Finite Fields I
Tutorial 1

Group theory and ring theory.

1. Find all the subgroups of $U(\mathbb{Z}_{28})$. For each subgroup, determine its order and index.

2. Prove that if the order of a finite group G is a prime power p^k, then the order of its center $C(G)$ is divisible by p.

3. The ring of *Gaussian integers* is the subring $G = \{a + bi \mid a, b \in \mathbb{Z}\}$ of $\mathbb{C}$. Find the quotient ring $G/\langle 3 - i\rangle$. Is it a field? Is it isomorphic to a ring you already know?

4. What is the least possible size of a maximal ideal of a commutative ring with 2020 elements? Give an example of such a ring and its maximal ideal.

5. Let R be a commutative ring with 1, without nilpotents (i.e. $x^n = 0$ implies $x = 0$) and of prime characteristic p. Prove that the *Frobenius map* $x \mapsto x^p$ is an injective endomorphism. Show that if R is a finite field, it is an automorphism. Does this remain true for infinite fields?

6. Find the gcd of the following polynomials in the ring $\mathbb{Z}_2[x]$:

$$f(x) = x^5 + 2x^4 + 3x^3 + x^2 + 2x + 3 \quad \text{and}$$

$$g(x) = x^6 + 2x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 3.$$

7. Show that if F is a field, $f, g \in F[x]$ are coprime and not simultaneously constant polynomials, then there exist such $u, v \in F[x]$ that $uf + vg = 1$, $\deg(u) < \deg(g)$ and $\deg(v) < \deg(f)$.

8. Show that for a polynomial f of positive degree over a field F, the following are equivalent:
   1) f is irreducible;
   2) the principal ideal (f) is a maximal ideal;
   3) the principal ideal (f) is a prime ideal.

9*. Take a non-square $n \in \mathbb{N}$, an odd prime p, $R_n = \{a + \sqrt{n} \cdot b \mid a, b \in \mathbb{Z}\}$, and $I_p = \{a + \sqrt{n} \cdot b \in R_n \mid p \mid a \wedge p \mid b\}$. Show that I_p is an ideal of R_n and find a necessary and sufficient condition in terms of n and p for R_n/I_p to be a field. Is this field finite, and if so, how many elements does it have?