Arithmetik elliptischer Kurven

Blatt 5 — 14.01.2015

Aufgabe 1.
Seien $p \neq 2$ eine Primzahl, $a, b, c, d \in \mathbb{F}_p$ mit $acd \neq 0$ und C die durch

$$C \ : \ aX^2 + bXY + cY^2 = dZ^2.$$

gegebene Kurve.

(a) Zeigen Sie, dass im Fall $b^2 \neq 4ac$ gilt: $\#C(\mathbb{F}_p) = p + 1$.

(b) Zeigen Sie, dass im Fall $b^2 = 4ac$ gilt: $\#C(\mathbb{F}_p) = 1$ oder $\#C(\mathbb{F}_p) = 2p + 1$. Geben Sie für jeden der beiden Fälle ein Beispiel an.

Aufgabe 2.
Seien p eine Primzahl mit $p \equiv 2 \mod 3$ und $c \in \mathbb{F}_p^*$. Zeigen Sie, dass für die Kurve

$$C \ : \ Y^2 = X^3 + c$$

gilt: $\#C(\mathbb{F}_p) = p + 1$.

Aufgabe 3.
Sei $b \in \mathbb{Z}$ mit $p^4 \nmid b$ für alle Primzahlen p. Ferner sei C die durch

$$C \ : \ Y^2 = X^3 + bX$$

gegebene elliptische Kurve. Mit $C(\mathbb{Q})_{\mathrm{Tor}} \subset C(\mathbb{Q})$ bezeichnen wir die Untergruppe der $\mathbb{Q}$-rationalen Torsionspunkte von C.

(a) Zeigen Sie: $\#C(\mathbb{Q})_{\mathrm{Tor}} \mid 4$.

(b) Zeigen Sie, dass gilt:

$$C(\mathbb{Q})_{\mathrm{Tor}} \simeq \begin{cases} \frac{\mathbb{Z}}{4\mathbb{Z}}, & \text{falls } b = 4, \\ \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}, & \text{falls } -b \text{ eine Quadratzahl ist} \\ \frac{\mathbb{Z}}{2\mathbb{Z}}, & \text{sonst.} \end{cases}$$

Abgabe: Am kommenden Mittwoch, den 21.01.2015 in der Vorlesung. Downloads von Übungsblättern und Informationen zur Vorlesung unter

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