Computer Algebra **Summer 2011**
Michael Sagraloff **Discussion on May 4th.**

Exercise 3

Euclidean and principle ideal domains

Let R be an integral domain. Show that:

- If R is an Euclidean domain, then R is principle.
- $\mathbb{Z}[x]$ is not principle but $\mathbb{Q}[x]$ is principle.
- $\mathbb{Q}[x_1, \ldots, x_n]$ is not Euclidean for all $n > 1$.

Euclidean Algorithm

Implement the extended Euclidean Algorithm. Consider pairs f, $g \in \mathbb{Z}[x]$ of polynomials (random, multiples of a random polynomial, etc.) and test your implementation, that is, determine polynomials u and v with

$$u \cdot f + v \cdot g = \gcd(f, g).$$

What do you observe (test polynomials of larger degrees as well)?

Square-free part

Let f be a univariate polynomial with real coefficients and l be defined as in extended Euclidean algorithm applied to f and $g := f'$, that is,

$$s_l \cdot f + t_l \cdot f' = \gcd(f, f').$$

Show that t_{l+1} is the square-free part of f.

Kronecker's method to factoring polynomials

Let $f = \mathbb{Z}[x]$ be a univariate polynomial with integer coefficients. We aim to factorize f into irreducible factors $f_1, \ldots, f_k \in \mathbb{Z}$. The idea is to reduce the latter task to factoring integers and polynomial interpolation. Exploit the fact that $f(m) \in \mathbb{Z}$ for any integer m, thus $f_i(m)$ divides $f(m)$. Formulate an algorithm to factor a polynomial f based on the latter observation and implement this algorithm!

Have fun with the solution!