Number Theory

Haipeng Dai

haipengdai@nju.edu.cn
313 CS Building
Department of Computer Science and Technology
Nanjing University

How to compute gcd(x,y)

- Observation: gcd(x,y) = gcd(x-y, y) = gcd(x-2y, y) = ….
- Suppose x>y, x=ky+d where d<y, thus

  gcd(x,y)=gcd(ky+d, y)=gcd(ky+d-ky, y)=gcd(d,y)
- Euclid's Algorithm:

  integer euclid(pos. integer *m*, pos. integer *n*)

  x = *m*, *y* = *n*

  while(*y* > 0)

          r = *x* mod *y*

          x = *y*

          y = *r*

  return *x*

How to compute gcd(x,y)

- Euclid's Algorithm:

$r_{-2} \leftarrow x$, $r_{-1} \leftarrow y$, $u_{-2} \leftarrow 1$, $v_{-2} \leftarrow 0$, $u_{-1} \leftarrow 0$, $v_{-1} \leftarrow 1$

//Note that this makes $r_n = u_n x + v_n y$ for $n=-2$ and $n=-1$

$n \leftarrow 0$

while $r_{n-1} \neq 0$ do

$r_n \leftarrow r_{n-2} \bmod r_{n-1}$, $q_n \leftarrow r_{n-2} / r_{n-1}$,

// $r_{n-2} = q_n r_{n-1} + r_n$; so, $u_{n-2}x + v_{n-2}y = q_n(u_{n-1}x + v_{n-1}y) + r_n$;

// So, $(u_{n-2} - q_n u_{n-1})x + (v_{n-2} - q_n v_{n-1})y = r_n$

$u_n \leftarrow u_{n-2} - q_n u_{n-1}$, $v_n \leftarrow v_{n-2} - q_n v_{n-1}$,

$n \leftarrow n+1$

end

return gcd(a, b)= r_{n-2}

Euclid’s Algorithm Example

- Compute gcd(408, 595)

n	q_n	r_n	u_n	v_n
-2		408	1	0
-1		595	0	1
0	0	408	1	0
1	1	187	-1	1
2	2	34	3	-2
3	5	17	-16	11
4	2	0	35	-24

595/408 = 1 remainder 187

408/187 = 2 remainder 34

187/34 = 5 remainder 17

34/17 = 2 remainder 0

Hence gcd(408, 595)= r_3=17=-16×408+11×595

Finding Multiplicative Inverses

- Compute the **multiplicative inverse** a^{-1} mod n
- It is equivalent to find a number u such that $ua = 1 \bmod n$
- In other words, there is an integer v such that $ua + vn = 1$
- Using Euclid's algorithm, we can compute gcd(a, n) to find u and v such that $ua + vn = 1$
- Fact: a and n are relatively prime iff there are integers u and v such that $ua + vn=1$.

  Proof: If gcd(a,n)=1, then we can find u and v such that $ua + vn = 1$ according to Euclid's algorithm. If gcd(a, n)=m>1, suppose $a=km$, $n=k'm$, then for any integers u and v, $ua+vn = ukm+vk'm=(uk+vk')m \neq 1$.

Group

- A group, denoted by $(G, \circ)$, is a set G with a binary operation $\circ$: $G \times G \rightarrow G$ such that
  - **Associativity**: $a \circ (b \circ c) = (a \circ b) \circ c$ (associative)
  - Existence of **identity**: there exists $e \in G$ s.t. $\forall x \in G$, $e \circ x = x \circ e = x$ (identity)
  - Existence of **inverse**: for any $x \in G$, there exists $y \in G$ s.t. $x \circ y = y \circ x = e$ (inverse)
- A group $(G, \circ)$ is commutative if $\forall x, y \in G$, $x \circ y = y \circ x$.
- Examples: $(Z, +)$, $(Q, +)$, $(Q\backslash\{0\}, \times)$, $(R, +)$, $(R\backslash\{0\}, \times)$

Integers modulo n (1/2)

- Let $n \geq 2$ be an integer
- Definition:

  a is congruent to b modulo n, denoted as $a \equiv b \bmod n$, if $n|(a-b)$, i.e., a and b have the same remainder when divided by n
- Definition:

  $[a]_n$ = {all integers congruent to a modulo n}
- $[a]_n$ is called a residue class modulo n, and a is a representative of that class.

Integers modulo n (2/2)

- $[a]_n = [b]_n$ if and only if $a \equiv b \bmod n$
- There are exactly n residue classes modulo n:

$$[0], [1], [2], \ldots, [n\text{-}1].$$

- If $x \in [a]$ and $y \in [b]$, then $x+y \in [a+b]$ and $x \cdot y \in [a \cdot b]$.
- Addition and multiplication for residue classes:

$$[a]+[b] = [a+b]$$

$$[a] \cdot [b] = [a \cdot b]$$

Z_n (1/2)

- Define Z_n={[0], [1], [2], …, [n-1]}.
- Or, more conveniently, Z_n={0, 1, 2, …, n-1}.
- (Z_n,+) forms a commutative additive group
  - Associavitivity: for $\forall$a, b, c $\in Z_n$, [a]+([b]+[c]) = [a]+[b+c]=[a+b+c]=[a+b]+[c]=([a]+[b])+[c]
  - Existence of identity: 0 is the identity element.
  - Existence of inverse: the inverse of a, denoted by –a, is n-a.
  - Communitivity: for $\forall$a, b$\in Z_n$, [a]+[b] = [b]+[a]
- When doing addition/subtraction in Z_n, just do the regular addition/subtraction and then compute the result modulo n.
  - In Z_{10}, 5+9=4

Z_n (2/2)

- $(Z_n, \times)$ is not a group, because 0^{-1} does not exist.
- Even if we exclude 0 and consider only $Z_n^+ = Z_n \backslash \{0\}$, $(Z_n^+, \times)$ is not necessarily a group; some a^{-1} may not exist.
- For $a \in Z_n$, a^{-1} exists if and only if $\gcd(a, n)=1$
- $\gcd(a, n) = 1 \Leftrightarrow$ there exists integers x and y *s.t.*

$$ax + ny = 1$$

$$\Leftrightarrow [a][x] + [n][y] = [1] \text{ in } Z_n$$

$$\Leftrightarrow [a][x] = [1] \text{ in } Z_n$$

$$\Leftrightarrow [a]^{-1} = [x] \text{ in } Z_n$$

Z_n* (1/2)

- Let $Z_n^* = \{a \in Z_n : \gcd(a, n) = 1\}$.
- *Theorem*: Z_n* is closed under multiplication mod n

Proof:

This means if a and b are in Z_n*, then ab mod n is in Z_n*

Since a and b are relatively prime to n, there are integers u_a, v_a, u_b, and v_b such that

$$u_a a + v_a n = 1 \quad \text{and} \quad u_b b + v_b n = 1$$

Multiply these two equations

$$(u_a u_b)ab+(u_a v_b a+v_a u_b b+v_a v_b n)n = 1$$

Hence ab mod n is in Z_n*

Z_n^* (2/2)

- $(Z_n^*, \times)$ is a commutative multiplicative group.
  - Associativity: for $\forall a, b, c \in Z_n^*$, $(a \times b) \times c = abc \bmod n = a \times (b \times c)$.
  - Existence of identity: 1 is the identity element.
  - Existence of inverse: the inverse of a, denoted as a^{-1}, can be computed by the Euclid's algorithm.
  - Commutativity: for $\forall a, b \in Z_n^*$, $a \times b = ab \bmod n = b \times a$.
- For example, $Z_{12}^* = \{1, 5, 7, 11\}$. $5 \times 7 = 35 \bmod 12 = 11$

How many elements are there in Z_n^*?

- Euler's totient function:

$$\varphi(n) = |Z_n^*| = |\{a \in Z_n : \gcd(a, n) = 1\}|$$

- Facts:
  - $\varphi(p) = (p-1)$ for prime p.
  - $\varphi(pq) = \varphi(p)\varphi(q)$ if $\gcd(p, q) = 1$

Euler's Theorem

- *Theorem:* For all a in Z_n*, $a^{\varphi(n)} = 1 \bmod n$

  Proof: Let $Z_n^* = \{x_1, x_2, \ldots, x_k\}$ and $y = x_1 \cdot x_2 \ldots x_k \bmod n$

  Since Z_n^* is closed under multiplication,

  y is in Z_n^* and it has an inverse y^{-1}

  Multiply each element of Z_n^* by a

  $Z = \{ax_1 \bmod n, ax_2 \bmod n, \ldots, ax_k \bmod n\}$

  How to prove $Z = Z_n^*$?

  Hint: Prove $ax_i \bmod n \neq ax_j \bmod n$ $(1 \leq i \neq j \leq k)$

  Since $Z = Z_n^*$,

  $ax_1 \cdot ax_2 \ldots ax_k \bmod n = x_1 \cdot x_2 \ldots x_k \bmod n = y$

  Also $ax_1 \cdot ax_2 \ldots ax_k \bmod n = a^{\varphi(n)} x_1 \cdot x_2 \ldots x_k = a^{\varphi(n)} y$, Thus

  $$a^{\varphi(n)} y = y \bmod n$$

  Since y has an inverse y^{-1}, we have $a^{\varphi(n)} = 1 \bmod n$

- Fermat's theorem: If p is a prime and $0 < a < p$, $a^{p-1} = 1 \bmod n$

Chinese Remainder Theorem (1/6)

- One of the most useful results in number theory
  - Discovered by Chinese mathematician Sun-Tzu in 400~500 A.D.
  - Problem: we have a number of things, but we do not know exactly how many. If we count them by threes we have two left over. If we count them by fives we have three left over. If we count them by sevens we have two left over. How many things are there?

    Formally: if $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 2 \bmod 7$, x =?
- It is used to speed up modulo computations
- If working modulo a product of numbers
  - eg. `mod M = ` $m_1 m_2 .. m_k$
- Chinese Remainder Theorem lets us work in each moduli m_i separately when they are pair wise relatively prime
- Since computational cost is proportional to size, this is faster than working in the full modulus M

Chinese Remainder Theorem (2/6)

- To compute `A(mod M)where M=`$m_1 m_2 \ldots m_k$
  - 1. compute all $a_i = A \bmod m_i$ separately
  - 2. determine constants c_i below, where $M_i = M/m_i$

$$c_i = M_i \times (M_i^{-1} \bmod m_i) \quad \text{for } 1 \leq i \leq k$$

  - 3. then combine results to get answer using:

$$A \equiv \left(\sum_{i=1}^{k} a_i c_i \right) (\bmod M)$$

Chinese Remainder Theorem (3/6)

- Let $M=m_1m_2\ldots m_k$, where the m_i are pairwise relatively prime, i.e., gcd(m_i, m_j) =1 ($1 \le i \ne j \le k$), we can represent any integer A in Z_M by a k-tuple whose elements are in Z_{m_i} using the following correspondence:

$$A \leftrightarrow (a_1, a_2, \ldots, a_k)$$

where $A \in Z_M$, $a_i \in Z_{m_i}$, and $a_i = A \bmod m_i$ ($1 \le i \le k$)

Chinese Remainder Theorem (4/6)

- **Assertion 1**: $A \leftrightarrow (a_1, a_2, \ldots, a_k)$ is an one-to-one mapping, called a bijection, between Z_M and $Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_k}$.
- ***Proof*:**

(1) $A \rightarrow (a_1, a_2, \ldots, a_k)$ is obviously unique, i.e., each is a_i uniquely calculated as $a_i = A \bmod m_i$

(2) $(a_1, a_2, \ldots, a_k) \rightarrow A$ can be done as follows.

Let $M_i = M/m_i$ $(1 \leq i \leq k)$. Note: $M_i = m_1 \times m_2 \times \ldots \times m_{i-1} \times m_{i+1} \times \ldots \times m_k$

Thus, $M_i \equiv 0 \pmod{m_j}$ for all $j \neq i$.

Let $c_i = M_i \times (M_i^{-1} \bmod m_i)$ $(1 \leq i \leq k)$

Because M_i is relatively prime to m_i, it has a unique multiplicative inverse mod m_i. Thus c_i is unique.

We compute: $A \equiv \left(\sum_{i=1}^{k} a_i c_i \right) \pmod{M}$

To show the above equation is correct, we must show $A = a_i \bmod m_i$ $(1 \leq i \leq k)$.

This is true because $c_j \equiv M_j \equiv 0 \pmod{m_i}$ for all $j \neq i$ and $c_i \equiv 1 \pmod{m_i}$

Chinese Remainder Theorem (5/6)

- **Assertion 2**:

  Operations in Z_M can be performed individually in each Z_{m_i}.

  If $\begin{cases} A \leftrightarrow (a_1, a_2, \ldots, a_k) \\ B \leftrightarrow (b_1, b_2, \ldots, b_k) \end{cases}$

  Then

$$A \pm B \bmod M \leftrightarrow (a_1 \pm b_1 \bmod m_1, \ldots, a_k \pm b_k \bmod m_k)$$

$$A \times B \bmod M \leftrightarrow (a_1 \times b_1 \bmod m_1, \ldots, a_k \times b_k \bmod m_k)$$

$$A \div B \bmod M \leftrightarrow (a_1 \div b_1 \bmod m_1, \ldots, a_k \div b_k \bmod m_k)$$

Chinese Remainder Theorem (6/6)

$$\begin{cases} x = 1 \bmod 3 \\ x = 6 \bmod 7 \\ x = 8 \bmod 10 \end{cases}$$

By the Chinese remainder theorem, the solution is

$M = m_1 m_2 m_3 = 3 \times 7 \times 10 = 210$

$M_1 = M/m_1 = 210/3 = 70$, $M_2 = M/m_2 = 210/7 = 30$,

$M_3 = M/m_3 = 210/10 = 21$

$x = 1 \times 70 \times (70^{-1} \bmod 3) + 6 \times 30 \times (30^{-1} \bmod 7) + 8 \times 21 \times (21^{-1} \bmod 10)$

$= 1 \times 70 \times (1^{-1} \bmod 3) + 6 \times 30 \times (2^{-1} \bmod 7) + 8 \times 21 \times (1^{-1} \bmod 10)$

$= 1 \times 70 \times 1 + 6 \times 30 \times 4 + 8 \times 21 \times 1 \bmod 210$

$= 958 \bmod 210$

$= 118 \bmod 210$