Chapter 3 (Part 2)
Number Theory and Cryptography

MAD101

Ly Anh Duong

duongla3@fe.edu.vn

Table of Contents

Division

1 The Integers and Division

Definition. Let a and b are integers, then b **is said to be divisible by** a (or b is a multiple of a, or a is a divisor of b, or a divides b), if there exists an integer k such that $b = ka$. We also write $a|b$

Example.

1. $3 \nmid 13$
2. $4 \mid 12$
3. Let n and d be positive integer. How many positive integers not exceeding ($\leq$) n are divisible by d ?

Suppose $d|m \implies m = kd$. We have $0 < kd \leq n \implies k \leq \frac{n}{d}$. Thus, the number of those integers are $\lfloor \frac{n}{d} \rfloor$

An algorithm to find k

1. Let $i = 0$
2. If $(i + 1)d > n$ then $k = i$
3. Othersewise go back to step 2. with i is replaced by $i + 1$

Notes.

- Let $r = n - kd$. Then we have $n = kd + r$. The integers k and r are called the **quotient** (thương) and the **remainder** (số dư) in the division of n by d.
- Thus the above algorithm allows us to find the quotient and the remainder of **the division algorithm** (thuật toán chia).

The Division algorithm

Let a be an integer and d a positive integer. Then there are unique integers q and r such that

$$\boxed{a = dq + r, 0 \leq r < d}$$

- d is called the **divisor** (số chia),
- a the **dividend** (số bị chia),
- q the **quotient** (thương) and r the **remainder** (số dư).

Note. We also write $q = a \text{ div } d$, $r = a \bmod d$.

Example.

1. Find the quotient and the remainder in the division of 101 by 11
2. Find the quotient and the remainder in the division of –11 by 3

Solution

Example. Find the quotient and the remainder in the division of 101 by 11

Solution. We have $101 = 11 \times 9 + 2$

Hence $9 = 101 \text{ div } 11$ and $2 = 101 \bmod 11$

Example. Find the quotient and the remainder in the division of -11 by 3

Solution. We have $-11 = 3 \times (-4) + 1$

Hence $-4 = -11 \text{ div } 3$ and $1 = -11 \bmod 3$

Note. We may write $-11 = 3 \times (-3) - 2$

However -2 is not the remainder r because r always satisfies $0 \le r < d$.

Quizz

1 The Integers and Division

What are -17 div 5 and -17 mod 5?

Select one:

- a. -3 and 2
- b. -4 and 3
- c. -3 and -2
- d. 3 and 2

Quizz

What are -17 div 5 and -17 mod 5?

Select one:

- a. -3 and 2
- b. -4 and 3
- c. -3 and -2
- d. 3 and 2

Ans: b

Quizz

1 The Integers and Division

How many integers in {1, 2, 3, ..., 100} are divisible by 2 but not by 5 ?

Select one:

- a. 39
- b. 51
- c. 49
- d. 40

Quizz

1 The Integers and Division

How many integers in {1, 2, 3, ..., 100} are divisible by 2 but not by 5 ?

Select one:

- a. 39
- b. 51
- c. 49
- d. 40

Ans: d

The Congruences (đồng dư)

$6|(17-5)? \rightarrow 17 \equiv 5 \bmod 6$

Definition. Let m be a positive integer and a and b are integers, then a is congruent to b modulo m if $a-b$ is divisible by m.

- We denote this relation by

$$a \equiv b \pmod{m}$$

- If a is not congruent to b modulo m then we write

$$a \not\equiv b \pmod{m}$$

Example. Are the following congruences true?

- $17 \equiv 5 \pmod 6$
- $24 \equiv 14 \pmod 6$

Solution

Solution. Since $17 - 5 = 12$ is divisible by 6 we see that

$$17 \equiv 5 \pmod 6$$

Since $24 - 14 = 10$ is not divisible by 6 we conclude that

$$24 \not\equiv 14 \pmod 6$$

Theorem. Let a, b be integers and m is a positive integer. Then $a \equiv b \pmod m$ if and only if there is an integer k such that $a = b + k\,m$.

Theorem

1. Let a, b be integers and m is a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.
2. Let a, b be integers and m is a positive integer. Then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.
3. let m is a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Corollary. Let a, b are integers and m is a positive integer. Then

1. $(a + b) \bmod m = (a \bmod m + b \bmod m) \pmod{m}$
2. $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \pmod{m}$

Applications of Congruences: Cryptography (mật mã)

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
10	11	12	13	14	15	16	17	18	19
U	**V**	**W**	**X**	**Y**	**Z**				
20	21	22	23	24	25				

$f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, f(p) = (p + k) \bmod 26$: **bijection**

- **Encryption** (mã hóa) $f(p) = (p + k) \bmod 26$
- **Decryption** (giải mã) $f^{-1}(p) = (p - k) \bmod 26$

Example.

Example.

1. What is the secret message produced from the message “MEET YOU IN THE PARK” using the Caesar cipher (k=3)?
2. Decrypt the ciphertext message “LEWLYPLUJL PZ H NYLHA ALHJOLY” that was encrypted with the shift cipher with shift k = 7.
3. What letter replaces the letter K when the function $f(p) = (7p + 3) mod 26$ is used for encryption?

Solution

"MEET YOU IN THE PARK"

$\rightarrow$ 12 4 4 19-24 14 20-8 13- 19 7 4-15 0 17 10

$f(p) = (p + 3) \bmod 26$, so:

f(12)=15mod26=15

f(4)=7mod26=7

.....

$\rightarrow$ 15 7 7 22-1 17 23- 11 16- 22 10 7- 18 3 20 13, so:

"PHHW BRX LQ WHK SDUN"

Solution

1 The Integers and Division

Solution: First replace the letters in the message with numbers. This produces

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3)$ **mod** 26. This gives

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating this back to letters produces the encrypted message "PHHW BRX LQ WKH SDUN." ◀

Solution: To decrypt the ciphertext "LEWLYPLUJL PZ H NYLHA ALHJOLY" we first translate the letters back to elements of $\mathbf{Z}_{26}$. We obtain

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.

Next, we shift each of these numbers by $-k = -7$ modulo 26 to obtain

4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17.

Finally, we translate these numbers back to letters to obtain the plaintext. We obtain "EXPERIENCE IS A GREAT TEACHER." ◀

Solution: First, note that 10 represents K. Then, using the encryption function specified, it follows that $f(10) = (7 \cdot 10 + 3)$ **mod** $26 = 21$. Because 21 represents V, K is replaced by V in the

Quizz

1 The Integers and Division

Encrypt the message NEED HELP by translating the letters into numbers (the character A is translated to 0), applying the encryption function $f(p) = (p + 3)$ **mod** 26, and then translating the numbers back into letters. Encrypted form:

Select one:

- a. BTTQ TTOA
- b. CHOS QHHG
- c. QHUG KHOS
- d. QHHG KHOS

Quizz

1 The Integers and Division

Encrypt the message NEED HELP by translating the letters into numbers (the character A is translated to 0), applying the encryption function $f(p) = (p + 3)$ **mod** 26, and then translating the numbers back into letters. Encrypted form:

Select one:

- a. BTTQ TTOA
- b. CHOS QHHG
- c. QHUG KHOS
- d. QHHG KHOS

Ans: d

Applications of Congruences: Pseudorandom Numbers (số giả ngẫu nhiên)

$$\boxed{x_{n+1} = (ax_n + c) \bmod m}$$

Notes.

- a: **Multiplier** (nhân tử) $(2 \leq a < m)$
- c: **Increment** (số gia) $(0 \leq < m)$
- x_0: **seed** (hạt giống) $(0 \leq x_0 < m)$
- m: **modulus** (mođun)

Example.(**Random numbers from 0 to 8**) Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus m $= 9$, multiplier a $= 7$, increment c $= 4$, and seed $x_0 = 3$.

$m = 9, a = 7, c = 4, x_0 = 3 \implies x_{n+1} = 7x_n + 4 \implies x_1, x_2, ...$

Solution.

1 The Integers and Division

Solution: We compute the terms of this sequence by successively using the recursively defined function $x_{n+1} = (7x_n + 4) \bmod 9$, beginning by inserting the seed $x_0 = 3$ to find x_1. We find that

$$
\begin{aligned}
x_1 &= 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,\\
x_2 &= 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,\\
x_3 &= 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,\\
x_4 &= 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,\\
x_5 &= 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,\\
x_6 &= 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,\\
x_7 &= 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = \ \ 4 \bmod 9 = 4,\\
x_8 &= 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,\\
x_9 &= 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.
\end{aligned}
$$

Because $x_9 = x_0$ and because each term depends only on the previous term, we see that the sequence

$$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, \ldots$$

is generated. This sequence contains nine different numbers before repeating. ◀

Example.

11. Suppose ***pseudo-random numbers*** are produced by using:
    $x_{n+1} = (3x_n + 5) \bmod 7$.
    If $x_3 = 5$, find x_2 and x_4.
12. Suppose ***pseudo-random numbers*** are produced by using:
    $x_{n+1} = (3x_n + 7) \bmod 13$ and the seed $x_1 = 1$.
    Find x_3 and x_4.

Applications of Congruences: Hashing Function

$$\boxed{H(k) = k \bmod m}$$

Using in searching data in memory

- k: data searched,
- m: memory block.

Example. Find the memory locations assigned by the hashing function $h(k) = k \bmod 111$ to the records of customers with Social Security numbers 064212848 and 037149212.

$h(064212848) = 064212848 \bmod 111 = 14 \rightarrow$memory location 14.

$h(037149212) = 037149212 \bmod 111 = 65 \rightarrow$ memory location 65.

Table of Contents

2 Integers and Algorithms

Representations of Integers

2 Integers and Algorithms

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0. \text{ Denote } (a_k a_{k-1} ... a_1 a_0)_b$$

Notes.

- n: positive integer.
- $b > 1$: integer.
- $a_0, a_1, ..., a_k < b, a_k \neq 0$: nonnegative integer.

This is **the base b expansion** of the integer n.

Examples.

1. $(241)_{10} = ? \rightarrow (241)_{10} = 2.10^2 + 4.10^1 + 1.10^0 = 241$
2. $(7016)_8 = ? \rightarrow (7016)_8 = 7.8^3 + 0.8^2 + 1.8^1 + 6.8^0 = 3598 = (3598)_{10}$
3. Suppose that the **letters A through F represent the digits corresponding to the numbers 10 through 15** (in decimal notation). Find $(2AE0B)_{16} \rightarrow = 175627$

Common Bases Expansions

- **Decimal Expansions** $(b = 10)$ (thập phân)
- **Binary Expansions** $(b = 2)$ (nhị phân)
- **Octal Expansions** $(b = 8)$ (bát phân)
- **Hexadecimal Expansions** $(b = 16)$ (thập lục phân)

Examples.

a. Find 2 expansion of $(241)_{10}$
b. Find 8 expansion of $(12345)_{10}$
c. Find 16 expansion of $(177130)_{10}$

Sol a.

$$241 = 120.2 + 1$$
$$= 60.2^2 + 1$$
$$= 30.2^3 + 1$$
$$= 15.2^4 + 1$$
$$= (7.2 + 1).2^4 + 1 = 7.2^5 + 2^4 + 1$$
$$= (3.2 + 1).2^5 + 2^4 + 1 = 3.2^6 + 2^5 + 2^4 + 1$$
$$(1.2 + 1).2^6 + 2^5 + 2^4 + 1 = 2^7 + 2^6 + 2^5 + 2^4 + 1$$

Thus, $(241)_{10} = 241 = (11110001)_2$

$$241 = 2.120 + 1$$
$$120 = 2.60 + 0$$
$$60 = 2.30 + 0$$
$$30 = 2.15 + 0$$
$$15 = 2.7 + 1$$
$$7 = 2.3 + 1$$
$$3 = 2.1 + 1$$
$$1 = 2.0 + 1$$

Thus, $(241)_{10} = 241 = (11110001)_2$

Solution.

2 Integers and Algorithms

$$12345 = 8 \cdot 1543 + 1.$$

---

y and Cryptography

Successively dividing quotients by 8 gives

$$\begin{aligned} 1543 &= 8 \cdot 192 + 7, \\ 192 &= 8 \cdot 24 + 0, \\ 24 &= 8 \cdot 3 + 0, \\ 3 &= 8 \cdot 0 + 3. \end{aligned}$$

The successive remainders that we have found, 1, 7, 0, 0, and 3, are the digits from the right to the left of 12345 in base 8. Hence,

$$(12345)_{10} = (30071)_8.$$

Solution.

2 Integers and Algorithms

Solution: First divide 177130 by 16 to obtain

$$177130 = 16 \cdot 11070 + 10.$$

Successively dividing quotients by 16 gives

$$\begin{aligned} 11070 &= 16 \cdot 691 + 14, \\ 691 &= 16 \cdot 43 + 3, \\ 43 &= 16 \cdot 2 + 11, \\ 2 &= 16 \cdot 0 + 2. \end{aligned}$$

The successive remainders that we have found, 10, 14, 3, 11, 2, give us the digits from the right to the left of 177130 in the hexadecimal (base 16) expansion of $(177130)_{10}$. It follows that

$$(177130)_{10} = (2B3EA)_{16}.$$

(Recall that the integers 10, 11, and 14 correspond to the hexadecimal digits A, B, and E, respectively.) ◀

Constructing Base b Expansions

procedure *base b expansion*(n, b: positive integers with $b > 1$)
$q := n$
$k := 0$
while $q \neq 0$
    $a_k := q$ **mod** b
    $q := q$ **div** b
    $k := k + 1$
return $(a_{k-1}, \ldots, a_1, a_0)$ {$(a_{k-1} \ldots a_1 a_0)_b$ is the base b expansion of n}

Example. Find base 2 expansion of 241.

Solution.

2 Integers and Algorithms

$q = 241 \neq 0$

k=0: $a_0 = 241 \bmod 2 = 1, q = 241 \text{ div } 2 = 120 \neq 0$

k=1:$a_1 = 0, q = 60$

k=2:$a_2 = 0, q = 30$

k=3:$a_3 = 0, q = 15$

k=4:$a_4 = 1, q = 7$

k=5:$a_5 = 1, q = 3$

k=6:$a_6 = 1, 1 = 1$

k=7:$a_7 = 1, q = 0$

$\rightarrow 11110001$,so $241 = (11110001)_2$

Quizz

2 Integers and Algorithms

Find the ***base 7 expansion*** of 186

a. 354

b. 331

c. 413

d. 271

e. None of these

Find the ***base 7 expansion*** of 186

a. 354
b. 331
c. 413
d. 271
e. None of these

Ans: a

Quizz

2 Integers and Algorithms

Find the ***binary format*** of $(1011)_3$.

a. 11110

b. 11111

c. 100000

d. 10101

e. None of these

Quizz

2 Integers and Algorithms

Find the ***binary format*** of $(1011)_3$.

a. 11110

b. 11111

c. 100000

d. 10101

e. None of these

Ans:b

Binary Operations: Addition

2 Integers and Algorithms

Rules.

$$\boxed{0+0=0, 1+0=1, 1+1=0\,(\text{remind } 1)}$$

Add $a=(1110)_2$ and $b=(1011)_2$

$$\begin{array}{r} \mathbf{1\ 1\ 1\ 0} \\ 1\ 1\ 1\ 0\ (a) \\ +\ 1\ 0\ 1\ 1\ (b) \\ \hline 1\ 1\ 0\ 0\ 1\ (s) \end{array}$$

$1 = 0.2 + 1$ $\qquad$ $3 = 1.2 + 1$

$2 = 1.2 + 0$ $\qquad$ $1 = 0.2 + 1$

$2 = 1.2 + 0$

Thus, $(1110)_2 + (1011)_2 = (11001)_2$

Binary Operations: Difference

Rules.

- $0 - 0 = 0$
- $1 - 0 = 1$
- $1 - 1 = 0$
- $0 - 1 = 1(\text{remind} - 1)$
- $-1 - 1 = 0(\text{remind} - 1)$

Let $a = (1110)_2$ and $b = (1011)_2$. Find $a - b$

$(1110)_2 - (1011)_2 = (11)_2$

Binary Operations: Multiplication

2 Integers and Algorithms

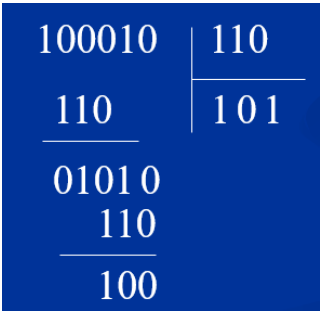
Find the product of $a = (110)_2$ and $b = (101)_2$

$$
\begin{array}{r}
1\ 1\ 0 \\
\times\ 1\ 0\ 1 \\
\hline
1\ 1\ 0 \\
0\ 0\ 0 \\
1\ 1\ 0 \\
\hline
1\ 1\ 1\ 1\ 0
\end{array}
$$

Thus, $(110)_2.(101)_2 = (11110)_2$

Binary Operations: Division

Find quotient and remainder (if exists) in the division of $(100010)_2$ by $(110)_2$



Thus, the quotient $q = 101$ and remainder $r = 100$

Addition Algorithm

procedure *add*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}a_{n-2}\dots a_1a_0)_2$
and $(b_{n-1}b_{n-2}\dots b_1b_0)_2$, respectively}
$c := 0$
for $j := 0$ **to** $n-1$
$d := \lfloor (a_j + b_j + c)/2 \rfloor$
$s_j := a_j + b_j + c - 2d$
$c := d$
$s_n := c$
return $(s_0, s_1, \dots, s_n)$ {the binary expansion of the sum is $(s_n s_{n-1} \dots s_0)_2$}

Example. Find $(1110)_2 + (1011)_2$

Solution

2 Integers and Algorithms

$c = 0$

$j = 0 : d = \lfloor \frac{0+1+0}{2} \rfloor = \lfloor 0.5 \rfloor = 0$

$s_0 = 1, c = 0$

$j = 1 : d = \lfloor \frac{1+1+0}{2} \rfloor = \lfloor 1 \rfloor = 1$

$s_1 = 0, c = 1$

$j = 2 : d = 1$

$s_2 = 0, c = 1$

$j = 3 : d = 1$

$s_3 = 1, c = 1$

$s_4 = 1$

$\rightarrow 10011$, so the sum is $(11001)_2$

Multiplication Algorithm

procedure *multiply*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}a_{n-2}\dots a_1a_0)_2$
and $(b_{n-1}b_{n-2}\dots b_1b_0)_2$, respectively}
for $j := 0$ **to** $n-1$
if $b_j = 1$ **then** $c_j := a$ shifted j places
else $c_j := 0$
{$c_0, c_1, \dots, c_{n-1}$ are the partial products}
$p := 0$
for $j := 0$ **to** $n-1$
$p := add(p, c_j)$
return p {p is the value of ab}

Example. Find the product of $(110)_2$ and $(101)_2$

Solution.

2 Integers and Algorithms

$j = 0 : b_0 = 1 \to c_0 = 110$

$j = 1 : b_1 = 0 \to c_1 = 0000$

$j = 2 : b_2 = 1 \to c_2 = 11000$

$p = 0$

$j = 0 : p = 0 + 110 = 110$

$j = 1 : p = 110 + 0000 = 0110$

$j = 2 : p = 0110 + 11000 = 11110$

$\to p = 11110$. Hence, the product $(11110)_2$

Division Algorithm

procedure *division algorithm*(a: integer, d: positive integer)
$q := 0$
$r := |a|$
while $r \geq d$
    $r := r - d$
    $q := q + 1$
if $a < 0$ and $r > 0$ **then**
    $r := d - r$
    $q := -(q + 1)$
return (q, r) {$q = a$ **div** d is the quotient, $r = a$ **mod** d is the remainder}

Example. Find the quotient and the remainder in the division of 101 by 11

Solution.

2 Integers and Algorithms

$q = 0, r = |101| = 101$

$r = 101 \geq 11 = d \rightarrow r = 101 - 11 = 90, q = 0 + 1 = 1$

$r = 90 \geq 11 = d \rightarrow r = 79, q = 2$

$r = 79 \geq 11 = d \rightarrow r = 61, q = 3$

$r = 61 \geq 11 = d \rightarrow r = 57, q = 4$

$r = 57 \geq 11 = d \rightarrow r = 46, q = 5$

$r = 46 \geq 11 = d \rightarrow r = 35, q = 6$

$r = 35 \geq 11 = d \rightarrow r = 24, q = 7$

$r = 24 \geq 11 = d \rightarrow r = 13, q = 8$

$r = 13 \geq 11 = d \rightarrow r = 2, q = 9$

$r = 2 \geq 11 = d(!)$

Hence, $(q = 9, r = 2)$

Modular Exponentiation

procedure *modular exponentiation*(b: integer, $n = (a_{k-1}a_{k-2}\dots a_1a_0)_2$,
m: positive integers)
$x := 1$
$power := b$ **mod** m
for $i := 0$ **to** $k - 1$
  if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
  $power := (power \cdot power)$ **mod** m
return $x\{x$ equals b^n **mod** $m\}$

Example. Find 3^{644} mod 645

Solution.

We have $b = 3, m = 645, 644 = (1010000100)_2$

$x = 1$

$power = 3 \bmod 645 = 3$

$i = 0 : a_0 = 0 \rightarrow x = 1, power = 3^2 \bmod 645 = 9$

$i = 1 : a_1 = 0 \rightarrow x = 1, power = 9^2 \bmod 645 = 81$

$i = 2 : a_2 = 1 \rightarrow x = 1.81 \bmod 645 = 81, power = 81^2 \bmod 645 = 111$

$i = 3 : a_3 = 0 \rightarrow x = 81, power = 111^2 \bmod 645 = 66$

$i = 4 : a_4 = 0 \rightarrow x = 81, power = 66^2 \bmod 645 = 486$

$i = 5 : a_5 = 0 \rightarrow x = 81, power = 486^2 \bmod 645 = 126$

$i = 6 : a_6 = 0 \rightarrow x = 81, power = 126^2 \bmod 645 = 396$

Solution.

$i = 7 : a_7 = 1 \rightarrow x = (81.396) \bmod 645 = 471, power = 396^2 \bmod 645 = 81$

$i = 8 : a_8 = 0 \rightarrow x = 471, power = 81^2 \bmod 645 = 111$

$i = 9 : a_9 = 1 \rightarrow x = (471.111) \bmod 645 = 36, power = 111^2 \bmod 645 = 66$

$\rightarrow x = 36$. Hence, $3^{644} \bmod 645 = 36$

Table of Contents

Definition.

- A positive integer p greater than 1 is called **prime** (số nguyên tố) if the only positive factors (ước số) are 1 and p.
- A positive integer that is greater than 1 and is not prime is called **composite** (hợp số).

Example.

3 Primes and Greatest Common Divisors

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

The fundamental theorem of arithmetic (ĐL cơ bản của số học)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Examples. Find the prime factorizations of 100, 999, and 1024.

Solution.

$100 = 2^2.5^2$

$999 = 3^3.37$

$1024 = 2^{10}$

Theorem

If n is a composite integer, then n has a prime divisor (ước nguyên tố) less than or equal to $\sqrt{n}$.

Examples.

1. Show that 101 is prime.
2. Find the prime factorization of 7007.

Solutions.

3 Primes and Greatest Common Divisors

Solution: The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime. ◀

Solution: To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with $7007/7 = 1001$. Next, divide 1001 by successive primes, beginning with 7. It is immediately seen that 7 also divides 1001, because $1001/7 = 143$. Continue by dividing 143 by successive primes, beginning with 7. Although 7 does not divide 143, 11 does divide 143, and $143/11 = 13$. Because 13 is prime, the procedure is completed. It follows that $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$. Consequently, the prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$. ◀

Theorem

3 Primes and Greatest Common Divisors

1. There are infinite many primes.
2. **(The prime number theorem)**The ratio of $\pi(x)$, the number of primes not exceeding x and x/lnx approaches 1 and grows with bound (lnx: natural logarithm of x).

TABLE 2 Approximating $\pi(x)$ by $x/\ln x$.

x	$\pi(x)$	$x/\ln x$	$\pi(x)/(x/\ln x)$
10^3	168	144.8	1.161
10^4	1229	1085.7	1.132
10^5	9592	8685.9	1.104
10^6	78,498	72,382.4	1.084
10^7	664,579	620,420.7	1.071
10^8	5,761,455	5,428,681.0	1.061
10^9	50,847,534	48,254,942.4	1.054
10^{10}	455,052,512	434,294,481.9	1.048

Greatest Common Divisors

3 Primes and Greatest Common Divisors

Definition. Let a, b be integers, not both zero. The largest integer d such that d|a and d|b is called **the greatest common divisor** (ước chung lớn nhất) of a and b.

Notation. $gcd(a, b)$

To find $gcd(a, b)$**:**

$$a = p_1^{a_1}.p_2^{a_2}...p_k^{a_k} \quad (p_1 < p_2 < ... < p_k)$$

$$b = p_1^{b_1}.p_2^{b_2}...p_k^{b_k}$$

$$\gcd(a,b) = p_1^{\min(a_1,b_1)}.p_2^{\min(a_2,b_2)}...p_k^{\min(a_k,b_k)}$$

Examples.

1. $gcd(24, 36) \rightarrow gcd(24, 36) = 12$
2. $gcd(17, 22) \rightarrow gcd(17, 22) = 1$

Definition.

- The integers a, b are **relatively prime** (nguyên tố cùng nhau) if their greatest common divisor is 1
- The integers $a_1, a_2, a_3, \ldots, a_n$ are **pairwise relatively prime** (đôi 1 nguyên tố cùng nhau) if $gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$

Examples. Show that

7, 10, 11, 17, 23 are pairwise relatively prime.

17, 22 are relative prime.

The Least common multiple

Definition. The Least common multiple (bội chung nhỏ nhất) of the positive integer a and b is the smallest integer that is divisible by both a and b.

Notation. $lcm(a, b)$

To find $lcm(a, b)$**:**

$$a = p_1^{a_1}.p_2^{a_2}...p_k^{a_k} \quad (p_1 < p_2 < ... < p_k)$$

$$b = p_1^{b_1}.p_2^{b_2}...p_k^{b_k}$$

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)}.p_2^{\max(a_2,b_2)}...p_k^{\max(a_k,b_k)}$$

Examples.

1. $lcm(12, 36) \rightarrow lcm(12, 36) = 36$
2. $lcm(7, 17) \rightarrow lcm(7, 17) = 119$

Theorem

3 Primes and Greatest Common Divisors

Let a, b be positive integers then $ab = gcd(a, b).lcm(a, b)$
Example. gcd(8, 12) = 4, lcm(8,12)=24 $\rightarrow$ 8.12 = 4.24

The Euclidean Algorithm

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\text{gcd}(a, b) \text{ is } x\}$

Example. Find $gcd(24, 36)$

Solution.

$x = 24$

$y = 36$

$y = 36 \neq 0 : r = 24 \bmod 36 = 24, x = 36, y = 24$

$y = 24 \neq 0 : r = 36 \bmod 24 = 12, x = 24, y = 12$

$y = 12 \neq 0 : r = 24 \bmod 12 = 0, x = 12, y = 0$

$y = 0 \neq 0$(!)

$\rightarrow$ return 12. Hence, $gcd(24, 36) = 12$

Euler φ-function

3 Primes and Greatest Common Divisors

$$\varphi : \mathbb{N}^* \to \mathbb{N}^*$$
$$n \mapsto \varphi(n)$$

$\varphi(n)$ = the number of positive integers less than or equal to n that are **relatively prime** to n.

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$$

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right).....\left(1-\frac{1}{p_k}\right)$$

if p is the prime, then $\varphi(p) = p\left(1-\frac{1}{p}\right) = p-1$

Example. $\varphi(6) = 2$ because of the positive integers less or equal to 6, only 1 and 5 are relatively prime to 6.

Example. Find $\varphi(10)$ and $\varphi(100)$

Quiz

Which pair of integers are ***relatively prime***?

a. (17, 51)

b. (5, 24)

c. (11, 121)

d. (37, 111)

e. None of the others

Quiz

Which pair of integers are ***relatively prime***?

a. (17, 51)
b. (5, 24)
c. (11, 121)
d. (37, 111)
e. None of the others

Ans: b

Quiz

3 Primes and Greatest Common Divisors

If a, b are positive integers such that gcd(a, b) = 5 and ab = 120, find lcm(a, b).

a. 24
b. 600
c. 120
d. 5
e. None of the others

If a, b are positive integers such that gcd(a, b) = 5 and ab = 120, find lcm(a, b).

a. 24
b. 600
c. 120
d. 5
e. None of the others

Ans: a

Table of Contents

4 Problems

The Integers and Division

4 Problems

1. Does 17 divide each of these numbers?

a) 68 b) 84 c) 357 d) 1001

2. What are the quotient and remainder when

a) 19 is divided by 7? b) -111 is divided by 11? c) 789 is divided by 23?

d) 1001 is divided by 13? e) 0 is divided by 19? f) 3 is divided by 5?

3. Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

a) $c \equiv 9a \pmod{13}$. b) $c \equiv 11b \pmod{13}$. c) $c \equiv a + b \pmod{13}$.

d) $c \equiv 2a + 3b \pmod{13}$. e) $c \equiv a^2 + b^2 \pmod{13}$. f) $c \equiv a^3 - b^3 \pmod{13}$.

The Integers and Division

4 Problems

4. Evaluate these quantities.

a) 13 mod 3 b) −97 mod 11 c) 155 mod 19 d) −221 mod 23

5. Find a **div** m and a **mod** m when

a) a = −111, m = 99. b) a = −9999, m = 101.

c) a = 10299, m = 999. d) a = 123456, m = 1001.

6. Decide whether each of these integers is congruent to 5 modulo 17.

a) 80 b) 103 c) −29 d) −122

The Integers and Division

4 Problems

7. Find each of these values.

a) $(992 \bmod 32)^3 \bmod 15$ b) $(34 \bmod 17)^2 \bmod 11$

c) $(193 \bmod 23)^2 \bmod 31$ d) $(893 \bmod 79)^4 \bmod 26$

8. Convert the decimal expansion of each of these integers to a binary expansion.

a) 23 b) 45 c) 241 d) 1025

9. Convert the binary expansion of each of these integers to a decimal expansion.

a) $(1\ 1011)_2$ b) $(10\ 1011\ 0101)_2$

c) $(11\ 1011\ 1110)_2$ d) $(111\ 1100\ 0001\ 1111)_2$

The Integers and Division

4 Problems

10. Convert the octal expansion of each of these integers to a binary expansion.

a) $(572)_8$ b) $(1604)_8$ c) $(423)_8$ d) $(2417)_8$

11. Convert each of the following expansions to **decimal expansion**.

a) $(1021)_3$ b) $(325)_7$ c) $(A3)_{12}$ d) $(401)_5$ e) $(12B7)_{13}$

12. Convert 69 to

a) a binary expansion b) a base 6 expansion c) a base 9 expansion

11. Suppose a $a \bmod 3 = 2$ and $b \bmod 6 = 4$, find $ab \bmod 3$.

Primes and Greatest Common Divisors

4 Problems

1. Determine whether each of these integers is prime.

a) 21 b) 29 c) 71 d) 97

e) 111 f) 143 g) 93 h) 101

2. Find the prime factorization of each of these integers.

a) 39 b) 81 c) 101

d) 143 e) 289 f) 899

3. Find the prime factorization of 10!

Primes and Greatest Common Divisors

4 Problems

4. Which positive integers less than 12 are relatively prime to 12?

5. Which positive integers less than 30 are relatively prime to 30?

6. Find these values of the Euler φ-function.

a) $\varphi(4)$ b) $\varphi(10)$ c) $\varphi(13)$

7. What are the greatest common divisors of these pairs of integers?

a) $37 \cdot 53 \cdot 73, 211 \cdot 35 \cdot 59$ b) $11 \cdot 13 \cdot 17, 29 \cdot 37 \cdot 55 \cdot 73$ c) $2331, 2317$

d) $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$ e) $313 \cdot 517, 212 \cdot 721$

Integers and Algorithms

4 Problems

1. Suppose ***pseudo-random numbers*** are produced by using: $x_{n+1} = (3x_n + 11) \bmod 13$. If $x_3 = 5$, find x_2 and x_4.

2. Suppose pseudo-random numbers are produced by using: $x_{n+1} = (2x_n + 7) \bmod 9$.

a) If $x_0 = 1$, find x_2 and x_3 b) If $x_3 = 3$, find x_2 and x_4.

3. Using the function $f(x) = (x + 10) \bmod 26$ to encrypt messages. Answer each of these questions.

a) Encrypt the message STOP b) Decrypt the message LEI

Integers and Algorithms

4 Problems

4. Which memory locations are assigned by the **hashing function** h(k) = k mod 101 to the records of insurance company customers with these Social Security Numbers?

a) 104578690 b) 432222187

5. Use the **Euclidean algorithm** to find

a) gcd(14, 28) b) gcd(8, 28) c) gcd(100, 101) d) gcd(28,35)

e) lcm(7, 28) f) lcm(12, 28) g) lcm(100, 101) h) lcm(28,35)

Q&A

Thank you for listening!