

# Computer Algebra (2014)-Aalborg University

## Lecture 4, October 7th

**4th Lecture:** Tuesday October 7th, 12:30-16:15 at room G5-109.

- 12:30-14:15 Lecture: The Chinese remainder Algorithm. Modular determinant Computation. Hermite interpolation. Rational function reconstruction. Cauchy interpolation (pages 104–121).
- 14:15-16:15 Work in groups, exercises with Sage: A, 4.13, 5.4, B, C, 5.43 + exercises from previous lectures

Exercise A: 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.

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

Exercise C: Compute a polynomial  $f$  in  $\mathbb{Q}[X]$  of degree less than 6 such that  $f(0) = 0$ ,  $f'(0) = 1$ ,  $f(1) = 1$ ,  $f'(1) = 0$ ,  $f(2) = 1$ ,  $f'(2) = 1$ . Draw it.

Best regards,

Diego