第四章练习题

(1) 求模 $p = 13, 23, 31, 37, 47$ 的二次剩余和二次非剩余.

(12) 求解同余式 $x^2 \equiv 511 \pmod{1155}$.

(20) ① $\left(\frac{17}{37}\right)$; ② $\left(\frac{151}{373}\right)$; ③ $\left(\frac{191}{397}\right)$; ④ $\left(\frac{911}{2003}\right)$; ⑤ $\left(\frac{37}{200\,723}\right)$; ⑥ $\left(\frac{7}{20\,040\,803}\right)$.

(22) 求下列同余方程的解数:

① $x^2 \equiv -2 \pmod{67}$; ② $x^2 \equiv 2 \pmod{67}$;

③ $x^2 \equiv -2 \pmod{37}$; ④ $x^2 \equiv 2 \pmod{37}$.

(24) 设 p 是奇素数. 证明:

(i) 模 p 的所有二次剩余的乘积对模 p 的剩余是 $(-1)^{(p+1)/2}$.

(ii) 模 p 的所有二次非剩余的乘积对模 p 的剩余是 $(-1)^{(p-1)/2}$.

(iii) 模 p 的所有二次剩余之和对模 p 的剩余是: 1, 当 $p = 3$ 时; 0, 当 $p > 3$ 时.

(iv) 所有二次非剩余之和对模 p 的剩余是多少?

(37) 设 $p = 401$. 求解下列同余式:

(i) $x^2 = 2 \pmod{p}$. (ii) $x^2 = 3 \pmod{p}$. (iii) $x^2 = 5 \pmod{p}$.

(iv) $x^2 = 7 \pmod{p}$. (v) $x^2 = 11 \pmod{p}$.

强化练习题

【注：强化练习题不强制要求同学们提交作业，留给大家课后练习】

(25) 设 p 是奇素数, 且 $p \equiv 1 \pmod{4}$. 证明:

(i) $1, 2, \cdots, \frac{p-1}{2}$ 中模 p 的二次剩余与二次非剩余的个数均为 $\frac{p-1}{4}$ 个.

(ii) $1, 2, \cdots, (p-1)$ 中有 $\frac{p-1}{4}$ 个偶数为模 p 的二次剩余, $\frac{p-1}{4}$ 个奇数为模 p 的二次剩余.

(iii) $1, 2, \cdots, (p-1)$ 中有 $\frac{p-1}{4}$ 个偶数为模 p 的二次非剩余, $\frac{p-1}{4}$ 个奇数为模 p 的二次非剩余.

(iv) $1, 2, \cdots, (p-1)$ 中全体模 p 的二次剩余之和等于 $\frac{p(p-1)}{4}$.

(v) $1, 2, \cdots, (p-1)$ 中全体模 p 的二次非剩余之和等于 $\frac{p(p-1)}{4}$.

(26) 判断下列同余方程是否有解:

① $x^2 \equiv 7 \pmod{227}$; ② $x^2 \equiv 11 \pmod{511}$;

③ $11x^2 \equiv -6 \pmod{91}$; ④ $5x^2 \equiv -14 \pmod{6193}$.

(33) 证明: 对任意素数 p, 必有整数 a, b, c, d 使得

$$x^4 + 1 \equiv (x^2 + ax + b)(x^2 + cx + d) \pmod{p}.$$

(34) 证明: 对任意素数 p, 同余式

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) \equiv 0 \pmod{p}$$

有解.

【作业要求】

1. 禁止抄袭
2. 作业提交 1）可以先手写再拍照或者 2）直接在 word 或 latex 输入公式和数学符号，word 或者 pdf 格式，文件命名格式为：专业+学号+姓名+第几次作业
3. 作业提交方式为邮箱提交：sysu_mfis2020@163.com
4. 提交截至日期：**2020 年 7 月 24 日 23:59 前**