同余

李淳风

长郡中学

2024 年 4 月 6 日

定义

若整数 a 和整数 b 除以正整数 m 的余数相等，则称 a,b 模 m 同余，记为 $a \equiv b \pmod{m}$。

一些定理

费马小定理：

一些定理

费马小定理：若 p 是质数，则对于任意正整数 a，有：

$$a^{p-1} \equiv 1 \pmod{p}$$

一些定理

费马小定理：若 p 是质数，则对于任意正整数 a，有：

$$a^{p-1} \equiv 1 \pmod{p}$$

欧拉定理：

一些定理

费马小定理：若 p 是质数，则对于任意正整数 a，有：

$$a^{p-1} \equiv 1 \pmod{p}$$

欧拉定理：若正整数 a,n 互质，则：

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

一些定理

费马小定理：若 p 是质数，则对于任意正整数 a，有：

$$a^{p-1} \equiv 1 \pmod p$$

欧拉定理：若正整数 a,n 互质，则：

$$a^{\phi(n)} \equiv 1 \pmod n$$

欧拉定理推论：

一些定理

费马小定理：若 p 是质数，则对于任意正整数 a，有：

$$a^{p-1} \equiv 1 \pmod{p}$$

欧拉定理：若正整数 a,n 互质，则：

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

欧拉定理推论：对于正整数 a,n，若 $b > \phi(n)$，则有：

$$a^b \equiv a^{(b \bmod \phi(n))+\phi(n)} \pmod{n}$$

最大公约数

若 $a > b$，$\gcd(a, b) = \gcd(a - b, b)$，从而 $\gcd(a, b) = \gcd(a \bmod b, b)$。

最大公约数

若 $a > b$，$\gcd(a, b) = \gcd(a - b, b)$，从而 $\gcd(a, b) = \gcd(a \bmod b, b)$。

简要证明：
令 k 为 a,b 的公约数，则有 $k|a, k|b$，令 $a = xk, b = yk$，则
$a - b = (x - y)k$，有 $k|(a - b)$。
因此所有 a,b 的公约数也是 a-b,b 的公约数。同理可证若 k 是 a-b,b 的公约数，则 k 也是 a,b 的公约数。
因此 $\gcd(a, b) = \gcd(a - b, b)$。

裴蜀定理 (贝祖定理)

对于任意整数 a,b，存在一对整数 x,y，满足 $ax + by = \gcd(a, b)$。

裴蜀定理 (贝祖定理)

对于任意整数 a,b，存在一对整数 x,y，满足 $ax + by = \gcd(a, b)$。
证明过程就是扩展欧几里得算法的过程。

扩展欧几里得算法

在求 $\gcd(a,b)$ 的欧几里得算法的最后一步，即 $b=0$ 时，显然有一对整数 $x=1, y=0$ 满足 $a*1+0*0=\gcd(a,0)$。

扩展欧几里得算法

在求 $\gcd(a,b)$ 的欧几里得算法的最后一步，即 $b=0$ 时，显然有一对整数 $x=1,y=0$ 满足 $a*1+0*0=\gcd(a,0)$。
若 $b>0$，则有 $\gcd(a,b)=\gcd(b,a \bmod b)$。假设有一对整数 x,y，满足 $bx+(a \bmod b)y=\gcd(b,a \bmod b)$。
设 $k=\lfloor\frac{a}{b}\rfloor$，则有 $a \bmod b=a-bk$。
因此 $bx+(a \bmod b)y=bx+(a-bk)y=ay+b(x-ky)$。
令 $x'=y,y'=x-\lfloor\frac{a}{b}\rfloor y$，就得到了 $ax'+by'=\gcd(a,b)$。
应用数学归纳法即可证明裴蜀定理。

扩展欧几里得算法

来看看代码：

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

上述代码求出了方程 $ax + by = \gcd(a, b)$ 的一组特解 x_0, y_0，并返回了最大公约数。

拓展欧几里得方程

对于更加一般的方程 $ax+by=c$，令 $d=\gcd(a,b)$，它有解当且仅当 $d|c$。我们可以先求出 $ax+by=d$ 的一组解 x_0,y_0，乘上 c/d 即可得到原方程的一组解。

拓展欧几里得方程

对于更加一般的方程 $ax + by = c$，令 $d = \gcd(a, b)$，它有解当且仅当 $d|c$。我们可以先求出 $ax + by = d$ 的一组解 x_0, y_0，乘上 c/d 即可得到原方程的一组解。
不难发现，方程通解即为：

$$x = \frac{c}{d}x_0 + k\frac{b}{d}, y = \frac{c}{d}y_0 - k\frac{a}{d}$$

其中 k 为任意整数。

定义

如果一个线性同余方程 $bx \equiv 1 \pmod{p}$，则 x 称为 b 在模 p 意义下的逆元，记作 b^{-1}。
所以若 $b|a$，$a/b \equiv a * b^{-1} \pmod{p}$，因为 $a \equiv a * b^{-1} * b \pmod{p}$。
因此我们可以通过逆元来完成模意义下的除法运算。

求逆元

运用之前的知识，来尝试求逆元

求逆元

运用之前的知识，来尝试求逆元
若 p 是质数，根据费马小定理，我们知道：$b^{p-1} \equiv 1 \pmod p$，即 $b * b^{p-2} \equiv 1 \pmod p$。
此时 b 的逆元为 $b^{p-2} \pmod p$。

求逆元

运用之前的知识，来尝试求逆元
若 p 是质数，根据费马小定理，我们知道：$b^{p-1} \equiv 1 \pmod p$，即 $b * b^{p-2} \equiv 1 \pmod p$。
此时 b 的逆元为 $b^{p-2} \pmod p$。
否则我们需要求解同余方程 $b * x \equiv 1 \pmod p$。

线性同余方程

给出 a,b,p，求一个整数 x 满足 $a * x \equiv b \pmod{p}$，或者无解。

线性同余方程

给出 a,b,p，求一个整数 x 满足 $a * x \equiv b \pmod{p}$，或者无解。
上述方程等价于 $a * x - b$ 是 p 的倍数，所以我们可以将其写作 $a * x + p * y = b$。
根据裴蜀定理，该方程有解当且仅当 $\gcd(a, p) | b$。
有解时可以使用拓展欧几里得算法来求解。

线性同余方程组

设 $m_1, m_2, \cdots, m_n$ 是两两互质的整数，对于 n 个整数 $a_1, a_2, \cdots, a_n$，解方程组：

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

中国剩余定理

中国剩余定理给出了上述方程组的一种特解。
令 $m = \prod_{i=1}^{n} m_i$，$M_i = m/m_i$，$t_i = M_i^{-1} \pmod{m_i}$，则解为：

$$x = \sum_{i=1}^{n} a_i M_i t_i \pmod{m}$$

通解即为 $x + km$。

中国剩余定理

中国剩余定理给出了上述方程组的一种特解。
令 $m = \prod_{i=1}^{n} m_i$，$M_i = m/m_i$，$t_i = M_i^{-1} \pmod{m_i}$，则解为：

$$x = \sum_{i=1}^{n} a_i M_i t_i \pmod{m}$$

通解即为 $x + km$。
中国剩余定理的过程实际上就是在构造 x。
观察 x 求和的 n 个式子，可以发现在模 m_i 的情况下，只有第 i 个式子 $a_i M_i t_i$ 不为零。
而 $a_i M_i t_i \equiv a_i M_i M_i^{-1} \equiv a_i \pmod{m_i}$，因此 x 对每一个同余方程都成立。

其它线性同余方程组

若 $m_1, m_2, \cdots, m_n$ 不再两两互质，又应该如何求解呢?
考虑使用数学归纳法。假设已经求出了前 k-1 个方程的解 x，记 $m = lcm(m_1, m_2, \cdots, m_{k-1})$，则通解为 $x + t * m$。
现在，对于第 k 个同余方程，可以写为 $x + t * m \equiv a_k \pmod{m_k}$。
这是一个线性同余方程，可以使用拓展欧几里得算法求解。
因此，我们使用 n 次拓展欧几里得算法，即可求出方程组的解。

高次同余方程

高次同余方程有两种形式，$a^x \equiv b \pmod p$ 和 $x^a \equiv b \pmod p$。
我们这里解决前者，对后者感兴趣的同学可以去学习原根相关知识。

大步小步法 (BSGS)

问题：给定整数 a,b,p，其中 a,p 互质，求一个非负整数 x，使得 $a^x \equiv b \pmod p$。
大步小步法可以在 $O(\sqrt{n})$ 的复杂度内解决该问题。

大步小步法 (BSGS)

问题：给定整数 a,b,p，其中 a,p 互质，求一个非负整数 x，使得 $a^x \equiv b \pmod p$。
大步小步法可以在 $O(\sqrt{n})$ 的复杂度内解决该问题。
我们令 $t = \lceil \sqrt{p} \rceil$，则我们可以把 x 写为 $i * t - j$，其中 $j < t$。
原方程变为 $a^{i*t-j} \equiv b \pmod p$，即 $a^{i*t} \equiv b * a^j \pmod p$。
由于 i,j 都只有不超过 t 种取值，我们可以先把所有的 $b * a^j \pmod p$ 预处理出来存入哈希表，并逐步计算 a^{i*t} 即 a^{t^i} 的值，判断是否在哈希表中出现过。
若找到了一组合适的 i,j，则说明有解，否则无解。

递推求逆元

对于 $1, 2, \cdots, n$，求每个数在模 p 意义下的逆元。
显然直接求的复杂度是 $O(n \log p)$ 的。

递推求逆元

对于 $1, 2, \cdots, n$，求每个数在模 p 意义下的逆元。
显然直接求的复杂度是 $O(n \log p)$ 的。
首先，1 的逆元是 1。

递推求逆元

对于 $1, 2, \cdots, n$，求每个数在模 p 意义下的逆元。
显然直接求的复杂度是 $O(n \log p)$ 的。
首先，1 的逆元是 1。
我们令 $k = \lfloor \frac{p}{i} \rfloor$，$j = p \bmod i$，有 $p = ki + j$，即 $ki + j \equiv 0 \pmod p$。
我们在等式两边同时乘以 $i^{-1} * j^{-1}$，得到 $kj^{-1} + i^{-1} \equiv 0 \pmod p$。
即 $i^{-1} \equiv -kj^{-1} \pmod p$。因此

$$i^{-1} \equiv -\lfloor \frac{p}{i} \rfloor (p \bmod i)^{-1} \pmod p$$

而 $p \bmod i < i$，因此 $(p \bmod i)^{-1}$ 已经在之前求过了，直接递推就是 $O(n)$ 的复杂度。

递推求逆元

代码也很简单:

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

使用 $p - \lfloor \frac{p}{i} \rfloor$ 来防止出现负数。

线性求任意 n 个数的逆元

如果我们需要快速求任意给定的 n 个数 $a_1, a_2, \cdots, a_n$ 在模 p 下的逆元，就需要其它方法。

线性求任意 n 个数的逆元

如果我们需要快速求任意给定的 n 个数 $a_1, a_2, \cdots, a_n$ 在模 p 下的逆元，就需要其它方法。
首先计算 n 个数的前缀积，记为 $s_1, s_2, \cdots, s_n$。我们首先计算 s_n 的逆元，记为 sv_n。
由于 $sv_n \equiv (a_1 a_2 \cdots a_n)^{-1} = {a_1}^{-1} {a_2}^{-1} \cdots {a_n}^{-1} \pmod p$
因此 $sv_{n-1} \equiv sv_n a_n \pmod p$。
计算出所有的 sv_i 之后，$s_{i-1} * sv_i$ 即为 ${a_i}^{-1}$。
复杂度为 $O(n + \log p)$。

线性求任意 n 个数的逆元

代码也很简短：

```
s[0] = 1;
for (int i = 1; i <= n; ++i) s[i] = s[i - 1] * a[i] % p;
sv[n] = qpow(s[n], p - 2);//使用快速幂求逆元
// 这里也可以使用 exgcd 来求逆元
for (int i = n; i >= 1; --i) sv[i - 1] = sv[i] * a[i] % p;
for (int i = 1; i <= n; ++i) inv[i] = sv[i] * s[i - 1] % p;
```