TUTORIAL 4

1 Applications of the extended euclidean algorithm

1.1 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 $a^{-1} \mod n$ in time $O(M(\log n) \log\log n)$. (Hint : use the extended euclidean algorithm).

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.

1.2 Diofantine 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. (Hint: Use Extended Euclidean Algorithm.)

4. Observe that t must be divisible by $\gcd(a, b)$.

5. Using the previous questions, give the general solution of (1).

2 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 $k \in \{1, \ldots, n\}$, we want to find a pair of polynomials $(r, t) \in K[X]^2$, satisfying

$$r = t \cdot f \mod m, \qquad \deg r < k, \qquad \deg t \leqslant n - k \quad \text{and} \quad t \neq 0 \tag{2}$$

1. Consider $A(X) = \sum_{l=0}^{N-1} a_l X^l \in K[X]$ a polynomial. Show that if $A(X) = P(X)/Q(X) \mod X^N$, 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 a 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.

3 Introduction to resultant

The objective of this exercise is to compute the gcd of elements in the ring $K[X, Y]$ with K a field, or in $\mathbb{Z}[X]$. Then, we will use the same idea to compute the intersection of two curves parametrized by a polynomial equation in $\mathbb{R}^2$.

1. Can we compute the euclidean division of X by 2 in $\mathbb{Z}[X]$? Give an equivalent in $K[X, Y]$, i.e. find two elements in $K[X, Y]$ such that we cannot compute their euclidean division (where we see $K[X, Y] = (K[Y])[X]$ as polynomials in X with coefficients in $K[Y]$).

   The problem here, when we want to compute the euclidean division of elements in $(K[Y])[X]$ and $\mathbb{Z}[X]$, is that the coefficients of our polynomials in X are not in a field but in the rings $K[Y]$ and $\mathbb{Z}$. In order to circumvent this problem, we embed these rings in their fraction field, that is we embed $K[Y]$ in $K(Y)$ and $\mathbb{Z}$ in $\mathbb{Q}$.

   If P and Q are elements of $\mathbb{Z}[X]$, we will see them as elements of $\mathbb{Q}[X]$ and compute their gcd D in $\mathbb{Q}[X]$. Our objective is then to recover their gcd in $\mathbb{Z}[X]$ (this works in the same way for $K[Y][X]$ and $K(Y)[X]$).

2. What is the gcd of $6X$ and $4X^2 + 8X$ in $\mathbb{Q}[X]$? And in $\mathbb{Z}[X]$?

   Let $\mathcal{R}$ be one of the rings $\mathbb{Z}$ or $K[Y]$, and $P \in \mathcal{R}[X]$. We say that P is primitive if the gcd of the coefficients of P is 1 (for instance, $2 + 4X + 5X^2 \in \mathbb{Z}[X]$ is a primitive polynomial).

3. **(Gauss Lemma)** Let P and Q be primitive polynomials in $\mathbb{Z}[X]$. Prove that their product PQ is also primitive.

4. Let $P, Q \in \mathbb{Z}[X]$ with Q primitive. Assume we have $R \in \mathbb{Q}[X]$ such that $P = QR$. Prove that the coefficients of R are in fact in $\mathbb{Z}$.

5. Let P and Q be primitive polynomials in $\mathbb{Z}[X]$. Deduce from the previous questions a way of computing the gcd of P and Q in $\mathbb{Z}[X]$, from the one in $\mathbb{Q}[X]$.

6. What can we do if P and Q are not primitive ?

   Remark. This method for computing the gcd of polynomials in $\mathbb{Z}[X]$ also works the same way in $K[Y][X]$.

7. **(Resultant)** Let $A[Y, X]$ and $B[Y, X]$ be coprime polynomials in $K[Y][X]$. Prove that there exist polynomials $U, V \in K[X][Y]$ and $S \in K[Y]$ such that

   $$U[Y, X]A[Y, X] + V[Y, X]B[Y, X] = S[Y]$$

   (Hint : use Bezout in $K(Y)[X]$, with $K(Y)$ a field).

8. **(Application)** Find the polynomials U, V and S for $P = X^2 - XY + Y - 1$ and $Q = X + Y^2 - 1$ in $\mathbb{R}[X]$.

9. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be curves in $\mathbb{R}^2$ parametrized by the equations $x = 1 - y^2$ and $x^2 - xy = 1 - y$ respectively. Find all the intersection points of theses curves in $\mathbb{R}^2$. (Hint: this is equivalent to finding all $(x, y) \in \mathbb{R}^2$ that are common roots of the polynomials P and Q of the previous question).