Kryptographie - Algebraischer Hintergrund
Prof . Dr. F.-O. Schreyer
Übungsblatt 6: Der Hintergrund von Hasses Theorem

Abgabetermin 25.6.2002
Voraussetzungen: Vorlesungskapitel Endliche Körper, Hintergrund von Hasses Theorem.

1. Schreiben Sie ein Maple-Skript, das über einem endlichen Körper $\mathbb{F}_{p^r}$ die Anzahl Punkte
$$N_r = \left|E\left(\mathbb{F}_{p^r} \right)\right|$$
einer elliptischen Kurve $E : x^3 + a \cdot x + b - y^2 = 0$, $a, b \in \mathbb{F}_{p^r}$ zählt. Zum Rechnen in $\mathbb{F}_{p^r}$ sind folgende Maple-Kommandos hilfreich (wenn Sie nicht Ihre Implementation vom letzten Übungsblatt verwenden wollen oder diese noch nicht fertig ist)

   $G := GF(p, r)$ ist $\mathbb{F}_{p^r}$
   $G[input](i)$ mit $i = 0, ..., p^r - 1$ die Repr. der Elemente von $\mathbb{F}_{p^r}$
   $G[extension]$ das verwendete irreduzible Polynom
   $G[`+`](a, b)$ berechnet $a + b$
   $G[`-`](a, b)$ berechnet $a - b$
   $G[`\hat{}`](a, j)$ berechnet a^j
   $G[`inverse`](a)$ berechnet $\frac{1}{a}$

2. Schreiben Sie ein Maple-Skript, das aus N_1 die reziproken Nullstellen α, β von $1 - at + pt^2$ bestimmt und
$$N_r = 1 + p^r - \alpha^r - \beta^r$$
für festes N_1 berechnet.

3. Schreiben Sie ein Maple-Skript, das aus N_1 mit der Weilformel N_r berechnet, indem Sie für vorgegebenes r die Potenzreihenentwicklung der logarithmischen Ableitung von $Z(E/\mathbb{F}_p, t)$ in t bis zur Ordnung r ausrechnen.

4. Vergleichen Sie an Beispielen die Ergebnisse von Aufgabe 1, 2 und 3.

5. Sei $f(x, y) := xy(x^2 - y^2) - 1$ und C die durch $f = 0$ definierte Kurve und $N_r := \left|\left\{(a, b) \in (\mathbb{F}_{p^r})^2 \mid f(a, b) = 0\right\}\right| + 4$ die Anzahl der Punkte von C über $\mathbb{F}_{p^r}$ (Bemerkung: Es gibt 4 Punkte im Unendlichen, da es 4 Asymptoten gibt). Bestimmen Sie N_1,...,N_7 für $p = 3$ und stellen Sie eine Vermutung für die Gestalt der Zetafunktion
$$Z(C/\mathbb{F}_p; t) := \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right) \in \mathbb{Q}[[t]]$$
auf, indem Sie $Z(C/\mathbb{F}_p; t) \cdot (1 - t) \cdot (1 - pt)$ bis zur Ordnung 7 bestimmen.

   Welchen Betrag haben die reziproken Nullstellen (Maple-Kommandos *solve* und *abs*)?

Abgabe der Aufgaben bitte als email an

boehm@btm8x5.mat.uni-bayreuth.de
oder
boehm@math.uni-sb.de