Wolfgang K. Seiler
Tel. 2515

A5, C201

19. Mai 2017

8. Übungsblatt Elliptische Kurven

Aufgabe 1: *(6 Punkte)*

a) Wie viele Isomorphietypen abelscher Gruppen der Ordnung 360 gibt es?

b) Geben Sie für jeden dieser Typen eine Darstellung an als Produkt von möglichst vielen zyklischen Gruppen und eine als Produkt von möglichst wenigen!

Aufgabe 2: *(5 Punkte)*

Zeigen Sie, daß das Polynom $3x^4 + 6ax^2 + 12bx - a^2 = 0$ zur elliptischen Kurve

$$E : y^2 = x^3 + ax + b$$

auch in den beiden Fällen $a = 0$ und $b = 0$ keine mehrfachen Nullstellen hat!

Aufgabe 3: *(4 Punkte)*

Für die elliptische Kurve E über dem endlichen Körper k sei $E(k) \cong \mathbb{Z}/2 \times \mathbb{Z}/102$. Wie viele Punkte aus $E[2]$ *bzw.* $E[3]$ liegen in $E(k)$?

Aufgabe 4: *(5 Punkte)*

a) $E_1, \ldots, E_r$ seien elliptische Kurven über dem endlichen Körper k mit $\operatorname{char} k \neq 2, 3$. Was wissen Sie über die Gruppe

$$\left\{ (P_1, \ldots, P_r) \in E_1(\bar{k}) \times \cdots \times E_r(\bar{k}) \;\middle|\; 2 \cdot (P_1, \ldots, P_r) = (O, \ldots, O) \right\} ?$$

b) Auch E sei eine elliptische Kurve über k, und $\varphi\colon E(\bar{k}) \to \bar{k}^\times$ sei ein Gruppenhomomorphismus. Zeigen Sie, daß φ nicht injektiv sein kann!