Computeralgebra (2013)-Aalborg Universitet
Spiseseddel 2

2. gang , tirsdag d. 10. september, 8:15-12:00 i lokale G5-109

- 8:15-10:00 Forelæsning: 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. Modular algorithms and interpolation. Change of representation. Evaluation and interpolation. Secret sharing (sider 69–83 og 97-104)

- 10:00-12:00 Arbejde i grupper med følgende opgaver (fra [GG]): 4.22, 4.10, 4.26, 4.25, 4.13, 4.9, 3.11 (med Maple eller Sage), A, 3.17, 4.19, 4.27, B.

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

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

Med venlig hilsen,

Diego