# Chapter 4.
# Number Theory

## Discussion on CMath: A Foundation for CS

Zhang GW

China Univ. of Geosciences

February 26, 2024

## The Divisible

### Definition (Divisibility)

$m \mid n \iff m > 0 \land n = mk$ for some int $k$.

- That is, $n$ is a multiple of $m$, and it is not possibly positive.

# Greatest Common Divisor

### Definition (GCD and LCM)

- Defn. $\gcd(m, n) = \max\{k : k \mid m \wedge k \mid n\}$,
- Defn. $\operatorname{lcm}(m, n) = \max\{k : m > 0 \wedge m \mid k \wedge n \mid k\}$,

# The Euclid Algorithm

We assert that $\gcd(m, n) = \gcd(n, m \bmod n)$ (proof later).
Extended: Compute integers $m'$ and $n'$ s.t.

$$m'm + n'n = \gcd(m, n).$$

- At the end of the formula, $m = 0, n = \gcd(m, n)$.
- take $m' = 0, n' = 1$.
- Otherwise, keep an eye on the derivation process:

# The Euclid Algorithm

We assert that $\gcd(m, n) = \gcd(n, m \bmod n)$ (proof later).

Extended: Compute integers $m'$ and $n'$ s.t.

$$m'm + n'n = \gcd(m, n).$$

the derivation process, (q=quotient, r=remainder)

$$
\begin{aligned}
b &= rq_1 + r_1 & 0 \leqslant r_1 < r \\
r &= r_1 q_2 + r_2 & 0 \leqslant r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 & 0 \leqslant r_3 < r_2 \\
&\cdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} & 0 \leqslant r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n + r_n & 0 \leqslant r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}
$$

# Euclid Algo: Substitution back

$$b = rq_1 + r_1 \qquad\qquad 0 \leqslant r_1 < r$$
$$r = r_1 q_2 + r_2 \qquad\qquad 0 \leqslant r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \qquad\qquad 0 \leqslant r_3 < r_2$$
$$\cdots$$
$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \quad 0 \leqslant r_{n-1} < r_{n-2}$$
$$r_{n-2} = r_{n-1} q_n + r_n \qquad 0 \leqslant r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1}$$

Hence,

$$
\begin{aligned}
d = 1 r_n + 0 \times 0 &= 1 r_{n-2} - q_n r_{n-1} \\
&= 1 r_{n-2} - (r_{n-3} - q_n r_{n-2} q_{n-1}) \\
&= -q_n r_{n-3} + (1 + q_{n-1} q_n) r_{n-2} \\
&= \cdots \\
&= xa + yb \quad (x, y \in \mathbb{Z}).
\end{aligned}
$$

# Euclid Algo: Code

- Use RECURSION to maintain the relation.
  EXTENDED-EUCLID $(a, b)$

  1   if $b == 0$
  2  return$(a, 1, 0)$
  3  else $(d', x', y') = \text{EXTENDED} - \text{EUCLID}(b, a \bmod b)$
  4  $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$
  5  return$(d, x, y)$

# Euclid Algo: Code

- Use RECURSION to maintain the relation.
  EXTENDED-EUCLID $(a, b)$

  1    if $b == 0$
  2    return$(a, 1, 0)$
  3    else $(d', x', y') = \text{EXTENDED} - \text{EUCLID}(b, a \bmod b)$
  4    $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$
  5    return$(d, x, y)$

Why $(d', y', x' - \lfloor a/b \rfloor y')$?

- Condition:
  - $ax_1 + by_1 = \gcd(a, b)$
  - $bx_2 + (a \bmod b)y_2 = \gcd(b, a \bmod b)$

- Derivation:
  - $ax_1 + by_1 = bx_2 + (a \bmod b)y_2$
  - and we have that $a \bmod b = a - \left( \left\lfloor \frac{a}{b} \right\rfloor \times b \right)$
  - So we get $ax_1 + by_1 = bx_2 + \left( a - \left( \left\lfloor \frac{a}{b} \right\rfloor \times b \right) \right) y_2$
  - $ax_1 + by_1 = ay_2 + bx_2 - \left\lfloor \frac{a}{b} \right\rfloor \times by_2 = ay_2 + b \left( x_2 - \left\lfloor \frac{a}{b} \right\rfloor y_2 \right)$
  - Compare the coeffs.

## Euclid Algo: Code

- Use RECURSION to maintain the relation.
  EXTENDED-EUCLID $(a, b)$

  1    if $b == 0$
  2    return$(a, 1, 0)$
  3    else $(d', x', y') = \text{EXTENDED} - \text{EUCLID}(b, a \bmod b)$
  4    $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$
  5    return$(d, x, y)$

An Example:

| $a$ | $b$ | $\lfloor a/b \rfloor$ | $d$ | $x$ | $y$ |
|----|----|------|----|-----|-----|
| 99 | 78 | 1 | 3 | -11 | 14 |
| 78 | 21 | 3 | 3 | 3 | -11 |
| 21 | 15 | 1 | 3 | -2 | 3 |
| 15 | 6 | 2 | 3 | 1 | -2 |
| 6 | 3 | 2 | 3 | 0 | 1 |
| 3 | 0 | - | 3 | 1 | 0 |

## Props about Divisions

Theorem

$$(k \mid m) \wedge (k \mid n) \Leftrightarrow k \mid \gcd(m, n)$$

- follows directly from definition.

Theorem (The conjuctuce of factors)

$$\sum_{m \mid n} a_m = \sum_{m \mid n} a_{n \mid m}, \text{ integer } n > 0.$$

- Are there anything similar to this?

Motivation for this (by definition):

$$\sum_{m \mid n} a_m = \sum_{k} \sum_{m > 0} a_m [n = mk]$$

# Props about Divisions

Theorem

$$(k \mid m) \wedge (k \mid n) \Leftrightarrow k \mid \gcd(m, n)$$

$$\sum_{m \mid n} a_m = \sum_{k} \sum_{m > 0} a_m [n = mk]$$

Following above, we have

Theorem (Interchange summation order)

$$\sum_{m \mid n} \sum_{k \mid m} a_{k,m} = \sum_{k \mid n} \sum_{l \mid (n/k)} a_{k,kl}$$

## Proof for Interchange the order

### Theorem

$$\sum_{m|n} \sum_{k|m} a_{k,m} = \sum_{k|n} \sum_{l|(n/k)} a_{k,kl}$$

Consider LHS:

# Proof for Interchange the order

## Theorem

$$\sum_{m|n} \sum_{k|m} a_{k,m} = \sum_{k|n} \sum_{l|(n/k)} a_{k,kl}$$

Consider LHS:

$$\sum_{j,l} \sum_{k,m>0} a_{k,m}[n=jm][m=kl] =$$

# Proof for Interchange the order

## Theorem

$$\sum_{m|n} \sum_{k|m} a_{k,m} = \sum_{k|n} \sum_{l|(n/k)} a_{k,kl}$$

Consider LHS:

$$\sum_{j,l} \sum_{k,m>0} a_{k,m}[n=jm][m=kl] = \sum_{j} \sum_{k,l>0} a_{k,kl}[n=jkl]$$

# Proof for Interchange the order

## Theorem

$$\sum_{m|n} \sum_{k|m} a_{k,m} = \sum_{k|n} \sum_{l|(n/k)} a_{k,kl}$$

Consider LHS:

$$\sum_{j,l} \sum_{k,m>0} a_{k,m}[n = jm][m = kl] = \sum_{j} \sum_{k,l>0} a_{k,kl}[n = jkl]$$

Consider RHS:

# Proof for Interchange the order

## Theorem

$$\sum_{m|n}\sum_{k|m} a_{k,m} = \sum_{k|n}\sum_{l|(n/k)} a_{k,kl}$$

Consider LHS:

$$\sum_{j,l}\sum_{k,m>0} a_{k,m}[n=jm][m=kl] = \sum_{j}\sum_{k,l>0} a_{k,kl}[n=jkl]$$

Consider RHS:

$$\sum_{j,m}\sum_{k,l>0} a_{k,kl}[n=jk][n/k=ml] = \sum_{m}\sum_{k,l>0} a_{k,kl}[n=mlk]$$

They are the same, standing the same meaning.

## Interchange of Order Example

If $k = 12$:

$$
\begin{array}{c|cccccc}
m = 1 & k = 1 \\
m = 2 & k = 1 & k = 2 \\
m = 3 & k = 1 & k = 3 \\
m = 4 & k = 1 & k = 2 & k = 4 \\
m = 6 & k = 1 & k = 2 & k = 3 & k = 6 \\
m = 12 & k = 1 & k = 2 & k = 3 & k = 4 & k = 6 & k = 12
\end{array}
$$

to

| $k = 1$ | $k = 2$ | $k = 3$ | $k = 4$ | $k = 6$ | $k = 12$ |
|---------|---------|---------|---------|---------|----------|
| $m = 1$ | $m = 2$ | $m = 3$ | $m = 4$ | $m = 6$ | $m = 12$ |
| $m = 2$ | $m = 4$ | $m = 6$ | $m = 12$ | $m = 12$ | |
| $m = 3$ | $m = 6$ | $m = 12$ | | | |
| $m = 4$ | $m = 12$ | | | | |
| $m = 6$ | | | | | |
| $m = 12$ | | | | | |

# Prime

### Definition

A positive integer $p$ is called prime if it has just two divisors, namely $1$ and $p$. We will also take $p$ to represent some prime in this chapter.

Example:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots$$

## Prime Factorlization

### Theorem
*Any positive integer $n$ can be written as a product of primes.*

$$n = p_1 \ldots p_m = \prod_{k=1}^{m} p_k, \quad p_1 \leqslant \ldots \leqslant p_m$$

Proof idea.

- By Contradiction, assume $n = p_1 \ldots p_m = q_1 \ldots q_k$, $\quad p_1 \leqslant \cdots \leqslant p_m$ and $\quad q_1 \leqslant \cdots \leqslant q_k$
- Prove $p_1 = q_1$
  - assume $p_1 < q_1$, and they are primes, their gcd must be 1.
  - Using Euclid's Algo, we get $ap_1 + bq_1 = 1$
  - we will get $ap_1 q_2 \ldots q_k + bq_1 q_2 \ldots q_k = q_2 \ldots q_k$.
  - teal has factor of $q_1$
  - but $q_2 \ldots q_k < n$, contradiction, unless eq.

## Alternative means for GCD and LCM

$$n = \prod_p p^{n_p}, \qquad \text{where each } n_p \geqslant 0$$

- Unique!
- linear combination!
- just like coordinate system
- infinite dimensions

We can formally describe like this:

- $\langle n_2, n_3, n_5, \ldots \rangle$
- $12 = \langle 2, 1, 0, 0, \ldots \rangle$

## Alternative means for GCD and LCM

$$n = \prod_p p^{n_p}, \qquad \text{where each } n_p \geqslant 0$$

$$k = mn \quad \Longleftrightarrow \quad k_p = m_p + n_p \quad \text{for all } p.$$

$$m \mid n \quad \Longleftrightarrow \quad m_p \leqslant n_p \text{ for all } p$$

$$k = \gcd(m, n) \quad \Longleftrightarrow \quad k_p = \min(m_p, n_p) \quad \text{for all } p;$$
$$k = \mathrm{lcm}(m, n) \quad \Longleftrightarrow \quad k_p = \max(m_p, n_p) \quad \text{for all } p.$$

# There Are Infinitely Many primes

*"Oi    πρῶτοι    ἀριθμο`πλείοις    εἰσὶπαντὰςτοῦ πλήθουςπρῶτων ἀριθμῶν."* — *Euler*

- Notice that $\gcd(m, m+1) = 1$.

List:

$$e_1 = 1 + 1 = 2;$$
$$e_2 = 2 + 1 = 3;$$
$$e_3 = 2 \cdot 3 + 1 = 7$$
$$e_4 = 2 \cdot 3 \cdot 7 + 1 = 43$$

# Prime density

- the $n$th prime, $P_n$, is about $n$ times the natural $\log$ of $n$:

$$P_n \sim n \ln n$$

- the number of primes $\pi(x)$ not exceeding $x$ is

$$\pi(x) \sim \frac{x}{\ln x}$$

## Factorial

Definition (Factorial)

$$n! = 1 \cdot 2 \cdot \ldots \cdot n = \prod_{k=1}^{n} k, \quad \text{integer } n \geqslant 0,$$

and we define that $0! = 1$.

Some fun properties:

- the number of digits in $n!$ exceeds $n$ when $n \geq 25$
- $1 \times 10^9$ at around 10.

How fast is factorial growing?

- Take the idea of Gaussian's trick
- we have $(n!)^2 = \prod_{k=1}^{n} k(n+1-k)$,
- hence

$$n \leqslant k(n+1-k) \leqslant \frac{1}{4}(n+1)^2$$

## Factorial: Example

### Example

For any given prime $p$, the largest power of $p$ divides $n!$ . We denote this number by $\epsilon_p(n!)$. Pattern of $\epsilon_p(n!)$?

- Observation on $p = 2, n = 10$: