Elementary Number Theory

Pelatnas 1 TOKI 2016
Ahmad Zaky (TOMI 2010-2012)
Turfa Auliarachman (TOKI 2015)

Table of Contents

Modular Arithmetic

- $a \equiv b \pmod{m}$ iff $a - b$ is divisible by m

- If $a \equiv c$ and $b \equiv d \pmod{m}$, then
  $a \pm b \equiv c \pm d \pmod{m}$
  $a \times b \equiv c \times d \pmod{m}$
  $a^k \equiv c^k \pmod{m}$ for all integers k
  $\frac{a}{b} \equiv ? \pmod{m}$

Prime Number

- Positive integers which have exactly 2 positive divisors

- 2, 3, 5, 7, …

Primality Testing

- Obvious $O(\sqrt{n})$ loop
- Sieve Eratosthenes ($O(n \log \log n)$)

```
for (int i = 1; i <= MAXN; i++) {
    p[i] = i;
}
for (int i = 2; i * i <= MAXN; i++) {
    if (p[i] == i) {
        for (int j = i * i; j <= MAXN; j += i) {
            p[j] = i;
        }
    }
}
```

  - It is fast; 186ms for $n = 10^7$

Theorems Involving Primes

- Fermat Little Theorem

  $a^p \equiv a \pmod{p}$

  $a^{p-1} \equiv 1 \pmod{p}$ for $a \neq 0 \pmod{p}$

- Wilson's Theorem

  $(n-1)! \equiv -1 \pmod{n}$ if and only if n isprime

Multiplicative Functions

- $f: N \to N$ such that $f(xy) = f(x)f(y)$ for all relatively prime numbers x and y (i.e. $\gcd(x, y) = 1$)

- Obvious example: $f(x) = x$

Sigma, Tau, Phi

- $\sigma(x)$ denotes the *sum* of positive divisors of x
- $\tau(x)$ denotes the *number* of positive divisors of x
- $\phi(x)$ (also called *Euler totient function*) denotes the number of i such that $i \leq x$ and $\gcd(i, x) = 1$

- All of them are multiplicative functions

Sigma, Tau, Phi

Let $x = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$

- $\tau(x) = \prod_{i=1}^{k} (e_i + 1)$
- $\sigma(x) = \prod_{i=1}^{k} \left(\frac{p_i^{e_i+1} - 1}{p_i - 1} \right)$
- $\phi(x) = x \prod_{i=1}^{k} \left(1 - \frac{1}{p_i} \right)$

Euler's Theorem

- $a^{\phi(n)} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$

Euclidean Algorithm

- $\gcd(a, b) = \gcd(b - a, a)$

```
long long gcd(long long a, long long b) {
    if (a == 0) {
        return b;
    }
    else {
        return gcd(b % a, a);
    }
}
```

Extended Euclidean Algorithm

- Find x and y such that $ax + by = \gcd(a, b)$
- Computes sequence of remainders and quotients:
  - $r_0 = a$
  - $r_1 = b$
  - …
  - $r_{i+1} = r_{i-1} - q_i r_i$ and $0 \leq r_{i+1} < |r_i|$

Extended Euclidean Algorithm

- Also maintain two other sequences s_i and t_i

  $s_0 = 1$ $\quad\quad\quad\quad$ $s_1 = 0$

  $t_0 = 0$ $\quad\quad\quad\quad$ $t_1 = 1$

  …

  $s_{i+1} = s_{i-1} - q_i s_i$

  $t_{i+1} = t_{i-1} - q_i t_i$

- We stop when $r_{k+1} = 0$

  $\gcd(a, b) = r_k = a s_k + b t_k$

Extended Euclidean Algorithm

```
pair<long long, long long> extendedEuclid(long long a, long long b){
    long long s = 0, old_s = 1;
    long long t = 1, old_t = 0;
    long long r = b, old_r = a;
    while (r != 0){
        long long quotient = old_r / r, temp;
        // (old_r, r) = (r, old_r - quotient * r)
        temp  = old_r;
        old_r = r;
        r     = temp - quotient * r;
        // (old_s, s) = (s, old_s - quotient * s)
        temp  = old_s;
        old_s = s;
        s     = temp - quotient * s;
        // (old_t, t) = (t, old_t - quotient * t)
        temp  = old_t;
        old_t = t;
        t     = temp - quotient * t;
    }
    return make_pair(old_s, old_t);
}
```

Multiplicative Inverse

- $\frac{a}{b} = a *? \pmod{p}$

- Fermat Little Theorem

  $? = b^{p-2}$

- Extended Euclid

  Find x and y such that $xp + yb = 1$

  $? = y$

Linear Diophantine Equation

- Find x and y satisfying $ax + by = c$

- Solution exists iff c is divisible by $\gcd(a, b)$

- If (x_0, y_0) is a solution, then $\left(x_0 + k\frac{y}{\gcd(x,y)}, y_0 - k\frac{x}{\gcd(x,y)}\right)$ is

Fast Exponentiation

$x^{yz} = (x^y)^z$

$x^{2y} = (x^y)^2$

Matrix Multiplication

M x N

- M -> a x b
- N -> b x c
- MN -> a x c

MN(i,j) $= \sum_{k=1}^{b} M_{ik} N_{kj}$

MN != NM !!!!

Matrix Exponentiation

Misal M_i x N = M_{i+1}

- $M_2 = M_1$ x N
- $M_3 = M_2$ x N = M_1 x N x N = M_1 x N^2
- $M_4 = M_3$ x N = M_1 x N^2 x N = M_1 x N^3

Fast Exponentiation ^.^)9

M_i -> a x b   N -> b x b
N -> b x b M_i -> b x a

M x I = M

I = Matriks identitas = $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Problem: Benefit (UVa11889)

- Given a and c, find the smallest positive integer b such that $lcm(a, b) = c$

Problem: Permasalahan DP (P1 2014)

- If $f(a, b)$ is known, then so is $f(a \times k, b \times k)$
- How many values of f should be calculated to find all $f(a, b), 1 \leq a, b \leq n$?

Problem: Fungsi Haha

- Diketahui haha(0) = x dan haha(1)=y
- Diketahui haha(i) = haha(i-1) – haha(i-2)
- Cari nilai t(n), 0 <= n <= 10^9