10^{th} EXERCISE
104.272 Discrete Mathematics

(91) Let (e, n) and (d, n) be Bob's public and private RSA key, respectively. Suppose that Bob sends an encrypted message c and Alice wants to find out the original message m. She has the idea to send Bob a message and ask him to sign it. How can she find out m?

Hint: Pick a random integer r and consider the message $r^e c$ mod n. What property does r need to satisfy?

(92) Let G be a finite 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 $\mathrm{ord}_G(a)$.

(93) Prove that if G is a finite group and $a \in G$ is an element with $\mathrm{ord}_G(a) = r$, then for every $k \in \mathbb{N}$, $\mathrm{ord}_G(a^k) = r/\gcd(r, k)$.

(94) Use the Euclidean algorithm to find all greatest common divisors of $x^3 + 5x^2 + 7x + 3$ and $x^3 + x^2 - 5x + 3$ in $\mathbb{Q}[x]$.

(95) Prove that $x^4 + x^3 + 1$ is irreducible over $\mathbb{Z}_2$.

(96) List all irreducible polynomials up to degree 3 in $\mathbb{Z}_3$.

(97) Let $\mathbb{K}$ be a field and $p(x) \in \mathbb{K}[x]$ a polynomial of degree m. Prove that $p(x)$ cannot have more than m zeros (counted with multiplicities).

Hint: Use the fact that $\mathbb{K}[x]$ is a factorial ring.

(98) Let R be a ring and $(I_j)_{j \in J}$ be a family of ideals of R. Prove that $\bigcap_{j \in J} I_j$ is also an ideal of R.

(99) Let R be a ring and I an ideal of R. Then $(R/I, +)$ is the factor group of $(R, +)$ over $(I, +)$. Define a multiplication on R/I by

$$(a + I) \cdot (b + I) := (ab) + I.$$

Prove that this operation is well defined, i.e. that

$$a + I = c + I \ \textbf{ and } \ b + I = d + I \qquad \Longrightarrow \qquad (ab) + I = (cd) + I.$$

Furthermore, show that $(R/I, +, \cdot)$ is a ring.

(100) Let $U = \{\overline{0}, \overline{2}, \overline{4}\} \subseteq Z_6$. Show that U is an ideal of $(\mathbb{Z}_6, +, \cdot)$. Is it a subring as well? Does it have a 1-element?