Public-Key Cryptography: a Mathematical Insight

Edoardo Persichetti | Lecture 6: Elliptic Curves | 26/03/2014

Exercise 1 Recall the generalized Weierstrass equation for an elliptic curve over $\mathbb{K}$ when $char(\mathbb{K}) = 2$. Show that, through a change of variables, it is possible to obtain two standard forms for the equation, depending whether $a_1 = 0$ or $a_1 \neq 0$. For both cases, write explicit formulas for doubling a point.

Exercise 2 Let E be an elliptic curve over $\mathbb{K}$, with $char(\mathbb{K}) = 2$. Prove that we have either $E[2] \simeq \mathbb{Z}_2$ or $E[2] \simeq \{\infty\}$. Moreover, prove that $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Exercise 3 Let E be an elliptic curve defined by a homogeneous polynomial $F(x, y, z) \in \mathbb{P}^2(\mathbb{K})$. Show that a point P is in $E[3]$ if and only if the determinant of the Hessian matrix is 0.

Exercise 4 Let E be the elliptic curve defined by $y^2 + xy = x^3 + 1$. Describe $E(\mathbb{F}_4)$.

Exercise 5 Let E be the elliptic curve defined by $y^2 = x^3 + 7x + 12$ over $\mathbb{F}_{103}$.

- Find two points P_1 and P_2 on E.
- Determine the order of P_1 and P_2.
- Use Hasse-Weil's theorem to compute $\#E(\mathbb{F}_{103})$.

You might need the help of a computer for the first two questions.