Computer Algebra (2012)-Aalborg University
Lecture 3, September 14th

3rd Lecture: Monday September 14th, 8:15-12:00 at room G5-109.

- 8:15-8:45 Repetition: 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).
- 8:45-10:45 Work in groups. Exercises from [GG] (you are very welcome to use a Computer algebra system): 4.22, 4.10, 4.26, 4.25, 4.13, 4.9, 4.19, 3.17, 4.27.
- 10:45-12:00 Lecture: Modular algorithms and interpolation. Change of representation. Evaluation and interpolation. Secret sharing. The Chinese remainder Algorithm. Modular determinant Computation (pages 95–109).

Best regards,

Diego