SS 2010 2010/04/23

Exercises to the Lecture Computer Algebra
Sheet 2

Prof. Dr. Klaus Madlener Delivery until 2010/04/30

Exercise 1: [GCD]

a) Relating to Theorem 2.13: Let F_i for $i \in \mathbb{N}$ be the i-th Fibonacci-Number (i.e. $F_0 = 0$, $F_1 = 1$ and $F_i = F_{i-1} + F_{i-2}$ for $i \geq 2$). Prove that $\lfloor F_{i+2}/F_{i+1} \rfloor = 1$ and $F_{i-1} = F_{i+1} \bmod F_i$ for all $i \geq 2$.

b) Let $F[x]$ be the (Euclidean) univariate polynomial ring over a field F and furthermore $a, b \in F[x] \setminus \{0\}$ and $g = gcda, b \in F[x]$. Show that for every polynomial $c \in F[x]$ with $g \mid c$ there are unique polynomials $\sigma, \tau \in F[x]$, such that $\sigma a + \tau b = c$ and $\deg(\sigma) < \deg(b) - \deg(g)$ hold. If furthermore $\deg(c) < \deg(a) + \deg(b) - \deg(g)$ holds, then $\deg(\tau) < \deg(a) - \deg(g)$.

c) Let $a, b \in \mathbb{N}^+$ and $a > b$. We want to decide wether there are $i, j \in \mathbb{N}^+$, such that $a^i = b^j$. Consider the following decision procedure:

First check, if $b \mid a$. If not, then answer "no" . If yes, replace (a, b) with $(a/b, b)$, if $a \geq b^2$, or with $(b, a/b)$, if $a < b^2$. If – by iterating – finally a tuple $(a', 1)$ is reached, answer "yes".

Show that this procedure terminates and correctly solves our Problem for every input and that it requires – in the worst case – $O(\lambda(a)^2)$ bit operations.

Exercise 2: [Division in $\mathbb{Z}$]

a) We reconsider the division algorithm for non-negative base-b-integers for $b \geq 2$. Let $u = (u_0 \cdots u_n)_b$ and $v = (v_1 \cdots v_n)_b$ with $\lfloor u/v \rfloor < b$. As in the lecture let $\hat{q} = \min\left(\left\lfloor \frac{u_0 b + u_1}{v_1} \right\rfloor, b - 1\right)$ be the approximation of $q = \lfloor u/v \rfloor$ with $u = qv + r$ and $0 \leq r < v$.

Prove that $\hat{q} \geq q$ and for $v_1 \geq \lfloor b/2 \rfloor$ also $\hat{q} - 2 \leq q$.

b) Find an example for u and v with base 10 that illustrates the necessity of the conditional statement

if $(u_j \cdots u_{j+n})_b < \hat{q} \cdot (v_1 \cdots v_n)_b$ **then** $\hat{q} := \hat{q} - 1$