

Computer Algebra (2014)-Aalborg University

Lecture 5, October 14th

5th Lecture: Tuesday October 14th, 12:30-16:15 at room G5-109.

- 12:30-14:15 Lecture: Karatsuba's multiplication algorithm. The discrete Fourier Transform (pages 221–232).
- 14:15-16:15 Work in groups, exercises with Sage: A, 8.4, B, C, D, E, 8.9 (only i) + exercises from previous lectures

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

Exercise B: 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 C: Write Algorithm 8.1 (Karatsuba) in Sage.

Exercise D: Check the computations in example 8.6 in [GG].

Exercise E: Which elements of $\mathbb{F}_3[X]/\langle X^3 + X + 1 \rangle$ are units and compute their inverse?, solve it using Sage.

Best regards,

Diego