# Algebraic Curves over Finite Fields

## Homework 1

The first 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). It is **due on Monday, ~~October 8~~ October 15**.

**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.** Let $k = \mathbb{C}$ and let $X$ be the (affine) conic described by the polynomial

$$f(x, y) = x^2 + y^2 - 1 \in k[x, y].$$

(a) Find the rational parametrization

$$\begin{array}{ccc} k & \longrightarrow & X \\ t & \longmapsto & (\varphi(t), \psi(t)) \end{array}$$

obtained via the construction given in class by using the point $(-1, 0) \in X$.

(b) Interpret geometrically the parametrization found in (a) in order to prove the trigonometric identities:

$$\sin(\theta) = \frac{2\tan\left(\frac{\theta}{2}\right)}{1+\tan^2\left(\frac{\theta}{2}\right)}, \qquad \cos(\theta) = \frac{1-\tan^2\left(\frac{\theta}{2}\right)}{1+\tan^2\left(\frac{\theta}{2}\right)}, \qquad \text{for all } \theta \in (-\pi, \pi) \subset \mathbb{R}.$$

(c) Find the general form for the solution in $\mathbb{Q}^2$ of the equation $x^2 + y^2 - 1 = 0$.

(d) A *Pythagorean triple* is a triple $(a, b, c)$ of positive integers such that $a^2 + b^2 = c^2$. Use (c) in order to prove the *Euclid's formula* that generates a Pythagorean triple for each $m, n \in \mathbb{N}$ with $m > n > 0$:

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

**Ex 2.** The *Weak Nullstellensatz* states:

*"If $k$ is an algebraically closed field and $I$ is a proper ideal of $k[X_1, \dots, X_n]$, then $V(I) \neq \emptyset$."*

(a) Explain why the *Weak Nullstellensatz* can be considered a generalized version of the *Fundamental Theorem of Algebra*.

(b) In $\mathbb{C}[x]$ consider the polynomials $f(x) = 1 + x + x^2$ and $g(x) = 1 + x + x^2 + x^3$. Show that $V(f, g) = \emptyset$.

**Ex 3.** In class we proved that the *Weak Nullstellensatz* implies *Hilbert's Nullestellensatz*. Prove that they are indeed equivalent statements, i.e. that also *Hilbert's Nullestellensatz* implies the *Weak Nullstellensatz*.

**Ex 4.** Consider the ideal $I = (x^3 + y^3 - 1) \subset \mathbb{Q}[x, y]$.

(a) Show that $I$ is a prime ideal of $\mathbb{Q}[x, y]$.

(b) Show that $V(I)$ is a reducible algebraic set of $\mathbb{A}^2(\mathbb{Q})$.

(c) Explain why this proves that in the Hilbert's Nullstellensatz the hypothesis that $k$ is algebraically closed can not be removed.

**Ex 5.** Let $k$ be an algebraically closed field and consider the algebraic set $V = V(y - F(x)) \subset \mathbb{A}^2(k)$, where $F(x) \in k[x]$.

(a) Show that $V$ is an affine variety.

(b) Show that $V$ is isomorphic to $\mathbb{A}^1(k)$ by exhibiting an example of two morphisms $\varphi : V \to \mathbb{A}^1(k)$ and $\psi : \mathbb{A}^1(k) \to V$ such that $\psi \circ \varphi = \mathrm{id}_V$ and $\varphi \circ \psi = \mathrm{id}_{\mathbb{A}^1(k)}$.

(c) Explain why $k[V] \cong k[x]$ (where $k[x]$ is the ring of polynomials in one variable) and exhibit a ring isomorphism that fixes $k$ (i.e. an isomorphism of $k$-algebras) between $k[V]$ and $k[x]$.

**Ex 6.** Let $k$ be an algebraically closed field and let $X$ be the algebraic set in $\mathbb{A}^4(k)$ defined as:

$$X = V(y - x^2, xy - z, w - y^2, w - xz)$$

(a) Show that $I(X)$ can be generated by three elements.

(b) Prove that $X$ is isomorphic to $\mathbb{A}^1(k)$.

**Ex 7.** Let $k$ be an algebraically closed field. Consider in $\mathbb{A}^2(k)$ the affine plane curves $V = V(y - x^2)$ and $W = V(xy - 1)$.

(a) Show that $V$ and $W$ are not isomorphic.

(b) Show that $V$ and $W$ are both rational curves.

(c) Explain why $V$ and $W$ are birational equivalent and exhibit an example of two rational maps $\varphi : V \to W$ and $\psi : W \to V$ such that $\psi \circ \varphi$ and $\varphi \circ \psi$ are the identities respectively on $V$ and $W$ (for all points where they are defined).

(d) For the rational maps $\psi$ and $\varphi$ you found in (c), write the corresponding sets of points where they are regular.

**Ex 8.** Let $X$ be a plane curve of degree 3.

(a) Prove that if $X$ has two singular points, then the line joining them is contained in $X$.

(b) Prove that if $X$ has three singular points, then it breaks up as a union of 3 lines.