

COMP9020 Week 1

Number Theory

- [LLM] - Ch. 8
- [RW] - Ch. 1, Ch. 3

Number theory in Computer Science

Applications of number theory include:

- Cryptography/Security (primes, divisibility)
- Large integer calculations (modular arithmetic)
- Date and time calculations (modular arithmetic)
- Solving optimization problems (integer linear programming)
- Interesting examples for future topics in this course

Notation for numbers

Definition

- Natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$
- Integers $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$
- Positive integers $\mathbb{N}_{>0} = \mathbb{Z}_{>0} = \{1, 2, \dots\}$
- Rational numbers (fractions) $\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$
- Real numbers (decimal or binary expansions) \mathbb{R}
 $r = a_1 a_2 \dots a_k . b_1 b_2 \dots$

In \mathbb{N} and \mathbb{Z} different symbols denote different numbers.

In \mathbb{Q} and \mathbb{R} the standard representation is not necessarily unique.

NB

*Proper ways to **introduce reals** include Dedekind cuts and Cauchy sequences, neither of which will be discussed here. Natural numbers etc. are either axiomatised or constructed from sets*
 $(0 \stackrel{\text{def}}{=} \{\}, n + 1 \stackrel{\text{def}}{=} n \cup \{n\})$

Floor and ceiling

Definition

$\lfloor \cdot \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$ — **floor** of x , the greatest integer $\leq x$

$\lceil \cdot \rceil : \mathbb{R} \longrightarrow \mathbb{Z}$ — **ceiling** of x , the least integer $\geq x$

Example

$$\lfloor \pi \rfloor = 3 = \lceil e \rceil \quad \pi, e \in \mathbb{R}; \lfloor \pi \rfloor, \lceil e \rceil \in \mathbb{Z}$$

Simple properties

- $\lfloor -x \rfloor = -\lceil x \rceil$, hence $\lceil x \rceil = -\lfloor -x \rfloor$
- $\lfloor x + t \rfloor = \lfloor x \rfloor + t$ and $\lceil x + t \rceil = \lceil x \rceil + t$, for all $t \in \mathbb{Z}$

Fact

Let $k, m, n \in \mathbb{Z}$ such that $k > 0$ and $m \geq n$. The number of multiples of k between n and m (inclusive) is

$$\left\lfloor \frac{m}{k} \right\rfloor - \left\lfloor \frac{n-1}{k} \right\rfloor$$

Exercises

Exercises

RW: 1.1.4

- (b) $2 \lfloor 0.6 \rfloor - \lfloor 1.2 \rfloor =$
 $2 \lceil 0.6 \rceil - \lceil 1.2 \rceil =$
- (d) $\lceil \sqrt{3} \rceil - \lfloor \sqrt{3} \rfloor =$

RW: 1.1.19

- (a) Give x, y such that $\lfloor x \rfloor + \lfloor y \rfloor < \lfloor x + y \rfloor$:

Exercises

Exercises

RW: 1.1.4

(b) $2 \lfloor 0.6 \rfloor - \lfloor 1.2 \rfloor = ?$

$$2 \lceil 0.6 \rceil - \lceil 1.2 \rceil = ?$$

(d) $\lceil \sqrt{3} \rceil - \lfloor \sqrt{3} \rfloor = ?$

RW: 1.1.19

(a) Give x, y such that $\lfloor x \rfloor + \lfloor y \rfloor < \lfloor x + y \rfloor$:
?

Divisibility

Definition

For $m, n \in \mathbb{Z}$, we say m **divides** n if $n = k \cdot m$ for some $k \in \mathbb{Z}$.

We denote this by $m|n$

Also stated as: ' n is divisible by m ', ' m is a divisor of n ', ' n is a multiple of m '

$m \nmid n$ — negation of $m|n$

Notion of divisibility applies to all integers — positive, negative and zero.

$1|m$, $-1|m$, $m|m$, $m|-m$, for every m

$n|0$ for every n ; $0 \nmid n$ except $n = 0$

Definition

Let $m, n \in \mathbb{Z}$.

- The **greatest common divisor** of m and n , $\gcd(m, n)$, is the largest positive d such that $d|m$ and $d|n$.
- The **least common multiple** of m and n , $\text{lcm}(m, n)$, is the smallest positive k such that $m|k$ and $n|k$.
- Exception: $\gcd(0, 0) = \text{lcm}(0, 0) = 0$.

NB

$\gcd(m, n)$ and $\text{lcm}(m, n)$ are always taken as non-negative, even if m or n is negative.

$$\begin{aligned}\gcd(-4, 6) &= \gcd(4, -6) = \gcd(-4, -6) = \gcd(4, 6) = 2 \\ \text{lcm}(-5, -5) &= \dots = 5\end{aligned}$$

Primes and relatively prime

Definition

- A number $n > 1$ is **prime** if it is only divisible by ± 1 and $\pm n$.
- m and n are **relatively prime** if $\gcd(m, n) = 1$

Absolute Value

Definition

$$|x| = \begin{cases} x & , \text{ if } x \geq 0 \\ -x & , \text{ if } x < 0 \end{cases}$$

Fact

$$\gcd(m, n) \cdot \text{lcm}(m, n) = |m| \cdot |n|$$

Exercises

Exercises

RW: 1.2.2 True or False. Explain briefly.

(a) $n|1$

(b) $n|n$

(c) $n|n^2$

RW: 1.2.7(b) $\gcd(0, n) \stackrel{?}{=}$

RW: 1.2.12 Can two even integers be relatively prime?

RW: 1.2.9 Let m, n be positive integers.

(a) What can you say about m and n if $\text{lcm}(m, n) = m \cdot n$?

(b) What if $\text{lcm}(m, n) = n$?

Exercises

Exercises

RW: 1.2.2 True or False. Explain briefly.

(a) $n|1$?

(b) $n|n$?

(c) $n|n^2$?

RW: 1.2.7(b) $\gcd(0, n) \stackrel{?}{=}$

RW: 1.2.12 Can two even integers be relatively prime?

RW: 1.2.9 Let m, n be positive integers.

(a) What can you say about m and n if $\text{lcm}(m, n) = m \cdot n$?

(b) What if $\text{lcm}(m, n) = n$?

Exercises

Exercises

RW: 1.2.2 True or False. Explain briefly.

(a) $n|1$?

(b) $n|n$?

(c) $n|n^2$?

RW: 1.2.7(b) $\gcd(0, n) \stackrel{?}{=} ?$

RW: 1.2.12 Can two even integers be relatively prime?

RW: 1.2.9 Let m, n be positive integers.

(a) What can you say about m and n if $\text{lcm}(m, n) = m \cdot n$?

(b) What if $\text{lcm}(m, n) = n$?

Exercises

Exercises

RW: 1.2.2 True or False. Explain briefly.

(a) $n|1$?

(b) $n|n$?

(c) $n|n^2$?

RW: 1.2.7(b) $\gcd(0, n) \stackrel{?}{=} ?$

RW: 1.2.12 Can two even integers be relatively prime? ?

RW: 1.2.9 Let m, n be positive integers.

(a) What can you say about m and n if $\text{lcm}(m, n) = m \cdot n$?

(b) What if $\text{lcm}(m, n) = n$?

Exercises

Exercises

RW: 1.2.2 True or False. Explain briefly.

(a) $n|1$?

(b) $n|n$?

(c) $n|n^2$?

RW: 1.2.7(b) $\gcd(0, n) \stackrel{?}{=} ?$

RW: 1.2.12 Can two even integers be relatively prime? ?

RW: 1.2.9 Let m, n be positive integers.

(a) What can you say about m and n if $\text{lcm}(m, n) = m \cdot n$?

(b) What if $\text{lcm}(m, n) = n$?

Euclid's gcd Algorithm

$$\gcd(m, n) = \begin{cases} m & \text{if } m = n \\ \gcd(m - n, n) & \text{if } m > n \\ \gcd(m, n - m) & \text{if } m < n \end{cases}$$

Euclid's gcd Algorithm

$$\gcd(m, n) = \begin{cases} m & \text{if } m = n \\ \gcd(m - n, n) & \text{if } m > n \\ \gcd(m, n - m) & \text{if } m < n \end{cases}$$

Fact

For $m > 0, n > 0$ the algorithm always terminates.

Euclid's gcd Algorithm

$$\gcd(m, n) = \begin{cases} m & \text{if } m = n \\ \gcd(m - n, n) & \text{if } m > n \\ \gcd(m, n - m) & \text{if } m < n \end{cases}$$

Fact

For $m > 0, n > 0$ the algorithm always terminates.

Fact

For $m, n \in \mathbb{Z}$, if $m > n$ then $\gcd(m, n) = \gcd(m - n, n)$

Euclid's gcd Algorithm

$$\gcd(m, n) = \begin{cases} m & \text{if } m = n \\ \gcd(m - n, n) & \text{if } m > n \\ \gcd(m, n - m) & \text{if } m < n \end{cases}$$

Fact

For $m > 0, n > 0$ the algorithm always terminates.

Fact

For $m, n \in \mathbb{Z}$, if $m > n$ then $\gcd(m, n) = \gcd(m - kn, n)$

Euclid's gcd Algorithm

Fact

For $m, n \in \mathbb{Z}$, if $m > n$ then $\gcd(m, n) = \gcd(m - n, n)$

Proof.



Euclid's gcd Algorithm

Fact

For $m, n \in \mathbb{Z}$, if $m > n$ then $\gcd(m, n) = \gcd(m - n, n)$

Proof.

We first show that for all $d \in \mathbb{Z}$, $(d|m \text{ and } d|n)$ if, and only if, $(d|m - n \text{ and } d|n)$:



Euclid's gcd Algorithm

Fact

For $m, n \in \mathbb{Z}$, if $m > n$ then $\gcd(m, n) = \gcd(m - n, n)$

Proof.

We first show that for all $d \in \mathbb{Z}$, ($d|m$ and $d|n$) if, and only if, ($d|m - n$ and $d|n$):

" \Rightarrow ": if $d|m$ and $d|n$ then $m = a \cdot d$ and $n = b \cdot d$, for some $a, b \in \mathbb{Z}$,
so $m - n = (a - b) \cdot d$,
hence $d|m - n$



Euclid's gcd Algorithm

Fact

For $m, n \in \mathbb{Z}$, if $m > n$ then $\gcd(m, n) = \gcd(m - n, n)$

Proof.

We first show that for all $d \in \mathbb{Z}$, ($d|m$ and $d|n$) if, and only if, ($d|m - n$ and $d|n$):

" \Rightarrow ": if $d|m$ and $d|n$ then $m = a \cdot d$ and $n = b \cdot d$, for some $a, b \in \mathbb{Z}$,
so $m - n = (a - b) \cdot d$,
hence $d|m - n$

" \Leftarrow ": if $d|m - n$ and $d|n$ then $m - n = a \cdot d$ and $n = b \cdot d$, for some $a, b \in \mathbb{Z}$,

so $m = (m - n) + n = (a + b) \cdot d$,
hence $d|m$



Euclid's gcd Algorithm

Fact

For $m, n \in \mathbb{Z}$, if $m > n$ then $\gcd(m, n) = \gcd(m - n, n)$

Proof.

We first show that for all $d \in \mathbb{Z}$, ($d|m$ and $d|n$) if, and only if, ($d|m - n$ and $d|n$):

“ \Rightarrow ”: if $d|m$ and $d|n$ then $m = a \cdot d$ and $n = b \cdot d$, for some $a, b \in \mathbb{Z}$,
so $m - n = (a - b) \cdot d$,
hence $d|m - n$

“ \Leftarrow ”: if $d|m - n$ and $d|n$ then $m - n = a \cdot d$ and $n = b \cdot d$, for some $a, b \in \mathbb{Z}$,
so $m = (m - n) + n = (a + b) \cdot d$,
hence $d|m$

Therefore, any common divisor of m and n is a common divisor of $m - n$ and n , and vice versa.



Euclid's gcd Algorithm

Fact

For $m, n \in \mathbb{Z}$, if $m > n$ then $\gcd(m, n) = \gcd(m - n, n)$

Proof.

We first show that for all $d \in \mathbb{Z}$, ($d|m$ and $d|n$) if, and only if, ($d|m - n$ and $d|n$):

“ \Rightarrow ”: if $d|m$ and $d|n$ then $m = a \cdot d$ and $n = b \cdot d$, for some $a, b \in \mathbb{Z}$,
so $m - n = (a - b) \cdot d$,
hence $d|m - n$

“ \Leftarrow ”: if $d|m - n$ and $d|n$ then $m - n = a \cdot d$ and $n = b \cdot d$, for some $a, b \in \mathbb{Z}$,
so $m = (m - n) + n = (a + b) \cdot d$,
hence $d|m$

Therefore, any common divisor of m and n is a common divisor of $m - n$ and n , and vice versa.

Therefore, the greatest common divisor of m and n is the greatest common divisor of $m - n$ and n .



Euclid's gcd Algorithm

Example

$$\text{gcd}(45, 27) =$$

Euclid's gcd Algorithm

Example

$$\gcd(45, 27) = \gcd(18, 27)$$

Euclid's gcd Algorithm

Example

$$\begin{aligned}\gcd(45, 27) &= \gcd(18, 27) \\ &= \gcd(18, 9)\end{aligned}$$

Euclid's gcd Algorithm

Example

$$\begin{aligned}\gcd(45, 27) &= \gcd(18, 27) \\ &= \gcd(18, 9) \\ &= \gcd(9, 9)\end{aligned}$$

Euclid's gcd Algorithm

Example

$$\begin{aligned}\gcd(45, 27) &= \gcd(18, 27) \\ &= \gcd(18, 9) \\ &= \gcd(9, 9) \\ &= 9\end{aligned}$$

Euclid's gcd Algorithm

Example

$$\text{gcd}(108, 8) =$$

Euclid's gcd Algorithm

Example

$$\gcd(108, 8) = \gcd(100, 8)$$

Euclid's gcd Algorithm

Example

$$\begin{aligned}\gcd(108, 8) &= \gcd(100, 8) \\ &= \gcd(92, 8)\end{aligned}$$

Euclid's gcd Algorithm

Example

$$\begin{aligned}\gcd(108, 8) &= \gcd(100, 8) \\ &= \gcd(92, 8) \\ &= \gcd(84, 8)\end{aligned}$$

Euclid's gcd Algorithm

Example

$$\begin{aligned}\gcd(108, 8) &= \gcd(100, 8) \\ &= \gcd(92, 8) \\ &= \gcd(84, 8) \\ &\vdots \\ &= \gcd(4, 8)\end{aligned}$$

Euclid's gcd Algorithm

Example

$$\begin{aligned}\gcd(108, 8) &= \gcd(100, 8) \\ &= \gcd(92, 8) \\ &= \gcd(84, 8) \\ &\vdots \\ &= \gcd(4, 8) \\ &= \gcd(4, 4)\end{aligned}$$

Euclid's gcd Algorithm

Example

$$\begin{aligned}\gcd(108, 8) &= \gcd(100, 8) \\ &= \gcd(92, 8) \\ &= \gcd(84, 8) \\ &\vdots \\ &= \gcd(4, 8) \\ &= \gcd(4, 4) \\ &= 4\end{aligned}$$

mod and div

Definition

Let $m, p \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$.

- $m \operatorname{div} n = \lfloor \frac{m}{n} \rfloor$
- $m \% n = m - (m \operatorname{div} n) \cdot n$
- $m \equiv_n p$ if $n \mid (m - p)$

NB

$m \equiv_n p$ is **not standard**. More commonly written as

$$m = p \pmod{n}$$

mod and div

Fact

- $0 \leq (m \% n) < n$.

mod and div

Fact

- $0 \leq (m \% n) < n$.

mod and div

Fact

- $0 \leq (m \% n) < n$.
- $m \stackrel{\text{mod } n}{=} p$ if, and only if, $(m \% n) = (p \% n)$.

mod and div

Fact

- $0 \leq (m \% n) < n$.
- $m \equiv p \pmod n$ if, and only if, $(m \% n) = (p \% n)$.
- If $m \equiv m' \pmod n$ and $p \equiv p' \pmod n$ then:
 - $m + p \equiv m' + p' \pmod n$ and
 - $m \cdot p \equiv m' \cdot p' \pmod n$.

Exercises

Exercises

- $42 \text{ div } 9$?
- $42 \% 9$?
- $-42 \text{ div } 9$?
- $-42 \% 9$?
- *True or False.* $(a + b) \% n = (a \% n) + (b \% n)$?

Exercises

Exercises

- $42 \text{ div } 9?$?
- $42 \% 9?$?
- $-42 \text{ div } 9?$?
- $-42 \% 9?$?
- *True or False.* $(a + b) \% n = (a \% n) + (b \% n)?$

Exercises

Exercises

- $42 \text{ div } 9?$?
- $42 \% 9?$?
- $-42 \text{ div } 9?$?
- $-42 \% 9?$?
- *True or False.* $(a + b) \% n = (a \% n) + (b \% n)?$
?

Exercises

Exercises

- $10^3 \% 7?$
- $10^6 \% 7?$
- $10^{2020} \% 7?$
- What is the last digit of 7^{2020} ?

Exercises

Exercises

- $10^3 \% 7?$?
- $10^6 \% 7?$?
- $10^{2020} \% 7?$?
- What is the last digit of 7^{2020} ?

Exercises

Exercises

- $10^3 \% 7?$?
- $10^6 \% 7?$?
- $10^{2020} \% 7?$?
- What is the last digit of 7^{2020} ? ?

Exercises

Exercises

RW: 3.5.20

- (a) Show that the 4 digit number $n = abcd$ is divisible by 2 if and only if the last digit d is divisible by 2.
- (b) Show that the 4 digit number $n = abcd$ is divisible by 5 if and only if the last digit d is divisible by 5.

RW: 3.5.19

- (a) Show that the 4 digit number $n = abcd$ is divisible by 9 if and only if the digit sum $a + b + c + d$ is divisible by 9.

Faster Euclidean gcd Algorithm

$$\text{gcd}(m, n) = \begin{cases} m & \text{if } m = n \text{ or } n = 0 \\ n & \text{if } m = 0 \\ \text{gcd}(m \% n, n) & \text{if } m > n > 0 \\ \text{gcd}(m, n \% m) & \text{if } 0 < m < n \end{cases}$$

Fact

For $m, n \in \mathbb{Z}$, if $m > n$ then $\text{gcd}(m, n) = \text{gcd}(m \% n, n)$

Proof.

Let $k = m \text{ div } n$. Then $m \% n = m - k \cdot n$.

Faster Euclidean gcd Algorithm

Example

$$\gcd(108, 8) =$$

Faster Euclidean gcd Algorithm

Example

$$\gcd(108, 8) = \gcd(100, 8)$$

Faster Euclidean gcd Algorithm

Example

$$\begin{aligned}\gcd(108, 8) &= \gcd(100, 8) \\ &= \gcd(4, 8)\end{aligned}$$

Faster Euclidean gcd Algorithm

Example

$$\begin{aligned}\gcd(108, 8) &= \gcd(100, 8) \\ &= \gcd(4, 8) \\ &= \gcd(4, 4)\end{aligned}$$

Faster Euclidean gcd Algorithm

Example

$$\begin{aligned}\gcd(108, 8) &= \gcd(100, 8) \\ &= \gcd(4, 8) \\ &= \gcd(4, 4) \\ &= 4\end{aligned}$$