Kryptologie, SS03 Aufgabenblatt 6

Eine elliptische Kurve über dem Körper K, $\operatorname{char} K \neq 2,3$ [1] ist gegeben durch eine Gleichung $y^2 = x^3 + ax + b;\ a,b \in K,\ 4a^3 + 27b^2 \neq 0$, als Menge $\left\{(x,y) \in K \times K \,\middle|\, y^2 = x^3 + ax + b\right\} \cup \{\infty\}$
Auf dieser Menge ist eine Gruppenoperation gegeben, mit ∞ als neutralem Element, durch folgende Formeln:

$$x_1 \neq x_2:\ \ (x_1,y_1) \oplus (x_2,y_2) := (x_3,y_3);\ \alpha := \frac{y_2 - y_1}{x_2 - x_1},\ x_3 := \alpha^2 - x_1 - x_2,\ y_3 := \alpha(x_1 - x_3) - y_1$$

$$y \neq 0:\ \ 2(x,y) := (x,y) \oplus (x,y) := (x_3,y_3),\ \alpha := \frac{3x^2 + a}{2y},\ x_3 := \alpha^2 - x - x_2,\ y_3 := \alpha(x - x_3) - y$$

$$(x,y) \oplus (x,-y) := \infty$$

Diese Formeln sind so konstruiert, daß i.a. die Summe dreier auf einer Geraden in $K \times K$ liegenden Punkte das neutrale Element ergibt.

Aufgabe 1

a) Über $K := \mathbb{Z}_7$ betrachte man die Gleichung $y^2 = x^3 + x + 1$. Man berechne per Hand alle Punkte der zugehörigen elliptischen Kurve und stelle die zugehörige Gruppentafel auf, d.h. eine Tabelle der Ergebnisse der „Addition“ sämtlicher Elemente.

b) Betrachten Sie dieselbe Gleichung wie in a), diesmal über $K := \mathbb{Z}_{1019}$. Mit dem Befehl E=ellinit([Mod(0,1019),Mod(0,1019),Mod(0,1019),Mod(1,1019),Mod(1,1019)]) initialisieren Sie in Pari die entsprechende elliptische Kurve. Die Elementezahl dieser Kurve, also die Gruppenordnung, hat den Betrag „1020-ellap(*E*,1019)“ (siehe Pari User-Manual). Berechnen Sie per Hand einen Punkt *P*=(*x*,*y*) der Kurve und berechnen Sie die Ordnung dieses Punktes, die ja ein Teiler der Gruppenordnung sein muß. Die Addition auf der Gruppe erhalten Sie mit der Pari-Funktion $\operatorname{ellad}(E, z_1, z_2)$; offenbar müssen Sie selbst eine darauf aufsetzende Funktion $\operatorname{ellmult}(E, n, z)$ schreiben, die einen Punkt *z* *n*-mal zu sich selbst addiert. Beachten Sie noch, daß der Punkt ∞, also das Nullement der Gruppe, in Pari durch den Vektor [0] repräsentiert wird, während die üblichen Punkte auf der Kurve durch ihre „Koordinaten“ [x,y] repräsentiert werden, wobei diese Koordinaten selbst die Form Mod(*k*,1019) haben.

c) Sonderaufgabe: Versuchen Sie, in einem Computeralgebrasystem wie Maple die Gültigkeit des Assoziativgesetzes für die Gruppenoperation einer elliptischen Kurve durch direkte Rechnung nachzuweisen. Da Sie nur symbolisch rechnen, berücksichtigen Sie nur die erste Variante der Additionsformel, also diejenige, bei der sich die ersten Koordinaten der aller beteiligten Punkte unterscheiden.

---

[1] char K ist die kleinste Zahl $k \in \mathbb{N}$ mit $\underbrace{1+\ldots+1}_{k\text{-mal}} = 0$. Falls es keine solche Zahl gibt, setzt man char K = 0.

Ist char K $\neq 0$, so zeigt man leicht, daß char K eine Primzahl ist. Für einen Körper mit p^n Elementen ist char K = *p*.

Aufgabe 2

a) Finden Sie durch geeignete Computerexperimente einen „Rückkopplungsvektor“ $(a_6 \ldots a_0) \in \mathbb{Z}_2^7$, so daß die durch die Vorschrift $x_{k+1} := \sum_{i=0}^{6} a_i x_{k-6+i}$, ausgehend von einem beliebigen Startvektor $(x_0, \ldots, x_6) \neq 0$ definierte Bitfolge (x_i) die maximal mögliche Periode 127 besitzt.

b) Man betrachte den Rückkopplungsvektor $(0,0,\ldots,0,1,1) \in \mathbb{Z}_2^{127}$. Wir werden später zeigen, daß die dadurch definierte Schieberegisterfolge die maximal mögliche Periode $2^{127} - 1$ besitzt. Schreiben Sie ein Computerprogramm, welches möglichst schnell (darauf soll es hier ankommen!), ausgehend vom Vektor $(x_{126}, x_{125}, \ldots, x_1, x_0) = (0,0,\ldots,0,1) \in \mathbb{Z}_2^{127}$ die ersten 100000 Werte der Schieberegisterfolge berechnet und dann den Vektor $(x_{100000}, x_{99999}, \ldots, x_{99874})$ ausgibt.