Elliptische Kurven & Kryptologie Serie 9

Punkte endlicher Ordnung, Diskriminante, Ring R_p Abgabe: 9. Mai

1. Sei $f(x) = x^3 + ax^2 + bx + c$ mit $a, b, c \in \mathbb{Z}$ und sei $C_f : y^2 = f(x)$ eine nicht-singuläre Kurve. Ferner sei $P = (x, y)$ ein Punkt auf C_f, welcher $y \neq 0$ erfi¿½llt. Die x-Koordinate von $2P$ ist

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2} =: \frac{\phi(x)}{4f(x)}\,.$$

(a) Zeige, dass es Polynome $F(x)$ (vom Grad 3) und $\Phi(x)$ (vom Grad 2) in $\mathbb{Z}[x]$ gibt, so dass

$$F(x)f(x) + \Phi(x)\phi(x) = D_f\,,$$

wobei D_f die Diskriminante von f ist.

(b) Zeige: Ist $P = (x, y) \in C_f$ ein rationaler Punkt von endlicher Ordnung, dann ist entweder $2P = \mathcal{O}$ oder $y^2 \mid D_f$.

2. (a) Sei $f(x) = x^2 + ax + b = (x - \alpha_1)(x - \alpha_2)$ ein quadratisches Polynom mit der angegebenen Faktorisierung. Beweise:

$$(\alpha_1 - \alpha_2)^2 = a^2 - 4b.$$

(b) Sei $f(x) = x^3 + ax^2 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ ein cubisches Polynom mit der angegebenen Faktorisierung. Beweise:

$$(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

(c) Sei $f(x) = x^n + a_1x^{n-1} + \ldots + a_n = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$ ein Polynom mit der angegebenen Faktorisierung. Die *Diskriminante* von f ist definiert als

$$D_f = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\alpha_i - \alpha_j)^2.$$

Offenbar ist $D_f = 0$ genau dann, wenn f eine mehrfache Nullstelle besitzt. Beweise, dass D_f ein Polynom in den Koeffizienten $a_1, \ldots, a_n$ von f ist.

3. Sei $p \geq 3$ eine Primzahl und sei $C_p : y^2 = x^3 + px$.

Finde alle Punkte endlicher Ordnung der elliptischen Kurve $E_p = \big(C_p(\mathbb{Q}), \mathcal{O}, +\big)$.

4. Finde alle Punkte endlicher Ordung der elliptischen Kurven $E[0, 0, -2]$ und $E[0, 1, 0]$.

5. Sei p eine Primzahl und sei R wie in der Vorlesung definiert:

$$R := R_p := \{\tfrac{a}{b} \mid \mathrm{ggT}(a,b) = 1,\ p \nmid b\}$$

(a) Beweise, dass R ein Unterring von $\mathbb{Q}$ ist.

(b) Beweise, dass $pR \subseteq R$ ein maximales Ideal ist und beschreibe den Körper R/pR.

(c) Beweise, dass R^* (die Gruppe der Einheiten von R) die rationalen Zahlen $\frac{a}{b}$ sind, welche $p \nmid ab$ erfüllen.

(d) Beweise, dass R ein faktorieller Ring ist.

(e) Beschreibe alle Ideale von R. Benutze diese Beschreibung, um zu zeigen, dass pR das einzige maximale Ideal in R ist. (Ein Ring, welcher genau ein maximales Ideal enthält, heisst *lokaler Ring*.)