

Aufgaben zur Zahlentheorie und Kryptologie WS 2004/05, Blatt 3

Michael Hortmann

Ist K ein Körper mit $\text{char } K \neq 2, 3$, $x^3 + ax + b \in K[x]$ ein Polynom dritten Grades ohne mehrfache Nullstellen, so ist eine elliptische Kurve über K gegeben durch

$$\mathcal{C} = \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$$

Die folgenden Additionsregeln wurden abgeleitet durch die Forderung, daß drei Punkte auf der Kurve, die zudem auf einer Geraden liegen, die Summe ∞ besitzen sollen. Mit dieser Verknüpfung erhält \mathcal{C} eine abelsche Gruppenstruktur, wobei das neutrale Element der „unendlich ferne Punkt“ ∞ ist.

Ist $P \in \mathcal{C}$, $P = (x, y)$, ergibt sich $\ominus P = (x, -y)$ und somit $(x, y) \oplus (x, -y) = \infty$.

Sind $(x_1, y_1), (x_2, y_2) \in \mathcal{C}$, so setzt man zunächst $\alpha = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{falls } x_2 \neq x_1 \\ \frac{3x_1^2 + a}{2y_1}, & \text{falls } x_2 = x_1, y_1 \neq -y_2 \end{cases}$

und erhält $(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$ mit $\begin{cases} x_3 = \alpha^2 - x_1 - x_2 \\ y_3 = -y_1 + \alpha^2(x_1 - x_3) \end{cases}$.

Aufgabe 1

a) Ist $\text{char } K = 3$, so benutze man für eine elliptische Kurve die Gleichung $y^2 = x^3 + ax^2 + bx + c$ und bestimme für diesen Fall ein Additionsgesetz nach obigem Schema, daß nämlich die Summe dreier auf einer Geraden liegenden Punkte Null sein soll.

b) Dieselbe Aufgabe¹ für $\text{char } K = 2$ und Kurven mit der Gleichung $y^2 + xy = x^3 + ax^2 + b$ oder Kurven mit der Gleichung $y^2 + y = x^3 + ax + b$.

Aufgabe 2

Studieren und üben Sie die Funktionen in Pari zum Rechnen mit Elliptischen Kurven, also `ellinit`, `elladd`, `ellsub`, `ellmult`, `ellisoncurve`, `ellorder`, `ellordinate`. Studieren Sie die Kapitel über Elliptische Kurven in den Büchern von Koblitz, *A Course in Number Theory and Cryptography*, *Algebraic Aspects of Cryptography*.

¹Die Glattheitsbedingung, die oben über das Verbot mehrfacher Nullstellen in der rechten Seite formuliert war, lautet allgemein für eine durch die Gleichung $F(x, y) = 0$ gegebene Kurve

$\forall x, y \in K: dF(x, y) = \frac{\partial F}{\partial x} dx + \frac{\partial F}{\partial y} dy \neq 0$, d.h. es darf keine gemeinsamen Nullstellen von $F, \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ geben. Dies macht auch im Falle $\text{char } K = 2$ Sinn.

Aufgabe 3

- a) Man gebe ein Beispiel einer elliptischen Kurve über \mathbb{R} , die die genau 2 Punkte der Ordnung 2 besitzt, und ein weiteres Beispiel mit genau 4 Punkten der Ordnung 2.
- b) Sei $P \neq \infty$ ein Punkt auf einer elliptischen Kurve über \mathbb{R} . Welches sind die geometrischen Bedingungen dafür, daß P die Ordnung 2,3 oder 4 besitzt.

Aufgabe 4

Berechnen Sie die (in diesen Fällen endliche) Ordnung der folgenden Punkte auf elliptischen Kurven über \mathbb{Q} :

- a) $P=(0,16)$ auf $y^2=x^3+256$
- b) $P=(\frac{1}{2}, \frac{1}{2})$ auf $y^2=x^3+\frac{1}{4}x$
- c) $P=(3,8)$ auf $y^2=x^3-43x+166$
- d) $P=(0,0)$ auf $y^2+y=x^3-x^2$. (Diese Kurve läßt sich in der üblichen Form schreiben, wenn man die Substitutionen $y \rightarrow y-\frac{1}{2}, x \rightarrow x+\frac{1}{3}$ vornimmt.)

Aufgabe 5

- a) Man berechne die Kettenbruchentwicklungen der folgenden rationalen Zahlen: $\frac{45}{89}, \frac{55}{89}, 1.13$

b) Sei $a \in \mathbb{N}$ und $x = a + \frac{1}{a + \frac{1}{a + \frac{1}{a + \dots}}}$. Bestimmen Sie x !

- c) Zeigen Sie: Wenn $a=1$ in a), dann ist x die Goldene Schnitt Zahl $\frac{\sqrt{5}+1}{2}$ und die Zähler und Nenner der approximierenden Brüche $1, 1+\frac{1}{1}, 1+\frac{1}{1+\frac{1}{1}}, \dots$ sind die Fibonacci-Zahlen.

- d) Man rate ein Muster in der Kettenbruchentwicklung von e !