Number Theory: Intro, Divisibility, Modular Arithmetic

Adila A. Krisnadhi

Fakultas Ilmu Komputer, Universitas Indonesia

Version date: 2022-02-16 04:44:05+07:00

Reference: Rosen, Ed.8, Ch.4

Introduction

- Number theory: a branch of mathematics that studies integers, their characteristics, operations, and further generalization derivable from them.
  - Integer (basic) operations: addition, subtraction, multiplication, division
  - The core part of number theory is called arithmetic.
- Applications: cryptography, hashing, digit error checking.

Notation

- Set of (all) **integers**: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- Set of (all) **positive integers**: $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$
- Set of (all) **negative integers**: $\mathbb{Z}^- = \{\ldots, -3, -2, -1\}$
- Set of **natural numbers** atau **nonnegative integers**: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Agenda

1. Divisibility and Modular Arithmetic
2. Integer Representations

Discussion

- What's the difference between the divisions: $18/3$ and $16/5$?
- What makes division special for integers compared to addition, subtraction, and multiplication?
- What is the relation between 3 and 18 in the context of division?
- What is the relation between 5 and 16 in the context of division?
- What do we need in the division operation between two integers so that the result is also in an integer?

Divisibility

Definition

Let a and b be two integers with $a \neq 0$.

We say that a **divides** b iff there exists an integer c such that $b = ac$. That is, a divides b iff $\frac{a}{b} \in \mathbb{Z}$.

$a \mid b$ denotes "a divides b". Also, $a \nmid b$ denotes "a does not divide b".

If $a \mid b$, then a is called a **factor** or **divisor** of b, and b is called a **multiple** of a.

Divsibility Examples

- Is $7 \mid 13$?
- Is $3 \mid 12$?
- If n and d are positive integers, how many positive integers are there that is no greater than n and divisible by d?

Discussion

Can we generalize anything from the following facts?

- $13 \mid 65$, $13 \mid 221$, and $13 \mid 286$
- $8 \mid -24$, $8 \mid 32$, and $8 \mid 56$
- $11 \mid 44$. So, $11 \mid -88$, $11 \mid 88$, $11 \mid 176$, etc.
- $7 \mid 35$, $35 \mid 245$, and $7 \mid 245$.
- $6 \mid 18$, $6 \mid 24$, and $6 \mid 102$.

Theorem

Let a, b, c be integers with $a \neq 0$. Then,

1. *if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;*
2. *if $a \mid b$, then $a \mid bd$ for every integer d;*
3. *if $a \mid b$ and $b \mid c$, then $a \mid c$;*
4. *if $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any two integers m dan n.*

Proof?

Discussion

- What happens when we divide 19 by 5, 12 by 4, or -13 by 7?
- From your answer for the above question, can you express 19 in terms of 5, 12 in terms of 4, and -13 in terms of 7?

Division algorithm, quotient, and remainder

Theorem (The Division Algorithm)

Let a, d be integers with $d \neq 0$. Then, there exists two unique integers q and r with $0 \leqslant r < d$ such that $a = dq + r$

In the above theorem,

- the integer q is called the **quotient** and written $q = a \textbf{ div } d$
- the integer r is called **remainder** and written $r = a \textbf{ mod } d$.

Note that r is never negative.

Divison algorithm: Examples

Give the quotient and remainder when:

- 111 is divided by 13;
- -13 is divided by 3.

Divisibility and $\mathbf{mod}$ operations

Theorem

Let a and b be integers with $a \neq 0$. Then, $a \mid b$ if and only if $b \bmod a = 0$.

Proof?

Floor and ceiling functions

- Floor function:
  $\lfloor x \rfloor$ = the largest integer less than or equal to x.
- Ceiling function:
  $\lceil x \rceil$ = the smallest integer greater than or equal to x.

Theorem

For integers a, d with $d > 1$,

- $a \ \mathbf{div}\ d = \left\lfloor \frac{a}{d} \right\rfloor$
- $a \ \mathbf{mod}\ d = a - d\left\lfloor \frac{a}{d} \right\rfloor$

Proof?

Modular congruences

Sometimes, we only care about the remainder of an integer division.

- What time is 100 hours from now?
- A baby must be vaccincated on the 30th day of his/her life. If (s)he was born on February 2, 2021, then what date must (s)he be vaccinated? What if (s)he was born on February 2, 2020?

Modular congruences

Sometimes, we only care about the remainder of an integer division.

- What time is 100 hours from now?
- A baby must be vaccincated on the 30th day of his/her life. If (s)he was born on February 2, 2021, then what date must (s)he be vaccinated? What if (s)he was born on February 2, 2020?

Definition

Let a, b, m be integers with m positive. Then, $a \equiv b \pmod{m}$ iff $m \mid (a - b)$.

- The notation $a \equiv b \pmod{m}$ is called **congruence** and read "a is congruent to b modulo m". The integer m is called the **modulus**
- If a is not congruent to b modulo m, then we write $a \not\equiv b \pmod{m}$
- What is the difference between $a \equiv b \pmod{m}$ dan $a \;\mathbf{mod}\; m = b$?

Relationship between $\pmod{}$ dan $\mathbf{mod}$

Fill in this table. Can you generalize anything from this?

a	b	m	Is $a \equiv b \pmod{m}$?	$a \mathbin{\mathbf{mod}} m$	$b \mathbin{\mathbf{mod}} m$
7	12	5			
3	14	7			
-5	23	14			
-7	-4	3			
21	9	6			
17	4	6			

Relationship between $\pmod{}$ dan $\mathbf{mod}$

Theorem

Let a, b be integers and m a positive integer.
Then, $a \equiv b \pmod{m}$ if and only if $a \mathbin{\mathbf{mod}} m = b \mathbin{\mathbf{mod}} m$.

That is, $a \equiv b \pmod{m}$ if and only if a dan b have the same remainder when divided by m.

Proof?

Modular congruence and division algorithm

Fill in the table:

a	b	m	Is $a \equiv b \pmod{m}$?	$a = b + km$ (if possible)
7	12	5		
3	14	7		
-5	23	14		
-7	-4	3		
21	9	6		
17	4	6		

Modular congruence and division algorithm

Theorem

Let m be a positive integer. Then, $a \equiv b \pmod{m}$ if and only if there exists an integer k such that $a = b + km$.

Proof?

Congruence classes

If we take 5 as the modulus,

- how many integers are congruent to 7? What are they?
- what integers are congruent to 6?

Congruence classes

If we take 5 as the modulus,

- how many integers are congruent to 7? What are they?
- what integers are congruent to 6?

Definition

Let a be an integer and m a positive integer. **The congruence class of a modulo m**, written $[a]_m$, is the set of all integers congruent to a modulo m.

Give all congruence classes modulo 3!

Modular addition and multiplication

Theorem

Let m be a positive integer. Then, whenever $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ hold, then the following also hold:

- $a + c \equiv b + d \pmod{m}$, *and*
- $ac \equiv bd \pmod{m}$.

Proof?

Give an application example of the previous theorem!

Remarks

- Does $ac \equiv bc \pmod{m}$ imply $a \equiv b \pmod{m}$?

- If $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, does $a^c \equiv b^d \pmod{m}$ necessarily hold?

Remarks

- Does $ac \equiv bc \pmod{m}$ imply $a \equiv b \pmod{m}$?
  - No. For example, $2 \cdot 4 \equiv 5 \cdot 4 \pmod{6}$, but $2 \not\equiv 5 \pmod{6}$.

  So, you **cannot** cross out the multiplier from both sides of congruences.
- If $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, does $a^c \equiv b^d \pmod{m}$ necessarily hold?

Remarks

- Does $ac \equiv bc \pmod{m}$ imply $a \equiv b \pmod{m}$?
  - No. For example, $2 \cdot 4 \equiv 5 \cdot 4 \pmod{6}$, but $2 \not\equiv 5 \pmod{6}$.

  So, you **cannot** cross out the multiplier from both sides of congruences.
- If $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, does $a^c \equiv b^d \pmod{m}$ necessarily hold?
  - No. For example, $3 \equiv 8 \pmod{5}$ and $6 \equiv 1 \pmod{5}$, but $729 = 3^6 \not\equiv 8^1 = 8 \pmod{5}$.

  So, pair of congruent bases and congruent exponents do not make the result of the exponentiation congruent.

Modulo addition and multiplication

Theorem

Let m be a positive integer and a, b integers. Then,

- $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$

Proof?

Example

Calculate $(19^3 \bmod 31)^4 \bmod 23$?

Applications of modular congruence

- Hasing functions, e.g., for load balancing of storing data or for servers when responding to requests, etc.
- Pseudorandom number generation.
- Cryptology:
  - Caesar cipher encrypts messages using a modular congruence, e.g., the encryption of a letter p is $f(p) = (p + 1) \mathbf{mod}\, 26$, and the encrypted message can be decrypted using the function $g(p) = (p - 1) \mathbf{mod}\, 26$.
  - What is the original message of J MPWF ZPT?

Agenda

Integer representation: Overview

- Representation depends on base of choice.
- Every **positive** integer $b > 1$ can be used of basis.
- A base-b representation employs b different symbols.
- Some commonly used bases:
  - Base 10 (decimal) $\rightsquigarrow$ 10 symbols: $0, 1, \ldots, 9$
  - Base 2 (binary) $\rightsquigarrow$ 2 symbols: $0, 1$
  - Base 8 (octal) $\rightsquigarrow$ 8 symbols: $0, 1, \ldots, 7$
  - Base 16 (hexadecimal) $\rightsquigarrow$ 16 symbols: $0, 1, \ldots, 9, A, B, \ldots, F$.

- Write the binary representation of 21
- Write the decimal representation $(326)_8$

Integer representation

Theorem

Given an integer $b > 1$ *as base, every positive integer* n *can be expressed uniquely in the following form:*

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots a_1 b + a_0$$

where $k, a_0, a_1, \ldots, a_k$ *are nonnegative integers,* $0 \leqslant a_0, a_1, \ldots, a_k < b$*, and* $a_k \neq 0$

We call the expression on the right-hand side of the equation in Theorem 12 above **the base-b expansion of n**.

Decimal to non-decimal conversion

Let n be a positive integer in a decimal representation. Conversion to base b can be done using the following algorithm.

Algorithm (Converting n to base b)

Input: n positive integer in a decimal representation, b an integer $(b > 1)$.

$q := n$

$k := 0$

while $q \neq 0$

  $a_k := q \bmod b$

  $q := q \textbf{ div } b$

  $k := k + 1$

return $(a_{k-1} \dots a_1 a_0)_b$ $\rightsquigarrow$ base-b expansion of n.

Example

Convert 54321 to an octal expansion.

Example

Convert 54321 to an octal expansion.

$$54321 = 8 \cdot 6790 + 1$$

Example

Convert 54321 to an octal expansion.

$$54321 = 8 \cdot 6790 + 1$$
$$6790 = 8 \cdot 848 + 6$$

Example

Convert 54321 to an octal expansion.

$$
\begin{aligned}
54321 &= 8 \cdot 6790 + 1 \\
6790 &= 8 \cdot 848 + 6 \\
848 &= 8 \cdot 106 + 0
\end{aligned}
$$

Example

Convert 54321 to an octal expansion.

$$\begin{aligned} 54321 &= 8 \cdot 6790 + 1 \\ 6790 &= 8 \cdot 848 + 6 \\ 848 &= 8 \cdot 106 + 0 \\ 106 &= 8 \cdot 13 + 2 \end{aligned}$$

Example

Convert 54321 to an octal expansion.

$$\begin{aligned} 54321 &= 8 \cdot 6790 + 1 \\ 6790 &= 8 \cdot 848 + 6 \\ 848 &= 8 \cdot 106 + 0 \\ 106 &= 8 \cdot 13 + 2 \\ 13 &= 8 \cdot 1 + 5 \end{aligned}$$

Example

Convert 54321 to an octal expansion.

$$
\begin{aligned}
54321 &= 8 \cdot 6790 + 1 \\
6790 &= 8 \cdot 848 + 6 \\
848 &= 8 \cdot 106 + 0 \\
106 &= 8 \cdot 13 + 2 \\
13 &= 8 \cdot 1 + 5 \\
1 &= 8 \cdot 0 + 1
\end{aligned}
$$

Example

Convert 54321 to an octal expansion.

$$
\begin{aligned}
54321 &= 8 \cdot 6790 + 1 \\
6790 &= 8 \cdot 848 + 6 \\
848 &= 8 \cdot 106 + 0 \\
106 &= 8 \cdot 13 + 2 \\
13 &= 8 \cdot 1 + 5 \\
1 &= 8 \cdot 0 + 1
\end{aligned}
$$

Final result is $(152061)_8$.

Example

Convert 331771 to hexadecimal

Example

Convert 331771 to hexadecimal

$$331771 = 16 \cdot 20735 + 11$$

Example

Convert 331771 to hexadecimal

$$331771 = 16 \cdot 20735 + 11$$
$$20735 = 16 \cdot 1295 + 15$$

Example

Convert 331771 to hexadecimal

$$\begin{aligned} 331771 &= 16 \cdot 20735 + 11 \\ 20735 &= 16 \cdot 1295 + 15 \\ 1295 &= 16 \cdot 80 + 15 \end{aligned}$$

Example

Convert 331771 to hexadecimal

$$\begin{aligned}
331771 &= 16 \cdot 20735 + 11 \\
20735 &= 16 \cdot 1295 + 15 \\
1295 &= 16 \cdot 80 + 15 \\
80 &= 16 \cdot 5 + 0
\end{aligned}$$

Example

Convert 331771 to hexadecimal

$$
\begin{aligned}
331771 &= 16 \cdot 20735 + 11 \\
20735 &= 16 \cdot 1295 + 15 \\
1295 &= 16 \cdot 80 + 15 \\
80 &= 16 \cdot 5 + 0 \\
5 &= 16 \cdot 0 + 5
\end{aligned}
$$

Example

Convert 331771 to hexadecimal

$$\begin{aligned}
331771 &= 16 \cdot 20735 + 11 \\
20735 &= 16 \cdot 1295 + 15 \\
1295 &= 16 \cdot 80 + 15 \\
80 &= 16 \cdot 5 + 0 \\
5 &= 16 \cdot 0 + 5
\end{aligned}$$

The result is $(50\text{FFB})_{16}$. Here, B dan F are the hexadecimal digit for 11 and 15, resp.

Conversion between binary, octal, and hexadecimal expansion

- Converting between two non-decimal expansion b_1 dan b_2
  1. convert base-b_1 expansion to a decimal expansion (Theorem 12);
  2. convert the result into a base-b_2 expansion (Algorithm 1).
- Rapid conversion between binary, octal and hexadecimal:
  - 3 binary digits for 1 octal digit, and 4 binary digits for 1 hexadecimal
  - proceed from right

$$\begin{aligned}(11111010111100)_2 &= \underbrace{011}_{3_8}\underbrace{111}_{7_8}\underbrace{010}_{2_8}\underbrace{111}_{7_8}\underbrace{100}_{4_8} = (37274)_8 \\ &= \underbrace{0011}_{3_{16}}\underbrace{1110}_{E_{16}}\underbrace{1011}_{B_{16}}\underbrace{1100}_{C_{16}} = (3EBC)_{16} \\ (567)_8 &= (101\ 110\ 111)_2 \\ (D8A)_{16} &= (1101\ 1000\ 1010)_2\end{aligned}$$

Modular exponentiation

In cryptography applications, we often need to calculate $b^n \mathbf{mod}\, m$ rapidly without calculating b^n first, for example, $3^{644} \mathbf{mod}\, 645$

Main idea:

- By Theorem 12, n can be written in binary as $(a_{k-1} \ldots a_1 a_0)_2$:
  $n = a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0$
  where $a_0, \ldots, a_{k-1}$ are either 0 atau 1.
- So, $b^n = b^{a_{k-1} 2^{k-1} + \cdots + a_1 \cdot 2 + a_0} = b^{a_{k-1} \cdot 2^{k-1}} \cdots b^{a_1 \cdot 2} b^{a_0}$
- If $a_i = 0$ for some i, then $b^{a_i \cdot 2^i} = b^0 = 1$. So, it suffices to consider $b^{a_i \cdot 2^i}$ for which $a_i \neq 0$ in the above product. For example, for the case of 3^{11}, we note that $11 = (1011)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 8 + 2 + 1$. Hence, we only need to consider $2^3, 2^1, 2^0$.
- We perform exponentiation and multiplication while doing modulo operation every time exponentiation and multiplication is done.

Modular exponentiation algorithm

Algorithm (Calculating $b^n \bmod m$)

Input: b integer, $n = (a_{k-1}a_{k-2}\dots a_1a_0)_2$, m positive integer.
$x := 1$
$p := b \bmod m$
for $i := 0$ to $k-1$
 if $a_i = 1$ then $x := (x \cdot p) \bmod m$
 $p := (p \cdot p) \bmod m$
return x $\rightsquigarrow$ x is equal to $b^n \bmod m$.

Modular exponentiation example

Calculate $3^{644} \mathbf{\ mod\ } 645$.