Exercises for the course: Introduction to elliptic curves

AESIM school on

Algebra, Number theory and their applications to Cryptography

Salahaddin University, Erbil, Kurdistan Region, Iraq

25/02/2024 - 7/03/2024

Exercise 1. ***Legendre equation***

(a) Let K be a field with characteristic different from 2. Let

$$E : y^2 = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3).$$

Consider the following change of coordinates

$$\begin{cases} w = \dfrac{x - e_1}{(e_2 - e_1)} \\ \\ z = \dfrac{y}{(e_2 - e_1)^{3/2}} \end{cases}$$

and set

$$\lambda = \frac{e_3 - e_1}{(e_2 - e_1)}.$$

Prove that $\lambda \neq 0, 1$ and that the equation for E in the new coordinates is

$$z^2 = w(w - 1)(w - \lambda)$$

(b) For each $\sigma \in S_3$ express

$$\lambda_\sigma = \frac{e_{\sigma(3)} - e_{\sigma(1)}}{e_{\sigma(2)} - e_{\sigma(1)}}$$

in terms of λ.

(c) Put the Legendre equation $y^2 = x(x - 1)(x - \lambda)$ into Weierstrass form and use this to show that the j-invariant is

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

(d) Show that if $j \neq 0, 1728$ then there are six distinct values of λ giving this j, and that if λ is one such value then the full set is

$$\left\{ \lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1 - \lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda} \right\}.$$

(e) Show that if $j = 1728$ then $\lambda = -1, 2, 1/2$, and if $j = 0$ then λ is a root of $t^2 - t + 1 = 0$.