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.

Solution. Noting

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q},$$

we have the line $L_{P,Q} : y = \lambda(x - x_P) + y_P$. ◯

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

Solution. We only have to inject the equation of $L_{P,Q}$ into the equation of E:

$$x^3 + ax + b - (\lambda(x - x_P) + y_P)^2 = 0.$$

Since we know x_P and x_Q are solutions of this equation, we can factor it as

$$(x - x_P)(x - x_Q)(x - x_R) = 0,$$

which by identification with the previous one gives

$$x_P + x_Q + x_R = \lambda^2.$$

Hence, $x_R = \lambda^2 - x_P - x_Q$ and, from the line equation, $y_R = \lambda(x_R - x_P) + y_P$. ◯

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

Solution. $P + Q = (\lambda^2 - x_P - x_Q, \lambda(x_P - x_R) - y_P)$. ◯

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

Solution. This case is the same, only with the slope of the tangent being

$$\lambda = \frac{3x_P^2 + a}{2y_P}.$$

○

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.

Solution. Don't forget that the three points are on the curve! Hence you should compute modulo the curve equation for the coordinates of these points.

○