UE Discrete Mathematics

Exercises for Dec 19, 2023

101) Use the Chinese remainder theorem to solve the following system of congruence relations:

$$4x \equiv 12\ (13), \qquad 3x \equiv 7\ (20), \qquad 2x \equiv 3\ (7).$$

102) Use the Chinese remainder theorem to solve the following system of congruence relations:

$$7x \equiv 8\ (24), \qquad 12x \equiv 4\ (28), \qquad 9x \equiv 3\ (15).$$

103) Prove that the sum of two squares of odd integers is always even, but never divisible by 4.

104) Let $(m, e) = (3233, 49)$ be a public RSA key. Compute the private key (m, d).

105) Use the key of Exercise 104) to encrypt the string „`COMPUTER`“. Decompose the string into blocks of length 2 and apply the mapping $\texttt{A} \mapsto 01,\ \texttt{B} \mapsto 02, \ldots,\ \texttt{Z} \mapsto 26$.

106) Prove that the identity

$$\varphi(m \cdot n) = \varphi(m)\varphi(n)\frac{\gcd(m,n)}{\varphi(\gcd(m,n))}$$

holds for all $m, n \in \mathbb{N}^+$. φ denotes Euler's totient function.

107) Let G be a finite, abelian group and $a \in G$ an element for which $\mathrm{ord}_G(a)$ is maximal. Prove that for all $b \in G$ the order $\mathrm{ord}_G(b)$ is a divisor of $\mathrm{ord}_G(a)$.

108) Let λ and φ denote the Carmichael function and Euler's totient function, respectively. Compute $\lambda(351384)$ and $\varphi(351384)$.

109) Show that $m \mid n$ implies $\lambda(m) \mid \lambda(n)$ where λ denotes the Carmichael function.

Hint: Prove first that $a_i \mid b_i$ for $i = 1, \ldots, k$ implies $\mathrm{lcm}(a_1, a_2, \ldots, a_k) \mid \mathrm{lcm}(b_1, b_2, \ldots, b_k)$.

110) Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ where $i = \sqrt{-1}$. Show that $\mathbb{Z}[i]$ is a subring of $(\mathbb{C}, +, \cdot)$ and determine its group of units $(\mathbb{Z}[i]^*, \cdot)$. Is $\mathbb{Z}[i]$ an integral domain?