中山大学 计算机学院 2022 春季学期
学生姓名: 武自厚 指导老师: 韦宝典 & 杜育松
学生学号: 20336014

信息安全数学基础 @A104

Chap.5 原根与指标

问题 1

计算 2,5,10 模 13 的指数.

回答

经计算:

$$2^{12} \equiv 3^3 \equiv 10^6 \equiv 1 \pmod{13}$$

$$\mathrm{ord}_{13}2 = 12, \quad \mathrm{ord}_{13}3 = 3, \quad \mathrm{ord}_{13}10 = 6$$

问题 2

求模 47 的原根数量.

回答

已知 47 为奇素数, 所以模 47 的原根存在, 原根数量为:

$$\varphi(47-1) = \varphi(46) = \varphi(2) \cdot \varphi(23) = 1 \cdot 22 = 22$$

问题 3

设 $m = a^n - 1$, 其中 a 与 n 是正整数. 证明: $\mathrm{ord}_m a = n$, 从而得到 $n \mid \varphi(m)$.

回答

容易得到 $a \neq 1$, 且

$$a^n = m + 1 \equiv 1 \pmod{m}$$

由题设知 $a > 1$, 则 $\forall k(1 \leq k < n) : 1 < a^k < m + 1$. 因此 n 是满足 $a^n \equiv 1 \pmod{m}$ 的最小整数, 即 $\mathrm{ord}_m a = n$.

又由 Euler 公式得到 $a^{\varphi(m)} \equiv 1 \pmod{m}$. 所以可以得到 $\mathrm{ord}_m a \varphi(m)$ 即 $n \mid \varphi(m)$

问题 4

求模 167^2 的原根.

回答

已知 167 是素数, 所以 167^2 存在原根. 先找 167 的原根 g. $167-1=166=2\cdot 83$.

已知 g 满足 $g^{\frac{p-1}{q_i}}\not\equiv 1 \pmod{167}$, 其中 $q_i=2,83$. 经过检验, $g=6$. 所以 $g_1=g=6$ 或 $g_2=g+p=173$ 是模 167 的原根. 计算验证:

$$g_1^{167-1}\equiv 1+114\cdot 167,\quad g_2^{167-1}\equiv 1+86\cdot 167 \pmod{167^2}$$

因此 $g_1=6, g_2=173$ 都是模 167^2 的原根.

问题 5

求解同余方程 $x^{22}\equiv 5 \pmod{41}$.

回答

已知模 41 的一个原根是 6, 且 $\gcd(22,\varphi(41))=2$, 可以得知这个方程解数为 2. 又 $\operatorname{ind}_6 5\equiv 22 \pmod{41}$.

可以得出原方程等价于 $22\operatorname{ind}_6 x=\operatorname{ind}_6 5 \pmod{40}$. 解得 $\operatorname{ind}_6 x\equiv 1,21 \pmod{40}$.

因此 $x\equiv 6,35 \pmod{41}$.