NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Assignment 2

2023 年 9 月 15 日

Problem 1

若 $a \equiv b \pmod{m_i}$, $i = 1, 2, \ldots, k$, 证明

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}.$$

Problem 2

设 m, n 是两个互素的正整数. $x_1, x_2, \ldots, x_{\phi(m)}$ 是模 m 的一个简化剩余系, $y_1, y_2, \ldots, y_{\phi(n)}$ 是模 n 的一个化剩余系, 证明 $my_1 + nx_1, my_1 + nx_2, \ldots, my_1 + nx_{\phi(m)}, \ldots, my_{\phi(n)} + nx_1, my_{\phi(n)} + nx_2, \ldots, my_{\phi(n)} + nx_{\phi(m)}$ 是模 mn 的一个简化剩余系.