

11. Exercise sheet
Hand in solutions until Thursday, 2. February 2012, 13.00

Exercise 11.1 (Addition on elliptic curves). (16+5 points)

Consider an elliptic curve $E = \{(u, v) \in F^2 : v^2 = u^3 + au + b\} \dot{\cup} \{\mathcal{O}\}$.

(i) Prove: If $(u, v) \in E$ then $(u, -v) \in E$. 1

In the lecture we defined a group structure $+$ on E . The neutral element is \mathcal{O} and the inverse of $P = (u, v) \in E$ is $-P = (u, -v)$.

(ii) For $(u, v) \in E$ compute $(u, v) + (u, -v)$. 1

For $P \in E$ and an positive integer n we define

$$n \cdot P = \underbrace{P + \dots + P}_{n \text{ times}}.$$

(iii) For $(u, 0) \in E$ compute $2 \cdot (u, 0)$. What is the order of $(u, 0)$? 1

Now let us consider the elliptic curve E over \mathbb{F}_7 with $a = 3$ and $b = 0$. That is $E = \{(u, v) \in \mathbb{F}_7^2 : v^2 = u^3 + 3u\} \dot{\cup} \{\mathcal{O}\}$.

(iv) Compute all points on E and draw an illustrative picture of E as you have seen it in the lecture. 5

(v) Compute $(3, 1) + (0, 0)$. 2

(vi) Compute $2 \cdot (3, 1)$. 2

(vii) Compute $3 \cdot (3, 1)$ and the inverse of $(3, 1)$. What is the order of $(3, 1)$? 4

(viii) We have $E \cong \mathbb{Z}_k \times \mathbb{Z}_\ell$ for some integers k and ℓ . Compute k and ℓ . +5