第 3 章　同余方程

在数学的浩瀚星空中，同余理论犹如一颗璀璨的星辰，它不仅连接了代数与数论的桥梁，还深刻揭示了整数间的一种特殊等价关系——同余关系. 同余方程，作为这一理论的核心内容，是研究整数在给定模数下的等价类性质的重要工具. 它不仅是初等数论的基石，也是密码学、信息安全、计算机科学等领域不可或缺的理论基础.

本章从最基础最重要的一次同余方程入手，通过辗转相除法（欧几里德算法）求解最大公约数，并结合线性同余关系，有效找到一次同余方程的所有解或判断其无解. 这一过程不仅展示了数学方法的精妙，为处理整数问题提供了新的视角和方法，也为后续更复杂问题的求解奠定了基础. 而对于由多个一次同余方程组成的方程组，著名的中国剩余定理提供了强大的求解工具. 不仅在理论上具有重要意义，其应用也广泛涉及密码学、信息安全、计算机科学等多个领域. 另一方面，随着方程次数的提升，同余方程的求解复杂度显著增加. 二次同余方程的求解，涉及到平方剩余与平方非剩余的概念、勒让得符号的判定、二次互反定律的深刻内涵，以及雅可比符号的推广应用. 这些理论不仅丰富了同余方程的理论体系，也展现了数学逻辑之美和解决问题的巧妙思路. 而对于更高次的同余方程，其解的存在性、解的个数以及求解方法变得更为复杂，但同时高次同余方程求解的相关结果也给我们以宏观的指导、一般性思想启迪和独特求解技巧的绝妙呈现.

总之，同余方程及其求解方法是数论中极具魅力和挑战性的领域之一. 从一次同余方程的基础求解，到一次同余方程组的中国剩余定理，再到二次及高次同余方程的深入探索，每一步都蕴含着数学智慧的火花，引领我们不断前行，在数学的海洋中遨游，发现更多未知的美丽与奥秘.

本章的知识要点：

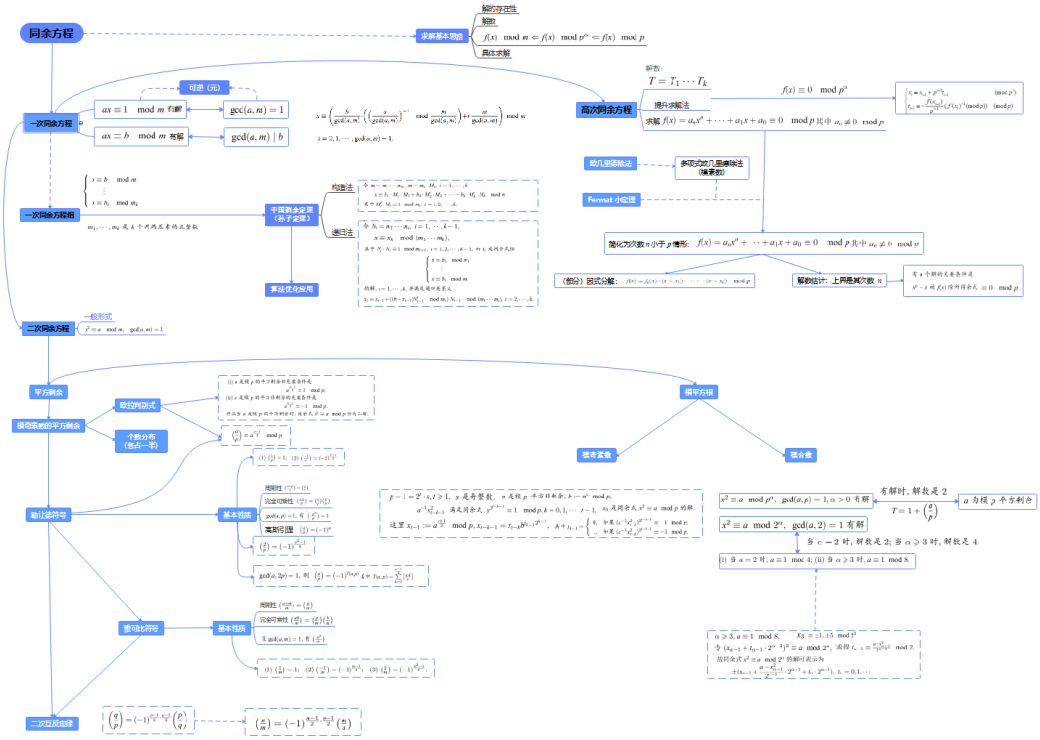

图 3-1 同余方程知识点图谱

3.1 一次同余方程

3.1.1 同余方程的基本概念

在第二章我们引入了同余的概念，现在考虑在模 m 的情况下多项式的求解（即同余方程）的基本概念.

定义 3.1.1 (*i*) 设 m 是一个正整数，设 $f(x)$ 为多项式

$$f(x)=a_n x^n+\cdots+a_1 x+a_0$$

其中 a_i 是整数，则

$$f(x)\equiv 0 \pmod m$$

叫做 m 的**同余方程**. 若 $a_n \not\equiv 0 \pmod m$，则 n 叫做 $f(x)$ 的**次数,** 记为 $\deg f$. 此时，该式又叫做模 m 的 n **次同余方程,** $a_n \bmod m$ 称为其**首项系数**.

(*ii*) 如果整数 a 使得

$$f(a)\equiv 0 \pmod m$$

成立，则 a 叫做同余方程 $f(x)\equiv 0 \pmod m$ 的**解**. 此时，满足 $x\equiv a \pmod m$ 的所有整数都使得同余方程 $f(x)\equiv 0 \pmod m$ 成立，即 a 所在剩余类

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

中的每个剩余都使得同余方程 $f(x)\equiv 0 \pmod m$ 成立. 因此，同余方程 $f(x)\equiv 0 \pmod m$ 的解 a 通常写成

$$x\equiv a \pmod m .$$

(*iii*) 在模 m 的完全剩余系中，使得同余方程成立的剩余个数叫做同余方程的**解数**.

例 3.1.1 同余方程 $2x^4+x^3+2\equiv 0 \pmod 7$ 是首项系数为 2 的模 7 的四次同余方程. 而 $x\equiv 2 \pmod 7$ 是该同余方程的解. 事实上，我们有

$$2\cdot 2^4+2^3+2 \equiv 4+1+2 \equiv 0 \pmod 7.$$

而其他剩余均不满足，故解数为 1.

注: 如例 3.1.1 所示，当模 m 比较小时，我们可以依次将剩余代入验算是否满足来求解同余方程. 但对于一般的模 m，我们需要探索新的求解思路. 下面我们将针对一次、二次和高次同余方程，分别介绍其求解及相关结果.

3.1.2 一次同余方程求解

首先，考虑常数项为 1 的一次同余方程的求解，我们有下面的结果.

定理 3.1.1 设 m 是一个正整数，a 是满足 $m\nmid a$ 的整数. 则一次同余方程

$$ax \equiv 1 (\mathrm{mod}\, m)$$

有解的充分必要条件是 $(a,m)=1$. 而且，当同余方程有解时，其解是唯一的.

证：充分性.

(存在性) 因为 $(a, m) = 1$, 根据广义欧几里德除法或贝祖等式 (定理 1.2.4)，可得到整数 s, t 使得 $s\cdot a+t\cdot m = (a, m) = 1$. 因此，$x\equiv s \pmod m$ 是同余方程 $ax \equiv 1 (\mathrm{mod}\, m)$ 的解.

(唯一性) 若还有解 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. 若同余方程 $ax \equiv 1 (\mathrm{mod}\, m)$ 有解, 不妨设为 $x\equiv x_0 \pmod m$, 则存在整数 q 使得 $a\cdot x_0 = 1+q\cdot m$. 根据定理 1.2.5，有 $(a, m) = 1$.

定义 3.1.2 设 m 是一个正整数，a 是一个整数. 如果存在整数 a' 使得

$$aa' \equiv 1 (\mathrm{mod}\, m)$$

成立，则 a 叫做模 m **可逆元**. 这时 a' 叫做 a 的模 m **逆元**，记作 $a' \equiv a^{-1} (\mathrm{mod}\, m)$.

根据定理 3.1.1，在模 m 的意义下，a' 是唯一存在的.

现在我们给出模简化剩余的一个等价描述.

定理 3.1.2 设 m 是一个正整数. 则整数 a 是模 m 简化剩余的充要条件是整数 a 是模 m 可逆元.

证 必要性. 如果整数 a 是模 m 简化剩余，则 $(a,m)=1$.

根据定理 3.1.1，存在整数 a' 使得 $aa' \equiv 1 (\mathrm{mod}\, m)$

因此，由定义 3.1.2, a 是模 m 逆元.

充分性. 如果 a 是模 m 可逆元，则存在整数 a' 使得 $aa' \equiv 1 (\mathrm{mod}\, m)$

即同余方程 $ax \equiv 1 (\mathrm{mod}\, m)$

有解 $x \equiv a' (\mathrm{mod}\, m)$.

根据定理 3.1.1，有 $(a,m) \mid 1$. 从而，$(a,m)=1$.

因此，整数 a 是模 m 简化剩余.

其次，考虑通常的一次同余方程的求解. 实际上，一次同余方程求解的思路是:

$$(a, m)=1,\ ax \equiv 1 (\mathrm{mod}\, m).$$

↓

$(a, m)=1,\ ax \equiv b(\mathrm{mod}\, m)$.

↓

$ax \equiv b(\mathrm{mod}\, m)$.

我们有以下结果.

定理 3.1.3 设 m 是一个正整数，a 是满足 $m\nmid a$ 的整数. 则一次同余方程

$$ax \equiv b(\mathrm{mod}\, m)$$

有解的充分必要条件是 $(a,m)\mid b$. 而且，当该同余方程有解时，其解为

$$x \equiv \frac{b}{(a,m)} \cdot \left(\left(\frac{a}{(a,m)} \right)^{-1} (\mathrm{mod} \frac{m}{(a,m)}) \right) + t \frac{m}{(a,m)} (\mathrm{mod}\, m),$$

$t = 0,1,\cdots,(a,m)-1$.

证 必要性. 设同余方程 $ax \equiv b(\mathrm{mod}\, m)$ 有解 $x \equiv x_0 (\mathrm{mod}\, m)$，即存在整数 y_0 使得

$$ax_0 - my_0 = b.$$

因为 $(a,m)\mid a,(a,m)\mid m,$ 所以根据定理 1.1.3,

$$(a,m)\mid ax_0 - my_0 = b.$$

因此，必要性成立.

充分性. 设 $(a,m)\mid b$，则 $\frac{b}{(a,m)}$ 为整数.

首先，考虑同余方程 $\frac{a}{(a,m)} x \equiv 1\ (\mathrm{mod} \frac{m}{(a,m)})$

因为 $(\frac{a}{(a,m)}, \frac{m}{(a,m)}) = 1$,

由定理 3.1.1，存在整数 x_0 (或运用广义欧几里德除法求出该整数 x_0),

使得同余方程 $\frac{a}{(a,m)} x \equiv 1\ (\mathrm{mod} \frac{m}{(a,m)})$ 成立. 而且有唯一解

$$x \equiv x_0\ (\mathrm{mod} \frac{m}{(a,m)}).$$

事实上，如果同时有同余方程

$$\frac{a}{(a,m)} x \equiv 1\ (\mathrm{mod} \frac{m}{(a,m)}) \text{ 和 } \frac{a}{(a,m)} x_0 \equiv 1\ (\mathrm{mod} \frac{m}{(a,m)})$$

成立，两式相减得到

$$\frac{a}{(a,m)}(x-x_0)\equiv 0 \pmod{\frac{m}{(a,m)}}.$$

因为$(\frac{a}{(a,m)},\frac{m}{(a,m)})=1$，我们立即得到

$$x\equiv x_0 \pmod{\frac{m}{(a,m)}}.$$

其次，写出同余方程

$$\frac{a}{(a,m)}x\equiv\frac{b}{(a,m)} \pmod{\frac{m}{(a,m)}}$$

的唯一解 $x\equiv x_1\equiv x_0\frac{b}{(a,m)}(\bmod m)$，

而且，该解是同余方程$ax\equiv b(\bmod m)$的一个特解.

最后，写出同余方程$ax\equiv b(\bmod m)$的全部解：

$$x\equiv x_1+t\frac{m}{(a,m)}(\bmod m),\quad t=0,1,\cdots,(a,m)-1.$$

事实上，如果同时有同余方程

$$ax\equiv b(\bmod m)\text{和}ax_1\equiv b(\bmod m)$$

成立. 两式相减得到

$$a(x-x_1)\equiv 0(\bmod m).$$

根据性质 2.1.5 和性质 2.1.3，这等价于

$$x\equiv x_1 \pmod{\frac{m}{(a,m)}}.$$

因此，同余方程$ax\equiv b(\bmod m)$的全部解可写成

$$x\equiv x_1+t\frac{m}{(a,m)}(\bmod m),\quad t=0,1,\cdots,(a,m)-1.$$

例 3.1.2 求解一次同余方程

$$39x\equiv 65 \pmod{91}$$

解 首先，计算最大公因数 (39, 65) = 13，并且有 (39, 65) | 91，

所以原同余方程有解.

其次，运用广义欧几里德除法，求出同余方程 $3x\equiv 1 \pmod 7$

的一个解$x_0'\equiv 5(\bmod 7)$.

第三，写出同余方程 $3x \equiv 5 \pmod 7$

的一个特解 $x_0 \equiv 5 \cdot x_0' \equiv 5 \cdot 5 \equiv 4 \pmod 7$.

最后，写出原同余方程的全部解

$$x \equiv 4+t\frac{91}{(39,91)} \equiv 4+7t \pmod{91},\ t = 0, 1, \cdots, 12$$

或者

$$x \equiv 4, 11, 18, 25, 32, 39, 46, 53, 60, 67, 74, 81, 88 \pmod{91}.$$

3.2 中国剩余定理

3.2.1 同余方程组

定理 3.2.1 设 $m_1, \cdots, m_k$ 是 k 个两两互素的正整数，$m = m_1 \cdots m_k$. 则同余方程

$$f(x) \equiv 0 \pmod m \tag{3.2.1}$$

与同余方程组

$$\begin{cases} f(x) \equiv 0 \pmod{m_1} \\ \cdots\cdots \\ f(x) \equiv 0 \pmod{m_k} \end{cases} \tag{3.2.2}$$

等价.

证 设 x_0 是同余方程(3.2.1)的解，则

$$f(x_0) \equiv 0 \pmod m$$

根据性质 2.1.6，我们有

$$f(x_0) \equiv 0 \pmod{m_i}, \quad i = 1, \cdots, k.$$

即 x_0 是同余方程组(3.2.2)的解.

反过来，设

$$f(x_0) \equiv 0 \pmod{m_i}, \quad i = 1, \cdots, k$$

根据性质 2.1.7，我们有

$$f(x_0) \equiv 0 \pmod m.$$

即同余方程组(3.2.2)的解 x_0 也是同余方程(3.2.1)的解.

3.2.2 中国剩余定理及其证明

关于中国剩余定理或孙子定理，其最早见于《孙子算经》的**“物不知数”**题：

“今有物不知其数，三三数之有二，五五数之有三，七七数之有二，问物有多少？”

答案：二十三.

解答过程为：三三数之有二对应于一百四十，五五数之有三对应于六十三，七七数之有二对应于三十，将这些数相加得到二百三十三，再减去二百一十，即得数之数二十三.

将“物不知数”问题用同余方程组表示就是：

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

而解答过程就为：

$$2\cdot 5\cdot 7\cdot 2 = 140, \qquad 1\cdot 3\cdot 7\cdot 3 = 63,$$
$$1\cdot 3\cdot 5\cdot 2 = 30, \qquad 2\cdot 3\cdot 5\cdot 7 = 210,$$
$$140 + 63 + 30 = 233, \quad 233 - 210 = 23$$

在“数不知数”问题中，如果我们将

3，5，7 分别看作模 m_1, m_2, m_3；　　2，3，2 分别看作 b_1, b_2, b_3；

$5\cdot 7$，$3\cdot 7$，$3\cdot 5$ 分别看作 M_1，M_2，M_3；

2，1，1 分别看做 M_1'，M_2'，M_3'；

233 作为所构造的整数；105 作为模 $m = m_1 \cdot m_2 \cdot m_3$.

则它们满足同余方程：$M_i' \cdot M_i \equiv 1 (\mathrm{mod}\, m_i)$，$i = 1, 2, 3$

和 $x \equiv M_1' \cdot M_1 b_1 + \cdots + M_k' \cdot M_k b_k \pmod m$.

现在我们考虑“物不知数”问题的推广形式，即非常重要的中国剩余定理或孙子定理.

定理 3.2.1（中国剩余定理） 设 $m_1, \cdots, m_k$，是 k 个两两互素的正整数，则对任意的整数 $b_1, \cdots, b_k$，同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \cdots\cdots \\ x \equiv b_k \pmod{m_k} \end{cases} \tag{3.2.3}$$

一定有解，且解是唯一的，即

（i）若令 $m = m_1 \cdots m_k$，$m = m_i M_i$，$i = 1, \cdots, k$，

则同余方程组 (3.2.3) 的解可表示为：

$$x \equiv M_1' \cdot M_1 b_1 + \cdots + M_k' \cdot M_k b_k \pmod m$$

其中 $M_i' \cdot M_i \equiv 1 (\mathrm{mod}\, m_i), \quad i = 1, 2, \cdots, k$

（*ii*）若令 $N_i = m_1 \cdots m_i, \quad i = 1, \cdots, k-1$,

则同余方程组(3.2.3)的解可表示为：$x \equiv x_k (\mathrm{mod}\, m_1 \cdots m_k)$,

其中 $N_i' N_i \equiv 1 (\mathrm{mod}\, m_{i+1}), \quad i = 1, 2, \cdots, k-1,$

而 x_i 是同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \cdots\cdots \\ x \equiv b_i \pmod{m_i} \end{cases}$$

的解，$i = 1, 2, \cdots, k,$ 并满足递归关系式

$$x_i \equiv x_{i-1} + N_{i-1}(N_{i-1}^{'}(b_i - x_{i-1})(\mathrm{mod}\, m_i))(\mathrm{mod}\, m_1 \cdots m_i) \quad i = 2, \cdots, k\ .$$

证 （*i*）构造法证明.

首先，证明解的存在性.

直接构造同余方程组的解：根据假设条件，

对任意给定的 $i, 1 \le j \le k,\ j \ne i$ 我们有

$$(m_i, m_j) = 1, 1 \le j \le k,\ j \ne i\ .$$

又根据推论 1.2.1，有 $(m_i, M_i) = 1.$

再运用广义欧几里德除法，可分别求出整数 $M_i', i = 1, 2, \cdots, k,$ 使得

$$M_i' M_i \equiv 1 (\mathrm{mod}\, m_i), \quad i = 1, 2, \cdots, k$$

这样，我们构造出一个如下的整数，即

$$x \equiv M_1' \cdot M_1 b_1 + \cdots + M_k' \cdot M_k b_k \ (\mathrm{mod}\, m)$$

因为 $m = m_i M_i$ 及 $m_i \mid M_j, \quad 1 \le j \le k,\ j \ne i,$

所以，这个整数 x 满足同余方程

$$x \equiv M_i' \cdot M_i b_i \equiv b_i \ (\mathrm{mod}\, m_i), \quad i = 1, \cdots, k$$

即，$x \equiv M_1' \cdot M_1 b_1 + \cdots + M_k' \cdot M_k b_k \ (\mathrm{mod}\, m)$ 是同余方程组(3.2.3)的解.

其次，证明解的唯一性.

设 x, x' 都是满足(3.2.3)的解，则

$$x \equiv b_i \equiv x' (\mathrm{mod}\, m_i), \quad i = 1, \cdots, k$$

因为 $m_1, \cdots, m_k$ 是两两互素的正整数，根据性质 2.1.7，我们得到

$$x \equiv x' (\mathrm{mod}\, m)\ .$$

（*ii*）递归法证明.

k=1 时，同余方程 $x \equiv b_1 \pmod{m_1}$ 的解为

$$x \equiv x_1 \equiv b_1 \pmod{m_1}.$$

k=2 时，原同余方程组等价于

$$\begin{cases} x \equiv b_1 \pmod{N_1} \\ x \equiv b_2 \pmod{m_2} \end{cases} \tag{3.2.4}$$

由同余方程组(3.2.4)的第一个同余方程有解 $x \equiv x_1 \equiv b_1 \pmod{N_1}$，其中 $N_1=m_1$，我们可以将同余方程组的解表示为（y_1 待定参数） $x = x_1 + N_1 y_1$.

将 *x* 代入同余方程组(3.2.4)的第二个同余方程，我们有

$$x_1 + N_1 y_1 \equiv b_2 \pmod{m_2}$$

或

$$N_1 y_1 \equiv b_2 - x_1 \pmod{m_2} \tag{3.2.5}$$

运用广义欧几里德除法，对整数 N_1 及模 m_2，可求出整数 N_1' 使得

$$N_1' N_1 \equiv 1 \pmod{m_2}.$$

将同余方程(3.2.5)的两端同乘 N_1'，我们有 $y_1 \equiv N_1'(b_2 - x_1) \pmod{m_2}$.

故同余方程组(3.2.4)的解为

$$x = x_2 = x_1 + N_1(N_1'(b_2 - x_1) \pmod{m_2}) \pmod{m_1 m_2}.$$

假设 $i-1 (i \geq 2)$ 时，结论成立，即

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

有解 $x \equiv x_{i-1} \pmod{m_1 \cdots m_{i-1}}$.

对于 *i*，同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \cdots\cdots \\ x \equiv b_i \pmod{m_i} \end{cases}$$

等价于同余方程组

$$\begin{cases} x \equiv x_{i-1} \pmod{N_{i-1}} \\ x \equiv b_i \pmod{m_i} \end{cases} \tag{3.2.6}$$

类似于 *k*=2 的情形，由同余方程组(3.2.6)的第一个同余方程有解

$$x \equiv x_{i-1} \pmod{N_{i-1}},$$

我们可以将同余方程组的解表示为（y_{i-1} 待定参数）$x = x_{i-1} + N_{i-1}y_{i-1}$.

将 x 代入同余方程组(3.2.6)的第二个同余方程，我们有

$$x_{i-1} + N_{i-1}y_{i-1} \equiv b_i \pmod{m_i}$$

或

$$N_{i-1}y_{i-1} \equiv b_i - x_{i-1} \pmod{m_i} \tag{3.2.7}$$

运用广义欧几里德除法，对整数 N_{i-1} 及模 m_i，求出整数 N_{i-1}' 使得

$$N_{i-1}'N_{i-1} \equiv 1 \pmod{m_i}.$$

将同余方程(3.2.7)的两端同乘 N_{i-1}'，我们有

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

故同余方程组(3.2.5)的解为

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

根据数学归纳法原理，结论成立.

例 3.2.1 求解同余方程组

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

解 令 $m = 5 \cdot 6 \cdot 7 \cdot 11 = 2310,$

$$\begin{aligned} M_1 &= 6 \cdot 7 \cdot 11 = 462, \quad M_2 = 5 \cdot 7 \cdot 11 = 385, \\ M_3 &= 5 \cdot 6 \cdot 11 = 330, \quad M_4 = 5 \cdot 6 \cdot 7 = 210 \end{aligned}.$$

分别求解同余方程

$$M_i'M_i \equiv 1 \pmod{m_i}, \quad i = 1,2,3,4.$$

得到

$$M_1' = 3, \quad M_2' = 1, \quad M_3' = 1, \quad M_4' = 1.$$

故同余方程组的解为

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

例 3.2.2 韩信点兵：有兵一队，若列成五行纵队，则末行一人；成六行纵队，则末行五人；成七行纵队，则末行四人，成十一行纵队，则末行十人，求兵数.

解 韩信点兵问题可转化为同余方程组

$$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 5 \pmod 6 \\ x \equiv 4 \pmod 7 \\ x \equiv 10 \pmod{11} \end{cases}$$

解一 对 $b_1 = 1,\ \ b_2 = 5,\ \ b_3 = 4,\ \ b_4 = 10$ 应用例 1，得到

$$\begin{aligned} x &\equiv 3 \cdot 462 + 385 \cdot 5 + 330 \cdot 4 + 210 \cdot 10 \\ &\equiv 6731 \\ &\equiv 2111 \pmod{2310} \end{aligned} .$$

解二 归纳构造同余方程的解.

令 $N_1 = 5$，同余方程组的第一个同余方程有解 $x \equiv x_1 \equiv 1 \pmod 5$，

我们将同余方程组的解表示为（y 待定参数）$x=1+5y$.

将 x 代入同余方程组的第二个同余方程，我们有

$1 + 5y \equiv 5 \pmod 6$，或 $5y \equiv 4 \pmod 6$.

运用广义欧几里德除法，对整数 $N_1 = 5$ 及模 $m_2 = 6$，

可求出整数 $N_1^{'} \equiv N_1^{-1} \equiv 5 \pmod 6$，我们有 $y \equiv 5 \cdot 4 \equiv 2 \pmod 6$.

故同余方程组的解为 $x = x_2 = 1 + 5 \cdot 2 \equiv 11 \pmod{30}$.

我们将它表示为（y 待定参数）$x = x_2 = 11 + 30y$.

将 x 代入同余方程组的第三个同余方程，我们有

$11 + 30y \equiv 4 \pmod 7$，或 $30y \equiv 4 - 11 \equiv 0 \pmod 7$.

运用广义欧几里德除法，对整数 $N_2 = 30$ 及模 $m_3 = 7$，

可求出整数 $N_2^{'} \equiv N_2^{-1} \equiv 4 \pmod 7$，我们有 $y \equiv 4 \cdot 0 \pmod 7$.

故同余方程组的解为 $x = x_3 = 11 + 30 \cdot 0 \equiv 11 \pmod{210}$.

我们将它表示为（y 待定参数）$x = x_3 = 11 + 210y$.

将 x 代入同余方程组的第三个同余方程，我们有

$11 + 210y \equiv 10 \pmod{11}$，或 $210y \equiv 10 - 11 \equiv 10 \pmod{11}$.

运用广义欧几里德除法，对整数 $N_3 = 210$ 及模 $m_4 = 11$，

可求出整数 $N_3^{'} \equiv N_3^{-1} \equiv 1 \pmod{11}$，我们有 $y \equiv 1 \cdot 10 \pmod{11}$.

故同余方程组的解为 $x = x_3 = 11 + 210 \cdot 10 \equiv 2111 \pmod{2310}$.

3.2.3 中国剩余定理应用

应用中国剩余定理，可以将一些复杂的运算转化为较简单的运算.

例 3.2.3 计算 $2^{1000000} \pmod{77}$.

解一 利用定理 2.2.13（欧拉定理）及模重复平方计算法进行求解.

因为 $77 = 7 \cdot 11,\ \varphi(77) = \varphi(7) \cdot \varphi(11) = 60$，所以由定理 2.2.13（欧拉定理），

$$2^{60} \equiv 1 (\mathrm{mod}\, 77).$$

又 $1000000 = 16666 \cdot 60 + 40$，所以

$$2^{1000000} = (2^{60})^{16666} \cdot 2^{40} \equiv 2^{40} (\mathrm{mod}\, 77).$$

设 m=77，b=2，令 a=1. 将 40 写成二进制，$40 = 2^3 + 2^5$.

运用模重复平方法，我们依次计算如下:

（1）$n_0 = 0$，计算 $a_0 = a \equiv 1,\quad b_1 \equiv b^2 \equiv 4 (\mathrm{mod}\, 77)$.

（2）$n_1 = 0$，计算 $a_1 = a_0 \equiv 1,\quad b_2 \equiv b_1^2 \equiv 16 (\mathrm{mod}\, 77)$.

（3）$n_2 = 0$，计算 $a_2 = a_1 \equiv 1,\quad b_3 \equiv b_2^2 \equiv 25 (\mathrm{mod}\, 77)$.

（4）$n_3 = 1$，计算 $a_3 = a_2 \cdot b_3 \equiv 25,\quad b_4 \equiv b_3^2 \equiv 9 (\mathrm{mod}\, 77)$.

（5）$n_4 = 0$，计算 $a_4 = a_3 \equiv 25,\quad b_5 \equiv b_4^2 \equiv 4 (\mathrm{mod}\, 77)$.

（6）$n_5 = 1$，计算 $a_5 = a_4 \cdot b_5 \equiv 23 (\mathrm{mod}\, 77)$.

最后，计算出 $2^{1000000} \equiv 23 (\mathrm{mod}\, 77)$.

解二 利用中国剩余定理进行优化求解.

令 $x = 2^{1000000}$，因为 $77 = 7 \cdot 11$，所以计算 x（mod77）等价于求解同余方程组

$$\boxed{y \equiv x (\mathrm{mod}\, 77) \Leftrightarrow \begin{cases} y \equiv x\ (\mathrm{mod}\, 7) \\ y \equiv x\ (\mathrm{mod}\, 11) \end{cases}}.$$

$$\begin{cases} x \equiv b_1\ (\mathrm{mod}\, 7) \\ x \equiv b_2\ (\mathrm{mod}\, 11) \end{cases}.$$

因为欧拉定理给出 $2^{\varphi(7)} \equiv 2^6 \equiv 1 (\mathrm{mod}\, 7)$，

以及 $1000000 = 166666 \cdot 6 + 4$，所以

$$b_1 \equiv 2^{1000000} \equiv (2^6)^{166666} \cdot 2^4 \equiv 2 (\mathrm{mod}\, 7).$$

类似地，因为 $2^{\varphi(11)} \equiv 2^{10} \equiv 1 (\mathrm{mod}\, 11)$，$1000000 = 100000 \cdot 10$，所以

$$b_2 \equiv 2^{1000000} \equiv (2^{10})^{100000} \equiv 1(\mathrm{mod}\,11).$$

即：求下列解同余方程组的解：

$$\begin{cases} x \equiv 2\ (\mathrm{mod}\,7) \\ x \equiv 1\ (\mathrm{mod}\,11) \end{cases}$$

令 $m_1 = 7,\ m_2 = 11,\ m = m_1 \cdot m_2 = 77,$

$M_1 = m_2 = 11,\ M_2 = m_1 = 7.$

分别求解同余方程 $11M_1' \equiv 1(\mathrm{mod}\,7),\ 7M_2' \equiv 1(\mathrm{mod}\,11).$

得到 $M_1' = 2,\ M_2' = 8.$

故 $x = 2 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 1 \equiv 100 \equiv 23(\mathrm{mod}\,77).$

因此，$2^{1000000} \equiv 23(\mathrm{mod}\,77).$

例 3.2.4 （RSA 公钥密码系统原型）

系统建立. 假设 RSA 公钥密码系统使用 $N = 26$ 字符集 $\boldsymbol{N}$. 明文信息空间为 $k = 4$-字符组组成的集合 $\boldsymbol{M} = \boldsymbol{N}^k$, 密文信息空间为 $l = 5$-字符组组成的集合 $\boldsymbol{C} = \boldsymbol{N}^l$.

针对每个用户(譬如信息接收方 A), 选取素数对 $p = 2017, q = 2027$.

(*i*) 计算 $n = pq = 4088459$ 和 $\varphi(n) = (p\text{-}1)(q\text{-}1) = 4084416$.

(*ii*) 随机选取整数 $e = 365, 1 < e < \varphi(n)$ 使得 $(e, \varphi(n)) = 1$.

(*iii*) 运用广义欧几里德除法计算唯一的整数 $d = 1051877, 1 < d < \varphi(n)$ 使得 $e \cdot d \equiv 1 \pmod{\varphi(n)}$.

则用户 A 的公钥 K_e 是数组 $(n, e) = (4088459, 365)$，私钥是 $K_d = d = 1051877$.

加密算法. 为加密信息 m = math, 将明文 math 转换成数字信息: $m = 13 \cdot 26^3 + 1 \cdot 26^2 + 20 \cdot 26 + 8 = 229692$. 任意发送方 B，利用接收方 A 的公钥 K_e 计算出

$$c = m^e \pmod{n} = 229692^{365} \pmod{4088459} \equiv 3937358 \pmod{4088459}.$$

再将其转换成字符信息 $c = 3937358 = 8 \cdot 26^4 + 16 \cdot 26^3 + 0 \cdot 26^2 + 12 \cdot 26 + 22$ = hpzlv, 即为待发送的密文.

解密算法. 为解密接收到信息 hpzlv, 用户 A 将其转换成数字信息 $c = 8 \cdot 26^4 + 16 \cdot 26^3 + 0 \cdot 26^2 + 12 \cdot 26 + 22 = 3937358$. 再利用自己的私钥 K_d 计算出

$$c^d \pmod{n} = 3937358^{1051877} \pmod{4088459} \equiv 229692 \pmod{4088459}.$$

并将其转换成字符信息 $229692 = 13 \cdot 26^3 + 1 \cdot 26^2 + 20 \cdot 26 + 8$ = math, 即为明文.

需要强调的是, 在加密算法中因发送方 B 不知道用户 A 的公钥中 n 的整数分解, 即 p 和 q, 所以在计算 $c = m^e \pmod{n}$ 时无法使用中国剩余定理进行优化运算. 但在解密算法

中, 用户 A 知道自己的私钥, 进而可等同于知道 n 的整数分解, 所以可以利用中国剩余定理简化计算 $c^d \pmod n$.

事实上, 令 $x = 3937358^{1051877}$, 因为 $4088459 = 2017 \cdot 2027$, 所以计算 $x \pmod{4088459}$ 等价于求解同余方程组

$$\begin{cases} x \equiv b_1 (mod\ 2017) \\ x \equiv b_2 (mod\ 2027) \end{cases}.$$

由同余性质、费马小定理和模重复平方计算法得, $b_1 \equiv 3937358^{1051877} \equiv 174^{1541} \equiv 1771 \pmod{2017}$ 和 $b_2 \equiv 3937358^{1051877} \equiv 924^{383} \equiv 641 \pmod{2027}$.

根据中国剩余定理, 先分别求出 $qq' \equiv 1 \pmod p$ 和 $pp' \equiv 1 \pmod q$, 即 $2027q' \equiv 1 \pmod{2017}$ 和 $2017p' \equiv 1 \pmod{2027}$, 亦即 $q' \equiv 1412 \pmod{2017}$ 和 $p' \equiv 608 \pmod{2027}$; 再得出同余方程组的解 $x \equiv 1771 \cdot 1412 \cdot 2027 + 641 \cdot 608 \cdot 2017 \equiv 229692 \pmod{4088459}$.

除了上述加速公钥密码系统的运算外, 中国剩余定理还被广泛应用于构造具有特定性质的密码学序列、批量数字签名、盲签名、零知识证明等密码学领域. 中国剩余定理还在计算机科学、物理、化学、生物等多个学科领域中得到应用. 特别地, 中国剩余定理作为一个重要的数学工具被用于解决数论中的其他问题.

下面, 我们推广定理 2.2.4.

定理 3.2.2 在定理 3.2.1 的条件下, 若 $b_1, \cdots, b_k$ 分别遍历模 $m_1, \cdots, m_k$ 的完全剩余系, 则

$$x \equiv M_1' M_1 b_1 + \cdots + M_k' M_k b_k \pmod m$$

遍历模 $m = m_1 \cdots m_k$ 的完全剩余系.

证 令 $x_0 \equiv M_1' M_1 b_1 + \cdots + M_k' M_k b_k \pmod m$,

则当 $b_1, \cdots, b_k$ 分别遍历模 $m_1, \cdots, m_k$ 的完全剩余系时, x_0 遍历 $m_1 \cdots m_k$ 个数.

如果能够证明它们模 m 两两不同余, 则结论成立. 事实上, 若

$$M_1' M_1 b_1 + \cdots + M_k' M_k b_k \equiv M_1' M_1 b_1' + \cdots + M_k' M_k b_k' \pmod m.$$

则根据性质 2.1.6, $M_i' M_i b_i \equiv M_i' M_i b_i' \pmod{m_i}, \quad i = 1, \cdots, k$.

因为 $M_i' M_i \equiv 1 \pmod{m_i}, \quad i = 1, \cdots, k$ 所以, $b_i \equiv b_i' \pmod{m_i}, \quad i = 1, \cdots, k$.

但 b_i, b_i' 是同一个完全剩余系中的两个数, 故 $b_i = b_i', \quad i = 1, \cdots, k$.

3.3 二次同余方程

前面讨论了一次同余方程的具体求解以及一般同余方程的解数，本节我们继续讨论二次同余方程是否有解，解数以及如何求解.

3.3.1 平方剩余及平方非剩余

二次同余方程的一般形式是 $ax^2+bx+c\equiv 0\ (\mathrm{mod}\, m)$，其中 $a\not\equiv 0\ (\mathrm{mod}\, m)$.

因为正整数 m 有素因数分解式 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，所以该二次同余方程等价于同余方程组:

$$\begin{cases} ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p_1^{\alpha_1}) \\ \cdots\cdots \\ ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p_k^{\alpha_k}) \end{cases}.$$

因此，我们只需讨论模为素数幂 p^α 的同余方程:

$$ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p^\alpha),\quad p\nmid a.$$

两端同乘 $4a$，我们得到 $4a^2x^2+4abx+4ac\equiv 0\ (\mathrm{mod}\ p^\alpha)$

或 $(2ax+b)^2\equiv b^2-4ac\ (\mathrm{mod}\ p^\alpha)$

令 $y=2ax+b$，我们有 $y^2\equiv b^2-4ac\ (\mathrm{mod}\ p^\alpha)$

特别地，当 p 是奇素数时，（p，$2a$）=1，

同余方程 $y^2\equiv b^2-4ac\ (\mathrm{mod}\ p^\alpha)$ 等价于同余方程

$ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p^\alpha),\quad p\nmid a$.

定义 3.3.1 设 m 是正整数. 若同余方程

$$x^2\equiv a\ (\mathrm{mod}\, m),\quad (a,m)=1$$

有解，则 a 叫做模 m 的**平方剩余**（或**二次剩余**）；否则，a 叫做模 m 的**平方非剩余**（或**二次非剩余**）.

例 3.3.1 1 是模 3 平方剩余，-1 是模 3 平方非剩余.

例 3.3.2 1，2，4 是模 7 平方剩余，-1，3，5 是模 7 平方非剩余.

因为 $1^2\equiv 1,\ 2^2\equiv 4,\ 3^2\equiv 2,\ 4^2\equiv 2,\ 5^2\equiv 4,\ 6^2\equiv 1\ (\mathrm{mod}\, 7)$.

例 3.3.3 -1, 1, 2, 3, 4, 9, 10 是模 13 平方剩余；5, 6, 7, 8, 11 是模 13 平方非剩余.

因为

$1^2\equiv 12^2\equiv 1\ (\mathrm{mod}\ 13)$, $2^2\equiv 11^2\equiv 4\ (\mathrm{mod}\ 13)$, $3^2\equiv 10^2\equiv 9\ (\mathrm{mod}\ 13)$, $4^2\equiv 9^2\equiv 3\ (\mathrm{mod}$

13), $5^2 \equiv 8^2 \equiv -1 \pmod{13}$, $6^2 \equiv 7^2 \equiv 10 \pmod{13}$.

例 3.3.4 求满足方程 E: $y^2 = x^3 + x + 1 \pmod 7$ 的所有点.

解 对 x=0，1，2，3，4，5，6，分别求出 y.

$x = 0, y^2 = 1 \pmod 7,\ y = 1, 6 \pmod 7,$

$x = 1, y^2 = 3 \pmod 7,$ 无解,

$x = 2, y^2 = 4 \pmod 7,\ y = 2, 5 \pmod 7,$

$x = 3, y^2 = 3 \pmod 7,$ 无解,

$x = 4, y^2 = 6 \pmod 7,$ 无解,

$x = 5, y^2 = 5 \pmod 7,$ 无解,

$x = 6, y^2 = 6 \pmod 7,$ 无解.

例 3.3.5 求满足方程 E: $y^2 = x^3 + x + 2 \pmod 7$ 的所有点.

解 对 x=0，1，2，3，4，5，6，分别求出 y.

$x = 0, y^2 = 2 \pmod 7,\ y = 3, 4 \pmod 7,$

$x = 1, y^2 = 4 \pmod 7,\ y = 2, 5 \pmod 7,$

$x = 2, y^2 = 5 \pmod 7,$ 无解,

$x = 3, y^2 = 4 \pmod 7,\ y = 2, 5 \pmod 7,$

$x = 4, y^2 = 0 \pmod 7,\ y = 0 \pmod 7,$

$x = 5, y^2 = 6 \pmod 7,$ 无解,

$x = 6, y^2 = 0 \pmod 7,\ y = 0 \pmod 7.$

下面讨论如何判断同余方程 $x^2 \equiv a \pmod m,\ \ (a, m) = 1$ 有解. 首先考虑模为素数 p 的二次同余方程 $x^2 \equiv a \pmod p,\ \ (a, p) = 1$

定理 3.3.1（欧拉判别条件） 设 p 为奇素数，（a，p）=1，则

（i）a 是模 p 的平方剩余的充分必要条件是 $a^{\frac{p-1}{2}} \equiv 1 \pmod p$;

（ii）a 是模 p 的平方非剩余的充分必要条件是 $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

并且当 a 是模 p 的平方剩余时，同余方程 $x^2 \equiv a \pmod p,\ \ (a, p) = 1$ 恰有二解.

证 （i）因为 p 是奇素数，所以有表达式

$$x^p - x = x((x^2)^{\frac{p-1}{2}} - a^{\frac{p-1}{2}}) + (a^{\frac{p-1}{2}} - 1)x$$
$$= (x^2 - a)xq(x) + (a^{\frac{p-1}{2}} - 1)x \quad , \tag{3.3.1}$$

其中 $q(x)$ 是关于 x 的整系数多项式.

根据定理 2.2.14 (费马小定理)，对于任意的 x，有 x^p-x≡0 (mod p).

若 a 是模 p 的平方剩余，即存在某个 x_0 使得$x_0^2 \equiv a \pmod p$，其中 $(x_0, p) = 1$. 则 $0 \equiv x_0^p - x_0 \equiv (x_0^2 - a)x_0 q(x_0) + \left(a^{\frac{p-1}{2}} - 1\right)x_0 \equiv \left(a^{\frac{p-1}{2}} - 1\right) x_0 \pmod p$. 而 $(x_0, p) = 1$，所以$a^{\frac{p-1}{2}} \equiv 1 \pmod p$ 成立.

同时，由 p 是奇素数易知 p-x_0 是同余方程 $x^2 \equiv a \pmod p,\ \ (a, p) = 1$的另外一个解，且仅有此二解. 事实上，若存在第三个解 a_1，则 a_1 也满足同余方程 x^2-$a \equiv (x-x_0)(x-p+x_0) \equiv 0 \pmod p$，其中 $a_1 \not\equiv x_0 \pmod p$ 且 $a_1 \not\equiv p-x_0 \pmod p$，矛盾！所以该同余方程有且仅有此二解.

反过来，若$a^{\frac{p-1}{2}} \equiv 1 \pmod p$ 成立，则由(3.3.1)式知，

$$x^p - x \equiv (x^2 - a)xq(x) \pmod p.$$

根据定理 2.2.14 (费马小定理)知 x^p-x≡0 (mod p) 有 p 个不同的解，而 $q(x)$ 是次数为 p-3 的多项式，故 $q(x)$ ≡0 (mod p)最多有 p-3 个不同的解(见后面的定理 3.4.4). 所以同余方程 $x^2 \equiv a \pmod p$ 一定有解，即 a 是模 p 平方剩余.

（*ii*）因为 p 是奇素数，（a，p）=1，根据定理 2.2.13（欧拉定理），我们有

$$(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) = (a^{p-1} - 1) \equiv 0 \pmod p$$

再根据定理 1.2.10，我们有 $p \mid a^{\frac{p-1}{2}} - 1$或 $p \mid a^{\frac{p-1}{2}} + 1$

因此，a 是模 p 的平方非剩余的充分必要条件是$a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

例 3.3.6 判断 211 是否为模 2027 平方剩余.

解 根据定理 3.3.1，我们计算：

$$211^{(2027-1)/2} = 211^{1013} \pmod{2027}$$

运用模重复平方计算法. 设 m=2027，b=211，令 a=1，将 1013 写成二进制，

$$1013 = 1 + 2^2 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9$$

我们依次计算如下：

（1）n_0=1，计算 $a_0 = a \cdot b^{n_0} \equiv 211 \pmod{2027}$, $b_1 = b^2 \equiv 1954 \pmod{2027}$.

（2）n_1=0，计算 $a_1=a_0\cdot b_1^{n_1}\equiv 211 \pmod{2027}$, $b_2=b_1^2\equiv 1275 \pmod{2027}$.

（3）n_2=1，计算 $a_2=a_1\cdot b_2^{n_2}\equiv 1461 \pmod{2027}$, $b_3=b_2^2\equiv 1998 \pmod{2027}$.

（4）n_3=0，计算 $a_3=a_2\cdot b_3^{n_3}\equiv 1461 \pmod{2027}$, $b_4=b_3^2\equiv 841 \pmod{2027}$.

（5）n_4=1，计算 $a_4=a_3\cdot b_4^{n_4}\equiv 339 \pmod{2027}$, $b_5=b_4^2\equiv 1885 \pmod{2027}$.

（6）n_5=1，计算 $a_5=a_4\cdot b_5^{n_5}\equiv 510 \pmod{2027}$, $b_6=b_5^2\equiv 1921 \pmod{2027}$.

（7）n_6=1，计算 $a_6=a_5\cdot b_6^{n_6}\equiv 669 \pmod{2027}$, $b_7=b_6^2\equiv 1101 \pmod{2027}$.

(8) n_7=1，计算 $a_7=a_6\cdot b_7^{n_7}\equiv 768 \pmod{2027}$, $b_8=b_7^2\equiv 55 \pmod{2027}$.

(9) n_8=1，计算 $a_8=a_7\cdot b_8^{n_8}\equiv 1700 \pmod{2027}$, $b_9=b_8^2\equiv 998 \pmod{2027}$.

(10) n_9=1，计算 $a_9=a_8\cdot b_9^{n_9}\equiv 1 \pmod{2027}$.

因此，221 为模 2027 平方剩余.

推论 3.3.1 设 p 是奇素数，$(a_1, p)=1, (a_2, p)=1$. 则

（*i*）如果 a_1, a_2 都是模 p 的平方剩余，则 a_1a_2 是模 p 的平方剩余；

（*ii*）如果 a_1, a_2 都是模 p 的平方非剩余，则 a_1a_2 是模 p 的平方剩余；

（*iii*）如果 a_1 是模 p 的平方剩余，a_2 是模 p 的平方非剩余，则 a_1a_2 是模 p 的平方非剩余；

证 因为

$$(a_1a_2)^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}\cdot a_2^{\frac{p-1}{2}}$$

所以由定理 3.3.1 即得结论.

定理 3.3.2 设 p 是奇素数，则模 p 的简化剩余系中平方剩余与平方非剩余的个数各为（p-1）/2，且（p-1）/2 个平方剩余与序列：

$$1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$$

中的一个数同余，且仅与一个数同余.

证 由定理 3.3.1，平方剩余的个数等于同余方程 $x^{\frac{p-1}{2}}\equiv 1 \pmod{p}$ 的解数，

但 $x^{\frac{p-1}{2}}-1 \mid x^{p-1}-1$，由 3.4 节定理 3.4.5（后面给予证明），此同余方程的解数恰好是次数 $\frac{p-1}{2}$，故平方剩余的个数是 $\frac{p-1}{2}$，而平方非剩余个数是

$$p-1-\frac{p-1}{2}=\frac{p-1}{2}.$$

再证明定理的第二部分:

若$1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2$中的两个数模 p 同余，即存在$k_1\neq k_2$使得

$$k_1^2\equiv k_2^2 \pmod p,$$

则$(k_1+k_2)(k_1-k_2)\equiv 0 \pmod p$.

因此，$p\mid k_1+k_2$或$p\mid k_1-k_2$.

但$1\le k_1,k_2\le (p-1)/2$，故$2\le k_1+k_2\le p-1<p,\quad |k_1-k_2|\le p-1<p$.

从而，$k_1=k_2$，矛盾.

3.3.2 勒让得符号及二次互反定律

定理 3.3.1 给出了整数 a 是否是模奇素数 p 二次剩余的判别法则，但需要作较复杂的运算. 我们希望有一种更简单的判别法则.

定义 3.3.2 设 p 是素数，我们定义**勒让得（*Legendre*）符号**如下:

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若}a\text{是模}p\text{的平方剩余}\\ -1, & \text{若}a\text{是模}p\text{的平方非剩余}\\ 0, & \text{若}p|a\end{cases}.$$

例 3.3.7 根据例 3.3.3，我们有

$$\left(\frac{-1}{13}\right)=\left(\frac{1}{13}\right)=\left(\frac{2}{13}\right)=\left(\frac{3}{13}\right)=\left(\frac{4}{13}\right)=\left(\frac{9}{13}\right)=\left(\frac{10}{13}\right)=1,$$
$$\left(\frac{5}{13}\right)=\left(\frac{6}{13}\right)=\left(\frac{7}{13}\right)=\left(\frac{8}{13}\right)=\left(\frac{11}{13}\right)=-1.$$

利用勒让得符号，我们可以将定理 3.3.1 叙述为:

定理 3.3.3（欧拉判别法则） 设 p 是奇素数，则对任意整数 a,

$$\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}} \pmod p.$$

例 3.3.8 证明 1，2，4 是模 7 平方剩余，-1，3，5 是模 7 平方非剩余.

因为: $1^2\equiv 1,\ 2^2\equiv 4,\ 3^2\equiv 2,\ 4^2\equiv 2,\ 5^2\equiv 4,\ 6^2\equiv 1 \pmod 7$.

又由于:

$1^{\frac{7-1}{2}} \equiv 1 \pmod 7$，$4^{\frac{7-1}{2}} \equiv 1 \pmod 7$，$2^{\frac{7-1}{2}} \equiv 1 \pmod 7$

即：$x^{\frac{7-1}{2}} \equiv 1 \pmod 7$ 有 3 个解，平方剩余有$\frac{p-1}{2}$=3 个.

且这 3 个平方剩余，分别为：$3^2 \equiv 2,\ 2^2,\ 1^2 \pmod 7$.

根据欧拉判别法则，并注意到 a=1 时，$a^{\frac{p-1}{2}} \equiv 1$ 以及 a=-1 时，$a^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}$，且 p 是奇数. 我们有

定理 3.3.4 设 p 是奇素数，则

（1）$\left(\frac{1}{p}\right)=1$；

（2）$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

可以进一步给出 p 的表达式.

推论 3.3.2 设 p 是奇素数，那么

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & 若 p \equiv 1 \pmod 4 \\ -1, & 若 p \equiv 3 \pmod 4\end{cases}.$$

证 根据欧拉判别法则，我们有

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

若 $p \equiv 1 \pmod 4$，则存在正整数 k 使得 p=4k+1. 从而

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=(-1)^{2k}=1.$$

若 $p \equiv 3 \pmod 4$，则存在正整数 k 使得 p=4k+3. 从而

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=(-1)^{2k+1}=-1.$$

例 3.3.9 判断同余方程 $x^2 \equiv -1 \pmod{365}$ 是否有解，有解时，求出其解数.

解 $365=5\cdot 73$ 不是素数，原同余方程等价于

$$\begin{cases}x^2 \equiv -1 \pmod 5 \\ x^2 \equiv -1 \pmod{73}\end{cases}$$

因为

$$\left(\frac{-1}{5}\right)=\left(\frac{-1}{73}\right)=1.$$

故同余方程组有解，原同余方程有解. 根据中国剩余定理知，解数为 4.

下面给出勒让得符号的性质.

定理 3.3.5 设 p 是奇素数，则

（i）(周期性) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$;

（ii）(完全可乘性) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

（iii）设（a，p）=1，则$\left(\frac{a^2}{p}\right)=1$.

证 （i）因为同余方程 $x^2\equiv a+p\pmod p$

等价于同余方程 $x^2\equiv a\pmod p$,

所以

$$\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$$

（ii）根据欧拉判别法则，我们有

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\pmod p,\quad \left(\frac{b}{p}\right)\equiv b^{\frac{p-1}{2}}\pmod p$$

以及

$$\left(\frac{ab}{p}\right)\equiv (ab)^{\frac{p-1}{2}}\pmod p.$$

因此

$$\left(\frac{ab}{p}\right)\equiv (ab)^{\frac{p-1}{2}}=a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\pmod p.$$

因为勒让得符号取值±1，且 p 是奇素数，所以我们有

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

（iii）由（ii）立得.

推论 3.3.3 设 p 是奇素数，如果整数 a，b 满足 $a \equiv b \pmod{p}$，则

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$$

对于一个与 p 互素的整数 a，*Gauss* 给出了另一个判别法则，以判断 a 是否为模 p 二次剩余.

引理 3.3.1（*Gauss*） 设 p 是奇素数，a 是整数，$(a, p)=1$，如果整数 $a\cdot 1, a\cdot 2, \cdots, a\cdot\frac{p-1}{2}$ 中模 p 的最小正剩余大于 $\frac{p}{2}$ 的个数是 m，则

$$\left(\frac{a}{p}\right)=(-1)^m.$$

证 设 $a_1, \cdots, a_t$ 是整数 $a\cdot 1, a\cdot 2, \cdots, a\cdot\frac{p-1}{2}$ 模 p 的小于 $\frac{p}{2}$ 的最小正剩余，

$b_1, \cdots, b_m$ 是这些整数模 p 的大于 $\frac{p}{2}$ 的最小正剩余，则

$$\begin{aligned} a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= \prod_{k=1}^{\frac{p-1}{2}} ak \\ &\equiv \prod_{i=1}^{t} a_i \prod_{j=1}^{m} b_j \\ &\equiv (-1)^m \prod_{i=1}^{t} a_i \prod_{j=1}^{m} (p-b_j) \pmod{p} \end{aligned}$$

易知，$a_1, \cdots, a_t, p-b_1, \cdots, p-b_m$ 是模 p 两两不同余的. 否则，我们有

$$ak_i \equiv p-ak_j, \text{或} ak_i+ak_j \equiv 0 \pmod{p}$$

因而 $k_i+k_j \equiv 0 \pmod{p}$，这不可能，因为 $1 \le k_i+k_j \le \frac{p-1}{2}+\frac{p-1}{2} < p$.

因为 $(ak, p)=1, \quad k=1, \cdots, \frac{p-1}{2}$，

所以，$\frac{p-1}{2}$ 个整数 $a_1, \cdots, a_t, p-b_1, \cdots, p-b_m$ 是 $1, \cdots, \frac{p-1}{2}$ 的一个排列.

故

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv (-1)^m \prod_{i=1}^{t} a_i \prod_{j=1}^{m} (p-b_j) = (-1)^m \left(\frac{p-1}{2}\right)! \pmod{p}.$$

因此，

$$a^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p}.$$

再根据定理 3.3.3 及 p 是奇素数，我们得到

$$\left(\frac{a}{p}\right) = (-1)^m.$$

下面给出 2 是否为模 p 平方剩余的判断，以及将 a 是否为模 p 平方剩余转化成整数个数的计算，即模 p 平方剩余个数 $T(a,p)$为$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{a\cdot k}{p}\right]$.

定理 3.3.6 设 p 是奇素数.

（i） $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

（ii）若（a，$2p$）=1，则$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]}$.

证 因为

$$ak = p\left[\frac{ak}{p}\right] + r_k, \quad 0 < r_k < p, \quad k = 1, \cdots, \frac{p-1}{2},$$

对$k = 1, \cdots, \frac{p-1}{2}$求和，我们有

$$\begin{aligned} a\frac{p^2-1}{8} &= p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right] + \sum_{i=1}^{t} a_i + \sum_{j=1}^{m} b_j \\ &= p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right] + \sum_{i=1}^{t} a_i + \sum_{j=1}^{m}(p - b_j) + 2\sum_{j=1}^{m}(b_j - mp), \\ &= p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right] + \frac{p^2-1}{8} - mp + 2\sum_{j=1}^{m} b_j \end{aligned}$$

因此，

$$(a-1)\frac{p^2-1}{8} = \sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right] + m \pmod 2.$$

若 a=2，则$0 \le \left[\frac{ak}{p}\right] \le \left[\frac{p-1}{p}\right] = 0$，因而 $m = \frac{p^2-1}{8} \pmod 2$.

若 a 为奇数，则$m = \sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right] \pmod 2$

故由引理 3.3.1 知，结论成立.

推论 3.3.4 设 p 是奇素数，那么

$$\left(\frac{2}{p}\right)=\begin{cases}1, & 若p\equiv\pm1\,(\mathrm{mod}\,8)\\ -1, & 若p\equiv\pm3\,(\mathrm{mod}\,8)\end{cases}.$$

证 根据定理 3.3.6（i）我们有

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

若 $p\equiv\pm1\,(\mathrm{mod}\,8)$，则存在正整数 k 使得 $p\equiv8k\pm1$. 从而

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=(-1)^{2(4k^2\pm k)}=1.$$

若 $p\equiv\pm3\,(\mathrm{mod}\,8)$，则存在正整数 k 使得 $p\equiv8k\pm3$. 从而

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=(-1)^{2(4k^2\pm3k)+1}=-1.$$

例 3.3.10 判断同余方程 $x^2\equiv2\ (\mathrm{mod}\ 4088459)$是否有解，有解时求出其解数.

解 4088459=2017·2027 不是素数，原同余方程等价于

$$\begin{cases}x^2\equiv 2\ (mod\ 2017)\\ x^2\equiv 2\ (mod\ 2027)\end{cases}.$$

因为

$$\left(\tfrac{2}{2027}\right)=(-1)^{(2027^2-1)/8}=-1,$$

故该同余方程组无解，原同余方程无解.

为进一步简化二次剩余判别问题，设 p, q 是不同的奇素数，下面给出二次同余方程 $x^2\equiv q\ (\mathrm{mod}\,p)$与 $x^2\equiv p\ (\mathrm{mod}\,q)$之间的联系，即 q 模 p 平方剩余与 p 模 q 平方剩余之间的联系——二次互反律. 同时，基于勒让得符号的函数性质、二次互反律以及欧几里德除法，可以将模数较大的二次剩余判别问题转为模数较小的二次剩余判别问题，并最后归结为较少的几个情况，从而通过快速计算判断整数 a 是否为模 p 平方剩余.

定理 3.3.7 （二次互反律）若 p，q 是互素奇素数，则

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

注 欧拉和勒让得都曾经提出过二次互反律的猜想. 但第一个严格的证明是由高斯在 1796 年做出的，随后他又发现了另外 7 个不同的证明. 在《算术研究》一书和相关论文中，

高斯将其称为“基石”. 私下里高斯把二次互反律誉为算术理论中的宝石，是一个黄金定律.

高斯之后雅可比、柯西、刘维尔、克罗内克、弗洛贝尼乌斯等也相继给出了新的证明. 至今，二次互反律已有超过两百个不同的证明. 下面给出其中的一种证明.

证：因为（2，pq）=1，根据定理 3.3.6，有

$$\left(\frac{q}{p}\right)=(-1)^{\sum_{h=1}^{\frac{p-1}{2}}\left[\frac{qh}{p}\right]},\quad \left(\frac{p}{q}\right)=(-1)^{\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{pk}{q}\right]}.$$

所以只需证明

$$\sum_{h=1}^{\frac{p-1}{2}}\left[\frac{qh}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{pk}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

事实上，考查长为 $\frac{p}{2}$，宽为 $\frac{q}{2}$ 的长方形内的整点个数，如图 3.2 所示：

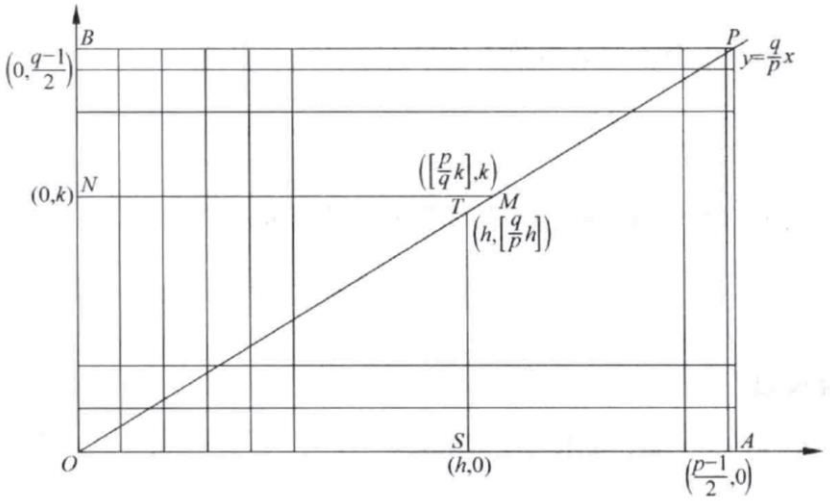

图 3.2 二次互反定理的证明

在垂直直线 ST 上，整点个数为 $\left[\frac{qh}{p}\right]$，因此，下三角形内的整点个数为 $\sum_{h=1}^{\frac{p-1}{2}}\left[\frac{qh}{p}\right]$；

在水平直线 NM 上，整点个数为 $\left[\frac{pk}{q}\right]$，因此，下三角形内的整点个数为 $\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{pk}{q}\right]$.

因为对角线上无整点，所以长方形内整点个数为

$$\sum_{h=1}^{\frac{p-1}{2}}\left[\frac{qh}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{pk}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

例 3.3.11 证明 2 是模 17 平方剩余；3 是模 17 平方非剩余.

证 根据定理 3.3.6，有 $\left(\frac{2}{17}\right)=(-1)^{\frac{17^2-1}{8}}=(-1)^{2\cdot 18}=1$.

因此，2 是模 17 平方剩余.

根据二次互反定律定理 3.3.7，$\left(\frac{3}{17}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{3}\right)$.

又根据定理 3.3.5，$\left(\frac{17}{3}\right)=\left(\frac{-1}{3}\right)=(-1)^{\frac{3-1}{2}}=-1$.

因此，$\left(\frac{3}{17}\right)=-1$.

因此，3 是模 17 的平方非剩余.

例 3.3.12 判断同余方程 $x^2\equiv 1037 \pmod{2027}$ 是否有解?

解 根据二次互反定律定理 3.3.7，

$$\left(\frac{1037}{2027}\right)=(-1)^{\frac{1037-1}{2}\cdot\frac{2027-1}{2}}\left(\frac{2027}{1037}\right).$$

根据定理 3.3.5，

$$\left(\frac{2027}{1037}\right)=\left(\frac{990}{1037}\right)=\left(\frac{2}{1037}\right)\left(\frac{3^2}{1037}\right)\left(\frac{5}{1037}\right)\left(\frac{11}{1037}\right)=\left(\frac{2}{1037}\right)\left(\frac{5}{1037}\right)\left(\frac{11}{1037}\right)$$

由定理 3.3.6，我们有 $\left(\frac{2}{1037}\right)=(-1)^{\frac{1037^2-1}{8}}=(-1)^{\frac{1038\cdot 1036}{8}}=-1$

又有 $\left(\frac{5}{1037}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{5}\right)=\left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1$.

$\left(\frac{11}{1037}\right)=(-1)^{\frac{11-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{11}\right)=\left(\frac{3}{11}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}}\left(\frac{11}{3}\right)=-\left(\frac{2}{3}\right)=-(-1)^{\frac{3^2-1}{8}}=1$.

因此，$\left(\frac{1037}{2027}\right)=1$. 故同余方程 $x^2\equiv 1037 \pmod{2027}$ 有解，且有二解.

例 3.3.13 求所有奇素数 p，它以 3 为其二次剩余.

解 即要求所有奇素数 p，使得 $\left(\frac{3}{p}\right)=1$.

易知，p 是大于 3 的奇素数. 根据二次互反律，$\left(\frac{3}{p}\right)=(-1)^{(p-1)/2}\left(\frac{p}{3}\right)$.

因为 $(-1)^{(p-1)/2}=\begin{cases}1, & \text{当} p\equiv 1 \pmod 4\\ -1, & \text{当} p\equiv -1 \pmod 4\end{cases}$,

以及 $\left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1, & \text{当} p\equiv 1 \pmod 6\\ \left(\frac{-1}{3}\right)=-1, & \text{当} p\equiv -1 \pmod 6\end{cases}$.

所有$\left(\frac{3}{p}\right)=1$的充分必要条件是 $\begin{cases}p\equiv 1 \pmod 4\\ p\equiv 1 \pmod 6\end{cases}$或$\begin{cases}p\equiv -1 \pmod 4\\ p\equiv -1 \pmod 6\end{cases}$.

这分别等价于 $p\equiv 1 \pmod{12}$ 或 $p\equiv -1 \pmod{12}$.

因此，3 是模 p 二次剩余的充分必要条件是

$$p\equiv \pm 1 \pmod{12}.$$

3.3.3 雅可比符号

在勒让得符号的计算中，要求模 p 为素数. 此外，在二次互反定律的应用中，也要求 q 为素数. 这些都是很强的条件，因此希望这些条件可以弱化，只要求模为奇整数，现在将勒让得符号推广为一般的模 m.

定义 3.3.3 (雅可比 *Jacobi* 符号) 设 $m=p_1\cdots p_r$ 是奇素数 p_i 的乘积. 对任意整数 a，定义雅可比符号为

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)$$

雅可比符号形式上是勒让得符号的推广，但所蕴含的意义已经不同.

雅可比符号为-1，可判断 a 是模 m 平方非剩余;

但雅可比符号为 1，却不能判断 a 是模 m 平方剩余.

例 3.3.14 已知 3 是模 10403 平方非剩余，但

$$\left(\tfrac{3}{10403}\right)=\left(\tfrac{3}{101}\right)\left(\tfrac{3}{103}\right)=(-1)(-1)=1.$$

定理 3.3.8 设 m 是正奇数，则

(i) $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$;

(ii) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$;

（*iii*）设（a，m）=1，则$\left(\frac{a^2}{m}\right)=1$.

证 设$m=p_1\cdots p_r$，其中p_i为奇素数. 根据雅可比符号的定义以及定理 3.3.5，我们有

（*i*） $$\left(\frac{a+m}{m}\right)=\left(\frac{a+m}{p_1}\right)\cdots\left(\frac{a+m}{p_r}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)=\left(\frac{a}{m}\right).$$

（*ii*）

$$\begin{aligned}\left(\frac{ab}{m}\right)&=\left(\frac{ab}{p_1}\right)\cdots\left(\frac{ab}{p_r}\right)\\&=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)\\&=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{b}{p_r}\right)\\&=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\end{aligned}.$$

（*iii*） $$\left(\frac{a^2}{m}\right)=\left(\frac{a^2}{p_1}\right)\cdots\left(\frac{a^2}{p_r}\right)=1.$$

引理 3.3.2 设$m=p_1\cdots p_r$是奇数，则

$$\begin{aligned}\frac{m-1}{2}&\equiv\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}\pmod 2\\\frac{m^2-1}{8}&\equiv\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}\pmod 2\end{aligned}.$$

证 因为我们有表达式

$$m\equiv(1+2\cdot\frac{p_1-1}{2})\cdots(1+2\cdot\frac{p_r-1}{2})\equiv1+2\cdot\left(\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}\right)\pmod 4$$

$$m^2\equiv(1+8\cdot\frac{p_1^2-1}{8})\cdots(1+8\cdot\frac{p_r^2-1}{8})\equiv1+8\cdot\left(\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}\right)\pmod{16}$$

所以结论成立.

定理 3.3.9 设 m 是奇数，则

（*i*） $\left(\frac{1}{m}\right)=1$;

（*ii*） $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$;

$$(iii)\ \left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}.$$

证 因为 $m=p_1\cdots p_r$ 是奇数，其中 p_i 是奇素数. 根据雅可比符号的定义，有

$$(i)\ \left(\frac{1}{m}\right)=\left(\frac{1}{p_1}\right)\cdots\left(\frac{1}{p_r}\right)=1.$$

$$(ii)\ \left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_r}\right)=(-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}}=(-1)^{\frac{m-1}{2}}.$$

再根据雅可比符号的定义 3.3.3、定理 3.3.6 以及引理 3.3.2，我们有

$$(iii)\ \left(\frac{2}{m}\right)=\left(\frac{2}{p_1}\right)\cdots\left(\frac{2}{p_r}\right)=(-1)^{\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}}=(-1)^{\frac{m^2-1}{8}}.$$

定理 3.3.10 设 m，n 都是奇数，则 $\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$.

证 设 $m=p_1\cdots p_r, n=q_1\cdots q_s$. 如果（$m$，$n$）>1，

则根据雅可比符号的定义 3.3.3 和勒让得符号的定义 3.3.2，我们有

$$\left(\frac{n}{m}\right)=\left(\frac{m}{n}\right)=0.$$

结论成立. 因此，可设（m，n）=1.

根据雅可比符号的定义和定理 3.3.7，我们有

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=\prod_{i=1}^{r}\left(\frac{n}{p_i}\right)\prod_{j=1}^{s}\left(\frac{m}{q_j}\right)=\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)=(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\frac{q_j-1}{2}}$$

再根据引理 3.3.2，

$$\sum_{i=1}^{r}\sum_{j=1}^{S}\frac{p_i-1}{2}\frac{q_j-1}{2}\equiv\sum_{i=1}^{r}\frac{p_i-1}{2}\sum_{j=1}^{S}\frac{q_j-1}{2}\equiv\frac{m-1}{2}\cdot\frac{n-1}{2}\pmod 2.$$

因此，结论成立.

例 3.3.15 判断同余方程 $x^2\equiv 365 \pmod{2059}$ 是否有解.

解 不用考虑 2059 是否为素数，直接计算雅可比符号，因为

$$\left(\frac{365}{2059}\right)=\left(\frac{5}{2059}\right)\left(\frac{73}{2059}\right)=(-1)^{\frac{5-1}{2}\frac{2059-1}{2}}\left(\frac{2059}{5}\right)(-1)^{\frac{73-1}{2}\frac{2059-1}{2}}\left(\frac{2059}{73}\right)=\left(\frac{2^2}{5}\right)\left(\frac{15}{73}\right)=\left(\frac{3}{73}\right)\left(\frac{5}{73}\right)=\left(\frac{5}{73}\right)$$

$$=(-1)^{\frac{5-1}{2}\frac{73-1}{2}}\left(\frac{73}{5}\right)=\left(\frac{3}{5}\right)=-1.$$

所以原同余方程无解.

例 3.3.16 求出同余方程 $y^2 \equiv x^3 + x + 1 (\mathrm{mod} 17)$ 的所有解及解数.

解 令 $f(x) = x^3 + x + 1$，我们有

f（0）=1，　y=1，y=16；　　f（1）=3，　无解

f（2）=11，　无解　　f（3）=14，　无解

f（4）=1，　y=1，y=16；　　f（5）=12，　无解

f（6）=2，　y=6，y=11；　　f（7）=11，　无解

f（8）=11，　无解　　f（9）=8，y=5，y=12

f（10）=8，　y=5，y=12　　f（11）=0，　y=0

f（12）=7，　无解　　f（13）=1，y=1，y=16

f（14）=5，　无解　　f（15）=8，y=5，y=12

f（16）=-1，y=4，y=13；　　（*mod* 17）

因此，原同余方程的解为

（0，1），（0，16），（4，1），（4，16），（6，6），（6，11），（9，5），（9，12），（10，5），（10，12），（11，0），（13，1），（13，16），（15，5），（15，12），（16，4），（16，13）.

3.3.4 二次同余方程求解

设 p 为奇素数，对任意给定的整数 a，应用二次互反律 (定理 3.3.7) 可以快速的判断 a 是否为模 p 平方剩余，即二次同余方程 $x^2 \equiv a \pmod{p}$ 是否有解，也就是说解的存在性. 本节考虑二次同余方程的具体求解。

首先，考虑模 p 平方根.

在 $x^2 \equiv a \pmod{p}$ 有解的情况下，即 a 满足 $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \pmod{p}$，求该二次同余方程的解.

定理 3.3.11 设 p 是奇素数，将 p-1 写成形式 $p-1 = 2^t \cdot s, \quad t \geq 1$，其中 s 是奇数. 设 n 是模 p 平方非剩余，$b := n^s \pmod{p}$，如果同余方程

$$x^2 \equiv a \pmod{p}$$

有解，则 $a^{-1}x_{t-k-1}^2$ 满足同余方程 $y^{2^{t-k-1}} \equiv 1 \pmod p$, k=0, 1, …, t-1,

这里，$x_{t-1} \coloneqq a^{\frac{s+1}{2}} \pmod p$, $x_{t-k-1} = x_{t-k} b^{j_{k-1}2^{k-1}}$,

其中 $j_{k-1} = \begin{cases} 0, & \text{如果 } (a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv 1 \pmod p; \\ 1, & \text{如果 } (a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1 \pmod p. \end{cases}$

特别地, x_0 是同余方程 $x^2 \equiv a \pmod p$ 的解.

证 对于奇素数 p，将 p-1 写成形式 $p-1 = 2^t \cdot s, \quad t \geq 1$ 其中 s 是奇数.

（i）任意选取一个模 p 平方非剩余 n, 即整数 n 使得 $\left(\frac{n}{p}\right) = -1$. 再令 $b \coloneqq n^s \pmod p$.

我们有

$$b^{2^t} \equiv 1, \quad b^{2^{t-1}} \equiv -1 \pmod p,$$

即 b 是模 p 的 2^t 次单位根，但非模 p 的 2^{t-1} 次单位根. 事实上,

$b^{2^t} \equiv (n^s)^{2^t} \equiv n^{s \cdot 2^t} \equiv n^{p-1} \equiv 1 \mod p$， $b^{2^{t-1}} \equiv (n^s)^{2^{t-1}} \equiv n^{\frac{p-1}{2}} \equiv -1 \mod p$.

（ii）计算

$$x_{t-1} \coloneqq a^{\frac{s+1}{2}} \pmod p$$

我们有 $a^{-1}x_{t-1}^2$ 满足同余方程

$$y^{2^{t-1}} \equiv 1 \pmod p,$$

即 $a^{-1}x_{t-1}^2$ 是模 p 的 2^{t-1} 次单位根. 事实上,

$$(a^{-1}x_{t-1}^2)^{2^{t-1}} \equiv a^{2^{t-1}s} \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \equiv 1 \pmod p.$$

（iii）如果 t=1，则 $x = x_{t-1} = x_0 \equiv a^{\frac{s+1}{2}} \pmod p$ 满足同余方程 $x^2 \equiv a \pmod p$.

如果 $t \geq 2$，我们要寻找整数 x_{t-2} 使得 $a^{-1}x_{t-2}^2$ 满足同余方程

$$y^{2^{t-2}} \equiv 1 \pmod p,$$

即 $a^{-1}x_{t-2}^2$ 是模 p 的 2^{t-2} 次单位根.

（a）如果

$$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \pmod p,$$

我们令 $j_0 \coloneqq 0, \quad x_{t-2} \coloneqq x_{t-1} = x_{t-1} b^{j_0} \pmod p$，则 x_{t-2} 即为所求;

（b）如果

$$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \equiv (b^{-2})^{2^{t-2}} \pmod{p},$$

我们令 $j_0 := 1, \quad x_{t-2} := x_{t-1}b = x_{t-1}b^{j_0} \pmod{p}$，则 x_{t-2} 即为所求.

如此下去，……

假设找到的整数 x_{t-k} 使得 $a^{-1}x_{t-k}^2$ 满足同余方程

$$y^{2^{t-k}} \equiv 1 \pmod{p},$$

即 $a^{-1}x_{t-k}^2$ 是模 p 的 2^{t-k} 次单位根：$(a^{-1}x_{t-k}^2)^{2^{t-k}} \equiv 1 \pmod{p}$.

$$\vdots$$

（k+2）如果 $t=k$，则 $x = x_{t-k} \pmod{p}$ 满足同余方程 $x^2 \equiv a \pmod{p}$.

如果 $t \geq k+1$，我们要寻找整数 x_{t-k-1} 使得 $a^{-1}x_{t-k-1}^2$ 满足同余方程

$$y^{2^{t-k-1}} \equiv 1 \pmod{p},$$

即 $a^{-1}x_{t-k-1}^2$ 是模 p 的 2^{t-k-1} 次单位根.

（a）如果

$$(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv 1 \pmod{p},$$

我们令 $j_{k-1} := 0, \quad x_{t-k-1} := x_{t-k} = x_{t-k}b^{j_{k-1}2^{k-1}} \pmod{p}$，则 x_{t-k-1} 即为所求；

（b）如果

$$(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1 \equiv (b^{-2^k})^{2^{t-k-1}} \pmod{p},$$

我们令 $j_{k-1} := 1, \quad x_{t-k-1} := x_{t-k}b^{2^{k-1}} = x_{t-k}b^{j_{k-1}2^{k-1}} \pmod{p}$，则 x_{t-k-1} 即为所求.

特别地，对于 k=t-1，我们有

$$\begin{aligned} x &= x_0 \\ &\equiv x_1 b^{j_{t-2}2^{t-2}} \\ &\vdots \\ &\equiv x_{t-1} b^{j_0 + j_1 2 + \cdots + j_{t-2}2^{t-2}} \\ &\equiv a^{\frac{s+1}{2}} b^{j_0 + j_1 2 + \cdots + j_{t-2}2^{t-2}} \pmod{p} \end{aligned}$$

满足同余方程

$$x^2 \equiv a \pmod{p}.$$

例 3.3.17 求解同余方程 $x^2 \equiv 157 \pmod{2029}$.

解 计算勒让得符号

$$\left(\frac{157}{2029}\right) = (-1)^{\frac{157-1}{2}\cdot\frac{2029-1}{2}}\left(\frac{2029}{157}\right) = \left(\frac{145}{157}\right) = \left(\frac{5}{157}\right)\left(\frac{29}{157}\right).$$

而 $\left(\frac{5}{157}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{157-1}{2}}\left(\frac{157}{5}\right)=\left(\frac{2}{5}\right)=-1$,

$\left(\frac{29}{157}\right)=(-1)^{\frac{29-1}{2}\cdot\frac{157-1}{2}}\left(\frac{157}{29}\right)=\left(\frac{12}{29}\right)=\left(\frac{3}{29}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{29-1}{2}}\left(\frac{29}{3}\right)=\left(\frac{2}{3}\right)=-1.$

所以

$$\left(\frac{157}{2029}\right)=\left(\frac{5}{157}\right)\left(\frac{29}{157}\right)=1.$$

故原同余方程有解.

对于奇素数 p=2029，将 p-1 写成形式 p-1=2028=$2^2\cdot$507，其中 t=2，s=507 是奇数.

（i）任意选取一个模 2029 的平方非剩余 n=2，即整数 n=2 使得$\left(\frac{2}{2029}\right)=-1$.

再令 b:=$2^{507}\equiv$992 (mod 2029).

（ii）计算

$$x_{t-1}=x_1:=157^{\frac{507+1}{2}}\equiv 157^{254}\equiv 729 \pmod{2029},$$

以及$a^{-1}\equiv$1861 (mod 2029).

（iii）因为

$$a^{-1}x_1^2\equiv 1861\cdot 729^2\equiv -1 \pmod{2029},$$

令 j_0:=1, x_0:=$x_1b\equiv$729·992≡844 (mod 2029),

则 $x\equiv x_0\equiv$844 (mod 2029) 和 $x\equiv p-x_0\equiv$2029-844≡1185 (mod 2029)是同余方程 $x^2\equiv$157 (mod 2029)的两个解.

其次，考虑模 *m* 平方根.

即模为合数 m 的二次同余方程 $x^2\equiv a\pmod m,\quad (a,m)=1$，有解的条件及解的个数.

当 $m=2^\delta p_1^{\alpha_1}\dots p_k^{\alpha_k}$ 时，同余方程 $x^2\equiv a\pmod m,\quad (a,m)=1$等价于同余方程组:

$$\begin{cases} x^2\equiv a \pmod{2^\delta} \\ x^2\equiv a \pmod{p_1^{\alpha_1}} \\ \quad\cdots\cdots \\ x^2\equiv a \pmod{p_k^{\alpha_k}} \end{cases}.$$

因此，需要讨论二次同余方程 $x^2\equiv a\pmod{p^\alpha},\quad (a,p)=1,\alpha>0$ 有解的条件及解的个数. 此外，还需要讨论同余方程 $x^2\equiv a\pmod{2^\alpha},\quad (a,2)=1,\alpha>0$有解的条件及解的个数.

先讨论二次同余方程 $x^2\equiv a\pmod{p^\alpha},\quad (a,p)=1,\alpha>0$ 有解的条件及解的个数.

定理 3.3.12 设 p 为素奇数，则同余方程 $x^2\equiv a\pmod{p^\alpha},\quad (a,p)=1,\alpha>0$ 有解的充分必要条件是 a 为模 p 平方剩余，且有解时，解数为 2.

证 设同余方程有解，即存在整数 $x \equiv x_1 \pmod{p^\alpha}$ 使得

$$x_1^2 \equiv a \pmod{p^\alpha},$$

则我们有 $x_1^2 \equiv a \pmod{p}$，即 a 为模 p 平方剩余，因此必要性成立.

反过来，设 a 为模 p 平方剩余，那么存在整数 $x \equiv x_1 \pmod{p}$ 使得

$$x_1^2 \equiv a \pmod{p}.$$

令 $f(x) = x^2 - a$，则 $f'(x) = 2x,\ (f'(x_1), p) = (2x_1, p) = 1$，根据定理 3.4.6（后面给出高次同余方程的定理结论及其证明），从同余方程 $x^2 \equiv a \pmod{p}$ 的解 $x \equiv x_1 \pmod{p}$，可递归地推出唯一的

$$x \equiv x_\alpha \pmod{p^\alpha}$$

使得 $x_\alpha^2 \equiv a \pmod{p^\alpha}$.

因为 $x^2 \equiv a \pmod{p}$ 只有两个解，所以 $x^2 \equiv a \pmod{p^\alpha}$ 的解数为 2.

再讨论同余方程 $x^2 \equiv a \pmod{2^\alpha},\ (a,2) = 1, \alpha > 0$ 有解的条件及解的个数.

定理 3.3.13 设 $\alpha > 1$，则同余方程 $x^2 \equiv a \pmod{2^\alpha},\ (a,2) = 1, \alpha > 0$ 有解的必要条件是

（i）当 $\alpha = 2$ 时，$a \equiv 1 \pmod{4}$；

（ii）当 $\alpha \geq 3$ 时，$a \equiv 1 \pmod{8}$.

且当 $\alpha = 2$ 时，解数为 2；当 $\alpha \geq 3$ 时，解数为 4.

证 必要性. 若同余方程 $x^2 \equiv a \pmod{2^\alpha},\ (a,2) = 1, \alpha > 0$ 有解，

则存在整数 x_1，使得 $x_1^2 \equiv a \pmod{2^\alpha}$.

根据（a，2）=1，我们有 $(x_1, 2) = 1$. 记 $x_1 = 1 + 2t$，上式可写成

$$a \equiv 1 + 4t(t+1) \pmod{2^\alpha}.$$

注意到 2|t（t+1），我们有

（i）当 $\alpha = 2$ 时，$a \equiv 1 \pmod{4}$；

（ii）当 $\alpha \geq 3$ 时，$a \equiv 1 \pmod{8}$.

因此，必要性成立.

充分性. 当必要条件满足时，则

（i）当 $\alpha = 2$ 时，$a \equiv 1 \pmod{4}$，这时 $x \equiv 1,\ 3 \pmod{2^\alpha}$

是同余方程 $x^2 \equiv a \pmod{2^\alpha}$, $(a,2)=1, \alpha>0$ 仅有的二解.

（*ii*）当 $\alpha \geq 3$ 时，$a \equiv 1 \pmod 8$，这时，

对 $\alpha=3$，易验证：$x \equiv \pm 1, \pm 5 \pmod{2^3}$

是 $x^2 \equiv a \pmod{2^\alpha}$, $(a,2)=1, \alpha>0$ 仅有的 4 解，它们可表示为

$$\pm(1+2^2 t_3), t_3 = 0,1,\cdots$$

或者 $\pm(x_3 + 2^2 t_3), t_3 = 0,1,\cdots$

对 $\alpha=4$，考虑到 $x^2 \equiv a \pmod{2^4}$的解一定满足 $x^2 \equiv a \pmod{2^3}$，故令

$$(x_3 + 2^2 t_3)^2 \equiv a \pmod{2^4},$$

并注意到 $2x_3(2^2 t_3) \equiv 2^3 t_3 \pmod{2^4}$，

我们有 $x_3^2 + 2^3 t_3 \equiv a \pmod{2^4}$，

进而求得 $t_3 \equiv \dfrac{a - x_3^2}{2^3} \pmod 2$.

故同余方程 $x^2 \equiv a \pmod{2^4}$ 的解可表示为

$$x = \pm\left(1 + 4 \cdot \tfrac{a-x_3^2}{2^3} + 2^3 t_4\right),\ t_4 = 0,1,\cdots$$

或者 $x = \pm(x_4 + 2^3 t_4),\ t_4 = 0,1,\cdots$

对于 $\alpha \geq 4$，如果满足同余方程 $x^2 \equiv a \pmod{2^{\alpha-1}}$ 的解为

$$x = \pm(x_{\alpha-1} + 2^{\alpha-2} t_{\alpha-1}), \qquad t_{\alpha-1} = 0,1,\cdots$$

则同理地令 $(x_{\alpha-1} + 2^{\alpha-2} t_{\alpha-1})^2 \equiv a \pmod{2^\alpha}$，

并注意到 $2x_{\alpha-1}(2^{\alpha-2} t_{\alpha-1}) \equiv 2^{\alpha-1} t_{\alpha-1} \pmod{2^\alpha}$，

有 $x_{\alpha-1}^2 + 2^{\alpha-1} t_{\alpha-1} \equiv a \pmod{2^\alpha}$，

进而求得 $t_{\alpha-1} \equiv \dfrac{a - x_{\alpha-1}^2}{2^{\alpha-1}} \pmod 2$.

故同余方程 $x^2 \equiv a \pmod{2^\alpha}$ 的解可表示为

$$x = \pm\left(x_{\alpha-1} + 2^{\alpha-2} \cdot \tfrac{a-x_{\alpha-1}^2}{2^{\alpha-1}} + 2^{\alpha-1} t_\alpha\right),\ t_\alpha = 0,1,\cdots$$

或 $x = \pm(x_\alpha + 2^{\alpha-1} t_\alpha),\ t_\alpha = 0,1,\cdots$

它们对模 2^α 为 4 个解，即 $x_\alpha, x_\alpha + 2^{\alpha-1}, -x_\alpha, -(x_\alpha + 2^{\alpha-1})$.

例 3.3.18 求解同余方程 $x^2 \equiv 57 \pmod{64}$, $64 \equiv 2^6$

解 因为 $57 \equiv 1 \pmod 8$，所以同余方程有 4 的解.

$\alpha = 3$ 时，解为 $\pm(1 + 4t_3)$，$t_3 = 0, 1, \cdots$

$\alpha = 4$ 时，令 $(1+4t_3)^2 \equiv 57 \pmod{2^4}$，求得

$$t_3 \equiv \frac{57-1^2}{8} \equiv 1 \pmod 2,$$

故同余方程 $x^2 \equiv a \pmod{2^4}$ 的解为：

$$\pm(1 + 4 \cdot 1 + 8t_4) = \pm(5 + 8t_4), \quad t_4 = 0, \quad 1, \cdots$$

$\alpha = 5$ 时，令 $(5+8t_4)^2 \equiv 57 \pmod{2^5}$，求得

$$t_4 \equiv \frac{57-5^2}{16} \equiv 0 \pmod 2,$$

故同余方程 $x^2 \equiv a \pmod{2^5}$ 的解为：

$$\pm(5 + 8 \cdot 0 + 16t_5) = \pm(5 + 16t_5), \quad t_5 = 0, \quad 1, \cdots$$

$\alpha = 6$ 时，令 $(5+16t_5)^2 \equiv 57 \pmod{2^5}$，求得

$$t_5 \equiv \frac{57-5^2}{32} \equiv 1 \pmod 2$$

故同余方程 $x^2 \equiv a \pmod{2^6}$ 的解为：

$$\pm(5 + 16 \cdot 1 + 32t_6) = \pm(21 + 32t_6), \quad t_6 = 0, \quad 1, \cdots$$

因此，同余方程模 $64 \equiv 2^6$ 的解是：

$$21, 53, -21 \equiv 43, -53 \equiv 11 \pmod{64}.$$

3.4 高次同余方程

前面我们已经给出一次和二次同余方程的相关结论，现在我们考虑高次同余方程的求解. 本节首先讨论高次同余方程的解数，接着讨论模为素数的同余方程的求解，进而讨论如何由模为素数的高次同余方程的解提升至模为素数幂的高次同余方程的解.

3.4.1 高次同余方程的解数

首先，考虑如何将模正整数 $m = m_1 m_2 \cdots m_k$ 同余方程的求解转化为模 m_i 同余方程的求解，以及它们的解数关系.

定理 3.4.1 设 $m_1, \cdots, m_k$ 是 k 个两两互素的正整数，$m = m_1 \cdots m_k$. 则同余方程 $f(x) \equiv 0 \pmod m$ 与同余方程组

$$\begin{cases} f(x) \equiv 0 \pmod{m_1} \\ \cdots\cdots \\ f(x) \equiv 0 \pmod{m_k} \end{cases}$$

等价. 如果用 T_i 表示同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, m_i)$ 的解数，T 表示同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, m)$ 的解数，则 $T=T_1\cdots T_k$.

证 由中国剩余定理（定理 3.2.1），上述同余方程与同余方程组是等价的.

下面给出解数证明. 设同余方程 $f(x_0)\equiv 0\ (\mathrm{mod}\, m_i)$ 的解是 $b_i,\quad i=1,\cdots,k,$

由中国剩余定理（定理 3.2.1），可求的同余方程组

$$\begin{cases} x\equiv b_1\ (\mathrm{mod}\, m_1) \\ \quad\cdots\cdots \\ x\equiv b_k\ (\mathrm{mod}\, m_k) \end{cases}$$

的解是 $x\equiv M_1'M_1b_1+\cdots+M_k'M_kb_k\ (\mathrm{mod}\, m)$.

因为 $\quad f(x)\equiv f(b_i)\equiv 0\ (\mathrm{mod}\, m_i),\quad i=1,\cdots,k,$

所以 x 也是 $f(x)\equiv 0\ (\mathrm{mod}\, m)$ 的解.

故 x 随 b_i 遍历 $f(x)\equiv 0\ (\mathrm{mod}\, m_i)$ 的所有解而遍历 $f(x)\equiv 0\ (\mathrm{mod}\, m)$ 的所有解，即

$$\begin{cases} f(x)\equiv 0\ (\mathrm{mod}\, m_1) \\ \quad\cdots\cdots \\ f(x)\equiv 0\ (\mathrm{mod}\, m_k) \end{cases}$$

的解数为 $\quad T=T_1\cdots T_k$.

例 3.4.1 解同余方程 $f(x)\equiv x^4+2x^3+8x+9\equiv 0\ (\mathrm{mod}\, 35)$

解 由定理 3.4.1 知原同余方程等价于同余方程组

$$\begin{cases} f(x)\equiv 0\ (\mathrm{mod}\, 5) \\ f(x)\equiv 0\ (\mathrm{mod}\, 7) \end{cases}.$$

直接验算.

$f(x)\equiv 0\ (\mathrm{mod}\, 5)$ 的解为 $x=1,4(\mathrm{mod}\, 5)$，

$f(x)\equiv 0\ (\mathrm{mod}\, 7)$ 的解为 $x=3,5,6(\mathrm{mod}\, 7)$.

根据中国剩余定理，可求得同余方程组 $\begin{cases} x\equiv b_1\ (\mathrm{mod}\, 5) \\ x\equiv b_2\ (\mathrm{mod}\, 7) \end{cases}$ 的解为

$x\equiv 3\cdot 7\cdot b_1+3\cdot 5\cdot b_2(\mathrm{mod}\, 35)$.

故原同余方程的解为 $x\equiv 31,26,6,24,19,34(\mathrm{mod}\, 35)$, 共 $2\cdot 3=6$ 个.

3.4.2 素数模的高次同余方程

现在我们考虑如何求解模素数 p 同余方程 $f(x)\equiv a_nx^n+\cdots+a_1x+a_0\equiv 0(\mathrm{mod}\ p)$，

其中 $a_n \neq 0(\mathrm{mod}\ p)$.

首先，考虑多项式欧几里德除法.

引理 3.4.1（多项式欧几里德除法）设 $f(x) \equiv a_n x^n + \cdots + a_1 x + a_0$ 为 n 次整系数多项式，$g(x) \equiv x^m + \cdots + b_1 x + b_0$ 为 $m \geq 1$ 次首一整系数多项式，则存在整系数多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x)=g(x)q(x)+r(x),\ \deg r(x)<\deg g(x).$$

证 我们分两种情形讨论.

（i） $n < m$，我们取 $q(x) = 0, r(x) = f(x)$ 结论成立.

（ii） $n \geq m$，对 $f(x)$的次数 n 作数学归纳法.

$n=m$，有 $f(x) - a_n \cdot g(x) = (a_{n-1} - a_n b_{m-1})x^{n-1} + \cdots + (a_1 - a_n b_0)x + a_0$

因此，$q(x) = a_n$，$r(x) = f(x) - a_n \cdot g(x)$ 为所求.

假设 $n-1 \geq m$ 时，结论成立.

对于 $n>m$，我们有

$$\begin{aligned} & f(x) - a_n x^{n-m} \cdot g(x) \\ &= (a_{n-1} - a_n b_{m-1})x^{n-1} + \cdots + (a_{n-m} - a_n b_0)x^{n-m} + a_{n-m-1}x^{n-m-1} + \cdots + a_0 \end{aligned}$$

这说明 $f(x) - a_n x^{n-m} \cdot g(x)$ 是次数小于等于 n-1 的多项式.

对其运用归纳假设或情形（i），存在整系数多项式 $q_1(x)$ 和 $r_1(x)$ 使得

$$f(x) - a_n x^{n-m} \cdot g(x) = g(x)q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x)$$

因此，$q(x) = a_n x^{n-m} + q_1(x), r(x) = r_1(x)$ 为所求.

根据数学归纳法原理，结论成立.

其次，由定理 2.2.14 (费马小定理)，多项式 $x^p - x(\mathrm{mod}\ p)$ 对任何整数取值为零，所以借助于它以及多项式欧几里德除法，可将高次多项式的求解转化为次数不超过 p-1 的多项式的求解.

定理 3.4.2 同余方程 $f(x) \equiv a_n x^n + \cdots + a_1 x + a_0 \equiv 0(\mathrm{mod}\ p)$ 与一个次数不超过 p-1 模 p 的同余方程等价.

证 由多项式的欧几里德除法，存在整系数多项式 $q(x)$，$r(x)$ 使得

$$f(x) = (x^p - x)q(x) + r(x),$$

其中 $r(x)$的次数小于等于 p-1. 由定理 2.2.14 (费马小定理)，对任何整数 x，都有

$$x^p - x \equiv 0(\mathrm{mod}\ p),$$

故同余方程 $f(x) \equiv 0(\mathrm{mod}\ p)$ 等价于同余方程 $r(x) \equiv 0(\mathrm{mod}\ p)$.

例 3.4.2 求与同余方程 $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod 5$ 等价于次数小于 5 的同余方程.

解 作多项式的欧几里德除法，我们有

$$\begin{aligned} &3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ &= (x^5 - x)(3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5) + 3x^3 + 16x^2 + 6x \end{aligned}$$

所以原同余方程等价于

$$3x^3 + 16x^2 + 6x \equiv 0 \pmod 5.$$

再次，考虑同余方程的解与一次同余方程的关系.

定理 3.4.3 设 $1 \le k \le n$，如果

$$x \equiv x_i \pmod p,\ i = 1, \cdots, k$$

是同余方程 $f(x) \equiv a_n x^n + \cdots + a_1 x + a_0 \equiv 0(\mathrm{mod}\ p)$ 的 k 个不同解，则对任何整数 x，都有

$$f(x) \equiv (x-x_1)\cdots(x-x_k) f_k(x) \pmod p,$$

其中 $f_k(x)$ 是 n-k 次多项式，首项系数是 a_n.

证 由多项式的欧几里德除法，存在多项式 $f_1(x)$ 和 $r(x)$ 使得

$$f(x) = (x-x_1) f_1(x) + r(x),\ \deg r(x) < \deg (x-x_1).$$

易知，$f_1(x)$ 的次数是 n-1，首项系数是 a_n，$r(x) = r$ 为整数.

因为 $f(x_1) \equiv 0 \pmod p$，所以 $r \equiv 0 \pmod p$.

即有 $f(x) \equiv (x-x_1) f_1(x) \pmod p$.

再由 $f(x_1) \equiv 0 \pmod p$ 及 $x_i \not\equiv x_1 \pmod p$, $i=2, \cdots, k$ 得到

$$f_1(x_i) \equiv 0 \pmod p,\ i=2, \cdots, k.$$

类似地，对于多项式 $f_1(x)$ 可找到多项式 $f_2(x)$ 使得

$$f_1(x) \equiv (x-x_2) f_2(x) \pmod p \ \text{且}\ f_2(x_i) \equiv 0 \pmod p,\ i=3, \cdots, k.$$

如此下去，有 $f_{k-1}(x) \equiv (x-x_k) f_k(x) \pmod p$. 故 $f(x) \equiv (x-x_1)\cdots(x-x_k) f_k(x) \pmod p$.

例 3.4.3 我们有同余方程

$$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x$$
$$=x(x-1)(x-2)(3x^{11}+3x^{10}+3x^9+4x^7+3x^6+x^5+2x^4+x^2+3x+3)\ (\mathrm{mod}\,5)$$

根据定理 3.4.3 及定理 2.2.14 (费马小定理)，可以立即得到.

推论 3.4.1 设 p 是一个素数，则

（i）对任何整数 x，我们有

$$x^{p-1}-1\equiv(x-1)\cdots(x-(p-1))\ (\mathrm{mod}\ p).$$

（ii）（Wilson 定理）$(p-1)!+1\equiv 0\ (\mathrm{mod}\ p)$.

注：由 Wilson 定理，可得到整数是否为素数的判别条件. 整数 n 为素数的充分必要条件是 $(n-1)!+1\equiv 0\ (\mathrm{mod}\,n)$.

最后，讨论模 p 同余方程的解数. 现在，我们先给出同余方程解数的上界估计.

定理 3.4.4 同余方程 $f(x)\equiv a_nx^n+\cdots+a_1x+a_0\equiv 0(\mathrm{mod}\ p)$，$a_n\not\equiv 0\ (\mathrm{mod}\ p)$ 的解数不超过它的次数.

证 反证法. 设同余方程 $f(x)\equiv a_nx^n+\cdots+a_1x+a_0\equiv 0(\mathrm{mod}\ p)$ 的解数超过 n 个，则它至少有 n+1 个解. 设它们为

$$x\equiv c_i\ (\mathrm{mod}\ p),\quad i=1,\cdots,n,n+1.$$

对于 n 个解 $c_1,\cdots,c_n$，可得到

$$f(x)\equiv(x-c_1)\cdots(x-c_n)f_n(x)\ (\mathrm{mod}\ p).$$

因为 $f(c_{n+1})\equiv 0\ (\mathrm{mod}\ p)$，所以

$$(c_{n+1}-c_1)\cdots(c_{n+1}-c_n)f_n(c_{n+1})\equiv 0\ (\mathrm{mod}\ p).$$

又因为 $c_i\not\equiv c_{n+1}\ (\mathrm{mod}\ p)$, i=1, , n, 且 p 是素数，所以 $f_n(c_{n+1})\equiv 0\ (\mathrm{mod}\ p)$.

但 $f_n(x)$ 是首项系数为 $a_n\not\equiv 0\ (\mathrm{mod}\ p)$，次数为 n-n=0 的多项式，故 $p\mid a_n$，矛盾.

推论 3.4.2 次数小于 p 的整系数多项式对所有整数取值模 p 为零的充要条件是其系数被 p 整除.

证 充分性显然. 下证必要性. 若不然，多项式 $f(x)$有某个系数不能被 p 整除，则 $f(x)$ $(\mathrm{mod}\ p)$ 是一个首项系数$\not\equiv 0\ (\mathrm{mod}\ p)$且次数小于 p 的多项式. 根据定理 3.4.4，同余方程 $f(x)\equiv 0\ (\mathrm{mod}\ p)$的解的个数小于 p，这与题设条件“对所有整数取值模 p 为零”，即有 p 个解，矛盾！故结论成立.

再给出同余方程解数的判断.

定理 3.4.5 设 p 是一个素数，n 是一个正整数，$n \le p$ ．那么同余方程

$$f(x) \equiv x^n + \cdots a_1 x + a_0 \equiv 0 \pmod{p}$$

有 n 个解的充分必要条件是 $x^p - x$ 被 $f(x)$除所得余式的所有系数都是 p 的倍数.

证 必要性：因为 $f(x)$是首一多项式，由多项式的欧几里德除法知，

存在整系数多项式 $q(x)$和 $r(x)$使得

$$x^p - x = f(x)q(x) + r(x)$$

其中 $r(x)$的次数小于 n，$q(x)$的次数是 p-n.

现在，若同余方程 $f(x) \equiv x^n + \cdots a_1 x + a_0 \equiv 0 \pmod{p}$ 有 n 个解，

则由定理 2.2.14 (费马小定理)，这 n 个解都是 $x^p - x \equiv 0 \pmod{p}$ 的解.

又由 $x^p - x = f(x)q(x) + r(x)$ 知，这 n 个解也是 $r(x) \equiv 0 \pmod{p}$ 的解.

但 $r(x)$的次数小于 n，由推论 3.4.2 知，$r(x)$的系数都是 p 的倍数.

充分性：若多项式 $r(x)$的系数都被 p 整除，则由推论 3.4.2 知，$r(x)$对所有整数 x 取值模 p 为零.

根据定理 2.2.14 (费马小定理)，对任何整数 x，有 $x^p - x \equiv 0 \pmod{p}$.

因此，对任何整数 x，有 $f(x)q(x) \equiv 0 \pmod{p}$，即有 p 个不同的解，

$$x \equiv 0, 1, \cdots, p-1 \pmod{p}.$$

由此可得，$f(x) \equiv 0 \pmod{p}$ 的解数 $k = n$. 若不然, $k<n$.

又因为次数为 p-n 的多项式 $q(x)$的同余方程 $q(x) \equiv \pmod{p}$ 的解数 $h \le p - n$，

所以 $f(x)q(x) \equiv 0 \pmod{p}$ 的解数小于等于 $k+h<p$，矛盾.

推论 3.4.3 设 p 是一个素数，d 是 p-1 的正因数. 那么多项式 $x^d - 1$ 模 p 有 d 个不同的根.

证 因为 $d \mid p-1$，所以存在整数 q 使得 p-1=dq. 这样，我们有因式分解:

$$x^{p-1}\text{-}1=(x^d\text{-}1)(x^{d(q-1)}+x^{d(q-2)}+\cdots+x^d+1)+p\cdot 0.$$

根据定理 3.4.5，多项式 $x^d - 1$ 模 p 有 d 个不同的根.

例 3.4.4 判断同余方程 $2x^3 + 5x^2 + 6x + 1 \equiv 0 \pmod{7}$ 是否有三个解.

解 首先，需将多项式变成首一的. 注意到 $4 \cdot 2 \equiv 1 \pmod{7}$，我们有

$$4(2x^3 + 5x^2 + 6x + 1) \equiv x^3 - x^2 + 3x - 3 \pmod{7}.$$

此同余方程与原同余方程等价. 作多项式的欧几里德除法，我们有

$$x^7-x=(x^3-x^2+3x-3)(x^3+x^2-2x-2)x+7x(x^2-1).$$

根据定理 3.4.5，原同余方程的解数为 3.

例 3.4.5 求解同余方程 $21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0 \pmod 7$.

解 首先，去掉系数为 7 的倍数的项，得到

$$2x^{15}-x^{10}+4x-3\equiv \pmod 7.$$

其次，作多项式的欧几里德除法，我们有

$$2x^{15}-x^{10}+4x-3=(x^7-x)(2x^8-x^3+2x^2)+(-x^4+2x^3+4x-3).$$

原同余方程等价于同余方程

$$x^4-2x^3-4x+3\equiv 0 \pmod 7.$$

直接验算 $x=0,\pm1,\pm2,\pm3$，（或 0,1,2,3,4,5,6）知同余方程无解.

例 3.4.6 求解同余方程

$$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x\equiv 0 \pmod 5.$$

解一 作多项式的欧几里德除法，我们有

$$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x$$
$$=(x^5-x)(3x^9+4x^8+2x^6+3x^5+5x^4+2x^2+4x+5)+3x^3+16x^2+6x$$

原同余方程等价于 $3x^3+16x^2+6x\equiv 3x^3+x^2+x \pmod 5$.

直接验算，解为 $x\equiv 0,1,2 \pmod 5$.

解二 由恒等同余方程 $x^p-x\equiv 0 \pmod p$ 可得，对于任意正整数 t，k，

$$x^{t+k(p-1)}\equiv x^t \pmod p.$$

特别（p=5），

$$x^{14}\equiv x^{10}\equiv x^6\equiv x^2,\quad x^{13}\equiv x^9\equiv x^5\equiv x,$$
$$x^{11}\equiv x^7\equiv x^3, \qquad \pmod 5$$

因此，原同余方程等价于 $3x^3+16x^2+6x\equiv 0 \pmod 5$.

进而等价于 $2(3x^3+16x^2+6x)\equiv x^3+2x^2+2x\equiv 0 \pmod 5$.

直接验算，同余方程的解为 $x\equiv 0,1,2 \pmod 5$.

3.4.3 素数幂模的高次同余方程——幂指数提升

因为任一正整数 m 有标准分解式

$$m=\prod_p p^{\alpha},$$

由定理 3.4.1 知，求解同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, m)$ 只需求解同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, p^{\alpha})$.

因此，我们讨论 p 为素数时，同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, p^{\alpha})$ 的解法.

设 $f(x)\equiv a_n x^n+\cdots+a_2x^2+a_1x+a_0$ 为整系数多项式，我们记

$$f'(x)\equiv na_nx^{n-1}+\cdots+2a_2x+a_1,$$

称 $f'(x)$ 为 $f(x)$ 的导式.

定理 3.4.6 设 $x\equiv x_1\ (\mathrm{mod}\, p)$ 是同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, p)$ 的一个解，且

$$(f'(x_1),p)=1,$$

则同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, p^{\alpha})$ 有解 $x\equiv x_{\alpha}\ (\mathrm{mod}\, p^{\alpha})$，其中 x_{α} 由下面关系式递归得到：

$$\begin{cases} x_i\equiv x_{i-1}+p^{i-1}t_{i-1} & (\mathrm{mod}\, p^i)\\ t_{i-1}\equiv -\dfrac{f(x_{i-1})}{p^{i-1}}\,(f'(x_1)^{-1}(\mathrm{mod}\, p)) & (\mathrm{mod}\, p)\end{cases},$$

$i=2,\cdots,\alpha$.

证 我们对 $\alpha\geq 2$ 作数学归纳法：

当 $\alpha=2$，根据假设条件，同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, p)$ 有解：

$$x=x_1+pt_1,\quad t_1=0,\pm1,\pm2,\cdots$$

所以，我们考虑关于 t_1 的同余方程 $f(x_1+pt_1)\equiv 0\ (\mathrm{mod}\, p^2)$ 的求解.

由泰勒公式，我们有 $f(x_1)+pt_1f'(x_1)\equiv 0\ (\mathrm{mod}\, p^2)$.

因为 $f(x_1)\equiv 0\ (\mathrm{mod}\, p)$，所以上述同余方程可写成

$$t_1f'(x_1)\equiv -\frac{f(x_1)}{p}\ (\mathrm{mod}\, p).$$

又因为 $(f'(x_1),p)=1$，根据定理 3.1.3，这个同余方程对模 p 有且仅有一解

$$t_1\equiv -\frac{f(x_1)}{p}\,(f'(x_1)^{-1}(\mathrm{mod}\, p))(\mathrm{mod}\, p)$$

即 $x\equiv x_2\equiv x_1+pt_1(\mathrm{mod}\, p^2)$ 是同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, p^2)$ 的解.

设 $3\leq i\leq\alpha$，假设定理对 i-1 成立，即同余方程 $f(x)\equiv 0\ (\mathrm{mod}\, p^{i-1})$ 有解

$$x=x_{i-1}+p^{i-1}t_{i-1},\quad t_{i-1}=0,\pm1,\pm2,\cdots$$

我们考虑关于t_{i-1}的同余方程 $f(x_{i-1}+p^{i-1}t_{i-1})\equiv 0\ (\mathrm{mod}\ p^i)$ 的求解.

由泰勒公式及 $p^{2(i-1)}\geq p^i$，我们有

$$f(x_{i-1})+p^{i-1}t_{i-1}f'(x_{i-1})\equiv 0\ (\mathrm{mod}\ p^i).$$

因为 $f(x_{i-1})\equiv 0\ (\mathrm{mod}\ p^{i-1})$，所以上述同余方程可写成

$$t_{i-1}f'(x_{i-1})\equiv -\frac{f(x_{i-1})}{p^{i-1}}(\mathrm{mod}\ p).$$

又因为 $f'(x_{i-1})\equiv f'(x_{i-2})\equiv\cdots\equiv f'(x_1)(\mathrm{mod}\ p)$，进而

$$(f'(x_{i-1}),p)=\cdots=(f'(x_1),p)=1.$$

根据定理 3.1.3，这个同余方程对模 p 有且仅有一解

$$\begin{aligned}t_{i-1}&\equiv -\frac{f(x_{i-1})}{p^{i-1}}(f'(x_{i-1})^{-1}(\mathrm{mod}\ p))\\&\equiv -\frac{f(x_{i-1})}{p^{i-1}}(f'(x_1)^{-1}(\mathrm{mod}\ p))\ (\mathrm{mod}\ p)\end{aligned}.$$

即 $x\equiv x_i\equiv x_{i-1}+p^{i-1}t_{i-1}(\mathrm{mod}\ p^i)$ 是同余方程 $f(x)\equiv 0\ (\mathrm{mod}\ p^i)$ 的解.

最后，根据数学归纳法原理，定理对所有 $2\leq i\leq\alpha$ 成立.

特别地，定理对 $i=\alpha$ 成立.

例 3.4.7 求解同余方程

$$f(x)\equiv x^4+7x+4\equiv 0\ (\mathrm{mod}\,27).$$

解一 由定理 3.4.6 证明过程，对于 $f(x)\equiv x^4+7x+4\ (\mathrm{mod}\,27)$，有

$$f'(x)\equiv 4x^3+7\ (\mathrm{mod}\,27).$$

直接验算，知同余方程 $f(x)\equiv 0\ (\mathrm{mod}\,3)$ 有一解

$$x_1\equiv 1(\mathrm{mod}\,3).$$

以 $x=1+3t_1$ 代入同余方程 $f(x)\equiv 0\ (\mathrm{mod}\,9)$，可得到

$$f(1)+3t_1f'(1)\equiv 0\ (\mathrm{mod}\,9).$$

因为 $f(1)\equiv 3(\mathrm{mod}\,9),\quad f'(1)\equiv 2(\mathrm{mod}\,9)$,

所以上述同余方程可写成 $3+3t_1\cdot 2\equiv 0(\mathrm{mod}\,9)$ 或 $2t_1\equiv -1(\mathrm{mod}\,3)$,

解得 $t_1\equiv 1(\mathrm{mod}\,3)$.

因此，同余方程 $f(x)\equiv 0\ (\mathrm{mod}\,9)$ 的解为

$$x_2\equiv 1+3t_1\equiv 4(\mathrm{mod}\,9).$$

再以 $x \equiv 4+9t_2$ 代入同余方程 $f(x) \equiv 0 \pmod{27}$，可得到

$$f(4)+9t_2 f'(4) \equiv 0 \pmod{27}.$$

因为 $f(4) \equiv 18 \pmod{27}$, $f'(4) \equiv 20 \pmod{27}$,

所以上述同余方程可写成

$$18+9t_2 \cdot 20 \equiv 0 \pmod{27} \text{ 或 } 2t_2 \equiv -2 \pmod{3},$$

解得 $t_2 \equiv 2 \pmod{3}$.

因此，同余方程 $f(x) \equiv 0 \pmod{27}$ 的解为

$$x_3 \equiv 4+9t_2 \equiv 22 \pmod{27}.$$

解二 由定理 3.4.6 的结论. 对于 $f(x) \equiv x^4+7x+4 \pmod{27}$，有

$$f'(x) \equiv 4x^3+7 \pmod{27}.$$

直接验算，知同余方程 $f(x) \equiv 0 \pmod{3}$ 有一解 $x_1 \equiv 1 \pmod{3}$.

首先，计算

$$\begin{aligned} f'(x) &= 4 \cdot 1^3+7 \equiv -1 \pmod{3} \\ f'(x)^{-1} &\equiv -1 \pmod{3} \end{aligned}.$$

其次，计算

$$\begin{cases} t_1 \equiv -\dfrac{f(x_1)}{3^1}(f'(x_1)^{-1} \pmod{3}) \equiv 1 & \pmod{3} \\ x_2 \equiv x_1+3t_1 \equiv 4 & \pmod{9} \end{cases}.$$

最后，计算

$$\begin{cases} t_2 \equiv -\dfrac{f(x_2)}{3^2}(f'(x_1)^{-1} \pmod{3}) \equiv 2 & \pmod{3} \\ x_3 \equiv x_2+3^2 t_2 \equiv 22 & \pmod{27} \end{cases}.$$

因此，同余方程 $f(x) \equiv 0 \pmod{27}$ 的解为

$$x_3 \equiv 22 \pmod{27}.$$

例 3.4.8 解同余方程 $f(x)=3x^4+2x^3+x^2+x+2 \equiv 0 \left(\bmod\ 3^3 \times 2^2\right)$.

解 导式有

$$f'(x)=12x^3+6x^2+2x+1.$$

（1）解同余方程 $f(x)=3x^4+2x^3+x^2+x+2 \equiv 0 \left(\bmod\ 2^2\right)$.

$x \pmod 2$	0	1

$f(x)(\mathrm{mod}\ 2)$	0	1
是解否	是	否

即 $x\equiv 0(\mathrm{mod}\ 2)$ 是 $f(x)=3x^4+2x^3+x^2+x+2\equiv 0(\mathrm{mod}\ 2)$ 的 1 个解.

将 $x\equiv 0(\mathrm{mod}\ 2)$，即 $x=2y_1$，代入 $f(x)\equiv 0(\mathrm{mod}\ 2^2)$ 得,

$$f(0)+2y_1 f'(0)\equiv 0(\mathrm{mod}\ 2^2),$$

由于 $f(0)\equiv 2(\mathrm{mod}\ 2^2)$，$f'(0)\equiv 1\not\equiv 0(\mathrm{mod}\ 2^2)$，所以有唯一解：$y_1=1+2y_2$，即 $x=2+2^2y_2\equiv 2(\mathrm{mod}\ 2^2)$.

所以同余方程 $f(x)=3x^4+2x^3+x^2+x+2\equiv 0(\mathrm{mod}\ 2^2)$ 有一个解:

$$x\equiv 2(\mathrm{mod}\ 2^2).$$

（2）解同余方程 $f(x)=3x^4+2x^3+x^2+x+2\equiv 0(\mathrm{mod}\ 3^3)$.

x（mod 3）	0	1	2
$f(x)(\mathrm{mod}\ 3)$	2	0	0
是解否	否	是	是

即 $x\equiv 1,2(\mathrm{mod}\ 3)$ 是 $f(x)=3x^4+2x^3+x^2+x+2\equiv 0(\mathrm{mod}\ 3)$ 的两个解.

① 将 $x\equiv 1(\mathrm{mod}\ 3)$，即 $x=1+3y_1$，代入 $f(x)\equiv 0(\mathrm{mod}\ 3^2)$ 得

$$f(1)+3y_1 f'(1)\equiv 0(\mathrm{mod}\,3^2),$$

由于 $f'(1)\equiv 0(\mathrm{mod}\,3), f(1)\equiv 0(\mathrm{mod}\,3^2)$，所以有 3 个解：$y_1=(0,1,2)+3y_2$，即 $x=1+3\times(0,1,2)+3^2y_2=(1,4,7)+3^2y_2$.

将 $x=1+3^2y_2$ 代入 $f(x)\equiv 0(\mathrm{mod}\ 3^2)$ 得，$f(1)+3^2y_2 f'(1)\equiv 0(\mathrm{mod}\ 3^3)$，

由于 $f'(1)\equiv 0(\mathrm{mod}\ 3)$，$f(1)\equiv 9\not\equiv 0(\mathrm{mod}\ 3^2)$，所以无解.

将 $x=4+3^2y_2$ 代入 $f(x)\equiv 0(\mathrm{mod}\ 3^2)$ 得，$f(4)+3^2y_2 f'(4)\equiv 0(\mathrm{mod}\ 3^3)$，

由于 $f'(4)\equiv 0(\mathrm{mod}\ 3)$，$f(4)\equiv 0(\mathrm{mod}\ 3^3)$，所以有 3 个解：$y_2=(0,1,2)+3y_3$，即 $x=4+3^2\times(0,1,2)+3^3y_3=4,13,22(\mathrm{mod}\ 3^3)$.

将 $x=7+3^2y_2$ 代入 $f(x)\equiv 0(\mathrm{mod}\ 3^3)$ 得，$f(7)+3^2y_2 f'(7)\equiv 0(\mathrm{mod}\ 3^3)$，

由于 $f'(7)\equiv 0(\mathrm{mod}\ 3)$，$f(7)\equiv 9\not\equiv 0(\mathrm{mod}\ 3^3)$，所以无解.

因此，这时有解 $x=4,13,22\left(\mathrm{mod}\ 3^3\right)$.

② 将 $x\equiv 2\left(\mathrm{mod}\ 3\right)$，即 $x=2+3y_1$，代入 $f(x)\equiv 0\left(\mathrm{mod}\ 3^2\right)$ 得,

$$f(2)+3y_1 f'(2)\equiv 0\left(\mathrm{mod}\ 3^3\right),$$

由于 $f'(2)\equiv 0\left(\mathrm{mod}\ 3\right), f(2)\equiv 0\left(\mathrm{mod}\ 3^2\right)$，所以有唯一解： $y_1=3y_2$

即 $x=2+3^2 y_2$.

将 $x=2+3^2 y_2$ 代入 $f(\mathrm{x})\equiv 0\left(\mathrm{mod}\ 3^3\right)$ 得,

$$f(2)+3^2 y_2 f'(2)\equiv 0\left(\mathrm{mod}\ 3^3\right),$$

由于 $f'(2)\equiv 2\not\equiv 0\left(\mathrm{mod}\ 3\right)$， $f(2)\equiv 18\not\equiv 2\times 3^2\left(\mathrm{mod}\ 3^3\right)$，所以有唯一解:

$y_2=2+3y_3$，即 $x=2+3^2\times 2+3^3 y_3\equiv 20\left(\mathrm{mod}\ 3^3\right)$,

因此，这时有解 $x\equiv 20\ \left(\mathrm{mod}\ 3^3\right)$.

所以同余方程 $f(x)=3x^4+2x^3+x^2+x+2\equiv 0\left(\mathrm{mod}\ 3^3\right)$ 有 4 个解:

$$x=4,13,20,22\ \left(\mathrm{mod}\ 3^3\right).$$

(3) $f(x)\equiv 0\left(\mathrm{mod}\ 2^2\times 3^3\right)$ 的解由同余方程组

$$\begin{cases} x\equiv a\left(\mathrm{mod}\ 2^2\right) \\ x\equiv b\left(\mathrm{mod}\ 3^3\right) \end{cases}$$

给出，其中

$$(a,\ b)=(2,4),(2,13),(2,20),(2,22).$$

由中国剩余定理得， $f(x)\equiv 0\left(\mathrm{mod}\ 2^2\times 3^3\right)$ 有 4 个解:

$$x\equiv 3^3\times 3a+2^2\times 7b\equiv 58\text{，}94\text{，}74\text{，}22\left(\mathrm{mod}\ 2^2\times 3^3\right).$$

另外，也可以利用欧拉定理，费马小定理和同余方程的多项式次数的定义来化简同余方程并求解.

例 3.4.9 解同余方程 $f(x)=5x^7+x+3\equiv 0\left(\mathrm{mod}\ 3^2\times 7\times 5\right)$.

解 (1) 利用欧拉定理，当 $\left(x,3^2\right)=1$ 时,

$$f(x)=5x^7+x+3\equiv 5x+x+3\equiv 6x+3\equiv 0\left(\mathrm{mod}\ 3^2\right)\text{有解}$$

$$x=1,4,7\left(\mathrm{mod}\ 3^2\right);$$

当$\left(x,3^2\right)\neq 1$，即$x=(0,3,6)\left(\mathrm{mod}\ 3^2\right)$时，

$f(x)=5x^7+x+3\equiv(3,6,0)\left(\mathrm{mod}\ 3^2\right)$有解$x=6\left(\mathrm{mod}\ 3^2\right)$，

所以$f(x)=5x^7+x+3\equiv 0\left(\mathrm{mod}\ 3^2\right)$有解$x=1,4,6,7\left(\mathrm{mod}\ 3^2\right)$.

（2）利用费马小定理得，

$$f(x)=5x^7+x+3\equiv 5x+x+3\equiv 6x+3\equiv 0\left(\mathrm{mod}\ 7\right)$$

有解$x=3\left(\mathrm{mod}\ 7\right)$.

（3）利用同余方程的多项式次数的定义得，

$f(x)=5x^7+x+3\equiv x+3\equiv 0\left(\mathrm{mod}\ 5\right)$有解$x=\left(\mathrm{mod}5\right)$.

最后，$f(\mathrm{x})\equiv 0\left(\mathrm{mod}\ 3^2\times 7\times 5\right)$的解由同余方程组

$$\begin{cases} x\equiv a\left(\mathrm{mod}\ 3^2\right) \\ x\equiv b\left(\mathrm{mod}\ 7\right) \\ x\equiv c\left(\mathrm{mod}\ 5\right) \end{cases}$$

给出，其中$(a,b,c)=(1,3,2),(4,3,2),(6,3,2),(7,3,2)$，

由中国剩余定理得到，$f(x)\equiv 0\left(\mathrm{mod}\ 3^2\times 7\times 5\right)$有四个解，

$x\equiv 7\times 5\times(-1)a+3^2\times 5\times 5b+3^2\times 7\times 2c\equiv\ 262,157,87,52\left(\mathrm{mod}\ 3^2\times 7\times 5\right)$.