Übungen zur Vorlesung **Blatt 9**
Elliptische Kurven und Kryptographie 22.06.2015

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

Abgabetermin: Montag, 29. Juni 2015, bis 12:15 Uhr in die Briefkästen

Aufgabe 1:

Für eine elliptische Kurve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

seien $b_2 := a_1^2 + 4a_2$, $b_4 := a_1a_3 + 2a_4$ und $c_4 := b_2^2 - 24b_4$. Dann heißt die Zahl $j(E) := \frac{c_4^3}{\Delta}$ die j–Invariante der Kurve E, wobei Δ die Diskriminante von E bezeichnet.

Wir betrachten die elliptische Kurve $E_\lambda : y^2 = x(x-1)(x-\lambda)$ über $\mathbb{C}$, wobei $\lambda \neq 0, 1$.

(a) Bringen Sie E_λ in Weierstraßform und zeigen Sie

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

(b) Weisen Sie nach, dass es in den Fällen $a \neq 0, 12^3$ sechs verschiedene Werte $\lambda \in \mathbb{C} \setminus \{0, 1\}$ mit $j(E_\lambda) = a$ gibt. Zeigen Sie außerdem: Ist λ ein solcher Wert, so sind alle sechs Werte gegeben durch

$$\{\lambda, \frac{1}{\lambda}, \frac{\lambda - 1}{\lambda}, \frac{\lambda}{\lambda - 1}, \frac{1}{1 - \lambda}, 1 - \lambda\}.$$

(Hinweis: Gilt $j(E_\lambda) = j(E_\mu)$, lassen sich E_λ und E_μ via $x \mapsto u^2x + r$, $y \mapsto u^3y$, $u \in \mathbb{C}^*$, $r \in \mathbb{C}$ ineinander überführen).

(c) Zeigen Sie: Aus $j = 12^3$ folgt $\lambda \in \{-1, \frac{1}{2}, 2\}$ und aus $j = 0$ folgt $\lambda \in \{\frac{1+\sqrt{3}i}{2}, \frac{1-\sqrt{3}i}{2}\}$.

Aufgabe 2:

Wir betrachten die elliptische Kurve $E : y^2 = x^3 - 7x + 6$ über $\mathbb{F}_{17}$.

(a) Faktorisieren Sie das Polynom $x^3 - 7x + 6$ über $\mathbb{F}_{17}$.
(b) Bringen Sie E in die Form $y^2 = x(x-1)(x-\lambda)$ (vgl. dazu Blatt 6, Aufgabe 2 (a)).
(c) Natürlich wurde bei (b) eine bestimmte Reihenfolge der Nullstellen gewählt. Berechnen Sie λ für jede andere Permutation der Nullstellen.

Aufgabe 3:

Sei k ein Körper mit $\operatorname{char} k = 2$. Dann hat jede elliptische Kurve $E(k)$ die Gestalt $y^2 + xy = x^3 + a_2x^2 + a_6$ oder $y^2 + a_3y = x^3 + a_4x + a_6$. Wir betrachten die Untergruppe $E[2]$ von E (zur Def. vgl. Aufgabe 4). Zeigen Sie mithilfe der expliziten Formel: Es gilt $E[2] \simeq \mathbb{Z}_2$ oder $E[2] = \{\mathcal{O}\}$.

Aufgabe 4:

Sei G eine (endliche) additive abelsche Gruppe und $G[n] := \{g \in G : \operatorname{ord}(g) \mid n\}$. Zeigen Sie: Gilt $n = ab$ mit $\operatorname{ggT}(a, b) = 1$, so ist $G[n] \simeq G[a] \times G[b]$.