Modul Computeralgebra mit Gröbnerbasen 7. April 2011
Sommersemester 2011
Schmale

Aufgabenblatt 1

(**1**) Zum Problem des „Ratens“ bei der Division mit Rest bei ganzen Zahlen: Lesen Sie den Abschnitt Theorem A, Theorem B in 4.3.1 bei Knuth in [K] oder [K'].

(**2**) Ein Beispiel aus [Kap], Seite 135. Seien $f = x^7 - 3*x^2 + 3*x + 1$ und $g = 3*x^3 - 4*x + 2$ Polynome in $\mathbb{Z}[x]$. Führen Sie Schritt für Schritt die Division mit Rest durch in $\mathbb{Q}[x]$ und die Pseudodivision in $\mathbb{Z}[x]$. Verbessern Sie die Pseudodivision durch ganzzahliges Kürzen, wo es Ihnen möglich erscheint und interpretieren Sie das dann veränderte Ergebnis hinsichtlich des Ergebnisses der üblichen Pseudodivision.

(**3**) Eine Aufgabe aus [GaGe], Seite 246:

8.7 Karatsuba's method for polynomial multiplication can be generalized as follows. Let F be a field, $m, n \in \mathbb{N}_{>0}$, and $f = \sum_{0 \le i < n} f_i x^i$, $g = \sum_{0 \le i < n} g_i x^i$ in $F[x]$. To multiply f and g, we divide each of them into $m \ge 2$ blocks of size $k = \lceil n/m \rceil$:

$$f = \sum_{0 \le i < m} F_i x^{ki}, \quad g = \sum_{0 \le i < m} G_i x^{ki},$$

with all $F_i, G_i \in F[x]$ of degree less than k. Then $fg = \sum_{0 \le i < 2m-1} H_i x^{ki}$, where $H_i = \sum_{0 \le j \le i} F_j G_{i-j}$ for $0 \le i < 2m-1$ and we assume that $F_j, G_j = 0$ if $j \ge m$.

(i) Find a way to compute $H_0, \ldots, H_4$ when $m = 3$ using at most 6 multiplications of polynomials of degree less than k. Use this method to construct a recursive algorithm à la Karatsuba and analyze its cost when n is a power of 3.

(ii) Suppose that you have found a scheme to compute $H_0, \ldots, H_{2m-2}$ using d multiplications of polynomials of degree less than k, and made this scheme into a recursive algorithm as in (i). How large may d be at most such that your algorithm is asymptotically faster than Karatsuba's? Compare with your result from (i).

Bearbeiten Sie (i). Loesungshinweise sind bei Bedarf unter
`http://cosec.bit.uni-bonn.de/fileadmin/user_upload/science/mca/solutions.pdf`
zu finden.