Kryptographie **Blatt 12**

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 22.1.2024, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Punkte der Ordnung 3

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

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

Aufgabe 2: Punkteanzahl elliptischer Kurven über endlichen Körpern

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

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

das verallgemeinerte Legendresymbol. Zeigen Sie:

(a) $\#E(\mathbb{F}_p) \leq 2p + 1$.

(b) $\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right)$.

(c) Wir betrachten die elliptische Kurve $E : y^2 = x^3 + x + 1$ über $\mathbb{F}_7$. Berechnen Sie $\#E(\mathbb{F}_7)$ mithilfe von (b).

Aufgabe 3: Zweiteilungspunkte

Sei k ein Körper mit $\mathrm{char}(k) \neq 2, 3$ und $E(k)$ die elliptische Kurve mit affiner Gleichung $y^2 = f(x) := x^3 + ax + b$. Ein Punkt $P \in E(k)$ heißt Zweiteilungspunkt, wenn $2P = O$ gilt.
Zeigen Sie: $E(k)$ hat einen, zwei oder vier Zweiteilungspunkte.
Kommt der Fall vor, dass es genau einen Zweiteilungspunkt gibt?