Übungen zur Vorlesung **Blatt 7**
Elliptische Kurven und Kryptographie 8.06.2015

PD Dr. K. Halupczok
Dipl.–Math. A. Juhas SoSe 2015

Abgabetermin: Montag, 15. Juni 2015, bis 12:15 Uhr in die Briefkästen

Aufgabe 1:

Bestimmen Sie (die in diesen Fällen endliche) Ordnung von P auf der ell. Kurve $E = E(\mathbb{C})$:

(a) $P = (0, 16)$ auf $E : y^2 = x^3 + 256$
(b) $P = \left(\frac{1}{2}, \frac{1}{2}\right)$ auf $E : y^2 = x^3 + \frac{x}{4}$
(c) $P = (3, 8)$ auf $E : y^2 = x^3 - 43x + 166$
(d) $P = (0, 0)$ auf $E : y^2 + y = x^3 - x^2$.

Was ist eine geometrische Bedingung dafür, dass P die Ordnung 3 besitzt?

Aufgabe 2:

Sei E die elliptische Kurve mit affiner Gleichung $y^2 = x^3 + ax + b$ über einem Körper k mit $\operatorname{char} k \neq 2, 3$. Zeigen Sie: Ein Punkt $P = (x, y) \in E$ hat genau dann die Ordnung 3, wenn $3x^4 + 6ax^2 + 12bx - a^2 = 0$ gilt.

Aufgabe 3:

Sei k ein endlicher Körper mit $\operatorname{char} k \neq 2$ und $E(k)$ die elliptische Kurve mit affiner Gleichung $y^2 = f(x) := x^3 + ax + b$. Zeigen Sie:

(a) Genau dann gilt $2 \mid \#E(k)$, wenn f eine Nullstelle in k besitzt.
(b) E ist nicht zyklisch, falls f drei verschiedene Nullstellen in k besitzt.
(c) Wir betrachten die ell. Kurve $E : y^2 = x^3 + x + 1$ über $\mathbb{F}_5$. Bestimmen Sie die Gruppe $E(\mathbb{F}_5)$ und zeigen Sie, dass sie zyklisch ist.

Aufgabe 4:

Sei $p > 2$, $E : y^2 = x^3 + ax + b$ elliptische Kurve über $\mathbb{F}_p$ und

$$\left(\frac{a}{\mathbb{F}_p}\right) := \begin{cases} 0 & : a = 0, \\ 1 & : \exists b \in \mathbb{F}_p^* : \ b^2 = a, \\ -1 & : a \neq 0, b^2 \neq a \ \forall b \in \mathbb{F}_p^* \end{cases}$$

das verallgemeinerte Legendre–Symbol. Zeigen Sie

(a) $\#E(\mathbb{F}_p) \leq 2p + 1$.
(b) $\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3+ax+b}{\mathbb{F}_p}\right)$.
(c) Wir betrachten die ell. Kurve $E : y^2 = x^3 + x + 1$ über $\mathbb{F}_7$. Berechnen Sie $\#E(\mathbb{F}_7)$ mithilfe von (b).