Chapter 4
Number Theory

Topics

- Divisibility and Modular Arithmetic
- Integer Representations and Algorithms
- Prime and Greatest Common Divisors
- Applications of Congruences
- Cryptography

DIVISIBILITY AND MODULAR ARITHMETIC

Integers

- **Number theory** is a branch of mathematics that explores integers and their properties.
- **Integers:**
  - **Z integers {…, -2,-1, 0, 1, 2, …}**
  - **Z+ positive integers {1, 2, …}**
- Number theory has many applications within computer science, including:
  - Indexing - Storage and organization of data
  - Encryption
  - Error correcting codes
  - Random numbers generators

Division

Definition: Assume 2 integers a and b, such that a ≠ 0 (a is not equal 0). We say that **a divides b** if there is an integer c such that b = ac. If a divides b we say that **a is a *factor* of b** and that **b is *multiple* of a**.

- The fact that a divides b is denoted as **a | b (b ⋮ a)**.

Examples.

- 4 | 24 True or False? True
  - 4 is a factor of 24
  - 24 is a multiple of 4
- 3 | 7 True or False? False

Divisibility

All integers divisible by d > 0 can be enumerated as:

$$\ldots, -kd, \ldots, -2d, -d, 0, d, 2d, \ldots, kd, \ldots$$

- **Question:**

Let n and d be two positive integers. How many positive integers not exceeding n are *divisible by* d?

- $0 < kd \leq n$

- **Answer:**

Count the number of integers kd that are less than n. What is the number of integers k such that $0 < kd \leq n$?

$0 < kd \leq n \rightarrow 0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

Divisibility

Properties: Let a, b, c be integers. Then the following hold:

1. if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$
2. if $a \mid b$ then $a \mid bc$ for all integers c
3. if $a \mid b$ and $b \mid c$ then $a \mid c$

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

If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ whenever m and n are integers.

The division algorithm

Definition: Let a be an integer and d a positive integer. Then there are unique integers, q and r, with $0 \le r < d$, such that

$$a = dq + r.$$

- a is called the **dividend**,
- d is called the **divisor**,
- q is called the **quotient** and
- r the **remainder** of the division.

Relations: q = a div d , r = a mod d

Example. a = 14, d = 3
$14 = 3 * 4 + 2$
$14/3 = 4.6666$
14 div 3 = 4
14 mod 3 = 2

Remark. when a is an integer and d is a positive integer, we have a div d $= \lfloor a/d \rfloor$ and a mod d = a − d.

Modular Arithmetic

Problem. What time it will be (on a 24-hour clock) 50 hours from now?

We care only about the remainder when 50 plus the current hour is divided by 24. Because we are often interested only in remainders, we have special notations for them. We have already introduced the notation a mod m to represent the remainder when an integer a is divided by the positive integer m.

Modular Arithmetic

Definition: Let $a, b \in \boldsymbol{Z}$, $m \in \boldsymbol{Z}^+$.

a is **congruent** to b modulo m if $m \mid (a - b)$.

Notation:

$a \equiv b \pmod{m}$: a is congruent to b modulo m. We say that is a **congruence** and that m is its **modulus** (plural **moduli**).

$a \not\equiv b \pmod{m}$: a and b are **not congruent modulo m**.

Examples.

15 is congruent to 6 modulo 3 since $3 \mid (15 - 6)$

15 is not congruent to 7 modulo 3 since $3 \nmid (15 - 7)$

Modular Arithmetic

Theorem 1.

a, b: integers, m: positive integer

a ≡ b (mod m) ↔ a mod m = b mod m

Theorem 2.

a, b: integers, m: positive integer

a and b are congruent modulo m if and only if there is an integer k such that a = b + km

$$a \equiv b \pmod{m} \Leftrightarrow a = km + b \ (k \in \mathbb{Z})$$

Modular Arithmetic

Theorem 3.

m: positive integer

$(a \equiv b \pmod{m}) \wedge (c \equiv d \pmod{m}) \rightarrow (a + c \equiv b + d \pmod{m}) \wedge (ac \equiv bd \pmod{m})$

Corollary.

a, b: integers, m: positive integer

$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

and **$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$**

Modular Arithmetic

$$a_i \equiv b_i \pmod{m} \quad (i = 1, 2, \ldots., k)$$

$$\Rightarrow \sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod{m}$$

$$\Rightarrow \prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{m}$$

$$if \begin{cases} a_1 = a_2 = \ldots. = a_k = a \\ b_1 = b_2 = \ldots. = b_k = b \end{cases} then \begin{cases} a^k \equiv b^k \pmod{m} \\ ka \equiv kb \pmod{m} \end{cases}$$

Exercises

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?

g) -1 is divided by 3?

h) 4 is divided by 1?

Exercises

3. Find a div m and a mod m when

a) $a = 228$, $m = 119$.

b) $a = 9009$, $m = 223$.

c) $a = -10101$, $m = 333$.

d) $a = -765432$, $m = 38271$.

4. Evaluate these quantities.

a) $-17 \bmod 2$

b) $144 \bmod 7$

c) $-101 \bmod 13$

d) $199 \bmod 19$

5. Find the integer a such that

a) $a \equiv 43 \pmod{23}$ and $-22 \le a \le 0$.

b) $a \equiv 17 \pmod{29}$ and $-14 \le a \le 14$.

c) $a \equiv -11 \pmod{21}$ and $90 \le a \le 110$

Exercises

6. Decide whether each of these integers is congruent to 3 modulo 7.

a) 37 b) 66 c) −17 d) −67

7. Find each of these values.

a) (177 mod 31 + 270 mod 31) mod 31

b) (177 mod 31 · 270 mod 31) mod 31

8. Find each of these values.

a) $(19^2 \bmod 41) \bmod 9$

b) $(32^3 \bmod 13)^2 \bmod 11$

c) $(7^3 \bmod 23)^2 \bmod 31$

d) $(21^2 \bmod 15)^3 \bmod 22$

Exercises

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

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

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

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

d) $c \equiv 2a + 3b \pmod{13}$

10. What are – 17 div 5 and – 17 mod 5?

Select the correct answer.

A. – 3 and 2

B. – 4 and 3

C. – 3 and – 2

D. 3 and 2

Exercises

11. How many integers in {1, 2, 3, …, 100} are divisible by 2 but not by 5? Select the correct answer.

A. 39 C. 49

B. 51 D. 40

12. Find 2^{28} mod 19

A. 18 B. 15 C. 17 D. 16 E. None of the other choices is correct

13. Let a = 137 mod 31 and b = - 137 mod 31. Find b – a

A. 5 B. -7 C. 23 D. -13 E. 17

INTEGER REPRESENTATIONS AND ALGORITHMS

Representations of Integers

Theorem: Let b be a positive integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

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

Where k is a nonnegative integer, $a_0, a_1, a_2, \ldots, a_k$ are nonnegative integers less than b and $a_k \neq 0$.

Remark. The representation of n given in Theorem is called the **base b expansion of n**.

Notation. $(a_k a_{k-1} \ldots a_1 a_0)_b$

Example. $(12)_{10}$ represents $1 \cdot 10^1 + 2 \cdot 10^0 = 12$

Decimal expansions

In the modern world, we use **decimal**, or **base 10** notation to represent integers.

Example. $965 = 9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$

The bases $b = 2$ (binary), $b = 8$ (octal) and $b = 16$ (hexadecimal) are important for computing and communications.

Binary Expansions

Choosing **2** as the **base** gives **binary expansions of integers**.

In binary notation each digit is either a 0 or a 1. In other words, the binary expansion of an integer is just a bit string.

Example. What is the decimal expansion of the integer that has $(1\ 0101\ 1111)_2$ as its binary expansion?

$$(1\ 0101\ 1111)_2 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 351$$

Octal expansions

Base 8 expansions are called **octal expansions**.

The base 8 uses the digits {**0, 1, 2, 3, 4, 5, 6, 7**}.

Example. What is the decimal expansion of the number with octal expansion $(7016)_8$?

Solution.

$$(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$$

Hexadecimal Expansions

The **hexadecimal expansion/base 16** needs 16 digits, but our decimal system provides only 10. So letters are used for the additional symbols. The hexadecimal system uses the digits {**0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F**}. The letters A through F represent the decimal numbers 10 through 15.

Example. What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

Solution.

$$\begin{aligned}(2AE0B)_{16} &= 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 \\ &= 175627\end{aligned}$$

Base conversion

- **An algorithm for constructing the base b expansion of an integer n**

1. divide n by b to obtain a quotient and remainder

$$n = bq_0 + a_0,\ 0 \le a_0 \le b$$

The remainder, a_0, is the rightmost digit in the base b expansion of n.

2. divide q_0 by b

$$q_0 = bq_1 + a_1,\ 0 \le a_1 \le b$$

a_1 is the second digit from the right in the base b expansion of n.

3. …

This process terminates when we obtain a quotient equal to zero. It produces the base b digits of n from the right to the left.

Base conversion

Example. Find the octal expansion of $(12345)_{10}$.

Solution.

$12345 = 8 \cdot 1543 + 1$

$1543 = 8 \cdot 192 + 7$

$192 = 8 \cdot 24 + 0$

$24 = 8 \cdot 3 + 0$

$3 = 8 \cdot 0 + 3$

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,

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

Base conversion

Example.

a) Find the hexadecimal expansion of $(177130)_{10}$.

b) Find the binary expansion of $(241)_{10}$.

Base conversion

ALGORITHM 1. 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$\}$

Note.

- q represents the quotient obtained by successive divisions by b, starting with q = n.
- The digits in the base b expansion are the remainders of the division given by q mod b.
- The algorithm terminates when q = 0 is reached.

Base conversion

Example.

Find the octal and hexadecimal expansions of $(11\ 1110\ 1011\ 1100)_2$ and the binary expansions of $(765)_8$ and $(A8D)_{16}$.

Solution: To convert $(11\ 1110\ 1011\ 1100)_2$ into octal notation we group the binary digits into blocks of three, adding initial zeros at the start of the leftmost block if necessary. These blocks, from left to right, are 011, 111, 010, 111, and 100, corresponding to 3, 7, 2, 7, and 4, respectively. Consequently, $(11\ 1110\ 1011\ 1100)_2 = (37274)_8$. To convert $(11\ 1110\ 1011\ 1100)_2$ into hexadecimal notation we group the binary digits into blocks of four, adding initial zeros at the start of the leftmost block if necessary. These blocks, from left to right, are 0011, 1110, 1011, and 1100, corresponding to the hexadecimal digits 3, E, B, and C, respectively. Consequently, $(11\ 1110\ 1011\ 1100)_2 = (3EBC)_{16}$.

To convert $(765)_8$ into binary notation, we replace each octal digit by a block of three binary digits. These blocks are 111, 110, and 101. Hence, $(765)_8 = (1\ 1111\ 0101)_2$. To convert $(A8D)_{16}$ into binary notation, we replace each hexadecimal digit by a block of four binary digits. These blocks are 1010, 1000, and 1101. Hence, $(A8D)_{16} = (1010\ 1000\ 1101)_2$. ◀

Comparision of decimal, octal, binary and hexadecimal representations

TABLE 1 **Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.**

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

- Each octal digit corresponds to a block of 3 binary digits.
- Each hexadecimal digit corresponds to a block of 4 binary digits.
- So, conversion between binary, octal, and hexadecimal is easy.

Algorithms for Integer Operations

- Addition/Subtraction of Integers
- Multiplication of Integers
- Computing div and mod
- Fast Modular Exponentiation

Binary addition of integers

- Algorithms for performing operations with integers using their binary expansions are important as computer chips work with binary numbers. Each digit is called a bit.
- **Rules**

A	B	A + B	Carry
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Binary addition of integers

Example.

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

$$
\begin{array}{lr}
 & 1\ 1\ 1\ 0 \\
 & 1\ 1\ 1\ 0\ (a) \\
+ & \underline{1\ 0\ 1\ 1}\ (b) \\
 & 1\ 1\ 0\ 0\ 1\ (s)
\end{array}
$$

A	B	A + B	Carry
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Binary addition of integers

ALGORITHM 2 Addition of Integers.

procedure *add*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}a_{n-2}\ldots a_1a_0)_2$
 and $(b_{n-1}b_{n-2}\ldots b_1b_0)_2$, 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 $(s_0, s_1, \ldots, s_n)$ {the binary expansion of the sum is $(s_ns_{n-1}\ldots s_0)_2$}

- The number of additions of bits used by Algorithm 2 to add two n-bit integers is O(n).

Binary addition of integers

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

$c = 0$

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

$s_0 = 1, c = 0$

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

$s_1 = 0, c = 1$

$j = 2 : d = 1$

$s_2 = 0, c = 1$

$j = 3 : d = 1$

$s_3 = 1, c = 1$

$s_4 = 1$

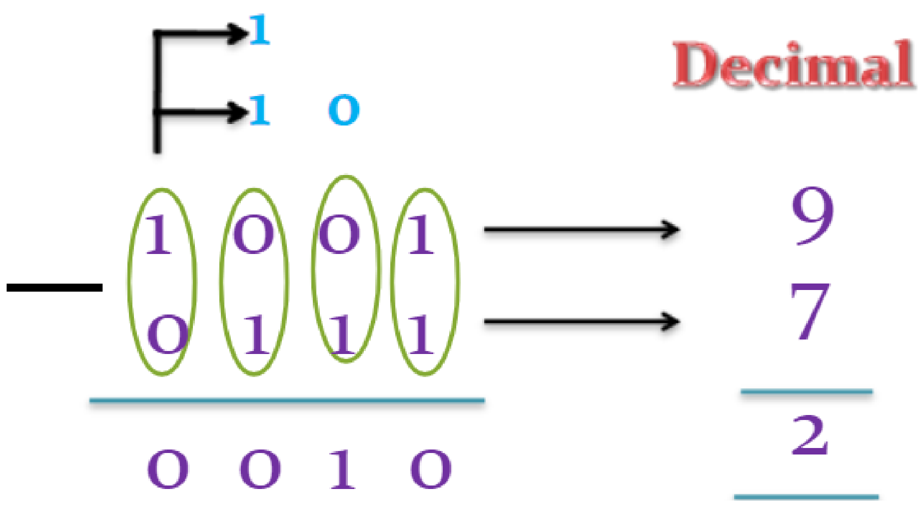
$\rightarrow$ 10011, so the sum is $(11001)_2$

Binary subtraction of integers

- **Rules**

A	B	A – B	Borrow
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	0

Example.



Binary multiplication of integers

- **Rule.**

A	B	A × B
0	0	0
0	1	0
1	0	0
1	1	1

- **Example.**

$$\begin{array}{r} 110 \\ \times\ 101 \\ \hline 110 \\ 000 \\ 110 \\ \hline 11110 \end{array}$$

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

Binary multiplication of integers

ALGORITHM 3 Multiplication of Integers.

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}

- The number of additions of bits used by the algorithm to multiply two n-bit integers is $O(n^2)$.

Binary multiplication of integers

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

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

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

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

$p = 0$

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

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

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

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

Binary division of integers

- **Rule**.
  - $1 \div 1 = 1$
  - $1 \div 0 =$ Meaningless
  - $0 \div 1 = 0$
  - $0 \div 0 =$ Meaningless

Binary division of integers

Example. Find quotient and remainder (if exists) in the division of $(10011111)_2$ by $(1100)_2$.

Solution.

$$
\begin{array}{r|l}
10011111 & 1100 \\ \cline{2-2}
-\ 1100 & 1101 \\ \cline{1-1}
1111 & \\
-\ 1100 & \\ \cline{1-1}
1111 & \\
-\ 1100 & \\ \cline{1-1}
11 &
\end{array}
$$

The quotient q = 1101 and the remainder r = 11

Binary division

ALGORITHM 4 Computing div and mod.

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$\}$

$a = 17\ ,\ d = 5$

$+ r := 17 > 5 = d\ \ ,\ q := 0$

$17 = 5.0 + 17$

$r := r - d = 17 - 5 = 12$

$q = 0 + 1 = 1$

$+ r := 12 > 5 = d$

$17 = 5.1 + 12$

$r := r - d = 12 - 5 = 7$

$q = 1 + 1 = 2$

$+ r := 7 > 5 = d$

$17 = 5.2 + 7$

$r := r - d = 7 - 5 = 2$

$q = 2 + 1 = 3$

$+ r := 2 < 5 = d \Rightarrow stop$

$17 = 5.3 + 2$

$q = 3, r = 2$

Binary division

Example. Using the algorithm find the quotient and the remainder in the division of 101 by 11.

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

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

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

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

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

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

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

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

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

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

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

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

Binary modular exponential algorithm

- The algorithm successively finds b mod m, b^2 mod m, b^4 mod m, …, $b^{2^{k-1}}$ mod m, and multiples together the terms b^{2^j} where $a_j = 1$.

ALGORITHM 5 Fast Modular Exponentiation.

```
procedure modular exponentiation(b: integer, n = (a_{k-1}a_{k-2} ... 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 · power) mod m
    power := (power · power) mod m
return x{x equals b^n mod m}
```

- $O\left((\log n)^2 \log n\right)$ bit operations are used to find b^n mod m.

Binary modular exponential algorithm

Example. Find 3^{644} **mod** 645 by using the binary modular exponential algorithm.

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

$x = 1$

$power = 3 \bmod 645 = 3$

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

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

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

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

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

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

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

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

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

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

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

Exercises

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

a) 231 b) 4532 c) 97644

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

a) $(1\ 1111)_2$ b) $(10\ 0000\ 0001)_2$ c) $(1\ 0101\ 0101)_2$

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

a) $(572)_8$ **b)** $(1604)_8$

c) $(423)_8$ **d)** $(2417)_8$

Exercises

4. Convert the binary expansion of each of these integers to an octal expansion
   a) $(1111\ 0111)_2$
   b) $(1010\ 1010\ 1010)_2$
   c) $(111\ 0111\ 0111\ 0111)_2$
   d) $(101\ 0101\ 0101\ 0101)_2$

5. Convert the hexadecimal expansion of each of these integers to a binary expansion.

   a) $(80E)_{16}$
   b) $(135AB)_{16}$
   c) $(ABBA)_{16}$
   d) $(DEFACED)_{16}$

Exercises

6. Find the base 7 expansion of 186

A. 354 B. 331 C. 413 D. 271 E. None of the answers is correct

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

A. 11110 B. 11111 C. 1000 D. 10101 E. None of the answers is correct

8. Find the sum and the product of each of these pairs of numbers. Express your answers as a binary expansion.

a) $(100\ 0111)_2$, $(111\ 0111)_2$

b) $(1110\ 1111)_2$, $(1011\ 1101)_2$

c) $(10\ 1010\ 1010)_2$, $(1\ 1111\ 0000)_2$

d) $(10\ 0000\ 0001)_2$, $(11\ 1111\ 1111)_2$

Exercises

9. Find the sum and product of each of these pairs of numbers. Express your answers as an octal expansion.

a) $(763)_8$, $(147)_8$

b) $(6001)_8$, $(272)_8$

10. Find the sum and product of each of these pairs of numbers. Express your answers as a hexadecimal expansion.

a) $(1AE)_{16}$, $(BBC)_{16}$

b) $(20CBA)_{16}$, $(A01)_{16}$

11. Use Fast Modular Exponential to find

a) 7^{644} mod 645

b) 123^{1001} mod 101

PRIME AND GREATEST COMMON DIVISORS

Primes and composites

Definition:

- A positive integer p that greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**.
- A positive integer that is greater than 1 and is not prime is called **composite**.

Examples:

- 2, 3, 5, 7, … are primes

1 | 2 and 2 | 2, 1 | 3 and 3 | 3, etc

- 4, 6, 8, 9, … are composites

4 | 4, 2 | 4 and 1 | 4; 6 | 6, 3 | 6, 2 | 6 and 1 | 6, etc

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

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

  - 12 = 2*2*3
  - 21 = 3*7
- Process of finding out factors of the product: **factorization**.

Primes and composites

Theorem 1. If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Example. 12 is a composite, prime divisors less than or equal to $\sqrt{12}$ are 2 and 3.

Theorem 2. There are infinitely many primes.

Primes and composites

Theorem 3. (The prime number theorem) The ratio of $\pi(x)$, the number of primes not exceeding x, and x/ln x approaches 1 as x grows without bound. (Here ln x is the natural logarithm of x.)

$$\lim_{x\to\infty} \frac{\pi(x)}{\left[\frac{x}{\log(x)}\right]} = 1$$

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

Conjectures and Open Problems About Primes

- Number theory is noted as a subject for which it is easy to formulate conjectures, some of which are difficult to prove and others that remained open problems for many years.
- Many famous problems about primes still await ultimate resolution by clever people.

Conjectures and Open Problems About Primes

- **Goldbach's Conjecture.** Every even integer n, $n > 2$, is the sum of two primes.

Example. $4 = 2 + 2$, $8 = 5 + 3$, …

- **Twin primes** are pairs of primes that differ by 2, such as 3 and 5, 5 and 7, …
- **The Twin Prime Conjecture.** There are infinitely many twin primes. The strongest result proved concerning twin primes is that there are infinitely many pairs p and $p + 2$, where p is prime and $p + 2$ is prime or the product of two primes (proved by J. R. Chen in 1966).

Primes and composites

How to determine whether the number is a prime or a composite?

Let n be a number. Then in order to determine whether it is a **prime** we can test:

- **Approach 1:** if any number $x < n$ divides it. If yes it is a composite. If we test all numbers $x < n$ and do not find the proper divisor then n is a prime.
- **Approach 2:** if any prime number $x < n$ divides it. If yes it is a composite. If we test all primes $x < n$ and do not find a proper divisor then n is a prime.
- **Approach 3:** if any prime number $x < \sqrt{n}$ divides it. If yes it is a composite. If we test all primes $x < \sqrt{n}$ and do not find a proper divisor then n is a prime.

Greatest common divisor

Definition: Let a and b are two positive integers. The largest integer d such that d | a and d | b is called the greatest common divisor of a and b. The **greatest common divisor** is denoted as **gcd(a,b)**.

Example:

- What is gcd(24,36) =?
- Give me the positive common divisors of 24 and 36:
- The largest number?

Greatest common divisor

Suppose that the prime factorization of the positive integers a and b are $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$, b $= p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$. Then

$$\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{p}_{\mathbf{1}}^{\boldsymbol{min}(\boldsymbol{a}_{\mathbf{1}}, \boldsymbol{b}_{\mathbf{1}})} \boldsymbol{p}_{\mathbf{2}}^{\boldsymbol{min}(\boldsymbol{a}_{\mathbf{2}}, \boldsymbol{b}_{\mathbf{2}})} \ldots \boldsymbol{p}_{\boldsymbol{n}}^{\boldsymbol{min}(\boldsymbol{a}_{\boldsymbol{n}}, \boldsymbol{b}_{\boldsymbol{n}})}$$

Least common divisor

Definition: Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b)**.

Example:

- What is lcm(12,9) =?
- Give me a common multiple:
- Can we find a smaller number?

Least common divisor

Suppose that the prime factorization of the positive integers a and b are $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, b $= p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$. Then

$$\mathbf{lcm}(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \dots p_n^{max(a_n,b_n)}}$$

Relatively prime

Definitions.

- The integers a and b are **relatively prime** if their **greatest common divisor is 1**.
- The integers a_1, a_2, …, a_n are **pairwise relatively prime** if $\mathbf{gcd}(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example.

Since $\gcd(17,22) = 1$, 17 and 22 are relatively prime.

10, 17 and 21 are pairwise relatively prime because $\gcd(10,17) = \gcd(10,21) = \gcd(17,21) = 1$.

10, 19, 24 are not pairwise relatively prime since $\gcd(10,24) = 2 > 1$

Relationship between the greatest common divisor and least common multiple

Theorem. Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$$

The Euclidean Algorithm

Lemma. Let $a = bq + r$, where a, b, q, and r are integers. Then

$$\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b}) = \mathbf{gcd}(\boldsymbol{b}, \boldsymbol{r})$$

Algorithm.

procedure *gcd*(a, b: positive integers)

x := a

y := b

while y ≠ 0

  r := x mod y

  x := y

  y := r

return x{gcd(a, b) is x}

The Euclidean Algorithm

Example. Using the Euclidean algorithm find gcd(24, 36)

$x = 24$
$y = 36$

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

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

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

$y = 0 \neq 0 (!)$

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

The Euclidean Algorithm

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\
&\ \ \vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n.
\end{aligned}$$

Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms. Furthermore, it follows from Lemma 1 that

$$\begin{aligned}
\gcd(a, b) &= \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) \\
&= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.
\end{aligned}$$

Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

The Euclidean Algorithm

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$82 = 2 \cdot 41.$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

Divisibility

Lemmas.

- If a, b and c are positive integers such that gcd(a, b) = 1 and a | bc then a | c.
- If p is a prime and $p \mid a_1 a_2 \ldots a_n$, where each $a_i \in Z$, then $p \mid a_i$ for some i.

Theorem. Let $m \in Z^+$, and let a, b, and c be integers. If $ac \equiv bc$ (mod m) and $\gcd(c, m) = 1$ then $a \equiv b$ (mod m).

Exercises

1. Determine whether each of these integers is prime.

a) 21 b) 29 c) 71 d) 97 e) 111 f) 143

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

a) 39 b) 81 c) 101 d) 143 e) 289 f) 899

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

4. Determine whether the integers in each of these sets are pairwise relatively prime.

a) 21, 34, 55 b) 14, 17, 85

c) 25, 41, 49, 64 d) 17, 18, 19, 23

Exercises

5. What are the greatest common divisors and the least common multiple of these pairs of integers?

a) $2^2 \cdot 3^3 \cdot 5^5,\ 2^5 \cdot 3^3 \cdot 5^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13,\ 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

c) $17,\ 17^{17}$

6. Use the Euclidean algorithm to find

a) gcd(1, 5).　　　　　　b) gcd(100, 101)

7. Using the method followed in example of the Euclidean algorithm, express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

a) 10, 11　　　b) 21, 44　　　c) 36, 48

Exercises

8. Which pair of integers are relatively prime?

A. (17, 51)

B. (5, 24)

C. (11, 121)

D. (37, 111)

9. If a and 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

APPLICATIONS OF CONGRUENCES

Applications of Congruences

Modular arithmetic and congruencies are used in CS:

– Pseudorandom number generators

– Hash functions

– Check digits

– Cryptology

Pseudorandom number generators

- Some problems we want to program need to simulate a random choice.

Examples: flip of a coin, roll of a dice

We need a way to generate random outcomes

- Basic problem:
  – assume outcomes: 0, 1, .. N
  – generate the random sequences of outcomes
- Pseudorandom number generators let us generate sequences that look random
- The most commonly used procedure for generating pseudorandom numbers: linear congruential method

Pseudorandom number generators

- **Linear congruential method**
  - Choosing 4 numbers:
    - The modulus m
    - Multiplier a
    - Increment c
    - Seed x_0

such that $2 \leq a < m$, $0 \leq c < m$ and $0 \leq x_0 < m$

Generating a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by using the recursively defined function

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

Pseudorandom number generators

Example. Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus m = 9, multiplier a = 7, increment c = 4, and seed $x_0 = 3$.

Solution. $x_{n+1} = (7x_n + 4) \bmod 9$

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

Hash functions

A **hash function** is an algorithm that maps data of arbitrary length to data of a fixed length.

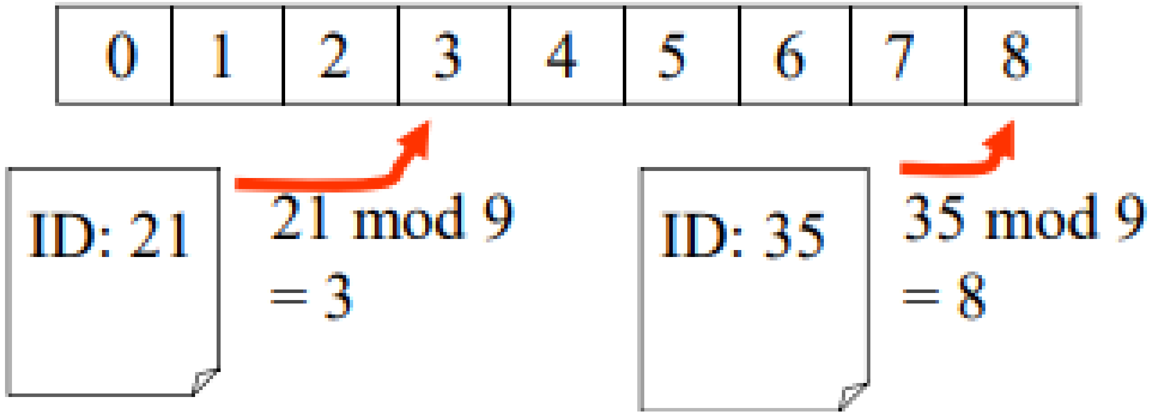
The values returned by a hash function are called **hash values** or **hash codes**.

Example. The central computer at an insurance company maintains records for each of its customers. How can memory locations be assigned so that customer records can be retrieved quickly? The solution to this problem is to use a suitably chosen hashing function. Records are identified using a **key**, which uniquely identifies each customer's records. For instance, customer records are often identified using the Social Security number of the customer as the key. A hashing function h assigns memory location h(k) to the record that has k as its key.

Hash functions

- **Problem:** Given a large collection of records, how can we store and find a record quickly?
- **Solution:** Use a hash function calculate the location of the record based on the record's ID.
- **Example:** A common hash function is
  - $h(k) = k \textbf{ mod } n$,

  where n is the number of available storage locations.



Hash functions

In practice, many different hashing functions are used. One of the most common is the function

$$h(k) = k \ \mathbf{mod} \ m$$

where m is the number of available memory locations.

Example. Assume we have a database of employes, each with a unique ID – a social security number that consists of 8 digits. We want to store the records in a smaller table with m entries. Using h(k) function we can map a social security number in the database of employes to indexes in the table.

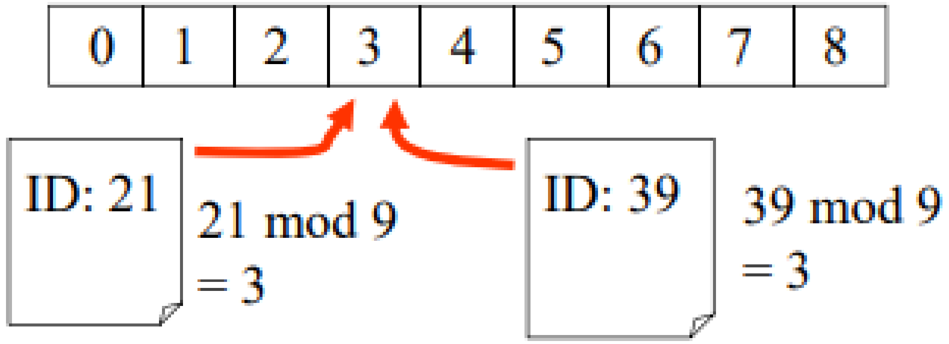
Assume $h(k) = k$ mod 111

Then h(064212848) = 064212848 mod 111 = 14

The record of the customer with Social Security number 064212848 is assigned to memory location 14

Hash functions

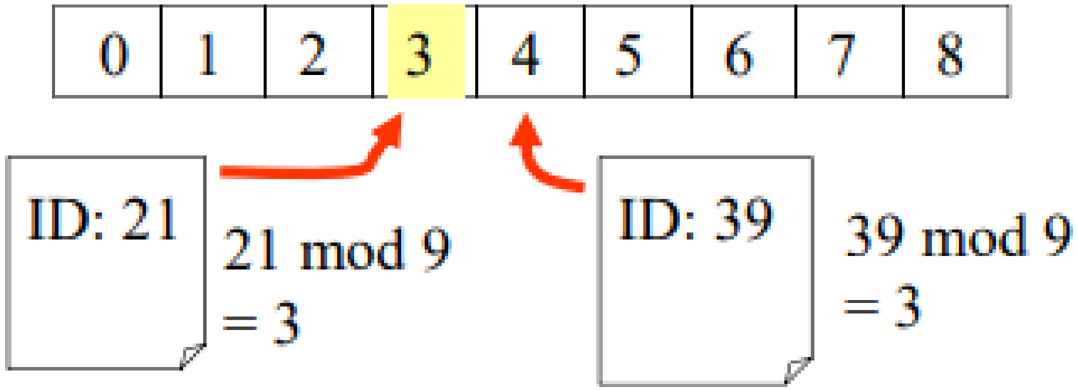
- **Problem:** two files mapped to the same location



Hash functions

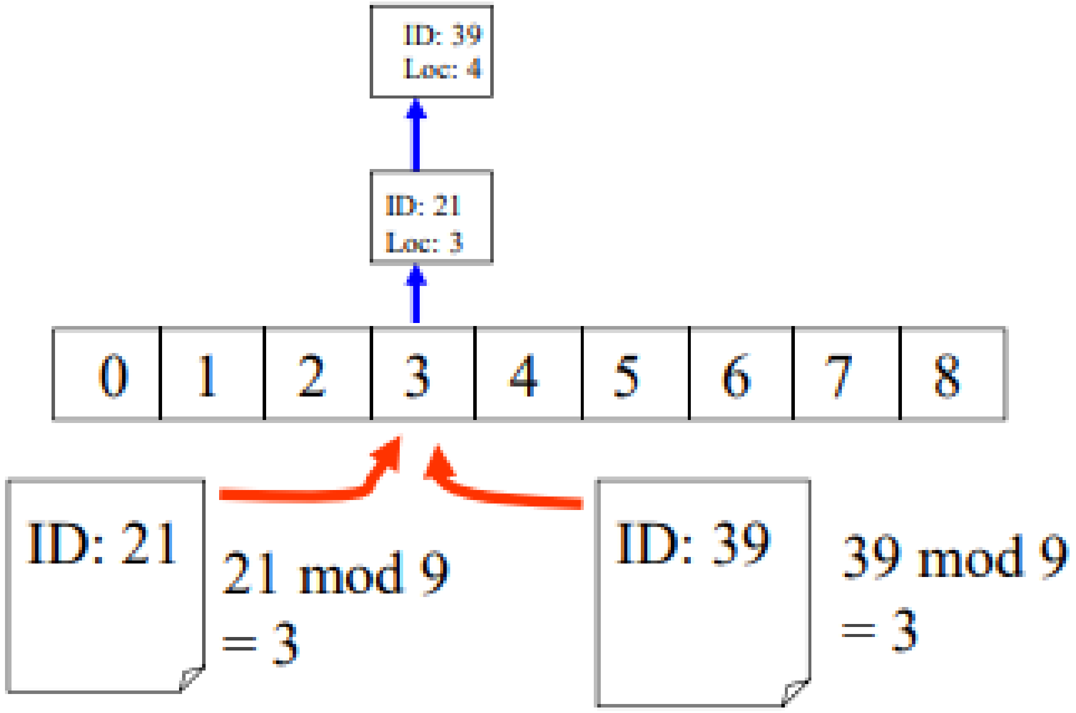
- **Solution 1:** move the next available location
  - Method is represented by a sequence of hash functions to try

$$h_0(k) = k \textbf{ mod } n$$
$$h_1(k) = (k+1) \textbf{ mod } n$$
$$\ldots$$
$$h_m(k) = (k+m) \textbf{ mod } n$$



Hash functions

- **Solution 2:** remember the exact location in a secondary structure that is searched sequentially



Check digits

Congruences are used to check for errors in digit strings. A common technique for detecting errors in such strings is to add an extra digit at the end of the string. This final digit, or check digit, is calculated using a particular function. Then, to determine whether a digit string is correct, a check is made to see whether this final digit has the correct value.

Exercises

1. Which memory locations are assigned by the hashing function h(k) = k mod 97 to the records of insurance company customers with these Social Security numbers?

a) 034567981　　　　　b) 183211232

c) 220195744　　　　　d) 987255335

2. A parking lot has 31 visitor spaces, numbered from 0 to 30. Visitors are assigned parking spaces using the hashing function h(k) = k mod 31, where k is the number formed from the first three digits on a visitor's license plate. Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates: 317, 918, 007, 100, 111, 310?

Exercises

3. What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 2) \bmod 13$ with seed $x_0 = 1$?
4. What sequence of pseudorandom numbers is generated using the pure multiplicative generator $x_{n+1} = 3x_n \bmod 11$ with seed $x_0 = 2$?

Cryptography

Encryption of messages

One of the earliest known uses of cryptography was by Julius Caesar .

Shifting each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three). For example, A is shifted to D, K is shifted to N.

How to represent the idea of a shift by 3?

There are 26 letters in the alphabet. Assign each of them a number from 0,1, 2, 3, .. 25 according to the alphabetical order

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

Caesar's encryption method can be represented by the function *f* that assigns to the nonnegative integer p, p $\le$ 25, the integer *f*(p) in the set {0, 1, 2, … , 25} with

$$f(p) = (p + 3) \bmod 26$$

Cryptography

Encryption of messages

The encryption of the letter with an index p is represented as: $f(p) = (p + 3) \bmod 26$

Coding of letters

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

Example

a. MEET YOU IN THE PARK → 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

Replace each of these numbers p by f(p) → 15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13

→ PHHW BRX LQ WKH SDUN

b. What is the secret message produced from the message I LIKE DISCRETE MATH using the Caesar cipher?

Cryptography

Encryption of messages

The encryption of the letter with an index p is represented as: $f(p) = (p + 3) \bmod 26$

Coding of letters

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

What method would you use to decode the message? (Decryption)

$$\boldsymbol{f^{-1}(p) = (p - 3) \bmod 26}$$

Cryptography

Encryption of messages

There are various ways to generalize the Caesar cipher. For example, we can **shift the numerical equivalent of each letter by k**, a shift cipher, $\boldsymbol{f(p) = (p + k) \bmod 26}$ and **decryption** can be carried out using $\boldsymbol{f^{-1}(p) = (p - k) \bmod 26}$.

The integer k is called a **key**.

We can generalize shift ciphers further to slightly enhance security by using a function of the form $\boldsymbol{f(p) = (ap + b) \bmod 26}$, where a and b are integers, chosen so that f is a bijection. (The function $f(p) = (ap + b) \bmod 26$ is a bijection if and only if $\gcd(a, 26) = 1$).

Cryptography

Example.

a. Encrypt the plaintext message "STOP GLOBAL WARMING" using the shift cipher with shift k = 11.

b. Decrypt the ciphertext message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted with the shift cipher with shift k = 7.

Exercises

1. Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

a) $f(p) = (p + 3) \bmod 26$ (the Caesar cipher)

b) $f(p) = (p + 13) \bmod 26$

c) $f(p) = (3p + 7) \bmod 26$

2. Decrypt these messages that were encrypted using the Caesar cipher.

a) EOXH MHDQV

b) WHVW WRGDB

c) HDW GLP VXP

3. Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10) \bmod 26$.

a) CEBBOXNOB XYG

b) LO WI PBSOXN

c) DSWO PYB PEX

Exercises

4. Using the function f(x) = (x + 10) mod 26 to encrypt messages. Answer each of these questions.

a) Encrypt the message STOP

b) Decrypt the message LEI

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

Choose the correct answer.

A. BTTQ TTOA B. CHOS QHHG C. QHUG KHOS D. QHHG KHOS

Thanks