Computeralgebra (2013)-Aalborg Universitet
Spiseseddel 3

3. gang , torsdag d. 12. september, 8:15-12:00 i lokale G5-109

- 8:15-10:00 Forelæsning: Modular algorithms and interpolation. Change of representation. Evaluation and interpolation. Secret sharing The Chinese remainder Algorithm. Modular determinant Computation (sider 97–113)
- 10:00-12:00 Arbejde i grupper med følgende opgaver (fra [GG]): 5.4, A, B, 5.14, 5.5, 5.7 + opgaver fra spiseseddel 2.

  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.

Med venlig hilsen,

Diego