

2. 数论初步

xiaoga@mailustc.edu.cn

P42

25. 证明:

(1) 如果 $6|n$, 则 $\phi(n) \leq \frac{n}{3}$ 。

证明:

$6|n$, $6=2 \times 3$, 且 $(2, 3) = 1$

$\therefore 2|n$, 且 $3|n$

$\therefore 2|n$, 则 n 所有偶因子都不与之互素

$\therefore \phi(n) \leq \frac{n}{2}$

$\therefore 3|n$, 则有奇因子 $m=3k$ (k 为奇数, $m \leq n$) $\frac{n}{6}$ 个

$\therefore \phi(n) \leq \frac{n}{2} - \frac{n}{6} = \frac{n}{3}$ 。

28. 7^{355} 的末位数是什么? 末两位数是什么?

解:

$\phi(100) = 40$

$(7, 100) = 1$

由欧拉定理:

$$7^{355} = (7^{40})^8 \times 7^{35} = 7^{35} \pmod{100}$$

又

$$7^4 \equiv 1 \pmod{100}$$

得到

$$7^{355} \equiv 7^{35} = (7^4)^8 \times 7^3 \equiv 7^3 \equiv 43 \pmod{100}$$

33. 证明

$$\sum_{d|n} \frac{1}{d} = \frac{1}{n} \sigma(n)。$$

证明:

$\therefore d|n$

$\therefore \frac{n}{d} | n$, 且 $d \Leftrightarrow \frac{n}{d}$

$$\therefore \sum_{d|n} \frac{1}{d} = \sum_{d|n} \frac{1}{n/d} = \sum_{d|n} \frac{d}{n} = \frac{1}{n} \sum_{d|n} d = \frac{1}{n} \sigma(n)。$$

38 (3) 利用此表解 $x^9 \equiv 2 \pmod{29}$ 。

解:

29的最小原根为2.

$$(9, 28) = 1$$

先解 $9y \equiv 1 \pmod{28}$

$$\Rightarrow y \equiv 25 \pmod{28}$$

\therefore 解为 $x \equiv 2^{25} \pmod{29}$, 即 $x \equiv 11 \pmod{29}$ 。

42. 证明: 若 a 模 p 的阶为3, 则 $a+1$ 模 p 的阶为6.

证明:

$$\because a^3 \equiv 1 \pmod{p}$$

$$\therefore a^3 = (a-1)(a^2 + a + 1) \equiv 0 \pmod{p}$$

$$\therefore (a-1) \equiv 0 \pmod{p} \text{ 或 } (a^2 + a + 1) \equiv 0 \pmod{p}$$

又 a 模 p 的阶为3

$$\text{则 } (a^2 + a + 1) \equiv 0 \pmod{p}$$

\Rightarrow

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

$$(a + 1)^2 \equiv a^2 + 2a + 1 \equiv a \pmod{p}$$

$$(a + 1)^3 \equiv (-a^3) \pmod{p}$$

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

$$(a + 1)^5 \equiv (-a^4) \pmod{p}$$

$$(a + 1)^6 \equiv a^3 \equiv 1 \pmod{p}$$

但 a 模 m 的阶还有可能为6的因子, 即1, 2, 3

若阶为1, $a + 1 \equiv 1 \pmod{p}$, $a \equiv 0 \pmod{p}$, 与 $a^3 \equiv 1 \pmod{p}$ 矛盾。

若阶为2, $(a + 1)^2 \equiv a \pmod{p}$, 与 a 模 p 的阶为3矛盾。

若阶为3, $(a + 1)^3 \equiv a^3 + 3a^2 + 3a + 1 \equiv 3a^2 + 3a + 3 - 1 \equiv -1 \equiv 1 \pmod{p}$ 矛盾。

\therefore $a+1$ 模 p 的阶为6。