to be prepared for 27.10.2022

Exercise 16. Let $\mathbb{F}$ denote a field, and $a, b \in \mathbb{F}$ polynomials with $\deg a < (\deg b) \cdot e$, where $e \in \mathbb{N} \setminus 0$. Develop an algorithm that computes $a_1, \ldots, a_e \in \mathbb{F}[x]$ with $\deg a_i < \deg b$ $(1 \leq i \leq e)$ s.t.

$$\frac{a}{b^e} = \frac{a_1}{b} + \frac{a_2}{b^2} + \cdots + \frac{a_e}{b^e}.$$

Hint: Consider polynomial division in a Horner scheme style.

Exercise 17. Let R be a Euclidean domain, $m_1, \ldots, m_p \in R \setminus 0$ pairwise coprime, and set $m = m_1 \cdots m_p$. Give a precise proof that the rings $R/\langle m \rangle$ and $\prod_{i=1}^{p} R/\langle m_i \rangle$ are isomorphic.

Exercise 18. Let R be a Euclidean domain. Prove the following:

1. If $m_1, \ldots, m_n \in R \setminus 0$ are pairwise coprime and $M = \prod_{i=1}^{n-1} m_i$. Then m_n and M are relatively prime.

2. Assume that $r, r' \in R$, and $m_1, m_2 \in R \setminus 0$ are coprime. Then $r \equiv r' \mod m_1$ and $r \equiv r' \mod m_2$ if and only if $r \equiv r' \mod m_1 m_2$.

Exercise 19. Use the facts formulated in the previous exercise for developing a recursive algorithm that computes a solution of a Chinese remainder problem in a Euclidean domain.

Exercise 20. Solve the Chinese remainder problem

$$\begin{aligned} r &\equiv 62 \mod 79 \\ r &\equiv 66 \mod 83 \\ r &\equiv 72 \mod 89 \end{aligned}$$

over the integers.