第五章课后习题

P196-197. 习题 (1), (3), (7), (11), (13), (16)

(1) $2^{ord_{13}2} \equiv 1 \pmod{13}$

$2^1 \equiv 2 \qquad 2^4 \equiv 3$

$2^2 \equiv 4 \qquad 2^5 \equiv 6$

$2^3 \equiv 8 \qquad 2^6 \equiv 12 \equiv -1 \pmod{13}$

$\therefore ord_{13}2 = 12$

同理得 $ord_{13}5 = 4$

$\because (ord_{13}(2), ord_{13}(5)) = (12,4) = 4$

$\therefore$ 不能使用 $ord_m(a\cdot b) = ord_m(a)\cdot ord_m(b)$

求 $ord_{13}10$

$10^2 \equiv 100 \equiv 9$

$10^3 \equiv 90 \equiv -1$

$\therefore ord_{13}10 = 6$

(3) 求模81的原根.

$\because 81 = 3^4$

$\therefore \cancel{\varphi(81) = [\varphi(3)]^4 = 16 = \underbrace{2^4}_{q_1}}$

不能这么用

$\varphi(81) = 54 = \underbrace{2}_{q_1} \times \underbrace{3^3}_{q_2}$

$\therefore \varphi(m)/q_1 = 8$

验证 $a^8 \not\equiv 1 \pmod{81}$

对 $\underbrace{2, 3, \cdots}_{\text{81的简化剩余系}}$ 逐一验证

$\varphi(m)/2 = 27$

$\varphi(m)/3 = 18$

$2^8 = 256 \equiv 13 \not\equiv 1 \pmod{81}$

$\therefore$ 2为81的一个原根

最后得到

$\therefore\ 2^0, 2, 2^2, \cdots, 2^{\varphi(81)-1}$ 构成一个简化剩余系
2^{53}

对于 2^r，若 $(r, \varphi(m))=1$，则 2^r 为原根

个数 $\varphi(\varphi(m))$ 个，遍历 0~53 找.

(7) 设 m>1 为整，$(a,m)=1$，若 $ord_m(a)=st$，求证 $ord_m(a^s)=t$

? 证明：已知 $a^{st}\equiv 1 \pmod m$

又 $\because (a,m)=1$

$\therefore st \mid \varphi(m)$，st 为满足最小值

即 $(st, \varphi(m))=st$ ↑

$\therefore$ 证得 $ord_m(a^s)=t$

(11) 求模 113 的原根

$\varphi(113)=112$，113 为素数

$112=2^4\times 7$

$\therefore \varphi(112)/2=56$

$\varphi(112)/7=16$

1024

1008

对于 2，3，5，6，7… 判断

$2^{56}\not\equiv 1 \pmod{112}$

$2^4\equiv 16$

$2^{16}\not\equiv 1 \pmod{112}$

$2^8\equiv 32$

$2^{16}\equiv 16 \pmod{112}$

$\therefore$ 2 为其的一个原根

$\therefore 2^0, 2, 2^1, 2^2, \cdots, 2^{111}$ 为其一个简化剩余系

对于如上 2^r，若 $(r, 112)=1$，则 2^r 为一个原根　　$(112=2^4\times 7)$

$\therefore 2, 2^3, 2^5, 2^7, 2^9, 2^{11}\cdots \pmod{112}$

(13) 同 (11)

(16) 解同余式 $x^{22} \equiv 5 \pmod{41}$ → 指标

1) 找 41 的一个原根 —) 为查指标表作准备

$\varphi(41) = 40 = 2^3 \times 5$

$40/2 = 20$, $40/5 = 8$

从 2, 3, 5, 6, 7 … 中找

$2^{20} \equiv 1$ $\quad 3^{20} \not\equiv 1$ … 6为一个原根.

$2^{8} \not\equiv 1 \pmod{41}$ $\quad 3^{8} \equiv 1 \pmod{41}$

2) 查指标表.

$\mathrm{ind}\,5 = 22$ 即 $6^{22} \equiv 5 \pmod{41}$ $\quad x^{22} \equiv 5 \pmod{41}$

设 $x = 6^y$ 有 $6^{22y} \equiv 6^{22} \pmod{41}$

$\therefore 22y \equiv 22 \pmod{\varphi(41)}$

$22y \equiv 22 \pmod{40}$

3) 解同余式.

$(22, 40) = 2 \mid 22$ 有解

$\frac{22}{2} = 11$, $\frac{40}{2} = 20$

求解 $11y_0 \equiv 1 \pmod{20}$

$y_0 \equiv 11 \pmod{20}$

$\therefore$ 特解 $y_1 \equiv \frac{22}{2} \cdot 11 \equiv 1 \pmod{20}$

$\therefore$ 解为 $y \equiv 1, 21 \pmod{40}$

4) 得 x

$\because x = 6^y$ $\quad \therefore x \equiv 6 \pmod{41}$ 或 $x \equiv 6^{21} \equiv 35 \pmod{41}$

例：求 $x^5 \equiv 9 \pmod{41}$ ↑类似题目

$\mathrm{ind}_6 9 = 30$

$\because (5, 40) = 5 \mid 30$ ∴有解

$\therefore 6^{30} \equiv 9 \pmod{41}$

设 $x \equiv 6^y \pmod{41}$

则有 $6^{5y} \equiv 6^{30} \pmod{41}$

即 $\underbrace{5y \equiv 30 \pmod{40}}$

$(5, 40) = 5 \mid 30$，有解

$\therefore y_0 \equiv 1 \pmod{8}$

$\therefore$ 特解 $y_1 \equiv \frac{30}{5} \equiv 6 \pmod{8}$

$\therefore y \equiv 6, 14, 22, 30, 38 \pmod{40}$

$\therefore x \equiv 6^6, 6^{14} \cdots \pmod{41}$