Computer Algebra (2014)-Aalborg University
Lecture 2, September 16th

2nd Lecture: Tuesday September 16th, 12:30-16:15 at room G5-109.

- 12:30-16:15 Lecture: Euclidean domains and the extended Euclidean algorithm. Cost analysis of Extended Euclidean Algorithm. Applications of the Euclidean Algorithm. Modular Arithmetic. Modular inverses via Euclid. Repeated squaring. Modular inverses via Fermat. Linear Diophantine equations. Continued fractions and Diophantine approximation. (pages 45-53, 69-82).

- 10:00-12:00 Work in groups. A, 4.22, 4.10, 4.26, 4.25, 4.13, 4.9, 3.11 , A, 3.17, 4.19, 4.27, B.

  Exercise A: Compute the gcd of example 3.7.

  Exercise B: Implement Algorithm 2.5. Represent a polynomial by its coefficients. Consider the polynomial ring over the rings $\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

  Exercise C: Proof Theorem 3.11 (including detailed technical arguments and the previous lemmas).

Best regards,

Diego