COMP9020

Foundations of Computer Science

Lecture 2: Number Theory

Lecturers: Katie Clinch (LIC)
Paul Hunter
Simon Mackenzie

Course admin: Nicholas Tandiono

Course email: cs9020@cse.unsw.edu.au

Announcements

Quiz 1

- Available now (inspera link)
- Due **18:00 Wednesday 21 February (AEDT)** (next week)
- Tests what you will learn this lecture

Assignment 1

- Available now (inspera link)
- Due **18:00 Thursday 29 February (AEDT)** (in 2 weeks)
- The first question tests material from today's lecture.
- The other questions test material from next week's lectures.

Available support available to help with the above

- In-person help sessions (immediately after this lecture!) And every Thursday and Friday
- Online consultations (Tuesday and Wednesday evenings)
- edforum

Further reading

If you'd like to read more about the topics covered in this lecture, check out the following chapters of the recommended textbooks:

		[LLM]	[RW]
Week 1	Number Theory	Ch. 8	Ch. 1, 3

- **[RW]** is KA Ross and CR Wright: Discrete Mathematics
- **[LLM]** is Lehman, Leighton, Meyer: Mathematics for Computer Science

Number Theory in Computer Science

In this course, we are interested in **discrete mathematics**. This is the theory of e.g. the integers.

Continuous mathematics instead considers number systems with no "gaps", e.g. the real numbers.

Applications of **discrete 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

Question

What is something that is easy to do with real numbers but hard to do with integers?

Outline

Outline

Notation for numbers

Definition

- Natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$
- Integers $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$
- Positive integers $\mathbb{N}_{>0} = \mathbb{Z}_{>0} = \{1, 2, \ldots\}$

- Rational numbers (fractions) $\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$
- Real numbers (decimal or binary expansions) $\mathbb{R}$
  $r = a_1 a_2 \ldots a_k \,.\, b_1 b_2 \ldots$

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

$$1 \neq 2 \neq 3$$

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

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6}$$

It's quite easy to intuitively understand what the real numbers $\mathbb{R}$ or the natural numbers $\mathbb{N}$ are.

It's quite easy to intuitively understand what the real numbers $\mathbb{R}$ or the natural numbers $\mathbb{N}$ are.

But it's surprisingly difficult to write a precise mathematical explanation of this!

It's quite easy to intuitively understand what the real numbers $\mathbb{R}$ or the natural numbers $\mathbb{N}$ are.

But it's surprisingly difficult to write a precise mathematical explanation of this!

NB

Proper ways to introduce reals include Dedekind cuts and Cauchy sequences.

Natural numbers etc. are either axiomatised or constructed from **sets** $(0 \stackrel{def}{=} \{\}, n+1 \stackrel{def}{=} n \cup \{n\})$

Dedekind cuts and Cauchy sequences are far beyond the scope of this course.

We will see **set theory** next week (and then the above definition for the natural numbers will make a bit more sense).

Floor and ceiling

Definition

$\lfloor . \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$ — **floor** of x, the greatest integer $\leq x$
$\lceil . \rceil : \mathbb{R} \longrightarrow \mathbb{Z}$ — **ceiling** of x, the least integer $\geq x$

Example

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

Floor and ceiling

Definition

$\lfloor . \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$ — **floor** of x, the greatest integer $\leq x$
$\lceil . \rceil : \mathbb{R} \longrightarrow \mathbb{Z}$ — **ceiling** of x, the least integer $\geq x$

Example

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

Simple properties

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

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*

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

Absolute value

Definition

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

Example

$|3| = |-3| = 3 \qquad 3, -3 \in \mathbb{Z};\ |3|, |-3| \in \mathbb{N}$

Exercises

Exercises

$\boxed{\text{RW: 1.1.4}}$

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

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

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

$\boxed{\text{RW: 1.1.19}}$

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

$\boxed{\text{20T2: Q1 (a)}}$

(i) True or false for all $x \in \mathbb{R}$:

$\lceil |x| \rceil = |\lceil x\rceil|$

Exercises

$\boxed{\text{RW: 1.1.4}}$

(b) $2\lfloor 0.6 \rfloor - \lfloor 1.2 \rfloor = -1$

$2\lceil 0.6 \rceil - \lceil 1.2 \rceil = 0$

(d) $\lceil \sqrt{3} \rceil - \lfloor \sqrt{3} \rfloor = 1$

$\boxed{\text{RW: 1.1.19}}$

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

$x = y = 0.9$

$\boxed{\text{20T2: Q1 (a)}}$

(i) True or false for all $x \in \mathbb{R}$:

$\lceil |x| \rceil = |\lceil x \rceil|$ — false (e.g. $x = -1.5$)

Outline

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'

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'

$m \nmid n$ is the negation of $m|n$.

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'

$m \nmid n$ is the negation of $m|n$.
In other words, $m \nmid n$ means 'm **does not divide** n'

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'

$m \nmid n$ is the negation of $m|n$.
In other words, $m \nmid n$ means 'm **does not divide** n'

NB

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

Exercises

Exercises

True or *False* for all $n \in \mathbb{Z}$:

- $1 | n$
- $-1 | n$
- $0 | n$
- $n | 0$

$\boxed{\text{RW: 1.2.2}}$

(a) $n | 1$
(b) $n | n$
(c) $n | n^2$

Exercises

Exercises

True or *False* for all $n \in \mathbb{Z}$:

- $1|n$ — true
- $-1|n$ — true
- $0|n$ — false (only when $n = 0$)
- $n|0$ — true

RW: 1.2.2

(a) $n|1$ — false (only when $n = \pm 1$)
(b) $n|n$ — true
(c) $n|n^2$ — true

Outline

gcd and lcm

Definition

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

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

Example

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

gcd and lcm

NB

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

Fact

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

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 $\gcd(m, n) = 1$

Examples

- $2, 3, 5, 7, 11, 13, 17, 19$ are all the primes less than 20.
- 4 and 9 are relatively prime; 9 and 14 are relatively prime.

Exercises

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

$\boxed{\text{RW: 1.2.12}}$ Can two even integers be relatively prime?

$\boxed{\text{RW: 1.2.9}}$ Let m, n be positive integers.
(a) What can you say about m and n if $\operatorname{lcm}(m, n) = m \cdot n$?

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

Exercises

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

$\boxed{\text{RW: 1.2.12}}$ Can two even integers be relatively prime?

$\boxed{\text{RW: 1.2.9}}$ Let m, n be positive integers.
(a) What can you say about m and n if $\operatorname{lcm}(m, n) = m \cdot n$?

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

Exercises

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

$\boxed{\text{RW: 1.2.12}}$ Can two even integers be relatively prime?

$\boxed{\text{RW: 1.2.9}}$ Let m, n be positive integers.
(a) What can you say about m and n if $\operatorname{lcm}(m, n) = m \cdot n$?

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

Exercises

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

$\boxed{\text{RW: 1.2.12}}$ Can two even integers be relatively prime? No. (why?)

$\boxed{\text{RW: 1.2.9}}$ Let m, n be positive integers.
(a) What can you say about m and n if $\operatorname{lcm}(m, n) = m \cdot n$?

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

Exercises

Exercises

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

$\boxed{\text{RW: 1.2.12}}$ Can two even integers be relatively prime? No. (why?)

$\boxed{\text{RW: 1.2.9}}$ Let m, n be positive integers.
(a) What can you say about m and n if $\operatorname{lcm}(m, n) = m \cdot n$?
They must be relatively prime since always $\operatorname{lcm}(m, n) = \frac{mn}{\gcd(m,n)}$
(b) What if $\operatorname{lcm}(m, n) = n$?
m must be a divisor of n

Outline

Euclid's gcd Algorithm

Question. How do we compute the greatest common divisor $\gcd(m, n)$? Especially when the numbers m, n are large?

Answer. Euclid's algorithm gives a way of doing this by repeatedly replacing m and n with smaller numbers. This method is over 2000 years old!

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

Euclid's gcd Algorithm

Question. How do we compute the greatest common divisor $\gcd(m, n)$? Especially when the numbers m, n are large?

Answer. Euclid's algorithm gives a way of doing this by repeatedly replacing m and n with smaller numbers. This method is over 2000 years old!

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

Example

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

Euclid's gcd Algorithm

Question. How do we compute the greatest common divisor $\gcd(m, n)$? Especially when the numbers m, n are large?

Answer. Euclid's algorithm gives a way of doing this by repeatedly replacing m and n with smaller numbers. This method is over 2000 years old!

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

Example

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

Euclid's gcd Algorithm

Question. How do we compute the greatest common divisor $\gcd(m,n)$? Especially when the numbers m, n are large?

Answer. Euclid's algorithm gives a way of doing this by repeatedly replacing m and n with smaller numbers. This method is over 2000 years old!

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

Example

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

Euclid's gcd Algorithm

Question. How do we compute the greatest common divisor $\gcd(m, n)$? Especially when the numbers m, n are large?

Answer. Euclid's algorithm gives a way of doing this by repeatedly replacing m and n with smaller numbers. This method is over 2000 years old!

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

Example

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

Euclid's gcd Algorithm

Question. How do we compute the greatest common divisor $\gcd(m, n)$? Especially when the numbers m, n are large?

Answer. Euclid's algorithm gives a way of doing this by repeatedly replacing m and n with smaller numbers. This method is over 2000 years old!

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

Fact

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

Euclid's gcd Algorithm

Question. How do we compute the greatest common divisor $\gcd(m, n)$? Especially when the numbers m, n are large?

Answer. Euclid's algorithm gives a way of doing this by repeatedly replacing m and n with smaller numbers. This method is over 2000 years old!

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

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

Fact

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

Proof.

$\square$

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 $d|n$):

$\square$

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 $d|m - n$

$\square$

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.

$\square$

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. $\square$

Outline

Euclid's division lemma

Fact

For $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ *there exists* $q, r \in \mathbb{Z}$ *with* $0 \leq r < n$ *such that*

$$m = q \cdot n + r$$

Euclid's division lemma

Fact

For $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ *there exists* $q, r \in \mathbb{Z}$ *with* $0 \leq r < n$ *such that*

$$m = q \cdot n + r$$

Observe:

- $q = \lfloor \frac{m}{n} \rfloor$

Euclid's division lemma

Fact

For $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ *there exists* $q, r \in \mathbb{Z}$ *with* $0 \leq r < n$ *such that*

$$m = q \cdot n + r$$

Observe:

- $q = \lfloor \frac{m}{n} \rfloor$
- $r = m - q \cdot n$

mod and div

Definition

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

- m div $n = \lfloor \frac{m}{n} \rfloor$
- $m \,\%\, n = m - (m \text{ div } n) \cdot n$
- $m =_{(n)} p$ if $n | (m - p)$

mod and div

Definition

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

- $m \text{ div } n = \lfloor \frac{m}{n} \rfloor$
- $m \% n = m - (m \text{ div } n) \cdot n$
- $m =_{(n)} p$ if $n | (m - p)$

Important!

$m =_{(n)} p$ is **not standard**. More commonly written as

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

mod and div

Fact

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

mod and div

Fact

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

mod and div

Fact

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

mod and div

Fact

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

Exercises

Exercises

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

Exercises

Exercises

- $42 \text{ div } 9 \stackrel{?}{=} 4$
- $42 \,\%\, 9 \stackrel{?}{=} 6$
- $(-42) \text{ div } 9 \stackrel{?}{=} -5$
- $(-42) \,\%\, 9 \stackrel{?}{=} 3$
- *True* or *False*:
  $(a+b) \,\%\, n = (a \,\%\, n) + (b \,\%\, n)$?

Exercises

Exercises

- $42 \text{ div } 9 \stackrel{?}{=} \quad 4$
- $42 \ \% \ 9 \stackrel{?}{=} \quad 6$
- $(-42) \text{ div } 9 \stackrel{?}{=} \quad -5$
- $(-42) \ \% \ 9 \stackrel{?}{=} \quad 3$
- *True* or *False*:

  $(a + b) \ \% \ n = (a \ \% \ n) + (b \ \% \ n)$?

  False (take $a = b = 1$, $n = 2$)

Exercises

Exercises

- $10^3 \% 7 \stackrel{?}{=}$
- $10^6 \% 7 \stackrel{?}{=}$
- $10^{2021} \% 7 \stackrel{?}{=}$
- What is the last digit of 7^{2023}?

Exercises

- $10^3 \ \% \ 7 \stackrel{?}{=}$ 6
- $10^6 \ \% \ 7 \stackrel{?}{=}$ 1
- $10^{2021} \ \% \ 7 \stackrel{?}{=}$ 5
- What is the last digit of 7^{2023}?

Exercises

- $10^3 \,\%\, 7 \stackrel{?}{=}$ 6
- $10^6 \,\%\, 7 \stackrel{?}{=}$ 1
- $10^{2021} \,\%\, 7 \stackrel{?}{=}$ 5
- What is the last digit of 7^{2023}? 3

Exercises

$\boxed{\text{RW: 3.5.20}}$

(a) Show that the 4 digit number $n = \mathtt{abcd}$ is divisible by 2 if and only if the last digit $\mathtt{d}$ is divisible by 2.

(b) Show that the 4 digit number $n = \mathtt{abcd}$ is divisible by 5 if and only if the last digit $\mathtt{d}$ is divisible by 5.

$\boxed{\text{RW: 3.5.19}}$

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

Outline

Faster Euclidean gcd Algorithm

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

Fact

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

Proof.
Let $k = m \operatorname{div} n$*. Then* $m \,\%\, n = m - k \cdot n$*.*

Faster Euclidean gcd Algorithm

Example

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

Faster Euclidean gcd Algorithm

Example

$$\gcd(108, 8) \quad = \quad \gcd(4, 8)$$

Faster Euclidean gcd Algorithm

Example

$$\begin{aligned} \gcd(108, 8) &= \gcd(4, 8) \\ &= \gcd(4, 0) \end{aligned}$$

Faster Euclidean gcd Algorithm

Example

$$\begin{aligned} \gcd(108, 8) &= \gcd(4, 8) \\ &= \gcd(4, 0) \\ &= 4 \end{aligned}$$

Outline

Weekly Feedback

We would appreciate any comments/suggestions/requests you have on this week's lectures.

https://forms.office.com/r/aHRCGANHiB