Übungen zur Vorlesung **Blatt 8**
Elliptische Kurven und Kryptographie 15.06.2015

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

Abgabetermin: Montag, 22. Juni 2015, bis 12:15 Uhr in die Briefkästen

Aufgabe 1:

Sei k ein Körper mit $\operatorname{char} k \neq 2, 3$ und P_1, P_2 endliche Punkte auf der ell. Kurve $E(k) : y^2 = x^3 + ax + b$, wobei P_1 in Jakobinischen Koordinaten und P_2 in affinen Koordinaten gegeben seien. Bestimmen Sie die Jakobinischen Koordinaten von $P_1 + P_2$.

Aufgabe 2:

Sei k ein Körper mit $\operatorname{char} k \neq 2, 3$ und $E(k)$ die elliptische Kurve mit affiner Gleichung $y^2 = f(x) := x^3 + ax + b$. Ein Punkt $P \in E$ heißt Zweiteilungspunkt, wenn $2P = \mathcal{O}$ gilt. Zeigen Sie: $E(k)$ hat einen, zwei oder vier Zweiteilungspunkte.

Aufgabe 3:

Seien k und $E(k)$ wie in Aufgabe 2. Zeigen Sie:

(a) Der affine Teil von E besitzt entweder keinen, zwei oder acht Wendepunkte.

(b) Welche Fälle können für $k = \mathbb{R}$ auftreten?

Aufgabe 4:

Seien $a_1, a_2, a_3, a_4 \in \mathbb{C}$ paarweise verschieden, $f(x) := \prod_{i=1}^{4}(x - a_i) \in \mathbb{C}[x]$ und $\mathcal{C}, \mathcal{C}' \subset \mathbb{P}^2(\mathbb{C})$ die Kurven mit den affinen Gleichungen $y^2 = f(x)$ bzw. $y^3 = f(x)$. Bestimmen Sie alle Singularitäten von $\mathcal{C}$ und $\mathcal{C}'$.