Einführung in die Computeralgebra

Übungsblatt 11

Sommersemester 2016

Michael Stoll

24. Juni 2016

Abgabe:
Donnerstag, 30. Juni, bis 10:00 Uhr im Briefkasten (NW II, 2. Stockwerk rechts).

Übungsaufgaben bitte **handschriftlich** bearbeiten (außer Programmieraufgaben);
nur ein Name pro Blatt! —
Schnellhefter und **Deckblatt** nicht vergessen!

(1) **Programmieraufgabe:**

(a) Implementieren Sie die Algorithmen „edf“ und „factor“ aus dem Skript (für q ungerade). Sie können dabei Magma-Funktionen für Polynome über $\mathbb{F}_q$ und für das Rechnen ist Restklassenringen verwenden:
`R, q := quo<P | f>` erzeugt den Restklassenring `R` des Polynomrings `P` modulo dem von `f` erzeugten Ideal; `q` ist der kanonische Epimorphismus `P` → `R`.
`a @@ q` für `a` ∈ `R` liefert den kanonischen Repräsentanten der Restklasse.
`Random(R)` liefert ein zufälliges Element von `R`.

(b) Sei $f = X^{2002} - 1 \in \mathbb{F}_{101}[X]$. Faktorisieren Sie f mit Ihrer Implementierung aus (a) hundertmal und bestimmen Sie Mittelwert und Standardabweichung der Laufzeiten.

(c) (Bonus) Implementieren Sie eine Variante des Faktorisierungsalgorithmus, die die effizientere Berechnung von X^{q^d} rem f verwendet (dazu müssen Sie auch „evalmult“ implementieren). Vergleichen Sie die Laufzeiten für verschiedene Werte von n und q mit dem Programm aus Teil (a). (30+10+30 extra)

(2) Sei $q = 2^m$ und sei $f = h_1 \cdots h_k$ ein Produkt von verschiedenen normierten irreduziblen Polynomen $h_j \in \mathbb{F}_q[X]$ vom Grad d. Sei weiter

$$t(x) = x + x^2 + x^4 + \ldots + x^{2^{md-1}} = \sum_{j=0}^{md-1} x^{2^j} .$$

(a) Zeigen Sie: Ist $a \in \mathbb{F}_q[X]/\langle f\rangle$ zufällig und gleichverteilt gewählt, dann ist (mit φ wie im Skript) $\varphi(t(a)) \in (\mathbb{F}_{q^d})^k$ ein zufälliges und gleichverteiltes k-Tupel aus $\{0,1\}^k$.

(b) Formulieren Sie ein Analogon „edf2“ zur Equal Degree Factorization „edf“ für endliche Körper der Charakteristik 2 (Pseudocode) und begründen Sie, warum es funktioniert.

(c) **Programmieraufgabe:**
Implementieren Sie „edf2“ in Magma. (20+20+20)