Due date: 29.10.2019

Exercise 1
Let U be a UFD and consider arbitrary polynomials $f, g \in U[x]$. We write $f \sim g$ if and only if there is a unit $\epsilon \in U$ such that $f = \epsilon \cdot g$. Now prove the following statements:

1. $\text{cont}(f \cdot g) \sim \text{cont}(f) \cdot \text{cont}(g)$
2. $\text{pp}(f \cdot g) \sim \text{pp}(f) \cdot \text{pp}(g)$
3. $\text{cont}(\gcd(f, g)) \sim \gcd(\text{cont}(f) \cdot \text{cont}(g))$
4. $\text{pp}(\gcd(f, g)) \sim \gcd(\text{pp}(f) \cdot \text{pp}(g))$

Hint: Decompose the polynomials and use Gauss's lemma.

Exercise 2
Recall from the lecture that polynomial division might not be possible over an integral domain. This is the case when leading coefficients are not divisible. In this exercise you will show that the usual polynomial division is still possible if the dividend is multiplied with a suitable constant first. This operation is known as *pseudo-division*.

Let I be an integral domain. Consider the polynomials $a(x), b(x) \in I[x]$, where $b \neq 0$, with $n = \deg(a(x)) \geq \deg(b(x)) = m$. Show that there are unique polynomials $q(x), r(x) \in I[x]$ such that

- $\text{lc}(b(x))^{n-m+1} \cdot a(x) = q(x) \cdot b(x) + r(x)$ and
- $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$.

Hint I: Such proofs are usually split into two parts: existence and uniqueness. For existence you should demonstrate that we can perform standard polynomial division with this construction. Uniqueness can be shown in the usual way: Assume that there are two different quotients/remainders and derive that they must be equal (use the second item).

Hint II: If you are unsure, try a simple example first: Perform pseudo-division for $a(x) = x^2 + 2x + 1$ and $b(x) = 3x - 1$ in the domain $\mathbb{Z}[x]$. Is the power of $\text{lc}(b(x))$ which is multiplied with $a(x)$ somehow related to the (maximum) number of division steps we have to carry out?

Exercise 3
Compute the pseudo-quotient $q(x)$ and the pseudo-remainder $r(x)$ of the following polynomials over the integers:

$$a(x) = x^6 + x^5 - x^4 + 2x^3 + 3x^2 - x + 2,$$
$$b(x) = 2x^3 + 2x^2 - x + 3.$$

Exercise 4
Solve the subsequent Chinese remainder problem

$$x \equiv 62 \bmod 79$$
$$x \equiv 66 \bmod 83$$
$$x \equiv 72 \bmod 89$$

over the integers. Describe how to solve such a problem using GCD computations.