Algebraic Curves over Finite Fields

Homework 2

The second homework assignment consists in **5 problems** of your choice among those ones listed here below (if you hand in more exercises, I will count the 5 with the highest score). Each exercise will count for 20 points (if you score above 20 in an exercise, your grade for that exercise will be 20). **Due date: Wednesday, November 28**.

Note: This homework assignment is in constant evolution... Problems will be added as the semester goes on, but once an exercise is posted, it will not change (up to ordering). Discussion of the homework problems with me, or collaboration (in a reasonable degree) with your classmates, is encouraged, but you have to provide a note on which problems you had assistance.

Ex 1. In $\mathbb{A}^2(\mathbb{R})$, a **conic** $\mathcal{C}$ is an algebraic set of the form $V(f(x,y))$, where $f(x,y) \in \mathbb{R}[x,y]$ is a polynomial of degree two. In other terms one has:

$$\mathcal{C} : Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0,$$

where $A, B, C, D, E, F \in \mathbb{R}$ and A, B, C are not all zero.

(a) **(Bonus)** A conic $\mathcal{C}$ is called non-degenerate if $\mathcal{C}$ is absolutely irreducible, i.e. $\mathcal{C}$ is irreducible over $\mathbb{C}$. Show that $\mathcal{C}$ is non-degenerate if and only if

$$\begin{vmatrix} A & \frac{B}{2} & \frac{D}{2} \\ \frac{B}{2} & C & \frac{E}{2} \\ \frac{D}{2} & \frac{E}{2} & F \end{vmatrix} \neq 0.$$

(b) **(10 points)** If $\mathcal{C}$ is non-degenerate, then $\mathcal{C}$ can be classified as follows:

- $\mathcal{C}$ is an **ellipse** if and only if $B^2 - 4AC < 0$;
- $\mathcal{C}$ is a **parabola** if and only if $B^2 - 4AC = 0$;
- $\mathcal{C}$ is a **hyperbola** if and only if $B^2 - 4AC > 0$.

Let $\overline{\mathcal{C}} \subseteq \mathbb{P}^2(\mathbb{R})$ be the projective closure of $\mathcal{C}$. Show that the above classification is equivalent to the following one:

- $\mathcal{C}$ is an ellipse if and only if $\overline{\mathcal{C}}$ has no points at infinity;
- $\mathcal{C}$ is a parabola if and only if $\overline{\mathcal{C}}$ has one point at infinity;
- $\mathcal{C}$ is a hyperbola if and only if $\overline{\mathcal{C}}$ has two different points at infinity.

(c) **(10 points)** Consider the family of conics $\{\mathcal{C}_t\}_{t\in\mathbb{R}}$ where

$$\mathcal{C}_t : x^2 - txy - 8ty^2 - x - y = 0.$$

Classify $\mathcal{C}_t$ with respect to the parameter t, and for $t = 4$ find the points at infinity of $\overline{\mathcal{C}}_4$.

Ex 2. (a) **(10 points)** Let $K \subseteq L$ be a separable field extension of degree n. For $i = 1, \ldots, n$, let $\sigma_i : L \to \overline{K}$ be a K-embedding of L into $\overline{K}$. Prove that $\gamma \in L$ is in K if and only if $\sigma_i(\gamma) = \gamma$, for all $i = 1, \ldots, n$.

(b) **(10 points)** Let k be a perfect field and $P \in \mathbb{A}^n(\overline{k})$. Prove that $P \in \mathbb{A}^n(k)$ if and only if $P^\sigma = P$ for all $\sigma \in \mathrm{Gal}_k(\overline{k})$.

Ex 3. (30 points) Prove that the following conditions are equivalent for a field k.

(a) Every irreducible polynomial in $k[x]$ is separable.

(b) Every algebraic extension of k is separable.

(c) Either k has characteristic 0, or, when k has characteristic $p > 0$, every element of k is a pth power, i.e. for all $\alpha \in k$ there exists $\beta \in k$ such that $\beta^p = \alpha$.

(d) Either k has characteristic 0, or, when k has characteristic $p > 0$, the Frobenius endomorphism $x \to x^p$ is an automorphism of k.

You may use the fact that $f(x) \in k[x]$ is separable if and only if $\gcd(f(x), f'(x)) = 1$.

Ex 4. Recall that a point of $\mathbb{P}^n(\mathbb{Q})$ has the form $[x_0 : \ldots : x_n]$, with $x_i \in \mathbb{Q}$.

(a) **(10 points)** Let $V \subseteq \mathbb{P}^n$ be a projective algebraic set defined over $\mathbb{Q}$ such that $I(V) = (F_1, \ldots, F_s)$, where $F_1, \ldots, F_s$ are homogeneous polynomials in $\mathbb{Q}[X_0, \ldots, X_n]$. Prove that the set of $\mathbb{Q}$-rational points can be described as:

$$V(\mathbb{Q}) = \{[x_0 : \ldots : x_n] : x_i \in \mathbb{Z}, \gcd(x_1, \ldots, x_n) = 1 \text{ and } F_i(x_0, \ldots, x_n) = 0 \text{ for all } i\}.$$

(b) **(20 points)** Consider now the following algebraic set defined over $\mathbb{Q}$:

$$V : X^2 + Y^2 = 3Z^2.$$

b.1) Show that the equation $x^2 + y^2 = 0$ has no solutions modulo 3, a part $(0, 0)$.

b.2) Using (a), explain why (b.1) implies $V(\mathbb{Q}) = \emptyset$.

b.3) Is V isomorphic over $\mathbb{Q}$ to $W : X^2 + Y^2 = Z^2$? Why?

b.4) Are V and W isomorphic over $\mathbb{Q}(\sqrt{3})$? Why?

Ex 5. Consider the projective algebraic curve V defined over $\mathbb{F}_7$ which is described by the affine equation

$$y^2 = x^3 + 2.$$

(a) **(10 points)** Find the $\mathbb{F}_7$-rational points on V.

(b) Let $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ be two distinct points on V. Let ℓ be the line through P_1 and P_2.

b.1) **(8 points)** Show that $V \cap \ell = \{P_1, P_2, P_3\}$ and express P_3 in terms of the coordinates of P_1 and P_2. (If ℓ is tangent to V, then P_3 may equal P_1 or P_2.)

b.2) **(4 points)** Show that if $P_1, P_2 \in V(\mathbb{F}_7)$, then $P_3 \in V(\mathbb{F}_7)$.

b.3) **(4 points)** Calculate P_3 for $P_1(3, 1)$ and $P_2(5, 6)$.

Ex 6. Let k be a field of characteristic $p \neq 2, 3$. Consider the projective algebraic curve V defined over k which is described by the affine equation:

$$V : y^2 = x^3 + ax + b.$$

(a) **(5 points)** Show that V has exactly one point at infinity.

(b) **(10 points)** Prove that V is non-singular if and only if $-4a^3 - 27b^2 \neq 0$.

You may use the fact that a cubic polynomial of the form $f(x) = x^3 + px + q \in k[x]$ has a double root if and only if its discriminant $-4p^3 - 27q^2$ is different from zero.

(c) **(10 points)** Let $k = \mathbb{F}_q$. Prove that $\sharp E(\mathbb{F}_q) \leq 2q + 1$.

Ex 7. (a) **(10 points)** Prove that $\sharp \mathbb{P}^n(\mathbb{F}_q) = q^n + q^{n-1} + \cdots + q + 1$.

(b) **(15 points)** Let X be an absolutely irreducible algebraic curve defined over $\mathbb{F}_q$. The *zeta function* associated to X, denoted by $Z_X(T)$, is defined as the formal power series:

$$Z_X(T) = \exp\left(\sum_{n=1}^{\infty} \sharp X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

Prove that, if $X = \mathbb{P}_1$, then one has

$$Z_{\mathbb{P}^1}(T) = \frac{1}{(1-T)(1-qT)}.$$