UNIVERSITÄT DES SAARLANDES
Fachrichtung Mathematik
Prof. Dr. Frank-Olaf Schreyer

Universität des Saarlandes - Campus E2 4 - D-66123 Saarbrücken

Computer Algebra Summer Term 2019

Exercise Sheet 8. Hand in by Tuesday, June 11.

Exercise 1. Let $q = 2^d$ be a power of 2 and $\mathbb{F}_q$ a field with q elements. Consider the polynomial

$$h = x + x^2 + x^4 + \ldots + x^{2^{d-1}}$$

and the map

$$\widetilde{h} : \mathbb{F}_q \to \mathbb{F}_q, a \mapsto h(a).$$

Prove: $\widetilde{h}$ is $\mathbb{F}_2$ linear and takes values in $\mathbb{F}_2 \subset \mathbb{F}_q$.

Exercise 2. Let $f = f_1 f_2$ be a square free polynomial which is the product of two irreducible monic polynomials in $\mathbb{F}_2[x]$ of degree d. Use the Chinese remainder theorem to prove that for precisely half of the polynomials $g \in \mathbb{F}_2[x]$ of degree $< 2d$ the $gcd(f, h(g))$ is a proper factor of f.

Design a probabilistic algorithms, which from an square equal degree product $f = f_1 f_2 \cdots f_k$

(1) finds an nontrivial factor,
(2) finds the irreducible factors $f_1, f_2, \ldots, f_k$.

Exercise 3. Consider $x^4 - 1 \in \mathbb{Z}[x]$ and the factorisation

$$x^4 - 1 \equiv (x-2)(x^3 + 2x^2 - x - 2) \mod 5.$$

Extend this factorisation to a factorisation mod 25 and mod 625.

Exercise 4. Consider $f = x^3 - x + t \in \mathbb{Q}[t, x]$. Then

$$f \equiv x(x-1)(x+1) \mod t.$$

Extend this factorisation to a facorisation mod t^2.