Computer Algebra (2012)-Aalborg University
Second set of exercises

The deadline for this set of exercises is Thursday 8/11. I would like to get (by email) an electronic file with your solutions. Furthermore, a (brief) reasoned explanation should follow the solution of the exercises, you can write your explanation in the electronic file or print the computer solution and hand-write your explanation.

Solve the following exercises using a Computer Algebra System:

Exercise 1

- Write a table/list with all the elements of $\mathbb{F}_{32}$ in Maple where you consider the representation using a power of a primitive element and the polynomial notation.
- 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 2 Which elements of $\mathbb{F}_3/\langle X^3 + X + 1\rangle$ are units and compute their inverse?, solve it using Sage.

Exercise 3 Implement Algorithm 8.1 (Karatsuba) in Maple or Sage. Compute an example.

Exercise 4 Solve Exercise 8.10 in [GG]. For "$V_1\alpha, V_1\beta$" read "$V_1 f, V_1 g$", where $f, g \in F^8$ are the coefficients of the polynomials f and g.

Exercise 5 Compute the distinct-degree decomposition of the polynomial f in exercise 14.3 in [GG] using a command in Maple or Sage.

Exercise 6 Solve Exercise 14.3 in [GG] using Maple or Sage. You do not have to implement Algorithm 14.3, but you are welcome to do it.

Exercise 7 Factor the polynomial f in exercise 14.12 in [GG] using a command in Maple or Sage.

Exercise 8 Solve Exercise 14.12 in [GG] using Maple or Sage. You do not have to implement Algorithm 14.10, but you are welcome to do it.

Best regards,

Diego