Algorithmique de base

Master 1, Université de Rennes

29/11/2024 – TD 10

Exercise 1. Let $\mathbb{F} = \mathbb{F}_9$.

(i) Find a 4-th root of unity ω of $\mathbb{F}$.

(ii) Let $f = x^3 + 2x + 1 \in \mathbb{F}[x]$. Compute $\hat{f} = \mathrm{DFT}_\omega(f)$.

(iii) Let $g = x^3 + x^2 + x + 1 \in \mathbb{F}[x]$. Compute $\hat{g} = \mathrm{DFT}_\omega(g)$, $\hat{h} = \hat{f} \cdot \hat{g}$ with coordinate-wise product, and $h = \mathrm{DFT}_{\omega^{-1}}(\hat{h})$.

(iv) Compute $f \cdot g$ in $\mathbb{F}[x]$ and $f \cdot g \mod x^8 - 1$. Compare with your result from (iii).

Exercise 2. Let M be a multiplication function for polynomials. Assume that $M(n)/n \geq M(m)/m$ if $n \geq m$. Show for all $n, m \in \mathbb{N}_+$

1. $M(mn) \geq mM(n)$.
2. $M(n) \geq n$.
3. $M(n) \leq M(n-1) + O(n)$.

Exercise 3. Let $a = x^4 + 2x^3 + 3x^2 + 4x + 5$ and $b = x^2 + 2x + 3$ in $\mathbb{F}_5[x]$, and let $f \in \mathbb{F}_5[x]$ be the reversal of b.

(i) Compute $f^{-1} \mod x^3$.

(ii) Use (i) to find $q, r \in \mathbb{F}_5[x]$ such that $a = qb + r$ and $\deg r < 2$.

Exercise 4.

1. Let f and g be two nonzero polynomials in $\mathbb{C}[x]$. Show that $\mathrm{res}(f, g) = 0$ if and only if f and g have a common factor.
2. Let $a \in \mathbb{C}$. Determine a necessary and sufficient condition on a for the two polynomials

$$x^3 - ax + 1 \quad \text{and} \quad x^2 + a$$

to have a common root.

3. Let $A(T) = \frac{T}{1+T^2}$ and $B(T) = \frac{1-T^2}{1+T^2}$. Find the polynomial defining the curve with $A(T), B(T)$ as parametrization.

4. Let α and β be two algebraic elements over a field K, represented by their minimal polynomials $f(x)$ and $g(x) \in K[x]$. The minimal polynomial of $\alpha+\beta$ over K is one of the irreducible factors of the polynomial $f \star g \in K[x]$ defined by

$$f \star g = \prod_{a,b} (x - (a+b))$$

where a describes the set of roots of f and b the set of roots of g in K.

The polynomial $f \star g$ can also be expressed as

$$f \star g = \mathrm{Res}_y \left(f(x-y), g(y) \right) \in K[x]$$

and its computation can therefore be performed using operations over K.

Calculate the minimal polynomials over $\mathbb{Q}$ of:

$$\sqrt{2} + \sqrt{3} \qquad \text{and} \quad \sqrt{3} + i.$$

Exercise 5. 1. Write 74 in binary.

2. Compute $2^{74} \mod 503$ using the "square-and-multiply" algorithm, detailing the steps.

Exercise 6. Let $x_1, \ldots, x_n \in K$. We define $P_k = x_1^k + \cdots + x_n^k$, for $1 \leq k \leq n$, as the k-th Newton sum.

(1) Write a pseudo-code algorithm that takes as input an element $x \in K$ and an integer n, and returns the list of x^k for k a power of 2 less than or equal to n in $O(\log n)$ arithmetic operations in K.

(2) Deduce an algorithm that takes as input the list $x_1, \ldots, x_n$ and returns the list of P_k for k a power of 2 less than or equal to n in $O(n \log n)$ arithmetic operations in K.

(3) Prove the following equality in formal power series:

$$\frac{X}{1-X} = X + X^2 + X^3 + \cdots$$

(4) Deduce that:

$$\sum_{i=1}^{n} \frac{x_i X}{1 - x_i X} = \sum_{k \geq 1} P_k X^k.$$

(5) Deduce that all P_k for $k \leq n$ can be computed in $O(M(n) \log n)$ operations in K using the fast algorithm for summing fractions.

Exercise 7. Let $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ over $\mathbb{F}_2[x]$, the finite field of two elements. Explain the idea of Berlekamp's Algorithm and use it to factorize $f(x)$ into irreducible polynomials.

Exercise 8. An element $a \neq 0$ in the finite field $\mathbb{F}_q$ is a **square** if the equation $x^2 = a$ has a solution in $\mathbb{F}_q$.

1. Show that when $\mathrm{char}(\mathbb{F}_q) \neq 2$ then exactly half the elements of $\mathbb{F}_q^*$ squares.
2. Find all Fermat liars for $n = 15$.
3. Euler showed that if p is an odd prime, then $a \in \mathbb{F}_p^*$ is a square if and only if $a^{\frac{p-1}{2}} = 1 \mod p$. Show that if p and $2p-1$ are both prime and $n = p(2p-1)$, then 50% of the elements in $\mathbb{Z}_n^*$ are Fermat liars, namely all those which are squares modulo $2p-1$.
4. Compute $2^{1000005} \mod 55$.

Exercise 9.

1. How can the extended Euclidean algorithm be used to compute the inverse of an element in the finite field $\mathbb{F}_p$?
2. The basic building block of the classical algorithm is the fact that the gcd of a and b is equal to the gcd of $a \mod b$ and b. This allows the size of the operands to decrease through successive applications of this property. On which property is the binary version of this algorithm based?
3. What does the binary version bring compared to the classical version (justify your answers)?