Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Blatt 10

Aufgabe 1

Studieren Sie die Pari-Funktionen zu Elliptischen Kurven in der Reference Card und im Tutorial soweit, daß Sie eine Elliptische Kurve mit der der Gleichung $y^2 = x^3 + a\,x + b$ und $4a^3 + 27b^2 \neq 0$ über dem Körper $K = \mathbb{Z}_7$ definieren können.

Beschäftigen Sie sich also mit den Funktionen `ellinit, ellisoncurve, ellordinate, ellorder, elladd, ellsub, ellpow`.

Berechnen Sie damit für einige zufällig gewählte Kurven über $\mathbb{Z}_7$ die Ordnung und die Gruppenstruktur: Von letzterer weiß man abstrakt, daß sie entweder zyklisch oder das Produkt zweier zyklischer Gruppen ist.

Wäre eine Ihrer Gruppen also zyklisch von der Ordnung 5, so notieren Sie bei Typ Wert 5 und geben einen Erzeuger an.
Wäre eine Ihrer Gruppen von der Ordnung 6 und von der Struktur $\mathbb{Z}_2 \times \mathbb{Z}_3$, so notieren Sie als Typ (2,3) und geben einen Erzeuger der Ordnung 2 und den zweiten Erzeuger der Ordnung 3 an.

Gesucht wird also eine Liste

a	b	Typ	Erzeuger1	Erzeuger2
1	1	5	[0,1]	
etc				

Stellen Sie fest, welche unter allen Kurven über setZ_7 maximale Ordnung und welche minimale Ordnung besitzt.

Fertigen Sie eine Statistik über die Ordnungen an.

Aufgabe 2

Wählen Sie eine Elliptische Kurve so, daß Sie einen Punkt $P=(x,y)$ zufällig vorgeben, dann a zufällig wählen und dann b so, daß (x,y) auf der Kurve liegt. Dadurch sparen Sie das Wurzelziehen bei der Bestimmung eines Punktes auf der Kurve.

Wählen Sie jetzt eine Primzahl p so groß, daß für eine nach obigem Schema gewählte zufällige Kurve E über $\mathbb{Z}_p$, die Funktion `ellorder(E,P)` noch relativ schnell zu einem Resultat kommt.

Wie verteilen sich die Ordnungen, die Sie erhalten, um die Zahl p herum?