Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

January 18, 2023

What we have shown last week

- Binary linear Diophantine equation
- (Euclidean) Division Algorithm
- Bézout's identity
- Greatest common divisor
- Homogeneous linear equation
- Least common multiple
- Solution set of the linear Diophantine equation

Part II

Prime Numbers

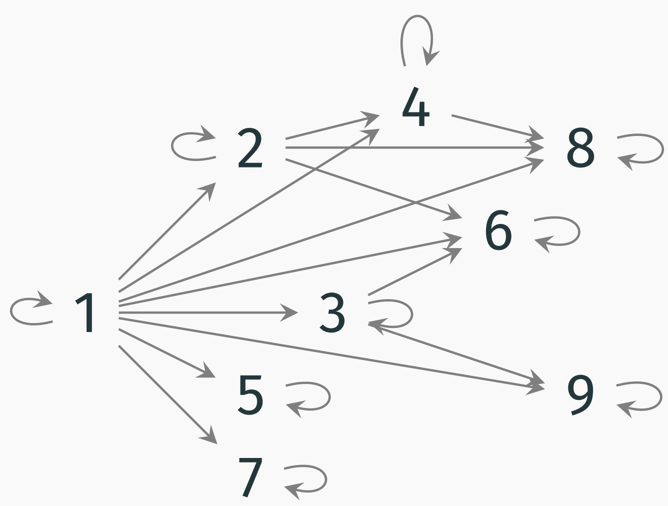
Today's topics

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

Hasse diagram

Hasse diagram

We want to illustrate the divisibility relation between positive integers. The first attempt is to list all the positive integers and whenever $a \mid b$ draw an arrow from a to b. But the result diagram is cluttered and confusing



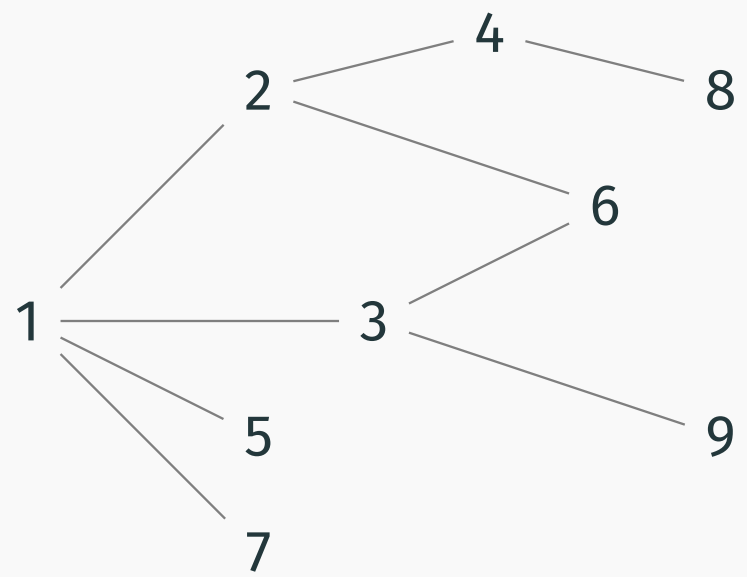
Divisibility of integers from 1 to 9

To simplify the diagram, we introduce the following omission:

- We may choose a global direction (for example, from left to right) to assemble the integers and omit the heads of arrows.
- We may omit the self-loops corresponding to the ***reflexivity***: $a \mid a$ ($a \in \mathbb{Z}_+$).
- By the ***transitivity***, we may only draw the arrows connecting ***adjacent*** nodes. Here, saying a and b are adjacent means $a \mid b$ and there is no other positive integer c between them in the sense $a \mid c$ and $c \mid b$.

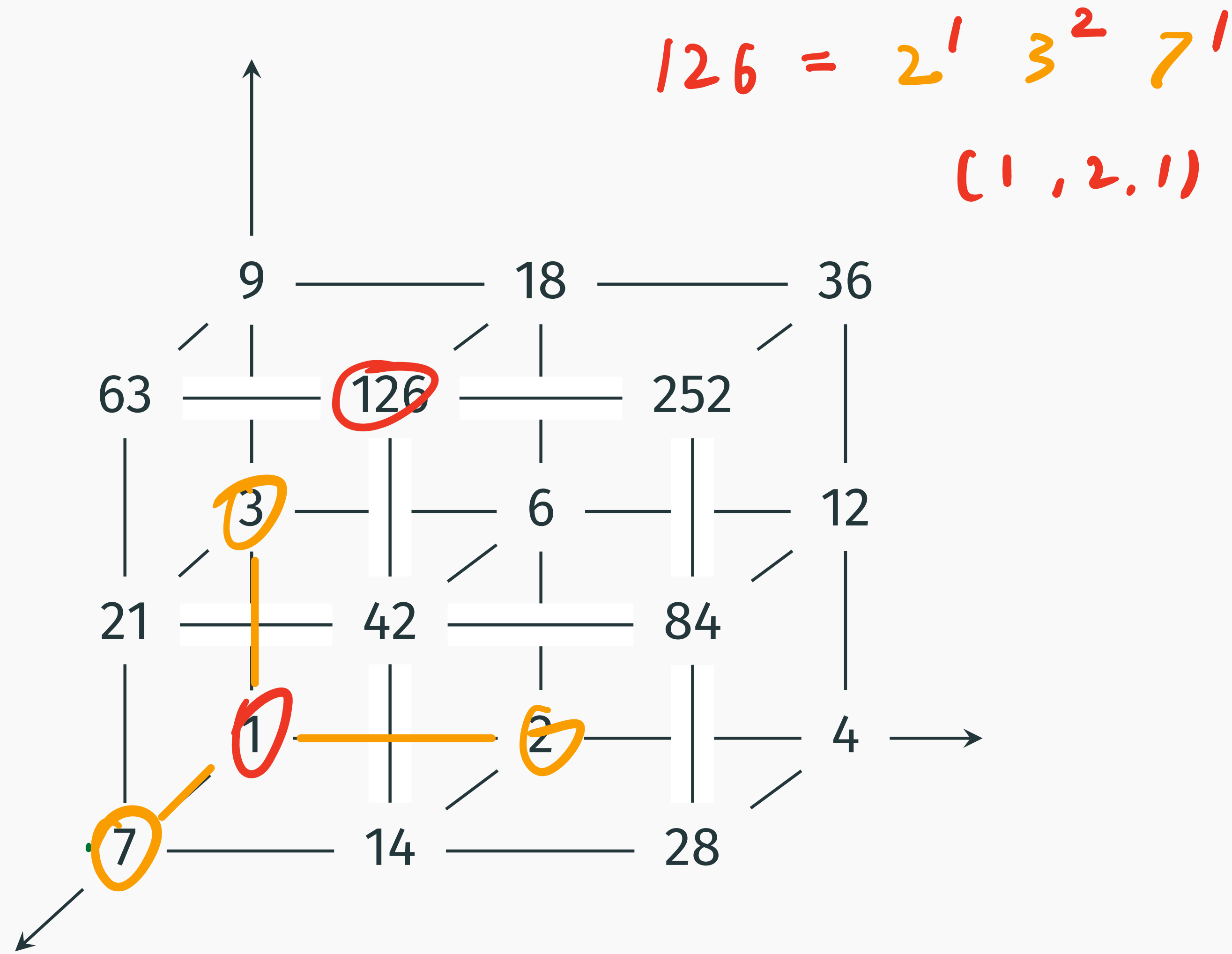
- By the ***antisymmetry***, after above simplifications, the diagram contains no loops and crossings.

The diagram obtained through previous simplification is called a ***Hasse diagram (of divisibility of positive integers)***.



Hasse diagram of integers from 1 to 9 (from left to right)

Hasse diagram



Hasse diagram of 1 and multiples of 2, 3, 7 (from inner to outer)

Prime factorization

Definition 4.1

A ***prime number***[3] is a positive integer having no divisors other than 1 and itself. If a positive integer is not 1 and is not a prime number, then it is called a ***composite number***.

In the Hasse diagram of divisibility of positive integers, the above notions can be interpreted as follows:

- 1 is the root/origin;
- prime numbers are nodes adjacent to 1;
- composite number are other nodes.

[3] There is no standard notation for the set of prime numbers. But many use $\mathbb{P}$.

$$p \nmid ab \Leftarrow p \nmid a \text{ and } p \nmid b$$

Theorem 4.2 (Primarity, fundamental property of primes)

Let p be a prime number. Then for any integers a, b, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b$$

$$p \mid ab \wedge p \nmid a \Rightarrow p \mid b$$

Theorem 4.2 (Primarity, fundamental property of primes)

Let p be a prime number. Then for any integers a, b, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof. We may assume $p \nmid a$. Then since there is no other divisor of p than 1 and p, we must have $\gcd(p, a) = 1$.

By ***Bézout's identity***, there are integers x_0, y_0 such that $px_0 + ay_0 = 1$. Lets multiple both sides by b, we get

$$pbx_0 + aby_0 = b.$$

Since $p \mid ab$, by ***2-out-of-3 principle***, we must have $p \mid b$. $\square$

$a^x b^y c^z = a^{x'} b^{y'} c^{z'}$

$\not\Rightarrow$ $x = x'$, $y = y'$, $z = z'$

$2^3 3^2 6^1 = 2^2 3^1 6^2$

Theorem 4.3 (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*[4]

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

has to be a finite product.

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

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

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

e.g. $42 = 2^1 \cdot 3^1 \cdot 7^1 = 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdots$

$\Rightarrow$ $e_2 = 1$ $e_5 = 0$ $e_p = 0$ $(p > 7)$
$e_3 = 1$ $e_7 = 1$

[4]Note that this is a finite product.

Proof of uniqueness

We first prove the uniqueness.

Suppose we have two distinct prime factorizations of n, say

$$n = 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots ,$$
$$n = 2^{f_2} \cdot 3^{f_3} \cdots p^{f_p} \cdots .$$

Then there is a prime p such that $e_p \neq f_p$, say $e_p > f_p$.

We first prove the uniqueness.

Suppose we have two distinct prime factorizations of n, say

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

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

$a = 2^{f_2} \cdot 3^{f_3} \cdots \cancel{p^{f_p}} \cdots$

$p^{e_p} \mid n$

$\Rightarrow p^{e_p - f_p} \mid \frac{n}{p^{f_p}} =: a$

$\Rightarrow p \mid a$

Then there is a prime p such that $e_p \neq f_p$, say $e_p > f_p$.

Consider $a = \frac{n}{p^{f_p}}$. By the first factorization, we have $p \mid a$. By the second factorization and theorem 4.2, $p \nmid a$ (indeed, 4.2 implies: if each factor of a product is not a multiple of p, then the product is not a multiple of p). This gives a contradiction. Therefore, we must have $e_p = f_p$ for all prime p.

$p \nmid ab \Leftarrow p \nmid a$ and $p \nmid b$

not divided by

Proof of existence

Now we prove the existence.

For each prime p. Consider the sequence

$$1 = p^0, p, p^2, \cdots$$

$1 \mid n$

Among them, there is a largest one, say p^{e_p}, such that $p^{e_p} \mid n$.

Proof of existence

Now we prove the existence.

For each prime p. Consider the sequence

$$1 = p^0, p, p^2, \cdots$$

Among them, there is a largest one, say p^{e_p}, such that $p^{e_p} \mid n$.

In next lecture, we will show that, from $p^{e_p} \mid n$ for all prime p, we can conclude that

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

Let's say $n = d \cdot 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots$. Then if $d \neq 1$, there must be a prime divisor p_0 of d (e.g. the smallest divisor of d other than 1). Then we have $p_0^{e_{p_0}+1} \mid n$, which contradicts with the maximality of e_{p_0}.

After Class Work

Terminology

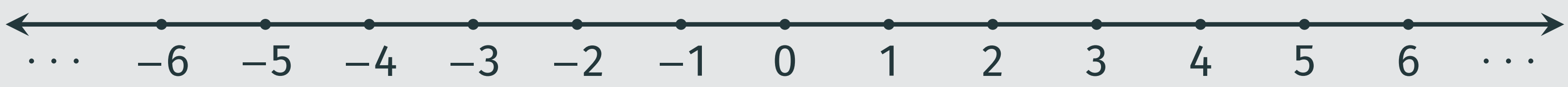
Given an ordered set $(S, \preccurlyeq)$, we can illustrate the partial order by a ***Hasse diagram***:

- the nodes are the elements of S, listed from smaller to larger;
- if two elements a, b are ***adjacent***, namely $a \preccurlyeq b$ and there is no other elements c between them ($a \preccurlyeq c$ and $c \preccurlyeq b$), we draw an arrow (omitting the head) from a to b.

We can read out the partial order from the Hasse diagram as follows: $a \preccurlyeq b$ if and only if there is a path from a to b.

Exercise 4.1

Consider the set of integers $\mathbb{Z}$ equipped with the usual order $\leqslant$, show that the Hasse diagram looks as follows:



Exercise 4.2

In the definition of Hasse diagram, we implied assumed that every pair (a, b) with the partial order relation $a \preccurlyeq b$ can be decomposed into a chain of adjacent ones: $a = x_0 \preccurlyeq x_1 \preccurlyeq \cdots \preccurlyeq x_n = b$. However, this is NOT true in general:
Show that in $(\mathbb{R}, \leqslant)$, every pair $a \leqslant b$ is NOT adjacent.

Terminology

A partial order $\preccurlyeq$ on a set S is called a ***linear order*** if every two elements of S is comparable: namely, either $a \preccurlyeq b$ or $b \preccurlyeq a$. If this is the case, we say $(S, \preccurlyeq)$ is a ***linear ordered set***.

Exercise 4.3 (†)

If an ordered set $(S, \preccurlyeq)$ is linear ordered set (and if it has a Hasse diagram), then we can assemble its Hasse diagram as a line (for example, exercise 4.1). To see this, show that there is no ***branch*** in the Hasse diagram, namely for every element $a \in S$, there can be at most one inward edge and one outward edge adjacent to a.

Notations

We will use the following notations for ***indexed sum*** and ***product***:

$$\begin{aligned}
\sum S &:= \text{the sum of elements of } S, \\
\sum_{a \in S} f(a) &:= \text{the sum of values of } f(a) \text{ when } a \text{ is taken over } S, \\
\prod S &:= \text{the product of elements of } S, \\
\prod_{a \in S} f(a) &:= \text{the product of values of } f(a) \text{ when } a \text{ is taken over } S.
\end{aligned}$$

Example 4.4

The prime factorization can be written as $n = \prod_{p \in \mathbb{P}} p^{e_p}$.

Notations

When a presentation of a set S is given:

$$S = \{\text{expression} \mid \text{rule}\},$$

we usually write indexed sum and product in a more compact way:

$\sum_{\text{rule}} f(\text{expression}) :=$ the sum of values of $f(\text{expression})$ when the value of expression is specified by rule,

$\prod_{\text{rule}} f(\text{expression}) :=$ the product of values of $f(\text{expression})$ when the value of expression is specified by rule.

Example 4.5

The prime factorization can be written as $n = \prod_{p \text{ is prime}} p^{e_p}$.

Notations

It is worth to point out that a ***sequence*** and a ***map*** are more or less the same thing.

- A sequence $(a_1, \cdots, a_n)$ is the same as a map from $\{1, \cdots, n\}$ mapping i to a_i.
- Similarly, a sequence $(a_1, \cdots)$ is the same as a map from $\mathbb{Z}_+$ mapping $i \in \mathbb{Z}_+$ to a_i.
- More generally, a sequence $(x_i)_{i \in I}$ is a map from I mapping $i \in I$ to x_i.
- Conversely, a map from a set I to some target set T is the same as a sequence $(x_i)_{i \in I}$ with each $x_i \in T$.