Übungen zur Vorlesung **Blatt 6**
Elliptische Kurven und Kryptographie 1.06.2015

PD Dr. K. Halupczok
Dipl.–Math. A. Juhas SoSe 2015

Abgabetermin: Montag, 8. Juni 2015, bis 12:15 Uhr in die Briefkästen

Aufgabe 1:

Sei k ein Körper und $E(k)$ eine elliptische Kurve, gegeben durch das Polynom $f(x,y) = \sum_{i+j\leq 3} a_{i,j}x^iy^j \in k[x,y]$. Die Tangente $\mathcal{G}$ im Wendepunkt $\mathcal{O} = [0:1:0]$ ist gegeben durch $Z = 0$.

(a) Geben Sie die Homogenisierung F_f an und finden Sie eine lineare Parametrisierung $G(t)$, $t \in k$, der Punkte auf $\mathcal{G}$ mit $G(0) = \mathcal{O}$.
(b) Berechnen Sie das Polynom $\Psi = F \circ G$.
(c) Nach Definition eines Wendepunktes hat Ψ eine dreifache Nullstelle in $t = 0$. Formulieren Sie die entsprechenden Bedingungen an die Koeffizienten von F.
(d) Substituieren Sie $x = -\frac{a_{0,2}}{a_{3,0}}u$ und $y = \frac{a_{0,2}}{a_{3,0}}v$ in F. Zeigen Sie, dass dies auf eine Kubik $S(u,v)$ in langer Weierstraßform führt.

Aufgabe 2:

Sei k ein Körper und $E, \widetilde{E} \subset \mathbb{P}^2(k)$ elliptische Kurven mit affinen Gleichungen $y^2 = F(x)$ bzw. $y^2 = \widetilde{F}(x)$, wobei $F, \widetilde{F} \in k[x]$ mit $\deg F = \deg \widetilde{F} = 3$ ohne mehrfache Nullstellen in $\overline{k}$ seien. Für diese Aufgabe heißen $E, \widetilde{E}$ isomorph über k, wenn sie sich via

$$x \mapsto \alpha x + \beta, \quad y \mapsto \gamma y, \qquad (\alpha, \gamma \in k^*, \beta \in k),$$

ineinander überführen lassen. Zeigen Sie:

(a) Über $\mathbb{C}$ ist jede elliptische Kurve $y^2 = x^3 + Ax + B$ isomorph zu einer Kurve der Gestalt

$$y^2 = x(x-1)(x-\lambda), \qquad \lambda \in \mathbb{C} \setminus \{0,1\}.$$

(b) Über $\mathbb{C}$ ist jede elliptische Kurve $y^2 = x^3 + B$ isomorph zu einer Kurve mit affiner Gleichung $y^2 = x^3 + 1$.

Aufgabe 3:

Wir betrachten die elliptische Kurve $E(\mathbb{F}_{11})$ mit affiner Gleichung

$$y^2 = x^3 - 3x + 5.$$

Bestimmen Sie alle Punkte von E.

Aufgabe 4:

Sei $\mathcal{C}$ eine Kurve über $\mathbb{C}$ mit affiner Gleichung $y^2 = x^3 + ax^2 + bx + c$. Berechnen Sie die Diskriminante $\Delta(\mathcal{C})$. Für welche c definiert die Gleichung $y^2 = x^3 - 4x^2 + c$ eine elliptische Kurve $E(\mathbb{C})$?