Computer Algebra (2012)-Aalborg University
Lecture 4, September 17th

4th Lecture: Monday September 17th, 8:15-12:00 at room G5-109.

- 8:15-8:45 Repetition: Modular algorithms and interpolation. Change of representation. Evaluation and interpolation. Secret sharing. The Chinese remainder Algorithm. Modular determinant Computation (pages 95–107).
- 8:45-10:45 Work in groups. Exercises from [GG] (you are very welcome to use a Computer algebra system): 5.4, 5.14, A, B, 5.5, 5.7.

  Exercise A: Compute $f \in \mathbb{Z}[X]$ of degree lower than 4 such that $f \equiv x (\text{mod } x^2)$ and $f \equiv 1 (\text{mod } (x-1)^2)$.

  Exercise B: Write a program that will allow 4 players to share the pin code of a Dankort in a such a way that 3 players cannot recover it. Consider now the same problem where 2 players cannot recover it but 3 players can recover it.
- 10:45-12:00 Lecture: Modular determinant computation. Hermite interpolation. Rational function reconstruction. Cauchy interpolation (pages 107–119)

Best regards,

Diego