

第四章 二次同余
2015年04月21日



信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 1 页 共 130 页

返回

全屏显示

关闭

退出



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院





*第四章 二次同余式与平方剩余

思考题:

模为素数 p 的二次同余式

$$x^2 \equiv a \pmod{p}, \quad (a, p) = 1. \quad (1)$$

1. 同余式(5)有解的判断?
2. 同余式(5)有解的个数?
3. 同余式(5)求解的方法和过程?

Rabin 密码系统: $n = p \cdot q$

加密: $m^2 \equiv a \pmod{p \cdot q}$

解密: $x^2 \equiv a \pmod{p \cdot q}$

[访问主页](#)[标题页](#)[目录页](#)[«](#) [»](#)[◀](#) [▶](#)

第 2 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



*第四章 二次同余式与平方剩余

本章主要讨论如下问题.

1. 二次同余式的基本概念
2. 模平方剩余与模平方非剩余
3. 勒让得符号 二次互反律
4. 二次同余式有解的判断
5. 高斯引理 二次互反律之证明
6. 雅克比符号
7. 模 p 平方根的计算
8. 椭圆曲线点的计算

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 3 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

4.1 一般二次同余式

二次同余式的一般形式是

$$ax^2 + bx + c \equiv 0 \pmod{m} \quad (2)$$

其中 $m \nmid a$. 因为

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

所以二次同余式(1)式等价于同余式组:

$$\begin{cases} ax^2 + bx + c \equiv 0 \pmod{p_1^{\alpha_1}}, \\ \dots\dots\dots \\ ax^2 + bx + c \equiv 0 \pmod{p_k^{\alpha_k}}. \end{cases}$$

故只需讨论模为 p^α 同余式:

$$ax^2 + bx + c \equiv 0 \pmod{p^\alpha}, \quad p \nmid a. \quad (3)$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 4 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



$$\underline{ax^2 + bx + c \equiv 0 \pmod{p^\alpha}}$$

将(3) 的两端同乘 $4a$, 得到

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p^\alpha}$$

或

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p^\alpha}.$$

令 $y = 2ax + b$, 有

$$y^2 \equiv b^2 - 4ac \pmod{p^\alpha}.$$

特别地, 当 p 是奇素数时, $(2a, p) = 1$. 上述同余式等价于(3).

[访问主页](#)[标题页](#)[目录页](#)[◀◀](#) [▶▶](#)[◀](#) [▶](#)[第 5 页 共 130 页](#)[返 回](#)[全屏显示](#)[关 闭](#)[退 出](#)



定义4.1.1 若同余式

$$x^2 \equiv a \pmod{m}, \quad (a, m) = 1 \quad (4)$$

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).

问题:

- 1) 整数 a 模 m 平方剩余与实数中平方根 \sqrt{a} 有什么区别?
- 2) 如何判断同余式(4) 有解?
- 3) 如何求同余式(4) 的解?

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 6 页 共 130 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.1.1 1 是模4 平方剩余, -1 是模4 平方非剩余.

例4.1.2 1, 2, 4 是模7 平方剩余, -1 , 3, 5 是模7 平方非剩余.

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

例4.1.3 -1 , 1, 2, 4, 8, 9, 13, 15 是模17 平方剩余;

3, 5, 6, 7, 10, 11, 12, 14 是模17 平方非剩余. 因为

$$\begin{aligned} 1^2 \equiv 16^2 \equiv 1, \quad 2^2 \equiv 15^2 \equiv 4, \quad 3^2 \equiv 14^2 \equiv 9, \quad 4^2 \equiv 13^2 \equiv 16 \equiv -1, \\ 5^2 \equiv 12^2 \equiv 8, \quad 6^2 \equiv 11^2 \equiv 2, \quad 7^2 \equiv 10^2 \equiv 15, \quad 8^2 \equiv 9^2 \equiv 13 \pmod{17}. \end{aligned}$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 7 页 共 130 页](#)[返 回](#)[全屏显示](#)[关 闭](#)[退 出](#)



例4.1.4 求满足方程 $E: y^2 = x^3 + x + 1 \pmod{7}$ 的所有点 (x, y) .

解 对 $x = 0, 1, 2, 3, 4, 5, 6$, 分别求出 y .

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

$$x = 1, y^2 = 3 \pmod{7}, \quad \text{无解},$$

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

$$x = 3, y^2 = 3 \pmod{7}, \quad \text{无解},$$

$$x = 4, y^2 = 6 \pmod{7}, \quad \text{无解},$$

$$x = 5, y^2 = 5 \pmod{7}, \quad \text{无解},$$

$$x = 6, y^2 = 6 \pmod{7}, \quad \text{无解}.$$

共有4个点.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 8 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.1.5 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 .

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

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

$$x = 2, y^2 = 5 \pmod{7}, \quad \text{无解},$$

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

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

$$x = 5, y^2 = 6 \pmod{7}, \quad \text{无解},$$

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

共有8个点.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第9页共130页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.1.6 求满足方程 $E : y^2 = x^3 + 2x - 1 \pmod{7}$ 的所有点.

解 对 $x = 0, 1, 2, 3, 4, 5, 6$, 分别求出 y .

$x = 0, y^2 = 6 \pmod{7}$, 无解,

$x = 1, y^2 = 2 \pmod{7}$, $y = 3, 4 \pmod{7}$,

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

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

$x = 4, y^2 = 1 \pmod{7}$, $y = 1, 6 \pmod{7}$,

$x = 5, y^2 = 1 \pmod{7}$, $y = 1, 6 \pmod{7}$,

$x = 6, y^2 = 3 \pmod{7}$, 无解,

共有10个点.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 10 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.1.7 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 .

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

$$x = 1, y^2 = 1 \pmod{7}, \quad y = 1, 6 \pmod{7},$$

$$x = 2, y^2 = 0 \pmod{7}, \quad y = 0 \pmod{7},$$

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

$$x = 4, y^2 = 5 \pmod{7}, \quad \text{无解},$$

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

$$x = 6, y^2 = 1 \pmod{7}, \quad y = 1, 6 \pmod{7}.$$

共有11 个点.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 11 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.1.8 求满足方程 $E: y^2 = x^3 + 3x - 1 \pmod{7}$ 的所有点.

解 对 $x = 0, 1, 2, 3, 4, 5, 6$, 分别求出 y .

$x = 0, y^2 = 6 \pmod{7}$, 无解,

$x = 1, y^2 = 3 \pmod{7}$, 无解,

$x = 2, y^2 = 6 \pmod{7}$, 无解,

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

$x = 4, y^2 = 5 \pmod{7}$, 无解,

$x = 5, y^2 = 6 \pmod{7}$, 无解,

$x = 6, y^2 = 2 \pmod{7}$, $y = 3, 4 \pmod{7}$,

共有3个点.

访问主页

标题页

目录页



第 12 页 共 130 页

返回

全屏显示

关闭

退出



例4.1.9 求解同余式 $x^2 \equiv 46 \pmod{105}$.

解 因为 $105 = 3 \cdot 5 \cdot 7$, 原同余式等价于同余式组:

$$\begin{cases} x^2 \equiv 46 \equiv 1 \pmod{3} \\ x^2 \equiv 46 \equiv 1 \pmod{5} \\ x^2 \equiv 46 \equiv 4 \pmod{7} \end{cases}$$

分别求出三个同余式的解为:

$$x = x_1 \equiv \pm 1 \pmod{3}, \quad x = x_2 \equiv \pm 1 \pmod{5}, \quad x = x_1 \equiv \pm 2 \pmod{7},$$

由物不知数和中国剩余定理即得解为:

$$x = 1 \cdot 70 + 1 \cdot 21 + 2 \cdot 15 = 121 \equiv 16 \pmod{105}$$

$$x = 1 \cdot 70 + 1 \cdot 21 + (-2) \cdot 15 = 61 \equiv 61 \pmod{105}$$

$$x = 1 \cdot 70 + (-1) \cdot 21 + 2 \cdot 15 = 79 \equiv 79 \pmod{105}$$

$$x = 1 \cdot 70 + (-1) \cdot 21 + (-2) \cdot 15 = 19 \equiv 19 \pmod{105}$$

$$x = (-1) \cdot 70 + 1 \cdot 21 + 2 \cdot 15 = -19 \equiv 86 \pmod{105}$$

$$x = (-1) \cdot 70 + 1 \cdot 21 + (-2) \cdot 15 = -79 \equiv 26 \pmod{105}$$

$$x = (-1) \cdot 70 + (-1) \cdot 21 + 2 \cdot 15 = -62 \equiv 44 \pmod{105}$$

$$x = (-1) \cdot 70 + (-1) \cdot 21 + (-2) \cdot 15 = -121 \equiv 89 \pmod{105}$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 13 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.1.10 求解同余式 $x^2 \equiv 1219 \pmod{2310}$.

解 因为 $2310 = 5 \cdot 6 \cdot 7 \cdot 11$, 原同余式等价于同余式组:

$$\begin{cases} x^2 \equiv 1219 \equiv 4 \pmod{5} \\ x^2 \equiv 1219 \equiv 1 \pmod{6} \\ x^2 \equiv 1219 \equiv 1 \pmod{7} \\ x^2 \equiv 1219 \equiv 9 \pmod{11} \end{cases}$$

分别求出三个同余式的解为:

$$x = x_1 \equiv \pm 2 \pmod{5}, \quad x = x_2 \equiv \pm 1 \pmod{6},$$

$$x = x_3 \equiv \pm 1 \pmod{7}, \quad x = x_4 \equiv \pm 3 \pmod{7},$$

由韩信点兵和中国剩余定理即得解为:

$$x \equiv b_1 \cdot 1386 + b_2 \cdot 385 + b_3 \cdot 330 + b_4 \cdot 210 \pmod{2310}$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 14 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



$$x = 2 \cdot 1386 + 1 \cdot 385 + 1 \cdot 330 + 3 \cdot 210 = 4117 \equiv 1807 \pmod{2310}$$

$$x = 2 \cdot 1386 + 1 \cdot 385 + 1 \cdot 330 + (-3) \cdot 210 = 2857 \equiv 547 \pmod{2310}$$

$$x = 2 \cdot 1386 + 1 \cdot 385 + (-1) \cdot 330 + 3 \cdot 210 = 3457 \equiv 1147 \pmod{2310}$$

$$x = 2 \cdot 1386 + 1 \cdot 385 + (-1) \cdot 330 + (-3) \cdot 210 = 2197 \equiv 2197 \pmod{2310}$$

$$x = 2 \cdot 1386 + (-1) \cdot 385 + 1 \cdot 330 + 3 \cdot 210 = 3347 \equiv 1037 \pmod{2310}$$

$$x = 2 \cdot 1386 + (-1) \cdot 385 + 1 \cdot 330 + (-3) \cdot 210 = 2087 \equiv 2087 \pmod{2310}$$

$$x = 2 \cdot 1386 + (-1) \cdot 385 + (-1) \cdot 330 + 3 \cdot 210 = 2687 \equiv 377 \pmod{2310}$$

$$x = 2 \cdot 1386 + (-1) \cdot 385 + (-1) \cdot 330 + (-3) \cdot 210 = 1427 \equiv 1427 \pmod{2310}$$

$$x = (-2) \cdot 1386 + 1 \cdot 385 + 1 \cdot 330 + 3 \cdot 210 = -1427 \equiv 883 \pmod{2310}$$

$$x = (-2) \cdot 1386 + 1 \cdot 385 + 1 \cdot 330 + (-3) \cdot 210 = -2687 \equiv 1933 \pmod{2310}$$

$$x = (-2) \cdot 1386 + 1 \cdot 385 + (-1) \cdot 330 + 3 \cdot 210 = -2087 \equiv 223 \pmod{2310}$$

$$x = (-2) \cdot 1386 + 1 \cdot 385 + (-1) \cdot 330 + (-3) \cdot 210 = -3347 \equiv 1273 \pmod{2310}$$

$$x = (-2) \cdot 1386 + (-1) \cdot 385 + 1 \cdot 330 + 3 \cdot 210 = -2197 \equiv 113 \pmod{2310}$$

$$x = (-2) \cdot 1386 + (-1) \cdot 385 + 1 \cdot 330 + (-3) \cdot 210 = -3457 \equiv 1163 \pmod{2310}$$

$$x = (-2) \cdot 1386 + (-1) \cdot 385 + (-1) \cdot 330 + 3 \cdot 210 = -2857 \equiv 1763 \pmod{2310}$$

$$x = (-2) \cdot 1386 + (-1) \cdot 385 + (-1) \cdot 330 + (-3) \cdot 210 = -4117 \equiv 503 \pmod{2310}$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 15 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



4.2 模为奇素数的平方剩余与平方非剩余

讨论模为素数 p 的二次同余式

$$x^2 \equiv a \pmod{p}, \quad (a, p) = 1. \quad (5)$$

定理4.2.1 (欧拉判别条件) 设 p 是奇素数, $(a, p) = 1$. 则

(i) a 是模 p 的平方剩余的充分必要条件是

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}; \quad (6)$$

(ii) a 是模 p 的平方非剩余的充分必要条件是

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (7)$$

并且当 a 是模 p 的平方剩余时, 同余式(5)恰有二解.

[访问主页](#)[标题页](#)[目录页](#)[«](#) [»](#)[◀](#) [▶](#)

第 16 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



证 (i) 因为 p 是奇素数, 所以有表达式

$$\begin{aligned}x^p - x &= x\left((x^2)^{\frac{p-1}{2}} - a^{\frac{p-1}{2}}\right) + (a^{\frac{p-1}{2}} - 1)x \\&= x \cdot q(x) \cdot (x^2 - a) + (a^{\frac{p-1}{2}} - 1)x,\end{aligned}$$

其中 $q(x)$ 是 x 的整系数多项式.

若 a 是模 p 的平方剩余, 即

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

有二个解 x , 根据§3.4 定理3.4.5, 余式的系数被 p 整除, 即

$$p \mid a^{\frac{p-1}{2}} - 1.$$

所以(6)成立.

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 17 页 共 130 页

返回

全屏显示

关闭

退出



反过来, 若(6)成立, 则同样根据§3.4 定理3.4.5, 我们有同余式

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

有解, 即 a 是模 p 平方剩余.

(ii) 因为 p 是奇素数, $(a, p) = 1$, 根据欧拉定理(§2.4 定理2.4.1), 我们有表达式

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

再根据§1.4 定理1.4.2, 我们有

$$p \mid a^{\frac{p-1}{2}} - 1 \quad \text{或} \quad p \mid a^{\frac{p-1}{2}} + 1.$$

因此, 结论(i)告诉我们: a 是模 p 的平方非剩余的充分必要条件是

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

证毕



访问主页

标题页

目录页

◀ ▶

◀ ▶

第 18 页 共 130 页

返回

全屏显示

关闭

退出



例4.2.1 判断137 是否为模227 平方剩余.

解 根据定理4.2.1, 我们要计算:

$$137^{(227-1)/2} = 137^{113} \pmod{227}.$$

运用模重复平方法. 设 $m = 227$, $b = 137$. 令 $a = 1$. 将113 写成二进制, $113 = 1 + 2^4 + 2^5 + 2^6$.

我们依次计算如下:

- 1). $n_0 = 1$. 计算 $a_0 = a \cdot b^{n_0} \equiv 137$, $b_1 \equiv b^2 \equiv 155 \pmod{m}$.
- 2). $n_1 = 0$. 计算 $a_1 = a_0 \cdot b_1^{n_1} \equiv 137$, $b_2 \equiv b_1^2 \equiv 190 \pmod{m}$.
- 3). $n_2 = 0$. 计算 $a_2 = a_1 \cdot b_2^{n_2} \equiv 137$, $b_3 \equiv b_2^2 \equiv 7 \pmod{m}$.
- 4). $n_3 = 0$. 计算 $a_3 = a_2 \cdot b_3^{n_3} \equiv 137$, $b_4 \equiv b_3^2 \equiv 49 \pmod{m}$.
- 5). $n_4 = 1$. 计算 $a_4 = a_3 \cdot b_4^{n_4} \equiv 130$, $b_5 \equiv b_4^2 \equiv 131 \pmod{m}$.
- 6). $n_5 = 1$. 计算 $a_5 = a_4 \cdot b_5^{n_5} \equiv 5$, $b_6 \equiv b_5^2 \equiv 136 \pmod{m}$.
- 7). $n_6 = 1$. 计算 $a_6 = a_5 \cdot b_6^{n_6} \equiv 226 \equiv -1 \pmod{m}$.

因此, 137 为模227 平方非剩余.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 19 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



推论 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 $a_1 \cdot a_2$ 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 $a_1 \cdot a_2$ 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 $a_1 \cdot a_2$ 是模 p 的平方非剩余.

证 因为

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

所以由定理4.2.1即得结论.

证毕

[访问主页](#)

[标题页](#)

[目录页](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

第 20 页 共 130 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





定理4.2.2 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 $\frac{p-1}{2}$, 且 $\frac{p-1}{2}$ 个平方剩余与序列:

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \quad (8)$$

中的一个数同余, 且仅与一个数同余.

证 由定理4.2.1, 平方剩余的个数等于 $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

的解数. 但 $x^{\frac{p-1}{2}} - 1 \mid x^{p-1} - 1$.

由定理3.4.5, 此同余式的解数是 $\frac{p-1}{2}$, 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(8)中有两个数模 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 $1 \leq k_1, k_2 \leq (p-1)/2$, 故

$2 \leq k_1 + k_2 \leq p-1 < p$, $|k_1 - k_2| \leq p-1 < p$.

从而, $k_1 = k_2$. 矛盾.

证毕

访问主页

标题页

目录页

« »

◀ ▶

第 21 页 共 130 页

返回

全屏显示

关闭

退出





4.3 勒让得符号

§4.2 定理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4.3.1 设 p 是素数. 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4.3.1 根据§4.1 例4.1.3, 我们有

$$\left(\frac{-1}{17}\right) = \left(\frac{1}{17}\right) = \left(\frac{2}{17}\right) = \left(\frac{4}{17}\right) = \left(\frac{8}{17}\right) = \left(\frac{9}{17}\right) = \left(\frac{13}{17}\right) = \left(\frac{15}{17}\right) = 1;$$

$$\left(\frac{3}{17}\right) = \left(\frac{5}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{11}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{14}{17}\right) = -1.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 22 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

利用勒让得符号, 可将§4.2 定理4.2.1 叙述为:

定理4.3.1 (欧拉判别法则) 对任意整数 a ,

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

证 根据定义及定理4.2.1, 我们有

$$\left(\frac{a}{p}\right) = 1 \iff a \text{ 是模 } p \text{ 平方剩余} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

和

$$\left(\frac{a}{p}\right) = -1 \iff a \text{ 是模 } p \text{ 平方非剩余} \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

以及

$$\left(\frac{a}{p}\right) = 0 \iff p \mid a \iff a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$$

所以定理成立.

证毕



访问主页

标题页

目录页

◀ ▶

◀ ▶

第 23 页 共 130 页

返回

全屏显示

关闭

退出





例4.3.2 证明2 是模17 平方剩余; 3 是模17 平方非剩余.

因为 $(17 - 1)/2 = 2^3$, 且有

$$2^2 \equiv 4, \quad 2^4 \equiv 4^2 \equiv -1, \quad 2^8 \equiv (-1)^2 \equiv 1 \pmod{17};$$

$$3^2 \equiv 9, \quad 3^4 \equiv 9^2 \equiv -4, \quad 3^8 \equiv (-4)^2 \equiv -1 \pmod{17}.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 24 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

定理4.3.2 设 p 是奇素数, 则

$$(1) \left(\frac{1}{p}\right) = 1; \quad (9)$$

$$(2) \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \quad (10)$$

证 根据欧拉判别法则(定理4.3.1),

对于 $a = 1$ 时, 有

$$a^{\frac{p-1}{2}} = 1,$$

所以(9)成立;

而对于 $a = -1$ 时, 有

$$a^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}},$$

又因为 p 是奇数, 所以(10)成立.

证毕



访问主页

标题页

目录页

◀ ▶

◀ ▶

第 25 页 共 130 页

返回

全屏显示

关闭

退出





推论 设 p 是奇素数, 那么

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

证 根据欧拉判别法则, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

若 $p \equiv 1 \pmod{4}$, 则 $p = 4k + 1$,

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

若 $p \equiv 3 \pmod{4}$, 则 $p = 4k + 3$,

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

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 26 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.3.3 判断同余式

$$x^2 \equiv -1 \pmod{365}$$

是否有解, 有解时, 求出其解数.

解 $365 = 5 \cdot 73$ 不是素数, 原同余式等价于:

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

因为

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

故同余式组有解. 原同余式有解, 解数为4.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 27 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

下面我们给出勒让得符号的函数性质(周期性和完全可乘性):

定理4.3.3 设 p 是奇素数, 则

$$(i) \text{ (周期性)} \quad \left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right); \quad (11)$$

$$(ii) \text{ (完全可乘性)} \quad \left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right); \quad (12)$$

$$(iii) \text{ 设 } (a, p) = 1, \text{ 则 } \left(\frac{a^2}{p}\right) = 1. \quad (13)$$

证 (i) 因为同余式 $x^2 \equiv a + p \pmod{p}$

等价于同余式 $x^2 \equiv a \pmod{p}$,

所以

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

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 28 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

(ii) 根据欧拉判别法则(定理4.3.1), 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 $\left(\frac{a \cdot b}{p}\right) \equiv (a \cdot b)^{\frac{p-1}{2}} \pmod{p}$.

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

因为勒让得符号取值 ± 1 , 且 p 是奇素数, 所以我们有

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

(iii) 由(ii) 立即得到.

证毕

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

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



访问主页

标题页

目录页

◀ ▶

◀ ▶

第 29 页 共 130 页

返回

全屏显示

关闭

退出



4.3.2 高斯引理

对于一个与 p 互素的整数 a , Gauss 给出了另一判别法则, 以判断 a 是否为模 p 二次剩余.

引理4.3.1 (Gauss) 设 p 是奇素数. a 是整数, $(a, p) = 1$. 如果整数

$$a \cdot 1, a \cdot 2, \dots, a \cdot \frac{p-1}{2}$$

中模 p 的最小正剩余大于 $\frac{p}{2}$ 的个数是 m , 则

$$\left(\frac{a}{p}\right) = (-1)^m. \quad (14)$$

证 设 a_1, \dots, a_t 是 $a \cdot 1, a \cdot 2, \dots, a \cdot \frac{p-1}{2}$ 模 p 的小于 $\frac{p}{2}$ 的最小正剩余, b_1, \dots, b_m 是这些整数模 p 的大于 $\frac{p}{2}$ 的最小正剩余, 则

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

[访问主页](#)[标题页](#)[目录页](#)[<<](#)[>>](#)[<](#)[>](#)

第 30 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



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

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

$$a \cdot k_i \equiv p - a \cdot k_j, \quad \text{或} \quad a \cdot k_i + a \cdot k_j \equiv 0 \pmod{p}.$$

因而 $k_i + k_j \equiv 0 \pmod{p}$, 这不可能, 因为

$$1 \leq k_i + k_j \leq \frac{p-1}{2} + \frac{p-1}{2} < p.$$

这样, $a_1, \dots, a_t, p - b_1, \dots, p - b_m$ 是 $1, \dots, \frac{p-1}{2}$ 的一个排列,

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

$$\text{因而, } a^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p}. \quad \left(\frac{a}{p} \right) = (-1)^m.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 31 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



下面我们给出2 是否为模 p 平方剩余的判断, 以及将判断 a 是否为模 p 平方剩余转化为整数个数的计算($T(a, p) = \sum_{k=1}^{(p-1)/2} \left[\frac{a \cdot k}{p} \right]$).

定理4.3.4 p 是奇素数.

$$(i) \quad \left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}. \quad (15)$$

$$(ii) \quad \text{若 } (a, 2p) = 1, \text{ 则 } \left(\frac{a}{p} \right) = (-1)^{T(a, p)}. \quad (16)$$

证: 因为

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

对 $k = 1, \dots, \frac{p-1}{2}$ 求和, 并记 $T(a, p) = \sum_{k=1}^{(p-1)/2} \left[\frac{a \cdot k}{p} \right]$, 我们有

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 32 页 共 130 页

返回

全屏显示

关闭

退出





$$\begin{aligned} a \cdot \frac{p^2 - 1}{8} &= T(a, p) \cdot p + \sum_{i=1}^t a_i + \sum_{j=1}^m b_j \\ &= T(a, p) \cdot p + \sum_{i=1}^t a_i + \sum_{j=1}^m (p - b_j) + 2 \sum_{j=1}^m b_j - m \cdot p \\ &= T(a, p) \cdot p + \frac{p^2 - 1}{8} - m \cdot p + 2 \sum_{j=1}^m b_j, \end{aligned}$$

因此,

$$(a - 1) \cdot \frac{p^2 - 1}{8} \equiv T(a, p) + m \pmod{2}.$$

若 $a = 2$, 则对于 $0 \leq k \leq \frac{p-1}{2}$, 有 $0 \leq \left\lfloor \frac{a \cdot k}{p} \right\rfloor \leq \left\lfloor \frac{p-1}{p} \right\rfloor = 0$, 从

而 $T(a, p) = 0$, 因而 $m \equiv \frac{p^2 - 1}{8} \pmod{2}$;

若 a 为奇数, 则 $m \equiv T(a, p) \pmod{2}$.

故由引理4.3.1知定理成立.

证毕

访问主页

标题页

目录页

◀

▶

◀

▶

第 33 页 共 130 页

返回

全屏显示

关闭

退出





例4.3.4 判断2, 3 是否为模17 平方剩余.

解 1) 根据定理4.3.4 (i), 我们有

$$\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = (-1)^{2 \cdot 18} = 1.$$

因此, 2 是模17 平方剩余.

2) 根据定理.4.4.1 (ii),

$$T(3, 17) = \sum_{k=1}^{(17-1)/2} \left[\frac{3 \cdot k}{17}\right] = \left[\frac{3 \cdot 6}{17}\right] + \left[\frac{3 \cdot 7}{17}\right] + \left[\frac{3 \cdot 8}{17}\right] = 1 + 1 + 1 = 3,$$

所以3 是模17 平方非剩余.

证毕

[访问主页](#)

[标题页](#)

[目录页](#)

[«](#) [»](#)

[◀](#) [▶](#)

第 34 页 共 130 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)



例4.3.5 假设 $p = 8k + 5$ 为素数. 则2 为模 p 平方非剩余.

证 计算勒让得符号

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8k+5)^2-1}{8}} = (-1)^{(4k+3)(2k+1)} = -1,$$

2 为模 p 平方非剩余.

证毕

例4.3.6 判断同余式

$$x^2 \equiv 2 \pmod{3599}$$

是否有解, 有解时求出其解数.

解 $3599 = 59 \cdot 61$ 不是素数, 原同余式等价于:

$$\begin{cases} x^2 \equiv 2 \pmod{59}, \\ x^2 \equiv 2 \pmod{61}. \end{cases}$$

因为 $\left(\frac{2}{59}\right) = (-1)^{\frac{59^2-1}{8}} = -1,$

故同余式组无解. 原同余式无解.



访问主页

标题页

目录页

◀ ▶

◀ ▶

第 35 页 共 130 页

返回

全屏显示

关闭

退出





推论 设 p 是奇素数, 那么

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{若 } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{若 } p \equiv \pm 3 \pmod{8}. \end{cases}$$

证 根据定理3 (i), 我们有

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

若 $p \equiv \pm 1 \pmod{8}$, 则存在整数 k 使得 $p = 8k \pm 1$. 从而

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

若 $p \equiv \pm 3 \pmod{8}$, 则存在整数 k 使得 $p = 8k \pm 3$. 从而

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2(4k^2 \pm 3k) + 1} = -1.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#)[▶](#)[◀](#)[▶](#)[第 36 页 共 130 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)

4.4 二次互反律

设 p, q 是不同的奇素数. 我们要问二次同余式

$$x^2 \equiv q \pmod{p} \quad (17)$$

与二次同余式

$$x^2 \equiv p \pmod{q} \quad (18)$$

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. 下面的定理(二次互反律)给出了明确的回答. 同时, 基于勒让得符号的函数性质、二次互反律以及欧几里得除法, 我们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4.4.1 (二次互反律) 若 p, q 是互素奇素数, 则

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) \quad (19)$$

[访问主页](#)[标题页](#)[目录页](#)[«](#) [»](#)[◀](#) [▶](#)

第 37 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



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年作出的, 随后他又发现了另外七个不同的证明. 在《算数研究》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200个不同的证明。

[访问主页](#)[标题页](#)[目录页](#)[«](#) [»](#)[◀](#) [▶](#)

第 38 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



证 我们要证明:

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

因为 $(2, pq) = 1$), 根据定理4.3.4 ,我们有

$$\left(\frac{q}{p}\right) = (-1)^{T(q,p)}, \quad \left(\frac{p}{q}\right) = (-1)^{T(p,q)},$$

其中 $T(q, p) = \sum_{h=1}^{\frac{p-1}{2}} \left[\frac{q \cdot h}{p} \right]$, $T(p, q) = \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{p \cdot k}{q} \right]$, 所以只需证明

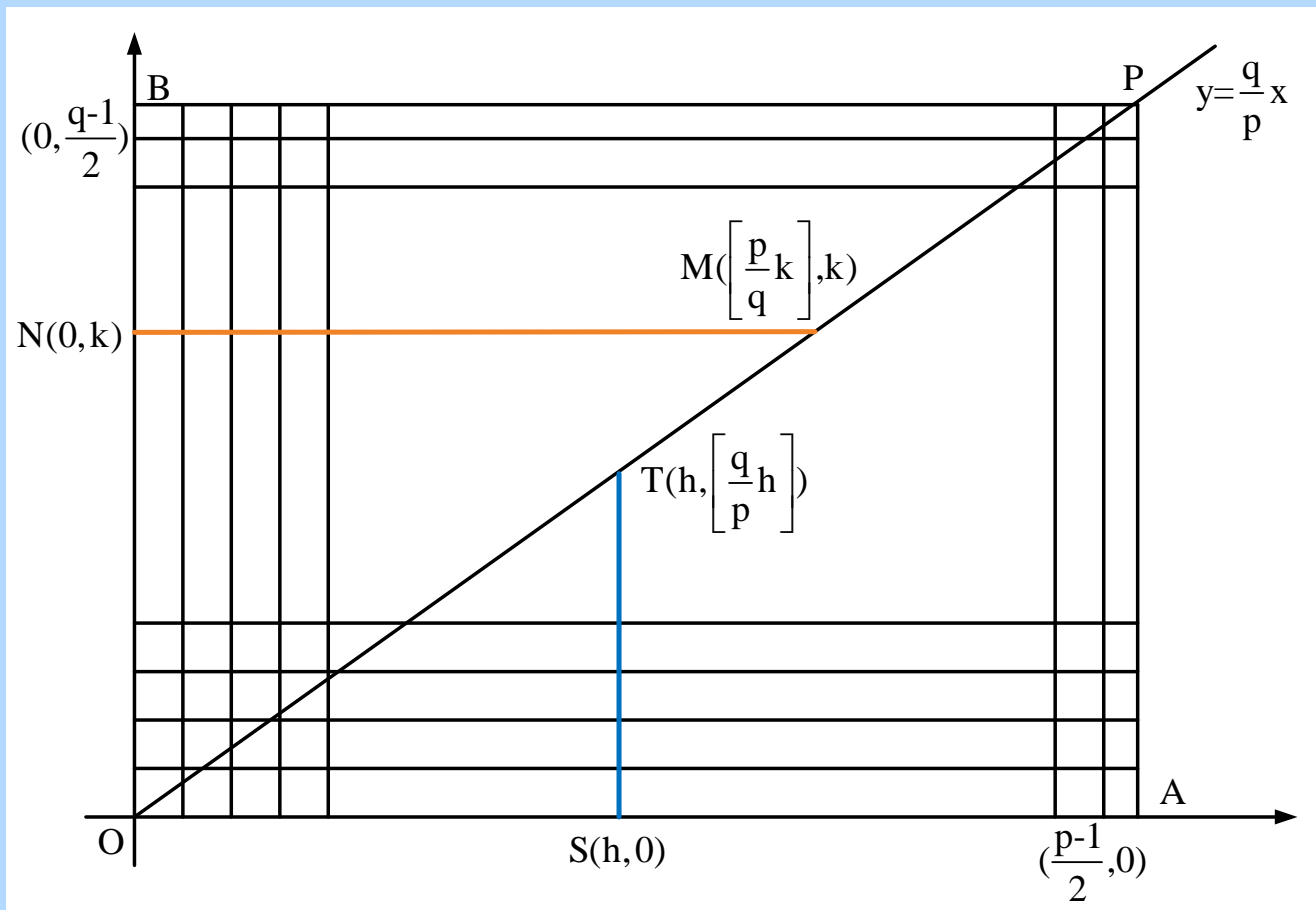
$$T(q, p) + T(p, q) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

[访问主页](#)[标题页](#)[目录页](#)[«](#) [»](#)[◀](#) [▶](#)

第 39 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

考察长为 $\frac{p}{2}$, 宽为 $\frac{q}{2}$ 的长方形内的整点个数:



[访问主页](#)

[标题页](#)

[目录页](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

第 40 页 共 130 页

[返回](#)

[全屏显示](#)

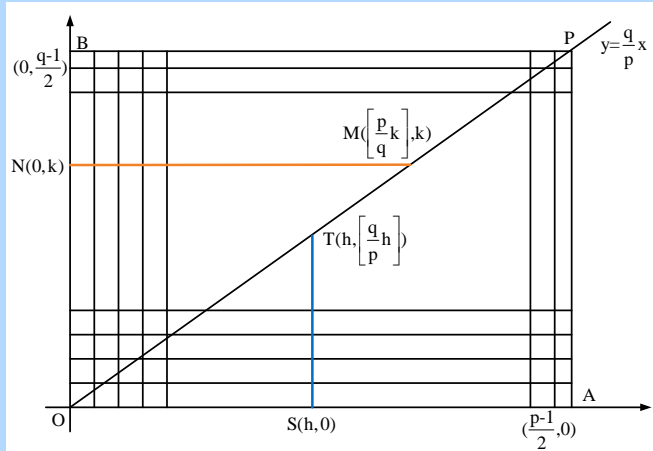
[关闭](#)

[退出](#)



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院





考察长为 $\frac{p}{2}$, 宽为 $\frac{q}{2}$ 的长方形内的整点个数:

在垂直直线ST 上, 整点个数为 $\left\lfloor \frac{q}{p} \cdot h \right\rfloor$, 因此, 下三角形内的整点个数为 $T(q, p)$;

在水平直线NM 上, 整点个数为 $\left\lfloor \frac{p}{q} \cdot k \right\rfloor$, 因此, 上三角形内的整点个数为 $T(p, q)$.

因为对角线OP 上无整点, 所以长方形内整点个数为

$$T(q, p) + T(p, q) = \frac{p-1}{2} \frac{q-1}{2}.$$

这就完成了定理的证明.

证毕

[访问主页](#)

[标题页](#)

[目录页](#)

◀

▶

◀

▶

第 41 页 共 130 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





例4.4.1 判断同余式 $x^2 \equiv 137 \pmod{227}$ 是否有解.

解 因为227 是素数, 根据定理4.3.3,

$$\left(\frac{137}{227}\right) = \left(\frac{-90}{227}\right) = \left(\frac{-1}{227}\right) \left(\frac{2 \cdot 3^2 \cdot 5}{227}\right) = (-1) \left(\frac{2}{227}\right) \left(\frac{5}{227}\right).$$

由定理4.3.4 (i), 我们有

$$\left(\frac{2}{227}\right) = (-1)^{\frac{227^2-1}{8}} = (-1)^{\frac{226 \cdot 228}{8}} = -1.$$

又由定理4.4.1 及定理4.3.4 (i), 我们有

$$\left(\frac{5}{227}\right) = (-1)^{\frac{227-1}{2} \frac{5-1}{2}} \left(\frac{227}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

因此,

$$\left(\frac{137}{227}\right) = -1.$$

同余式 $x^2 \equiv 137 \pmod{227}$ 无解.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 42 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.4.2' 设素数

[illegible]

判断同余式 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p, q 是素数, 根据定理4.4.1及定理4.3.3 (ii), 我们有

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{12}{17}\right) = \left(\frac{3}{17}\right).$$

又

$$\left(\frac{3}{17}\right) = (-1)^{\frac{17-1}{2}\frac{3-1}{2}} \left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1.$$

所以 $\left(\frac{q}{p}\right) = -1$, 同余式 $x^2 \equiv q \pmod{p}$ 无解.

[访问主页](#)

标题页

目 录	页
第一章 绪论	1
第二章 线性规划	10
第三章 非线性规划	25
第四章 动态规划	40
第五章 图论	55
第六章 网络流	70
第七章 排队论	85
第八章 存储论	100
第九章 决策论	115
第十章 模糊数学	130
第十一章 灰色系统理论	145
第十二章 粗糙集	160
第十三章 遗传算法	175
第十四章 神经网络	190
第十五章 专家系统	205
第十六章 智能模拟	220
第十七章 混沌理论	235
第十八章 分形理论	250
第十九章 小波分析	265
第二十章 模糊控制	280
第二十一章 专家控制	295
第二十二章 神经网络控制	310
第二十三章 模糊决策	325
第二十四章 灰色决策	340
第二十五章 粗糙决策	355
第二十六章 遗传决策	370
第二十七章 神经网络决策	385
第二十八章 专家决策	400
第二十九章 智能决策	415
第三十章 混沌决策	430
第三十一章 分形决策	445
第三十二章 小波决策	460
第三十三章 模糊优化	475
第三十四章 专家优化	490
第三十五章 神经网络优化	505
第三十六章 模糊控制	520
第三十七章 专家控制	535
第三十八章 神经网络控制	550
第三十九章 模糊决策	565
第四十章 专家决策	580
第四十一章 神经网络决策	595
第四十二章 智能决策	610
第四十三章 混沌决策	625
第四十四章 分形决策	640
第四十五章 小波决策	655
第四十六章 模糊优化	670
第四十七章 专家优化	685
第四十八章 神经网络优化	700
第四十九章 模糊控制	715
第五十章 专家控制	730
第五十一章 神经网络控制	745
第五十二章 模糊决策	760
第五十三章 专家决策	775
第五十四章 神经网络决策	790
第五十五章 智能决策	805
第五十六章 混沌决策	820
第五十七章 分形决策	835
第五十八章 小波决策	850
第五十九章 模糊优化	865
第六十章 专家优化	880
第六十一章 神经网络优化	895
第六十二章 模糊控制	910
第六十三章 专家控制	925
第六十四章 神经网络控制	940
第六十五章 模糊决策	955
第六十六章 专家决策	970
第六十七章 神经网络决策	985
第六十八章 智能决策	1000
第六十九章 混沌决策	1015
第七十章 分形决策	1030
第七十一章 小波决策	1045
第七十二章 模糊优化	1060
第七十三章 专家优化	1075
第七十四章 神经网络优化	1090
第七十五章 模糊控制	1105
第七十六章 专家控制	1120
第七十七章 神经网络控制	1135
第七十八章 模糊决策	1150
第七十九章 专家决策	1165
第八十章 神经网络决策	1180
第八十一章 智能决策	1195
第八十二章 混沌决策	1210
第八十三章 分形决策	1225
第八十四章 小波决策	1240
第八十五章 模糊优化	1255
第八十六章 专家优化	1270
第八十七章 神经网络优化	1285
第八十八章 模糊控制	1300
第八十九章 专家控制	1315
第九十章 神经网络控制	1330
第九十一章 模糊决策	1345
第九十二章 专家决策	1360
第九十三章 神经网络决策	1375
第九十四章 智能决策	1390
第九十五章 混沌决策	1405
第九十六章 分形决策	1420
第九十七章 小波决策	1435
第九十八章 模糊优化	1450
第九十九章 专家优化	1465
第一百章 神经网络优化	1480

◀ ▶

1

第 43 页 共 130 页

[返回](#)

全屏显示

关闭

退出



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院





例4.4.3 设素数 $p = 200000000000000000000000000029967$, $q = 71$. 判断同余式 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p, q 是素数, 根据定理4.4.1及定理4.3.3 (ii), 我们有

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = (-1) \left(\frac{45}{71}\right) = (-1) \left(\frac{5}{71}\right),$$

又

$$\left(\frac{5}{71}\right) = (-1)^{\frac{71-1}{2} \frac{5-1}{2}} \left(\frac{71}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

所以 $\left(\frac{q}{p}\right) = -1$, 同余式 $x^2 \equiv q \pmod{p}$ 无解.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 48 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.4.4 设素数 $p = 2000000000000000000000000000037023 \approx 2^{103} \approx 2^{31}$, $q = 41$. 判断同余式 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p, q 是素数, 根据定理4.4.1及定理4.3.3 (ii), 我们有

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{20}{41}\right) = \left(\frac{5}{41}\right).$$

又

$$\left(\frac{5}{41}\right) = (-1)^{\frac{41-1}{2} \frac{5-1}{2}} \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = (-1)^{\frac{5-1}{2}} = 1.$$

所以 $\left(\frac{q}{p}\right) = 1$, 同余式 $x^2 \equiv q \pmod{p}$ 有解.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 49 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.4.6 设 $p = 2^{192} - 2^{64} - 1$, $q = 79$. 问 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p, q 是素数, 根据定理4.4.1及定理4.3.3 (ii), 我们有

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = (-1) \left(\frac{37}{79}\right).$$

又

$$\left(\frac{37}{79}\right) = (-1)^{\frac{79-1}{2} \frac{37-1}{2}} \left(\frac{79}{37}\right) = \left(\frac{5}{37}\right) = (-1)^{\frac{37-1}{2} \frac{5-1}{2}} \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = 1.$$

所以 $\left(\frac{q}{p}\right) = 1$, 同余式 $x^2 \equiv q \pmod{p}$ 有解.

例4.4.7 设 $p = 2^{192} - 2^{64} - 1$, $q = 31$. 问 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p, q 是素数, 根据定理4.4.1及定理4.3.3 (ii), 我们有

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = (-1) \left(\frac{18}{31}\right) = (-1) \left(\frac{2}{31}\right) = (-1)(-1)^{\frac{31^2-1}{8}} = -1.$$

所以 $\left(\frac{q}{p}\right) = -1$, 同余式 $x^2 \equiv q \pmod{p}$ 无解.

访问主页

标题页

目录页

« »

◀ ▶

第 51 页 共 130 页

返回

全屏显示

关闭

退出



例4.4.8 设素数 $p = 2^{192} - 2^{64} - 1$, $q = 31$. 令 $a_k = k^3 + k + 1$. 则对于 $k = 0, 1, \dots, 99$, a_k 模 p 的平方剩余判别为:

k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$
0	1	10	-1	20	1	30	-1	40	1
1	1	11	1	21	-1	31	1	41	1
2	-1	12	1	22	1	32	-1	42	1
3	-1	13	1	23	1	33	1	43	-1
4	-1	14	-1	24	-1	34	1	44	1
5	-1	15	1	25	1	35	1	45	-1
6	-1	16	1	26	1	36	1	46	-1
7	1	17	1	27	-1	37	1	47	-1
8	1	18	-1	28	-1	38	1	48	1
9	-1	19	-1	29	1	39	1	49	1

共有30 个模 p 平方剩余, 20 个模 p 平方非剩余.


[访问主页](#)
[标题页](#)
[目录页](#)
[◀](#)
[▶](#)
[◀](#)
[▶](#)

第 52 页 共 130 页

[返回](#)
[全屏显示](#)
[关闭](#)
[退出](#)


例4.4.9 设素数 $p = 2^{192} - 2^{64} - 1$, $q = 31$. 令 $a_k = k^3 + 2k + 3$. 则对于 $k = 0, 1, \dots, 99$, a_k 模 p 的平方剩余判别为:

k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$
0	1	10	-1	20	1	30	-1	40	1
1	1	11	-1	21	-1	31	-1	41	-1
2	1	12	-1	22	-1	32	1	42	1
3	1	13	1	23	-1	33	-1	43	-1
4	-1	14	1	24	1	34	1	44	1
5	1	15	-1	25	-1	35	1	45	-1
6	1	16	1	26	-1	36	1	46	1
7	-1	17	-1	27	1	37	1	47	-1
8	1	18	-1	28	1	38	1	48	-1
9	-1	19	1	29	1	39	1	49	-1

共有27 个模 p 平方剩余, 23 个模 p 平方非剩余.



[访问主页](#)

[标题页](#)

[目录页](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

第 53 页 共 130 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





例4.4.10 设素数 $p = 2^{192} - 2^{64} + 2^5 + 2^4 - 1$, $q = 79$. 判断同余式 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p, q 是素数, 根据定理4.4.1及定理4.3.3 (ii), 我们有

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = (-1) \left(\frac{6}{79}\right) = (-1) \left(\frac{2}{79}\right) \left(\frac{3}{79}\right).$$

$$\left(\frac{2}{79}\right) = (-1)^{\frac{79^2-1}{8}} = 1, \quad \left(\frac{3}{79}\right) = (-1)^{\frac{79-1}{2} \frac{3-1}{2}} \left(\frac{79}{3}\right) = (-1) \left(\frac{1}{3}\right) = -1,$$

所以 $\left(\frac{q}{p}\right) = 1$, 同余式 $x^2 \equiv q \pmod{p}$ 有解.

例4.4.11 设素数 $p = 2^{192} - 2^{64} + 2^5 + 2^4 - 1$, $q = 31$. 判断同余式 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p, q 是素数, 根据定理4.4.1及定理4.3.3 (ii), 我们有

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = (-1) \left(\frac{4}{31}\right) = -1.$$

所以 $\left(\frac{q}{p}\right) = -1$, 同余式 $x^2 \equiv q \pmod{p}$ 无解.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 54 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

例4.4.10' 设素数 $p = 2^{192} - 2^{64} + 2^5 + 2^4 - 1$, $q = 79$. 对于 a , $101 \leq a \leq 200$. 判断同余式 $x^2 \equiv a \pmod{p}$ 是否有解.

a	$\left(\frac{a}{p}\right)$	a	$\left(\frac{a}{p}\right)$	a	$\left(\frac{a}{p}\right)$	a	$\left(\frac{a}{p}\right)$	a	$\left(\frac{a}{p}\right)$
101	-1	121	1	141	1	161	1	181	1
102	1	122	-1	142	-1	162	1	182	1
103	1	123	-1	143	-1	163	-1	183	-1
104	-1	124	-1	144	1	164	-1	184	-1
105	1	125	-1	145	1	165	-1	185	1
106	1	126	-1	146	-1	166	-1	186	-1
107	-1	127	1	147	1	167	1	187	1
108	1	128	1	148	-1	168	-1	188	1
109	-1	129	-1	149	1	169	1	189	-1
110	-1	130	1	150	1	170	-1	190	-1
111	-1	131	1	151	-1	171	1	191	-1
112	-1	132	1	152	1	172	-1	192	1
113	-1	133	-1	153	1	173	1	193	1
114	1	134	1	154	-1	174	-1	194	-1
115	1	135	-1	155	1	175	-1	195	1
116	-1	136	1	156	-1	176	1	196	1
117	-1	137	-1	157	1	177	-1	197	1
118	-1	138	-1	158	1	178	-1	198	1
119	-1	139	-1	159	1	179	1	199	1
120	-1	140	1	160	-1	180	-1	200	1



访问主页

标题页

目录页



第 55 页 共 130 页

返回

全屏显示

关闭

退出





例4.4.12 证明: 形为 $4k + 1$ 的素数有无穷多个.

证 反证法. 如果形为 $4k + 1$ 的素数只有有限多个, 设这些素数为 p_1, \dots, p_s . 考虑整数

$$P = (2p_1 \cdots p_s)^2 + 1.$$

因为 P 形为 $4k + 1$, $P > p_i, i = 1, \dots, s$, 所以 P 为合数, 其素因数 p 为奇数. 因为-1 为模 p 平方剩余, 即

$$\left(\frac{-1}{p}\right) = \left(\frac{-1 + P}{p}\right) = \left(\frac{(2p_1 \cdots p_s)^2}{p}\right) = 1,$$

所以-1 为模 p 平方剩余, 从而 p 是形为 $4k + 1$ 的素数. 但显然有 $p \neq p_i, i = 1, \dots, s$. 矛盾.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 56 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 57 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

例4.4.13 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 $\left(\frac{3}{p}\right) = 1$.

根据二次互反律, $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \left(\frac{p}{3}\right)$. 因为

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

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

故 $\left(\frac{-1}{p}\right) = 1$ 的充要条件是

$$\begin{cases} p \equiv 1 \pmod{4} \\ p \equiv 1 \pmod{6} \end{cases} \quad \text{或} \quad \begin{cases} p \equiv -1 \pmod{4} \\ p \equiv -1 \pmod{6}. \end{cases}$$

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





例4.4.14 设 p 是奇素数, d 是整数. 如果 $\left(\frac{d}{p}\right) = -1$, 则 p 一定不能表示为 $x^2 - dy^2$ 的形式.

证 如果 p 有表达式 $p = x^2 - dy^2$, 则由 p 是素数, 可得到

$$(x, p) = (y, p) = 1.$$

事实上, 若 $(x, p) \neq 1$, 则 $p \mid x$, $p \mid x^2 - p = dy^2$.

但 $(d, p) = 1$, 所以 $p \mid y^2$, 进而 $p \mid y$. 这样 $p^2 \mid x^2$, $p^2 \mid y^2$.
从而

$$p^2 \mid x^2 - dy^2 = p.$$

这不可能. 因此,

$$\left(\frac{d}{p}\right) = \left(\frac{d}{p}\right) \left(\frac{y^2}{p}\right) = \left(\frac{dy^2}{p}\right) = \left(\frac{x^2}{p}\right) = 1.$$

这与题设矛盾.

证毕

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 58 页 共 130 页

返回

全屏显示

关闭

退出



4.5 雅可比符号

在勒让得符号的计算中, 要求模 p 为素数. 此外, 在二次互反律的应用中, 要求 $a = q$ 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 m 为奇整数, a 为任意整数.

定义4.5.1 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(Jacobi)符号为

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right). \quad (20)$$

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. 与(3.10)作比较, 对于 $(a, m) = 1$, 有

$$\begin{aligned} \left(\frac{a}{m}\right) = 1 &\iff x^2 \equiv a \pmod{m} \text{ 有解} \\ \left(\frac{a}{m}\right) = -1 &\implies x^2 \equiv a \pmod{p} \text{ 无解} \end{aligned} \quad (21)$$

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. 例如, 3 是模 119 平方非剩余, 但

$$\left(\frac{3}{119}\right) = \left(\frac{3}{7}\right) \left(\frac{3}{17}\right) = (-1)(-1) = 1.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 59 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



在勒让得符号的计算中, 要求模 p 为素数. 现在将它推广为一般的模 m .

定义4.5.1 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(Jacobi)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. 例如, 3 是模119 平方非剩余, 但

$$\left(\frac{3}{119}\right) = \left(\frac{3}{7}\right) \left(\frac{3}{17}\right) = (-1)(-1) = 1.$$

[访问主页](#)[标题页](#)[目录页](#)[«](#) [»](#)[◀](#) [▶](#)

第 60 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



定理4.5.1 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. 根据定义,

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

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 61 页 共 130 页

返回

全屏显示

关闭

退出





引理4.5.1: 设 $m = p_1 \cdots p_r$ 是奇数. 则

$$\frac{m-1}{2} \equiv \frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2} \pmod{2};$$

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

证 因为我们有表达式

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

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

所以引理成立. 证毕.

访问主页

标题页

目录页

返回

前进

第 62 页 共 130 页

返回

全屏显示

关闭

退出





定理4.5.2 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) $\left(\frac{2}{m}\right) \equiv (-1)^{\frac{m^2-1}{8}};$

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和§4.3 定理1之推论1 以及引理, 我们有

(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和§4.3 定理3 以及引理, 我们有

(iii)

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

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 63 页 共 130 页

返回

全屏显示

关闭

退出





定理4.5.3 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 $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) = 0$. 结论成立. 因此, 可设 $(m, n) = 1$. 根据雅可比符号的定义和§4.3 定理4, 我们有

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

再根据引理,

$$\begin{aligned} \sum_{i=1}^r \sum_{j=1}^s \frac{p_i-1}{2} \cdot \frac{q_j-1}{2} &\equiv \sum_{i=1}^r \frac{p_i-1}{2} \sum_{j=1}^s \frac{q_j-1}{2} \\ &\equiv \frac{m-1}{2} \cdot \frac{n-1}{2} \pmod{2}. \end{aligned}$$

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

因此, 定理成立. 证毕.

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 64 页 共 130 页

返回

全屏显示

关闭

退出





例4.5.1 判断同余式

$$x^2 \equiv 286 \pmod{563}$$

是否有解.

解 不用考虑563 是否为素数, 直接计算雅可比符号. 因为

$$\begin{aligned} \left(\frac{286}{563}\right) &= \left(\frac{2}{563}\right) \left(\frac{143}{563}\right) \\ &= (-1)^{\frac{563^2-1}{8}} (-1)^{\frac{143-1}{2} \cdot \frac{563-1}{2}} \left(\frac{563}{143}\right) \\ &= \left(\frac{-9}{143}\right) \\ &= \left(\frac{-1}{143}\right) = -1, \end{aligned}$$

所以原同余式无解.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 65 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.5.2 判断同余式 $x^2 \equiv 17 \pmod{m}$ 是否有解. 这里,

$$m = p \cdot q = 4000000000000000000000000000673386 \\ 00000000000000000000000000001109468241$$

$$p = 2000000000000000000000000000029967,$$

$$q = 2000000000000000000000000000037023$$

解 不用考虑 m 是否为素数, 直接计算雅可比符号. 因为

$$\left(\frac{17}{m}\right) = (-1)^{\frac{m-1}{2} \frac{17-1}{2}} \left(\frac{m}{17}\right) = \left(\frac{-3}{17}\right) = \left(\frac{-1}{17}\right) \left(\frac{3}{17}\right),$$

而

$$\left(\frac{-1}{17}\right) = (-1)^{\frac{17-1}{2}} = 1$$

$$\left(\frac{3}{17}\right) = (-1)^{\frac{17-1}{2} \frac{3-1}{2}} \left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1,$$

所以 $\left(\frac{17}{m}\right) = -1$, 原同余式无解.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 66 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.5.3 判断同余式 $x^2 \equiv 59 \pmod{m}$ 是否有解. 这里,

$$m = p \cdot q = 4000000000000000000000000000673386$$

$$00000000000000000000000000001109468241$$

$$p = 2000000000000000000000000000029967,$$

$$q = 2000000000000000000000000000037023$$

解 不用考虑 m 是否为素数, 直接计算雅可比符号. 因为

$$\left(\frac{59}{m}\right) = (-1)^{\frac{m-1}{2} \frac{17-1}{2}} \left(\frac{m}{59}\right) = \left(\frac{2}{59}\right) = (-1)^{\frac{59^2-1}{8}} = -1,$$

所以 $\left(\frac{59}{m}\right) = -1$, 原同余式无解.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 67 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.5.4 求出 $y^2 \equiv x^3 + x + 1 \pmod{17}$ 的所有解及解数.

解 令 $f(x) = x^3 + x + 1$. 根据§4.1 例3, 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;	$f(15)=8,$	$y=5, y=12;$
$f(16)=-1,$	$y=4, y=13$	$(\text{mod } 17).$	

故原同余式解: $(0, 1), (0, 16), (4, 1), (4, 16), (6, 6), (6, 11), (9, 5), (9, 12), (10, 5), (10, 12), (11, 0), (13, 1), (13, 16), (15, 5), (15, 12), (16, 4), (16, 13).$

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 68 页 共 130 页

返回

全屏显示

关闭

退出



4.6.1 模 p 平方根 (p 形为 $4k + 3$)

设 p 是形为 $4k + 3$ 的素数. 我们讨论此情形的模 p 平方根.

定理4.6.1 设 p 是形为 $4k + 3$ 的素数. 如果同余式

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

有解, 则其解是

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}. \quad (22)$$

解 因为 p 是形为 $4k + 3$ 的素数, 所以存在奇数 q 使得 $p - 1 = 2q$. 现在同余式 $x^2 \equiv a \pmod{p}$ 有解, 则我们有

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

或者 $a^q \equiv 1 \pmod{p}$.

两端同时乘以 a , 得到

$$\left(a^{\frac{q+1}{2}}\right)^2 \equiv a^{q+1} \equiv a \pmod{p}.$$

因此, 同余式的解为(22).

证毕



[访问主页](#)

[标题页](#)

[目录页](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

第 69 页 共 130 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





例4.6.1 设素数 $p = 200000000000000000000000000029967$, $a = 41$. 求解同余式 $x^2 \equiv a \pmod{p}$.

解 因为 p 是形为 $4k + 3$ 的素数, 根据定理4.6.1及例4.4.2, 知原同余式有解, 且解为

$$x \equiv \pm a^{\frac{p+1}{4}} \equiv 1539250749819107362858845139474 \pmod{p}.$$

例4.6.2 设素数 $p = 200000000000000000000000000037023$, $q = 41$. 判断同余式 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p 是形为 $4k + 3$ 的素数, 根据定理4.6.1及例4.4.4, 知原同余式有解, 且解为

$$x \equiv \pm a^{\frac{p+1}{4}} \equiv 3406794145708458557038951337364 \pmod{p}.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 70 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.6.3 设素数 $p = 2^{192} - 2^{64} - 1$, $q = 79$. 判断同余式 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p 是形为 $4k + 3$ 的素数,根据定理4.6.1及例4.4.6, 知原同余式有解, 且解为

$$x \equiv \pm a^{\frac{p+1}{4}} \equiv 3, 441, 509, 450, 523, 406, 068, 648, 946, 248, 998, 374, \backslash \backslash \\ 727, 265, 234, 715, 111, 696, 917, 117 \pmod{p}.$$

例4.6.4 设素数 $p = 2^{192} - 2^{64} + 2^5 + 2^4 - 1$, $q = 79$. 判断同余式 $x^2 \equiv q \pmod{p}$ 是否有解.

解 因为 p 是形为 $4k + 3$ 的素数,根据定理4.6.1及例4.4.10, 知原同余式有解, 且解为

$$x \equiv \pm a^{\frac{p+1}{4}} \equiv 714, 966, 419, 491, 317, 688, 312, 388, 325, 572, 327, \backslash \backslash \\ 012, 170, 027, 743, 594, 638, 939, 954 \pmod{p}.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 71 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



定理4.6.2 设 p, q 是形为 $4k + 3$ 的不同素数. 如果整数 a 满足

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1,$$

则同余式

$$x^2 \equiv a \pmod{p \cdot q} \quad (23)$$

有解

$$x \equiv \pm(a^{\frac{p+1}{4}} \pmod{p}) \cdot s \cdot q \pm (a^{\frac{q+1}{4}} \pmod{q}) \cdot t \cdot p \pmod{p \cdot q}. \quad (24)$$

其中 s, t 满足 $s \cdot q + t \cdot p = 1$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 72 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



解 因为同余式(23) 等价于同余式组

$$\begin{cases} x^2 \equiv a \pmod{p} \\ x^2 \equiv a \pmod{q}, \end{cases}$$

而同余式 $x^2 \equiv a \pmod{p}$ 的解为

$$x = b_1 \equiv \pm a^{\frac{p+1}{4}} \pmod{p},$$

同余式 $x^2 \equiv a \pmod{q}$ 的解为

$$x = b_2 \equiv \pm a^{\frac{q+1}{4}} \pmod{q},$$

根据§3.2 定理3.2.3(中国剩余定理), 原同余式的解为(25). 证毕

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 73 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

例4.6.5 求解同余式 $x^2 \equiv 41 \pmod{m}$, 这里,

$$\begin{aligned} m = p \cdot q &= 40000000000000000000000000673386 \setminus \setminus \\ &\quad 0000000000000000000000001109468241 \\ p &= 200000000000000000000000000029967, \\ q &= 200000000000000000000000000037023 \end{aligned}$$

解 因为同余式等价于同余式组 $\begin{cases} x^2 \equiv 41 \pmod{p} \\ x^2 \equiv 41 \pmod{q}, \end{cases}$

$$x^2 \equiv 41 \pmod{p} \text{ 的解为 } x = b_1 \equiv \pm 41^{\frac{p+1}{4}} \pmod{p},$$
$$x^2 \equiv 41 \pmod{q} \text{ 的解为 } x = b_2 \equiv \pm 41^{\frac{q+1}{4}} \pmod{q},$$

根据定理4.6.2, 原同余式的解为

$$x_{+,+} \equiv \begin{array}{l} 3219361862449568351065835035035862391088 \setminus \setminus \\ 0892989312244092077738 \end{array} \pmod{m}$$

$$x_{+,-} \equiv \begin{array}{l} 1041192581336200089352477694437062967525 \setminus \setminus \\ 9359495491351853561501 \end{array} \pmod{m}$$

$$x_{-,+} \equiv \begin{array}{l} 2958807418663799910647522372901537032474 \setminus \setminus \\ 0640504508649255906740 \end{array} \pmod{m}$$

$$x_{-,+} \equiv \begin{array}{l} 78063813755043164893416503230273760891191 \setminus \setminus \\ 07010687757017390503 \end{array} \pmod{m}$$

[访问主页](#)

标题页

目 录	页
第一章 绪论	1
第二章 线性代数	10
第三章 微分方程	25
第四章 概率论与数理统计	40
第五章 复变函数	55
第六章 数值分析	70
第七章 数学物理方程	85
第八章 变分法	100
第九章 拓扑学	115
第十章 群论	130
第十一章 微分几何	145
第十二章 泛函分析	160
第十三章 代数几何	175
第十四章 非交换几何	190
第十五章 量子场论	205
第十六章 弦理论	220
第十七章 黑洞物理学	235
第十八章 宇宙学	250
第十九章 粒子物理学	265
第二十章 凝聚态物理学	280
第二十一章 生物物理学	295
第二十二章 环境物理学	310
第二十三章 天体物理学	325
第二十四章 宇宙学	340
第二十五章 粒子物理学	355
第二十六章 凝聚态物理学	370
第二十七章 生物物理学	385
第二十八章 环境物理学	400
第二十九章 天体物理学	415
第三十章 宇宙学	430
第三十一章 粒子物理学	445
第三十二章 凝聚态物理学	460
第三十三章 生物物理学	475
第三十四章 环境物理学	490
第三十五章 天体物理学	505
第三十六章 宇宙学	520
第三十七章 粒子物理学	535
第三十八章 凝聚态物理学	550
第三十九章 生物物理学	565
第四十章 环境物理学	580
第四十一章 天体物理学	595
第四十二章 宇宙学	610
第四十三章 粒子物理学	625
第四十四章 凝聚态物理学	640
第四十五章 生物物理学	655
第四十六章 环境物理学	670
第四十七章 天体物理学	685
第四十八章 宇宙学	700
第四十九章 粒子物理学	715
第五十章 凝聚态物理学	730
第五十一章 生物物理学	745
第五十二章 环境物理学	760
第五十三章 天体物理学	775
第五十四章 宇宙学	790
第五十五章 粒子物理学	805
第五十六章 凝聚态物理学	820
第五十七章 生物物理学	835
第五十八章 环境物理学	850
第五十九章 天体物理学	865
第六十章 宇宙学	880
第六十一章 粒子物理学	895
第六十二章 凝聚态物理学	910
第六十三章 生物物理学	925
第六十四章 环境物理学	940
第六十五章 天体物理学	955
第六十六章 宇宙学	970
第六十七章 粒子物理学	985
第六十八章 凝聚态物理学	1000
第六十九章 生物物理学	1015
第七十章 环境物理学	1030
第七十一章 天体物理学	1045
第七十二章 宇宙学	1060
第七十三章 粒子物理学	1075
第七十四章 凝聚态物理学	1090
第七十五章 生物物理学	1105
第七十六章 环境物理学	1120
第七十七章 天体物理学	1135
第七十八章 宇宙学	1150
第七十九章 粒子物理学	1165
第八十章 凝聚态物理学	1180
第八十一章 生物物理学	1195
第八十二章 环境物理学	1210
第八十三章 天体物理学	1225
第八十四章 宇宙学	1240
第八十五章 粒子物理学	1255
第八十六章 凝聚态物理学	1270
第八十七章 生物物理学	1285
第八十八章 环境物理学	1300
第八十九章 天体物理学	1315
第九十章 宇宙学	1330
第九十一章 粒子物理学	1345
第九十二章 凝聚态物理学	1360
第九十三章 生物物理学	1375
第九十四章 环境物理学	1390
第九十五章 天体物理学	1405
第九十六章 宇宙学	1420
第九十七章 粒子物理学	1435
第九十八章 凝聚态物理学	1450
第九十九章 生物物理学	1465
第一百章 环境物理学	1480



第 74 页 共 130 页

[返回](#)

全屏显示

关闭

退出



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院





例4.6.6 $x^2 \equiv 79 \pmod{m}$ 这里,

$$m = p \cdot q = 394020061963944792122790401001436138048481550919908 \setminus \setminus \\ 142773898981140561332709274572379174587204093236476 \setminus \setminus \\ 16188447457233$$

$$p = 2^{192} - 2^{64} - 1, \quad q = 2^{192} - 2^{64} + 2^5 + 2^4 - 1$$

解 因为同余式等价于同余式组 $\begin{cases} x^2 \equiv 79 \pmod{p} \\ x^2 \equiv 79 \pmod{q}, \end{cases}$

$$x_{+,+} \equiv 356541886340970955975573605910602125196073155329396776634554 \\ 55391814330450309366771353307780624206492557200223624044 \pmod{m}$$

$$x_{+,-} \equiv 39124685690152141858578435772213652342275697555214526165323 \\ 60937951191083476382054741614245077810604204779704913862 \pmod{m}$$

$$x_{-,+} \equiv 277320506242337353700604327929961462572457536469361660857537 \\ 176104942187451075183175844475331513043411408742543371 \pmod{m}$$

$$x_{-,-} \equiv 374781756229738361472167950908340128524083955905113661393444 \\ 2722241802820618090466564150939785117155058988223833189 \pmod{m}$$

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 75 页 共 130 页

返回

全屏显示

关闭

退出



4.6.1 模 p 平方根

现在在有解的情况下, 即 a 满足 $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \pmod{p}$

的情况下, 考虑二次同余式 $x^2 \equiv a \pmod{p}$ 的具体求解.

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

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

可写成

$$(a^s)^{2^{t-1}} \equiv 1 \pmod{p} \quad \text{或} \quad (a^{-1}(a^{\frac{s+1}{2}})^2)^{2^{t-1}} \equiv 1 \pmod{p}.$$

令 $x_{t-1} := a^{\frac{s+1}{2}} \pmod{p}$. 则 $a^{-1}x_{t-1}^2$ 满足同余式

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

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

现在要寻找整数 x_{t-2} 使得 $a^{-1}x_{t-2}^2$ 满足同余式

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

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

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 76 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



任取一个模 p 平方非剩余 n , 即整数 n 使得 $\left(\frac{n}{p}\right) = -1$. 再令 $b := n^s \pmod{p}$. 我们有

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

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

因为

$$((a^{-1}x_{t-1}^2)^{2^{t-2}} - 1)((a^{-1}x_{t-1}^2)^{2^{t-2}} + 1) \equiv 0 \pmod{p},$$

所以我们有

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

或

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

因此, 我们令

$$j_0 = \begin{cases} 0 & \text{如果 } (a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \pmod{p}; \\ 1 & \text{如果 } (a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \pmod{p}. \end{cases}$$

这时, $x_{t-2} = x_{t-1}b^{j_0}$ 为所求.

[访问主页](#)[标题页](#)[目录页](#)

第 77 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



定理4.6.3 设 p 奇素数, $p-1=2^t \cdot s$, $t \geq 1$, 其中 s 是奇整数. 设 n 是模 p 平方非剩余. $b := n^s \pmod{p}$. 如果同余式

$$x^2 \equiv a \pmod{p} \quad (25)$$

有解, 则 $a^{-1}x_{t-k-1}^2$ 满足同余式

$$y^{2^{t-k-1}} \equiv 1 \pmod{p} \quad (26)$$

$k = 0, 1, \dots, t-1$, 这里, $x_{t-1} := a^{\frac{s+1}{2}} \pmod{p}$,

$$x_{t-k-1} = x_{t-k} b^{j_{k-1} 2^{k-1}}, \quad (27)$$

$$\text{其中 } j_{k-1} = \begin{cases} 0 & \text{如果 } (a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv 1 \pmod{p}; \\ 1 & \text{如果 } (a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1 \pmod{p}. \end{cases} \quad (28)$$

特别, x_0 是同余式(25)的解.

[访问主页](#)
[标题页](#)
[目录页](#)
[◀](#)
[▶](#)
[◀](#)
[▶](#)

第 78 页 共 130 页

[返回](#)
[全屏显示](#)
[关闭](#)
[退出](#)




访问主页

标题页

目录页



第 79 页 共 130 页

返回

全屏显示

关闭

退出



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院





访问主页

标题页

目录页



第 80 页 共 130 页

返回

全屏显示

关闭

退出



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院





访问主页

标题页

目录页



第 81 页 共 130 页

返回

全屏显示

关闭

退出



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院



4.6.1 模 p 平方根

设 p 为奇素数. 对任意给定的整数 a , 应用高斯二次互反律 (§4.3 定理4) 可以快速判断 a 是否为模 p 平方剩余, 即二次同余式

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

是否有解, 也就是说解的存在性.

现在在有解的情况下, 即 a 满足 $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \pmod{p}$ 的情况下, 考虑二次同余式的具体求解. 求解过程如下:

对奇素数 p , 将 $p-1$ 写成 $p-1 = 2^t \cdot s$, $t \geq 1$, 其中 s 是奇数.

(0) 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 $b := n^s \pmod{p}$. 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.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 82 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



(i) 计算 $x_{t-1} := a^{\frac{s+1}{2}} \pmod{p}$. 有 $a^{-1}x_{t-1}^2$ 满足同余式

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

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

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

(ii) 如果 $t = 1$, 则 $x = x_{t-1} = x_0 \equiv a^{\frac{s+1}{2}} \pmod{p}$ 满足

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

如果 $t \geq 2$, 要寻找 x_{t-2} 使得 $a^{-1}x_{t-2}^2$ 满足

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

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

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 83 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

要寻找 x_{t-2} 使得 $a^{-1}x_{t-2}^2$ 满足 $y^{2^{t-2}} \equiv 1 \pmod{p}$.

由

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

$$\text{得 } (a^{-1}x_{t-1}^2)^{2^{t-1}} \equiv 1 \quad \text{或} \quad (a^{-1}x_{t-1}^2)^{2^{t-1}} \equiv -1$$

(a) 如果

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

则令 $j_0 := 0$, $x_{t-2} := x_{t-1} = x_{t-1}b^{j_0} \pmod{p}$;

(b) 如果

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

则令 $j_0 := 1$, $x_{t-2} := x_{t-1}b = x_{t-1}b^{j_0} \pmod{p}$.

上述 x_{t-2} 为所求.



访问主页

标题页

目录页

◀ ▶

◀ ▶

第 84 页 共 130 页

返回

全屏显示

关闭

退出





如此下去,....

假设找到整数 x_{t-k} 使得 $a^{-1}x_{t-k}^2$ 满足

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

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

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

(k+1) 如果 $t = k$, 则 $x = x_{t-k} \pmod{p}$ 满足 $x^2 \equiv a \pmod{p}$.

如果 $t \geq k + 1$, 要寻找 x_{t-k-1} 使得 $a^{-1}x_{t-k-1}^2$ 满足

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

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

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 85 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

寻找 x_{t-k-1} 使得 $a^{-1}x_{t-k-1}^2$ 满足 $y^{2^{t-k-1}} \equiv 1 \pmod{p}$.

由

$$(a^{-1}x_{t-k}^2)^{2^{t-k}} - 1 = ((a^{-1}x_{t-k}^2)^{2^{t-k-1}} - 1)((a^{-1}x_{t-k}^2)^{2^{t-k-1}} + 1) \equiv 0 \pmod{p},$$

$$\text{得 } (a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv 1 \quad \text{或} \quad (a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1$$

(a) 如果

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

则令 $j_{k-1} := 0, x_{t-k-1} := x_{t-k} = x_{t-k}b^{j_{k-1}2^{k-1}} \pmod{p}$;

(b) 如果

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

则令 $j_{k-1} := 1, x_{t-k-1} := x_{t-k}b^{2^{k-1}} = x_{t-k}b^{j_{k-1}2^{k-1}} \pmod{p}$.

上述 x_{t-k-1} 为所求.



[访问主页](#)

[标题页](#)

[目录页](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

第 86 页 共 130 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





寻找 x_{t-k-1} 使得 $a^{-1}x_{t-k-1}^2$ 满足 $y^{2^{t-k-1}} \equiv 1 \pmod{p}$.

递归关系式: $x_{t-k-1} := x_{t-k}b^{2^{k-1}} = x_{t-k}b^{j_{k-1}2^{k-1}}$

特别地, 对于 $k = t - 1$, 有

$$\begin{aligned}x &= x_0 \equiv x_1 b^{j_{t-2}2^{t-2}} \\&\equiv \dots \equiv x_{t-1} b^{j_0+j_12+\dots+j_{t-2}2^{t-2}} \\&\equiv a^{\frac{s+1}{2}} b^{j_0+j_12+\dots+j_{t-2}2^{t-2}} \pmod{p}\end{aligned}$$

满足同余式

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

[访问主页](#)[标题页](#)[目录页](#)[<<](#)[>>](#)[<](#)[>](#)

第 87 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.6.1 应用上述算法求解同余式 $x^2 \equiv 186 \pmod{401}$.

解 因为 $a = 186 = 2 \cdot 3 \cdot 31$, 计算勒让得符号

$$\begin{aligned}\left(\frac{2}{401}\right) &= (-1)^{(401^2-1)/8} = 1, \\ \left(\frac{3}{401}\right) &= (-1)^{\frac{3-1}{2} \frac{401-1}{2}} \left(\frac{401}{3}\right) = \left(\frac{-1}{3}\right) = -1, \\ \left(\frac{31}{401}\right) &= (-1)^{\frac{31-1}{2} \frac{401-1}{2}} \left(\frac{401}{31}\right) = \left(\frac{-2}{31}\right) \\ &= \left(\frac{-1}{31}\right) \left(\frac{2}{31}\right) = (-1)^{\frac{31-1}{2}} (-1)^{\frac{31^2-1}{8}} = -1,\end{aligned}$$

所以

$$\left(\frac{186}{401}\right) = \left(\frac{2}{401}\right) \left(\frac{3}{401}\right) \left(\frac{31}{401}\right) = 1 \cdot (-1) \cdot (-1) = 1.$$

故原同余式有解.

下面具体求解:

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 88 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



对 $p = 401$, 写 $p - 1 = 400 = 2^4 \cdot 25$, 其中 $t = 4$, $s = 25$ 是奇数.

任选一个模401 平方非剩余 $n = 3$, 即 $n = 3$ 使得 $(\frac{3}{401}) = -1$.

再令 $b := 3^{25} \equiv 268 \pmod{401}$.

(i) 计算 $x_3 := 186^{\frac{25+1}{2}} \equiv 103 \pmod{401}$. 以及 $a^{-1} \equiv 235 \pmod{401}$.

(ii) 因为 $(a^{-1}x_3^2)^{2^2} \equiv 98^4 \equiv -1 \pmod{401}$,

我们令 $j_0 := 1$, $x_2 := x_3 b^{j_0} = 103 \cdot 268 \equiv 336 \pmod{401}$,

(iii) 因为 $(a^{-1}x_2^2)^2 \equiv (-1)^2 \equiv 1 \pmod{401}$,

我们令 $j_1 := 0$, $x_1 := x_2 b^{j_1 2} = 336 \pmod{401}$.

(iv) 因为 $a^{-1}x_1^2 \equiv -1 \pmod{401}$,

我们令 $j_2 := 1$, $x_0 := x_1 b^{j_2 2^2} = 336 \cdot 268^4 \equiv 304 \pmod{401}$,

则 $x \equiv x_0 \equiv 304 \pmod{p}$ 满足同余式

$$x^2 \equiv 186 \pmod{401}.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 89 页 共 130 页

[返 回](#)[全屏显示](#)[关 闭](#)[退 出](#)



例4.6.2 求解同余式 $x^2 \equiv 103 \pmod{1601}$.

解 对于 $a = 103$, 计算勒让得符号(这里注意到 $1601 = 15 \cdot 103 + 56$)

$$\left(\frac{103}{1601}\right) = (-1)^{\frac{103-1}{2} \frac{1601-1}{2}} \left(\frac{1601}{103}\right) = \left(\frac{56}{103}\right) = \left(\frac{2^3 \cdot 7}{103}\right) = \left(\frac{2}{103}\right) \left(\frac{7}{103}\right),$$

继续计算勒让得符号(这里注意到 $103 = 15 \cdot 7 + (-2)$),

$$\left(\frac{2}{103}\right) = (-1)^{\frac{103^2-1}{8}} = 1$$

$$\begin{aligned} \left(\frac{7}{103}\right) &= (-1)^{\frac{7-1}{2} \frac{103-1}{2}} \left(\frac{103}{7}\right) = (-1) \left(\frac{-2}{7}\right) \\ &= (-1) \left(\frac{-1}{7}\right) \left(\frac{2}{7}\right) = (-1)(-1)^{\frac{7-1}{2}} (-1)^{\frac{7^2-1}{8}} = 1, \end{aligned}$$

所以 $\left(\frac{103}{1601}\right) = \left(\frac{2}{103}\right) \left(\frac{7}{103}\right) = 1$.

故原同余式有解.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 90 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



对于奇素数 $p = 1601$, 将 $p - 1$ 写成形式 $p - 1 = 1600 = 2^6 \cdot 25$, 其中 $t = 4$, $s = 25$ 是奇数.

(i) 任意选取一个模1601 平方非剩余 $n = 3$, 即整数 $n = 3$ 使得 $\left(\frac{3}{1601}\right) = -1$. 再令 $b := 3^{25} \equiv 828 \pmod{p}$.

(ii) 计算 $x_5 := a^{\frac{s+1}{2}} \equiv 595 \pmod{p}$ 以及 $a^{-1} \equiv 886 \pmod{p}$.

(iii) 因为 $(a^{-1}x_3^2)^{2^2} \equiv 98^4 \equiv -1 \pmod{401}$,

我们令 $j_0 := 1$, $x_2 := x_3 b^{j_0} = 103 \cdot 268 \equiv 336 \pmod{401}$,

(iv) 因为 $(a^{-1}x_2^2)^2 \equiv (-1)^2 \equiv 1 \pmod{401}$,

我们令 $j_1 := 0$, $x_1 := x_2 b^{j_1 2} = 336 \pmod{401}$.

(v) 因为 $a^{-1}x_1^2 \equiv -1 \pmod{401}$,

我们令 $j_2 := 1$, $x_0 := x_1 b^{j_2 2^2} = 336 \cdot 268^4 \equiv 304 \pmod{401}$, 则 $x \equiv x_0 \equiv 304 \pmod{p}$ 满足同余式

$$x^2 \equiv 186 \pmod{401}.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 91 页 共 130 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



访问主页

标题页

目录页



第 92 页 共 130 页

返回

全屏显示

关闭

退出



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院





例4.6.11 设 $p = 8k + 5$ 为素数. 如果 a 为模 p 平方非剩余, 则同余式

$$x^2 \equiv -1 \pmod{p}$$

的解为 $x = \pm a^{\frac{p-1}{4}} \pmod{p}$.

证 因为勒让得符号

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

所以原同余式有解.

又因为 a 为模 p 平方非剩余, 即有 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, 从而

$$(a^{\frac{p-1}{4}})^2 \equiv a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

故结论成立.

证毕

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 93 页 共 130 页

返回

全屏显示

关闭

退出



4.6.3 合数的情形

本节我们讨论模 m 为合数的二次同余式

$$x^2 \equiv a \pmod{m}, \quad (a, m) = 1. \quad (29)$$

有解的条件及解的个数.

当 $m = 2^\delta p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 时, 同余式等价于同余式组:

$$\begin{cases} x^2 \equiv a \pmod{2^\delta}, \\ x^2 \equiv a \pmod{p_1^{\alpha_1}}, \\ \dots\dots\dots \\ x^2 \equiv a \pmod{p_k^{\alpha_k}}. \end{cases} \quad (30)$$

因此, 我们先讨论模为奇素数幂 p^α 的二次同余式

$$x^2 \equiv a \pmod{p^\alpha}, \quad (a, p) = 1, \alpha > 0. \quad (31)$$

有解的条件及解的个数.

[访问主页](#)[标题页](#)[目录页](#)[<<](#)[>>](#)[<](#)[>](#)

第 94 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



定理4.6.3 设 p 是奇素数. 则同余式(31)有解的充分必要条件是 a 为模 p 平方剩余, 且有解时, (31)式的解数是2.

证 设同余式(31)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 $x_1^2 \equiv a \pmod{p}$. 这就是说, 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§3.3 定理3.3.2, 从 $x^2 \equiv a \pmod{p}$ 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.
证毕

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 95 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



推论 设 p 是奇素数. 则对于任意的整数 a , 同余式(31)的解数是

$$T = 1 + \left(\frac{a}{p} \right).$$

证 分3 种情形讨论. 当 $\left(\frac{a}{p} \right) = 0$ 时, $x^2 \equiv a \equiv 0 \pmod{p}$ 有惟一解 $x \equiv 0 \pmod{p}$, 所以解数 $T = 1 = 1 + \left(\frac{a}{p} \right)$.

当 $\left(\frac{a}{p} \right) = 1$ 时, $x^2 \equiv a \pmod{p}$ 有2 解, 所以解数 $T = 2 = 1 + \left(\frac{a}{p} \right)$.

当 $\left(\frac{a}{p} \right) = -1$ 时, $x^2 \equiv a \pmod{p}$ 无解, 所以解数 $T = 0 = 1 + \left(\frac{a}{p} \right)$.
故结论成立. 证毕

[访问主页](#)[标题页](#)[目录页](#)[«](#) [»](#)[◀](#) [▶](#)

第 96 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

再讨论同余式

$$x^2 \equiv a \pmod{2^\alpha}, \quad (a, 2) = 1, \alpha > 0, \quad (32)$$

有解的条件及解的个数.

定理4.6.4 设 $\alpha > 1$, 则同余式(32)有解的必要条件是

(i) 当 $\alpha = 2$ 时, $a \equiv 1 \pmod{4}$; (ii) 当 $\alpha \geq 3$ 时, $a \equiv 1 \pmod{8}$.

若上述条件成立, 则(32)有解.

进一步, 当 $\alpha = 2$ 时, 解数是2; 当 $\alpha \geq 3$ 时, 解数是4.

证 若同余式(32)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 $x_1 = 1 + t \cdot 2$, 上式可写成

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

注意到 $2 \mid t(t+1)$, 我们有

(i) 当 $\alpha = 2$, $a \equiv 1 \pmod{4}$; (ii) 当 $\alpha \geq 3$, $a \equiv 1 \pmod{8}$.

因此, 必要性成立.

[访问主页](#)[标题页](#)[目录页](#)[«](#) [»](#)[◀](#) [▶](#)

第 97 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



现在, 若必要条件满足, 则

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

$$x \equiv 1, 3 \pmod{2^\alpha}$$

是同余式(32)仅有的二解.

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

对 $\alpha = 3$, 易验证:

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

是同余式(32)仅有的4解, 它们可表示为

$$\pm(1 + t_3 \cdot 2^2), \quad t_3 = 0, \pm 1, \dots,$$

或者

$$\pm(x_3 + t_3 \cdot 2^2), \quad t_3 = 0, \pm 1, \dots$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#)[▶](#)[◀](#)[▶](#)

第 98 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

对 $\alpha = 4$, 由

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

并注意到

$$2 x_3(t_3 \cdot 2^2) \equiv t_3 \cdot 2^3 \pmod{2^4},$$

我们有

$$x_3^2 + t_3 \cdot 2^3 \equiv a \pmod{2^4}, \text{ 或 } t_3 \equiv \frac{a - x_3^2}{2^3} \pmod{2}.$$

故同余式

$$x^2 \equiv a \pmod{2^4}$$

的解可表示为

$$x = \pm(1 + 4 \cdot \frac{a - x_3^2}{2^3} + t_4 \cdot 2^3), \quad t_4 = 0, \pm 1, \dots,$$

或者

$$x = \pm(x_4 + t_4 \cdot 2^3), \quad t_4 = 0, \pm 1, \dots$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 99 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

[访问主页](#)[标题页](#)[目录页](#)[◀](#)[▶](#)[◀](#)[▶](#)

第 100 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

类似地, 对于 $\alpha \geq 4$, 如果满足同余式 $x^2 \equiv a \pmod{2^{\alpha-1}}$

的解为 $x = \pm(x_{\alpha-1} + t_{\alpha-1}) \cdot 2^{\alpha-2}$, $t_{\alpha-1} = 0, \pm 1, \dots$

则由 $(x_{\alpha-1} + t_{\alpha-1} \cdot 2^{\alpha-2})^2 \equiv a \pmod{2^\alpha}$,

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

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

或 $t_{\alpha-1} \equiv \frac{a - x_{\alpha-1}^2}{2^{\alpha-1}} \pmod{2}$.

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

$$x = \pm(x_{\alpha-1} + \frac{a - x_{\alpha-1}^2}{2^{\alpha-1}} \cdot 2^{\alpha-2} + t_\alpha \cdot 2^{\alpha-1}), \quad t_\alpha = 0, \pm 1, \dots,$$

或者

$$x = \pm(x_\alpha + t_\alpha \cdot 2^{\alpha-1}), \quad t_\alpha = 0, \pm 1, \dots$$

它们对模 2^α 为 4 个解:

$$x_\alpha, x_\alpha + 2^{\alpha-1}, -x_\alpha, -(x_\alpha + 2^{\alpha-1}).$$

证毕



[访问主页](#)[标题页](#)[目录页](#)[<<](#)[>>](#)[<](#)[>](#)

第 101 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

例4.6.12 求解同余式 $x^2 \equiv 57 \pmod{64}$. $64 = 2^6$

解 因为 $57 \equiv 1 \pmod{8}$, 所以同余式有4个解.

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

$\alpha = 4$ 时, 由于 $(1 + 4t_3)^2 \equiv 57 \pmod{2^4}$, 或 $t_3 \equiv \frac{57-1^2}{8} \equiv 1 \pmod{2}$.

故 $x^2 \equiv a \pmod{2^4}$ 的解: $\pm(1 + 4 \cdot 1 + 8t_4) = \pm(5 + 8t_4)$, $t_4 = 0, \pm 1, \dots$

$\alpha = 5$ 时, 由于 $(5 + 8t_4)^2 \equiv 57 \pmod{2^5}$, 或 $t_4 \equiv \frac{57-5^2}{16} \equiv 0 \pmod{2}$.

故 $x^2 \equiv a \pmod{2^5}$ 的解: $\pm(5 + 8 \cdot 0 + 16t_5) = \pm(5 + 16t_5)$, $t_5 = 0, \pm 1, \dots$

$\alpha = 6$ 时, 由于 $(5 + 16t_5)^2 \equiv 57 \pmod{2^5}$ 或 $t_5 \equiv \frac{57-5^2}{32} \equiv 1 \pmod{2}$.

故 $x^2 \equiv a \pmod{2^6}$ 的解为

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

因此, 同余式模 $64 = 2^6$ 的解是: $21, 53, -21 \equiv 43, -53 \equiv 11 \pmod{64}$.



4.7 $x^2 + y^2 = p$

定理4.7.1 设 p 是素数. 那么 $x^2 + y^2 = p$ 有解的充分必要条件是 $p = 2$ 或 -1 为模 p 平方剩余, 即 $p = 2$ 或 $p = 4k + 1$.

证 设 (x_0, y_0) 是方程 $x^2 + y^2 = p$ 的解, 即 $x_0^2 + y_0^2 = p$, 则一定有

$$0 < |x_0|, |y_0| < p, \quad (x_0, p) = (y_0, p) = 1.$$

因此, 存在 y_0^{-1} 使得

$$y_0^{-1}y_0 \equiv 1 \pmod{p}.$$

当 $p > 2$ 时,

$$(x_0 y_0^{-1})^2 = (p - y_0^2)(y_0^{-1})^2 \equiv -(y_0^{-1}y_0)^2 \equiv -1 \pmod{p}.$$

即 $x^2 \equiv -1 \pmod{p}$ 有解, 从而 $p = 4k + 1$. 必要性成立.

[访问主页](#)[标题页](#)[目录页](#)[◀](#)[▶](#)[◀](#)[▶](#)

第 102 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



再证充分性. $p = 2$ 时, $p = 1^2 + 1^2$. 方程有解.

$p > 2$ 时, $p = 4k + 1$. 因为 $\left(\frac{-1}{p}\right) = 1$, 所以存在整数 x_0 使得

$$x_0^2 \equiv -1 \pmod{p}, \quad 0 < |x_0| < \frac{p}{2}.$$

由此推出, 对于整数 $x_0, y_0 = 1$, 存在整数 m_0 使得

$$x_0^2 + y_0^2 = m_0 p, \quad 0 < m_0 < p.$$

设 m 是使得

$$x^2 + y^2 = mp, \quad 0 < m < p.$$

成立的最小正整数. 要证明 $m = 1$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 103 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

$x^2 + y^2 = mp$, $0 < m < p$. 要证明 $m = 1$.

若 $m > 1$, 我们令 $u \equiv x, v \equiv y \pmod{m}$, $|u|, |v| \leq \frac{m}{2}$. 则有

$$0 < u^2 + v^2 \leq \frac{m^2}{2}, \quad u^2 + v^2 \equiv x^2 + y^2 \pmod{m}.$$

进而 $(u^2 + v^2)(x^2 + y^2) = m'm^2p$, $0 < m' < m$.

将上式变形为

$$(ux + vy)^2 + (uy - vx)^2 = m'm^2p.$$

因为

$$ux + vy \equiv x^2 + y^2 \equiv 0, \quad uy - vx \equiv 0 \pmod{m},$$

所以整数 $x' = \frac{ux + vy}{m}$, $y' = \frac{uy - vx}{m}$ 和 m' 满足

$$x'^2 + y'^2 = \left(\frac{ux + vy}{m}\right)^2 + \left(\frac{uy - vx}{m}\right)^2 = m'p.$$

这与 m 的最小性矛盾. 故 $m = 1$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 104 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.7.1 设 $p = 797$ 为素数. 求正整数 x, y 使得 $x^2 + y^2 = p$

解 因为 p 是 $8k + 5$ 形式的素数,所以

$$x = x_0 = 2^{(p-1)/4} \equiv 215 \pmod{p}$$

是同余式 $x^2 \equiv -1 \pmod{p}$ 的解.

现在令 $y_0 = 1$, 有 $x_0^2 + y_0^2 = m_0 \cdot p$, 其中 $m_0 = 58$.

再令 $u_0 \equiv x_0 \equiv -17 \pmod{m_0}$, $v_0 \equiv y_0 \equiv 1 \pmod{m_0}$ 以及

$$x_1 = \frac{u_0 \cdot x_0 + v_0 \cdot y_0}{m_0} = -63, \quad y_1 = \frac{u_0 \cdot y_0 - v_0 \cdot x_0}{m_0} = -4$$

有 $x_1^2 + y_1^2 = m_1 \cdot p$, 其中 $m_1 = 5$.

最后令 $u_1 \equiv x_1 \equiv 2 \pmod{m_1}$, $v_1 \equiv y_1 \equiv 1 \pmod{m_1}$ 以及

$$x_2 = \frac{u_1 \cdot x_1 + v_1 \cdot y_1}{m_1} = -26, \quad y_2 = \frac{u_1 \cdot y_1 - v_1 \cdot x_1}{m_1} = 11$$

有 $x_2^2 + y_2^2 = p$.

故正整数 $x = 26, y = 11$ 使得 $x^2 + y^2 = p$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 105 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

例4.7.2 $p = 100069$ 为素数. 求正整数 x, y 使得

$$x^2 + y^2 = p$$

解 因为 p 是 $8k + 5$ 形式的素数, 根据例4.3.5 和例4.6.11, 知

$$x = x_0 = 2^{\frac{p-1}{4}} \equiv -39705 \pmod{p}$$

是同余式 $x^2 \equiv -1 \pmod{p}$ 的解.

首先, 令 $y_0 = 1$, 有 $x_0^2 + y_0^2 = m_0 \cdot p$, 其中 $m_0 = 15754$.

其次, 令 $u_0 \equiv x_0 \equiv 7557 \pmod{m_0}$, $v_0 \equiv y_0 \equiv 1 \pmod{m_0}$ 以及

$$x_1 = \frac{u_0 \cdot x_0 + v_0 \cdot y_0}{m_0} = -19046, \quad y_1 = \frac{u_0 \cdot y_0 - v_0 \cdot x_0}{m_0} = 3$$

有 $x_1^2 + y_1^2 = m_1 \cdot p$, 其中 $m_1 = 3625$.

依次, 令 $u_1 \equiv x_1 \equiv -921 \pmod{m_1}$, $v_1 \equiv y_1 \equiv 3 \pmod{m_1}$ 以及

$$x_2 = \frac{u_1 \cdot x_1 + v_1 \cdot y_1}{m_1} = 4839, \quad y_2 = \frac{u_1 \cdot y_1 - v_1 \cdot x_1}{m_1} = 15$$

有 $x_2^2 + y_2^2 = m_2 \cdot p$, 其中 $m_2 = 234$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 106 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



依次, 令 $u_2 \equiv x_2 \equiv -75 \pmod{m_2}$, $v_2 \equiv y_2 \equiv 15 \pmod{m_2}$ 以及

$$x_3 = \frac{u_2 \cdot x_2 + v_2 \cdot y_2}{m_2} = -1550, \quad y_3 = \frac{u_2 \cdot y_2 - v_2 \cdot x_2}{m_2} = -315$$

有 $x_3^2 + y_3^2 = m_3 \cdot p$, 其中 $m_3 = 25$.

依次, 令 $u_3 \equiv x_3 \equiv 0 \pmod{m_3}$, $v_3 \equiv y_3 \equiv 10 \pmod{m_3}$ 以及

$$x_4 = \frac{u_3 \cdot x_3 + v_3 \cdot y_3}{m_3} = -126, \quad y_4 = \frac{u_3 \cdot y_3 - v_3 \cdot x_3}{m_3} = 620$$

有 $x_4^2 + y_4^2 = m_4 \cdot p$, 其中 $m_4 = 4$.

最后, 令 $u_4 \equiv x_4 \equiv 2 \pmod{m_4}$, $v_4 \equiv y_4 \equiv 0 \pmod{m_4}$ 以及

$$x_5 = \frac{u_4 \cdot x_4 + v_4 \cdot y_4}{m_4} = -63, \quad y_5 = \frac{u_4 \cdot y_4 - v_4 \cdot x_4}{m_4} = 310$$

有 $x_5^2 + y_5^2 = m_5 \cdot p$, 其中 $m_5 = 1$.

故正整数 $x = -63$, $y = 310$ 使得 $x^2 + y^2 = p$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 107 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例4.7.3 设 $p = 100000037$ 为素数. 求正整数 x, y 使得

$$x^2 + y^2 = p$$

解 因为 p 是 $8k + 5$ 形式的素数, 根据例4.3.5 和例4.6.11, 知

$$x = x_0 = 2^{\frac{p-1}{4}} \equiv 55387563 \pmod{p}$$

是同余式 $x^2 \equiv -1 \pmod{p}$ 的解.

首先, 令 $y_0 = 1$, 有 $x_0^2 + y_0^2 = m_0 \cdot p$, 其中 $m_0 = 30677810$.

其次, 令 $u_0 \equiv x_0 \equiv -5968057 \pmod{m_0}$, $v_0 \equiv y_0 \equiv 1 \pmod{m_0}$ 以及

$$x_1 = \frac{u_0 \cdot x_0 + v_0 \cdot y_0}{m_0} = -10775089, \quad y_1 = \frac{u_0 \cdot y_0 - v_0 \cdot x_0}{m_0} = -2$$

有 $x_1^2 + y_1^2 = m_1 \cdot p$, 其中 $m_1 = 1161025$.

依次, 令 $u_1 \equiv x_1 \equiv -325864 \pmod{m_1}$, $v_1 \equiv y_1 \equiv -2 \pmod{m_1}$ 以及

$$x_2 = \frac{u_1 \cdot x_1 + v_1 \cdot y_1}{m_1} = 3024236, \quad y_2 = \frac{u_1 \cdot y_1 - v_1 \cdot x_1}{m_1} = -18$$

有 $x_2^2 + y_2^2 = m_2 \cdot p$, 其中 $m_2 = 91460$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 108 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



依次, 令 $u_2 \equiv x_2 \equiv 6056 \pmod{m_2}$, $v_2 \equiv y_2 \equiv -18 \pmod{m_2}$ 以及

$$x_3 = \frac{u_2 \cdot x_2 + v_2 \cdot y_2}{m_2} = 200249, \quad y_3 = \frac{u_2 \cdot y_2 - v_2 \cdot x_2}{m_2} = 594$$

有 $x_3^2 + y_3^2 = m_3 \cdot p$, 其中 $m_3 = 401$.

依次, 令 $u_3 \equiv x_3 \equiv 150 \pmod{m_3}$, $v_3 \equiv y_3 \equiv 193 \pmod{m_3}$ 以及

$$x_4 = \frac{u_3 \cdot x_3 + v_3 \cdot y_3}{m_3} = 75192, \quad y_4 = \frac{u_3 \cdot y_3 - v_3 \cdot x_3}{m_3} = -96157$$

有 $x_4^2 + y_4^2 = m_4 \cdot p$, 其中 $m_4 = 149$.

依次, 令 $u_4 \equiv x_4 \equiv 6812 \pmod{m_4}$, $v_4 \equiv y_4 \equiv -52 \pmod{m_4}$ 以及

$$x_5 = \frac{u_4 \cdot x_4 + v_4 \cdot y_4}{m_4} = -63, \quad y_5 = \frac{u_4 \cdot y_4 - v_4 \cdot x_4}{m_4} = 60445$$

有 $x_5^2 + y_5^2 = m_5 \cdot p$, 其中 $m_5 = 37$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 109 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



依次, 令 $u_5 \equiv x_5 \equiv 4 \pmod{m_5}$, $v_5 \equiv y_5 \equiv -13 \pmod{m_5}$ 以及

$$x_6 = \frac{u_5 \cdot x_5 + v_5 \cdot y_5}{m_5} = -20501, \quad y_6 = \frac{u_5 \cdot y_5 - v_5 \cdot x_5}{m_5} = 8928$$

有 $x_6^2 + y_6^2 = m_6 \cdot p$, 其中 $m_6 = 5$.

最后, 令 $u_6 \equiv x_6 \equiv -1 \pmod{m_6}$, $v_6 \equiv y_6 \equiv -2 \pmod{m_6}$ 以及

$$x_7 = \frac{u_6 \cdot x_6 + v_6 \cdot y_6}{m_6} = 529, \quad y_7 = \frac{u_6 \cdot y_6 - v_6 \cdot x_6}{m_6} = -9986$$

有 $x_7^2 + y_7^2 = m_7 \cdot p$, 其中 $m_7 = 1$.

故正整数 $x = 529$, $y = -9986$ 使得 $x^2 + y^2 = p$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 110 页 共 130 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)