Polynômes et nombres entiers

Margaret Bilu

4 avril 2015

1 Introduction

Un polynôme est une expression P de la forme

$$P = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_1 X + a_0$$

où

- d est un entier naturel appelé *degré* du polynôme. Un polynôme de degré 0 est dit *constant* ;
- X est une indéterminée ;
- $a_0, \ldots, a_d$ sont des nombres (avec $a_d \neq 0$), appelés les *coefficients* du polynôme.

On appelle a_d le *coefficient dominant* du polynôme, et a_0 le *coefficient constant*. Si $a_d = 1$, on dit que P est *unitaire*. Pour choisir les coefficients du polynôme, nous avons différents ensembles de nombres à notre disposition : les entiers relatifs $\mathbf{Z}$, les nombres rationnels $\mathbf{Q}$, ainsi que les nombres réels $\mathbf{R}$, qui sont inclus les uns dans les autres de la manière suivante :

$$\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}.$$

On notera respectivement $\mathbf{Z}[X]$, $\mathbf{Q}[X]$, $\mathbf{R}[X]$ l'ensemble des polynômes dont tous les coefficients sont entiers, rationnels, réels. Ainsi, nous avons clairement :

$$\mathbf{Z}[X] \subset \mathbf{Q}[X] \subset \mathbf{R}[X].$$

Quand nous ne voudrons parler de n'importe lequel de ces ensembles sans préciser lequel, nous noterons $A = \mathbf{Z}$, $\mathbf{Q}$ ou $\mathbf{R}$ et écrirons $A[X]$ pour l'ensemble des polynômes à coefficients dans A. Remarquons que la somme, la différence et le produit de deux éléments de $A[X]$ est encore un élément de $A[X]$.

Tout polynôme comme ci-dessus induit une fonction réelle

$$\begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \mapsto & a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0 \end{array}$$

que nous appellerons également P.

Exemple 1.1. Si P est de degré 0, cela donne la fonction constante égale à a_0. Si P est de degré 1, on obtient la fonction affine $x \mapsto a_1 x + a_0$.

Lorsqu'on calcule $P(x)$ pour un certain réel x, on dit qu'on *évalue* P en x. En particulier, $P(0) = a_0$. Remarquons que si P est à coefficients rationnels (resp. entiers) et que x est rationnel (resp. entier), alors $P(x)$ est une somme de produits de rationnels (resp. entiers), donc est rationnel (resp. entier).

Le but de ce cours est d'évoquer quelques résultats apparaissant lorsqu'on impose à certaines valeurs d'un polynôme, ou bien à ses coefficients, d'être entiers. Nous verrons que c'est une hypothèse assez restrictive, et qu'en particulier, l'étude des polynômes dans $\mathbf{Z}[X]$ est assez différente de celle des polynômes à coefficients rationnels ou réels, et est très liée à l'arithmétique des entiers.

2 Polynômes à valeurs entières

Comme nous l'avons dit plus haut, lorsqu'on évalue un polynôme à coefficients entiers en un entier, on obtient un entier. La question suivante est alors naturelle :

Question : Si un polynôme ne prend que des valeurs entières lorsqu'on l'évalue en des entiers, est-il nécessairement à coefficients entiers ?

Autrement dit, si on appelle $P(\mathbf{Z}) = \{P(n), n \in \mathbf{Z}\}$ l'ensemble des valeurs prises par le polynôme P lorsqu'on l'évalue en un entier, on demande si $P(\mathbf{Z}) \subset \mathbf{Z}$ implique $P \in \mathbf{Z}[X]$.

La réponse est en fait négative, comme le montre l'exemple du polynôme $\frac{1}{2}X^2 - \frac{1}{2}X$. En effet, ce dernier se factorise sous la forme

$$\frac{X(X-1)}{2}.$$

Or pour tout entier n, $\frac{n(n-1)}{2}$ est entier, car parmi les deux entiers consécutifs $n-1$ et n, il y en a au moins un qui est pair. Reformulons alors notre question :

Nouvelle question : Pouvons-nous décrire tous les polynômes P tels que $P(\mathbf{Z}) \subset \mathbf{Z}$?

Cette question semble vague, mais nous y répondrons de manière très précise plus bas. Commençons pour cela par trouver d'autres exemples du même type que $\frac{X(X-1)}{2}$. De même que parmi deux entiers consécutifs, il y en a toujours un qui est pair, parmi trois entiers consécutifs, il y en a toujours un qui est divisible par 3. Ainsi, le polynôme

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

est à coefficients entiers. Mais en fait nous pouvons mieux faire : parmi trois entiers consécutifs, il y en a aussi un qui est divisible par 2, et, 2 et 3 sont premiers entre eux, donc en fait, les valeurs prises par ce polynôme sont divisibles par 2, et le polynôme

$$\frac{X(X-1)(X-2)}{6} = \frac{1}{6}X^3 - \frac{1}{2}X^2 + \frac{1}{3}X$$

est encore à coefficients entiers.

Remarque 2.1. Il n'y a pas besoin d'écrire le développement de ce polynôme pour vérifier qu'il est à coefficients entiers. En effet, on voit directement à partir de la forme factorisée que le coefficient dominant du numérateur est 1, et donc celui du polynôme tout entier est $\frac{1}{6} \notin \mathbf{Z}$.

Continuons encore un peu. Parmi quatre entiers consécutifs, on trouve deux multiples de 2. De plus, l'un d'eux est nécessairement un multiple de 4. Il y aura également un multiple de 3. Ainsi, un entier de la forme

$$n(n-1)(n-2)(n-3)$$

pour $n \in \mathbf{Z}$ sera toujours divisible par $2 \times 3 \times 4 = 24$, et le polynôme

$$\frac{X(X-1)(X-2)(X-3)}{2 \times 3 \times 4}$$

(dont nous laissons au lecteur le soin de vérifier qu'il n'est pas à coefficients entiers) ne prend que des valeurs entières aux entiers.

On sent bien qu'en continuant comme ceci, on va pouvoir obtenir des exemples de polynômes à valeurs entières et à coefficients non entiers de degrés de plus en plus grands. Dans le paragraphe suivant nous expliquons en détail comment cela fonctionne.

2.1 Coefficients binomiaux

Rappelons que pour tout entier $k > 0$ on peut définir la factorielle de k, notée $k!$, par

$$k! = 1 \times 2 \times \ldots \times k,$$

c'est à dire que $k!$ est le produit des k premiers entiers. Par convention, on pose également $0! = 1$.

L'astuce utilisée dans le paragraphe précédent était toujours la même : on partait d'un entier n, on faisait le produit des k nombres $n, n-1, n-2, \ldots, n-(k-1)$, et on divisait le tout par le produit des k premiers entiers, c'est-à-dire $k!$, ce qui donnait l'entier

$$\frac{n(n-1)\ldots(n-k+1)}{k!}.$$

Nous avons observé dans le paragraphe précédent que pour $k = 2, 3, 4$, l'expression obtenue est toujours entière, quel que soit n. Elle l'est clairement aussi pour $k = 1$. Maintenant nous allons étudier cela plus généralement pour tout $k \geq 0$.

Définition 2.2. Soient n et $k \geq 1$ des entiers. On pose

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!}.$$

Ce nombre ce lit « k parmi n », et est appelé un coefficient binomial. Par convention, on pose également $\binom{n}{0} = 1$.

La proposition suivante montre que notre recette pour construire des polynômes à valeurs entières continue à fonctionner pour de grandes valeurs de k :

Proposition 2.3. *Pour tout $n \in \mathbf{Z}$ et pour tout $k \geq 0$, le nombre $\binom{n}{k}$ est un entier.*

Commençons par le montrer pour les n positifs, et dans ce cas nous pouvons également supposer $k \leq n$ car sinon le nombre considéré est nul. Nous utiliserons un raisonnement relevant de la combinatoire (ce qui peut paraître surprenant, car à l'origine, nous avons considéré ce type d'objet pour des raisons arithmétiques). On interprète d'abord séparément le numérateur et le dénominateur.

- Un groupe de n personnes participe à un concours. A l'issue des épreuves, k d'entre elles sont récompensées : on leur attribue à chacune un rang entre 1 et k, sans ex-aequo. Alors il y a

  $$n(n-1)\ldots(n-k+1)$$

  palmarès différents possibles. En effet, nous avons n choix pour choisir le premier lauréat du concours. Ensuite, il reste $n-1$ personnes, parmi lesquelles nous choisissons le 2ème, ce qui fait $n-1$ choix. De même, ensuite nous avons $n-2$ choix pour choisir le 3ème. En continuant comme ceci, pour tout i entre 1 et k nous avons $n-(i-1)$ choix pour choisir le i-ème lauréat. Finalement, en multipliant tout cela, nous avons le résultat.
- On considère la même situation que ci-dessus, et on fixe un certain groupe de k personnes parmi les n personnes. Si elles sont toutes récompensées, combien de classements différents pouvons-nous avoir ? De la même manière que ci-dessus, nous avons k choix pour choisir le premier, $k-1$ choix pour choisir le deuxième, $k-2$ choix pour choisir le troisième, etc. Ainsi, pour tout i entre 1 et k, nous avons $k-(i-1)$ choix pour choisir le i-ème lauréat, si bien qu'il restera un seul choix pour choisir le k-ième lauréat, et le nombre total de choix que nous avons est bien $k \times (k-1) \times \ldots \times 1 = k!$.

Ceci étant dit, les k lauréats sont invités à une soirée. La liste des invités étant donnée par ordre alphabétique (ne tenant plus compte du classement), combien de listes d'invités différentes pouvons-nous avoir ?

La première remarque ci-dessus nous dit que si les listes d'invités tenaient compte du classement, il y en aurait

$$n(n-1)\dots(n-k+1)$$

différentes. Mais deux classements différents des mêmes k personnes donnent $k!$ listes identiques d'après la seconde remarque. Pour avoir le nombre de listes distinctes possibles, nous divisons donc le premier nombre par le deuxième, ce qui nous donne exactement $\binom{n}{k}$.

Remarquons d'autre part que le nombre de listes d'invités correspond exactement au nombre de choix de k personnes parmi n (on choisit qui est récompensé, sans préciser le classement). Ainsi, nous avons prouvé

Proposition 2.4. *Soient $n > 0$ et $0 \leq k \leq n$ des entiers. Alors $\binom{n}{k}$ est exactement le nombre de manières de choisir k objets parmi n. En particulier, c'est un entier.*

Cette proposition explique entre autres pourquoi $\binom{n}{k}$ est lu « k parmi n ».

Exemple 2.5. Dans une classe de 30 élèves, on veut choisir deux délégués. On a 30 choix pour le premier, que nous appellerons A, et 29 choix pour le 2ème, que nous appellerons B. Or choisir A d'abord et B ensuite ou le contraire fournit la même équipe de délégués à la fin. Ainsi, pour obtenir le nombre de choix de délégués, on divise 30×29 par 2, de sorte à obtenir

$$\frac{30 \times 29}{2} = \binom{30}{2}.$$

La démonstration du fait que $\binom{n}{k}$ est entier pour n négatif se déduit facilement du cas des n positifs. En effet, soit $n < 0$, et soit $m = -n$. Alors

$$\binom{n}{k} = \frac{(-m)(-m-1)\dots(-m-k+1)}{k!} = (-1)^k \frac{(m+k-1)(m+k-2)\dots(m+1)m}{k!}$$

en mettant un -1 en facteur pour chacun des k facteurs du numérateur. Maintenant, ceci ressemble franchement à un autre coefficient binomial : il y a k facteurs positifs au numérateur, le premier étant $m+k-1$, qui diminuent de 1 à chaque fois, si bien que le dernier est $m+k-1-(k-1) = m$. Ainsi,

$$\binom{n}{k} = (-1)^k \binom{k-n-1}{k}$$

qui est entier par le résultat précédent. Nous avons donc bien prouvé que tous les coefficients binomiaux sont entiers.

Citons une propriété importante des coefficients binomiaux, qui permet de faire des récurrences pour prouver des identités combinatoires :

Proposition 2.6. *Soient $k \geq 0$ et $n \geq 0$ des entiers. Alors*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Démonstration. On peut simplement faire le calcul :

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n(n-1)\dots(n-k+1)}{k!} + \frac{n(n-1)\dots(n-k)}{(k+1)!} \\
&= \frac{n(n-1)\dots(n-k+1)[k+1+(n-k)]}{(k+1)!} \\
&= \frac{(n+1)n(n-1)\dots(n+1-k)}{(k+1)!} = \binom{n+1}{k+1}
\end{aligned}$$

Une autre manière de faire utilise à nouveau un raisonnement combinatoire. Supposons que nous voulons choisir une équipe de $k+1$ personnes dans une classe de $n+1$ élèves. Bien entendu, nous avons $\binom{n+1}{k+1}$ manières de faire cela. Mais nous avons aussi une autre manière de compter le nombre d'équipes possibles : mettons pour cela un élève A de la classe à part. Tout groupe de $k+1$ personnes que nous choisirions ou bien contient A, ou bien ne le contient pas. Dans le premier cas nous devons choisir les k autres membres de l'équipe parmi les n élèves autres que A, ce qui fait $\binom{n}{k}$ choix, alors que dans le second cas, nous devons choisir les $k+1$ membres parmi les n élèves autres que A, ce qui fait $\binom{n}{k+1}$ choix. Le nombre total d'équipes possibles est donc la somme des deux, et on retrouve bien le côté gauche de l'énoncé de la proposition. □

Avant de passer à la suite, nous allons également démontrer une identité vérifiée par les coefficients binomiaux, qui nous sera utile :

Lemme 2.7. *Soient $k \geq 0$ et $n \geq k$ des entiers. Alors*

$$\binom{k}{k} + \binom{k+1}{k} + \ldots + \binom{n}{k} = \binom{n+1}{k+1}.$$

Démonstration. Nous allons le démontrer par récurrence sur n en utilisant la proposition 2.6.
Initialisation : Pour $n = k$, nous avons $\binom{k}{k} = \frac{k!}{k!} = 1 = \binom{k+1}{k+1}$.
Hérédité : Supposons que le résultat est vrai pour $n-1$. Alors par hypothèse de récurrence

$$\binom{k}{k} + \binom{k+1}{k} + \ldots + \binom{n-1}{k} + \binom{n}{k} = \binom{n}{k+1} + \binom{n+1}{k+1},$$

et la proposition 2.6 conclut. □

2.2 Caractérisation des polynômes à valeurs entières

Grâce à l'étude de la section précédente, nous avons, pour tout k, un exemple de polynôme de degré k à valeurs entières mais pas à coefficients entiers :

Définition 2.8. Soit $k \geq 1$ un entier. On définit le k-ième polynôme de Hilbert [1] par

$$H_k = \frac{X(X-1)\ldots(X-k+1)}{k!}.$$

On définit également $H_0 = 1$.

Ainsi, pour tout $k \geq 0$, H_k est un polynôme de degré k et de coefficient dominant $\frac{1}{k!}$ (donc non à coefficients entiers dès que $k \geq 2$). De plus, pour tout entier n, $H_k(n) = \binom{n}{k}$, donc $H_k(\mathbf{Z}) \subset \mathbf{Z}$. Plus précisément, nous avons

$$H_k(n) = \begin{cases} 0 & \text{si} \quad 0 \leq n \leq k-1 \\ \binom{n}{k} & \text{si} \quad n \geq k \\ \binom{k-n-1}{k} & \text{si} \quad n < 0 \end{cases}$$

En particulier, nous pouvons reformuler le lemme 2.7 en termes de polynômes de Hilbert :

Lemme 2.9. *Soient $k \geq 0$ et $n \geq 0$ des entiers. Alors*

$$H_k(0) + H_k(1) + \ldots + H_k(n) = H_{k+1}(n+1).$$

1. David Hilbert (1862-1943) était un grand mathématicien allemand, l'un des derniers mathématiciens à avoir une bonne connaissance de tous les domaines mathématiques, avant que ceux-ci ne s'étendent et ne se multiplient grandement au cours du 20ème siècle. En particulier, au Congrès International des Mathématiques à Paris en 1900, il a présenté à la communauté mathématique une liste de 23 problèmes ouverts (connus depuis comme les « problèmes de Hilbert ») dont il jugeait qu'ils devaient occuper les mathématiciens pendant le 20ème siècle. Certains de ces problèmes, dont la célèbre hypothèse de Riemann, ne sont toujours pas résolus.

Démonstration. D'après ce qu'on vient de remarquer, les k premiers termes sont nuls, donc on retrouve exactement l'identité de 2.7. □

Bien entendu, ce ne sont pas les seuls polynômes à valeurs entières n'ayant pas tous leurs coefficients entiers. Ainsi, $H_2 + H_3$, qui est de degré 3 et de coefficient dominant $\frac{1}{3!}$ en est un également. Plus généralement, on peut sommer des polynômes de Hilbert autant qu'on veut, tant qu'on prend garde à garder au moins un coefficient non entier, on trouve encore des polynômes ayant cette propriété. Mais, et c'est ce que nous allons prouver, c'est la seule manière d'obtenir des polynômes à valeurs entières et à coefficients non entiers ! Autrement dit, les polynômes de Hilbert sont les « briques élémentaires » des polynômes à valeurs entières :

Théorème 2.10. *Soit P un polynôme de degré d tel que $P(\mathbf{Z}) \subset \mathbf{Z}$. Alors il existe des entiers $m_0 \dots m_k$ tels que*

$$P = m_0 H_0 + m_1 H_1 + \ldots + m_d H_d.$$

Démonstration. Nous allons le montrer par récurrence sur d.
Initialisation : Pour $d = 0$, P est constant, égal à une constante entière m_0, et donc on a bien $P = m_0 H_0$.
Hérédité : Supposons le résultat vrai pour d, et prenons un polynôme P de degré $d+1$ satisfaisant $P(\mathbf{Z}) \subset \mathbf{Z}$. Alors $Q(X) = P(X+1) - P(X)$ est un polynôme de degré d, qui est aussi à valeurs entières. Par hypothèse de récurrence, il existe des entiers $n_0 \dots n_d$ tels que

$$Q(X) = n_0 H_0 + \ldots n_d H_d.$$

Soit $n \in \mathbf{N}$. Alors

$$\begin{aligned} P(n) - P(0) &= (P(n) - P(n-1)) + (P(n-1) - P(n-2)) + \ldots + (P(2) - P(1)) + (P(1) - P(0)) \\ &= Q(n-1) + Q(n-2) + \ldots + Q(1) + Q(0) \\ &= \sum_{p=0}^{n-1} (n_0 H_0(p) + \ldots + n_d H_d(p)) \\ &= n_0 \sum_{p=0}^{n-1} H_0(p) + n_1 \sum_{p=0}^{n-1} H_1(p) + \ldots + n_d \sum_{p=0}^{n-1} H_d(p) \end{aligned}$$

En utilisant le lemme 2.9, on obtient alors

$$P(n) - P(0) = n_0 H_1(n) + \ldots n_d H_{d+1}(n),$$

d'où, en posant $m_0 = P(0)$ (qui est bien entier), $m_1 = n_0$, $m_2 = n_1$, …, $m_{d+1} = n_d$, nous avons

$$P(n) = m_0 H_0(n) + m_1 H_1(n) + \ldots m_{d+1} H_{d+1}(n).$$

Ainsi, les deux polynômes P et $m_0 H_0 + \ldots + m_{d+1} H_{d+1}$ coïncident sur tous les entiers positifs, c'est-à-dire que leur différence est un polynôme qui a une infinité de racines. Un tel polynôme est forcément nul, donc nous avons finalement :

$$P = m_0 H_0 + \ldots + m_{d+1} H_{d+1}.$$

□

Remarque 2.11. Ce résultat montre en particulier que si P est de degré d et vérifie $P(\mathbf{Z}) \subset \mathbf{Z}$, alors les dénominateurs de ses coefficients sont tous des diviseurs de $d!$.

3 Polynômes à coefficients entiers

3.1 Une identité remarquable

Vous avez appris au collège l'identité remarquable

$$a^2 - b^2 = (a - b)(a + b).$$

Elle se généralise de la manière suivante pour des cubes :

$$a^3 - b^3 = (a - b)(a^2 + ab + b^2),$$

et pour des puissances quatrièmes :

$$a^4 - b^4 = (a - b)(a^3 + a^2b + ab^2 + b^3).$$

Pour le vérifier, on développe le côté droit :

$$(a - b)(a^2 + ab + b^2) = a^3 + a^2b + ab^2 - ba^2 - ab^2 - b^3$$

et on remarque que plusieurs termes se simplifient, de sorte qu'on se retrouve avec $a^3 - b^3$.

Essayons d'observer ces identités pour comprendre comment les généraliser plus loin. Dans les trois identités ci-dessus, le deuxième facteur dans la factorisation de $a^n - b^n$ commence toujours par a^{n-1} et se termine par b^{n-1}. Entre les deux, il y a des termes qui permettent de « passer de l'un à l'autre ». En effet, on remarque que pour passer d'un terme au suivant, on diminue de 1 l'exposant de a, et on augmente de 1 l'exposant de b. Ainsi, dans la factorisation de $a^4 - b^4$, on commence par $a^3 = a^3b^0$, puis on continue avec $a^{3-1}b^{0+1} = a^2b$, puis avec $a^{2-1}b^{1+1} = ab^2$, et on termine avec $a^{1-1}b^{2+1} = b^3$.

On peut maintenant tenter une généralisation en suivant ce schéma : pour la factorisation de $a^n - b^n$, on devrait avoir un facteur $a - b$, et un facteur

$$a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + a^2b^{n-3} + ab^{n-2} + b^{n-1}.$$

Plus précisément, il contient tous les termes sont de la forme $a^{n-1-k}b^k$ pour $k \in \{0, \ldots, n-1\}$. Si on développe, on obtient :

$$(a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + a^2b^{n-3} + ab^{n-2} + b^{n-1})$$

$$\begin{aligned} = a^n &+ a^{n-1}b + a^{n-2}b^2 + \ldots + a^3b^{n-3} + a^2b^{n-2} + ab^{n-1} \\ &- a^{n-1}b - a^{n-2}b^2 - a^{n-3}b^3 - \ldots - a^2b^{n-2} - ab^{n-1} - b^n \end{aligned}$$

Comme pour le développement de $a^4 - b^4$, on remarque que tous les termes se simplifient, et qu'il reste seulement $a^n - b^n$. Nous avons donc montré

Proposition 3.1. *Pour tout $n \in \mathbf{N}^*$,*

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + a^2b^{n-3} + ab^{n-2} + b^{n-1}). \tag{1}$$

Remarque 3.2. Une conséquence importante de ceci est la chose suivante : si a et b sont des entiers distincts, alors $a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + a^2b^{n-3} + ab^{n-2} + b^{n-1}$ est un entier également, et donc $a - b$ divise $a^n - b^n$.

Remarque 3.3. Si vous connaissez les suites géométriques, vous avez en fait déjà vu cette identité. En effet, en divisant les deux côtés par $a - b$ et par b^{n-1}, on obtient

$$\frac{\left(\frac{a}{b}\right)^n - 1}{\frac{a}{b} - 1} = \left(\frac{a}{b}\right)^{n-1} + \ldots + \frac{a}{b} + 1.$$

qui est la somme des n premiers termes de la suite géométrique de premier terme 1 et de raison $\frac{a}{b}$.

3.2 Propriétés de divisibilité

Dans cette section, nous allons reformuler l'identité (1) en termes de polynômes, et nous allons en tirer une conséquence importante.

Soit $n \in \mathbf{N}^*$ et soit P le polynôme X^k. Alors $a^k - b^k = P(a) - P(b)$. Ainsi, si on suppose que a et b sont des entiers, cela veut dire, d'après la remarque 3.2, que $a-b$ divise $P(a)-P(b)$. La propriété suivante dit qu'en fait ceci est vrai pour tous les polynômes à coefficients entiers, et pas seulement X^n. Essayons de nous en convaincre sur des polynômes de petits degrés d'abord.

Soit $P = a_1X + a_0$ un polynôme de degré 1. Alors pour tous les entiers a et b distincts, nous avons

$$P(a) - P(b) = a_1a + a_0 - (a_1b + a_0) = a_1(a - b)$$

donc $a - b$ divise bien $P(a) - P(b)$.

Supposons maintenant $P = a_2X^2 + a_1X + a_0$ de degré 2. Alors

$$P(a) - P(b) = a_2a^2 + a_1a + a_0 - (a_2b^2 + a_1b + a_0) = a_2(a^2 - b^2) + a_1(a - b) = a_2(a - b)(a + b) + a_1(a - b)$$

Ainsi, dans ce cas aussi, $a-b$ divise $P(a)-P(b)$, et nous avons eu besoin de l'identité 1 dans le cas $n = 2$ pour le voir. Plus généralement, pour un polynôme de degré n, nous aurons besoin des identités

Proposition 3.4. *(Lemme fondamental) Soit P un polynôme à coefficients entiers. Alors pour tous entiers a, b distincts, $a - b$ divise $P(a) - P(b)$.*

Démonstration. On écrit $P = a_dX^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0$. Alors

$$P(a) - P(b) = a_d(a^d - b^d) + a_{d-1}(a^{d-1} - b^{d-1}) + \ldots + a_1(a - b)$$

et donc $P(a) - P(b)$ est une somme de termes divisibles par $a - b$, ce qui conclut. □

Exercice 3.5. Existe-t-il un polynôme à coefficients entiers P tel que $P(3) = 18$ et $P(5) = 57$?

Solution : Si c'était le cas, on aurait $2 = 5 - 3$ qui divise $P(5) - P(3) = 57 - 18$ qui est impair, contradiction. Donc un tel polynôme n'existe pas.

Exercice 3.6. Soit P un polynôme à coefficients entiers tel que n divise $P(n)$ pour une infinité d'entiers n non nuls. Que peut-on dire de P ?

Solution : D'après le lemme fondamental, n divise $P(n) - P(0)$, donc il existe une infinité d'entiers $n \neq 0$ tels que n divise $P(0)$. Cela veut dire que $P(0)$ a une infinité de diviseurs, donc il est nul. Ainsi, le polynôme P est forcément de la forme $XQ(X)$ avec Q un autre polynôme à coefficients entiers. Réciproquement, si P est de cette forme, alors nous avons pour tout n entier :

$$P(n) = nQ(n).$$

Ainsi, $Q(n)$ étant entier, n divise $P(n)$ pour tout $n \neq 0$.

Conclusion : les polynômes qui vérifient l'hypothèse de l'énoncé sont exactement les polynômes divisibles par le polynôme X.

Remarque 3.7. Nous avons donc même montré que si on avait $n|P(n)$ pour une infinité de n, alors en fait c'était vrai pour tous les n.

3.3 Racines d'un polynôme à coefficients entiers

Dans ce paragraphe nous allons voir que le fait qu'un polynôme soit un coefficients entiers impose des contraintes arithmétiques importantes sur ses éventuelles racines entières ou rationnelles. En particulier, le lemme suivant montre qu'il convient de chercher les racines entières parmi les diviseurs du coefficient constant, ce qui donne seulement un nombre fini de valeurs possibles :

Lemme 3.8. *Soit m une racine entière de $P \in \mathbf{Z}[X]$. Montrer que m divise le coefficient constant de P.*

Démonstration. Par hypothèse, nous avons $P(m) = 0$. Ainsi, $m = m - 0$ divise $P(m) - P(0) = -P(0)$, qui est l'opposé du coefficient constant. □

Des contraintes sur des valeurs prises par le polynôme en certains points peuvent aussi avoir une forte influence sur les racines.

Exercice 3.9. Soit $P \in \mathbf{Z}[X]$ tel qu'il existe trois entiers a, b, c tels que $P(a), P(b), P(c) \in \{-1, +1\}$. Montrer que P n'a pas de racine entière.

Solution : Supposons que P a une racine entière m. Alors

$$P(a) - P(m),\ P(b) - P(m),\ P(c) - P(m) \in \{-1, +1\}.$$

Ainsi, par le lemme fondamental, les entiers $a - m$, $b - m$, $c - m$ divisent tous 1 ou -1, et sont donc eux-mêmes égaux à 1 ou -1. Ainsi, a, b, c appartiennent tous à l'ensemble $\{m - 1, m + 1\}$, qui n'a que deux éléments. Comme a, b et c sont distincts, ceci est une contradiction.

Le résultat suivant montre que dans le cas d'un polynôme unitaire, la recherche des racines rationnelles se ramène à celle des racines entières.

Proposition 3.10. *Toute racine rationnelle d'un polynôme unitaire à coefficients entiers est entière.*

Démonstration. On écrit $P = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0$. Supposons que P a une racine rationnelle $\frac{p}{q}$ avec p et q des entiers premiers entre eux, et $q \neq 0$. Cela veut dire que $P\left(\frac{p}{q}\right) = 0$, c'est-à-dire

$$\left(\frac{p}{q}\right)^d + a_{d-1}\left(\frac{p}{q}\right)^{d-1} + \ldots + a_1\frac{p}{q} + a_0 = 0$$

ce qui donne, en multipliant le tout par q^d,

$$p^d + a_{d-1}p^{d-1}q + \ldots + a_1pq^{d-1} + a_0q^d = 0.$$

On remarque que tous les termes dans cette expression à part le tout premier ont un q en facteur, donc sont divisibles par q. Cela veut dire que le premier est également divisible par q, c'est-à-dire que nous avons p^d divisible par q. Or p et q sont premiers entre eux, donc cela implique que $q = 1$, donc $\frac{p}{q}$ est entier. □

Remarque 3.11. Dans cette proposition nous avons supposé le polynôme unitaire. On peut raffiner le résultat dans le cas où le polynôme P a un coefficient dominant a_d non nécessairement égal à 1. Dans ce cas, par le même raisonnement que ci-dessus, on trouve que si $\frac{p}{q}$ est racine de P, alors q divise a_dp^d. Comme q est premier avec p, cela veut dire que q divise a_d. Ainsi, les racines rationnelles d'un polynôme à coefficients entiers ne peuvent avoir (lorsqu'elles sont écrites sous forme réduite $\frac{p}{q}$ avec p et q premiers entre eux) comme dénominateur que des diviseurs du coefficients dominant a_d.

Exemple 3.12. Nous allons illustrer cette propriété pour certains polynômes de degrés 1,2,3.

1. Observons cette propriété directement dans le cas des polynômes de degré 1. Un polynôme unitaire à coefficients entiers de degré 1 s'écrit sous la forme $X + b$, $b \in \mathbf{Z}$. La seule racine est $-b$, qui est bien entière. Plus généralement, un polynôme à coefficients entiers de degré 1 s'écrit sous la forme $aX + b$ avec $a, b \in \mathbf{Z}$. Sa seule racine est $\frac{-b}{a}$, qui est un rationnel non entier (sauf si a divise b), mais dont le dénominateur divise bien a.
2. Prenons maintenant des exemples de degré 2. Le polynôme $X^2 + 3X + 2$ est à coefficients entiers et unitaire. De plus, nous pouvons écrire

$$X^2 + 3X + 2 = (X + 1)(X + 2)$$

et donc ses seules racines sont -1 et -2, qui sont entières. De même, le polynôme

$$6X^2 - X - 1 = (2X - 1)(3X + 1)$$

a pour racines $\frac{1}{2}$ et $-\frac{1}{3}$, dont les dénominateurs divisent bien le coefficient dominant, 6.
3. Soit le polynôme $X(X^2 - 2)$, unitaire de degré 3. Nous voyons qu'il a 0 pour racine, qui est bien entier. Il a aussi deux autres racines, qui sont $+\sqrt{2}$ et $-\sqrt{2}$, qui sont réelles mais non rationnelles. La proposition ne dit rien sur celles-ci.

3.4 Un peu d'arithmétique des polynômes

Nous pouvons dire qu'un entier a divise un entier b s'il existe un entier c tel que $b = ac$. Cette même définition s'adapte aux polynômes :

Définition 3.13. Soient P, Q des polynômes dans $A[X]$. On dit que Q divise P dans $A[X]$ s'il existe un polynôme $R \in A[X]$ tel que $P = QR$.

Exemple 3.14. Nous avons $X^2 - 4X + 3 = (X - 1)(X - 3)$, donc $X - 1$ et $X - 3$ divisent $X^2 - 4X + 3$ dans $\mathbf{Z}[X], \mathbf{Q}[X]$ et $\mathbf{R}[X]$. Nous avons aussi $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$, donc $X - \sqrt{2}$ et $X + \sqrt{2}$ divisent $X^2 - 2$ dans $\mathbf{R}[X]$ (et seulement dans cet ensemble-là, car ils n'appartiennent pas aux deux autres !).

Remarque 3.15. Il est vraiment important de préciser « dans $A[X]$ ». Le polynôme constant égal à 2 divise le polynôme $2X + 1$ dans $\mathbf{Q}[X]$ ou $\mathbf{R}[X]$:

$$2X + 1 = 2\left(X + \frac{1}{2}\right).$$

En revanche, il ne le divise pas dans $\mathbf{Z}[X]$ car $X + \frac{1}{2} \notin \mathbf{Z}[X]$. Plus généralement, un polynôme constant égal à $c \neq 0$ divise tous les polynômes dans $\mathbf{Q}[X]$ ou $\mathbf{R}[X]$. En revanche, dans $\mathbf{Z}[X]$ il ne divise que ceux dont tous les coefficients sont divisibles par c. La divisibilité des polynômes dans $\mathbf{Z}[X]$ a donc des liens très forts avec la divisibilité des entiers.

Nous dirons que deux polynômes sont premiers entre eux dans $A[X]$ si leurs seuls diviseurs communs dans $A[X]$ sont constants. Cette notion est en fait indépendante de A, si bien que nous parlerons simplement de polynômes premiers entre eux. Nous disposons du résultat suivant, qui est un analogue du résultat que vous connaissez peut-être déjà pour les entiers :

Proposition 3.16. *(Théorème de Bézout) Soient P et Q dans $A[X]$ des polynômes premiers entre eux. Alors il existe deux polynômes U et V dans $A[X]$ et un élément $c \in A$ tels que*

$$UP + VQ = c.$$

Remarque 3.17. Dans le cas où $A = \mathbf{Q}$ ou $\mathbf{R}$, nous pouvons en fait supposer de plus que $c = 1$, en remplaçant U et V par $\frac{1}{c}U$ et $\frac{1}{c}V$. En revanche, pour $A = \mathbf{Z}$ nous ne pouvons pas faire cela car $\frac{1}{c}U$ et $\frac{1}{c}V$ ne serons plus nécessairement à coefficients entiers.

Exercice 3.18. Soient P et Q deux polynômes premiers entre eux. On définit pour tout $n \geq 0$

$$a_n = \text{pgcd}(P(n), Q(n)).$$

Montrer que la suite (a_n) est périodique, c'est-à-dire qu'il existe un entier $k \geq 1$ tel que pour tout $n \geq 0$

$$a_n = a_{n+k}.$$

Solution : On applique le théorème de Bézout pour trouver U et V dans $\mathbf{Z}[X]$ et $c \in \mathbf{Z}$ tels que $UP + VQ = c$. Alors pour tout n nous avons $U(n)P(n) + V(n)Q(n) = c$, si bien que a_n, qui divise par hypothèse $P(n)$ et $Q(n)$, divise aussi c. Ainsi, tous les termes de la suite divisent c. Montrons que nous avons $a_n = a_{n+c}$ pour tout $n \geq 0$. D'après le lemme fondamental, $c|P(n+c) - P(n)$, et donc a_n, qui divise c et $P(n)$, divise également $P(n+c)$. Il en est de même pour Q, donc a_n divise le pgcd de $P(n+c)$ et $Q(n+c)$, à savoir a_{n+c}. Mais le même raisonnement peut être fait dans l'autre sens pour montrer que $a_{n+c}|a_n$, donc $a_{n+c} = a_n$.

3.5 Polynômes et nombres premiers

3.5.1 Diviseurs premiers d'un polynôme

Vous avez peut-être déjà vu la démonstration du fait qu'il existe une infinité de nombres premiers : on suppose qu'il y en a un nombre fini $p_1, \dots p_k$, et on considère le nombre $N = p_1 \dots p_k + 1$. C'est un entier strictement plus grand que 1, donc il admet un diviseur premier p. Si c'était l'un des nombres $p_1, \dots p_k$, alors p diviserait 1, ce qui n'est pas possible. Donc cela prouve l'existence d'un nombre premier autre que $p_1, \dots, p_k$, contradiction.

Revenons aux polynômes, et posons-nous la question suivante :

Question : Soit $P \in \mathbf{Z}[X]$. L'ensemble

$$\{p \text{ premier tel qu'il existe } n \in \mathbf{Z} \text{ tel que } P(n) \neq 0 \text{ et } p|P(n)\}$$

peut-il être fini ? infini ?

On appellera les éléments de cet ensemble les diviseurs premiers du polynôme P. Remarquons que si nous arrivons à montrer qu'il y en a un nombre infini pour un certain P, cela fournit par la même occasion une nouvelle preuve de l'infinité des nombres premiers.

La proposition suivante fournit une réponse précise à notre question :

Proposition 3.19. *Soit $P \in \mathbf{Z}[X]$. Alors l'ensemble de ses diviseurs premiers est infini.*

Démonstration. Si le coefficient constant de P est nul c'est immédiat. Traitons le cas où $P(0) = 1$ en nous inspirant de la preuve de l'infinité des nombres premiers ci-dessus. On raisonne par l'absurde en supposant qu'il y en a un nombre fini, $p_1, \dots, p_k$. Considérons alors

$$P(p_1 \dots p_k) = a_d(p_1 \dots p_k)^d + a_{d-1}(p_1 \dots p_k)^{d-1} + \dots + a_1(p_1 \dots p_k) + 1.$$

Là où il faut faire un peu attention par rapport à la preuve ci-dessus, c'est que ce nombre pourrait très bien valoir 1 ou -1, et donc ne pas avoir de diviseur premier. Mais ce petit souci se règle très facilement : en effet, un polynôme tend vers l'infini en l'infini, donc il suffit de remplacer, si nécessaire, le produit $p_1 \dots p_k$ par $mp_1 \dots p_k$ pour un entier m suffisamment grand. Alors $N = P(mp_1 \dots p_k)$ a un diviseur premier, qui ne peut être parmi $p_1, \dots, p_k$, contradiction.

Passons maintenant au cas général, en supposant $a_0 \neq 0$: ce qui est gênant, c'est que le coefficient constant a_0 pourrait être divisible par l'un des p_i, et dans ce cas p_i est un diviseur de $P(mp_1 \dots p_k)$. Il faudrait donc se ramener au cas où le coefficient constant est 1. Pour cela, on considère le polynôme

$$P(a_0X) = a_d a_0^d X^d + a_{d-1} a_0^{d-1} X^{d-1} + \dots + a_1 a_0 X + a_0.$$

Les coefficients de ce dernier sont tous divisibles par a_0, donc le polynôme

$$Q(X) = \frac{P(a_0 X)}{a_0}$$

est à coefficients entiers, et son coefficient constant est égal à 1. De plus, si un nombre premier p divise $Q(n)$, alors p divise également $P(a_0 n)$, donc l'ensemble des diviseurs premiers de Q (qui est infini d'après ce qui précède) est inclus dans celui de P, ce qui conclut. □

Remarque 3.20. La preuve de l'infinité des nombres premiers au début du paragraphe consiste exactement à prouver que le polynôme $P = X + 1$ a une infinité de diviseurs premiers par la méthode ci-dessus.

3.5.2 Polynômes générateurs de nombres entiers

Nous venons de voir que les valeurs entières des polynômes ont une infinité de diviseurs premiers distincts. Pouvez-vous trouver un polynôme dont « plein » de valeurs consécutives sont des nombres premiers distincts (pas nécessairement consécutifs) ? Un exemple : considérons le polynôme $P = X^2+X+1$. Nous avons $P(1) = 3$, $P(2) = 7$, $P(3) = 13$, ce qui fait 3 valeurs premières consécutives. Malheureusement, $P(0) = 1$ et $P(4) = 21$, qui ne sont pas premiers, donc cela s'arrête là. Le mathématicien Leonhard Euler a trouvé un exemple assez impressionnant :

Proposition 3.21. *(Euler) On considère le polynôme $P = X^2 + X + 41$. Alors les 40 nombres*

$$P(0), P(1), \ldots, P(39)$$

sont premiers.

Il faut beaucoup de patience pour vérifier la primalité de ces nombres, et nous ne le ferons pas. En revanche, nous pouvons constater que

$$P(40) = 40^2 + 40 + 41 = 40^2 + 2 \times 40 + 1 = (40 + 1)^2 = 41^2,$$

et que donc $P(40)$ n'est pas premier.

Il a fallu attendre la fin du 20ème siècle pour faire « mieux » que cet exemple : le record est actuellement détenu par un polynôme qui donne 57 valeurs consécutives premières distinctes.