COMP9020

Foundations of Computer Science

Lecture 2: Number Theory

Administrivia

- Quiz 1 released Saturday; due **15:00 Tuesday 20 September (AEST)**
- First Challenge Problem available following the lecture
- Reminder: Consultation on Today 8:30pm, Sunday 8pm
- Weekly feedback

Topic 0: Number Theory

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

Outline

Numbers and Numerical Operations

Divisibility

Greatest Common Divisor and Least Common Multiple

Modular Arithmetic

Euclidean Algorithm, again

Feedback

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.

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

$\lfloor . \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$ — **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

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 $\lfloor x \rfloor + \lfloor y \rfloor < \lfloor x + y \rfloor$:

20T2: Q1 (a)

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

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

Exercises

Exercises

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) $\left\lceil \sqrt{3}\right\rceil - \left\lfloor \sqrt{3}\right\rfloor = 1$

RW: 1.1.19

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

$x = y = 0.9$

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'

$m \nmid n$ — negation of $m|n$

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

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

(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 such that $d|m$ and $d|n$.
- The **least common multiple** of m and n, $\operatorname{lcm}(m, n)$, is the smallest positive k 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

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 $\mathrm{lcm}(m, n) = m \cdot n$?
They must be relatively prime since always $\mathrm{lcm}(m, n) = \frac{mn}{\gcd(m,n)}$
(b) What if $\mathrm{lcm}(m, n) = n$?
m must be a divisor of 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

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

Example

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

Euclid's gcd Algorithm

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

Example

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

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.

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*

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

Observe:

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

mod and div

Definition

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

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

Important!

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

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

mod and div

Fact

- $0 \leq (m \% n) < n$.
- $m =_{(n)} p$ *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*:
  $(a + b) \% n = (a \% n) + (b \% n)$?
  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^{2021}?

Exercises

Exercises

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

Exercises

Exercises

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.

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

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

Outline

Weekly Feedback

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

https://forms.office.com/r/JKu4mNk5rS