Arithmetik Elliptischer Kurven

Universität Frankfurt
Institut für Mathematik
Marius Leonhardt

Warm-Up Quiz
Wintersemester 2024/25
15.01.2025

Teamname:

Teil 1: Elliptische Kurven (5×2 Punkte)
Welche der folgenden Kurven $E \subset \mathbb{P}^2$, definiert über dem Körper K, zusammen mit dem angegebenen Punkt $O \in E(K)$, sind Elliptische Kurven?

(a) $(K = \mathbb{Q})$ $E : y^2 = x^3 - 4x^2 + 3x$, $O = [0 : 1 : 0]$.

(b) $(K = \mathbb{F}_2)$ $E : y^2 = x^3 - 4x^2 + 3x$, $O = [0 : 1 : 0]$.

(c) $(K = \mathbb{F}_5)$ $E : y^2 = x^3 - 4x^2 + 3x$, $O = [0 : 1 : 0]$.

(d) $(K = \mathbb{Q})$ $E\colon y - 3xy = x^3 - 4x^2y$, $O = (0, 0)$.

(e) $(K = \mathbb{Q})$ Für welche $n \in \mathbb{N}$ ist $E\colon X^n + Y^n = Z^n$, $O = [1 : 0 : 1]$ eine Elliptische Kurve?

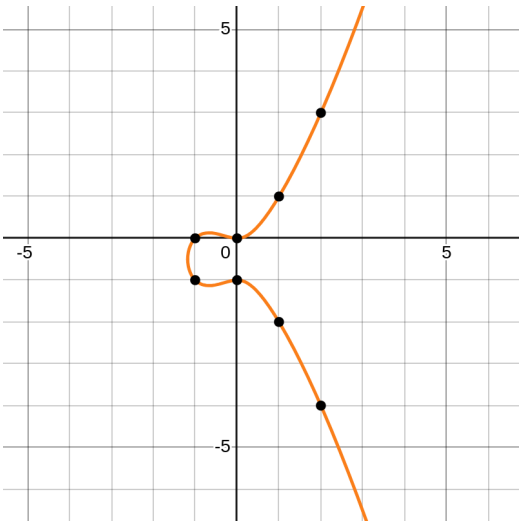
Teil 2: Gruppengesetz (10 Punkte)
Auf der Elliptische Kurve E über $\mathbb{Q}$ gegeben durch die Weierstraß-Gleichung

$$E\colon y^2 + y = x^3 + x^2$$

liegen die Punkte $A_1 = (-1, 0)$, $A_2 = (-1, -1)$, $A_3 = (0, 0)$, $A_4 = (0, -1)$, $A_5 = (1, 1)$, $A_6 = (1, -2)$, $A_7 = (2, 3)$, $A_8 = (2, -4)$, $A_9 = (21, 98)$ und $A_{10} = (21, -99)$. Finde einen Punkt $P \in \{A_1, \dots, A_{10}\}$ und für jedes $i \in \{1, \dots, 10\}$ ein $k_i \in \mathbb{Z}$ mit

$$A_i = k_i P, \quad i \in \{1, \dots, 10\}.$$

Wie viele solche P gibt es?



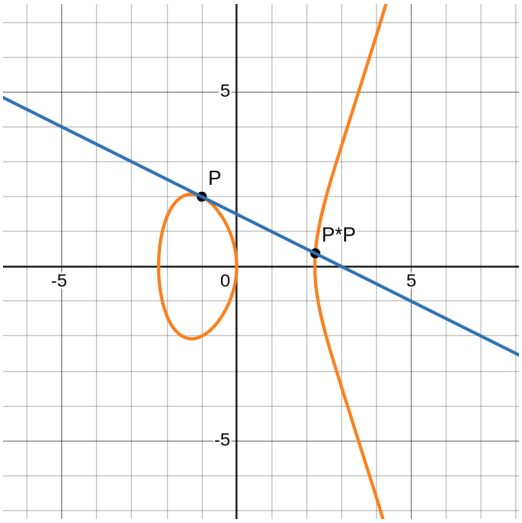
Teil 3: Naives Gruppengesetz (4×2 Punkte)
Es sei $E \subset \mathbb{P}^2$ eine Elliptische Kurve in Weierstraß-Form über dem Körper K. Wir definieren $P * Q$ für $P, Q \in E(K)$ als den dritten Schnittpunkt der eindeutigen Gerade durch P und Q mit E (gezählt mit Vielfachheit, also gilt $P = Q$, so nehmen wir die Tangente etc.). Welche der Gruppenaxiome gelten für die Verknüpfung $*$?

(a) Wohldefiniertheit, d.h. $P * Q$ ist dadurch eindeutig bestimmt und liegt in $E(K)$?

(b) Assoziativität?

(c) Kommutativität?

(d) Existenz eines neutralen Elementes?



Teil 4: Geraden (5×2 Punkte)
Es sei $E \subset \mathbb{P}^2$ eine Elliptische Kurve in Weierstraß-Form über dem algebraisch abgeschlossenen Körper K und $P, Q, R, S \in E(K)$ Punkte auf E. Wahr oder Falsch?

(a) Gilt $P + Q = O$, so gibt es eine Gerade $L \subset \mathbb{P}^2$ durch P und Q.

(b) Gilt $P + Q + R = O$, so gibt es eine Gerade $L \subset \mathbb{P}^2$ durch P, Q und R.

(c) Gilt $P + Q + R + S = O$, so gibt es eine Gerade $L \subset \mathbb{P}^2$ durch P, Q, R und S.

(d) Gilt $P + Q + R + S = O$, so gibt es keine Gerade $L \subset \mathbb{P}^2$ durch P, Q, R und S.

(e) Gilt $P + Q - R - S = O$, so ist $(P) + (Q) - (R) - (S) \in \mathrm{Div}(E)$ ein Hauptdivisor.

Teil 5: Elliptische Kurven über endlichen Körpern ($2 \times 4 + 2$ Punkte)
Es sei

$$E \colon y^2 = x^3 + x + 1.$$

Bestimme $\#E(\mathbb{F}_p)$ und die Gruppenstruktur von $E(\mathbb{F}_p)$ für $p = 3$ und $p = 7$. Was passiert für $p = 2$?