Elliptic Curves - Homework 1

Francesco Minnocci

December 15, 2024

1. (in collaboration with Davide Pierrat)

Since $f \in \kappa(E) = \kappa(E_z)$ has no poles in the affine patch E_z, it lies in the intersection

$$\bigcap_{P \in E_z} \mathcal{O}_{E_z,P} = \mathcal{A}_{E_z} = \kappa[x,y]/(F_z),$$

where $F_z = F(x,y,1) = y^2 - x^3 - Ax - B$. This implies that f is of the form

$$g(x) + y \cdot h(x) \tag{1}$$

for some $g, h \in \kappa[x]$. Furthermore, through the identification seen in class between elements $\kappa(E_z)$ and quotients of homogeneous polynomials of the same degree, we can view f as the polynomial

$$g\left(\frac{x}{z}\right) + y \cdot h\left(\frac{x}{z}\right).$$

If moreover f has no poles, then we look at the affine patch E_y, where the curve becomes

$$F_y = z - x^3 - Axz^2 - Bz^3.$$

Then, we have seen that x generates the local ring at $O = (0,1,0)$ (because $\partial_z F_y(O) \neq 0$), so we get $v_O\left(\frac{x}{z}\right) = -2$ as

$$z = \frac{x^3}{1 - Axz - Bz^2},$$

and thus $v_O\left(\frac{1}{z}\right) = -3$. Now, via the canonical isomorphism $\mathcal{O}_{E_z,O} \simeq \mathcal{O}_{E_y,O}$ the polynomial (1) corresponds to

$$g\left(\frac{x}{z}\right) + \frac{1}{z} \cdot h\left(\frac{x}{z}\right),$$

and comparing the parity of the valuation at O of the two summands we deduce that f must be constant.

2. Throughout this exercise we will tacitly use the fact that, for a smooth projective plane curve X,

$$\deg(\operatorname{div}(f)) = 0$$

holds for any $f \in \kappa(X)^\times$.

Suppose first $D = \operatorname{div}(g)$ is the divisor of a function. Then,

$$\mathcal{L}(D) = \{f \mid \operatorname{div}(f) + \operatorname{div}(g) \geq 0\},$$

so we are looking for those functions f such that $v_P(g)+v_P(f) \geq 0$ for all $P \in X$, and since

$$\sum_P v_P(g) = \sum_P v_P(f) = 0,$$

this means that $v_P(g) = -v_P(f)$ for all $P \in X$. In other words,

$$v_P\left(\frac{g}{f}\right) = 0 \ \ \forall P \in X \implies \frac{g}{f} \in \kappa^\times,$$

where the last implication follows from the fact that

$$\bigcap_P \mathcal{O}_{X,P} = \kappa$$

for any smooth projective plane curve X. This implies that $\dim(\mathcal{L}(D)) = 1$, as we have shown

$$\mathcal{L}(D) = \{\lambda \cdot \frac{1}{f} \mid \lambda \in \kappa\}$$

Let us now proceed by contrapositive: assume that the dimension of $\dim \mathcal{L}(D)$ is strictly positive, where $D = \sum_P m_P P$. Then, there must be a function $f \in \kappa(X)^\times$ such that

$$v_P(f) \geq -m_P$$

for all $P \in X$, and by hypothesis we have

$$\sum_P m_P = \sum_P v_P(f) = 0.$$

Therefore, as in the above argument we deduce $v_P(f) = -m_P$ for all $p \in X$, which shows that D is the divisor of the function $\frac{1}{f} \in \kappa(X)^\times$.

3. We begin by noting that the conic

$$C : x^2 + y^2 = z^2$$

defined over the finite field $\mathbb{F}_q$ is isomorphic to the projective line $\mathbb{P}^1 = \mathbb{P}^1_{\mathbb{F}_q}$, via the morphism

$$\begin{aligned} \mathbb{P}^1 &\longrightarrow C \\ [x_0 : x_1] &\longmapsto [x_0^2 - x_1^2 : 2x_0x_1 : x_0^2 + x_1^2], \end{aligned}$$

whose inverse is given by the morphism

$$\begin{aligned} C &\longrightarrow \mathbb{P}^1 \\ [x : y : z] &\longmapsto \begin{cases} [y : x+z] & \text{if } y(z+x) \neq 0 \\ [z-x : y] & \text{if } y(z-x) \neq 0 \end{cases} \end{aligned}$$

Therefore, if $q = p^m$ the number of $\mathbb{F}_q$-points on C is equal to

$$N_m = \left|\mathbb{P}^1\right| = 1 + q^m,$$

and we can compute its zeta function as

$$\begin{aligned}
Z_C(t) &= \exp\left(\sum_{m\geq 1} \frac{t^m}{m}(1+q^m)\right) \\
&= \exp\left(\sum_{m\geq 1} \frac{t^m}{m}\right) \exp\left(\sum_{m\geq 1} \frac{(qt)^m}{m}\right) \\
&= \frac{1}{(1-t)(1-qt)},
\end{aligned}$$

where the last equality follows from the well-known logarithmic expansion

$$\log\left(\frac{1}{1-x}\right) = \sum_{m\geq 1} \frac{x^m}{m}$$

Finally, we prove the functional equation for C:

$$\begin{aligned}
Z_C(t) = \frac{1}{1-t} \cdot \frac{1}{1-qt} &= \frac{1}{qt^2}\left(\frac{t}{1-t}\right)\left(\frac{qt}{1-qt}\right) \\
&= q^{-1}t^{-2}\left(\frac{1}{1-\frac{1}{t}}\right)\left(\frac{1}{1-\frac{1}{qt}}\right) \\
&= q^{g-1}t^{g-2} Z_C\left(\frac{1}{qt}\right),
\end{aligned}$$

which concludes since C has genus

$$g = \frac{(2-1)(2-2)}{2} = 0.$$