Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

January 20, 2023

What we have seen last lecture

- Hasse diagram
- Division network of positive integers
- Prime numbers
- Prime factorization
  - uniqueness
  - existence

    need to show:

$$\forall \text{ prime number } p, p^{e_p} \mid n \implies \prod_{p \text{ is prime}} p^{e_p} \mid n.$$

Today's topics

- Prime factorization
- Translation between $(\mathbb{Z}_+, \cdot, 1, |)$ and $(\mathbb{N}, +, 0, \leqslant)$

Prime factorization

Prime factorization

Theorem 5.1 (Fundamental Theorem of Arithmetic)

Let n be any positive integer.

1. *(existence) n admits a prime factorization, i.e. there exist natural numbers e_p for each prime p such that*

$$n = \prod_{p \text{ is prime}} p^{e_p}$$

2. *(uniqueness) Suppose n admits another prime factorization, say*

$$n = \prod_{p \text{ is prime}} p^{f_p}.$$

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

Continue proof of existence

Last time, we have constructed e_p for each prime number p so that $p^{e_p} \mid n$ and have seen that what remains to show is

$$\prod_{p \text{ is prime}} p^{e_p} \mid n.$$

Continue proof of existence

Last time, we have constructed e_p for each prime number p so that $p^{e_p} \mid n$ and have seen that what remains to show is

$$\prod_{p \text{ is prime}} p^{e_p} \mid n.$$

For this, we need a lemma:

Lemma 5.2

Let a, b, n be integers. If $a \mid n$, $b \mid n$, and $\gcd(a, b) = 1$, then $ab \mid n$.

Proof. Since $a \mid n$, $b \mid n$, by the defining property of least common multiple, $\operatorname{lcm}(a, b) \mid n$. Since $\gcd(a, b) = 1$, we have $\operatorname{lcm}(a, b) = ab$. $\square$

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$$

Coprime

Definition 5.3

Two integers a, b are called ***coprime*** if $\gcd(a, b) = 1$.

Example 5.4

Two distinct primes p, q are coprime.

Proof. Indeed, since the divisors of p are $1, p$, while the divisors of q are $1, q$, the only common divisor of p, q is 1. $\square$

Coprime

Lemma 5.5

Let $a, b, \cancel{k}$ c be integers. If a, b are coprime and a, c are coprime, then a, bc are coprime.

Proof. Suppose $\gcd(a, bc) = g$ >1. Let p be the smallest divisor of g other than 1. Then p has to be a prime number, otherwise it will have another divisor $d > 1$, which is also a divisor of g by the transitivity, but this contradicts to the minimality of p. Now, since $p \mid bc$, by the fundamental property of prime, we have either $p \mid b$ or $p \mid c$. But we also have $p \mid a$. Hence, p is a common divisor of either a, b or a, c, which contradicts to $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. $\square$

Back to proof of existence

$p_1, \underbrace{p_2, \cdots, p_s}$

Apply 5.5 to $a = p_i$ $(i>1)$

$b = c = p_1$

p_1^2 coprime to p_i

We need to show

$$\prod_{p \text{ is prime}} p^{e_p} \mid n.$$

Let $p_1, \cdots, p_s$ be all the prime divisors of n. By example 5.4, any two of $p_1, \cdots, p_s$ are coprime to each other. Apply lemma 5.5 to them, we see that any two of $p_1^{e_{p_1}}, \cdots, p_s^{e_{p_s}}$ are coprime to each other.

By lemma 5.2, $p_1^{e_{p_1}} p_2^{e_{p_2}} \mid n$ and by lemma 5.5, $p_1^{e_{p_1}} p_2^{e_{p_2}}$ is coprime to $p_3^{e_{p_3}}$. Repeat this, we see that $p_1^{e_{p_1}} \cdots p_s^{e_{p_s}} \mid n$. $\square$

Translation between two worlds

Translation between two worlds

The unique prime factorization provides a family of functions

$$v_p : \mathbb{Z}_+ \longrightarrow \mathbb{N},$$

where p is a prime number, mapping each positive integer n to the exponent e_p of p in its prime factorization.

These functions provide a translator between the following two worlds:

1. positive integers, equipped with multiplication and ordered by the divisibility $|$,
2. natural numbers, equipped with additions and ordered by the natural order $\leqslant$.

Translation between two worlds

Theorem 5.6

Let a, b be two positive integers.

1. $a = 1$ *if and only if for all prime* p, $v_p(a) = 0$. neutral to neutral.
2. $a = b$ *if and only if for all prime* p, $v_p(a) = v_p(b)$. global bijectivity
3. *For all prime* p, $v_p(ab) = v_p(a) + v_p(b)$. mult. to addition
4. $a \mid b$ *if and only if for all prime* p, $v_p(a) \leqslant v_p(b)$. divisibility to nat.order
5. *For all prime* p, $v_p(\gcd(a, b)) = \min\{v_p(a), v_p(b)\}$. gcd to min
6. *For all prime* p, $v_p(\operatorname{lcm}(a, b)) = \max\{v_p(a), v_p(b)\}$. lcm to max

Proof.

1. Follows by the prime factorization of 1.
2. Follows by the uniqueness of prime factorization.
3. Follows by the prime factorization and the power rules.
4. ($\implies$) Suppose $a \mid b$, say $b = ac$. By 3, for all prime p,

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

$$v_p(b) = v_p(a) + v_p(c) \geqslant v_p(a).$$

($\impliedby$) Conversely, suppose for all prime p, $v_p(a) \leqslant v_p(b)$, say $v_p(b) = v_p(a) + e_p$. Note that there are only finitely many positive e_p, otherwise there will be infinitely many prime divisors of b, which is impossible. Let $c = \prod_p p^{e_p}$, then $v_p(c) = e_p$. By 3, for all prime p,

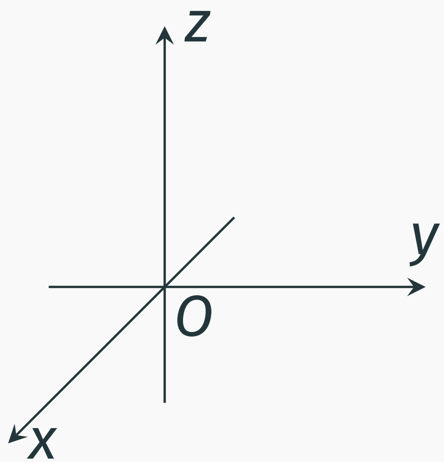
$$v_p(b) = v_p(a) + e_p = v_p(a) + v_p(c) = v_p(ac).$$

By 2, $b = ac$. Namely, $a \mid b$.

5. Let $g = \gcd(a, b)$. The first defining property says that $g \mid a$ and $g \mid b$. By 4, for all prime p, $v_p(g) \leqslant v_p(a)$ and $v_p(g) \leqslant v_p(b)$. Now, suppose e is any natural number smaller than both $v_p(a)$ and $v_p(b)$. By 4, $p^e \mid a$ and $p^e \mid b$. By the second defining property of gcd, $p^e \mid g$. By 4, $e \leqslant v_p(g)$. Now, $v_p(g) = \min\{v_p(a), v_p(b)\}$ follows from the defining property of min.
6. Similar to 5. □

Translation between two worlds

Moreover, the family of functions $v_p : \mathbb{Z}_+ \to \mathbb{N}$ $(p \in \mathbb{P})$ decomposes the Hasse diagram of divisibility of positive integers into individual dimensions: the value of $v_p(n)$ can be viewed as the coordinate of n on the p-axis.



This can be analogous to the decomposition of the usual Euclidean space into (three) individual dimensions via the x, y, z-axises.

After Class Work

The purpose of what follows is to explain the meaning of the last slide of the lecture.

Terminology

An ***ordered monoid*** is a monoid $(M, *, e)$ equipped with a partial order $\leqslant$ such that for all $a, b, c \in M$, we have

$$a \leqslant b \implies c * a \leqslant c * b \text{ and } a * c \leqslant b * c.$$

Example 5.7

We have seen two ordered monoid: $(\mathbb{Z}_+, \cdot, 1, |)$ and $(\mathbb{N}, +, 0, \leqslant)$. Besides them, $(\mathbb{Z}, +, 0, \leqslant)$ is also an ordered monoid.

Homomorphism of ordered monoids ii

Terminology

You may have heard the notion ***homomorphism***, that is a structure-preserving map between two algebraic structures of the same type (e.g. monoids, groups, $\mathbb{Z}$-modules, ordered sets, etc.). For example, a homomorphism between ordered monoids $f\colon (M, *, e, \preccurlyeq) \to (N, *, e, \preccurlyeq)$ is a map from M to N such that:

1. (preserving the operation) $\forall a, b \in M : f(a * b) = f(a) * f(b)$;
2. (preserving the neutral) $f(e) = e$;
3. (preserving the order) $\forall a, b \in M : a \preccurlyeq b \implies f(a) \preccurlyeq f(b)$.

If a homomorphism $f\colon M \to N$ has two-side inverses (i.e. there are homomorphisms $g, h\colon N \to M$ such that $g \circ f = \mathrm{id}_M$ and $g \circ h = \mathrm{id}_N$), then it is called an ***isomorphism***.

Exercise 5.1

Show that for each prime p, the function v_p gives a homomorphism between ordered monoids

$$v_p\colon (\mathbb{Z}_+, \cdot, 1, |) \longrightarrow (\mathbb{N}, +, 0, \leqslant)$$

Moreover, show that it is surjective but not injective. Hence, none of v_p is an isomorphism.

However, we can combine all the homomorphisms v_p. To do this, we need to first organize the (infinitely many) copies of $(\mathbb{N}, +, 0, \leqslant)$ into a single ordered monoid. The underlying set is

$$\mathbb{N}_{\mathbb{P}} := \left\{(e_p)_{p\in\mathbb{P}} \,\middle|\, e_p \in \mathbb{N} \text{ and only finitely many of } e_p \text{ are nonzero}\right\}.$$

The operation is the componentwise addition:

$$(e_p)_{p\in\mathbb{P}} + (f_p)_{p\in\mathbb{P}} := (e_p + f_p)_{p\in\mathbb{P}},$$

the neutral is the zero sequence $(0)_{p\in\mathbb{P}}$, and the order is the componentwise order

$$(e_p)_{p\in\mathbb{P}} \preccurlyeq (f_p)_{p\in\mathbb{P}} \qquad \text{defined as:} \qquad \forall p \in \mathbb{P}, e_p \leqslant f_p$$

Exercise 5.2 (†)

Show that the above is an ordered monoid and the map

$$\mathbf{v} \colon \mathbb{Z}_+ \longrightarrow \mathbb{N}_\mathbb{P} \colon n \mapsto (v_p(n))_{p\in\mathbb{P}}$$

is an isomorphism of ordered monoid. (Hint: use the unique prime factorization and 5.6.)

Prime factorization i

The followings are complements for Problem 4 of HW 2.

Terminology

A ***unit*** in an abelian monoid $(M, *, e)$ is an invertible element.

Example 5.8

- The only unit in $(\mathbb{Z}_+, \cdot, 1)$ is 1.
- The only unit in $(\mathbb{N}, +, 0)$ is 0.
- In $(\mathbb{Z}, \cdot, 1)$, there are two units: 1 and -1.
- In $(\mathbb{Z}, +, 0)$, every element is a unit.

Prime factorization ii

Terminology

Let a, b be two elements in an abelian monoid $(M, *, e)$. We say a ***divides*** b, a is a ***divisor*** of b, or b is ***divided by*** a, if there is an element $c \in M$ such that $b = a * c$. We will use $a \mid b$ to denote this. (***Warn***: distinguish this with the divisibility of integers, which is an example of the above notion.)

Exercise 5.3

Show that in $(\mathbb{N}, +, 0)$, we have $a \mid b$ if and only if $a \leqslant b$.

Exercise 5.4 (†)

Show that, if the monoid $(M, *, e)$ has only one unit, then $\cdot \mid \cdot$ is a partial order on it.

Terminology

An element p in an abelian monoid $(M, *, e)$ is a ***prime*** if

- p is not the neutral e,
- p is not a unit, and
- whenever $p = a * b$ with $a, b \in M$, we necessarily have one of a, b being a unit.

Example 5.9

- Prime elements in $(\mathbb{Z}_+, \cdot, 1)$ are prime numbers.
- Prime elements in $(\mathbb{Z}, \cdot, 1)$ are prime numbers and their negations.
- The only prime elements in $(\mathbb{N}, +, 0)$ is 1.

Terminology

Let a, b be two elements in an abelian monoid $(M, *, e)$. We say a, b are ***associated***, denoted by $a \sim b$, if both $a \mid b$ and $b \mid a$.

Exercise 5.5 (†)

Show that, "being associated" is an equivalent relation. Namely,

- (***reflexivity***) for all $a \in M$, $a \sim a$;
- (***symmetry***) for all $a, b \in M$, if $a \sim b$, then $b \sim a$;
- (***transitivity***) for all $a, b, c \in M$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

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