网络安全技术

刘振

上海交通大学 计算机科学与工程系

电信群楼3-509

liuzhen@sjtu.edu.cn

Number Theory

We work on integers only

Divisors

Two integers: a and b (b is non-zero)

- b divides a if there exists some integer m such that a = m·b
- Notation: b|a
- eg. 1,2,3,4,6,8,12,24 divide 24
- b is a **divisor** of a

Relations

1. If $b|1$ $\Rightarrow$ $b = \pm 1$
2. If $b|a$ and $a|b$ $\Rightarrow$ $b = \pm a$
3. If $b|0$ $\Rightarrow$ any $b \neq 0$
4. If $b|g$ and $b|h$ then $b \mid (mg + nh)$ for any integers m and n.

Congruence

a is **congruent** to b modulo n if n | a-b.

Notation: $a \equiv b \pmod{n}$

Examples

1. $23 \equiv 8 \pmod{5}$ because 5 | 23-8
2. $-11 \equiv 5 \pmod{8}$ because 8 | -11-5
3. $81 \equiv 0 \pmod{27}$ because 27 | 81-0

Properties

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$

Modular Arithmetic

- **modular reduction:** a mod n = r

  r is the remainder when a is divided by a natural number n
- **r** is also called the **residue of a mod n**
  - it can be represented as: a = qn + r where **0 ≤ r < n**, q = ⌊a/n⌋ where ⌊x⌋ is the largest integer less than or equal to x
  - q is called the quotient
- 18 mod 7 = ?
- 29345723547 mod 2 = ?
- Relation between **modular reduction** and **congruence**
  - -12 ≡ -5 ≡ 2 ≡ 9 (mod 7)
  - -12 mod 7 = 2 (what's the quotient?)
  - For any integers a, b and positive integer m, a ≡ b (mod n) iff a mod n = b mod n.

Modular Arithmetic Operations

- **can do modular reduction at any point**,
  - a + b mod n = [a mod n + b mod n] mod n
  - E.g. 97 + 23 mod 7 = [97 mod 7 + 23 mod 7] mod 7 = [6 + 2] mod 7 = 1
  - E.g. 11 – 14 mod 8 = -3 mod 8 = 5
  - E.g. 11 x 14 mod 8 = 3 x 6 mod 8 = 2

Modular Arithmetic

- $Z_n = \{0, 1, \ldots, n-1\}$
- If $a+b \equiv a+c \pmod{n}$

  then $b \equiv c \pmod{n}$
- but if $ab \equiv ac \pmod{n}$

  then $b \equiv c \pmod{n}$ only if a is relatively prime to n
  - $n \mid ab - ac \Rightarrow n \mid a(b - c)$
  - E.g. $7 \times 11 \equiv 7 \times 5 \pmod{6}$ $\Rightarrow 11 \equiv 5 \pmod{6}$
  - $9 \times 3 \equiv 9 \times 5 \pmod{6}$ but $3 \not\equiv 5 \pmod{6}$

Prime and Composite Numbers

- An integer p is prime if its only divisors are ±1 and ±p only.
- Otherwise, it is a composite number.
- E.g. 2,3,5,7 are prime; 4,6,8,9,10 are not
- List of prime number less than 200:

  2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79
  83 89 97 101 103 107 109 113 127 131 137 139 149 151 157
  163 167 173 179 181 191 193 197 199

- Prime Factorization: If a is a composite number, then a can be factored in a unique way as

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$$

  where $p_1 > p_2 > \dots > p_t$ are prime numbers and each α_i is a natural number (i.e. a positive nonzero integer).

e.g. $12{,}250 = 7^2 \cdot 5^3 \cdot 2$

Prime Factorization

- It is generally hard to do (prime) factorization when the number is large
- E.g. factorize
  1. 24070280312179
  2. 1089300248092491025 1
  3. 938740932174981739832107481234871432497 61

Greatest Common Divisor (GCD)

- GCD (a,b) of a and b is the largest number that divides both a and b
  - E.g. GCD(60,24) = 12
- If GCD(a, b) = 1, then a and b are said to be **relatively prime**
  - E.g. GCD(8,15) = 1
  - 8 and 15 are relatively prime (co-prime)

Question: How to compute gcd(a,b)?

Naive method: factorize a and b and compute the product of all their common factors.

e.g. $540 = 2^2 \times 3^3 \times 5$
$144 = 2^4 \times 3^2$
$gcd(540, 144) = 2^2 \times 3^2 = 36$

Problem of this naive method: factorization becomes very difficult when integers become large.

Better method: Euclidean Algorithm (a.k.a. Euclid's GCD algorithm)

Euclidean Algorithm

Compute gcd(911, 999) :

999=911*1+88
911=88*10+31
88=31*2+26
31=26*1+5
26=5*5+1
5=1*5+0

Hence gcd(911, 999) = 1

Euclid's Algorithm:

```
A=a, B=b
while B>0
        R = A mod B
        A = B, B = R
return A
```

Rationale

Theorem gcd(a, b) = gcd(b, a mod b)

Euclidean Algorithm

Proof Sketch.

"$\Rightarrow$" (if d divides a and b then d also divides b mod a)

Suppose d|a and d|b.

For any positive integer a, b can be expressed in the form

$$b = qa + r \equiv r \pmod{a} \qquad \text{— (1)}$$

$$\Rightarrow \quad b \bmod a = b - qa \qquad \text{— (2)}$$

Since d|a, it also divides qa.

Hence from (2), we see that d | b mod a.

"$\Leftarrow$" (if d divides a and b mod a then d also divides b)

Similarly, if d|a and d|qa.

Thus d | (qa + (b mod a)),

which is equivalent to d | b.

Thus the sets of common divisors of a and b, and a and b mod a, are identical.

Hence gcd(911, 999) = gcd(911, 999 mod 911) = gcd(911 mod 88, 88)
= gcd(31, 88 mod 31) = gcd(31 mod 26, 26) = gcd(5, 26 mod 5)
= gcd(5, 1) = 1.

Modular Inverse

A is the modular inverse of B mod n if AB mod n = 1.

A is denoted as B^{-1} mod n.

e.g.
- 3 is the modular inverse of 5 mod 7. In other words, 5^{-1} mod 7 = 3.
- 7 is the modular inverse of 7 mod 16. In other words, 7^{-1} mod 16 = 7.

However, there is no modular inverse for 8 mod 14.

There exists a modular inverse for B mod n iff B is relatively prime to n.

Question:
What's the modular inverse of 911 mod 999?

Extended Euclidean Algorithm

The extended Euclidean algorithm can be used to solve the integer equation

$$ax + by = \gcd(a, b)$$

For any given integers a and b.

Example

Let a = 911 and b = 999. From the Euclidean algorithm,

$$\begin{aligned} 999 &= 1 \times 911 + 88 \\ 911 &= 10 \times 88 + 31 \\ 88 &= 2 \times 31 + 26 \\ 31 &= 1 \times 26 + 5 \\ 26 &= 5 \times 5 + 1 \qquad \Rightarrow \gcd(a, b) = 1 \end{aligned}$$

Now by tracing backward, we get

$$\begin{aligned} 1 &= 26 - 5 \times 5 \\ &= 26 - 5 \times (31 - 1 \times 26) = -5 \times 31 + 6 \times 26 \\ &= -5 \times 31 + 6 \times (88 - 2 \times 31) = 6 \times 88 - 17 \times 31 \\ &= 6 \times 88 - 17 \times (911 - 10 \times 88) = -17 \times 911 + 176 \times 88 \\ &= -17 \times 911 + 176 \times (999 - 1 \times 911) = \mathbf{176 \times 999 - 193 \times 911} \end{aligned}$$

we now have

gcd(911, 999) = 1 = -193 x 911 + 176 x 999.

If we do a modular reduction of 999 to this equation, we have

1 (mod 999) = -193 x 911 + 176 x 999 (mod 999)
$\Rightarrow$1 = -193 x 911 mod 999
$\Rightarrow$1 = (-193 mod 999) x 911 mod 999
$\Rightarrow$1 = 806 x 911 mod 999

1 ≡ 806 x 911 (mod 999).

Hence 806 is the **modular inverse** of 911 modulo 999.

Suppose GCD(a,n)=1, Compute $a^{-1}\ mod\ n$:
Compute $x\ and\ y, such\ that\ ax + ny = \gcd(a, n)$,then $x^{-1}\ mod\ n$ is $a^{-1}\ mod\ n$.

The Euler phi Function

For $n \geq 1$, $\phi(n)$ denotes the number of integers in the interval $[1, n]$ which are relatively prime to n. The function ϕ is called the **Euler phi function** (or the **Euler totient function**).

Fact 1. The Euler phi function is multiplicative. I.e. if $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m) \times \phi(n)$.

Fact 2. For a prime p and an integer $e \geq 1$, $\phi(p^e) = p^{e-1}(p-1)$.

- From these two facts, we can find ϕ for any composite n if the prime factorization of n is known.
- Let $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ where $p_1, \ldots, p_k$ are prime and each e_i is a nonzero positive integer.
- Then

$$\phi(n) = n (1 - 1/p_1) (1 - 1/p_2) \ldots (1 - 1/p_k).$$

The Euler phi Function

$$\phi(n) = \left|\{x : 1 \le x \le n \quad and \quad \gcd(x,n) = 1\}\right|$$

- $\phi(2) = |\{1\}| = 1$
- $\phi(3) = |\{1,2\}| = 2$
- $\phi(4) = |\{1,3\}| = 2$
- $\phi(5) = |\{1,2,3,4\}| = 4$
- $\phi(6) = |\{1,5\}| = 2$

- $\phi(37) = 36$
- $\phi(21) = (3-1)\times(7-1) = 2\times 6 = 12$

Fermat's Little Theorem

Let p be a prime. Any integer a not divisible by p satisfies $a^{p-1} \equiv 1 \pmod{p}$.

- If a is not divisible by p and if $n \equiv m \pmod{p-1}$, then $a^n \equiv a^m \pmod{p}$.
- We can generalize the Fermat's Little Theorem as follows. This is due to Euler.

  Euler's Generalization **Let n be a composite. Then $a^{\phi(n)} \equiv 1 \pmod{n}$ for any integer a which is relatively prime to n.**

- E.g. a=3;n=10; $\varphi(10)=4 \Rightarrow 3^4 \equiv 81 \equiv 1 \pmod{10}$
- E.g. a=2;n=11; $\varphi(11)=10 \Rightarrow 2^{10} \equiv 1024 \equiv 1 \pmod{11}$

Exercise: Compute $11^{1,073,741,823} \bmod 13$.

For integer a and positive integer k, n, if a and n are co-prime, then $a^k \bmod n = a^{k \bmod \phi(n)} \bmod n$.

Modular Exponentiation

Let Z = { …, -2, -1, 0, 1, 2, … } be the set of integers.

Let a, e, n ∈ Z.

Modular exponentiation a^e mod n is defined as repeated multiplications of a for e times modulo n.

Method 1 : Repeated Modular Multiplication (as defined)

e.g. 11^{15} mod 13 = $\underline{11 \times 11} \times 11 \times 11 \times \ldots \times 11 \bmod 13$
= $\underline{4 \times 11} \times 11 \times \ldots \times 11 \bmod 13$
= $\underline{5 \times 11} \times \ldots \times 11 \bmod 13$
:
= 5

- performed 14 modular multiplications
- Complexity = O(e)
- Compute $11^{103741,823}$ mod 1073741823

Modular Exponentiation

Method 2 : Square-and-Multiply Algorithm

e.g. $11^{15} \bmod 13 = 11^8 \times 11^4 \times 11^2 \times 11 \bmod 13$ — (1)

- $11^2 = 121 \equiv 4 \pmod{13}$ — (2)
- $11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$ — (3)
- $11^8 = (11^4)^2 \equiv 3^2 \equiv 9 \pmod{13}$ — (4)

Put (2), (3) and (4) to (1) and get

$11^{15} \equiv 9 \times 3 \times 4 \times 11 \equiv 5 \pmod{13}$

- performed at most $2\lfloor \log_2 15 \rfloor$ modular multiplications
- Complexity = $O(|e|)$ or $O(\lg(e))$

Modular Exponentiation

Pseudo-code of Square-and-Multiply Algorithm to compute a^e mod n :

Let the binary representation of e be $(e_{t-1}\ e_{t-2}\ \ldots\ e_1\ e_0)$.
Hence t is the number of bits in the binary representation of e.

```
1.   z = 1
2.   for i = t-1 downto 0 do
3.        z = z^2 mod n
4.        if e_i = 1 then z = z x a mod n
```

Group Theory

- very important in cryptography, especially in public key cryptography
- concern an operation on “a set of numbers”

Groups

- Let G be a nonempty set and $\circ$ be a binary operation.
- A binary operation $\circ$ on a set G is a mapping from $G \times G$ to G.
  - i.e. $\circ$ is a rule which assigns to each ordered pair of elements from G to an element of G.

$(G, \circ)$ is a group if the following conditions are satisfied:

1. **closed** : for any $a, b \in G$, $a \circ b \in G$
2. **associative** : any $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$
3. there exists an **identity** element e in G, such that for any $a \in G$, $a \circ e = e \circ a = a$.
4. For each $a \in G$, there exists an **inverse** of a denoted by a^{-1}, such that $a \circ a^{-1} = e$.

If $\circ$ is also **commutative**, i.e. for any $a, b \in G$, $a \circ b = b \circ a$, then $(G, \circ)$ is an Abelian group.

Example 1

- a set: {1,2,3,4} with operator * (mod 5)
- obeys:
  - close law
  - associative law: $(a*b)*c = a*(b*c) \pmod 5$
  - identity $e=1$: $1*a = a*1 = a$
  - How about inverses a^{-1}?
    - 1 has an inverse (itself)
    - 2 has an inverse: 3 since $2*3=6=1 \pmod 5$
    - 3 has an inverse: 2.
    - 4 has an inverse: 4 since $4*4=16=1 \pmod 5$
- It is a group
- It is commutative: $a*b = b*a$
- Therefore, this multiplicative group is an Abelian Group

Example 2

- a set: {0,1,2,3} with operator * (mod 4)
- obeys:
  - close law
  - associative law: $(a*b)*c = a*(b*c) \pmod 4$
  - identity $e=1$: $1*a = a*1 = a$
  - How about inverses a^{-1}?
    - First of all, 0 has no inverse
    - 1 has an inverse (itself)
    - 3 has an inverse (itself) $3.3=9=1 \pmod 4$
    - 2 has no inverse
- Cannot be a group

Example 3

- a set: {1,2,3} with operator + (mod 5)
- Is it a group?

More on Multiplicative Groups

- For multiplication, not all $Z_n \backslash \{0\}$ form (multiplicative) groups with the identity element 1.
- It depends on the value of n.
- For example, $Z_8 \backslash \{0\}$ does not while $Z_7 \backslash \{0\}$ under multiplication forms a group.
- Reason: Only those elements which are relatively prime to n have multiplicative inverses. Hence $Z_n \backslash \{0\}$ forms a multiplicative group only when n is a prime.

- As an extension, the set $Z_n^* = \{a \in Z_n \mid \gcd(a,n)=1 \}$ forms a multiplicative group for any positive integer n.

Cyclic Groups

- A group is **cyclic** if there is an element $g \in G$ such that for each $a \in G$, there is an integer i with $a = g^i$, that is g operates (e.g. modular multiply) on itself for i times.
- g is called a **generator** or a **primitive element** of G.
- g is also said to be a **primitive root** of n.
- Example: (Z_7^*, x) is a cyclic multiplicative group with g=3.

Let n=7 and g=3.

i	1	2	3	4	5	6
$g^i \bmod 7$	3	2	6	4	5	1

But not all the multiplicative groups of positive composite integers n have generators (are cyclic).

Fact. Z_n^* has a (at least one) generator if and only if $n = 2, 4, p^k, 2p^k$, where p is an odd prime and $k \geq 1$.

Example

- Is the group {1,2,3,4; * (mod 5)} cyclic?
  - The identity is 1.
  - Let a=2
  - Recall that the notation: a^3 = a.a.a
  - 1= a^0
  - a^1=2
  - a^2= 4 (mod 5)
  - a^3 =2*2*2=8=3 (mod 5)
  - a^4 =16=1 (mod 5)
- 2 is a generator of the group
- Therefore, the group is cyclic.
- Ex: Is 3 (or 4) a generator of this group?