Hasse Diagram

Start with a set of positive integers

Basic Idea: If $m \mid n$, then draw an arrow from m to n.

We will just use a line segment

$(m \mid n \Rightarrow m \leq n)$

Some simplification

1. Reflexive $m \mid m$

$m \circlearrowleft$ will be omit

2. Antisymmetric $m \mid n,\ n \mid m \Rightarrow m = n$

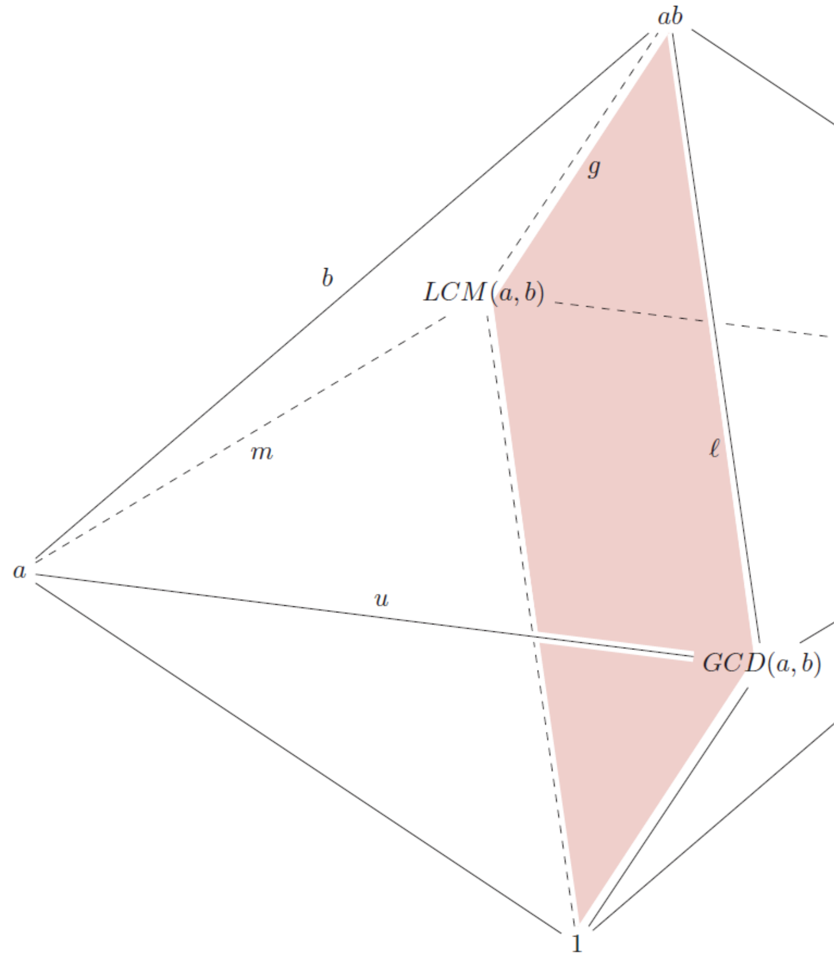
$m \rightleftarrows n \rightsquigarrow m = n \circlearrowleft$ omit.

3. transitive $a \mid b,\ b \mid c \Rightarrow a \mid c$

$a \longrightarrow b \longrightarrow c$ then also an arrow $a \longrightarrow c$.

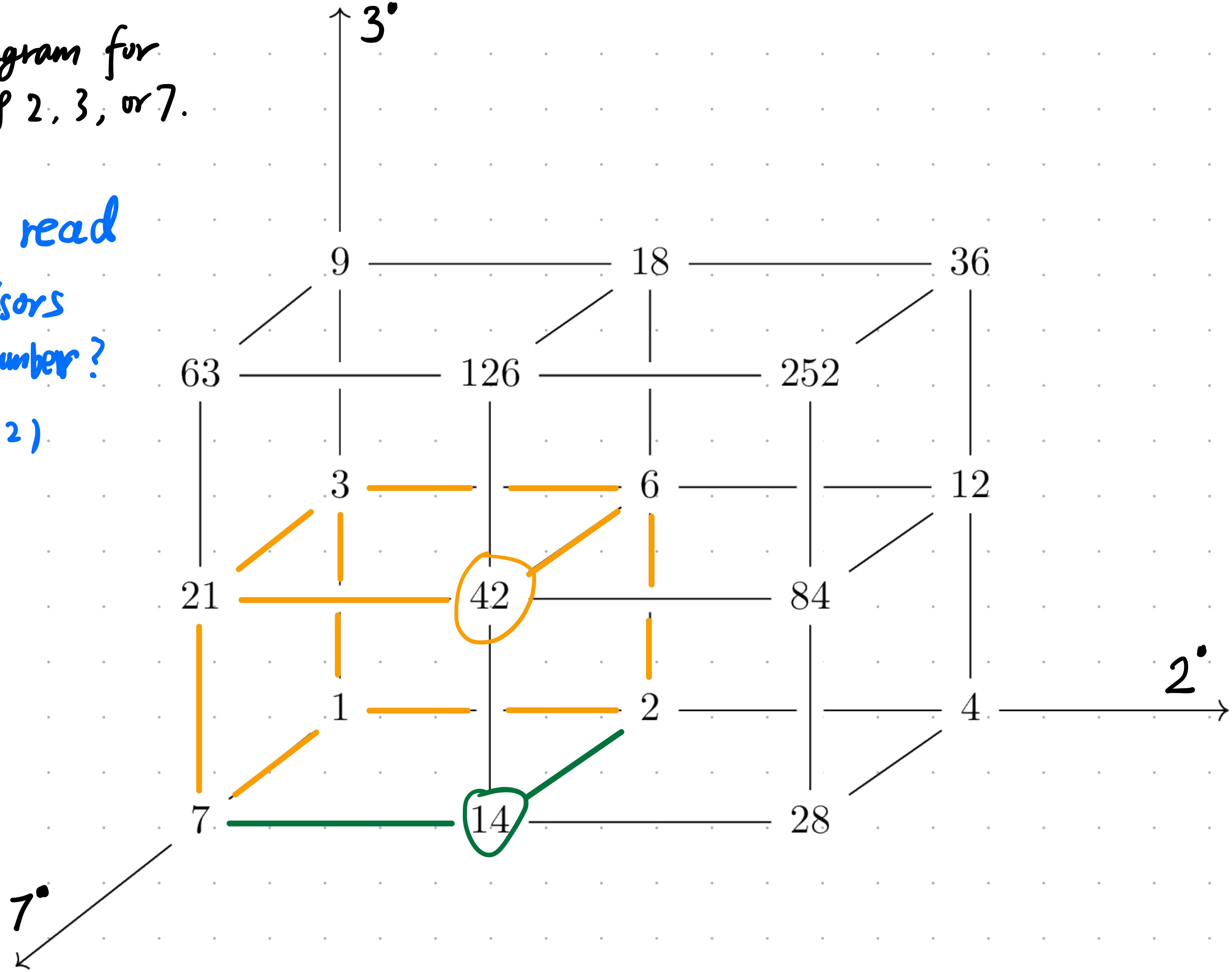
omit $a \to c$, viewing it as the path from a to c via b.

Example $\{1, a, b, GCD(a,b), LCM(a,b), ab\}$



Hasse Diagram for multiples of 2, 3, or 7.

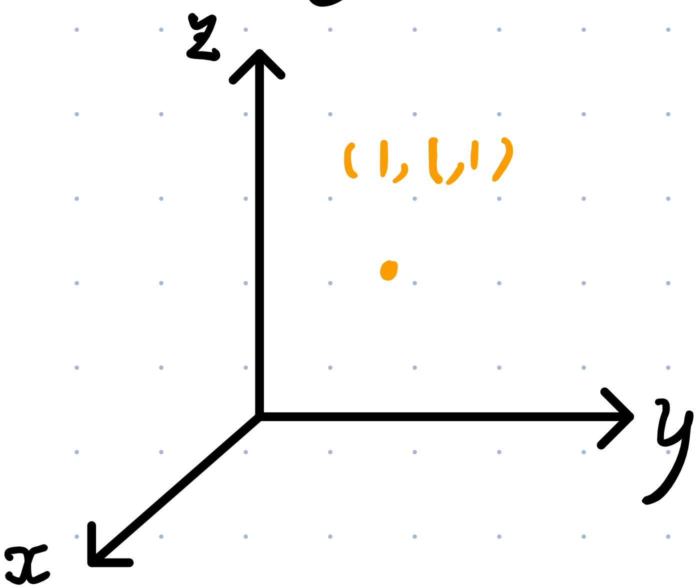
Can you read out divisors of a number? (e.g. 252)



division network
of
all positive integers

decompose $\longrightarrow$ Individual dimensions

Just as how the Euclidean space being decomposed into 3 dimensions!



Ex: How to compare two points in the Euclidean space? How does it related to each dimension?

Analogous of the networks.

Def. Let $n > 0$ be an iteger.

- If $n > 1$ and has no divisor other than 1 and n itself

  $\rightsquigarrow$ n is a prime number.

  $$1 \text{ --- } n$$

- If $n > 1$ and not a prime, namely $d \mid n$ for some $1 < d < n$

  $\rightsquigarrow$ n is a composite number

  $$1 \text{ --- } \cdots d \cdots \text{ --- } n$$

- $n = 1$ is called a unit.

Prop (primeness / Fundamental property of primes) (Euclidean's lemma)

Let p be a prime number and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

(by contradiction)

Proof: Suppose $p \nmid a$ and $p \nmid b$.

Then $GCD(p, b) = 1$ because the only divisors of p are 1 and p but $p \nmid b$ and $1 \mid b$.

By "Bézout Identity", there are integers x_0, y_0 such that

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

$$p a x_0 + ab y_0 = a.$$

But $p \mid ab$. Then 2-out-of-3 $\Rightarrow$ $p \mid a$. $\Rightarrow\Leftarrow$

$\blacksquare$

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

↖ there is a FINITE product

(Uniqueness of prime factorization)

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

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

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

exponent order valuation

Proof of Existence :

Need to do two things

1) For each prime p, find the integer e_p

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

For 1) : Consider the sequence:

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

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

We thus find the integer e_p.

2). We need a lemma:

<u>Lemma</u>: 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 Identity, there are integers x_0, y_0 such that

$$ax_0 + by_0 = 1$$

$$\Rightarrow \quad nax_0 + nby_0 = n$$

$b \mid n \Rightarrow ab \mid nax_0$, $a \mid n \Rightarrow ab \mid nby_0$.

By 2-out-of-3, we have

$$ab \mid n$$

Back to the proof.

For 2): By the lemma, and the fact that $GCD(p_1^x, p_2^y)=1$ if $p_1 \neq p_2$ are distinct primes, we have

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

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

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

Why?

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

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

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

$\boxed{\nearrow}$

Reading suggestions

- The **Hasse diagram** is a way to visualize order relation between a given ordered set. Note that how the three properties (reflexivity, anti-symmetry, and transitivity) allow us to draw a simplified, loop-free diagram.
- Two integers a and b are **coprime** if $\mathrm{GCD}(a, b) = 1$. This notion plays an important role. Try to prove all the involved coprime statement in today's lecture and find more results using the results on GCD in Chapter 1 of the textbook.
- We will continue on prime factorization in next class. Read pp. 56 – 63.