Computeralgebra (2014)-Aalborg University
First set of exercises

The deadline for this set of exercises is Friday November 21st. A (brief) reasoned explanation should follow the solution of the exercises. I would like to get (by email) an electronic file with your solutions and a printed copy in my mail box.

Solve the following exercises using a Computer Algebra System (Maple or Sage, for instance):

Exercise 1

- Let $f = 1+2X+3X^2+4X^3+5X^4+X^{10}$ and $g = 2+5X+6X^2+4X^3+6X^4+3X^5$ polynomials in $\mathbb{Z}[X]$ compute $f \cdot g$. Consider f and g in $\mathbb{Z}/3\mathbb{Z}[X]$, compute $f \cdot g$ in $\mathbb{Z}/3\mathbb{Z}[X]$.
- Implement algorithm 2.3. Represent a polynomial by its coefficients (an array). Consider the polynomial rings over the ring $\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. Compute $f \cdot g$ in $\mathbb{Z}[X]$ and $\mathbb{Z}/3\mathbb{Z}[X]$ using your implementation.
- Consider a new variable in your implementation of algorithm 2.3 that counts the number of operations in R, where $R[X]$ is the polynomial ring that your algorithm is considering. What is the difference between the cost of computing $f \cdot g$ with your algorithm and the bound in section 2.3?

Exercise 2

- Let $f = 5+X+2X^3+3X^4$ and $g = 3+2X+X^2$ polynomials in $\mathbb{Z}[X]$. Compute the polynomial division with remainder of f by g.
- Let $f = 5+X+2X^3+3X^4$ and $h = 3+2X+2X^2$ polynomials in $\mathbb{Z}[X]$. Can we divide f by h?, Consider now f and h in $\mathbb{Z}/3\mathbb{Z}[X]$, compute the polynomial division with remainder of f by h.

Exercise 3 Use Sage to compute the GCD and the Bezout equation ($h = sf + tg$) of two elements f, g (you choose them) in the following rings $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[X]$ and $\mathbb{F}_5[X]$.

Exercise 4 Implement the Traditional Euclidean Algorithm (Algorithm 3.6) for $\mathbb{Z}$ and for $\mathbb{Q}[X]$. Consider a variable in your implementation of algorithm 3.6 that counts the number of operations in $\mathbb{Z}$ (resp. $\mathbb{Q}$) that your algorithm is performing. Consider a couple of examples, What is the difference between the cost of computing the EEA with your algorithm and the bound in section 3.3?

Exercise 5 Let p prime, $a \in \mathbb{F}_p$ and $b \in \mathbb{Z}$ (you choose them).

- Compute $a^b \in \mathbb{F}_p$ using the repeated squaring algorithm (it is implemented in Sage).
- Write an example that shows that Sage cannot perform this computation without using the repeated squaring algorithm

Exercise 6 Compute the inverse of 12345 in the finite field with 12347 elements:

- Using a command in Sage
- Using the Extended Euclidean Algorithm
- Using Little's Fermat Theorem.

Exercise 7 Solve exercise 4.26 in [GG].

Exercise 8 Solve exercise 4.13 in [GG].

Exercise 9 Solve exercise 5.4 in [GG].

Exercise 10 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 11 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 but 4 players can recover it. Consider now the same problem where 2 players cannot recover it but 3 players can recover it.

Exercise 12 Compute a polynomial f in $\mathbb{Q}[X]$ of degree less than 6 such that $f(0) = 0$, $f'(0) = 1$, $f(1) = 1$, $f'(1) = 0$, $f(2) = 1$, $f'(2) = 1$. Draw f using Sage.

Exercise 13 Solve exercise 5.43 in [GG] using Sage.

Exercise 14 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 15 Implement Algorithm 8.1 (Karatsuba), you can represent a polynomial by its coefficients (an array). Compute an example (and trace the algorithm).

Exercise 16

- Implement Algorithm 8.14, the Fast Fourier Transform, you can represent a polynomial by its coefficients (an array).
- Solve Exercise 8.10 in [GG] (you can use the previous algorithm for 8.10-V).

Exercise 17 Compute the distinct-degree decomposition of the polynomial f in exercise 14.3 in [GG] with the help of a command in Sage.

Exercise 18 Solve Exercise 14.3 in [GG]. You do not have to implement Algorithm 14.3, but you are very welcome to do it (and trace it for f).

Exercise 19 Factor the polynomial f in exercise 14.12 in [GG] with the help of a command in Sage.

Exercise 20 Solve Exercise 14.12 in [GG] using Sage. You do not have to implement Algorithm 14.10, but you are very welcome to do it (and trace it for f).

Best regards,

Diego