Due date: 20.10.2020

5. Exercise

Implement the extended Euclidean algorithm `GCD_EUCLID` from the lecture notes for finite fields of prime order. The input of the algorithm should be the polynomials $a, b \in \mathbb{F}_p[x]$ and the order $p \in \mathbb{P}$ of the finite field. Test your implementation with at least two non-trivial examples of different order.

Note: You may use the field operations as well as quotient and remainder for finite fields offered by your CAS. You may NOT use any built-in GCD methods.

6. Exercise

Given a unique factorization domain U. For polynomials $f, g \in U[x]$, write $f \sim g$ if and only if there exists a unit $\varepsilon \in U$ such that $f = \varepsilon\, g$. Prove the following claims:

1. $\mathrm{cont}(f\, g) \sim \mathrm{cont}(f)\, \mathrm{cont}(g)$
2. $\mathrm{pp}(f\, g) \sim \mathrm{pp}(f)\, \mathrm{pp}(g)$.

7. Exercise

Prove or disprove the following claims:

1. Let R be a commutative ring. The polynomial ring $R[x]$ is a Euclidean domain (ED), i.e. admits a degree function with the usual properties, if and only if R is a field.
2. The quadratic integer ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is a ED.

8. Exercise

Find the GCD of the polynomials

$$f = 6\,x^5 + 2\,x^4 - 19\,x^3 - 6\,x^2 + 15\,x + 9$$
$$g = 5\,x^4 - 4\,x^3 + 2\,x^2 - 2\,x - 2$$

over $\mathbb{Z}$ by a polynomial remainder sequence.

9. Exercise

Show that the bivariate polynomial ring $K[x, y]$ is not a principal ideal domain (PID), where K is a field.