Theorem (Fundamental Theorem of Arithmetic)

Let $n > 0$ pe an integer.

(Existence of prime factorization)

There exist integers $e_p \geq 0$ for each prime p such that

- $e_p = 0$, for all $p > n$
- $n = 2^{e_2} \cdot 3^{e_3} \cdot \ldots \cdot p^{e_p} \cdot \ldots$

there is a FINITE product

(Uniqueness of prime factorization)

Suppose n has another prime factorization $n = 2^{f_2} \cdot 3^{f_3} \cdot \ldots \cdot p^{f_p} \cdot \ldots$

Then for every prime p, we have $e_p = f_p$.

Notation(s): $e_p(n)$, $\mathrm{ord}_p(n)$, $\nu_p(n)$

exponent order valuation

Proof of Existence :

Need to do two things

1) For each prime p, find the integer e_p

2) Show that $n = 2^{e_2} \cdot 3^{e_3} \cdot \ldots \cdot p^{e_p} \cdot \ldots$

For 1) : Consider the sequence:

$1, p, p^2, p^3, \ldots \ldots$

There is a largest one dividing n, saying p^{e_p}

We thus find the integer e_p.

2). We need a lemma:

Lemma (Multicativity of divisors): Let a, b, and n be three integers. If $a \mid n$, $b \mid n$, and $GCD(a, b) = 1$, then

$$ab \mid n$$

proof: By Bézout Indentity and $GCD(a, b) = 1$, there are two integers x_0, y_0 such that

$$a x_0 + b y_0 = 1.$$

$$a n x_0 + b n y_0 = n.$$

$a \mid n \Rightarrow ab \mid b n y_0$

$b \mid n \Rightarrow ab \mid a n x_0$

By 2-out-of-3, $ab \mid n$. ∎

Def. Two integers a and b are coprime if

$$GCD(a, b) = 1.$$

Example: If p and q are distinct prime numbers, then they are coprime.

proof: $GCD(p, q) =: g$

But the only divisors of p are 1 and p.

the only divisors of q are 1 and q.

Note that $p \neq q \neq 1$, thus g has to be 1.

$\square$

Prop: If $GCD(a, b) = 1$ and $GCD(a, c) = 1$, then $GCD(a, bc) = 1$.

Proof: By Bézout Identity, $\exists\, x_1, y_1, x_2, y_2 \in \mathbb{Z}$ s.t.

$$a x_1 + b y_1 = 1 \qquad ac x_1 + bc y_1 = c$$

$$a x_2 + c y_2 = 1 \qquad a(x_2 + c x_1 y_2) + bc y_1 y_2 = 1.$$

Namely $ax + bcy = 1$ has integer solutions!

Hence, $GCD(a, bc) \mid 1 \Rightarrow GCD(a, bc) = 1$. ∎

Coro: $p_1, \cdots, p_s$ are distinct prime numbers, then $p_1^{v_1} \cdots p_{s-1}^{v_{s-1}}$ and $p_s^{v_s}$ are coprime.

Back to the proof.

For 2): By the lemma (multiplicativity of divisors) and the coro,

$$2^{e_2}\cdot 3^{e_3}\cdots p^{e_p}\cdots \mid n.$$

If they are not equal, saying $n = d\cdot 2^{e_2}\cdot 3^{e_3}\cdots p^{e_p}\cdots$

Then there is a prime $p_0 \leq d$ such that $p_0 \mid d$

Why? Take p_0 to be the smallest divisor of d which not 1.

$$n = d\cdot 2^{e_2}\cdot 3^{e_3}\cdots p^{e_p}\cdots$$

we have a $p_0^{e_p}$

So $p_0\cdot 2^{e_2}\cdot 3^{e_3}\cdots p^{e_p}\cdots \mid d\cdot 2^{e_2}\cdot 3^{e_3}\cdots p^{e_p}\cdots = n.$

$\Rightarrow p_0^{e_{p_0}+1} \mid n$ But $p_0^{e_{p_0}}$ is the largest one among powers of p_0 which divides n! $\Rightarrow\!\Leftarrow$

$\square$

Proof of Uniqueness

Suppose we have two prime factorizations

$$n = 2^{e_2} \cdot 3^{e_3} \cdot \dots \cdot p^{e_p} \cdot \dots$$

$$n = 2^{f_2} \cdot 3^{f_3} \cdot \dots \cdot p^{f_p} \cdot \dots$$

If they are different, there is $p \leq n$ such that $e_p \neq f_p$.

We may assume $e_p > f_p$. Then consider $\frac{n}{p^{f_p}}$

$$\frac{n}{p^{f_p}} = 2^{e_2} \cdot 3^{e_3} \cdot \dots \cdot \boxed{p^{e_p - f_p} \cdot \dots}$$

p divides it

So $p \mid \frac{n}{p^{f_p}}$.

$$GCD\left(p, \frac{n}{p^{f_p}}\right) = p$$

$$\frac{n}{p^{f_p}} = 2^{f_2} \cdot 3^{f_3} \cdot \dots \cdot \cancel{p^{f_p}} \cdot \dots$$

is coprime to p.

$\#$

$$GCD\left(p, \frac{n}{p^{f_p}}\right) = 1$$

Proposition (Translation between division world & order world)

Structure 1: positive integers, equipped with multiplication, and ordered by the relation "$\mid$".

Structure 2: natural numbers, equipped with addition, and ordered by the relation "$\leq$".

(i) $v_p(a\cdot b) = v_p(a) + v_p(b)$

In other words, $a\cdot b = 2^{v_2(a)+v_2(b)} \cdot 3^{v_3(a)+v_3(b)} \cdots\cdots$

$a = 2^{v_2(a)} \cdots p^{v_p(a)} \cdots$, $b = 2^{v_2(b)} \cdots p^{v_p(b)} \cdots \Rightarrow ab = 2^{\sim} \cdots p^{\sim}$

$p^{v_p(a)} \cdot p^{v_p(b)} = p^{v_p(a)+v_p(b)}$

(ii) $a \mid b \iff \forall p$ prime, $v_p(a) \leq v_p(b)$

a = prod of $p^{v_p(a)} \Rightarrow p^{v_p(a)} \mid b \Rightarrow p^{v_p(a)} \mid p^{v_p(b)}$ or $v_p(a) \leq v_p(b)$

Conversely, $p^{v_p(a)} \mid p^{v_p(b)} \Rightarrow$ prod of $p^{v_p(a)} \mid$ prod of $p^{v_p(b)}$.

(iii) $\nu_p(GCD(a,b)) = \min\{\nu_p(a), \nu_p(b)\}$

$\nu_p(g) = \min\{\nu_p(a), \nu_p(b)\}$

WTS: $GCD(a,b) = \underbrace{\boxed{\text{prod of } p^{\min\{\nu_p(a), \nu_p(b)\}}}} = g$

(i) First, g is a common divisor of a & b

(ii) Suppose d is a common divisor of a & b, then

$$\nu_p(d) \leq \nu_p(a), \quad \nu_p(d) \leq \nu_p(b) \quad \text{for all } p$$

$$\Rightarrow \nu_p(d) \leq \min\{\nu_p(a), \nu_p(b)\} = \nu_p(g) \quad \text{for all } p$$

$$\Rightarrow d \mid g$$

Therefore $g = GCD(a,b)$. ∎

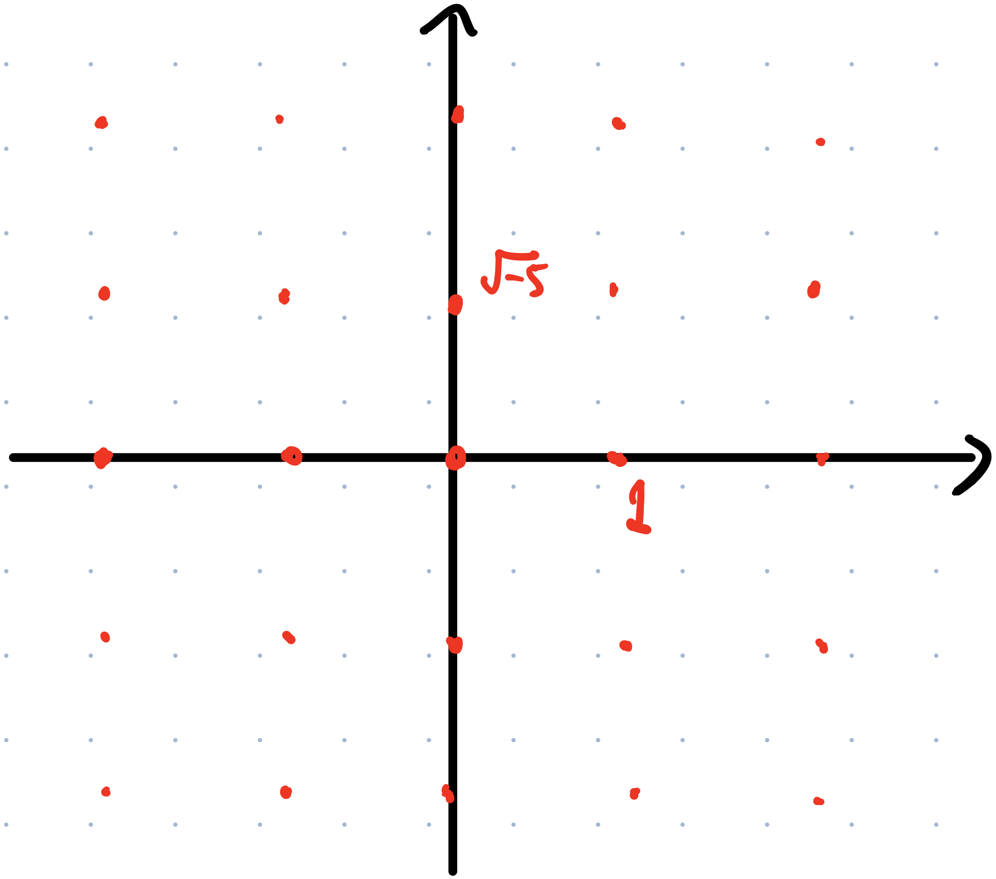
(iv) $\nu_p(LCM(a,b)) = \max\{\nu_p(a), \nu_p(b)\}$

proof is similar.

Appreciating unique prime factorization.

A counterexample:

$$\mathcal{O} = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$



$$6 = 2 \cdot 3 = (-2)(-3)$$

$$= (1+\sqrt{-5})(1-\sqrt{-5})$$

- What does "unique prime factorization" (UPF) mean?

<u>Defn</u>. A **monoid** is a triple $(M, \cdot, 1)$, where M is a set, $\cdot$ is a binary operation: $M \times M \to M$ and 1 is a specified element in M, satisfying.

<u>Axioms</u> i) $\forall x \in M$, $x \cdot 1 = 1 \cdot x = x$

ii) $\forall x, y, z \in M$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

A monoid M is "**commutative**" if

$$\forall x, y \in M. \quad x \cdot y = y \cdot x.$$

E.g. $(\mathbb{Z}, \times)$, $(\mathbb{N}, \times)$, $(\mathbb{Z}_{>0}, \times)$, $(\mathbb{C}, \times)$, $(\mathbb{Z}[\sqrt{-5}], \times)$

Let M be a commutative monoid.

<u>Defn</u>. Let $\alpha, \beta \in M$.

Say $\alpha \mid \beta$ if $\beta = m \cdot \alpha$ for some $m \in M$.

Say $\underset{\text{associated}}{\alpha \sim \beta}$ if both $\alpha \mid \beta$ and $\beta \mid \alpha$.

<u>Defn</u>. Let $\alpha \in M$.

- If there is $\beta \in M$ such that $\alpha \cdot \beta = 1$. Then α is a unit.
- If α is not a <u>unit</u> and $\beta \mid \alpha \Rightarrow \beta \sim \alpha$ or $\beta \sim 1$. Then α is a prime element.

Defn. A prime factorization of $\alpha \in \mathcal{M}$ is a representation

$$\alpha = \varepsilon \cdot \beta_1 \cdots \beta_r$$

where ε is a unit and $\beta_1, \cdots, \beta_r$ are prime element

Say α has a unique prime factorization if it has one and whenever it has another

$$\alpha = \varepsilon' \cdot \beta_1' \cdots \beta_s'$$

we necessarily have $r=s$ and a bijection $\phi : \{1, \cdots, r\} \to \{1, \cdots, s\}$ s.t. β_i $(1 \leq i \leq r)$ is associated to $\beta'_{\phi(i)}$.

After-class reading.

- The **unique prime factorization** provide a powerful tool to study problems on integer division through inequalities of integers. Try to use it to solve the Homework 2 problems.
- I encourage you to work out detailed proofs of the propositions in today's lecture: e.g. the corollary on pp. 5, and propositions (i) – (iv) on pp.8–9.
- You already have the methods to solve HW 2. For the notation $\sigma_0(N)$ in Problem 2, it just means "the number of divisors of N". For Problem 4, read pp. 11 – 13 of today's lecture notes for the background of the questions. Be aware of the **due date** (Oct 10).
- The first **Glossary** submission is due **this Friday**, be aware of it.