Exercise Sheet 12

Exercise 12.1. (Eisenstein criterion) Let $P(x) = \sum_{i=0}^{n} c_i x^i$ with $c_i \in \mathbb{Z}$, $c_n \neq 0$ and suppose that a prime p exists such that

- p does not divide c_n,
- p divides all the c_i for $i < n$, and
- p^2 does not divide c_0.

1. Show that the above conditions imply that $P(x)$ is irreducibile over $\mathbb{Z}$. (*Hint:* express $P(x)$ as a product of two polynomials and look at their coefficients modulo p).
2. Let $\mathbb{F}$ be a field. Extend the above result to obtain sufficient conditions for irreducibility of a bivariate polynomial in $\mathbb{F}[X, Y]$.

Exercise 12.2. (Schwartz-Zippel lemma) Let $P(x_1, \ldots, x_n)$ be a nonzero n-variate polynomial of total degree d over $\mathbb{F}_q$.

1. First, suppose that $n = 1$, and $x_1 \in \mathbb{F}_q$ is chosen uniformly at random. How large can the probability $\Pr[P(x_1) = 0]$ be?
2. Now let $n > 1$. Use induction on n to show that, if $x_1, \ldots x_n$ are chosen uniformly at random, $\Pr[P(x_1, \ldots, x_n) = 0] \leq d/q$.

   (*Hint:* Write $P(x_1, \ldots, x_n) = \sum_{i=0}^{d} x_1^i P_i(x_2, \ldots, x_n)$, let j be the largest integer such that P_j is not identically zero and consider the events where $P_j(x_2, \ldots, x_n) = 0$ and $P_j(x_2, \ldots, x_n) \neq 0$.
3. Conclude that P can have at most dq^{n-1} roots.

Exercise 12.3. Consider the ideal in $\mathbb{F}_{q^2}[x, y, z]$ generated by the polynomials $f(x, y, z) := x^q + x - y^{q+1}$ and $g(x, y, z) := y^q + y - z^{q+1}$.

1. Find the number of points $(x, y, z) \in \mathbb{F}_{q^2}^3$ satisfying both equations;
2. Let $q := 4$, and calculate the dimension of the space of polynomials of degree less than n in $F_{q^2}[x, y, z]/(f, g)$;
3. Find the dimension and a lower bound on the minimum distance of the AG-code obtained from this construction.