Cryptography

JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

7. Tutorial: Elliptic curves and group law

Let F be a field of characteristic different from 2 or 3. In the following we consider a non-singular elliptic curve E defined over F by its Weierstraß equation $E : y^2 = x^3 + ax + b$, where a and $b \in F$.

Exercise 7.1 (Addition formulae).

(i) Given two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on the curve E, give the equation of the line passing through P and Q.

(ii) Find the coordinates (x_R, y_R) of the third intersection point of this line with E.

(iii) What are the coordinates $P + Q$?

(iv) What about the coordinates of $2P = P + P$?

Exercise 7.2 (Associativity).

Using the previous formulae for point addition, prove the associativity of the group law with the help of your favourite computer algebra system.