Exercises to the Lecture Computer Algebra
Sheet

Prof. Dr. Klaus Madlener Delivery until 23.04.2010

**Exercise 1:** [Rings and fields]
We want to show some Theorems:

a) Let $R$ be an integral domain and $a, b \in R^*$ (the set of non-0-elements of $R$). $a$ and $b$ are associated iff there is a $u \in E(R)$ (the unit group of $R$) with $a = ub$.

b) Let $R$ be a Euclidean Ring and $I$ an ideal of $R$. If $0 \neq a \in I$, then $I = aR$ iff $v(a) \leq v(b)$ for all $b \in I \setminus \{0\}$ (where $v$ is the euclidean function of $R$).

   Show further, that $R$ is a principal ideal domain (i.e., that all ideals of $R$ are principal ideals).

c) If $K$ is a field, then $K[x]$ is an Euclidean ring.

d) If $K$ is a field and $L$ is an extension of $K$ (i.e. a field containing $K$ as a subfield), and if furthermore $f \in K[x]$ and $\ell \in L$ a root of $f$, then $f$ is divisible by $x - \ell$ in $L[x]$.

**Exercise 2:** [Polynomial division]
We examine the run-time of the classical polynomial division. Consider the following algorithm:

**Function:** PolyQuoRem$(a, b)$
**Input:** $a, b \in \mathbb{R}[x]$,
$a = \sum_{0 \leq i \leq n} a_i x^i$, $b = \sum_{0 \leq i \leq m} b_i x^i$,
$R$ is a commutative ring with 1, all $a_i, b_i \in R$,
$b_m$ is a unit in $R$ and $n \geq m \geq 0$.
**Output:** $q, r \in R[x]$ with $a = qb + r$ and $\deg r < m$ or $r = 0$

$r \leftarrow a$
**for** $i \leftarrow n - m$ **to** $0$ **do**
  **if** $\deg(r) = m + i$ **then**
    $q_i \leftarrow \mathrm{lc}(r)/b_m; r \leftarrow r - q_i x^i b$
  **else**
    $q_i \leftarrow 0$
  **end if**
**end for**
**return** $q = \sum_{0 \leq i \leq n-m} q_i x^i$ und $r$

Assume that a polynomial $p = \sum_{0 \leq i \leq k} p_i x^i$ of degree $k$ is given in dense representation, i.e. it is represented by a coefficient vector $\vec{p} = (p_0, \ldots, p_k)$. Calculate the worst-case-run-time, measured in the number of ring operations in $R$, depending on $n$ and $m$. Are $q$ and $r$ unique?

**Exercise 3:** [Diophantische Gleichungen]

Are there $s, t \in \mathbb{Z}$, such that $24s + 14t = 1$ resp. $61s + 37t = 56$? Find all possible solutions.

Show: The linear diophantine Equation $ax + by = c$ with $a, b, c \in \mathbb{Z}$ has a solution in $\mathbb{Z}$ iff $d|c$ for $d = \gcd(a, b)$. If $(x_0, y_0)$ is a given solution, then

$$\{(x_0 + k \cdot \frac{b}{d}, y_0 - k \cdot \frac{a}{d} \,|\, k \in \mathbb{Z}\}$$

is the set of all solutions. What does the term $\frac{a}{d}$ mean in this context?)

**Exercise 4:** [GCD]

a) Calculate greatest common divisors of $f = x^5 + x^4 + x^3 - x^2 - x + 1$ and $g = x^3 + x^2 + x + 1$ ($f, g \in \mathbb{Z}_p[x]$) for $p = 3$ and $p = 5$. Calculate polynomials $s$ and $t$ with $\gcd(f, g) = sf + tg$.

b) We consider the following gcd-Algorithm after J. Stein (possibly known in ancient China):

**Function:** BinaryGCD($u, v \in \mathbb{N}^+$)<br>
{Returns the g.c.d of $u$ and $v$}<br>
$g \leftarrow 1$<br>
**while** $(u \bmod 2 = 0) \wedge (v \bmod 2 = 0)$ **do**<br>
    $u \leftarrow u/2; v \leftarrow v/2; g \leftarrow 2g$<br>
**end while**<br>
**while** $(u \neq 0)$ **do**<br>
    **if** $(u \bmod 2 = 0)$ **then**<br>
        $u \leftarrow u/2$<br>
    **else if** $(v \bmod 2 = 0)$ **then**<br>
        $v \leftarrow v/2$<br>
    **else**<br>
        $t \leftarrow |u - v|/2$<br>
        **if** $u \geq v$ **then**<br>
            $u \leftarrow t$<br>
        **else**<br>
            $v \leftarrow t$<br>
        **end if**<br>
    **end if**<br>
**end while**<br>
**return** $g \cdot v$

Show that this algorithm actually calculates $\gcd(u, v)$ for any input $u, v \in \mathbb{N}^+$ and that it requires $O((\lambda(uv))^2)$ in the worst case. We assume that positive natural numbers are given in binary representation and that $\lambda(x)$ is the length of this representation (without leading zeros). Sow finally, that $O(\lambda(u)\lambda(v))$ bit operations *do not suffice* in the worst case.