ulm university universität
uulm

Prof. Dr. Irene Bouw
Christian Steck
Sommersemester 2014

Übungsblatt 2

Elliptische Kurven

Die Besprechung erfolgt am Mittwoch, dem 14.5.2014,
um 12:00 Uhr in He18 - E60.

Aufgabe 1 (2+4+4)

Sei p eine Primzahl und $\left(\frac{\cdot}{p}\right)$ das zugehörige Legendre Symbol.

(a) Zeigen Sie, dass für $a \in \mathbb{F}_p$ gilt: $\#\left\{y \in \mathbb{F}_p \,;\, y^2 = a\right\} = 1 + \left(\frac{a}{p}\right)$.

(b) Sei $E/\mathbb{F}_7$ die projektive Kurve gegeben durch die affine Gleichung $y^2 = x^3 + 3x + 1$. Bestimmen Sie alle Punkte von $E(\mathbb{F}_7)$.

(c) Ist $E(\mathbb{F}_7)$ eine zyklische Gruppe?

Aufgabe 2 (2+3)

Von Blatt 1 - Aufgabe 2 kennen wir bereits die Kurve $E/\mathbb{C}$ gegeben durch die affine Gleichung $y^2 = x^3 + 1$ und die Punkte $P = (2,3)$, $Q = (0,-1)$ in $E(\mathbb{Q})$.

(a) Zeigen Sie: $2P = -Q$.

(b) Zeigen Sie $\mathrm{ord}(Q) = 3$ und bestimmen Sie auch die Ordnung von P.

Aufgabe 3 (3+3+4)

Wir betrachten die Gerade $G : X - Y = 0$ in $\mathbb{P}_2(\mathbb{C})$. Berechnen Sie jeweils alle Schnittpunkte und die zugehörige Schnittmultiplizität von G mit den Kurven C_i gegeben durch die folgenden affinen Gleichungen.

(a) $C_1 : X + Y = 0$

(b) $C_2 : (X + Y)^2 = X - Y + 1$

(c) $C_3 : X + Y = (X - Y)^4$