

1. 设 p 为奇素数，求证： $\forall a, b \in \mathbb{Z}$ ，同余方程
 $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{p}$ 必有解.

分类讨论：

(1)： a 或者 b 是二次剩余

则有 $x^2 - a \equiv 0 \pmod{p}$ 或 $x^2 - b \equiv 0 \pmod{p}$ 有解 x_0

于是 $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{p}$ 有解 x_0

(2)： a 和 b 都不是二次剩余

则根据勒让德符号，有：

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$$

$$\text{于是} \left(\frac{ab}{p}\right) = (-1)(-1) = 1$$

所以 $x^2 - ab \equiv 0 \pmod{p}$ 有解 x_0

于是 $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{p}$ 有解 x_0

综上，原式必有解

2. 设 p 为奇素数，若 $x^2 - 7 \equiv 0 \pmod{p}$ 有解，求 p .

即 $x^2 \equiv 7 \pmod{p}$ 有解

于是根据勒让德符号，有 $\left(\frac{7}{p}\right) = 1$

由于 $p, 7$ 是奇素数，而且根据题设， $p \nmid 7$ ，所以 $(p, 7) = 1$

根据二次互反律， $\left(\frac{7}{p}\right) = (-1)^{\frac{7-1}{2} \frac{p-1}{2}} \left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right)$

分类讨论：

(1)

$p = 1 + 4k$ 时，原式化为 $\left(\frac{p}{7}\right)$

(2)

$p = 3 + 4k$ 时，原式化为 $-\left(\frac{p}{7}\right)$

而 $\left(\frac{p}{7}\right) = 1$ ，当 $p = (1, 2, 4) + 7k$

$\left(\frac{p}{7}\right) = -1$ ，当 $p = (3, 5, 6) + 7k$

根据以上讨论，有 $p = 1 + 4k$ 且 $p = (1, 2, 4) + 7k$ 时有 $\left(\frac{7}{p}\right) = 1$

或者 $p = 3 + 4k$ 且 $p = (3, 5, 6) + 7k$ 时有 $\left(\frac{7}{p}\right) = 1$

通过中国剩余定理，求解6个方程组

$$\begin{cases} p \equiv 1 \pmod{4} \\ p \equiv 1, 2, 4 \pmod{7} \end{cases} \quad \begin{cases} p \equiv 3 \pmod{4} \\ p \equiv 3, 5, 6 \pmod{7} \end{cases}$$

解得 $p \equiv 1, 9, 25, 27, 19, 3 \pmod{28}$

3. 设 p 为奇素数， $p \mid x^4 + 1$ ，证： $p \equiv 1 \pmod{8}$.

由 $p|x^4 + 1$, 所以 $x^4 + 1 = kp, x^4 = kp - 1$
 所以 $x^4 \equiv -1 \pmod{p}$
 设二次同余式 $(x^2)^2 \equiv -1 \pmod{p}$, 故本同余式有解
 根据勒让德符号, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1$
 所以 $p = 1 + 4k \equiv 1, 5 \pmod{8}$
 又根据 $(x^2)^2 \equiv -1 \pmod{p}$, 有
 $(x^2 + 1)^2 = x^4 + 2x^2 + 1 \equiv 2x^2 \pmod{p}$, 有解
 根据勒让德符号, 有 $(\frac{2x^2}{p}) = 1$
 所以, $(\frac{2}{p})(\frac{x}{p})(\frac{x}{p}) = (\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$
 而 $p \equiv 1, 5 \pmod{8}$
 所以为满足条件, $p \equiv 1 \pmod{8}$

4. 判断下列方程是否有解

(1) $x^2 \equiv 118 \pmod{229}$;

(2) $x^2 \equiv 681 \pmod{1789}$;

$$\begin{aligned} & \text{(1)} \\ & \text{根据勒让德符号 } (\frac{118}{229}) = (\frac{2}{229})(\frac{59}{229}) = (-1)^{\frac{228*230}{8}}(\frac{59}{229}) \\ & = -(\frac{59}{229}) \\ & = -1 * (-1)^{29*114}(\frac{229}{59}) = -1 * (\frac{52 = 13 * 4}{59}) = -1(\frac{13}{59}) = 1 \end{aligned}$$

有解

$$\begin{aligned} & \text{(2)} \\ & \text{根据勒让德符号 } (\frac{681}{1789}) = -1, \text{无解} \end{aligned}$$

7. 求解同余方程 $3x^2 + x + 6 \equiv 0 \pmod{45}$.

$45 = 5 \times 9, (5, 9) = 1$, 所以原方程可以等价为 :

$$\begin{cases} f(x) \equiv 0 \pmod{5} \dots (1) \\ f(x) \equiv 0 \pmod{9} \dots (2) \end{cases}$$

将 0, 1, 2, 3, 4 代入 (1) 得到解, $x \equiv 1, 2 \pmod{5}$

将 0 - 8 代入 (2) 得到解, $x \equiv 3 \pmod{9}$

由中国剩余定理求解同余方程组 :

$$\begin{cases} x \equiv b_1 \pmod{5} \\ x \equiv b_2 \pmod{9} \end{cases}$$

解得 $x \equiv 36b_1 + 10b_2 \pmod{45}$

最终得到解为 :

$$x \equiv 36 + 30, 2 * 36 + 30 \pmod{45}$$

$$x \equiv 21, 12 \pmod{45}$$