OI Math Docs

目录

数论

GCD

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

```
int gcd(int a, int b) {
    return a == 0 ? b : gcd(b, a % b);
}
```

exGCD

求解 $ax+by=\gcd(a,b)$ 的一组特解 $\begin{cases} x=x_0 \\ y=y_0 \end{cases}$。

$$\operatorname{exgcd}(a,b)\to(d,x_0,y_0)$$

```
void exgcd(int a, int b, int &d, int &x, int &y) {
    if (b == 0) d = a, x = 1, y = 0;
    else {
        exgcd(b, a % b, d, x, y);
        int t = x; x = y; y = t - a / b * y;
    }
}
```

二元一次不定方程

求解 $ax+by=c$ 的一组特解 $\begin{cases}x=x_0\\y=y_0\end{cases}$。

$$
\begin{aligned}
& \operatorname{exgcd}(a,b)\to(d,x_0,y_0) \\
\Rightarrow\quad & ax_0+by_0=\gcd(a,b) \\
\Rightarrow\quad & a\frac{x0}{\gcd(a,b)}+b\frac{y0}{\gcd(a,b)}y=1 \\
\Rightarrow\quad & a\frac{x_0c}{\gcd(a,b)}+b\frac{y_0c}{\gcd(a,b)}=c \\
\Rightarrow\quad & \begin{cases}x=\dfrac{x_0c}{\gcd(a,b)}\\ y=\dfrac{y_0c}{\gcd(a,b)}\end{cases}
\end{aligned}
$$

有解条件： $c \bmod \gcd(a,b)=0$。

```
bool linearEquation(int a, int b, int c, int &x, int &y) {
    int d; exgcd(a, b, d, x, y);
    if (c % d) return false;
    int t = c / d;
    x *= t, y *= t;
    return true;
}
```

线性同余方程

求解 $ax \equiv b \pmod c$ 的最小正整数解。

$$
\begin{aligned}
& ax \equiv b \pmod c \\
\Rightarrow \quad & ax + cy = b \\
\Rightarrow \quad & \text{linearEquation}(a, c, b) \to (x, y)
\end{aligned}
$$

有解条件：$b \bmod \gcd(a, c) = 0$。

```
int equiv(int a, int b, int c) {
    int x, y;
    if (linearEquation(a, c, b, x, y)) {
        int t = gcd(a, c);
        return (x % t + t) % t;
    } else return -1;
}
```

逆元

求解 $ax \equiv 1 \pmod p$ 的最小整数解，记 $x = a^{-1}$ 为 a 的逆元。

1. p 为质数时，由费马小定理（$x^p \equiv x \pmod p$）得 $x = a^{-1} = a^{p-2} \bmod p$。

   ```
   #define inv(a, p) qpow(a, p - 2, p)
   ```

2. $\gcd(a, p) = 1$ 时， 解同余方程即可得出。

   ```
   #define inv(a, p) equiv(a, 1, p)
   ```

3. $\gcd(a, p) \neq 1$ 时， a 不存在逆元。

中国剩余定理（CRT)

求解

$$\begin{cases} x \equiv a_1 \pmod {m_1} \\ x \equiv a_2 \pmod {m_2} \\ \quad \vdots \\ x \equiv a_n \pmod {m_n} \end{cases}$$

（m_i 两两互质）的最小整数解。

设 $M=\prod_{i=1}^n m_i$，$M_i=\frac{M}{m_i}$，c_i 为模 m_i 意义下 M_i 的乘法逆元，则方程最小整数解为

$$x=\sum_{i=1}^n c_i M_i a_i \bmod M$$

```
int CRT(int n, int a[], int m[]) {
    int M = 1; for (int i = 1; i <= n; i++) M *= m[i];
    int ans = 0;
    for (int i = 1; i <= n; i++) ans = (ans + inv(M / m[i]) * M
    return ans;
}
```

拓展中国剩余定理（exCRT）

问题同中国剩余定理（CRT），但 m_i 不保证两两互质。

$$
\begin{aligned}
& \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \\
\Rightarrow \quad & \begin{cases} x + y_1 m_1 = a_1 \\ x - y_2 m_2 = a_2 \end{cases} \\
\Rightarrow \quad & y_1 m_1 + y_2 m_2 = a_1 - a_2 \\
\Rightarrow \quad & \text{linearEquation}(m_1, m_2, a_1 - a_2) \to ({y_1}_0, {y_2}_0) \\
\Rightarrow \quad & x \equiv a_1 - y_1 m_1 \pmod{\operatorname{lcm}(m_1, m_2)}
\end{aligned}
$$

```
int exCRT(int n, int a[], int m[]) {
    int A = a[1], M = m[1];
    for (int i = 2; i <= n; i++) {
        if (A < a[i]) swap(A, a[i]), swap(M, m[i]);

        int x, y;
        if (!linearEquation(M, m[i], A - a[i], x, y)) return -1
        A = A - x * M, M = M / gcd(M, m[i]) * m[i];
    }
}
```