The Fundamental Theorem of Arithmetic

(TFTA) — integers have unique factorization into primes

(1) Why it's true
(2) Analogues

So far: Every $n \in \mathbb{Z}$ has a prime factor

Lemma: Suppose $a, b, c \in \mathbb{Z}$, $(a, b) = 1$, and $a \mid bc$. Then $a \mid c$.

Pf: Since $(a, b) = 1$, $\exists\, x, y \in \mathbb{Z}$ s.t. $ax + by = 1$

$$\Rightarrow \underbrace{acx}_{\text{div. by } a} + \underbrace{bcy}_{\text{div. by } a} = \underbrace{c}_{\text{conclude: div. by } a}$$

So $a \mid c$.

Lemma: Suppose p is prime and $p \mid a_1 a_2 \cdots a_n$ for $a_1, \ldots, a_n \in \mathbb{Z}$. Then there exists i with $1 \le i \le n$ $(\exists\, 1 \le i \le n)$ s.t. $p \mid a_i$.

Pf: By ind. on n.

$n=1$: WTS: if $p \mid a_1$, then $p \mid a_1$ ✓

Suppose: if $p \mid b_1 \cdots b_{n-1}$, then $p \mid b_i$ (for some i)

Assume $p \mid a_1 \cdots a_n$

product

Since p is prime, $(p, a_1 \cdots a_{n-1}) = 1$ or p.

If $(p, a_1 \cdots a_{n-1}) = 1$, then $p \mid a_n$

(by prev. lemma since $p \mid (a_1 \cdots a_{n-1})\, a_n$)

If $(p, a_1 \cdots a_{n-1}) = p$, then $p \mid a_1 \cdots a_{n-1}$

and by ind. hyp. $p \mid a_i$ for some $1 \le i \le n-1$

So $p \mid a_i$ for some $1 \le i \le n$ ✓

Thm (FTA): Let $n \in \mathbb{Z}$, $n \neq 0$. Then

$$n = (-1)^b \prod_{i=1}^{g} p_i^{v_i}$$ where each p_i is (and $b \in \{0,1\}$)

prime and each $v_i \in \mathbb{Z}_{>0}$. Moreover, this factorization is unique up to reordering the p_i

Pf: We will prove this for $n > 1$.

Two pieces: (1) n has a prime fact.
(2) that fact. is unique

For (1), by contradiction.

By W.O.P. there must be a least integer n w.th no prime fact.

We've shown: n has a prime factor, p

$\frac{n}{p} \in \mathbb{Z}_{>0}$

Case 1: $\frac{n}{p} = 1$

$\rightarrow n = p$ is a prime fact. $\lightning$

Case 2: $\frac{n}{p} > 1$ (smallest int. > 1 w/o prime fact.)

$\rightarrow 1 < \frac{n}{p} < n \rightarrow \frac{n}{p}$ has a prime fact.

$\Rightarrow n = p \left(\begin{matrix} \text{prime fact.} \\ \text{of } \frac{n}{p} \end{matrix} \right)$ is a prime fact. $\lightning$

So no integer > 1 has no prime fact.

Now, to show (2)

Suppose $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$

where $p_1, \ldots, p_k, q_1, \ldots, q_\ell$ are all prime. (may be the same)

Note $p_1 \mid q_1 q_2 \cdots q_\ell$ and by lemma, $p_1 \mid q_i$ for some $1 \le i \le \ell$

Without loss of generality ($i = 1$)

WLOG

$\rightarrow p_1 = q_1 \rightarrow p_2 \cdots p_k = q_2 \cdots q_\ell$

Repeat $p_2 = q_2, p_3 = q_3, \dots, p_k = q_k$

So $\ell \geq k$

By symmetry, $\ell \leq k$, so $\ell = k$.

$1 = q_{k+1} \cdots q_\ell$ is a problem

In other contexts

Q1: when can you factor things?

Q2: If you can factor, is it unique?

A1: polynomials

$\mathbb{Q}[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_0, \dots, a_n \in \mathbb{Q}\}$

↳ all polys. factor

↳ lose some uniqueness: $x = 2 \cdot \frac{x}{2} = 3 \cdot \frac{x}{3} = \cdots$

↳ only nonuniqueness comes from factoring out constants.

A1: $\mathbb{Q}$

Every $x \in \mathbb{Q}$ can be written $x = \frac{r}{s}$,

$r \in \mathbb{Z}$, $s \in \mathbb{Z}_{>0}$, and $(r, s) = 1$

Factor r, s into primes

$$x = \prod_{i=1}^{g} p_i^{v_i} \quad \text{where } v_i \in \mathbb{Z},\ v_i \neq 0$$

and p_i prime

A1: $\mathbb{R}$? $\mathbb{C}$?

No factorization here...

$$x = \frac{x}{\pi}\,\pi = \frac{x}{e}\,e = \cdots$$

When there is factorization, is it unique?

Ex: $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

↳ $2 = 2 + 0\sqrt{-5}$

$3 = 3 + 0\sqrt{-5}$

$1+\sqrt{-5}$, $1-\sqrt{-5}$

Just like in $\mathbb{Z}$, we can add and multiply elts. of $\mathbb{Z}[\sqrt{-5}]$ and stay in $\mathbb{Z}[\sqrt{-5}]$

$$(a + b\sqrt{-5}) + (x + y\sqrt{-5})$$

$$= (a+x) + (b+y)\sqrt{-5}$$

$$(a + b\sqrt{-5})(x + y\sqrt{-5})$$

$$ax - 5by + (xb + ay)\sqrt{-5}$$

Feature of $\mathbb{Z}[\sqrt{-5}]$:

if $x, y \in \mathbb{Z}[\sqrt{-5}]$ and

$xy = 0$, then $x = 0$ or $y = 0$.

Q: what are the "primes" of $\mathbb{Z}[\sqrt{-5}]$

Def: An elt. $x \in \mathbb{Z}[\sqrt{-5}]$ is <u>irreducible</u> if

$x = yz$, then $y = \pm 1$ or $z = \pm 1$

i.e. the only way to factor x is "trivially"

You can check: $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are all irreducible

Consequence: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

↳ non-unique factorization into irreducibles!

Q: What about other $\mathbb{Z}[\sqrt{d}]$?

- some questions are answered
- some questions are open.

$\mathbb{Z}[i]$ has unique factorization and Euclidean division

$\{a+bi : a, b \in \mathbb{Z}\}$

any $a, b \in \mathbb{Z}[i]$, you can write

$a = bq + r$ where r is "smaller than" b

In $\mathbb{Z}[i]$, integer primes may not be prime any more:

$5 = (1+2i)(1-2i) = 1^2 + 2^2$

↳ 5 = sum of two squares

$7 = a^2 + b^2$ for $a, b \in \mathbb{Z}$ has no solns.

Q: Which $n \in \mathbb{Z}$ can be written $n = a^2 + b^2$?