OI Math Docs

author: APJifengc

请自行脑补一个毛一探的图片（？）

目录

- 数论
  - GCD
  - exGCD
  - 二元一次不定方程
  - 线性同余方程
  - 逆元
    - 线性求逆元
  - 中国剩余定理（CRT）
  - 拓展中国剩余定理（exCRT）
  - 欧拉函数
    - 性质
    - 线性筛求欧拉函数
    - 欧拉定理
- 组合数学
  - 排列数
  - 组合数
  - 二项式定理
  - 多重组合数
  - Lucas 定理
- 概率与期望
  - 概率
  - 期望

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 $\begin{cases} x=x_0 \\ y=y_0 \end{cases}$。

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

```
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 $\begin{cases} x=x_0 \\ y=y_0 \end{cases}$。

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

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。

线性求逆元

设 $p = k \times i + q \ (r < i, 1 < i < p)$， 则

$$\begin{aligned}
k \times i + r &\equiv 0 && \pmod p \\
k \times r^{-1} + i^{-1} &\equiv 0 && \pmod p \\
i^{-1} &\equiv -k \times r^{-1} && \pmod p \\
i^{-1} &= p - \lfloor \frac{p}{i} \rfloor \times (p \bmod i)^{-1}
\end{aligned}$$

```
inv[1] = 1;
for (int i = 2; i <= n; i++)
    inv[i] = p - (p / i) * inv[p % i] % p;
```

中国剩余定理（CRT）

求解

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

（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 / M[i] * a[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。

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

```
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];
    }
}
```

欧拉函数

性质

1. **定义:** $\varphi(n)$ 为 $x \in [1, n]$ 当中 n 与 x 互质（$\gcd(n, x) = 1$）的个数。
2. **积性函数:** 若 $\gcd(a, b) = 1$，那么$\varphi(a) \times \varphi(b) = \varphi(a \times b)$。
3. 若 n 为质数，则 $\varphi(n) = n - 1$。
4. 若 $x \bmod p^2 \neq 0$，则 $\varphi(x \times p) = \varphi(x) \times (p - 1)$，
   若 $x \bmod p^2 = 0$，则 $\varphi(x \times p) = \varphi(x) \times p$。
5. 设 $x = p_1^{c1} \times p_2^{c2} \times \cdots \times p_n^{c_n}$，则$\varphi(x) = x \times \prod_{i=1}^{n}(1 - \frac{1}{p})$。

```
int phi(int x) {
    int ans = x;
    for (int i = 1; i * i <= x; i++)
        if (x % i == 0) {
            while (x % i == 0) x /= i;
            ans = ans / i * (i - 1);
        }
    if (x > 1) ans = ans / x * (x - 1);
    return ans;
}
```

线性筛求欧拉函数

根据性质4，我们可以用线性筛在 $\mathrm{O}(n)$ 的时间内求出 $x \in [1, n]$ 中的所有 $\varphi(x)$ 值。

```
int pre(int n) {
    for (int i = 2; i <= n; i++) {
        if (!vis[i]) {
            pri[++cnt] = i;
            phi[i] = i - 1;
        }
        for (int j = 1; j <= cnt && i * pri[j] <= n; j++) {
            vis[i * pri[j]] = 1;
            if (i % pri[j] == 0) {
                phi[i * phi[j]] = phi[i] * pri[j];
                break;
            } else phi[i * pri[j]] = phi[i] * (pri[j] - 1);
        }
    }
}
```

欧拉定理

$$x^b \equiv \begin{cases} x^{b \bmod \varphi(p)}, & \gcd(x,p)=1 \\ x^{b \bmod \varphi(p)+\varphi(p)}, & \gcd(x,p)\neq 1, b<\varphi(p) \\ x^b, & \gcd(x,p)\neq 1, b\geq\varphi(p) \end{cases} \pmod p$$

组合数学

排列数

1. $\mathrm{A}_n^m = \dfrac{n!}{(n-m)!}$
2. $\mathrm{A}_n^n = n!$

组合数

1. $\dbinom{n}{m} = \dfrac{\mathrm{A}_n^m}{m!} = \dfrac{n!}{m!(n-m)!}$
2. $\dbinom{n}{m} = \dbinom{n-1}{m} + \dbinom{n-1}{m-1}$
3. $\displaystyle\sum_{i=0}^{n} \binom{n}{i} = 2^n$
4. 将 n 个数分为 m 组（无空组）：$\dbinom{n-1}{m}$

   将 n 个数分为 m 组（有空组）：$\dbinom{n+m-1}{m}$

二项式定理

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

多重组合数

将 n 个数分为 k 组，每组大小为 m_k 的方案数。

$$\binom{n}{m_1, m_2, \cdots, m_k} = \frac{n!}{\prod_{i=1}^{k} m_i}$$

Lucas 定理

$$\binom{a}{b} \bmod p = \binom{a \bmod p}{b \bmod p} \times \binom{\lfloor \frac{a}{p} \rfloor}{\lfloor \frac{b}{p} \rfloor} \bmod p$$

我拒绝写拓展卢卡斯定理

概率与期望

概率

1. $P(X)$ 表示 X 的概率， $P(X|Y)$ 表示 X 在 Y 发生的情况下发生的概率。
2. 独立事件： $P(A\cap B)=P(A)P(B)$
3. 全概率公式： $P(B)=\sum_{i=1}^{n}P(A_i)P(B|A_i)$
4. 贝叶斯公式： $P(B_i|A)=\dfrac{P(B_i)P(A|B_i)}{\sum_{j=1}^{n}P(B_j)P(A|B_j)}$

期望

1. $E(X)$ 表示 X 的期望。

$$E(X)=\sum_{\alpha\in I(X)}\alpha\cdot P(X=\alpha)=\sum_{\omega\in S}X(\omega)P(\omega)$$

2. 全期望公式： $E(Y)=\sum_{\alpha\in I(X)}P(X=\alpha)E(Y|(X=\alpha))$
3. 期望的线性性： $E(aX+bY)=aE(X)+bE(Y)$