Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 3

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen						**Gruppe**	**Tutor**
1	2a	b	c	d	e	**Summe**	**bearbeitet**
1	1	1	1	1	1	5 Punkte=100%	

Aufgabe 1. Sei $f = X^3 + aX + b$ ein Polynom in $K[X]$, K ein Körper mit char $K \neq 2,3$.
Zeigen Sie ohne Benutzung von Differentialrechnung, daß f genau dann keine mehrfache Nullstelle in K besitzt, wenn in K gilt: $4a^3 + 27b^2 \neq 0$.

Eine elliptische Kurve über einem Körper K mit char $K \neq 2,3$ ist gegeben durch eine Gleichung $y^2 = x^3 + ax + b$, wobei $a, b \in K$ und $4a^3 + 27b^2 \neq 0$ Die zugehörige kommutative Gruppe besteht aus der Menge $\{0\} \cup \left\{(x, y) \in K \times K \;\middle|\; y^2 = x^3 + a\,x + b\right\}$. Dabei ist 0 ein zusätzliches Element, welches bezüglich der unten definierten Gruppenoperation als neutrales Element fungiert.
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 $R = (x_3, y_3)$. Dazu berechnet man $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ und setzt $x_3 = \alpha^2 - x_1 - x_2$, $y_3 = \alpha(x_1 - x_3) - y_1$.

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 $R = (x_3, y_3)$; diesmal berechnet man $\alpha = \frac{3x_1 + a}{2y_1}$ und setzt $x_3 = \alpha^2 - x_1 - x_2$, $y_3 = \alpha(x_1 - x_3) - y_1$.

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 $y^2 = x^3 + a\,x + b$ kreieren. Dabei hängt es vom Datentyp von a, b ab, über welchem Körper gerechnet wird. Durch `C=ellinit([0,0,0,Mod(2,11),Mod(5,11)])` wird z.B. eine Kurve über $\mathbb{Z}_{11}$ definiert.

Die Abfrage `ellisoncurve(C,[Mod(4,7),Mod(0,11)])` bestätigt, daß der Punkt $P=(4,0)\in\mathbb{Z}_{11}\times\mathbb{Z}_{11}$ auf dieser Kurve liegt, und die Funktionen `elladd`, `ellsub`, `ellpow` realisieren die Gruppenoperationen, vgl. auch die Pari-Dokumentation. Entsprechendes wird es auch in Sage geben.

Aufgabe 2. Gegeben sei also die elliptische Kurve $y^2=x^3+2x+5$ über $\mathbb{Z}_{11}$.

a) Man berechne alle Punkte der Kurve und rechne konkret (mit Hilfe von Pari oder Sage) nach, daß die durch die Kurve gegebene Gruppe zyklisch ist.

b) Aus a) ist die Gruppenordnung der Kurve bekannt, nennen wir sie N_1.
Man setze p=11 und berechne die komplexe Zahl α, für die die Gleichungen $N_1=1+p-\alpha-\overline{\alpha}$, $\alpha\overline{\alpha}=p$ gelten.

Sei $f\in\mathbb{Z}_{11}[X]$ irreduzibel, grad $f=r$. Man betrachte den Erweiterungskörper $K=\mathbb{Z}_{11}[X]/<f>$ von $\mathbb{Z}_{11}$, der offenbar 11^r Elemente besitzt. Die oben gewählte elliptische Kurve läßt sich auch als Kurve über K auffassen, ihre Punktezahl und damit ihre Gruppenordnung sei N_K.

Es gilt nun (vgl. Koblitz, A Course in Number Theory and Cryptography) $N_K=1+p^r-\alpha^r-\overline{\alpha}^r$;

c) Das Polynom $f=X^{50}+3\in\mathbb{Z}_{11}[X]$ ist irreduzibel. Man berechne für den durch dieses Polynom definierten Körper $K=\mathbb{Z}_{11}[X]/<f>$ die Zahl N_K.
(N_1 ist Teiler von N_K, die Kurvengruppe über dem kleinen Körper setZ_11 läßt sich als Untergruppe der Kurvengruppe über dem großen Körper $K=\mathbb{Z}_{11}[X]/<f>$ auffassen.)

d) Man berechne einen zufälligen Punkt P auf der Kurve über K!

(Dazu gehe man aus von einem zufälligen Polynom x vom Grad <50 mit Koeffizienten in $\mathbb{Z}_{11}$, berechne anschließend den Wert $x^3+2x+5\in K$ und versuche, daraus eine Quadratwurzel zu ziehen. Falls keine Wurzel existiert, so wähle man so lange neue $x\in K$, bis es klappt. Man benutze ggf. den in der Vorlesung präsentierten Quadratwurzelalgorithmus.)

e) Wenn N_K wirklich die Gruppenordnung der Kurve über K ist, muß für den eben berechnen Punkt P gelten: $N_K P=0$. Rechnen Sie dies nach und dokumentieren Sie die Rechnung.