

初等数论及其应用

第二章 同余

2.6 中国剩余定理

求解同余方程组的例子

- 本节讨论一次同余方程组的求解. 在代数方程体系中, 两个不同的一元一次方程不可能有公共解, 因此不存在一元一次方程组的求解问题.
- 但对于模不相同的一元一次同余方程组, 该问题有意义, 因为它等价于求满足不同整除条件的整数.
- 韩信点兵问题: 一队1000人以上的士兵, 排成每行3人余2人, 每行5人余1人, 每行7人余6人. 问这队士兵至少有多少人?
- 1091

求解同余方程组的例子

- **例2.5.1** 求满足被3除余2, 被5除余1, 被7除余6的最小正整数.

- **解:** 易知等价求满足如下三个同余方程组的最小正整数:

$$x \equiv 2 \pmod{3}, x \equiv 1 \pmod{5}, x \equiv 6 \pmod{7}$$

由式1知, 存在整数 k 使得 $x = 3k + 2$, 代入式2得:

$$3k + 2 \equiv 1 \pmod{5}, \text{即 } 3k \equiv 4 \pmod{5}$$

它有唯一解 $k \equiv 3 \pmod{5}$.

故存在整数 r 使得 $k = 5r + 3$,

从而 $x = 3(5r + 3) + 2 = 15r + 11$, 代入式3得:

$$15r + 11 \equiv 6 \pmod{7}, \text{即 } 15r \equiv 2 \pmod{7}$$

它有唯一解 $r \equiv 2 \pmod{7}$.

故存在整数 s 使得 $r = 7s + 2$,

从而 $x = 15(7s + 2) + 11 = 105s + 41$, 即要求的解为41.

中国剩余定理

- 关于一般同余方程组的求解, 我们有下面的**中国剩余定理**, 也称为**孙子定理**. 该定理来源于我国古代孙子在大约公元3世纪的数学著作《孙子算经》. 宋代数学家秦九韶在《数书九章》中对此类问题有系统的论述, 称为大衍求一术. 很多数论问题的本质就是中国剩余定理, 这一定理是我国古代数学的辉煌成就!
- **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?
- **解题思路:** 三人同行七十稀, 五树梅花廿一枝, 七子团圆正半月, 除百零五便得知.

中国剩余定理

- 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?

- 解题思路:

三人同行七十稀, 把除以3所得的余数用70乘.

五树梅花廿一枝, 把除以5所得的余数用21乘.

七子团圆正半月, 把除以7所得的余数用15乘.

除百零五便得知, 把上述三个积加起来, 减去105的倍数, 所得的差即为所求.

- 列式为: $2 \times 70 + 3 \times 21 + 2 \times 15 = 233, 233 - 105 \times 2 = 23$

中国剩余定理

- **定理2.5.1(中国剩余定理)** 设 $m_1, m_2, \dots, m_k$ 是 k 个两两互素的正整数, $m = m_1 m_2 \dots m_k$, $M_i = m/m_i$, $1 \leq i \leq k$, 则下面的同余方程组:

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

有唯一解

$$x \equiv \sum_{i=1}^k b_i M_i M'_i \pmod{m}$$

其中 M'_i 满足 $M_i M'_i \equiv 1 \pmod{m_i}$.

中国剩余定理

- 证明: 因为对任意 $1 \leq i, j \leq k$, 当 $i \neq j$ 时 $(m_i, m_j) = 1$,
所以 $(M_i, m_i) = 1$, 于是存在整数 M'_i 使得 $M_i M'_i \equiv 1 \pmod{m_i}$
(考虑最大公因数的线性组合表示: $sM_i + tm_i = 1$).
因为当 $i \neq j$ 时, 显然 $m_j | M_i$,
所以对每个 j ($1 \leq j \leq k$) 有: $\sum_{i=1}^k b_i M_i M'_i \equiv b_j M_j M'_j \equiv b_j \pmod{m_j}$
即 $x \equiv \sum_{i=1}^k b_i M_i M'_i \pmod{m}$ 是同余方程组的解.
下面证解的唯一性. 设 x_1, x_2 是同余方程组的解,
对每个 j ($1 \leq j \leq k$) 有: $x_1 \equiv x_2 \pmod{m_j}$
于是 $x_1 \equiv x_2 \pmod{[m_1, m_2, \dots, m_k]}$.
因为 $m_1, m_2, \dots, m_k$ 两两互素, 所以 $[m_1, m_2, \dots, m_k] = m$,
故 $x_1 \equiv x_2 \pmod{m}$, 即原同余方程组有唯一解.

中国剩余定理

- 例2.5.2 解下面的同余方程组:

$$x \equiv 2 \pmod{3}, \quad x \equiv 1 \pmod{5}, \quad x \equiv 6 \pmod{7}$$

- 解: 直接利用中国剩余定理.

这里 $m_1 = 3, m_2 = 5, m_3 = 7, m = 105,$

$M_1 = 35, M_2 = 21, M_3 = 15.$ 分别解同余方程:

$$35M'_1 \equiv 1 \pmod{3}, \quad 21M'_2 \equiv 1 \pmod{5}, \quad 15M'_3 \equiv 1 \pmod{7}$$

得到:

$$M'_1 \equiv 2 \pmod{3}, M'_2 \equiv 1 \pmod{5}, M'_3 \equiv 1 \pmod{7}$$

于是同余方程组的解为:

$$x \equiv 2 \times 35 \times 2 + 1 \times 21 \times 1 + 6 \times 15 \times 1 \equiv 41 \pmod{105}$$

中国剩余定理

- **注2.5.1** 考虑中国剩余定理的如下推广. 设 m 的标准分解为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, 那么由中国剩余定理知, 下面的同余方程组:

$$x \equiv r_1 \pmod{p_1^{\alpha_1}}$$

$$x \equiv r_2 \pmod{p_2^{\alpha_2}}$$

... ..

$$x \equiv r_k \pmod{p_k^{\alpha_k}}$$

关于模 m 有唯一解. 因此, 对任意的 x ($1 \leq x \leq m$), 如果知道了所有 $p_i^{\alpha_i}$ ($1 \leq i \leq k$) 除 x 的余数 r_i , 则可唯一确定 x 的值.

模不互素的同余方程组

- 上述中国剩余定理中模 $m_1, m_2, \dots, m_k$ 是两两互素的. 因此, 模两两互素的同余方程组, 可以直接由中国剩余定理来求解.
- 下面我们考虑模不互素的情形. 由推论2.1.2知, 当 $(m, n) = 1$, 同余方程:

$$x \equiv b \pmod{mn}$$

的解是同余方程组

$$x \equiv b \pmod{m}, x \equiv b \pmod{n}$$

的解, 反过来也成立. 因此, 模不互素的同余方程组也可以由中国剩余定理来求解.

模不互素的同余方程组

● 例2.5.3 解同余方程组

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$

- 解: 因为 $12 = 3 \times 4$, 且 $(3, 4) = 1$, 所

以原同余方程组与下面的同余方程组同解:

$$x \equiv 3 \pmod{8}, x \equiv 7 \equiv 1 \pmod{3}, x \equiv 7 \equiv 3 \pmod{4}$$

因为 $x \equiv 3 \pmod{8}$ 蕴含 $x \equiv 3 \pmod{4}$ (即满足前式的 x 必满足后式),

所以原同余方程组等价于:

$$x \equiv 3 \pmod{8}, x \equiv 1 \pmod{3}$$

由于 $(3, 8) = 1$, 由中国剩余定理可得 $x \equiv 19 \pmod{24}$,

这里, $m_1 = 8$, $m_2 = 3$, $M_1 = 3$, $M_2 = 8$, $M'_1 = 3$, $M'_2 = 2$. 易知:

$$M_1 M'_1 \equiv 1 \pmod{8}, M_2 M'_2 \equiv 1 \pmod{3}.$$

模不互素的同余方程组

● 例2.5.4 解同余方程组

$$\begin{cases} x \equiv 5 \pmod{8} \\ x \equiv 7 \pmod{12} \end{cases}$$

- 解: 原同余方程组与下面的同余方程组同解:

$$x \equiv 5 \pmod{8}, x \equiv 7 \equiv 1 \pmod{3}, x \equiv 7 \equiv 3 \pmod{4}$$

易得 $x \equiv 5 \pmod{8}$ 与 $x \equiv 3 \pmod{4}$ 没有公共解,

否则存在整数 k, t 使得 $x = 8k + 5 = 4t + 3$,

即 $4k + 1 = 2t$, 产生矛盾.

因此, 原同余方程组无解.

- 由上面的例子可知, 模不互素的同余方程组未必有解. 下面考虑给出模不互素的同余方程组有解的充要条件.

模不互素的同余方程组

● 定理2.5.2 同余方程组

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

有解的**充要条件**是 $(m_1, m_2) | b_1 - b_2$. 如果该方程组有解, 那么它关于模 $[m_1, m_2]$ 只有唯一解.

● 证明: 先证必要性. 设 x_0 是原方程组的一个解, 则有

$$x_0 \equiv b_1 \pmod{m_1}, \quad x_0 \equiv b_2 \pmod{m_2}$$

所以 $m_1 | x_0 - b_1, m_2 | x_0 - b_2$.

由此易得 $(m_1, m_2) | x_0 - b_1, (m_1, m_2) | x_0 - b_2$.

因此, $(m_1, m_2) | (x_0 - b_2) - (x_0 - b_1) = b_1 - b_2$. 即必要性成立.

模不互素的同余方程组

- 证明: 再证充分性. 设 $(m_1, m_2) | b_1 - b_2$,

则由定理2.4.2知, 同余方程: $m_2 y \equiv b_1 - b_2 \pmod{m_1}$ 有解, 不妨设为 t .

于是下面两式成立:

$$m_2 t + b_2 \equiv b_1 \pmod{m_1}, \quad m_2 t + b_2 \equiv b_2 \pmod{m_2}$$

这说明 $m_2 t + b_2$ 是原方程组的一个解.

最后证解的唯一性.

设 x_1, x_2 是原方程组的解, 则有

$$x_1 \equiv x_2 \pmod{m_1}, \quad x_1 \equiv x_2 \pmod{m_2}$$

由此易知 $x_1 - x_2$ 是 m_1, m_2 的公倍数,

于是 $[m_1, m_2] | x_1 - x_2$, 即 $x_1 \equiv x_2 \pmod{[m_1, m_2]}$.

因此, 原方程组关于模 $[m_1, m_2]$ 只有唯一解.

模不互素的同余方程组

- 定理2.5.2可以做如下推广. 对于一般的同余方程组

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

不难证明它有解的**充要条件**是对任意 $1 \leq i, j \leq k$, 都有 $(m_i, m_j) \mid b_i - b_j$. 并且可以证明, 如果上述同余方程组有解, 那么它的解关于模 $[m_1, m_2, \dots, m_k]$ 是唯一的.

课堂练习

- 计算：解同余方程组

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

- 解：直接利用中国剩余定理.

这里 $m_1 = 3, m_2 = 5, m_3 = 7, m = 105, M_1 = 35, M_2 = 21, M_3 = 15$.

分别解同余方程：

$$35M'_1 \equiv 1 \pmod{3}, 21M'_2 \equiv 1 \pmod{5}, 15M'_3 \equiv 1 \pmod{7}$$

$$\text{得到: } M'_1 \equiv 2 \pmod{3}, M'_2 \equiv 1 \pmod{5}, M'_3 \equiv 1 \pmod{7}$$

于是同余方程组的解为：

$$x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \equiv 23 \pmod{105}$$

课堂练习

- 计算: 解同余方程组

$$\begin{cases} x \equiv 6 \pmod{10} \\ x \equiv 10 \pmod{12} \\ x \equiv 1 \pmod{15} \end{cases}$$

- 解: 上述同余方程组等价于:

$$x \equiv 6 \equiv 0 \pmod{2}, x \equiv 6 \equiv 1 \pmod{5}$$

$$x \equiv 10 \equiv 1 \pmod{3}, x \equiv 10 \equiv 2 \pmod{4}$$

$$x \equiv 1 \pmod{3}, x \equiv 1 \pmod{5}$$

由于 $x \equiv 2 \pmod{4}$ 蕴含 $x \equiv 0 \pmod{2}$, 只需解方程组:

$$x \equiv 1 \pmod{3}, x \equiv 2 \pmod{4}, x \equiv 1 \pmod{5}$$

直接由中国剩余定理求得解为:

$$x \equiv 1 \times 20 \times 2 + 2 \times 15 \times 3 + 1 \times 12 \times 3 \equiv 46 \pmod{60}$$

课堂练习

- 计算: 解同余方程组

$$\begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 4 \pmod{7} \end{cases}$$

- 解: 上述方程组等价于:

$$6x \equiv 3 \pmod{5}, 6x \equiv 8 \equiv 1 \pmod{7}$$

这里, 由于 $(3, 5) = 1$ 且 $(2, 7) = 1$, 容易由新方程组推出原方程组.

令 $y = 6x$, 只需求解方程组:

$$y \equiv 3 \pmod{5}, y \equiv 0 \pmod{6}, y \equiv 1 \pmod{7}$$

直接由中国剩余定理求得解为:

$$y \equiv 3 \times 42 \times 3 + 0 \times 35 \times 5 + 1 \times 30 \times 4 \equiv 78 \pmod{210}$$

因此原方程组的解为: $x \equiv 13 \pmod{35}$

课堂练习

- 计算: 解同余方程组

$$7x \equiv 3 \pmod{12}, \quad 10x \equiv 6 \pmod{14}$$

- 解: 易知存在整数 s, t 使得下面两式成立:

$$7x = 12s + 3, \quad 10x = 14t + 6$$

等价为解决不定方程: $60s - 49t = 6$.

由于 $60 \times 9 - 49 \times 11 = 1$,

故该不定方程的特解为 $s_0 = 54, t_0 = 66$.

从而其通解为

$$s = 54 + 49k, t = 66 + 60k$$

将 s 代入 $7x = 12s + 3$ 得到

$$7x = 12(54 + 49k) + 3 = 651 + 12 \times 49k,$$

即 $x = 93 + 12 \times 7k$. 故要求的解为: $x \equiv 93 \equiv 9 \pmod{84}$

课堂练习

- **计算:** 在已知数列1,4,8,10,16,19,21,25,30,43中, 相邻若干数之和能被11整除的数组共有多少组?

- **解:** 该数列各对应项记为 $a_i, i = 1, 2, \dots, 10$. 并记

$$S_k = a_1 + a_2 + \dots + a_k$$

故数列 $S_1, S_2, \dots, S_{10}$ 为

1,5,13,23,39,58,79,104,134,177

它们被11除的余数依次为

1,5,2,1,6,3,2,5,2,1

故 $S_1 \equiv S_4 \pmod{11}, S_1 \equiv S_{10} \pmod{11}, S_4 \equiv S_{10} \pmod{11}, S_2 \equiv S_8 \pmod{11}, S_3 \equiv S_7 \pmod{11}, S_7 \equiv S_9 \pmod{11}, S_3 \equiv S_9 \pmod{11}$

由于 $S_k - S_j (k > j)$ 是数列 $\{a_i\}$ 的相邻项之和

(S_j 若等于零表示1~j的数列之和也能被11整除(此处无))并且当 $S_k \equiv S_j \pmod{11}$ 时,
 $11 | S_k - S_j$, 故符合题目要求的数组共有7组

课堂练习

● **计算:** 对任意正整数 n , 求 n^{100} 的最后三位数字?

● **解:** 设 n 的个位数字为 m , 则

$$n^{100} \equiv (10k + m)^{100} \equiv m^{100} \pmod{1000}. \quad (\text{提示: 二项式分解定理})$$

若 $m = 0$, 则答案为000;

若 $m = 5$, 则有 $5^{100} \equiv 1 \pmod{8}$, $5^{100} \equiv 0 \pmod{125}$, 解同余方程组
 $x \equiv 1 \pmod{8}$, $x \equiv 0 \pmod{125}$, 根据中国剩余定理得解为 $x \equiv 625 \pmod{1000}$,

若 $5 \nmid m$, 由欧拉定理得 $m^{\phi(125)} = m^{100} \equiv 1 \pmod{125}$,

又当 $m = 1, 3, 7, 9$ 时, 有 $m^{100} \equiv 1 \pmod{8}$, 答案为001

当 $m = 2, 4, 6, 8$ 时, 有 $m^{100} \equiv 0 \pmod{8}$, 答案为376

总结

- **定理2.5.1(中国剩余定理)** 设 $m_1, m_2, \dots, m_k$ 是 k 个两两互素的正整数, $m = m_1 m_2 \dots m_k$, $M_i = m/m_i$, $1 \leq i \leq k$, 则下面的同余方程组:

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

有唯一解

$$x \equiv \sum_{i=1}^k b_i M_i M'_i \pmod{m}$$

其中 M'_i 满足 $M_i M'_i \equiv 1 \pmod{m_i}$.

总结

- **定理2.5.2** 同余方程组

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

有解的**充要条件**是 $(m_1, m_2) | b_1 - b_2$. 如果该方程组有解, 那么它关于模 $[m_1, m_2]$ 只有唯一解.