$\boxed{1}$

Thm: The set $\mathbb{P} = \{\text{primes}\}$ was infinite.

Idea: If $\mathbb{P} = \{p_1, \dots, p_m\}$, produce a $p \in \mathbb{P}$ not equal to any of the p_i's.

Look at $N = p_1 \cdots p_m + 1$ has the property that $p_i \nmid N$. (bc if it did

2

then $p_i \mid N - p_1 \cdots p_n = 1$)

$2 \cdot 3 + 1 = 7$, $2, 3 \nmid 7$.

Find <u>any</u> prime divisor $p \mid N$.

§1 Why are primes important

Thm (Fundamental theorem of arithmetic):
Every positive integer can be factored **uniquely** as a product of primes.

4

Definition: Prime factorization is unique if $X = p_1^{e_1} \cdots p_m^{e_m}$ and $X = q_1^{f_1} \cdots q_n^{f_n}$ w/ $p_1 < p_2 < \ldots < p_m$ and $q_1 < \cdots < q_n$ then $m = n$ and $p_1 = q_1, \ldots, p_m = q_n$ and $e_1 = f_1, \ldots, e_m = f_m$.

$$108 = 2 \cdot 54 = 2^2 \cdot 27$$
$$= 2^2 \cdot 3 \cdot 9$$
$$= 2^2 \cdot 3 \cdot 3 \cdot 3$$
$$= 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdots$$

$$108 \longleftrightarrow (2, 3, 0, 0, 0, \ldots)$$

Idea: Every $x = \prod_{p \in \mathbb{P}} p^{e_p}$ where only finitely many $e_p \neq 0$.

$$X = \prod_{p \in \mathbb{P}} p^{e_p}$$

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

$$e_p = f_p$$

Intuition: primes are building blocks of integers

Pf (existence portion): Let $S = \{x \in \mathbb{N} : x \text{ does not factor into primes}\}$.
Suppose S is non-empty. Then, by L.I.P., there is a minimal element x_0 of S.

Note, x_0 can't be a prime, or

$$x_0 = \prod_{p \in P} p^{e_p}, \text{ where } e_p = \begin{cases} 0 & \text{if } p \neq x_0 \\ 1 & \text{if } p = x_0 \end{cases}$$

is a prime factorization.

Since x_0 is not prime we can write $x_0 = y_0 z_0$ w/ $1 < y_0, z_0 < x_0$ integers. As $y_0, z_0 < x_0$ and x_0 is minimal element of S, $y_0, z_0 \notin S$. So,

$$y_0 = \prod_{p \in P} p^{e_p} \quad \text{and} \quad z_0 = \prod_{p \in P} p^{f_p}$$

Thus,

$$x_0 = y_0 z_0 = \prod_{p \in P} p^{e_p + f_p}.$$

So we have prime factorized x_0. Contradiction. $\blacksquare$

2 The p-adic valuation

NB: We are assuming Thm 1 in this Section!

$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \right\}$

= "rational numbers"

TIP

Proposition: Every $0 \neq x \in \mathbb{Q}$ admits a unique factorization $x = (-1)^s \prod_{p \in \mathbb{P}} p^{e_p}$ w/ $e_p \in \mathbb{Z}$ and $e_p = 0$ for almost all p, and $s \in \{0,1\}$.

Pf: Write $x = (-1)^s \frac{a}{b}$ w/ $a, b \in \mathbb{N}$. By Thm 1

$$a = \prod_{p \in \mathbb{P}} p^{f_p} \quad \text{and} \quad b = \prod_{p \in \mathbb{P}} p^{g_p}$$

where $f_p, g_p \in \mathbb{N}$ and are zero for almost all p. Then

$$x = (-1)^s \prod p^{f_p - g_p}.$$

and $f_p - g_p \in \mathbb{Z}$ and is 0 for almost p. So existence is established.

For uniqueness suppose

$$x = (-1)^s \prod_{p\in\mathbb{P}} p^{e_p} = (-1)^t \prod_{p\in\mathbb{P}} p^{f_p}$$

w/ $e_p, f_p \in \mathbb{Z}$ and 0 for almost p. Clearly s=t. Cross-multiplying:

$$\prod_{p\in\mathbb{P}} p^{g_p} = \prod_{p\in\mathbb{P}} p^{h_p}$$

where

$$(g_p, h_p) = \begin{cases} (e_p, f_p) & \text{if } e_p, f_p \geq 0 \\ (e_p - f_p, 0) & \text{if } e_p \geq 0,\ f_p < 0 \\ (0, f_p - e_p) & \text{if } e_p < 0,\ f_p \geq 0 \\ (f_p, e_p) & \text{if } e_p, f_p < 0 \end{cases} \quad (*)$$

Note in all cases $g_p, h_p \geq 0$ and 0 for almost p. By Thm 1 we deduce $g_p = f_p$. By inspection of the 4 cases in $(*)$ this implies $e_p = f_p$. So uniqueness is established. ▨

"By inspection" is more formal way of saying "just look at it..."

Definition: The <u>p-adic valuation</u> (for a prime p) is the function v_p on $\mathbb{Q}$ defined by

$$v_p(x) = \begin{cases} e_p & \text{if } 0 \neq x = \prod_{p \in \mathbb{P}} p^{e_p} \\ \infty & \text{if } x = 0 \end{cases}$$

Remark: This is only well-defined because of Prop 1.

e.g., $v_p(57) = \begin{cases} 1 & \text{if } p = 3, 19 \\ 0 & \text{otherwise.} \end{cases}$

A function is <u>well-defined</u> if the output depends unambiguously on the input

$\boxed{\text{TIP}}$ **Prop:** (1) $\mathbb{Z} = \{x \in \mathbb{Q} : v_p(x) \geq 0\}$

(2) $v_p(xy) = v_p(x) + v_p(y)$ for $x, y \in \mathbb{Q}$.

(3) $v_p(x^{-1}) = -v_p(x)$ for $0 \neq x \in \mathbb{Q}$.

(4) For $x, y \in \mathbb{Z}$, one has $x \mid y$ if and only if $v_p(y) \geq v_p(x)$ for all $p \in \mathbb{P}$.

For statements P and Q, the statement "P if and only if Q" (also written "P iff Q" or "$P \Longleftrightarrow Q$") means if P is true then Q is true (i.e., $P \Rightarrow Q$) AND if Q is true then P is true (i.e., $Q \Rightarrow P$).

Pf:

(1) If $y \in \mathbb{Z}$, then by Thm 1 $y = \pm \prod_{p \in \mathbb{P}} p^{e_p}$ w/ $e_p \geq 0$ and $e_p = 0$ for almost p. So $v_p(y) = e_p \geq 0$

So $y \in \{x \in \mathbb{Q} : v_p(x) \geq 0 \text{ for all } p\}$.

If $y \in \{x \in \mathbb{Q} : v_p(x) \geq 0\}$, then $y = \pm \prod_{p \in \mathbb{P}} p^{v_p(y)}$, which is clearly in $\mathbb{Z}$.

(2) $xy = \prod_{p \in \mathbb{P}} p^{v_p(x)} p^{v_p(y)} = \prod_{p \in \mathbb{P}} p^{v_p(x) + v_p(y)}$.

But, $xy = \prod_{p \in \mathbb{P}} p^{v_p(xy)}$, So, by Prop 1, $v_p(xy) = v_p(x)\, v_p(y)$.

For sets S and T, to show $S = T$ we must show ($s \in S \Rightarrow s \in T$)

And

($t \in T \Rightarrow t \in S$).

i.e., $x \in S$ iff $x \in T$.

(3) $0 = v_p(1) = v_p(x \cdot x^{-1}) = v_p(x) + v_p(x^{-1})$

by (2). So, $v_p(x^{-1}) = -v_p(x)$.

(4) Note $x \mid y$ iff $\frac{y}{x} \in \mathbb{Q}$ which by (1)

happens iff $v_p\left(\frac{y}{x}\right) \geq 0$ for all p, but

by (1) + (2), $v_p\left(\frac{y}{x}\right) = v_p(y \cdot x^{-1}) = v_p(y) + v_p(x^{-1}) = v_p(y) - v_p(x)$

So, $v_p\left(\frac{y}{x}\right) \geq 0$ iff $v_p(y) \geq v_p(x)$, as desired. ☒

For statements like

prop

(1)

(2)

⋮

good to structure proof like

Pf:

(1)

(2)

⋮

Thm 2: For $0 \neq x \in \mathbb{Q}$ positive and n a positive integer, $\sqrt[n]{x} \in \mathbb{Q}$ iff $n \mid v_p(x)$ for all $p \in \mathbb{P}$.

Pf: Suppose $x = y^n$ for $y \in \mathbb{Q}$. Then, $v_p(x) = v_p(y^n) = n\, v_p(y)$ where the second equality follows from Prop 2.(2).
So, $n \mid v_p(x)$.

Suppose $n \mid v_p(x)$ for all p. Then we can write $v_p(x) = n a_n$ for some $a_n \in \mathbb{Z}$. Then

$$x = \prod_{p \in \mathbb{P}} p^{v_p(x)} = \prod_{p \in \mathbb{P}} p^{n a_n} = \left(\prod_{p \in \mathbb{P}} p^{a_n}\right)^n.$$

So $\sqrt[n]{x} = \prod_{p \in \mathbb{P}} p^{a_n} \in \mathbb{Q}$. $\blacksquare$

<u>Corollary:</u> $\sqrt{2}$ is irrational.

<u>Pf:</u> If $\sqrt{2} \in \mathbb{Q}$, then by Thm 2 $v_p(x)$ is even for all p. But $v_2(2) = 1$. $\blacksquare$