

# 初等数论

## 第三章 同余方程

中山大学 数据科学与计算机学院

# 1. 基本概念

- 同余式:

设  $m \in \mathbb{Z}^+$ , 称 **多项式**

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{m}$$

为 **模  $m$  的同余式**, 其中  $a_i \in \mathbb{Z}, i = 1, 2, \cdots, n$ .

如果  $m \nmid a_n$ , 则称  $n$  为  $f(x)$  的 **次数**, 记为  $\deg f$ . 上述同余式就称为 **模  $m$  的  $n$  次同余式**.

如果恰好有  $a \in \mathbb{Z}$ , 使得

$$a_n a^n + a_{n-1} a^{n-1} + \cdots + a_1 a + a_0 \equiv 0 \pmod{m},$$

则这个  $a$  就称为上述同余式的一个解.

可以验证: 如果  $a$  是同余式的一个解, 则所有满足  $a' \equiv a \pmod{m}$  的  $a'$  也都是该同余式的解, 换句话说,  $a$  所在的剩余类

$$C_a = \{a' \mid a \in \mathbb{Z}, a' \equiv a \pmod{m}\}$$

中的任一元素也都满足该同余式。这些解可以看做是相同的, 把他们的全体算作该同余式的一个解。

一般把同余式的解写成模 $m$ 同余的形式, 比如 $x \equiv a \pmod{m}$

当 $a_1, a_2$ 都是同余式的解, 并且他们对模 $m$ 不同余(即 $a_1 \pmod{m}$ 和 $a_2 \pmod{m}$ 是不同的剩余类)时, 才把它们看作是同余式的不同的解。

把所有对模 $m$ 两两不同余的同余式的解的个数, 即满足同余式的模 $m$ 的剩余类的个数, 称为该同余式的解数。

因此,我们只要在模 $m$ 的一组完全剩余系中来解模 $m$ 的同余式即可. 显然, 模 $m$ 同余式的解数至多为 $m$ .

示例:

$$x^5 + x + 1 \equiv 0 \pmod{7}$$

是模7的5次同余式, 因为有

$$2^5 + 2 + 1 \equiv 0 \pmod{7},$$

所以,  $x \equiv 2 \pmod{7}$  是该同余式的一个解.

类似的, 可以检查到  $x \equiv 4 \pmod{7}$  也是该同余式的一个解.

但是,

$$1^5 + 1 + 1 \not\equiv 0 \pmod{7}$$

所以,  $x \equiv 1 \pmod{7}$  不是该同余式的解. 类似地, 还可以检查  $x \equiv 3 \pmod{7}, x \equiv 5 \pmod{7}, x \equiv 6 \pmod{7}, x \equiv 0 \pmod{7}$  都不是该同余式的解.

所以该同余式的解数为2.

# 一次同余式

## 定理

设 $m$ 是正整数,  $a$ 是整数. 一次同余式 $ax \equiv 1 \pmod{m}$ 有解当且仅当 $(a, m) = 1$ , 且在有解时解是唯一的.

**证明:** (存在性) 因为 $(a, m) = 1$ , 所以存在整数 $s$ 和 $t$ 使得

$$sa + tm = 1.$$

两边模 $m$ 可得 $sa \equiv 1 \pmod{m}$ , 即 $x \equiv s \pmod{m}$ 是一次同余式 $ax \equiv 1 \pmod{m}$ 的解.

(唯一性) 如果还有解 $x'$ , 即 $ax' \equiv 1 \pmod{m}$ , 则有

$$a(x' - x) \equiv 0 \pmod{m}.$$

因为 $(a, m) = 1$ , 所以 $x' \equiv x \pmod{m}$ , 解是唯一的.

(必要性) 如果同余式 $ax \equiv 1 \pmod{m}$ 有解 $x \equiv x_0 \pmod{m}$ , 则存在整数 $q$ , 使得 $ax_0 = 1 + qm$ , 即 $ax_0 - qm = 1$ , 所以有 $(a, m) = 1$ .

# 一次同余式

## 定理

设  $m \in \mathbb{Z}^+$ ,  $m \nmid a$ ,  $d = (a, m)$ , 则  $ax \equiv b \pmod{m}$  有解  $\iff d \mid b$ . 且在有解时解数必为  $d$ .

证明: " $\implies$ ": 该同余式有解

$$x \equiv x_0 \pmod{m}$$

也就是说,

$$m \mid (ax_0 - b)$$

所以我们有

$$\left. \begin{array}{l} d \mid m, m \mid (ax_0 - b) \implies d \mid (ax_0 - b) \\ d \mid a \implies d \mid (ax_0) \end{array} \right\} \implies d \mid b$$

" $\impliedby$ ": 设  $d = (a, m)$ , 因为  $\frac{a}{d}$  与  $\frac{m}{d}$  互素, 从而存在  $s, t$  使得

$$s \cdot \frac{a}{d} + t \cdot \frac{m}{d} = 1$$

即

$$\frac{m}{d} \mid \left( \frac{a}{d} \cdot s - 1 \right)$$

从而

$$\frac{m}{d} \mid \left( \frac{a}{d} \cdot s - 1 \right) \cdot \frac{b}{d}$$

即

$$\frac{m}{d} \mid \left( \frac{a}{d} \cdot \left( s \cdot \frac{b}{d} \right) - \frac{b}{d} \right)$$

从而我们有

$$m \mid \left( a \cdot \left( s \cdot \frac{b}{d} \right) - b \right)$$

这说明  $x \equiv s \cdot \frac{b}{d} \pmod{m}$  是

$$ax \equiv b \pmod{m}$$

的一个解.

第一部分证完.

另一方面, 如果同时有两个解:  $x \equiv x_1 \pmod{m}, x \equiv x_2 \pmod{m}$  使得

$$ax_1 \equiv b \pmod{m}, \quad ax_2 \equiv b \pmod{m}$$

所以:

$$a(x_1 - x_2) \equiv 0 \pmod{m}$$

从而(根据:  $a \equiv b \pmod{c}, d|a, d|b, d|c \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{c}{d}}$ )

$$\frac{a}{d} \cdot (x_1 - x_2) \equiv 0 \pmod{\frac{m}{d}}$$

从而

$$x_1 - x_2 \equiv 0 \pmod{\frac{m}{d}} \quad \text{即} \quad x_1 \equiv x_2 \pmod{\frac{m}{d}}$$

即  $x_1 = k \cdot \frac{m}{d} + x_2, k \in \mathbb{Z}$

所以,  $ax \equiv b \pmod{m}$  的全部解就是

$$x \equiv s \cdot \frac{b}{d} + k \cdot \frac{m}{d} \pmod{m}, \quad (k \in \mathbb{Z})$$

即

$$x \equiv s \cdot \frac{b}{d} + k \cdot \frac{m}{d} \pmod{m}, \quad (k = 0, 1, 2, \dots, d-1) \quad \diamond$$



所以,求解一次同余式

$$ax \equiv b \pmod{m}$$

的步骤就是:

- 计算  $d = (a, m)$ ;
- 判断是否  $d \mid b$ , 如果不是则无解;如果整除的话:
- 计算  $\frac{a}{d}, \frac{b}{d}, \frac{m}{d}$ , 和使得  $s \cdot \frac{a}{d} + t \cdot \frac{m}{d} = 1$  的  $s$ ;
- 写出全部的解

$$x \equiv s \cdot \frac{b}{d} + k \cdot \frac{m}{d} \pmod{m}, \quad (k = 0, 1, 2, \dots, d-1)$$

示例:

求解  $33x \equiv 22 \pmod{77}$ , 这里  $a = 33, b = 22, m = 77$

$d = (a, m) = 11$ ,  $d$  能够整除  $b$ , 所以有解.

$$\frac{a}{d} = 3, \frac{b}{d} = 1, \frac{m}{d} = 7$$

$(3, 7) = 1$ , 求出  $3s + 7t = 1$  的  $s = 5$ ;

$$x \equiv s \cdot \frac{b}{d} + k \cdot \frac{m}{d} \pmod{m}, \quad (k = 0, 1, 2, \dots, d - 1) \text{ 即为}$$

$$x \equiv 5 \cdot 2 + k \cdot 7 \pmod{77}, \quad k = 0, 1, 2, \dots, 10$$

因为  $x_1 \equiv x_2 \pmod{\frac{m}{d}}$ , 而  $10 \equiv 3 \pmod{7}$ , 所以结果也可以表示为

$$x \equiv 3 + 7k \pmod{77}, k = 0, 1, 2, \dots, 10,$$

写成  $3, 10, 17, 24, 31, 38, 45, 52, 59, 66, 73$

此外, 根据这个定理,  $(a, m) = 1 \implies ax \equiv 1 \pmod{m}$  有唯一解:

$d = 1$  时,

$$x \equiv s \cdot \frac{b}{d} + k \cdot \frac{m}{d} \pmod{m}, \quad (k = 0, 1, 2, \dots, d - 1)$$

就退化为

$$x \equiv s \cdot b \pmod{m}$$

# 逆元

$m \in \mathbb{Z}^+, a \in \mathbb{Z}$ , 如果存在  $a' \in \mathbb{Z}$  使得

$$aa' \equiv 1 \pmod{m}$$

成立, 则称  $a$  为模  $m$  的可逆元, 或者模  $m$  的乘法逆.

根据前面的结论, 这个乘法逆在模  $m$  的意义下是唯一的, 记作  $a^{-1} \pmod{m}$ .

因此, 求解  $s$  使得  $s \cdot \frac{a}{d} + t \cdot \frac{m}{d} = 1$ , 或使得  $s \cdot \frac{a}{d} \equiv 1 \pmod{\frac{m}{d}}$ , 就是计算  $\frac{a}{d}$  模  $\frac{m}{d}$  的乘法逆.

一次同余式  $ax \equiv b \pmod{m}$  的解就可以表示为

$$x \equiv \left( \left( \frac{a}{d} \right)^{-1} \pmod{\frac{m}{d}} \right) \cdot \frac{b}{d} + k \cdot \frac{m}{d} \pmod{m}$$

类似地, 模  $m$  的简化剩余系也可以用可逆元的概念来表述:

$a$  是模  $m$  的简化剩余  $\iff a$  是模  $m$  的可逆元.

# 孙子定理

求解一次同余方程组问题最早可见于中国南北朝时期（公元5世纪）的数学著作《孙子算经》卷下第二十六题，叫做“物不知数”问题，原文如下：

“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？”

《孙子算经》中首次提到了同余方程组问题，以及以上具体问题的解法，因此在中文数学文献中也会将中国剩余定理称为孙子定理。

宋朝数学家秦九韶于1247年《数书九章》卷一、二《大衍类》对“物不知数”问题做出了完整系统的解答，即“大衍求一术”。这比西方著名数学家高斯在1801年建立的同余理论早554年，被西方称为“中国剩余定理”。

明朝数学家程大位将解法编成易于上口的《孙子歌诀》：“三人同行七十稀，五树梅花廿一支，七子团圆正半月，除百零五使得知”。歌诀给出了模数为3、5、7时候的同余方程的秦九韶解法。意思是：将除以3得到的余数乘以70，将除以5得到的余数乘以21，将除以7得到的余数乘以15，全部加起来后减去105（或者105的倍数），得到的余数就是答案。例如，在以上的物不知数问题里面，按歌诀求出的结果就是23。

## 2. 中国剩余定理(孙子定理)

设 $f_1(x), f_2(x), \dots, f_k(x)$ 是整系数多项式, 我们把含有变量 $x$ 的一组同余式

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1} \\ f_2(x) \equiv 0 \pmod{m_2} \\ \dots\dots\dots \\ f_k(x) \equiv 0 \pmod{m_k} \end{cases}$$

称为是**同余方程组** 如有整数 $c$ 满足

$$\begin{cases} f_1(c) \equiv 0 \pmod{m_1} \\ f_2(c) \equiv 0 \pmod{m_2} \\ \dots\dots\dots \\ f_k(c) \equiv 0 \pmod{m_k} \end{cases}$$

则称 $c$ 是这个同余方程组的解.

令  $m = [m_1, m_2, \dots, m_k]$ , 如果  $c$  是同余方程组的解, 而且  $c' \equiv c \pmod{m}$ , 则  $c' \equiv c \pmod{m_1}$ , 从而  $f_1(c') \equiv f_1(c) \pmod{m_1}$ , 从而  $f_1(c') \equiv 0 \pmod{m_1}$ ,

同样的, 由  $c' \equiv c \pmod{m}$ , 知  $c' \equiv c \pmod{m_2}$ , 从而  $f_2(c') \equiv f_2(c) \pmod{m_2}$ , 从而  $f_2(c') \equiv 0 \pmod{m_2}, \dots, f_k(c') \equiv 0 \pmod{m_k}$ ,

即与  $c$  模  $m$  同余的  $c'$  也满足这个同余方程组. 这样,  $c$  所在的剩余类中的每个元素都是这个同余方程组的解, 它们可以看作是一个解, 记为  $x \equiv c \pmod{m}$ .

只有当  $c_1$  和  $c_2$  都是这个同余式组的解, 且  $c_1$  和  $c_2$  对模  $m$  不同余时, 才把它们看作是这同余式方程组的不同解.

把所有对模  $m$  不同余的解的个数称为是这个同余方程组的解数. 因此, 我们只需要在模  $m$  的一组完全剩余系中来求解这个方程组, 它们的解数至多为  $m$ .

另外, 只要同余方程组中任一同余方程无解, 那么整个方程组自然也无解.

# 中国剩余定理

两两互素的 $m_1, m_2, \dots, m_k \in \mathbb{Z}^+$ ,  $b_1, b_2, \dots, b_k \in \mathbb{Z}$ , 则下面的一次同余方程组有解, 且解在模 $m_1 m_2 \cdots m_k$ 的意义下唯一:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

其解可以如下表示: 令

$$M = m_1 \cdot m_2 \cdot \dots \cdot m_k, \quad M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \dots, M_k = \frac{M}{m_k}$$

$$M'_1 M_1 \equiv 1 \pmod{m_1}, M'_2 M_2 \equiv 1 \pmod{m_2}, \dots, M'_k M_k \equiv 1 \pmod{m_k}$$

解为

$$x \equiv M'_1 M_1 b_1 + M'_2 M_2 b_2 + \dots + M'_k M_k b_k \pmod{M}$$

**唯一性:** 假设 $r$ 与 $s$ 都满足上述同余式组:

$$\begin{cases} r \equiv b_1 \pmod{m_1} \\ r \equiv b_2 \pmod{m_2} \\ \dots\dots \\ r \equiv b_k \pmod{m_k} \end{cases} \quad \begin{cases} s \equiv b_1 \pmod{m_1} \\ s \equiv b_2 \pmod{m_2} \\ \dots\dots \\ s \equiv b_k \pmod{m_k} \end{cases}$$

从而有

$$\begin{cases} r \equiv s \pmod{m_1} \\ r \equiv s \pmod{m_2} \\ \dots\dots \\ r \equiv s \pmod{m_k} \end{cases}$$

从而

$$r \equiv s \pmod{[m_1, m_2, \dots, m_k]}$$

而 $m_1, m_2, \dots, m_k$ 两两互素, 所以

$$r \equiv s \pmod{(m_1 m_2 \dots m_k)},$$

即 $r$ 与 $s$ 在模 $M = m_1 m_2 \dots m_k$ 意义下相等.



存在性: 构造性证明.

$$(m_1, m_2) = 1, (m_1, m_3) = 1, \dots, (m_1, m_k) = 1 \implies (m_1, m_2 m_3 \dots m_k) = 1$$

即  $(m_1, M_1) = 1$ , 从而  $M_1 y \equiv 1 \pmod{m_1}$  有解, 记为  $M'_1$ , 满足  $M'_1 M_1 \equiv 1 \pmod{m_1}$ .  
类似地, 可以构造出

$$M'_2 M_2 \equiv 1 \pmod{m_2}, M'_3 M_3 \equiv 1 \pmod{m_3}, \dots, M'_k M_k \equiv 1 \pmod{m_k}$$

计算整数

$$M'_1 M_1 b_1 + M'_2 M_2 b_2 + M'_3 M_3 b_3 + \dots + M'_k M_k b_k$$

我们可以检查

$$M'_1 M_1 b_1 + M'_2 M_2 b_2 + M'_3 M_3 b_3 + \dots + M'_k M_k b_k \equiv b_1 \pmod{m_1}$$

$$M'_1 M_1 b_1 + M'_2 M_2 b_2 + M'_3 M_3 b_3 + \dots + M'_k M_k b_k \equiv b_2 \pmod{m_2}$$

.....

$$M'_1 M_1 b_1 + M'_2 M_2 b_2 + M'_3 M_3 b_3 + \dots + M'_k M_k b_k \equiv b_k \pmod{m_k}$$

所以  $M'_1 M_1 b_1 + M'_2 M_2 b_2 + M'_3 M_3 b_3 + \dots + M'_k M_k b_k$  是同余方程组的一个解.

又根据唯一性证明知道:

任意两个上述同余方程组的解 $r$ 和 $s$ 模 $M$ 同余, 即一定有 $r \equiv s \pmod{M}$ . 所以该同余方程组的解都可以表达为:

$$x \equiv M'_1 M_1 b_1 + M'_2 M_2 b_2 + M'_3 M_3 b_3 + \dots + M'_k M_k b_k \pmod{M}$$

证完.  $\diamond$

构造性证明可以比较简单地证明中国剩余定理的正确性, 但是如何想到一次同余方程组的解恰好具有

$$M'_1 M_1 b_1 + M'_2 M_2 b_2 + M'_3 M_3 b_3 + \dots + M'_k M_k b_k$$

这种形式, 却并没体现出来。

要理解这一问题, 就必须知道一次同余方程组解的递归表达式, 并理解中国剩余定理的递归证明.

# 两个一次同余方程的中国剩余定理

考虑下面的一次同余方程组:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

其中 $m_1, m_2, \dots, m_k$ 两两互素.

对于同余式 $x \equiv b_1 \pmod{m_1}$ 可以将其解 $x$ 表示为

$$x = b_1 + y_1 m_1 = b_1 + y_1 M_2,$$

其中 $y_1$ 是某一整数,  $M_2 = m_1$ .

把 $x$ 带入同余方程组的第二个同余方程 $x \equiv b_2 \pmod{m_2}$ , 可得

$$b_1 + y_1 \cdot M_2 \equiv b_2 \pmod{m_2} \quad \text{即} \quad y_1 \cdot M_2 \equiv b_2 - b_1 \pmod{m_2}.$$

因为 $(M_2, m_2) = (M_2, M_1) = 1$ , 可以求出整数 $M_2'$ 和 $M_1'$ , 满足

$$M_2' M_2 + M_1' M_1 = 1.$$

即 $M_2' M_2 \equiv 1 \pmod{m_2}$ . 将 $y_1 \cdot M_2 \equiv b_2 - b_1 \pmod{m_2}$ 两端同乘以 $M_2'$ , 可得

$$y_1 \equiv (b_2 - b_1) \cdot M_2' \pmod{m_2}.$$

所以, 同余方程组的解为

$$x = b_1 + ((b_2 - b_1) \cdot M_2' \pmod{m_2}) \cdot M_2 \pmod{m_1 m_2}.$$

这是因为 $x \equiv b_1 \pmod{m_1}$ , 而 $x \equiv b_1 + (b_2 - b_1) \cdot (M_2 \cdot M_2') \equiv b_2 \pmod{m_2}$ .  
同余方程组的解还可以表示为

$$\begin{aligned} x &= b_1 + ((b_2 - b_1) \cdot M_2' + qm_2) \cdot M_2 \\ &= b_1(1 - M_2' M_2) + b_2 M_2' M_2 + qm_2 M_2 \\ &= b_1 M_1' M_1 + b_2 M_2' M_2 + qm_1 m_2. \end{aligned}$$

即 $x \equiv b_1 M_1' M_1 + b_2 M_2' M_2 \pmod{m_1 m_2}$ .

# 中国剩余定理的递归证明（数学归纳法）

仍然考虑下面的一次同余方程组:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

其中 $m_1, m_2, \dots, m_k$ 两两互素.

当 $k = 1$ 时, 设同余式 $x \equiv b_1 \pmod{m_1}$ 的解为 $x \equiv x_1 \equiv b_1 \pmod{m_1}$ .

当 $k = 2$ 时, 原同余方程组等价于

$$\begin{cases} x \equiv b_1 \pmod{N_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

其中 $N_1 = m_1$ .

因为同余式 $x \equiv b_1 \pmod{m_1}$ 的解为 $x \equiv x_1 \equiv b_1 \pmod{m_1}$ , 则存在整数 $y_1$ 使得

$$x = x_1 + y_1 \cdot N_1.$$

把 $x$ 带入同余方程组的第二个同余方程 $x \equiv b_2 \pmod{m_2}$ , 可得

$$x_1 + y_1 \cdot N_1 \equiv b_2 \pmod{m_2} \quad \text{即} \quad y_1 \cdot N_1 \equiv b_2 - x_1 \pmod{m_2}.$$

因为 $(N_1, m_2) = 1$ , 可以求出 $N_1$ 模 $m_2$ 的乘法逆 $N'_1$ , 满足 $N_1 \cdot N'_1 \equiv 1 \pmod{m_2}$ .  
将 $y_1 \cdot N_1 \equiv b_2 - x_1 \pmod{m_2}$ 两端同乘以 $N'_1$ , 可得

$$y_1 \equiv (b_2 - x_1) \cdot N'_1 \pmod{m_2}.$$

所以, 同余方程组的解为

$$x = x_1 + ((b_2 - x_1) \cdot N'_1 \pmod{m_2}) \cdot N_1 \pmod{m_1 m_2}.$$

这是因为 $x \equiv x_1 \pmod{m_1}$ , 而 $x \equiv x_1 + (b_2 - x_1) \cdot (N_1 \cdot N'_1) \equiv b_2 \pmod{m_2}$ .

假设 $k = i - 1 (i \geq 2)$ 时, 命题成立, 即同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv b_{i-1} \pmod{m_{i-1}} \end{cases}$$

有解 $x = x_{i-1} \pmod{m_1 m_2 \cdot m_{i-1}}$ . 对于 $k = i$ , 同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv b_i \pmod{m_i} \end{cases}$$

等价于同余方程组

$$\begin{cases} x \equiv x_{i-1} \pmod{N_{i-1}} \\ x \equiv b_i \pmod{m_i} \end{cases}$$

其中 $N_{i-1} = m_1 m_2 \cdot m_{i-1}$ .

类似于 $k = 2$ 的情形, 因为 $x \equiv x_{i-1} \pmod{N_{i-1}}$ , 则存在整数 $y_{i-1}$ 使得

$$x = x_{i-1} + y_{i-1} \cdot N_{i-1}.$$

把 $x$ 带入同余方程组的第二个同余方程 $x \equiv b_i \pmod{m_i}$ , 可得

$$x_{i-1} + y_{i-1} \cdot N_{i-1} \equiv b_i \pmod{m_i} \quad \text{即} \quad y_{i-1} \cdot N_{i-1} \equiv b_i - x_{i-1} \pmod{m_i}.$$

因为 $(N_{i-1}, m_i) = 1$ , 求出 $N_{i-1}$ 模 $m_i$ 的乘法逆 $N'_{i-1}$ , 满足 $N_{i-1} \cdot N'_{i-1} \equiv 1 \pmod{m_i}$ .  
将 $y_{i-1} \cdot N_{i-1} \equiv b_i - x_{i-1} \pmod{m_i}$ 两端同乘以 $N'_{i-1}$ , 可得

$$y_{i-1} \equiv (b_i - x_{i-1}) \cdot N'_{i-1} \pmod{m_i}.$$

所以, 同余方程组的解为

$$x = x_{i-1} + ((b_i - x_{i-1}) \cdot N'_{i-1} \pmod{m_i}) \cdot N_{i-1} \pmod{m_1 m_2 \cdots m_i}.$$

这是因为 $x \equiv x_{i-1} \pmod{N_{i-1}}$ , 而

$$x \equiv x_{i-1} + (b_i - x_{i-1}) \cdot (N_{i-1} \cdot N'_{i-1}) \equiv b_i \pmod{m_i}.$$



# 中国剩余定理的应用

如果给定的整数 $x$ 是一个很大的数字, 要求计算它模 $M$ 后的值, 可以将 $M$ 分解成两两互素的 $m_1, m_2, \dots, m_k$ 之后, 计算 $x$ 模 $m_1$ 后的值记为 $b_1$ , 计算 $x$ 模 $m_2$ 后的值记为 $b_2$ ,  $\dots$ , 计算 $x$ 模 $m_k$ 后的值记为 $b_k$ , 从而建立一个一次同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

求解这个一次同余式组的解即可得到 $x$ 模 $M$ 后的值.

计算 $2^{1000000} \bmod 77$

$$77 = 7 \times 11$$

$$1000000 = 166666 \times 6 + 4 \implies 2^{1000000} \equiv 2 \bmod 7 \quad \text{即} \quad b_1 = 2$$

$$1000000 = 100000 \times 10 \implies 2^{1000000} \equiv 1 \bmod 11 \quad \text{即} \quad b_2 = 1$$

求解同余式组

$$\begin{cases} y \equiv 2 \bmod 7 \\ y \equiv 1 \bmod 11 \end{cases}$$

对这个同余式组,  $m_1 = 7$ ,  $m_2 = 11$ ,  $M_1 = 11$ ,  $M_2 = 7$ ,  $M = 77$ ,  $M'_1 = 2$ ,  $M'_2 = 8$ , 从而同余式组的解为23, 所以

$$2^{1000000} \bmod 77 = 23.$$

示例: 求解同余式组

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv -1 \pmod{5} \\ x \equiv 2 \pmod{7} \\ x \equiv -2 \pmod{11} \end{cases}$$

$$m_1 = 3, m_2 = 5, m_3 = 7, m_4 = 11, M = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$$

$$M_1 = 5 \cdot 7 \cdot 11, M_2 = 3 \cdot 7 \cdot 11, M_3 = 3 \cdot 5 \cdot 11, M_4 = 3 \cdot 5 \cdot 7$$

$$M'_1 = 1, M'_2 = 1, M'_3 = 2, M'_4 = 2$$

所以同余式组的解为:

$$x \equiv 385 - 231 + 660 - 420 \pmod{1155}$$

即

$$x \equiv 394 \pmod{1155}$$

示例: 求解同余式组

$$\begin{cases} x \equiv b_1 \pmod{5} \\ x \equiv b_2 \pmod{6} \\ x \equiv b_3 \pmod{7} \\ x \equiv b_4 \pmod{11} \end{cases}$$

$$m_1 = 5, m_2 = 6, m_3 = 7, m_4 = 11, M = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$$

$$M_1 = 462, M_2 = 385, M_3 = 330, M_4 = 210$$

$$M'_1 = 3, M'_2 = 1, M'_3 = 1, M'_4 = 1$$

所以同余式组的解为:

$$x \equiv 3 \times 462 \times b_1 + 385 \times b_2 + 330 \times b_3 + 210 \times b_4 \pmod{2310}$$

示例: 求解同余式组 
$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 11 \pmod{20} \\ x \equiv 1 \pmod{15} \end{cases}$$

这里的模数8, 20, 15不是两两互素的, 需要对这个方程组做变形.  
容易看到第二个同余方程等价于方程组:

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 1 \pmod{5} \end{cases}$$

容易看到第三个同余方程等价于方程组:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases}$$

这样要求解同余方程组就等价于求解同余方程组

$$\begin{cases} x \equiv 3 \pmod{8} & (1) \\ x \equiv 3 \pmod{4} & (2) \\ x \equiv 1 \pmod{3} & (3) \\ x \equiv 1 \pmod{5} & (4) \end{cases}$$

$$\begin{cases} x \equiv 3 \pmod{8} & (1) \\ x \equiv 3 \pmod{4} & (2) \\ x \equiv 1 \pmod{3} & (3) \\ x \equiv 1 \pmod{5} & (4) \end{cases}$$

这里可以看到, 满足(1)式的解也一定满足(2)式, 这样, 在上述同余式组中可以不要(2)式, 所以得到一个等价的同余方程组:

$$\begin{cases} x \equiv 3 \pmod{8} & (1) \\ x \equiv 1 \pmod{3} & (3) \\ x \equiv 1 \pmod{5} & (4) \end{cases}$$

这个方程组满足中国剩余定理条件, 可以使用中国剩余定理求解.

这个例子告诉我们在模不两两互素情况下的同余方程组的求解思路.

示例: 求解同余式组

$$\begin{cases} x \equiv 3 \pmod{7} \\ 6x \equiv 10 \pmod{8} \end{cases}$$

这个同余方程组不是中国剩余定理所适用的形式, 但可以将它转换为适用的形式. 考虑同余式  $6x \equiv 10 \pmod{8}$ : 可以看到它确实有解且解数为2:

$$x \equiv -1 \pmod{8} \text{ 和 } x \equiv 3 \pmod{8}$$

这样要求解的同余方程组就相当于要求解两个同余方程组了:

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv -1 \pmod{8} \end{cases}$$

和

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 3 \pmod{8} \end{cases}$$

它们的解分别为  $x \equiv 31 \pmod{56}$ ,  $x \equiv 3 \pmod{56}$ , 原同余方程组的解也就出来了.