ulm university universität
uulm

Prof. Dr. Irene Bouw
Christian Steck
Sommersemester 2014

Übungsblatt 5

Elliptische Kurven

Die Besprechung erfolgt am Mittwoch, dem 11.6.2014,
um 12:00 Uhr in He18 - E60.

Aufgabe 1 (*Divisoren auf* $\mathbb{P}^1$) (4+1)
Sei $C = \mathbb{P}^1$ und $D, D_1, D_2 \in \mathrm{Div}(C)$. Zeigen Sie:

(a) $\deg D = 0 \Leftrightarrow D = \mathrm{div}(f)$ für ein $f \in K(C)$,

(b) $D_1 \sim D_2 \Leftrightarrow \deg D_1 = \deg D_2$.

Aufgabe 2 (*Isomorphismen*) (2+2+3+3)
Sei K ein Körper mit $\mathrm{char}\, K \neq 2, 3$.

(a) Für $a, b \in K$ mit $\Delta := 4a^3 + 27b^2 \neq 0$ schreiben wir $E_{a,b}$ für die elliptische Kurve mit der affinen Gleichung $y^2 = x^3 + ax + b$. Bestimmen Sie alle $(a,b) \in K \times K$ mit $j(E_{a,b}) = 0$.

(b) Sei (a,b) wie in (a) mit $j(E_{a,b}) = 0$. Zeigen Sie:

$$(E_{a,b}, O) \xrightarrow{\sim} (E_{0,1}, O) \quad \Longleftrightarrow \quad \exists u \in K \,:\, u^6 = b.$$

Sei nun $K = \mathbb{F}_5$.

(c) Finden Sie die K-Isomorphieklassen von elliptischen Kurven $E_{a,b}$ mit $j(E_{a,b}) = 0$.

(d) Zeigen Sie, dass alle elliptischen Kurven aus (c) isomorph sind über $\mathbb{F}_{5^2}$.

Hinweis: Zeigen Sie die Existenz eines Elementes $\alpha \in \mathbb{F}_{5^2}$ mit $\alpha^6 = 2$.

Aufgabe 3 (*Verkürzte Weierstraß Form*) (2+3)
Wir arbeiten über dem Körper $K = \mathbb{C}$. Bringen Sie die folgenden Gleichungen auf verkürzte Weierstraß Form, d.h. in die Form $y^2 = x^3 + ax + b$.

(a) $y^2 + xy = x^3$

(b) $y^2 = \frac{1}{6}x(x+1)(2x+1)$