Homework 3: Elliptic curves over finite fields and L-functions

Deadline: 6th August (23:55 JST), 2024 at TACT

Exercise 8. Compute the group $E(\mathbb{F}_p)$ for the curve

$$E : y^2 = x^3 + x + 1$$

and the primes $p = 3, 7$ and 11.

Exercise 9. Let $p \equiv 3 \pmod 4$ be a prime, and let $b \in \mathbb{F}_p^\times$.

(i) Show that the equation

$$v^2 = u^4 - 4b$$

has $p - 1$ solutions (u, v) with $u, v \in \mathbb{F}_p$.

(ii) Show that if (u, v) is a solution of the equation in (i), then

$$\varphi(u, v) = \left(\frac{u^2 + v}{2}, \frac{u(u^2 + v)}{2} \right)$$

is a point on the elliptic curve

$$E : y^2 = x^3 + bx.$$

(iii) Prove that the curve E defined in (ii) satisfies $|E(\mathbb{F}_p)| = p + 1$.

Exercise 10. Let $E/\mathbb{Q}$ be an elliptic curve. Define the coefficients a_n, for all $n \geq 1$ as follows. Let $a_1 = 1$ if $p \geq 2$ is prime define

$$a_p = \begin{cases} p + 1 - |E(\mathbb{F}_p)| & \text{if } E \text{ has good reduction at } p; \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p; \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p; \\ 0 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

If $n = p^r$ for some $r \geq 1$, we define a_{p^r} recursively using the relation:

$$a_p \cdot a_{p^r} = a_{p^{r+1}} + p \cdot a_{p^{r-1}} \quad \text{if } E/\mathbb{Q} \text{ has good reduction at } p,$$

and $a_{p^r} = (a_p)^r$ if $E/\mathbb{Q}$ has bad reduction at p. Finally, if $(m, n) = 1$ then we define $a_{mn} = a_m \cdot a_n$.

Show that the L-function (as defined in Definition 7.1 below) of E is given by

$$L(E, s) = \sum_{n \geq 1} \frac{a_n}{n^s}.$$

References

[LR] A. Lozano-Robledo: *Elliptic Curves, Modular Forms, and Their L-functions*, Student Mathematical Library, No. 58. American Mathematical Society, Providence, RI, 2011.

Definition 7.1: The L-function of an elliptic curve $E/\mathbb{Q}$ is defined by

$$L(E,s) = \prod_{\substack{p \geq 2 \\ p\text{prime}}} \frac{1}{L_p(p^{-s})},$$

where

$$L_p(T) = \begin{cases} 1 - a_p T + pT^2 & \text{if } E \text{ has good reduction at } p; \\ 1 - T & \text{if } E \text{ has split multiplicative reduction at } p; \\ 1 + T & \text{if } E \text{ has non-split multiplicative reduction at } p; \\ 1 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

Here $a_p = p + 1 - |E(\mathbb{F}_p)|$. (Recall that by definition $E(\mathbb{F}_p)$ always contains the point $\mathcal{O}$)