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:

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

所以,

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

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 $n \mid \varphi(m)$.

问题 4

求模 167^2 的原根.

问题 5

求解同余方程

$$x^{22} \equiv 5 \pmod{41}$$