

初等数论练习题

一、填空题

- 1、 $d(2420)=12$; $\phi(2420)= 880$
- 2、设 a, n 是大于 1 的整数, 若 a^n-1 是质数, 则 $a=$ 2.
- 3、模 9 的绝对最小完全剩余系是 $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$.
- 4、同余方程 $9x+12= 0(\text{mod } 37)$ 的解是 $x \equiv 11(\text{mod } 37)$ 。
- 5、不定方程 $18x-23y=100$ 的通解是 $x=900+23t, y=700+18t \ t \in \mathbb{Z}$ 。
- 6 分母是正整数 m 的既约真分数的个数为 $\phi(m)$ 。

8、 $\frac{65}{103} \equiv -1$ 。

7、 18^{100} 被 17^2 除的余数是 256。

9、若 p 是素数, 则同余方程 $x^{p-1} \equiv 1(\text{mod } p)$ 的解数为 $p-1$ 。

二、计算题

1、解同余方程： $3x^2+11x+20 \equiv 0(\text{mod } 105)$ 。

解：因 $105 = 3 \cdot 5 \cdot 7$,

同余方程 $3x^2+11x+20 \equiv 0(\text{mod } 3)$ 的解为 $x \equiv 1(\text{mod } 3)$,

同余方程 $3x^2+11x+20 \equiv 0(\text{mod } 5)$ 的解为 $x \equiv 0, 3(\text{mod } 5)$,

同余方程 $3x^2+11x+20 \equiv 0(\text{mod } 7)$ 的解为 $x \equiv 2, 6(\text{mod } 7)$,

故原同余方程有 4 解。

作同余方程组： $x \equiv b_1(\text{mod } 3)$, $x \equiv b_2(\text{mod } 5)$, $x \equiv b_3(\text{mod } 7)$,

其中 $b_1 = 1, b_2 = 0, 3, b_3 = 2, 6$,

由孙子定理得原同余方程的解为 $x \equiv 13, 55, 58, 100(\text{mod } 105)$ 。

2、判断同余方程 $x^2 \equiv 42(\text{mod } 107)$ 是否有解？

故同余方程 $x^2 \equiv 42(\text{mod } 107)$ 有解。

3、求 $(1271^{56}+34)^{28}$ 除以 111 的最小非负余数。

解：易知 $1271 \equiv 50(\text{mod } 111)$ 。

由 $50^2 \equiv 58 \pmod{111}$, $50^3 \equiv 58 \times 50 \equiv 14 \pmod{111}$, $50^9 \equiv 14^3 \equiv 80 \pmod{111}$ 知
 $50^{28} \equiv (50^9)^3 \times 50 \equiv 80^3 \times 50 \equiv 68 \times 50 \equiv 70 \pmod{111}$

从而 $50^{56} \equiv 16 \pmod{111}$ 。

故 $(1271^{56} + 34)^{28} \equiv (16 + 34)^{28} \equiv 50^{28} \equiv 70 \pmod{111}$

三、证明题

1、已知 p 是质数, $(a, p) = 1$, 证明:

(1) 当 a 为奇数时, $a^{p-1} + (p-1)^a \equiv 0 \pmod{p}$;

2、设 a 为正奇数, n 为正整数, 试证 $2^n \equiv 1 \pmod{2^{n+2}}$ 。 (1)

成立。

(2) 当 a 为偶数时, $a^{p-1} - (p-1)^a \equiv 0 \pmod{p}$ 。

证明: 由欧拉定理知 $a^{p-1} \equiv 1 \pmod{p}$ 及 $(p-1)^a \equiv -1 \pmod{p}$ 立得(1)和(2)

证明设 $a = 2m + 1$, 当 $n = 1$ 时, 有

$$a^{2^k} \equiv 1 \pmod{2^{k+2}} \quad a = (2m+1)^2 = 4m(m+1) + 1 \equiv 1 \pmod{2^{k+2}}, \text{ 即原式成立。}$$

其中 q 是某个整数。这说明式 (1) 当 $n = k + 1$ 也成立。

其中 $q \in \mathbb{Z}$, 所以 $a \equiv (1 + q2^k) \equiv 1 + q2^k \pmod{2^{k+2}}$,

由归纳法知原式对所有正整数 n 成立。

3、设 p 是一个素数, 且 $k < p-1$ 。证明: $C_{p-1}^k \equiv (-1)^k \pmod{p}$ 。

证明: 设 $A = C_{p-1}^k = \frac{(p-1)(p-2)\dots(p-k)}{k!}$ 得: $p \mid k!$

$$k! \cdot A = (p-1)(p-2)\dots(p-k) \equiv (-1)(-2)\dots(-k) \pmod{p}$$

$$\text{又 } (k!, p) = 1, \text{ 故 } A \equiv C_{p-1}^k \equiv (-1)^k \pmod{p}$$

4、设 p 是不等于 3 和 7 的奇质数, 证明: $p^6 \equiv 1 \pmod{84}$ 。

说明: 因为 $84 = 4 \times 3 \times 7$, 所以, 只需证明:

$$p^6 \equiv 1 \pmod{4} \quad p^6 \equiv 1 \pmod{3} \quad p^6 \equiv 1 \pmod{7} \text{ 同时成立即可。}$$

证明: 因为 $84 = 4 \times 3 \times 7$ 及 p 是不等于 3 和 7 的奇质数, 所以

$$(p, 4) = 1, (p, 3) = 1, (p, 7) = 1。$$

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/918040027143006107>