TD 1: Multiprecision

Exercice 1. Polynomial Arithmetic

A polynomial $P = p_0 + p_1X + \cdots + p_{n-1}X^{n-1}$ is represented by an array of n elements $[p_0, p_1, \ldots, p_{n-1}]$.

a. If you have access to an algorithm computing the product of two polynomials, explain how you can deduce an algorithm computing the product of two multiprecision integers

b. Propose a *Divide and Conquer* algorithm for the multiplication of two polynomials of same degree.
Indication: one can use the identity:

$$(P_0 + XP_1)(Q_0 + XQ_1) = P_0Q_0 + X(P_0Q_1 + P_1Q_0) + X^2P_1Q_1$$

c. Analyse its cost (when the size of the polynomials is a power of two).

d. In 1960, Karatsuba proposed to use instead the following formula:

$$(P_0 + XP_1)(Q_0 + XQ_1) = P_0Q_0 + X((P_0 + P_1)(Q_0 + Q_1) - P_0Q_0 - P_1Q_1) + X^2P_1Q_1$$

Deduce an algorithm and analyse it complexity.

We now investigate the decomposition of polynomials in three: $P = P_0 + XP_1 + X^2P_2$ et $Q = Q_0 + XQ_1 + X^2Q_2$. Toom proposed a formula computing $P \times Q$ using the five following values:

$$\begin{aligned}
M_0 &= P_0Q_0 \\
M_1 &= (P_0 + P_1 + P_2)(Q_0 + Q_1 + Q_2) \\
M_2 &= (P_0 - P_1 + P_2)(Q_0 - Q_1 + Q_2) \\
M_3 &= (P_0 + 2P_1 + 4P_2)(Q_0 + 2Q_1 + 4Q_2) \\
M_4 &= P_2Q_2
\end{aligned}$$

The product $R = P \times Q = R_0 + R_1X + R_2X^2 + R_3X^3 + R_4X^4$ is obtained as follows:

$$\left\{\begin{aligned}
R_0 &= M_0 \\
R_1 &= \tfrac{1}{6}(-3M_0 + 6M_1 - 2M_2 - M_3 + 12M_4) \\
R_2 &= \tfrac{1}{2}(-2M_0 + M_1 + M_2 - 2M_4) \\
R_3 &= \tfrac{1}{6}(3M_0 - 3M_1 - M_2 + M_3 - 12M_4) \\
R_4 &= M_4
\end{aligned}\right. \tag{1}$$

e. What is the cost of the corresponding algorithm multiplying polynomials of arbitrary degrees?

f. Justify that the formulas computing the M_i can be viewed as evaluations. State in which points?

g. Deduce how the coefficients of the formule (1) have been found.

More generally, Toom-Cook algorithms at order k compute the product $P \times Q$ of two polynomials of size k in $(2k-1)$ multiplications.

h. What is the cost of these algorithms ?

i. Explain how to construct them.

j. Conclude on the cost of multiplying polynomials.

Exercice 2. Fast exponentiation algorithm

We will study the cost of computing a^k where a is an element of a ring R and k a positive integer.

a. Propose a naive algorithm, named $\texttt{NaiveExp}(a, k)$.

b. By relating a^k with $a^{\frac{k}{2}}$, propose a recursive algorithm, named $\texttt{RecExp}(a, k)$

c. Propose an iterative algorithm $\texttt{IterExp}(a, k)$ (equivalent to $\texttt{RecExp}(a, k)$ in cost), based on the binary representation of k

d. When $R = \mathbb{Z}/n\mathbb{Z}$ with $n < 2^{32}$, all basic arithmetic operations in R take $\Theta(1)$. What is the cost of the three above algorithms?

e. Same question when n may be any integer (possibly larger than 2^{32}). Which of these algorithms can actually be run in practice for n of bit-size 128?

f. Same question when $R = \mathbb{Z}$.