htw saar

Studiengang Kommunikationsinformatik (Master)
Prof. Dr.–Ing. Damian Weber

Sicherheit und Kryptographie

Praktische Übung 3

Aufgabe 1 (Elliptische Kurven)

Implementieren Sie in PARI/GP Funktionen für eine elliptische Kurve

$$E : y^2 \equiv x^3 + ax + b \bmod p.$$

a) Berechnen des Hasse–Intervalls für die Punktanzahl einer Kurve mod p.

b) Testen, ob eine Kurve gültig ist ($4a^3 + 27b^2 \neq 0 \bmod p$).

c) Berechne aller Punkte auf E:

   i) betrachte alle x mit $0 \leq x \leq p - 1$

   ii) wenn $x^3 + ax + b \equiv 0 \bmod p$ ist, dann ist $(x, 0)$ ein Punkt auf E

   iii) wenn $x^3 + ax + b \bmod p$ ein Quadrat ist (Test durch Potenzieren mit $(p-1)/2$), dann sind (x, y) und $(x, -y)$ Punkte auf E. Die Quadratwurzel y können Sie aus y^2 nach folgendem Muster ausrechnen:

```
lift(polrootsmod(X^2-2,7)[1])
lift(polrootsmod(X^2-2,7)[2])
```

   Die Ausdrücke ergeben die beiden Quadratwurzeln von 2 mod 7.

   iv) wenn $x^3+ax+b \bmod p$ kein Quadrat ist, dann gibt es keinen Punkt (x, y) auf E.

d) Rückgabe der Anzahl der Punkte, d.h. alle Punkte berechnen, diese aber nicht ausgeben, sondern nur ihre Anzahl.

e) Arithmetik auf E. Gegeben sind zwei Punkte $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, berechne den Punkt $P_3 = P_1 + P_2$.

f) Multiplikation von Punkten: berechne für gegebenes m und gegebenen Punkt P den Punkt

$$m \cdot P = \underbrace{P + P + P + \ldots + P}_{m\text{–mal}}.$$