Diekert/Weiß Sommersemester 2019

Konkrete Mathematik

Aufgabenblatt 3

Besprechung: Letzte Semesterwoche

1. In allgemeiner Form wird eine elliptische Kurve durch eine Gleichung vom folgenden Typ definiert.

$$(y'')^2 + cx''y'' + dy'' = (x'')^3 + e(x'')^2 + A''x'' + B'' \tag{1}$$

a) Zeigen Sie, dass sich (1) über Körpern der Charakteristik ungleich 2 durch Koordinatenwechsel auf die folgende Form bringen lässt.

$$y^2 = (x')^3 + e'(x')^2 + A'x' + B' \tag{2}$$

b) Zeigen Sie, dass sich (2) über Körpern der Charakteristik ungleich 3 durch eine Koordinatenverschiebung von x als Weierstrass-Gleichung $y^2 = x^3 + Ax + B$ schreiben lässt.

2. Sei $p \geq 3$ eine Primzahl und $y^2 = x^3 + Ax + B$ eine elliptische Kurve über $\mathbb{F}_p$. Für $z \in \mathbb{F}_p$ setzen wir

$$\left(\frac{z}{p}\right) = \begin{cases} 1 & \text{falls } z \neq 0 \text{ und } z \text{ ein Quadrat in } \mathbb{F}_p \text{ ist} \\ -1 & \text{falls } z \neq 0 \text{ und } z \text{ kein Quadrat in } \mathbb{F}_p \text{ ist} \\ 0 & \text{falls } z = 0 \end{cases}$$

Zeigen Sie $|E(\mathbb{Z}_p)| = p + \sum_{x=0}^{p-1} \left(\frac{x^3+Ax+B}{p}\right)$.

3. Sei $y^2 = x^3 + x + 6$ eine Kurve über $\mathbb{F}_{11}$. Zeigen Sie:

a) $y^2 = x^3 + x + 6$ ist eine glatte elliptische Kurve über $\mathbb{F}_{11}$.

b) $E(\mathbb{F}_{11}) \cup \mathcal{O}$ ist zyklisch.

c) Berechnen Sie $m \cdot (2,4) = \underbrace{(2,4) + \cdots + (2,4)}_{m \text{ mal}}$ für $m = 2, 3, 4$ in $E(\mathbb{F}_{11}) \cup \mathcal{O}$.

4. Sei $y^2 = x^3 + x$ eine Kurve über $\mathbb{F}_5$. Zeigen Sie:

a) $y^2 = x^3 + x$ ist eine glatte elliptische Kurve über $\mathbb{F}_5$.

b) $E(\mathbb{F}_5) \cup \mathcal{O}$ ist isomorph zur Klein'schen Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.