Chair of Symbolic Computation
Prof. Dr. Martin Kreuzer
Julian Danner

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

Computeralgebra – Sheet 1

Summer term 2025

Date: 24.04.2025
Discussion: 02.05.2025

Exercise 1 (Extended Euclidean Algorithm)**.**
Let $a, b \in \mathbb{Z}$. Consider the following sequence of instructions.

(1) If $a = 0$ and $b = 0$, **return** the triple $[0, 0, 0]$.
If $a = 0$ and $b \neq 0$, **return** the triple $[0, \frac{|b|}{b}, |b|]$.
If $a \neq 0$ and $b = 0$, **return** the triple $[\frac{|a|}{a}, 0, |a|]$.

(2) Set the triples $[c_0, d_0, e_0] \leftarrow [\frac{|a|}{a}, 0, |a|]$ and $[c_1, d_1, e_1] \leftarrow [0, \frac{|b|}{b}, |b|]$.

(3) If $e_0 < e_1$, swap $[c_0, d_0, e_0] \longleftrightarrow [c_1, d_1, e_1]$.

(4) Repeat steps (4.1)–(4.3) until $e_1 = 0$.
   (4.1) Write e_0 in the form $e_0 = qe_1 + r$, where $q, r \in \mathbb{N}$ and $0 \leq r < e_1$.
   (4.2) Compute $[c_2, d_2, e_2] \leftarrow [c_0 - qc_1,\ d_0 - qd_1,\ r]$.
   (4.3) Assign $[c_0, d_0, e_0] \leftarrow [c_1, d_1, e_1]$ and $[c_1, d_1, e_1] \leftarrow [c_2, d_2, e_2]$.

(6) **return** the triple $[c_0, d_0, e_0]$.

This algorithm is known as the *Extended Euclidean Algorithm* (EEA) and computes $[c, d, e] \in \mathbb{Z}^3$ such that $e = \gcd(a, b)$ and $ac + bd = e$.

(a) Show that this is indeed an algorithm, i.e., that it stops after finitely many steps.

(b) Show that the output is correct, i.e., a triple with the claimed properties.

Hint: Show that $ac_0 + bd_0 = e_0$ is an invariant of the algorithm, then it suffices to show that $e = \gcd(a, b)$.

Exercise 2. Let p be a prime and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the finite field with p elements. Explain how the *Extended Euclidean Algorithm* can be used to compute the inverse of a unit in $\mathbb{F}_p$.

Exercise 3. Let K be a field, $P = K[x]$, let $f_1, f_2 \in P$ be non-zero polynomials, and let

$$I = Pf_1 + Pf_2 = \{\, g_1 f_1 + g_2 f_2 \mid g_1, g_2 \in P \,\}.$$

(a) Show that the set I is an ideal of P.

(b) Show that the ideal I is generated by $\gcd(f_1, f_2)$, i.e., $I = \langle \gcd(f_1, f_2) \rangle$.
Recall that the greatest common divisor of f_1 and f_2, denoted by $\gcd(f_1, f_2)$, is the unique monic polynomial $h \in P$ with $h \mid f_1$, $h \mid f_2$, and if $g \mid f_1$ and $g \mid f_2$ then $g \mid h$.

Exercise 4. Let p be a prime number, let $K = \mathbb{F}_p$, let $f \in P = K[x]$ be a non-zero polynomial, and let f' be the derivative of f. Show that $f' = 0$ if and only if f is of the form $f = g^p$ for some $g \in P$.

Exercise 5. Let p be a prime number, let $K = \mathbb{F}_p$ or $\mathbb{Q}$, let $f \in K[x]$ be a non-zero polynomial, and let f' be the derivative of f. Show that if f is irreducible then we have $\gcd(f, f') = 1$.