Retake 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 –

1.1. Let $\phi_3 : \mathbb{F}_3 \to \mathbb{F}_3$, $x \mapsto x^3$. Show that ϕ_3 is a bijection. Let $\phi_7 : \mathbb{F}_7 \to \mathbb{F}_7$, $x \mapsto x^3$. What is $\phi_7(\mathbb{F}_7)$?

Let $\mathrm{C}_0 \colon x^3 + y^3 + 1 = 0$ be a curve in the affine plane $\mathbb{A}^2$ over $\mathbb{F}_7$ with coordinates (x, y).

1.2. 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 $\mathbb{F}_7$-rational points of C.

1.3. Check that C is smooth.

1.4. Compute $\mathrm{div}(x)$ and $\mathrm{div}(y)$.

Let P_1, P_2 and P_3 be the points at infinity ($\mathrm{Z} = 0$) of C. *You may assume that* C *has genus 1.*

1.5. Compute $\dim_{\mathbb{F}_q}(\mathcal{L}(\mathrm{P}_1 + \mathrm{P}_2 + \mathrm{P}_3))$.

1.6. Prove that C has at most 64 points with coordinates in $\mathbb{F}_{49}$.

We now consider the projective closure $\mathrm{D} \subset \mathbb{P}^2$ of the curve $x^3 + y^3 + 1 = 0$ in $\mathbb{A}^2$ over $\mathbb{F}_3$ (with coordinates (x, y)).

1.7. For each finite extension $\mathbb{F}_3 \subset \mathbb{F}_q$ compute the number of $\mathbb{F}_q$-rational points on D.

1.8. Compute the zeta-function of D.

1.9. Does the zeta function of D satisfy the Riemann Hypothesis? Comment on this.

Exercise 2 – Let $p \geqslant 5$ be a prime number and $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ be the finite field with p elements.

2.1. For any integer $n \geqslant 0$, we let $\mathrm{S}_p(n) := \sum_{x \in \mathbb{F}_p} x^n$. Prove that $\mathrm{S}_p(n) = \begin{cases} -1 & \text{if } p-1 \text{ divides } n \\ 0 & \text{otherwise.} \end{cases}$

Let $\mathrm{E} \subset \mathbb{P}^2$ be the projective curve defined over $\mathbb{F}_p$ by the equation $\mathrm{Y}^2\mathrm{Z} = \mathrm{X}^3 + \mathrm{XZ}^2$.

2.2. Check that E is smooth, and prove that E has only one point at infinity, which is $\mathbb{F}_p$-rational.

We denote by $\lambda_p : \mathbb{F}_p \to \mathbb{Z}$ the Legendre symbol modulo p: $\lambda_p(0) = 0$ and, for all $y \in \mathbb{F}_p^\times$, $\lambda_p(y) = +1$ if y is a square in $\mathbb{F}_p^\times$ and $\lambda_p(y) = -1$ otherwise. Recall that $\lambda_p(y) \equiv y^{(p-1)/2} \bmod p$ for all $y \in \mathbb{F}_p$.

2.3. Show that $\#\mathrm{E}(\mathbb{F}_p) = p + 1 + \Sigma_p$ where $\Sigma_p = \sum_{x \in \mathbb{F}_p} \lambda_p(x^3 + x)$.

2.4. Show that $|\Sigma_p| \leqslant 2\sqrt{p} < p$. *You may assume that the curve* E *has genus* 1.

Let $\mathrm{H}_p(x) := (x^3 + x)^{(p-1)/2} \in \mathbb{F}_p[x]$ and write $\mathrm{H}_p(x) = \sum_{n \geqslant 0} \alpha_n \cdot x^n$.

2.5. Prove that $\Sigma_p \equiv \sum_{n \geqslant 0} \alpha_n \cdot \mathrm{S}_p(n) \bmod p$, and deduce that $\Sigma_p \equiv -\alpha_{p-1} \bmod p$.

2.6. Show that $\alpha_{p-1} = 0$ if $p \equiv 3 \bmod 4$.

2.7. We assume that $p \equiv 3 \bmod 4$. Deduce from the previous questions that $\#\mathrm{E}(\mathbb{F}_p) = p + 1$, and give an expression of the L-function of $\mathrm{E}/\mathbb{F}_p$.

2.8. We now assume that $p \equiv 1 \bmod 4$. *Recall that -1 is then a square modulo p.*

Let $\Gamma \subset \mathrm{E}(\mathbb{F}_p)$ denote the subgroup of 2-torsion points in $\mathrm{E}(\mathbb{F}_p)$. Show that $\#\Gamma = 4$.

2.9. Deduce that $\#\mathrm{E}(\mathbb{F}_p) \equiv 0 \bmod 4$ in both cases ($p \equiv 1$ or $3 \bmod 4$).

Exercise 3 – 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 $\mathrm{P}_1, \ldots, \mathrm{P}_n$ be distinct $\mathbb{F}_q$-rational points on C. For each divisor D, we defined the Goppa code G_D associated with (C, D) in the lecture notes as the image of

$$\alpha_\mathrm{D} : \mathcal{L}(\mathrm{D}) \to \mathbb{F}_q^n \colon f \mapsto (f(\mathrm{P}_1), \ldots, f(\mathrm{P}_n)).$$

In the lecture notes we proved that α_D is injective if $\deg(\mathrm{D}) \leqslant n-1$ and $\mathrm{P}_1, \ldots, \mathrm{P}_n$ are not in the support of D.

3.1. Give an example of a curve C, points $\mathrm{P}_1, \ldots, \mathrm{P}_n$ and a divisor D of degree at most $n-1$, such that α_D is not injective.

Let Q be an $\mathbb{F}_q$-rational point of C different from $\mathrm{P}_1, \ldots, \mathrm{P}_n$. Let g be a function on C with a simple zero at Q. For each integer k, let

$$\beta_k : \mathcal{L}(k \cdot \mathrm{Q}) \to \mathbb{F}_q^{n+1} \colon f \mapsto (f(\mathrm{P}_1), \ldots, f(\mathrm{P}_n), (g^k \cdot f)(\mathrm{Q})).$$

3.2. Prove that the map β_k is well-defined.

3.3. Prove that β_n is injective.

3.4. Prove that the minimum distance of the code $\mathrm{Im}(\beta_k)$ is at least $n+1-k$.

Let $\mathrm{A} = \{(x_1, x_2, x_3) \in \mathbb{F}_q^3 : x_1 + x_2 + x_3 = 0\}$ be the generalised parity bit code in $\mathbb{F}_q^3$.

3.5. Compute the dimension, length and minimum distance of $\mathrm{A}^\vee \otimes \mathrm{A}^\vee$ and $\mathrm{A} \otimes \mathrm{A}$.

3.6. Does there exist an $[5, 3, 3]$-code over $\mathbb{F}_3$?

Exercise 4 – Here are a list of 5 curves $\mathrm{C}_i \subset \mathbb{P}^2$ defined over $\mathbb{F}_7$ which are all smooth and projective, and a list of 5 polynomials L_α in $\mathbb{Z}[\mathrm{T}]$. Each L_α is actually the L-function of one of the C_i's.

C_1 :	$x^4 - z^4 + xy^3 + 2x^2z^2 = 0.$	$\mathrm{L}_a(\mathrm{T}) = (7\mathrm{T}^2+1)^2(7\mathrm{T}^2+4\mathrm{T}+1).$
C_2 :	$3x^4 + x^2yz + y^3z + yz^3 = 0.$	$\mathrm{L}_b(\mathrm{T}) = (49\mathrm{T}^4+1)(7\mathrm{T}^2-2\mathrm{T}+1).$
C_3 :	$x^4 + z^4 + 3y^3z + y^2z^2 + 3yz^3 = 0.$	$\mathrm{L}_c(\mathrm{T}) = (7\mathrm{T}^2+1)(7\mathrm{T}^2-4\mathrm{T}+1)(7\mathrm{T}^2+2\mathrm{T}+1).$
C_4 :	$x^4 + z^4 + 3y^3z + y^2z^2 + yz^3 = 0.$	$\mathrm{L}_d(\mathrm{T}) = (7\mathrm{T}^2+1)^2(7\mathrm{T}^2-4\mathrm{T}+1).$
C_5 :	$x^4 + z^4 + y^3z + y^2z^2 + yz^3 = 0.$	$\mathrm{L}_e(\mathrm{T}) = (7\mathrm{T}^2-\mathrm{T}+1)(7\mathrm{T}^2+\mathrm{T}+1)(7\mathrm{T}^2+4\mathrm{T}+1).$

4.1. Tabulate the values of $x \in \mathbb{F}_7 \mapsto x^4 + 1 \in \mathbb{F}_7$.

We give the following table:

$y \in \mathbb{F}_7$	0	1	2	3	4	5	6
$3y^3 + y^2 + 3y$	0	0	6	1	3	2	2
$3y^3 + y^2 + y$	0	5	2	2	2	6	4
$y^3 + y^2 + y$	0	3	0	4	0	1	6

4.2. Deduce the number of $\mathbb{F}_7$-rational points on C_3, C_4 and C_5.

4.3. Explain the link between $\#\mathrm{C}_i(\mathbb{F}_7)$ and the coefficient of T in the L-function of $\mathrm{C}_i/\mathbb{F}_7$.

4.4. Explain the link between $\#\mathrm{Pic}^0(\mathrm{C}_i)$ and a value of the L-function of $\mathrm{C}_i/\mathbb{F}_7$.

We give the following information: $\#\mathrm{Pic}^0(\mathrm{C}_1) = 2^2 \cdot 3^3 \cdot 7$, $\#\mathrm{Pic}^0(\mathrm{C}_3) = 2^2 \cdot 3 \cdot 5^2$.

4.5. Assign to each curve C_i its L-function. Explain your argument. *Avoid unnecessary computations.*
