HOMEWORK #3

Conventions – Let $\mathbb{F}_q$ be a finite field. For any smooth projective curve C defined over $\mathbb{F}_q$, we let $\mathrm{L}(\mathrm{C}/\mathrm{F}_q, \mathrm{T})$ be the numerator of the zeta function $\mathrm{Z}(\mathrm{C}/\mathbb{F}_q, \mathrm{T})$ of $\mathrm{C}/\mathbb{F}_q$. We denote by g the genus of C, and by $\alpha_1, \ldots, \alpha_{2g}$ the inverse roots of $\mathrm{L}(\mathrm{C}/\mathbb{F}_q, \mathrm{T})$, so that:

$$\mathrm{L}(\mathrm{C}/\mathbb{F}_q, \mathrm{T}) = \prod_{i=1}^{2g} (1 - \alpha_i \cdot \mathrm{T}) \in \mathbb{Z}[\mathrm{T}].$$

We assume that the α_j's are numbered in such a way that $\mathrm{Im}(\alpha_j) \geqslant 0$ and $\alpha_j \cdot \alpha_{j+g} = q$ for all $j = 1, \ldots, g$. The set $\{\alpha_1, \ldots, \alpha_{2g}\}$ thus numbered (with multiplicities allowed) will be called the set of *Frobenius eigenvalues of* C.

By Weil's theorem, we may pick angles $\theta_j \in [0, \pi]$ such that $\alpha_j = \sqrt{q} \cdot \mathrm{e}^{i\theta_j}$ for all $j = 1, \ldots, g$. The set $\{\theta_1, \ldots, \theta_g\}$ (with multiplicities allowed) is called the set of *Frobenius angles of* C.

Exercise 1 – Let $\mathbb{F}_q$ be a finite field and C be a smooth projective curve of genus $g \geqslant 1$ defined over $\mathbb{F}_q$. Denote by $\{\alpha_1, \ldots, \alpha_{2g}\}$ the set of Frobenius eigenvalues of C.

Let us assume that there exists an angle $\theta \in [0, \pi/2)$ such that $\alpha_j = \sqrt{q} \cdot \mathrm{e}^{i\theta}$ for all $j = 1, \ldots, g$.

1.1. Put $t = \sqrt{q} \cdot \mathrm{e}^{i\theta} + \sqrt{q} \cdot \mathrm{e}^{-i\theta}$. Prove that $t > 0$ and that t is an integer.

1.2. Using a relation between $\#\mathrm{C}(\mathbb{F}_q) \geqslant 0$ and t, prove that $g \leqslant q + 1$.

Now consider the Hermitian curve $\mathrm{X}/\mathbb{F}_q$ defined by

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

In Homework #1 (Exercise 2), we have proved that X is a smooth curve, and that $\#\mathrm{X}(\mathbb{F}_q) = q + 1$, $\#\mathrm{X}(\mathbb{F}_{q^2}) = q^3 + 1$.

1.3. Compare $\#\mathrm{X}(\mathbb{F}_{q^2})$ to the Hasse-Weil bound.

Hint: you may use without proof that a smooth projective curve $\mathrm{X} \subset \mathbb{P}^2$ *defined by a single homogeneous equation* $\mathrm{F}(x, y, z) \in \mathbb{F}_q[x, y, z]$ *of degree d has genus* $g = (d-1)(d-2)/2$.

1.4. With as little computation as possible, prove that

$$\mathrm{Z}(\mathrm{X}/\mathbb{F}_q, \mathrm{T}) = \frac{(1 + q \cdot \mathrm{T}^2)^{\frac{q(q-1)}{2}}}{(1 - \mathrm{T})(1 - q\mathrm{T})}.$$

1.5. Can the result of *1.2* be extended to $\theta = \pi/2$?

Exercise 2 – Let $\mathrm{S} \subset [0, \pi]$ be a nonempty finite set of "angles". In this exercise, we prove that there exists an explicit constant $\mathrm{B_S} > 0$ (depending only on S and q) such that: a smooth projective curve $\mathrm{C}/\mathbb{F}_q$ whose Frobenius angles are all in S has genus $g \leqslant \mathrm{B_S}$.

Let $\mathrm{C}/\mathbb{F}_q$ be a smooth projective curve of genus g over $\mathbb{F}_q$, and $\{\theta_1, \ldots, \theta_g\}$ be its set of Frobenius angles.

2.1. Let $\mathrm{G}(x) = \sum_{k \geqslant 1} a_k x^k \in \mathbb{R}[x]$ be a polynomial with $\mathrm{G}(0) = 0$. Show the following variant of the explicit formula:

$$\sum_{k \geqslant 1} \frac{a_k \cdot \#\mathrm{C}(\mathbb{F}_{q^k})}{q^{k/2}} = \mathrm{G}(q^{1/2}) + \mathrm{G}(q^{-1/2}) - 2 \sum_{j=1}^{g} \mathrm{Re}(\mathrm{G}(\mathrm{e}^{i\theta_j})).$$

We say that a polynomial $\mathrm{G}(x) \in \mathbb{R}[x]$ is S-positive if

(H1) the coefficients of $\mathrm{G}(x)$ are nonnegative, (H2) $\mathrm{G}(0) = 0$, (H3) $\mathrm{Re}(\mathrm{G}(\mathrm{e}^{i\theta})) \geqslant 1$ for all $\theta \in \mathrm{S}$.

2.2. We assume that all the Frobenius angles of C are in S (*i.e.* that $\theta_j \in \mathrm{S}$ for all $j = 1, \ldots, g$). Prove that, for all S-positive polynomials $\mathrm{G} \in \mathbb{R}[x]$, one has:

$$g \leqslant \frac{1}{2} \cdot \left(\mathrm{G}(q^{1/2}) + \mathrm{G}(q^{-1/2})\right).$$

2.3. If $\mathrm{S} = \{0\}$, find a S-positive polynomial, and deduce that $g \leqslant \left(q^{1/2} + q^{-1/2}\right)/2$.

To any angle $\phi \in (0, \pi]$, we associate a polynomial $\mathrm{H}_\phi(x) \in \mathbb{R}[x]$, as follows. For $\phi = \pi$, put $\mathrm{H}_\phi(x) := 1 + x$. For any $\phi \in (0, \pi)$, choose an integer $m \geqslant 1$ such that $\cos(m\phi) \leqslant 0$, and put $\mathrm{H}_\phi(x) := 1 - 2\cos(m\phi) \cdot x^m + x^{2m}$.

2.4. Check that, for any $\phi \in (0, \pi]$, the polynomial $\mathrm{H}_\phi(x) \in \mathbb{R}[x]$ has nonnegative coefficients and satisfies: $\mathrm{H}_\phi(0) = 1$, $\mathrm{H}_\phi(\mathrm{e}^{i\phi}) = 0$, and $\mathrm{H}_\phi(1) \geqslant 2$.

For a nonempty finite set $\mathrm{S} \neq \{0\}$, define $\mathrm{K_S}(x) := \prod_{\theta \in \mathrm{S} \smallsetminus \{0\}} \mathrm{H}_\theta(x) \in \mathbb{R}[x]$, and $\mathrm{G_S}(x) := (\mathrm{K_S}(x) - 1)^2 \in \mathbb{R}[x]$.

2.5. Check that $\mathrm{K_S}(x)$ has nonnegative coefficients, and prove that $\forall z > 0$, one has $1 \leqslant \mathrm{K_S}(z) \leqslant (1+z)^{\deg \mathrm{K_S}}$.

2.6. Prove that $\mathrm{G_S}(x)$ is S-positive. Check that $\mathrm{G_S}(z) \leqslant (1+z)^{2\deg \mathrm{K_S}}$ for all $z > 0$, and deduce that

$$\mathrm{G_S}(q^{1/2}) + \mathrm{G_S}(q^{-1/2}) \leqslant (\sqrt{q}+1)^{2\deg \mathrm{K_S}} \cdot (1 + q^{-\deg \mathrm{K_S}}).$$

2.7. Let $\mathrm{S} \subset [0, \pi]$ be an nonempty finite set of angles, and put

$$\mathrm{B_S} := \begin{cases} \left(q^{1/2} + q^{-1/2}\right)/2 & \text{if } \mathrm{S} = \{0\}, \\ (\sqrt{q}+1)^{2\deg \mathrm{K_S}} \cdot (1 + q^{-\deg \mathrm{K_S}})/2 & \text{otherwise.} \end{cases}$$

Conclude that the following assertion is true: *A smooth projective curve* C *over* $\mathbb{F}_q$*, all of whose Frobenius angles lie in* S*, has genus* $g \leqslant \mathrm{B_S}$.

2.8. Bonus question: give an upper bound for $\deg \mathrm{K_S}$, in terms of the angles $\theta \in \mathrm{S}$.

Exercise 3 – First, we work with the projective plane $\mathbb{P}^2$ over $\mathbb{F}_2$. A *line* in $\mathbb{P}^2$ is a curve $\mathrm{L} \subset \mathbb{P}^2$ defined by a homogeneous polynomial $\mathrm{F}(x,y,z) \in \mathbb{F}_2[x,y,z]$ of degree 1.

3.1. List all points $\mathrm{P} \in \mathbb{P}^2(\mathbb{F}_2)$, and give a list $\mathcal{L}$ of all lines $\mathrm{L} \subset \mathbb{P}^2$. Compare $\#\mathbb{P}^2(\mathbb{F}_2)$ to the number of lines $\#\mathcal{L}$.

3.2. Form a blank array B_0 whose rows are indexed by $\mathrm{P} \in \mathbb{P}^2(\mathbb{F}_2)$ and whose columns indexed by $\mathrm{L} \in \mathcal{L}$. For a point P and a line L, shade the cell (P, L) if $\mathrm{P} \in \mathrm{L}$.

What do you notice about the resulting array B? Give a geometric interpretation.

Now, consider the *Klein quartic* $\mathrm{K} \subset \mathbb{P}^2$ defined over $\mathbb{F}_2$ by

$$\mathrm{K} \subset \mathbb{P}^2 \quad : \qquad x^3y + y^3z + z^3x = 0.$$

3.3. Check that $\mathrm{K}/\mathbb{F}_2$ is a smooth projective curve, and give its genus (*you may use the Hint in 1.3*).

3.4. Prove that K has 2 points at infinity, which are $\mathbb{F}_2$-rational (*i.e.* solve equations for $\mathrm{K} \cap \{z = 0\}$). Give the equation $f(x,y) \in \mathbb{F}_2[x,y]$ for the "affine part" of K (*i.e.* $\mathrm{K} \cap \{z = 1\}$ has equation $f(x,y) = 0 \subset \mathbb{A}^2$).

3.5. Let $\alpha \in \mathbb{F}_8$ be an element such that $\alpha^3 + \alpha + 1 = 0$: the field $\mathbb{F}_8$ is generated by α over $\mathbb{F}_2$.

Prove that $\#\mathrm{K}(\mathbb{F}_8) = 24$, and compare $\#\mathrm{K}(\mathbb{F}_8)$ to the Serre bound.

3.6. Deduce, as simply as possible, that

$$\mathrm{Z}(\mathrm{K}/\mathbb{F}_2, \mathrm{T}) = \frac{1 + 5\mathrm{T}^3 + 8\mathrm{T}^6}{(1-\mathrm{T})(1-2\mathrm{T})}.$$

Hint: if you think you need these numbers, you may use that:

$$\#\mathrm{K}(\mathbb{F}_2) = 3,\ \#\mathrm{K}(\mathbb{F}_4) = 5,\ \#\mathrm{K}(\mathbb{F}_{16}) = 17,\ \#\mathrm{K}(\mathbb{F}_{32}) = 33,\ \#\mathrm{K}(\mathbb{F}_{64}) = 38,\ \ldots$$

3.7. Let $f(x,y) \in \mathbb{F}_2[x,y]$ and $\alpha \in \mathbb{F}_8$ be as above. Form a 7×7 blank array C_0, whose cells are indexed by $(i,j) \in \{0, \ldots, 6\}^2$. For all $(i,j) \in \{0, \ldots, 6\}^2$, shade the (i,j)-th cell in C_0 if $f(\alpha^i, \alpha^j) = 0$. Denote by C the resulting array.

Compare the number of shaded cells to $\#\mathrm{K}(\mathbb{F}_8)$. Compare the properties of B and C. Comment.
