

近世代数第一次作业

任课教师：刘玉明 答疑教师：陈红星、李喜凤

专业：数学与应用数学 2008 级

1. 证明： $3 \mid 4^n - 1$, 其中 $n \in \mathbb{N}$.

2. 解同余方程组

$$\begin{cases} x \equiv 0 \pmod{2}, \\ x \equiv 2 \pmod{3}, \\ x \equiv 4 \pmod{5}. \end{cases}$$

3. 设 $N = pq$ 是两个不同素数的乘积. 证明 p 和 q 是方程

$$x^2 + (\varphi(N) - N - 1)x + N = 0$$

的两个根. 由此说明：分解 $N = pq$ 与计算 $\varphi(N)$ 有相同的难度.

4. 令 p 是一个素数. 证明：

(1) $p \mid \binom{p}{i}$, 其中 $1 \leq i \leq p-1$.

(2) $(a+b)^p \equiv a^p + b^p \pmod{p}$, 其中 $a, b \in \mathbb{Z}$.