Diophantische Gleichungen: Blatt 11

Stefan Wewers
Michael Eskin

Abgabe: 12.01.2015, vor der Übung

Hinweis zur Abgabe der Übungsblätter: Die Übungsaufgaben sollen in Dreiergruppen abgegeben werden!

Aufgabe 1 *(5+5 Punkte)*
Sei E die elliptische Kurve definiert über $\mathbb{F}_5$ mit der affinen Gleichung

$$Y^2 = X^3 + 1.$$

(a) Bestimmen Sie alle $\mathbb{F}_5$-rationalen Punkte von E.

(b) Zeigen Sie: $E(\mathbb{F}_5)$ ist eine zyklische Gruppe. Geben Sie dazu einen Erzeuger P an, sodass $E(\mathbb{F}_5) = \langle P \rangle$.

Aufgabe 2 *(2+3+3+2 Punkte)*
Sei $\Lambda = \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}} \subset \mathbb{C}$ ein Gitter (d.h. ω_1, ω_2 sind linear unabhängig über $\mathbb{R}$) und sei

$$E := \mathbb{C}/\Lambda.$$

Wir betrachten E als abelsche Gruppe bezüglich der Addition. Zeigen Sie:

(a) $E[n] := \{P \in E \mid n \cdot P = 0\}$ ist eine Untergruppe von E.

Anmerkung : Man nennt $E[n]$ die *Gruppe der n-Torsionspunkte.*

(b) $P := \{t_1\omega_1 + t_2\omega_2 \mid t_i \in [0, 1)\}$ ist ein Repräsentantensystem von E.

(c) Für $n \geq 2$ gibt zwei Elemente $P_1, P_2 \in E$ sodass die Abbildung

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to E[n], \quad (\bar{a}_1, \bar{a}_2) \mapsto a_1 \cdot P_1 + a_2 \cdot P_2$$

ein Isomorphismus ist.

(d) $E[n]$ ist nicht zyklisch.