HOMEWORK #1

Exercise 1 – We fix a perfect field k of *odd characteristic.* Let $f = \sum_{j=0}^{d} a_j x^j \in k[x]$ be a monic squarefree polynomial of degree $d \geqslant 2$. Define $h_0(x,y) := y^2 - f(x) \in \bar{k}[x,y]$ and consider the affine set $C_0 \subset \mathbb{A}^2$ corresponding to the ideal $(h_0) \subset \bar{k}[x,y]$.

1.1. Prove that C_0 is a smooth affine algebraic variety of dimension 1, which is defined over k.

1.2. Let $\overline{C}_0 \subset \mathbb{P}^2$ be the projective closure of C_0. Give an equation for $\overline{C}_0$ (in the $[x:y:z]$-coordinates on $\mathbb{P}^2$).

1.3. We know that $\overline{C}_0 \cap \{z=1\}$ "is" $C_0 \subset \mathbb{A}^2$ (see Lecture Notes). Compute the set $\overline{C}_0 \cap \{z=0\}$ of "points at infinity" on $\overline{C}_0$. Check that all the points in this set are k-rational.

1.4. Is $\overline{C}_0$ smooth? If not, give a list of singular points. *Your answer can depend on d.*

We now assume that $d > 3$; if d is odd (resp. if d is even), we write $d = 2g+1$ (resp. $d = 2g+2$) with $g \in \mathbb{Z}_{\geqslant 1}$. Consider the projective algebraic set $\overline{C} \subset \mathbb{P}^{g+2}$, whose ideal $I_h(\overline{C}) \subset \bar{k}[x_0, x_1, \ldots, x_{g+2}]$ is generated by the following $2g$ homogeneous polynomials of degree 2:

$$\begin{array}{rlrl}
Q_1 &= x_1^2 - x_0x_2 & Q_{g+1} &= x_0x_{g+1} - x_1x_g \\
Q_2 &= x_2^2 - x_1x_3 & Q_{g+2} &= x_1x_{g+1} - x_2x_g \\
&\vdots & &\vdots \\
Q_{g-1} &= x_{g-1}^2 - x_{g-2}x_g & Q_{2g-1} &= x_{g-2}x_{g+1} - x_{g-1}x_g \\
Q_g &= x_g^2 - x_{g-1}x_{g+1} & &
\end{array}$$

$$\begin{cases}
H_o = -x_{g+2}^2 + \sum_{j=0}^{g} a_j \cdot x_0x_j + \sum_{j=0}^{g} a_{j+g+1} \cdot x_{g+1}x_j & \text{if } d \text{ is odd,} \\
H_e = -x_{g+2}^2 + \sum_{j=0}^{g} a_j \cdot x_0x_j + \sum_{j=0}^{g+1} a_{j+g+1} \cdot x_{g+1}x_j & \text{if } d \text{ is even.}
\end{cases}$$

1.5. Give equations for $\overline{C} \cap \{x_0 \neq 0\}$. Prove that the map $f : \mathbb{A}^2 \to \mathbb{P}^{g+2}$ given by $(x,y) \mapsto [1 : x : x^2 : \cdots : x^{g+1} : y]$ induces a well-defined bijection between C_0 and $\overline{C} \cap \{x_0 \neq 0\}$.

Hint: start by proving that, for all $[x_0 : x_1, \ldots, x_{g+2}] \in \overline{C}$, one has $x_j x_0^{j-1} = x_1^j$ for $j = 1, \ldots, g+1$.

1.6. Show that $\overline{C} \cap \{x_0 = 0\}$ consists of the one point $P_\infty = [0:0:\cdots:0:1:0]$ if d is odd, and of the two points $P_\pm = [0:0:\cdots:0:1:\pm1]$ if d is even.

We view $C_1 := \overline{C} \cap \{x_{g+1} = 1\}$ as an affine subset of $\mathbb{A}^{g+2}$ with coordinates $(x_0, x_1, \ldots, x_g, x_{g+2})$.

1.7. By dehomogenizing the equations of $\overline{C}$ with respect to the variable x_{g+1}, give equations for $C_1 \subset \mathbb{A}^{g+2}$ (*i.e.* exhibit generators of the ideal of C_1 in $\bar{k}[x_0, \ldots, x_g, x_{g+2}]$).

1.8. In the case when d is odd, compute the rank of the Jacobian matrix of C_1 at the point $(0, \ldots, 0) \in \mathbb{A}^{g+2}$. Is C_1 smooth at $(0, \ldots, 0)$? In the case when d is even, compute the rank of the Jacobian matrix of C_1 at the points $(0, \ldots, 0, \pm1) \in \mathbb{A}^{g+2}$. Is C_1 smooth at these points?

1.9. Conclude about the smoothness of $\overline{C} \subset \mathbb{P}^{g+2}$.

Exercise 2 – Let $C/\mathbb{F}_q$ be a smooth projective curve defined over $k = \mathbb{F}_q$. As such, C is also defined over any finite extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ (because one can see the equations $f_a \in \mathbb{F}_q[X]$ defining C as equations with coefficients in $\mathbb{F}_{q^m}$). In this exercise, we study the relation between the zeta functions of $C/\mathbb{F}_q$ and $C/\mathbb{F}_{q^m}$.

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

2.2. 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,

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

2.3. For any integers $m, d \geqslant 1$, prove the identity in $\mathbb{C}[\mathrm{T}]$:

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

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

2.4. 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 group the* w*'s "coming from" a given* $\mathbb{F}_q$*-place* v *of* C *(by Q.2.2).*

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 there exists a constant $c_q > 0$ (depending only on q) such that for all $d \geqslant 1$,

$$\left| \mathrm{Ir}_d - \frac{q^d}{d} \right| \leqslant c_q \cdot \frac{q^{d/2}}{d}.$$

Comment on why this result is called "the analogue of the prime number theorem for $\mathbb{F}_q[\mathrm{X}]$".

Exercise 4 – Let $k = \mathbb{F}_q$ be a finite field. Consider the projective variety $\mathrm{X}/\mathbb{F}_q$ defined by the equation

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

4.1. 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" $\mathrm{Y} = \mathrm{X} \cap \{z = 1\} \subset \mathbb{A}^2$.

4.2. 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* $\mathbb{F}_q^\times$*?*

4.3. 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

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

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

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