A Euclidean approach through resultants

Mohab Safey El Din

In this course, we target to obtain a full algorithm for solving bivariate polynomial systems of equations, say in $\mathbb{K}[x_1, x_2]$ where $\mathbb{K}$ is a field. Further, $\overline{\mathbb{K}}$ denotes an algebraic closure of $\mathbb{K}$. Recall that, given a polynomial system $f_1 = \cdots = f_p = 0$ in $\mathbb{K}[x_1, x_2]$, we aim at

- deciding whether the solution set $V \subset \overline{\mathbb{K}}^2$ of our input polynomial system has solutions;
- if V has solutions, decide whether the number of solutions is finite and in that case, provide a *triangular description* of the solution set

$$w(x_1) = 0, w_2(x_1, x_2) = 0.$$

The core rationale that underlies these algorithms is as follows. Two bivariate polynomials f_1, f_2 as above have a common solution (α, β) in $\overline{\mathbb{K}}^2$ if and only if $f_1(\alpha, x_2)$ and $f_2(\alpha, x_2)$ (which lie in $\overline{\mathbb{K}}[x_2]$) have a greatest common divisor (gcd) of positive degree in $\overline{\mathbb{K}}[x_2]$. To see this, one can just remark that since β is a common root of $f_1(\alpha, x_2)$ and $f_2(\alpha, x_2)$, $x_2 - \eta$ divides these two polynomials and then their gcd has degree at least 1.

Hence, in a way, the vanishing of the first (univariate) polynomial w we want to compute is an algebraic (polynomial) condition such that for all $\alpha \in \overline{\mathbb{K}}$ at which w vanishes, the univarite polynomials $f_1(\alpha, x_2)$ and $f_2(\alpha, x_2)$ have a gcd of degree greater than or equalled to 1.

As a consequence, we need to investigate more about gcd computations. This will lead us to recall the Euclidean *division* and the Euclidean algorithm which hold in the univariate cases.

We will see that these simple concepts will allow us to understand well the structure of algebraic objects that we call ideals in $\mathbb{K}[x]$ and solve the algorithmic questions raised at the end of the previous chapter for bivariate polynomial systems.

The study of these division algorithms will also be instructive to tackle the multivariate case in the next chapters.

Hereafter, all rings will be considered commutative and unitary.

Contents

1 Back to univariate polynomials

1.1 Division algorithm

Let $\mathbb{K}$ be a field and a, b be two polynomials in $\mathbb{K}[x]$.

Proposition 1. *Assume that $b \neq 0$. There exist unique polynomials q, r in $\mathbb{K}[x]$ such that*

$$a = qb + r \qquad \text{with} \qquad \deg(r) < \deg(b).$$

The polynomial q (resp. r) is called the quotient (resp. remainder) of the Euclidean division of a by b.

Proof. Assume first that a has degree 0. When b has positive degree, observe that one can take $q = 0$ and $r = a$. When b has degree 0, it is a *non-zero* constant in the field $\mathbb{K}$ (by assumtion), one can take $q = \frac{a}{b}$ and $r = 0$. Uniqueness is immediate.

The sequel of the proof is by increasing induction on the degree α of a ; hence we assume that the result holds for any pair of polynomials (a', b') with $\deg(a') < \alpha$.

Let α be the degree of a and β be the degree of b. We deduce that

$$a = a_\alpha x^\alpha + a_{\alpha-1}x^{\alpha-1} + \cdots + a_0, \qquad \text{with } a_\alpha \neq 0$$
$$b = b_\beta x^\alpha + b_{\beta-1}x^{\alpha-1} + \cdots + b_0, \qquad \text{with } b_\beta \neq 0$$

Since $b_\beta \neq 0$ and $\mathbb{K}$ is a field, one can invert it. In particular, $\frac{a_\alpha}{b_\beta}x^{\alpha-\beta}b$ has the same degree and leading coefficient as a. Hence, $a' = a - \frac{a_\alpha}{b_\beta}x^{\alpha-\beta}b$ has degree $\leqslant \alpha - 1$. Then, applying our induction assumption, we deduce that there exists (q', r') such that $a' = q'b + r'$. Hence, taking $q = \frac{a_\alpha}{b_\beta}x^{\alpha-\beta} + q'$ ends the proof of the existence of the couple (q, r).

The uniqueness statement is left to the reader. □

Exercise 1

The above proof exhibits the genesis of the Euclidean division algorithm. Formalize it to write it in pseudo-code. Analyze its theoretical complexity.
Finally, complete the proof by establishing the uniqueness of the remainder r.

Theorem 2. *Let a, b be polynomials in $\mathbb{K}[x]$ of respective degrees n and m. On input (a, b), the Euclidean division algorithm performs $O(m(n-m))$ arithmetic operations in $\mathbb{K}$.*

Exercise 2

Perform the division algorithm with inputs

- $a = x^3 + 2x^2 - x + 1$ and $b = 3x + 1$
- $a = x^3 + 2x^2 - x + 1$ and $b = x^2 - 2x - 2$

Observe that when dividing a polynomial a by a polynomial $b = \alpha x + \beta$, the obtained remainder is a constant which coincides with the evaluation a at $-\frac{\beta}{\alpha}$.

Actually, at the roots of b, a and the remainder r coincide.

Lemma 3. *Let D be the degree of $f \in \mathbb{K}[x] - \{0\}$. Then f has* at most *D roots in $\mathbb{K}$.*

Proof. The proof is by induction on the degree D of f. Of course, when $D = 0$, f is a non-zero constant and hence it has no root.

Now let $D > 0$ be the degree of f and assume that our statement holds for all polynomials in $\mathbb{K}[x] - \{0\}$ of degree $\leqslant D - 1$. If f has no root, then we are done. Else let x be a root of f. Using the division algorithm, we can write uniquely f as follows

$$f = q(x - x) + r.$$

with $\deg(r) < 1$. Also, since x is a root of f, we have $r = 0$ and we deduce that $f = q(x - x)$. Remark that $\deg(q) = D-1$ and all roots of q are roots of f. Also q cannot be the zero polynomial else f would be and this is forbidden by our assumption. Applying our induction assumption on q, we are done. □

1.2 Ideals of univariate polynomial rings and divisions

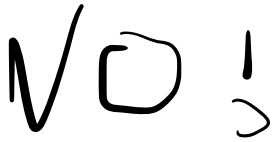
Definition 4. *Let R be a ring and I be a subset of R. One says that I is an ideal of R if and only if the following holds:*

- *for all a, b in I, $a + b$ lies in I*
- *for all $r \in R$ and $a \in I$, $r.a \in I$.*

For instance, the subset of even integers in $\mathbb{Z}$ is an ideal of $\mathbb{Z}$ equipped with the addition and multiplication of integers.

Exercise 3

Prove the above statement. Is the set of odd integers an ideal of $\mathbb{Z}$?



Exercise 4

Let R be a ring equipped with binary operations $(+, \times)$. Denote by 0 its identity element for $+$. Prove that $\{0\}$ is an ideal of R.

Definition 5. *Let R be a ring and S be a subset of R. The ideal generated by S is the subset of R*

$$\{r_1 s_1 + \cdots + r_k s_k \mid k \geqslant 1, r_i \in R \text{ and } \{s_1, \ldots, s_k\} \subset S\}.$$

We will denote it by $\langle S \rangle$.

Exercise 5

In the above definition, prove that

$$\{r_1 s_1 + \cdots + r_k s_k \mid k \geqslant 1, r_i \in R \text{ and } \{s_1, \ldots, s_k\} \subset S\}.$$

is an ideal of R.

We will see that *ideals of multivariate polynomial rings* are important mathematical objects which play a central role in the design of algorithms for polynomial system solving. We will see that, in some sense, algorithms are as involved as the structure of rings and polynomial ideals are complicated.

However, the univariate case yields some interesting simplifications.

Definition 6. *Let R be a ring and $I \subset R$. One says that I is a* principal *ideal if and only if I is generated by a* single *element of R.*

One says that R is a principal ring if all its ideals are principal.

Exercise 6

Let $R = \mathbb{K}[x, y]$. Prove that R is not a principal ring.
Hint. Consider the ideal $\langle x, y \rangle$.

Exercise 7

Let 1 be the identity element of multiplication in the ring R. What is the ideal generated by 1 in R ?

Theorem 7. *The univariate polynomial ring $\mathbb{K}[x]$ is principal.*

Proof. Let I be an ideal of $\mathbb{K}[x]$. If $I = \langle 0 \rangle$ (i.e. $I = \mathbb{K}[x]$) our statement holds trivially. Else, there exists a polynomial of *minimal* degree in I ; that degree being $\geqslant 0$ (because, now, we assume $I \neq \langle 0 \rangle$). Let us call a such an element.

We prove now that $I = \langle a \rangle$. Take $b \in I$; our goal is now to prove that there exists $w \in \mathbb{K}[x]$ such that $b = aw$ (and then one can conclude that I is radical). Using the division algorithm we deduce that there exist unique q and r in $\mathbb{K}[x]$ with $\deg(r) < \deg(a)$ such that

$$b = qa + r.$$

Since $r = b - qa$, we deduce that $r \in I$. But since $\deg(r) < \deg(a)$ and a has minimal degree in amongst the degrees of the polynomial in I, we deduce that $r = 0$. Hence $b = aq$ and one can conclude that I is principal and generated by a. □

Exercise 8

Is the generator of a principal ideal in $\mathbb{K}[x]$ unique (up to multiplication by elements in $\mathbb{K}$)?

1.3 Gcd and Euclide's algorithm

Definition 8. *Let a and b be polynomials in $\mathbb{K}[x]$. A greatest common divisor (gcd) for (a, b) is a polynomial $g \in \mathbb{K}[x]$ such that:*

- *g divides a and b;*
- *if another polynomial $h \in \mathbb{K}[x] - \mathbb{K}$ divides a and b then, h divides g.*

Further, given a and b in $\mathbb{K}[x]$, we denote by $\gcd(a, b)$ the gcd of (a, b).

Lemma 9. *Let a and b in $\mathbb{K}[x]$ and $g = \gcd(a, b)$. Let (q, r) be the unique polynomials such that:*

$$a = bq + r$$

with $\deg(r) < \deg(b)$. Then $g = \gcd(b, r)$.

Proof. First, we prove that g divides b and r. Since $g = \gcd(a, b)$, there exist c and d in $\mathbb{K}[x]$ such that $a = cg$ and $b = dg$. Then, we have

$$\begin{aligned} r &= a - bq \\ &= cg - dgq \\ &= (c - dq)g \end{aligned}$$

and our claim follows.

Now, take h which divides both b and r. We prove that h divides g. So, let d' and e' be in $\mathbb{K}[x]$ such that $b = d'h$ and $r = e'h$. We deduce that

$$\begin{aligned} a &= qb + r \\ &= qd'h + e'h \\ &= (qd' + e')h \end{aligned}$$

and then h divides a. Since $g = \gcd(a, b)$, we deduce that h divides g as requested. □

The above lemma is at the foundations of Euclide's algorithm which takes as input a and b and consists in repeatedly perform Euclidean divisions as indicated be the pseudo-code below.

Input. a, b in $\mathbb{K}[x]$
Output. a gcd of (a, b) in $\mathbb{K}[x]$.

- $s \leftarrow a, t \leftarrow b$
- while $t \neq 0$ do
  $r \leftarrow \text{remainder}(s, t)$
  $s \leftarrow t$
  $t \leftarrow r$
- return s

Exercise 9

Analyze the complexity of the above algorithm.

Theorem 10. *Let a, b in $\mathbb{K}[x]$ of respective degrees $n \geqslant m$. On input (a, b), Euclide's algorithm performs $O(n^2)$ arithmetic operations in $\mathbb{K}$.*

Proposition 11. *Let a and b in $\mathbb{K}[x]$. Then the following holds:*

- $\gcd(a, b)$ *exists and is unique up to multiplication by a scalar in $\mathbb{K}$;*
- $\gcd(a, b)$ *is a generator of the ideal $\langle a, b\rangle$;*
- *Euclide's algorithm finds* $\gcd(a, b)$.

Proof. Let us consider the ideal $I = \langle a, b\rangle \subset \mathbb{K}[x]$. Thanks to Theorem 7, we know that there exists $g \in \mathbb{K}[x]$ such that $I = \langle g\rangle$ (I is principal). Thanks to the proof of that theorem, we know that up to multiplication by elements in $\mathbb{K} - \{0\}$, g is unique and has minimal degree among the polynomials in I. We claim that one can take $g = \gcd(a, b)$.

The intuitive idea supporting this claim is that any common root of a and b is a root of g, as is the case for $\gcd(a, b)$.

More formally, note that since $I = \langle g\rangle$, one deduces that g divides both a and b. Now, take $h \in \mathbb{K}[x]$ which divides both a and b. According to Definition 8, we need to prove that h divides g. To prove this, it suffices to establish that $h \in \langle g\rangle = \langle a, b\rangle$.

So let c and d such that $a = ch$ and $b = dh$. Since $g \in \langle a, b\rangle$, we deduce that there exist q_1 and q_2 such that

$$q_1 a + q_2 b = g$$

$$q_1 ch + q_2 dh = g$$
$$(q_1 c + q_2 d)h = g$$

which establishes that h divides g.

we just established the existence of the gcd. It remains to show that it is unique up to multiplication by a scalar in $\mathbb{K} - \{0\}$. So assume that there is another gcd g' for (a, b). Using again Definition 8 (2nd assertion), we deduce that both g divides g' and g' divides g. This implies that g' is obtained by multiplying g with a non-zero element of $\mathbb{K}$.

We established the first two claims of the proposition. It remains to show that Euclide's algorithm allows us to find $\gcd(a, b)$. But this comes with an immediate induction argument using Lemma 9. □

Exercise 10

Detail the proof that, on input a and b as above, Euclide's algorithm outputs $\gcd(a, b)$.

We defined the gcd for couples of polynomials in $\mathbb{K}[x]$ but actually, that definition can be extended to finite sequences of polynomials in $\mathbb{K}[x]$.

Definition 12. *Let $f_1, \ldots, f_p$ be polynomials in $\mathbb{K}[x]$. A greatest common divisor (gcd) for $(f_1, \ldots, f_p)$ is a polynomial $g \in \mathbb{K}[x]$ such that:*

- *g divides f_i for $1 \leqslant i \leqslant p$;*
- *if another polynomial $h \in \mathbb{K}[x] - \mathbb{K}$ divides all the f_i's then, h divides g.*

The proof of the next result is left to the reader.

Proposition 13. *Let $f_1, \ldots, f_p$ in $\mathbb{K}[x]$. Then the following holds:*

- *$\gcd(f_1, \ldots, f_p)$ exists and is unique up to multiplication by a scalar in $\mathbb{K}$;*
- *$\gcd(f_1, \ldots, f_p)$ is a generator of the ideal $\langle f_1, \ldots, f_p \rangle$;*
- *when $p \geqslant 3$, $\gcd(f_1, \ldots, f_p) = \gcd(f_1, \gcd(f_2, \ldots, f_p))$;*

Exercise 11

Prove the above proposition.

Exercise 12

Design an algorithm for computing $\gcd(f_1, \ldots, f_p)$ and analyze its complexity.

It should be observed that the material in this section allows us to answer algorithmic questions which were raised at the end of the previous chapter. We exhibit here how to tackle them for ideals generated by two elements of $\mathbb{K}[x]$.

For instance, it is now clear that all ideals of $\mathbb{K}[x]$ are finitely generated. Also, given (a, b) in $\mathbb{K}[x]$ and $c \in \mathbb{K}[x]$, one can decide now easily if $c \in \langle a, b \rangle$. Indeed, it suffices to compute $g = \gcd(a, b)$ (Euclide's algorithm) and check that g divides c (Division algorithm).

Finally, observe that computing $I_{\mathbb{K}}(V(a, b))$ could be reduced to computing the gcd of (a, b) and computes its square-free form.

Exercise 13

Generalize the above solutions to ideals of $\mathbb{K}[x]$ generated by more than two polynomials.

2 Euclide's algorithm, linear algebra and resultants

We have studied the division and Euclide's algorithms to compute gcds of polynomials in univariate polynomial rings. Recall that our goal in this chapter is to solve polynomial systems in $\mathbb{K}[x_1, x_2]$.

2.1 Sylvester matrix and resultant

In the sequel, we let R be a ring.

Definition 14. *Let a and b be two polynomials of $R[x]$ of degree $p > 0$ and $q > 0$.*

$$a = a_p x^p + \cdots + a_0$$
$$b = b_q x^q + \cdots + b_0.$$

The Sylvester matrix *associated to (a, b), denoted by $Sylv(a, b)$ is the transpose of the $(p+q)\times(p+q)$ matrix*

$$\begin{bmatrix}
a_p & 0 & \cdots & 0 & b_q & 0 & \cdots & 0 \\
a_{p-1} & a_p & & \vdots & b_{q-1} & b_q & & \vdots \\
\vdots & a_{p-1} & \ddots & \vdots & \vdots & b_{q-1} & \ddots & \vdots \\
a_1 & \vdots & & 0 & b_1 & \vdots & & 0 \\
a_0 & a_1 & & a_p & b_0 & b_1 & & b_q \\
0 & a_0 & & a_{p-1} & 0 & b_0 & & b_{q-1} \\
\vdots & 0 & & \vdots & \vdots & 0 & & \vdots \\
\vdots & \vdots & \ddots & a_1 & \vdots & \vdots & \ddots & b_1 \\
0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0
\end{bmatrix}$$

Note that the first row of $Sylv(a, b)$ is the row vector of coefficients of $x^{q-1}a$ in the monomial basis $\mathcal{B} = \left(x^{p+q-1}, x^{p+q-2}, \ldots, 1\right)$, the second row is the row vector of coefficients of $x^{q-2}a$ in $\mathcal{B}$, the next one is the same for $x^{q-3}a$ and so on up to reaching a and switching to $x^{p-1}b$, followed by $x^{p-2}b$, and so on up to reaching b.

$$\begin{bmatrix}
a_p & a_{p-1} & 0 & \cdots & a_0 & 0 & \cdots & 0 \\
0 & a_p & a_{p-1} & \cdots & \cdots & a_0 & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & & & \ddots & 0 \\
0 & \cdots & 0 & a_p & a_{p-1} & \cdots & \cdots & a_0 \\
b_q & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\
0 & b_q & \cdots & \cdots & b_0 & 0 & \cdots & \vdots \\
\vdots & 0 & \ddots & & & \ddots & & \vdots \\
\vdots & \vdots & \ddots & \ddots & & & \ddots & 0 \\
0 & 0 & \cdots & 0 & b_q & \cdots & \cdots & b_0
\end{bmatrix}
\begin{matrix}
\leftarrow x^{q-1}a \\
\leftarrow x^{q-2}a \\
\vdots \\
\leftarrow a \\
\leftarrow x^{p-1}b \\
\leftarrow x^{p-2}b \\
\vdots \\
\vdots \\
\leftarrow b
\end{matrix}$$

Note that the above definitions only hold when both p and q are positive. When $q = 0$ (hence b is a non-zero constant in $\mathbb{K}$), the Sylvester matrix associated to (a, b) boils down to writing the coefficients of $x^{p-1}b, \ldots, b$ in the basis $\mathcal{B}$ (with $q = 0$) which is then a diagonal matrix of size $p \times p$ with b on the diagonal.

This matrix arises naturally when considering the following problem: given $a, b \in R[X]$, is there any u, v in $R[X]$ such that $\deg u < \deg b = q$, $\deg v < \deg a = p$ and $au + bv = 0$?

Indeed, for $u = u_0 + \cdots + u_{q-1}x^{q-1}$ and $v = v_0 + \cdots + v_{p-1}x^{p-1}$ satisfying the above degree constraints, $au + bv = 0$

$$\begin{bmatrix}
a_p & 0 & \cdots & 0 & b_q & 0 & \cdots & 0 \\
a_{p-1} & a_p & & \vdots & b_{q-1} & b_q & & \vdots \\
\vdots & a_{p-1} & \ddots & \vdots & \vdots & b_{q-1} & \ddots & \vdots \\
a_1 & \vdots & & 0 & b_1 & \vdots & & 0 \\
a_0 & a_1 & & a_p & b_0 & b_1 & & b_q \\
0 & a_0 & & a_{p-1} & 0 & b_0 & & b_{q-1} \\
\vdots & 0 & & \vdots & \vdots & 0 & & \vdots \\
\vdots & \vdots & \ddots & a_1 & \vdots & \vdots & \ddots & b_1 \\
0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0
\end{bmatrix}
\begin{bmatrix}
u_{q-1} \\ \vdots \\ u_0 \\ v_{p-1} \\ \vdots \\ v_0
\end{bmatrix} = 0.$$

In the sequel, applying the superscript ^{t} to a matrix means that we consider its transpose.

Theorem 15. *For a and b as above, the kernel of $Sylv(a, b)^t$ coincides with the set of all couples of polynomials (u, v) satisfying $au + bv = 0$ with $\deg(u) < \deg(b)$ and $\deg(v) < \deg(a)$.*

Proof. This proof has already been done during class. □

Proposition 16. *The polynomials a and b are coprime if and only if $\det(Sylv(a, b)) \neq 0$.*

Proof. If a and b are coprime, then from $au + bv = 0 \iff au = -bv$, one deduces that b divides u and a divides v. But $\deg u < \deg b$ and $\deg v < \deg a$, so that $u = v = 0$ and $\det Sylv(a, b) \neq 0$.

If they are not coprime, $u = b/\gcd(a, b)$ and $v = -a/\gcd(a, b)$ are nontrivial solutions of the problem, so that $\det Sylv(a, b) = 0$. □

Definition 17 (Resultant). *For a and b as above, the resultant associated to (a, b), denoted by $res(a, b)$ is the determinant of $Sylv(a, b)$.*

Exercise 14

When a has degree $p > 0$ and b has degree 0 (hence b is a constant), the resultant associated to (a, b) is b^p.

Proposition 18. *For a and b as above in $R[x]$, there exist (u, v) in $R[x] \times R[x]$ such that $\deg(u) < \deg(b)$, $\deg(v) < \deg(b)$ and*

$$au + bv = res(a, b).$$

Proof. This proof has already been done during class. □

Theorem 19 (Poisson formula). *Let a and b in $R[x]$. Assume that $a = a_p \prod_{i=1}^{p}(a - \alpha_i)$ and $b = b_q \prod_{i=1}^{q}(x - \beta_i)$.*

Then, the following holds.

$$res(a, b) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j)$$

Proof. This proof has already been done during class. □

Corollary 20. *Let a, b and h be polynomials in $R[x]$. The following holds.*

$$res(a, bh) = res(a, b)res(a, h).$$

Proof. This proof has already been done during class. □

The above results can be used to prove the following extra properties.

Lemma 21. *Let $a = a_p \prod_{i=1}^{n}(x - \alpha_i)$*

$$res(a, b) = a_p^q \prod b(\alpha_i)$$

Proof. This proof has already been done during class. □

Proposition 22. *Assume now that a and b have coefficients in a field $\mathbb{K}$ and let r be the remainder of the euclidean division of a by b. Then the following holds:*

$$res(a, b) = (-1)^{pq} lc(b)^{p - \deg(r)} res(b, r)$$

where $lc(b)$ stands for the leading coefficient of b.

Theorem 23. *There exists an algorithm which on input a and b in $\mathbb{K}[x]$ computes the resultant associated to (a, b) in time $O(D^2)$ where $D = \max(\deg(a), \deg(b))$.*

Remark. This is not the state-of-the art. Nowadays, there exist algorithms computing the resultant in time $O\tilde{}(\deg(A))$ when the coefficients lie in a ring that supports FFT (Fast Fourier Transform).

Exercise 15

Compute and compare

- the resultant associated to $ax^2 + bx + c$ and $dx + e$ when considering these polynomials in the ring $\mathbb{Q}[a, b, c, d, e][x]$;
- the resultant associated to $bx + c$ and $dx + e$ (hence specializing the input at $a = 0$).

2.2 Specialization properties

We investigate now the specialization properties of the resultant.

Proposition 24. *Let R_1 and R_2 be two rings and $\phi : R_1 \to R_2$ be a ring homomorphism. This map is naturally extended to a map sending $R_1[x]$ to $R_2[x]$ by applying ϕ coefficientwise.*

Now, let a and b in $R_1[x]$ and assume that $\deg(\phi(a)) = \deg(a)$ and $\deg(\phi(b)) = \deg(b)$. Then, the following holds:

$$\phi(res(a, b)) = res(\phi(a), \phi(b)).$$

Proof. This proof has already been done during class. □

Exercise 16

Compute the resultant associated to $x^3 + x^2 + x + 1$ and $2x^2 - x - 2$. What is its image in $\frac{\mathbb{Z}}{2\mathbb{Z}}$? Compare with what you obtain when computing the resultant associated to $x^3 + x^2 + x + 1$ and x which are the images of the former polynomials in $\frac{\mathbb{Z}}{2\mathbb{Z}}[x]$.
Same questions but now considering $2x^2 + x + 1$ and $2x^2 - x - 2$.

Exercise 17

Deduce from the above lemma a multi-modular approach (through the Chinese Remainder Theorem) for computing the resultant of polynomials in $\mathbb{Z}[x]$ assuming you are given a subroutine computing resultants of couples of polynomials in $\frac{\mathbb{Z}}{p\mathbb{Z}}[x]$ where p is a prime number.
Hint. Recall that Hadamard's inequality allows us to bound the absolute value of the determinant of a matrix with entries in $\mathbb{Z}$.

2.3 Resultant computation

We consider now the problem of computing the resultant of two polynomials

$$a = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_0$$

and

$$b = b_1 x^q + b_{q-1}x^{q-1} + \cdots + b_0$$

in $\mathbb{K}[x]$. We then let p and q be the respective degrees of a and b and assume without loss of generality that $p \geqslant q$.

Let r be the remainder of the Euclidean division of a by b ; remark that r has degree at most $q-1$. We start by relating the resultant of (a, b) with the resultant of (b, r).

Proposition 25. *Let a, b and r be as above and let ρ be the degree of r. Then the following holds.*

$$res(a, b) = (-1)^{pq} b_q^{p-\rho} res(b, r)$$

Proof. The idea is to replace the rows of the Sylvester matrix containing the coefficients of a with rows containing the coefficients of r using elementary operations.

Recall that if L_1 and L_2 are two lines of a square matrix M, replacing L_1 by $\alpha L_1 + \beta L_2$ in M, yielding a matrix M', implies that the determinant of M' is the one of M multiplied by β.

We explain now how this process can work. Remark that the first row of $Sylv(a, b)$ corresponds to $x^{q-1}a$ (we denote it by A_{q-1}) and the one corresponding to $x^{p-1}b$ (we denote it by B_{p-1}).

The idea is then to replace A_{q-1} by $A_{q-1} - \frac{a_p}{b_q} B_{p-1}$ in the Sylvester matrix associated to (a, b). Note that this replacement leaves the determinant invariant but the new row contains now the coefficients of the polynomial $x^{q-1}a - \frac{a_p}{b_q} x^{p-1}b$ which is the first one computed by the division algorithm applied to (a, b) (and which has degree less than the one of $x^{q-1}a$). We let a' be the leading coefficient of this polynomial. Note that the row (let us call it A'_{q-1}) corresponding to this new polynomial can be reduced by the line containing the coefficients of $x^{p-2}b$ (which we call B_{p-2}) as above, i.e. replacing A'_{q-1} with $A'_{q-1} - \frac{a'}{b_q} B_{p-2}$. Again, the determinant of the obtained matrix is the same as the determinant of the Sylvester matrix associated to (a, b).

Keeping on this way, one ends up with a matrix where all rows which were containing the coefficients of a are replaced with rows containing the coefficients of the remainder of the Euclidean division of a by b.

Exercise 18

Simulate the above process with $a = 2x^2 - 3x + 1$ and $b = 3x - 1$.

Now observe that this matrix contains the Sylvester matrix associated to (r, b) with one lower triangular part of size $p - \rho$ with b_q on the anti-diagonal. □

Exercise 19

Based on the above propositio, Write a formal algorithm computing which takes as input two polynomials a and b in $\mathbb{K}[x]$ and returns the resultant associated to (a, b).
Hint. Exploit the fact that the degree of r is less than the degree of b.

Theorem 26. *Let a and b be two polynomials of respective degrees $p \geqslant q$. One can compute the resultant associated to (p, q) within $O(pq)$ arithmetic operations in $\mathbb{K}$.*

Exercise 20

Prove the above theorem.

Exercise 21

Using the algorithm computing resultants through the Euclide's algorithm, compute the resultant associated to

- $x^3 + x^2 + x + 1$ and $x^2 + 2x + 3x + 4$;
- $x^4 - x^3 + x^2 - x + 1$ and $4x^3 - 3x^2 + 2x - 1$.