Exercises: Week 11

Computation in Algebra and Arithmetic

David Loeffler & Tim Gehrunger

12.5.2022

1 Number of Rational Points

Let q be the power of a prime and let $E/\mathbf{F}_q$ be an elliptic curve. At the end of the last lecture it has been hinted that $\#E(\mathbf{F})_{\mathbf{q}}$ will be close to $q+1$. The goal of this exercise is to verify this statement in a special case.

Write a script that goes trough all elliptic curves defined over $\mathbf{F}_5$ and tabulate the number of their rational points. Note that it suffices to go through all short Weierstrass equations, for which the smoothness condition can be checked by a polynomial equation.

2 Legendre Form and j-invariant

There is another form of Weierstrass equation that is sometimes convenient.
A Weierstrass equation over K is said to be in **Legendre Form** if it can be written as

$$y^2 = x(x-1)(x-\lambda).$$

For this exercise, assume that $\mathrm{char}(K) \neq 2$ and that K is algebraically closed.

(a) Show that every elliptic curve over K is isomorphic to an elliptic curve in Legendre form

$$E_\lambda : \ y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \in K \setminus \{0,1\}$.

(b) Write down the group law for the points of E_λ.

Let E be an elliptic curve over K, given by a Weierstrass equation

$$E : y^2 = x^3 + Ax + B.$$

The **j-invariant** of this equation is defined by

$$j = 1728 \frac{(4A)^3}{16(4A^3 + 27B^2)}.$$

One can show that j completely classifies elliptic curves up to isomorphism, i.e. two elliptic curves over K are isomorphic if they both have the same j-invariant (For this one really needs that K is algebraically closed). The proof of this statement exceeds the scope of this exercise.

(c) Show that for two isomorphic elliptic curves C_1, C_2 over K, we have $j(C_1) = j(C_2)$.

(d) Show that the j-invariant of E_λ is given by

$$2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1))}.$$

(e) Show that the association

$$K \backslash \{0, 1\} \setminus K, \quad \lambda \longmapsto j\left(E_\lambda\right),$$

is surjective and exactly six-to-one except above $j = 0$ and $j = 1728$, where it is two-to-one and three-to-one, respectively (unless $\mathrm{char}(K) = 3$, in which case it is one-to-one above $j = 0 = 1728$).