Arithmetik elliptischer Kurven
Blatt 3 — 26.11.2014

Aufgabe 1.

Gegeben seien die elliptische Kurve

$$E:\ Y^2 - Y = X^3 - X$$

und der Punkt $P = (0, 0)$ auf E. Bestimmen Sie kP für $2 \leq k \leq 6$.

Aufgabe 2.

Seien $p \geq 2$ eine Primzahl und C die durch

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

beschriebene Kubik. Bestimmen Sie alle Punkte endlicher Ordnung in $C(\mathbb{Q})$.

Aufgabe 3.

Gegeben sei die elliptische Kurve

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

Wir definieren rekursiv die m-Teilungspolynome $\psi_m \in \mathbb{Z}[A, B, X, Y]$ durch

$\psi_{-1} := -1, \qquad \psi_0 := 0, \qquad \psi_1 := 1, \qquad \psi_2 := 2Y,$

$\psi_3 := 3X^4 + 6AX^2 + 12BX - A^2,$

$\psi_4 := 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3),$

$\psi_{2m+1} := \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad$ für $m \geq 2,$

$2Y\psi_{2m} := \psi_m(\psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2) \quad$ für $m \geq 3.$

(a) Zeigen Sie, dass ψ_m für alle $m \geq 1$ ein Polynom ist.

Wir definieren ferner Polynome ϕ_m und ω_m durch

$$\phi_m := X\psi_m^2 - \psi_{m+1}\psi_{m-1}$$

und

$$4Y\omega_m := \psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2.$$

(b) Zeigen Sie:

1. Ist m ungerade, so sind ψ_m, ϕ_m und $(2Y)^{-1}\omega_m$ Polynome in $\mathbb{Z}[A, B, X, Y^2]$.
2. Ist m gerade, so sind $(4Y)^{-1}\psi_m, \phi_m$ und ω_m Polynome in $\mathbb{Z}[A, B, X, Y^2]$.

Wir ersetzen Y^2 durch $X^3 + AX + B$ und fassen diese Polynome als Elemente in $\mathbb{Z}[A, B, X]$ auf.

(c) Zeigen Sie, dass für ϕ_m und ψ_m (aufgefasst als Polynome in X) gilt:

$$\phi_m(X) = X^{m^2} + (\text{Terme kleineren Grades}),$$

$$\psi_m(X)^2 = m^2 X^{m^2-1} + (\text{Terme kleineren Grades}).$$

(d) Zeigen Sie, dass $\phi_m(X)$ und $\psi_m(X)^2$ teilerfremde Polynome in $K[X]$ sind.

(e) Sei $P = (x, y)$ ein Punkt der elliptischen Kurve $E: Y^2 = X^3 + aX + b$. Zeigen Sie:

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3} \right).$$

(f) Zeigen Sie, dass die m-Multiplikationsabbildung $[m] : E \to E$ Grad m^2 hat.

Abgabe: Am kommenden Mittwoch, den 03.12.2014 in der Vorlesung. Downloads von Übungsblättern und Informationen zur Vorlesung unter

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