Final Exam

Duration : 3 hours
The use of electronic devices or books is not allowed, but you can use the lecture notes of the 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 $\mathrm{C}_0 \subset \mathbb{A}^2$ defined over $\mathbb{F}_q$ given (in the (x, y)-coordinates on $\mathbb{A}^2$) by the equation

$$\mathrm{C}_0 \subset \mathbb{A}^2 : \qquad y^2 = (x - e_1)(x - e_2)(x - e_3).$$

1.1. Give an equation of the projective closure $\mathrm{C} \subset \mathbb{P}^2$ of C_0 (in the $[\mathrm{X} : \mathrm{Y} : \mathrm{Z}]$-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:

$$\mathrm{P}_0 := [0 : 1 : 0], \quad \mathrm{P}_1 := [e_1 : 0 : 1], \quad \mathrm{P}_2 := [e_2 : 0 : 1], \quad \mathrm{P}_3 := [e_3 : 0 : 1].$$

1.3. Prove that, for $i = 1, 2, 3$, $\mathrm{div}(x - e_i) = 2\mathrm{P}_i - 2\mathrm{P}_0$ and $\mathrm{div}(y) = \mathrm{P}_1 + \mathrm{P}_2 + \mathrm{P}_3 - 3\mathrm{P}_0$.

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

For each $i \in \{1, 2, 3\}$, let c_i be the class in $\mathrm{Pic}^0(\mathrm{C})$ of the divisor $\mathrm{D}_i := \mathrm{P}_i - \mathrm{P}_0 \in \mathrm{Div}(\mathrm{C})$.

1.5. Deduce from the two previous questions that, in $\mathrm{Pic}^0(\mathrm{C})$, 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 $\mathrm{Pic}^0(\mathrm{C})$.

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

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

1.8. Let $c \in \mathrm{Pic}^0(\mathrm{C})$ 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 $g = g(\mathrm{C})$ defined over $\mathbb{F}_q$. We denote by $\mathrm{Pic}^0(\mathrm{C})$ the group of classes of divisors of degree 0 on C, and we let $h(\mathrm{C}) := \#\mathrm{Pic}^0(\mathrm{C})$.

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

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

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

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

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

For any point $\mathrm{P} \in \mathrm{C}(\mathbb{F}_{q^{2g}})$, we construct a divisor $\mathrm{D}_\mathrm{P} \in \mathrm{X}$ as follows. Let $v_\mathrm{P} = \{\sigma(\mathrm{P}),\ \sigma \in \mathrm{Gal}(\mathbb{F}_{q^{2g}}/\mathbb{F}_q)\} \subset \mathrm{C}(\mathbb{F}_{q^{2g}})$ 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 $a_\mathrm{P} = \#v_\mathrm{P}$. Then a_P divides $2g$ and we set $\mathrm{D}_\mathrm{P} := \frac{2g}{a_\mathrm{P}} \cdot v_\mathrm{P} \in \mathbb{Z} \cdot v_\mathrm{P} \subset \mathrm{Div}(\mathrm{C})$.

2.3. Explain why a_P divides $2g$, and check that $\mathrm{D}_\mathrm{P} \in \mathrm{X}$.

2.4. Prove that $\mathrm{D}_\mathrm{P} \neq \mathrm{D}_\mathrm{Q}$ if $\mathrm{P}, \mathrm{Q} \in \mathrm{C}(\mathbb{F}_{q^{2g}})$ are not in the same $\mathrm{Gal}(\mathbb{F}_{q^{2g}}/\mathbb{F}_q)$-orbit.

2.5. Using this construction, prove that $\#\mathrm{X} \geqslant \dfrac{\#\mathrm{C}(\mathbb{F}_{q^{2g}})}{2g}$.

2.6. Using the Hasse-Weil bound, deduce that

$$h(\mathrm{C}) \geqslant \frac{q-1}{2} \cdot \frac{q^{2g} - 2g \cdot q^g + 1}{g \cdot (q^{g+1} - 1)}.$$

2.7. Fix a finite field $\mathbb{F}_q$ and a sequence $(\mathrm{C}_n)_{n \geqslant 1}$ of smooth projective curves C_n over $\mathbb{F}_q$. Assume that the genus $g_n = g(\mathrm{C}_n)$ of C_n tends to infinity as $n \to \infty$. Prove that, as $n \to \infty$, one has

$$h(\mathrm{C}_n) \geqslant \frac{q^{g_n}}{g_n} \cdot \left(\frac{q-1}{2q} + \varepsilon_q(g_n) \right),$$

for some function $\varepsilon_q : \mathbb{R}_{\geqslant 0} \to \mathbb{R}$ such that $|\varepsilon_q(x)| \to 0$ as $x \to \infty$.

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

Prove the following assertions:

3.1. For any integer n such that $1 \leqslant n < p-1$, 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 $a_1 = \#\mathrm{C}(\mathbb{F}_p) - (p+1)$.

3.3. One has $|a_g| \leqslant \binom{2g}{g} \cdot p^{g/2}$.

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

3.5. If $\#\mathrm{C}(\mathbb{F}_{p^m}) = p^m + 1$ for all $m \in \{1, \ldots, \mathrm{M}\}$ with $\mathrm{M} \leqslant g$, then $a_1 = \cdots = a_{\mathrm{M}} = 0$.

Here are a list of 4 curves $\mathrm{C}_i \subset \mathbb{P}^2$ defined over $\mathbb{F}_5$ which are smooth projective of genus $g = 3$, and a list of 5 polynomials L_α in $\mathbb{Z}[\mathrm{T}]$. Four of the L_α's are actually the L-functions of one of the C_i's.

C_1 : $y^4 - x^4 + x^2z^2 + yz^3 = 0$.

C_2 : $x^3y + y^3z + z^3x = 0$.

C_3 : $x^4 + y^3z + yz^3 = 0$

C_4 : $x^4 + y^4 + z^4 = 0$.

$$\mathrm{L}_a(\mathrm{T}) = 125\mathrm{T}^6 - 50\mathrm{T}^5 - 5\mathrm{T}^4 + 12\mathrm{T}^3 - \mathrm{T}^2 - 2\mathrm{T} + 1.$$

$$\mathrm{L}_b(\mathrm{T}) = 125\mathrm{T}^6 - 150\mathrm{T}^5 + 135\mathrm{T}^4 - 68\mathrm{T}^3 + 27\mathrm{T}^2 - 6\mathrm{T} + 1.$$

$$\mathrm{L}_c(\mathrm{T}) = 125\mathrm{T}^6 + 150\mathrm{T}^5 + 125\mathrm{T}^4 + 64\mathrm{T}^3 + 25\mathrm{T}^2 + 6\mathrm{T} + 1.$$

$$\mathrm{L}_d(\mathrm{T}) = 125\mathrm{T}^6 + 150\mathrm{T}^5 + 135\mathrm{T}^4 - 235\mathrm{T}^3 + 27\mathrm{T}^2 - 6\mathrm{T} + 1.$$

$$\mathrm{L}_e(\mathrm{T}) = 125\mathrm{T}^6 + 1.$$

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

Note: $\sqrt{5} = 2.23606...$, $\sqrt{5}^3 = 11.18034...$ *and* $\binom{6}{3} = 20$.

Exercise 4 – Let q be a prime power, and let n be a positive integer. Let C be a curve of genus g over $\mathbb{F}_q$, and let $\mathrm{Q}, \mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_n$ be distinct $\mathbb{F}_q$-rational points of C. For each integer $r \geqslant 0$, we defined the Goppa code G_r associated with $(\mathrm{C}, r \cdot \mathrm{Q})$ in the lecture notes as the image of

$$\alpha_r : \mathcal{L}(r \cdot \mathrm{Q}) \to \mathbb{F}_q^n \colon f \mapsto (f(\mathrm{P}_1), f(\mathrm{P}_2), \ldots, f(\mathrm{P}_n)).$$

4.1. Prove that α_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 $\mathrm{Q}, \mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_n$, such that α_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 $r > \mathrm{N}$ the map α_r is surjective.

4.4. In this question, we take $q = 3$ and consider $\mathrm{C} = \mathbb{P}^1$ over $\mathbb{F}_3$. We choose $\mathrm{Q} = (1:0)$, $\mathrm{P}_1 = (0:1)$, $\mathrm{P}_2 = (1:1)$ and $\mathrm{P}_3 = (2:1)$. Compute the dimension, length and minimum distance of the codes G_1, G_2 and $\mathrm{G}_1 \otimes \mathrm{G}_1$.

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 $\mathbb{F}_2$?
