Homework #1

Choose three exercises among the following four.

Exercise 1 – Let $\mathrm{C}/\mathbb{F}_q$ be a smooth projective curve defined over $\mathbb{F}_q$. As such, C is also defined over any finite extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ (because one can see the equations $f_a \in \mathbb{F}_q[\mathrm{X}]$ defining C as equations with coefficients in $\mathbb{F}_{q^m}$). In this exercise, we study the relation between the zeta functions of $\mathrm{C}/\mathbb{F}_q$ and $\mathrm{C}/\mathbb{F}_{q^m}$.

1.1. We denote by $\mathrm{Fr}_q : \mathrm{C} \to \mathrm{C}$ the Frobenius morphism. Let v be a $\mathbb{F}_q$-place of C, and $\mathrm{P} \in v$. Prove that $v = \left\{\mathrm{Fr}_q^j(\mathrm{P}),\ j = 0, 1, 2, \dots\right\}$, and that $\deg(v)$ is the least positive integer j such that $\mathrm{Fr}_q^j(\mathrm{P}) = \mathrm{P}$.

1.2. Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be an extension of degree $m \geqslant 1$, and let v be a $\mathbb{F}_q$-place of C of degree $d \geqslant 1$. Prove that v splits into $r = \gcd(d, m)$ places of C over $\mathbb{F}_{q^m}$ of degree $d/\gcd(d, m)$: that is to say,

$$v = w_1 \sqcup \dots \sqcup w_r, \text{ where } w_i \text{ are } \mathbb{F}_{q^m}\text{-places of C of degree } \deg w_i = d/\gcd(d, m).$$

1.3. For any integers $m, d \geqslant 1$, prove the identity:

$$\left(1 - \mathrm{T}^{md/\gcd(d,m)}\right)^{\gcd(d,m)} = \prod_{\zeta^m = 1} \left(1 - (\zeta\mathrm{T})^d\right),$$

where the product is over the m-th roots of unity in $\mathbb{C}$. (Hint: remember that $1 - \mathrm{T}^m = \prod_{\zeta^m=1}(1 - \zeta\mathrm{T})$.)

1.4. Deduce the relation:

$$\mathrm{Z}(\mathrm{C}/\mathbb{F}_{q^m}, \mathrm{T}^m) = \prod_{\zeta^m=1} \mathrm{Z}(\mathrm{C}/\mathbb{F}_q, \zeta\mathrm{T}).$$

Hint: in the Euler product $\prod_w \left(1 - \mathrm{T}^{\deg w}\right)^{-1}$ over all $\mathbb{F}_{q^m}$-places of C defining $\mathrm{Z}(\mathrm{C}/\mathbb{F}_{q^m}, \mathrm{T})$, you may want to regroup the w's "coming from" a given $\mathbb{F}_q$-place v of C (by *Q.1.2)*.

Exercise 2 – Let $k = \mathbb{F}_q$ be a finite field. Consider the projective variety $\mathrm{X}/\mathbb{F}_q$ defined by the equation

$$\mathrm{X} \subset \mathbb{P}^2 : \qquad zy^q + z^q y - x^{q+1} = 0.$$

2.1. Show that X is a smooth projective curve, and that it has only one point at infinity (that is, $\#(\mathrm{X} \cap \{z = 0\}) = 1$). Give an equation for the "affine part" $\mathrm{Y} = \mathrm{X} \cap \{z = 1\} \subset \mathbb{A}^2$.

2.2. Using that $z \in \overline{\mathbb{F}_q}$ is an element of $\mathbb{F}_q$ if and only if $z^q = z$, prove that $\#\mathrm{Y}(\mathbb{F}_q) = q$ and deduce that $\#\mathrm{X}(\mathbb{F}_q) = q+1$. (Hint: how many squares and non-squares are there in $\mathbb{F}_q^\times$?)

We next prove that $\#\mathrm{X}(\mathbb{F}_{q^2}) = q^3 + 1$.

2.3. Show that the trace $\mathrm{T} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ ($y \mapsto y^q + y$) is a surjective $\mathbb{F}_q$-linear map, and that the norm $\mathrm{N} : \mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times$ ($x \mapsto x^{q+1}$) is a surjective group homomorphism

2.4. Prove that $\#\left\{(x, y) \in \mathrm{Y}(\mathbb{F}_{q^2}) \mid x = 0\right\} = q$ and that, for all $t \in \mathbb{F}_q^\times$,

$$\#\left\{(x, y) \in \mathrm{Y}(\mathbb{F}_{q^2}) \mid x^{q+1} = t = y^q + y\right\} = q(q + 1).$$

2.5. Conclude that $\#\mathrm{Y}(\mathbb{F}_{q^2}) = q^3$ and that $\mathrm{X}(\mathbb{F}_{q^2}) = q^3 + 1$.

Exercise 3 – Let $\mathbb{F}_q$ be a finite field and consider the affine line $\mathbb{A}^1$ over $\mathbb{F}_q$.

3.1. For any integer $d \geqslant 1$, show that there is a bijection between $\mathbb{F}_q$-places of $\mathbb{A}^1$ of degree d and the monic irreducible polynomials in $\mathbb{F}_q[\mathrm{X}]$ of degree d.

3.2. By a direct point-count (*i.e.* by computing $\#\mathbb{A}^1(\mathbb{F}_{q^m})$), prove that $\mathrm{Z}(\mathbb{A}^1/\mathbb{F}_q, \mathrm{T}) = (1 - q\mathrm{T})^{-1}$.

3.3. Let Ir_d be the number of monic irreducible polynomials of degree d in $\mathbb{F}_q[\mathrm{X}]$. With the help of your computation of the zeta function, prove that

$$\forall m \geqslant 1, \qquad q^m = \sum_{d|m} d \cdot \mathrm{Ir}_d \qquad \text{and that} \qquad \forall d \geqslant 1, \qquad \mathrm{Ir}_d = \frac{1}{d} \sum_{e|d} \mu(d/e) q^e,$$

where μ denotes the Möbius function on integers.

3.4. Conclude that, for $d \geqslant 1$,

$$\mathrm{Ir}_d = \frac{q^d}{d} + \mathrm{O}(q^{d/2}), \qquad (\text{as } d \to \infty)$$

where the implicit constant depends only on q. Comment on why this result is called the "prime number theorem for $\mathbb{F}_q[\mathrm{X}]$".

Exercise 4 – Let p be a prime number and $\zeta := \exp(2i\pi/p) \in \mathbb{C}$.

4.1. We identify elements of $\mathbb{F}_p$ with the set $\{0, 1, \ldots, p-1\}$. Let $v \in \mathbb{F}_p$. Show that

$$\sum_{u \in \mathbb{F}_p} \zeta^{u \cdot v} = \begin{cases} p & \text{if } v = 0, \\ 0 & \text{otherwise.} \end{cases}$$

4.2. Given a nonzero homogeneous polynomial $\mathrm{F}(x, y, z) \in \mathbb{F}_p[x, y, z]$, let $\mathrm{N}_p(\mathrm{F})$ be the number of solutions $(x, y, z) \in (\mathbb{F}_p)^3$ to the equation $\mathrm{F}(x, y, z) = 0$. Prove that $\mathrm{N}_p(\mathrm{F})$ is given by the exponential sum

$$\mathrm{N}_p(\mathrm{F}) = p^2 + \frac{1}{p} \sum_{u \in \mathbb{F}_p^\times} \sum_{(x,y,z) \in \mathbb{F}_p^3} \zeta^{u \cdot \mathrm{F}(x,y,z)}.$$

4.3. The polynomial F defines a projective algebraic set $\mathrm{C} \subset \mathbb{P}^2$ over $\mathbb{F}_p$ (meaning that C is given by the equation $\mathrm{F}(x, y, z) = 0$). From the previous question, deduce an expression of $\#\mathrm{C}(\mathbb{F}_p)$ in terms of exponential sums.

4.4. Specialize to the case where F is diagonal: $\mathrm{F} = \mathrm{F}_r(x, y, z) = x^r + y^r + z^r \in \mathbb{F}_p[x, y, z]$ for some integer $r \geqslant 1$. In which case, we denote by $\mathrm{C}_r \subset \mathbb{P}^2$ the projective algebraic set associated to F_r (called the Fermat curve of degree r over $\mathbb{F}_p$). Prove that C_r is a smooth projective curve over $\mathbb{F}_p$ if r is prime to p.

4.5. Use the previous point-counts to prove that

$$\mathrm{N}_p(\mathrm{F}_r) = p^2 + \frac{1}{p} \sum_{u \in \mathbb{F}_p^\times} \left(\sum_{x \in \mathbb{F}_p} \zeta^{u \cdot x^r} \right)^3,$$

and to express $\#\mathrm{C}_r(\mathbb{F}_p)$ with exponential sums.

4.6. For any $y \in \mathbb{F}_p$, let $b_r(y)$ be the number of solutions of the equation $y = x^r$ (in the unknown $x \in \mathbb{F}_p$). Prove that

$$\forall u \in \mathbb{F}_p^\times, \qquad \sum_{x \in \mathbb{F}_p} \zeta^{u \cdot x^r} = \sum_{y \in \mathbb{F}_p} b_r(y) \cdot \zeta^{u \cdot y},$$

and give a sufficient condition (relating $r \geqslant 1$ to p) for the map $y \mapsto b_r(y)$ to be constant on $\mathbb{F}_p$.

4.7. Conclude that, for any $r \geqslant 1$ coprime to $p - 1$, one has $\#\mathrm{C}_r(\mathbb{F}_p) = p + 1$.
