1

Thm (Fundamental theorem of Arithmetic):

Every positive integer x admits a unique factorization into a product of primes.

Recall: $$x = \prod_{p \in \mathbb{P}} p^{e_p}$$

where $e_p \in \mathbb{N}$ and are 0 for almost all p.

Uniqueness: $$x = \prod_{p \in \mathbb{P}} p^{f_p}$$

then $e_p = f_p$ for all p.

2

Lemma (Euclidean algorithm): For any n pos. int and d pos. int, there exists $q, r \in \mathbb{N}$ s.t.

$n = qd + r$ w/ $0 \leq r < d$.

q = "quotient"

r = "remainder"

Pf: To show uniqueness w/ same conds. assume $n = q'd + r'$. Want to show $q = q'$ and $r = r'$. To see this note

$$0 = qd + r - (q'd + r') \iff d(q' - q) = r - r'.$$

But $r - r' \in (-d, d)$. So, as $d \mid r - r'$

3

We conclude $r - r' = 0$, or $r = r'$.

This implies $d(q' - q) = 0$. So, $q' - q = 0$.

So $q' = q$.

For existence, consider (fix d)

$$S = \{ n : \text{no } q \text{ and } r \text{ exist} \}$$

Assume, $S \neq \emptyset$. By LNP S has a minimal element n_0.

L1

<u>Case 1</u>; $n_0 < d$.

$$n_0 = \underset{q}{\underset{\shortparallel}{0}} \cdot d + \underset{r}{\underset{\shortparallel}{n_0}}.$$

Contradiction.

<u>Case 2</u>; $n_0 = d$

$$n_0 = \underset{q}{\underset{\shortparallel}{1}} \cdot d + \underset{r}{\underset{\shortparallel}{0}}$$

Contradiction.

<u>Case 3</u>; $n_0 > d$.

Then $0 < n_0 - d < n_0 \in \mathbb{Z}$

So, by minimality of n_0, $n_0 - d = qd + r$.

So, $n_0 = (q+1)d + r$.

But, this is a contradiction. ∎

5

Prop (Bezout's lemma): Let $a, b \in \mathbb{Z}$. Then, TFAE:

(1) a and b are coprime

(2) there exists $x, y \in \mathbb{Z}$ s.t.

$(-a)(-x)$ $\quad ax + by = 1.$ $\quad x \mapsto -x$

Pf: (1) $\Rightarrow$ (2) Let d_0 be a min. element of

$$S = \{d \text{ pos. int.} : d = ax + by\}.$$

TFAE = The following are equivalent

6

I Claim $d_0 | a$ and $d_0 | b$, which will imply as a and b are coprime that $d_0 = 1$. WLOG $a \geq 0$. Write $a = qd_0 + r$ w/ $0 \leq r < d_0$ by Euclidean Algorithm. Then

So $d_0 = ax + by = (qd_0 + r)x + by$.

$d_0 rx = x(qd_0 \ldots + by$. But, $d_0 r \in S$. So, as d_0 is minimal is $r = 0$. So, $d_0 | a$. By symmetry $d_0 | b$.

WLoG = without loss of generality

7

(2) $\Rightarrow$ (1): If $d \mid a$ and $d \mid b$. But this implies $d \mid ax$ and $d \mid by$, so $d \mid ax + by = 1$. So, if $d > 0$, then $d = 1$. ∎

<u>Prop</u> (Euclid's prop): If p is a prime, $p \mid ab$, then $p \mid a$ or $p \mid b$.

8

Corollary (to Euclid's prop):

If $p \mid x_1 \cdots x_n$, $x_1, \ldots, x_n \in \mathbb{Z}$

then $p \mid x_i$ for some i.

Pf: Iteratively apply Euclid's prop.

Pf (uniqueness of FTA): Assume $\prod_{p \in \mathbb{P}} p^{e_p} = x = \prod_{p \in \mathbb{P}} p^{f_p}$.

Assume $e_q > f_q$. Then, $q^{e_q - f_q} \prod_{q \neq p \in \mathbb{P}} p^{e_p} = \prod_{q \neq p \in \mathbb{P}} p^{f_p}$. But $q \mid$ LHS, so $q \mid$ RHS.

So, by Euclid's prop $q \mid p^{f_p}$ for $p \neq q$, So again by Euclid's prop., $q \mid p$ for $p \neq q$. Contradiction.