

## Musterlösung zum Zusatz-Übungsblatt zur Vorlesung Kryptologie

### Übung 2

In  $\mathbb{Z}_7$  gilt:

$y$	0	1	2	3	4	5	6
$y^2$	0	1	4	2	2	4	1

$x$	0	1	2	3	4	5	6
$x^3 - 3x - 1$	6	4	1	3	2	4	1

Also ist  $K = \{\mathcal{O}, (1, 2), (1, 5), (2, 1), (2, 6), (4, 3), (4, 4), (5, 2), (5, 5), (6, 1), (6, 6)\}$

### Übung 3

In  $\mathbb{Z}_5$  gilt:

$(0, 1) + (4, 4)$ :

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{4 - 1}{4 - 0} = 3 \cdot (4)^{-1} = 3 \cdot 4 = 2$$

$$x_3 = \lambda^2 - x_1 - x_2 = 2^2 - 0 - 4 = 0$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 2 \cdot (0 - 0) - 1 = 4.$$

$$\Rightarrow (0, 1) + (4, 4) = (0, 4).$$

$(0, 4) + (0, 4)$ :

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 0^2 - 1}{2 \cdot 4} = \frac{4}{3} = 4 \cdot (3)^{-1} = 4 \cdot 2 = 3$$

$$x_3 = \lambda^2 - x_1 - x_2 = 3^2 - 0 - 0 = 4$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 3 \cdot (0 - 4) - 4 = 4$$

$$\Rightarrow (0, 4) + (0, 4) = (4, 4).$$

Also ist  $((0, 1) + (4, 4)) + (0, 4) = (0, 4) + (0, 4) = (4, 4)$ . Andererseits:

$(4, 4) + (0, 4)$ :

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{4 - 4}{0 - 4} = 0$$

$$x_3 = \lambda^2 - x_1 - x_2 = 0 - 4 - 0 = 1$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 0 - 4 = 1$$

$$\Rightarrow (4, 4) + (0, 4) = (1, 1).$$

$(0, 1) + (1, 1)$ :

$$\begin{aligned}\lambda &= \frac{y_2 - y_1}{x_2 - x_1} = \frac{1 - 1}{1 - 0} = 0 \\ x_3 &= \lambda^2 - x_1 - x_2 = 0 - 0 - 1 = 4 \\ y_3 &= \lambda(x_1 - x_3) - y_1 = 0 - 1 = 4\end{aligned}$$

Also ist auch  $(0, 1) + ((4, 4) + (0, 4)) = (4, 4)$ .

#### Übung 4

Ist  $p > 2$  eine Primzahl, so ist  $p - 1 = 2n$  gerade. Mit  $M_1 := \{1, \dots, n\}$  und  $M_2 := \{n + 1, \dots, p - 1\}$  kann man  $\mathbb{Z}_p$  in drei verschiedenen Mengen zerlegen:  $\mathbb{Z}_p = \{0\} \cup M_1 \cup M_2$ .

Ist  $x \in \mathbb{Z}_p$ , so gilt:  $x^2 = (-x)^2 = (p - x)^2 \pmod{p}$ , also  $1^2 = (p - 1)^2$ ,  $2^2 = (p - 2)^2$ ,  $\dots$ ,  $n^2 = (p - n)^2$  (wobei  $p - n = n + 1$  gilt). Die Quadrate zu  $x \in M_2$  kommen also schon als Quadrate zu  $x \in M_1$  vor, d.h. es gibt höchstens  $0^2$  und die Quadrate zu  $x \in M_1$ , insgesamt also  $1 + n = 1 + \frac{p-1}{2} = \frac{p+1}{2}$ .

Man muss nun noch zeigen, dass  $0^2$  und die Quadrate zu  $x \in M_1$  alle verschieden sind:

Für  $x \in M_1$  ist insbesondere  $x \neq 0$ , also  $x^2 \neq 0 = 0^2$  (da  $\mathbb{Z}_p$  als Körper nullteilerfrei ist).

Seien nun  $x, y \in M_1$  mit  $x^2 = y^2 \pmod{p}$ . Dann gilt:

$$\begin{aligned}x^2 - y^2 &= 0 \pmod{p} \\ \Leftrightarrow (x + y)(x - y) &= 0 \pmod{p}.\end{aligned}$$

Da  $\mathbb{Z}_p$  nullteilerfrei ist, folgt  $x + y = 0 \pmod{p}$  oder  $x - y = 0 \pmod{p}$ . Wegen  $x, y \in M_1$  ist  $x + y \in \{2, \dots, 2n = p - 1\}$ , also  $x + y \neq 0 \pmod{p}$ . Damit muss  $x - y = 0 \pmod{p}$ , also  $x = y$  sein.

Damit ist gezeigt, dass auch die Quadrate zu  $x \in M_1$  alle verschieden sind.