Eberhard Karls Universität Tübingen Wintersemester 2018/19
Fachbereich Mathematik
PD Dr. Jörg Zintl

Elliptische Funktionen und elliptische Kurven

Übungsaufgaben zum 7. Tutorium am 04.12.2018

Aufgabe 25
Sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen. Bestimmen Sie die Anzahl der Punkte in $\mathbb{P}^n(\mathbb{F}_q)$.

Aufgabe 26
Sei $F \in \mathbb{Z}[X,Y,Z]$ mit $F(X,Y,Z) := Y^2Z - X^3 - Z^3$, und $C := V(F) \subset \mathbb{P}^2$ die dadurch definierte elliptische Kurve in Weierstraß-Normalform. Sei $F_5 := F \mod 5 \in \mathbb{F}_5[X,Y,Z]$, und $C_5 := V(F_5)$ die dadurch definierte Kurve über $\mathbb{F}_5$. Zeigen Sie: $(C_5, (0:1:0))$ ist eine elliptische Kurve, und bestimmen Sie die Gruppentafel.

Aufgabe 27
Sei p eine Primzahl. Zeigen Sie:

a) Sei $m := \max\{\mathrm{ord}(a) : a \in \mathbb{F}_p^*\}$. Dann gilt für alle $a \in \mathbb{F}_p^*$ stets $\mathrm{ord}(a) | m$.

b) Die Einheitengruppe $(\mathbb{F}_p^*, \cdot)$ ist zyklisch.

c) Für $p \not\equiv 1 \mod 3$ ist die Abbildung $\varphi : \mathbb{F}_p \to \mathbb{F}_p$ mit $\varphi(a) = a^3$ bijektiv.

Aufgabe 28
Sei $F \in \mathbb{Z}[X,Y,Z]$ mit $F(X,Y,Z) := Y^2Z + YZ^2 - X^3$, und $C := V(F) \subset \mathbb{P}^2$ die dadurch definierte projektive ebene Kurve. Sei $\mathcal{O} := (0:1:0) \in \mathbb{P}^2$.

a) Ist $(C, \mathcal{O})$ eine elliptische Kurve?

b) Bestimmen Sie alle Primzahlen p, für die die Reduktion $F_p := F \mod p \in \mathbb{F}_p[X,Y,Z]$ eine glatte Kurve C_p über $\mathbb{F}_p$ definiert.

c) Zeigen Sie: Durch die projektive Transformation $\varphi : \mathbb{P}^2 \to \mathbb{P}^2$ mit $\varphi(X:Y:Z) := (4X : 8Y + 4Z : Z)$ wird die elliptische Kurve $(C, \mathcal{O})$ in eine elliptische Kurve $C' := \varphi(C)$ in Weierstraß-Normalform transformiert.

d) Bestimmen Sie alle Primzahlen p, für die die Reduktion von C' modulo p eine glatte Kurve C'_p über $\mathbb{F}_p$ definiert.

Keine Abgabe, nur zur Vorbereitung auf das Tutorium!