Basic Concepts in Number Theory

Somesh Jha

1 Basics

Given a positive integer n, we will write $a \pmod{n}$ as the remainder when a is divided by n (for example $17 \pmod{7}$ is equal to 3 and $-17 \pmod{7}$ is equal to 4). If $a \pmod{n} = b \pmod{n}$, then we write it as $a \equiv b \pmod{n}$. The ***greatest common divisor*** and ***least common multiple*** of a and b are denoted by $gcd(a, b)$ and $lcm(a, b)$, respectively. For example, $gcd(6, 15) = 3$ and $lcm(6, 15) = 30$. Figure 1 gives an algorithm to compute $gcd(x, y)$. The algorithm returns an array of three numbers $[c, a, b]$ such that $c = gcd(x, y)$ and $ax + by = gcd(x, y)$.

Exercise 1 Execute the algorithm on $x = 7$ and $y = 15$.

The following theorem (called the *Fermat's Little Theorem (FLT)*) is very useful.

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

2 Groups

Definition 1 A *semigroup* is a nonempty set G together with a binary operation on G which is:

- *(associative)* for all a, b, c in G, $a(bc) = (ab)c$

A *monoid* is a semigroup G which contains a

- *(identity)* identity element $e \in G$ such that $ae = ea = a$ for all $a \in G$.

A *group* is a monoid G such that

- *(inverse)* for every $a \in G$ there exists a (two-sided) inverse element $a^{-1} \in G$ such that $a^{-1}a = aa^{-1} = e$

Let Z_n be the set $\{0, 1, 2, \cdots, n-1\}$. We add two numbers i and j in Z_n by computing $(i + j) \pmod{n}$. Note that $(Z_n, +)$ is a group (where $+$ is the addition operation that was just described).

Exercise 2 Verify that $(Z_n, +)$ satisfies the three group laws.

```
long int *gcdEuler(long int x, long int y) {

  long int *result, *recursive_result;


  //malloc three elements for the result
  result = (long int *)malloc(sizeof(long int)*3);

  //the base step
  if (y == 0) {
    result[0] = x;
    result[1] = 1;
    result[2] = 0;
    return(result);
  }

  //the recursive step
  recursive_result = gcdEuler(y,x % y);
  result[0] = recursive_result[0];
  result[1] = recursive_result[2];
  result[2] = recursive_result[1]-((int)(x/y))*recursive_result[2];

  //free the array from recursive_result
  free(recursive_result);

  return(result);

} // end of method gcdEuler
```

Figure 1: C code for computing gcd.

Let $Z_n^\star$ be all elements of Z_n that are relatively prime to n, which can be written as

$$\{i \mid i \in Z_n \text{ and } gcd(n,i) = 1\}$$

Recall that $gcd(a,b)$ is the *greatest common divisor* of a and b. We multiply two elements i and j in $Z_n^\star$ as follows: $(i \times j) \pmod n$. We now note that $(Z_n^\star, \cdot)$ (where $\cdot$ is the multiplication operation just described) is a group.

- It is clear that $\cdot$ is associative.
- The element $1 \in Z_n^\star$ is the identity.
- Let $i \in Z_n^\star$. Since $gcd(n,i) = 1$ there exists a and b such that $an + bi \;=\; 1$. Let $b' = b \pmod n$. In this case $b' \cdot i \;=\; i \cdot b' \;=\; 1$. Therefore, each element in $Z_n^\star$ has an inverse.

Note: For a prime p, $Z_p = \{0, 1, 2, \cdots, p-1\}$ and $Z_p^\star = \{1, 2, \cdots, p-1\}$.

The size of $Z_n^\star$ is denoted by $\phi(n)$. Note that $\phi(n)$ also denotes the the number of elements in Z_n that are relatively prime to n. If p is prime, we have the following two equations if p is prime:

$$\begin{aligned} \phi(p) &= p - 1 \\ \phi(p^c) &= p^c - p^{c-1} \end{aligned}$$

Given a number n with prime factorization $p_1^{a_1} \cdots p_k^{a_k}$, we have the following equation:

$$\phi(n) \;=\; \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k})$$

Example 1 Let $n = 3^2 5^3$. Then $\phi(n)$ is calculated below:

$$\begin{aligned} \phi(3^2 5^3) &= \phi(3^2)\phi(5^3) \\ &= (3^2 - 3) \cdot (5^3 - 5^2) \\ &= 6 \cdot 100 \\ &= 600 \end{aligned}$$

Definition 2 A group G is called cyclic if there exists an element $g \in G$ such that $\{g^0, g^1, g^2, \cdots\}$ is equal to G. Element g is called a *generator* of G.

Fact 1 The group $Z_p^\star$ is cyclic. Moreover, there are algorithms for finding the generator for $Z_p^\star$.

Example 2 Consider $Z_5^\star \;=\; \{1, 2, 3, 4\}$. Note that $2^2 \equiv 4 \pmod 5$, $2^3 \equiv 3 \pmod 5$, and $2^4 \equiv 1 \pmod 5$. Therefore, 2 is a generator for $Z_5^\star$.

3 Chinese Remainder Theorem (CRT)

Theorem 2 Let $m_1, \cdots, m_r$ be r positive integers that are relatively prime to each other, i.e., $gcd(m_i, m_j) \;=\; 1$ for $1 \leq i < j \leq r$. Consider the following system of equations:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

The Chinese Remainder Theorem (CRT) states that:

- [Existence]: There exists a solution to the system of equations.
- [Uniqueness]: Two solutions to the system of equations are congruent modulo M (where $M = m_1 m_2 \cdots m_r$), i.e., any two solutions z_1 and z_2 to the system of equations given above satisfy $z_1 \equiv z_2 \pmod{M}$.

[Uniqueness:]
First, we will prove the uniqueness part of CRT. Let z_1 and z_2 be two solutions to the following system of equations:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

Since $z_1 \equiv a_1 \pmod{m_1}$ and $z_2 \equiv a_1 \pmod{m_1}$, $z_1 \equiv z_2 \pmod{m_1}$. Therefore, $m_1 \mid (z_1 - z_2)$. Similarly, $m_i|(z_1 - z_2)$ for $1 \leq i \leq r$, which proves that $M|(z_1 - z_2)$ (recall that m_is are relatively prime to each other).
[Existence:]
Let $M_i = \frac{M}{m_i}$. Note that $gcd(m_i, M_i) = 1$ and for $j \neq i$, $m_i \mid M_j$. Since $gcd(m_i, M_i) = 1$ there exists a N_i such that $M_i N_i \equiv 1 \pmod{m_i}$, i.e., N_i is the inverse of M_i. The following integer is a solution to the system of equations:

$$\sum_{i=1}^{r} a_i M_i N_i$$

Since $M_i N_i \equiv 1 \pmod{m_i}$ we have that $a_i M_i N_i \equiv a_i \pmod{m_i}$. Recall that $m_i | M_j$ for $i \neq j$. Therefore, $a_j M_j N_j \equiv 0 \pmod{m_i}$. Combining the two observations we obtain that $\sum_{i=1}^{r} a_i M_i N_i \;=\; a_i \pmod{m_i}$.

Example 3 Consider $m_1 = 5$ and $m_2 = 7$ and the following system of equations:

$$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

Let z_1 and z_2 be two solutions to the equations given above. We have that $z_1 \equiv z_2 \pmod 5$ and $z_1 \equiv z_2 \pmod 7$. Therefore, $5 \mid (z_1 - z_2)$ and $7 \mid (z_1 - z_2)$. Since 5 and 7 are relatively prime, $35|(z_1 - z_2)$. Therefore, $z_1 \equiv z_2 \pmod{35}$.

Let $M = 5 \times 7 = 35$, $M_1 = 7$, and $M_2 = 5$. We also have $N_1 = 3$ and $N_2 = 3$, and note that $M_1 N_1 \equiv 1 \pmod 5$ and $M_2 N_2 \equiv 1 \pmod 7$. Consider the following integer:

$$2 \times 7 \times 3 + 3 \times 5 \times 3 \quad = \quad 87$$

Note that $87 \equiv 2 \pmod 5$ and $87 \equiv 3 \pmod 7$.

Exercise 3 Note that $17 \equiv 2 \pmod 5$ and $17 \equiv 3 \pmod 7$, so 17 is another solution to the system of equations:

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

We showed that 85 was another solution to the system of equations given above. Why doesn't this violate the uniqueness part of CRT?