Crypto 2 WS 12

24. JAN. 2012

„Unofficial" registration to exam: maier@ti...

Review Exercise: Fr. 24.2.12 Crypto 1 14:00
Crypto 2 15:30
Consultation hour: Fr. 2.3.12 14:00
Exam, Gr Fr. 9.3.12 14:00

} WSII 24407

Ex 34.)

Per def.: $E: y^2 = x^3 + ax + b$ $a, b \in K$ with

$\Delta = -16(4a^3 + 27b^2) \neq 0$ describes an elliptic curve.

↑ Diskriminante

a.) Here: $E: y^2 = x^3 + x + 1$ i.e. $a = b = 1$

$K = \mathbb{F}_7$

$\Rightarrow \Delta = -16(4 \cdot 1^3 + 27 \cdot 1^2) \equiv 5 \cdot 3 \equiv 1 \pmod 7$

$\Rightarrow$ E is EC

b.) For determining the points (and for c) use the following table

z^{-1}	z	z^2	z^3	z^3+z+1
-	0	0	0	1
1	1	1	1	3
4	2	4	1	4
5	3	2	6	3
2	4	2	1	6
3	5	4	6	5
6	6	1	6	6

It follows $y^2 \in \{0, 1, 2, 4\} = A$

and $1 + x + x^3 \in \{1, 3, 4, 5, 6\} = B$

$C = A \cap B = \{1, 4\}$

$y^2 = 1 \Rightarrow y \in \{1, 6\}$

$1 + x + x^3 = 1 \iff x \in \{0\}$

$\Rightarrow (0,1), (0,6) \in E(\mathbb{F}_7)$

$y^2 = 4 \iff y \in \{2, 5\}$

$1 + x + x^3 = 4 \iff x \in \{2\}$

$\Rightarrow (2,2), (2,5) \in E(\mathbb{F}_7)$

$\Rightarrow E(\mathbb{F}_7) = \{ \mathcal{O}, (0,1), (0,6), (2,2), (2,5) \}$

often forgotten!

Abelian groups: for every x, y there must be a $n(x,y)$ s.th. $y + y' = 0$

For the trace t it holds:

$\#E(\mathbb{F}_q) = q + 1 - t$

$5 = 7 + 1 - t \iff t = 3$

elements in E

Hasse: $t < 2\sqrt{q}$

c.)

with the group law addition as in 13.2. $E(\mathbb{F}_7)$ is a finite abelian group.

3.7 holds $\operatorname{ord}(P) \mid \#E(\mathbb{F}_7) = 5$

It follows for $P \neq \mathcal{O} \Rightarrow 1 < \operatorname{ord}(P) = 5$,

i.e. every $P \neq \mathcal{O}$ is a generator

As in 13.2. the addition for $P = (x,y)$, $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$

(i) $P + \mathcal{O} = P$

(ii) $P + (x, -y) = \mathcal{O}$

(iii) $P_1 \neq \pm P_2 \Rightarrow P_3 = (x_3, y_3) = P_1 + P_2$ with

$$z = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)$$ → will not be $=0$ because of i.) and ii.)

$x_3 = z^2 - x_1 - x_2$, $y_3 = z(x_1 - x_3) - y_1$

(iv.) $P_1 \neq -P_1 \Rightarrow 2P_1 = P_1 + P_1 = (x_3, y_3)$ with

$c = \frac{3x_1^2 + a}{2y_1}$ $\quad x_3 = c^2 - 2x_1$, $y_3 = c(x_1 - x_3) - y_1$

start with $P = (0,1)$

$2P = 2 \cdot (0,1) \overset{(iv.)}{=} (2,5)$ $\quad c = \frac{1}{2} \equiv 4 \Rightarrow x_3 = 4^2 - 0 \equiv 2$

$y_3 = 4(0-2) - 1 \equiv 5 \pmod 7$

$3P = 2 \cdot P + P = (2,5) + (0,1) \overset{(iii)}{=} (2,2)$ $\quad z = \frac{-4}{-2} = 4 \cdot 2^{-1} \equiv 2$

$x_3 = 4 - 0 - 2 = 2$

$y_3 = 2(0) - 5 \equiv 2$

$4P = (2,2) + (0,1) \overset{(iii)}{=} (0,6)$

$5P = 4P + P = (0,6) + (0,1) \overset{(i)}{=} \mathcal{O}$

$6P = \mathcal{O} + (0,1) \overset{(i)}{=} (0,1)$

⋮