Exercise Sheet 11

Exercise 11.1. We call *Klein quartic* $\mathcal{K}_4$ the curve defined by the equation $f(x,y) = x^3y + y^3 + x = 0$.

1. Check that $f(x,y)$ is irreducible in any ring $\mathbb{F}_q[x,y]$.
2. Count the number of points on the curves $\mathcal{K}_4(\mathbb{F}_2)$, $\mathcal{K}_4(\mathbb{F}_4)$ and $\mathcal{K}_4(\mathbb{F}_8)$. To construct $\mathbb{F}_8$, you might introduce after justification an element α such that $\alpha^3 + \alpha + 1 = 0$.
3. Show that you can construct $[22, 10, \geq 10]_8$, $[22, 14, \geq 6]_8$ and $[22, 18, \geq 2]_8$ codes. Compare their performance with the best codes you can find on www.codetables.de.

Exercise 11.2. Let $\mathcal{F}_9$ be the *Fermat curve* defined by the equation $f(x,y) = x^9 + y^9 + 1$ over $\mathbb{F}_2$.

1. Show that $f(x,y)$ is irreducible.
2. Check that $\mathbb{F}_8$ is a subfield of $\mathbb{F}_{64}$. Show that the map $\mathbb{F}_8 \to \mathbb{F}_8$, $x \mapsto x^9$ is a bijection. Prove that the map $\mathbb{F}_{64}^\times \to \mathbb{F}_{64}^\times$ $x \mapsto x^9$ is a 9-to-1 map and give its image.
3. Count the numer of points of $\mathcal{F}_9(\mathbb{F}_2)$, $\mathcal{F}_9(\mathbb{F}_8)$ and $\mathcal{F}_9(\mathbb{F}_{64})$. Compare this number to Hasse–Weil's bound : $|\mathcal{F}_9(\mathbb{F}_q) - q + 1| \leq 2g\sqrt{q}$ where $g = \frac{(\deg f - 1)(\deg f - 2)}{2}$.
4. Describe the space $\Gamma_{<m}$ of polynomial functions of degree $< m$ on $\mathcal{F}_9(\mathbb{F}_{64})$ and give its dimension. Show how to construct $[504, 9m - 36, \geq 513 - m]_{64}$-codes.

Exercise 11.3. 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 common roots $(x,y,z) \in \mathbb{F}_{q^2}^3$ of 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. Assume an appropriate constraint on n.

Exercise 11.4. (Schwartz-Zippel lemma) Let $P(x_1, \ldots, x_n)$ be a nonzero n-variate polynomial of total degree d over $\mathbb{F}_q$. We would like to bound the number of roots of P in $\mathbb{F}_q^n$.

1. First, suppose that $n = 1$, and $x_1 \in \mathbb{F}_q$ is chosen uniformly at random. Upper bound the probability $\Pr[P(x_1) = 0]$.
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 11.5. Let $\mathbb{F}_q[x,y]_{<k,<k}$ denote the space of bivariate polynomials over $\mathbb{F}_q$ in which the degree in x and the degree in y are both less than k.

1. Show that if $f \in \mathbb{F}_q[x,y]_{<k,<k}$ vanishes on $I \times I$ for some subset I of $\{1,\ldots,q\}$ of size $\geq k$, then $f = 0$.

2. Consider the code C obtained by evaluating polynomials in $\mathbb{F}_q[x,y]_{<k,<k}$ on all points $(x,y) \in \mathbb{F}_q^2$. What is the dimension of C if $k < q$?

3. Given elements $y_{\alpha,\beta}$, $\alpha,\beta \in \mathbb{F}_q$, show that there exists a nonzero polynomial $Q(x,y,z) \in \mathbb{F}_q[x,y,z]$ of x-degree $< \ell$, of y-degree $< \ell$, and of z-degree $< t$ such that $Q(\alpha,\beta,y_{\alpha,\beta}) = 0$ for all $\alpha,\beta \in \mathbb{F}_q$, provided that $\ell^2 t > q^2$.