g. let $f(x) = x^2 - x - 4$ and $m = 4$). So, the converse of Corollary 4.2 will entail questions which ask under what conditions can we deduce that $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ implies that $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$.

Before ending this subsection, we make one last tiny notational definition.

Definition 4.9

Let v and m be in $\mathbb{N}^*$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Then, by a *solution* to

$$f(x_1, \ldots, x_v) = 0 \mod m \tag{65}$$

we mean a $(a_1, \ldots, a_v) \in \mathbb{Z}$ such that $f(a_1, \ldots, a_v) = 0 \mod m$.

The set of solutions to $f(x_1, \ldots, x_v) = 0 \mod m$ and the elements of $X_f(\mathbb{Z}/m\mathbb{Z})$ are essentially the same thing. Namely, $\mathbf{a} \in \mathbb{Z}^v$ is a solution to $f(x_1, \ldots, x_v) = 0$ if and only if $\mathbf{a} \mod m$ is in $X_f(\mathbb{Z}/m\mathbb{Z})$. We will often conflate the two notions. The reason this notation is useful is just that it's easier to things like 'solve $x^3 - 3y = 0 \mod 8$' than things like 'solve the equation $x^3 - 3y = 0$ with $x, y \in \mathbb{Z}/8\mathbb{Z}$', even though we will really mean the latter.

Remark 4.5

Again, the yoga of moving between thinking of solving $f(x_1, \ldots, x_v) = 0 \mod m$ and computing $X_f(\mathbb{Z}/m\mathbb{Z})$ is both pivotal and subtle. For example, one might start with some $a \in X_f(\mathbb{Z}/m\mathbb{Z})$, so $a \in \mathbb{Z}/m\mathbb{Z}$, then think of a as an integer, do some operation to it, then think about its image in $\mathbb{Z}/m\mathbb{Z}$ again, and then... Special attention should be paid to making these operations seem second nature.

4.3 Moving between moduli

The last thing we want to comment on is the ability to move between different $\mathbb{Z}/m\mathbb{Z}$. Namely, we have the following basic fact:

Lemma 4.4

Let m and n be elements of $\mathbb{N}^*$ and assume that $m \mid n$. Let $a, b \in \mathbb{Z}$ be such that $r_n(a) = r_n(b)$. Then, $r_m(a) = r_m(b)$

Proof 4.1

If $r_n(a) = r_n(b)$ then this says precisely that $n \mid a - b$. Since $m \mid n$ this implies that $m \mid a - b$ so that $r_m(a) = r_m(b)$.

The reason that this lemma is important is because it makes the following definition sensical:

Definition 4.10

Let m and n be elements of $\mathbb{N}^*$ and assume that $m \mid n$. Let $x \in \mathbb{Z}/n\mathbb{Z}$. Then, the *reduction of x modulo m*, denoted $r_m(x)$ or $x \mod m$, is defined to be $r_m(a)$ for any $a \in \mathbb{Z}$ such that $r_n(a) = x$.

The content of Lemma 4.4 is that the above is well-defined in the sense that $r_m(a)$ is independent of which a such that $r_n(a) = x$ one chose. Concretely one just computes $r_m(a)$ by just pretending that a is an integer and computing $r_m(a)$ in the usual way. The reason that Lemma 4.4 is useful is the following. Recall that we will often times drop the r maps in various computations. For example, $8 \cdot 2$ in $\mathbb{Z}/9\mathbb{Z}$ might be computed as follows $8 \cdot 2 = 16 = 7 \mod 9$. The point of Lemma 4.4 is that in such a sloppy computation in $\mathbb{Z}/n\mathbb{Z}$, you can apply r_m at any time and be ok. For example, if I wanted to compute $r_3(8 \cdot 2)$ where $r_3 : \mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ I could compute $r_3(16)$ or $r_3(7)$—it makes no difference.

We have for this version of the reduction map essentially all the results and definitions we had from moving from $\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$. We now repeat them for completeness.

Firstly, we have the following properties about the reduction map:

Lemma 4.5

Let m and n be in $\mathbb{N}^*$ and suppose that $m \mid n$. The map $r_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ satisfies

1. $r_m(x \pm y) = r_m(x) \pm r_m(y)$
2. $r_m(xy) = r_m(x)r_m(y)$

3. $r_m(0) = 0$
4. $r_m(1) = 1$

We also have the notion of reduction of polynomials over $\mathbb{Z}/n\mathbb{Z}$ to polynomials over $\mathbb{Z}/m\mathbb{Z}$:

Definition 4.11

Let m, n, and v be in $\mathbb{N}^*$ and suppose that $m \mid n$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}/n\mathbb{Z}[x_1, \ldots, x_v]$. Then, the *reduction modulo* m of f, denoted $r_m(f)$, is the polynomial $g(x_1, \ldots, x_n)$ obtained by reducing all the coefficients of f modulo m (i.e. applying r_m to them).

It enjoys the properties you'd expect:

Lemma 4.6

Let m, n and v be elements of $\mathbb{N}^*$ and suppose that $m \mid n$. The reduction map

$$r_m : \mathbb{Z}/n\mathbb{Z}[x_1, \ldots, x_v] \to \mathbb{Z}/m\mathbb{Z}[x_1, \ldots, x_v] \tag{66}$$

satisfies the following properties:

1. $r_m(f_1 \pm f_2) = r_m(f_1) \pm r_m(f_2)$.
2. $r_m(f_1 \cdot f_2) = r_m(f_1) \cdot r_m(f_2)$.
3. $r_m(1) = 1$.
4. $r_m(0) = 0$.

We also have notion of reduction of tuples:

Definition 4.12

Let v, m, and n be in $\mathbb{N}^*$ and suppose that $m \mid n$. Then, given $\mathbf{a} = (a_1, \ldots, a_v) \in (\mathbb{Z}/n\mathbb{Z})^v$ the *reduction of* $\mathbf{a}$ *modulo* m, denoted either $r_m(\mathbf{a})$ or $\mathbf{a} \mod m$, is the element $(r_m(a_1), \ldots, r_m(a_v))$ in $(\mathbb{Z}/m\mathbb{Z})^v$.

This gives rise to the obvious analogue of Theorem 4.2:

Theorem 4.2

Let v, m, and n be in $\mathbb{N}^*$ and suppose that $m \mid n$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}/n\mathbb{Z}[x_1, \ldots, x_v]$. Then, the map

$$r_m : (\mathbb{Z}/n\mathbb{Z})^v \to (\mathbb{Z}/m\mathbb{Z})^v \tag{67}$$

restricts to a map

$$r_m : X_f(\mathbb{Z}/n\mathbb{Z}) \to X_g(\mathbb{Z}/m\mathbb{Z}) \tag{68}$$

Remark 4.6

Again, if $f(x_1, \ldots, x_n) \in \mathbb{Z}/n\mathbb{Z}[x_1, \ldots, x_v]$ we will often times sloppily write $X_f(\mathbb{Z}/m\mathbb{Z})$ to mean

$X_{r_m(f)}(\mathbb{Z}/m\mathbb{Z})$.

Thus, we also obtain the analogue of Corollary 4.2:

Corollary 4.2

Let v, m, and n be in $\mathbb{N}^*$ and suppose that $m \mid n$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}/n\mathbb{Z}[x_1, \ldots, x_v]$. If $X_f(\mathbb{Z}/n\mathbb{Z})$ is non-empty, then so is $X_f(\mathbb{Z}/m\mathbb{Z})$. Phrased differently, $X_f(\mathbb{Z}/m\mathbb{Z}) = \varnothing$ implies that $X_f(\mathbb{Z}/n\mathbb{Z}) = \varnothing$.

4.4 Exercises

Exercise 4.1

Problem: Show that the Diophantine equation $x^6 - 5y^4 = 2$ has no solutions.

Solution: If this Diophantine equation has a solution, then reducing modulo 5, shows that the Diophantine equation modulo 5 given by $x^6 = 2$ has a solution in $\mathbb{Z}/5\mathbb{Z}$. But, $0^6 = 0, 1^6 = 1, 2^6 = 4, 3^6 = 4$ and $4^6 = 1$ in $\mathbb{Z}/5\mathbb{Z}$. So, $x^6 = 2$ has no solution in $\mathbb{Z}/5\mathbb{Z}$, so $x^6 - 5y^4 = 2$ has no solution in $\mathbb{Z}$.

Exercise 4.2

Problem: Let p be an odd prime and k an element of $\mathbb{N}^*$. Find all solutions to $x^2 = 1 \mod p^k$.

Solution: Clearly if $x = \pm 1 \in \mathbb{Z}/p^k\mathbb{Z}$ then this satisfies the equation. Conversely, if $x^2 = 1 \mod p^k$ then this says that $p^k \mid x^2 - 1 = (x-1)(x+1)$. But, this means that for some $m, n \in \mathbb{N}$ such that $m + n = k$ we have that $p^m \mid x - 1$ and $p^n \mid x + 1$. But, note that $\gcd(x-1, x+1) \mid 2$. In particular, since p is odd we have that p can't divide both $x - 1$ and $x + 1$. Thus, we see that either $p^k \mid x - 1$ or $p^k \mid x + 1$. This means that $x = 1 \mod p^k$ or $x = -1 \mod p^k$. Thus, $x = \pm 1$ are the only solutions.

5 Lecture 5: Units modulo m, Euler's theorem and Euler's criterion

5.1 Setup: motivation

We begin today our true study of the differences between $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$. In particular, we will analyze a key difference between $(\mathbb{Z}, \cdot)$ and $(\mathbb{Z}/m\mathbb{Z}, \cdot)$—the existence of a rich number of units (i.e. things with multiplicative inverses). We will then analyze a particularly important modulus Diophantine equation and begin our long journey to understand its solutions.

5.2 Units modulo m, linear equations, and cancellation

One of the main properties of $(\mathbb{Z}, \cdot, +)$ that we highlighted in the first lecture was that $(\mathbb{Z}, \cdot)$ and $(\mathbb{Z}, +)$ were relatively simple. So, one of the first questions might ask is whether or not the same holds true for $\mathbb{Z}/m\mathbb{Z}$ for some $m \in \mathbb{N}^*$. It's pretty clear that essentially the same thing that holds true for $(\mathbb{Z}, +)$ is true for $(\mathbb{Z}/m\mathbb{Z}, +)$: it's still generated by 1 and such (minimal) expressions are unique. That said, while it is still true that $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ is generated by the primes and -1 it's now no longer true that we have anything resembling Theorem 1.1 in terms of unicity.

For example, we have the following monumental result that we won't prove (the proof is analytic in nature) in this course:

Theorem 5.1: Dirichlet's theorem on primes in arithmetic progressions

Let m be an element of $\mathbb{N}^*$ and a an element of $\mathbb{Z}$ with $\gcd(a, m) = 1$. Then, there exists infinitely many primes p such that $p = a \mod m$.

In particular, while it's still true that every $a \in \mathbb{Z}/m\mathbb{Z}$ can be factored into a product of primes, these primes are far from unique. Namely, Theorem 5.1 shows that for every $a \in \mathbb{Z}/m\mathbb{Z}$ with $\gcd(a, m) = 1$ one can write (and thus 'factor') $a = p$ for infinitely many distinct primes p. Thus, unique factorization is out the window.

Thus, the study of $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ is not as open and shut as $(\mathbb{Z}, \cdot)$. And, in fact, the two structures are quite different. One of the main differences comes from the dearth of elements of $\mathbb{Z}$ with multiplicative inverse (there is just ± 1) in contrast to the richness of such objects modulo m.

To help make sense of this, let us make the following definition:

Definition 5.1

Let $m \in \mathbb{N}^*$. Then, a *unit modulo* m is an element $a \in \mathbb{Z}/m\mathbb{Z}$ for which there exists a $b \in \mathbb{Z}/m\mathbb{Z}$ such that $ab = 1$. The set of units modulo m is denoted $\Phi(m)$.

Note that if $ab = 1 = ab'$ then left multiplying by b gives $bab = bab'$ and since $ba = 1$ we get that $b = b'$. In other words, the b in Definition 5.1 is unique—we denote it by a^{-1}.

Example 5.1

The element 3 in $\mathbb{Z}/4\mathbb{Z}$ is a unit modulo m with $3 = 3^{-1}$.

Example 5.2

The number 3 is not a unit modulo 9.

In words, $\Phi(m)$ is the set of elements of $\mathbb{Z}/m\mathbb{Z}$ that have a multiplicative inverse. Now, as we've already said, there are not so many such elements for $\mathbb{Z}$ but, generally, there are usually quite a few units modulo m.

To understand this, let us observe that checking whether $a \in \Phi(m)$ comes down to whether the equation $ax = 1 \mod m$ has a solution. But, as we will now see, such equations are something we have already implicitly studied!

Lemma 5.1

Let a and c be elements of $\mathbb{Z}$. The equation

$$ax = c \mod m \tag{69}$$

has a solution if and only if $\gcd(a, m) \mid c$. If $ax_0 = c \mod m$ is a solution, then the full set of solutions

to $ax = c \mod m$ in $\mathbb{Z}/m\mathbb{Z}$ are $x_0 + k\frac{m}{\gcd(m,a)}$ for $k = 0, \ldots, \gcd(a,m) - 1$ none of which are equal.

Proof 5.1

By definition $ax = c \mod m$ has a solution if and only if there exists a $y' \in \mathbb{Z}$ such that $ax = c + my'$. Thus, $ax = c \mod m$ has a solution if and only $ax + my = c$ has a solution in $\mathbb{Z}$ (where we have set $y := -y'$). But, by Theorem 2.4 this has a solution if and only if $\gcd(a,m) \mid c$. The second claim follows immediately from the parameterization of $ax + my = c$ in Theorem 2.4 using the fact that $k_1\frac{m}{\gcd(a,m)} = k_2\frac{m}{\gcd(a,m)}$ if and only if $k_1 = k_2 \mod \gcd(a,m)$.

In particular, we deduce a useful characterization of the units modulo m:

Lemma 5.2

Let m be a positive integer and $a \in \mathbb{Z}$ then a is a unit modulo m if and only if $\gcd(a,m) = 1$. Moreover, there is an algorithmic approach to compute a^{-1}.

Example 5.3

If $m = 12$ then the units modulo m are $\{1, 5, 7, 11\}$.

Example 5.4

If $m = 25$ then the units modulo m are $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$.

One nice corollary of this result is the following:

Corollary 5.1

If $a, b \in \Phi(m)$ then $ab \in \Phi(m)$. Moreover, if $a \in \Phi(m)$ then $a^{-1} \in \Phi(m)$.

In particular, since $\Phi(m)$ is closed under multiplication and $\cdot$ we could attempt to study $\Phi(m)$ itself as an algebraic object (a set with a multiplication operation). This is something that shall implicitly underly a lot of what we will do in the next few lectures.

It is often convenient to talk about the cardinality of $\Phi(m)$, and so we make the following definition:

Definition 5.2

The *Euler totient function*, denoted $\varphi(m)$, is the function $\mathbb{N} \to \mathbb{N}$ given by $\varphi(m) := \#\Phi(m)$.

By Lemma 5.2 one can also think of $\varphi(m)$ as the number of elements of $\{1, \ldots, m-1\}$ that are coprime to m, and thus φ is an interesting function independent of $\Phi(m)$. We will see later on, in Corollary 7.4, that one can write down an explicit formula for φ in terms of a prime factorization of m.

Example 5.5

We calculated above that $\varphi(25) = 20$.

Now, as if to maintain cosmic balance, the introduction of an abundance of units modulo m also, in many cases, introduces less desirable elements. Namely, recall that if $r, x, y \in \mathbb{Z}$ and $r \neq 0$ then obviously if $rx = ry$ then $x = y$. Unfortunately, the ability to perform such cancellations is not always possible modulo m:

Example 5.6

One has that $3 \cdot 2 = 0 \cdot 2$ in $\mathbb{Z}/6\mathbb{Z}$, but it's not true that $3 = 0$.

So, it'll be helpful to know when we can, in fact, cancel factors in an equation:

Theorem 5.2

Let m be a positive integer and let $a, b, r \in \mathbb{Z}$. Then,

$$ra = rb \mod m \tag{70}$$

if and only if

$$a = b \mod \frac{m}{\gcd(r, m)} \tag{71}$$

Remark 5.1

As a corollary to this we obtain the fact that if $r \in \Phi(m)$ then we can cancel r from equations, although this is already obvious since if $rx = ry$ then $r^{-1}rx = r^{-1}ry$ and so $x = y$. We will actually see later, in Exercise 5.3, that cancellability modulo m is actually equivalent to being a unit.

Proof 5.2: Theorem 5.2

Suppose first that $ra = rb \mod m$. Then, by definition, there exists some $\ell \in \mathbb{Z}$ such that $ra - rb = \ell m$. Dividing through by $\gcd(r, m)$ we get

$$\frac{r}{\gcd(r, m)}(a - b) = \frac{r}{\gcd(r, m)}a - \frac{r}{\gcd(r, m)}b = \frac{\ell m}{\gcd(r, m)} \tag{72}$$

and so $\frac{r}{\gcd(r, m)} \mid \ell \frac{m}{\gcd(r, m)}$. Since $\gcd\left(\frac{r}{\gcd(r, m)}, \frac{m}{\gcd(r, m)}\right) = 1$ we see that this implies that $\frac{r}{\gcd(r, m)} \mid \ell$. Thus, dividing the two extreme sides of (72) by $N := \frac{r}{\gcd(r, m)}$ gives

$$a - b = \frac{\ell}{N}\frac{m}{\gcd(r, m)} \tag{73}$$

which shows that $a = b \mod \frac{m}{\gcd(r,m)}$ as desired.

Conversely, if $a = b \mod \frac{m}{\gcd(r,m)}$ then this means that $a - b = \ell\frac{m}{\gcd(r,m)}$ for some integer ℓ. So, we see that $ra - rb = m\frac{\ell r}{\gcd(r,m)}$ so that $m \mid ra - rb$ so that $ra = rb \mod m$.

5.3 Power equations and Euler's theorem

Now, since the structure of $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ is more nuanced than that of $(\mathbb{Z}, \cdot)$ one might suspect that equations in the latter might also be more nuanced than equations in the former, and this is true. An example of such an equation is given as follows:

Definition 5.3

Let n and m be elements of $\mathbb{N}^*$ and $a \in \mathbb{Z}/m\mathbb{Z}$. An equation of the form $x^n = a \mod m$ is called a *power equation*.

In words one can think of power equations as the question of whether or not a given element of $\mathbb{Z}/m\mathbb{Z}$ has an n^{th}-root (in $\mathbb{Z}/m\mathbb{Z}$). Our first major waypoint to fulfilling Goal 4.1, at least in the context of our course, is the following:

Goal 5.1: First major step

Develop a fully theory of power equations modulo m—in particular, be able to algorithmically list all solutions to a power equation.

This is a surprisingly massive undertaking. We will have to develop a really non-trivial amount of theory about the object $\mathbb{Z}/m\mathbb{Z}$ and modulus Diophantine equations to be able to fulfill Goal 5.1.

It's worth explicitly pointing out that Goal 5.1 really is an incredibly worthwhile. Indeed, while equations like $x^n = a$ in $\mathbb{Z}$ are not very interesting (they have solutions if and only if $n \mid v_p(a)$ for all primes p), equations like $x^n = a \mod m$ are:

1. Much more nuanced.
2. But still solvable.
3. Show up constantly in Diophantine equations.

Here is a very basic example:

Example 5.7

Let $n \in \mathbb{N}^*$. Recall q_n from Example 1.12, and suppose that p is a prime that q_n represents, then we claim that the equation $z^2 = -n \mod p$ has a solution. Indeed, note that if $x^2 + ny^2 = p$ then $\gcd(y, p) = 1$. Indeed, if $p \mid y$ then $p^2 \mid ny^2$ which implies that $p \mid x^2 = p - ny^2$. But, this then implies that $p^2 \mid x^2$ and so $p^2 \mid x^2 + ny^2 = p$ which is a contradiction. Thus, we see that $y \in \Phi(p)$. Thus, reducing $x^2 + ny^2 = p$ modulo p gives $x^2 + ny^2 = 0$ and since $y \in \Phi(p)$ we may divide through by y^2 and obtain $z^2 = -n \mod p$ where $z := xy^{-1}$.

Thus, if we had a satisfactory enough solution to Goal 5.1 to give conditions on when $z^2 = -n \mod p$ is solvabe, in terms of p, we'd obtain, by Corollary 4.2, conditions for p on when p is represented by q_n. Thus, fulfilling Goal 5.1 is not a totally contentless thing—in fact, quite the opposite!

In general, modulus power equations come up whenever one has a Diophantine equation of the form

$$bx_1^n + mf(x_2, \ldots, x_v) = c \tag{74}$$

where m is some integer, $c \in \mathbb{Z}$, $b \in \Phi(m)$, and $f(x_2, \ldots, x_v) \in \mathbb{Z}[x_2, \ldots, x_v]$. Note, in particular while (74) is a polynomial equation in $v > 1$ variables, that reducing modulo m gives

$$x_1^n = b^{-1}c \mod m \tag{75}$$

which is a modulus power equation and, in particular, an equation in one variable.

Note, also, that the existence of solutions to various power equations draw a major difference between $(\mathbb{Z}, \cdot)$ and $(\mathbb{Z}/m\mathbb{Z}, \cdot)$. For example, consider the following:

Lemma 5.3

The only solutions to $x^n = 1$ in $\mathbb{Z}$ are:

1. 1 if n is odd.
2. ± 1 if n is even.

In stark contrast, we have the following lovely, foundationaly result:

Theorem 5.3: Euler's theorem

Let $m \in \mathbb{N}^*$ and let $a \in \mathbb{Z}/m\mathbb{Z}$. Then, the following are equivalent:

1. $a \in \Phi(m)$ (i.e. a is a unit modulo m).
2. $a^{\varphi(m)} = 1$.

In other words, this result says that the solutions to the modulus power equation $x^{\varphi(m)} = 1 \mod m$ are precisely the elements of $\Phi(m)$ (i.e. the units modulo m).

Example 5.8

Let $m = 25$. Then, thanks to Exercise 5.1 we know that $\varphi(25) = 5 \cdot 4 = 20$. And, in fact

$$\Phi(25) = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\} \tag{76}$$

Theorem 5.3 then says that the solutions to $x^{20} = 1 \mod 25$ are precisely the set $\Phi(25)$ listed above. Let's do a reality check and see that 14 does, in fact, satisfy the claim.

$$\begin{aligned} 14^2 &= 196 = 21 = -4 \mod 25 \\ 14^4 &= (14^2)^2 = (-4)^2 = 16 \mod 25 \\ 14^{20} &= (14^4)^5 = 16^5 \mod 25 \\ 14^{20} &= (16)^5 = (16^2) \cdot 16 = (256)^2 \cdot 16 \mod 25 \\ 14^{20} &= 6^2 \cdot 16 = 36 \cdot 16 = 11 \cdot 16 \mod 25 \\ 14^{20} &= 176 = 1 \mod 25 \end{aligned} \tag{77}$$

Whew!

This is a somewhat remarkable theorem in that it not only does it show the richness of power equations modulo m (they have lots) of solutions, they also provide a way to quickly exponentiate things modulo m:

Corollary 5.2

Let $m \in \mathbb{N}^*$ and $a \in \Phi(m)$, then for any $n \in \mathbb{Z}$ one has that

$$a^n = a^{r_{\varphi(m)}(n)} \mod m \tag{78}$$

Proof 5.3

Write $n = \varphi(m)q + r_{\varphi(m)}(n)$ using Theorem 2.2. Then,

$$\begin{aligned} a^n &= a^{\varphi(m)q + r_{\varphi(m)}(n)} \\ &= (a^{\varphi(m)})^q \cdot a^{r_{\varphi(m)}(\varphi(n)} \\ &= 1^q \cdot a^{r_{\varphi(m)}(n)} \\ &= a^{r_{\varphi(m)}(n)} \end{aligned} \tag{79}$$

Example 5.9

Let us compute the last digit of 7^{101}. Note that this digit is precisely $r_{10}(7^{101})$, so we aim to compute $7^{101} \mod 10$. But, note that $7 \in \Phi(10)$ and $\varphi(10) = 4$. Since $r_4(101) = 1$ we see from Corollary 5.2 that $7^{101} = 7 \mod 10$. Thus, the last digit of 7^{101} is 7.

Let us now give the proof of Theorem 5.3. The proof we give here is a bit arduous, but is the 'morally correct' proof (in the sense that it's what generalizes to the correct level of generality). We sketch a simpler proof in Exercise 5.6.

To facilitate the proof of Theorem 5.3 it's useful to first make the following remarkably useful definition:

Definition 5.4

Let $m \in \mathbb{N}^*$ and $a \in \Phi(m)$. The *order* of a, denoted $|a|$ is the smallest $k \in \mathbb{N}^*$ such that $a^k = 1$. If $b \in \mathbb{Z}$ is coprime to m we denote by $|b|_m$ the order of $r_m(b) \in \Phi(m)$.

Remark 5.2

This is another instance of the yoga. We will often times in the future start with an element $a \in \mathbb{Z}/m\mathbb{Z}$, think about its order, then think of a as being an integer, take its order modulo a different number, etc.

Example 5.10

Let $m = 8$. Then, $\Phi(8) = \{1, 3, 5, 7\}$. One can quickly check that $|1| = 1$ and $|3| = |5| = |7| = 2$.

Example 5.11

Let $m = 17$. The, one can check that $|3| = |10| = 16$ and $|9| = 8$.

The first key observation about the notion of order is the following:

Lemma 5.4

Let $m \in \mathbb{N}^*$ and $a \in \Phi(m)$. Then, the order of a exists (i.e. there exists some $k \in \mathbb{N}^*$ such that $a^k = 1$).

Proof 5.4

We need to show that $a^k = 1$ for some $k \in \mathbb{N}^*$. That said, since $\Phi(m)$ is finite, we know that the multiset $\{1, a, a^2, \ldots\}$ is also finite, and thus has repeat elements. Say, $a^k = a^\ell$ with $\ell > k \geqslant 1$. Then, $a^{\ell-k} = 1$ and $\ell - k \geqslant 1$ from where the conclusion follows.

Note that this already shows that every $a \in \Phi(m)$ satisfies the equation $x^k = 1$ for some k (e.g. $k = |a|$). Let us then continue on to the proof of Theorem 5.3:

Proof 5.5: Theorem 5.3

Note that if $a^{\varphi(m)} = 1$ then $a^{\varphi(m)-1}a = 1$ so that a has a multiplicative inverse modulo m. Thus, if $a^{\varphi(m)} = 1$ then $a \in \Phi(m)$.

Conversely, suppose that $a \in \Phi(m)$. Let $g := |a|$. Note then that, almost by definition, if we let $G(a) := \{1, a, a^2, a^3, \cdots\}$ then $G(a)$ is a finite set of size g.

Now, for each $x \in \Phi(m)$ let $xG(a) := \{x, xa, xa^2, xa^3, \cdots\}$. By the cancellation property of a one has that $xG(a)$ is a finite set of size g for all x. Note that for every $x \in \Phi(m)$ one has that $x \in yG(a)$ for some y (e.g. $y = x$). Moreover, note that if $xG(a) \cap yG(a) \neq \varnothing$ then the sets $xG(a)$ and $yG(a)$ are equal. Indeed, if $xG(a) \cap yG(a)$ is non-empty, then one has that $xa^s = ya^t$ for some a, say with $s \geqslant t$. This implies that $xa^{s-t} = y$ so that $y \in xG(a)$. Clearly then $ya^k = xa^{s-t+k} \in xG(a)$. So, $yG(a) \subseteq xG(a)$. But, since $\#yG(a) = \#xG(a) = g$ this implies that $yG(a) = xG(a)$.

Let us denote by $x_1, \ldots, x_c$ a set of $x_i \in \Phi(m)$ such that for all $x \in \Phi(m)$ we have that $x \in x_iG(a)$ for some a and we have that $x_iG(a) \cap x_jG(a) = \varnothing$ for $i \neq j$. This is possible by the previous paragraph. Then, we have that

$$\Phi(m) = \bigsqcup_{i=1}^{c} x_iG(a) \tag{80}$$

where the square cup means 'disjoint union'. This implies that

$$\varphi(m) = \#\Phi(m) = \sum_{i=1}^{c} \#x_iG(a) \tag{81}$$

But, we have that $\#x_iG(a) = g$. So, we deduce that

$$\varphi(m) = cg \tag{82}$$

Then, we have that

$$a^{\varphi(m)} = a^{cg} = (a^g)^c = 1^c = 1 \tag{83}$$

as desired.

Remark 5.3

It should be clear for those that have taken algebra that this is just mimicry of the proof of the more general result of Lagrange's theorem.

Since this proof is kind of complicated, let's consider a special case:

Example 5.12

Let $m = 15$ and $a = 4$. Note that

$$\Phi(15) = \{1, 2, 4, 7, 8, 11, 13, 14\} \tag{84}$$

Note that $4^2 = 16 = 1 \mod 15$ so that g from the above proof is 2. We need to find a (there are more than one) set of x_i as in the above proof. We claim that $\{1, 2, 7, 11\}$ work. Indeed:

$$\begin{aligned} 1G(4) &= \{1, 4\} \\ 2G(4) &= \{2, 8\} \\ 7G(4) &= \{7, 13\} \\ 11G(4) &= \{11, 14\} \end{aligned} \tag{85}$$

One then sees, as desired, that

$$\Phi(15) = 1G(4) \sqcup 2G(4) \sqcup 7G(4) \sqcup 11G(4) \tag{86}$$

which, upon taking cardinalities, gives the correct equation

$$\varphi(15) = 4 \cdot 2 \tag{87}$$

If one inspects of the proof of Theorem 5.3 what it really shows is that for all $a \in \Phi(m)$ one has that $|a| \mid \varphi(m)$. In fact, this is equivalent to Theorem 5.3 by the following basic observation:

Lemma 5.5

Let $m \in \mathbb{N}^*$ and $a \in \Phi(m)$. Suppose that $a^k = 1$. Then, $|a| \mid k$.

Proof 5.6

Use Theorem 2.2 to write $k = q|a| + r$ for $0 \leqslant r < |a|$. Note then that

$$1 = a^k = a^{q|a|+r} = (a^{|a|})^q a^r = a^r \tag{88}$$

But, since $r < |a|$ if $r > 0$ this would contradict the definition of $|a|$. So, $r = 0$ and thus $|a| \mid k$.

From this lemma and Theorem 5.3 we also deduce the following:

Corollary 5.3

Let $m \in \mathbb{N}^*$ and let $a \in \Phi(m)$. Then, $|a| \mid \varphi(m)$.

Using this corollary and Lemma 5.5 we can, amazingly, already show that infinitely many ('most' in some sense) power equations have unique solutions:

Corollary 5.4

Let m and n be in $\mathbb{N}^*$ and assume that $\gcd(n, \varphi(m)) = 1$. Then, for all $a \in \Phi(m)$ the equation $x^n = a \mod m$ has a unique solution.

Proof 5.7

Define the map $f : \Phi(m) \to \Phi(m)$ by the equation $f(x) = x^n$. We wish to show that this map is bijective. That said, since $\Phi(m)$ is finite, it suffices to show that f is injective. To do this, suppose that $f(x) = f(y)$, then $x^n = y^n$ and so $z^n = 1$ where $z = xy^{-1}$. In particular, by Lemma 5.5 we have that $|z| \mid n$. But, by Corollary 5.3 we also know that $|z| \mid \varphi(m)$. Thus, $|z| \mid \gcd(n, \varphi(m)) = 1$. Thus, $|z| = 1$. Thus, $z^1 = 1$ and so $z = 1$. So, $x = y$ as desired.

The proof of this corollary is remarkably simple, deceptively so. For example, it says that 7 is a 101^{st} power in $\mathbb{Z}/11\mathbb{Z}$, but gives no way to actually solve $x^{101} = 7 \mod 11$. Later on, in Theorem 6.3, we will give a much more constructive proof of the above theorem but it will still rely on a lot of work (i.e. finding a primitive root) that will only be fully completed much later.

Let us end this section by noting the following special case of Euler's theorem that is usually given it's own name:

Corollary 5.5: Fermat's little theorem

Let p be a prime and let $p \nmid a$. Then, $a^{p-1} = 1 \mod p$. Thus, $a^p = a \mod p$.

Proof 5.8

If $p \nmid a$ then $a^{p-1} = 1 \mod p$ by Theorem 5.3 since $\varphi(p) = p - 1$.In particular, if $p \nmid a$ then multiplying both sides of $a^{p-1} = 1 \mod p$ by a gives $a^p = a \mod p$. If $p \mid a$ then $a = 0 \mod p$ so evidently $a^p = a = 0 \mod p$. Thus, the second claim holds.

5.4 Euler's criterion: initial observations

Another upshot of Euler's theorem is that it gives us a necessary condition for a power equation, at least when $a \in \Phi(m)$, to have a solution:

Corollary 5.6

Let $m, n \in \mathbb{N}^*$ and $a \in \Phi(m)$. Then, if $x^n = a \mod m$ has a solution, then $a^{\frac{\varphi(m)}{\gcd(\varphi(m),n)}} = 1 \mod m$.

Proof 5.9

Suppose that $x^n = a \mod m$ has the solution x_0. Note that $x_0 \in \Phi(m)$. Indeed, $x_0^n = a \in \Phi(m)$. Let $y := a^{-1}$. Then, $x_0^n y = 1$. But, this implies that $x_0(x_0^{n-1}y) = 1$ so that $x_0 \in \Phi(m)$. So, by Theorem 5.3 we have that

$$\begin{aligned} a^{\frac{\varphi(m)}{\gcd(\varphi(m),n)}} &= (x_0^n)^{\frac{\varphi(m)}{\gcd(\varphi(m),n)}} \\ &= x_0^{\varphi(m)\frac{n}{\gcd(\varphi(m),n)}} \\ &= (x_0^{\varphi(m)})^{\frac{n}{\gcd(\varphi(m),n)}} \\ &= 1^{\frac{n}{\gcd(\varphi(m),n)}} \\ &= 1 \end{aligned} \tag{89}$$

In particular, taking $n = 2$ we have the following:

Corollary 5.7

Let $p > 2$ be a prime and $a \in \Phi(m)$. If $x^2 = a \mod p$ has a solution, then $a^{\frac{p-1}{2}} = 1$.

Proof 5.10

This follows immediately from Corollary 5.6 since $\gcd(p-1, 2) = 2$.

Example 5.13

The equation $x^2 = 7 \mod 11$ has no solution. Indeed, we need to check that $7^5 \neq 1 \mod 11$. But, $7^2 = 49 = 5 \mod 11$. So, $7^4 = 5^2 = 25 = 3 \mod 11$. So, $7^5 = 7 \cdot 3 = 21 = -1 \mod 11$. Thus, the equation $x^2 = 7 \mod 11$ has no solution.

We also see that we get the following proof of half of Theorem 1.5 part (1), our first real step towards handling quadratic forms:

Corollary 5.8

Let p be an odd prime. Then, if $x^2 + y^2 = p$ has a solution, then $p = 1 \mod 4$.

Proof 5.11

Given the discussion in and following Example 5.7 it suffices to show that $z^2 = -1 \mod p$ having a solution implies that $p = 1 \mod 4$. By Corollary 5.7 we see that $z^2 = -1 \mod p$ having a solution implies that $(-1)^{\frac{p-1}{2}} = 1 \mod p$ which, since $p > 2$, is equivalent to $(-1)^{\frac{p-1}{2}} = 1$. This implies that

$\frac{p-1}{2}$ is even, so that $2 \mid \frac{p-1}{2}$ and so $4 \mid p-1$ and thus $p = 1 \mod 4$.

Example 5.14

The Diophantine equation $x^2 + y^2 = 103$ has no solutions. Indeed, this follows from Corollary 5.8 since $103 = 3 \mod 4$.

Of course, we are interested in positive statements, namely we would love for the converse of Corollary 5.6 to hold true.

For example, consider the following:

Example 5.15

Let $m = 11$. Let's compute a^5 for all $a \in \Phi(11)$. Namely, we have that

$$\Phi(11) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \tag{90}$$

and taking these to the fifth power we get

$$\begin{aligned} 1^5 &= 1 \\ 2^5 &= 10 \\ 3^5 &= 1 \\ 4^5 &= 1 \\ 5^5 &= 1 \\ 6^5 &= 10 \\ 7^5 &= 10 \\ 8^5 &= 10 \\ 9^5 &= 1 \\ 10^5 &= 10 \end{aligned} \tag{91}$$

So that the $a \in \Phi(11)$ such that $a^5 = 1$ is $\{1, 3, 4, 5, 9\}$. Let's now compute which numbers are squares modulo 11:

$$\begin{aligned} 1^2 &= 1 \\ 2^2 &= 4 \\ 3^2 &= 9 \\ 4^2 &= 16 = 5 \\ 5^2 &= 25 = 3 \\ 6^2 &= 3 \\ 7^2 &= 5 \\ 8^2 &= 9 \\ 9^2 &= 4 \\ 10^2 &= 1 \end{aligned} \tag{92}$$

so that the squares modulo 11 are $\{1, 4, 9, 5, 3\}$. In this case we see that the converse of Theorem 5.6 *does* hold.

Fortunately, the world is a much more interesting place and the converse of Theorem 5.6 does not hold in general:

Example 5.16

Let $m = 36$. Then, $\varphi(m) = 12$. So, taking $n = 2$ the converse of Theorem 5.6 would say that for $a \in \Phi(36)$ one has that $a^6 = 1$ implies that $x^2 = a$ has a solution in $\mathbb{Z}/36\mathbb{Z}$. But, one can check that $5^6 = 1 \mod 36$ but that $x^2 = 5 \mod 36$ does not have a solution.

The goal of the next lecture will be to discuss a condition on m for which Theorem 5.6 has a converse.

5.5 Wilson's theorem

We finish this lecture with a bit of modulo p buffoonery showing how strange the modulo p world can be, which will also allows us to prove the converse of the condition on the existence of a solution to $z^2 = -1 \mod p$ discussed in Corollary 5.8:

Theorem 5.4: Wilson's theorem

Let p be a prime. Then, $(p-1)! = -1 \mod p$.

Let us just check this empirically for one prime:

Example 5.17

Let $p = 7$. Then, $6! = 720 = 6 = -1 \mod 7$.

The proof will be another manipulation, as in the proof of Theorem 5.3, of the fact that $\Phi(p)$ has interesting multiplicative structure:

Proof 5.12: Theorem 5.4

Note that $(p-1)!$ is just $1 \cdot 2 \cdots (p-1)$. In other words,

$$(p-1)! = \prod_{x \in \Phi(p)} x \tag{93}$$

Now, if $x \in \Phi(p)$ then $x^{-1} \in \Phi(p)$. So, we can try to pair each x on the right hand side of (93) with x^{-1} and cancel. It seems like all the terms should match with their inverse and cancel, except this is a product over the distinct elements of $\Phi(p)$, so we can pair x with its inverse and cancel if and only if $x^{-1} \neq x$. So, for all $x \neq x^{-1}$ we see that we can pair x with x^{-1} on the right hand side of (93) and cancel them, leaving only x with $x = x^{-1}$. In other words, we see deduce that

$$(p-1)! = \prod_{x = x^{-1}} x \tag{94}$$

But $x = x^{-1}$ is the same thing as saying $x^2 = 1$. And, in Exercise 4.2 that the only solutions to $x^2 = 1$

mod p are $x = \pm 1$. So, we deduce that

$$(p-1)! = \prod_{x=x^{-1}} x = 1 \cdot -1 = -1 \tag{95}$$

Remark 5.4

For those that have taken algebra, one can interpret the above as giving a proof of the following fact: if G is a finite abelian group, then

$$\prod_{x \in G} x = \prod_{x \in G,\, |x|=2} x \tag{96}$$

Wilson's theorem is just this observation together with the fact that $|x| = 2$ for $x \in \Phi(p)$ implies $x = -1$.

And, from Wilson's theorem, we deduce the following:

Corollary 5.9

Let p be an odd prime. Then, the equation $x^2 = -1 \mod p$ has a solution if and only if $p = 1 \mod 4$.

Proof 5.13

We already discussed the necessity part in Corollary 5.8. Conversely, since p is odd we can write it as $2m+1$ for some $m \in \mathbb{Z}$. We can then see that

$$p! = 1 \cdot (p-1) \cdot 2 \cdot (p-2) \cdots m \cdot (p-m) = 1 \cdot -1 \cdot 2 \cdot (-2) \cdots m \cdot (-m) = (-1)^m (m!)^2 \mod p \tag{97}$$

But, by Wilson's theorem we deduce

$$-1 = (m!)^2 (-1)^m \mod p \tag{98}$$

and so

$$(m!)^2 = (-1)^{m+1} \mod p \tag{99}$$

Since $p = 1 \mod 4$ we know that m is even, and so $(-1)^{m+1} = -1$. The conclusion follows.

5.6 Exercises

Exercise 5.1

Problem: Show that if p is prime and $k \geqslant 1$, then $\varphi(p^k) = p^{k-1}(p-1)$.

Solution: By Lemma 5.2, $\varphi(p^k)$ is the number of elements of $0, \ldots, p^k - 1$ which are coprime to p^k. This is equivalent to being not divisible by p. There are p^{k-1} multiples of p in $0, \ldots, p^k - 1$, so there are $p^k - p^{k-1} = p^{k-1}(p-1)$ non-multiples of p.

Exercise 5.2

Problem: Show that if p is prime, then $\Phi(p) = \{1, \ldots, p-1\}$ (i.e. the only non-unit modulo p is zero). Can this happen if p is not prime?

Solution: By Lemma 5.2 the units modulo p are the elements of $\{0, \ldots, p-1\}$ which are coprime to p. Since p is prime this is equivalent to not being divisible by p. The only element of $\{0, \ldots, p-1\}$ divisible by p is 0, so the units are precisely $\{1, \ldots, p-1\}$ (i.e. the non-zero elements). If m is positive and composite, say $m = ab$ with $m > a, b > 1$, then the units modulo m are not the non-zero elements. Indeed, a and b are certainly non-zero but cannot be units since $\gcd(m, a) = a > 1$ and $\gcd(m, b) = b > 1$. Another way to see this is that if $0 = ab = a \cdot 0$ and so we can't cancel a (similarly for b).

Exercise 5.3

Problem: Show that if $r \in \mathbb{Z}/m\mathbb{Z}$ has the cancellation property (i.e. that $ra = rb \mod m$ implies that $a = b \mod m$) then r is a unit modulo m.

Solution: Consider the map $M_r : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ given by $M_r(a) := ra$. By the assumption that r has the cancellation property we see that M_r is injective. But, since $\mathbb{Z}/m\mathbb{Z}$ is a finite set, this implies (by the pigeonhole principle) that M_r is surjective, and so $M_r(a) = 1$ for some a. But, this means that $ra = 1$ so that r is a unit.

Exercise 5.4

Problem: Show that the Dophantine equation $x^4 + 7xy = 3$ has no solution.

Solution: If it did have a solution, then reducing it modulo 7 shows that $x^4 = 3 \mod 7$ has a solution. By Theorem 5.6 if this had a solution, then $3^{\frac{3}{\gcd(4,3)}}$ would need to be 1 modulo 7. But, one checks that this is -1. Thus, $x^4 = 3 \mod 7$ has no solution, and thus neither does $x^4 + 7xy = 3$.

Exercise 5.5

Problem: Show by example that the naive extension of Corollary 5.5, namely $a^{m-1} = 1 \mod m$ for m an arbitrary integer and $a \in \Phi(m)$, does not hold.

Solution: One has that $5^7 = 5 \mod 8$. Thus, one can take $m = 8$ and $a = 5$.

Exercise 5.6

Problem: This exercise gives a trickier, less intuitive proof of Theorem 5.3.

1. Show that if $r \in \Phi(m)$ then the map $M_r : \Phi(m) \to \Phi(m)$ given by $M_r(x) := rx$ is a bijection.

2. Deduce that
$$\prod_{x\in\Phi(m)} x = \prod_{x\in\Phi(m)} (rx) \tag{100}$$
3. Factor out $r^{\varphi(m)}$ and deduce Theorem 5.3.

Solution:

1. Since r is a unit the map M_r is an injection. By the pigeonhole principle we know that M_r is a bijection.
2. This follows from the fact that we are taking a product over the same set of things since M_r is a bijection.
3. We deduce that $\prod_{x\in\Phi(m)} x = r^{\varphi(m)} \prod_{x\in\Phi(m)} x$. Since $\prod_{x\in\Phi(m)} x$ is a unit, we can cancel it to deduce that $r^{\varphi(m)} = 1$.

Exercise 5.7

Problem: Show that 8 is a 77^{th} power in $\mathbb{Z}/17\mathbb{Z}$.

Solution: Note that $8 \in \Phi(17)$ and that $\gcd(77, \varphi(17)) = 1$. Thus, the claim follows from Corollary 5.4.

6 Lecture 6: Primitive roots and Euler's criterion

6.1 Setup

Our goal today is the following:

Goal 6.1: Today

Give conditions on m for which the converse of Corollary 5.6 holds.

Along the way, this will necessitate us understanding some of the intricacies of the structure of $\Phi(m)$ and, in particular, as us about replacing the generators provided by Theorem 1.1 (i.e. those primes not dividing m) with some sort of minimal set of generators for which we do have uniqueness of factorization modulo m. In particular, we will need to understand conditions on m such that $\Phi(m)$ is generated by a single element.

6.2 Motivation for primitive roots

As stated above, our goal today is to study conditions on when $\Phi(m)$ is generated by a single element. Considering that $(\mathbb{Z}, \cdot)$ needed infinitely many elements to generate it, it's somewhat surprising that we'd need only a single element to generate $\Phi(m)$ sometimes. That said, the key observation is that $\Phi(m)$ is precisely the set of solutions to an equation of the form $x^n = 1$ (namely take $n = \Phi(m)$ and apply Theorem 5.3) and it's really this fact that's making the behind-the-scenes cogs turn.

To see why, we first take a brief detour to recall basic facts about the solutions to the equation $x^n = 1$ not over $\mathbb{Z}/m\mathbb{Z}$ but, instead, over $\mathbb{C}$. To prove these properties it will be helpful to recall some basic definitions of objects associated to the complex numbers:

Definition 6.1

Recall that the *complex numbers*, denoted $\mathbb{C}$, are the set

$$\mathbb{C} := \{a + bi : a, b \in \mathbb{R}\} \tag{101}$$

where $\mathbb{R}$ is the set of real numbers. One adds as follows:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \tag{102}$$

and multiplies as follows:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \tag{103}$$

Now, there is a function of particular importance on the complex numbers:

Definition 6.2

The *complex exponential function*, denoted exp, is the following function $\mathbb{C} \to \mathbb{C}$:

$$\exp(z) := \sum_{n=0}^{\infty} \frac{z^n}{n!} \tag{104}$$

The *normalized complex exponential function*, denoted E, is the following function $\mathbb{C} \to \mathbb{C}$:

$$E(z) := \exp(2\pi i z) \tag{105}$$

The normalized complex exponential function enjoys the following properties which are elementary to verify:

Lemma 6.1

The following properties hold:

1. $E(z)$ is never zero.
2. If $z_1, z_2 \in \mathbb{C}$ then $E(z_1)E(z_2) = E(z_1 + z_2)$.
3. If $x \in \mathbb{R}$ then $E(x) = 1$ if and only if $x \in \mathbb{Z}$.

Remark 6.1

The only non-trivial part of Lemma 6.1 is part (3). To understand it, in particular understand the normalization, recall the following classical theorem of Demoivre:

$$e^{ix} = \cos(x) + i \sin(x) \tag{106}$$

which holds for any $x \in \mathbb{R}$. In particular, one sees that $e^{ix} = 1$ if and only if $\cos(x) = 1$ and $\sin(x) = 0$. This happens if and only if x is an integer multiple of 2π. Thus, we see that $E(x) = 1$ if and only if x is an integer.

The corollary we obtain from this is the following:

Theorem 6.1

Let $n \in \mathbb{N}^*$. Then, then equation $x^n = 1$ has exactly n solutions in $\mathbb{C}$. They are given by $E\left(\frac{k}{n}\right)$ for $k = 0, \ldots, n-1$.

Proof 6.1

Note that $E\left(\frac{k}{n}\right) \neq E\left(\frac{\ell}{n}\right)$ for $\ell \neq k$ in $0, \ldots, n-1$. Indeed, if they were equal then this would say that $E\left(\frac{\ell - k}{n}\right) = 1$ which implies that $\frac{\ell - k}{n} \in \mathbb{Z}$ which is not true. Thus, the values $E\left(\frac{k}{n}\right)$ for $k = 0, \ldots, n-1$ are distinct. Moreover, note that

$$E\left(\frac{k}{n}\right)^n = E\left(\frac{nk}{n}\right) = E(k) = 1 \tag{107}$$

Thus, the $E\left(\frac{k}{n}\right)$ are all solutions to $x^n = 1$. Since $x^n = 1$ has at most n solutions in $\mathbb{C}$, we deduce that $\left\{E\left(\frac{k}{n}\right)\right\}$ is precisely the set of solutions as desired.

In particular, we see the following peculiarity about the set of solutions to $x^n = 1$ in $\mathbb{C}$:

Corollary 6.1

Let $n \in \mathbb{N}^*$ and set $\zeta := E\left(\frac{1}{n}\right)$. Then, the solutions to $x^n = 1$ are precisely the powers ζ^k for $k = 0, \ldots, n-1$.

In other words, the set of solutions to $x^n = 1$ are 'generated' multiplicatively by the a single element: ζ. That said, one should observe that ζ is not the only generator of the solutions to $x^n = 1$. Indeed:

Lemma 6.2

The generators of the solutions to $x^n = 1$ are precisely ζ^ℓ for $\ell \in \{0, \ldots, n-1\}$ such that $\gcd(\ell, n) = 1$.

Proof 6.2

Note that since ζ generates the solutions it's clearly necessary and sufficient that ζ^ℓ generates ζ. In other words, ζ^ℓ generates all solutions if and only if the equation $(\zeta^\ell)^k = \zeta$ has a solution. But, note that this is equivalent to $E\left(\frac{\ell k}{n}\right) = E\left(\frac{1}{n}\right)$ which is equivalent to $\frac{\ell k - 1}{n} \in \mathbb{Z}$ or $n \mid \ell k - 1$. In other words, we see that ζ^ℓ is a generator if and only if $\ell \in \Phi(n)$ and so we are done by Lemma 5.2.

6.3 Primitive roots and Euler's criterion

Motivated by the last subsection, and the fact that $\Phi(m)$ is precisely the set of solutions to $x^{\varphi(m)} = 1$ in $\mathbb{Z}/m\mathbb{Z}$ by Theorem 5.3, we make the following definition:

Definition 6.3

An element $a \in \Phi(m)$ is called a *primitive root modulo* m if a multiplicative generates $\Phi(m)$ (i.e. for all $b \in \Phi(m)$ there exists some $k \geqslant 0$ such that $a^k = b$).

Remark 6.2

For those that have taken algebra, it's clear that $\Phi(m)$ is always a finite abelian group—in fact, it's just the group of units of the ring $\mathbb{Z}/m\mathbb{Z}$. The existence of a primitive root modulo m is then the question of whether $\Phi(m)$ is cyclic. In particular, if there is a primitive root modulo m then $\Phi(m) \cong \mathbb{Z}/\varphi(m)\mathbb{Z}$ as groups (the left group being multiplicative and the right group being additive).

Example 6.1

If $m = 7$ then 3 is a primitive root. Indeed,

$$\begin{aligned} 3^1 &= 3 \\ 3^2 &= 2 \\ 3^3 &= 6 \\ 3^4 &= 4 \\ 3^5 &= 5 \\ 3^6 &= 1 \end{aligned} \tag{108}$$

so that every $a \in \Phi(7) = \{1, 2, 3, 4, 5, 6\}$ is 3^ℓ for some ℓ. One can check that 5 is also a primitive root modulo 7.

Example 6.2

If $m = 22$ one can check that 13 is a primitive root. Indeed

$$\begin{aligned} 13^1 &= 13 \\ 13^2 &= 5 \\ 13^3 &= 19 \\ 13^4 &= 5 \\ 13^5 &= 21 \\ 13^6 &= 9 \\ 13^7 &= 7 \\ 13^8 &= 3 \\ 13^9 &= 17 \\ 13^{10} &= 1 \end{aligned} \tag{109}$$

and $\Phi(22) = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$ one concludes.

Let us make the following notational definition:

Definition 6.4

Let $m \in \mathbb{N}^*$ and let $a \in \Phi(m)$. Then, the *group generated by* a, denoted by $\langle a \rangle$, is the set

$$\langle a \rangle := \{a^k : k \in \mathbb{N}\} \tag{110}$$

The reason this is relevant, of course, is that $a \in \Phi(m)$ is a primitive root if and only if $\langle a \rangle = \Phi(m)$. The subgroup generated by a satisfies the following basic properties:

Lemma 6.3

Let $m \in \mathbb{N}^*$ and let $a \in \Phi(m)$. Then:

1. The subgroup $\langle a \rangle$ contains 1, is closed under multiplication, and is closed under inversion.
2. One has that $\#\langle a \rangle = |a|$.

In particular, we deduce from Lemma 6.3 that for $a \in \Phi(m)$ one has that a is primitive root modulo m if and only if $|a| = \#\Phi(m) = \varphi(m)$.

The reason why we care about primitive roots, from an abstract perspective, is the following:

Lemma 6.4

Let m be an element of $\mathbb{N}^*$ and let ξ be a primitive root modulo m. Then, for every $a \in \Phi(m)$ one can write $a = \xi^\ell$ for a unique $\ell \in \{0, \ldots, \varphi(m) - 1\}$. Moreover, if $i, j \in \mathbb{Z}$ then $\xi^i = \xi^j$ if and only if $i = j \mod \varphi(m)$.

Proof 6.3

We know by definition that since ξ generates $\Phi(m)$ that $a = \xi^\ell$ for some $\ell \geqslant 1$. By Corollary 5.2 we

know that $\xi^\ell = \xi^{r_{\varphi(m)}(\ell)}$ and so we can take $\ell \in \{0, \dots, \varphi(m) - 1\}$. To prove the unicity statement it suffices to prove the second claim that if $i, j \in \mathbb{Z}$ then $\xi^i = \xi^j$ if and only if $i = j \mod \varphi(m)$.

To see this we merely note that $\xi^i = \xi^j$ if and only if $\xi^{i-j} = 1$ which happens, thanks to Corollary 5.5 if and only if $\varphi(m) \mid i - j$. Thus, $\xi^i = \xi^j$ if and only if $i = j \mod \varphi(m)$ as desired.

The takeaway from this is that when there is a primitive root modulo m, one can partially fill the whole left missing by the fact that Theorem 1.1 doesn't hold for $(\mathbb{Z}/m\mathbb{Z}, \cdot)$, by at least giving a sort of 'unique factorization' in $\Phi(m)$. Indeed, the above can be read as the statement that for any $u \in \Phi(m)$ there is a 'unique factorization' $u = \xi^\ell$ for some $\ell \in \{0, \dots, \varphi(m) - 1\}$.

Remark 6.3

One can actually improve the above 'unique factorization' statement from one concerning $\Phi(m)$ to a concerning all of $\mathbb{Z}/m\mathbb{Z}$, at least if $m = p^k$ for p prime and odd prime. Indeed, thanks to Theorem 6.5 we know that there is a primitive root ξ modulo p, and we can then say that every element of $\mathbb{Z}/m\mathbb{Z}$ can be written uniquely as $p^j\xi^\ell$ with $j \in \{0, \dots, k\}$ and $\ell \in \{0, \dots, \varphi(m) - 1\}$. This follows from Lemma 6.4 and Lemma 11.1.

Given Lemma 6.4 we make the following definition:

Definition 6.5

Let m be in $\mathbb{N}^*$, and assume that $\xi \in \Phi(m)$ is a primitive root. Then, we define the *ξ-adic valuation* of a, denoted $v_\xi(a)$, to be the unique element ℓ of $\{0, \dots, \varphi(m) - 1\}$ such that $\xi^\ell = a$.

Warning 6.1

Note that $v_\xi(a)$ is something that makes sense only modulo m! So, if $a \in \mathbb{Z}$ and ξ is a primitive root modulo m, then $a = \xi^{v_\xi(a)} \mod m$ only. In particular, if $\xi = p \mod m$ for some prime $p \in \mathbb{Z}$, there is no apparent relationship between $v_\xi(a)$ and $v_p(a)$ where, to be completely clear, in the former we are thinking of $a \in \mathbb{Z}/m\mathbb{Z}$ and in the latter we are thinking of $a \in \mathbb{Z}$.

As an example, suppose that $m = 17$. Then one can take $\xi = 3$. One can check that $v_\xi(-1) = 8$, but of course $v_3(-1)$, where -1 is thought of as an integer, is 0.

Now, recall that our current goal was to try and find a converse to Theorem 5.6. Given that the understanding to power equations in $\mathbb{Z}$ used Theorem 1.1, and the above remark that primitive roots fill the hole for Theorem 1.1 in the setting of $\Phi(m)$, it's not too shocking that primitive roots will factor heavily into our understanding of power equations. To wit:

Theorem 6.2: Euler's criterion

Let $m, n \in \mathbb{N}^*$ and $a \in \Phi(m)$. Suppose that there exists a primitive root modulo m, and fix one such primitive root, call it ξ. Then, the following are equivalent:

1. $x^n = a \mod m$ has a solution.
2. $a^{\frac{\varphi(m)}{\gcd(\varphi(m), n)}} = 1 \mod m$.

3. $\gcd(\varphi(m), n) \mid v_\xi(a)$.

Remark 6.4

Note that Theorem 6.2 is precisely the analogue of the result concerning power equations in $\mathbb{Z}$. Namely, we know that $x^n = a$, with $a \in \mathbb{N}^*$, has a solution in $\mathbb{Z}$ if and only if $n \mid v_p(a)$ for all primes p. Or, written differently, if and only if the equation $nx = v_p(a)$ has a solution for all primes p. Similarly, one can interpret the above as the statement that $x^n = a \mod m$ if and only if $nx = v_\xi(a) \mod \varphi(m)$ has where the advent of $\mod \varphi(m)$ is because the exponent i of ξ^i is only determined up to equivalence modulo $\varphi(m)$.

Proof 6.4: Theorem 6.2

Showing that 1. implies 2. has already been done in Corollary 5.6.

Let us now show that 1. and 3. are equivalent. Let us write $\ell := v_\xi(a)$ for short. Note that in the equation $x^n = \xi^\ell$ we can write x as ξ^k for some $k \in \{0, \dots, \varphi(m) - 1\}$, so that $x^n = \xi^{nk}$. Thus, we're trying to show that for some k the equation $\xi^{nk} = \xi^\ell$ has a solution. This is equivalent to $\xi^{nk-\ell} = 1$. But, by Lemma 6.4 we see that this is equivalent to $nk = \ell \mod \varphi(m)$. By Lemma 5.1 this is equivalent to $\gcd(\varphi(m), n) \mid \ell$ as desired.

Finally, let us show that 2. implies 3. To do this, we note that we can write $a = \xi^\ell$ for $\ell := v_\xi(a) \in \{0, \dots \varphi(m) - 1\}$. The claim is then that the equation $nx = \ell \mod \varphi(m)$ has a solution. To see this we note that since $a^{\frac{\varphi(m)}{\gcd(\varphi(m),n)}} = 1$ that

$$\begin{aligned} 1 &= a^{\frac{\varphi(m)}{\gcd(\varphi(m),n)}} \\ &= (\xi^\ell)^{\frac{\varphi(m)}{\gcd(\varphi(m),n)}} \\ &= \xi^{\frac{\ell\varphi(m)}{\gcd(\varphi(m),n)}} \end{aligned} \tag{111}$$

But, by Lemma 6.4 this is equivalent to the claim that

$$\frac{\ell\varphi(m)}{\gcd(\varphi(m), n)} = 0 \mod \varphi(m) \tag{112}$$

But, applying Lemma 5.2 with $r = \dfrac{\varphi(m)}{\gcd(\varphi(m), n)}$, $x = \ell$, and $y = 0$ shows that this is equivalent to

$$\ell = 0 \mod \gcd(\varphi(m), n) \tag{113}$$

from where the conclusion follows.

Moreover, using this, we can parameterize all the solutions to $x^n = a \mod m$ assuming that there is a primitive root modulo m:

Theorem 6.3: Explicit Euler criterion

Let $m, n \in \mathbb{N}^*$ and $a \in \Phi(m)$. Suppose that there exists a primitive root modulo m, and fix one such primitive root, call it ξ. Then, the following are equivalent:

1. $x^n = a \mod m$ has a solution.

2. $a^{\frac{\varphi(m)}{\gcd(\varphi(m),n)}} = 1 \mod m$.

3. $\gcd(\varphi(m), n) \mid v_\xi(a)$.

Moreover, assuming that ξ^{k_0} is a solution to $x^n = a \mod m$, the set of all solutions to $x^n = a \mod m$ is

$$\left\{\xi^{k_0 + k\frac{\varphi(m)}{\gcd(\varphi(m),n)}} : k = 0, \ldots, \gcd(\varphi(m), n) - 1\right\} \tag{114}$$

and this set has no repeats. Moreover, one can find an initial solution ξ^{k_0} by taking k_0 to be a solution to $nk = v_\xi(a) \mod \varphi(m)$, which one can find algorithmically using the Euclidean algorithm.

Proof 6.5

Set $\ell := v_\xi(a)$. We saw that solving $x^n = \xi^\ell \mod m$ was equivalent to solving $nx = \ell \mod m$. The rest follows from Lemma 5.1.

We immediately obtain the following corollary:

Corollary 6.2

Let $m \in \mathbb{N}^*$ and assume that there is a primitive root modulo m. Let $n \in \mathbb{N}^*$ and let $a \in \Phi(m)$. Then, the equation $x^n = a \mod m$ has either 0 or $\gcd(\varphi(m), n)$ solutions.

Let us give an example to the above:

Example 6.3

Let us compute the solutions to $x^3 = 15 \mod 31$ given that 3 is a primitive root modulo 31.

Let us first check that this has a solution. In other words, we need to compute $15^{\frac{30}{\gcd(30,3)}} = 15^{10} \mod 31$. But, $15^2 = 8 \mod 31$ and so $15^5 = 8^2 \cdot 15 = 2 \cdot 15 = -1 \mod 31$. So, evidently $15^{10} = (15^5)^2 = (-1)^2 = 1 \mod 30$. So, $x^3 = 15 \mod 31$ has a solution.

Now, to find all the solutions, we need to compute $v_\xi(15)$ with $\xi = 3$ or, in other words, we need to write $15 = 3^\ell$ for some ℓ. To do this we first compute that $15^2 = 8 \mod 31$. So, $15^3 = 8 \cdot 15 = 27 = 3^3 \mod 31$. So, $15^3 = 3^3 \mod 31$. So, we see that $3^{3\ell} = 3^3 \mod 31$ which says that $3\ell = 3 \mod 30$ or that $\ell = 1 \mod 10$ by Theorem 5.2. So, we know that ℓ is either $1, 11$, or 21. Clearly $\ell \neq 1$, and

$$3^{11} = (3^4)^2 \cdot 3^2 = 19^2 \cdot 9 = (-12)^2 \cdot 9 = 13 \mod 31 \tag{115}$$

so that $\ell \neq 11$. So, $\ell = 21$. Thus, we see that $15 = 3^{21}$. Thus, by Theorem 6.3 we need to solve $3x = 21 \mod 30$. An obvious answer to this is $x = 7$, and the other answers by Lemma 5.1 are $7 + 1 \cdot \frac{30}{3} = 17$ and $7 + 2 \cdot \frac{30}{3} = 27$. So, we see that the solutions to $x^3 = 15 \mod 31$ are $3^7, 3^{17}$, and 3^{27} which, if one wants to multiply out the numbers, is $17, 22$, and 23 modulo 31.

Let us also use Theorem 6.3 to give an alternate proof of Corollary 5.9 assuming that there is always a primitive root modulo p for p prime (which is true—see Theorem 6.5):

Proof 6.6: Corollary 5.9

Again it suffices to show that $z^2 = -1 \mod p$ has a solution if $p = 1 \mod 4$. Let ξ be a primitive root modulo p. Note then that $z := \xi^{\frac{p-1}{4}}$ has the property that $(z^2)^2 = \xi^{p-1} = 1$. By Exercise 4.2 this implies that $z^2 = \pm 1$. Now, if $z^2 = 1$ this would say that $\xi^{\frac{p-1}{2}} = 1$ so that $|\xi| \mid \frac{p-1}{2}$ by Lemma 5.5 which contradicts that $|\xi| = p - 1$. So, $z^2 = -1$, and the conclusion follows.

So, in conclusion we see that Theorem 6.3 gives, essentially, a complete, algorithmic understanding of power equations of the form $x^n = a \mod m$ assuming:

1. $a \in \Phi(m)$.
2. There is a primitive root modulo m.
3. We can effectively find an explicit primitive root ξ modulo m.
4. We can compute $v_\xi(a)$ effectively.

The first of these assumptions is fairly superficial, and will be removed quite easily in §11.1. It's the next three assumptions that are more serious. We will see in subsequent lectures that we have a pretty good understanding of 2. and 3. (handled in §6.5 and §10.3 respectively) but the question of 4. is a famously hard one. It is generally called the *discrete logarithm problem* and its computational complexity is notorious. In later lectures we will discuss some examples of algorithms to attack this problem, but they are still somewhat complicated and disappointingly slow.

6.4 An alternative parametrization

We would like to give an alternative, to Theorem 6.3, way to parametrize all the solutions to $x^n = a \mod m$ given a single solution $x_0 = \xi^{k_0}$. Along the way we will discuss some useful results in and of themselves.

The key observation is the following. Let's assume that x_0 is an initial solution (which is not a vacuous assumption) to $x^n = a \mod m$. Then, if x_1 is a second solution, then setting $z := x_0^{-1} x_1$ we have that

$$z^n = (x_0^n)^{-1} x_1^n = a^{-1} a = 1 \tag{116}$$

and, moreover, $x_1 = z x_0$. Conversely, we see that if $z^n = 1$ in $\Phi(m)$, then $z x_0$ is a solution to the equation $x^n = 1 \mod m$. Thus, in conclusion we see that the mapping $z \mapsto z x_0$ creates a bijection

$$\{z \in \Phi(m) : z^n = 1\} \to \{x \in \Phi(m) : x^n = a\} \tag{117}$$

Thus, to really flesh out Theorem 6.2 we need to figure out how to solve the equation $z^n = 1 \mod m$.

Now, there is an obvious way to solve this equation using Theorem 6.3, namely it's clear that we're trying to solve $\xi^{nk} = \xi^0 \mod m$ and thus we're trying to solve $nk = 0 \mod \varphi(m)$. This has the solutions $k \frac{\varphi(m)}{\gcd(\varphi(m), n)}$ for $k = 0, \dots, \gcd(\varphi(m), n) - 1$ from where we rederive Theorem 6.3 by adding k_0 using the observation from the previous paragraph.

That said, there is another fundamentally different way to think about finding the solutions to the equation $z^n = 1 \mod m$. To do this, we begin by making the following obvious, but insightful observation:

$$\{z \in \Phi(m) : z^n = 1\} = \bigsqcup_{\substack{d \mid n \\ d > 0}} \{z \in \Phi(m) : |z| = d\} \tag{118}$$

Indeed, if $z^n = 1$ then by Lemma 5.5 we know that $|z| \mid n$. Moreover, if $|z| = d$ for $d \mid n$ then evidently $z^n = 1$. The equality in (118) is then clear. Thus, to determine the identity of the set $\{z \in \Phi(m) : z^n = 1\}$ it suffices to understand what elements of $\Phi(m)$ have a given order.

The solution to that is the following:

Lemma 6.5

Let $m \in \mathbb{N}^*$, and suppose that there is a primitive root modulo m. Fix $\xi \in \Phi(m)$ to be one such primitive root. Let $d \in \mathbb{N}^*$. Then:

1. If $d \nmid \varphi(m)$ then $\{z \in \Phi(m) : |z| = d\}$ is empty.
2. If $d \mid \varphi(m)$, then
$$\{z \in \Phi(m) : |z| = d\} = \left\{\xi^{\frac{\varphi(m)r}{d}} : r \in \Phi(d)\right\} \tag{119}$$
and no two elements of the right-hand (multi)set are equal

Proof 6.7

1. If $|z| = d$ then we know from Corollary 5.3 that $d \mid \varphi(m)$. The claim follows.
2. We know that any $z \in \Phi(m)$ is of the form ξ^ℓ for some $\ell \geqslant 0$. Now, by Exercise 6.3 and the fact that $|\xi| = \varphi(m)$ we know that
$$|\xi^\ell| = \frac{\varphi(m)}{\gcd(\varphi(m), \ell)} \tag{120}$$
Thus, we're trying to solve the equation
$$\frac{\varphi(m)}{\gcd(\varphi(m), \ell)} = d \tag{121}$$
Now, note that since $d \mid \varphi(m)$ we can rewrite this as
$$\gcd(\varphi(m), \ell) = \frac{\varphi(m)}{d} \tag{122}$$
Now, since $\gcd(\varphi(m), \ell) \mid \ell$ we thus deduce that $\frac{\varphi(m)}{d} \mid \ell$. Let us write $\ell = \frac{\varphi(m)}{d}r$ for some $r \in \mathbb{N}$. Let us then note that
$$\gcd\left(\frac{\varphi(m)}{d}r, \varphi(m)\right) = \frac{\varphi(m)}{d}\gcd(r, d) \tag{123}$$
Indeed, this follows immediately from Exercise 3.6 by taking $a = \frac{\varphi(m)}{r}$, $b = \varphi(m)$, and $c = \frac{\varphi(m)}{d}$. Thus, we see that
$$\frac{\varphi(m)}{\gcd\left(\frac{\varphi(m)}{d}r, \varphi(m)\right)} = \frac{d}{\gcd(r, d)} \tag{124}$$
and thus if we want (122) to hold, we require that $\gcd(r, d) = 1$. Thus, we see that $|\xi^\ell| = d$ if and only if $\ell = \frac{\varphi(m)}{d}r$ for some $r \in \mathbb{Z}$.
Now, observe that if $r \notin \{0, \ldots, d-1\}$ then we can write $r = qd + r'$ for some $r' \in \{0, \ldots, d-1\}$

by Theorem 2.2. So then, note that

$$\begin{aligned}\xi^{\frac{\varphi(m)}{d}r} &= \xi^{\frac{\varphi(m)}{d}(qd+r')} \\ &= \xi^{\varphi(m)q+\frac{\varphi(m)}{d}r'} \\ &= (\xi^{\varphi(m)})^q\xi^{\frac{\varphi(m)}{d}r'} \\ &= \xi^{\frac{\varphi(m)}{d}r'}\end{aligned} \tag{125}$$

so we may as well assume that $r \in \{0,\dots,d-1\}$. Finally, we claim that if $r, r' \in \{0,\dots,d-1\}$ and

$$\xi^{\frac{\varphi(m)}{d}r} = \xi^{\frac{\varphi(m)}{d}r'} \tag{126}$$

then $r = r'$. Indeed, if this were true then we would see that dividing the left side by the right that

$$\xi^{\frac{\varphi(m)}{d}(r-r')} = 1 \tag{127}$$

Since $|\xi| = \varphi(m)$ Lemma 5.5 then implies that $\varphi(m) \mid \dfrac{\varphi(m)}{d}(r-r')$. This implies that $d \mid r-r'$. But, since $r, r' \in \{0,\dots,d-1\}$ this can only happen if $r = r'$.

In particular, from this we deduce the following useful corollary:

Corollary 6.3

Let $m \in \mathbb{N}^*$ be such that there is a primitive root modulo m. For any $d \in \mathbb{N}^*$ let N_d denote the number of elements of $\Phi(m)$ of order d. Then,

$$N_d = \begin{cases} 0 & \text{if} \quad d \nmid \varphi(m) \\ \varphi(d) & \text{if} \quad d \mid \varphi(m) \end{cases} \tag{128}$$

Putting all of our discussion together, we can give an alternative, to Theorem 6.3, way to make Theorem 6.2 significantly more explicit:

Theorem 6.4: Explicit Euler criterion (alternate)

Let $m, n \in \mathbb{N}^*$ and $a \in \Phi(m)$. Suppose that there exists a primitive root modulo m, and fix one such primitive root, call it ξ. Then, the following are equivalent:

1. $x^n = a \mod m$ has a solution.
2. $a^{\frac{\varphi(m)}{\gcd(\varphi(m),n)}} = 1 \mod m$.
3. $\gcd(\varphi(m), n) \mid v_\xi(a)$.

Moreover, assuming that ξ^{k_0} is a solution to $x^n = a \mod m$, the set of all solutions to $x^n = a \mod m$ is

$$\bigsqcup_{\substack{d \mid \gcd(\varphi(m),n) \\ d>0}} \left\{ \xi^{k_0+\frac{\varphi(m)}{d}r} : r \in \{0,\dots,d-1\} \text{ and } \gcd(r,d) = 1 \right\} \tag{129}$$

and this set has no repetitive elements.

Proof 6.8

The only thing that needs justifying is why the disjoint union in (129) runs over positive d dividing $\gcd(\varphi(m), n)$. Well, as observed in (118) there is a natural disjoint union over d dividing n, but by Lemma 6.5 part (1), we know that $\{z \in \Phi(m) : z^d = 1\}$ is empty if $d \nmid \varphi(m)$. Thus, we really only need to consider positive d dividing n and $\varphi(m)$, which is the same thing as positive d dividing $\gcd(\varphi(m), n)$.

Let us give an example of of this version of solving power equations carried out in practice:

Example 6.4

Let us find all the solutions to $x^4 = 4 \mod 17$ given by 3 is a primitive root modulo 17. To do this we begin by checking that $x^4 = 4$ has a solution modulo 17. Namely, we compute that

$$4^{\frac{16}{\gcd(4,16)}} = 4^4 = 256 = 1 \mod 17 \tag{130}$$

Next, we need to find ℓ such that $3^\ell = 4$. One can compute that $4^2 = 17 = -1 = 3^8 \mod 17$. The latter equality is clear since $(3^8)^2 = 1 \mod 17$ so that $3^8 = \pm 1 \mod 17$ by Exercise 4.2 but since $|3| = 16$ we know that $3^8 \neq 1$. So, we know that $4^2 = 3^8 \mod 17$ so that $3^{2\ell} = 3^8 \mod 17$. This implies that $2\ell = 8 \mod 16$ and this has only two solutions, which are $\ell = 4$ and $\ell = 12$ (by Lemma 5.1). One sees that $3^4 = 13 \neq 4$ so we deduce that $3^{12} = 4 \mod 17$.

So, we see that we need to find a solution to $3^{4k} = 3^{12} \mod 17$ which is equivalent to $4k = 12 \mod 16$. This has the obvious solution $k = 3$, so that one initial solution to $x^4 = 4 \mod 17$ is $3^3 = 10 \mod 17$. We then use Theorem 6.4 to find all the solutions as follows. The only positive divisors of $\gcd(4, 16) = 4$ are $1, 2$ and 4. For $d = 1$ we have $\frac{16}{1}r$ for $r \in \{0\}$ is just 0 so that the initial solution contributed by $d = 1$ is just 10. For $d = 2$ we have that $\frac{16}{2}r$ for $r \in \{0, 1, 2\}$ with $\gcd(r, 2) = 1$ is just $\frac{16}{2} \cdot 1 = 8$. So, the contributed solution for $d = 2$ is $10 \cdot 3^8 = 7$. Finally, for $d = 4$ we have that $\frac{16}{4}r$ for $r \in \{0, 1, 2, 3\}$ with $\gcd(r, 4) = 1$ is just $\frac{16}{4} \cdot 1 = 4$ and $\frac{16}{4} \cdot 3 = 12$. Thus, we see that the contribution of solutions when $d = 4$ are $10 \cdot 3^4 = 11$ and $10 \cdot 3^{12} = 6$. Thus, the total set of solutions to $x^4 = 4 \mod 17$ is $\{10, 7, 11, 6\}$.

6.5 Existence of primitive roots

Now, as mentioned at the end of §6.3, Theorem 6.2 gives an essentially complete understanding of the power equation $x^n = a \mod m$ up to four assumptions, for which the first serious one is the question of existence of a primitive root modulo m. This is a surprisingly complicated question.

Let us consider some examples:

Example 6.5

The number 2 is a primitive root modulo 25. Indeed, we know from Corollary 5.3 that $|2|$ divides $\varphi(25) = 20 = 2^2 \cdot 5$. If $|2| \neq 20$ then it's clear that either $2^4 = 1 \mod 25$ or $2^5 = 1 \mod 25$. But, neither of these is strue, so 2 is a primitive root modulo 25.

Example 6.6

The number 5 is a primitive root modulo 6. Indeed, $\Phi(6) = \{1, 5\}$ and so the result is clear.

Unfortunately it's not always true that there are primitive roots:

Example 6.7

Let $m = 8$. Then, $\Phi(m) = \{1, 3, 5, 7\}$. One can easily check that $3^2 = 5^2 = 7^2 = 1 \mod 8$ so that every element of $\Phi(8)$ has either order 1 or 2, and none of the required order $\varphi(8) = 4$ to be a primitive root.

The question then becomes for which $m \in \mathbb{N}^*$ do there, in fact, exist primitive roots modulo m. To answer that, we have the following compact result:

Theorem 6.5

Let $m \in \mathbb{N}^*$. Then, the following are equivalent:

1. There is a primitive root modulo m.
2. The integer m one of the following: 2, 4, p^k where p is an odd prime and $k \in \mathbb{N}^*$, or $2p^k$ where p is an odd prime and $k \in \mathbb{N}^*$.

This theorem is remarkable and, in particular, not at all easy to prove—it will be a triumph when we do prove it. In addition to being remarkable, this theorem is also mysterious. Why are the numbers m listed in Theorem 6.5 the only m such that there is a primitive root modulo m? It seems totally unmotivated. The answer to this is a beautiful story that will unfold to us as we develop more understanding of the objects $\mathbb{Z}/m\mathbb{Z}$ and modulus Diophantine equations.

Remark 6.5

For those that have taken algebra, if $m = p^k$ for an odd prime p, then Theorem 6.5 says that, as a group, $\Phi(m) \cong \mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$. If $m = 2^k$ for $k > 2$, then what is true is that $\Phi(m) \cong (\mathbb{Z}/2^{k-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

6.6 Exercises

Exercise 6.1

Problem: Find all solutions to $x^4 = 9 \mod 14$ using Theorem 6.3.

Solution: We first need to find a primitive root modulo 14. Note that $\Phi(14) = \{1, 3, 5, 9, 11, 13\}$. Note that $3^2 = 9 \neq 1 \mod 14$, and $3^3 = 27 = -1 \neq 1 \mod 14$ so that 3 is a primitive root modulo 14. Next we need to find ℓ such that $9 = 3^\ell \mod 14$. Clearly we can take $\ell = 2$. We next need to find k such that $\varphi(14) = 6 \mid 4k - 2$. We can clearly take $k = 2$. We then see form Theorem 6.3 that the set

of solutions to $x^4 = 9 \mod 14$ is

$$\{3^2, 3^{2+3}\} = \{9, 5\} \tag{131}$$

Exercise 6.2

Problem: Show that the Diophantine equation $51x^8 - 202xy = 2$ has no solution (note: 101 is prime).

Solution: Suppose that this Diophantine equation had a solution. Then, reducing it modulo 101 shows that $51x^8 = 2 \mod 101$ has a solution. Note that $51^{-1} = 2$ and so this equation is equivalent to $x^8 = 4 \mod 101$. To show that this has no solution it suffices, by Theorem 6.3, to show that $4^{\frac{50}{\gcd(8,50)}} = 4^{25} \neq 1 \mod 101$. But, using modular exponentiation one computes that $4^{25} = -1 \mod 101$. Specifically, $4^5 = 1024 = 14 \mod 101$. Then,

$$14^2 = 196 = 95 = -6 \mod 101 \tag{132}$$

So then,

$$14^4 = (-6)^2 = 36 \mod 101 \tag{133}$$

So, then, finally,

$$4^{25} = (4^5)^5 = 14^5 = 14^4 \cdot 14 = 36 \cdot 14 = 504 = -1 \mod 101 \tag{134}$$

Thus, $4^{25} = -1 \neq 1 \mod 101$, so that $x^8 = 4 \mod 101$ has no solution.

Exercise 6.3

Problem: Let $m > 1$ be an integer and $a \in \Phi(m)$. Show that for all $\ell \geqslant 0$ one has that

$$|a^\ell| = \frac{|a|}{\gcd(|a|, \ell)} \tag{135}$$

Solution: Let us set $g := \frac{|a|}{\gcd(|a|, \ell)}$. Let's first show that $(a^\ell)^g = 1$. But, note that

$$\begin{aligned} (a^\ell)^g &= a^{\frac{\ell|a|}{\gcd(|a|,\ell)}} \\ &= (a^{|a|})^{\frac{\ell}{\gcd(|a|,\ell)}} \\ &= 1^{\frac{\ell}{\gcd(|a|,\ell)}} \\ &= 1 \end{aligned} \tag{136}$$

Thus, we see that $|a^\ell| \mid g$ by Lemma 5.5. Conversely, note that $(a^\ell)^{|a^\ell|} = 1$ and so $a^{\ell|a^\ell|} = 1$. Thus, again by Lemma 5.5, we see that $|a| \mid \ell|a^\ell|$. Dividing both sides by $\gcd(|a|, \ell)$ shows that $g \mid \frac{\ell}{\gcd(|a|,\ell)}|a^\ell|$. Now, evidently $\gcd\left(g, \frac{\ell}{\gcd(|a|,\ell)}\right) = 1$ and thus we deduce that $g \mid |a^\ell|$. The claim then follows.

7 Lecture 7: The Chinese remainder theorem

7.1 Setup

As discussed at the end of §6.3 Theorem 6.3 gives us an essentially full understanding of power equations of the form $x^n = a \mod m$, up to four assumptions, one of which is that there is a primitive root modulo m. But, Theorem 6.5 shows that this limits the domain of Theorem 6.3 to, essentially, powers of an odd prime p. This is, of course, unacceptable. We would like to be able to have an algorithmic way to solve equations like $x^3 = 18 \mod 36$.

One ray of hope that we may be able to make use of Theorem 6.3 even in the situation when there is no primitive root modulo m is the following observation. Namely, note that for any $m \in \mathbb{N}^*$ (where, for now, we assume that $v_2(m) \leqslant 2$ so that $2^k \nmid m$ for $k > 2$) we can prime factorize $m = p_1^{e_1} \cdots p_s^{e_s}$ and modulo each prime power $p_i^{e_i}$ we have primitive roots. Thus, with an eye towards solving power equations modulo m without primitive roots, it would be excellent if we could try to solve equations modulo m by trying to solve equations modulo each $p_i^{e_i}$ individually and try to piece them together to actual solutions modulo m.

This is less crazy than it sounds since, in some sense, the world of coprime moduli don't really see each other. Namely, if we factorize $m = n_1 n_2$ with $n_1, n_2 > 1$ and $\gcd(n_1, n_2) = 1$ then for $x \in \mathbb{Z}$ we have that $m \mid x$ if and only if $n_1 \mid x$ and $n_2 \mid x$ and, moreover, whether $n_1 \mid x$ is entirely independent of whether $n_2 \mid x$. Thus it seems like checking things modulo m should reduce, in some sense, to checking things modulo n_1 and n_2 independently.

Thus, our goal for today is to make sense of the following:

Goal 7.1: Today

Explain in what way solving equations in $\mathbb{Z}/m\mathbb{Z}$ is the same thing as solving equations in $\mathbb{Z}/n_1\mathbb{Z}$ and $\mathbb{Z}/n_2\mathbb{Z}$ separately but simultaneously.

In particular this will allow us (in most situations) to reduce ourselves from solving equations modulo m where there are no primitive roots to solving equations modulo m where there are primitive roots. But, that's not all. We will, in fact, see that fulfilling Goal 7.1 will actually clarify why only the listed numbers m in Theorem 6.5 can have primitive roots modulo m (the more difficult claim that the listed numbers do have primitive roots modulo m will come later).

7.2 The Chinese remainder theorem

The way to rigorize Goal 7.1 is to first consider an object which, in some sense, encapsulates the integers moduli two different numbers simultaneously, but separately. In particular, let us make the following definition:

Definition 7.1

Let n_1 and n_2 be in $\mathbb{N}^*$. Then, the *product of* $\mathbb{Z}/n_1\mathbb{Z}$ *and* $\mathbb{Z}/n_2\mathbb{Z}$, denoted $(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ is the following set:

$$(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) := \{(a, b) : a \in \mathbb{Z}/n_1\mathbb{Z} \text{ and } b \in \mathbb{Z}/n_2\mathbb{Z}\} \tag{137}$$

Less cryptically, the product of $\mathbb{Z}/n_1\mathbb{Z}$ and $\mathbb{Z}/n_2\mathbb{Z}$ is just the set of all pairs of elements of $\mathbb{Z}/n_1\mathbb{Z}$ and $\mathbb{Z}/n_2\mathbb{Z}$. We also turn the product into an algebraic object as follows:

Definition 7.2

Let n_1 and n_2 be in $\mathbb{N}^*$. Given (a, b) and (c, d) in $(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ define the *addition/subtraction*

of (a, b) and (c, d) as

$$(a, b) \pm (c, d) = (a \pm c, b \pm d) \tag{138}$$

and the *multiplication* of (a, b) and (c, d) as

$$(a, b) \cdot (c, d) = (ac, bd) \tag{139}$$

Example 7.1

Let $n_1 = 3$ and $n_2 = 4$. Then,

$$(1, 2) + (2, 1) = (0, 3) \tag{140}$$

and

$$(1, 0) \cdot (0, 1) = (0, 0) \tag{141}$$

Let us make the following notion of modulus Diophantine equation in $(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$:

Definition 7.3

Let n_1, n_2, and v be in $\mathbb{N}^*$. Given $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$ we evaluate f on an element $((a_1, b_1), \ldots, (a_v, b_v)) \in ((\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}))^v$ using the addition/subtraction and multiplication from Definition 7.2 and interpreting constants $z \in \mathbb{Z}$ as (z, z). We then define the set $X_f((\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}))$ as follows:

$$X_f((\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})) := \{\mathbf{c} = ((a_1, b_1), \ldots, (a_v, b_v)) \in ((\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}))^v : f(\mathbf{c}) = (0, 0)\} \tag{142}$$

Example 7.2

Let $n_1 = 3$, $n_2 = 4$, and $f(x, y) = x^2 + 3xy - 1$. Note then that we evaluate f on $((1, 2), (3, 1))$ as follows

$$\begin{aligned} f((1, 2), (3, 1)) &= (1, 2)^2 + 3(1, 2)(3, 1) - (1, 1) \\ &= (1^2, 2^2) + (3 \cdot 1 \cdot 3, 3 \cdot 2 \cdot 1) - (1, 1) \\ &= (1, 0) + (0, 2) - (1, 1) \\ &= (1 + 0 - 1, 0 + 2 - 1) \\ &= (0, 1) \end{aligned} \tag{143}$$

so that $((1, 2), (3, 1))$ is not in $X_f((\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}))$. One can check that $((1, 1), (0, 0)$ is in $X_f((\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}))$.

Now, given n_1, n_2, and v in $\mathbb{N}^*$ there is a natural bijection

$$(\mathbb{Z}/n_1\mathbb{Z})^v \times (\mathbb{Z}/n_2\mathbb{Z})^v \to ((\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}))^v \tag{144}$$

given by

$$((a_1, \ldots, a_v), (b_1, \ldots, b_v)) \mapsto ((a_1, b_1), \ldots, (a_v, b_v)) \tag{145}$$

and under this identification Definition 7.3 becomes much more intuitively. Namely, it is really just describing the notion of a *simultaneous Diophantine equation*:

Lemma 7.1

Let n_1, n_2, and v be in $\mathbb{N}^*$. Given $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$, then under the bijection (144) one has the following equality:

$$X_f((\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})) = X_f(\mathbb{Z}/n_1\mathbb{Z}) \times X_f(\mathbb{Z}/n_2\mathbb{Z}) \tag{146}$$

Proof 7.1

Let us show this only in the case $v = 1$ to less notation. Since addition and multiplication of elements of $(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ happen coordinate-by-coordinate it's easy to see that for any $(a, b) \in (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ that

$$f(a, b) = (f(a), f(b)) \tag{147}$$

Thus, we see that $f(a, b) = (0, 0)$ if and only if $f(a) = 0$ in $\mathbb{Z}/n_1\mathbb{Z}$ and $f(b) = 0$ in $\mathbb{Z}/n_2\mathbb{Z}$.

Let us now go back to the setting of §7.1. Namely, let n_1 and n_2 be elements of $\mathbb{N}^*$ and set $m := n_1 n_2$. Note then that since $n_1 \mid m$ and $n_2 \mid m$ we get, for any $v \in \mathbb{N}^*$, natural reduction maps

$$r_{n_1} : (\mathbb{Z}/m\mathbb{Z})^v \to (\mathbb{Z}/n_1\mathbb{Z})^v \tag{148}$$

and

$$r_{n_2} : (\mathbb{Z}/m\mathbb{Z})^v \to (\mathbb{Z}/n_2\mathbb{Z})^v \tag{149}$$

as in §4.3. We then obtain a natural reduction map to the product:

Definition 7.4

Let n_1, n_2, and v be in $\mathbb{N}^*$ and set $m := n_1 n_2$. We then define the *reduction map*

$$r_{n_1,n_2} = r : (\mathbb{Z}/m\mathbb{Z})^v \to (\mathbb{Z}/n_1\mathbb{Z})^v \times (\mathbb{Z}/n_2\mathbb{Z})^v \tag{150}$$

as follows:

$$r(a_1, \ldots, a_v) = (r_{n_1}(a_1, \ldots, a_v), r_{n_2}(a_1, \ldots, a_v)) \tag{151}$$

as well as the *reduction map*

$$r_{n_1,n_2} = r : (\mathbb{Z}/m\mathbb{Z})^v \to ((\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}))^v \tag{152}$$

given by

$$r(a_1, \ldots, a_n) = ((r_{n_1}(a_1), r_{n_2}(a_1), \ldots, (r_{n_1}(a_v), r_{n_2}(a_v))) \tag{153}$$

The two maps in (150) and (152) are really the same map, as they become equal under the identification given in 144.

Example 7.3

Take $n_1 = 2$ and $n_2 = 3$. The map is then

$$r : \mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \tag{154}$$

given by

$$\begin{aligned} r(0) &= (0 \mod 2, 0 \mod 3) = (0,0) \\ r(1) &= (1 \mod 2, 1 \mod 3) = (1,1) \\ r(2) &= (2 \mod 2, 2 \mod 3) = (0,2) \\ r(3) &= (3 \mod 2, 3 \mod 3) = (1,0) \\ r(4) &= (4 \mod 2, 4 \mod 3) = (0,1) \\ r(5) &= (5 \mod 2, 5 \mod 3) = (1,2) \end{aligned} \tag{155}$$

Let us note the following basic properties of the map r:

Lemma 7.2

The map $r : \mathbb{Z}/m\mathbb{Z} \to (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ satisfies the following basic properties:

1. $r(0) = (0,0)$
2. $r(1) = (1,1)$
3. $r(xy) = r(x)r(y)$
4. $r(x+y) = r(x) + r(y)$

The way we wish to justify the claim that working modulo n_1 and n_2 are indepdent operations is the following:

Theorem 7.1: Baby Chinese remainder theorem

Let n_1 and n_2 be in $\mathbb{N}^*$ and set $m := n_1 n_2$. Then, the map

$$r : \mathbb{Z}/m\mathbb{Z} \to (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \tag{156}$$

is a bijection if and only if n_1 and n_2 are coprime.

Proof 7.2

Suppose that n_1 and n_2 are coprime. If $r(a) = r(b)$ then $r(a-b) = 0$. This says that $a - b \mod n_1$ and $a - b \mod n_2$ are zero. This is equivalent to saying that $n_1 \mid a-b$ and $n_2 \mid a-b$. Since n_1 and n_2 are coprime this implies that $m = n_1 n_2 \mid a-b$ and so $a = b \mod m$. This shows that r is injective, but since both $\mathbb{Z}/m\mathbb{Z}$ and $(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ have the same finite cardinality, any injection between them is a bijection.

Suppose now that $d := \gcd(n_1, n_2) > 1$ and thus, by Exercise 3.4 this implies that

$$0 < \operatorname{lcm}(n_1, n_2) < m \tag{157}$$

In particular, $\operatorname{lcm}(n_1, n_2) \neq 0$. That said, $r(\operatorname{lcm}(n_1, n_2)) = (0,0) = r(0)$. Thus, r is not bijective.

Now, the reason that we have called this the 'baby' Chinese remainder theorem is that it's too inexplicit—instead of giving an explicit inverse to r it evoked the fact that an injection from a finite set to itself is a bijection. So, it'd be better to explicitly describe an inverse to r. This is what the Chinese remainder theorem does:

Theorem 7.2: Chinese remainder theorem

Let n_1 and n_2 be coprime elements of $\mathbb{N}^*$ and set $m := n_1 n_2$. Let $x, y \in \mathbb{Z}$ be such that $n_1 x = 1 \mod n_2$ and $n_2 y = 1 \mod n_1$ (possible by Lemma 5.2). Then, r is a bijection with inverse

$$s : (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \to \mathbb{Z}/m\mathbb{Z} \tag{158}$$

given by

$$s(a, b) = n_1 x b + n_2 y a \tag{159}$$

Proof 7.3

We need to check that $r \circ s$ and $s \circ r$ are the identity. To see that $r \circ s$ is the identity we need to show that for all $(a, b) \in (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ that

$$r(n_1 x b + n_2 y a) = (a, b) \tag{160}$$

but

$$\begin{aligned} r(n_1 x b + n_2 y a) &= (n_1 x b + n_2 y a \mod n_1, n_1 x b + n_2 y a \mod n_2) \\ &= (n_2 y a \mod n_1, n_1 x b \mod n_2) \\ &= (a \mod n_1, b \mod n_2) \end{aligned} \tag{161}$$

as desired. To show that $s \circ r = \mathrm{id}$ we need to show that for all $z \in \mathbb{Z}/m\mathbb{Z}$ that

$$n_1 x z + n_2 y z = z \mod m \tag{162}$$

To do this means we need to show that $m \mid (n_1 x z + n_2 y z - z)$. But, $n_1 x z + n_2 y z - z = (n_1 x + n_2 y - 1) z$. Now, modulo n_1 $n_1 x + n_2 y - 1$ is zero, and similarly modulo n_2 $n_1 x + n_2 y - 1$ is zero. Since $\gcd(n_1, n_2) = 1$ and $m = n_1 n_2$ this implies that modulo m one has that $n_1 x + n_2 y - 1$ is zero. The conclusion follows.

One corollary of the Chinese remainder theorem is the following:

Corollary 7.1: Chinese remainder theorem (equational form)

Let n_1 and n_2 be coprime elements of $\mathbb{N}^*$. Then, the simultaneous modulus Diophantine equation

$$\begin{cases} z = a \mod n_1 \\ z = b \mod n_2 \end{cases} \tag{163}$$

has a solution. In fact, one can take $z = n_1 x b + n_2 y a$ (with notation as in Theorem 7.2). Moreover, this integer z is unique modulo $n_1 n_2$

Example 7.4

Let's solve the simultaneous modulus Diophantine equation:

$$\begin{cases} z = 6 \mod 8 \\ z = 5 \mod 15 \end{cases} \tag{164}$$

To do this we first need to find $8^{-1} \mod 15$ and $15^{-1} \mod 8$. It's clear that $8^{-1} = 2 \mod 15$ and that $15^{-1} = 7 \mod 8$. Thus, we see that $z = 8 \cdot 2 \cdot 5 + 6 \cdot 15 \cdot 710$ works. Moreover, this integer is unique modulo 120. In particular, we see that $r_{120}(710) = 110$ works as well.

There is also a version of the Chinese Remainder Theorem for more than two coprime numbers:

Theorem 7.3: General Chinese Remainder Theorem

Let k be an element of $\mathbb{N}^*$, $n_1, \ldots, n_k$ pairwise coprime elements of $\mathbb{N}^*$, and set $m := n_1 \cdots n_k$. Then, the natural reduction map

$$\begin{aligned} r : \mathbb{Z}/m\mathbb{Z} &\to (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}) \\ : x \mod m &\mapsto (x \mod n_1, \cdots, x \mod n_k) \end{aligned} \tag{165}$$

is a bijection with inverse s given as follows. For each $i = 1, \ldots, k$ let x_i be

$$x_i := \left(\prod_{\substack{j=1,\ldots,k \\ j \neq i}} x_j \right)^{-1} \mod n_i \tag{166}$$

then we set

$$s(a_1, \ldots, a_k) = a_1 n_1 x_1 + \cdots a_k n_k x_k \tag{167}$$

The proof is exactly the same as in the case of Theorem 7.2. This result is no conceptually harder than the case when $k = 2$, but we will often times restrict to the case $k = 2$ for notational convenience. Moreover, it's easy to see that the obvious analagous results from Lemma 7.2 holds true for the map from Theorem 7.3.

7.3 Consequences for modulus Diophantine equations

One of the main reasons that we care about Theorem 7.2 is the implication it has about solving modulus Diophantine equations modulo the product of two coprime integers:

Corollary 7.2

Let n_1 and n_2 be coprime elements of $\mathbb{N}^*$ and set $m := n_1 n_2$. Let $v \in \mathbb{N}^*$ and let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Then the map

$$X_f(\mathbb{Z}/m\mathbb{Z}) \to X_f(\mathbb{Z}/n_1\mathbb{Z}) \times X_f(\mathbb{Z}/n_2\mathbb{Z}) \tag{168}$$

given by

$$\mathbf{a} \mapsto (\mathbf{a} \mod n_1, \mathbf{a} \mod n_2) \tag{169}$$

is a bijection. Moreover, if $n_1 x = 1 \mod n_2$ and $n_2 y = 1 \mod n_1$ then the inverse s of r is given by

$$s((b_1, \ldots, b_v), (c_1, \ldots, c_v)) = (n_1 x c_1 + n_2 y b_1, \ldots, n_1 x c_v + n_2 y b_v) \tag{170}$$

Let's give an example:

Example 7.5

Let's solve the equation $x^3 + x = 2 \mod 30$. We first solve the equation modulo 3 and modulo 10. Modulo 3 one checks that the only solutions are $x = 1$. Modulo 10 one checks that the only solutions are $x = 1, 6$. Now $10^{-1} = 1 \mod 3$ and $3^{-1} = 7 \mod 10$. So, to get the solutions modulo 30 we take $10 \cdot 1 \cdot 1 + 3 \cdot 7 \cdot 1$ and $10 \cdot 1 \cdot 1 + 3 \cdot 7 \cdot 6$. Simplifying these we see that the solutions modulo 30 are 1 and 16.

Let's do an example with more than one variable:

Example 7.6

Solve $x^3 - 2y = 1 \mod 6$. Let's first solve $x^3 - 2y = 1 \mod 2$ and $x^3 - 2y = 1 \mod 3$. Now, modulo 2 one can easily check that the only solutions are $(1, 0)$ and $(1, 1)$ (note that $x^3 - 2y = x^3$ modulo 2). Modulo 3 one can check that the solutions are $(1, 0)$, $(0, 1)$, and $(2, 2)$. Note that $2^{-1} = 2 \mod 3$ and $3^{-1} = 1 \mod 2$. Thus, for a solution (a, b) modulo 2 and a solution (c, d) modulo 3 we get the solution $(3a + 4c, 3b + 4d)$ modulo 6. Doing this for our pairs above gives the solution set

$$\{(1, 0), (3, 4), (5, 2), (1, 3), (3, 1), (5, 5)\} \tag{171}$$

The slogan one should take away from this is the following: "to solve equations modulo m is the same thing as solving equations modulo n_1 and modulo n_2 separately". In other words, we've justified our goal for today.

Note that one corollary we get from the above is the following:

Corollary 7.3

Let n_1 and n_2 be coprime elements of $\mathbb{N}^*$ and set $m := n_1 n_2$. Let $v \in \mathbb{N}^*$ and let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Then,

$$\#X_f(\mathbb{Z}/m\mathbb{Z}) = (\#X_f(\mathbb{Z}/n_1\mathbb{Z}))(\#X_f(\mathbb{Z}/n_2\mathbb{Z})) \tag{172}$$

Thus, in particular, $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ if and only if $X_f(\mathbb{Z}/n_1\mathbb{Z}) \neq \varnothing$ and $X_f(\mathbb{Z}/n_2\mathbb{Z}) \neq \varnothing$.

Example 7.7

The equation $x^2 - 3y^2 = 2 \mod 6$ has no solutions. Indeed, since $6 = 3 \cdot 2$ it suffices to check that $x^2 - 3y^2 = 2 \mod 3$ has no solutions. But, $x^2 - 3y^2 = x^2 \mod 3$. Moreover, x^2 is always 0 or 1 (by Corollary 5.5) and so clearly never 2. The conclusion follows.

Remark 7.1

Note that there is a direct analogue of Corollary 7.2 for the product of k pairwise coprime numbers, in the exact obvious way using Theorem 7.3, but it's just too notationally cumbersome to deal with. We will use its corollarious implication that if $n_1, \ldots, n_k$ are coprime, then to solve a Diophantine equation modulo $n_1 \cdots n_k$ is the same as to solve it modulo each n_i individually.

7.4 Implications for units modulo m, the Euler totient function, and primitive roots

Another nice result that follows from Theorem 7.2 is the following:

Theorem 7.4

Let n_1 and n_2 be coprime elements of $\mathbb{N}^*$ and set $m := n_1 n_2$. Then, the reduction map

$$r : \mathbb{Z}/m\mathbb{Z} \to (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_1\mathbb{Z}) \tag{173}$$

induces a bijection

$$\Phi(m) \to \Phi(n_1) \times \Phi(n_2) \tag{174}$$

with inverse s as in Theorem 7.2.

Proof 7.4

By Theorem 7.2 it suffices to show that $r(\Phi(m)) = \Phi(n_1) \times \Phi(n_2)$. Since $r(1) = (1, 1)$ and r is a bijection we see that for $x \in \mathbb{Z}/m\mathbb{Z}$ the equation

$$xy = 1 \mod m \tag{175}$$

has a solution if and only if the equation

$$r(xy) = (1, 1) \tag{176}$$

has a solution. But, since

$$r(xy) = (xy \mod n_1 m, xy \mod n_2) \tag{177}$$

we see that this has a solution if and only if

$$xy \mod n_1 \tag{178}$$

and

$$xy \mod n_2 \tag{179}$$

both have a solution. The conclusion follows.

From this we deduce the following nice result about the Euler totient function:

Theorem 7.5

Let n_1 and n_2 be coprime elements of $\mathbb{N}^*$ and set $m := n_1 n_2$. Then, $\varphi(m) = \varphi(n_1)\varphi(n_2)$.

This is often times referred to as the statement that φ is *multiplicative*. From it we deduce the following nice formula for the Euler totient function:

Corollary 7.4

Let m be an element of $\mathbb{N}^*$, and suppose that $m = p_1^{e_1} \cdots p_\ell^{e_\ell}$ with p_i prime, $p_i \neq p_j$ for $i \neq j$, and $e_i \geqslant 1$. Then,

$$\varphi(m) = \prod_{i=1}^{\ell} p_i^{e_i - 1}(p_i - 1) \tag{180}$$

Moreover, from Theorem 7.4 and Corollary 7.4 we are able to justify a portion of why only the numbers m listed in Theorem 6.5 can actually have primitive roots modulo m. Namely:

Theorem 7.6

Let $m \in \mathbb{N}^*$ and suppose that m is not of the form p^k or $2p^k$ for p a prime. Then, there is no primitive root modulo m.

Note that this doesn't shown that there is no primitive root modulo 2^k for $k > 2$, we'll return to this later. In fact, one can actually give two proofs of this theorem. Besides the following, there is one exercise in our notes.

Proof 7.5: Theorem 7.6, proof 1

The assumptions on m allow us to write $m = n_1 n_2$ with n_1 and n_2 coprime elements of $\mathbb{N}^*$ both of which are greater than 2. In particular, from Theorem 7.4 we get a bijection

$$r : \Phi(m) \to \Phi(n_1) \times \Phi(n_2) \tag{181}$$

which satisfies $r(1) = (1, 1)$ and $r(xy) = r(x)r(y)$. Let us now assume that there is a primitive root x modulo m.

Let $k := \text{lcm}(\varphi(n_1), \varphi(n_2))$. From Corollary 7.4 one can easily see that since n_1 and n_2 are both greater than 2 that $\varphi(n_1)$ and $\varphi(n_2)$ are both even. Thus, $\gcd(\varphi(n_1), \varphi(n_2)) > 1$ and thus $k < \varphi(n_1)\varphi(n_2) = \varphi(m)$ (thanks to Exercise 3.4 and Theorem 7.5). Now, from Theorem 5.3 we know that $a^k = 1$ in $\mathbb{Z}/n_1\mathbb{Z}$ and $b^k = 1$ in $\mathbb{Z}/n_2\mathbb{Z}$. Thus, $(a, b)^k = (1, 1)$ in $(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$.

Thus, we know that $r(x)^k = (1, 1)$ and, since $r(x)^k = r(x^k)$ and r is a bijection we deduce that $x^k = 1$. But, this implies that $|x| \leqslant k < \varphi(m)$. This contradicts that $|x| = \varphi(m)$ since x is a primitive root modulo m.

7.5 Generalized Euler criterion for more general m

Thanks to Corollary 7.2 and Theorem 6.2 we deduce the following:

Theorem 7.7

Let $m \in \mathbb{N}^*$ be such that $v_2(m) \leqslant 2$. Let $m = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of m with each $e_i \geqslant 1$ and $p_i \neq p_j$ for $i \neq j$. Let $n \in \mathbb{N}^*$ and $a \in \Phi(m)$. Then, $x^n = a \mod m$ has a solution if and only if for $i = 1, \ldots, k$ we have that

$$a^{\frac{p_i^{e_i-1}(p_i-1)}{\gcd(n, p_i^{e_i-1}(p_i-1))}} = 1 \mod p_i^{e_i} \tag{182}$$

Moreover, assuming that $x^n = a \mod m$ has a solution, it has

$$\prod_{i=1}^{k} \gcd(\varphi(p_i^{e_i}), n) \tag{183}$$

solutions. These solutions can be constructed modulo each $p_i^{e_i}$ using Theorem 6.3 and then reconstructed as solutions modulo $\mathbb{Z}/m\mathbb{Z}$ using Theorem 7.3.

Proof 7.6

This follows immediately from Theorem 6.2, Theorem 6.5 (with the assumption that $v_2(m) \leqslant 2$ so that no power of 2 greater than 4 shows up), and Corollary 7.5.

7.6 Exercises

Exercise 7.1

Problem: Find all solutions to the simultaneous Diophantine equation

$$\begin{cases} z = 7 \mod 15 \\ z = 14 \mod 17 \end{cases} \tag{184}$$

Solution: We begin by computing $x = 15^{-1}$ in $\mathbb{Z}/17\mathbb{Z}$ and $y = 17^{-1}$ in $\mathbb{Z}/15\mathbb{Z}$. One can take $x = 8$ and $y = 8$. Thus, from Corollary 7.1 we deduce that the set of all solutions to (184) are $z = 8 \cdot 17 \cdot 7 + 8 \cdot 15 \cdot 14 + 15 \cdot 17k$ for some $k \in \mathbb{Z}$. Simplifying, this says that the set of all solutions are those integers of the form $82 + 255k$ for $k \in \mathbb{Z}$.

Exercise 7.2

Problem: Find all solutions to $x^2 = 11$ in $\mathbb{Z}/35\mathbb{Z}$.

Solution: Let us first compute all the solutions to $x^2 = 11$ in $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$. In $\mathbb{Z}/5\mathbb{Z}$ one has that $11 = 1$ and so the solutions to $x^2 = 11 \mod 5$ are $x = 1, 4$. In $\mathbb{Z}/7\mathbb{Z}$ one has that $11 = 4$ and so the solutions to $x^2 = 11 \mod 7$ are $x = 2, 5$. Thus, to compute the solutions in $\mathbb{Z}/35\mathbb{Z}$ it suffices to use Corollary 7.2. To do this we first compute 5^{-1} in $\mathbb{Z}/7\mathbb{Z}$ which is 3 and 7^{-1} in $\mathbb{Z}/5\mathbb{Z}$ which 2. Set $f(x) = x^2 - 11$. Then, for each $a \in X_f(\mathbb{Z}/5\mathbb{Z})$ and $b \in X_f(\mathbb{Z}/7\mathbb{Z})$ we obtain the element $7 \cdot 2 \cdot a + 3 \cdot 5 \cdot b$ in $X_f(\mathbb{Z}/35\mathbb{Z})$. In particular, doing this for the above solutions gives

$$\begin{aligned} 7 \cdot 2 \cdot 1 + 3 \cdot 5 \cdot 2 = 44 &= 9 \\ 7 \cdot 2 \cdot 1 + 3 \cdot 5 \cdot -2 = -16 &= 19 \\ 7 \cdot 2 \cdot 4 + 3 \cdot 5 \cdot 2 = 86 &= 16 \\ 7 \cdot 2 \cdot 4 + 3 \cdot 5 \cdot -2 = 26 &= 26 \end{aligned} \tag{185}$$

Thus, $X_f(\mathbb{Z}/35\mathbb{Z}) = \{9, 16, 19, 26\}$.

Exercise 7.3

Problem: Prove Corollary 7.4 and use it to compute $\varphi(18)$.

Solution: This follows immediately from Theorem 7.5 and Exercise 5.1. To compute $\varphi(18)$ one writes $18 = 2 \cdot 3^2$ then Corollary 7.4 implies that $\varphi(18) = (2-1)3^1(3-1) = 6$.

Exercise 7.4

Problem: Let $m \in \mathbb{N}^*$. Show that $\sum_{\substack{d|m \\ d>0}} \varphi(d) = m$ as follows:

1. Set $g(m) := \sum_{\substack{d|m \\ d>0}} \varphi(d)$. Show that if n_1 and n_2 are coprime elements of $\mathbb{N}^*$ then $g(n_1 n_2) = g(n_1)g(n_2)$.
2. Check that $g(p^k) = p^k$ by hand.
3. By prime factorizing m and using 1. and 2. deduce that $g(m) = m$ for all $m \in \mathbb{Z}$.

Solution: Homework problem.

Exercise 7.5

Problem: Let us give an alternative proof of Corollary 7.4 as follows. Let us set $X = \{0, \ldots, m-1\} \subseteq \mathbb{Z}$ to be our *sample space* and recall that for a property P the notation $\mathbb{P}(x : x \text{ satisfies } P)$ means, by definition, the probability that a given $x \in X$ satisfies property P.

1. Justify why $\mathbb{P}(x : x \text{ is a unit}) = \dfrac{\varphi(m)}{m}$.
2. Explain why for $x \in X$ the condition that 'x is a unit' is the same thing as the condition '$p_1 \nmid x$' AND '$p_2 \nmid x$' AND $\cdots$ AND '$p_\ell \nmid x$' and why these conditions are independent.
3. Deduce, from the basic theory of probability, that
$$\mathbb{P}(x : x \text{ is a unit}) = \prod_{i=1}^{\ell} \mathbb{P}(x : p_i \nmid x) \tag{186}$$
4. Explain why
$$\mathbb{P}(x : p_i \nmid x) = 1 - \mathbb{P}(x : p_i \mid x) \tag{187}$$
5. Explain why $\mathbb{P}(x : p_i \mid x) = \dfrac{\frac{m}{p_i}}{m} = \dfrac{1}{p_i}$
6. Deduce the formula in Corollary 7.4.

Solution:

1. This is by definition since the probability of an x satisfying a condition P is $\dfrac{\#\{x \in X : x \text{ satisfies } P\}}{\#X}$.
2. We know that $x \in X$ is a unit if and only if $\gcd(x, m) = 1$. This is equivalent to the claim tha x and m have no primes in common, or equivalent, that for all $i = 1, \ldots, \ell$ one has that $p_i \nmid x$. Since being divisible by two separate primes are independent events, the independence is clear.
3. This equality follows from the basic theory of probability since the probability of k-indepedent events happening simultaneously is the product of the individual properties.
4. This is clear since one always has that $\mathbb{P}(x : x \text{ satisfies } P) + \mathbb{P}(x : x \text{ doesn't satisfy } P) = 1$.

5. It's clear that the number $x \in X$ has $p_i \mid x$ is $\dfrac{m}{p_i}$. Thus, the probability that $x \in X$ is divisible by p_i is $\dfrac{\frac{m}{p_i}}{m} = \dfrac{1}{p_i}$.

6. Combining the above we see that

$$\begin{aligned}
\frac{\varphi(m)}{m} &= \mathbb{P}(x : x \text{ is a unit}) \\
&= \prod_{i=1}^{\ell} \mathbb{P}(x : p_i \nmid x) \\
&= \prod_{i=1}^{\ell} (1 - \mathbb{P}(x : p_i \mid x)) \\
&= \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right) \\
&= \prod_{i=1}^{\ell} \frac{p_i - 1}{p_i}
\end{aligned} \tag{188}$$

Thus, cross multiplying gives

$$\varphi(m) = m \prod_{i=1}^{\ell} \frac{p_i - 1}{p_i} = \prod_{i=1}^{\ell} p_i^{e_i - 1}(p_i - 1) \tag{189}$$

8 Lecture 8: Hensel's lemma

8.1 Setup

Thanks to Theorem 7.3 (in particular Remark 7.1) we have essentially reduced solving modulus Diophantine equations modulo a general m to solving a modulus Diophantine equation modulo a prime power p^k. Thus, the next logical question one might ask is whether there is a technique to reduce solving a modulus Diophantine question modulo a prime power p^k to solving it just modulo the prime p?

The content of today's lecture is that, in a certain sense, you can. Namely, we wish to carry out the following goal:

Goal 8.1: Today

Give conditions on when one can reduce solving a modulus Diophantine equation modulo p^k to solving the same equation modulo p.

Working in $\mathbb{Z}/p\mathbb{Z}$ versus $\mathbb{Z}/p^k\mathbb{Z}$ has the obvious size advantage—it's much easier to check results by hand in $\mathbb{Z}/p\mathbb{Z}$ than it is in $\mathbb{Z}/p^k\mathbb{Z}$. But, with an eye towards the more theoretical, we will see in the next lecture that modulus Diophantine equations in $\mathbb{Z}/p\mathbb{Z}$ enjoy properties that modulus equations in more general $\mathbb{Z}/m\mathbb{Z}$ do not. Thus, it is often times useful to reduce to the setting of $\mathbb{Z}/p\mathbb{Z}$ to take advantage of these properties—this will be a key technical point to proving Theorem 6.5.

8.2 The notion of lifting

The way we might rigorize Goal 8.1 might be to ask the following question:

Question 8.1

Let p be a prime, $v \in \mathbb{N}^*$, and $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Given $k \in \mathbb{N}^*$, under what conditions is the reduction map $r : X_f(\mathbb{Z}/p^{k+1}\mathbb{Z}) \to X_f(\mathbb{Z}/p^k\mathbb{Z})$ bijective? Under what conditions is the map surjective? Under what conditions is the map injective?

Example 8.1

Let $f(x) = x^3 - 1$. Then, $X_f(\mathbb{Z}/3\mathbb{Z}) = \{1\}$ and $X_f(\mathbb{Z}/9\mathbb{Z}) = \{1, 4, 7\}$. The map $X_f(\mathbb{Z}/9\mathbb{Z}) \to X_f(\mathbb{Z}/3\mathbb{Z})$ is then given by $x \mapsto x \mod 3$. It evidently takes 1, 4, and 7 all to 1. Thus, in this case, the reduction map is surjective but not injective.

Let us make the following definition:

Definition 8.1

Let p be a prime and m, k, and v elements of $\mathbb{N}^*$ with $m \geqslant k$. Then, for $\mathbf{a} \in (\mathbb{Z}/p^k\mathbb{Z})^v$ a *lift* to $(\mathbb{Z}/p^m\mathbb{Z})^v$ is some $\mathbf{b} \in (\mathbb{Z}/p^m\mathbb{Z})^v$ such that $\mathbf{b} = \mathbf{a} \mod p^k$.

Example 8.2

Let $p = 7$. Then, $(132, 45, 72, 1) \in (\mathbb{Z}/7^3\mathbb{Z})^4$ is a lift of $(34, 45, 23, 1) \in (\mathbb{Z}/7^2\mathbb{Z})^4$.

The set of lifts from $(\mathbb{Z}/p^k\mathbb{Z})^v$ to $(\mathbb{Z}/p^m\mathbb{Z})^v$ can be quite easily described:

Lemma 8.1

Let p be a prime and m, k, and v elements of $\mathbb{N}^*$ with $m \geqslant k$. Fix $\mathbf{a} = (a_1, \ldots, a_v)$ in $(\mathbb{Z}/p^k\mathbb{Z})^v$. Then, the following holds:

1. An element $\mathbf{b} = (b_1, \ldots, b_v)$ of $(\mathbb{Z}/p^m\mathbb{Z})^v$ is a lift of $\mathbf{a}$ if and only if there exists $\mathbf{t} = (t_1, \ldots, t_v) \in \mathbb{Z}^v$ such that for all $i = 1, \ldots, v$ we have that $b_i = a_i + p^k t_i$. We denote this element $\mathbf{b}_\mathbf{t}$.
2. For $\mathbf{t}, \mathbf{t}' \in \mathbb{Z}^v$ one has that $\mathbf{b}_\mathbf{t} = \mathbf{b}_{t'}$ as elements of $(\mathbb{Z}/p^m\mathbb{Z})^v$ if and only if $\mathbf{t} = \mathbf{t}' \mod p^{m-k}$.

Thus, in essence we see that the set of lifts of $\mathbf{a}$ looks, in some sense, like a copy of $(\mathbb{Z}/p^{m-k}\mathbb{Z})^v$ inside of $(\mathbb{Z}/p^m\mathbb{Z})^v$—this intuition will factor heavily into a lot of the discussion to come.

Remark 8.1

For those more familiar with algebra the above is really just the observation that we have a short exact sequence

$$0 \to \mathbb{Z}/p^{m-k}\mathbb{Z} \xrightarrow{[p^k]} \mathbb{Z}/p^m\mathbb{Z} \xrightarrow{r} \mathbb{Z}/p^k\mathbb{Z} \to 0 \tag{190}$$

where $[p^k]$ denotes the multiplication-by-p^k map. The point being that we have then described the fibers of r as cosets of $\mathbb{Z}/p^{m-k}\mathbb{Z}$ in $\mathbb{Z}/p^m\mathbb{Z}$.

We are not interested in arbitary lifts of $\mathbf{a}$ from $(\mathbb{Z}/p^k\mathbb{Z})^v$ to $(\mathbb{Z}/p^m\mathbb{Z})^v$ though, we would like to consider lifts of solutions of $f(x_1,\dots,x_v) = 0 \mod p^k$ to elements of $(\mathbb{Z}/p^m\mathbb{Z})^v$ that are solutions to the equation $f(x_1,\dots,x_v) = 0 \mod p^m$. In other words, we want to know about lifting an element of $X_f(\mathbb{Z}/p^k\mathbb{Z})$ to an element of $X_f(\mathbb{Z}/p^m\mathbb{Z})$. To this end, we make the following definition:

Definition 8.2

Let p be a prime and m, k, and v elements of $\mathbb{N}^*$ with $m \geqslant k$. Let $f(x_1,\dots,x_v) \in \mathbb{Z}[x_1,\dots,x_v]$. Then, for $\mathbf{a} \in X_f(\mathbb{Z}/p^k\mathbb{Z})$ an *f-lift* to $\mathbb{Z}/p^m\mathbb{Z}$ is a lift $\mathbf{b}$ of $\mathbf{a}$ to $(\mathbb{Z}/p^m\mathbb{Z})^v$ that lies in $X_f(\mathbb{Z}/p^m\mathbb{Z})$. If $\mathbf{a}$ has an f-lift to $(\mathbb{Z}/p^m\mathbb{Z})^v$ we say that $\mathbf{a}$ is *f-liftable*.

Example 8.3

Let $f(x) = x^2 - 5$ and $p = 11$. Note that $4 \in X_f(\mathbb{Z}/11\mathbb{Z})$ and 15 and 48 are both lifts of 4 to $\mathbb{Z}/11^2\mathbb{Z}$ but only the latter is an f-lift.

One can then understand Question 8.1 as the question of when elements of $X_f(\mathbb{Z}/p^k\mathbb{Z})$ are f-liftable to $(\mathbb{Z}/p^m\mathbb{Z})^v$ or, even better, how many f-lifts are there?

We already saw in Example 8.1 that the reduction map can be surjective but not injective. Let's now give examples to show that it can be injective but not surjective and that it can be bijective. Later on, in Example 8.9, we will see an example of where the reduction map is neither surjective nor injective:

Example 8.4

Let $f(x) = x^3 - 3$. Then, $X_f(\mathbb{Z}/3\mathbb{Z}) = \{0\}$ but $X_f(\mathbb{Z}/9\mathbb{Z}) = \varnothing$. So, the map $X_f(\mathbb{Z}/9\mathbb{Z}) \to X_f(\mathbb{Z}/3\mathbb{Z})$ is not surjective.

Example 8.5

Let $f(x) = x^2 - 3$. Then, the map $X_f(\mathbb{Z}/11\mathbb{Z}) = \{5, 6\}$, $X_f(121) = \{27, 94\}$ and the map $X_f(\mathbb{Z}/121\mathbb{Z}) \to X_f(\mathbb{Z}/11\mathbb{Z})$ takes 27 to 5 and takes 94 to 6. Thus, the map $X_f(\mathbb{Z}/121\mathbb{Z}) \to X_f(\mathbb{Z}/11\mathbb{Z})$ is bijective.

These examples show that there must be some nuance in answering Question 8.1.

8.3 Hensel's lemma

To answer Question 8.1 will require the advent of something, *a priori*, entirely unexpected: differential calculus. Namely, we have the following definition:

Definition 8.3

Let p be a prime and let v be in $\mathbb{N}^*$. Let $f(x_1,\dots,x_v) \in \mathbb{Z}[x_1,\dots,x_v]$. Let $k \in \mathbb{N}^*$. For $\mathbf{a} \in (\mathbb{Z}/p^k\mathbb{Z})^v$

we define the *differential of f at* $\mathbf{a}$, denoted $df(\mathbf{a})$, as follows:

$$df(\mathbf{a}) := \left(\frac{\partial f}{\partial x_1}(\mathbf{a}), \ldots, \frac{\partial f}{\partial x_v}(\mathbf{a})\right) \tag{191}$$

We then call an element $\mathbf{a} \in X_f(\mathbb{Z}/p\mathbb{Z})$ *smooth* if $df(\mathbf{a}) \neq (0, \ldots, 0)$ and *singular* if $df(\mathbf{a}) = (0, \ldots, 0)$. If every $\mathbf{a} \in X_f(\mathbb{Z}/p\mathbb{Z})$ is smooth, we say that f is *smooth modulo* p. A point $\mathbf{a} \in X_f(\mathbb{Z}/p^k\mathbb{Z})$ is called *smooth* (resp. *singular*) if its image in $X_f(\mathbb{Z}/p\mathbb{Z})$ is smooth (resp. *singular*). We denote the set of smooth points in $X_f(\mathbb{Z}/p^k\mathbb{Z})$ by $X_f^{\mathrm{sm}}(\mathbb{Z}/p^k\mathbb{Z})$ and the set of singular points by $X_f^{\mathrm{sing}}(\mathbb{Z}/p^k\mathbb{Z})$.

The following lemma gives an alternative characterization for smooth points (which really only differs from the above when $k > 1$):

Lemma 8.2

Let p be a prime and v an element of $\mathbb{N}^*$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Let $k \in \mathbb{N}^*$. Then, the following hold true:

1. For all $\mathbf{a} \in X_f(\mathbb{Z}/p^k\mathbb{Z})$ one has that

$$df(\mathbf{a}) \mod p = df(\mathbf{a} \mod p) \tag{192}$$

2. A point $\mathbf{a} \in X_f(\mathbb{Z}/p^k\mathbb{Z})$ is smooth if and only if $df(\mathbf{a}) \in \Phi(p^k)$.

Remark 8.2

On the small off-chance that a reader is familiar with algebraic geometry, I feel compelled to point out that the above definition is 'wrong'. Namely, to say that the hypersurface $V(f) \subseteq \mathbb{A}^v_{\mathbb{F}_p}$ is smooth over $\mathrm{Spec}(\mathbb{F}_p)$ one should require that $df(a) \neq 0$ not only for $a \in X_f(\mathbb{F}_p) = V(f)(\mathbb{F}_p)$ but also for $a \in V(f)(\mathbb{F}_q)$ for all prime powers q of p. For such $\mathbb{F}_q$-points, f-liftability would actually be about lifting $\mathbb{F}_q$-points to $W_n(\mathbb{F}_q)$.

Example 8.6

Let $f(x) = x^2 - 5$ and let $p = 11$. Then, $X_f(\mathbb{Z}/11\mathbb{Z}) = \{4, 7\}$. Note that $df(x) = 2x$ and $df(4) = 8 \neq 0$, so $4 \in X_f^{\mathrm{sm}}(\mathbb{Z}/11\mathbb{Z})$ Also, $df(7) = 14 = 3 \neq 0$ so $7 \in X^{\mathrm{sm}}(\mathbb{Z}/11\mathbb{Z})$. Thus, f is smooth modulo 7.

Example 8.7

Let $f(x) = x^3 - 3$ and let $p = 3$. Then, $X_f(\mathbb{Z}/3\mathbb{Z}) = \{0\}$. Note though that $df(x) = 3x^2$ and $df(0) = 0$ so that $0 \in X_f^{\mathrm{sing}}(\mathbb{Z}/3\mathbb{Z})$.

Example 8.8

Let $f(x,y) = x^4 + 4x^2y + y^3 - 5$. Note that $X_f(\mathbb{Z}/3\mathbb{Z}) = \{(0,2),(1,2),(2,2)\}$. Note that

$$df = (4x^3 + 8xy, 4x^2 + 3y^2) \tag{193}$$

Note that

$$\begin{aligned} \frac{\partial f}{\partial x}(0,2) &= 0, & \frac{\partial f}{\partial y}(0,2) &= 0 \\ \frac{\partial f}{\partial x}(1,2) &= 2, & \frac{\partial f}{\partial y}(1,2) &= 1 \\ \frac{\partial f}{\partial x}(2,2) &= 1, & \frac{\partial f}{\partial y}(1,2) &= 1 \end{aligned} \tag{194}$$

so that $(0,2) \in X_f^{\text{sing}}(\mathbb{Z}/3\mathbb{Z})$ and $(1,2),(2,2) \in X_f^{\text{sm}}(\mathbb{Z}/3\mathbb{Z})$.

Remark 8.3

Before we move on, it's worth giving a very vague idea of why differential calculus is showing up in discussions of modulus Diophantine equations. The key idea is that p in $\mathbb{Z}/p^2\mathbb{Z}$ behaves very much like an infinitesimal. Namely, recall that from calculus one uses ε to mean an 'infinitesimally small quantity that is not zero'. In particular, one often times thinks that ε is so small that while $\varepsilon \neq 0$ one has that $\varepsilon^2 = 0$. In fact, there are whole areas of math that are rigorizations of calculus with such literal infinitesimals. So, the reason that differential calculus is showing up is that $p \neq 0$ in $\mathbb{Z}/p^2\mathbb{Z}$ but $p^2 = 0$ in $\mathbb{Z}/p^2\mathbb{Z}$ so that p acts like an infinitesimal.

We have the following elementary observation:

Lemma 8.3

Let p be a prime and v an element of $\mathbb{N}^*$. Let $f(x_1,\ldots,x_v) \in \mathbb{Z}[x_1,\ldots,x_v]$. Let k and m be elements of $\mathbb{N}^*$ with $m \geqslant k$. Then, the reduction map $r : X_f(\mathbb{Z}/p^m\mathbb{Z}) \to X_f(\mathbb{Z}/p^k\mathbb{Z})$ satisfies the following:

$$r(X_f^{\text{sm}}(\mathbb{Z}/p^m\mathbb{Z})) \subseteq X_f^{\text{sm}}(\mathbb{Z}/p^k\mathbb{Z}), \qquad r(X_f^{\text{sing}}(\mathbb{Z}/p^m\mathbb{Z})) \subseteq X_f^{\text{sing}}(X/p^k\mathbb{Z}) \tag{195}$$

In other words, for $\mathbf{b} \in X_f(\mathbb{Z}/p^m\mathbb{Z})$ one has that $\mathbf{b}$ is smooth if and only if $r(\mathbf{b})$ is smooth and $\mathbf{b}$ is singular if and only if $r(\mathbf{b})$ is singular.

We then have the following beautiful result relating smoothness to liftability:

Theorem 8.1: Hensel's lemma

Let p be a prime and v an element $\mathbb{N}^*$. Let $f(x_1,\ldots,x_v) \in \mathbb{Z}[x_1,\ldots,x_v]$. Let k and m be in $\mathbb{N}^*$ and let $\mathbf{a} \in X_f^{\text{sm}}(\mathbb{Z}/p^k\mathbb{Z})$. Then there is an f-lift of $\mathbf{a}$ to $X_f^{\text{sm}}(\mathbb{Z}/p^m\mathbb{Z})$. This lift is unique if and only if $v = 1$.

In particular, we deduce the following:

Corollary 8.1

Let p be a prime and v an element of $\mathbb{N}^*$. Let $f(x_1,\ldots,x_v) \in \mathbb{Z}[x_1,\ldots,x_v]$. Let k and m be elements of $\mathbb{N}^*$ with $m \geqslant k$. Then, the reduction map $r : X_f^{\text{sm}}(\mathbb{Z}/p^m\mathbb{Z}) \to X_f^{\text{sm}}(\mathbb{Z}/p^k\mathbb{Z})$ is surjective and is

bijective if and only if $v = 1$.

Let us give the proof of Theorem 8.1 and then discuss some examples:

Proof 8.1: Theorem 8.1

By iterating the below proof it suffices to take $m = k + 1$. By lemma 8.1 the set of of lifts of $\mathbf{a} = (a_1, \ldots, a_v)$ are precisely

$$\mathbf{b_t} = (a_1 + p^k t_1, \ldots, a_v + p^k t_v) \tag{196}$$

for some $\mathbf{t} = (t_1, \ldots, t_v) \in \mathbb{Z}^v$. So the question remains as to whether we can choose $\mathbf{t}$ such that $\mathbf{b_t}$ is actually an f-lift. Now, take the Taylor expansion of f around $\mathbf{a} = (a_1, \ldots, a_v)$:

$$f(\mathbf{b_t}) = f(\mathbf{a}) + \sum_{j=1}^{v} \frac{\partial f}{\partial x_j}(\mathbf{a}) p^k t_j + \underbrace{\frac{1}{2} \sum_{i,j=1}^{v} \frac{\partial^2 f}{\partial x_i \partial x_j}(\mathbf{a})(p^k t_i)(p^k t_j) + \cdots}_{\text{terms divisible by } p^{k+1}} \tag{197}$$

In particular, we see that

$$f(\mathbf{b_t}) = f(\mathbf{a}) + \sum_{j=1}^{v} \frac{\partial f}{\partial x_j}(\mathbf{a}) p^k t_j \mod p^{k+1} \tag{198}$$

Now, since $\mathbf{a} \in X_f(\mathbb{Z}/p^k\mathbb{Z})$ we know that

$$f(\mathbf{a}) = p^k z \tag{199}$$

for some $z \in \mathbb{Z}$. Factoring out p^k we see that

$$f(\mathbf{b_t}) = p^k \left(z + \sum_{j=1}^{v} \frac{\partial f}{\partial x_j}(\mathbf{a}) t_j \right) \mod p^{k+1} \tag{200}$$

Thus, we're trying to solve the equation

$$0 = p^k z + \sum_{j=1}^{v} \frac{\partial f}{\partial x_j}(\mathbf{a}) p^k t_j \tag{201}$$

Now, factoring p^k out, we see that what we really need is that

$$0 = z + \sum_{j=1}^{v} \frac{\partial f}{\partial x_j}(\mathbf{a}) t_j \mod p \tag{202}$$

In other words, we can write this as the matrix equation

$$-z = df(\mathbf{a}) \begin{pmatrix} t_1 \\ \vdots \\ t_v \end{pmatrix} \mod p \tag{203}$$

Since $\mathbf{a}$ is smooth, $df(\mathbf{a}) \mod p$ is non-zero, and thus this matrix equation is solvable. Moreover, such an equation is *uniquely solvable* if and only if $v = 1$. Thus, the conclusion follows.

Let's now verify the claim in the case of Example 8.8:

Example 8.9

Consider notation as in Example 8.8. Note that, using computer software, one can check

$$X_f(\mathbb{Z}/9\mathbb{Z}) = \{(4,2),(5,2),(2,5),(7,5),(1,8),(8,8)\} \tag{204}$$

and so the image of the reduction map $X_f(\mathbb{Z}/9\mathbb{Z}) \to X_f(\mathbb{Z}/3\mathbb{Z})$ is $\{(1,2),(2,2)\}$. Thus, r surjects onto $X_f^{\text{sm}}(\mathbb{Z}/3\mathbb{Z})$ but the singular point $(0,2) \in X_f^{\text{sing}}(\mathbb{Z}/3\mathbb{Z})$ is not hit (i.e. $(0,2)$ is not f-liftable).

Of course, one should be wary that Hensel's lemma doesn't claim that singular points are not f-liftable. In fact, one can, in some situations, lift singular points. For example:

Example 8.10

Let $f(x) = x^2 - 4$ and let $p = 2$. Then, $X_f(\mathbb{Z}/2\mathbb{Z}) = \{0\}$. Clearly $0 \in X_f^{\text{sing}}(\mathbb{Z}/2\mathbb{Z})$. Note though that $X_f(\mathbb{Z}/4\mathbb{Z}) = \{0,2\}$ and evidently both of these are lifts of 0.

The dichotomy given by Theorem 8.1 is that smooth points are always liftable, whereas singular points are only sometimes liftable.

That said, if one studies the proof of Theorem 8.1 one notices that one can deduce a very strong property concerning the f-liftability of singular points:

Theorem 8.2

Let p be a prime and let $v \in \mathbb{N}^*$. Let $f(x_1,\ldots,x_v) \in \mathbb{Z}[x_1,\ldots,x_v]$. Let $k \in \mathbb{N}^*$ and let $\mathbf{a} \in X_f^{\text{sing}}(\mathbb{Z}/p^k\mathbb{Z})$. Then, one of the following two situations holds:

1. Every lift $\mathbf{b}$ of $\mathbf{a}$ to $(\mathbb{Z}/p^{k+1}\mathbb{Z})^v$ is an f-lift.
2. No lift $\mathbf{b}$ of $\mathbf{a}$ to $(\mathbb{Z}/p^{k+1}\mathbb{Z})^v$ is an f-lift.

In fact, if $\mathbf{a}$ is singular, then the value $f(\mathbf{b})$ is constant on lifts $\mathbf{b}$ of $\mathbf{a}$.

Proof 8.2

This follows almost immediately from our proof of Theorem 8.1, namely Equation (198). Indeed, if $\mathbf{a}$ is singular, then $p \mid \frac{\partial f}{\partial x_j}(\mathbf{a})$ for all j and so, in particular, $p^{k+1} \mid \frac{\partial f}{\partial x_j}(\mathbf{a})p^k t_j$ and so Equation (198) reduces to

$$f(\mathbf{b_t}) = f(\mathbf{a}) \mod p^{k+1} \tag{205}$$

which says precisely that f is constant on lifts of $\mathbf{a}$ to $(\mathbb{Z}/p^{k+1}\mathbb{Z})^v$.

Another observation we can make to sharpen Theorem 8.1 is the realization that if $\mathbf{a}$ is a smooth point then there is an f-lift from $(\mathbb{Z}/p^k\mathbb{Z})^v$ to $(\mathbb{Z}/p^{k+1}\mathbb{Z})^v$ but, moreover, there are precisely p^{v-1} of them:

Theorem 8.3

Let p be a prime and $v \in \mathbb{N}^*$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Let $k \in \mathbb{N}^*$ and let $\mathbf{a} \in X_f^{\text{sm}}(\mathbb{Z}/p^k\mathbb{Z})$. Then, there are precisely p^{v-1} f-lifts of $\mathbf{a}$ to $(\mathbb{Z}/p^{k+1}\mathbb{Z})^v$.

Proof 8.3

By the proof of Theorem 8.1 it suffices to show that (198) has exactly p^{v-1} solutions in $\mathbb{Z}/p\mathbb{Z}$. To do this, we let

$$T : (\mathbb{Z}/p\mathbb{Z})^v \to \mathbb{Z}/p\mathbb{Z} \tag{206}$$

be the $\mathbb{Z}/p\mathbb{Z}$-linear map given as follows:

$$T(t_1, \ldots, t_j) := \sum_{j=1}^{v} \frac{\partial f}{\partial x_j}(\mathbf{a}) t_j \mod p \tag{207}$$

We are then trying to count the size of $T^{-1}(-z)$. Since $\mathbf{a} \in X_f^{\text{sm}}(\mathbb{Z}/p^k\mathbb{Z})$ we know that T is not the zero transformation. Thus, by the rank-nullity theorem we know that T is surjective and that $\dim_{\mathbb{Z}/p\mathbb{Z}} \ker T = v - 1$. Let $w_0 \in (\mathbb{Z}/p\mathbb{Z})^v$ be any element of $T^{-1}(-z)$. Then, by basic linear algebra, we know that

$$T^{-1}(z) = w_0 + \ker T = \{v_0 + x : x \in \ker T\} \tag{208}$$

In particular, we see that $\#T^{-1}(z) = \# \ker T$. But, $\ker T$ is a $(v-1)$-dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space, and so is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{v-1}$. Thus, $\ker T$, and thus $T^{-1}(z)$, has p^{v-1} elements.

We collect the above results into the following theorem:

Theorem 8.4: Omnibus Hensel lemma

Let p be a prime and $v \in \mathbb{N}^*$. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Let $k \in \mathbb{N}^*$ and consider the reduction map

$$r : X_f(\mathbb{Z}/p^{k+1}\mathbb{Z}) \to X_f(\mathbb{Z}/p^k\mathbb{Z}) \tag{209}$$

Then, the following holds:

1. If $\mathbf{a} \in X_f^{\text{sm}}(\mathbb{Z}/p^k\mathbb{Z})$, then $\#r^{-1}(\mathbf{a}) = p^{v-1}$.
2. If $\mathbf{a} \in X_f^{\text{sing}}(\mathbb{Z}/p^k\mathbb{Z})$, f is constant on $r^{-1}(\mathbf{a})$ and, in particular $\#r^{-1}(\mathbf{a})$ is either 0 or p^v.

Remark 8.4

Note that it's quite easy to generalize Theorem 8.4 part (1) to allow for any $m \geqslant k$, not just $k+1$. One merely replaces p^{v-1} by $p^{m(v-1)}$. Must be careful though when trying to generalize Theorem 8.4 part (2) to more general m. Namely, looking at the proof of Theorem 8.2 to get constancy on the fibers lifting from $\mathbb{Z}/p^k\mathbb{Z}$ to $\mathbb{Z}/p^{k+1}\mathbb{Z}$ we needed that $\dfrac{\partial f}{\partial x_j}(\mathbf{a}) = 0 \mod p$ for all j which, of course, is equivalent to singularity. But, in lifting from $\mathbb{Z}/p^k\mathbb{Z}$ to $\mathbb{Z}/p^{k+2}\mathbb{Z}$ for instance, you actually need $\dfrac{\partial f}{\partial x_j}(\mathbf{a}) = 0 \mod p^2$. This is not, in fact, guaranteed by singularity!

In particular, it can be true that a point $\mathbf{a} \in X_f^{\text{sing}}(\mathbb{Z}/p\mathbb{Z})$ has p^v f-lifts to $X_f^{\text{sing}}(\mathbb{Z}/p\mathbb{Z})$ and that

some of these have f-lifts to $X_f^{\mathrm{sing}}(\mathbb{Z}/p^3\mathbb{Z})$ and some do not. We'll see an example of this in Exercise 8.3 below.

Finally, it is worth noting that the proof of Theorem 8.4 is algorithmic in the sense that it actually gives an algorithm about how to produce all f-lifts of a given $\mathbf{a} \in X_f(\mathbb{Z}/p^k\mathbb{Z})$ to $X_f(\mathbb{Z}/p^{k+1}\mathbb{Z})$, and thus an algorithm to compute $X_f(\mathbb{Z}/p^{k+1}\mathbb{Z})$ given $X_f(\mathbb{Z}/p^k\mathbb{Z})$. Namely, one proceeds as follows:

Algorithm 8.1

Let p be a prime and k an element of $\mathbb{N}^*$. The following gives an algorithm to compute $X_f(\mathbb{Z}/p^{k+1}\mathbb{Z})$ given $X_f(\mathbb{Z}/p^k\mathbb{Z})$ as input:

Step 1: Compute df.

Step 2: Using Step 1, compute explicitly compute the decomposition

$$X_f(\mathbb{Z}/p^k\mathbb{Z}) = X_f^{\mathrm{sm}}(\mathbb{Z}/p^k\mathbb{Z}) \sqcup X_f^{\mathrm{sing}}(\mathbb{Z}/p^k\mathbb{Z}) \tag{210}$$

Step 2: For each $\mathbf{a} \in X_f^{\mathrm{sm}}(\mathbb{Z}/p^k\mathbb{Z})$ one merely finds all the solutions $\mathbf{t} \in (\mathbb{Z}/p\mathbb{Z})^v$ to (203) and takes $\mathbf{b_t}$ for each solution to find the set of elements of $X_f(\mathbb{Z}/p^{k+1}\mathbb{Z})$ lifting $\mathbf{a}$.

Step 3: For each $\mathbf{a} \in X_f^{\mathrm{sing}}(\mathbb{Z}/p^k\mathbb{Z})$ choose any lift $\mathbf{b}$ of $\mathbf{a}$ and test whether $f(\mathbf{b})$ is zero or not. If it is zero then all lifts, parameterized as in Lemma 8.1, are f-lifts. If $f(\mathbf{b})$ is non-zero then there are no f-lifts of $\mathbf{a}$.

As an example, we see that we can use the above to understand some power equations modulo p^k in terms of power equations modulo p:

Corollary 8.2

Let p be prime and let n and k be elements of $\mathbb{N}^*$ with $p \nmid n$. Let $a \in \mathbb{Z}$ be such that $p \nmid a$ and set $f(x) := x^n - a$. Then, the mapping $X_f(\mathbb{Z}/p^k\mathbb{Z}) \to X_f(\mathbb{Z}/p\mathbb{Z})$ is bijective with algorithmically constructible inverse.

Proof 8.4

This follows immediately from Corollary 8.1 and Algorithm 8.1 since $X_f(\mathbb{Z}/p\mathbb{Z}) = X_f^{\mathrm{sm}}(\mathbb{Z}/p\mathbb{Z})$. Indeed, if $x_0 \in X_f(\mathbb{Z}/p\mathbb{Z})$ then $df(x_0) = nx_0^{n-1}$. Now, $p \nmid n$ so that n is a unit, and x_0^{n-1} is a unit, so nx_0^{n-1} is a unit and so, in particular, non-zero.

Remark 8.5

It's worth noting that the only new part of Corollary 8.2 is, essentially, the case when $\gcd(n, p-1) > 1$. Indeed, if $\gcd(n, p-1) = 1$ then since $p \nmid n$ we deduce that $\gcd(n, \varphi(p^k)) = 1$. Then, Corollary 8.2 is trivial by Corollary 5.4.

Let us now show this algorithm in practice:

Example 8.11

Let us find all the solutions to $x^2 = 5 \mod 121$. Noting that $121 = 11^2$, we first solve $x^2 = 5 \mod 11$. One can check by hand that $x = 4$ and $x = 7$ are the only solutions. Moreover, setting $f(x) = x^2 - 5$ we see that $df(4) = 8 \neq 0$ and $df(7) = 14 = 3 \neq 0 \mod 11$. Thus, we see that 4 and 7 are smooth points, and so f is smooth modulo 11. Thus, we know that $X_f(\mathbb{Z}/121\mathbb{Z}) \to X_f(\mathbb{Z}/11\mathbb{Z})$ is bijective, so we should get 2 solutions to $x^2 = 5 \mod 121$. So, to find the f-lift of 4 we first note that $f(4) = 11$ and so the z in (203) is 1. Since $df(4) = 8$ we're then trying to solve the equation $-1 = 8 \cdot t \mod 11$. This clearly has solution $t = 4$. Thus, we see that the f-lift of 4 is $4 + 11 \cdot 4 = 48$. Similarly, let's compute the f-lift of 7. We see that $f(7) = 44 = 4 \cdot 11$ so in this case $z = 4$. Since $df(7) = 3$ we are trying to solve the equation $-4 = 3t \mod 11$ which has solution $t = 6$. Thus, we see that the f-lift of 7 is $7 + 11 \cdot 6 = 73$.

Let's carry out the procedure for Example 8.8:

Example 8.12

Let us find the set of solutions to $x^4 + 4x^2y + y^3 = 5 \mod 9$. Let's start by finding the set of solutions modulo 3. Now, modulo 3 we know that either $x = 0$, in which case $y = 2$, or $x^2 = x^4 = 1$ and $y^3 = y$ (by Theorem 5.3) so that $x^4 + 4x^2y + y^3$ reduces to $1 + y + y$ and $5 = 2 \mod 3$ so we are trying to solve the equation $2y + 1 = 2 \mod 5$ or $2y = 1 \mod 3$. This clearly has the solution $y = 2$. Since x can be anything we deduce that $X_f(\mathbb{Z}/3\mathbb{Z}) = \{(0,2), (1,2), (2,2)\}$. Let us now use the algorithmic nature of Theorem 8.4 to find all solutions to our equation modulo 9.

Let's start with $(0,2)$. We already checked in Example 8.8 that $(0,2)$ is singular. Let's then figure out what its f-lifts to $\mathbb{Z}/9\mathbb{Z}$ are. To do this we need only check whether $f(0,2) = 0 \mod 9$. But, $f(0,2) = 3 \neq 0 \mod 9$. So, no lift of $(0,2)$ is an f-lift.

Let's next move to $(1,2)$. We checked in Example 8.8 that $(1,2)$ is smooth. Now, note that $f(1,2) = 12 = 3 \mod 9$. So we see that $z = 1$. Since $df(1,2) = (2,1)$ we see that we are trying to solve the equation

$$-1 = 2t_1 + t_2 \mod 3 \tag{211}$$

with $t_1, t_2 \in \mathbb{Z}/3\mathbb{Z}$. It's clear that this has the solutions $\{(0,2), (1,0), (2,1)\}$. Thus, we see that the f-lifts of $(1,2)$ are

$$\begin{aligned} (1 + 3 \cdot 0, 2 + 3 \cdot 2) &= (1,8) \\ (1 + 3 \cdot 1, 2 + 3 \cdot 0) &= (4,2) \\ (1 + 3 \cdot 2, 2 + 3 \cdot 1) &= (7,5) \end{aligned} \tag{212}$$

Finally, let's take care of the case $(2,2)$. We see that $f(2,2) = 51 = 6 \mod 9$ so that $z = 2$. Since $df(2,2) = (1,1)$ we see that we are trying to solve the equation

$$-2 = t_1 + t_2 \mod 3 \tag{213}$$

This has the solutions $\{(0,1), (1,0), (2,2)\}$. Thus, we see that the f-lifts of $(2,2)$ are

$$\begin{aligned} (2 + 3 \cdot 0, 2 + 3 \cdot 1) &= (2,5) \\ (2 + 3 \cdot 1, 2 + 3 \cdot 0) &= (5,2) \\ (2 + 3 \cdot 2, 2 + 3 \cdot 2) &= (8,8) \end{aligned} \tag{214}$$

From which we are done.

8.4 Exercises

Exercise 8.1

Find all solutions to $x^5 - 5xy = 7 \mod 75$.

Solution: With an eye towards Corollary 7.2 we first solve $x^5 - 5xy = 7 \mod 3$ and $x^5 - 5xy = 7 \mod 5^2$.

One quickly sees, using Corollary 5.5 (in particular the conclusion that $x^3 = x$ for all $x \in \mathbb{Z}/3\mathbb{Z}$) that $x^5 - 5xy = 7 \mod 7$ is equivalent to solving $x - 2xy = 1 \mod 3$ or $x(1-2y) = 1 \mod 3$. One quickly checks that the solutions to this are $\{(1,0),(2,1)\}$.

Now, let us set $f(x,y) = x^5 - 5xy - 7$. We next wish to compute $X_f(\mathbb{Z}/5^2\mathbb{Z})$. Let us first compute $X_f(\mathbb{Z}/5\mathbb{Z})$. But, using Corollary 5.5 again, we see that solving $x^5 - 5xy = 7 \mod 5$ is the same thing as solving $x = 2 \mod 5$. Thus,

$$X_f(\mathbb{Z}/5\mathbb{Z}) = \{(2,0),(2,1),(2,2),(2,3),(2,4)\} \tag{215}$$

Now, $df = 0 \mod 5$ and so $X_f(\mathbb{Z}/5\mathbb{Z}) = X_f^{\text{sing}}(\mathbb{Z}/5\mathbb{Z})$. But, one sees that

$$\begin{aligned} f(2,0) = 25 &= 0 \mod 25 \\ f(2,1) = 15 &\neq 0 \mod 25 \\ f(2,2) = 5 &\neq 0 \mod 25 \\ f(2,3) = -5 &\neq 0 \mod 25 \\ f(2,4) = -15 &\neq 0 \mod 25 \end{aligned} \tag{216}$$

Thus, we see that $X_f(\mathbb{Z}/25\mathbb{Z})$ is the set of all lifts of $(2,0)$ which, using Lemma 8.1, is the set

$$\{(2+5t_1, 5t_2) : t_1, t_2 \in \{0,\ldots,4\}\} \tag{217}$$

To compute $X_f(\mathbb{Z}/75\mathbb{Z})$ we then use Corollary 7.2. Namely, note that 25^{-1} in $\mathbb{Z}/3\mathbb{Z}$ is 1 and 3^{-1} in $\mathbb{Z}/25\mathbb{Z}$ is 17. Thus, for each $(a,b) \in X_f(\mathbb{Z}/3\mathbb{Z})$ and $(c,d) \in X_f(\mathbb{Z}/25\mathbb{Z})$ we get the solution

$$(25a + 51c, 25b + 51d) \in X_f(\mathbb{Z}/75\mathbb{Z}) \tag{218}$$

Thus, we see that $X_f(\mathbb{Z}/75\mathbb{Z}) = S \cup T$ where

$$\begin{aligned} S &= \{(25 + 51(2+5t_1), 51 \cdot 5t_2) : t_1, t_2 \in \{0,\ldots,4\}\} \\ &= \{(52 + 5t_1, 30t_2) : t_1, t_2 \in \{0,\ldots,4\}\} \end{aligned} \tag{219}$$

and

$$\begin{aligned} T &= \{(50 + 51(2+5t_1), 25 + 51 \cdot 5 \cdot t_2 : t_1, t_2 \in \{0,\ldots,4\}\} \\ &= \{(32 + 5t_1, 25 + 30t_2) : t_1, t_2 \in \{0,\ldots,4\}\} \end{aligned} \tag{220}$$

In particular $\#X_f(\mathbb{Z}/75\mathbb{Z}) = 50$.

Exercise 8.2

Problem: Prove Lemma 8.2.

Solution: The claim 1. is clear since $df(\mathbf{a})$ is a polynomial in $\mathbf{a}$. The second claim follows since $\mathbf{a}$ is

smooth if and only if $df(\mathbf{a} \mod p) \neq 0$ which is equivalent to $df(\mathbf{a}) \neq 0 \mod p$ by 1. But, this just means that $p \nmid df(\mathbf{a})$ which is equivalent to $df(\mathbf{a}) \in \Phi(p^k)$.

Exercise 8.3

Problem: Let p be an odd prime. Show that the equation $x^p = 1 \mod p^3$ has p solutions in the following two says:

1. Using Theorem 6.3 and Theorem 6.5.
2. Using Theorem 8.4.

Solution:

1. Since $x^p = 1 \mod p^3$ obviously has a solution, and there is a primitive root modulo p by Theorem 6.5 we use Theorem 6.3 to deduce that $x^p = 1 \mod p^3$ has $\gcd(p, \varphi(p^3)) = \gcd(p, p^2(p-1)) = p$ solutions.

2. Let us set $f(x) = x^p - 1$. Note by Corollary 5.5 one easily deduces that $X_f(\mathbb{Z}/p\mathbb{Z}) = \{1\}$. Since $1 \in X_f^{\text{sing}}(\mathbb{Z}/p\mathbb{Z})$ and 1 is a lift of 1 to $\mathbb{Z}/p^2\mathbb{Z}$ satisfying $f(x) = 0 \mod p^2$ we deduce form Theorem 8.4 that all lifts of 1 to $\mathbb{Z}/p^2\mathbb{Z}$ are f-lifts. Thus

$$X_f(\mathbb{Z}/p^2\mathbb{Z}) = \{1 + ap : a \in \{0, \dots, p-1\}\} \tag{221}$$

Note, again, that all these points are singular. Again, since $1 \in \mathbb{Z}/p^2\mathbb{Z}$ evidently has the f-lift 1 to $\mathbb{Z}/p^3\mathbb{Z}$ we use Theorem 8.4 to deduce that all lifts of 1 are f-lifts. Thus,

$$X_f(\mathbb{Z}/p^3\mathbb{Z}) \supseteq \{1 + p^2 b : b \in \{0, \dots, p-1\}\} \tag{222}$$

The claim that $\#X_f(\mathbb{Z}/p^3\mathbb{Z}) = p$ is then clearly equivalent to the claim that for $a \in \{1, \dots, p-1\}$ no lift of $1 + ap \in \mathbb{Z}/p^2\mathbb{Z}$ to $\mathbb{Z}/p^3\mathbb{Z}$ is an f-lift. Since $1 + ap \in \mathbb{Z}/p^3\mathbb{Z}$ is evidently a lift of $1 + ap \in \mathbb{Z}/p^2\mathbb{Z}$ it suffices, by Theorem 8.4, to show that $1 + ap \in \mathbb{Z}/p^3\mathbb{Z}$ is not an f-lift. In other words, we need to show that

$$(1 + ap)^p \neq 1 \mod p^3 \tag{223}$$

for $a \in \{1, \dots, p-1\}$. To do this we use the binomial theorem to write

$$(1 + ap)^p = \sum_{j=0}^{p} \binom{p}{j} a^j p^j = 1 + ap^2 + \sum_{j=2}^{p} \binom{p}{j} a^j p^j \tag{224}$$

We claim that for $j \geqslant 2$ and p odd that $\binom{p}{j} a^j p^j = 0 \mod p^3$. This is clear if $j \geqslant 3$ and so it suffices to show the claim when $j = 2$. In this case, since 2 is invertible modulo p (since p is odd), we can rewrite

$$\binom{p}{2} a^2 p^2 = a^2 \left(\frac{p^4}{2} - \frac{p^3}{2} \right) \tag{225}$$

which clearly is divisible by p^3. Thus, we deduce that

$$(1 + ap)^p = 1 + ap^2 \mod p^3 \tag{226}$$

So, if $(1 + ap)^p = 1 \mod p^3$ then we'd deduce that $1 + ap^2 = 1 \mod p^3$ and so $p^3 \mid ap^2$. This implies that $p \mid a$, which is untrue. The conclusion follows.

9 Lecture 9: The structure of polynomials modulo m

9.1 Setup

Thanks to the contents of Lectures 7 and 8, specifically Corollary 7.2 and Theorem 8.4, we have, in some sense, reduced our study of modulus Diophantine equations modulo a general m to the study of modulus Diophantine equations modulo p where p is a prime. So, our final goal will be to show that modulus Diophantine equations modulo p have properties that, in general, are not shared by general modulus Diophantine equations. Once we have done this, we will, in the next lecture, reap the rewards of our efforts by finally proving Theorem 6.5 in its entirety.

Let us now try to give more meat the statement that modulus Diophantine equations modulo a prime p behave 'nicer' than modulus Diophantine equations modulo a non-prime. Namely, we reobserve a phenomenon already remarked upon several times:

Observation 9.1

Let m and v be elements of $\mathbb{N}^*$. Then, it is possible that a polynomial $f(x) \in \mathbb{Z}/m\mathbb{Z}[x]$ of degree v can have more than v roots in $\mathbb{Z}/m\mathbb{Z}$.

Part of the issue, as what happened in Proof **??** is that Corollary 7.3 rears its head and shows that an element m in $\mathbb{N}^*$ having many distinct prime factors will lead, in general, to many solutions. But, this is a problem even for a single prime power:

Example 9.1

Let p be a prime. Then, the equation $x^2 = 0 \mod p$ has p solutions in $\mathbb{Z}/p^2\mathbb{Z}$. Namely it's clear that for an integer x, one has that $x^2 = 0 \mod p$ if and only if $p \mid x$. The number of elements of $\mathbb{Z}/p^2\mathbb{Z}$ of the form py for some $y \in \mathbb{Z}/p^2\mathbb{Z}$ is evidently p. The conclusion follows.

That said, one notices empirically that such a phenomenon does not really occur modulo a prime p, and this will be the main technical workhorse we will prove today. We will do so by studying the polynomial ring $\mathbb{Z}/p\mathbb{Z}[x]$ and, in particular, proving an analogue of Theorem 2.2.

9.2 The polynomial ring $\mathbb{Z}/m\mathbb{Z}[x]$ and functions

Up until this point we have mostly thought about elements of $\mathbb{Z}/m\mathbb{Z}[x]$ as being objects which define modulus Diophantine equations, and not so much as interesting mathematical objects unto themselves. But to show anything substantive about the number of solutions to a modulus Diophantine equations in terms of the degree of its defining polynomial we'll need to know a little bit more about polynomials as abstract objects.

So in this section we clarify a very subtle point that occurs when working with polynomials modulo m. This will not be strictly necessary to prove that polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$ have no more solutions than their degree, but it's an invaluable observation to make.

To do this though, it will help first to make the following definition:

Definition 9.1

Let m be an element of $\mathbb{N}^*$. Then, by $\mathrm{Fun}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ we mean the set of all functions (mappings of sets) $F : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. If F and G are elements of $\mathrm{Fun}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ then we define $F \pm G$ and $F \cdot G$ as follows:

$$(F \pm G)(z) := F(z) \pm G(z), \qquad (F \cdot G)(z) := F(z) \cdot G(z) \tag{227}$$

Now, as per usual, we can view polynomials as being special kinds of functions:

Definition 9.2

Let m be an element of $\mathbb{N}^*$. Then, given a polynomial $f(x) \in \mathbb{Z}/m\mathbb{Z}[x]$ the *associated function*, denoted F_f, is the function $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ given by sending $z \in \mathbb{Z}/m\mathbb{Z}$ to $f(z)$.

The notation F_f may seem overly-pedantic, and somewhat confusing. Why not just use f itself? The reason is that the relation between polynomials and functions over $\mathbb{Z}/m\mathbb{Z}$ is much more nuanced, and much stranger, than the analogous situation over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, or $\mathbb{R}$. Namely, we have the following:

Lemma 9.1

Let m be an element of $\mathbb{N}^*$. The mapping $F_\square : \mathbb{Z}/m\mathbb{Z}[x] \to \mathrm{Fun}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ given by $F_\square(f) = F_f$ satisfies the following properties:

1. For $f, g \in \mathbb{Z}/m\mathbb{Z}[x]$ one has that $F_{f\pm g} = F_f \pm F_g$.
2. For $f, g \in \mathbb{Z}/m\mathbb{Z}[x]$ one has that $F_{f\cdot g} = F_f \cdot F_g$.
3. For a constant $c \in \mathbb{Z}/m\mathbb{Z}$ the constant polynomial $c(x)$ is sent to the constant function $z \mapsto c$.
4. The mapping $F_\square$ is surjective and has infinite fibers.

The first three claims are obvious, and routine. It's the last claim that is scandalous. Let us say in plain-spoken English what it means:

1. Every single function $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is a polynomial function.
2. For every polynomial function f, there are infinitely many other polynomial functions g such that $F_f = F_g$.

In particular, we see that a polynomial is not, in an extreme way, determined by its associated function. This is a large departure from our usual situation over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ where can essentially conflate a polynomial and the function it represents.

Let us see some obvious examples, and so not so obvious examples:

Example 9.2

Consider the polynomial

$$f(x) := \prod_{a \in \mathbb{Z}/m\mathbb{Z}} (x - a) \tag{228}$$

Then, $f(x)$ is a non-zero element of $\mathbb{Z}/m\mathbb{Z}[x]$, in fact it has degree m, but certainly for every $z \in \mathbb{Z}/m\mathbb{Z}$ we have that $f(z) = 0$. Thus, while $f(z)$ is a large (by degree), non-zero polynomial, its associated function is identically zero.

Example 9.3

Let p be a prime. Then, the polynomial $f(x) = x^p - x$ is a non-zero polynomial of degree p. That said, by Corollary 5.5 we know that for every $a \in \Phi(p)$ we have that $a^{p-1} = 1$ and so $a^p = a$. Moreover,

$0^p = 0$. Thus, $F_f(z) = 0$ for all $z \in \mathbb{Z}/m\mathbb{Z}$.

This being said, it's actually 'obvious' that the map $F_\square$ can't be injective, since $\mathbb{Z}/m\mathbb{Z}[x]$ is infinite (e.g. it contains $1, x, x^2, \ldots$) and $\mathrm{Fun}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ is finite (it has size m^m). In fact, this reasoning also shows us that $F_{x^k} = F_{x^\ell}$ for infinitely many pairs x^k and x^ℓ.

Let us now prove Lemma 9.1:

Proof 9.1: Lemma 9.1

It suffices to prove part (4). To prove surjectivity let us define for all $a \in \mathbb{Z}/m\mathbb{Z}$ the function $\delta_a \in \mathrm{Fun}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ given as follows:

$$\delta_a(z) := \begin{cases} 1 & \text{if} \quad z = a \\ 0 & \text{if} \quad \text{otherwise} \end{cases} \tag{229}$$

Note then that for all $F \in \mathrm{Fun}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ one has that

$$F = \sum_{a \in \mathbb{Z}/m\mathbb{Z}} F(a)\delta_a \tag{230}$$

Since the image of $F_\square$ is closed under addition and multiplication by $\mathbb{Z}/m\mathbb{Z}$, it suffices to show that for all $a \in \mathbb{Z}/m\mathbb{Z}$ one has that δ_a is in the image of $F_\square$.

Let us define for each $a_0 \in \mathbb{Z}/m\mathbb{Z}$ the polynomial

$$f_{a_0}(x) := a_0 + \prod_{a \in \mathbb{Z}/m\mathbb{Z}} (x - a) \tag{231}$$

Then, as one can easily see one has that $F_{f_a} = \delta_a$. Thus, the surjectivity of $F_\square$ follows.

To see that each fiber of $F_\square$ is infinite, we proceed as follows. Let $f(x) \in \mathbb{Z}/m\mathbb{Z}[x]$. Then, for every $n \in \mathbb{N}^*$ let $g_n(x) := f(x) + f_0^n$ where $f_0(x)$ is as in (231). Since $F_{f_0^n} = 0$ for all $n \geqslant 1$ we see that $F_{g_n} f$ for all $n \geqslant 1$. The conclusion follows.

The conclusion of all of this is that one needs to take care when trying to understand polynomials in terms of their associated functions. In particular, note that $X_f(\mathbb{Z}/m\mathbb{Z})$ for $f \in \mathbb{Z}/m\mathbb{Z}[x]$ really only depends on F_f and not f.

9.3 Polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$

We now explain prime numbers have the property that their (univariate) polynomials don't, in fact, have more roots then their degree. The key observation is that if p is prime the set $\mathbb{Z}/p\mathbb{Z}[x]$ actually behaves, in many ways, like $\mathbb{Z}$. In particular, it has a division algorithm:

Lemma 9.2

Let p be a prime number. Then, given any f and g elements of $\mathbb{Z}/p\mathbb{Z}[x]$ with $g \neq 0$ there exists a unique $q(x)$ and $r(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ such that

$$f(x) = q(x)g(x) + r(x) \tag{232}$$

and either $r(x) = 0$ or $0 \leqslant \deg(r(x)) < \deg(g(x))$.

To prove this it will be helpful to observe the following pivotal property of $\mathbb{Z}/p\mathbb{Z}[x]$:

Lemma 9.3

Let p be a prime. If $f(x)$ and $g(x)$ are elements of $\mathbb{Z}/p\mathbb{Z}[x]$ and $f(x)g(x) = 0$ in $\mathbb{Z}/p\mathbb{Z}[x]$, then either $f(x) = 0$ or $g(x) = 0$.

Proof 9.2

Suppose that neither $f(x)$ nor $g(x)$ are zero. Then, we can write

$$f(x) = a_n x^n + \cdots + a_0 \tag{233}$$

for some $n \geqslant 0$ and $a_n \neq 0$ as well as

$$g(x) = b_m x^m + \cdots + b_0 \tag{234}$$

for some $m \geqslant 0$ and $b_m \neq 0$. Then, note that

$$f(x)g(x) = a_n b_m x^{n+m} + (\text{smaller degree terms}) \tag{235}$$

So, if $f(x)g(x) = 0$ then $a_n b_m = 0$. But, since p is prime and $a_n, b_m \neq 0$ we have that $a_n, b_m \in \Phi(p)$. Thus, $a_m b_m \in \Phi(p)$ and so, in particular, $a_n b_m \neq 0$. We thus arrive at a contradiction.

Proof 9.3: Lemma 9.2

Let us first show the existence of such an equation as in (232). If $f = 0$ then claim is clear. Also, if $\deg(f) < \deg(g)$ then claim is clear with $q = 0$ and $r = f$. Thus, we assume without loss of generality that $\deg(f) \geqslant \deg(g)$. We will proceed by induction on $\deg(f)$.

The base case will be when $\deg(f) = 0$. But, if $\deg(f) = 0$ the fact that $g \neq 0$ implies that $\deg(g) = 0$. Thus, f and g are both constants, say $f(x) = a$ and $g(x) = b \neq 0$. We can then take $q(x) = b^{-1}a$ and $r(x) = 0$. Thus, this case is done.

Let us now do the induction step. So, assume that we've proven the result for all $\deg(f) < n$, and we'll prove the case $\deg(f) = n$. Since $\deg(f) = n$ we can write

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \tag{236}$$

with $a_n \in \mathbb{Z}/p\mathbb{Z}$ and $a_n \neq 0$. Set $m := \deg(g) \leqslant \deg(f) = n$ and write

$$g(x) = b_m x^m + \cdots + b_1 x + b_0 \tag{237}$$

with $b_m \in \mathbb{Z}/p\mathbb{Z}$ and $b_m \neq 0$. Note then that $b_m^{-1} a_n x^{n-m} g(x)$ is a polynomial of degree n with leading coefficient a_n. Thus, $f(x) - b_m^{-1} a_n x^{n-m} g(x)$ is a polynomial of degree strictly smaller than n. By induction hypothesis we can write

$$f(x) - b_m^{-1} a_n x^{n-m} g(x) = q_1(x)g(x) + r(x) \tag{238}$$

with $r(x)$ either 0 or $\deg(r(x)) < \deg g(x)$. Note then that rearranging this equation gives

$$f(x) = (b_m^{-1} a_n x^{n-m} + q_1(x))g(x) + r(x) \tag{239}$$

and the induction is complete.

It remains to show why such an expression as in(232) is unique subject to $r = 0$ or $\deg(r) < \deg(g)$. To see this, suppose that

$$q_1(x)g(x) + r_1(x) = f(x) = q_2(x)g(x) + r_2(x) \tag{240}$$

with each $r_i(x)$ either 0 or $\deg(r_i) < \deg(g)$. Then, we rearrange to get

$$r_1(x) - r_2(x) = g(x)(q_2(x) - q_1(x)) \tag{241}$$

But, since the left hand side is either 0 or has degree strictly less than $\deg(g)$ and the right hand side is either 0 or has degree at least $\deg(g)$ we conclude that both sides are 0. Thus, $r_1(x) = r_2(x)$ and by Lemma 9.3 we also deduce $q_1(x) = q_2(x)$ since $g(x) \neq 0$.

Remark 9.1

It's worth noting that the fact that p was prime was used in two pivotal places. First is that if $a \neq 0$ then a is invertible in $\mathbb{Z}/p\mathbb{Z}$. This is only true for p prime. The reason this was relevant was that the statement of the theorem involved degree and degree only involves the largest term without a non-zero coefficient. But, one can see that the method of proof used not only the non-zeroness of the leading coefficient but the fact that it was then, subsequently, invertible. The second pivotal result used was Lemma 9.3 which evidently used that p was prime.

Remark 9.2

For those that have taken algebra, the above evidently works if if $\mathbb{Z}/p\mathbb{Z}$ is replaced by any field k, to show that $k[x]$ is always Euclidean domain (and thus a PID). Moreover, this was really the point. The reason that p was important is that primes are the only integers m for which $\mathbb{Z}/m\mathbb{Z}$ is a field. The conclusions below also hold for a general field k.

The key corollary of all of this, the thing that will be pivotal to relating the degree of $f(x)$ to the size of $X_f(\mathbb{Z}/p\mathbb{Z})$, is the following:

Corollary 9.1

Let p be a prime and let $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. If $a \in \mathbb{Z}/p\mathbb{Z}$ is such that $f(a) = 0$, then $f(x) = (x - a)q(x)$ for some $q(x) \in \mathbb{Z}/p\mathbb{Z}[x]$.

Proof 9.4

By Lemma 9.2 we know that we can write

$$f(x) = q(x)(x - a) + r(x) \tag{242}$$

for some $r(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ that is either 0 or $\deg(r) < \deg(x - a) = 1$. But, in the latter case $r(x) = c$ for some $c \neq 0 \in \mathbb{Z}/p\mathbb{Z}$. But, plugging in a to (242) gives $0 = 0 + r(a)$. So, $c = r(a) = 0$, which is a contradiction. Thus, $r(x) = 0$ and we're done.

This is something that does <u>not</u> happen for general m:

Example 9.4

Let $f(x) = x^2 - 1$. Then, $5 \in X_f(\mathbb{Z}/8\mathbb{Z})$. Note though that $x^2 - 1 = q(x)(x-5)$ has no solution with $q(x) \in \mathbb{Z}/8\mathbb{Z}[x]$. Indeed, it's clear that $q(x)$ would need to be of the form $q(x) = x - a$. But,

$$(x-a)(x-5) = x^2 - (5+a)x + 5a \tag{243}$$

From this we deduce that $a = -5$ and $5a = 1$. But, these can't both hold.

And, in fact, Corollary 9.1 is exactly what we need to say that $\#X_f(\mathbb{Z}/p\mathbb{Z}) \leqslant \deg(f)$:

Theorem 9.1

Let p be a prime number and d an element of $\mathbb{N}$. Let $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ have degree d (in particular be non-zero). Then, $X_f(\mathbb{Z}/p\mathbb{Z})$ contains at most d elements.

Proof 9.5

Suppose that $X_f(\mathbb{Z}/p\mathbb{Z}) = \{a_1, \ldots, a_n\}$ with $n > d$. Note since $f(a_1) = 0$ we know from Corollary 9.1 that $f(x) = q_1(x)(x - a_1)$. Note though that $f(a_2) = 0$ and so $q_1(a_2)(a_2 - a_1) = 0$. Since $a_2 - a_1 \neq 0$ this implies that $q_1(a_2) = 0$, and so $q_1(x) = q_2(x)(x - a_2)$ and so $f(x) = q_2(x)(x - a_1)(x - a_2)$. Continuing this process shows that $f(x) = q_2(x)(x - a_1) \cdots (x - a_n)$. But, this implies that $\deg(f) \geqslant n > d$, which is a contradiction.

Another corollary we obtain is the following:

Corollary 9.2

Let p be a prime and let $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ be a polynomial of degree d. Suppose that $a_1, \ldots, a_d \in X_f(\mathbb{Z}/p\mathbb{Z})$ are distinct. Then, if the leading coefficient of $f(x)$ is a then $f(x) = a(x - a_1) \cdots (x - a_d)$.

9.4 Exercises

Exercise 9.1

Problem: Use Corollary 5.5 and Corollary 9.2 to give an alternative proof of Theorem 5.4.

Solution: By Corollary 5.5 we know that $1, \ldots, p-1$ are all roots of $f(x) = x^{p-1} - 1$. We thus deduce from Corollary 9.2 that $f(x) = (x-1) \cdots (x-(p-1))$. But, $f(0) = 0^{p-1} - 1 = -1$. On the other hand

$$f(0) = (0-1) \cdots (0-(p-1)) = (-1)^{p-1} p! \tag{244}$$

Since p is odd $(-1)^{p-1} = 1$ and so we deduce that $p! = -1 \mod p$ as desired.

Exercise 9.2

Problem: Let p be a prime. Let us show that for all $0 < k < p$ we have that $p \mid \binom{p}{k}$.

1. Use Corollary 5.5 to show that $(1+a)^p = 1 + a = 1 + a^p$ for all $a \in \mathbb{Z}/p\mathbb{Z}$.
2. Deduce that $f(x) = (x+1)^p - x^p - 1$ has p solutions.
3. Show that $\deg(f) < p$ and deduce from Corollary 9.1 that $f(x) = 0$ in $\mathbb{Z}/p\mathbb{Z}[x]$.
4. Deduce that $p \mid \binom{p}{k}$ by applying the binomial theorem.

Solution:

1. This follows immediately from Corollary 5.5.
2. From 1. we see that $f(a) = 0$ for all $a \in \mathbb{Z}/p\mathbb{Z}$ from where the claim follows.
3. The fact that $\deg(f) < p$ follows from the fact that $(x+1)^p$ has highest degree term x^p and so $(x+1)^p - x^p - 1$ will have only terms of degree lower than p. If $f(x) \neq 0$ then Corollary 9.1 would imply that $f(x)$ as less than p roots. Since it doesn't we have that $f(x) = 0$ in $\mathbb{Z}/p\mathbb{Z}[x]$.
4. Using the binomial theorem we see that

$$f(x) = \sum_{j=1}^{p-1} \binom{p}{j} x^j \tag{245}$$

Since $f(x) = 0$ in $\mathbb{Z}/p\mathbb{Z}[x]$ all the coefficients of x^j must be zero in $\mathbb{Z}/p\mathbb{Z}$. This proves the claim.

10 Lecture 10: Primitive roots revisited

Having developed all the machinery we have since Lecture 6 we are finally able to prove Theorem 6.5 in its entirety. In fact, our goal for today will be to try and prove a more explicit version of Theorem 6.5 that not only shows that the m lsited there are the only m where there is a primitive root modulo m, but also for those listed m, give an algorithm to find a primitive root modulo m.

Obviously finding a primitive root modulo m is of great importance since, after all, the reason we cared about primitive roots were results like Theorem 6.3 which help us explicitly solve modulus Diophantine equations. But, such theorems usually require an explicitly given primitive root to function. So, if we are interested in not only solving power equations in theory, but solving them in practice, having an algorithm to find primitive roots is key. As we will see, this essentially will boil down to finding primitive roots modulo p, for which there is a semi-brute force approach.

10.1 Structure of $\Phi(2^k)$

Before we begin proving the positive part of Theorem 6.5, the existence of primitive roots modulo the listed integers, we first need to tie up loose end left by Theorem 7.6. Namely, we showed that no numbers m not on the list of Theorem 6.5 can have primitive roots modulo m except the case $m = 2^k$ for $k > 2$. So, let us quickly address this. In fact, let us prove something even stronger:

Theorem 10.1

Let k be an element of $\mathbb{N}^*$ greater than 2. Set $m := 2^k$. Then, every $z \in \Phi(m)$ has a unique representation in the form $(-1)^s 5^\ell$ where $s \in \{0,1\}$ and $t \in \{0,\dots,2^{k-2}-1\}$. Moreover, for any integers s_1, ℓ_1 and s_2, ℓ_2 we have that $(-1)^{s_1}5^{\ell_1} = (-1)^{s_2}5^{\ell_2}$ if and only if $s_1 = s_2 \mod 2$ and $\ell_1 = \ell_2 \mod 2^{k-2}$.

This explains the claim earlier that while $\Phi(2^k)$ is not, in general, generated by a single element, it is also generated by 2 elements. Note, also, that this lemma has the positive aspect of giving very explicit generators for $\Phi(m)$ when $m = 2^k$, whereas for the m in Theorem 6.5 that have a primitive root modulo m the generators for $\Phi(m)$ are only known to exist—they have no explicit description, only algorithms to find them.

Proof 10.1: Theorem 10.1

Let us begin by showing that $|5| = 2^{k-2}$. Indeed, it suffices to show that $5^{2^{k-2}} = 1 \mod 2^k$ and $5^{2^{k-3}} \neq 1 \mod 2^k$. Indeed, if $5^{2^{k-2}} = 1 \mod 2^k$ then $|5| \mid 2^{k-2}$. If $|5| < 2^{k-2}$ then it must be of the form 2^ℓ for $\ell \leqslant 2^{k-3}$ and thus $5^{2^{k-3}} = 1 \mod 2^k$ which is a contradiction.

To prove these claims we show that for all $k \geqslant 3$ one has that $5^{2^{k-3}} = 1 + 2^{k-1} \mod 2^k$ for all $k \geqslant 3$. Indeed, this evidently holds for $k = 3$. We then apply induction. Namely,

$$(1 + 2^{k-1})^2 = 1 + 2^k + 2^{2k-2} \tag{246}$$

Then, applying Exercise 10.2 together with with the fact that $2k-2 \geqslant k+1$ we deduce that $5^{2^{k-2}} = 1+2^k \mod 2^{k+1}$ as desired. From this we deduce that $5^{2^{k-3}} = 1 + 2^{k-1} \neq 1 \mod 2^k$. But, we also see that $5^{2^{k-2}} = 1 \mod 2^k$. Thus, $|5| = 2^{k-2}$ as desired.

Let us now prove the stated claim. Let us first note that if $(-1)^{s_1}5^{t_1} = (-1)^{s_2}5^{t_2}$ in $\mathbb{Z}/2^k\mathbb{Z}$ for $s_1, s_2 \in \{0,1\}$ and $t_1, t_2 \in \{0,\dots,2^{k-2}-1\}$ then $s_1 = s_2$ and $t_1 = t_2$. Indeed, reducing modulo 4 this equation becomes $(-1)^{s_1} = (-1)^{s_2} \mod 4$ which clearly implies that $s_1 = s_2$. Thus, it suffices to show that if $5^{t_1} = 5^{t_2}$ in $\mathbb{Z}/2^k\mathbb{Z}$ with $t_1, t_2 \in \{0,\dots,2^{k-2}-1\}$ then $t_1 = t_2$. But, this immediately follows from the fact that $|5| = 2^{k-2}$.

Thus, the set

$$S := \{(-1)^s 5^t : s \in \{0,1\} \text{ and } t \in \{0,\dots,2^{k-2}-1\} \tag{247}$$

forms a subset of $\Phi(m)$ of size $2 \cdot 2^{k-2} = 2^{k-1}$. But, $\#\Phi(m) = \varphi(2^k) = 2^{k-1}$. Thus, we see that $S = \Phi(m)$.

Finally, the claim that $(-1)^{s_1}5^{\ell_1} = (-1)^{s_2}5^{\ell_2}$ if and only if $s_1 = s_2 \mod 2$ and $\ell_1 = \ell_2 \mod 2^{k-2}$ is clear.

So, of course, we derive the following:

Corollary 10.1

Let $k > 2$ be an integer. Then, there is no primitive root modulo 2^k.

Proof 10.2

For any $x \in \Phi(2^k)$ we can write $x = (-1)^s 5^\ell$ for $s \in \{0,1\}$ and $\ell \in \{0, \ldots, 2^{k-2}-1\}$. Note then that

$$x^{2^{k-2}} = (-1)^{2^{k-2}s} 5^{2^{k-2}\ell} = ((-1)^{2^{k-2}})^s (5^{2^{k-2}})^\ell = 1^s 1^\ell = 1 \tag{248}$$

In particular, we deduce from Lemma 5.5 that for all $x \in \Phi(2^k)$ that $|x| \mid 2^{k-2}$. In particular, there exists no $x \in \Phi(2^k)$ such that $|x| = 2^{k-1} = \varphi(2^k)$. Thus, there is no primitive root modulo 2^k.

Theorem 10.1 will also be pivotal when we try to solve power equations modulo 2^k.

10.2 The proof of Theorem 6.5

Thus, considering Theorem 7.6 and Theorem 10.1, to prove Theorem 6.5 it suffices to show that if m is on the list of Theorem 6.5 then there is a primitive root modulo m.

The key point will be combining Theorem 9.1 with the following:

Lemma 10.1

Let m be an element of $\mathbb{N}^*$. The following are equivalent:

1. There is a primitive root modulo m.
2. For all positive divisors d of $\varphi(m)$ the equation $x^d = 1$ has at most d solutions in $\Phi(m)$.
3. For all positive divisors d of $\varphi(m)$ the equation $x^d = 1$ has exactly d solutions in $\Phi(m)$.

The intuition for why Lemma 10.1 is true is, roughly, as follows. We know from Theorem 5.3 that the elements of $\Phi(m)$ are all solutions of the equation $x^{\varphi(m)} = 1$ in $\Phi(m)$. Now, if there is no primitive root, then for all $x \in \Phi(m)$ one must have that $|x|$ is a strict divisor of $\varphi(m)$. The goal is then to show that forcing these $\varphi(m)$ elements to be solutions to the polynomials $x^d = 1$ for d strict divisors of $\varphi(m)$ will force one of the $x^d = 1$ to have more than d solutions.

Remark 10.1

For those that have taken algebra, it's worth mentioning the natural extension of the above result. Namely, if one inspects the proof of Lemma 10.1 below one will see that it shows the more general claim that a finite possibly non-abelian group G is cyclic if and only if the equation $x^d = e$, where $e \in G$ is the identity element, has at most d solutions for all positive integers d dividing $|G|$. The fact that this is really a statement about algebra comes from inspecting the argument in the proof of Lemma 10.1 which, when one looks closely, just uses the same sort of group/action combinatorics arguments that naturally show up in finite group theory.

If one is willing to assume their finite group G is abelian, as is the case for us, then one can prove Lemma 10.1 more simply assuming that one knows the Fundamental Theorem of Finitely Generated Abelian Groups. Namely, any finite abelian G can be decomposed as a product of cyclic groups $C_{m_1} \times \cdots \times C_{m_\ell}$ (here C_m is the cyclic group of order m) where $m_i > 1$ for all i and $m_i \mid m_{i+1}$. One then sees that G is cyclic if and only if $\ell = 1$. But, if $\ell > 1$ then $m_2 > 1$. Let $d \mid m_2$ be non-trivial. Then, it's easy to see that $|G[d]| \geqslant d^2$. Thus, if $|G[d]| \leqslant d$ for all $d \mid |G|$ one deduces that $\ell = 1$ and thus G is cyclic.

To do this, it will be helpful to make the following definition:

Definition 10.1

Let m be an element of $\mathbb{N}^*$. A subset S of $\Phi(m)$ is called a *cyclic subgroup of order* d if $S = \langle a \rangle$ for some $a \in \Phi(m)$, and $\#S = d$.

It's clear that $S \subseteq \Phi(m)$ is a cyclic subgroup of order d if and only if $S = \langle a \rangle$ for $a \in \Phi(m)$ and $|a| = d$. Let us now proceed with the proof of Lem 10.1:

Proof 10.3: Lemma 10.1

Let us begin by showing that (1) implies (3). Suppose that there is a primitive root modulo m. Then, by 6.2 we know that $x^d = 1$ has precisely $\gcd(d, \varphi(m)) = d$ solutions. The claim then follows.

Let us now show that (2) implies (1). To do this we begin by making the following obvious observation:

$$\Phi(m) = \bigsqcup_{\substack{d|\varphi(m) \\ d>0}} \{z \in \Phi(m) : |z| = d\} \tag{249}$$

which follows from the fact that every $d \in \Phi(m)$ has a unique order, and that if $z \in \Phi(m)$ that, by Lemma 5.5, one has that $|z| \mid \varphi(m)$. In particular, we deduce that

$$\varphi(m) = \sum_{\substack{d|\varphi(m) \\ d>0}} \underbrace{\#\{z \in \Phi(m) : |z| = d\}}_{Q_d} \tag{250}$$

Let us denote by C_d the set of all cyclic subgroups of $\Phi(m)$ of order d. Note that every $a \in \Phi(m)$ is contained in a unique cyclic subgroup of order d. Moreover, in any given cyclic subgroup S of order d there are exactly $\varphi(d)$ elements of order d. Indeed, this is equivalent to saying that there are exactly $\varphi(d)$ generators of S. The proof then follows exactly as in Lemma 6.2. Thus, we deduce that $Q_d = C_d\varphi(d)$.

Now, let us note that if S is a cyclic subgroup of order d, then $x^d = 1$ for all $x \in S$. Indeed, we know that $S = \langle a \rangle$ for some $a \in \Phi(m)$ with $|a| = d$. Then, every $x \in S$ is of the form a^ℓ for some ℓ. Evidently then $x^d = 1$. Since $\#S = d$, we deduce from the assumption that there are most d elements of $\Phi(m)$ satisfying $x^d = 1$ that $C_d \leqslant 1$. So, we get the equality

$$\varphi(m) = \sum_{\substack{d|\varphi(m) \\ d>0}} C_d\varphi(d) \tag{251}$$

But, recall from Exercise 7.4 that we have

$$\varphi(m) = \sum_{\substack{d|\varphi(m) \\ d>0}} \varphi(d) \tag{252}$$

Since $C_d \leqslant 1$ combining (251) and (252) implies that $C_d = 1$ for all d. In particular, $C_{\varphi(m)} = 1$. But, in particular, this implies that there is a cyclic subgroup of order $\varphi(m)$ of $\Phi(m)$ which, in particular, implies that there is a primitive root modulo m.

The rest of the implications are clear, and so the conclusion follows.

Combining this with Theorem 9.1 we immediately obtain the following:

Corollary 10.2

Let p be a prime. Then, there is a primitive root modulo p.

Remark 10.2

Considering Remark 9.2 and Remark 10.1 what the above really shows is that if k is any field then $k^\times[n]$ is a finite cyclic group of order dividing n for any n. What makes the above then tick is the fact that if k is finite then $k^\times$ is finite, so that $k^\times = k^\times[n]$ with $n := k^\times$. In particular, $k^\times$ is cyclic if k is finite.

This result is pure, unadulterated black magic. It is entirely non-constructive. That said, taking this black magic as given, we can give a much more concrete, explicit explanation for why primitive roots exist modulu the other numbers on the list in Theorem 6.5. We start with the case of p^2 where p is a prime:

Lemma 10.2

Let p be an odd prime. Then, there is a primitive root modulo p^2.

Proof 10.4

By Lemma 10.1 it suffices to show that for all positive divisors d of $\varphi(p^2) = p(p-1)$ that the equation $x^d = 1 \mod p^2$ has at most d solutions. Let us begin by assuming that $p \nmid d$. Then, $x^d = 1 \mod p$ has exactly d solutions by Lemma 10.1 and the fact that there is a primitive root modulo p. But, note that if $f(x) := x^d - 1$ then any $a \in X_f(\mathbb{Z}/p\mathbb{Z})$ is a unit. Thus, $df(a) = da^{d-1}$ is also a unit and so, in particular, non-zero. Thus, we see that f is smooth modulo p and so by Corollary 8.1 we see that $X_f(\mathbb{Z}/p^2\mathbb{Z}) \to X_f(\mathbb{Z}/p\mathbb{Z})$ is a bijection. Thus, $\#X_f(\mathbb{Z}/p^2\mathbb{Z}) = d$.

Now let us suppose that $p \mid d$. Write $d = pe$ with $p \nmid e$. Let us set $f(x) := x^d - 1$ again. Let us note that $\#X_f(\mathbb{Z}/p\mathbb{Z}) = e$. Indeed, note that by Corollary 5.5 that for all $x \in \mathbb{Z}/p\mathbb{Z}$ we have that $x^p = x$. Thus, $x^{pe} = x^e$. So, solving $x^{pe} = 1 \mod p$ is equivalent to solving $x^e = 1 \mod p$ which, as previously discussed, has exactly e solutions. Thus, $\#X_f(\mathbb{Z}/p\mathbb{Z}) = e$. Now, it's clear that $X_f(\mathbb{Z}/p\mathbb{Z}) = X_f^{\text{sing}}(\mathbb{Z}/p\mathbb{Z})$. Thus, by Theorem 8.4 for every $a \in X_f(\mathbb{Z}/p\mathbb{Z})$ there are either 0 or p elements of $X_f(\mathbb{Z}/p^2\mathbb{Z})$ lying over it. In particular, we see that

$$\#X_f(\mathbb{Z}/p^2\mathbb{Z}) \leqslant p(\#X_f(\mathbb{Z}/p\mathbb{Z})) = pe = d \tag{253}$$

from where the claim follows.

That said, we promised that things would be constructive after Corollary 10.2, so let us give a much more constructive proof of Lemma 10.2, also using Hensel's lemma:

Lemma 10.3

Let p be an odd prime. Suppose that ξ is a primitive root modulo p. Then, either ξ or $\xi + p$ is a primitive root modulo p^2.

Proof 10.5

Let us set g as either ξ or $\xi + p$. Note that $|g|_{p^2} \mid \varphi(p^2) = p(p-1)$ by Corollary 5.3. But, note that $p - 1 \mid |g_{p^2}|$. Indeed, since $g^{|g|_{p^2}} = 1 \mod p^2$ evidently we have that $g^{|g|_{p^2}} = 1 \mod p$. Thus, by Lemma 5.5, we have that $|g|_p = p - 1 \mid |g|_{p^2}$ where the former equality follows from the fact that $g = \xi$

mod p and ξ is a primitive root modulo p. Thus, the only possibilities for $|g|_{p^2}$ are p, $p-1$, and $p(p-1)$.

Note that $|g|_{p^2} \neq p$ since $g = \xi \mod p$. So, if $|g|_{p^2} = p$ then $g^p = 1 \mod p^2$ and so $g^p = 1 \mod p$. But, $g^p = g \mod p$ by Corollary 5.5 and $g = \xi \mod p$, so if $g^p = 1 \mod p$ then $\xi = 1 \mod p$ which is impossible since $p > 1$ (and ξ is a primitive root). Thus, it remains to show that $|g|_{p^2} \neq p-1$ for at least one of $g = \xi$ or $g = \xi + p$. Note though that if $f(x) = x^{p-1} - 1$ that f is smooth modulo p. Thus, the map $X_f(\mathbb{Z}/p^2\mathbb{Z}) \to X_f(\mathbb{Z}/p\mathbb{Z})$ is bijective. In particular, in the set of lifts to $\mathbb{Z}/p^2\mathbb{Z}$ of an element $a \in X_f(\mathbb{Z}/p\mathbb{Z})$ is a unique f-lift. Note that ξ and $\xi + p$ are distinct lifts of ξ, which is an element of $X_f(\mathbb{Z}/p\mathbb{Z})$. Thus, only one of them can be an f-lift. Whichever one is not an f-lift then does not satisfy $x^{p-1} = 1 \mod p^2$, and thus must have order $p(p-1)$. The conclusion follows.

Let us now show how to constructively build primitive roots modulo p^k, for $k \geqslant 2$, from primitive roots modulo p^2:

Lemma 10.4

Let p be an odd prime and let $k \in \mathbb{N}^*$ such that $k \geqslant 2$. If ζ is a primitive root modulo p^2 then ζ is a primitive root modulo p^k.

Proof 10.6

We prove the claim by induction. Suppose that ζ is a primitive root modulo p^k, we then need to show that ζ is a primitive root modulo p^{k+1}. Note that by Corollary 5.3 we have that

$$|\zeta|_{p^{k+1}} \mid \varphi(p^{k+1}) = p^k(p-1) \tag{254}$$

But, using the same argument as in the beginning of the proof of Lemma 10.3 we know that $|\zeta|_{p^k} \mid |\zeta|_{p^{k+1}}$ and, since ζ was assumed to be a primitive root modulo p^k, we have that $|\zeta|_{p^k} = p^{k-1}(p-1)$. Thus, we have that either $|\zeta|_{p^{k+1}} = p^{k-1}(p-1)$ or $|\zeta|_{p^{k+1}} = p^k(p-1)$. Thus, it suffices to prove that $|\zeta|_{p^{k+1}} \neq p^{k-1}(p-1)$ or, what amounts to the same thing, $\zeta^{p^{k-1}(p-1)} \neq 1 \mod p^{k+1}$.

Let us begin by noting that Theorem 5.3 implies that $\zeta^{p^{k-2}(p-1)} = 1 \mod p^{k-1}$. By definition, this then means that we can write $\zeta^{p^{k-2}(p-1)} = 1 + ap^{k-1}$ for some $a \in \mathbb{Z}$. Now, let us raise both side of this equation to the p^{th}-power to get

$$\zeta^{p^{k-1}(p-1)} = (1+ap^{k-1})^p = \sum_{j=0}^{p} \binom{p}{j} (ap^{k-1})^j = 1 + ap^k + \underbrace{\binom{p}{2} a^2 p^{2k-2} + \cdots}_{\text{terms divisible by } p^{k+1}} \tag{255}$$

Thus, we see that

$$\zeta^{p^{k-1}(p-1)} = 1 + ap^k \mod p^{k+1} \tag{256}$$

Thus, if $\zeta^{p^{k-1}(p-1)} = 1 \mod p^{k+1}$ then $1 + ap^k = 1 \mod p^{k+1}$. This says that $p \mid a$. But, since $\zeta^{p^{k-2}(p-1)} = 1 + ap^k$ this would imply $\zeta^{p^{k-2}(p-1)} = 1 \mod p^k$ which contradicts that $|\zeta|_{p^k} = p^{k-1}(p-1)$ by the induction hypothesis that ζ is a primitive root modulo p^k. The conclusion follows.

Remark 10.3

Something subtle happened in the above proof. Namely, Lemma 10.4 must have used that p was odd somewhere, since the statement doesn't hold for $p = 2$ and $k = 3$. Where did it use oddness? The key was in the claim in (255) that the terms listed as divisible by p^{k+1} are, in fact, so. Note that these

terms look like $\binom{p}{j}a^j p^{jk-j}$ where $j \geqslant 2$. Note that if $j > 2$ and $k \geqslant 2$ then $jk - j > k + 1$. But, note that for $j = 2$ one has that $2k - 2 \geqslant k + 1$ only holds for $k \geqslant 3$, in particular p^{2k-2} isn't divisible by p^{k+1} if $k = 2$ and so can't be used in proceeding from the induction step $k = 2$ to $k = 3$. That said, the full term is not p^{2k-2} it's actually $\binom{p}{2}a^2 p^{2k-2}$. So, the question becomes whether $\binom{p}{2}p^{2k-2}$ is divisible by p^{k+1} when $k = 2$. But, this seems trivial since when $k = 2$ this reduces to $\frac{p^4}{2} - \frac{p^3}{2}$ which clearly seems divisible by p^3. But, to write that, to separate $\binom{p}{2}$, an integer, into $\frac{p^2}{2} - \frac{p}{2}$ in $\mathbb{Z}/p\mathbb{Z}$ you need to be able to invert 2. In particular, you need $p \neq 2$. And, indeed, when $p = 2$ one has that $\binom{p}{2}p^2$ is actually 4 which is not divisible by $2^3 = 8$. This is where we need p odd.

Remark 10.4

For those that have taken more advanced algebra, it's clear that one soup up the above Hensel's lemma arguments to show that if R is any infinitesimal thickening of a field k, then $R^\times[n]$ is cyclic for any n. The above then follows by taking $R = \mathbb{Z}/p^\ell\mathbb{Z}$ which is an infinitesimal thickening of $\mathbb{F}_p$, and one can take $n := |R^\times|$.

Thus, the last real case we need to address is the case $2p^k$ where p is an odd prime. This is quite easy, and handled as follows:

Lemma 10.5

Let p be an odd prime and k an element of $\mathbb{N}^*$. Let κ be a primitive root modulo p^k. If κ is odd then κ is a primitive root modulo $2p^k$. If κ is even then $\kappa + p^k$ is a primitive root modulo $2p^k$.

Proof 10.7

Consider the reduction map

$$r : \Phi(2p^k) \to \Phi(2) \times \Phi(p^k) \tag{257}$$

This map is a bijection and satisfies $r(1) = (1, 1)$ and $r(xy) = r(x)r(y)$. In particular, if $r(x)$ is a generator of $\Phi(2) \times \Phi(p^k)$ then x is a generator of $\Phi(2p^k)$. But, since $\Phi(2) = \{1\}$ it's clear that $(1, \kappa)$ is a generator of $\Phi(2) \times \Phi(p^k)$. Thus, it remains to find an $x \in \Phi(2p^k)$ such that $r(x) = (1, \kappa)$. This can be done explicitly by the inverse in Theorem 7.2 and yields the claimed answer.

We have thus, finally, proven Theorem 6.5 in its entirety.

10.3 Algorithmically finding primitive roots

One nice upside of the above proofs is that they actually make Theorem 6.5 much more explicit and, in fact, algorithmically construct a primitive root modulo p^k or $2p^k$ (where p is an odd prime) given a primitive root modulo p. Thus, we can algorithmically find primitive roots modulo any p^k or $2p^k$ assuming that we are able to find an algorithm to compute primitive roots modulo p.

There is an obvious brute force algorithm to do this (just check the powers of every element of $\Phi(p)$ until you find one that generates $\Phi(p)$), but there is a quick way to reduce the running time significantly. It's based on the following simple observation:

Lemma 10.6

Let p be a prime. Then, $a \in \Phi(p)$ is a primitive root modulo p if and only if for all primes $q \mid p-1$ one has that $a^{\frac{p-1}{q}} \neq 1 \mod p$.

Proof 10.8

Suppose that a is not a primitive root modulo p. Then, $|a|$ is a strict divisor of $\varphi(p) = p-1$. But, note that all strict divisors of $p-1$ divide a number of the form $\dfrac{p-1}{q}$ for a prime factor q of $p-1$. In particular, $a^{\frac{p-1}{q}} = 1 \mod p$ for some prime divisor q of $p-1$. The claim follows.

Thus, we have the following:

Algorithm 10.1

Let p be a prime. Then, the following is an algorithm to compute a primitive root modulo p:

Step 1: Factorize $p-1 = q_1^{e_1} \cdots q_\ell^{e_\ell}$, where q_i is prime, $q_i \neq q_j$ for $i \neq j$, and $e_i \geqslant 1$ for all i.

Step 2: Set $a = 1$ and compute $b_i = a^{\frac{p-1}{q_i}} \mod p$ for $i = 1, \ldots, \ell$.

Step 3: If $b_i \neq 1$ for all i then a is a primitive root. Otherwise, iterate a and repeat Step 2.

Thus, combining everything above, we then obtain a very explicit, algorithmic version of Theorem 6.5:

Theorem 10.2

Let m be an element of $\mathbb{N}^*$. Then, there is a primitive root modulo m if and only if m is a number on the following list: 2, 4, p^k where p is an odd prime and $k \in \mathbb{N}^*$, or $2p^k$ where p is an odd prime and $k \in \mathbb{N}^*$.

Moreover, if there is a primitive root modulo m, then the following gives an algorithm to compute it:

Case 1: If $m = 2$, then one can take 1.

Case 2: If $m = 4$, then one can take 3.

Case 3: If $m = p$ a prime, one proceeds as in Algorithm 10.1 to find a primitive root ξ.

Case 4: If $m = p^k$ where p is an odd prime and $k \geqslant 1$, one finds ξ as in Case 3. One computes $b := (\xi^{p-1} \mod p^2)$. If $b \neq 1$, then ξ is a primitive root modulo p^k. If $b = 1$ then $\xi + p$ is a primitive root modulo p^k. This finds a primitive root ζ.

Case 5: If $m = 2p^k$ where p is an odd prime, find a primitive root ζ modulo p^k as in Case 4. If ζ is odd then one can take ζ, if ζ is even then one can take $\zeta + p^k$.

Let us end this section by noting that Algorithm 10.1 should, in general, terminate fairly quickly. Namely, one shouldn't have to look at numbers much bigger than 1 before they find a primitive root modulo p. A nice theorem to this effect is the following:

Theorem 10.3: Shoup '92

Suppose that the Generalized Riemann Hypothesis is true. Let p be a prime, and let g_p be the smallest element of $\{1, \ldots, p-1\}$ that is a primitive root modulo p. Then, $g_p = \mathrm{O}(\ln(p)^6)$.

So, one should only have to approximately perform the iteration part of Step 3 of Algorithm 10.1 about $\log^6(p)$ times which, at least compared to p, is miniscule. So, in practice, Algorithm 10.1 should actually be surprisingly quick.

10.4 Exercises

Exercise 10.1

Problem: Find a primitive root modulo $2 \cdot 11^3$.

Solution: Following Theorem 10.2 we first find a primitive root modulo 11. Clearly 1 doesn't work. To check if 2 is a primitive root we factor $11 - 1 = 2 \cdot 5$. We need to see if 2^2 and 2^5 are not 1 in $\mathbb{Z}/11\mathbb{Z}$. But, $2^2 = 4 \neq 1 \mod 11$ and $2^5 = 32 = -1 \neq 1 \mod 11$. Thus, 2 is a primitive root modulo 11. We then continue on and check whether or not $2^{10} = 1 \mod 11^2$. But, $2^{10} = 1024 \neq 1 \mod 11^2$. Thus, 2 is also a primitive root modulo 11^2. Then, continuing on we see that 2 is a primitive root modulo 11^3. Finally, since 2 is even we deduce that $2 + 11^3 = 1333$ is a primitive root modulo $2 \cdot 11^3$.

Exercise 10.2

Problem: Let p be a prime, a and b be elements of $\mathbb{Z}$, and k be in $\mathbb{N}^*$. Show that if $a = b \mod p^k$ then $a^p = b^p \mod p^{k+1}$.

Solution: If $a = b \mod p^k$ we can write $a = b + cp^k$ for some $c \in \mathbb{Z}$. So, we see that

$$a^p = (b + cp^k)^p = b^p + \binom{p}{1} b^{p-1} cp^k + (\text{terms divisible by } p^{2k}) \tag{258}$$

but since $\binom{p}{1} = p$ we deduce also that the second term on the right hand side is divisible by p^{k+1} so the claim follows.

11 Lecture 11: Solving the general power equation

After having developed the massive amount of machinery in the previous lectures we would finally, triumphantly like to put together everything and give a complete fulfillment of Goal 5.1. Now, while the vast majority of the heavy lifting has already be done, there are some odds and ends that need to be addressed. Let us specify what remains to be done.

By Corollary 7.2 applied to an arbitrary number of primes, to solve $x^n = a \mod m$ it suffices to solve $x^n = a \mod p^k$ for p a prime. We have, thanks to Theorem 6.3 and Theorem 6.5, essentially solved this assuming that p is odd and $a \in \Phi(p^k)$. Thus, what remains is to fill in the holes and do the following:

1. Show how to reduce solving $x^n = a \mod p^k$ for a general $a \in \mathbb{Z}/p^k\mathbb{Z}$ to solving an equation of the form $x^n = b \mod p^\ell$ for some ℓ and some $b \in \Phi(p^\ell)$.

2. Explain how to mend Theorem 6.3 in the case when $m = 2^k$ for $k > 2$.

The next two sections will be devoted to addressing precisely these two questions.

11.1 Power equations with non-units

Let us begin by trying to remove the assumption that $a \in \Phi(p^k)$ when trying to solve equations of the form $x^n = a \mod p^k$. The first key observation is the following parameterization of elements of $\mathbb{Z}/p^k\mathbb{Z}$ in terms of units and powers of p:

Lemma 11.1

Let p be prime and let k be an element of $\mathbb{N}^*$. Then, every $0 \neq x \in \mathbb{Z}/p^k\mathbb{Z}$ can be written in the form $x = p^\ell u$ for a $\ell \in \{0, \ldots, k-1\}$ and a (possibly non-unique) $u \in \Phi(p^k)$. If, in addition, $x = p^{\ell_2} u_2$ for an arbitrary $\ell_2 \in \mathbb{N}$ and $u_2 \in \Phi(p^k)$ then $\ell = \ell_2$ and $u = u_2 \mod p^{k-\ell}$.

Proof 11.1

Let $0 \neq x \in \mathbb{Z}/p^k\mathbb{Z}$. Factorizing x as an integer we can certainly write it as $p^\ell u$ with $\gcd(u, p) = 1$ and $\ell \geqslant 0$. If $\ell \geqslant k$ then $x = 0$ and so $\ell \in \{0, \ldots, k-1\}$. Since $\gcd(u, p) = 1$ we know that u is a unit.

Suppose now that $p^\ell u = x = p^{\ell_2} u_2$ with $u_2 \in \Phi(p^k)$ and $\ell_2 \in \mathbb{N}^*$. Begin by noting that ℓ_2 is actually in $\{0, \ldots, k-1\}$ else $p^{\ell_2} u_2 = 0$ which is impossible $x \neq 0$. Next we suppose without loss of generality, $\ell \geqslant \ell_2$. If $\ell > \ell_2$ then multiplying both sides by $p^{k-\ell}$ shows that

$$0 = p^{k-\ell+\ell_2} u_2 \mod p^k \tag{259}$$

Note though that $0 \leqslant k - \ell + \ell_2 < k$ and since $u_2 \in \Phi(p^k)$ this is a contradiction. Thus, $\ell = \ell_2$. To see that $u = u_2 \mod p^{k-\ell}$ we then merely apply Theorem 5.2.

Using this we deduce the following spectacular result:

Theorem 11.1

Let p be a prime and k and n elements of $\mathbb{N}^*$. Let $0 \neq a \in \mathbb{Z}/p^k\mathbb{Z}$ and write $a = p^\ell u$ for some $\ell \in \{0, \ldots, k-1\}$ and $u \in \Phi(p^k)$. The equation $x^n = a \mod p^k$ has a solution if and only if $n \mid \ell$ and $x^n = u \mod p^{k-\ell}$ has a solution. Moreover, the set of solutions is precisely the set

$$\{p^{\frac{\ell}{n}}(v + tp^{k-\ell}) : v \in \Phi(p^{k-\ell}) \text{ is such that } v^n = a \mod p^{k-\ell} \text{ and } t \in \mathbb{Z}/p^{\ell-\frac{\ell}{n}}\mathbb{Z}\} \tag{260}$$

and no two elements on right hand side (multi)set are equal.

Remark 11.1

In Theorem 11.1 we are committing a useful, but possibly confusing, impreciseness. Namely, for $v \in \Phi(p^{k-\ell})$ and $t \in \mathbb{Z}/p^{\ell-\frac{\ell}{n}}$ the expression $p^{\frac{\ell}{n}}(v + tp^{k-\ell})$ doesn't *really* make sense. What we really mean by the above is the following:

> "The solutions to $x^n = a \mod p^k$ are integers of the form $p^{\frac{\ell}{n}}(v + tp^{k-\ell})$ where v and t are integers and $v^n = u \mod p^{k-\ell}$. Moreover two solutions $p^{\frac{\ell}{n}}(v_1 + t_1 p^{k-\ell})$ and $p^{\frac{\ell}{n}}(v_2 + t_2 p^{k-\ell})$

are equal modulo p^k if and only if $v_1 = v_2 \mod p^{k-\ell}$ and $t_1 = t_2 \mod p^{\ell-\frac{\ell}{n}}$."

And thus, it really behooves one to think of $v \in \Phi(p^{k-\ell})$ and $t \in \mathbb{Z}/p^{\ell-\frac{\ell}{n}}\mathbb{Z}$.

Proof 11.2: Theorem 11.1

Let us begin by showing that every element in the set on the right hand side of (260) is a solution to $x^n = a \mod p^k$. But, for such a $p^{\frac{\ell}{n}}(v + tp^{k-\ell})$ we see that

$$(p^{\frac{\ell}{n}}(v + tp^{k-\ell}))^n = p^\ell (v + tp^{k-\ell})^n \tag{261}$$

To have this be equal to $a = p^\ell u$ we see from Lemma 11.1 that it's necessary and sufficient that

$$u = (v + tp^{k-\ell})^n \mod p^{k-\ell} \tag{262}$$

which we see is equivalent to $u = v^n \mod p^{k-\ell}$ from where the conclusion follows.

Let us now show that every element of the set on the left hand side of (260) is in the set on the right hand side. So, suppose that $x \in \mathbb{Z}/p^k\mathbb{Z}$ is such that $x^n = a \mod p^\ell$. Since $a \neq 0$ evidently $x \neq 0$. Write $x = p^t w$ as in Lemma 11.1. Then, $x^n = p^{tn} w^n$. Thus, we see that $p^{tn} w^n = p^\ell u$. Thus, by Lemma 11.1, $tn = \ell$ and $w^n = u \mod p^{k-\ell}$. So, the conditions that x are a solution is that $x = p^{\frac{n}{\ell}} w$ where $w \in \Phi(p^k)$ and $w^n = u \mod p^{k-\ell}$. Now, note that since $p^{\frac{n}{\ell}} w = p^{\frac{n}{\ell}} w'$ if and only if $w = w' \mod p^{k-\frac{\ell}{n}}$ we may as well think of w as lying in $\Phi(p^{k-\frac{\ell}{n}})$. Now, note that any such $w \in \Phi(p^{k-\frac{\ell}{n}})$ such that $w^n = u \mod p^{k-\ell}$ can be written, using Lemma 8.1, as $v + tp^{k-\ell}$ for some $t \in \mathbb{Z}$ which is only relevant modulo $p^{\ell-\frac{\ell}{n}}$, and thus can be thought about as an element of $\mathbb{Z}/p^{\ell-\frac{\ell}{n}}$.

All that remains to be shown is that no two terms in the right hand side of (260) are equal. So, suppose that

$$p^{\frac{\ell}{n}}(v + tp^{k-\ell}) = p^{\frac{\ell}{n}}(v' + t'p^{k-\ell}) \tag{263}$$

Then, using Lemma 11.1 we deduce that

$$v + tp^{k-\ell} = v' + t'p^{k-\ell} \mod p^{k-\frac{\ell}{n}} \tag{264}$$

from where the claim follows from Lemma 8.1.

One corollary we immediately get is the following:

Corollary 11.1

Let p be an odd prime and k and n elements of $\mathbb{N}^*$. Let $0 \neq a \in \mathbb{Z}/p^k\mathbb{Z}$ and write $a = p^\ell u$ for some $\ell \in \{0, \ldots, k\}$ and $u \in \Phi(p^k)$. If the equation $x^n = a \mod p^k$ has a solution, then $\ell \mid n$ it has

$$\begin{aligned} p^{\ell-\frac{\ell}{n}} \gcd(n, \varphi(p^{k-\ell})) &= p^{\ell-\frac{\ell}{n}} \gcd(n, p^{k-\ell-1}(p-1)) \\ &= p^{\ell-\frac{\ell}{n}+\min\{v_p(n), k-\ell-1\}} \gcd(n, p-1) \end{aligned} \tag{265}$$

solutions.

We now handle the case of $a = 0$ separately:

Theorem 11.2

Let p be a prime and k and n elements of $\mathbb{N}^*$. Then, the equation $x^n = 0 \mod p^k$ has the following

set of solutions

$$\{p^\ell u : \ell \in \{0, \ldots, k\} \text{ and } n\ell \geqslant k \text{ and } u \in \Phi(p^k)\} \tag{266}$$

Moreover, the set of such solutions is $\left(k - \left\lfloor \frac{k}{n} \right\rfloor\right) p^{k-1}(p-1)$.

We thus see that combining Theorem 11.1 and Theorem 11.2 allows us to reduce solving power equations involving non-units to solving power equations involving units modulo a possibly smaller power of p.

Let us give an example of the above:

Example 11.1

Let us solve $x^2 = 3^4 \cdot 7 \mod 3^6$. By the above we begin by solving $x^2 = 7 \mod 9$. One quickly checks by hand that the solutions are 4 and 5. Thus, we see that the solutions to the equation $x^2 = 3^4 \cdot 7 \mod 3^6$ are

$$\{3^2(4 + t \cdot 3^2) : t \in \mathbb{Z}/3^2\mathbb{Z}\} \cup \{3^2(5 + t \cdot 3^2) : t \in \mathbb{Z}/3^2\mathbb{Z}\} \tag{267}$$

11.2 Solving power equations modulo 2^k

Let us now deal with how to solve equations of the form $x^n = a \mod 2^k$ where $a \in \Phi(2^k)$ and $k > 2$. The key result, not shockingly, is Theorem 10.1:

Theorem 11.3

Let k and n be elements of $\mathbb{N}^*$with $k > 2$. Let $a \in \Phi(2^k)$. Write $a = (-1)^s 5^t$ where $s \in \{0, 1\}$ and $t \in \{0, \ldots, 2^{k-2} - 1\}$. The equation $x^n = a \mod 2^k$ is solvable if and only if the following simultaneous modulus Diophantine equation is solvable

$$\begin{cases} nx = s_0 \mod 2 \\ ny = t_0 \mod 2^{k-2} \end{cases} \tag{268}$$

which is the case if and only if $\gcd(n, 2) \mid s$ and $\gcd(n, 2^{k-2}) \mid t$. If $x = (-1)^{s_0} 5^{t_0}$ are a solution to $x^n = a \mod 2^k$, then the full set of solutions to $x^n = a \mod 2^k$, without repeats, is

$$\{(-1)^{s_0 + k\frac{2}{\gcd(n,2)}} 5^{t_0 + \ell \frac{2^{k-2}}{\gcd(n, 2^{k-2})}} : k \in \{0, \gcd(n, 2) - 1\} \text{ and } \ell \in \{0, \ldots, \gcd(n, 2^{k-2}) - 1\}\} \tag{269}$$

Proof 11.3

Note that for $a, b, c, d \in \mathbb{Z}$ one has that $(-1)^a 5^b = (-1)^c 5^d \mod 2^k$ if and only if $a = c \mod 2$ and $b = d \mod 2^{k-2}$. The claim then immediatley follows by writing an arbitrary element x of $\Phi(2^k)$ as $(-1)^a 5^b$ and noting that $x^n = a \mod 2^k$ if and only if $(-1)^{na} 5^{nb} = (-1)^s 5^t$. Thus, solving $x^n = a \mod 2^k$ comes down to solving the simultaneous modulus Diophantine equation (268). The rest of the proposition then follows immediately from Lemma 5.1.

This a result analogous to most of Theorem 6.3 with one major difference. In Theorem 6.3 one could check whether $x^n = a \mod m$ has a solution without having to explicitly express a as a power of a primitive root. We would like the analogous result here. We will handle the case when $2 \nmid n$ and $n = 2^\ell$ separately, from where the general case is done by applying the two results separately/iteratively.

The first case is remarkably simple, owing to the fact that $\varphi(2^k)$ is remarkably simple (it's just 2^{k-1}):

Lemma 11.2

Suppose that n is odd and k is an element of $\mathbb{N}^*$. Then, for any $a \in \Phi(2^k)$ the equation $x^n = a \mod 2^k$ has a unique solution.

Proof 11.4

This is just Corollary 5.4 since $\gcd(n, \varphi(2^k)) = \gcd(n, 2^{k-1}) = 1$.

The case of $n = 2^\ell$ is more nuanced:

Lemma 11.3

Let ℓ and k be elements of $\mathbb{N}^*$ with $k > 2$. Set $m := \min\{\ell, k-2\}$. Let $a \in \Phi(2^k)$. Then, the equation $x^{2^\ell} = a \mod 2^k$ is solvable if and only if $a = 1 \mod 2^{m+2}$.

Proof 11.5

Write $a = (-1)^s 5^t$ with $s \in \{0, 1\}$ and $t \in \{0, \ldots, 2^{k-2} - 1\}$. From Theorem 11.3 we know that $x^{2^\ell} = a \mod 2^k$ has a solution if and only if $\gcd(2^\ell, 2) = 2 \mid s$ and $\gcd(2^\ell, 2^{k-2}) = 2^m \mid t$. Of course, the statement $2 \mid s$ is equivalent to $s = 0$. Thus, $x^n = a \mod m$ has a solution if and only if $a = 5^t$ where $2^m \mid t$. We claim that this is equivalent to $a = 1 \mod 2^{m+2}$. Indeed, applying Theorem 10.1 one sees that $(-1)^s 5^t = 1 \mod 2^{m+2}$ if and only if $s = 0$ and $t = 0 \mod 2^m$.

Combining them, we get the result we've desired:

Corollary 11.2

Let n and k be elements of $\mathbb{N}^*$ with $k > 2$. Set $m := \min\{v_2(n), k-2\}$. Let $a \in \Phi(2^k)$ Then, the equation $x^n = a \mod 2^k$ has a solution if and only if one of the following holds:

1. n is odd.
2. n is even and $a = 1 \mod 2^{m+2}$.

Proof 11.6

If 1. holds then this is Lemma 11.2, so we assume that n is even Write $n = 2^{v_2(n)} r$ for r odd. Then, solving $x^n = a \mod 2^k$ is equivalent to solving $(x^r)^{v_2(n)} = a \mod 2^k$. Since $x^r = b \mod m$ has a unique solution for every $b \in \Phi(2^k)$, it's clear that $x^n = a \mod m$ has a solution if and only if $x^{v_2(n)} = a \mod 2^k$ has a solution. One then applies Lemma 11.3.

Putting all of this together we get the full analogue of Theorem **??** for 2^k:

Theorem 11.4

Let k and n be elements of $\mathbb{N}^*$ with $k > 2$. Let $a \in \Phi(2^k)$. Set $m := \min\{v_2(n), k-2\}$. The equation $x^n = a \mod 2^k$ has a solution if and only if one of the following holds:

1. n is odd.
2. n is even and $a = 1 \mod 2^{m+2}$.

Moreover, assuming that $x^n = a \mod 2^k$ has a solution the set of solutions is, without repeats, the following set:

$$\{(-1)^{s_0+k\frac{2}{\gcd(n,2)}} 5^{t_0+\ell\frac{2^{k-2}}{\gcd(n,2^{k-2})}} : k \in \{0, \gcd(n,2)-1\} \text{ and } \ell \in \{0,\ldots,\gcd(n,2^{k-2})-1\}\} \tag{270}$$

where (s_0, t_0) is any pair of integers such that $ns_0 = s \mod 2$ and $nt_0 = t \mod 2^{k-2}$. There is an algorithm to find such integers.

11.3 A complete understand of power equations

Thus, the glorious culmination of our work over the last few weeks is the following procedure:

Algorithm 11.1: Omnibus Euler criterion

Let n and m be elements of $\mathbb{N}^*$. Let $a \in \mathbb{Z}$. Set $f(x) = x^n - a$. Then, the following gives a process to completely, algorithmically understand $X_f(\mathbb{Z}/m\mathbb{Z})$:

Step 1: Iteratively applying Theorem 7.2 allows one to form an explicit, algorithmic bijection

$$X_f(\mathbb{Z}/m\mathbb{Z}) \to X_f(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots X_f(\mathbb{Z}/p_\ell^{e_\ell}\mathbb{Z}) \tag{271}$$

where $m = p_1^{e_1}\cdots p_\ell^{e_\ell}$, p_i is prime for all i, $p_i \neq p_j$ for $i \neq j$, and $e_i \geqslant 1$ for each i. Thus, it suffices to understand $X_f(\mathbb{Z}/p^k\mathbb{Z})$ for p a prime and $k \in \mathbb{N}^*$.

Step 2: If $p \mid a$ then Theorem 11.1 and Theorem 11.2 allow us to reduce to solving $x^n = b \mod p^j$ for some $j \leqslant k$ and $b \in \Phi(p^j)$. Thus, we may reduce to the case of solving $x^n = a \mod p^k$ where $a \in \Phi(p^k)$.

Step 4: If p is odd, $p^k = 2$, or $p^k = 4$, then we have a complete, algorithmic understanding of $X_f(\mathbb{Z}/p^k\mathbb{Z})$ by applying Theorem 6.3. If, in addition, $\gcd(n,p) = 1$ we can apply Corollary 8.2 to form an algorithmic bijection $X_f(\mathbb{Z}/p^k\mathbb{Z}) \to X_f(\mathbb{Z}/p\mathbb{Z})$.

Step 5: If $p^k = 2^k$ with $k > 2$ then we have a complete, algorithmic understanding of $X_f(\mathbb{Z}/2^k\mathbb{Z})$ by Theorem 11.4

For example, the above allows us to deduce the following:

Corollary 11.3

Let n and m be elements of $\mathbb{N}^*$. Let $a \in \mathbb{Z}$. Set $f(x) := x^n - a$. Assume that $X_f(\mathbb{Z}/m\mathbb{Z})$ is non-empty. Then,

$$\#X_f(\mathbb{Z}/m\mathbb{Z}) = N_{\text{odd}}(n,m,a)N_{\text{even}}(n,m,a) \tag{272}$$

where

$$N_{\text{odd}}(n,m,a) = \prod_{\substack{p \mid m, p \nmid a \\ p \text{ odd}}} \gcd(n, p^{v_p(m)-1}(p-1)) \prod_{p \mid \gcd(a,m)} \delta_p(n,m,a) \tag{273}$$

where for p odd and $p \mid \gcd(a,m)$:

$$\delta_p(n,m,a) := \begin{cases} p^{v_p(a) - \frac{v_p(a)}{n} + \min\{v_p(n), v_p(m) - v_p(a) - 1\}} \gcd(n, p-1) & \text{if} \quad a \neq 0 \mod p^{v_p(m)} \\ \left(v_p(m) - \left\lfloor \frac{v_p(m)}{n} \right\rfloor\right) p^{v_p(m)-1}(p-1) & \text{if} \quad a = 0 \mod p^{v_p(m)} \end{cases} \tag{274}$$

and

$$N_{\text{even}}(n,m,a) = \begin{cases} 1 & \text{if} \quad 2 \nmid m \\ \delta_2(n,m,a) & \text{if} \quad 2 \mid m \end{cases} \tag{275}$$

where

$$\delta_2(n,m,a) = \begin{cases} 1 & \text{if} \quad n \text{ odd} \\ 2^{\min\{v_2(n), v_2(m)-2\}+1} & \text{if} \quad a \in \Phi(2^k) \\ 2^{v_2(a) - \frac{v_2(a)}{n} + \min\{v_2(n), v_2(m)-2\}+1} & \text{if} \quad 0 \neq a \notin \Phi(2^k) \\ \left(v_2(m) - \left\lfloor \frac{v_2(m)}{n} \right\rfloor\right) 2^{v_2(m)-1} & \text{if} \quad 0 = a \notin \Phi(2^k) \end{cases} \tag{276}$$

12 Lecture 12: Quadratic reciprocity: Basic definitions and examples

Even though we have a pretty complete understanding of modulus power equations, we venture now to give an even more comprehensive study of the power equation $x^2 = a \mod p$ where p is a prime.

12.1 Setup

Thanks to Theorem 11.1 we have a pretty thorough understanding of solving the equation $x^n = a \mod m$, where $a \in \mathbb{Z}$ and n and m are in $\mathbb{N}^*$. In particular, we certainly have a good understanding of solving $x^2 = a \mod m$ where m is some natural number and $a \in \Phi(m)$. Let us try to summarize what we know, essentially specializing Theorem 11.1 to the case of $n = 2$ and $a \in \Phi(m)$:

Algorithm 12.1: Omnibus Euler's criterion($n = 2$)

Let m be an element of $\mathbb{N}^*$ and a an element of $\mathbb{Z}$ coprime to m. Set $f(x) := x^2 - a$. The following gives an algorithmic description of $X_f(\mathbb{Z}/m\mathbb{Z})$:

- If one gives a prime factorization $m = 2^e p_1^{e_1} \cdots p_\ell^{e_\ell}$ where p_i are odd primes, $p_i \neq p_j$ for $i \neq j$, $e \geqslant 0$ and $e_i > 0$ then to solve $x^2 = a \mod m$ it suffices to solve $x^2 = a \mod 2^e$ and $x^2 = a \mod p_i^{e_i}$ for each i. More explicitly, the reduction map

$$X_f(\mathbb{Z}/m\mathbb{Z}) \to X_f(\mathbb{Z}/2^e\mathbb{Z}) \times X_f(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times X_f(\mathbb{Z}/p^{e_\ell}\mathbb{Z}) \tag{277}$$

  is bijective with algorithmically constructible inverse.

- To solve $x^2 = a \mod 2^e$ is simple:
  - If $e = 0$ there is a unique solution $x = 0$.
  - If $e = 1$ there is a unique solution $x = 1$.
  - If $e = 2$ then there is a solution if and only if $a = 1$ in which case the solutions are $x = 1, 3$.

- If $e > 2$ then the equation has a solution if and only if $a = 1 \mod 8$ in which case there will be 4 solutions.
- Finding explicit solutions to $x^2 = a \mod 2^e$, for $e > 2$, assuming it has solutions, comes down to expression $a = (-1)^s 5^t$ and solving an equation of the form $2x = t \mod 2^{e-2}$ which can be done explicitly using the Euclidean algorithm.

- For each $p_i^{e_i}$ the following hold:
  - The map reduction map $X_f(\mathbb{Z}/p^{e_i}\mathbb{Z}) \to X_f(\mathbb{Z}/p\mathbb{Z})$ is a bijection with an explicit, algorithmically constructable inverse.
  - The equation $x^2 = a \mod p_i$ has a solution if and only if $a^{\frac{p_i-1}{2}} = 1 \mod p_i$.
  - Assuming that $x^2 = a \mod p_i$ has a solution, it suffices to find a primitive root ξ modulo p_i, expressing $a = \xi^\ell$ and solving the equation $2x = \ell \mod p_i - 1$, which can be done explicitly using the Euclidean algorithm.
  - There is an algorithm to compute a primitive root ξ modulo p_i.

To save a lot of writing, let us make the following notational definition. Let us define the function

$$S(a, b) : \mathbb{Z}^2 \to \{\pm 1\} \tag{278}$$

as follows

$$S(a, b) := \begin{cases} 1 & \text{if and } x^2 = a \mod b \text{ has a solution} \\ -1 & \text{if } x^2 = a \mod b \text{ has no solution} \end{cases} \tag{279}$$

(here one can interpret $\mathbb{Z}/b\mathbb{Z}$ as $\mathbb{Z}/|b|\mathbb{Z}$ for an arbitrary integer b). Then, the above procedure gives us a pretty thorough understanding of how to determine $S(a, b)$ algorithmically for a given fixed a and b. That said, we don't have a very good understanding of the qualitative properties of $S(a, b)$ as a function.

To see the difference, consider the following:

Example 12.1

Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) := x^6 - x^2 + x + 1$. Certainly for a given input value x we can algorithmically determine the output value $f(x)$ quite simply. But, basic qualitative properties about f are non-obvious. What are its roots? What x satisfy $f(x) > 0$? Is f surjective? Is f injective? If $|x - y| < 1$ is $|f(x) - f(y)| < 1$?

One can then think of the theory of quadratic reciprocity as a result that deduces multiple highly non-trivial qualtitative properties about the function $S(a, b)$ (correctly interpreted) and, along the way, will give us an even more efficient method to determine $S(a, b)$ algorithmically for fixed a and b.

Let us try to, briefly, indicate what sort of qualitative properties of $S(a, b)$ the theory of quadratic reciprocity addresses. There are two, and both essentially try to bridge the gap between the inputs a and b in $S(a, b)$ by providing some sort of symmetry property. Namely, let us observe that if we fix the second entry b, then describing the function $S(-, b)$ (i.e. where b is fixed but a is allowed to vary) is a finitary process since evidently it only depends on $r_b(a)$. That said, fixing a and describing the function $S(a, -)$ is certainly no longer of an, *a priori*, finitary nature.

Equivalently, we can state this problem in terms of the 'direct' versus 'indirectness' of the problem we are considering. Namely, *direct problem* of determining which $a \in \mathbb{Z}$ are squares modulo $|b|$ is a simple, finitary process (just check the finitely many entires of $\mathbb{Z}/|b|\mathbb{Z}$). But, the *indirect problem* of determining for which b is $a \in \mathbb{Z}$ a square modulo $|b|$ is certainly no longer finitary.

Example 12.2

If we fix $b = 7$ then determining which $a \in \mathbb{Z}$ are squares modulo 7 are simple: it's true if and only if $r_7(a) \in \{0, 1, 2, 4\}$. That said, if we fix $a = 15$ then determining which $b \in \mathbb{Z}$ have the property that 15 is a square modulo $|b|$ is really not obvious.

The second goal of the theory of quadratic reciprocity is then the claim that one can give a nice, succinct answer to the indirect problem of nicely, concisely describing $S(a, -)$ by turning it into a direct problem (i.e. describing $S(-, b)$ for some fixed b). Since this sounds like a symmetry property, it's not shocking that this is done by the first main goal of the theory of quadratic reciprocity, which is a symmetry property that relates (in good settings) $S(a, b)$ and $S(b, a)$ directly. Moreover, as it will turn out, the first and second goals, *a priori* distinct symmetry properties of $S(a, b)$, are equivalent.

One should consider these theorems not only beautiful, but also deep and perplexing. One fundamentally does *not* expect there to be a direct relationship between, for example, $S(p, q)$ and $S(q, p)$ for distinct primes p and q. Indeed, one of the founding tenets of our understanding of Theorem 7.2 was that solving equations modulo p and solving equations modulo q were unconnected. But, a statement that there is a straightforward relationship between $S(p, q)$ and $S(q, p)$ says that the equation $x^2 = p \mod q$ and $x^2 = q \mod p$ are, in fact, intimately related.

In fact, the apparent depth of quadratic reciprocity is not misleading, and lies at the tip of a proverbial iceberg concerning unexpected and shocking relationships where there shouldn't be any. This is an area of math called the *Langlands program*, and is an area of active, and deep research.

12.2 Quadratic reciprocity: the statement

Our goal today is to understand the statement of quadratic reciprocity in its most nascent, stripped-down form. To do this, it will be helpful to make the following bit of notation:

Definition 12.1

Let p be an odd prime number. Define the *Legendre symbol* as the function $\mathbb{Z} \to \{-1, 0, 1\}$ defined as follows:

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a, \text{ and } x^2 = a \mod p \text{ has a solution} \\ -1 & \text{if } p \nmid a, \text{ and } x^2 = a \mod p \text{ has no solution} \end{cases} \tag{280}$$

One can see that our definition of $\left(\frac{a}{p}\right)$ is almost $S(a, p)$ with the distinct difference that if $p \mid a$ then $S(a, p) = 1$ but $\left(\frac{a}{p}\right) = 0$. The need for this distinction, and the reason for excluding the case $p = 2$, will be clear soon.

Example 12.3

One can easily check that $\left(\frac{-1}{7}\right) = -1$ and $\left(\frac{2}{7}\right) = 1$.

One can verify that the Legendre symbol satisfies the following basic properties:

Lemma 12.1

Let p be a fixed odd prime and let a and b be elements of $\mathbb{Z}$. Then, the following properties hold:

1. If $a = b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. One has that $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$.
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
4. If $a \in \Phi(p)$ then $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$.
5. $1 + \left(\frac{a}{p}\right) = \#X_f(\mathbb{Z}/p\mathbb{Z})$ where $f(x) := x^2 - a$.

Proof 12.1

1. This is obvious.
2. If $a = 0 \mod p$ this is clear, so suppose that $\gcd(a, p) = 1$. Note that $a^{\frac{p-1}{2}} = \pm 1 \mod p$. Indeed, by Exercise 4.2 it suffices to show that $(a^{\frac{p-1}{2}})^2 = 1 \mod p$, but this is immediate from Corollary 5.5. To see then that $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$ it suffices to show that $a^{\frac{p-1}{2}} = 1$ if and only if $x^2 = a \mod p$ has a solution. But, this follows immediately from Theorem 6.3.
3. Note that since $p > 2$ one has that $1 \neq -1 \mod p$. Thus, it suffices to show that
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p \tag{281}$$
But, by 2. this is equivalent to showing that $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \mod p$, but this is obvious.
4. Note that by 3. we have that $\left(\frac{a}{p}\right)\left(\frac{a^{-1}}{p}\right) = \left(\frac{aa^{-1}}{p}\right) = \left(\frac{1}{p}\right) = 1$. The second equality follows from the fact that $1^{-1} = 1$ and $(-1)^{-1} = -1$.
5. See Exercise 12.2.

From Lemma 12.1 4. we see that, in some ways, $\left(\frac{a}{p}\right)$ is preferable to $S(a, p)$ since the former knows the size of $X_f(\mathbb{Z}/p\mathbb{Z})$ whereas the latter can only tell whether or not $X_f(\mathbb{Z}/p\mathbb{Z})$ is empty. Also, because of Lemma 12.1 1. we will often think of $\left(\frac{-}{p}\right)$ as a function $\mathbb{Z}/p\mathbb{Z} \to \{-1, 0, 1\}$ and using 2. and 3. we will furthermore often times restrict ourselves to thinking of $\left(\frac{-}{p}\right)$ as a multiplicative function $\Phi(p) \to \{\pm 1\}$.

One non-obvious result of Lemma 12.1 1. (which we really could have proven after knowing Theorem 6.3) is the following:

Corollary 12.1

Let p be an odd prime and let a and b be elements of $\Phi(p)$. Then, the following holds:

1. If $x^2 = a \mod p$ and $x^2 = b \mod p$ has a solution, then $x^2 = ab \mod p$ has a solution.
2. If $x^2 = a \mod p$ has a solution and $x^2 = b \mod p$ has no solution, then $x^2 = ab \mod p$ has no solution.
3. If $x^2 = a \mod p$ and $x^2 = b \mod p$ both have no solution, then $x^2 = ab \mod p$ does have a solution.

We also obtain the following quantitative result on the frequency that $x^2 = a \mod p$ has a solution:

Corollary 12.2

Let p be an odd prime. Then, the number of $a \in \Phi(p)$ such that $x^2 = a \mod p$ has a solution is $\frac{p-1}{2}$. Consequenly, the number of $a \in \Phi(p)$ such that $x^2 = a \mod p$ has no solution is $\frac{p-1}{2}$.

Proof 12.2

We can write

$$\Phi(p) := \underbrace{\left\{a \in \Phi(p) : \left(\frac{a}{p}\right) = 1\right\}}_{X_1} \sqcup \underbrace{\left\{a \in \Phi(p) : \left(\frac{a}{p}\right) = -1\right\}}_{X_2} \tag{282}$$

Assume that $a_0 \in \Phi(p)$ is such that $\left(\frac{a_0}{p}\right) = -1$. Then, we claim the map $a \mapsto aa_0$ is a bijection $X_1 \to X_2$. But, it's clear that this mapping does, in fact, send X_1 into X_2 (this follows from Corollary 12.1), and the map $X_2 \to X_1$ given by $a \mapsto aa_0^{-1}$ is its inverse.

Thus, it suffices to show that there is at least one element a_0 of $\Phi(p)$ such that $x^2 = a_0 \mod p$ has no solution. But, take $a_0 = \xi$ where ξ is a primitive root modulo p. Note then that if $x^2 = \xi \mod p$ had a solution, call it x_0, then

$$p - 1 = |\xi| = |x_0^2| = \frac{|x_0|}{\gcd(2, |x_0|)} \tag{283}$$

by Exercise 6.3. Thus, $(p-1)\gcd(2, |x_0|) = |x_0|$. Since Corollary 5.3 implies that $|x_0| \mid p-1$ this implies that $\gcd(2, |x_0|) = 1$ so that $|x_0|$ is odd. But, $p - 1 \mid |x_0|$ and $p - 1$ is even. This is a contradiction.

Remark 12.1

Note that while Corollary 12.2 says that half the elements of $\Phi(p)$ are squares, it does not say that they are distributed in any uniform way. For example, nothing so naive as 'if $\left(\frac{a}{p}\right) = 1$ then $\left(\frac{a+1}{p}\right) = -1$' can work. All Corollary 12.2 shows is that the non-squares and the squares are connected by multiplication by a non-square. This distribution can be quite strange in practice.

Now, as we remarked in the setup, the main goal of quadratic reciprocity is to give, in good cases, a symmetry relationship for the function $S(a, b)$ (i.e. explicitly relate $S(a, b)$ and $S(b, a)$). The classical statement of quadratic reciprocity does just this, at least when a and b are distinct odd primes. We state this result here now:

Theorem 12.1: Quadratic reciprocity I

Let p and q be distinct odd primes. Then,

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) \tag{284}$$

We can rephrase this in another, equivalent, way using the fact that $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ is a pretty easy function to suss out:

Theorem 12.2: Quadratic reciprocity II

Let p and q be distinct odd primes. Then:

1. If $p = 1 \mod 4$ or $q = 1 \mod 4$ then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
2. If $p = q = 3 \mod 4$ then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Which gives an astoundingly simple symmetry relation for the function $S(a, b)$ (at least when a and b are distinct odd primes)! As we said before, *a priori*, the equations $x^2 = p \mod q$ and $x^2 = q \mod p$ should be totally unconnected, but Theorem 12.2 says this couldn't be further from the truth.

Let us finally say what the above says in words to really hammer the point in:

Theorem 12.3: Quadratic Reciprocity III

Let p and q be distinct odd primes. Then:

1. If $p = 1 \mod 4$ or $q = 1 \mod 4$ then $x^2 = q \mod p$ has a solution if and only if $x^2 = p \mod q$ has a solution.
2. If $p = q = 3 \mod 4$ then $x^2 = q \mod p$ has a solution if and only if $x^2 = p \mod q$ does not have a solution.

Not only does this give one a startlingly simple relationship between the equations $x^2 = p \mod q$ and $x^2 = q \mod p$, but it also gives us an incredibly powerful computational tool to check squareness of a number mod a given prime. Let us illustrate this:

Example 12.4

Is 7 a square in $\mathbb{Z}/101\mathbb{Z}$? Well, before Theorem 12.3 we would need to compute $7^{50} \mod 101$. Of cousre, we can do this iteratively, and it's not horrific. But, using Theorem 12.3 since $101 = 1 \mod 4$ whether 7 is a square modulo 101 is equivalent to whether 101 is a square modulo 7. But, this only depends on $r_7(101) = 3$. Now, one can quickly check that 3 is not a square modulo 7, and thus 7 is not a square modulo 101.

It also gives us our first real tool to trying to understand indirect problems. For example:

Example 12.5

Let us decide for which primes p is 3 is square modulo p. Well, it's evidently a square modulo 2 and 3, so we can assume that p is an odd prime distinct from 3. We now are stuck in two cases. Either $p = 1 \mod 4$, in which case $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ or $p = 3 \mod 4$ in which case $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$. Let's first assume that $p = 1 \mod 4$. Then, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ and the only squares modulo 3 are are $0, 1$ and since $p \neq 3$ this implies that $p = 1 \mod 3$. If $p = 3 \mod 4$ then $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ and so $\left(\frac{3}{p}\right) = 1$ if and only if $r_3(p)$ is not a square. Since $p \neq 3$, so that $r_3(p) \neq 0$, this happens if and only if $p = 2 \mod 3$. Thus, we see that 3 is a square modulo p if and only if $p = 1 \mod 4$ and $p = 1 \mod 3$ or $p = 3 \mod 4$ and $p = 2 \mod 3$. Using Corollary 7.1 this is equivalent to $p = 1, 5 \mod 12$.

So, for example, one can quickly check that $103 = 7 \mod 12$ and thus 3 is not a square modulo 103.

Now, note that for any $0 \neq x \in \mathbb{Z}$ we can try to compute $\left(\frac{x}{p}\right)$, $p \nmid x$, using Lemma 12.1 3. to write

$$\left(\frac{x}{p}\right) = \left(\frac{-1}{p}\right)^{v_{\text{sgn}}(x)} \left(\frac{2}{p}\right)^{v_2(x)} \prod_{q \text{ odd}} \left(\frac{p}{q}\right)^{v_q(x)} \tag{285}$$

or, since the Legendre symbol is only ever ± 1, writing it as

$$\left(\frac{x}{p}\right) = \left(\frac{-1}{p}\right)^{v_{\text{sgn}}(x)} \left(\frac{2}{p}\right)^{v_2(x) \mod 2} \prod_{q \text{ odd}} \left(\frac{p}{q}\right)^{v_q(x) \mod 2} \tag{286}$$

Now, for q odd we can use Theorem 12.1 (or any of its equivalent forms) to understand $\left(\frac{p}{q}\right)$. Thus, to get a rounded picture of $\left(\frac{x}{p}\right)$ from the perspective of quadratic reciprocity, we'd like to understand the terms $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ which are handled as separate cases:

Theorem 12.4: Quadratic reciprocity (supplemental law 1)

Let p be an odd prime. Then,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 1 \mod 4 \\ -1 & \text{if otherwise} \end{cases} \tag{287}$$

Theorem 12.5: Quadratic reciprocity (supplemental law 2)

Let p be an odd prime. Then,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if} \quad p = \pm 1 \mod 8 \\ -1 & \text{if} \quad \text{otherwise} \end{cases} \tag{288}$$

The first of these, Theorem 12.4, is much simpler than the other cases of quadratic reciprocity. In fact, we have already proven it in Corollary 5.9. The others will be considerably, considerably harder to prove.

Let us put the above ideas to use:

Example 12.6

Let's determine if -6860 is a square modulo 7001. One can factor $-6860 = (-1)^1 \cdot 2^2 \cdot 5 \cdot 7^3$. Thus, we deduce that

$$\left(\frac{-6860}{7001}\right) = \left(\frac{-1}{7001}\right)\left(\frac{5}{7001}\right)\left(\frac{7}{7001}\right) \tag{289}$$

Now, since $7001 = 1 \mod 4$ we know that $\left(\frac{-1}{7001}\right) = 1$. Moreover, by Theorem 12.2 we know that

$$\left(\frac{5}{7001}\right) = \left(\frac{7001}{5}\right) = \left(\frac{1}{5}\right) = 1 \tag{290}$$

and

$$\left(\frac{7}{7001}\right) = \left(\frac{7001}{7}\right) = \left(\frac{1}{7}\right) = 1 \tag{291}$$

Thus, we deduce that $\left(\frac{-6860}{7001}\right) = 1$ and so -6860 is a square modulo 7001.

Example 12.7

Let's figure out for what primes p is -15 a square modulo p. If $p = 3$ or $p = 5$ then clearly -15 is a square modulo p, so let us assume that $p > 7$. We are then trying to compute when $\left(\frac{-15}{p}\right) = 1$. Now, we clearly have the equality

$$\left(\frac{-15}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) \tag{292}$$

We know what $\left(\frac{-1}{p}\right)$ is by Theorem 12.4 and we already determined what $\left(\frac{3}{p}\right)$ is in Example 12.5. Let us now compute $\left(\frac{5}{p}\right)$.

Since $5 = 1 \mod 4$ we know that, at least for p and odd prime different than 5, we have that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Moreover, the only squares modulo 5 are $1, 4$. Thus, we see that $\left(\frac{5}{p}\right) = 1$ if and only if $p = 1, 4 \mod 5$. So, now, to compute when $\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = 1$ we see we have to break it into the cases when $\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = -1$. This breaks into a bunch of congruences on p modulo 12 and 5 and, if one does it out, one finds that $\left(\frac{15}{p}\right) = 1$ if and only if $p = 1, 11, 49, 59, 17, 7, 53, 43$

mod 60. To see when $\left(\frac{-15}{p}\right) = 1$ we need to compute the case when $\left(\frac{-1}{p}\right) = \left(\frac{15}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = \left(\frac{15}{p}\right) = -1$. These come down to congruences on p modulo 4 and p modulo 60 which, really, just come down to congruences on p modulo 60. Checking these one finds that $\left(\frac{-15}{p}\right) = 1$ if and only if $p = 1, 49, 17, 53, 19, 23, 31, 47$.

We end this section with an observation of a superficial, but useful, improvement one can make to Theorem 12.1 using Theorem 12.4:

Theorem 12.6

Let p and q be distinct odd primes. Define $q^* := (-1)^{\frac{q-1}{2}} q$. Then,

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) \tag{293}$$

Proof 12.3

We merely note that

$$\begin{aligned}\left(\frac{q^*}{p}\right) &= \left(\frac{(-1)^{\frac{q-1}{2}} p}{p}\right) \\ &= \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \\ &= \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)\end{aligned} \tag{294}$$

12.3 Proof of the second supplementary law

We will give the proof of Theorem 12.1 next time, but this time we explain the proof to Theorem 12.5. As will be the case for all the proofs of quadratic reciprocity, things will seem quite random. The 'correct' proofs of all of these results use machinery that is well-beyond our course and so, consequently, the proofs we can give here are somewhat ad hoc in nature. We hope the reader will forgive us for this:

Proof 12.4: Theorem 12.5

Let us begin by observing that

$$\begin{aligned}2 \cdot 4 \cdot 6 \cdots p-1 &= 2^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)\right) \\ &= \left(\frac{2}{p}\right) \left(\frac{p-1}{2}\right)! \mod p\end{aligned} \tag{295}$$

On the other hand, we can write

$$2 \cdot 4 \cdot 6 \cdots (p-1) = (-1)^u 2 \cdot 4 \cdot 6 \cdots \left(\frac{p-1}{2}\right)\left(p - \left(\frac{p-1}{2}+2\right)\right) \cdots (p-(p-1)) \mod p \tag{296}$$

where, here, we have defined

$$u := \# \left\{ x \in \mathbb{Z} : \frac{p-1}{2} + 2 \leqslant x \leqslant p-1 \text{ and } x \text{ is even} \right\} \tag{297}$$

Note though that as x travels from $\frac{p-1}{2}+2$ to $p-1$, with x even, the values $p-x$ travel along the odd integers from $\frac{p-1}{2}-1$ down to 1. Thus, we see that

$$2 \cdot 4 \cdot 6 \cdots \left(\frac{p-1}{2}\right)\left(p - \left(\frac{p-1}{2}+1\right)\right) \cdots (p-(p-1)) = \left(\frac{p-1}{2}\right)! \tag{298}$$

Thus, comparing (295) and (296) we deduce that

$$\left(\frac{2}{p}\right) = (-1)^u \mod p \tag{299}$$

which, since $p > 2$ implies that $\left(\frac{2}{p}\right) = (-1)^u$. Thus, it suffices to show that

$$(-1)^u = \begin{cases} 1 & \text{if } p = \pm 1 \mod 8 \\ -1 & \text{if otherwise} \end{cases} \tag{300}$$

But, this is easy and left to the reader (just consider the different classes of p modulo 8).

12.4 Exercises

Exercise 12.1

Problem: Determine for which primes p is 35 a square modulo p.
Solution: Just as before, excluding $p = 5$ and $p = 7$, for which 35 is obviously a square modulo such p, we need to determine for what p is $\left(\frac{35}{p}\right) = 1$. Now, we know that for $p \neq 5$ an odd prime that

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p = 1, 4 \mod 5 \\ -1 & \text{if } p = 2, 3 \mod 5 \end{cases} \tag{301}$$

from Example 12.7. So, it remains to determine $\left(\frac{7}{p}\right)$ when $p \neq 7$ is an odd prime. Note that since 7 is 3 modulo 4, we need to break this into two cases. If $p = 1 \mod 4$ then

$$\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = \begin{cases} 1 & \text{if } p = 1, 2, 4 \mod 7 \\ -1 & \text{if } p = 3, 5, 6 \mod 7 \end{cases} \tag{302}$$

If $p = 3 \mod 4$ then

$$\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = \begin{cases} 1 & \text{if } p = 3, 5, 6 \mod 7 \\ -1 & \text{if } p = 1, 2, 4 \mod 7 \end{cases} \tag{303}$$

So, we know that $\left(\frac{35}{p}\right) = 1$ if and only if $\left(\frac{5}{p}\right) = \left(\frac{7}{p}\right)$. If $p = 1 \mod 4$ this happens $p = 1, 4 \mod 5$ and $p = 1, 2, 4 \mod 7$. One can use Theorem 7.1 to turn this into the equalities $p = 1, 121, 81, 29, 9, 109$ mod 140. If $p = 3 \mod 4$ this happens when $p = 2, 3 \mod 5$ and $p = 3, 5, 6 \mod 7$. This happens when $p = 3, 103, 83, 87, 27, 47 \mod 140$. Thus, in conclusion we see that 35 is a square modulo p if and only if $p = 3$, $p = 5$, or $p = 1, 3, 9, 27, 29, 47, 81, 83, 87, 103, 109, 121 \mod 140$.

Exercise 12.2

Problem: Prove Lemma 12.1 part 5.

Solution: One can think about this from a case by case analysis. If $a = 0 \mod p$ then $1 + \left(\frac{a}{p}\right) = 1$ and $X_f(\mathbb{Z}/p\mathbb{Z}) = \{0\}$ so the claim is clear there. If $a \neq 0 \mod p$ but $x^2 = a \mod p$ has a solution, then it will have precisely two: a and $-a$ (which are distinct since $p > 2$). But, then $1 + \left(\frac{a}{p}\right) = 1 + 1 = 2$. So the claim is proven in this case. Finally, if $a \neq 0 \mod p$ but $x^2 = a \mod p$ has no solutions, then $\#X_f(\mathbb{Z}/p\mathbb{Z}) = 0$. But, $1 + \left(\frac{a}{p}\right) = 1 + (-1) = 0$. Thus, the claim follows.

Exercise 12.3

Problem: Using Algorithm 11.1, give a second proof to the fact (used in Corollary 12.2) that if ξ is a primitive root modulo p then $x^2 = \xi \mod p$ has no solution.

Solution: Using Algorithm 11.1 we see that solving $x^2 = \xi \mod p$ is equivalent to solving the equation $2x = 1 \mod p - 1$. But, this is impossible since $p - 1$ is even (since $p > 2$) and thus $2 \notin \Phi(p)$.

13 Lecture 13: Quadratic reciprocity II: A proof

13.1 Setup

Today we will give a proof of Theorem 12.1. As mentioned last time the 'correct' proof of Theorem 12.1 is well beyond the scope of the course, and so essentially all proofs we are able to do are of a somewhat unmotivated, ad hoc nature. The reason that I have chosen the proof that I have, amongst the multitude of other proofs, is the fact that it contains a valuable philosophical technique present in many other areas of mathematics, as well as necessitates developing some basic machinery to count solutions to modulus Diophantine equations.

This valuable technique is the idea that if one wants to study a set with minimal structure, to try and replace it with a larger set with more structure for which you can, by some sort of specialization, return to the original set. This is a bit cryptic, so let's talk it through here. Note that if we are trying to study $\left(\frac{q}{p}\right)$ what we are really doing is trying to study $X_f(\mathbb{Z}/p\mathbb{Z})$ where $f(x) = qx^2 - 1$. Indeed, note that $\#X_f(\mathbb{Z}/p\mathbb{Z})$ is, by Lemma 12.1, just $1 + \left(\frac{q^{-1}}{p}\right)$. But, $\left(\frac{q^{-1}}{p}\right) = \left(\frac{q}{p}\right)$. Thus, $X_f(\mathbb{Z}/p\mathbb{Z})$, in its size, really does capture

$\left(\frac{q}{p}\right)$. But, the set $X_f(\mathbb{Z}/p\mathbb{Z})$ has no really structure to exploit—there's really nothing to manipulate to try to massage $\left(\frac{q}{p}\right)$ into our desired $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$.

Thus, we would like to replace $X_f(\mathbb{Z}/p\mathbb{Z})$ by a more structured object, but one for which we really can recover $X_f(\mathbb{Z}/p\mathbb{Z})$ from. the idea is as follows. For all $n \geqslant 1$, let us set

$$f_n(x_1, \ldots, x_n) := x_1^2 + \cdots + x_n^2 - 1 \tag{304}$$

and let us shorten $X_{f_n}(\mathbb{Z}/p\mathbb{Z})$ to $X_n(\mathbb{Z}/p\mathbb{Z})$. Note that, in some sense, $X_h(\mathbb{Z}/p\mathbb{Z})$ is some sort of 'unit $(n-1)$-sphere' in $\mathbb{Z}/p\mathbb{Z}$.

We are going to be interested in the case of $n = q$ and so, in particular, on the set $X_q(\mathbb{Z}/p\mathbb{Z})$. The reason that one might expect $X_q(\mathbb{Z}/p\mathbb{Z})$ as a natural way to 'enlarge' $X_f(\mathbb{Z}/p\mathbb{Z})$ is to think of $f(x)$ as

$$f(x) = \underbrace{x^2 + \cdots + x^2}_{q \text{ times}} - 1 \tag{305}$$

so that, in particular, we see that

$$f(x) = f_q(x, \ldots, x) \tag{306}$$

thus, $X_q(\mathbb{Z}/p\mathbb{Z})$ is a lot like $X_f(\mathbb{Z}/p\mathbb{Z})$ but we've given the variables a bit more freedom.

Let us also note that (as promised), unlike $X_f(\mathbb{Z}/p\mathbb{Z})$, that $X_q(\mathbb{Z}/p\mathbb{Z})$ has some interesting, non-trivial structure. Namely, For $i = 1, \ldots, q-1$ let us define a symmetry of $X_q(\mathbb{Z}/p\mathbb{Z})$ as follows. The s_i will be a bijection

$$s_i : X_q(\mathbb{Z}/p\mathbb{Z}) \to X_q(\mathbb{Z}/p\mathbb{Z}) \tag{307}$$

given as follows:

$$s_i(a_1, \ldots, a_q) := (a_{q-i+1}, a_{q-i+2}, \ldots, a_1, \ldots, a_{q-i}) \tag{308}$$

or, in other words, s_i shifts the entries of a tuple $(a_1, \ldots, a_q) \in X_q(\mathbb{Z}/p\mathbb{Z})$ forward by i. So, for example,

$$s_1(a_1, \ldots, a_q) = (a_q, a_1, \ldots, a_{q-1}) \tag{309}$$

We extend the notation to $i = 0$ by declaring that s_0 is the identity map on $X_q(\mathbb{Z}/p\mathbb{Z})$.

We make the following elementary observations about these symmetries as follows:

Lemma 13.1

Let $i, j \in \{0, \ldots, p-1\}$. Then, the function $s_i \circ s_j : X_q(\mathbb{Z}/p\mathbb{Z}) \to X_q(\mathbb{Z}/p\mathbb{Z})$ is just the function $s_{r_q(i+j)}$.

In particular, let us write $s := s_1$ and for any $i \in \mathbb{Z}$ let us write

$$s^i := \begin{cases} \underbrace{s \circ \cdots \circ s}_{i \text{ times}} & \text{if} \quad i \geqslant 0 \\ \underbrace{s^{-1} \circ \cdots \circ s^{-1}}_{|i| \text{ times}} & \text{if} \quad i < 0 \end{cases} \tag{310}$$

Then, what Lemma 13.1 tells us is that for $i \in \{0, \ldots, q-1\}$ one has that $s^i = s_i$ and, more generally, for any $i \in \mathbb{Z}$ we have that $s^i = s_{r_q(i)}$. Thus, while it appears that we have written down $q-1$ non-trivial symmetry operators $s_1, \ldots, s_{q-1}$ of $X_q(\mathbb{Z}/p\mathbb{Z})$, the only one that really matters is $s = s_1$ since it 'generates' the rest of the symmetries.

So then, our goal is to replace studying the unstructured set $X_f(\mathbb{Z}/p\mathbb{Z})$ with the structured object $(X_q(\mathbb{Z}/p\mathbb{Z}), s)$ (i.e. the set $X_q(\mathbb{Z}/p\mathbb{Z})$ together with the structure of the symmetry operator s). Now, intuitively it's clear what $X_f(\mathbb{Z}/p\mathbb{Z})$ has to do with $X_q(\mathbb{Z}/p\mathbb{Z})$ (e.g. from (306)) but the symmetry operator also brings this more into focus. Namely, let us call $(a_1, \ldots, a_q) \in X_q(\mathbb{Z}/p\mathbb{Z})$ a *fixed point* of s if $s(a_1, \ldots, a_q) = (a_1, \ldots, a_q)$. Let us denote the set of fixed points by $\mathrm{Fix}(s)$.

We then have the following powerful observation.

Lemma 13.2

There is a bijection $X_f(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{Fix}(s)$.

Proof 13.1

Let $\mathbf{a} = (a_1, \ldots, a_q) \in X_q(\mathbb{Z}/p\mathbb{Z})$. Then, $\mathbf{a} \in \mathrm{Fix}(s)$ if and only if $s(\mathbf{a}) = \mathbf{a}$. But, note then that

$$s_2(\mathbf{a}) = s^2(\mathbf{a}) = s(s(\mathbf{a})) = s(\mathbf{a}) = \mathbf{a} \tag{311}$$

and, more generally, we see that $s_i(\mathbf{a}) = \mathbf{a}$ for all $i = 1, \ldots, p-1$. It's pretty easy then to see, that since shifting leaves the tuple $\mathbf{a}$ unchanged, that $a_1 = \cdots = a_q$. Call this common value a. Thus, since $\mathbf{a} \in X_q(\mathbb{Z}/p\mathbb{Z})$ we see that

$$f_q(\mathbf{a}) = f_q(a, \ldots, a) = f(a) \tag{312}$$

and so $a \in X_f(\mathbb{Z}/p\mathbb{Z})$. Conversely, it's clear that if one starts with $a \in X_f(\mathbb{Z}/p\mathbb{Z})$ then $(a, \ldots, a) \in \mathrm{Fix}(s)$. The claim follows.

So, we see that not only is $(X_q(\mathbb{Z}/p\mathbb{Z}), s)$ a structured object (it's not just a set, but a set with the extra structure of a symmetry) we can naturally recover the set of actual interest $X_f(\mathbb{Z}/p\mathbb{Z})$ from this structured object. The proof of Theorem 12.1 will then, roughly, to exploit the extra structure of $(X_q(\mathbb{Z}/p\mathbb{Z}), s)$ and the relationship to $X_f(\mathbb{Z}/p\mathbb{Z})$.

13.2 The proof

We now begin the proof in of Theorem 12.1 in earnest. The first step will be to have a better understanding on the non-fixed points of $X_q(\mathbb{Z}/p\mathbb{Z})$:

Lemma 13.3

Let $\mathbf{a} \in X_q(\mathbb{Z}/p\mathbb{Z})$. Then, the following are equivalent:

1. $\mathbf{a} \notin \mathrm{Fix}(s)$.
2. For all $i, j \in \{0, \ldots, q-1\}$ we have that $s_i(\mathbf{a}) \neq s_j(\mathbf{a})$.

Proof 13.2

It's clear that 2. implies 1. by taking $i = 1$ and $j = 0$. To see that 1. implies 2. suppose that

$$s^i(\mathbf{a}) = s_i(\mathbf{a}) = s_j(\mathbf{a}) = s^j(\mathbf{a}) \tag{313}$$

with $i \geqslant j$. Then, by applying s^{-j} to both sides we see that $s^{i-j}(\mathbf{a}) = \mathbf{a}$. Note then that by induction for all $k \geqslant 1$ we have that

$$(s^{i-j})^k(\mathbf{a}) = \mathbf{a} \tag{314}$$

So, for all $n \geqslant 1$, taking $k = (i-j)^{n-1}$ shows that

$$s^{(i-j)^n}(\mathbf{a}) = \mathbf{a} \tag{315}$$

But, recall that

$$s^{(i-j)^n} = s^{(i-j)^n \mod q} \tag{316}$$

In particular, taking $n = |i-j|$, where $i-j$ is thought of as an element of $\Phi(q)$, shows that

$$\mathbf{a} = s^{(i-j)^n}(\mathbf{a}) = s^{(i-j)^n \mod q}(\mathbf{a}) = s^1(\mathbf{a}) = s(\mathbf{a}) \tag{317}$$

so that $\mathbf{a} \in \mathrm{Fix}(\mathbf{a})$, which is a contradiction.

From this, we deduce the following pivotal corollary:

Corollary 13.1

The following equality holds:

$$1 + \left(\frac{q}{p}\right) = \#X_q(\mathbb{Z}/p\mathbb{Z}) \mod q \tag{318}$$

Proof 13.3

Indeed, note that we have an obvious decomposition

$$X_q(\mathbb{Z}/p\mathbb{Z}) = \mathrm{Fix}(s) \sqcup \underbrace{\{\mathbf{a} \in X_q(\mathbb{Z}/p\mathbb{Z}) : x \notin \mathrm{Fix}(s)\}}_{Y} \tag{319}$$

and so

$$\#X_q(\mathbb{Z}/p\mathbb{Z}) = \#\mathrm{Fix}(s) + \#Y \tag{320}$$

Now, by Lemma 13.2 we know that

$$\#\mathrm{Fix}(s) = \#X_f(\mathbb{Z}/p\mathbb{Z}) = 1 + \left(\frac{q}{p}\right) \tag{321}$$

But, by Lemma 13.3 we know that elements of Y come in groups of q. Indeed, if $\mathbf{a} \in Y$ then by Lemma 13.3 we know that $\mathbf{a}, s(\mathbf{a}), \ldots, s^{q-1}(\mathbf{a})$ are q distinct elements of Y. Moreover, two such groups of q-elements can't intersect since if $s^i(\mathbf{a}) = s^j(\mathbf{b})$ with $j \geqslant i$ then $\mathbf{a} = s^{j-i}(\mathbf{b})$ so that $s^i(\mathbf{a})$ is, in fact, in the packet of q elements obtained from $\mathbf{b}$. Thus, we can parse Y up evenly into packets of q elements which says, indeed, that $q \mid \#Y$. So, applying (320) and (321) together gives the desired result.

The idea now is to compute, by hand, the size $\#X_q(\mathbb{Z}/p\mathbb{Z})$. In fact, we will show the following:

Theorem 13.1

Let $n = 2k+1$. Then,

$$\#X_n(\mathbb{Z}/p\mathbb{Z}) = p^{2k} + (-1)^{\frac{k(p-1)}{2}} p^k \tag{322}$$

And, together with Corollary 13.1 this proves Theorem 12.1:

Proof 13.4: Theorem 12.1

Note that by applying Corollary 13.1 with Theorem 13.1 with $n = q$, so that $k = \frac{q-1}{2}$, we have that

$$1 + \left(\frac{q}{p}\right) = p^{q-1} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} \mod q \tag{323}$$

But, by Corollary 5.5 and Lemma 12.1 we know that $p^{q-1} = 1 \mod q$ and $p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right) \mod q$. Thus, we deduce that

$$1 + \left(\frac{q}{p}\right) = 1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \mod q \tag{324}$$

and so

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \mod q \tag{325}$$

which, since $q > 2$ and both sides are ± 1, implies that

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \tag{326}$$

as desired.

Thus, it remains to prove Theorem 13.1, which we shall do by induction. But, first, we need the following lemma involving sums of Legendre symbols:

Lemma 13.4

Let $a \in \mathbb{Z}/p\mathbb{Z}$. Then,

$$\sum_{y=1}^{p} \left(\frac{y^2 + a}{p}\right) = \begin{cases} -1 & \text{if} \quad a \neq 0 \\ p-1 & \text{if} \quad a = 0 \end{cases} \tag{327}$$

Proof 13.5

Assume first that $a = 0$. Then, evidently for all $y \in \{1, \ldots, p-1\}$ we have that $\left(\frac{y^2}{p}\right) = 1$ and since $\left(\frac{0^2}{p}\right) = 0$ we deduce that

$$\sum_{y=1}^{p} \left(\frac{y^2}{p}\right) = p - 1 \tag{328}$$

as desired. So, let us assume that $a \neq 0$. Let us then note that the sum

$$\sum_{y=1}^{p} \left(\frac{y^2 + a}{p}\right) \tag{329}$$

is heavily related to $\#X_g(\mathbb{Z}/p\mathbb{Z})$ where $g(x, y) := x^2 - y^2 - a$. Indeed, for each fixed $y \in \mathbb{Z}/p\mathbb{Z}$ we see that the size of $X_g(\mathbb{Z}/p\mathbb{Z})$ is precisely $1 + \left(\frac{y^2 + a}{p}\right)$. Thus, the total size $\#X_g(\mathbb{Z}/p\mathbb{Z})$ is precisely the

resul of varying these quantities over all $y \in Z/p\mathbb{Z}$. In other words, we see that

$$\#X_g(\mathbb{Z}/p\mathbb{Z}) = \sum_{y=1}^{p} \left(1 + \left(\frac{y^2+a}{p}\right)\right) = p + \sum_{y=1}^{p} \left(\frac{y^2+a}{p}\right) \tag{330}$$

But, we can compute $\#X_g(\mathbb{Z}/p\mathbb{Z})$ by hand. Namely, we can rewrite $g(x,y) = 0$ as $x^2 - y^2 = a$. This is equivalent to $(x-y)(x+y) = a$. But, setting $x - a = s$ and $x + y = t$ this is equivalent to $st = a$. Note then that the solutions to this are precisely $s = u$ and $t = u^{-1}a$ where u is an element of $\Phi(p)$. Thus, there are $p-1$ solutions, and so $\#X_g(\mathbb{Z}/p\mathbb{Z}) = p - 1$. Combining this with (330) gives that $\sum_{y=1}^{p} \left(\frac{y^2+a}{p}\right) = -1$ as desired.

Proof 13.6: Theorem 13.1

We prove this by induction on k. When, $k = 0$ we see that we need to show

$$\#X_1(\mathbb{Z}/p\mathbb{Z}) = p^{2\cdot 0} + (-1)^{\frac{0\cdot(p-1)}{2}} p^0 = 1 + 1 = 2 \tag{331}$$

But $f_1(x) = x^2 - 1$ and so from Exercise 4.2, we know that $\#X_1(\mathbb{Z}/p\mathbb{Z}) = 2$ as desired.

To handle the induction step we show that for $n > 2$ we have that

$$\#X_n(\mathbb{Z}/p\mathbb{Z}) = p^{n-1} + \left(\frac{-1}{p}\right)\left[p\#X_{n-2}(\mathbb{Z}/p\mathbb{Z}) - p^{n-2}\right] \tag{332}$$

Indeed, we note that we can rewrite the equation $f_n(x_1, \ldots, x_n) = 0$ as the equation

$$x_n^2 = 1 - (x_1^2 + \cdots + x_{n-1}^2) \tag{333}$$

Now, for each fixed choice of $x_1, \ldots, x_{n-1}$ in $\mathbb{Z}/p\mathbb{Z}$ we see that this equation has precisely $1 + \left(\frac{1-(x_1^2+\cdots+x_{n-1}^2)}{p}\right)$ solutions. So, we deduce that

$$\begin{aligned}
\#X_n(\mathbb{Z}/p\mathbb{Z}) &= \sum_{x_1,\ldots,x_{n-1}=1}^{p} \left(1 + \left(\frac{1-(x_1^2+\cdots+x_{n-1}^2)}{p}\right)\right) \\
&= p^{n-1} + \sum_{x_1,\ldots,x_n=1}^{p} \left(\frac{1-(x_1^2+\cdots+x_{n-1}^2)}{p}\right) \\
&= p^{n-1} + \sum_{x_{n-1}=1}^{p} \cdots \sum_{x_1=1}^{p} \left(\frac{1-(x_1^2+\cdots+x_n^2)}{p}\right) \\
&= p^{n-1} + \sum_{x_{n-1}=1}^{p} \cdots \sum_{x_1=1}^{p} \left(\frac{-1}{p}\right)\left(\frac{x_1^2+\cdots+x_{n-1}^2-1}{p}\right) \\
&= p^{n-1} + \left(\frac{-1}{p}\right) \sum_{x_{n-1}=1}^{p} \cdots \sum_{x_1=1}^{p} \left(\frac{x_1^2+\cdots+x_{n-1}^2-1}{p}\right)
\end{aligned} \tag{334}$$

Now, by Lemma 13.4 the innermost sum can be evaluated as follows:

$$\begin{aligned}\sum_{x_1=1}^{p}\left(\frac{x_1^2+\cdots+x_{n-1}^2-1}{p}\right) &= \sum_{x_1=1}^{p}\left(\frac{x_1^2+(x_2^2+\cdots+x_{n-1}^2-1)}{p}\right)\\ &= \begin{cases} p-1 & \text{if} \quad x_2^2+\cdots+x_{n-1}^2=1 \\ -1 & \text{if} \quad x_2^2+\cdots+x_{n-1}^2\neq 1 \end{cases}\end{aligned} \tag{335}$$

So, as we sum over $x_2,\ldots,x_{n-1}\in\mathbb{Z}/p\mathbb{Z}$ we see that the inner sum is $p-1$ if $(x_2,\ldots,x_{n-1})\in X_{n-2}(\mathbb{Z}/p\mathbb{Z})$ and -1 if $(x_2,\ldots,x_{n-1})\notin X_{n-2}(\mathbb{Z}/p\mathbb{Z})$. So, we see that

$$\sum_{x_{n-1}=1}^{p}\cdots\sum_{x_1=1}^{p}\left(\frac{x_1^2+\cdots+x_{n-1}^2-1}{p}\right) = (p-1)\#X_{n-2}(\mathbb{Z}/p\mathbb{Z}) - (p^{n-2}-\#X_{n-2}(\mathbb{Z}/p\mathbb{Z})) \tag{336}$$

Indeed, this is just saying that this sum is $p-1$ times the number of tuples where the innermost sum is $p-1$ (which is $\#X_{n-2}(\mathbb{Z}/p\mathbb{Z})$) plus -1 times the rest of the tuples which, since the sum (with the innermost sum evaluated), is $p^{n-2}-\#X_{n-2}(\mathbb{Z}/p\mathbb{Z})$. Thus, we see that

$$\begin{aligned}\#X_n(\mathbb{Z}/p\mathbb{Z}) &= p^{n-1}+\left(\frac{-1}{p}\right)\left[(p-1)\#X_{n-2}(\mathbb{Z}/p\mathbb{Z})-(p^{n-2}-\#X_{n-2}(\mathbb{Z}/p\mathbb{Z}))\right]\\ &= p^{n-1}+\left(\frac{-1}{p}\right)\left[p\#X_{n-2}(\mathbb{Z}/p\mathbb{Z})-p^{n-2}\right]\end{aligned} \tag{337}$$

as claimed. One can then easily prove the induction from k to $k+1$ on our desired formula using this recurrence.

13.3 Exercises

Exercise 13.1

Problem: Determine which primes p divide a number of the form $3n^2-2n+1$.

Solution: Note that p divides a number of the form $3n^2-2n+1$ if and only if $3n^2-2n+1=0 \mod p$ has a solution. Now, if $p=2$ this clearly has a solution ($n=1$) as well as if $p=3$ ($n=2$), so we may assume that $p>3$. Then, note that the quadratic formula says that a solution to $3n^2-2n+1=0 \mod p$ would have to be of the form

$$n=\frac{2\pm\sqrt{4-4(3)(1)}}{6}=\frac{2\pm\sqrt{-8}}{6} \tag{338}$$

and so we see that $3n^2-2n+1$ has a solution if and only if $\left(\frac{-8}{p}\right)=1$. But, note that since $-8=-2^3$ that

$$\left(\frac{-8}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \tag{339}$$

and we have both of these computed thanks to the second supplemental laws. The product of these terms is 1 if and only if they are equal, which happens when $p=1 \mod 4$ and $p=\pm 1 \mod 8$ or when $p=3 \mod 4$ and $p=3,5 \mod 8$. But, when can check that these can happen if and only if $p=1,3 \mod 8$. So, the conclusion is that p divides a number of the form $3n^2-2n+1$ if and only if $p=2,3$, or $p=1,3 \mod 8$.

Exercise 13.2

Problem: Evaluate $\sum_{y=1}^{p}\left(\frac{y}{p}\right)$ (hint: try to use the ideas in the proofs of Lemma 13.4 and Theorem 13.1 to interpret this sum as the number of solutions to some modulus Diophantine equation).

Solution: Let us note that if we set $g(x,y)=x^2-y$ then evidently

$$\#X_g(\mathbb{Z}/p\mathbb{Z})=\sum_{y=1}^{p}\left(1+\left(\frac{y}{p}\right)\right)=p+\sum_{y=1}^{p}\left(\frac{y}{p}\right) \tag{340}$$

On the other hand, note that for any given value of $x\in\mathbb{Z}/p\mathbb{Z}$ there is a unique value of $y\in\mathbb{Z}/p\mathbb{Z}$ such that $y=x^2$. So, it's easy to see that $\#X_g(\mathbb{Z}/p\mathbb{Z})=p$. Combining this with (340) shows that $\sum_{y=0}^{p}\left(\frac{y}{p}\right)=0$.

An alternative solution is as follows. Let $a_0\in\mathbb{Z}/p\mathbb{Z}$ be a non-square. Then, let us note that the map $\mathbb{Z}/p\mathbb{Z}\twoheadrightarrow\mathbb{Z}/p\mathbb{Z}$ given by $y\mapsto a_0y$ is a bijection. Thus,

$$\sum_{y\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{y}{p}\right)=\sum_{y\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{ay}{p}\right)=\left(\frac{a}{p}\right)\sum_{y\in\mathbb{Z}/pZ}\left(\frac{y}{p}\right)=-\sum_{y\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{y}{p}\right) \tag{341}$$

which implies that $\sum_{y=1}^{p}\left(\frac{y}{p}\right)=0$. Another way of saying this is that, thanks to Corollary 12.2 we essentially know that $\sum_{y=1}^{p}\left(\frac{y}{p}\right)$ is 0 plus $\frac{p-1}{2}$ copies of 1 and $\frac{p-1}{2}$ copies of -1, whose total sum is zero.

Exercise 13.3

Problem: Define a function $F:\mathbb{N}^*\to\mathbb{N}$ given by $F(m):=\#X_{f_3}(\mathbb{Z}/m\mathbb{Z})$. Show that there is no polynomial $g(x)\in\mathbb{Z}[x]$ such that $F(m)=g(m)$ for all $m\in\mathbb{N}^*$.

Solution: If there were such a polynomial, then, in particular, $F(p)=g(p)$ for p an odd prime. But, we have shown in Theorem 13.1 that $F(p)=p^2+(-1)^{\frac{p-1}{2}}p$. So, we see that $F(p)-p^2=g(p)-p^2$, and thus $(-1)^{\frac{p-1}{2}}p$ would need to be a polynomial in p. But, note that a polynomial in p can only change signs as many times as its degree. Clearly $(-1)^{\frac{p-1}{2}}p$ would have degree 1, but this changes signs more than once (e.g. from $p=3$ to $p=5$ to $p=7$ accounts for two sign changes).

14 Lecture 14: Quadratic reciprocity III: The Jacobi symbol and Euler's version of Quadratic Reciprocity

The goal for today is to extend the Legendre symbol to a more general setting, which will be useful in the computation of the Legendre symbol itself. Once we have done this we will give a really powerful equivalent version of Quadratic Reciprocity showing that every 'indirect problem' concerning $S(a,b)$ is equivalent to a 'direct problem' concerning $S(a,b)$.

14.1 Setup

Even though the Legendre symbol, together with quadratic reciprocity, give an ostensibly very quick algorithm to decide whether or not $x^2 = a \mod p$ has a solution, the method has one major downside. To illustrate this, let's consider an example:

Example 14.1

Let us determine of the equation $x^2 = -2017 \mod 5003$ has a solution. Begin by noting that 2017 and 5003 are both primes. Now, to see if -2017 is a square in $\mathbb{Z}/5003\mathbb{Z}$ we really want to compute $\left(\frac{-2017}{5003}\right)$. To do this we make the following computation using Theorem 7.2 together with Theorem

12.4 and Theorem 12.5:

$$\begin{aligned}
\left(\frac{-2017}{5003}\right) &= \left(\frac{-1}{5003}\right)\left(\frac{2017}{5003}\right) \\
&= -1 \cdot \left(\frac{2017}{5003}\right) \\
&= -\left(\frac{5003}{2017}\right) \\
&= -\left(\frac{969}{2017}\right) \\
&= -\left(\frac{3 \cdot 17 \cdot 19}{2017}\right) \\
&= -\left(\frac{3}{2017}\right)\left(\frac{17}{2017}\right)\left(\frac{19}{2017}\right) \\
&= -\left(\frac{2017}{3}\right)\left(\frac{2017}{17}\right)\left(\frac{2017}{19}\right) \\
&= -\left(\frac{1}{3}\right)\left(\frac{11}{17}\right)\left(\frac{3}{19}\right) \\
&= -1\left(\frac{11}{17}\right)\left(\frac{3}{19}\right) \\
&= -\left(\frac{17}{11}\right)\left(-\left(\frac{19}{3}\right)\right) \\
&= \left(\frac{6}{11}\right)\left(\frac{1}{3}\right) \\
&= \left(\frac{2 \cdot 3}{11}\right) \\
&= \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) \\
&= -1 \cdot \left(\frac{3}{11}\right) \\
&= -\left(\frac{3}{11}\right) \\
&= \left(\frac{11}{3}\right) \\
&= \left(\frac{2}{3}\right) \\
&= -1
\end{aligned} \tag{342}$$

Thus, $x^2 = -2017 \mod 5003$ has no solution.

We see that the rough outline of the 'algorithm' we are using to compute $\left(\frac{a}{p}\right)$ is 'flip then reduce, flip then reduce, ...' where, each time we flip then reduce, we make the number smaller and smaller. The thing that makes the above somewhat annoying, and really breaks up the 'flip then reduce, flip then reduce, ...' pattern is the fact that to apply Theorem 12.1, so that we can flip, we need the a in $\left(\frac{a}{p}\right)$ to be prime. So, if we flip then reduce, and get a non-prime, we first have to factorize this. This, of course, can be quite time-consuming and really puts a damper on the efficiency of the algorithm.

Thus, the goal for today will be to explain how we can adapt the above to allow us to give an 'flip then

reduce, flip then reduce, ...' algorithm to compute $\left(\frac{a}{p}\right)$ that will, in particular, not require us to prime factorize anything. Of course, to do this, we will have to adapt the Legendre symbol to a symbol of the form $\left(\frac{a}{m}\right)$ where m is not necessarily prime. Indeed, even if we start with $\left(\frac{q}{p}\right)$ where q and p are primes, maybe the flip produces a term of the form $\left(\frac{p}{q}\right)$ and maybe $r_q(p)$ is not prime. So, if one wants to flip again one needs to make sense of $\left(\frac{q}{r_q(p)}\right)$.

Thus, our first order of business will be this extension of the Legendre symbol and then, to make sure that our above 'flip then reduce, flip then reduce, ...' algorithm still applies, we'll need to know that some analogue of Theorem 12.1 still holds for this more general symbol.

Once we do this, we will be able to show that Theorem 12.1 is equivalent to an explicit statement of the form "every 'indirect problem' for $S(a,b)$ is equivalent to a 'direct problem' for $S(a,b)$" that is really quite remarkable.

14.2 The Jacobi symbol

We begin by extending the Legendre symbol to allow elements of the 'denominator' to be any positive odd integer:

Definition 14.1

Let $a \in \mathbb{Z}$ and let $n \in \mathbb{N}^*$ be odd. Then, we define the *Jacobi symbol*, denoted $\left(\frac{a}{n}\right)$, as follows:

$$\left(\frac{a}{n}\right) := \prod_{p \text{ odd}} \left(\frac{a}{p}\right)^{v_p(n)} \tag{343}$$

In other words, we extend $\left(\frac{a}{p}\right)$ to $\left(\frac{a}{n}\right)$, for general odd positive n, by declaring that $\left(\frac{a}{n}\right)$ is completely multiplicative in n—in other words, we extend by multiplicativity in the 'denominator'. Now, this is a wildly useful definition for computations, but the following must be carefully observed:

Warning 14.1

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}^*$ be odd and such that $\gcd(a,n) = 1$. Then, $\left(\frac{a}{n}\right) = -1$ implies that $x^2 = a \mod n$ has no solution, but $\left(\frac{a}{n}\right) = 1$ does not(!) imply that $x^2 = a \mod n$ has a solution. Thus, while $\left(\frac{a}{n}\right) = -1$ implies that $x^2 = a \mod n$ does not have a solution, the converse does not(!) hold in general.

Let us give the following simple example:

Example 14.2

Let p be any odd prime. Then, for any integer a with $p \nmid a$ we have that

$$\left(\frac{a}{p^2}\right) = \left(\frac{a}{p}\right)^2 = 1 \tag{344}$$

Thus, $\left(\frac{a}{p^2}\right) = 1$ regardless of whether or not a is a square modulo p^2.

The natural question is then: why do we even care about the Jacobi symbol? If $\left(\frac{a}{n}\right)$ has a somewhat tenuous relationship to $S(a,n)$ (i.e. to the squarehood of a modulo n), why is it a useful object? The answer is based on the following two observations:

1. If $n = p$ is prime, then $\left(\frac{a}{p}\right)$ determines whether $x^2 = a \mod p$ has a solution.
2. For general n, $\left(\frac{a}{n}\right)$ is very computable—there is (almost) a 'flip then reduce, flip then reduce,...' type algorithm to compute it.

So, what often times happens is practice is that we will really only be interested in computing $\left(\frac{a}{p}\right)$ where p is prime, but in the desired process of 'flip then reduce, flip then reduce,...' mentioned in 2. we are bound to run into situations of having to compute symbols of the form $\left(\frac{b}{n}\right)$ where n is not prime. So, even though the Legendre symbol, the case when n is a prime in the Jacobi symbol, is (usually) the only computation we are interested in, the quickest algorithm to compute the Legendre symbol inevitably involves the Jacobi symbol for non-prime denominators.

Let us now mention the main basic properties of the Jacobi symbol:

Lemma 14.1

Let n and m be odd positive integers, and let $a, b \in \mathbb{Z}$. Then, the following hold:

1. If $a = b \mod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
2. One has that $\left(\frac{a}{n}\right) \in \{-1, 0, 1\}$ and $\left(\frac{a}{n}\right) = 0$ if and only if $\gcd(a,n) \neq 1$.
3. One has that $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
4. One has that $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
5. If $\left(\frac{a}{n}\right) = -1$, then $x^2 = a \mod n$ does not have a solution

Proof 14.1

1. If $a = b \mod n$, then for all odd primes p dividing n we have that $a = b \mod p$. So,
$$\left(\frac{a}{n}\right) = \prod_{\substack{p \text{ odd} \\ p|n}} \left(\frac{a}{p}\right)^{v_p(n)} = \prod_{\substack{p \text{ odd} \\ p|n}} \left(\frac{b}{p}\right)^{v_p(n)} = \left(\frac{b}{n}\right) \tag{345}$$
2. By the definition of $\left(\frac{a}{n}\right)$ it's a product of numbers of the form -1, 0, and 1 thus itself is one

of those numbers. Note that since $\left(\frac{a}{n}\right) = \prod_{\substack{p \text{ odd} \\ p|n}} \left(\frac{a}{p}\right)^{v_p(n)}$ we see that $\left(\frac{a}{n}\right) = 0$ if and only if $\left(\frac{a}{p}\right) = 0$ for some prime prime p dividing n. But, $\left(\frac{a}{p}\right) = 0$ if and only if $p \mid a$, and thus we see that $\left(\frac{a}{n}\right) = 0$ if and only if $p \mid a$ for some prime p dividing n. This is equivalent to $\gcd(a, n) \neq 1$.

3. One sees that
$$\begin{aligned}\left(\frac{ab}{n}\right) &= \prod_{\substack{p \text{ odd} \\ p|n}} \left(\frac{ab}{p}\right)^{v_p(n)} \\ &= \prod_{\substack{p \text{ odd} \\ p|n}} \left(\frac{a}{p}\right)^{v_p(n)} \left(\frac{b}{p}\right)^{v_p(n)} \\ &= \left(\prod_{\substack{p \text{ odd} \\ p|n}} \left(\frac{a}{p}\right)^{v_p(n)}\right) \left(\prod_{\substack{p \text{ odd} \\ p|n}} \left(\frac{b}{p}\right)^{v_p(n)}\right) \\ &= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)\end{aligned} \tag{346}$$

4. This follows from the observation that
$$\begin{aligned}\left(\frac{a}{mn}\right) &= \prod_{p \text{ odd}} \left(\frac{a}{p}\right)^{v_p(mn)} \\ &= \prod_{p \text{ odd}} \left(\frac{a}{p}\right)^{v_p(m)+v_p(n)} \\ &= \prod_{p \text{ odd}} \left(\left(\frac{a}{p}\right)^{v_p(m)} \cdot \left(\frac{a}{p}\right)^{v_p(n)}\right) \\ &= \left(\prod_{p \text{ odd}} \left(\frac{a}{p}\right)^{v_p(m)}\right)\left(\prod_{p \text{ odd}} \left(\frac{a}{p}\right)^{v_p(n)}\right) \\ &= \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)\end{aligned} \tag{347}$$

5. See Exercise 14.1.

This is all fine and nice, but the fuel that made the 'flip and reduce, flip and reduce, ...' method (kind of) work for the Legendre symbol was Theorem 12.1. So, if we hope to adapt, and improve upon such a method for the Jacobi symbol we certainly need an analogue of the result to hold. Thankfully, it does:

Theorem 14.1: Quadratic reciprocity for Jacobi symbol

Let m and n be odd, positive, and coprime integers. Then,
$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right) \tag{348}$$

Moreover, we have the following two supplementary laws:

1. The equality
$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n = 1 \mod 4 \\ -1 & \text{if } n = 3 \mod 4 \end{cases} \tag{349}$$
holds.

2. The equality
$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n = \pm 1 \mod 8 \\ -1 & \text{if } n = 3, 5 \mod 8 \end{cases} \tag{350}$$
holds.

The proof of Theorem 14.1 is a pretty straightforward generalization of Theorem 12.1, and relies mostly on the following idle observation:

Lemma 14.2

Let n be a positive odd integer. Write $n = p_1 \cdots p_s$ where each p_i is prime (in particular, we don't require $p_i \neq p_j$ for $i \neq j$). Then,
$$\frac{n-1}{2} = \sum_{i=1}^{s} \frac{p_i - 1}{2} \mod 2 \tag{351}$$
and
$$\frac{n^2-1}{8} = \sum_{i=1}^{s} \frac{p_i^2 - 1}{8} \mod 2 \tag{352}$$

To be clear, the first expression makes sense since each n and p_i is odd, thus $\frac{n-1}{2}$ and $\frac{p_i - 1}{2}$ is an integer for all i. To see that $8 \mid n^2 - 1$, so that $\frac{n^2-1}{8}$ is an integer, one merely observes that if we write $n = 2k+1$ then $n^2 - 1 = 4k(k+1)$. In particular, since one of k or $k+1$ is even, we have that $8 \mid 4k(k+1) = n^2 - 1$. Similarly $\frac{p_i^2 - 1}{8}$ is an integer for all i.

Proof 14.2

To prove the first equality, let us note that for any two odd positive integers k_1 and k_2 we have that
$$\frac{1}{2}(k_1 - 1)(k_2 - 1) = 0 \mod 2 \tag{353}$$
Thus, we deduce that
$$\frac{1}{2}(k_1 - 1) + \frac{1}{2}(k_2 - 1) = \frac{1}{2}(k_1 k_2 - 1) - \frac{1}{2}(k_1 - 1)(k_2 - 1) = \frac{1}{2}(k_1 k_2 - 1) \mod 2 \tag{354}$$
from where the first claim follows by iteration.

Similarly, if k_1 and k_2 are odd then
$$\frac{1}{8}(k_1^2 - 1)(k_2^2 - 1) = 0 \mod 2 \tag{355}$$
and so
$$\frac{1}{8}(k_1^2 - 1) + \frac{1}{2}(k_2^2 - 1) = \frac{1}{8}(k_1^2 k_2^2 - 1) - \frac{1}{8}(k_1^2 - 1)(k_2^1 - 1) = \frac{1}{8}(k_1^2 k_2^2 - 1) \mod 2 \tag{356}$$

and the second claim also follows by iteration.

The proof of Theorem 14.1 then follows quite easily from Theorem 12.1:

Proof 14.3: Theorem 14.1

Factorize $n = p_1 \cdots p_s$ and $m = q_1 \cdots q_t$. Then,

$$\begin{aligned}\left(\frac{n}{m}\right) &= \prod_{i=1}^{s}\prod_{j=1}^{t}\left(\frac{p_i}{q_j}\right) \\ &= \prod_{i=1}^{s}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}\left(\frac{q_j}{p_i}\right) \\ &= (-1)^u\left(\frac{m}{n}\right)\end{aligned} \tag{357}$$

where

$$u = \sum_{i=1}^{s}\sum_{j=1}^{t}\left(\frac{p_i-1}{2}\frac{q_j-1}{2}\right) \tag{358}$$

But, by Lemma 14.2

$$\sum_{i=1}^{s}\sum_{j=1}^{t}\left(\frac{p_i-1}{2}\frac{q_j-1}{2}\right) = \left(\sum_{i=1}^{s}\frac{p_i-1}{s}\right)\left(\sum_{j=1}^{t}\frac{q_j-1}{2}\right) = \frac{n-1}{2}\frac{m-1}{2} \mod 2 \tag{359}$$

from where the desired equality follows.

The proof of the supplementary laws is precisely the same idea (using Lemma 14.2) noting that for an odd integer k

$$(-1)^{\frac{k^2-1}{2}} = \begin{cases}1 & \text{if } k = 1 \mod 4 \\ -1 & \text{if } k = 3 \mod 4\end{cases} \tag{360}$$

and

$$(-1)^{\frac{k^2-1}{8}} = \begin{cases}1 & \text{if } k = \pm 1 \mod 8 \\ -1 & \text{if } k = 3, 5 \mod 8\end{cases} \tag{361}$$

With this, we can now formalize our 'flip then reduce, flip then reduce,...' algorithm as follows:

Algorithm 14.1

Let n be an odd positive integer and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. The following is an algorithm to compute $\left(\frac{a}{n}\right)$:

Step 1: Replace a by $b := r_n(a)$.

Step 2: Write $b = 2^e c$ where $e := v_2(b)$. Evaluate $\left(\frac{b}{n}\right)$ as $\left(\frac{2}{n}\right)^e\left(\frac{c}{n}\right)$. To evaluate the first term use Theorem 14.1 part 2. To evaluate the term $\left(\frac{c}{n}\right)$ proceed to next step.

Step 3: Write $c = (-1)^t|c|$ where $t = v_{\text{sgn}}(c)$. Compute $\left(\frac{c}{n}\right)$ as $\left(\frac{-1}{n}\right)^t\left(\frac{|c|}{n}\right)$. Computing

$\left(\frac{-1}{n}\right)^t$ can be done using Theorem 14.1 part 1. To compute $\left(\frac{|c|}{n}\right)$ proceed to next step.

Step 4: To compute $\left(\frac{|c|}{n}\right)$ use Theorem 14.1 to equate it to $(-1)^{\frac{n-1}{2}\frac{|c|-1}{2}}\left(\frac{n}{|c|}\right)$. Compute $(-1)^{\frac{n-1}{2}\frac{|c|-1}{2}}$ by hand. To compute $\left(\frac{n}{|c|}\right)$ go back to Step 1.

Let us carry this process out in an example:

Example 14.3

Let us show that 1111 is not a square modulo 8093. To do this it suffices to show that $\left(\frac{1111}{8093}\right) = -1$. But, by Algorithm 14.1 we can compute this as follows:

$$\begin{aligned}
\left(\frac{1111}{8093}\right) &= \left(\frac{8093}{1111}\right) \\
&= \left(\frac{316}{1111}\right) \\
&= \left(\frac{2^2 \cdot 79}{1111}\right) \\
&= \left(\frac{2}{1111}\right)^2 \left(\frac{79}{1111}\right) \\
&= \left(\frac{79}{1111}\right) \\
&= -\left(\frac{1111}{79}\right) \\
&= -\left(\frac{5}{79}\right) \\
&= -\left(\frac{79}{5}\right) \\
&= -\left(\frac{4}{5}\right) \\
&= -1 \cdot 1 \\
&= -1
\end{aligned} \tag{362}$$

Thus, 1111 is not a square modulo 8093.

14.3 Euler's version of Theorem 12.1

The other great advantage of developing the Jacobi symbol, and proving Theorem 14.1, is that we can now formalize the claim that every 'indirect problem' for $S(a, b)$ can be phrased as 'direct problem' for $S(a, b)$, at least assuming that b is prime. Namely, in every above example, we saw that for $a \in \mathbb{Z}$ one has that the set of primes $p \nmid a$ such that $\left(\frac{a}{p}\right) = 1$ were described in terms of congruences on p modulo, every time, $4|a|$. We would now like to prove that this holds in essentially full generality.

The key is the following pivotal result, that follows quite easily from our work on the Jacobi symbol, but is woefully hard to show without it:

Theorem 14.2

Let $a \in \mathbb{Z}$ and let m and n be odd positive integers. Then, if $m = n \mod 4|a|$ then $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$.

Now, while $\left(\frac{a}{n}\right)$ evidently only depends on the 'numerator' up to some congruence (namely congruence modulo n), the 'denominator' has no apparent connection to congruences. The above fantastic theorem is that, in fact, the 'denominator' not only does have connection to congruences, but a very straightforward one at that.

Proof 14.4: Theorem 14.2

Let us first assume that a is odd and positive. Then, we know from Theorem 14.1 that

$$\left(\frac{a}{m}\right) = (-1)^{\frac{a-1}{2}\frac{m-1}{2}} \left(\frac{m}{a}\right) \tag{363}$$

and

$$\left(\frac{a}{n}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}} \left(\frac{n}{a}\right) \tag{364}$$

Thus, it suffices to show that if $m = n \mod 4a$ then

$$(-1)^{\frac{a-1}{2}\frac{m-1}{2}} \left(\frac{m}{a}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}} \left(\frac{n}{a}\right) \tag{365}$$

Now, since $m = n \mod 4a$ this implies that $m = n \mod a$ and thus $\left(\frac{m}{a}\right) = \left(\frac{n}{a}\right)$. Thus, it suffices to explain why

$$(-1)^{\frac{a-1}{2}\frac{m-1}{2}} \left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}} \tag{366}$$

But, to do this it suffices to note that since $m = n \mod 4a$ that $m = n \mod 4$. This then implies that $\frac{m-1}{2} = \frac{n-1}{2} \mod 2$ and the claim then immediately follows.

Suppose now that a is odd, but possibly negative. We can then write $a = (-1)^s|a|$ with $s = v_{\text{sgn}}(a)$. Thus, we see that

$$\left(\frac{a}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{|a|}{m}\right) \tag{367}$$

and

$$\left(\frac{a}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{|a|}{n}\right) \tag{368}$$

We have already shown, in previous paragraph, that $\left(\frac{|a|}{m}\right) = \left(\frac{|a|}{n}\right)$. Thus, it suffices to show that $\left(\frac{-1}{m}\right) = \left(\frac{-1}{n}\right)$. But, to do this it suffices to note that $\left(\frac{-1}{m}\right)$ and $\left(\frac{-1}{n}\right)$ only depend on the values of m and n modulo 4, and since $m = n \mod 4|a|$ they are, in particular, equal modulo 4.

Finally, suppose that $a \in \mathbb{Z}$. Write $a = 2^e b$ with $e = v_2(a)$ and $b \in \mathbb{Z}$ odd. Note then that

$$\left(\frac{a}{m}\right) = \left(\frac{2}{m}\right)^e \left(\frac{b}{m}\right) \tag{369}$$

and

$$\left(\frac{a}{n}\right) = \left(\frac{2}{n}\right)^e \left(\frac{b}{n}\right) \tag{370}$$

Since we have shown that $\left(\frac{b}{m}\right) = \left(\frac{b}{n}\right)$ in the last paragraph, it suffices to show that $\left(\frac{2}{m}\right)^e = \left(\frac{2}{n}\right)^e$. If $e = 0$ this is clear, so we may assume without loss of generality that $e > 0$. Then, it suffices to show that $\left(\frac{2}{m}\right) = \left(\frac{2}{n}\right)$. Note though that $\left(\frac{2}{m}\right)$ and $\left(\frac{2}{n}\right)$ only depend on what m and n are modulo 8. But, note that $m = n \mod 4|a|$ and, since $e > 1$ we have that $2 \mid a$ so that $8 \mid 4|a|$. Thus, we see that this implies that m and n are equal modulo 8, and the conclusion follows.

From this we deduce the following beautiful version of Quadratic Reciprocity often called 'Euler's version of Quadratic Reciprocity'. To state it,

Theorem 14.3: Euler's version of Quadratic Reciprocity

Let p_0 be a fixed prime. Then, for an odd prime p distinct from p_0 the equation $x^2 = p_0 \mod p$ has a solution if and only if $p = \pm\ell^2 \mod 4p_0$ where $\ell \in \{0, \ldots, 4p_0 - 1\}$ is odd.

Proof 14.5

Suppose first that $p = (-1)^s\ell^2 \mod 4p_0$ for some odd $\ell \in \{0, \ldots, 4p_0 - 1\}$ and $s = 0, 1$. If $s = 0$ then this is trivial since

$$\left(\frac{p_0}{p}\right) = \left(\frac{p_0}{\ell^2}\right) = \left(\frac{p_0}{\ell}\right)^2 = 1 \tag{371}$$

where the first equality follows from Theorem 14.2 and the second equality follows by definition of the Jacobi symbol. Suppose now that $s = 1$ so that $p = -\ell^2 \mod 4p_0$. Then, this implies that $p = -\ell^2 \mod 4$. But, the only odd squares modulo 4 are 1, so $p = 3 \mod 4$. So, now we now that $p = 4p_0 - \ell^2 \mod 4p_0$ and so, by Theorem 14.2 we know that

$$\left(\frac{p_0}{p}\right) = \left(\frac{p_0}{4p_0 - \ell^2}\right) \tag{372}$$

If $p_0 = 1 \mod 4$ then we know that

$$\left(\frac{p_0}{4p_0 - \ell^2}\right) = \left(\frac{4p_0 - \ell^2}{p_0}\right) = \left(\frac{-\ell^2}{p_0}\right) = \left(\frac{-1}{p_0}\right) = 1 \tag{373}$$

where the last equality uses Theorem 14.1 part 1. If $p_0 = 3 \mod 4$ then, since we are in the case $4p_0\ell^2 = p = 3 \mod 4$, this implies that

$$\left(\frac{p_0}{4p_0 - \ell^2}\right) = -\left(\frac{4p_0 - \ell^2}{p_0}\right) = -\left(\frac{-1}{p_0}\right) = -(-1) = 1 \tag{374}$$

where the last claim uses Theorem 14.1 part 1. again. Thus, this direction follows.

Conversely, suppose that $x^2 = p_0 \mod p$ has a solution. Then, $\left(\frac{p_0}{p}\right) = 1$. We will break this into the cases of $p_0 = 1 \mod 4$ and $p_0 = 3 \mod 4$.

If $p_0 = 1 \mod 4$ then by Theorem 12.1 we know that $\left(\frac{p}{p_0}\right) = \left(\frac{p_0}{p}\right)$. In particular, since $\left(\frac{p_0}{p}\right) = 1$ we see that $\left(\frac{p}{p_0}\right) = 1$ which, since p_0 is prime, implies that p is a square modulo p_0 and thus $p = \ell^2$ for some $\ell \in \{0, \ldots, p_0 - 1\}$. We want to promote this to a congruence modulo $4p_0$. To do this, it suffices to also note what p is modulo 4 by the Chinese Remainder Theorem. Suppose first that $p = 1 \mod 4$. Then, $p = \ell^2 \mod p_0$ and $p = \ell^2 \mod 4$, since the only odd squares modulo 4 are 1. Thus,

we see that $p = \ell^2 \mod 4p_0$. Suppose now that $p = 3 \mod 4$. Note that we can rewrite $p = \ell^2 \mod p_0$ as $p = -(i\ell)^2 \mod p_0$ where i is the non-trivial solution to $x^2 = -1 \mod p_0$ (which exists since $p_0 = 1 \mod 4$). Note then that $-(i\ell)^2 = 3 \mod 4$ and thus we see that $p = -(i\ell)^2 \mod 4$ and thus $p = -(i\ell)^2 \mod 4p_0$. Thus, we see that in either case, we can write p as plus or minus a square modulo $4p_0$.

Suppose now that $p_0 = 3 \mod 4$. Let us break the claim into cases depending on what p is modulo 4. If $p = 1 \mod 4$ then we know that $\left(\frac{p}{p_0}\right) = \left(\frac{p_0}{p}\right) = 1$. Thus, we know that we can write $p = \ell^2 \mod p_0$ for some ℓ. Since $p = 1 \mod 4$ this implies that $p = \ell^2 \mod 4$ and so $p = \ell^2 \mod 4p_0$. Suppose now that $p = 3 \mod 4$. Then, we know that $\left(\frac{p}{p_0}\right) = -\left(\frac{p_0}{p}\right) = -1$. But, since $p_0 = 3 \mod 4$, so that -1 is a non-square modulo 4, we know that $-p$ is a square modulo p_0, and so $-p = \ell^2 \mod p_0$ so that $p = -\ell^2 \mod p_0$. Since $p = 3 \mod 4$ and $-\ell^2 = 3 \mod 4$ we also see that $p = -\ell^2 \mod 4$ and so $p = -\ell^2 \mod 4p_0$. Thus, we see that any case, we can write p as plus or minus a square modulo $4p_0$ as desired.

Example 14.4

Let $p_0 = 17$. Then, the above says that the odd primes p distinct from 17 for which 17 is a square modulo p are those $p = \pm\ell^2 \mod 68$ where $\ell \in \{0, \dots, 67\}$ is odd. One can calculate that this means that 17 is a square modulo p if and only if $p = \pm 1, \pm 8, \pm 13, \pm 17, \pm 21, \pm 25, \pm 33, \pm 59, \pm 53 \mod 68$.

The reason that this turns an 'indirect problem' into a 'direct problem' is that determining for which p is p_0 a square modulo p is indirect, but determining what the possible values of ℓ^2 are modulo $4p_0$ is a 'direct problem'.

From this, we deduce that for a general integer a, whether or not a is a square modulo p only depends on congruence conditions on p modulo, not just $4|a|$, but more specifically modulo $4|\mathrm{sf}(a)|$ where this unknown symbol is defined as follows:

Definition 14.2

Let $a \in \mathbb{Z}$. Define the *squarefree part of* a, denoted $\mathrm{sf}(a)$ as follows:

$$\mathrm{sf}(a) := (-1)^{v_{\mathrm{sgn}}} \prod_{p|a} p^{r_2(v_p(a))} \tag{375}$$

In other words, the squarefree part of a is just the integer you obtain by taking the remainder of each prime exponent of a divided by 2.

Example 14.5

Let $a = 2^5 \cdot 3^2 \cdot 5 \cdot 7^8$ then $\mathrm{sf}(a) = 2 \cdot 5$.

We can then generalize Euler's version of Quadratic Reciprocity to general a as follows:

Corollary 14.1

Let $a \in \mathbb{Z}$. Then, there exists some set $S \subseteq \mathbb{Z}/4|\mathrm{sf}(a)|\mathbb{Z}$ such that for an odd prime p such that $p \nmid a$ we have that $x^2 = a \mod p$ has a solution if and only if $(p \mod 4|\mathrm{sf}(a)|) \in S$.

Proof 14.6

e are trying to find for which odd primes p such that $p \nmid a$ does $\left(\frac{a}{p}\right) = 1$ hold. Note that evidently $\left(\frac{a}{p}\right) = \left(\frac{\mathrm{sf}(a)}{p}\right)$. Now, we know that we can write

$$\mathrm{sf}(a) = (-1)^s 2^e \prod_{i=1}^{n} q_i \tag{376}$$

where $q_1, \ldots, q_n$ are the distinct odd primes that divide $\mathrm{sf}(a)$, and $s, e \in \{0, 1\}$. So,

$$\left(\frac{\mathrm{sf}(a)}{p}\right) = \left(\frac{-1}{p}\right)^s \left(\frac{2}{p}\right)^e \prod_{q|\mathrm{sf}(a)} \left(\frac{q}{p}\right) \tag{377}$$

Let us denote by T the set of all tuples in $\{\pm 1\}^s \times \{\pm 1\}^e \times \{\pm 1\}^n$ such that the product of all of its coordinates is 1. Clearly then we see that $\left(\frac{\mathrm{sf}(a)}{p}\right) = 1$ if and only if

$$\mathbf{a}(p) := \left(\left(\frac{-1}{p}\right)^s, \left(\frac{2}{p}\right)^e, \left(\frac{q_1}{p}\right), \ldots, \left(\frac{q_n}{p}\right)\right) \in T \tag{378}$$

Now, by Theorem 12.4 we know that $\left(\frac{-1}{p}\right)$ only depends on p modulo 4^s (i.e. if $s = 1$ then it's modulo 4 and if $s = 0$ this is a vaccuous condition on p). Similarly, by Theorem 12.5 if $e = 1$, so that $2 \mid \mathrm{sf}(a)$ we know that $\left(\frac{2}{p}\right)$ only depends on p modulo 8^e (with the same meaning as $\mod 4^s$). Finally, by Theorem 14.3 we know that each $\left(\frac{q}{p}\right)$ only depends on p modulo $4q$. Thus, every element of T corresponds to a system of congruence conditions on p of the form

$$\begin{cases} p &= a \mod 4^s \\ p &= b \mod 8^e \\ p &= c_1 \mod 4q_1 \\ &\vdots \\ p &= c_n \mod 4q_n \end{cases} \tag{379}$$

Now, not every such simultaneous congruence is solvable since $4^s, 8^e, 4q_1, \ldots, 4q_n$ are not coprime. Let $T' \subseteq T$ be the set of T that correspond to solvable congruences. Then, we see that, really, $\left(\frac{a}{p}\right) = 1$ if and only if $\mathbf{a}(p) \in T'$. Every solvable congruence corresponding to an element of T' then corresponds, by an obvious extension of the Chinese Remainder Theorem, to a congruence modulo $42^e q_1 \cdots q_n = 4|\mathrm{sf}(a)|$. We then let S denote this set of congruences. The conclusion follows.

The last thing we want to prove in this section is that, in fact, Euler's version of Quadratic Reciprocity is, as the name suggests, equivalent to Theorem 12.1. But, this is not too hard to see.

Theorem 14.4

Theorem 12.1 follows from Theorem 14.3.

Proof 14.7

It suffices to prove the equivalent version Theorem 12.3. So, we essentially need to show that $\left(\frac{q}{p}\right) = 1$ if and only if $\left(\frac{p^*}{q}\right) = 1$. But, by definition, $\left(\frac{p^*}{q}\right) = 1$ if and only if $p^* = \ell^2 \mod q$ for some $\ell \in \{0, \dots, q-1\}$ odd. It's not then hard to see that this is equivalent to $p = \pm\ell^2 \mod 4q$ since the $\pm$ in p^* and $\pm\ell^2$ are determined by $p \mod 4$. The claim then follows.

14.4 Exercises

Exercise 14.1

Problem: Prove Lemma 14.1 part 5.

Solution: Note that $\left(\frac{a}{n}\right) = \prod_{\substack{p \text{ odd} \\ p|n}} \left(\frac{a}{p}\right)^{v_p(n)}$. Since each $\left(\frac{a}{p}\right)$ is either 0, -1, or 1 if $\left(\frac{a}{n}\right) = -1$ at least one of the $\left(\frac{a}{p}\right) = -1$. This means that for some $p \mid n$ we have that $\left(\frac{a}{p}\right) = -1$ and so $x^2 = a \mod p$ has no solution. The claim then follows by Combining Theorem 7.2 and Theorem 8.1.

Exercise 14.2

Problem: Show that $x^2 = 2018 \mod 5001$ has no solution.

Solution: It suffices to show that the Jacobi symbol $\left(\frac{2018}{5001}\right)$ is equal to -1. We proceed as follows

using Algorithm 14.1:

$$\begin{aligned}
\left(\frac{2018}{5001}\right) &= \frac{2 \cdot 1009}{5001} \\
&= \left(\frac{2}{5001}\right)\left(\frac{1009}{5001}\right) \\
&= 1 \cdot \left(\frac{1009}{5001}\right) \\
&= \left(\frac{5001}{1009}\right) \\
&= \left(\frac{965}{1009}\right) \\
&= \left(\frac{1009}{965}\right) \\
&= \left(\frac{44}{965}\right) \\
&= \left(\frac{2}{965}\right)^2 \left(\frac{11}{965}\right) \\
&= \left(\frac{11}{965}\right) \\
&= \left(\frac{965}{11}\right) \\
&= \left(\frac{8}{11}\right) \\
&= \left(\frac{2}{11}\right)^3 \\
&= (-1)^3 \\
&= -1
\end{aligned} \tag{380}$$

Exercise 14.3

Problem: For which primes p is 19 a square modulo p?

Solution: Clearly $p = 2$ and $p = 19$ work, so we can assume that p is an odd prime distinct from 19. By Theorem 14.3 we then see that for such p we have that $x^2 = 19 \mod p$ has a solution if and only if $p = \pm\ell^2 \mod 76$ where $\ell \in \{0, \ldots, 75\}$ is odd. One can check that this is equivalent to $p = \pm 1, \pm 5, \pm 9, \pm 17, \pm 25, \pm 45, \pm 49, \pm 57, \pm 61, \pm 73 \mod 76$.

15 Lecture 15: Tonelli-Shanks algorithm

Thanks to Algorithm 14.1 we have an incredible quick way to determine whether or not $a \in \mathbb{Z}$ is a square modulo p. That said, in practice knowing that $a \in \mathbb{Z}$ has a square modulo p is not so useful if one can then not actually algorithmically find the square root. The goal of the Tonelli-Shanks algorithm it do exactly this. It will allow us to quickly actually find the solutions to the equation $x^2 = a \mod p$ assuming that it does, in fact, have a solution.

15.1 Motivational exact examples

To motivate the Tonelli-Shanks algorithm it's useful to first consider some cases where can give an exact (i.e. not requiring an iterative algorithm) method to produce square roots modulo p. This will only work for special types of p, before becoming to cumbersome to phrase non-iteratively.

Here is the simplest example of a method to produce exact square roots:

Lemma 15.1

Let p be a prime and $a \in \Phi(p)$. Set $f(x) := x^2 - a$. If $p = 4k + 3$ for some $k \in \mathbb{Z}$ (i.e. $p = 3 \mod 4$) then $X_f(\mathbb{Z}/p\mathbb{Z}) = \{\pm a^{k+1}\}$.

Proof 15.1

Note that since $a \neq 0$ that $a^{k+1} \neq -a^{k+1}$ in $\mathbb{Z}/p\mathbb{Z}$ since $p > 2$ thus if we can show that $\{\pm a^{k+1}\} \subseteq X_f(\mathbb{Z}/p\mathbb{Z})$ then we will necessarily have the desired equality since $\#X_f(\mathbb{Z}/p\mathbb{Z}) \leqslant 2$ (by Theorem 9.1). To see that $\{\pm a^{k+1}\} \subseteq X_f(\mathbb{Z}/p\mathbb{Z})$ we proceed as follows. Since $x^2 = a \mod p$ has a solution, we know from Theorem 6.3 that $a^{\frac{p-1}{2}} = 1 \mod p$. But, since $p = 4k+3$ this is equivalent to $a^{2k+1} = 1 \mod p$. Thus, we see that

$$(\pm a^{k+1})^2 = a^{2k+2} = a^{2k+1} \cdot a = 1 \cdot a = a \mod p \tag{381}$$

from where the conclusion follows.

Of course, this seems like a bit of a parlor trick. Namely, there are infinitely many primes p such that $p = 1 \mod 4$—in fact, interpreted correctly, about half of primes are 1 modulo 4—and the above method fails miserably, at least if copied naively, for primes that are 1 modulo 4. Namely, one can see that one can phrase the $k+1$ showing up in Lemma 15.1 was obtained as $k + 1 = \frac{1}{2}\left(\frac{1}{2}(p-1)+1\right)$. Of course, if $p = 1 \mod 4$ then this is not an integer.

That said, if we are more discerning about how one defines k we can, in fact, extend this technique to some cases where $p = 1 \mod 4$. Namely, we have the following:

Lemma 15.2

Let p be a prime such that $p = 8k+5$ for some $k \in \mathbb{Z}$ (i.e. $p = 5 \mod 8$). Then, if $a \in \Phi(p)$ and $x^2 = a \mod p$ has a solution, then either $a^{\frac{p-1}{4}} = 1 \mod p$ or $a^{\frac{p-1}{4}} = -1 \mod p$. Setting $f(x) := x^2 - a$, we have that $X_f(\mathbb{Z}/p\mathbb{Z}) = \{\pm a^{k+1}\}$ in the former case and $X_f(\mathbb{Z}/p\mathbb{Z}) = \{\pm 2^{2k+1} a^{k+1}\}$ in the latter.

Proof 15.2

Note that by Theorem 6.3 we have that $a^{\frac{p-1}{2}} = 1 \mod p$. Thus,

$$\left(a^{\frac{p-1}{4}}\right)^2 = a^{\frac{p-1}{2}} = 1 \mod p \tag{382}$$

and thus $a^{\frac{p-1}{4}}$ is a square root of 1 modulo p. This then implies that $a^{\frac{p-1}{4}} = \pm 1 \mod p$ as claimed.

Suppose first that $a^{\frac{p-1}{4}} = 1 \mod p$. Rewriting this in terms of k it says that $a^{2k+1} = 1 \mod p$.

Thus, much like as in the proof of Lemma 15.1, we see that

$$(\pm a^{k+1})^2 = a^{2k+2} = a^{2k+1} \cdot a = 1 \cdot a = a \mod p \tag{383}$$

from where $\{\pm a^{k+1}\} \subseteq X_f(\mathbb{Z}/p\mathbb{Z})$ and then equality follows by evoking Theorem 9.1 as in the proof of Lemma 15.1.

Suppose now that $a^{\frac{p-1}{4}} = a^{2k+1} = -1 \mod p$. Then, we see that

$$(\pm 2^{2k+1} a^{k+1})^2 = 2^{4k+2} a^{2k+2} = \left(\frac{2}{p}\right) a^{2k+1} \cdot a = -1 \cdot -1 \cdot a = a \mod p \tag{384}$$

where we have used Theorem 12.5 to deduce that $\left(\frac{2}{p}\right) = -1$ since $p = 5 \mod 8$.

So, we see that we have given a procedure to produce square roots modulo p if either $p = 3 \mod 4$ or $p = 5 \mod 8$. This accounts for, interpreted correctly, three quarters of primes p. We can attempt to continue this process by splitting the primes into more and more nuanced cases depending on what the prime is modulo 2^k, but the results will get, unsurprisingly, more and more complicated. That said, while describing the exact square roots in a concise way as in Lemma 15.1 and Lemma 15.2 quickly becomes impossible, we can describe *algorithmically* how to proceed for all primes p.

15.2 Approximate square roots and error terms

Before we begin, in earnest, trying to develop the algorithmic analogue of the general results of the last subsection it will be helpful to make some definitions to put us in the right mindset. To begin, we make the following silly definition:

Definition 15.1

Let p be an odd prime and $a \in \Phi(p)$. We call $x \in \Phi(p)$ an *approximate square root* of a if $x^2 = ba$ for some $b \in \Phi(p)$ which is called the *error term*. We call $x \in \Phi(p)$ a *true square root* if it's an approximate square root with error term 1 (i.e. $x^2 = a$).

The reason that this definition is exceedingly silly is because of the following observation: every element of $\Phi(p)$ is an approximate square root of a. Namely, if $x \in \Phi(p)$ then $x^2 = ba$ with $b = x^2 a^{-1}$. Thus, the definition itself doesn't carry a lot of content. But, it puts us in a decent mindset to figure out how we might find a true square root of a algorithmically, assuming that a square root of a does exist.

Namely, one might imagine that one chooses some informed initial guess x of an approximate square root, with error term b. Of course, this initial guess won't usually be a true square root—the error term b will not be 1—but it might be a good start. One can then imagine 'adjusting' the initial guess by some amount which, hopefully, produces another approximate square root with 'smaller' error.

While this is a nice idea, one needs some serious explanation about what the words 'adjusting' and 'smaller' mean. While the former could mean many things, since we would like to understand how adjusting an approximate square root adjusts its error term, a natural choice is that adjusting x means replacing it with xc for some $c \in \Phi(p)$. We see then that xc is an approximate square root of a with error term $c^2 b$. This multiplicative procedure is much preferred to something like, say, additively adjusting x (e.g. replacing it by $x + c$) which makes the resulting error term much harder to control (as well as the more subtle point that $x + c$ needn't be in $\Phi(p)$ any more). The notion of 'smaller' requires more care.

Namely, we want some quantitative measure of how far an element $b \in \Phi(p)$ is away from 1. While there are many ways one might define such a quantitative measure, there is a fairly tantalizing one which is the order function $|\cdot| : \Phi(p) \to \{0, \ldots, p-1\}$. Namely, if x is an approximate, but not true, square root of a with error term b, then we might imagine that the adjustment xc is 'better' if its error term $c^2 b$ satisfies the

relation $1 \leqslant |c^2 b| < |b|$. One then sees that if we can reliable adjust any initial guess for approximate square root of a to a better approximate square root of a then we must eventually end up with a true square root of a since the order of the error term can only decrease finitely many times before its order is 1.

Doing all of this is simpler said than done. Namely, the sticking point is the observation that the relationship between $|c^2 b|$ and $|b|$ can, in general, be quite complicated:

Example 15.1

Exercise **??** below shows that in some good cases $|c^2 b| = |c^2||b|$ which is about as simple of a relationship as one might imagine. Of course, this is not what we want since in this case $|c^2 b| > |b|$ if $c \neq \pm 1$ (Why?).

Example 15.2

If $c^2 = b^{-1}$ then $|c^2 b| = |1| = 1$. Of course, to find this adjustment factor would require us to solve $c^2 = b^{-1}$. Note that this is, in fact, doable. Namely, since $x^2 = ba$ we have that $b = x^2 a^{-1}$ and since x^2 and a^{-1} are squares this implies that b, and thus b^{-1}, is a square. Of course, since we are trying to find square roots to begin with, this doesn't feel like an ideal situation.

Remark 15.1

In Example 15.2 we made a somewhat silly observation: that if x is an approximate square root of a, then finding a true square root of a is (essentially) equivalent to finding a true square root of the error term b. As implied in that example, this seems wholly unhelpful in general. But, we will see that the same initial guess of an approximate square root of a makes the error term of a simpler nature to find square roots. This can be used as an alternative means to understand the Tonelli-Shanks idea, but one we won't pursue here.

As the above shows, to try and carry out this procedure of taking an initial guess of an approximate square root and iteratively adjusting it to get better and better approximations to a true square root, we need to choose our initial approximate square root well so that the error terms become manageable.

In both cases of Lemma 15.1 and Lemma 15.2 we see that there is an initial guess of $x = a^{k+1}$ which, in some cases when $p = 5 \mod 8$, need to be adjusted. This suggests that, perhaps, '$x = a^{k+1}$' is always a good choice of an initial guess of an approximate square root of a. The reason that '$x = a^{k+1}$' is in square quotes is that it's not clear what $k+1$ should mean for general p (e.g. if $p = 1 \mod 8$). So, let us begin by trying to suss this out.

To see the general procedure we carried out in Lemma 15.1 and Lemma 15.2 to get the '$k+1$ term' there, we make the following observation. Let us begin by assuming that $p = 4k+3$. Note then that $p - 1 = 2s$ and $s := 2k+1$, of course, is odd. We then see that $k + 1 = \frac{1}{2}(s+1)$. Similarly, if $p = 8k+5$ then we see that $p - 1 = 2^2 \cdot s$ and $s = 2k+1$, of course, is odd. In this case we see that $k + 1 = \frac{1}{2}(s+1)$ as well. Thus, for general p, this suggests that the correct definition of '$k+1$' is as follows. Namely, let p be an odd prime and write $p - 1 = 2^v s$ with $v \in \mathbb{N}^*$ and s odd. We see then that correct definition of '$k+1$' is $\frac{1}{2}(s+1)$.

Now, let us note that if we make our initial guess of an approximate square root of a to be $x = a^{\frac{1}{2}(s+1)}$ as the above suggests, then

$$x^2 = a^{s+1} = a^s \cdot a \tag{385}$$

so that the associated error term is $b = a^s$. Thus, to show that $x = a^{\frac{1}{2}(s+1)}$ is a good initial guess of an approximate square root of a, we need to show that this error term $b = a^s$ has understandable properties.

15.3 The structure of $\Phi(p)[2^\infty]$

We begin our study of the nice properties of the error term $b = a^s$ from the last section with the following definition:

Definition 15.2

Let m and n be elements of $\mathbb{N}^*$. We define the *n-torsion subgroup of* $\Phi(m)$, denoted $\Phi(m)[n]$, as follows:

$$\Phi(m)[n] := \{a \in \Phi(m) : a^n = 1\} \tag{386}$$

If q is a prime, we denote by $\Phi(m)[q^\infty]$ the following set

$$\Phi(m)[q^\infty] = \bigcup_{k \geqslant 1} \Phi(m)[q^k] = \left\{a \in \Phi(m) : a^{q^k} = 1 \text{ for some } k \geqslant 1\right\} \tag{387}$$

Remark 15.2

For those that have taken a course in algebra, the subgroup $\Phi(m)[q^\infty]$ is just the Sylow q-subgroup of $\Phi(m)$.

In other words, we see that $\Phi(m)[n]$ is nothing more than $X_f(\mathbb{Z}/m\mathbb{Z})$ where $f(x) = x^n - 1$. Let us note some examples:

Example 15.3

If $m = 8$ and $n = 2$ then

$$\{1, 3, 5, 7\} = \Phi(8)[2] = \Phi(8)[4] = \Phi(8)[8] = \cdots = \Phi(8)[2^\infty] \tag{388}$$

Example 15.4

If $m = 11$ and $n = 5$ one has that

$$\{1, 3, 4, 5, 9\} = \Phi(11)[5] = \Phi(11)[25] = \cdots = \Phi(11)[5^\infty] \tag{389}$$

Example 15.5

If $m = 17$ and $n = 2$ one has that

$$\begin{aligned}
\Phi(17)[2] &= \{1, 16\} \\
\Phi(17)[4] &= \{1, 4, 13, 16\} \\
\Phi(17)[8] &= \{1, 2, 4, 8, 9, 13, 15, 16\} \\
\Phi(17)[16] &= \Phi(17) \\
\Phi(17)[32] &= \Phi(17) \\
&\vdots \\
\Phi(17)[2^\infty] &= \Phi(17)
\end{aligned} \tag{390}$$

The relevance of the torsion subsets of $\Phi(m)$ is the following observation:

Lemma 15.3

Let p be an odd prime and $a \in \Phi(p)$. If we write $p - 1 = 2^v s$ with s odd, then $a^s \in \Phi(p)[2^\infty]$.

In other words, the error term $b = a^s$ for our initial guess of $x = a^{\frac{1}{2}(s+1)}$ of a true square root of a modulo p is an element of $\Phi(p)[2^\infty]$. Thus, we will certainly be interested in understanding the structure of $\Phi(p)[2^\infty]$.

Proof 15.3: Lemma 15.3

It suffices to note that

$$(a^s)^{2^v} = a^{2^v s} = a^{p-1} = 1 \mod p \tag{391}$$

by Corollary 5.5.

So, now that we are convinced that studying $\Phi(p)[2^\infty]$ is interesting, let us begin diving into its fine grain structures. The first elementary observations that hold for any $\Phi(m)[n]$ is the following:

Lemma 15.4

Let m and n be elements of $\mathbb{N}^*$. Then, the following properties hold:

1. $1 \in \Phi(m)[n]$.
2. If $a \in \Phi(m)[n]$ and $b \in \Phi(m)[n]$ then $ab \in \Phi(m)[n]$.
3. If $a \in \Phi(m)[n]$ then $a^{-1} \in \Phi(m)[n]$.
4. An element $a \in \Phi(m)$ is in $\Phi(m)[n]$ if and only if $|a| \mid n$.
5. $\#\Phi(m)[n] = \gcd(\varphi(m), n)$.
6. If $n = q$ is prime, then $a \in \Phi(m)$ is in $\Phi(m)[q^\infty]$ if and only if $|a|$ is a power of q.
7. If $n = q$ is prime, then $\Phi(m)[q^\infty] = \Phi(m)[q^v]$ where $v := v_q(\varphi(m))$.
8. If $m = p$ is prime, then $\Phi(p)[n]$ is cyclic (recall Definition 10.1).
9. Let $q_1, \ldots, q_l$ be the distinct primes dividing m. The map

$$\Phi(m)[q_1^\infty] \times \cdots \times \Phi(m)[q_l^\infty] \to \Phi(m) \tag{392}$$

given by $(x_1, \ldots, x_l) \mapsto x_1 \cdots x_l$ is a bijection.

Proof 15.4

See Exercise 15.2.

Now, Lemma 15.4 part 8. says that the structure of $\Phi(p)[2^\infty]$ cannot be too complicated—it is generated by a single element of $\Phi(p)$. Of course, actually finding such a generator appears, *a priori*, quite complicated. It seems very analogous to finding a primitive root modulo p (and, in fact, looking at the proof of Lemma 15.4 part 8. shows this is not too far from the case). That said, in the specific case of $\Phi(p)[2^\infty]$ things are shockingly simpler.

Namely, we have the following result which jumpstarts the whole Tonelli-Shanks algorithm:

Lemma 15.5

Let p be an odd prime and let $u \in \Phi(p)$ be a non-square (which we know exists by Lemma 12.2). Set $w := u^s$ where $p - 1 = 2^v s$ with s odd. Then, $\Phi(p)[2^\infty] = \langle w \rangle$.

In words this lemma says that finding a generator of $\Phi(p)[2^\infty]$ is no more difficult than finding a non-square modulo p. Doing this is quite quick by a trial-and-error method. Namely, Algorithm 14.1 allows us to check whether a randomly chosen element of $\Phi(p)$ is a non-square and since Lemma 12.2 says that half of $\Phi(p)$ are non-squares, this random choosing method should probabilistically quickly yield a non-square. Thus, in other words, it's algorithmically quite quick and simple to find a generator of $\Phi(p)[2^\infty]$ which is definitely not obvious at first glance.

Proof 15.5: Lemma 15.5

Let us begin by showing that $\langle w \rangle \subseteq \Phi(p)[2^\infty]$. By Lemma 15.4 part 2. it suffices to show that $w \in \Phi(p)[2^\infty]$. But, note that

$$w^{2^v} = u^{2^v s} = u^{p-1} = 1 \mod p \tag{393}$$

by Corollary 5.5 from where the conclusion follows.

To show that $\langle w \rangle \subseteq \Phi(p)[2^\infty]$ is an equality it suffices to show that

$$2^v = \#\Phi(p)[2^v] = \#\Phi(p)[2^\infty] = \#\langle w \rangle = |w| \tag{394}$$

To show that $|w| = 2^v$ we proceed as follows. Let ξ be a primitive root modulo p. We can write $u = \xi^\ell$ for some $\ell \in \{0, \ldots, p-1\}$. Moreover, since u is a non-square we know that ℓ is odd. Now, since $w = u^s = \xi^{s\ell}$ we know by Exercise 6.3 we know that

$$|w| = |\xi^{s\ell}| = \frac{|\xi|}{\gcd(s\ell, |\xi|)} = \frac{p-1}{\gcd(s\ell, p-1)} \tag{395}$$

Now, note that since s and ℓ are odd, so that $s\ell$ is odd, we evidently have that $\gcd(s\ell, p-1) = \gcd(s\ell, s)$ since the power 2^v dividing $p-1$ doesn't affect the greatest common divisor. But, evidently

$\gcd(s\ell, s) = s$. Thus, we see that

$$|w| = \frac{p-1}{\gcd(s\ell, p-1)} = \frac{p-1}{s} = 2^v \tag{396}$$

as desired.

Now, recall that the main thing we were interested in was a reliable way to adjust the initial guess $x = a^{\frac{1}{2}(s+1)}$ to some xc in a way that makes the resulting error term $c^2 b$ have smaller order than the initial guess $b = a^s$. But, now that we know that $b \in \Phi(p)[2^\infty] = \langle w \rangle$ where $w = u^s$ for any non-square u, we can give a reliable method of doing this.

Namely, we have the following basic observation which is the lynchpin in the Tonelli-Shanks algorithm:

Lemma 15.6

Let p be an odd prime and let A and B be elements of $\Phi(p)[2^\infty]$. If $|A| = 2^{r_1}$ and $|B| = 2^{r_2}$ with $r_1 > r_2 > 1$ (so that A and B are both not 1) then $|A^{2^{r_1-r_2}} B| = 2^{r_3}$ with $r_3 < r_2$.

In other words, this tells us that if we have an element B of $\Phi(p^\infty)[2^\infty]$ we can reliably modify its order by multiplying it by a power of another element of $\Phi(p)[2^\infty]$. With a little work this will be precisely the key we need to give a systematic way of iteratively adjusting our initial guess $x = a^{\frac{1}{2}(s+1)}$ to better and better guesses for a true square root of a.

Proof 15.6: Lemma 15.6

It suffices to show that

$$\left(A^{2^{r_1-r_2}} B\right)^{2^{r_2-1}} = 1 \tag{397}$$

since this implies by Lemma 5.5 that $|A^{2^{r_1-r_2}} B| \mid 2^{r_2-1}$ which implies the claim. Note though that

$$\left(A^{2^{r_1-r_2}} B\right)^{2^{r_2-1}} = A^{2^{r_1-1}} \cdot B^{2^{r_2-1}} \tag{398}$$

Since $|A| = 2^{r_1}$ it's not hard to see that $A^{2^{r_1-1}} = -1$ and similarly $B^{2^{r_2-1}} = -1$. Thus,

$$\left(A^{2^{r_1-r_2}} B\right)^{2^{r_2-1}} = A^{2^{r_1-1}} \cdot B^{2^{r_2-1}} = -1 \cdot -1 = 1 \tag{399}$$

as desired.

15.4 The Tonelli-Shanks algorithm

We are now ready to put the above structure results concerning $\Phi(p)[2^\infty]$ to use to give the Tonelli-Shanks algorithm to compute a true square root of a modulo p. Again, the summary idea is the observation if we make an initial guess of a true square root as $x = a^{\frac{1}{2}(s+1)}$ then this is an approximate square root with error $b = a^s$. But, this error term b is in $\Phi(p)[2^\infty]$ and so we can put Lemma 15.6 to use to make an adjustment $x = ca^{\frac{1}{2}(s+1)}$ with $c \in \Phi(p)[2^\infty]$ to obtain an approximate square root with smaller order. Moreover, using Lemma 15.5 we have a complete understanding of $\Phi(p)[2^\infty]$ which will allow us to choose this c quite simply, at least given a non-square u. We will then iteratively repeat this procedure until we end with a true square root.

We formalize this as follows:

Algorithm 15.1: The Tonelli-Shanks algorithm

Inputs: An odd prime p and an element $a \in \Phi(p)$ that has a square root.

Outputs: A true square root x of a modulo p.

Additional data required: The factorization $p-1 = 2^v s$ where s is odd and a non-square u modulo p. Set $w := u^s$.

The algorithm then starts with the following initial data:

Initial data: Set $x = a^{\frac{1}{2}(s+1)}$, $b = a^s$, $g = w$, and $r = v$.

The algorithm then runs as follows:

Step 1: Compute the smallest $k \geqslant 0$ such that $b^{2^k} = 1 \mod p$ (i.e. compute $\log_2 |b|$).

Step 2: If $k = 0$ then terminate the algorithm and output x. Otherwise, proceed to Step 3.

Step 3: Update the values of x, b, g, and r as follows:

$$\begin{aligned} x &\mapsto x g^{2^{r-k-1}} \\ b &\mapsto b g^{2^{r-k}} \\ g &\mapsto g^{2^{r-k}} \\ r &\mapsto k \end{aligned} \tag{400}$$

Return to Step 1.

To make sense of this algorithm, we should first prove the following basic observations:

Lemma 15.7

Let the notation be as in Algorithm 15.1. Then, the following claims are true:

1. At every iteration x is an approximate square root of a with error b.
2. At every iteration $|g| = 2^r$.
3. At every iteration where $k \neq 0$ we have that $k < r$.

Proof 15.7

It suffices, in all cases, to observe that the result holds true for the initial values of x, b, g, and r and that the update procedure in Step 3 of Algorithm 15.1 preserves these properties, from where the claim follows by induction.

1. This is clear for the initial data, so it suffices to prove this is preserved by the updating

procedure. But, note that if $x^2 = ba$ then

$$(xg^{2^{r-k-1}})^2 = x^2 g^{2^{r-k}} = bag^{2^{r-k}} = (bg^{2^{r-k}})a \tag{401}$$

which shows the desired claim.

2. This is clear for the initial data by Lemma 15.5. To show that it's preserved by the updating procedure we note that Exercise 6.3 shows that

$$\left|g^{2^{r-k}}\right| = \frac{|g|}{\gcd(2^{r-k}, |g|)} = \frac{2^r}{\gcd(2^{r-k}, 2^r)} = \frac{2^r}{2^{r-k}} = 2^k \tag{402}$$

from where the claim follows.

3. Note that if there exists an iteration where $k \neq 0$ then we have that $k \neq 0$ for the initial data. To prove the claim there we need to show that $|b| < 2^v$. That said, note that $b = a^s$ is a square since a is a square. Write $b = d^2$ for some $d \in \Phi(p)$. Then, note that

$$|b| = |d^2| = \frac{|d|}{\gcd(2, |d|)} \tag{403}$$

Now, since $b \neq 1$ (since $k \neq 0$) and $b \in \Phi(p)[2^\infty]$ we have that $2 \mid |b|$ which implies that $2 \mid |d|$ by (403). But, this then implies that $\gcd(2, |d|) = 2$ and so $|b| = \frac{1}{2}|d|$. In particular, if $|b| = 2^v$ then this implies that $|d| = 2^{v+1}$ which is impossible since $|d| \mid p - 1$. The induction step for this claim then follows from Lemma 15.6.

From this, we deduce the following:

Corollary 15.1

Algorithm 15.1 terminates in at most v steps and outputs a true square root of a.

Let us see this algorithm in practice:

Example 15.6

Let's use the Tonelli-Shanks algorithm to compute the solutions to $x^2 = 2 \mod 41$. Note that $41 = 1 \mod 8$ so we can't apply either Lemma 15.1 or Lemma 15.2. Thus, we apply Algorithm 15.1.

To do this we need to begin by finding a non-square modulo 41. Clearly 1 doesn't work, and since $p = 1 \mod 8$ we can use Theorem 12.5 to see that 2 is also not going to work. For 3 we use Theorem **??** to compute $\left(\frac{3}{41}\right)$. Namely, since $41 \mod 1 \mod 4$ we know that $\left(\frac{3}{41}\right) = \left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = -1$. Thus, 3 is a non-square modulo 41.

Next we need to write $41 - 1 = 2^v s$ with s odd. It's clear that this done as $40 = 2^3 \cdot 5$. Thus, $v = 3$ and $s = 5$.

We now start with our initial values $x = 2^{\frac{1}{2}(5+1)} = 8$, $b = 2^5 = 32 \mod 41$, $g = 3^5 = 38 \mod 41$, and $r = 3$.

We now start the algorithm. For the first iteration we need to compute $k = \log_2 |32|$. One can quickly check that this is $k = 2$. Since $k \geqslant 0$ we then update our values of x, b, g, and $r = 3$ as $x = 8 \cdot 38^{2^{3-2}-} = 17 \mod 41$, $b = 32 \cdot 3^{2^{3-2}} = 1 \mod 41$, $g = 38^{2^{3-2}} = 9$, and $r = 2$.

Now for the next iteration, since $b = 1$ we see that we terminate and we output $x = 17$ as our answer.

Example 15.7

Let us now compute the solutions to $x^2 = 7 \mod 113$. Note that $113 = 1 \mod 8$, so we cannot use Lemma 15.1 or Lemma 15.2. Thus, we use Algorithm 15.1.

To do this we need to start by finding a non-square modulo 113. Again, clearly 1 and 2 don't work. Let us note that

$$\left(\frac{3}{113}\right) = \left(\frac{113}{3}\right) = \left(\frac{2}{3}\right) = -1 \tag{404}$$

and so 3 is a non-square.

Next we need to write $113 - 1 = 2^v s$ with s odd. It's clear that this is $112 = 2^4 \cdot 7$ and thus $v = 4$ and $s = 7$.

We thus start with the initial values of $x = 7^{\frac{1}{2}(7+1)} = 28 \mod 113$, $b = 7^7 = 112 = -1 \mod 113$, $g = 3^7 = 40 \mod 41$, and $r = 4$.

We thus begin the first step of the first iteration of the algorithm by computing $\log_2 |-1|$ which is clear 1. Thus, we update the values of x, b, g, and r as follows. $x = 28 \cdot 40^{2^{4-1-1}} = 32$, $b = -1 \cdot 40^{(2^{4-1})} = 1 \mod 41$, $g = 40^{2^{4-1}} = -1$, and $r = 1$.

At the next iteration we see that $b = 1$ and thus we terminate and output $x = 32$ as a true square root of 7.

15.5 Exercises

Exercise 15.1

Problem: Let m be an element of $\mathbb{N}^*$ and a and b elements of $\Phi(m)$. Show that if $\gcd(|a|, |b|) = 1$ then $|ab| = |a||b|$.

Exercise 15.2

Problem: Prove Lemma 15.2.

16 Lecture 16: Equations modulo p and consecutive squares

16.1 Setup

One thing one can learn from much of what we have discussed so far concerning modulus Diophantine equations is that in the study of equations modulo p a sharp line in the sand is drawn between understanding $\#X_f(\mathbb{Z}/p\mathbb{Z})$ and explicitly understanding $X_f(\mathbb{Z}/p\mathbb{Z})$. Let us give some examples:

- Theorem 6.3 tells us that if $f(x) = x^n - a$ then $\#X_f(\mathbb{Z}/p\mathbb{Z}) = \gcd(n, p-1)$. To actually parametrize $X_f(\mathbb{Z}/p\mathbb{Z})$ one needs to run the full gambit of Theorem 11.1.

- Theorem 9.1 tells us that if $0 \neq f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ and $\deg(f) = n$ then $\#X_f(\mathbb{Z}/p\mathbb{Z}) \leqslant n$. To actually parametrize $X_f(\mathbb{Z}/p\mathbb{Z})$ is impossible without more information.
- Theorem 12.1 and Theorem 14.3 gives us an essentially complete understanding of $\#X_f(\mathbb{Z}/p\mathbb{Z})$ in a beautiful, concise way when $f(x) = x^2 - a$ (or, more generally, for a single variable quadratic polynomial). To actually parametrize $X_f(\mathbb{Z}/p\mathbb{Z})$ one needs to utilize something like Algorithm 15.1.

In all of these cases we see a general theme: structural properties of f (e.g. it's degree, how many terms it has, ...) affect $\#X_f(\mathbb{Z}/p\mathbb{Z})$ in a fairly straightforward way. It is this property that one loses when trying to explicitly parametrize $X_f(\mathbb{Z}/p\mathbb{Z})$—such a result cannot be of the structural nature concerning results of $\#X_f(\mathbb{Z}/p\mathbb{Z})$ but is necessarily of a more algorithmic nature.

We thus start today a goal of trying to understand how we can generalize the examples in the above list to give results of the desired form "structural result of f naturally affects $\#X_f(\mathbb{Z}/p\mathbb{Z})$". Note that this is reasonable, since one of our main goals, as expounded in the first lecture, is to give (in some cases) an algorithmic understanding of when $X_f(\mathbb{Z}) \neq \varnothing$ (i.e. the Diophantine equation $f(x) = 0$ has solutions). We have seen that a powerful way to try to understand the question of whether $X_f(\mathbb{Z}) \neq \varnothing$ is to understand when $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for a prime p. This, of course, is equivalent to $\#X_f(\mathbb{Z}/p\mathbb{Z}) \neq 0$. So, point counting will be valuable in our study of Diophantine equations.

Today we will focus mostly on a very basic case, of computing $\#X_g(\mathbb{Z}/p\mathbb{Z})$ when $g(x, y) = y^2 - f(x)$ (i.e. understanding the number of solutions to $y^2 = f(x)$ over $\mathbb{Z}/p\mathbb{Z}$) for some $f(x) \in \mathbb{Z}[x]$.

16.2 Distribution of squares modulo p

To prime ourselves for our general study of $\#X_f(\mathbb{Z}/p\mathbb{Z})$, for more general f, we begin with a natural example of where such a computation naturally comes up in the context of understanding the squares in $\mathbb{Z}/p\mathbb{Z}$. Namely, one can recall before, from Corollary 12.2 that the set of non-zero squares modulo p and the set non-zero non-squares modulo p are of equal size: they both have size $\dfrac{p-1}{2}$. This naturally leads one to wonder what the distribution of the squares/non-squares in $\mathbb{Z}/p\mathbb{Z}$ is.

For example, an incredibly naive guess might be that the squares and non-squares are interleaved. So, for example, you might imagine that if $x \in \mathbb{Z}/p\mathbb{Z}$ is a square, then maybe $x + 1$ is a non-square, and then $x + 2$ is a square, etc. Of course, this is too naive to work. For example, if $p = 7$ then one can check that 1 is a square and so is $2 = 1 + 1$. But, while this naive guess is certainly not correct, understanding to what extent it fails in and of itself gives one an interesting insight into the distribution of squares and non-squares in $\mathbb{Z}/p\mathbb{Z}$.

Thus, we would like to understand the following question:

Question 16.1

Let p be a prime. What number of $0 \neq x$ in $\mathbb{Z}/p\mathbb{Z}$ satisfy that x and $x + 1$ are both squares? What number of $0 \neq x$ in $\mathbb{Z}/p\mathbb{Z}$ satisfy that $0 \neq x$ satisfy that x and $x + 1$ are both non-squares?

Using the Legendre symbol, we might edulcerate this question as follows:

Question 16.2

Let p be a prime. What number of x in $\mathbb{Z}/p\mathbb{Z}$ satisfy $\left(\dfrac{x}{p}\right) = \left(\dfrac{x+1}{p}\right) = 1$. What number of x in $\mathbb{Z}/p\mathbb{Z}$ satisfy $\left(\dfrac{x}{p}\right) = \left(\dfrac{x+1}{p}\right) = -1$.

Intuitively the answer should be something close to $\frac{p-1}{4}$ in both cases. Indeed, assuming that $\left(\frac{x}{p}\right) = 1$ and $\left(\frac{x+1}{p}\right) = 1$ are independent events (in the sense of probability) one would expect that the probability that $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1$ is the product of the probabilities that $\left(\frac{x}{p}\right) = 1$ and $\left(\frac{x+1}{p}\right) = 1$. But, Theorem 12.2 implies that both of these have probability $\frac{1}{2}$ in $\Phi(p)$ so that the probability that $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1$ is $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. Thus, there should be about $\frac{p-1}{4}$ many x such that $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1$.

Of course, this cannot be quite correct since it implies, for example, that $p = 1 \mod 4$. But, even in this case things needn't be so simple:

Example 16.1

If $p = 5$ then the set of x such that $\left(\frac{x}{5}\right) = \left(\frac{x+1}{5}\right) = 1$ is empty and is thus not $\frac{5-1}{4} = 1$.

So, to try and actually answer the question, we need to work a little harder. To begin, we start with a simpler question:

Question 16.3

How many $x \in \mathbb{Z}/p\mathbb{Z}$ satisfy $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right)$?

From there we can try answer the more specific Question 16.1 and Question 16.2. But, assuming that neither x nor $x+1$ is a square, we see that $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right)$ is equivalent to $\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = \left(\frac{x(x+1)}{p}\right) = 1$. Indeed, if $x \neq 0, -1$ (so that neither x nor $x+1$ is zero) we have that $\left(\frac{x}{p}\right) \neq \left(\frac{x+1}{p}\right)$ if and only if one of the Legendre symbols is 1 and the other is -1 so that the product is -1. So, in essence, we are trying to find for how many x does $\left(\frac{x(x+1)}{p}\right) = 1$. Or, in other words, we want to see for how many $x \in \mathbb{Z}/p\mathbb{Z}$ does $y^2 = x(x+1)$ have a solution.

In summary we see the following:

Observation 16.1

To answer Question 16.3 is essentially the same as computing $\#X_f(\mathbb{Z}/p\mathbb{Z})$ where $f(x,y) := y^2 - x(x+1)$.

Thus, we see that understanding Question 16.1 and Question 16.2 come down, at least in part, to understanding the number of solutions to an equation modulo p. Thus, it would be desirable to have a general method to count such solutions. We begin today to discuss our general methodology, but before we do let us at least fully answer Question 16.1 and Question 16.2.

To begin let's set

$$X := \left\{x \in \Phi(p) : \left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1\right\} \tag{405}$$

and

$$Y := \left\{x \in \Phi(p) : \left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = -1\right\} \tag{406}$$

We can then clarify the relationship between the quantities we wish to compute (i.e. $\#X$ and $\#Y$) and $\#X_f(\mathbb{Z}/p\mathbb{Z})$ as follows. As we've already observed, note that $(x,y) \in X_f(\mathbb{Z}/p\mathbb{Z})$, with $x \neq 0, -1$, if and only if

$$1 = \left(\frac{x(x+1)}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) \tag{407}$$

which is equivalent to $\left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right)$. But, as long $x \neq 0, -1$ we then see that this means that $(x,y) \in X_f(\mathbb{Z}/p\mathbb{Z})$ if and only if $x \in X \cup Y$. Moreover, if $x \in X \cup Y$ we see that there will be precisely 2-elements of $X_f(\mathbb{Z}/p\mathbb{Z})$ with first coordinate x: if (x,y) is one, the other is $(x,-y)$. Thus, all in all we see that

$$\#X_f(\mathbb{Z}/p\mathbb{Z}) = 2 + 2\#(X \cup Y) = 2 + 2\#X + 2\#Y \tag{408}$$

Note here that 2 came from the solutions when $x = 0$, which only has the solution $(0,0)$, and when $x = -1$ which only has the solution $(-1,0)$. Thus, it suffices to find $\#X_f(\mathbb{Z}/p\mathbb{Z})$ to find $\#X + \#Y$.

We will understand a 'better way' of computing $\#X_f(\mathbb{Z}/p\mathbb{Z})$ in the next lecture, but for now we can attempt this computation using Legendre symbols. Namely, note that

$$\#X_f(\mathbb{Z}/p\mathbb{Z}) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(1 + \left(\frac{x(x+1)}{p}\right)\right) = p + \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x(x+1)}{p}\right) \tag{409}$$

Indeed, for each given $x \in \mathbb{Z}/p\mathbb{Z}$ we see that the set of elements of $X_f(\mathbb{Z}/p\mathbb{Z})$ with first coordinate x (i.e. how many y's in $\mathbb{Z}/p\mathbb{Z}$ there are such that $y^2 = x(x+1)$) will be $1 + \left(\frac{x(x+1)}{p}\right)$. We can then, in fact, exploit the symmetry of $\mathbb{Z}/p\mathbb{Z}$ to compute this sum of Legendre symbols.

We begin by observing that if $x = 0, -1$ we have that $\left(\frac{x(x+1)}{p}\right) = 0$. Thus,

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x(x+1)}{p}\right) = \sum_{x=1}^{p-2} \left(\frac{x(x+1)}{p}\right) \tag{410}$$

Now, if $x \in \{1, \ldots, p-2\}$ we see that

$$\left(\frac{x(x+1)}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = \left(\frac{x^{-1}}{p}\right)\left(\frac{x+1}{p}\right) = \left(\frac{x^{-1}(x+1)}{p}\right) = \left(\frac{1+x^{-1}}{p}\right) \tag{411}$$

where $\left(\frac{x}{p}\right) = \left(\frac{x^{-1}}{p}\right)$ by Lemma 12.1. Thus, we see that

$$\sum_{x=1}^{p-2} \left(\frac{x(x+1)}{p}\right) = \sum_{x=1}^{p-2} \left(\frac{1+x^{-1}}{p}\right) \tag{412}$$

Now, we really want to exploit that $x \mapsto x^{-1}$ is a symmetry so that we can try to meaningfully reindex this sum to involve x and not x^{-1}. Now, while $x \mapsto x^{-1}$ is actually a symmetry of $\{1, \ldots, p-2\}$ it's much more naturally a symmetry of $\Phi(p)$. Thus, to exploit the symmetry $x \mapsto x^1$ we're going to add in the missing term when $x = p-1$ which, of course, necessitates also subtracting this term. In other words

$$\sum_{x=1}^{p-2} \left(\frac{1+x^{-1}}{p}\right) - \left(\frac{1+(-1)^{-1}}{p}\right) = \sum_{x=1}^{p-2} \left(\frac{1+x}{p}\right) \tag{413}$$

where the last equality follows since $1 + (-1)^{-1} = 0$.

To compute this last sum, we merely observe that $x \mapsto x+1$ is a symmetry of $\mathbb{Z}/p\mathbb{Z}$, so to take advantage of this we want to change the range of the indices from $x \in \{1, \ldots, p-2\}$ to $x \in \{0, \ldots, p-1\}$ and so to

do this we have add/subtract the missing terms $\left(\frac{1+x}{p}\right)$ when $x=0$ and when $x=p-1$. Now, note that when $x=0$ this is $\left(\frac{0+1}{p}\right)=\left(\frac{1}{p}\right)=1$ and when $x=p-1$ this is $\left(\frac{1+p-1}{p}\right)=\left(\frac{p}{p}\right)=0$. So

$$\begin{aligned}\sum_{x=1}^{p-2}\left(\frac{1+x}{p}\right) &= \sum_{x=0}^{p-1}\left(\frac{1+x}{p}\right)-1\\ &= \sum_{x\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{1+x}{p}\right)-1\\ &= \sum_{x\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{x}{p}\right)-1\\ &= \sum_{x=0}^{p-1}\left(\frac{x}{p}\right)-1\end{aligned} \tag{414}$$

and we have already computed this sum in the last term to be zero in Exercise 13.2 which, one should note, we did by relating it to the solutions to an equation. Thus, finally, we deduce that

$$\#X_f(\mathbb{Z}/p\mathbb{Z}) = p+\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{x(x+1)}{p}\right)=p-1 \tag{415}$$

and thus

(416)

p-1=2+2# X+2# Y using (408).

So, if we want to determine $\#X$ and $\#Y$ it now suffices to compute $\#X-\#Y$. To do this, we can compute another sum of Legendre symbols to find the right answer. Namely, let us set

$$Z=\{x\in\{1,\ldots,p-2\}:\left(\frac{x}{p}\right)\neq\left(\frac{x+1}{p}\right)\} \tag{417}$$

Note then that for $a\in\{1,\ldots,p-2\}$ we have the following:

$$\left(\frac{a}{p}\right)+\left(\frac{a+1}{p}\right)=\begin{cases}2 & \text{if} \quad a\in X\\ -2 & \text{if} \quad a\in Y\\ 0 & \text{if} a\in Z\end{cases} \tag{418}$$

since $\mathbb{Z}/p\mathbb{Z}=\{0,p-1\}\sqcup X\sqcup Y\sqcup Z$ we deduce that

$$\begin{aligned}\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\left(\left(\frac{x}{p}\right)+\left(\frac{x+1}{p}\right)\right) &= \left(\left(\frac{0}{p}\right)+\left(\frac{1}{p}\right)\right)+\left(\left(\frac{p-1}{p}\right)+\left(\frac{0}{p}\right)\right)+2\#X-2\#Y+0\#Z\\ &= 1+\left(\frac{-1}{p}\right)+2\#X-2\#Y\end{aligned} \tag{419}$$

But, we have already computed that

$$\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{x}{p}\right)=\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{x+1}{p}\right)=0 \tag{420}$$

so that we deduce

$$0=1+\left(\frac{-1}{p}\right)+2\#X-2\#Y \tag{421}$$

or, equivalently,

$$\#X - \#Y = \frac{-1}{2}\left(1 + \left(\frac{-1}{p}\right)\right) \tag{422}$$

by simple calculation

Thus, we see that we have the following simultaneous equations for $\#X$ and $\#Y$:

$$\begin{cases} \#X - \#Y = \dfrac{-1}{2}\left(1 + \left(\dfrac{-1}{p}\right)\right) \\ \#X + \#Y = \dfrac{p-3}{2} \end{cases} \tag{423}$$

which has the solution

$$\#X = \frac{1}{4}\left(p - 4 - \left(\frac{-1}{p}\right)\right), \qquad \#Y = \frac{1}{4}\left(p - 2 + \left(\frac{-1}{p}\right)\right) \tag{424}$$

which, while not the most elegant formula in the world, is certainly quite succinct.

Let us now think about what this means for our original question. Namely, we asked to what extent the naive belief that the squares and non-squares of $\mathbb{Z}/p\mathbb{Z}$ interlace holds. Note that this does <u>not</u> hold for a given x, i.e. that x and $x+1$ have different 'squareness', if either $x = 0$, $x \in X$, $x \in Y$, or $x = -1$ assuming that $p = 1 \mod 4$. Thus, we see that the set of x that satisfy this naive belief is

$$p - 1 - \#X - \#Y + \delta_p \tag{425}$$

where

$$\delta_p = \begin{cases} 1 & \text{if} \quad p = 1 \mod 4 \\ 0 & \text{if} \quad p = 3 \mod 4 \end{cases} \tag{426}$$

or, simplifying this expression using (424)

$$\frac{p+1}{2} + \delta_p \tag{427}$$

Thus, asymptotically, about half of the elements of $\mathbb{Z}/p\mathbb{Z}$ satisfy the naive guess that the squares and non-squares interleaf.

16.3 Equations and sums of Legendre symbols

In the last section we not only saw that the natural question of how often the square and non-square are interleaved involved finding $\#X_g(\mathbb{Z}/p\mathbb{Z})$ for a choice g, but we also saw that, in good situations, we can relate $\#X_g(\mathbb{Z}/p\mathbb{Z})$ to an explicit sum of Legendre symbols. We would like then to formalize this observation. Throughout this section, let p be an odd prime.

To begin, we make the following definition:

Definition 16.1

Let p be a prime and $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. Then, we define the quantity $S(f) \in \mathbb{Z}$ as follows:

$$S(f) := \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{f(x)}{p}\right) \tag{428}$$

We then have the following elementary observation:

Lemma 16.1

Let p be a prime and $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. Set $g(x,y) := y^2 - f(x)$. Then,

$$\#X_g(\mathbb{Z}/p\mathbb{Z}) = p + S(f) \tag{429}$$

Proof 16.1

As noted before, for a given $x \in \mathbb{Z}/p\mathbb{Z}$ the equation $y^2 = f(x)$ has $1 + \left(\frac{f(x)}{p}\right)$ many solutions. So, as x varies over $\mathbb{Z}/p\mathbb{Z}$ we see that

$$\#X_g(\mathbb{Z}/p\mathbb{Z}) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(1 + \left(\frac{f(x)}{p}\right)\right) = p + \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{f(x)}{p}\right) = p + S(f) \tag{430}$$

as desired.

Let us give some examples:

Example 16.2

As we have already seen in the previous section, if p is any odd prime and $g(x,y) = y^2 - x(x+1)$ then $\#X_g(\mathbb{Z}/p\mathbb{Z}) = p - 1$ so that $S(f) = -1$ where $f(x) = x(x+1)$.

Example 16.3

Let p be an odd prime. Let us compute $\#X_g(\mathbb{Z}/p\mathbb{Z})$ where $g(x,y) = x^2 + y^2 - 1$. By Lemma 16.1 it suffices to compute $S(f(x))$ where $f(x) = 1 - x^2$. To do this, we make the following tricky observation:

$$\begin{aligned} S(f) &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{f(x)}{p}\right) \\ &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{1-x^2}{p}\right) \\ &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{-(x^2-1)}{p}\right) \\ &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{-1}{p}\right)\left(\frac{x^2-1}{p}\right) \\ &= \left(\frac{-1}{p}\right) \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x^2-1}{p}\right) \\ &= \left(\frac{-1}{p}\right) S(h) \end{aligned} \tag{431}$$

where $h(x) = x^2 - 1$. But, by Lemma 16.1 we know that $\#X_\rho(\mathbb{Z}/p\mathbb{Z}) = p + S(h)$ where $\rho(x,y) = y^2 - x^2 + 1$.

But, we can compute $\#X_\rho$ explicitly. Namely, $\rho(x,y) = 0$ is the same thing as $x^2 - y^2 = 1$ which is the same as $(x-y)(x+y) = 1$. To solve this we merely note that $x - y$ can be any unit u and then $x + y$ is then just u^{-1}. So, the number of solutions to this equation is the number of units in $\mathbb{Z}/p\mathbb{Z}$

which is $p-1$. So, we see that $\#X_\rho = p-1$ and so $p+S(h) = p-1$ which says that $S(h) = -1$. Thus, we see that $S(f) = -\left(\frac{-1}{p}\right)$ and thus $\#X_g(\mathbb{Z}/p\mathbb{Z}) = p - \left(\frac{-1}{p}\right)$.

Example 16.4

Let p be an odd prime. Let us compute $\#X_g(\mathbb{Z}/p\mathbb{Z})$ where $g(x,y) = y^2 - x^2 + x$. By Lemma 16.1 we need to compute $S(f)$ where $f(x) = x^2 - 2x$. This is very similar to the computation we did in §16.2. Namely we observe that $\left(\frac{f(0)}{p}\right) = 0$ so that

$$\begin{aligned}
S(f) &= \sum_{x=1}^{p-1}\left(\frac{f(x)}{p}\right) + \left(\frac{f(0)}{p}\right) \\
&= \sum_{x=1}^{p-1}\left(\frac{x^2-2x}{p}\right) \\
&= \sum_{x=1}^{p}\left(\frac{x(x-2)}{p}\right) \\
&= \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x-2}{p}\right) \\
&= \sum_{x=1}^{p-1}\left(\frac{x^{-1}}{p}\right)\left(\frac{x-2}{p}\right) \\
&= \sum_{x=1}^{p-1}\left(\frac{x^{-1}(x-2)}{p}\right) \\
&= \sum_{x=1}^{p-1}\left(\frac{1-2x^{-1}}{p}\right) \\
&= \sum_{x=1}^{p}\left(\frac{1-2x}{p}\right) \\
&= \left(\frac{-2}{p}\right)\sum_{x=1}^{p-1}\left(\frac{x-2^{-1}}{p}\right) \\
&= \left(\frac{-2}{p}\right)\left(\sum_{x=1}^{p}\left(\frac{x-2^{-1}}{p}\right) - \left(\frac{-2^{-1}}{p}\right)\right) \\
&= \left(\frac{-2}{p}\right)\left(\sum_{x=1}^{p}\left(\frac{x}{p}\right) - \left(\frac{-2^{-1}}{p}\right)\right) \\
&= \left(\frac{-2}{p}\right)\left(0 - \left(\frac{-2^{-1}}{p}\right)\right) \\
&= -1
\end{aligned} \tag{432}$$

So that $\#X_g(\mathbb{Z}/p\mathbb{Z}) = p + S(f) = p - 1$.

These examples all suggest a somewhat peculiar picture. Namely, these examples intimate that if $f(x)$ is quadratic and $g(x,y) := y^2 - f(x)$ then $\#X_g(\mathbb{Z}/p\mathbb{Z}) = p + \varepsilon$ where ε is a quantity satisfying $|\varepsilon| \leqslant 1$

(or equivalently $\varepsilon \in \{-1, 0, 1\}$ since $\varepsilon \in \mathbb{Z}$). Moreover, with an eye towards Example 16.3, maybe ε has something to do with a specific Legendre symbol.

Of course, Lemma 16.1 has given form to this 'error term' ε since we can clearly see that $\varepsilon = S(f)$. Thus, we see that we are equivalently noting that for quadratic f we seem to have that $|S(f)| \leqslant 1$ and, perhaps, $S(f)$ has something to do with a specific Legendre symbol.

Of course, one needs to put some conditions on $f(x)$, besides being quadratic, to try and formulate a correct statement as the following silly examples show:

Example 16.5

Let p be an odd prime and set $f(x) := x^2$. Then, evidently $S(f) = p - 1$ and so if $g(x, y) := y^2 - f(x)$ then $\#X_g(\mathbb{Z}/p\mathbb{Z}) = 2p - 1$.

Example 16.6

Let p be a prime such that $p = 3 \mod 4$. Set $f(x) := -x^2$. Then, evidently $S(f) = 1 - p$. Indeed, if $x \neq 0$ then $f(x) = -x^2$ is non-zero and a non-square since $\left(\frac{-x^2}{p}\right) = \left(\frac{-1}{p}\right) = -1$. Thus, $S(f) = 0 - (p - 1) = 1 - p$. Thus, if $g(x, y) := y^2 + x^2$then $\#X_g(\mathbb{Z}/p\mathbb{Z}) = 1$ (the only solution being $(x, y) = (0, 0)$).

But, we somehow would like to think of examples like $f(x) = x^2$ and $f(x) = -x^2$ as being 'degenerate' in some sense since it's sort of a 'degenerate quadratic'.

Thus, we make the following conjecture, which we pose in the form of a question:

Question 16.4

Let p be an odd prime and $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ a quadratic polynomial. Set $g(x, y) := y^2 - f(x)$. Then, except in 'degenerate cases' does $\#X_g(\mathbb{Z}p\mathbb{Z}) = p + \varepsilon$ with $|\varepsilon| \leqslant 1$? Equivalently, if $f(x)$ is 'not degenerate' is $|S(f)| \leqslant 1$ and maybe have something to do with a Legendre symbol?

Note that this conjecture posits something incredibly interesting besides an understanding on the size of the solution sets of certain equations. Namely, the claim that $|S(f)| \leqslant 1$ if $f(x)$ is (a 'non-degenerate') quadratic essentially says that if $f(x)$ is (a 'non-degenerate') quadratic then $f(x)$ will be a square essentially half of the time. More specifically, if we write

$$N(f) = \#\{x \in \mathbb{Z}/p\mathbb{Z} : f(x) \text{ is a non-zero square}\} \tag{433}$$

and

$$M(f) = \#\{x \in \mathbb{Z}/p\mathbb{Z} : f(x) \text{ is not a square}\} \tag{434}$$

then

$$S(f) = N(f) - M(f) \tag{435}$$

Thus, the claim that for ('non-degenerate') quadratic polynomials $f(x)$ we have that $|S(f)| \leqslant 1$ says that $N(f)$ and $M(f)$ are at most 1 apart.

Again, this is somewhat intuitively obvious. If we take $f(x) = x^2 + x$ then 'should' $f(x)$ be a square for some given x? Well, there is no obvious reason that it should be a square, and there is no obvious reason that it shouldn't. So, a naive guess might be that the probability that $f(x)$ is a square is roughly $\frac{1}{2}$ and the

probability that $f(x)$ is a non-square is roughly $\frac{1}{2}$. Thus, one expects that $S(f) = N(f) - M(f)$ 'should' be small, but it's really non-obvious how to prove this—how to rigorously answer Question 16.4.

The main goal of the next lecture will be to introduce some infrastructure that will allow us to precisely formulate Question 16.4 (i.e. rigorously define 'non-degenerate') and then show that the question has an affirmative answer.

17 Lecture 17: Homogenous polynomials, projective space, and projective equations

17.1 Setup

As stated at the end of the last lecture, we would like to introduce an idea which allow us to rigorously answer Question 16.4 in the affirmative. This idea is the notion of *projective equations*. The notion of projective equations is deceptively powerful. They fulfill all the following roles:

- At a first, practical level, we will see that they serve to reduce redundancy in the sets $X_f(R)$ (for R being $\mathbb{Z}$, or $\mathbb{Z}/m\mathbb{Z}$, or $\mathbb{Q}$, or...) for special types of polynomials f known as *homogenous*.
- At a slightly more theoretical level, we will see the thinking of projective equations allows us to relate the solution sets of various polynomials by thinking of them jointly as making up a single projective equation. This will be the key to answering Question 16.4.
- At a very theoretical level, which we will not really encounter in this course, projective equations provide natural 'compactifications' or 'completions' of the solution sets we have so far encountered.

Projective equations will also be helpful in the next lecture to try and consolidate our thoughts concerning the notion of 'local-to-global principles' for homogenous equations.

17.2 Motivation

Before we dive into the rigorous definition of projective space and projective equations, it will be helpful to have some motivation. We decline to give a highfalutin motivation for them and, instead, appeal to a procedure that the reader has almost certainly implicitly applied before in their mathematical life.

In our discussion of Diophantine equations, it has always been very important that we restrict ourselves to Diophantine solutions (i.e. solutions in $\mathbb{Z}$) versus rational solutions (i.e. solutions in $\mathbb{Q}$). Of course, every Diophantine solution is a rational solution, but certainly not vice versa. In fact, one can have no Diophantine solutions but have rational solutions.

Let us give some examples to illustrate the difference:

Example 17.1

The Diophantine equation $2x - 1 = 0$ has no Diophantine solution (since $2 \nmid 1$) but has a rational solution ($x = \frac{1}{2}$).

Example 17.2

For a less trivial example we can consider the Diophantine equation $f(x, y) = 0$ where $f(x, y) := x^2 - y^2 - 2$. We claim that $X_f(\mathbb{Z}) = \varnothing$ but $X_f(\mathbb{Q})$ is infinite.

To see this first claim it suffices to show that $X_f(\mathbb{Z}/4\mathbb{Z}) = \varnothing$. That said, it's not hard to see that the squares in $\mathbb{Z}/4\mathbb{Z}$ are 0 and 1. Thus, there is no solution to $x^2 - y^2 = 2 \mod 4$ since there is no way to write 2 as a difference of two elements of $\{0, 1\}$ modulo 4.

Let us now show that $X_f(\mathbb{Q})$ is infinite. In fact, we will show that $X_f(\mathbb{Q})$ is naturally in bijection

with the set $\mathbb{Q}-\{0\}$ of non-zero rational numbers. To do this, observe that $x^2-y^2=2$ factors as $(x-y)(x+y)=2$. Note that 2 is invertible (i.e. has multiplicative inverse) in $\mathbb{Q}$. Thus, it's clear that if $(x-y)(x+y)=2$ then $u:=x-y$ is a unit in $\mathbb{Q}$ (i.e. has multiplicative inverse, i.e. is non-zero) and $x+y$ is then just $2u^{-1}$. Thus, it's not hard to see that there is a bijection

$$X_f(\mathbb{Q})\to M:=\left\{u\in\mathbb{Q}-\{0\}:x-y=u \text{ and } x+y=2u^{-1} \text{ for some } x,y\in\mathbb{Q}\right\} \tag{436}$$

Note that, of course, $M\subseteq\mathbb{Q}-\{0\}$. We claim that this inclusion is actually an equality. In fact, we claim that for any $u\in\mathbb{Q}-\{0\}$ there exists unique $x,y\in\mathbb{Q}$ such that $x-y=u$ and $x+y=2u^{-1}$. To see this we merely write these two equations as a matrix equation

$$\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}u\\ 2u^{-1}\end{pmatrix} \tag{437}$$

The fact that this has a unique solution in $\mathbb{Q}^2$ then follows from the observation that $\det\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}=2\neq 0$ and thus $\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$ is invertible.

This is, in general, quite unfortunate. If we were able to study $X_f(\mathbb{Z})$ in a systematic way using $X_f(\mathbb{Q})$ we could take advantage of many of the nice properties of $\mathbb{Q}$ that don't exist in $\mathbb{Z}$ (first and foremost the ability to perform divisions). Unfortunately, as the above examples show, there can't be a straightforward way to study the subset $X_f(\mathbb{Z})$ of $X_f(\mathbb{Q})$ in general since, of course, $X_f(\mathbb{Z})$ can be empty and $X_f(\mathbb{Q})$ huge.

That said, there are certain types of Diophantine equations for which the distinction between Diophantine solutions and rational solutions is not so important. For example, consider the Diophantine equation

$$x^2-3y^2+2z^2=0 \tag{438}$$

It's not clear if this has a Diophantine solution, or even a rational solution, but what is clear is that unlike the previous examlpes if we have one of the former we will certainly have one of the latter. Namely, let's take a triple of rational numbers (x,y,z) and write it as $(x,y,z)=\left(\frac{a_1}{b_1},\frac{a_2}{b_2},\frac{a_3}{b_3}\right)$ where a_i and b_j are integers and we have written the fractions in lowest terms (i.e. $\gcd(a_i,b_i)=1$). Note then that by multiplying through by $(b_1b_2b_3)^2$ shows that

$$x^2-3y^2+2z^2=0\iff(a_1b_2b_3)^2-3(a_2b_1b_3)^2+2(a_3b_1b_2)^2=0 \tag{439}$$

In other words, we see that any rational solution $(x,y,z)=\left(\frac{a_1}{b_1},\frac{a_2}{b_2},\frac{a_3}{b_3}\right)$ would automatically produce a Diophantine solution $(a_1b_2b_3,a_2b_1b_3,a_3b_1b_2)$.

The key point here was that because all the terms in $x^2-3y^2+2z^2$ were squares we could multiply through by the product of the denominators of x,y and z squared and thus cancel the denominators. If we had instead been working with $x^3-3y^3+2z^3$ we could have done the exact same thing but instead of multiplying through by $(b_1b_2b_3)^3$. In fact, what one sees is that the only relevant thing here was that all the terms had the same exponent. The notion of a *homogenous polynomial* just generalizes this idea of being a sum of terms 'with the same exponent'.

So, for a homogenous polynomial there is a clear connection between Diophantine solutions and rational solutions obtained by the procedure of 'clearing denominators'. Of course, the rational solutions will, in general, be larger than the Diophantine solutions. For example, going back to (439) we see that if $(x,y,z)=\left(\frac{a_1}{b_1},\frac{a_2}{b_2},\frac{a_3}{b_3}\right)$ is a solution, then so is $(a_1b_2b_3,a_2b_1b_3,a_3b_1b_2)$ and, in general, they will be distinct solutions. That said, one is tempted to say that they aren't really 'different' solutions since they just differ by clearing denominators and so really shouldn't constitute distinct solutions.

The idea of projective space, and of projective equations, is to try to formalize the idea of identifying two solutions to a homogenous equation that differ by 'clearing denominators' (i.e. differ by scalar multiplication). Once we do this, we will be able to give a full systematic way in which $X_f(\mathbb{Z})$ and $X_f(\mathbb{Q})$ relate, and use

this to compute $X_f(\mathbb{Z})$ for interesting Diophantine equations using the methods that exist over $\mathbb{Q}$ (but not over $\mathbb{Z}$). For example, we will be able to describe $X_f(\mathbb{Z})$ for $f(x,y,z) := x^2 + y^2 - z^2$—we will be able to solve the degree 2 Fermat equation.

Another upshot to the idea of projective equations is that it allows us to relate in a somewhat non-trivial manner various ostensibly disparate equations. To illustrate this idea, let us go back to the equation

$$x^2 - 3y^2 + 2z^2 = 0 \tag{440}$$

Let us note that either $z = 0$ or $z \neq 0$. If $z = 0$ then our equation reduces to the somewhat simpler equation

$$x^2 - 3y^2 = 0 \tag{441}$$

If $z \neq 0$ then we can divide through (440) by z and obtain the equation

$$\left(\frac{x}{z}\right)^2 - 3\left(\frac{y}{z}\right)^2 + 2 = 0 \tag{442}$$

which, if we are thinking 'projectively' (i.e. identifying solutions that differ by scalar multiples) is the 'same equation' since the solutions $\left(\frac{x}{z}, \frac{y}{z}, 1\right)$ and (x,y,z) differ by scalar multiplication. Thus, calling $s := \frac{x}{z}$ and $t := \frac{y}{z}$ we see that we have obtained a solution to the equation

$$s^2 - 3t^2 + 2 = 0 \tag{443}$$

Thus, the solutions to (440) are, in some sense, comprised of the solutions to (441) and (443). Thus, we have provided a non-trivial relationship between the equations (441) and (443) using the projective equation (441).

It is this idea of relating various equations through a given projective equation that will be key to answering Question 16.4.

17.3 Projective space

We now rigorously define the notion of homogenous polynomial, projective space, and projective equation. For the rest of this section let R stand for any of $\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ unless specified otherwise.

Remark 17.1

For those that have taken algebra, here R can (and should) be thought of as being any ring.

We start with the notion of a homogenous polynomial. But, to define this, it will be helpful to first define the notion of a monomial:

Definition 17.1

Let v and d be elements of $\mathbb{N}^*$. Then, a *monomial of degree d* in $R[x_1, \ldots, x_v]$ is an element of $R[x_1, \ldots, x_v]$ of the form $ax_1^{n_1} \cdots x_v^{n_v}$ where $0 \neq a \in R$ and such that $n_1 + \cdots n_v = d$.

In simple terms, monomials are just polynomials with no instances of '+' and such a monomial is of degree d if the sum of the exponents is d.

Example 17.3

If $v = 3$, $d = 2$, and $R = \mathbb{Z}$ then $8x_1x_2$ and $-2x_1^2$ are monomials of degree 2 in $\mathbb{Z}[x_1, x_2]$

Example 17.4

If $v = 2$, $d = 4$, and $R = \mathbb{Z}/3\mathbb{Z}$ then $-7x_1^2x_2^2$ and $8x_1^3x_2$ are monomials of degree 2 in $\mathbb{Z}/3\mathbb{Z}[x_1, x_2]$.

Example 17.5

If $v = 4$, $d = 5$, and $R = \mathbb{R}$, then $5x_1^3x_1x_3 + x_4^5$ is not a monomial of degree 5 in $\mathbb{R}[x_1, x_2, x_3, x_4]$ but is the sum of two monomials of degree 5.

We make the following obvious observation:

Lemma 17.1

Let $v \in \mathbb{N}^*$ and R. Then, every $0 \neq f(x_1, \ldots, x_v) \in R[x_1, \ldots, x_v]$ can be written uniquely as the sum of monomials.

From this, we can very easily define the notion of a homogenous polynomial

Definition 17.2

Let v and d be elements of $\mathbb{N}^*$. We call an element $f(x_1, \ldots, x_v)$ of $R[x_1, \ldots, x_v]$ *homogenous of degree* d if its a sum of degree d monomials. We call $f(x_1, \ldots, x_v)$ *homogenous* if it is homogenous of some degree d.

Example 17.6

If $v = 3$, $d = 2$, and $R = \mathbb{Q}$ then $3x_1^2 + 6x_2^2 - 5x_3^2$ and $5x_1x_2 + 6x_2x_3 - 7x_1x_3 + x_1^2$ are homogenous elements of $\mathbb{Q}[x_1, x_2, x_3]$ of degree 2.

Example 17.7

The element $3x_1^3+5x_1x_2+x_2^2 \in \mathbb{Z}[x_1, x_2]$ is not homogenous. Indeed, its the sum of a degree 3 monomial $(3x_1^3)$ and two degree 2 monomials ($5x_1x_2$ and x_2^2).

Now, as indicated in the motivation to this lecture, the characteristic thing about homogenous polynomials is that their solution sets have a sort of 'built in redundancy' coming from scalar multiplication. Namely, let's suppose that $f(x_1, \ldots, x_v) \in R[x_1, \ldots, x_v]$ is homogenous of degree d. Then, if $(a_1, \ldots, a_v) \in R^v$ and let $\lambda \in R$. We then see that

$$f(\lambda a_1, \ldots, \lambda a_v) = \lambda^d f(a_1, \ldots, a_v) \tag{444}$$

In particular, if λ is a unit (i.e. λ has a multiplicative inverse in R) we deduce that

$$(a_1, \ldots, a_v) \in X_f(R) \iff (\lambda a_1, \ldots, \lambda a_v) \in X_f(R) \tag{445}$$

So, we see that there is a 'redundancy' in $X_f(R)$ in the sense that given any $(a_1, \ldots, a_v) \in X_f(R)$ we obtain many other elements of $X_f(R)$ by scalar multiplication by units. And, since this process is so simple, one is wont to not really think of $(a_1, \ldots, a_v)$ and $(\lambda a_1, \ldots, \lambda a_v)$ as being distinct solutions. For example, if one is developing an algorithm to find solutions, one would be pretty upset to find $(a_1, \ldots, a_v)$, perform many more steps of the algorithm and find $(\lambda a_1, \ldots, \lambda a_v)$—you already knew that was a solution!

Remark 17.2

Note that it is important to restrict only to the case when λ is a unit in the above. Namely, while equation (444) works regardless of whether or not λ is a unit, if λ is not a unit it could be possible that $f(a_1, \ldots, a_v)$ is non-zero but $f(\lambda a_1, \ldots, \lambda a_v)$ is zero. For example, maybe we're working in $R = \mathbb{Z}/6\mathbb{Z}$ and we have $f(x) = x$. This is certainly homogenous. Note then that $0 = f(0) = f(2 \cdot 3) = 2 \cdot f(3)$ but $f(3) \neq 0$. Thus, to relate (444) to solution sets, we really should restrict to the case when λ is a unit.

Example 17.8

Let $f(x, y, z) := x^2 + y^2 - z^2$. Then, $(3, 4, 5) \in X_f(\mathbb{R})$ and so evidently every $(3\lambda, 4\lambda, 5\lambda) \in X_f(\mathbb{R})$ for every $\lambda \in \mathbb{R} - \{0\}$ (so that λ is a unit).

The idea of projective space is that we want to somehow remove this redundancy in $X_f(R)$, where f is homogenous, by considering tuples like $(a_1, \ldots, a_v)$ and $(\lambda a_1, \ldots, \lambda a_v)$ as being the same. Namely, for $a_1, \ldots, a_v \in R$ we would like to think of the symbol $[a_1 : \ldots : a_v]$ as being just the tuple $(a_1, \ldots, a_v)$ but for which the equality

$$[a_1 : \ldots : a_v] = [\lambda a_1 : \ldots : \lambda a_v] \tag{446}$$

holds by fiat. In other words, we just declare that $(a_1, \ldots, a_v)$ 'equals' $(\lambda a_1, \ldots, \lambda a_v)$ for any scalar λ which is a unit and denote this common object by $[a_1 : \ldots : a_v]$ (using different notation so we don't confuse this object with the actual tuple $(a_1, \ldots, a_v)$).

This is essentially correct, in most situations, with one small caveat. Note that there is one tuple $(a_1, \ldots, a_v)$ that acts quite distinctly from the rest with respect to scalar multiplication by units: the zero tuple. Namely, if $(a_1, \ldots, a_v)$ is a non-zero tuple then multiplication by some unit scalar λ will produce a different tuple. But evidently

$$(0, \ldots, 0) = (\lambda 0, \ldots, \lambda 0) \tag{447}$$

for any scalar λ. Moreover, note that 0-tuple is always an element of $X_f(R)$ assuming that f is homogenous of degree $d > 0$. For these two reasons, the zero tuple is best excluded from our discussion of identifying tuples up to scalar multiplication.

The above discussion suggests that a good way to eliminate this redundancy in $X_f(R)$, when f is homogenous, is to think about the set of objects $[a_1 : \ldots : a_v]$ thought of as 'tuples defined up to scalar multiplication' where we require that $(a_1, \ldots, a_v) \neq (0, \ldots, 0)$ to eliminate the zero tuple as suggested in the last paragraph.

This is essentially the definition of projective space:

Definition 17.3

Let v be an element of $\mathbb{N}^*$ and let R be $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, we define *v-dimensional projective space over R*, denoted $\mathbb{P}^v(R)$, to be the set of symbols $[a_0 : \ldots : a_v]$ where $a_0, \ldots, a_v \in R$ and at least one of the a_i is non-zero we we declare that $[a_0 : \ldots : a_v] = [b_0 : \ldots : b_v]$ if and only if there exists $0 \neq \lambda \in R$ such that $a_i = \lambda b_i$ for all $i = 0, \ldots, v$.

We can think of the above, more rigorously, using equivalence relations. Namely, let us put an equivalence relation $\sim$ on R^{v+1} by declaring that $(a_0, \ldots, a_v) \sim (b_0, \ldots, b_v)$ if there exists a scalar $\lambda \in R$ which is a unit such that $a_i = \lambda b_i$ for all i (we leave it to the reader to check that this is, in fact, an equivalence relation). One then has the following expression for v-dimensional projective space:

$$\mathbb{P}^v(R) = (R^{v+1} - \{(0, \ldots, 0)\})/\sim \tag{448}$$

where we have chosen to write the equivalence class of $(a_0, \ldots, a_v) \in R^{v+1} - \{(0, \ldots, 0)\}$ as $[a_0 : \ldots : a_v]$.

Remark 17.3

For those that have taken algebra, an even better way to think of $\mathbb{P}^v(R)$ is as follows. Note that $R^\times$, the group of units of R, acts on $R^{v+1} - \{(0, \ldots, 0)\}$ by $\lambda \cdot (a_0, \ldots, a_v) := (\lambda a_0, \ldots, \lambda a_v)$. One can then see that $\mathbb{P}^v(R)$ is just the orbit space of this action.

There is one important thing to note here, which is that the indexing is a bit weird. Namely, we are calling it v-dimensional projective space but notice that since we are starting our indexing at 0 the object $[a_0 : \ldots : a_v]$ is like $(v+1)$-tuple. The reason for this will be clear as time progresses, but let us say something here in the meantime.

The intuition is that $\mathbb{P}^v(R)$ really does 'act' like a v-dimensional object since, in practice, its objects really only depend on v-parameters. Less cryptically, note that if $[a_0 : \ldots : a_v] \in \mathbb{P}^v(R)$ then one of the $a_i \neq 0$. Let's say $a_0 \neq 0$ for convenience. Then,

$$[a_0 : a_1 : \ldots : a_v] = [1 : a_1 a_1^{-1} : \ldots : a_v a_1^{-1}] \tag{449}$$

and so we see that to describe $[a_0 : a_1 : \ldots : a_v]$ we really only need the v numbers $a_1 a_0^{-1}, \ldots, a_v a_0^{-1}$. We'll generalize the observation later, but hopefully this gives the reader a rough idea of why the indexing seems 'off'. We will see later that, pictorially, the fact that $\mathbb{P}^1(R)$ 'looks one dimensional' will hold up in practice.

Example 17.9

Note that $[2 : 3 : 7] = [8 : 1 : 6]$ in $\mathbb{P}^2(\mathbb{Z}/11\mathbb{Z})$ since $8 = 4 \cdot 2$, $1 = 4 \cdot 3$, and $6 = 4 \cdot 7$.

Now, one might notice that in Definition 17.3 we restricted only to the cases when R was $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. What sets these choices of R apart from the remaining R we enumerated at the beginning of the section (i.e. $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ where m is not prime) is that for these choices of R we have that $\lambda \in R$ is a unit (i.e. has multiplicative inverse) if and only if $\lambda \neq 0$. For $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ this is not the case, and for this reason we will have to modify the definitions there.

As an example, let us define P_v to be the set of all objects $[a_0 : \ldots : a_v]$ with $a_0, \ldots, a_v \in \mathbb{Z}$ such that $a_i \neq 0$ for some i and where $[a_0 : \ldots : a_v] = [b_0 : \ldots : b_v]$ if and only if there exists a unit $\lambda \in \mathbb{Z}$ (i.e. $\lambda = \pm 1$) such that $a_i = \lambda b_i$ for all i. One would naively guess that one should set $\mathbb{P}^v(\mathbb{Z})$ to be this set P_v. Unfortunately, this set P_v has some issues coming from the fact that being a unit is not the same thing as being non-zero in $\mathbb{Z}$. For example, one would hope that the reduction map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ given by $a \mapsto r_p(a)$ would give rise to a map $\mathbb{P}^v(\mathbb{Z}) \to \mathbb{P}^v(\mathbb{Z}/p\mathbb{Z})$ given by

$$[a_0 : \ldots : a_v] \mapsto [r_p(a_0) : \ldots : r_p(a_v)] \tag{450}$$

If we define $\mathbb{P}^v(\mathbb{Z})$ to be this set P_v this has an obvious issue though. For example, $[3 : 6 : 15]$ is a perfectly fine element of P_2 but if we apply r_3 to its coordinates we get $[0 : 0 : 0]$ which is not an element of $\mathbb{P}^3(\mathbb{Z}/3\mathbb{Z})$.

We similarly have issues with P_v when we try to compare it to $\mathbb{P}^v(\mathbb{Q})$. Namely, one would think that, in fact, $\mathbb{P}^v(\mathbb{Z}) = \mathbb{P}^v(\mathbb{Q})$ since any element of $\mathbb{Q}$ differs from an element of $\mathbb{Z}$ by scalar multiplication. Now, there

is an obvious map $P_v \to \mathbb{P}^v(\mathbb{Q})$ that takes $[a_0 : \ldots : a_v]$ to itself. Moreover, this map is clearly surjective since for any $\left[\frac{a_0}{b_0} : \ldots : \frac{a_v}{b_v}\right] \in \mathbb{P}^v(\mathbb{Q})$ with a_i and b_j elements of $\mathbb{Z}$ we have that

$$\left[\frac{a_0}{b_0} : \ldots : \frac{a_v}{b_v}\right] = [a_0 b_1 \cdots b_v : \ldots : a_v b_1 \cdots b_{v_1}] \tag{451}$$

in $\mathbb{P}^v(\mathbb{Q})$ and $[a_0 b_1 \cdots b_v : \ldots : a_v b_1 \cdots b_{v_1}] \in P_v$. But, the map $P_v \to \mathbb{P}^v(\mathbb{Q})$ is not injective. For example, $[1 : 1]$ is not equal to $[2 : 2]$ in P_v since they don't differ by scalar multiplication by ± 1. That said, their images are certainly equal in $\mathbb{P}^v(\mathbb{Q})$ since they differ by scalar multiplication by a unit of $\mathbb{Q}$ (i.e. 2).

Thus, with the naive definition of $\mathbb{P}^v(\mathbb{Z})$ being P_v we see that we don't get nice interactions with either $\mathbb{P}^v(\mathbb{Z}/p\mathbb{Z})$ or $\mathbb{P}^v(\mathbb{Q})$. That said, both of these examples also hint at how to modify the definition of P_v to actually get the desired definition of $\mathbb{P}^v(\mathbb{Z})$. For example, note that if we want $[a_0 : \ldots : a_v]$ with $a_0, \ldots, a_v \in \mathbb{Z}$ to map to an element of $\mathbb{P}^v(\mathbb{Z}/p\mathbb{Z})$ for all primes p we need precisely that for all primes p at least one of the a_i is indivisible by p. In other words, we require that $\gcd(a_0, \ldots, a_v) = 1$.

Motivated by this, we make the following definition:

Definition 17.4

Let $v \in \mathbb{N}^*$. We define the *v-dimensional projective space over $\mathbb{Z}$*, denoted $\mathbb{P}^v(\mathbb{Z})$, to be all objects of the form $[a_0 : \ldots : a_v]$ with $a_0, \ldots, a_v \in \mathbb{Z}$ and such that $\gcd(a_0, \ldots, a_v) = 1$. We identify two objects $[a_0 : \ldots : a_v]$ and $[b_0 : \ldots : b_v]$ if and only if there exists some $\lambda \in \{\pm 1\}$ such that $a_i = \lambda b_i$ for all $i = 0, \ldots, v$.

Note then that with this definition we do, in fact, get maps $\mathbb{P}^v(\mathbb{Z}) \to \mathbb{P}^v(\mathbb{Z}/p\mathbb{Z})$ for all primes p defined by

$$[a_0 : \ldots : a_v] \mapsto [r_p(a_0) : \ldots : r_p(a_v)] \tag{452}$$

And, moreover, we have that the relationship to $\mathbb{P}^v(\mathbb{Q})$ is fixed:

Lemma 17.2

The natural map $\mathbb{P}^v(\mathbb{Z}) \to \mathbb{P}^v(\mathbb{Q})$ given by taking $[a_0 : \ldots : a_v]$ to itself is a bijection.

Proof 17.1

See Exercise 17.3.

Remark 17.4

One might wonder what the point of defining $\mathbb{P}^v(\mathbb{Z})$ is if it's just naturally in bijection with $\mathbb{P}^v(\mathbb{Q})$. The simple answer is that the set $\mathbb{P}^v(\mathbb{Z})$ naturally admits maps to each $\mathbb{P}^v(\mathbb{Z}/p\mathbb{Z})$ (and, in fact, to each $\mathbb{P}^v(\mathbb{Z}/m\mathbb{Z})$ once we define these) given by reduction. The set $\mathbb{P}^v(\mathbb{Q})$ does not admit such a map (how do I take $[\frac{1}{2} : 3 : -\frac{1}{7}]$ and reduce it modulo 12?).

Of course, one can use the identification of $\mathbb{P}^v(\mathbb{Q})$ to define a 'reduction map' to $\mathbb{P}^v(\mathbb{Z}/p\mathbb{Z})$. Namely, any $[x_0 : \ldots : x_v] \in \mathbb{P}^v(\mathbb{Q})$ is equal to a unique (up to multiplication by ± 1) element of the form $[a_0 : \ldots : a_v]$ with $a_i \in \mathbb{Z}$ and $\gcd(a_0, \ldots, a_v) = 1$. We then define the image of $[x_0 : \ldots : x_v]$ in $\mathbb{P}^v(\mathbb{Z}/p\mathbb{Z})$ to be $[r_p(a_0) : \ldots : r_p(a_v)]$. So, for example, the image of $[\frac{1}{2} : 3 : -\frac{1}{7}]$ in $\mathbb{Z}/12\mathbb{Z}$ is obtained by rewriting this element as $[7 : 42 : -2]$ and then taking its reduction modulo 12 to get $[7 : 6 : 10]$. Of course, this really is just routing the definition through $\mathbb{P}^v(\mathbb{Z})$, and thus shows why this definition is

useful.

We run into the same problems when defining $\mathbb{P}^v(\mathbb{Z}/m\mathbb{Z})$ for m non-prime. Namely, if we want a map $\mathbb{P}^v(\mathbb{Z}/m\mathbb{Z}) \to \mathbb{P}^v(\mathbb{Z}/p\mathbb{Z})$, for all primes $p \mid m$, given by

$$[a_0 : \ldots : a_v] \mapsto [r_p(a_0) : \ldots : r_p(a_v)] \tag{453}$$

we then need that for all primes p dividing m we have that p does not divide one of the a_i. Equivalently, we require that $\gcd(a_0, \ldots, a_v, m) = 1$.

We thus make this definition:

Definition 17.5

Let v and m be elements of $\mathbb{N}^*$. We define the *v-dimensional projective space over $\mathbb{Z}/m\mathbb{Z}$*, denoted $\mathbb{P}^v(\mathbb{Z}/m\mathbb{Z})$, to be the set of all objects of the form $[a_0 : \ldots : a_v]$ with $a_0, \ldots, a_v \in \mathbb{Z}/m\mathbb{Z}$ and such that $\gcd(a_0, \ldots, a_v, m) = 1$. We identify two objects $[a_0 : \ldots : a_v]$ and $[b_0 : \ldots, b_v]$ if and only there exists some $\lambda \in \Phi(m)$ such that $a_i = \lambda b_i$ for all $i = 0, \ldots, v$.

Remark 17.5

For those that have taken algebra, a warning is in order. No doubt one realizes that Definition 17.3 works whenever R is a field. If one is particularly astute, one will notice that the condition on $[a_0 : \ldots : a_v]$ that works uniformly for all the R we have considered is that that ideal $(a_0, \ldots, a_v)$ is the unit ideal (1) in R. Thus, one might naively imagine that for any ring R one can set $\mathbb{P}^v(R)$ to be the set $Q_v(R)$ of all objects $[a_0 : \ldots : a_v]$ where $a_0, \ldots, a_v \in R$ and $(a_0, \ldots, a_v) = (1)$ where we identify such objects up to unit multiplication. This is, in fact, not true.

In fact, the key to this has to do with our motivation above. Namely, we intuited our definitions of $\mathbb{P}^v(R)$ using the notions of greatest common denominator. This is a notion, the reader may be aware, that doesn't exist for general rings R. Moreover, this it not merely a matter of motivation. There is always an injective map $Q_v(R) \to \mathbb{P}^v(R)$ but it turns out that it needn't be surjective in general. In fact, assuming R is a Noetherian integral domain (for safety), this map is surjective if and only if R is a UFD (a weaker condition than being a PID, the condition to have greatest common divisors, but in the same vein). So, for example, the fact that $Q_v(\mathbb{Z})$ is the definition we took for $\mathbb{P}^v(\mathbb{Z})$ is a reflection of the fact that $\mathbb{Z}$ is a UFD.

Of course, this is all a bit fanciful because to make sense of this I would have to define $\mathbb{P}^v(R)$ for a general ring R. That is not something I will do here. If you'd like, one can read about this further in any text on algebraic geometry which the true realm of projective geometry.

17.4 Picturing the projective world

Before we move on to defining projective equations, it will be helpful to get a better sense of what $\mathbb{P}^v(R)$ looks like, at least in the cases when $v \in \{1, 2\}$ and R being $\mathbb{Z}/p\zeta$ for p prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. To do this we will give both an 'algebraic' decomposition of $\mathbb{P}^1(R)$ and $\mathbb{P}^2(R)$ which will allow us to more easily conceptualize what the elements of these sets look like. We will then explain what $\mathbb{P}^1(\mathbb{R})$, $\mathbb{P}^1(\mathbb{Q})$, $\mathbb{P}^1(\mathbb{C})$, and $\mathbb{P}^2(\mathbb{R})$ look like as geometric objects, and try to reconcile this with our algebraic understanding of these sets.

17.4.1 Projective space as the set of lines

One of the main tools that will be helpful to us in our picturing of $\mathbb{P}^v(R)$ is the elementary observation, but key, observation that $\mathbb{P}^v(R)$ can be just thought of as the set of 'lines' in R^{v+1}. To formalize this, let us first make the following definition:

Definition 17.6

Let $v \in \mathbb{N}^*$ and let R be any of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, a *line* ℓ in R^{v+1} is defined to be a linear subspace of R^{v+1} of dimension 1.

This definition doesn't really differ from our usual thought process of what a line in R^{v+1} is, except that we require that our line passes through the origin. The only reason that we haven chosen to emphasize the rigorous definition of a line, is the fact that linear subspaces (of a particular dimension) is the correct way to think of $\mathbb{P}^v(R)$ with an eye towards generalization, and it will be the linear algebraic foundation we will often use to rigorously work with elements of $\mathbb{P}^v(R)$.

The direct relationship between $\mathbb{P}^v(R)$ and lines in R^{v+1} is then the following:

Lemma 17.3

Let $v \in \mathbb{N}^*$ and let R be $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, there is a natural bijection

$$\mathbb{P}^v(R) \to \left\{\text{lines in } R^{v+1}\right\} \tag{454}$$

which takes $[a_0 : \ldots : a_v]$ to the line in R^{v+1} spanned by $(a_0, \ldots, a_v)$.

Proof 17.2

The mentioned map is, indeed, well-defined. Namely, if $[a_0 : \ldots : a_v] = [b_0 : \ldots : b_v]$ then there exists some non-zero $\lambda \in R$ such that $(a_0, \ldots, a_v) = \lambda(b_0, \ldots, b_v)$. It's then easy to see that the lines spanned by $(a_0, \ldots, a_v)$ and $(b_0, \ldots, b_v)$ are the same.

To see that the map is surjective is simple since any line through the origin in R^{v+1} is spanned by any one of its non-zero elements $(a_0, \ldots, a_v)$. Clearly then this line is the image of $[a_0 : \ldots : a_v]$.

Finally, to see that the map is injective it suffices to note that if $[a_0 : \ldots : a_v]$ and $[b_0 : \ldots : b_v]$ map to the same line in R^{v+1} then the span of $(a_0, \ldots, a_v)$ is equal to the span of $(b_0, \ldots, b_v)$. This then clearly implies that $(a_0, \ldots, a_v)$ is a non-zero scalar multiple of $(b_0, \ldots, b_v)$.

Intuitively, this is no more than the observation that the set of $(b_0, \ldots, b_v)$ such that the equality $[b_0 : \ldots : b_v] = [a_0 : \ldots : a_v]$ holds is nothing more than the span of $(a_0, \ldots, a_v)$. Thus, in some sense, the above map can be thought of as

$$[a_0 : \ldots : a_v] \mapsto \{(b_0, \ldots, b_v) \in R^{v+1} : [b_0 : \ldots : b_v] = [a_0 : \ldots : a_v]\} \tag{455}$$

which, hopefully, gives the reader further insight into the above identification.

One thing that is worth noting is that even though lines in R^{v+1} are quite simple objects to conceptualize, they are actually somewhat complicated to describe equationally for $v > 1$. Indeed, note that a line in R^{v+1} will, in general, require v linear equations to describe in R^{v+1}.

For example, a typical example of a line in $\mathbb{R}^3$ is given by the set of $(x, y, z) \in \mathbb{R}^3$ satisfying the simultaneous equations

$$\begin{cases} x + y + z = 0 \\ x + y - z = 0 \end{cases} \tag{456}$$

and, in general, one will require 2 simultaneous linear equations to describe a line in $\mathbb{R}^3$.

More theoretically, to describe a line ℓ equationally means to describe it as the kernel of a linear transformation T. Note that if $T : R^{v+1} \to R^{v+1}$ is a linear transformation, then the Rank-Nullity Theorem implies that if $\ell = \ker T$ then $\dim(\text{im}(T))$ (where $\text{im}(T)$ means the image, or range, of T) is v. Thus, T can

be represented by a $(v+1)\times(v+1)$ matrix with rank v. This is essentially exactly the same thing as saying that ℓ requires v linear equations to describe it.

That said, in the special case when $v=1$ we see that it really only takes a single linear equation to describe a line in R^2. And, in fact, one can concretely describe the line associated to $[a:b]\in\mathbb{P}^1(R)$ by Lemma 17.3 as the line $ay-bx=0$. Indeed, note that $ay-bx=0$ does describe a line in R^2 and to see that it's the same as the span of (a,b) it suffices to check that (a,b) is one the line $ay-bx=0$. But, plugging in (a,b) we get $ab-ba=0$ which, of course, is true.

The case of $\mathbb{P}^1(R)$

Let us begin by trying to more concretely understand what $\mathbb{P}^1(R)$ looks like by giving an 'algebraic' decomposition of its elements. To begin, note that by definition the elements of $\mathbb{P}^1(R)$ are precisely the objects of the form $[a:b]$ with $a,b\in R$ and not both of a and b are zero. We can break such objects into two concrete cases.

The first case is when $b\neq 0$. When this happens note that $[a:b]=\left[\frac{a}{b}:1\right]$. Indeed, it's clear that (a,b) and $\left(\frac{a}{b},1\right)$ differ by the scalar multiple b. In fact, we claim that every $[a:b]$ such that $b\neq 0$ can be written uniquely in the form $[s:1]$ where $s\in R$. As we have already observed, if we take $[a:b]$ with $b\neq 0$ then $[a:b]=[s:1]$ with $s=\frac{a}{b}$ and thus every $[a:b]$ with $b\neq 0$ is equal to an element of the form $[s:1]$. To see that such a representation is unique, note that if $[s:1]=[t:1]$ with $s,t\in R$ then there exists some $0\neq\lambda\in R$ such that $(s,1)=(\lambda t,\lambda)$. Comparing the second coordinates shows that $\lambda=1$ and thus, comparing the first coordinates, we see that $s=t$. Thus, the representation of $[a:b]$ with $b\neq 0$ as $[s:1]$ with $s\in R$ is unique. Note that this allows us to create a simple bijection between the set of $[a:b]\in\mathbb{P}^1(R)$ with $b\neq 0$ and R itself via the map $s\mapsto[s:1]$.

Let us now consider the case when $b=0$. This case is actually quite simple. Namely, note that if $[a:0]$ is in $\mathbb{P}^1(R)$ then, necessarily, $a\neq 0$. Thus, we see that $[a:0]=[1:0]$ since, in this case, we see that $(a,0)$ and $(1,0)$ differ by the scalar multiple a^{-1}.

We record this observation as follows:

Lemma 17.4

Let R be any of $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, one has a natural decomposition

$$\mathbb{P}^1(R)=\{[s:1]:s\in R\}\cup\{[1:0]\} \tag{457}$$

and the map $s\mapsto[s:1]$ is a bijection

$$R\to\{[s:1]:s\in R\} \tag{458}$$

Let us note that there is nothing special about the point $[1:0]$ in Lemma 17.4. Namely, if one takes any particular point $[a_0:b_0]\in\mathbb{P}^1(R)$ then there are natural bijections between the set $\mathbb{P}^1(R)-\{[a_0:b_0]\}$ (i.e. the complement of $[a_0:b_0]$ in $\mathbb{P}^1(R)$) and R itself thus giving a decomposition much like that in Lemma 17.4 with $[1:0]$ replaced by $[a_0:b_0]$. For example, one can check that if $a_0\neq 0$ then one such bijection takes $[a:b]$ to $\frac{a}{a_0b-b_0a}$. If $b_0\neq 0$ one can replace this by the map that takes $[a:b]$ to $\frac{b}{a_0b-b_0a}$.

Remark 17.6

These maps are not as random as they seem. One can describe the bijection $\mathbb{P}^1(R)-\{[1:0]\}$ form Lemma 17.4 as $[a:b]\mapsto\frac{a}{b}$. The above bijections $\mathbb{P}^1(R)-\{[a_0:b_0]\}\to R$ were then precomposing the bijection from the previous sentence with a linear map $R^2\to R^2$ taking (a_0,b_0) to $(1,0)$. In the case

when $a_0 \neq 0$ we took the map $\begin{pmatrix} a_0 & 0 \\ b_0 & 1 \end{pmatrix}$ and in the case when $b_0 \neq 0$ we took the map $\begin{pmatrix} a_0 & -1 \\ b_0 & 0 \end{pmatrix}$.

Summarizing, we see that the following holds:

Lemma 17.5

Let R be any of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $[a_0 : b_0] \in \mathbb{P}^1(R)$ be fixed. There is then a decomposition

$$\mathbb{P}^1(R) = (\mathbb{P}^1(R) - \{[a_0 : b_0]\}) \cup \{[a_0 : b_0]\} \tag{459}$$

and there is a bijection

$$\mathbb{P}^1(R) - \{[a_0 : b_0]\} \to R \tag{460}$$

which can be given by

$$[a : b] \mapsto \frac{a}{a_0 b - b_0 a} \tag{461}$$

in the case when $a_0 \neq 0$ and which can be given by

$$[a : b] \mapsto \frac{b}{a_0 b - b_0 a} \tag{462}$$

in the case when $b_0 \neq 0$.

One can check that when $[a_0 : b_0] = [1 : 0]$ the decomposition in Lemma 17.5 matches that from Lemma **??**.

Thus, we see that in all cases we can think of $\mathbb{P}^1(R)$ as being something like $R \cup \{p_0\}$ for some point $p_0 \in \mathbb{P}^1(R)$. In words, $\mathbb{P}^1(R)$ looks like R together with some extra point p_0. It is often times the case that one denotes the special extra point p_0 by ∞. There is a fairly down-to-earth motivation for this. Namely, let us consider the case $p_0 = [0 : 1]$. We can then interpret the decomposition $\mathbb{P}^1(R) = R \cup \{[0 : 1]\}$ in a fairly simple way using the content of the last subsection. Namely, recall that there is a natural bijection $\mathbb{P}^1(R) \to \{\text{lines in } R^2\}$ that takes $[a : b]$ to the line with equation $by - ax = 0$. Note that the bijection from Lemma 17.5 between $\mathbb{P}^1(R) - \{[0 : 1]\}$ and R takes $[a : b]$ to $\frac{b}{a}$. We can interpret this quantity quite simply in terms of the line $ay - bx = 0$. Namely, it's the slope of the line.

In other words, one can interpret the bijection $\mathbb{P}^1(R) - \{[0 : 1]\} \to R$ as taking a line ℓ to its slope. What then does $[0 : 1]$ correspond to? Well, this corresponds to the line $x = 0$ or, in other words, the y-axis. One often times thinks of this vertical line as having infinite slope. Thus one would imagine that where $[0 : 1]$ should map to under this slope map is ∞. Thus, it is common to denote $[0 : 1]$ by ∞. Of course, while this natural interpretation of the extraneous point $p_0 = [0 : 1]$ doesn't work as nicely for other choices of p_0 it is common to always denote this extraneous point by ∞.

Now, while one can choose their extraneous point ∞ to be essentially arbitrary, for us we shall always take $\infty := [1 : 0]$ as in Lemma 17.4. This is mostly for convenience since, as we shall see, this choice makes makes a lot of the notation later on simpler.

We now try to use this algebraic decomposition, together with Lemma 17.3 to understand what $\mathbb{P}^1(R)$ looks like in some special cases:

Example 17.10

Let us try to geometrically picture what $\mathbb{P}^1(\mathbb{R})$ might look like. Using Lemma 17.3 we equivalently want to somehow picture the 'space of all lines in $\mathbb{R}^2$'. What this might mean is that I want to take $\mathbb{R}^2 - \{(0, 0)\}$ and shrink every line down to a single point. What would this look like? Well, a good first step is to realize that if we're going to crunch all the lines down to a single point, we might as well

think about crushing together antipodal points on the unit circle

$$S^1 := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} \tag{463}$$

(antipodal means the points are on the opposite side of the circle—i.e. the antipodal point of (x, y) is $(-x, -y)$). To see why this is ok, note that every line ℓ in $\mathbb{R}^2$ passes through exactly two points of S^1, and these points are antipodal. So, crushing lines to points in $\mathbb{R}^2 - \{(0, 0)\}$ is the same thing as crushing together antipodal points of S^1.

What S^1 with its antipodal points identified look like? Well, let's think about only the left hand side of the circle (those with radians $(\frac{\pi}{2}, \frac{3\pi}{2})$). Their antipodal point will be on the right hand side of the circle (those with radians in $(\frac{-\pi}{2}, \frac{\pi}{2})$). Thus identifying these points with their andtipodal 'folds' the left hand side of the circle onto the right, resulting in a single semicircle. But, note that we have forgotten to identify one pair of antipodal points: the north and south pole $(0, 1)$ and $(0, -1)$. Identifying these points pulls the ends of the semicircle together giving us, well, another circle! So, one can picture $\mathbb{P}^1(\mathbb{R})$ as being a circle.

Note that this is actually completely fits into our statement that $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$. Specifically, let's picture a circle for a second. In fact, let's imagine the unit circle S^1 (since all circles look the same). Let's pick the point '∞' to be the north pole $p_0 := (0, 1)$. If we remove this from the circle $S^1 - \{p_0\}$ we claim that we have a natural bijection with $\mathbb{R}$. Intuitively one just imagines taking $C - \{p_0\}$ and 'unrolling it' onto the line $\mathbb{R}$. Specifically, the map takes $(x, y) \in S^1 - \{p_0\}$ to $\dfrac{x}{1 - y} =: u \in \mathbb{R}$.

Another, more geometric, way to think about this is that if one takes the line (not passing through origin necessarily) L which passes through p_0 and (x, y) it will intersect the x-axis ($\mathbb{R}$) in exactly one place. That place is u. This process is called *stereographic projection* and will be an important idea moving forward.

Example 17.11

Let us try to use an analogue of stereographic projection, as in the previous example, to give a plausibility argument for why $\mathbb{P}^1(\mathbb{C})$ looks like the unit sphere

$$S^2 := \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\} \tag{464}$$

Namely, we claim that stereographic projection gives us a way of thinking of S^2 as also being $\mathbb{C} \cup \{\infty\}$. Namely, let us fix p_0 to be the north pole $(0, 0, 1)$. We then note that for any point $p \in S^2 - \{p_0\}$ the line (not passing through the origin) L connecting p_0 and p will pass through a unique point of the xy-axis. Note though that xy-axis can be thought of as $\mathbb{R}^2$ or, equivalently, $\mathbb{C}$. One can check that this gives the desired bijection $S^2 - \{p_0\} \to \mathbb{C}$ which, hopefully, semi-convincingly suggests to the reader that $\mathbb{P}^1(\mathbb{C})$ can be pictured as S^2.

The case of $\mathbb{P}^2(R)$

Let us now try to understand more concretely what $\mathbb{P}^2(R)$ looks like in the same vein as we did for $\mathbb{P}^1(R)$, by giving an algebraic decomposition of $\mathbb{P}^2(R)$. Again, we start with $[a : b : c] \in \mathbb{P}^2$ and we will break our decomopsition into two cases.

First, let us assume that $c \neq 0$. In this case we can write $[a : b : c] = \left[\dfrac{a}{c} : \dfrac{b}{c} : 1\right]$. In fact, just as before, we claim that every element $[a : b : c]$ of $\mathbb{P}^2(R)$ with $c \neq 0$ can be written uniquely as $[s : t : 1]$ with $s, t \in R$. We have already seen that every such element can be written in this form. To see that such a representation is unique, suppose that $[s : t : 1] = [s' : t' : 1]$. Then, there exists some $0 \neq \lambda \in R$ such that $(s, t, 1) = (\lambda s', \lambda t', \lambda)$. Comparing last coordinates gives $\lambda = 1$ and thus comparing the first two coordinates gives $s = s'$ and $t = t'$ as desired. Thus, in this case we see that the set of $[a : b : c]$ with last coordinate not equal to zero are naturally in bijection with R^2.

Again, the case when $c = 0$ is simpler, but not quite as simple as in the setting of $\mathbb{P}^1(R)$. Namely, we note that if we have $c = 0$ then we have that $[a : b : c] = [a : b : 0]$ (clearly) and not much else can be simplified. That said, note that this set of $[a : b : 0]$ is naturally in bijection with $\mathbb{P}^1(R)$! Indeed, it's clear that the bijection is given by the simple map $[a : b : 0] \mapsto [a : b]$.

Thus, in this case, we see that $\mathbb{P}^2(R)$ doesn't look like R^2 together with an extraneous point, but R^2 together with an extraneous copy of $\mathbb{P}^1(R)$. We record this as follows:

Lemma 17.6

Let R be any of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, we have a decomposition

$$\mathbb{P}^2(R) = \{[s : t : 1] : s, t \in R\} \cup \{[a : b : 0] : a, b \in R \text{ not all } 0\} \tag{465}$$

Also, the map

$$\{[s : t : 1] : s, t \in R\} \to R^2 \tag{466}$$

given by $[s : t : 1] \mapsto (s, t)$ and

$$\{[a : b : 0] : a, b \in \mathbb{R}\} \to \mathbb{P}^1(R) \tag{467}$$

given by $[a : b : 0] \mapsto [a : b]$ are bijections.

That said, combining our decomposition of $\mathbb{P}^1(R)$ from the last subsection, together with this decomposition $\mathbb{P}^2(R) = R^2 \cup \mathbb{P}^1(R)$ we obtain a decomposition $\mathbb{P}^2(R) = R^2 \cup R \cup \{\infty\}$.

We now discuss what $\mathbb{P}^2(\mathbb{R})$ might look like geometrically:

Example 17.12

Picturing $\mathbb{P}^2(\mathbb{R})$ is quite difficult. The reason is that whereas $\mathbb{P}^1(\mathbb{R})$ and $\mathbb{P}^1(\mathbb{C})$ embed faithfully into $\mathbb{R}^2$ and $\mathbb{R}^3$ respectively, one can only embed $\mathbb{P}^2(\mathbb{R})$ faithfully into $\mathbb{R}^4$. Thus, giving a literal picture of what $\mathbb{P}^2(\mathbb{R})$ looks like is nigh impossible, one can give a procedure by which one might start to imagine its image. Namely, we can repeat the same idea we used to picture $\mathbb{P}^1(\mathbb{R})$. Namely, $\mathbb{P}^2(\mathbb{R})$ should be the result of taking all lines in $\mathbb{R}^3$ and crunching them down to a point. A good place to start is to notice, as analagous to the case of $\mathbb{P}^1(\mathbb{R})$, we can think of $\mathbb{P}^2(\mathbb{R})$ as being S^2 where we have crunched together antipodal points. Unfortunately, as mentioned before, we can't really draw a picture of what this looks like. If one wants to see an inaccurate, but suggestive picture of what $\mathbb{P}^2(\mathbb{R})$ looks like, Google the term 'Boy surface' and see how truly strange $\mathbb{P}^2(\mathbb{R})$ 'looks'.

That said, one often times **very imprecisely** pictures as S^2. This is for no other reason that both $\mathbb{P}^2(\mathbb{R})$ and S^2 are both (compact) surfaces. This picture can be helpful to give a very cartoonish, inaccurate picture of things going on in $\mathbb{P}^2(\mathbb{R})$ but one must be careful that it can also be misleading.

The case of $\mathbb{P}^v(R)$

In this section we merely note what the 'algebraic' decomposition from the last section looks like for general v. Namely, we have the following basic generalization of Lemma 17.4 and Lemma 17.6:

Lemma 17.7

Let $v \in \mathbb{N}^*$ and let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, there is a decomposition

$$\mathbb{P}^v(R) = \{[s_0 : \ldots : s_{v-1} : 1] : s_0, \ldots, s_{v-1} \in R\} \cup \{[a_0 : \cdots : a_{v-1} : 0] : a_0, \ldots, a_{v-1} \in R \text{ not all zero}\} \tag{468}$$

Also, the maps

$$\{[s_0 : \ldots : s_{v-1} : 1] : s_0, \ldots, s_{v-1} \in R\} \to R^v \tag{469}$$

given by

$$[s_0 : \ldots : s_{v-1} : 1] \mapsto (s_0, \ldots, s_{v-1}) \tag{470}$$

and

$$\{[a_0 : \cdots : a_{v-1} : 0] : a_0, \ldots, a_{v-1} \in R\} \to \mathbb{P}^{v-1}(R) \tag{471}$$

given by

$$[a_0 : \ldots : a_{v-1} : 0] \mapsto [a_0 : \ldots : a_{v-1}] \tag{472}$$

are bijections.

Writing this more loosely, we see that we have an inductive decomposition

$$\mathbb{P}^v(R) = R^v \cup \mathbb{P}^{v-1}(R) \tag{473}$$

Thus, carrying this out iteratively, we see that we get a decomposition

$$\mathbb{P}^v(R) = R^v \cup R^{v-1} \cup \cdots \cup R \cup \{\infty\} \tag{474}$$

where we identify $\mathbb{P}^0(R)$ with $\{\infty\}$.

17.5 Projective equations

Now that we have the notion of projective space (for all the possibilities of R we consider) at hand, we can define the projective solution set of a homogenous polynomial f:

Definition 17.7

Let $v \in \mathbb{N}^*$. If $f(x_0, \ldots, x_v) \in R[x_0, \ldots, x_v]$ is homogenous we define its *projective solution set*, denoted $P_f(R)$, to be the set of all $[a_0 : \ldots : a_v] \in \mathbb{P}^v(R)$ such that $f(a_0, \ldots, a_v) = 0$.

It is really worth unpacking this definition. Namely, note that it really does make sense to say that $f(a_0, \ldots, a_v) = 0$ for f homogenous, in the sense that if $[a_0 : \ldots : a_v] = [b_0 : \ldots : b_v]$ then $f(a_0, \ldots, a_v) = 0$ if and only if $f(b_0, \ldots, b_v) = 0$. Indeed, if $[a_0 : \ldots : a_v] = [b_0 : \ldots : b_v]$ then $(a_0 : \ldots : a_v) = (b_0 : \ldots : b_v)$ differ by scalar multiplication by a unit, say $a_i = \lambda b_i$ for all i. Then, if f is homogenous of degree d, we have that

$$f(a_0, \ldots, a_v) = \lambda^d f(b_0, \ldots, b_v) \tag{475}$$

and so $f(a_0, \ldots, a_v) = 0$ if and only if $f(b_0, \ldots, b_v)$ as desired. Note, in particular, that this only works for homogenous polynomials f.

Example 17.13

As a silly example of why this doesn't work for non-homogenous polynomials, consider $f(x, y) = x^2 - 4 \in \mathbb{R}[x, y]$. Note then that $[2 : 0] = [1 : 0] \in \mathbb{P}^1(\mathbb{R})$ but $f(2, 0) = 0$ and $f(1, 0) \neq 0$. Thus, one cannot define $P_f(\mathbb{R})$ if f is not homogenous.

Note also another subtle point concerning this definition. Namely, even though it makes sense to ask whether $[a_0 : \ldots : a_v] \in \mathbb{P}^v(R)$ is a zero of a homogenous polynomial f, it doesn't make sense to talk about 'evaluating' a homogenous polynomial f on an element of $\mathbb{P}^v(R)$. Namely, if $[a_0 : \ldots : a_v] \in \mathbb{P}^v(R)$ and $f(a_0, \ldots, a_v) = 0$ it's tempting to write $f([a_0 : \ldots : a_v]) = 0$. But, if $f(a_0, \ldots, a_v) \neq 0$ then $f(b_0, \ldots, b_v)$ will, in general, not be equal to $f(a_0, \ldots, a_v)$—they'll differ by a term of the form λ^d. Thus, in this case $f([a_0 : \ldots : a_v])$ does not make sense. All that makes sense is whether $[a_0 : \ldots : a_v] \in \mathbb{P}^v(R)$ is the zero of a homogenous polynomial f.

Example 17.14

Take $f(x,y,z) = x^2 + y^2 + z^2 \in \mathbb{Q}[x,y]$. It makes sense to consider $P_f(\mathbb{Q})$, but it doesn't make sense, for example, to write $f([1:1:1])$. Indeed, $f(1,1,1) = 3$ but $[1:1:1] = [2:2:2]$ and $f(2,2,2) = 12$.

Suppose now that R is one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. If $f \in R[x_1, \ldots, x_v]$ is homogenous, we have a natural map

$$X_f(R) - \{(0, \ldots, 0)\} \to P_f(R) \tag{476}$$

given by

$$(a_0, \ldots, a_v) \mapsto [a_0 : \ldots : a_v] \tag{477}$$

Moreover, this map will evidently be surjective, and two points $(a_0, \ldots, a_v)$ and $(b_0, \ldots, b_v)$ in $X_f(R)$ will map to the same point of $P_f(R)$ if and only if they differ by scalar multiplication. Thus, we see that $P_f(R)$ really does fulfill our initially stated desire (in the motivation) of eliminating the scalar multiplication redundancy in $X_f(R)$ (of course, ignoring the zero solution).

We record this as a lemma:

Lemma 17.8

Let $v \in \mathbb{N}^*$ and let R be any of $\mathbb{Z}/p\mathbb{Z}$ where p is a prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. If $f \in R[x_0, \ldots, x_v]$ is homogenous, the map

$$X_f(R) - \{(0, \ldots, 0)\} \to P_f(R) : (a_0, \ldots, a_v) \mapsto [a_0 : \ldots : a_v] \tag{478}$$

is surjective. Moreover, given a point $[a_0 : \ldots : a_v] \in P_f(R)$ its preimage in $X_f(R)$ is precisely $(\lambda a_0, \ldots, \lambda a_v)$ such that $\lambda \in R - \{0\}$.

We state the analogous result for $R = \mathbb{Z}$ for later use:

Lemma 17.9

Let $v \in \mathbb{N}^*$ and let $f(x_0, \ldots, x_v) \in \mathbb{Z}[x_0, \ldots, x_v]$. Then,

$$X_f(\mathbb{Z}) = \{(\lambda a_0, \ldots, \lambda a_v) : \lambda, a_0, \ldots, a_v \in \mathbb{Z},\ \gcd(a_0, \ldots, a_v) = 1,\ \text{and}\ [a_0 : \ldots : a_v] \in P_f(\mathbb{Z})\} \tag{479}$$

Thus, from this we see that to find $X_f(\mathbb{Z})$ it really suffices to find $P_f(\mathbb{Z})$. But, as was our original motivation, $P_f(\mathbb{Z})$ can be directly and simply related to $P_f(\mathbb{Q})$, as the following lemma shows:

Lemma 17.10

Let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$ be homogenous. Then, the natural map

$$P_f(\mathbb{Z}) \to P_f(\mathbb{Q}) \tag{480}$$

given by $[a_0 : \ldots : a_v]$ maps to itself, is a bijection.

Thus, we see that, in general, to compute $X_f(\mathbb{Z})$ it really suffices to compute $P_f(\mathbb{Q})$. Thus, combining this Lemma **??** with we do see that, using projective coordinates, we can simply phrase in what way we can understand $X_f(\mathbb{Z})$, for a homogenous polynomial f, in a complete way using $X_f(\mathbb{Q})$. Thus, for homogenous polynomials, we really have available to us rational methods.

Another thing that follows from Lemma 17.8 is that if f is a homogenous polynomial in $\mathbb{Z}/p\mathbb{Z}[x_0, \ldots, x_v]$, the relationship between the size of $X_f(\mathbb{Z}/p\mathbb{Z})$ and $P_f(\mathbb{Z}/p\mathbb{Z})$ is quite simple:

Lemma 17.11

Let v be an element of $\mathbb{N}^*$ and p a prime. Let $f(x_1, \ldots, x_v) \in \mathbb{Z}/p\mathbb{Z}[x_1, \ldots, x_v]$ be homogenous. Then, $\#X_f(\mathbb{Z}/p\mathbb{Z}) = (p-1)(\#P_f(\mathbb{Z}/p\mathbb{Z})) + 1$.

Proof 17.3

See Exercise 17.1.

Thus, in particular, we also see that if we are just interested in computing $\#X_f(\mathbb{Z}/p\mathbb{Z})$ for a homogenous polynomial f, considering $P_f(\mathbb{Z}/p\mathbb{Z})$ instead $X_f(\mathbb{Z}/p\mathbb{Z})$ is really no large loss since we can easily recover $\#X_f(\mathbb{Z}/p\mathbb{Z})$ from $\#P_f(\mathbb{Z}/p\mathbb{Z})$. This opens us up to using 'projective techniques' to compute $\#X_f(\mathbb{Z}/p\mathbb{Z})$.

17.6 Picturing $P_f(R)$

We would similarly like to explain how one can picture $P_f(R)$ and discuss some particular examples. Namely, we will write down analogues of the main theorems we wrote down to picture $\mathbb{P}^v(R)$ for $P_f(R)$ and then interpret them thusly.

To begin with, we write down the analogue of Lemma 17.3:

Lemma 17.12

Let $v \in \mathbb{N}^*$ and let R be $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x_0, \ldots, x_v) \in R[x_0, \ldots, x_v]$. Then,

$$X_f(R) = \bigcup_{\ell \in L(f)} \ell \tag{481}$$

where $L(f)$ is the set of lines intersecting $X_f(R)$. Moreover, one can identify $L(f)$ with $P_f(R)$ under the bijection from Lemma 17.3.

In other words, we can interpret this as saying that $X_f(R)$ is a union of some set $L(f)$ of lines in R^{v+1}, and thinking of $P_f(R)$ as a subset of $\mathbb{P}^v(R)$, the lines in R^{v+1}, we have that $L(f)$ is precisely $P_f(R)$. In some sense, this is a more geometric way of phrasing Lemma 17.8.

We now write down the analogue of Lemma 17.4:

Lemma 17.13

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x, y) \in R[x, y]$. Then,

$$P_f(R) = (P_f(R) \cap \{[s:1] : s \in R\}) \cup (P_f(R) \cap \{[1:0]\}) \tag{482}$$

Moreover, if we set $g(s) := f(s, 1)$ then the map $s \mapsto [s:1]$ is a bijection

$$X_g(R) \to P_f(R) \cap \{[s:1] : s \in R\} \tag{483}$$

Moreover,

$$P_f(R) \cap \{[1:0]\} = \begin{cases} \{[1:0]\} & \text{if} \quad f(1,0) = 0 \\ \varnothing & \text{if} \quad f(1,0) \neq 0 \end{cases} \tag{484}$$

Proof 17.4

This is evident from Lemma 17.4 except, perhaps, the claim that $s \mapsto [s:1]$ is a bijection $X_g(R) \to P_f(R) \cap \{[s:1] : s \in R\}$. But, note that $[s:1] \in X_g(R)\{[s:1] : s \in R\}$ if and only if $0 = f(s,1) = g(s)$. The conclusion follows.

We use this to show how to explicitly understand a very simple example of a projective equation:

Example 17.15

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $\alpha, \beta \in R$ and assume that $\alpha \neq 0$. Set $f(x,y) := \alpha x^2 + b\beta^2$. Then, $P_f(R)$ is in bijection with $X_h(R)$ where $h(s) := s^2 + \beta\alpha^{-1}$. In particular, we see that $\#P_f(R)$ is in bijection with the number of square roots of $-\beta\alpha^{-1}$ in R. So, if $R = \mathbb{Z}/p\mathbb{Z}$ then $\#P_f(\mathbb{Z}/p\mathbb{Z}) = 1 + \left(\frac{-\alpha\beta}{p}\right)$ (recall that $\left(\frac{\alpha^{-1}}{p}\right) = \left(\frac{\alpha}{p}\right)$).

To see this we note that $f(1,0) = a \neq 0$. Thus, we see that $P_f(R) \cap \{[1:0]\} = \varnothing$. Moreover, we note then that by Lemma 17.13 that $P_f(R)$ is in bijection with $X_g(R)$ where $g(s) = f(s,1) = \alpha s^2 + \beta$. But, it's clear that $g(s) = 0$ if and only if $h(s) = 0$. The claim then follows.

We now move on to the more complicated, contentful, analogue of Lemma 17.6:

Lemma 17.14

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x,y,z) \in R[x,y,z]$. Then,

$$P_f(R) = (P_f(R) \cap \{[s:t:1] : s,t \in R\}) \cup (P_f(R) \cap \{[a:b:0] : a,b \in R \text{ not all zero}\}) \tag{485}$$

Moreover, if we set $g(s,t) := f(s,t,1)$ and if we set $h(a,b) := g(a,b,0)$ then there is a bijection

$$X_g(R) \to P_f(R) \cap \{[s:t:1] : s,t \in R\} \tag{486}$$

given by $(s,t) \mapsto [s:t:1]$ and a bijection

$$P_h(R) \to P_f(R) \cap \{[a:b:0] : a,b \in R \text{ not all zero}\} \tag{487}$$

given by $[a:b] \mapsto [a:b:0]$.

We will often times refer to the set $P_f(R) \cap \{[a:b:0] : a,b \in R \text{ not all zero}\}$ as the *boundary* of $X_g(R)$ in $\mathbb{P}^2(R)$ and denote it $\partial X_g(R)$.

Remark 17.7

For those that have seen some amount of basic topology, one can understand the above terminology of 'boundary' as follows. Recall that if X is a topological space and $S \subseteq X$ is a subset then its *boundary* ∂S is $\overline{S} - S^\circ$, the closure of S (in X) minus the interior of S (in X). If one takes, for example, $R = \mathbb{C}$ in the above defintion all objects involved inherit a topology (which we won't define here). One can then show that $\partial X_g(\mathbb{C})$ really is the boundary of $X_g(\mathbb{C})$ in $P_f(\mathbb{C})$.

We would, in particular, like to understand a corollary of Lemma 17.14 in the case of counting over $\mathbb{Z}/p\mathbb{Z}$:

Corollary 17.1

Let p be a prime and let $f(x,y,z) \in \mathbb{Z}/p\mathbb{Z}[x,y,z]$ be homogenous. Then,

$$\#P_f(\mathbb{Z}/p\mathbb{Z}) = \#X_g(\mathbb{Z}/p\mathbb{Z}) + \#\partial X_g(\mathbb{Z}/p\mathbb{Z}) \tag{488}$$

Let us now use all three of these theorems to understand a particular example:

Example 17.16

Let us try to suss out what $P_f(\mathbb{R})$ is where $f(x,y,z) := x^2 + y^2 - z^2$. Let us begin by using Lemma 17.14 to reduce the computation of $P_f(\mathbb{R})$ to that of $X_g(\mathbb{R})$ where $g(s,t) = s^2 + t^2 - 1$ and $P_h(\mathbb{R})$ where $h(a,b) = a^2 + b^2$. Note that, almost by definition, $X_g(\mathbb{R}) = S^1$. And, by Example 17.15 we see that $P_h(\mathbb{R})$ is empty since -1 is not a square in $\mathbb{R}$. Thus, we see that $P_f(\mathbb{R})$ is naturally identified with S^1.

How can we picture this? Well, by Lemma 17.12 we know that $X_f(\mathbb{R})$ is a union of lines, and this set of lines can be identified with $P_f(\mathbb{R})$. Well, if one graphs $X_f(\mathbb{R}) \subseteq \mathbb{R}^3$ one finds that it's two cones whose vertices meet at the origin (it looks like an hourglass). Now, we see that $X_f(\mathbb{R})$ is, indeed, a union of these 'diagonal lines' comprising the sides of the double cone. Note then that we should be able to identify $P_f(\mathbb{R})$ with the set obtained by crunching these lines to a point. But, notice that if we fix the z-value, say r, then on each of these diagonal lines that comprise $X_f(\mathbb{R})$ there is a untion point with that z-value—this is clear since moving along one of these lines corresponds to scalar multiplication, which changes the z-value. Thus, a natural set to take that consists of exactly one point on each of these lines, and thus a natural way to think about crunching the lines to points, is the set $(x,y,z) \in P_f(\mathbb{R})$ with $z = r$ for some $r \in \mathbb{R}$. But, we then see that this set is precisely the set of $\{(x,y,r) : x^2 + y^2 = r^2\}$. In other words, we can identify this level set with a circle of radius r. Thus, we, again, see that $P_f(\mathbb{R})$ looks like a circle.

17.7 Exercises

Exercise 17.1

Problem: Prove Lemma 17.11

Exercise 17.2

Problem: Prove Lemma 18.1.

Exercise 17.3

Problem: Prove Lemma 17.2.

Exercise 17.4

Problem: Show that for any

18 Lecture 18: Projective conics

18.1 Setup

In this lecture we would like to show how thinking projectively, and geometrically, will allow us to explicitly parameterize the solutions to certain types of projective equations. Namely, we will show that if $f(x,y,z) \in R[x,y,z]$ is a ternary quadratic form, then $P_f(R)$ can be understood very simply, and geometrically in terms of projective geometry. We will use this to understand the solutions to the Fermat Diophantine equation $x^2+y^2=z^2$ as well as answer, in the affirmative, Question 16.4.

18.2 Conic sections

We begin by defining the type of projective equations that we will be interested in for this section:

Definition 18.1

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. A *(projective) conic section over* R is a set of the form $P_f(R)$ where $f(x,y,z) \in R[x,y,z]$ is a ternary quadratic form (i.e. a homogenous polynomial of degree 2).

Example 18.1

The circle S^1 is a conic section over $\mathbb{R}$ since, as we saw in Example 17.16 we have that S^1 can be identified with $P_f(\mathbb{R})$ where $f(x,y,z)=x^2+y^2-z^2$.

Example 18.2

More generally, any ellipse $\left(\frac{x}{\alpha}\right)^2+\left(\frac{y}{\beta}\right)^2=1$, where $\alpha,\beta>0$ are elements are $\mathbb{R}$, is a conic section. Indeed, one can easily generalize the last example show that this ellipse can be identified with $P_f(\mathbb{R})$ where $f(x,y,z)=\left(\frac{x}{\alpha}\right)^2+\left(\frac{y}{\beta}\right)^2-z^2$.

Remark 18.1

These examples suggest that when one thinks of a conic section one should, in some sense, think of an ellipse. Using the very imprecise caricature obtained by thinking of $\mathbb{P}^2(\mathbb{R})$ as S^2 (as discussed in Example 17.12) we are often times wont to think of a conic section $P_f(R)$ inside of $\mathbb{P}^2(R)$ as looking something like an ellipse in S^2 (something like a great circle in S^2). Again, this picture can be helpful to intuitively understand what geometrically conic sections look like, but they can also be somewhat misleading, so some caution must be taken.

Of course, one must be careful in using this ellipse picture in the case when one has a somewhat 'degenerate' ternary quadratic form (a term we will make precise later). Namely, if we take our

$f(x,y,z)$ to be something quite silly, we can get that $P_f(R)$ can look not like an ellipse but something simpler (e.g. the union of two lines—see §(ALEX)). Thus, this ellipse picture is really only accurate for 'non-degenerate' ternary quadratic forms.

Our goal in this section is to show that conic sections can be understood quite simply in terms of projective geometry. But, since we are going to be focusing on conic sections themselves, not necessarily the ternary quadratic form that defines it, we would like to understand conditions by which two ternary quadratic forms define essentially equivalent conic sections.

To this end, let us make the following definition:

Definition 18.2

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x,y,z)$ and $g(x,y,z)$ be ternary quadratic forms in $R[x,y,z]$. We say that f and g are *equivalent*, and write $f \sim g$, if there exists a 3×3 invertible matrix $\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ over R such that

$$g(x,y,z) = f(a_{11}x + a_{12}y + a_{13}z, a_{21}x + a_{22}y + a_{33}z, a_{31}x + a_{3x}y + a_{33}z) \tag{489}$$

Example 18.3

Recall that a 3×3 invertible matrix over R is a 3×3 matrix A with entries in R such that $\det(A) \neq 0$ where, be careful, one is thinking of $\det(A)$ as an element of R (e.g. if $R = \mathbb{Z}/p\mathbb{Z}$ the one needs that $\det(A) \neq 0 \mod p$).

Example 18.4

Note that $f(x,y,z) = x^2 - 2y^2 + 5z^2$ is equivalent to $g(x,y,z) = -2x^2 - 38xy - 38xz - 49y^2 - 154yz - 99z^2$ as one can take the matrix $\begin{pmatrix} 1 & 1 & 3 \\ 2 & 5 & 8 \\ 1 & 0 & 2 \end{pmatrix}$.

A conceptually simpler way to understand equivalence is made by realizing that ternary quadratic forms, themselves, can be understood in terms of matrices. For this we assume that $R \neq \mathbb{Z}/2\mathbb{Z}$ (so that 2 is invertible in R). Namely, let us note that the general form of a ternary quadratic form is the following:

$$\alpha x^2 + \gamma xy + \beta y^2 + \mu xz + \varepsilon yz + \delta z^2 \tag{490}$$

And, if we take v to be the column vector $v := \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ then we have that

$$\alpha x^2 + \mu xy + \beta y^2 + \delta xz + \varepsilon yz + \gamma z^2 = v^\top M_f v \tag{491}$$

where $(-)^\top$ denotes transpose and M_f is the following matrix

$$M_f := \begin{pmatrix} \alpha & \frac{1}{2}\mu & \frac{1}{2}\delta \\ \frac{1}{2}\mu & \beta & \frac{1}{2}\varepsilon \\ \frac{1}{2}\delta & \frac{1}{2}\varepsilon & \gamma \end{pmatrix} \tag{492}$$

which is called the matrix *defining* f.

We then have the following basic observation concerning equivalence:

Lemma 18.1

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ for an odd prime p, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x,y,z)$ and $g(x,y,z)$ be ternary quadratic forms in $R[x,y,z]$. Then, f and g are equivalent if and only if there exists a 3×3 invertible matrix A over R such that

$$M_g = A^\top M_f A \tag{493}$$

Proof 18.1

Note that $f\sim g$ is equivalent to the existence of a 3×3 invertible matrix A over R such that, writing $v := \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, we have that $g(v) = f(Av)$. But writing this in terms of defining matrices this says that

$$v^\top M_g v = (Av)^\top M_f (Av) = v^\top (A^\top M_f A) v \tag{494}$$

It's not hard to see that this then implies, as v can vary over all of R^3, that $M_g = A^\top M_f A$. The conclusion follows.

The reason why equivalence is useful when studying conic sections is the following observation:

Lemma 18.2

Let R be $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x,y,z)$ and $g(x,y,z)$ be equivalent ternary quadratic forms in $R[x,y,z]$. Then, $P_f(R)$ is naturally in bijection with $P_g(R)$.

Proof 18.2

Take an invertible 3×3 matrix A such that $g(v) = f(Av)$ forall $v\in R^3$. Note that A defines a bijection $R^3\to R^3$. Since this bijection takes 0 to 0 and satisfies $A(\lambda v) = \lambda A(v)$ it's not hard to see that A descends to a bijection $\mathbb{P}^2(R)\to\mathbb{P}^2(R)$. The equation $g(v) = f(Av)$ then implies that A maps $P_g(R)$ bijectively to $P_g(f)$. The conclusion follows.

Thus, if we are interested in understanding conic sections, equivalent forms give essentially equal conic sections. Thus, we are really only interested in ternary quadratic forms up to equivalence. And, as Example 18.4 shows, one can have that quite complicated ternary quadratic forms can be equivalent to quite simple ones. This gives one hope that, perhaps, all ternary quadratic forms are equivalent to particularly simple ones. This, as it turns out, is true.

To state this rigorously, let us make the following definition:

Definition 18.3

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, a ternary quadratic form $f(x,y,z)\in R[x,y,z]$ is called *diagonal* if $f(x,y,z) = \alpha x^2 + \beta y^2 + \gamma z^2$ for some $\alpha,\beta,\gamma\in R$ (necessarily all not zero).

For example, in Example 18.4 we saw that a very complicated quadratic form was equivalent to a diagonal one. This is true generally:

Lemma 18.3

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, every ternary quadratic form is equivalent to a diagonal one.

Proof 18.3

See Exercise 18.1.

Remark 18.2

There are multiple ways to attack proving Lemma 18.3, one being outlined in Exercise 18.1. Alternatively, one can think of the procedure of diagonalization as being a repeated application of the notion of completing the square. Of course, to explain this rigorously gets a little messy without matrices and, ultimately, is equivalent to the one outlined in Exercise 18.1.

Thus, in essence, Lemma 18.3 in conjunction with Lemma 18.2 shows that to study conic sections, we really only need to concern ourselves with diagonal ternary quadratic forms.

In particular, one can use the notion of diagonal forms to define important notions for general ternary quadratic forms. Namely, let us make the following definition:

Definition 18.4

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x,y,z) \in R[x,y,z]$ be a ternary quadratic form. We say that f is *non-degenerate* if $f(x,y,z)$ is equivalent to a diagonal form $\alpha x^2 + \beta y^2 + \gamma z^2$ with α, β, γ all non-zero.

Let us note that this notion is well-defined. Namely, note that the diagonal form in Lemma 18.3 is not unique. That said, the number of non-zero coefficients in its diagonal representation is unique. Indeed, note that saying that $f(x,y,z)$ is equivalent to $\alpha x^2 + \beta y^2 + \gamma z^2$ is equivalent to saying that

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} = A^\top M_f A \tag{495}$$

for some invertible matrix A. Note then that this implies that

$$\operatorname{rk} \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} = \operatorname{rk}(A^\top M_f A) = \operatorname{rk}(M_f) \tag{496}$$

where rk stands for the rank of a matrix. The last equality holds true since A and $A^\top$ are invertible. Finally, observe that $\operatorname{rk} \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ is the number of α, β, and γ that are non-zero.

In fact, this thought process shows the following:

Lemma 18.4

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x,y,z) \in R[x,y,z]$ be a ternary quadratic form. Consider the following conditions:

1. f is non-degenerate.
2. M_f is invertible.
3. P_f is smooth over R.
4. f cannot be written in the form $l_1 \cdot l_2$ where $l_1 \cdot l_2$ where l_1 and l_2 are homogenous elements of $R[x,y,z]$ of degree 1.

Then, properties 1., 2., and 3. are equivalent and 1. implies 4.

Before we prove this, we make the following definition of smoothness of P_f:

Definition 18.5

Let $v \in \mathbb{N}^*$ and let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x_0,\ldots,x_v) \in R[x_0,\ldots,x_v]$ be homogenous. We say that P_f is *smooth over* R if for all $[a_0 : \ldots : a_v] \in P_f(R)$ we have that $df(a_0,\ldots,a_v) \neq 0$.

Note that $df(a_0,\ldots,a_v)$ being non-zero is well-defined, since if we replace $(a_0,\ldots,a_v)$ by a non-zero scalar multiple λ this multiplies df by λ, and thus doesn't change zeroness.

Proof 18.4: Lemma 18.4

The fact that 1. and 2. are equivalent follows immediately from the fact that $\mathrm{rk}(M_f)$ is the number of non-zero coefficients in a diagonal from equivalent to f, and the fact that M_f diagonal is equivalent to $\mathrm{rk}(M_f) = 3$.

Example 18.5

The ternary quadratic form $f(x,y,z)$

Example 18.6

The ternary quadratic form $f(x,y,z) = x^2 + 5y^2 + xz + z^2$ in $\mathbb{Z}/7\mathbb{Z}[x,y,z]$ is degenerate. Indeed, it's easy to see that $M_f = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 7 \\ 1 & 7 & 1 \end{pmatrix}$ and $\det(M_f) = -49$ in $\mathbb{Z}/7\mathbb{Z}$.

In fact, one can see that for a ternary quadratic form $f(x,y,z)$ that $\mathrm{rk}(M_f)$ is a measure of how degenerate/non-degenerate f is. Our goal now is to try and understand conic sections $P_f(R)$ in terms of the rank of M_f. The only really challenging, interesting case will be when f is non-degenerate (i.e. $\mathrm{rk}(M_f) = 3$), so this will be our first focus.

18.3 Non-degenerate conic sections

Our goal in this section is to show that if $P_f(R)$ is a non-degenerate conic section then we can explicitly parametrize all of the points of $P_f(R)$ given a single point $p_0 \in P_f(R)$. This will allow us to, in particular, understand the Fermat Diophantine equation $x^2+y^2=z^2$ and given an affirmative answer to Question 16.4.

Projective lines

Before we start trying to understand non-degenerate conic sections, it will first be incredibly useful to understand the notion of projective lines as this will be one of the main geometric inputs used for our desired parametrization.

To start, we should explain what we mean by a projective line. This is somewhat confusing, but standard terminology. The reason it's confusing is that projective space itself is made of lines, and these are not the lines we are referencing when we say 'projective line'. What we mean more is something like a 'line on projective space'.

Before we explain the intuition for what this means, let us make the rigorous definition:

Definition 18.6

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, a *projective line* in $\mathbb{P}^2(R)$ is a subset L of $\mathbb{P}^2(R)$ of the form $L=P_l(R)$ where $l(x,y,z)$ is a homogenous polynomial of degree 1.

So, we would like to discuss some examples of projective lines, but before we do let us explain what a projective line 'looks like'. Note that if $l(x,y,z) \in R[x,y,z]$ is a homogenous polynomial of degree 1, then $X_l(R) \subseteq R^3$ is not a line, but a plane. When we then crunch lines to points, to go to $\mathbb{P}^2(R)$, we see that the plane, a 2-dimensional object, becomes a 1-dimensional object. In other words, if one thinks of a plane in R^3 as being a 'a line of lines' then the image of this plane in $\mathbb{P}^2(R)$, which is what we are calling a projective line, is like a line on projective space.

Let us give an example:

Example 18.7

Let $l(x,y,z)=z$. Then, $P_l(R)$ is precisely the set $\{[a:b:0] : a,b \in R \text{ not both zero}\}$. This is a set we have seen come up before in the context of Lemma 17.6 and for which we know there is a natural identification with $\mathbb{P}^1(R)$.

Example 18.8

Let $l(x,y,z)=y+z$. Then, $P_l(R)$ is, by definition, the set of $\{[a:b:c] : b+c=0\}$. Note that using Lemma 17.14 we see that we can identify $P_l(R)$ with the union of $X_g(R)$ (where $g(s,t)=s+1$) and $P_h(R)$ where $h(a,b)=b$. Now, note that $X_g(R)$ is a line in R^2 and thus can evidently be identified with R. Note that $P_h(R)$ is $\{[a:b] : b=0\}$ which is just $\{[1:0]\}$ as in Lemma 17.4. Thus, in this case we see that $P_l(R)$ can be identified with a copy of R and a single extraneous point. Thus, again, the projective line looks like $\mathbb{P}^1(R)$.

As these example suggest, one might imagine that every projective line looks like a copy of $\mathbb{P}^1(R)$ inside of $\mathbb{P}^2(R)$. This is, in fact, correct:

Lemma 18.5

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then, for every projective line $L \subseteq P^2(R)$ there exists a natural bijection between L and $\mathbb{P}^1(R)$.

Thus, in some sense, projective lines inside of $\mathbb{P}^2(R)$ are something like copies of $\mathbb{P}^1(R)$ inside of $\mathbb{P}^2(R)$.

Proof 18.5: Lemma 18.5

Write $L = P_l(R)$ for some homogenous polynomial $l(x, y, z) \in R[x, y, z]$ of degree 1. If $l(x, y, z) = z$ then we have seen how to do this in Example 18.7 the identification. For general l, note that we can take an invertible 3×3 matrix A over R such that $l(A(x, y, z)) = z$. One can then define the identification $L \to \mathbb{P}^1(R)$ as the precomposition of the bijection from the previous sentence with A.

We would now like to understand the basic properties of projective lines. Perhaps the most obvious thing one would want to know is whether, like normal lines (not necessarily through the origin), projective lines have the property given any two points p_0 and p_1 in $\mathbb{P}^2(R)$ there exists a unique projective line L in $\mathbb{P}^2(R)$ such that p_0 and p_1 both lie on L (i.e. such that $p_0 \in L$ and $p_1 \in L$).

Not shockingly, this is the case:

Lemma 18.6

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let p_0 and p_1 be distinct points of $\mathbb{P}^2(R)$. Then, there exists a unique projective line L such that p_0 and p_1 lie on L.

Proof 18.6

Let us write $p_0 = [a : b : c]$ and $p_1 = [a' : b' : c']$ for some $a, b, c, a', b', c' \in R$. Note then that giving a projective line containing p_0 and p_1 is equivalent to giving a plane $P \subseteq \mathbb{P}^2(R)$ such that (a, b, c) and (a', b', c') in P. Note that since p_0 and p_1 are distinct points of $\mathbb{P}^2(R)$ we have that (a, b, c) and (a', b', c') don't differ by scalars, and thus are linearly independent. Thus, there exists a unique plane P containing (a, b, c) and (a', b', c') (namely the plane spanned by (a, b, c) and (a', b', c')). The claim follows.

The only other bit of information we need about projective lines to study non-degenerate conics is to understand the set of projective lines that pass through a given point p_0. Namely, let us make the following notational definition:

Definition 18.7

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $p_0 \in \mathbb{P}^2(R)$ be fixed. Let us denote by $\mathscr{L}(p_0)$ the set of all projective lines L in $\mathbb{P}^2(R)$ such that $p_0 \in L$.

Let us explore a simple example before we state the general result:

Example 18.9

Let us take $p_0 = [0:0:1]$. We claim that, in this case, there is a natural identification between $\mathscr{L}(p_0)$ and $\mathbb{P}^1(R)$. Indeed, note that if $l(x,y,z) = \alpha x + \beta y + \gamma z$ then $L := P_l(R)$ contains p_0 if and only if $\gamma = 0$. Thus, we see that $\mathscr{L}(p_0)$ is equal to the set of $L = P_l(R)$ where $l(x,y,z) = \alpha x + \beta y$ for some $\alpha, \beta \in R$ where α and β are non-zero. Note that if $\lambda \in R$ is non-zero then $\lambda\alpha x + \lambda\beta y$ defines a projective line in $\mathbb{P}^2(R)$ which is equal to L. Thus, we see that scalar multiplying a homogenous linear polynomial doesn't affect the associated projective line. In fact, it's clear the converse holds.

Thus, we see that there is a bijection $\mathbb{P}^1(R) \to \mathscr{L}(p_0)$ given by taking $[a:b]$ to the line $L = P_l(R)$ with $l(x,y,z) = ax + by$.

As this lemma suggests, the projective lines passing through a given point p_0 should be identifiable with $\mathbb{P}^1$ where, roughly, one thinks of associating to an element $L \in \mathscr{L}(p_0)$ the 'slope' of the line passing through it. This is a little bit imprecise, so we give the following rigorous statement and proof:

Lemma 18.7

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Then,

1. For any $p_0 = [a_0 : b_0 : c_0]$ and $p_1 = [a_1 : b_1 : c_1]$ points of $\mathbb{P}^2(R)$ and A an invertible 3×3 matrix over R such that A maps (a_0, b_0, c_0) to (a_1, b_1, c_1) we have that $A \mapsto A(L)$ induces a bijection $\mathscr{L}(p_0) \to \mathscr{L}(p_1)$.
2. Giving an A such that takes $(0,0,1)$ to (a_0, b_0, c_0) produces a bijection $\mathbb{P}^1(R) \to \mathscr{L}(p_0)$ by composing the bijection from 1. together with the bijection from Example 18.9.

Proof 18.7

See Exercise 18.2.

Let us give an example to see what this would look like for a different point p_0 than that from Example 18.9:

Example 18.10

Set $p_0 := [1:0:1]$. Note then that if $l(x,y,z) = \alpha x + \beta y + \gamma z$ and $L := P_l(R)$, then $p_0 \in L$ if and only if $\alpha = -\gamma$. Thus, we see that the elements of $\mathscr{L}(p_0)$ are those of the form $L = P_l(R)$ with $l(x,y,z) = \alpha x + \beta y - \alpha z$ for some $\alpha, \beta \in R$ both non-zero. Since scaling the coefficients α and β by $0 \neq \lambda \in R$ doesn't affect the projective line L (the two equations define the same projective line) we see that we get a natural bijection $\mathbb{P}^1(R) \to \mathscr{L}(p_0)$ given by $[a:b]$ maps to $P_l(R)$ where $l(x,y,z) = ax + by - az$.

We note that this is the same thing as the bijection from Lemma 18.7 part 2. by taking A to be $\begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Indeed, note that this matrix does take $(0,0,1)$ to p_0. Note that the bijection $\mathbb{P}^1(R) \to \mathscr{L}([0:0:1])$ takes $[a:b]$ to $l(x,y,z) := ax + by$. The bijection $\mathscr{L}([0:0:1])$ then takes this to $l(A(x,y,z)) = a(z-x) - by = -ax - by + az$. Note then that the projective line associated to this equation is the same as that associated to he equation $ax + by - az$ (since they differ by the scalar -1).

Thus, we see that the bijections are the same.

Parameterizing the points on a non-degenerate conic

We are now ready to explain the beautiful, geometric way that one can parametrize all the points of a non-degenerate of a non-degenerate conic given one point on the conic. The rough, geometric idea is to copy the idea of stereographic projection discussed in Example 17.10 and Example 17.11. Namely, given a point $p_0 = [a_0 : b_0 : c_0]$ on a non-degenerate conic $P_f(R)$ we should be able to take a line L in $\mathscr{L}(p_0)$ and this line should pass through precisely one extra point p of $P_f(R)$. This is consistent with picturing $P_f(R)$ as a circle, in which case this, at least as a caricature, does look a lot like actual stereographic projection from Example 17.10.

Our goal is then try to show that this geometric process gives a bijection $\mathscr{L}(p_0) \to P_f(R)$. Then, of course, choosing any matrix A such that $A(0,0,1) = (a_0, b_0, c_0)$ allows us to apply Lemma 18.7 part 2. to give a bijection $\mathbb{P}^1(R) \to P_f(R)$. This bijection will allow us to explicitly parametrize the points of $P_f(R)$ in terms of the simple object $\mathbb{P}^1(R)$.

Of course, the above sketched argument is fraught with many technical pitfalls. Amongst these, the most obvious and pressing is the claim that if $L \in \mathscr{L}(p_0)$ then L passes through precisely two points of $P_f(R)$. In fact, this is not quite true, as there are lines L which pass only through p_0. This will turn out to be OK though, since the above procedure doesn't tell us how to obtain $p_0 \in P_f(R)$ from a line $L \in \mathscr{L}(p_0)$ and the answer will be that we will associate to a line $L \in \mathscr{L}(p_0)$ such that $P_f(R) \cap L = \{p_0\}$ the point $p_0 \in P_f(R)$. That said, while the claim that $L \cap P_f(R)$ always contains exactly two points is not always true it is, ignoring lines where $L \cap P_f(R) = \{p_0, p\}$, essentially correct. This claim is the real important part about where the non-degeneracy of f is used since, as we will see later, this claim is <u>not</u> correct if f is assumed to be degenerate.

So, let us begin by showing that for non-degenerate f this property does, in fact, hold:

Lemma 18.8

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x,y,z) \in R[x,y,z]$ be a non-degenerate ternary quadratic form. Then, if $l(x,y,z) \in R[x,y,z]$ is homogenous of degree 1 and $L := P_l(R)$ then $L \cap P_f(R)$ has at most 2 points.

Proof 18.8

Let A be a 3×3 invertible matrix over R such that $g(v) := f(Av)$ is diagonal, say $g(x,y,z) = \alpha x^2 + \beta y^2 + \gamma z^2$ where, since f is non-dgenerate, we know that all of α, β, and γ are non-zero. Note then that we get a bijection $A : P_g(R) \to P_f(R)$ given by $p \mapsto A(p)$. Note then that if we set $p_0' \in P_g(R)$ to be $A^{-1}(p_0)$ then there for any $L \in \mathscr{L}(p_0')$ then the association $p \mapsto A(p)$ is a bijection $L \cap P_g(R) \cap A(L) \cap P_f(R)$. Since $L \mapsto A(L)$ is a bijection $\mathscr{L}(p_0') \to \mathscr{L}(p_0)$, we conclude that the claim of the lemma holds for f if and only if it holds for g. Thus, we may assume that $f(x,y,z)$ is diagonal.

So, let $f(x,y,z) = \alpha x^2 + \beta y^2 + \gamma z^2$ be a non-degenerate diagonal ternary quadratic form. Let $p_0 = [a_0 : b_0 : c_0] \in P_f(R)$ be given. Let $L \in \mathscr{L}(p_0)$. We then need to show that $L \cap P_f(R)$ contains at most two points. Let us say that $L = P_l(R)$ where $l(x,y,z) = \alpha' x + \beta' y + \gamma' z$. Then, we see that

$$L \cap P_f(R) = \{[a : b : c] : f(a,b,c) = 0 \text{ and } l(a,b,c) = 0\} \tag{497}$$

Now, since l is not the zero polynomial we know that, without loss of generality, that one of the coefficients is non-zero. Without loss of generality we may assume that $\gamma' \neq 0$ and, since scaling doesn't change the projective line, we may as well assume that $\gamma' = -1$. Then, we see that

$$L \cap P_f(R) = \{[a : b : c] : \alpha a^2 + \beta b^2 + \gamma c^2 = 0 \text{ and } c = \alpha' a + \beta' b\} \tag{498}$$

Note that the equation $c = \alpha' a + \beta' b$ implies that c is determined by a and b. Note, also, that it implies that a and b cannot both be zero since then $c = 0$. Finally, note that if we scale a and b by a sclar, then the equation $c = \alpha' a + \beta' b$ implies that c scales by the same scalar. In conclusion we see that determining $[a : b : c]$ is equivalent to determining $[a : b]$ in $\mathbb{P}^1(R)$. In other words, we see that the set $L \cap P_f(R)$ is in bijection with the set of $[a : b] \in \mathbb{P}^1(R)$ such that (combining our equations) we have

$$\alpha a^2 + \beta b^2 + \gamma(\alpha' a + \beta' b)^2 = 0 \tag{499}$$

or, rewriting this

$$(\alpha + \gamma(\alpha')^2)a^2 + (\beta + \gamma(\beta')^2)b^2 + 2\gamma\alpha'\beta' ab = 0 \tag{500}$$

Note though that we can complete the square and make a linear change of variables to write this as $Aa^2 + Bb^2 = 0$ for some $A, B \in R$. By Example 17.15 if one of A or B is non-zero then this equation has at most 2 solutions. Thus, $A = B = 0$. This then implies that all the coefficients of the equation (500) are zero. Note that $2\gamma\alpha'\beta' = 0$ implies that $\alpha' = 0$ or $\beta' = 0$ since 2γ is a unit in R. But, if $\alpha' = 0$ this implies that $0 = \alpha + \gamma(\alpha')^2 = \alpha$ which is impossible. Similarly, if $\beta' = 0$ then $\beta = 0$ which is impossible. Thus, we see that we have arrived at a contradiction.

Remark 18.3

One should note the key last step used, in a pivotal way, that f was non-degenerate. Namely, the fact that $\gamma \neq 0$ was used to deduce that either $\alpha' = 0$ or $\beta' = 0$. The fact that $\alpha \neq 0$ and $\beta \neq 0$ is used to show that neither of these two cases could happen. So, the above really does pivotally use the non-degenerateness of f.

Now that we have this key foundational result we are able to rigorously define our map $\pi : \mathscr{L}(p_0) \to P_f(R)$ as mentioned above. Namely, we define $\pi(L)$ as follows:

$$\pi(L) = \begin{cases} p_0 & \text{if} \quad P_f(R) \cap L = \{p_0\} \\ p & \text{if} \quad P_f(R) \cap L = \{p_0, p\} \text{ with } p \neq p_0 \end{cases} \tag{501}$$

Of course, to make sense of this we need to know that for $L \in \mathscr{L}(p_0)$ we have that $P_f(R) \cap L$ is either of the form $\{p_0\}$ or $\{p_0, p\}$. This is, essentially, the content of Lemma 18.8.

We now need to show that π is bijective. The fact that its image contains $P_f(R) - \{p_0\}$ is clear from Lemma 18.6. Indeed, if $p \in P_f(R) - \{p_0\}$ then by Lemma 18.6 there exists a projective line L such that p and p_0 both lie on L. Then, evidently $P_f(R) \cap L = \{p_0, p\}$ and so $L \in \mathscr{L}(p_0)$ and $\pi(L) = p$. Also, it's clear that for any $p \in P_f(R) - \{p_0\}$ that there is at most one $L \in \mathscr{L}(p_0)$ such that $\pi(L) = p$. Indeed, if $\pi(L_1) = p = \pi(L_2)$ then

$$L_1 \cap P_f(R) = \{p_0, p\} = L_2 \cap P_f(R) \tag{502}$$

which, in particular, implies that L_1 and L_2 both contain p_0 and p. Note that since p_0 and p are distinct points of $\mathbb{P}^2(R)$ they can be represented by linearly independent points of R^3. If one thinks of the planes P_1 and P_2 in R^3 associated to L_1 and L_2 we see that p_0 and p lie in both P_1 and P_2. But, since p_0 and p are linearly independent this implies that P_1 and P_2 are spanned by p_0 and p, and thus equal. Thus, $L_1 = L_2$.

Thus, all that really remains to show is that there is a unique line $L \in \mathscr{L}(p_0)$ such that $\pi(L) = p_0$. Intuitively, this line L would have the property that it intersects $P_f(R)$ at a 'degree higher than 1' since $L \cap P_f(R) = \{p_0\}$ should mean that f is a quadratic polynomial with a double root on L. This, as per usual, should be related to some sort of statment conerning derivative of f since, after all, double roots correspond to zero derivative. This also makes sense geometrically since if one draws a picture of what a line that intersects an ellipse (our picture of non-degenerate concis) at precisely one point p_0, this line is clearly nothing else than the tangent line to $P_f(R)$ at p_0.

Given this, the following is not too surprising:

Lemma 18.9

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x,y,z)$ be a non-degenerate ternary quadratic form in $R[x,y,z]$ and let $p_0 \in P_f(R)$ be fixed. Then, there exists a unique line $L \in \mathscr{L}(p_0)$ such that $\pi(L) = p_0$. This line is the tangent line t_{p_0} defined as the projective line with the following equation

$$\frac{\partial f}{\partial x}(p_0)x + \frac{\partial f}{\partial y}(p_0)y + \frac{\partial f}{\partial z}(p_0)z = 0 \tag{503}$$

We can summarize our above arguments into the following master theorem:

Theorem 18.1

Let R be one of $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Let $f(x,y,z)$ be a non-dgenerate ternary quadratic form in $R[x,y,z]$ and let $p_0 = [a_0 : b_0 : c_0] \in P_f(R)$ be fixed. Then, the map π described by (501) gives a bijection $\mathscr{L}(p_0) \to P_f(R)$. In particular, choosing an invertible 3×3 matrix A over R such that A sends $(0,0,1)$ to (a,b,c) we get a bijection $\mathbb{P}^1(R) \to P_f(R)$.

In the next lecture we will show how to apply this theorem to answer concrete questions concerning non-degenerate conics. To finish out this lecture, we will consider what $P_f(R)$ looks like in the cases when $\text{rk}(M_f) < 3$.

18.4 The case $\text{rk}(M_f) = 2$

18.5 The case $\text{rk}(M_f) = 1$

18.6 Exercises

Exercise 18.1

Problem: Hey

Exercise 18.2

Problem: Hey

19 Lecture 19: Applications of non-degenerate conics

In this lecture we will apply Theorem 18.1 to two particularly interesting examples: the $n = 2$ Fermat equation and Question 16.4.

19.1 The $n = 2$ Fermat theorem

Recall from Example 1.1 that the Diophantine equation $x^n + y^n = z^n$ has essentially no non-trivial solutions when $n \geqslant 3$. This leaves a natural question: what are the solutions to this equation when $n = 2$?

The Diophantine solutions to the Diophantine equation $x^2 + y^2 = z^2$ are often times called *Pythagorean triples*. The reason for this is that if (x,y,z) is a Diophantine solution, then (x,y,z) form the lengths of

the sides of right triangle (with z being the length of the hypotenuse). In fact, it's not hard to see that the ascertainment of the solutions to the Diophantine equation $x^2 + y^2 = z^2$ is actually the same thing as the question of what triples of integers can be the side lengths of a right triangle.

We will now use Theorem 18.1 to actually parameterize the Diophantine solutions to $x^2 + y^2 = z^2$.

To do this, let us set $f(x, y, z) := x^2 + y^2 - z^2$. Let us note that this equation is homogenous of degree 2. Note also that $p_0 := [1 : 0 : 1] \in P_f(\mathbb{Q})$. Thus, from Theorem 18.1 we obtain a natural bijection $\pi : \mathbb{P}^1(\mathbb{Q}) \to P_f(\mathbb{Q})$. Or, said differently, we see that we get a bijection $\pi : \mathbb{P}^1(\mathbb{Z}) \to P_f(\mathbb{Z})$. Let us make this bijection explicit.

Let $[m : n] \in \mathbb{P}^1(\mathbb{Z})$ be given. Then, the element of $\mathscr{L}(p_0)$ corresponding to this is precisely $L = P_l(\mathbb{Q})$ where $l(x, y, z) = mx + ny - mz$ (see Example **??**). We then want to compute $L \cap P_f(\mathbb{Q})$. To do this we merely note that $[a : b : c] \in P_f(\mathbb{Q})$ if and only if $a^2 + b^2 - c^2 = 0$ and $ma + nb - mc = 0$. Let us begin by assuming that $m \neq 0$. In this case we can rewrite this second equation as $a + \frac{n}{m}b = c$. Plugging this into the equation $a^2 + b^2 - c^2 = 0$ gives $a^2 + b^2 - (a + \frac{m}{n}b)^2 = 0$. Expanding this gives $\frac{-2abm}{n} - \frac{b^2m^2}{n^2} + b^2 = 0$. Now, note that if $b = 0$ then it's not hard to see that $[a : b : c]$ would have to be $[1 : 0 : 1]$. So we can assume that $b \neq 0$. Note then that this equation becomes $\frac{-2am}{n} - \frac{bm^2}{n^2} + b = 0$. Or, rearranging we have that $\frac{-2am}{n} = (1 - \frac{m^2}{n^2})b$. Note that this right hand side is non-zero since $b \neq 0$ and $\frac{m^2}{n^2} \neq 1$ since m and n are coprime. Thus, we see that a and m are also non-zero. Thus, we may divide through and see that $\frac{a}{b} = \frac{1-\frac{m^2}{n^2}}{-\frac{2m}{n}} = \frac{m^2-n^2}{2mn}$. Since $c = a + \frac{n}{m}b$ we deduce that $\frac{c}{b} = \frac{m^2 - n^2}{2mn} + \frac{n}{m} = \frac{m^2 + n^2}{2mn}$.

Thus, we see that for $[m : n] \in \mathbb{P}^1(\mathbb{Z})$ with $m \neq 0$ we have that

$$\pi([m : n]) = \left[\frac{m^2 - n^2}{2mn} : 1 : \frac{m^2 + n^2}{2mn}\right] = [m^2 - n^2 : 2mn : m^2 + n^2] \tag{504}$$

If $m = 0$ then we see that $[m : n] = [0 : 1]$ in which case one can check that $\pi([m : n]) = [1 : 0 : 1]$.

In conclusion, we deduce the following:

Theorem 19.1

Let $f(x, y, z) : x^2+y^2-z^2$. Then, $P_f(\mathbb{Z}) = \{[m^2-n^2 : 2mn : m^2+n^2] : m, n \in \mathbb{Z} \text{ are non-zero and coprime}\}$.

This gives a concrete parameterization of the Pythagorean triples.

20 Lecture 20: Local-to-global principles and Legendre's theorem

20.1 Setup

In this lecture we finally attempt to return to Diophantine equations proper, instead of modulus Diophantine equations. In fact, the main question that this lecture seeks to understand is the following natural query. As mentioned at the advent of $\mathbb{Z}/m\mathbb{Z}$, one thinks of $\mathbb{Z}/m\mathbb{Z}$ as a kind of 'model' for $\mathbb{Z}$, but one which doesn't model everything. So, for example, it's possible that one can choose $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$ such that $X_f(\mathbb{Z}) = \varnothing$ even though $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ because $\mathbb{Z}/m\mathbb{Z}$, while a model for $\mathbb{Z}$, doesn't model everything (e.g. it can't model the non-existence of the Diophantine solution).

That said, as m gets bigger $\mathbb{Z}/m\mathbb{Z}$ becomes a better model for $\mathbb{Z}$, in the sense that there is less identification happening when one passes from $\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ as m increases. Thus a naive hope is that if we 'let m tend towards ∞' that the model $\mathbb{Z}/m\mathbb{Z}$ becomes so good that one can actual detect, for example, the non-existence of a Diophantine solution by checking it in $\mathbb{Z}/m\mathbb{Z}$ for all m sufficiently large.

Phrased differently, for a fixed m the statement "$X_f(\mathbb{Z}) \neq \varnothing \implies X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$" is true, but the converse is not—we can't replace $\implies$ by $\iff$. But, if we let 'm tend towards ∞' perhaps the staement does become an if and only if. Less cryptically, one might imagine that the statement "$X_f(\mathbb{Z}) \neq \varnothing \implies$

$X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all m", which is a surrogate statement for 'letting m tend towards ∞', does, in fact, have true converse.

This is a highly desirable property. Indeed, recall from Theorem **??** that there is no general algorithm which will decide whether or not a given $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$ satisfies $X_f(\mathbb{Z}) \neq \varnothing$. That said, there is a clear algorithm to decide whether or not $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ (e.g. one could just brute force check all the finitely many values). If one could check that non-emptiness of $X_f(\mathbb{Z})$ by checking the non-emptiness of $X_f(\mathbb{Z}/m\mathbb{Z})$ for all m or, even better just some m, then there is a hope that one could find an algorithm to check the non-emptiness of $X_f(\mathbb{Z})$.

Unfortunately, it's not the case that every f satisfies the property that $X_f(\mathbb{Z}) \neq \varnothing$ if and only if $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all m. Thus, our goal in this lecture is to really give some meat necessary to discuss what conditions on f are necessary for this property to hold, and what can we say of it.

20.2 The local-to-global principle(s)

Let us now try to formalize the property that we are interested in:

Definition 20.1

Let $v \in \mathbb{N}^*$ and let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Let us say that X_f *satisfies the finite local-to-global principle* if the following two statements are equivalent:

1. $X_f(\mathbb{Z}) \neq \varnothing$.
2. $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all $m \in \mathbb{N}^*$.

Remark 20.1

The inclusion of the word 'finite' in the above may seem a bit strange. The reason for its necessity will soon become clear, when we realize that just checking the non-emptiness of $X_f(\mathbb{Z}/m\mathbb{Z})$ for all m misses one valuable aspect of the non-emptiness of $X_f(\mathbb{Z})$, but the reason that we call this the 'finite' case is a bit more cryptic, and comes from algebraic number theory. We will attempt to give a rough reason for this later in Remark (ALEX).

We have seen that an obstruction to $X_f(\mathbb{Z}) \neq \varnothing$ is that $X_f(\mathbb{Z}/m\mathbb{Z}) = \varnothing$ for some m. In other words, an obvious obstruction/impediment to the non-emptiness of $X_f(\mathbb{Z})$ is the emptiness of $X_f(\mathbb{Z}/m\mathbb{Z})$ for some m. If X_f satisfies the finite local-to-global principle then these are the only obstructions to the non-emptiness of $X_f(\mathbb{Z})$ (i.e. $X_f(\mathbb{Z})$ is non-empty if and only if for all m the obstruction $X_f(\mathbb{Z}/m\mathbb{Z}) = \varnothing$ doesn't hold or, equivalently, for all m $X_f(\mathbb{Z}/m\mathbb{Z})$ is non-empty).

One way, of course, to check that X_f does, or does not, satisfy the finite local-to-global principle is to compute whether or not $X_f(\mathbb{Z}) = \varnothing$ and to compute whether or not $X_f(\mathbb{Z}/m\mathbb{Z}) = \varnothing$ for all $m \in \mathbb{N}^*$ and then see, by definition, whether X_f satisfies the desired property. But, in practice, the reason that the finite local-to-global property, or any of the closely related properties, is useful is that one can prove for abstract reasons that X_f satisfies the finite local-to-global property without actually having to check whether or not $X_f(\mathbb{Z})$ or any of the $X_f(\mathbb{Z}/m\mathbb{Z})$ are empty or not. Once one does this, one can actually check whether $X_f(\mathbb{Z})$ is empty or not by checking whether or the $X_f(\mathbb{Z}/m\mathbb{Z})$ are empty or not for all $m \in \mathbb{N}^*$.

As of now this seems crazy: how can one show that X_f satisfies the finite local-to-global principle without actually checking whether or not $X_f(\mathbb{Z})$ or any of the $X_f(\mathbb{Z}/m\mathbb{Z})$ are empty? That said, we will, in fact, be able to show such a thing for a large class of polynomials f later on. So, while it is somewhat crazy that such a thing can be done, we will do it.

Let us now note that the Chinese Remainder Theorem gives us another, slightly simpler, version of the finite local-to-global principle:

Lemma 20.1

Let $v \in \mathbb{N}^*$ and let $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. Then, X_f satisfies the finite local-to-global principle if and only if the following two statements are equivalent:

1. $X_f(\mathbb{Z}) \neq \varnothing$.
2. For all primes p and all $k \in \mathbb{N}^*$ one has that $X_f(\mathbb{Z}/p^k\mathbb{Z}) \neq \varnothing$).

Proof 20.1

Hey

Now, naively one would hope that essentially 'all reasonable polynomials f' have the property that X_f satisfies the finite local-to-global principle. Unfortunately, there are incredibly simple examples of polynomials f which don't satisfy the finite local-to-global principle.

We give the following poignant one, even if we are not able yet to justify it in full:

Example 20.1

Let $f(x, y, z, w) := x^2 + y^2 + z^2 + w^2 + 1$. We claim that $X_f(\mathbb{Z}) = \varnothing$ but that $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all $m \in \mathbb{N}^*$. The first claim is clear since for all $(x, y, z, w) \in \mathbb{Z}^4$ we have that $f(x, y, z, w) \geqslant 1$. The second claim actually follows from Theorem 1.8 that we will later justify. Indeed, we can write $x^2 + y^2 + z^2 + w^2 = -1 \mod n$ as $x^2 + y^2 + z^2 + w^2 = n - 1 \mod n$. The claim then immdiately follows from Theorem 1.8.

Now, while this is an example of a simple polynomial f which doesn't satisfy the finite local-to-global principle one can notice that the reason that $X_f(\mathbb{Z}) = \varnothing$ in Example 20.1 was essentially due to an observation about positivity which, really, is not so much a question involved in $\mathbb{Z}$, but in $\mathbb{R}$. Said differently, we didn't have to worry about anything so nuanced as solving equations in $\mathbb{Z}$ to show that $X_f(\mathbb{Z}) = \varnothing$ in Example **??**, since $X_f(\mathbb{R}) = \varnothing$ (so then evidently $X_f(\mathbb{Z}) = \varnothing$). This is nice because solving equations in $\mathbb{R}$ is much simpler. For example, we have the following famous result of Tarski:

Theorem 20.1: Tarski

Let $v \in \mathbb{N}^*$ and $f(x_1, \ldots, x_v) \in \mathbb{R}[x_1, \ldots, x_v]$. There is then an algorithm to decide whether or not $X_f(\mathbb{R})$ is empty.

Thus, if we are interested in algorithmic results, we see that the issue with the finite local-to-global principle in Example 20.1 can be fixed, without sacrificing algorithmic methods, by slightly strengthening the assumption in the finite local-to-global principle as follows:

Definition 20.2

Let $v \in \mathbb{N}^*$ and $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. We say that X_f *satisfies the local-to-global principle* if the following two things are equivalent:

1. $X_f(\mathbb{Z}) \neq \varnothing$

2. $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all $m \in \mathbb{N}^*$ and $X_f(\mathbb{R}) \neq \varnothing$.

In the opposite direction, throughout this course we have noticed that solving equations modulo p is, in general, much simpler than solving equations modulo p^n for $n > 1$. Thus, the finite local-to-global principle would be much more manageable if we only had to check the existence of solutions modulo primes.

To this end, we make the following definitions:

Definition 20.3

Let $v \in \mathbb{N}^*$ and $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. We say that X_f *satisfies the strong finite local-to-global principle* if the following are equivalent:

1. $X_f(\mathbb{Z}) \neq \varnothing$.
2. $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for all primes p.

Definition 20.4

Let $v \in \mathbb{N}^*$ and $f(x_1, \ldots, x_v) \in \mathbb{Z}[x_1, \ldots, x_v]$. We say that X_f *satisfies the strong local-to-global principle* if the following are equivalent:

1. $X_f(\mathbb{Z}) \neq \varnothing$.
2. $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for all primes p and $X_f(\mathbb{R}) \neq \varnothing$.

We also note that if $f(x_0, \ldots, x_v) \in \mathbb{Z}[x_0, \ldots, x_v]$ is homogenous and P is any of the local-to-global like properties we defined above, then we can define an analagous notion of P_f satisfying P by replacing every instance of X_f with P_f. We leave it to the reader to write down the exact statements for themselves.

It's clear that

$$\text{strong finite local-to-global} \implies \text{finite local-to-global} \implies \text{local-to-global} \tag{505}$$

and that

$$\text{strong local-to-global} \implies \text{local-to-global} \tag{506}$$

but it's not so clear that some of these arrows can't be replaced by $\iff$. Thus, it will be helpful to consider many examples. This is what we do in the next section.

20.3 Examples

In this section we will give many examples of polynomials f that either do, or do not, satisfy one version of the local-to-global property.

A particular family of examples

In this section we show that it's not even true that every f has the property that X_f satisfies the local-to-global property, the weakest condition we've listed on our X_f. This tells us that while the local-to-global properties are nice, they are not universally enjoyed by the sets X_f, and so to utilize them for some particular family of X_f's we will have to put in some (usually highly non-trivial) work to show that this family of X_f's does, in fact, satisfy one of our local-to-global properties.

The simple example is as follows:

Example 20.2

Let $f(x) := (x^2-2)(x^2-17)(x^2-34) \in \mathbb{Z}[x]$. We claim that X_f doesn't satisfy the local-to-global principle. Indeed, it's clear that $X_f(\mathbb{Z}) = \varnothing$ since none of 2, 17, or 34 have square roots in $\mathbb{Z}$. Thus, to show the claim it suffices to show that $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all $m \in \mathbb{N}^*$ and that $X_f(\mathbb{R}) \neq \varnothing$. The latter is clear since $X_f(\mathbb{R}) = \{\pm\sqrt{2}, \pm\sqrt{17}, \pm\sqrt{34}\}$. To see that $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all $m \in \mathbb{N}^*$ it suffices, by Lemma 20.1, to show that $X_f(\mathbb{Z}/p^k\mathbb{Z}) \neq \varnothing$ for all primes p and all $k \geqslant 1$.

Assume first that $p = 2$. Note that since $17 = 1 \mod 8$ we have that $x^2 = 17 \mod 2^k$ is solvable for all $k \geqslant 1$ by Algorithm **??**. Thus, it's easy to see that $X_f(\mathbb{Z}/2^k\mathbb{Z}) \neq \varnothing$ for all $k \geqslant 1$.

Next assume that $p = 17$. Note then that since $17 = 1 \mod 8$ we have that $\left(\frac{2}{p}\right) = 1$. Thus, 2 is a square modulo 17. By Hensel's lemma we then know that 2 is also a square modulo 17^k for all $k \geqslant 1$. Thus, we deduce that $X_f(\mathbb{Z}/17^k\mathbb{Z}) \neq \varnothing$ for all $k \geqslant 1$.

Assume now that $p \neq 2, 17$. Note first that $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$. Indeed, note that our assumptions on p imply that $2, 17$, and 34 are elements of $\Phi(p)$. Now if $\left(\frac{2}{p}\right) = 1$ or $\left(\frac{17}{p}\right) = 1$ we're done. Else we see that $\left(\frac{2}{p}\right) = \left(\frac{17}{p}\right) = -1$ in which case

$$\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = -1 \cdot -1 = 1 \tag{507}$$

Thus, in any case, we see that $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$. Since $p > 2$ and any element of $X_f(\mathbb{Z}/p\mathbb{Z})$ is necessarily non-zero, it's not hard to see that Hensel's lemma applies and therefore $X_f(\mathbb{Z}/p^k\mathbb{Z}) \neq \varnothing$ for all $k \geqslant 1$.

The claim that $X_f(\mathbb{Z}/p^k\mathbb{Z}) \neq \varnothing$ for all primes p and all $k \geqslant 1$ now follows from these cases.

Of course, the above had nothing to do really with 17, but really all that was needed was that $17 = 1 \mod 8$. Thus, it's trivial to see that we can extend the above example to the following family of examples:

Example 20.3

Let p_0 be a prime such that $p_0 = 1 \mod 8$. Set $f(x) = (x^2-2)(x^2-p_0)(x^2-2p_0)$. Then, X_f does not satisfy the local-to-global principle.

Since Theorem 5.1 implies that there exists infinitely many primes p_0 such that $p_0 = 1 \mod 8$, we see that this produces an infinite family of examples of f such that X_f doesn't satisfy the local-to-global principle.

The case of power equations

Now that we have a somewhat simple, but contrived, family of examples which violate the local-to-global principle we move on to evaluating the situation in, perhaps, the simplest non-contrived case possible. Namely, we want to study the various versions of the local-to-global property for X_f where f is of the form $f(x) = x^n - a$ for some $a \in \mathbb{Z}$.

Namely, we begin by observing the following:

Lemma 20.2

Let $n \in \mathbb{N}^*$ and $a \in \mathbb{Z}$. Set $f(x) := x^n - a$. Then,

1. If n is odd then X_f satisfies the finite local-to-global principle.

2. If n is even then X_f satisfies the local-to-global principle.

Proof 20.2

If $a = 0$ we're done, so assume that $a \neq 0$. Let us write $a = (\pm)^s p_1^{e_1} \cdots p_r^{e_r}$. Then, we know that $X_f(\mathbb{Z}) \neq \varnothing$ if and only if $n \mid e_i$ for $i = 1, \ldots, r$ and $s = 0$ assuming that n is even. Let us note that if n is odd then we may as well absorb the -1 into x^n and we may assume that a is positive. If n is even then the assumption that $X_f(\mathbb{R}) \neq \varnothing$ implies that a is positive. Thus, in all cases we may assume that a is positive.

Thus, we need to show that $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all m implies that $n \mid e_i$ for all i. Note though that by taking $m = p_i^{e_i+1}$ that Theorem 11.1 we have that $X_f(\mathbb{Z}/p_i^{e_i+1}\mathbb{Z}) \neq \varnothing$ implies precisely that $n \mid e_i$. The conclusion follows.

Now, somewhat surprisingly, even though the above proof technique cannot show it, one can actually strengthen the above result to say that X_f satisfies the finite local-to-global principle for any n, independent of the parity.

To see this, it will be helpful to prove the following non-trivial result which follows from Theorem 14.3 and Theorem 5.1:

Theorem 20.2

Let $a \in \mathbb{Z}$ and set $f(x) := x^2 - a$. Then, X_f satisfies the strong finite local-to-global principle. In fact, $X_f(\mathbb{Z}) \neq \varnothing$ if and only if $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for all but finitely many p (i.e. for all finite sets S of primes $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for all primes $p \notin S$).

Proof 20.3

Let us begin by noting that we can write a uniquely as $a = b^2 c$ where $v_p(c) \leqslant 1$ for all primes p. Indeed, if we factorize $a = (-1)^s p_1^{e_1} \cdots p_\ell^{e_\ell}$ we know by Theorem 2.2 that we can uniquely write $e_i = 2q_i + r_i$ with $r_i \in \{0, 1\}$. It's clear we can then take $b = p_1^{q_1} \cdots p_\ell^{q_\ell}$ and $c = (-1)^s p_1^{r_1} \cdots p_\ell^{r_\ell}$. Moreover, it's clear that $X_f(\mathbb{Z}) \neq \varnothing$ if and only if $X_g(\mathbb{Z}) \neq \varnothing$ where $g(x) := x^2 - c$. Indeed, a and c both have the same sign, and the exponents in their prime factorizations have the same parity. Similarly, we can see that $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ if and only if $X_g(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for any prime p. Thus, we may as well assume that $a = c$.

Now, since $a = c$ we see that $X_f(\mathbb{Z}) \neq \varnothing$ if and only if $a = 1$. Thus, it remains to show that if $a \neq 1$ then $X_f(\mathbb{Z}/p\mathbb{Z})$ for some prime p. Note that since $a = c$ and $a \neq 1$ we have either that $a = -1$ or $a = (-1)^s p_1 \cdots p_\ell$ for some primes $p_1, \ldots, p_\ell$ such that, without loss of generality, $p_1 < \cdots < p_\ell$ and $s \in \{0, 1\}$. Note that if $a = -1$ we see that we can take $p = 3$ since for $f(x) = x^2 + 1$ we have that $X_f(\mathbb{Z}/3\mathbb{Z}) = \varnothing$. Thus, we can assume that $a = (-1)^s p_1 \cdots p_\ell$. We find the p such that $X_f(\mathbb{Z}/p\mathbb{Z}) = \varnothing$ as follows.

Let us first assume that $a > 0$, so that $s = 0$. Note then that by Theorem 14.3 that p_i is a square modulo p if and only if $p = \pm t^2$ with $t \in \{0, \ldots, 4p_i - 1\}$ odd. Now, note that this set when $i = \ell$ $\{\pm t^2\}$ has size $2p_\ell$. In particular, there exists some $s \notin \{\pm t^2\}$ and, moreover, $s = 1 \mod 4$. Now, by

Theorem 7.2 since $s = 1 \mod 4$ there exists some $m_0 \in \mathbb{Z}/4a\mathbb{Z}$ such that for $x \in \mathbb{Z}$ we have that

$$x = m_0 \mod 4a \iff \begin{cases} x = 1 \mod 4p_1 \\ \vdots \\ x = 1 \mod 4p_{\ell-1} \\ x = s \mod 4p_\ell \end{cases} \tag{508}$$

Moreover, it's clear that $m_0 \in \Phi(4a)$. By Theorem 5.1 there then exists a prime p such that $p = m_0 \mod 4a$. Note then that for this p we have that

$$\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_{\ell-1}}{p}\right)\left(\frac{p_\ell}{p}\right) = 1 \cdots 1 \cdot -1 = -1 \tag{509}$$

and thus $X_f(\mathbb{Z}/p\mathbb{Z}) = \varnothing$.

Assume now that $a < 0$ so that $s = 1$. By the Chinese Remainder Theorem there exists some $m_0 \in \Phi(4|a|)$ such that

$$x = m_0 \mod 4|a| \iff \begin{cases} x = -1 \mod 4p_1 \\ \vdots \\ x = -1 \mod 4p_\ell \\ x = 3 \mod 4 \end{cases} \tag{510}$$

By Theorem 5.1 we have that there exists a prime p such that $p = m_0 \mod 4|a|$. Note then by construction we have tha t

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p_1}{p}\right) \cdots \left(\frac{p_\ell}{p}\right) = (-1) \cdot 1 \cdots 1 = -1 \tag{511}$$

and thus $X_f(\mathbb{Z}/p\mathbb{Z}) = \varnothing$.

The stronger conclusion follows from the above and Theorem 5.1 which says that theree are infinitely many primes satisfying any congruence conditions and, in particular, primes of arbitrarily large size satisfying any congruence condition. It's clear then that if $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for all but finitely many primes, then $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for all sufficiently large primes. But we showed the above shows that if a is not a square in $\mathbb{Z}$ then there are infinitely many primes p (those satisfying the congruence conditions constructed in the two cases $a < 0$ and $a > 0$) such that $X_f(\mathbb{Z}/p\mathbb{Z}) = \varnothing$. Thus, the second stronger claim also follows from the above argument.

Note that this theorem really uses the full force of Quadratic Reciprocity and thus is quite deep. Using it we can actually amend Lemma 20.2 to the much more pleasing result:

Theorem 20.3

Let $n \in \mathbb{N}^*$ and $a \in \mathbb{Z}$. Set $f(x) := x^n - a$. Then, X_f satisfies the finite local-to-global principle.

Proof 20.4

The only thing to check is that if n is even then $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all m implies that $X_f(\mathbb{R}) \neq \varnothing$. Note though that since n is even that $X_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all m implies, in particular, that a has a square root modulo p for all primes p. By Theorem 20.2 this implies that a has a square root in $\mathbb{Z}$ and thus, in particular, that a is positive. Thus, $X_f(\mathbb{R}) \neq \varnothing$ as desired.

A naive guess would be that, in alignment with Theorem 20.2, that for any $n \in \mathbb{N}^*$ and any $a \in \mathbb{Z}$ we have that X_f satisfies the strong finite local-to-global principle with $f(x) := x^n - a$. Somewhat surprisingly, this is not true:

Example 20.4

Set $f(x) := x^8 - 16$. Then, $X_f(\mathbb{Z}) = \varnothing$ clearly since $16 = 2^4$ and $8 \nmid 4$. That said, we claim that $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for all primes p. If $p = 2$ the claim is clear since $x = 0$ is a solution modulo 2. So, we may assume that p is odd. Note that by Theorem 6.3 we have that $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ if and only if $16^{\frac{p-1}{\gcd(8,p-1)}} = 1 \mod p$. Now, we can rewrite $16^{\frac{p-1}{\gcd(8,p-1)}} = 2^{\frac{4(p-1)}{\gcd(8,p-1)}}$. Note that unless $\gcd(8, p-1) = 8$ we have that $p-1$ divides $\dfrac{4(p-1)}{\gcd(8,p-1)}$ in which case $2^{\frac{4(p-1)}{\gcd(8,p-1)}} = 1$ by Theorem 5.3. So, assume that $\gcd(8, p-1) = 8$. Then $2^{\frac{4(p-1)}{\gcd(8,p-1)}} = 2^{\frac{p-1}{2}}$. But, note that since $\gcd(8, p-1) = 8$ we have that $p = 1 \mod 8$ and thus $2^{\frac{p-1}{2}} = \left(\dfrac{2}{p}\right) = 1 \mod p$ by Theorem 12.5. The claim then follows.

Even more surprisingly is that Example 20.4 is, in some sense, the only counterexample to the claim that $x^n - a$ doesn't satisfy the strong finite local-to-global principle. Namely, we have the following stupendous theorem:

Theorem 20.4: Rational Grunwald-Wang theorem

Let $n \in \mathbb{N}^*$ and $a \in \mathbb{Z}$. Set $f(x) := x^n - a$. Then, the following is true:

1. If $8 \nmid n$ then X_f satisfies the strong finite local-to-global principle and, in fact, satisfies the stronger claim that $X_f(\mathbb{Z}) \neq \varnothing$ if and only if $X_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ for all but finitely many primes p.
2. If $8 \mid n$ and X_f does not satisfy the strong finite local-to-global principle, then a can be written in the form $2^{\frac{n}{2}} b^n$ for some $b \in \mathbb{Z}$.

In other words, this theorem says that the only way X_f, with $f(x) = x^n - a$, can't satisfy the strong finite local-to-global principle is that $8 \mid n$ and $a = 2^{\frac{n}{2}} b^n$ for some $b \in \mathbb{Z}$. This essentially says that Example 20.4 is representative—all examples where X_f fail the strong local-to-global principle look essentially like that one. This theorem is incredibly difficult to prove, and is well beyond the ability of our course. Not shockingly, considering the proof of Theorem 20.2, the way that one usually proves Theorem 20.4 is by developing an analogue of quadratic reciprocity for n^{th}-powers, something that requires quite a bit more sophistication than we are currently equipped to deal with.

Further examples

In Example 20.3 we constructed an infinite family of polynomials f such that X_f doesn't satisfy the local-to-global principle. Of course, this family seems a bit contrived and one might imagine that its failure to satisfy the local-to-global principle is a function of this contrivedness. For example, maybe the fact that these f factor plays a pivotal role—it certainly does in the proof, since the factorization is what allowed us to break having a root modulo p into a question of when 3 separate numbers are squares—and so maybe if f doesn't factor then we have a chance.

This, as it turns out, is not the case. The failure of X_f or P_f to satisfy a local-to-global principle can happen for essentially almost any f. The only reason why we chose such a contrived example in Example 20.3 was to make it simple enough to show the essential properties. So, let us see some more intersting, less degenerate examples where the local-to-global principles can fail:

Example 20.5: Selmer's example

Probably the most famous example of a P_f failing the local-to-global principle is the following example due to Selmer. Set $f(x,y,z) := 3x^3+4y^3+5z^3$. Then, P_f fails the local-to-global principle—$P_f(\mathbb{Z}) = \varnothing$ but $P_f(\mathbb{R}) \neq \varnothing$ and $P_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all $m \in \mathbb{N}^*$. Showing that $P_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all m is well beyond the abilities of this course but is not so hard given a little bit of advanced machinery (the Weil conjectures for genus 1 curves—a theorem in algebraic geometry) and the fact that $P_f(\mathbb{R}) \neq \varnothing$ is obvious. That said, it is not very easy to show that $P_f(\mathbb{Z}) = P_f(\mathbb{Q}) = \varnothing$. In fact, a huge amount of was inspired by the original proof that $P_f(\mathbb{Q}) \neq \varnothing$. Thus, one should take the fact that P_f doesn't satisfy the local-to-global principle as a non-trivial black box.

Example 20.6

Another non-trivial example of a homogenous polynomial f such that P_f fails the local-to-global principle is the following example: $f(x,y,z) = 2y^2 - x^4 + 17z^4$. Showing that $P_f(\mathbb{R}) \neq \varnothing$ is trivial, and showing that $P_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ requires the same sort of advanced machinery mentioned in the last example. That said, showing htat $P_f(\mathbb{Z}) = P_f(\mathbb{Q})$ is empty requires much less machinery. I will later add a proof of this fact.

20.4 Local-to-global principles and quadratic forms

We would now like to discuss a triumphant class of examples of f for which P_f does satisfy the local-to-global principle that is much deeper, and more powerful than Theorem 20.3. Recall that an integral quadratic form is just a homogenous element $f(x_0,\dots,x_n) \in \mathbb{Z}[x_0,\dots,x_n]$ of degree 2.

We then have the following stupendous result:

Theorem 20.5: Hasse-Minkowski

Let $f(x_0,\dots,x_v) \in \mathbb{Z}[x_0,\dots,x_v]$ be an integral quadratic form. Then, P_f satisfies the local-to-global principle.

Now, proving this result as it stands is beyond the scope of this course. That said, we are able to prove it in the case of ternary quadratic forms (i.e. in the case when f is in 3 variables). In particular, we will be able to prove Theorem 20.5 when $f(x,y,z) = ax^2 + by^2 + cz^2$ for some $a,b,c \in \mathbb{Z}$.

To see this, it will first be helpful to reinterpret what the local-to-global principle means for P_f in this case, using our understanding of conics developed in Lectures 18 and 19. Namely, we have the following:

Lemma 20.3

Let $a,b,c \in \mathbb{Z}$ be pairwise coprime square-free integers. Set $f(x,y,z) := ax^2 + by^2 + cz^2$. Then, the following are equivalent:

1. P_f satisfies the local-to-global principle.
2. $P_f(\mathbb{Z}) \neq \varnothing$ if and only if the following conditions hold:
    (a) a,b, and c are not all the same sign.
    (b) $-ab$ is a square modulo $|c|$.

(c) $-ac$ is a square modulo $|b|$.

(d) $-cb$ is a square modulo $|a|$.

(e) $P_f(\mathbb{Z}/2^k\mathbb{Z}) \neq \varnothing$ for all $k \geqslant 1$.

Remark 20.2

It's not hard to show that one can replace pairwise coprime with $\gcd(a, b, c) = 1$. We leave this as an exercise to the reader.

Proof 20.5: Lemma 20.3, sketch

All that we need to check is that conditions (a), (b), (c), (d), and (e) are equivalent to the claim that $P_f(\mathbb{R}) \neq \varnothing$ and $P_f(\mathbb{Z}/m\mathbb{Z}) \neq \varnothing$ for all $m \in \mathbb{N}^*$. Now, it's clear that (a) is equivalent to $P_f(\mathbb{R}) \neq \varnothing$ and it's clear that (e) is equivalent to $P_f(\mathbb{Z}/2^k\mathbb{Z}) \neq \varnothing$ for all $k \geqslant 1$ (obviously). Thus, it remains to show that (b), (c), and (d) are equivalent to the claim that $P_f(\mathbb{Z}/p^k\mathbb{Z}) \neq \varnothing$ for all odd primes p and $k \geqslant 1$.

Now, let p be an odd prime such that $p \nmid abc$. Note then when we reduce $f(x, y, z)$ modulo p all the coefficients stay non-zero. Thus, we see that $P_f(\mathbb{Z}/p\mathbb{Z}) \neq \varnothing$ automatically by Theorem (ALEX). Moreover, we know that P_f is smooth, and thus we can apply Hensel's lemma to show that $P_f(\mathbb{Z}/p^k\mathbb{Z}) \neq \varnothing$ for all $k \geqslant 1$.

Suppose now that p is an odd prime such that $p \mid abc$. Let's assume that $p \mid a$. Note then when we reduce $f(x, y, z)$ modulo p we get $f(x, y, z) = by^2 + cz^2$ where, since a, b, c are pairwise coprime, we know that b and c are non-zero modulo p. Note then if $-bc$ is a square modulo $|a|$ then $-bc$ is also a square modulo p. Note then that $P_f(\mathbb{Z}/p\mathbb{Z})$ contains the point $[0 : t : 1]$ where t is such that $t^2 = -b^{-1}c$ (which exists since $\left(\frac{-b^{-1}c}{p}\right) = \left(\frac{-bc}{p}\right) = 1$). This point is clearly smooth, and thus lifts to a point modulo p^k for all k. Conversely, if $P_f(\mathbb{Z}/p^k\mathbb{Z}) \neq \varnothing$ for all $k \geqslant 1$ then we see, in particular, that $P_f(\mathbb{Z}/p^2\mathbb{Z}) \neq \varnothing$. Note that if $-bc$ is not a square modulo $|a|$ then it is not a square modulo one prime dividing $|a|$, say it's this p. Then, the point is that $P_f(\mathbb{Z}/p\mathbb{Z}) = \{[1 : 0 : 0]\}$ but this solution doesn't lift to a solution modulo p^2.

Repeating this process with $p \nmid a$ replaced by $p \nmid b$ and $p \nmid c$ proves the claim.

Thus, we see that to prove Theorem 20.5 for integral quadratic forms of the form $f(x, y, z) = ax^2+by^2+cz^2$ for pairwise coprime square-free integers a, b, c it suffices to prove condition 2. of Lemma 20.3. In fact, something even stronger is true:

Theorem 20.6: Legendre's theorem

Let a, b, and c be pairwise coprime square-free integers. Then, the following are equivalent:

1. $P_f(\mathbb{Z}) \neq \varnothing$.
2. The following three conditions hold:
   (a) a, b, and c have different signs.
   (b) $-ab$ is a square modulo $|c|$.
   (c) $-ac$ is a square modulo $|b|$.
   (d) $-cb$ is a square modulo $|a|$.

In other words, Legendre's theorem essentially says that to check whether or not $P_f(\mathbb{Z}) \neq \varnothing$, for $f(x,y,z)$ as in the statement, it suffices to check that $P_f(\mathbb{Z}/p^k\mathbb{Z}) \neq \varnothing$ for all odd primes p and $k \geqslant 1$. Namely, Legendre's theorem says that we don't even have to worry about what happens with $P_f(\mathbb{Z}/2^k\mathbb{Z})$. So, Legendre's theorem is like an even stronger version of local-to-global principle.

The immediate corollary we get from Legendre's theorem is the following:

Corollary 20.1

Let a, b, and c be pairwise coprime square-free integers. Set $f(x,y,z) := ax^2 + by^2 + cz^2$. There is an algorithm to determine whether or not $P_f(\mathbb{Z}) \neq \varnothing$.

Thus, there exists polynomials for which there is no algorithm to decide if they have Diophantine solutions, ternary quadratic forms are not such an example.

Proof 20.6: Theorem 20.6

To be added.

21 Lecture 21: Applications of local-to-global principles