Homework #2

Notations: if $\mathrm{C}/\mathbb{F}_q$ is a smooth projective curve over $\mathbb{F}_q$, and if $f \in \mathbb{F}_q(\mathrm{C})^\times$ is a nonzero rational function on C, we decompose $\mathrm{div}(f) \in \mathrm{Div}(\mathrm{C})$ in two parts:

$$\mathrm{div}(f) = \sum_{v \in |\mathrm{C}|} \mathrm{ord}_v f \cdot v = \underbrace{\sum_{\substack{v \in |\mathrm{C}| \\ \mathrm{ord}_v(f) > 0}} \mathrm{ord}_v f \cdot v}_{:= \mathrm{div}(f)_0} - \underbrace{\sum_{\substack{v \in |\mathrm{C}| \\ \mathrm{ord}_v(f) < 0}} (-\mathrm{ord}_v f) \cdot v}_{:= \mathrm{div}(f)_\infty}.$$

The first part $\mathrm{div}(f)_0$ (resp. the second one $\mathrm{div}(f)_\infty$) is called the divisor of zeros (resp. the divisor of poles) of f. Note that $\mathrm{div}(f)_0$ and $\mathrm{div}(f)_\infty$ are effective divisors, and that $\deg \mathrm{div}(f)_0 = \deg \mathrm{div}(f)_\infty$ (since $\deg \mathrm{div}(f) = 0$).

As usual, we identify an $\mathbb{F}_q$-rational point on C and the $\mathbb{F}_q$-place of C of degree 1 it defines.

Exercise 1 – Let $\mathbb{F}_q$ be a finite field and C be a smooth projective curve of genus g defined over $\mathbb{F}_q$. We denote by $\mathrm{L}(\mathrm{C}/\mathrm{F}_q, \mathrm{T}) \in \mathbb{Z}[\mathrm{T}]$ the numerator of the zeta function $\mathrm{Z}(\mathrm{C}/\mathbb{F}_q, \mathrm{T})$ of $\mathrm{C}/\mathbb{F}_q$. Since $\mathrm{L}(\mathrm{C}/\mathbb{F}_q, 0) = 1$, we can write $\mathrm{L}(\mathrm{C}/\mathbb{F}_q, \mathrm{T})$ in the form:

$$\mathrm{L}(\mathrm{C}/\mathbb{F}_q, \mathrm{T}) = \prod_{i=1}^{2g} (1 - \alpha_i \cdot \mathrm{T}) \text{ for some nonzero complex numbers } \alpha_i.$$

1.1. Expand $\frac{\mathrm{d}}{\mathrm{dT}} \log \mathrm{L}(\mathrm{C}/\mathbb{F}_q, \mathrm{T})$ as a power series in T, and prove that

$$\forall s \geqslant 1, \qquad \#\mathrm{C}(\mathbb{F}_{q^s}) = q^s + 1 - \sum_{i=1}^{2g} \alpha_i^s.$$

Hint: compute the (formal) derivative of $\log \mathrm{Z}(\mathrm{C}/\mathbb{F}_q, \mathrm{T})$ *in two different ways, and identify coefficients.*

1.2. Prove that the radius of convergence of the formal $\frac{\mathrm{d}}{\mathrm{dT}} \log \mathrm{L}(\mathrm{C}/\mathbb{F}_q, \mathrm{T})$ is $\rho = \min_i |\alpha_i|^{-1}$.

1.3. Prove that the set $\{\alpha_i\}_{1 \leqslant i \leqslant 2g}$ is stable under the map $\alpha \mapsto q/\alpha$.

Hint: use the functional equation satisfied by $\mathrm{L}(\mathrm{C}/\mathbb{F}_q, \mathrm{T})$.

1.4. Prove that the following two assertions are equivalent:

(i) For all $i \in \{1, 2, ..., 2g\}$, $|\alpha_i| = \sqrt{q}$,

(ii) Let $m \in \mathbb{Z}_{\geqslant 1}$, there exists a constant $\gamma_m > 0$ such that, for all sufficiently large $n \geqslant 1$,

$$\left| \#\mathrm{C}(\mathbb{F}_{q^{2nm}}) - q^{2nm} - 1 \right| \leqslant \gamma_m \cdot q^{nm}.$$

Exercise 2 – Let $\mathbb{F}_q$ be a finite field, and C be a smooth projective curve over $\mathbb{F}_q$, whose genus is denoted by g. We assume that q is a square, say $q = q_0^2$, and that $q > (g+1)^4$. Under these two hypotheses, the goal of this exercise is to prove that

$$\#\mathrm{C}(\mathbb{F}_q) < q + 1 + (2g+1) \cdot \sqrt{q}. \qquad (1)$$

We assume that C has a $\mathbb{F}_q$-rational point $\mathrm{Q} \in \mathrm{C}(\mathbb{F}_q)$ (otherwise, (1) is trivial). Let $m, n \in \mathbb{Z}_{\geqslant 1}$ be two integers. We define

$$\mathrm{J} := \left\{ j \in [0, m] \cap \mathbb{Z} \ : \ \exists u_j \in \mathbb{F}_q(\mathrm{C})^\times, \ \mathrm{div}(u_j)_\infty = j \cdot \mathrm{Q} \right\}.$$

For each $j \in \mathrm{J}$, we choose such a function $u_j \in \mathbb{F}_q(\mathrm{C})^\times$.

2.1. Prove that the set $\{u_j, \ j \in \mathrm{J}\}$ forms a basis of the Riemann-Roch space $\mathcal{L}(m \cdot \mathrm{Q})$.

Now, consider the $\mathbb{F}_q$-vector space $\mathcal{H} \subset \mathbb{F}_q(\mathrm{C})$ spanned by all products $u \cdot v^{q_0}$, where $u \in \mathcal{L}(m \cdot \mathrm{Q})$ and $v \in \mathcal{L}(n \cdot \mathrm{Q})$. That is to say,

$$\mathcal{H} = \mathcal{L}(m \cdot \mathrm{Q}) \cdot \mathcal{L}(n \cdot \mathrm{Q})^{q_0} = \left\{ \sum_{j \in \mathrm{J}} u_j \cdot v_j^{q_0}, \ v_j \in \mathcal{L}(n \cdot \mathrm{Q}) \right\} \subset \mathbb{F}_q(\mathrm{C}).$$

2.2. Prove that $\mathcal{H}$ is an $\mathbb{F}_q$-subvector space of $\mathcal{L}((m+nq_0)\cdot \mathrm{Q})$.

2.3. If $m < q_0$, prove that any $f \in \mathcal{H}$ can be written uniquely in the form

$$f = \sum_{j\in \mathrm{J}} u_j \cdot v_j^{q_0} \qquad \text{with } v_j \in \mathcal{L}(n\cdot \mathrm{Q}).$$

2.4. Deduce from the previous questions that, if $m < q_0$, one has $\#\mathrm{J} = \ell(m\cdot \mathrm{Q})$ and $\dim \mathcal{H} = \ell(m\cdot \mathrm{Q})\cdot \ell(n\cdot \mathrm{Q})$.

Let us define a map

$$\Phi : \mathcal{H} \to \mathcal{L}((q_0 m + n)\cdot \mathrm{Q}), \qquad \sum_{j\in \mathrm{J}} u_j \cdot v_j^{q_0} \in \mathcal{H} \;\mapsto\; \sum_{j\in \mathrm{J}} u_j^{q_0} \cdot v_j.$$

2.5. Explain why the map Φ is well-defined if $m < q_0$, and prove that it is additive, *i.e.* that

$$\Phi(f+g) = \Phi(f) + \Phi(g) \text{ for all } f, g \in \mathrm{H}.$$

2.6. From now on, we choose $m = q_0 - 1$ and $n = q_0 + 2g$. Using the Riemann-Roch theorem, prove that $\operatorname{Ker}\Phi \neq \{0\}$.
Remember our assumption that $q = q_0^2 > (g+1)^4$.

2.7. Let $z \in \operatorname{Ker}\Phi \smallsetminus \{0\}$. For all $\mathrm{P} \in \mathrm{C}(\mathbb{F}_q) \smallsetminus \{\mathrm{Q}\}$, explain why z is regular at P, and prove that $z(\mathrm{P}) = 0$.
Hint: what are the poles of z? To show that $z(\mathrm{P}) = 0$, you may compute $z(\mathrm{P})^{q_0}$ and remember that $q = q_0^2$.

2.8. Finally, prove the chain of inequalities:

$$\#(\mathrm{C}(\mathbb{F}_q) \smallsetminus \{\mathrm{Q}\}) \leqslant \deg \operatorname{div}(z)_0 = \deg \operatorname{div}(z)_\infty \leqslant m + nq_0,$$

and conclude that (1) holds (for our choice of m, n).

Exercise 3 – Given a finite field $\mathbb{F}_q$, let $n, k \geqslant 1$ be integers such that $1 \leqslant k \leqslant n-1$. Denote by $\mathcal{G}_{k,n}$ the Grassmannian variety over $\mathbb{F}_q$: for each finite extension $\mathbb{F}_{q^s}/\mathbb{F}_q$, the $\mathbb{F}_{q^s}$-rational points on $\mathcal{G}_{k,n}$ are the k-dimensional subspaces of $(\mathbb{F}_{q^s})^n$.

3.1. Show that $\mathrm{GL}_n(\mathbb{F}_q)$ acts transitively on $\mathcal{G}_{k,n}(\mathbb{F}_q)$, and that the stabilizer of each point $\mathrm{S} \in \mathcal{G}_{k,n}(\mathbb{F}_q)$ is in bijection with $\mathrm{GL}_k(\mathbb{F}_q) \times \mathrm{GL}_{n-k}(\mathbb{F}_q) \times \mathrm{M}_{k,n-k}(\mathbb{F}_q)$, where $\mathrm{GL}_n(\mathbb{F}_q)$ denotes the group of invertible matrices of size $n \times n$ with coefficients in $\mathbb{F}_q$, and $\mathrm{M}_{k,n-k}(\mathbb{F}_q)$ is the set of all matrices of size $k \times n-k$ with coefficients in $\mathbb{F}_q$.

3.2. Show that, for each $k \geqslant 1$, one has

$$\#\mathrm{GL}_k(\mathbb{F}_q) = q^{\frac{k(k-1)}{2}}(q^k - 1)(q^{k-1} - 1)\dots(q-1).$$

3.3. Use the previous questions to show that $\#\mathcal{G}_{k,n}(\mathbb{F}_q) = \binom{n}{k}_q$, where $\binom{n}{k}_q$ is the Gaussian binomial coefficient:

$$\binom{n}{k}_q := \frac{(q^n-1)\dots(q^{n-k+1}-1)}{(q^k-1)\dots(q-1)}.$$

3.4. Prove that

$$\binom{n}{k}_q = q^k \binom{n-1}{k}_q + \binom{n-1}{k-1}_q$$

3.5. Use this to deduce that there exist some $\lambda_{k,n}(i) \in \mathbb{Z}_{\geqslant 0}$ $(i = 0, ..., k(n-k))$ such that

$$\binom{n}{k}_q = \sum_{i=0}^{k(n-k)} \lambda_{k,n}(i)\cdot q^i.$$

3.6. With the same notations as in the previous question, deduce the following identity between formal power series:

$$\sum_{s=1}^{\infty} \frac{\#\mathcal{G}_{k,n}(\mathbb{F}_{q^s})}{s}\cdot \mathrm{T}^s = -\sum_{i=0}^{k(n-k)} \lambda_{k,n}(i)\cdot \log(1 - q^i \cdot \mathrm{T}).$$

Deduce an expression of the zeta function of $\mathcal{G}_{k,n}$ over $\mathbb{F}_q$, which is defined as:

$$\mathrm{Z}(\mathcal{G}_{k,n}/\mathbb{F}_q, \mathrm{T}) = \exp\left(\sum_{s=1}^{\infty} \frac{\#\mathcal{G}_{k,n}(\mathbb{F}_{q^s})}{s}\cdot \mathrm{T}^s\right).$$

3.7. Compare $\mathrm{Z}(\mathcal{G}_{1,2}/\mathbb{F}_q, \mathrm{T})$ and $\mathrm{Z}(\mathbb{P}^1/\mathbb{F}_q, \mathrm{T})$, and give a geometric interpretation of your result.
