HUMBOLDT–UNIVERSITÄT ZU BERLIN

MATHEMATISCH-NATURWISSENSCHAFTLICHE FAKULTÄT II

INSTITUT FÜR MATHEMATIK

PROF. ANDREAS GRIEWANK PHD,

DR. LUTZ LEHMANN

Humboldt-Universität zu Berlin, Institut für Mathematik, Unter den Linden 6, D-10099 Berlin

Berlin, den May 5, 2008

Exercises for the lecture "Introduction to Computer Algebra"

Series 2. (Return on Monday, May 19th 2008)

Aufg. 1: Consider the quadratic extension ring $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \sqrt{-5}\mathbb{Z}$ with arithmetic operations as in $\mathbb{C} \supset \mathbb{Z}[\sqrt{-5}]$.

(a) Examine whether $\mathbb{Z}[\sqrt{-5}]$ is an integral domain. **4 pts.**

(b) Determine the group of units $\mathcal{U}$. **4 pts.**

(c) Show that $a = 3(1 - \sqrt{-5})$ and $b = 6$ have maximal common divisors $c = 3$ and $\tilde{c} = (1 - \sqrt{-5})$, but neither $c \big| \tilde{c}$ nor $\tilde{c} \big| c$. **4 pts.**

Aufg. 2: Let $\mathcal{R}$ be a g.c.d. domain. Prove that

(a) $\gcd(ca, cb) = c \gcd(a, b)$ for any $a, b, c \in \mathcal{R}$. **2 pts.**

(b) $\gcd(\gcd(a, b), c) = gcd(a, \gcd(b, c))$ for any $a, b, c \in \mathcal{R}$. **2 pts.**

(c) $a = bq + r \implies \gcd(a, b) = \gcd(b, r)$ for any $b, q, r \in \mathcal{R}$ **2 pts.**

Aufg. 3: Euclidean algorithm

(a) Implement some variant of the (standard) extended euclidean algorithm for positive integers with smallest nonnegative remainder. Add in print statements that produce the extended quotient-remainder table for $(a_k,\ q_k,\ u_k,\ v_k)$, $k = 0, \ldots, m$, with **8 pts.**

$$a_0 = a,\ a_1 = b,$$
$$a_{k-1} = a_k \cdot q_k + a_{k+1},$$
$$a_k \cdot u_k + a_{k+1} \cdot v_k = gcd(a, b)\ .$$

Or alternatively the table for (a_k, q_k, s_k, t_k) with

$$s_k\, a + t_k\, b = a_k\ .$$

Report those tables for the pairs $(a, b) = (64\,879\,448\,976\,299, 2\,680\,241\,827\,180)$ and $(a, b) = (579\,521\,240\,621\,427, 320\,385\,477\,230\,257)$

(b) Show that for any given iteration count n in the euclidean algorithm, the smallest inputs realizing that count are the consecutive members of the Fibonacci sequence $(a, b) = (F_{n+1}, F_n)$. Deduce an estimate for the iteration count for any input. **4 pts.**

(c) Modify your implementation of the euclidean algorithm in such a way that it also accepts negative inputs and uses the smallest signed remainder, that is, $-|a_k| < 2 \cdot a_{k+1} \leq |a_k|$. Produce the same tables for the given inputs and compare their length. **6 pts.**

(d) (Optional) Find a sequence of pairs $\left((a^{(n)}, b^{(n)})\right)_{n\in\mathbb{N}}$ of integers such that no other pair of smaller absolute values than those of $(a^{(n)}, b^{(n)})$ uses more than n iterations of the modified euclidean algorithm. **8* pts.**

Aufg. 4: Lehmers algorithm for the computation of the gcd "guesses" the first quotients of the euclidean algorithm from the leading digits of the input numbers.

(a) Compute and report the quotient sequence $q_1, q_2, \ldots, q_m$ for the (standard) euclicean algorithm starting with $(a_1, b_1) = (880\,458\,755\,986, 307\,373\,752\,472)$. Compare the first elements of this sequence with those of the quotient sequences for (88, 30), (89, 30) and (88, 31), as well as those for (880 458, 307 373), (880 459, 307 373) and (880 458, 307 374). (And similar for any number of leading digits of your choice.) **6 pts.**

(b) Give an algorithm (without avoidable operations) to compute, given a pair $(a \div B^m, b \div B^m)$ of leading digits, the leading segment of the quotient sequence up to the point of divergence. **4 pts.**

(c) (Optional) Let C be some big number, e.g. some power of the digit base, and $a = xC + z$; $b = yC + w$ with $x, y, z, w \in \{0, 1, \ldots, C-1\}$, $x, y > 0$. Show that if the quotient sequences $q_1, \ldots, q_k$ of the euclidean algorithm for the pairs $(x+1, y)$ and $(x, y+1)$ coincide, they also coincide with the quotient sequence for (a, b). **8* pts.**

(d) (Optional) Expose a way to compute from the inputs (a_1, b_1) and $q_1, \ldots, q_{k-1}$ directly—that is, with as few biginteger operations as possible—the intermediate pair (a_k, b_k). Use this procedure and the guessing of the first coefficients to complete an algorithm for the gcd computation à la Lehmer. **10* pts.**

phone: 030/2093-5820 fax: 030/2093-5848
e-mail: griewank@math.hu-berlin.de llehmann@math.hu-berlin.de
Internet-Seite: http://www.math.hu-berlin.de/~gaggle/S08/COMPALG