Final Exam

Duration: 3 hours

The use of electronic devices or books is not allowed, but you can use the lecture notes of this course.
You may use results from the lecture notes without proof, provided you clearly state which results you use.
Write your name and student ID on each piece of paper you hand in. Please write legibly and give proper justification to your answers.

Exercise 1 – Let \( \mathbb{F}_q \) be a finite field of odd characteristic. Fix three distinct elements \( e_1, e_2, e_3 \in \mathbb{F}_q \). Consider the affine curve \( C_0 \subset \mathbb{A}^2 \) defined over \( \mathbb{F}_q \) given (in the \((x, y)\)-coordinates on \( \mathbb{A}^2 \)) by the equation
\[
C_0 \subset \mathbb{A}^2 : \quad y^2 = (x - e_1)(x - e_2)(x - e_3).
\]

1.1. Give an equation of the projective closure \( C \subset \mathbb{P}^2 \) of \( C_0 \) (in the \([X : Y : Z]\)-coordinates on \( \mathbb{P}^2 \)), list the points at infinity on \( C \) and check that they are \( \mathbb{F}_q \)-rational.

1.2. Check that \( C \) is smooth.

The curve \( C \) has genus 1. Consider the following four \( \mathbb{F}_q \)-rational points on \( C \):
\[
P_0 := [0 : 1 : 0], \quad P_1 := [e_1 : 0 : 1], \quad P_2 := [e_2 : 0 : 1], \quad P_3 := [e_3 : 0 : 1].
\]

1.3. Prove that, for \( i = 1, 2, 3 \), \( \text{div}(x - e_i) = 2P_i - 2P_0 \) and \( \text{div}(y) = P_1 + P_2 + P_3 - 3P_0 \).

1.4. Let \( P \in C(\mathbb{F}_q) \). Using the Riemann-Roch theorem, prove the following assertion: if \( f \in \mathbb{F}_q(C)^\times \) is a rational function satisfying \( \text{div}(f) \geq -P \) then \( f \) is constant.

For each \( i \in \{1, 2, 3\} \), let \( c_i \) be the class in \( \text{Pic}^0(C) \) of the divisor \( D_i := P_i - P_0 \in \text{Div}(C) \).

1.5. Deduce from the two previous questions that, in \( \text{Pic}^0(C) \), one has \( c_i \neq 0 \) and \( 2c_i = 0 \) for \( i = 1, 2, 3 \).

1.6. Show that \( c_1 + c_2 + c_3 = 0 \) in \( \text{Pic}^0(C) \).

Let \( \Gamma \) denote the subgroup of \( \text{Pic}^0(C) \) generated by \( c_1, c_2, c_3 \).

1.7. Deduce from the above questions that \( \Gamma \simeq (\mathbb{Z}/2\mathbb{Z})^3 \).

1.8. Let \( c \in \text{Pic}^0(C) \) be a divisor class such that \( c \neq 0 \) and \( 2c = 0 \). Prove that \( c \in \Gamma \). Hint: \( C \) is an elliptic curve.

Exercise 2 – Let \( \mathbb{F}_q \) be a finite field and let \( C \) be a smooth projective curve of genus \( g = g(C) \) defined over \( \mathbb{F}_q \). We denote by \( \text{Pic}^0(C) \) the group of classes of divisors of degree 0 on \( C \), and we let \( h(C) := \#\text{Pic}^0(C) \).

For all \( f \in \mathbb{F}_q(C)^\times \), we decompose \( \text{div}(f) \in \text{Div}(C) \) as \( \text{div}(f) = \text{div}(f)_0 - \text{div}(f)_\infty \) where both \( \text{div}(f)_0, \text{div}(f)_\infty \) are effective divisors. The degree of \( f \) is then defined to be \( \deg \text{div}(f)_0 = \deg \text{div}(f)_\infty \geq 0 \) (i.e., the degree of \( f \) is the number of zeroes/poles of \( f \) counted with multiplicities).

Recall that the gonality \( \gamma \) of \( C \) is the minimum degree of a nonconstant rational function \( f \in \mathbb{F}_q(C)^\times \).

2.1. Prove that \( \gamma = \min \{ \deg D : D \in \text{Div}(C) \text{ and } \ell(D) \geq 2 \} \).

2.2. If \( g = 0 \), show that \( \gamma = 1 \). In the case that \( g = 1 \), prove that \( \gamma = 2 \).

We now assume that \( g \geq 1 \). Let \( X \) be the set of effective divisors of degree \( 2g \) on \( C \). Recall from the lecture notes that \( \#X = h(C) \cdot (q^{2g+1} - 1)/(q - 1) \).

For any point \( P \in C(\mathbb{F}_q^{2g}) \), we construct a divisor \( D_P \in X \) as follows. Let \( v_P = \{ \sigma(P), \sigma \in \text{Gal}(\mathbb{F}_q^{2g}/\mathbb{F}_q) \} \subset C(\mathbb{F}_q^{2g}) \) be the set of Galois conjugates of \( P \). This set \( v_P \) is an \( \mathbb{F}_q \)-place of \( C \) and we denote its degree by \( \alpha_P = \#v_P \). Then \( \alpha_P \) divides \( 2g \) and we set \( D_P := \#v_P \cdot v_P \in Z \cdot v_P \subset \text{Div}(C) \).

2.3. Explain why \( \alpha_P \) divides \( 2g \), and check that \( D_P \in X \).

2.4. Prove that \( D_P \neq D_Q \) if \( P, Q \in C(\mathbb{F}_q^{2g}) \) are not in the same \( \text{Gal}(\mathbb{F}_q^{2g}/\mathbb{F}_q) \)-orbit.

2.5. Using this construction, prove that \( \#X \geq \frac{\#C(\mathbb{F}_q^{2g})}{2g} \).
2.6. Using the Hasse-Weil bound, deduce that
\[ h(C) \geq \frac{q - 1}{2} - \frac{q^{2g} - 2g \cdot q^g + 1}{g \cdot (q^{g+1} - 1)}, \]

2.7. Fix a finite field \( \mathbb{F}_q \) and a sequence \((C_n)_{n \geq 1}\) of smooth projective curves \( C_n \) over \( \mathbb{F}_q \). Assume that the genus \( g_n = g(C_n) \) of \( C_n \) tends to infinity as \( n \to \infty \). Prove that, as \( n \to \infty \), one has
\[ h(C_n) \geq \frac{q^{2n}}{g_n} \cdot \left( \frac{q - 1}{2q} + \varepsilon_q(g_n) \right), \]
for some function \( \varepsilon_q : \mathbb{R}_{\geq 0} \to \mathbb{R} \) such that \( |\varepsilon_q(x)| \to 0 \) as \( x \to \infty \).

---

**Exercise 3** – Let \( \mathbb{F}_p \) be a prime finite field with \( p \geq 3 \). Let \( C \) be a smooth projective curve of genus \( g \geq 1 \) over \( \mathbb{F}_p \). We denote by \( L(C/\mathbb{F}_p, T) = \sum_{i=0}^{\frac{g}{2}} a_i T^i \in \mathbb{Z}[T] \) the numerator of the zeta function of \( C/\mathbb{F}_p \).

Prove the following assertions:

3.1. For any integer \( n \) such that \( 1 \leq n < p - 1 \), the homogeneous equation \( \sum_{i=0}^{n} x_i^{p-1} = 0 \) has exactly one solution \((x_0, \ldots, x_n) \in (\mathbb{F}_p)^{n+1}\).

3.2. One has \( a_1 = \#C(\mathbb{F}_p) - (p + 1) \).

3.3. One has \( |a_g| \leq \left( \frac{q^{g-1} - 1}{q - 1} \right) \cdot pg/2 \).

3.4. If there is a permutation \( \tau : C(\mathbb{F}_p) \to C(\mathbb{F}_p) \) of order 3 acting without fixed points. Then \( \#C(\mathbb{F}_p) \equiv 0 \mod 3 \).

3.5. If \( \#C(\mathbb{F}_{p^n}) = p^{3n} + 1 \) for all \( m \in \{1, \ldots, M\} \) with \( M \leq g \), then \( a_1 = \cdots = a_M = 0 \).

Here are a list of 4 curves \( C_i \subset \mathbb{P}^2 \) defined over \( \mathbb{F}_1 \) which are smooth projective of genus \( g = 3 \), and a list of 5 polynomials \( L_\alpha \) in \( \mathbb{Z}[T] \). Four of the \( L_\alpha \)'s are actually the \( L \)-functions of one of the \( C_i \)'s.

\[ \begin{align*}
C_1 & : y^4 - x^4 + x^2 z^2 + y z^3 = 0, \quad L_a(T) = 125T^6 - 50T^5 - 5T^4 + 12T^3 - 2T^2 - 2T + 1, \\
C_2 & : x^3 y + y^3 z + z^3 x = 0, \quad L_b(T) = 125T^6 - 150T^5 + 135T^4 - 68T^3 + 27T^2 - 6T + 1, \\
C_3 & : x^4 + y^3 z + y z^3 = 0, \quad L_c(T) = 125T^6 + 150T^5 + 12T^4 + 64T^3 + 25T^2 + 6T + 1, \\
C_4 & : x^4 + y^4 + z^4 = 0, \quad L_d(T) = 125T^6 + 150T^5 + 135T^4 - 235T^3 + 27T^2 - 6T + 1, \\
C_5 & : \quad L_e(T) = 125T^6 + 1.
\end{align*} \]

3.6. Assign to each curve \( C_i \) its \( L \)-function. Explain your argument. *Hint: avoid unnecessary computations.*

Note: \( \sqrt{3} = 2.236206 \ldots, \sqrt{3} = 11.1834 \ldots \) and \((\frac{4}{3}) = 20 \).

---

**Exercise 4** – Let \( q \) be a prime power, and let \( n > 0 \) be a positive integer. Let \( C \) be a curve of genus \( g \) over \( \mathbb{F}_q \), and let \( Q, P_1, P_2, \ldots, P_n \) be distinct \( \mathbb{F}_q \)-rational points of \( C \). For each integer \( r \geq 0 \), we defined the Goppa code \( G_r \) associated with \((C, r \cdot Q)\) in the lecture notes as the image of \( \alpha_r : \mathcal{L}(r \cdot Q) \to \mathbb{F}_q^n ; f \mapsto (f(P_1), f(P_2), \ldots, f(P_n)) \).

4.1. Prove that \( \alpha_r \) is injective if \( r < n \).

4.2. For each integer \( n \), give an example of a prime power \( q \), a curve \( C \) over \( \mathbb{F}_q \), points \( Q, P_1, P_2, \ldots, P_n \), such that \( \alpha_n \) is not injective.

4.3. Prove that there exists an integer \( N \), possibly depending on \( q, g, n \) and/or \( C \), such that for all \( r > N \) the map \( \alpha_r \) is surjective.

4.4. In this question, we take \( q = 3 \) and consider \( C = \mathbb{F}_3 \) over \( \mathbb{F}_3 \). We choose \( Q = (1 : 0), P_1 = (0 : 1), P_2 = (1 : 1) \) and \( P_3 = (2 : 1) \). Compute the dimension, length and minimum distance of the codes \( G_1, G_2 \) and \( G_1 \otimes G_1 \).

4.5. Construct a \([6, 4, 2]\)-code over \( \mathbb{F}_2 \). *Hint: you may start by constructing a \([3, 2, 2]\)-code over \( \mathbb{F}_4 \).*

4.6. Does there exist a \([6, 4, 3]\)-code over \( \mathbb{F}_2 \)?

---

Page 2 of 2