

Zahlentheorie und Kryptologie, WS 2008/09

Michael Hortmann

Aufgabenblatt 10

Eine elliptische Kurve über einem Körper K mit $\text{char } K \neq 2, 3$ ist gegeben durch die Gleichung $y^2 = x^3 + ax + b$, $a, b \in K$, $4a^3 + 27b^2 \neq 0$. Die zugehörige kommutative Gruppe besteht aus der Menge $\{0\} \cup \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\}$. Dabei ist 0 das neutrale Element. Die Gruppenoperationen sind durch folgende Formeln gegeben:

Sind $P, Q \neq 0$ Gruppenelemente mit $P = (x_1, y_1), Q = (x_2, y_2)$, und

1) $x_1 \neq x_2$, so besitzt $P+Q=R$ die Form $R = (x_3, y_3)$, und mit $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ ist $x_3 = \alpha^2 - x_1 - x_2$, $y_3 = \alpha(x_1 - x_3) - y_1$.

2) $x_1 = x_2$ und

a) $y_1 = -y_2$, so ist $P+Q=0$ bzw. $Q=-P$. Dies umfaßt den Fall $y_1 = y_2 = 0$.

b) $y_1 = y_2 \neq 0$, d.h. $P=Q$, so besitzt $P+Q=R$ die Form $R = (x_3, y_3)$, und mit $\alpha = \frac{3x_1 + a}{2y_1}$ gilt $x_3 = \alpha^2 - x_1 - x_2$, $y_3 = \alpha(x_1 - x_3) - y_1$.

Zum Rechnen mit Elliptischen Kurven in Pari muß man die Gruppenoperationen nicht selbst neu programmieren. Man kann mit dem Aufruf `C=ellinit([0,0,0,a,b])` eine elliptische Kurve zur Gleichung $y^2 = x^3 + ax + b$ kreieren. Dabei hängt es vom Datentyp von a, b ab, über welchem Körper gerechnet wird. Durch `C=ellinit([0,0,0,Mod(2,7),Mod(3,7)])` wird z.B. die in der Vorlesung behandelte Kurve über \mathbb{Z}_7 definiert, die Abfrage `ellisoncurve(C,[Mod(6,7),Mod(0,7)])` bestätigt, daß der Punkt $P=(6,0) \in \mathbb{Z}_7 \times \mathbb{Z}_7$ auf dieser Kurve liegt, und die Funktionen `elladd, ellsub, ellpow` realisieren die Gruppenoperationen, vgl. auch die Pari-Dokumentation.

Aufgabe 1. Durch $y^2 = x^3 + ax + b$ sei eine elliptische Kurve über \mathbb{Z}_p gegeben, und $x^3 + ax + b$ besitze in \mathbb{Z}_p drei Nullstellen. Man zeige, daß die zugehörige Gruppe nicht zyklisch ist und bestätige dies durch Ausrechnen der Gruppentafel anhand einer konkreten Kurve über \mathbb{Z}_7 .

Aufgabe 2. Wieviele Punkte der Ordnung n besitzt eine elliptische Kurve über \mathbb{C} ?

Aufgabe 3. Man wähle eine konkrete elliptische Kurve über \mathbb{Z}_5 . Ihre Punktezahl N_1 läßt sich konkret zählen. Man setze $p=5$ und berechne die komplexe Zahl α , für die die Gleichungen $N_1 = 1 + p - \alpha - \bar{\alpha}$, $\alpha \bar{\alpha} = p$.

Sei $K = \mathbb{Z}_5[X]/\langle f \rangle$ ein Oberkörper von \mathbb{Z}_5 . Die eben gewählte elliptische Kurve läßt sich auch als Kurve über K auffassen, ihre Punktezahl sei N_K . Ist $r = \text{grad } f$, so gilt die Formel

$N_K = 1 + p^r - \alpha^r - \bar{\alpha}^r$, und man kann daher N_K konkret berechnen.

Man finde nun ein irreduzibles Polynom $f \in \mathbb{Z}_5[X]$ von so hohem Grad, daß $N_K \geq 10^{50}$.
Für einen zufälligen Punkt P auf der Kurve über K rechne man mit Pari nach, daß $N_K P = 0$.
(D.h. man wähle $x \in K$ zufällig und berechne y . Dazu muß man offenbar in K Quadratwurzeln ziehen können. Man verallgemeinere dazu den in der Vorlesung präsentierten Algorithmus zum Wurzelziehen in \mathbb{Z}_p , vgl. Algorithmus 3.39 und Bemerkung 3.41 aus HAC)