Computer Algebra (2014)-Aalborg University
Lecture 3, September 23rd

3rd Lecture: Tuesday September 23rd, 12:30-16:15 at room G5-109.

- 12:30-14:15 Lecture: Linear Diophantine equations. Continued fractions and Diophantine approximation. The Chinese remainder Algorithm. Modular determinant Computation. (pages 77-83, 97-104).
- 14:15-16:15 Work in groups, exercises with Sage: 4.26, 4.25, 4.27, 5.4, A, B, 5.14, 5.5, 5.7, 4.10, 4.13, 4.9

  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.

Best regards,

Diego