Exercise to the Lecture
COMPUTERALGEBRA II

UNIKASSEL VERSITÄT 06.04.2013

Exercise 1 (Extended euclidian algorithm: Rational numbers)

Let be *a*, $b \in \mathbb{Z}$.

(a) Consider the Bézout's identity

$$gcd(a, b) = s a + t b$$

where s and t are the Bézout coefficients. Use the following equations

 $x_k = x_{k+1}q_k + x_{k+2}$ and $x_k = s_k x_0 + t_k x_1$ $(x_k, q_k, s_k, t_k \in \mathbb{Z})$

with $x_0 = a$, $x_1 = b$ and $k \in \mathbb{N}_0$, to determine a recurrence equation for s_k and t_k respectively.

Hint: Use in the first equation $x_k = x_{k+1}q_k + x_{k+2}$ the expression $x_k = s_kx_0 + t_kx_1$ and proceed by the method of comparing coefficients.

(b) Program iteratively your algorithm in *Mathematica*.

(8 points)

Exercise 2 (Extended euclidian algorithm: Polynomials with integer coefficients)

Use the function PolynomialExtendedGCD to determine for each couple of polynomials $a(x), b(x) \in \mathbb{Z}[x]$ a representation of the form

$$g(x) = s(x)a(x) + t(x)b(x)$$

with $g(x), s(x), t(x) \in \mathbb{Z}[x]$, all of them with integer coefficients, where g(x) is a greatest common divisor of a(x) and b(x). The representation should be defined such that no further simplification with integers is possible. Test your function on different examples.

(8 points)