

---

## TUTORIAL 3

---

### 1 Recursive division

Let  $a$  and  $b$  be two polynomials in  $K[x]$  such that  $\deg a = 4n$  and  $\deg b = 2n$  and take  $n$  to be a power of 2. We decompose  $a$  and  $b$  such that  $a(x) = a_h(x)x^{2n} + a_l(x)$  and  $b(x) = b_h(x)x^n + b_l(x)$ , where  $\deg a_h, \deg a_l \leq 2n$  and  $\deg b_h, \deg b_l \leq n$ .

Consider  $D(n)$  as the complexity, in number of arithmetic operations over  $K$ , required to perform the Euclidean division of a degree  $2n$  polynomial by a degree  $n$  polynomial. Similarly, we denote by  $M(n)$  the complexity of multiplying two degree  $n$  polynomials over  $R$ .

We perform the Euclidean division of  $a_h$  by  $b_h$  (i.e.  $a_h = b_h q_h + r_h$ ,  $\deg r_h < \deg b_h$ ).

1. Show that  $\deg(a - bq_h x^n) < 3n$  and that  $a - bq_h x^n$  is computable using  $D(n) + M(n) + O(n)$  operations.
2. Show that we can finish dividing  $a$  by  $b$  using another  $D(n) + M(n) + O(n)$  operations.
3. What is the value of  $D(n)$  if  $M(n) = n^\alpha$ ,  $\alpha > 1$ ?
4. Same question as before, for  $M(n) = n(\log n)^\alpha$ ,  $\alpha > 1$ .

### 2 Applications of the Extended Euclidean Algorithm (EEA)

#### 2.1 Computing the inverse

1. Let  $n$  be an integer, and  $0 \leq a < n$  be such that  $\gcd(a, n) = 1$ . Give an algorithm that computes  $a^{-1} \pmod n$  in time  $O(M(\log n) \log \log n)$ .
2. Let  $P \in K[X]$  be a polynomial of degree  $d$  with coefficients in a field  $K$  and  $Q \in K[X]$  be a polynomial of degree less than  $d$ , such that  $\gcd(P, Q) = 1$ . Prove that  $Q$  is invertible modulo  $P$  and give an algorithm to compute its inverse using  $O(M(d) \log d)$  operations in  $K$ .

#### 2.2 Diophantine equation

The aim of this exercise is to describe the set of all solutions  $(u, v)$  of the equation

$$au + bv = t \tag{1}$$

1. Show that if  $(u, v) = (s_1, s_2)$  is a solution of (1), the general solution is of the form  $(u, v) = (s_1 + s'_1, s_2 + s'_2)$  for  $(s'_1, s'_2)$  satisfying  $as'_1 + bs'_2 = 0$ .
2. Find all solutions of  $au + bv = 0$  for  $a, b$  coprime.
3. Find a solution of (1) for  $a, b$  coprime.
4. Observe that  $t$  must be divisible by  $\gcd(a, b)$ .
5. Using the previous questions, give the general solution of (1).

### 3 Rational function reconstruction

Let  $K$  be a field,  $m \in K[X]$  of degree  $n > 0$ , and  $f \in K[X]$  such that  $\deg f < n$ . For a fixed  $k \in \{1, \dots, n\}$ , we want to find a pair of polynomials  $(r, t) \in K[X]^2$ , satisfying

$$r = t \cdot f \pmod{m}, \quad \deg r < k, \quad \deg t \leq n - k \quad \text{and} \quad t \neq 0 \quad (2)$$

1. Consider  $A(X) = \sum_{l=0}^{N-1} a_l X^l \in K[X]$  a polynomial. Show that if  $A(X) = P(X)/Q(X) \pmod{X^N}$ , where  $P, Q \in K[X]$ ,  $Q(0) = 1$  and  $\deg P < \deg Q$ , then the coefficients of  $A$ , starting from  $a_{\deg Q}$  can be computed as a linear recurrent sequence of previous  $\deg Q$  coefficients of  $A$ . What can you say in the converse setting when the coefficients of  $A$  satisfy a linear recurrence relation?
2. Inside (2), consider the case when  $m = x^n$ . Describe a linear algebra-based method for finding some  $t$  and  $r$ . (Hint: do **not** use the previous question).
3. Show that, if  $(r_1, t_1)$  and  $(r_2, t_2)$  are two pairs of polynomials that satisfy (2), then we have  $r_1 t_2 = r_2 t_1$ . We will use the Extended Euclidean Algorithm to solve problem (2).
4. Let  $r_j, u_j, v_j \in F[X]$  be the quantities computed during the  $j$ -th pass of the Extended Euclidean Algorithm for the pair  $(m, f)$ , where  $j$  is minimal such that  $\deg r_j < k$ . Show that  $(r_j, v_j)$  satisfy (2). What can you say about the complexity of this method?
5. **Application.** Given  $2n$  consecutive terms of a recursive sequence of order  $n$ , give the recurrence. (Hint: this is where you use question 1). Illustrate your method on the Fibonacci sequence.