SS 2010 2010/05/06

Exercises to the Lecture Computer Algebra
Sheet 4

Prof. Dr. Klaus Madlener Delivery until 2010/05/14

**Exercise 1:** [Potenzreihen]
Let $F$ be a field of characteristic 0. Show: The coefficients $a_k \in F$ for $k \geq K$ ($K$ fixed) of a power series $a(x) = \sum_{k=0}^{\infty} a_k x^k$ can be represented by a linear recurrence relation with constant coefficients $a_k = u_1 a_{k-1} + u_2 a_{k-2} + \cdots + u_n a_{k-n}$ ($n$ fixed) over $F$ iff $a(x)$ is representable as a rational fuction $x$ over $F$.

**Exercise 2:** [Pseudo-Restefolgen]
Determine wether the polynomial pseudo remainder series from the lecture can actually be used to calculate the gcd. Show:

If $a(x)$ and $b(x)$ are primitive polynomials over a UFD $D$ and if $f_1(x) = a(x)$, $f_2(x) = b(x)$, $f_3(x)$, …, $f_{k-1}(x)$, $f_k(x)$ is a polynomial remainder series for $a(x)$ and $b(x)$, where $f_k(x) = 0$ then:

$$\gcd(a(x), b(x)) = \mathrm{pp}(f_{k-1}(x)).$$

**Exercise 3:** [Anwendung]
Let $D$ be a euclidean Ring with valuation $\nu$. Sketch an algortihm according to the following specification:

**Input:** A positive integer $n$ and $a, d_1, \ldots, d_n \in D \setminus \{0\}$ with $\gcd(d_i, d_j) = 1$ for $i \neq j$.

**Output:** $a_0, a_1, \ldots, a_n \in D$, such that

$$\frac{a}{d_1 \cdots d_n} = a_0 + \sum_{i=1}^{n} \frac{a_i}{d_i}$$

and either$a_i = 0$ or $\nu(a_i) < \nu(d_i)$ for $i \geq 1$.

Explain why your algorithm is correct. Have you encountered this algorithm before?

**Exercise 4:** [Nachrichtenverifikation]
Assume, Alice and bob have Messages of $n$ bit length, $M_A$ und $M_B$. They would like to check wether they have identical messages. On the one hand they want to have a high probability for a correct answer, on the other hand they want to reduce communication overhead. In particular, a message exchange is out of question because of the size of $n$.

Alice and Bob uniformly choose $k$ primes $p_1, \ldots, p_k$ from the set of the first $2n$ primes and check if $M_A \equiv M_B \bmod p_i$ for $1 \leq i \leq k$.

Show: If $M_A = M_B$, then $M_A \equiv M_B \bmod p_i$ for all $i$. If, however, $M_A \neq M_B$, then $M_A \not\equiv M_B \bmod p_i$ for an $i$ with a probability of at least $1 - 2^{-k}$.

**Exercise 5:** [Karatsuba]

a) Assure yourself that the multiplication algorithm after Karatsuba and Ofman also works for univariate polynomials. Draft a recursive procedure.

b) Prove that this algorithm multiplies tho polynomials of degree at most $n$ (where $n$ be a power of 2) with at most $9n^{\log_2 3} + O(n)$ ring operations.

   To this end, show the following lemma:

   Let $b, d \in \mathbb{N}$ with $b > 0$, and let $S, T : \mathbb{N} \to \mathbb{N}$ be fuctions with $S(2n) \geq 2S(n)$ and $S(n) \geq n$ for all $n \in \mathbb{N}$. If $T(1) = d$ and $T(n) \leq bT(n/2) + S(n)$ for $n = 2^i$ and $i \in \mathbb{N}^+$, then for all $i \in \mathbb{N}$ and $n = 2^i$:

$$T(n) \leq \begin{cases} (2 - 2/n)S(n) + d \in O(S(n)) & \text{falls } b = 1, \\ S(n)\log_2 n + dn \in O(S(n)\log_2 n) & \text{falls } b = 2, \\ \frac{2}{b-2}(n^{\log_2 b - 1} - 1)S(n) + dn^{\log_2 b} \in O(S(n)n^{\log_2 b - 1}) & \text{falls } b \geq 3. \end{cases}$$

c) Convince yourself that for small inputs the algorithm after Karatsuba and Ofman is slower that the classical polynomial multiplication algorithm.

   Now examine a hybrid algorithm that recursively applies the Karatsuba/Ofman-idea, until the degrees become smaller than some bound $2^d \in \mathbb{N}$. Afterwards it uses classical multiplication.

   Show that this hybrid algorithm requires at most $\gamma(d)n^{\log_2 3} + O(n)$ ring operations, where $\gamma(d)$ only depends on $d$. Find a $d$, such that $\gamma(d)$ is minimal. (You will need a rather exact estimation of the number of ring operations for the classical multiplication algorithm.)