Arithmetik elliptischer Kurven
Blatt 6 — 28.01.2015

Aufgabe 1.

(a) Zeigen Sie, dass für alle zu 561 teilerfremden Zahlen $a \in \mathbb{N}$ gilt:

$$a^{560} \equiv 1 \pmod{561}.$$

(b) Sei $n = 199843247$. Wir betrachten die elliptische Kurve

$$C \ : \ Y^2 = X^3 + 59X - 59.$$

Verwenden Sie ein Computer-Algebra-Paket Ihrer Wahl und bestimmen Sie mithilfe von Lenstras Faktorisierungsalgorithmus einen nicht-trivialen Teiler von n.

Tipp: Setze $P = (1, 1)$ und $k = 16296$.

Aufgabe 2.

Wir betrachten die Kurvenschar

$$C_d \ : \ Y^2 = X^3 + d.$$

Mit $C_d(\mathbb{Z})$ bezeichnen wir die Menge der ganzzahligen Punkte von C_d.

(a) Zeigen Sie, dass es zu jedem $N \in \mathbb{N}$ ein $d \in \mathbb{N}$ gibt mit $\#C_d(\mathbb{Z}) \geq N$.

(b) Zeigen Sie, dass es eine Konstante $\kappa > 0$ und eine Folge $1 \leq d_1 < d_2 < d_3 < \dots$ natürlicher Zahlen gibt mit $\#C_{d_i}(\mathbb{Z}) \geq \kappa \log\log d_i$.

Aufgabe 3.

Wir betrachten die elliptische Kurve

$$E \ : \ Y^2 = X^3 + AX + B$$

über $\mathbb{F}_q$ mit $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$.

(a) Bestimmen Sie die Automorphismengruppe $\mathrm{Aut}(E)$ von E.

(b) Über $\overline{\mathbb{F}}_q$ sind zwei elliptische Kurven genau dann isomorph, wenn sie die gleiche j-Invariante haben. Über $\mathbb{F}_q$ gibt es allerdings nicht-isomorphe elliptische Kurven mit gleicher j-Invariante. In diesem Aufgabenteil sei $j(E) \neq 0, 1728$.

Sei $d \in \mathbb{F}_q^*$. Wir definieren eine elliptische Kurve E_d über $\mathbb{F}_q$ durch

$$E_d \ : \ dY^2 = X^3 + AX + B.$$

Zeigen Sie:

1. $j(E) = j(E_d)$.
2. Für alle $d_1, d_2 \in \mathbb{F}_q^*$ mit $\frac{d_1}{d_2} \in (\mathbb{F}_q^*)^2$ gilt: $E_{d_1} \simeq E_{d_2}$.

E_d bezeichent man auch als (quadratischen) Twist von E. Nach 2. hängt die Isomorphieklasse von E_d nur von der Restklasse von d in $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ ab, also gibt es (bis auf Isomorphie) genau 2 Twists.

(Man kann zeigen: Im Fall $j = 1728$ gibt es (bis auf Isomorphie) genau $|\mathbb{F}_q^*/(\mathbb{F}_q^*)^4|$-viele Twists und im Fall $j = 0$ genau $|\mathbb{F}_q^*/(\mathbb{F}_q^*)^6|$-viele).

(c) Bestimmen Sie $\sum\limits_{E/\mathbb{F}_q} \frac{1}{\#\mathrm{Aut}(E)}$, wobei die Summe über alle $\mathbb{F}_q$-Isomorphieklassen elliptischer Kurven laufe.

Abgabe: Am kommenden Mittwoch, den 04.02.2015 in der Vorlesung. Downloads von Übungsblättern und Informationen zur Vorlesung unter

`http://www.uni-frankfurt.de/52095239/AEK-WS20145`
