Computer Algebra (2012)-Aalborg University
Lecture 2, September 10th

2nd Lecture: Monday September 10th, 8:15-12:00 at room G5-109.

- 8:15-8:45 Repetition: Big-O notation. Representation and addition of numbers and polynomials. Multiplication and division with remainder. Euclidean domains and the extended Euclidean algorithm (pages 710–711, 27–39, 43–49) + Lecture: Cost analysis of Extended Euclidean Algorithm (49–51).

- 8:45-10:45 Work in groups. Exercises from [GG]: A, 3.19 (we did i, ii and iii in Algebra 2. Use Maple to solve iv and v), B, 2.8, 2.9, 3.11 (with Maple), 2.1, 2.7.

  Exercise A: Implement Algorithm 2.3 in Maple. Represent a polynomial by its coefficients. Consider the polynomial ring over the rings $\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

  Exercise B: Proof Theorem 3.11 (including detailed technical arguments).

- Lecture: 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 67–80).

Best regards,

Diego