

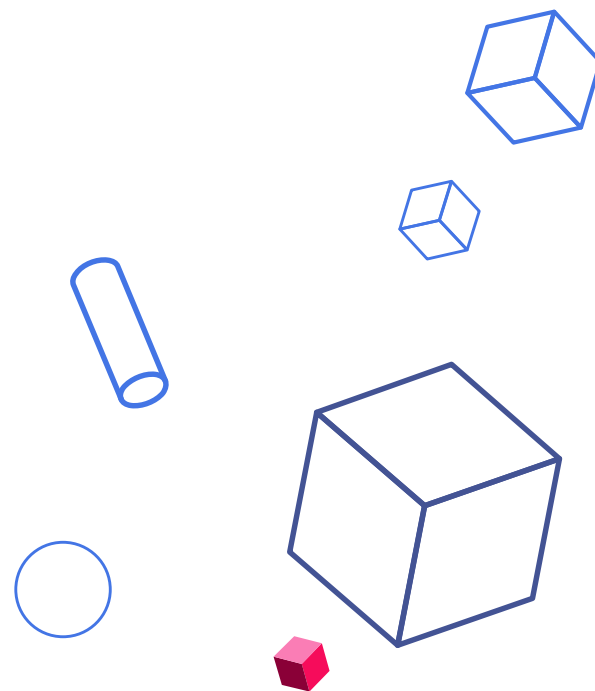
信息学

基础数论三-CRT与BSGS

西南大学附属中学校

信息奥赛教练组

01 线性同余方程组





中国剩余定理(CRT)



西南大学附属中学
High School Affiliated to Southwest University

在我国古代算书《孙子算经》中，记载着这样一个问题：

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”

这个问题通常称为“孙子定理”，民间俗称“韩信点兵”，国外的书籍上把这个定理叫做“中国剩余定理”。这个问题是世界数学史上闻名的问题，涉及到数论中一次同余式组的解法，即求被5除余4，被7除余5，被7除余4的最小正整数。

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

也称“孙子定理”

古人发现：

把 a_i 的变成1，其他的 a 变成0得到解 x
答案就是 $\sum(x * a_i)$

线性同余方程组



中国剩余定理(CRT)



西南大学附属中学
High School Affiliated to Southwest University

对于这样一个 m_i 之间互质的问题，古人给出了一个巧妙的“构造法”进行求解
用现代数学语言描述如下：

我们令 $m = \prod_{i=1}^n m_i$, $M_i = \frac{m}{m_i}$, 设 $t_i \equiv M_i^{-1} \pmod{m_i}$ 。(t_i 为 M_i 模 m_i 意义下的逆元, $M_i t_i \equiv 1 \pmod{m_i}$)

方程组S的通解形式为: $x = a_1 t_1 M_1 + a_2 t_2 M_2 + \cdots + a_n t_n M_n + kM = \sum_{i=1}^n a_i t_i M_i +$

kM , k 属于整数

在模 M 的意义下, 方程组(S)只有一个解: $x = \left(\sum_{i=1}^n a_i t_i M_i \right) \pmod{M}$

证明如下:

因为 $M_i = \frac{m}{m_i}$ 是除了 m_i 之外所有模数的倍数, 所以对于 $\forall k \neq i$, 有 $M_i \equiv 0 \pmod{m_k}$, 也即 $a_i M_i t_i \equiv 0 \pmod{m_k}$ 。

又因为 $a_i M_i t_i \equiv a_i \pmod{m_i}$, 所以如果代入 $x = \sum_{i=1}^n a_i M_i t_i$, 原方程组成立。

可以理解成每个 $a_i M_i t_i$ 只对 i 这个方程有贡献, 对其他方程都没有影响。

证毕。

因为 $\frac{M}{m_i}$ 是除 m_i 之外的所有 m 的倍数
所以 $\forall k \neq i, a_i \frac{M}{m_i} t_i \equiv 0 \pmod{m_k}$
又有 $\frac{M}{m_i} t_i \equiv 1 \pmod{m_i}$
两边同时乘 a_i 得 $a_i \frac{M}{m_i} t_i \equiv a_i \pmod{m_i}$
带入 $x = \sum_{i=1}^n a_i \frac{M}{m_i} t_i$
原方程组成立
——算法竞赛进阶指南

得到一个解 x , 这是一个特解

通解表示为 $x + k \cdot m$

求最小整数解, x 对 m 取模即可

```
11 CRT() {  
    11 ans = 0;  
    11 M = 1;  
    11 x, y;  
    for (int i = 1; i <= t; i++) M *= m[i]; //累乘 $m_i$   
    for (int i = 1; i <= t; i++) {  
        11 Mi = M / m[i];  
        exgcd(Mi, m[i], x, y);  
        x = (x % m[i] + m[i]) % m[i]; //最小非负的解  
        ans = (ans + mul(a[i] * Mi % M, x, M)) % M;  
    }  
    return (ans + M) % M; //防止负数  
}
```

如果 m_i 之间不互质怎么办?



扩展中国剩余定理(exCRT)



西南大学附属中学
High School Affiliated to Southwest University

核心思路：方程两两合并，用扩展欧几里得求解

举个栗子：

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 4 \pmod{6} \end{cases} \Rightarrow x \equiv 10 \pmod{12}$$

$$\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 3 \pmod{5} \end{cases} \Rightarrow x \equiv 28 \pmod{30}$$

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{6} \end{cases} \Rightarrow \emptyset$$

如下几个特点：

- 新方程与原方程具有同样的形式。
- 新方程的模数，是之前两个模数的lcm。
- 可能存在无解的情况

中|信|息|学|竞|赛
High School Affiliated to Southwest University



扩展中国剩余定理(exCRT)



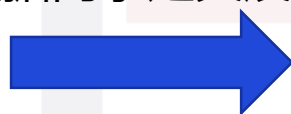
西南大学附属中学
High School Affiliated to Southwest University

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

两两合并:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

根据同余定义展开



$$\begin{cases} x = a_1 + k_1 \times m_1 \\ x = a_2 + k_2 \times m_2 \end{cases} \quad (k_1 \in \mathbb{Z}, k_2 \in \mathbb{Z})$$

联立可得 $a_1 + k_1 \times m_1 = a_2 + k_2 \times m_2$

此基础上移项得 $k_1 \times m_1 - k_2 \times m_2 = a_2 - a_1$

设 $A = m_1, B = m_2, C = a_2 - a_1$

则该式可转换为 $A \times k_1 + B \times k_2 = C$



扩展中国剩余定理(exCRT)



西南大学附属中学
High School Affiliated to Southwest University

$$A \times k_1 + B \times k_2 = C$$

我们可以利用扩展欧几里得算法求解 k_1 ，然后代入求解，得出一组特解 x_0

$$x = x_0 + lcm(m_1, m_2) \times k (k \in \mathbb{Z}) \quad \text{等价于} \quad x \equiv x_0 \pmod{lcm(m_1, m_2)}$$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \xrightarrow{\text{合并}} x \equiv x_0 \pmod{lcm(m_1, m_2)}$$

经过 $n-1$ 次合并，也就是 $n-1$ 次扩欧后，得到：

$$\text{通解式为 } x = x_0 + k \times lcm(m_1, m_2, m_3 \cdots, m_n) (k \in \mathbb{Z})$$



扩展中国剩余定理(exCRT)



西南大学附属中学
High School Affiliated to Southwest University

另一种更数学的证明

前情提示：是一种数学归纳法思想

假设已经求出前 $k-1$ 个方程组成的同余方程组的一个解为 x

且有 $M = \prod_{i=1}^{k-1} m_i$ $M = \text{lcm}\{m_i\}$ ($i \leq k-1$)时也成立

则前 $k-1$ 个方程的方程组通解为 $x + i * M (i \in \mathbb{Z})$

我们就是要求一个正整数 t ，使得 $x + t * M \equiv a_k \pmod{m_k}$

转化一下上述式子得 $t * M \equiv a_k - x \pmod{m_k}$

对于这个式子我们已经可以通过扩展欧几里得求解 t

若该同余式无解，则整个方程组无解，若有，则前 k 个同余式组成的方程组的一个解解为 $x_k = x + t * M$

所以整个算法的思路就是求解 k 次扩展欧几里得



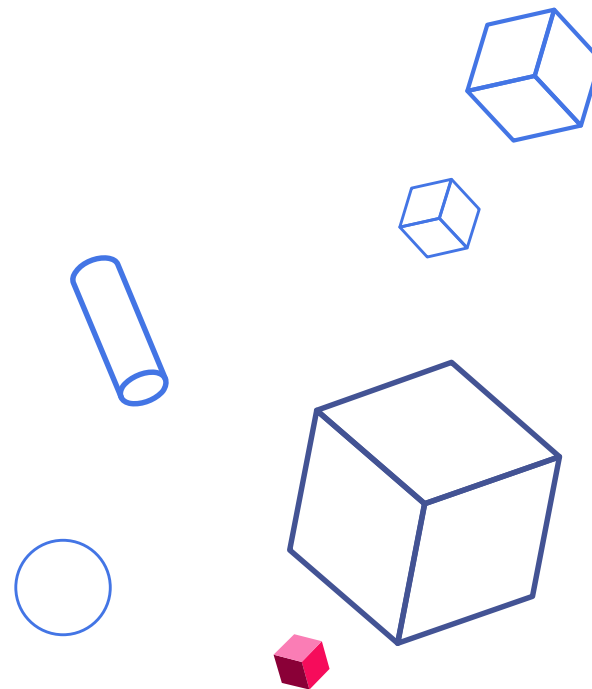
参考代码



西南大学附属中学
High School Affiliated to Southwest University

```
ll excrt()
{
    ll x,y,k;
    ll M=bi[1],ans=ai[1]; //第一个方程的解单独解决
    for(int i=2;i<=n;i++)
    {
        ll a=M,b=bi[i],c=(ai[i]-ans%b+b)%b;// $ax \equiv c \pmod b$ 
        ll gcd=exgcd(a,b,x,y),bg=b/gcd;
        if(c%gcd!=0) return -1; //判断是否无解
        x=((x*c/g)%bg+bg)%bg; //把x转化为最小非负整数解
        //x=mul(x,c/gcd,bg); //避免溢出, 建议使用慢速乘代替
        ans+=x*M; //更新前k个方程组的答案
        M*=bg //M更新, M为前k个方程的lcm
        ans=(ans%M+M)%M;
    }
    return (ans%M+M)%M;
}
```

02 高次同余方程





朴素BSGS



西南大学附属中学
High School Affiliated to Southwest University

求解 $a^x \equiv b \pmod{c}$ 高次同余方程中 x 的算法

朴素的BSGS只能求解 a, c 互质时的情况

当 a, c 互质时，由费马小定理可知，在 x 大于等于 $c-1$ 时会出现循环节，若 x 存在，则 x 必然小于 $c-1$

做法：

当 c 很小时，直接枚举 $0 \sim c-1$ ，检验是否为方程的解

当 c 很大的时候怎么办呢？

把 c 分块来做

西 | 大 | 附 | 中 | 信 | 息 | 学 | 竞 | 赛 |
High School Affiliated to Southwest University



朴素BSGS



西南大学附属中学
High School Affiliated to Southwest University

分块思想的考察可以很简单，也可以很难

这里只是朴素的分块思想

分块一般是分成 $t = \lceil \sqrt{c} \rceil$ 个，每块里有 $\lceil \sqrt{c} \rceil$ 个，这样才能保证 $t * t \geq c$

则， x 可以表示为 $x = t * i + j$

那么

$$a^x \equiv b \pmod{c}$$

代入， $a^{(t*i+j)} \equiv b \pmod{c}$ (t, i 属于正整数， $j < t$)

移项， $a^{(j)} \equiv a^{-(t*i)} * b \pmod{c}$

Baby step: 枚举 $j: 0 \sim t-1$ ，然后把 $a^j \bmod c$ 放入hash表或map中

Giant step: 枚举 $t*i: t \sim c-1$ ，算一下 $a^{-(t*i)} * b$ ，然后找一下hash表或map中有没有这个值
若有得到一组解 (i, j) ， $x = t*i + j$



扩展BSGS(目前仅作了解)



西南大学附属中学
High School Affiliated to Southwest University

利用消因数法, a, c 使得互质

自行学习:

https://blog.csdn.net/sdau_fangshifeng/article/details/81458934

西 | 大 | 附 | 中 | 信 | 息 | 学 | 竞 | 赛 |
High School Affiliated to Southwest University

Thanks

For Your Watching

