

# Computer Algebra (2014)-Aalborg University

## Lecture 7, October 28th

**7th Lecture:** Tuesday October 28th, 12:30-16:15 at room G5-109.

- 12:30-14:15 Lecture: Factoring polynomials over finite fields (pages 377-389).
- 14:15-16:15 Work in groups, exercises with Sage: A, B, 8.10, C, 8.4, D, E. + exercises from previous lectures

Opgave A: Compute the distinct-degree decomposition of the polynomial  $f$  in exercise 14.3 in [GG] using a command in Sage.

Opgave B: Solve Exercise 14.3 in [GG] using Sage. You do not have to implement Algorithm 14.3, but you are welcome to do it.

Exercise C: Trace Karatsuba's algorithm for multiplying two polynomials of degree lower than 4.

Exercise D: Write a table/list with all the elements of  $\mathbb{F}_{32}$  in Sage where you consider the representation using a power of a primitive element and the polynomial notation.

Exercise E: Write Algorithm 8.1 (Karatsuba) in Sage.

Best regards,

Diego