Université de Rennes 1 – École normale supérieure de Rennes
Préparation à l'agrégation externe de mathématiques
Mémoire de master

PGCD et PPCM, algorithmes de calcul. Applications.

Téofil Adamski

Encadré par Matthieu Romagny

Ce mémoire constitue une version possible et rédigée de la leçon 142. Les deux développements choisis sont les théorèmes 23 et 35.

Introduction

Dans l'anneau des entiers, les notions de plus grand commun diviseur et de plus petit commun multiple sont naturelles. Elles permettent d'étudier finement les propriétés arithmétiques des entiers. Dans ce texte, on constatera que ces notions se généralisent aux anneaux commutatifs et unitaires. Cependant, sans plus d'hypothèses sur les anneaux, le PGCD et le PPCM n'offrent pas beaucoup de résultats et, pire, leur existence n'est nullement garantie. Ainsi on ajoutera progressivement des hypothèses sur les anneaux considérés.

Dans la partie 1, on définira les PGCD et PPCM, puis on exhibera des propriétés vérifiées par ces derniers lorsqu'on se place dans un anneau principal ou, du moins, factoriel. On donnera quelques applications du PGCD dans ces cas précis. Dans la partie 2, on se concentra sur les anneaux euclidiens et on présentera un algorithme, dit d'Euclide, pour calculer le PGCD. Enfin, dans la partie 3, on donnera quelques applications en arithmétique : la résolution de certaines équations diophantiennes et certains systèmes de congruences.

Sommaire

1. PGCD et PPCM dans les anneaux factoriels et principaux

Au cours de cette section, on présente les éléments d'arithmétique sur un anneau puis la notion de PGCD et PPCM, principalement tirées des livres [7, 4]. Les anneaux seront systématiquement supposés *commutatifs et unitaires*. Soit $(A, +, \times)$ un anneau, abrégé par la lettre A.

1.1. Notion de divisibilité et définition des PGCD et PPCM

Définition 1. Un élément $a \in A$ *divise* un élément $b \in A$ s'il existe $c \in A$ tel que $b = ac$. Dans ce cas, on note $a \mid b$.

Notons que la relation $\mid$ est transitive et réflexive.

Exemples. Dans l'anneau $\mathbf{Z}$ des entiers, on écrit $2 \mid 4$ puisque $4 = 2 \times 2$. Dans l'anneau $k[X]$ des polynômes sur un corps k, le polynôme $X^2 + 1$ divise le polynôme $X(X^2 + 1)$.

On peut caractériser la divisibilité en termes d'idéaux, ces derniers étant bien souvent mieux manipulables. Pour un élément $a \in A$, son idéal engendré est noté $(a) \subset A$. Avec cette notation, pour deux éléments $a, b \in A$, on a $b \mid a$ si et seulement si $(a) \subset (b)$.

Deux éléments $a, b \in A$ seront dit *associés* s'ils se divisent mutuellement, c'est-à-dire si $(a) = (b)$. Dans la suite, le notation $A^\times$ désignera le groupe des éléments inversibles de l'anneau A.

Proposition 2. Lorsque l'anneau A est intègre, deux éléments $a, b \in A$ sont associés si et seulement s'il existe un élément $u \in A^\times$ tel que $a = bu$.

Preuve On suppose que les éléments a et b sont associés. Comme $a \mid b$, il existe un élément $c \in A$ tel que $b = ac$. Comme $b \mid a$, il existe un autre élément $d \in A$ tel que $a = bd$. De ces deux dernières égalités, on en déduit que $b = bdc$, c'est-à-dire $b(1 - dc) = 0$. Si $b = 0$, alors $a = bd = 0$ et les éléments a et b sont associés. Sinon l'intégrité donne $dc = 1$ ce qui implique $d \in A^\times$ avec $a = bd$.

Réciproquement, on suppose qu'il existe un élément $u \in A^\times$ tel que $a = bu$. Par définition, on peut écrire $b \mid a$. Mais comme $b = u^{-1}a$, on peut aussi écrire $a \mid b$ si bien que les éléments a et b sont associés. ◁

À partir de maintenant, on suppose que l'anneau A est *intègre*. On peut aisément vérifier que la relation d'association, notée $\sim$, est une relation d'équivalence sur A et que le quotient $A/\sim$ est un ensemble ordonné par la relation de divisibilité. Par ailleurs, avec cette hypothèse, si $a \neq 0$, l'élément c dans la définition 1 est unique et noté b/a. Attention, cette notation ne désigne pas l'élément ba^{-1} en toute généralité.

Ces premières définitions posées, on définit la notion centrale de cette leçon. Dans un premier temps, on ne fait pas d'hypothèse supplémentaire sur l'anneau A. Dans les prochains paragraphes, on en verra une caractérisation lorsqu'on rajoute des propriétés sur cet anneau A.

Définition 3. Un *plus grand commun diviseur* de deux éléments $a, b \in A$ est un élément $d \in A$ vérifiant les deux points suivants :

(D1) on a $d \mid a$ et $d \mid b$;

(D2) pour tout élément $c \in A$, si $c \mid a$ et $c \mid b$, alors $c \mid d$.

Un *plus petit commun multiple* de deux éléments $a, b \in A$ est un élément $m \in A$ vérifiant les deux points suivants :

(M1) on a $a \mid m$ et $b \mid m$;

(M2) pour tout élément $c \in A$, si $a \mid c$ et $b \mid c$, alors $m \mid c$.

Les points (D2) et (M2) s'interprètent respectivement comme des conditions de maximalité et de minimalité pour la relation d'ordre de divisibilité ce qui justifie l'appellation de ces deux notions, abrégées dans la suite sous les acronymes PGCD et PPCM. Par ailleurs, cette définition se généralise à un nombre fini d'éléments.

Exemples. Dans l'anneau $\mathbf{Z}$, les entiers 2 et 3 admettent 1 comme PGCD et 6 comme PPCM, les entiers 4 et 6 admettent -2 comme PGCD et 6 comme PPCM.

Cependant, deux éléments d'un anneau n'admettent pas nécessairement un PGCD ou un PPCM comme le montre l'exercice suivant, corrigé dans le livre [6].

Exercice 1. Dans l'anneau $\mathbf{Z}[i\sqrt{5}]$, montrer que les éléments $a := 3$ et $b := 2 + i\sqrt{5}$ ne possèdent pas de PPCM.

Solution Pour un élément $z := \alpha + i\beta\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ avec $\alpha, \beta \in \mathbf{Z}$, sa *norme* est l'entier

$$N(z) := |z|^2 = \alpha^2 + 5\beta^2.$$

On vérifie que l'application $N \colon \mathbf{Z}[i\sqrt{5}] \longrightarrow \mathbf{N}$ est multiplicative.

Raisonnons par l'absurde et supposons qu'ils admettent un PPCM $m \in \mathbf{Z}[i\sqrt{5}]$. Comme $a \mid ab$ et $b \mid ab$, le point (M2) donne $m \mid ab$, donc la multiplicativité permet d'écrire $N(m) \mid N(a)N(b) = 81$.

Par ailleurs, en notant $x := b(1+i\sqrt{5})$, on calcul $x = a(-1+i\sqrt{5})$ de telle sorte que $a \mid x$ et $b \mid x$. Le même point (M2) donne alors $m \mid x$, donc $N(m) \mid N(x) = 54$. En écrivant $54 = 2 \times 3^3$, on obtient

$$N(m) \in \{1, 2, 3, 6, 9, 18, 27, 54\}.$$

Comme $a \mid m$, on a $N(a) = 9 \mid N(m)$, donc $N(m) \in \{9, 18, 27, 54\}$. Enfin, comme $18 \nmid 81$ et $54 \nmid 81$, on en déduit $N(m) \in \{9, 27\}$.

On vérifie qu'aucun élément de l'anneau $\mathbf{Z}[i\sqrt{5}]$ n'est de norme 27. Cela force à avoir $N(m) = 9$. Soient $a', b' \in \mathbf{Z}[i\sqrt{5}]$ deux éléments vérifiant $m = aa' = bb'$. Comme $N(a) = N(b) = 9$, cela signifie que $N(a') = N(b') = 1$, donc $a', b' \in \{\pm 1\}$ ce qui conclut $a = \pm b$ et conduit à l'impossible.

Dans la prochaine proposition, on va voir que, s'ils existent, alors les PGCD et PPCM sont associés et que, réciproquement, tout élément associé à un PGCD ou un PPCM est encore un PGCD ou un PPCM. On pourra donc être tenté de définir ces notions à un inversible près ce qu'on fera dans la suite.

Proposition 4. Soient $a, b \in A$ deux éléments.

1. Les PGCD des éléments a et b sont associés.
2. Réciproquement, soient $d \in A$ un PGCD de ceux-ci et $u \in A^\times$ un élément inversible. Alors l'élément ud est un PGCD des éléments a et b.

Preuve

1. Soient $d, d' \in A$ deux PGCD des éléments a et b. Le point (D1) vérifié par l'élément d fournit $d \mid a$ et $d \mid b$. Avec le point (D2) vérifié par l'élément d', on en déduit $d \mid d'$. Comme les éléments d et d' jouent des rôles symétriques, on obtient également $d' \mid d$. Finalement, ils sont associés.
2. Avec le point (D1) vérifié par l'élément d, on obtient $d \mid a$. De plus, avec la proposition 2, les éléments d et ud sont associés, donc $ud \mid d$. Par associativité de la relation de divisibilité, on en déduit $ud \mid a$. De même, on trouve $ud \mid b$. Cela montre que l'élément ud vérifie le point (D1). Montrons qu'il satisfait le point (D2). Soit $c \in A$ un élément vérifiant $c \mid a$ et $c \mid b$. Avec le point (D2) vérifié par l'élément d, on peut écrire $c \mid d$ et l'association donne encore $c \mid ud$ ce qui conclut le point (D2). Finalement, l'élément ud est un PGCD. ◁

Définition 5. Deux éléments de l'anneau A sont *premiers entre eux* si tout diviseur commun est inversible dans A.

Exemples. Dans l'anneau $\mathbf{Z}$, les entiers 2 et 3 sont premiers entre eux et, dans l'anneau $\mathbf{R}[X]$, les polynômes $X^2 + X + 1$ et $X - 1$ le sont.

À partir des définitions et de la proposition précédente, on peut caractériser la primalité de deux éléments entre eux avec le PGCD.

Proposition 6. Soient $a, b \in A$ deux éléments. Alors ils sont premiers entre eux si et seulement si tout PGCD est inversible.

Preuve On suppose que les éléments a et b sont premiers entre eux. Soit $d \in A$ un PGCD de ces deux éléments. Le point (D1) donne $d \mid a$ et $d \mid b$. Comme les éléments a et b sont premiers entre eux, ceci conclut $d \in A^\times$.

Réciproquement, on suppose qu'ils admettent un PGCD inversible $u \in A^\times$. Soit $d \in A$ un diviseur commun. Montrons que ce dernier est inversible. Avec la proposition 4, le neutre $1 = u^{-1}u$ est un PGCD. Le point (D2) vérifié par ce dernier donne alors $d \mid 1$, c'est-à-dire $d \in A^\times$. ◁

Définition 7. Un anneau est *à PGCD* s'il est intègre et tout couple d'éléments admet un PGCD.

1.2. Dans les anneaux factoriels

1.2.1. Anneaux factoriels et PGCD

Définition 8. Un anneau A est *factoriel* s'il vérifie les trois points suivants :

(F1) il est intègre ;

(F2) tout élément $a \in A \setminus \{0\}$ s'écrit $a = up_1 \cdots p_r$ pour un élément inversible $u \in A^\times$ et des éléments irréductibles $p_1, \ldots, p_r \in A$;

(F3) pour tout élément $a \in A \setminus \{0\}$, si les écritures $a = up_1 \cdots p_r$ et $a = vq_1 \cdots q_s$ sont comme dans le point (F2), alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que

$$\forall i \in [\![1, s]\!], \qquad p_i \sim q_{\sigma(i)}.$$

Exemples. Les anneaux $\mathbf{Z}$ et $k[X]$ sont factoriels. L'anneau $\mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel puisqu'il ne satisfait pas le point (F3). En effet, l'élément 9 se décompose en les produits 3×3 et $(2+i\sqrt{5})(2-i\sqrt{5})$ mais, en considérant la norme, les éléments 3 et $2 \pm i\sqrt{5}$ sont irréductibles et non associés.

Soit A un anneau factoriel. Notons $\mathscr{P} \subset A$ un *système de représentants des irréductibles* de l'anneau A, c'est-à-dire une partie telle que tout élément irréductible de l'anneau A soit associé à un unique élément de la partie $\mathscr{P}$. Dès lors, les points (F2) et (F3) se reformulent comme suit :

($\tilde{\text{F}}$2) tout élément $a \in A \setminus \{0\}$ s'écrit sous la forme $a = u \prod_{p\in\mathscr{P}} p^{v_p(a)}$ pour un inversible $u \in A^\times$ et une famille presque nulle $(v_p(a))_{p\in\mathscr{P}}$ d'entiers naturels ;

($\tilde{\text{F}}$3) l'écriture du point ($\tilde{\text{F}}$2) est unique.

Exemples. Pour l'anneau $\mathbf{Z}$, on prend les nombres premiers strictement positifs comme représentants des irréductibles. Pour l'anneau $k[X]$, on prend les polynômes irréductibles unitaires.

Proposition 9. Soient A un anneau factoriel et $\mathscr{P} \subset A$ un système de représentants des irréductibles. Pour deux éléments $a, b \in A \setminus \{0\}$, on a

$$a \mid b \qquad \Longleftrightarrow \qquad \forall p \in \mathscr{P}, \quad v_p(a) \leqslant v_p(b).$$

Preuve Directement, on suppose $a \mid b$. Il existe un élément $c \in A$ tel que $b = ac$. Comme $b \neq 0$, l'élément c n'est pas nul et on peut considérer les entiers $v_p(c)$. Soit $p \in \mathscr{P}$. Avec l'égalité $b = ac$ et grâce à l'unicité donnée par le point ($\tilde{\text{F}}$3), on peut écrire $v_p(b) = v_p(a) + v_p(c)$. Comme $v_p(c) \geqslant 0$, on en déduit $v_p(b) \geqslant v_p(a)$. Réciproquement, on suppose $v_p(a) \geqslant v_p(b)$ pour tout élément $p \in \mathscr{P}$. Grâce au point ($\tilde{\text{F}}$2), on écrit

$$a = u \prod_{p\in\mathscr{P}} p^{v_p(a)} \qquad \text{et} \qquad b = v \prod_{p\in\mathscr{P}} p^{v_p(b)} \qquad \text{avec} \quad u, v \in A^\times.$$

En vertu de notre hypothèse, l'élément $c \coloneqq vu^{-1} \prod_{p\in\mathscr{P}} p^{v_p(b)-v_p(a)} \in A$ est bien défini et il vérifie l'égalité $b = ac$ ce qui montre $a \mid b$. ◁

On peut dès lors exhiber des PGCD et des PPCM dans un anneau factoriel. La preuve est immédiate grâce à la dernière proposition.

Proposition 10. Soient A un anneau factoriel et $\mathscr{P} \subset A$ un système de représentants des irréductibles. Soient $a, b, d \in A \setminus \{0\}$ trois éléments non nuls. Alors l'élément d est un PGCD de a et b si et seulement si

$$\forall p \in \mathscr{P}, \qquad v_p(d) = \min(v_p(a), v_p(b)). \tag{1}$$

En particulier, un anneau factoriel est à PGCD.

Preuve Pour simplifier l'écriture, on omettra de mettre les « $\forall p \in \mathscr{P}$ ».

Directement, on suppose que l'élément d est un PGCD de a et b. Comme $d \mid a$ et $d \mid b$, la proposition 9 donne $v_p(d) \leqslant v_p(a)$ et $v_p(d) \leqslant v_p(b)$, donc $v_p(d) \leqslant \min(v_p(a), v_p(b))$. Montrons l'autre inégalité. Pour cela, considérons un élément non nul $d' \in A \setminus \{0\}$ vérifiant

$$v_p(d') = \min(v_p(a), v_p(b)).$$

En particulier, on peut écrire $v_p(d') \leqslant v_p(a)$ et $v_p(d') \leqslant v_p(a)$, donc $d' \mid a$ et $d' \mid b$. Le point (D2) fournit ainsi $d' \mid d$ ce qui se réécrit

$$\min(v_p(a), v_p(a)) = v_p(d') \leqslant v_p(d).$$

Cela conclut l'assertion (1).

Réciproquement, on suppose que l'élément d vérifie la condition (1). Comme pour le sens direct, on trouve $d \mid a$ et $d \mid b$. Soit $c \in A$ un élément tel que $c \mid a$ et $c \mid b$. Comme $a \neq 0$, l'élément c n'est

pas nul, permettant ainsi de considérer ses valuations. Les divisibilités $c \mid a$ et $c \mid a$ entraînent les inégalités $v_p(c) \leqslant v_p(a)$ et $v_p(c) \leqslant v_p(b)$, donc

$$v_p(c) \leqslant \min(v_p(a), v_p(b)) = v_p(d)$$

ce qui conclut $c \mid d$. Finalement, l'élément d est un PGCD de a et b. ◁

La même proposition existe en version PPCM : il suffit de remplacer le minimum présent par un maximum. Ce dernier énoncé nous donne, en particulier, des PGCD et des PPCM privilégiés.

Définition-proposition 11. Soit A un anneau factoriel. Considérons un système $\mathscr{P} \subset A$ de représentants des irréductibles. Soient $a, b \in A$ deux éléments avec $(a, b) \neq (0, 0)$.

- Lorsque $a = 0$, les éléments $\operatorname{pgcd}(a, b) \coloneqq b$ et $\operatorname{ppcm}(a, b) \coloneqq 0$ sont respectivement un PGCD et un PPCM des éléments $a = 0$ et b.
- Sinon les éléments

$$\operatorname{pgcd}(a, b) \coloneqq \prod_{p \in \mathscr{P}} p^{\min(v_p(a), v_p(b))} \qquad \text{et} \qquad \operatorname{ppcm}(a, b) \coloneqq \prod_{p \in \mathscr{P}} p^{\max(v_p(a), v_p(b))} \tag{2}$$

  en sont d'après la proposition 10.

On dira que les éléments $\operatorname{pgcd}(a, b)$ et $\operatorname{ppcm}(a, b)$ sont *le* PGCD et *le* PPCM des éléments a et b.

Il ne faudra pas oublier que ceux-ci dépendent du système $\mathscr{P}$. On peut bien-sûr étendre ces définitions à un nombre finis d'éléments de A.

Remarque. Dans le cas des anneaux $\mathbf{Z}$ et $k[X]$, on choisit le système $\mathscr{P}$ de représentants des irréductibles comme dans l'exemple précédent. En particulier, tout PGCD est positif dans l'anneau $\mathbf{Z}$ et unitaire dans l'anneau $k[X]$. Par exemple, on a $\operatorname{pgcd}(2, -4) = 2$ et $\operatorname{ppcm}(X, 2X^2) = X^2$.

Notation. Lorsqu'on voudra spécifier l'anneau A dans lequel on travail — en particulier, lorsqu'on travaillera dans un sur-anneau $B \supset A$ —, on pourra les noter $\operatorname{pgcd}_A(a, b)$ et $\operatorname{ppcm}_A(a, b)$. Par exemple, on a

$$\operatorname{pgcd}_{\mathbf{Z}[X]}(2X, 4(X^2 + X)) = 2X \qquad \text{et} \qquad \operatorname{pgcd}_{\mathbf{Q}[X]}(2X, 4(X^2 + X)) = X.$$

À partir des définitions, la proposition suivante est immédiate.

Proposition 12. Soient A un anneau factoriel muni d'un système $\mathscr{P} \subset A$ de représentants des irréductibles et $a, b, \alpha \in A \setminus \{0\}$ trois éléments non nuls. Alors

$$\operatorname{pgcd}(\alpha a, \alpha b) \sim \alpha \operatorname{pgcd}(a, b).$$

Preuve On veut montrer que l'élément $\alpha \operatorname{pgcd}(a, b)$ est un PGCD des éléments αa et αb. Pour cela, on utilise la caractérisation donnée par la proposition 10. Pour tout élément $p \in \mathscr{P}$, par la définition 11 du PGCD, on peut écrire

$$\begin{aligned} v_p(\alpha \operatorname{pgcd}(a, b)) &= v_p(\alpha) + v_p(\operatorname{pgcd}(a, b)) && (\text{car } v_p(xy) = v_p(x) + v_p(y) \text{ avec } x, y \in A) \\ &= v_p(\alpha) + \max(v_p(a), v_p(b)) && (\text{par définition du PGCD}) \\ &= \max(v_p(\alpha) + v_p(a), v_p(\alpha) + v_p(b)) \\ &= \max(v_p(\alpha a), v_p(\alpha b)) \end{aligned}$$

L'élément $\alpha \operatorname{pgcd}(a, b)$ est alors un PGCD des éléments αa et $\alpha\beta$. Les PGCD étant associés d'après la proposition 4, on obtient $\alpha \operatorname{pgcd}(a, b) \sim \operatorname{pgcd}(\alpha a, \alpha b)$. ◁

Proposition 13. Soient A un anneau factoriel muni d'un système de représentants des irréductibles et $a, b \in A \setminus \{0\}$ deux éléments non nuls. Notons $m \coloneqq \operatorname{ppcm}(a, b)$. Alors

$$(a) \cap (b) = (m).$$

Preuve Montrons l'égalité par double inclusion. Soit $x \in (a) \cap (b)$. Alors $(x) \subset (a)$ et $(x) \subset (b)$, donc $a \mid x$ et $b \mid x$ et le point (M2) implique alors $m \mid x$, donc $(x) \subset (m)$ ce qui conclut $x \in (m)$. D'où $(a) \cap (b) \subset (m)$.

Réciproquement, soit $x \in (m)$. Alors $m \mid x$. Le point (M1) donne $a \mid m$ et $b \mid m$ et la transitivité assure alors $a \mid x$ et $b \mid x$, donc $(x) \in (a)$ et $x \in (b)$ ce qui donne $x \in (a) \cap (b)$. D'où $(m) \subset (a) \cap (b)$. Ceci achève la preuve. ◁

Remarque. En toute généralité, on ne peut pas écrire $(a) + (b) = (d)$ avec $d \coloneqq \operatorname{pgcd}(a, b)$ comme le montre le contre-exemple après le corollaire 21.

Proposition 14. Sous les mêmes hypothèses, on a

$$ab \sim \operatorname{pgcd}(a, b) \operatorname{ppcm}(a, b).$$

Preuve Il suffit de remarquer que $\min(m, n) + \max(m, n) = m + n$ pour deux entiers $m, n \in \mathbf{Z}$ et d'utiliser les relations (2). ◁

En particulier, lorsque les éléments a et b sont premiers entre eux, on a $\operatorname{ppcm}(a, b) \sim ab$. On notera que les trois derniers résultats ne nécessitent pas que l'anneau soit factoriel, mais leurs énoncés sont facilités par l'existence des PGCD.

1.2.2. Le contenu d'un polynôme et une application

Dans cette petite partie, on considère un anneau factoriel A. On rappelle que l'anneau $A[X]$ est lui aussi factoriel et qu'il vérifie en particulier le lemme d'Euclide. On a utilisé le livre [7].

Lemme 15 *(Euclide).* Soit B un anneau factoriel. Pour tout élément irréductible $p \in B$ et tous éléments $a, b \in B$ tels que $p \mid ab$, on a $p \mid a$ ou $p \mid b$.

Dans la suite, on fixe un système $\mathscr{P} \subset A$ de représentants des irréductibles.

Définition 16. Le *contenu* d'un polynôme $P \coloneqq a_0 + \cdots + a_n X^n \in A[X] \setminus \{0\}$ est l'élément

$$\mathfrak{c}(P) \coloneqq \operatorname{pgcd}(a_1, \ldots, a_n) \in A.$$

Le polynôme P est *primitif* si son contenu est inversible, c'est-à-dire associé au neutre 1.

Exemple. Sur l'anneau $\mathbf{Z}$, le contenu du polynôme $3X^4 + 6$ vaut $\operatorname{pgcd}(3, 6) = 3$.

Lemme 17 *(Gauss).* Soient $P, Q \in A[X] \setminus \{0\}$ deux polynômes non nuls. Alors $\mathfrak{c}(PQ) \sim \mathfrak{c}(P)\,\mathfrak{c}(Q)$.

Preuve Dans un premier temps, on suppose que les polynômes P et Q sont primitifs. Raisonnons par l'absurde et supposons que le polynôme PQ n'est pas primitif. Comme l'anneau A est factoriel, cela signifie qu'il existe un irréductible $p \in A$ qui divise l'élément $\mathfrak{c}(PQ)$. On note $P = \sum_{i=0}^{p} a_i X^i$ et $Q = \sum_{i=0}^{q} b_i X^i$. Comme les polynômes P et Q sont primitifs, leurs coefficients respectifs sont premiers entre eux dans leurs ensembles, donc on peut trouver deux indices $i_0 \in [\![1, p]\!]$ et $j_0 \in [\![1, q]\!]$ tels que

$$\begin{aligned} &\forall i < i_0, \quad p \mid a_i \qquad \text{et} \qquad p \nmid a_{i_0}, \\ &\forall j < j_0, \quad p \mid b_j \qquad \text{et} \qquad p \nmid b_{j_0}. \end{aligned} \tag{3}$$

Comme $p \mid \mathfrak{c}(PQ)$, le coefficient $c_{i_0+j_0}$ est divisible par p et ce coefficient vaut

$$c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_i = a_{i_0} b_{i_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_i.$$

Avec les relations (3), on en déduit $p \mid a_{i_0} b_{i_0}$. Le lemme d'Euclide donne alors $p \mid a_{i_0}$ ou $p \mid b_{i_0}$ ce qui est impossible. En conclusion, on vient de montrer que le polynôme PQ est primitif.

Revenons au cas général. Notons $d \coloneqq \mathfrak{c}(P)$ et $e \coloneqq \mathfrak{c}(Q)$. Les polynômes $P' \coloneqq P/d$ et $Q' \coloneqq Q/e$ sont alors primitifs et ils vérifient $PQ = deP'Q'$, donc la proposition 12 donne $\mathfrak{c}(PQ) \sim de\,\mathfrak{c}(P'Q')$. Mais le cas précédent assure que le polynôme $P'Q'$ est primitif si bien que $\mathfrak{c}(PQ) \sim de$. ◁

Le lemme de Gauss permet, entre autre, de montrer que les polynômes cyclotomiques $\Phi_n \in \mathbf{Z}[X]$ sont irréductibles sur $\mathbf{Z}$ et sur $\mathbf{Q}$. On pourra se référer au livre [7]. Une autre application est la caractérisation des polynômes irréductibles sur un anneau factoriel. Notons $\operatorname{Frac} A$ le corps des fractions d'un anneau intègre A.

Théorème 18. Soit A un anneau factoriel. Alors les polynômes irréductibles de $A[X]$ sont
- les polynômes constants égaux à un élément irréductible de A ;
- les polynômes de degré $\geqslant 1$, primitifs et irréductibles sur $K \coloneqq \operatorname{Frac} A$.

Preuve Vérifions d'abord que ces polynômes sont irréductibles sur A.
- Soit $p \in A$ un élément irréductible. Soient $P, Q \in A[X]$ deux polynômes tels que $p = PQ$. Alors ces deux derniers sont de degré nuls, donc ils sont constants. Comme l'élément p est irréductible, un de deux est inversible dans A et donc dans $A[X]$. Cela montre que le polynôme $p \in A[X]$ est irréductible dans $A[X]$.
- Soit $P \in A[X]$ un polynôme de degré $\geqslant 1$, primitif et irréductible sur K. Soient $Q, R \in A[X]$ deux polynômes tels que $P = QR$. Grâce à l'irréductibilité sur K, on peut supposer $Q \in K[X]^\times$. Ainsi le polynôme Q est égal à une constante $a \in K$ ce qui permet d'écrire $P = aR$. En passant au contenu, on obtient $1 \sim \mathfrak{c}(P) \sim a\,\mathfrak{c}(R)$, donc $a \in A^\times = A[X]^\times$ ce qui conclut.

Il s'agit maintenant de montrer que ce sont les seuls. Soit $P \in A[X]$ un polynôme irréductible sur A. S'il est de degré nul, alors il est du premier type. On suppose désormais que $\deg P > 0$. Montrons que le polynôme P est du second type. D'abord, il est bien primitif puisque sinon on pourrait écrire $P = P/d \times d$ où l'élément $d \coloneqq \mathfrak{c}(P)$ ne serait pas inversible.

Maintenant, il reste à montrer qu'il est irréductible sur K. Soient $Q, R \in K[X]$ deux polynômes tels que $P = QR$. En mettant au même dénominateur les coefficients du polynôme Q puis en prenant un PGCD de leurs numérateurs, on peut trouver deux éléments $a, b \in A$ premiers entre eux et un polynôme primitif $Q' \in A[X]$ tels que $Q = \frac{a}{b}Q'$. De la même manière, on écrit $R = \frac{c}{d}R'$ pour deux éléments $c, d \in A$ premiers entre eux et un polynôme primitif $R' \in A[X]$. L'égalité $P = QR$ implique $bdP = acQ'R'$, donc $bd\,\mathfrak{c}(P) \sim ac\,\mathfrak{c}(Q'R')$. Les polynômes P' et Q' étant primitifs, le lemme de Gauss donne $\mathfrak{c}(Q'R') \sim 1$. Comme le polynôme P est supposé primitif, on obtient $bd \sim ac$, c'est-à-dire qu'il existe un élément $u \in A^\times$ tel que $bd = uac$. Comme $bdP = acQ'R'$ et grâce à l'intégrité de l'anneau A, on en déduit $P = uQ'R'$ où $u \in A^\times$ et $Q', R' \in A[X]$. Mais le polynôme P est irréductible sur A, donc on peut supposer $Q \in A[X]^\times = A^\times$. Ainsi le polynôme Q est constant et *a fortiori* appartient à $K^\times = K[X]^\times$. Ceci conclut à l'irréductibilité du polynôme P sur K. ◁

Ce résultat sert notamment à montrer le critère d'Eisenstein. Celui-ci affirme également qu'un polynôme primitif de $\mathbf{Z}[X]$, de degré $\geqslant 1$ et irréductible sur $\mathbf{Q}$ est aussi irréductible sur $\mathbf{Z}$.

1.3. Dans les anneaux principaux : la relation de Bézout

1.3.1. *Anneaux principaux et relations de Bézout*

Définition 19. Un anneau A est *principal* s'il est intègre et si tous ses idéaux sont de la forme (a) pour un élément $a \in A$.

Exemples. Les anneaux $\mathbf{Z}$ et $k[X]$ sont principaux.

On rappelle qu'un anneau principal est factoriel. En particulier, d'après la sous-section précédente, il est à PGCD. L'avantage des anneaux principaux est l'existence d'une version analogue à la proposition 13 pour les PGCD, appelé le *théorème de Bézout*.

Théorème 20 *(Bézout).* Soient A un anneau principal et $a, b \in A \setminus \{0\}$ deux éléments non nuls. Soit $d \in A \setminus \{0\}$. Alors les points suivants sont équivalents :
(i) l'élément d est un PGCD des éléments a et b ;
(ii) on a $(d) = (a) + (b)$.

Dans ce cas, il existe deux éléments $u, v \in A$ tels que

$$d = ua + vb. \tag{4}$$

Une telle égalité (4) est appelée une *relation de Bézout* entre les éléments a et b. Dans la section suivante, on établira un algorithme pour trouver deux telles quantités u et v lorsque l'anneau sera euclidien, une propriété plus forte que la principalité.

Preuve Directement, on suppose le point (i). Comme $d \mid a$ et $d \mid b$, on obtient $(a) \subset (d)$ et $(b) \subset (d)$, donc $(a)+(b) \subset (d)$. Montrons qu'en fait, l'égalité est vérifiée. L'ensemble $(a)+(b)$ est un idéal de l'anneau principal A, donc il existe un élément $d' \in A$ tel que $(d') = (a)+(b)$. Dés lors, on peut écrire $a \in (d')$, donc $d' \mid a$. De même, on trouve $d' \mid b$. Avec le point (D2) vérifié par l'élément d, on en déduit que $d' \mid d$ ce qui donne $(d) \subset (d')$. Finalement, on a l'inclusion $(d) \subset (a)+(b)$ ce qui termine la preuve.

Réciproquement, on suppose le point (ii). Alors $(a) \subset (d)$ et $(b) \subset (d)$, donc $d \mid a$ et $d \mid b$ ce qui donne le point (D1). Vérifions le point (D2). Soit $c \in A$ un diviseur commun aux éléments a et b. Alors $(a) \subset (c)$ et $(b) \subset (c)$, donc $(d) = (a)+(b) \subset (c)$, donc $c \mid d$ ce qui conclut le point (D2). Finalement, l'élément d est un PGCD de a et b. ◁

Notons que la réciproque est vraie sans hypothèse de principalité.

Corollaire 21. On se place sous les mêmes hypothèses. On suppose que les éléments a et b sont premiers entre eux. Alors $A = (a)+(b)$. Autrement dit, il existe deux éléments $u, v \in A$ tels que

$$1 = ua + vb. \tag{5}$$

Le théorème de Bézout est mis en défaut lorsque l'anneau n'est pas principal. En effet, dans l'anneau factoriel $k[X,Y]$, les monômes X et Y sont premiers entre eux et pourtant ils vérifient

$$(X)+(Y) = (X,Y) \neq k[X,Y].$$

Par ailleurs, notons que la relation (5) implique que les éléments a et b sont premiers entre eux sans supposer que l'anneau A est principal. En effet, si une relation (5) existe, alors tout diviseur commun divise également le neutre 1, donc il est inversible.

Autrement dit, il suffit d'établir une relation de Bézout comme l'égalité (5) pour montrer que deux éléments sont premiers entre eux.

1.3.2. Deux applications

Les deux prochains résultats sont issus du livre [4]. Donnons d'abord une application intéressante du théorème de Bézout à l'algèbre linéaire, très utile pour la réduction des endomorphismes. On rappelle que la lettre k désigne un corps.

Théorème 22 *(lemme des noyaux).* Soient E un k-espace vectoriel et $f \in \mathrm{End}_k(E)$ un endomorphisme. Soient $P_1, \dots, P_\ell \in k[X]$ des polynômes deux à deux premiers entre eux. Alors

$$\mathrm{Ker}\, P_1 \cdots P_\ell(f) = \mathrm{Ker}\, P_1(f) \oplus \cdots \oplus \mathrm{Ker}\, P_\ell(f).$$

Preuve En effectuant ensuite une récurrence immédiate, on traite uniquement le cas $\ell = 2$. Les polynômes P_1 et P_2 étant premiers entre eux, le théorème de Bézout assure qu'il existe deux polynômes $U, V \in k[X]$ tels que $UP_1 + VP_2 = 1$.

Montrons que $\mathrm{Ker}\, P_1(f) \cap \mathrm{Ker}\, P_2(f) = \{0\}$. Soit $x \in \mathrm{Ker}\, P_1(f) \cap \mathrm{Ker}\, P_2(f)$. La relation de Bézout implique $UP_1(f)(x) + VP_1(f)(x) = x$. Comme $P_1(f)(x) = 0$ et $VP_1(f) = V(f) \circ P_1(f)$, on obtient $UP_1(f)(x) = 0$. En effectuant de même avec l'autre partie de la somme, on en déduit $x = 0$.

Pour conclure, il reste à montrer que $\mathrm{Ker}\, P_1P_2(f) = \mathrm{Ker}\, P_1(f) + \mathrm{Ker}\, P_2(f)$. L'inclusion $\supset$ est immédiate. Réciproquement, soit $x \in \mathrm{Ker}\, P_1P_2(f)$. On écrit $x = UP_1(f)(x) + VP_2(f)(x)$ grâce à la relation de Bézout. Il s'agit maintenant de montrer que ces deux termes appartiennent respectivement aux noyaux $\mathrm{Ker}\, P_2(f)$ et $\mathrm{Ker}\, P_1(f)$. Mais la première appartenance est vraie puisque

$$P_2(f)(UP_1(f)(x)) = UP_1P_2(f)(x) = U(f) \circ P_1P_2(f)(x) = 0$$

et la seconde se montre identiquement. D'où $x \in \mathrm{Ker}\, P_1(f)(x) + \mathrm{Ker}\, P_2(f)(x)$. ◁

Exemple. Soient E un k-espace vectoriel de dimension finie et $f \in \mathrm{End}_k(E)$ un endomorphisme. On suppose que son polynôme caractéristique s'écrit $\prod_{i=1}^{\ell}(X-\lambda_i)^{\alpha_i}$. Alors le lemme des noyaux associé au théorème de Cayley-Hamilton permet de décomposer l'espace E en la somme directe

$$E = \bigoplus_{i=1}^{\ell} \mathrm{Ker}(f - \lambda_i \,\mathrm{Id}_E)^{\alpha_i}.$$

Une autre application est le théorème de l'élément primitif, portant sur les extensions de corps, dont une preuve se trouve dans le livre [4]. On pourra le proposer en développement.

Théorème 23 *(de l'élément primitif).* Soient K un corps de caractéristique nulle et L une extension finie de ce dernier. Alors il existe un élément $z \in L$ tel que $L = K(z)$.

Preuve Pour un élément $x \in L$, on note $\pi_x \in K[X]$ son *polynôme minimal* sur K, c'est-à-dire l'unique polynôme unitaire engendrant l'idéal $\{P \in K[X] \mid P(x) = 0\}$. Rappelons qu'il est irréductible sur K.

• *Un cas particulier.* Soient $x, y \in L$. Dans un premier temps, on suppose que $L = K(x, y)$. On veut montrer qu'il existe un élément $z \in L$ tel que $L = K(z)$. Procédons en plusieurs étapes.

1. Soit M un corps de décomposition du polynôme $\pi_x\pi_y$ sur L. Les polynômes π_x et π_y peuvent s'écrire sous les formes
$$\pi_x = \prod_{i=1}^{p}(X - x_i) \qquad \text{et} \qquad \pi_y = \prod_{j=1}^{q}(X - y_j) \tag{6}$$
pour des éléments $x_i, y_j \in M$ avec $x = x_1$ et $y = y_1$. Vérifions d'abord que les éléments x_i sont deux à deux distincts. Le corps K étant de caractéristique nulle et le polynôme π_x étant de degré $\geqslant 1$, son dérivé π'_x n'est pas nul. Ainsi le polynôme π_x étant irréductible sur K, il est premier avec son dérivé π'_x dans $K[X]$. Le théorème de Bézout assure alors qu'il existe deux polynômes $U, V \in K[X]$ tels que $U\pi_x + V\pi'_x = 1$. Cette égalité vaut aussi dans $M[X]$ ce qui montre que les polynômes π_x et π'_x n'ont aucune racine commune dans M. On en déduit que le polynôme π_x est scindé simple sur M.

   Montrons qu'il existe un élément $t \in K^\times$ tels que les nombres $x_i + ty_j$ avec $i \in [\![1, p]\!]$ et $j \in [\![1, q]\!]$ soient deux à deux distincts. Pour cela, considérons l'ensemble fini
$$\Gamma \coloneqq \left\{ \frac{x_i - x_k}{y_j - y_\ell} \;\middle|\; i, k \in [\![1, p]\!],\ j \neq \ell \in [\![1, q]\!] \right\}.$$
Le corps K étant de caractéristique nulle, il est infini, donc il existe un élément $t \in K^\times$ tel que $t \notin \Gamma$. Ce dernier convient.

2. Posons $z \coloneqq x + ty$. Montrons que
$$\operatorname{pgcd}_{K(z)[X]}(\pi_y(X), \pi_x(z - tX)) = X - y. \tag{7}$$
   Commençons par montrer que
$$\operatorname{pgcd}_{M[X]}(\pi_y(X), \pi_x(z - tX)) = X - y. \tag{8}$$
Soit $\alpha \in M$ une racine commune des polynômes $\pi_y(X)$ et $\pi_x(z - tX)$. D'après les décompositions (6), il existe deux indices $i \in [\![1, p]\!]$ et $j \in [\![1, q]\!]$ tels que $a = y_j$ et $z - t\alpha = x_i$. Cela se réécrit $z = x_i + ty_j$. D'après l'étape 1, comme $z = x + ty$, cela impose $x = x_i$ et $y = y_j$. On en déduit $a = y$. Par conséquent, on a montré que l'élément y est la seule racine commune des polynômes $\pi_y(X)$ et $\pi_x(z - tX)$. Ces deux derniers étant scindés simples sur M, on conclut l'égalité (8).

   Déduisons-en l'égalité (7). Soit $D \coloneqq \operatorname{pgcd}_{K(z)[X]}(\pi_y(X), \pi_x(z - tX)) \in K[X]$. On écrit
$$\pi_y(X) = P_1 D \qquad \text{et} \qquad \pi_x(z - tX) = P_2 D$$
avec deux polynômes $P_1, P_2 \in K(z)[X]$. Ces deux derniers sont alors premiers entre eux dans $K(z)[X]$, donc il existe deux polynômes $U, V \in K(z)[X]$ tels que $UP_1 + VP_2 = 1$. Cette égalité tenant aussi dans $M[X]$, les polynômes P_1 et P_2 sont aussi premiers entre eux dans $M[X]$ ce qui donne l'égalité $D = \operatorname{pgcd}_{M[X]}(\pi_y(X), \pi_x(z - tX))$. L'égalité (8) conclut alors l'égalité (7).

3. Concluons que $L = K(z)$. L'égalité (7) donne $y \in K(z)$ puis $x = z - ty \in K(z)$ ce qui permet d'écrire $K(x, y) \subset K(z)$. Comme $z = x + ty \in K(x, y)$, on obtient $K(z) \subset K(x, y)$. Finalement, on a montré que $K(z) = K(x, y)$.

• *Le cas général.* À présent, revenons au cas général. L'extension L/K étant finie, il existe des éléments $x_1, \ldots, x_n \in L$ tels que $L = K(x_1, \ldots, x_n)$. Une récurrence immédiate, à partir du cas particulier, montre alors qu'il existe un élément $z \in K$ tel que $L = K(z)$. ◁

2. Le bon point de vue effectif : les anneaux euclidiens

2.1. Stathmes et anneaux euclidiens

Les éléments de cette sous-section proviennent du livre [7].

Définition 24. Un *stathme* sur un anneau A est une fonction $\nu\colon A\setminus\{0\}\longrightarrow \mathbf{N}$ telle que, pour tous éléments $a,b\in A\setminus\{0\}$, il existe des éléments $q,r\in A$ tels que
- $a=bq+r$,
- $r=0$ ou $\nu(r)<\nu(b)$.

Un anneau *euclidien* est un anneau intègre muni d'un stathme.

On dira que l'écriture $a=bq+r$ est une *division euclidienne* de a par b : les éléments q et r sont respectivement appelés son *quotient* et son *reste*.

Exemples. L'anneau $\mathbf{Z}$ muni de la valeur absolue $x\longmapsto|x|$ est euclidien, tout comme l'anneau $k[X]$ muni du degré $P\longmapsto\deg P$.

Exercice 2. Montrer que l'anneau des entiers de Gauss

$$\mathbf{Z}[i]=\{a+ib\mid a,b\in\mathbf{Z}\}$$

muni de la norme $z\longmapsto N(z):=z\overline{z}=|z|^2$ est euclidien.

Solution Soient $z,t\in\mathbf{Z}[i]\setminus\{0\}$. Notons $z/t=x+iy$ avec $x,y\in\mathbf{R}$. Soient $a,b\in\mathbf{Z}$ deux entiers tels que $|x-a|\leqslant 1/2$ et $|y-b|\leqslant 1/2$. Les nombres $q:=a+ib$ et $r:=z-qt$ vérifient $z=qt+r$. Par ailleurs, comme $|z/t-q|\leqslant 1/\sqrt{2}<1$, on obtient $|r|=|t|\,|z/t-q|<|t|$. Ainsi la norme N est un stathme euclidien sur l'anneau $\mathbf{Z}[i]$.

Théorème 25. Un anneau euclidien est principal.

Preuve Soit A un anneau muni d'un stathme ν. Soit $I\subset A$ un idéal non nul. On veut montrer qu'il est engendré par un élément. L'ensemble $\{\nu(b)\mid b\in I\setminus\{0\}\}$ est une partie non vide de $\mathbf{N}$, donc il admet un minimum atteint en un certain élément $b\in I\setminus\{0\}$. Une première inclusion $(b)\subset I$ est vérifiée puisque $b\in I$. Réciproquement, soit $a\in I$. En effectuant une division euclidienne, il existe deux éléments $q,r\in A$ tels que $a=bq+r$ avec $r=0$ ou $\nu(r)<\nu(b)$. Comme $r=a-bq\in I$, on a $r=0$ ou $\nu(r)\geqslant\nu(b)$. Mais comme $\nu(r)<\nu(b)$, cela conduit à avoir $r=0$, c'est-à-dire $a\in(b)$. D'où $I=(b)$. Finalement, l'anneau A est principal. ◁

Notons que la réciproque est fausse : on peut montrer que l'anneau $\mathbf{Z}[\frac{1}{2}(1+i\sqrt{19})]$ est principal et non euclidien (voir [7]).

En particulier, un anneau euclidien est à PGCD. Dans ce qui suit, on va développer un algorithme permettant de calculer le PGCD dans un anneau euclidien. Implicitement, on fixera un système de représentants des irréductibles.

2.2. L'algorithme d'Euclide classique

On considère un anneau A muni d'un stathme ν. Tous les éléments algorithmiques de cette sous-section et de la suivante sont tirés des livres de calcul formel [2, 8].

Proposition 26. Soient $a,b\in A\setminus\{0\}$ deux éléments non nuls. On écrit $a=bq+r$ la division euclidienne de a par b. Alors

$$\operatorname{pgcd}(a,b)\sim\operatorname{pgcd}(b,r).$$

Preuve Grâce à la relation $a=bq+r$, tout diviseur commun de a et b est un diviseur commun de b et r et réciproquement. On en déduit que $\operatorname{pgcd}(a,b)\sim\operatorname{pgcd}(b,r)$. ◁

On remarquera que cette proposition n'utilise pas l'hypothèse euclidienne dès lors qu'on écrit simplement $a=bq+r$ pour deux éléments quelconques $q,r\in A$.

Entrée Deux éléments a et b d'un anneau euclidien A
Sortie Un PGCD de a et b
$r_0 \longleftarrow a$
$r_1 \longleftarrow b$
Tant que $r_1 \neq 0$, faire
  $t \longleftarrow r_1$
  $r_1 \longleftarrow$ le reste de la division euclidienne de r_0 par r_1
  $r_0 \longleftarrow t$
Retourner r_0

Algorithme 1 – L'algorithme d'Euclide classique

Théorème 27 *(algorithme d'Euclide).* Soient $a, b \in A \setminus \{0\}$ deux éléments non nuls. Considérons la suite $(r_i)_{i\in\mathbf{N}}$ de A définies de la manière suivante :
- $r_0 = a$ et $r_1 = b$;
- si $r_i \neq 0$, alors l'élément r_{i+1} est le reste d'une division euclidienne de r_{i-1} par r_i ;
- si $r_i = 0$, alors $r_{i+1} = 0$.

Alors il existe un plus petit entier $N \in \mathbf{N}$ tel que $r_{N+1} = 0$. De plus, on a

$$\operatorname{pgcd}(a, b) \sim r_N.$$

Preuve On suppose qu'il n'existe pas d'entier $i \in \mathbf{N}$ tel que $r_{i+1} = 0$. La suite $(\nu(r_i))_{i\in\mathbf{N}}$ est alors bien définie et, par la définition 24, elle est strictement décroissante. Ceci est impossible puisqu'elle est minorée. On peut donc trouver un plus petit entier $N \in \mathbf{N}$ tel que $r_{N+1} = 0$.

Maintenant, la proposition 26 donne $\operatorname{pgcd}(r_i, r_{i-1}) \sim \operatorname{pgcd}(r_i, r_{i+1})$ pour tout $i \in [\![1, N]\!]$. Comme $(r_0, r_1) = (a, b)$, une récurrence immédiate assure alors $\operatorname{pgcd}(a, b) \sim \operatorname{pgcd}(r_i, r_{i+1})$ pour tout $i \in [\![1, N]\!]$. En particulier, pour $i = N$, on obtient $\operatorname{pgcd}(a, b) \sim \operatorname{pgcd}(r_N, 0) = r_N$ ◁

De ce théorème, on en déduit l'algorithme d'Euclide (classique) qui renvoie un PGCD de deux éléments d'un anneau euclidien (voir l'algorithme 1). Ce procédé, appelé l'anthyphérèse, a été introduit pour la première fois dans *Les Éléments* d'Euclide (environ 330–275 av. J.-C.), bien qu'Euclide lui-même ne l'aie probablement pas découvert. Ce procédé est sûrement le premier exemple historique d'algorithme connu.

Exemple. On appliquons l'algorithme d'Euclide aux polynômes

$$P \coloneqq X^4 - 13X^3 + 2X^2 - X - 1 \qquad \text{et} \qquad Q \coloneqq X^2 - X - 1.$$

dans l'anneau $\mathbf{Q}[X]$. La suite des restes vérifie

$$r_0 = A, \qquad r_1 = B, \qquad r_2 = -22X - 10, \qquad r_3 = -41/121 \qquad \text{et} \qquad r_4 = r_5 = \cdots = 0.$$

On en déduit que les polynômes P et Q sont premiers entre eux.

Dans le cas de l'anneau $k[X]$, on peut donner le coût de l'algorithme d'Euclide. Soient $P, Q \in k[X]$ deux polynômes de degrés respectifs m et n avec $m \geqslant n$. On rappelle que le calcul de la division euclidienne de P par Q demande au plus $(2n+1)(m-n+1)+1$ opérations dans k, comme expliqué dans le livre [2].

Théorème 28. L'algorithme d'Euclide classique calcul le PGCD de deux polynômes $P, Q \in k[X]$ en $\mathrm{O}(\deg P \deg Q)$ opérations sur le corps k.

Preuve La correction de l'algorithme vient du théorème précédent. Notons $(R_i)_{i\in\mathbf{N}}$ la suite des restes obtenus. Soit $N \in \mathbf{N}$ le plus petit entier tel que $R_{N+1} = 0$. D'après la rappel ci-dessus, son coût est majoré par la quantité

$$C \coloneqq \sum_{i=1}^{N} [(2 \deg R_i + 1)(\deg R_{i-1} - \deg R_i + 1) + 1]$$

Par ailleurs, comme la suite $(\deg R_i)_{i\in[\![1,N]\!]}$ d'entiers strictement positifs décroît strictement, on peut écrire

$$\deg R_i \leqslant \deg R_1 - i + 1 \leqslant \deg R_1 = \deg Q, \qquad i \in [\![1, N]\!]$$

et, en particulier, cela implique

$$N \leqslant \deg Q.$$

À partir de ces deux dernières inégalités, lorsque $\deg P \geqslant \deg Q$, on obtient alors

$$\begin{aligned} C &\leqslant (2\deg Q + 1)\sum_{i=1}^{N}(\deg R_{i-1} - \deg R_i + 1) + N \\ &\leqslant (2\deg Q + 1)(\deg R_0 - \deg R_N + N) + \deg Q \\ &\leqslant (2\deg Q + 1)(\deg P + \deg Q) + \deg Q \\ &\leqslant 2(\deg Q + 1)(\deg P + \deg Q) \\ &\leqslant 4(\deg Q + 1)\deg P. \end{aligned}$$

Lorsque $\deg Q \geqslant \deg P$, la première étape ne fait qu'échanger les polynômes P et Q et cette étape ne coûte pas d'opérations sur le corps k. Dans tous les cas, la borne ci-dessus est valable ce qui montre $C = \mathrm{O}(\deg P \deg Q)$. ◁

On peut estimer le coût de l'algorithme d'Euclide dans $\mathbf{Z}$. Soient $x, y \in \mathbf{Z}^*$ deux entiers avec $x > y$. On note $x = qy+r$ la division euclidienne. Cette dernière demande $\mathrm{O}(\log q \log y)$ opérations binaires avec l'algorithme naïf. En effet, pour trouver chaque chiffre du quotient q, on effectue $\mathrm{O}(\log y)$ opérations binaires et cela permet de conclure puisque le nombre q possède $\lfloor \log q \rfloor + 1$ chiffres. Une justification plus rigoureuse de ce fait peut-être trouvé dans le livre [8]

Théorème 29. L'algorithme d'Euclide calcul le PGCD de deux entiers $a, b \in \mathbf{Z}^*$ en $\mathrm{O}(\log a \log b)$ opérations binaires.

Preuve Notons $(q_i, r_i)_{i\in[\![1,N]\!]}$ la suite des quotients et restes successifs dans l'algorithme d'Euclide appliqué aux entiers a et b. L'algorithme effectuant les N divisions euclidiennes, il demande

$$\mathrm{O}\Big(\sum_{i=1}^{N} \log r_i \log q_i\Big)$$

opérations binaires. Or les restes r_i sont majorés par l'entier b et on vérifie que $a \geqslant q_1 \cdots q_N$ en effectuant une simple récurrence. Ainsi il demande $\mathrm{O}(\log a \log b)$ opérations. ◁

Il est aussi possible de borner le nombre d'étapes. Notons $\lambda(a, b)$ le nombre d'étapes dans l'algorithme appliqué aux entiers a et b. Par ailleurs, on définit l'ordre lexicographique sur $\mathbf{N}^2$ par

$$(a, b) \prec (a', b') \quad \Longleftrightarrow \quad a < a' \quad \text{ou} \quad (a = a' \quad \text{et} \quad b < b').$$

Proposition 30 *(Lamé).* Soient $a, b \in \mathbf{N}$ deux entiers vérifiant $a > b > 0$. Soit $N \in \mathbf{N}^*$ un entier. On suppose que

- $\lambda(a, b) = N$;
- pour tous entiers $a', b' \in \mathbf{N}$ vérifiant $a' > b' > 0$, si $\lambda(a', b') = N$, alors $(a, b) \preceq (a', b')$.

Soit $(F_n)_{n\in\mathbf{N}}$ la suite de Fibonacci. Alors $(a, b) = (F_{N+2}, F_{N+1})$.

Preuve Une récurrence immédiate sur l'entier $N \in \mathbf{N}^*$ montre que $\lambda(F_{N+2}, F_{N+1}) = N$ puisque la division euclidienne de F_{N+2} par F_{N+1} s'écrit $F_{N+2} = F_{N+1} + F_N$. La seconde hypothèse assure alors $(a, b) \preceq (F_{N+2}, F_{N+1})$. Il suffit donc de montrer que

$$(a, b) \not\prec (F_{N+2}, F_{N+1}). \tag{9}$$

Une récurrence sur l'entier $n \in \mathbf{N}^*$ permet de montrer que

$$\forall x, y \in \mathbf{N}^*, \qquad \lambda(x, y) = n \quad \Longrightarrow \quad x \geqslant F_{n+2} \quad \text{et} \quad y \geqslant F_{n+1}.$$

En particulier, on obtient $a \geqslant F_{N+2}$ et $b \geqslant F_{N+1}$ ce qui équivaut à la relation (9) et conclut. ◁

Corollaire 31. Soient $a, b, N \in \mathbf{N}^*$ deux entiers vérifiant $a > b > 0$. Soit $\varphi := \frac{1}{2}(1+\sqrt{5})$ le nombre d'or. On suppose que $\lambda(a,b) = N$. Alors $N \leqslant 1 + \lfloor \log_\varphi b \rfloor$.

Preuve La proposition 30 donne alors $b \geqslant F_{N+1} \geqslant F_N$. Par ailleurs, une simple récurrence montre que $F_N > \varphi^{N-1}$ ce qui permet de conclure le résultat. ◁

2.3. L'algorithme d'Euclide étendu et une application

2.3.1. *Un raffinement de l'algorithme classique*

On peut raffiner l'algorithme d'Euclide classique afin qu'il nous donne une relation de Bézout associée à deux éléments d'un anneau euclidien.

Théorème 32 *(algorithme d'Euclide étendu).* Soient $a, b \in A \setminus \{0\}$ deux éléments non nuls. Considérons les suites $(r_i)_{i\in\mathbf{N}}$, $(u_i)_{i\in\mathbf{N}}$ et $(v_i)_{i\in\mathbf{N}}$ de A définies de la manière suivante :
- $r_0 = a$ et $r_1 = b$;
- $u_0 = 1$ et $u_1 = 0$;
- $v_0 = 0$ et $v_1 = 1$;
- si $r_i \neq 0$, alors
  - l'élément r_{i+1} est le reste d'une division euclidienne de r_{i-1} par r_i, associé au quotient q_i,
  - si $i > 1$, alors $u_{i+1} = u_{i-1} - q_i u_i$ et $v_{i+1} = v_{i-1} - q_i v_i$.
- si $r_i = 0$, alors $r_{i+1} = 0$.

Soit $N \in \mathbf{N}$ le plus petit entier tel que $r_{N+1} = 0$. Alors

$$\operatorname{pgcd}(a,b) \sim r_N \qquad \text{et} \qquad u_N a + v_N a = r_N.$$

Preuve La première partie de l'énoncé correspond au théorème 27. Seule l'égalité $u_N a + v_N a = r_N$ reste à vérifier. On va montrer, en effectuant une récurrence sur l'entier $i \in [\![0, N]\!]$, que

$$u_i a + v_i b = r_i \tag{10}$$

ce qui conclura. Par définition des trois suites de l'énoncé, les cas $i = 0$ et $i = 1$ sont immédiats. Soit $i \in [\![2, N]\!]$. On suppose que l'égalité (10) tienne aux rangs i et $i-1$. Par définition, on écrit

$$r_{i-1} = q_i r_i + r_{i+1}$$

et, avec l'hypothèse de récurrence, on obtient

$$\begin{aligned} u_{i+1}a + v_{i+1}b &= (u_{i-1} - q_i u_i)a + (v_{i-1} - q_i v_i)b \\ &= (u_{i-1}a + v_{i-1}b) - (u_i a + v_i b)q_i \\ &= r_{i-1} - r_i q_i = r_{i+1} \end{aligned}$$

ce qui montre l'égalité (10) au rang $i+1$. Ceci achève la récurrence. En particulier, le cas $i = N$ donne la relation de Bézout recherchée. ◁

Exemple. Plaçons-nous dans l'anneau $\mathbf{Z}$. On veut calculer une relation de Bézout associée aux entiers 15 et 36. On commence par les réordonner et par écrire les deux égalités triviales

$$36 = 1 \times 36 + 0 \times 15, \tag{ℓ_0}$$

$$15 = 0 \times 36 + 1 \times 15. \tag{ℓ_1}$$

On calcule la division euclidienne de 36 par 15 : on obtient $36 = 2 \times 15 + 6$, c'est-à-dire

$$6 = 1 \times 36 - 2 \times 15. \tag{ℓ_2}$$

Cette dernière égalité est équivalente à l'opération $1 \times (\ell_0) - 2 \times (\ell_1)$. On recommence et on calcul la division euclidienne de 15 par 6 : on obtient $15 = 2 \times 6 + 3$, c'est-à-dire $3 = 1 \times 15 - 2 \times 6$. On effectue alors l'opération $1 \times (\ell_1) - 2 \times (\ell_2)$ ce qui donne l'égalité

$$3 = -2 \times 36 + 5 \times 15. \tag{ℓ_3}$$

Enfin, de même, on écrit $6 = 3 \times 2 + 0$. Cette fois-ci, on s'arrête. On en déduit que le PGCD des entiers 15 et 36 vaut 4 et qu'une relation de Bézout est donnée par l'égalité (ℓ_3).

De ce théorème, on en déduit l'algorithme d'Euclide étendu (voir l'algorithme 2). On se convaincra que son coût est le même que celui de la version classique.

Entrée Deux éléments a et b d'un anneau euclidien A
Sortie Un PGCD d de a et b et deux éléments $u, v \in A$ tels que $ua + vb = d$

$(r_0, r_1, u_0, u_1, v_0, v_1) \longleftarrow (a, b, 1, 0, 0, 1)$
Tant que $r_1 \neq 0$, faire
  $T \longleftarrow (r_1, u_1, v_1)$
  $(q, r_1) \longleftarrow$ le quotient et le reste d'une division euclidienne de r_0 et r_1
  $u_1 \longleftarrow u_1 - qu_0$
  $v_1 \longleftarrow v_1 - qv_0$
  $(r_0, u_0, v_0) \longleftarrow T$
Retourner r_0, u_0, v_0

Algorithme 2 – L'algorithme d'Euclide étendu

2.3.2. *Une application : calcul d'inverse modulaire*

Soient A un anneau euclidien et $a \in A \setminus (\{0\} \cup A^\times)$ un élément non inversible et non nul. L'algorithme d'Euclide étendu permet de trouver l'inverse d'un inversible de l'anneau $B \coloneqq A/(a)$. Soit $\overline{b} \in B$ un élément inversible dans B. Cela signifie qu'il existe un élément $v \in A$ tel que

$$bv \equiv 1 \mod a.$$

Ainsi il existe un autre élément $u \in A$ tel que $au + bv = 1$. L'inverse de l'élément $\overline{b}$ dans B étant l'élément $\overline{v}$, pour le trouver, il suffit donc de calculer une relation de Bézout dans A associée aux éléments a et b.

Exemple. On considère l'anneau quotient $\mathbf{R}[X]/(1 + X^2)$ qui se trouve être isomorphe au corps $\mathbf{C}$ des complexes. On souhaite trouver l'inverse de l'élément $\overline{a + bX} = a + ib$ pour deux réels $a, b \in \mathbf{R}$ avec $(a, b) \neq (0, 0)$. En appliquant l'algorithme d'Euclide étendu aux polynômes $a + bX$ et $1 + X^2$ dans $\mathbf{R}[X]$, on obtient successivement

$$\begin{aligned}
1 + X^2 &= \quad 0 \quad \times (a + bX) + \ 1 \ \times (1 + X^2), \\
a + bX &= \quad 1 \quad \times (a + bX) + \ 0 \ \times (1 + X^2), \\
b - aX = b(1 + X^2) - X(a + bX) &= -X \quad \times (a + bX) + \ b \ \times (1 + X^2), \\
a(a + bX) + b(b - aX) &= (a - bX) \times (a + bX) + b^2 \times (1 + X^2)
\end{aligned}$$

ce qui donne la relation de Bézout

$$(a - bX)(a + bX) + b^2(1 + X^2) = a^2 + b^2$$

si bien que

$$\frac{a - bX}{a^2 + b^2}(a + bX) + \frac{b^2}{a^2 + b^2}(1 + X^2) = 1.$$

De cette dernière égalité, on retrouve la formule bien connue

$$(a + ib)^{-1} = \frac{a - ib}{a^2 + b^2}.$$

3. Application à l'arithmétique

3.1. Résolution d'équations diophantiennes

On cherche maintenant à résoudre certaines équations diophantiennes, c'est-à-dire à trouver les racines entières de certains polynômes à coefficients entiers. Pour les exemples choisis, on verra que la notion de PGCD sera centrale. Les résultats cités viennent des livres [4, 3].

Théorème 33. Soient $a, b, d \in \mathbf{Z}$ trois entiers. Notons $d \coloneqq \operatorname{pgcd}(a, b)$.

1. Alors il existe un couple $(x, y) \in \mathbf{Z}^2$ vérifiant l'équation

$$ax + by = c \tag{11}$$

si et seulement si $d \mid c$.

2. On suppose que $d \mid c$. Notons $a' \coloneqq a/d$ et $b' \coloneqq b/d$. Soit $(x_0, y_0) \in \mathbf{Z}^2$ une solution de l'équation (11). Alors les solutions de cette dernière sont exactement les couples de la forme
$$(x_0 - kb', y_0 + ka') \quad \text{avec} \quad k \in \mathbf{Z}.$$

Preuve Montrons le premier point. Directement, on suppose qu'il existe un couple $(x, y) \in \mathbf{Z}^2$ vérifiant l'équation (11). Comme $d = \operatorname{pgcd}(a, b)$, on peut écrire $d \mid a$ et $d \mid b$. L'équation (11) assure alors $d \mid c$. Réciproquement, on suppose que $d \mid c$. Comme $d = \operatorname{pgcd}(a, b)$, on peut exhiber une relation de Bézout $au + bv = d$ pour deux entiers $u, v \in \mathbf{Z}$. Comme $d \mid c$, il existe un entier $\lambda \in \mathbf{Z}$ tel que $c = \lambda d$. En multipliant la relation de Bézout par l'entier λ, on obtient $a\lambda u + b\lambda v = c$. Le couple $(\lambda u, \lambda v) \in \mathbf{Z}^2$ vérifient donc l'équation (11).

Montrons le second point. On vérifie que les couples présentés sont bien des solutions puisque, pour tout entier $k \in \mathbf{Z}$, les égalités $ax_0 + by_0 = c$ et $ab' = ba'$ impliquent
$$a(x_0 - kb') + b(y_0 + ka') = c + (ab' - ba')k = c.$$
Réciproquement, montrons que ce sont les seules. Soit $(x, y) \in \mathbf{Z}^2$ une solution. Comme le couple (x_0, y_0) est aussi une solution, on peut écrire $a(x_0 - x) = b(y - y_0)$, donc $a'(x_0 - x) = b'(y - y_0)$. En particulier, cela donne la divisibilité $a' \mid b'(y - y_0)$. Comme les entiers a' et b' sont premiers entre eux, le lemme de Gauss assure $a' \mid y - y_0$, c'est-à-dire il existe un entier $k \in \mathbf{Z}$ tel que $y - y_0 = ka'$. De la sorte, en réinjectant ceci dans l'équation $a'(x_0 - x) = b'(y - y_0)$, on en déduit $x_0 - x = kb'$. Finalement, on a obtenu $x = x_0 - kb'$ et $y = y_0 + ka'$. ◁

Le théorème permet de trouver toutes les solutions dès lors que l'on a une solution particulière. Pour en trouver une, on procède comme dans la preuve : on exhibe une relation de Bézout $au + bv = d$ grâce à l'algorithme d'Euclide étendu et le couple $(\lambda u, \lambda v) \in \mathbf{Z}^2$ avec $\lambda \coloneqq c/d$ est alors une solution particulière de l'équation (11).

Exemple. On cherche à résoudre l'équation
$$6x + 4y = 10.$$
Comme $\operatorname{pgcd}(6, 4) = 2 \mid 10$, cette équation admet des solutions entières. D'abord, une relation de Bézout reliant les entiers 6 et 4 est
$$2 = 1 \times 6 - 1 \times 4.$$
Comme $10 = 2 \times 5$, une solution particulière est le couple $(5, -5)$. Comme $6 = 2 \times 3$ et $4 = 2 \times 2$, on en déduit que les solutions sont de la forme
$$(5 - 2k, 3k - 5) \quad \text{avec} \quad k \in \mathbf{Z}.$$

Une équation diophantienne célèbre est l'équation de Fermat
$$x^n + y^n = z^n$$
pour un entier $n \geqslant 1$. Un théorème très difficile, montré en 1993 par Andrew Wiles, montre que l'équation pour $n \geqslant 3$ ne possède pas de solutions non triviales, c'est-à-dire vérifiant $xyz \neq 0$. Ce résultat a valu la médaille Fields à Wiles. On va montrer que l'équation pour $n = 2$ admet des solutions et que celles-ci sont explicites.

Théorème 34. Les solutions de l'équation
$$x^2 + y^2 = z^2 \quad \text{avec} \quad (x, y, z) \in (\mathbf{N}^*)^3 \tag{12}$$
sont exactement les triplets de la forme
$$(2kmn, k(m^2 - n^2), k(m^2 + n^2)) \quad \text{ou} \quad (k(m^2 - n^2), 2kmn, k(m^2 + n^2))$$
pour trois entiers $k, m, n \in \mathbf{N}$ tels que $k \neq 0$ et $m > n$.

Preuve Soient $(x, y, z) \in (\mathbf{N}^*)^3$ une solution de l'équation (12). Quitter à diviser ce triplet par l'entier $\operatorname{pgcd}(x, y, z) \neq 0$ ce qui ne fera que changer l'entier k, on peut supposer que les entiers x, y et z sont premiers dans leur ensemble.

Alors les entiers x, y et z sont deux à deux premiers entre eux. Par symétrie, il suffit de le faire pour les entiers x et y. Raisonnons par l'absurde et supposons le contraire. Soit alors $p \geqslant 2$ un

diviseur premier de x et y. Alors $p \mid x^2+y^2$, donc l'équation (12) donne $p \mid z^2$. Comme p est premier, le lemme d'Euclide donne $p \mid z$. Mais ceci est contradictoire avec le fait que $\operatorname{pgcd}(x,y,z)=1$.

Montrons que l'un des entiers x et y est pair. Remarquons d'abord que, pour tout entier $n \in \mathbf{Z}$, on a $(2n+1)^2 = 4n^2+4n+1 \equiv 1 \mod 4$. Raisonnons par l'absurde et supposons que les entiers x et y sont impairs. Grâce à la remarque, on obtient $z^2 = x^2+y^2 \equiv 2 \mod 4$. Cependant, tout carré est congru à 0 ou 1 modulo 4 ce qui est impossible. Dans la suite, quitte à échanger les rôles des entiers x et y ce qui ne pose pas de problème vis-à-vis de l'énoncé, on suppose donc que l'entier x est pair. Comme $\operatorname{pgcd}(x,y)=1$ et $\operatorname{pgcd}(x,z)=1$ d'après le précédent paragraphe, cela signifie que les entiers y et z sont impairs.

Les entiers $z \pm y$ sont alors pairs et, avec l'équation (12), on peut écrire

$$\frac{z-y}{2} \times \frac{z+y}{2} = \frac{z^2-y^2}{4} = \left(\frac{x}{2}\right)^2.$$

Montrons que les éléments $a_\pm := \frac{1}{2}(z \pm y)$ sont des carrés. Raisonnons encore par l'absurde et supposons que l'élément a_+ n'en soit pas. Alors il existe un nombre premier $p \geqslant 2$ tel que

$$p \mid a_+ \quad \text{et} \quad p^2 \nmid a_+.$$

Comme $(x/2)^2 = a_-a_+$, on obtient $p \mid (x/2)^2$, donc $p^2 \mid (x/2)^2$. Comme $p^2 \nmid a_+$, cela donne $p^2 \mid a_-$, donc $p \mid a_-$. Mais alors l'entier p divise les entiers $a_- + a_+ = z$ et $a_- + a_+ = y$ ce qui est impossible puisque $\operatorname{pgcd}(y,z)=1$. Finalement, il existe deux entiers $n, m \in \mathbf{N}$ tels que

$$z-y = 2n^2 \qquad \text{et} \qquad z+y = 2m^2$$

Concluons. En sommant et en soustrayant ces deux dernières égalités, on déduit

$$z = m^2+n^2 \qquad \text{et} \qquad y = m^2-n^2.$$

Avec l'équation (12), on trouve alors

$$x^2 = z^2-y^2 = (z-y)(z+y) = 4m^2n^2, \qquad \text{donc} \qquad x = 2mn$$

car $x, m, n \geqslant 0$. Finalement, la solution (x,y,z) est bien de la forme annoncée. Réciproquement, on vérifie que de tels triplets sont solutions. ◁

Donnons enfin un cas particulier de l'équation de Fermat que l'on sait résoudre. Le théorème suivant est dû à Sophie Germain (1776–1831), il a été montré en 1823. Cet énoncé constituera notre second développement, sa preuve se trouve dans le livre [3].

À l'époque où les mathématiques étaient réservées aux hommes, elle dut emprunter le nom d'Antoine Auguste Le Blanc afin de se procurer les cours de l'École polytechnique. C'est sous ce nom sous lequel elle put ensuite échanger avec Joseph-Louis Lagrange. Ce dernier fut impressionné par ces travaux et, en la présentant à la communauté scientifique, elle acquit une notoriété.

Théorème 35 *(Germain).* Soit $p \geqslant 3$ un nombre premier tel que le nombre $q := 2p+1$ soit premier. Alors il n'existe pas de triplet $(x,y,z) \in \mathbf{Z}^3$ tel que

$$xyz \not\equiv 0 \mod p \qquad \text{et} \qquad x^p+y^p+z^p = 0. \tag{13}$$

Preuve Raisonnons par l'absurde et supposons qu'il existe un triplet $(x,y,z) \in \mathbf{Z}^3$ vérifiant les relations (13). Comme dans la preuve du théorème 34, on peut supposer que $\operatorname{pgcd}(x,y,z)=1$ et, dans ce cas, les éléments x, y et z sont deux à deux premiers entre eux.

Montrons d'abord que les éléments $y+z$ et $t := \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux. Raisonnons par l'absurde et supposons que $\operatorname{pgcd}(y+z,t) > 1$. Alors les éléments $y+z$ et t possèdent un diviseur premier commun $r \geqslant 2$. Un simple calcul combiné avec l'équation (13) et le fait $p \geqslant 3$ donnent

$$(y+z)t = y^p+z^p = -x^p = (-x)^p \tag{14}$$

Ainsi on a $r^2 \mid x^p$ ce qui, avec le lemme d'Euclide, assure $r \mid x$. Par ailleurs, comme $y \equiv -z \mod r$, on obtient

$$0 \equiv t \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1} \mod r, \tag{15}$$

donc $r \mid py^{p-1}$. Comme $r \mid x$ et $\operatorname{pgcd}(x,y) = 1$, on a $\operatorname{pgcd}(r,y) = 1$ et le lemme de Gauss conclut alors $r \mid p$, donc $r = p$, donc $p \mid x$ ce qui est impossible puisque $xyz \not\equiv 0 \mod p$. Par conséquent, les entiers $y+z$ et t sont premiers entre eux.

Grâce à l'égalité (14), le même argument que dans la preuve du théorème 34 montre que les entiers $y+z$ et t sont des puissances p-ièmes. Par symétrie, il en va de même pour les entiers $x+y$ et $x+z$. Il existe donc quatre entiers $a, b, c, \alpha \in \mathbf{Z}$ tels que

$$y+z = a^p, \qquad x+z = b^p, \qquad x+y = c^p \quad \text{et} \quad t = \alpha^p. \tag{16}$$

Soit $m \in \mathbf{Z}$ un entier tel que $q \nmid m$. Montrons que $m^p \equiv \pm 1 \mod q$. Le petit théorème de Fermat assure $m^{q-1} \equiv 1 \mod q$. Comme $q - 1 = 2p$, cela équivaut à l'équation $(m^p)^2 \equiv 1 \mod q$, c'est-à-dire $m^p \equiv \pm 1 \mod q$.

Déduisons-en qu'un seul des trois entiers x, y et z n'est divisible par q. Pour commencer, montrons qu'au moins un des trois est divisible par q. Si ce n'était pas le cas, alors le précédent paragraphe donnerait $x^p, y^p, z^p \equiv \pm 1 \mod q$, donc $0 = x^p + y^p + z^p \equiv \pm 3, \pm 1 \mod q$ ce qui est impossible car $q > 5$. Donc un des trois entiers x, y et z est divisible par q. Quitter à échanger leurs rôles, on suppose $q \mid x$. Mais comme ils sont deux à deux premiers entre eux, on a $q \nmid y$ et $q \nmid z$.

Concluons. On raisonne maintenant dans le corps $\mathbf{Z}/q\mathbf{Z}$. Avec les égalités (16) et comme $q \mid x$, on obtient $b^p + c^p - a^p = 2x = 0$. Comme $q \nmid y$, le lemme d'Euclide donne alors $q \nmid c$. Avec l'avant-dernier paragraphe, on en déduit $y = x + y = c^p = \pm 1$. De même, on trouve $z = \pm 1$. On peut maintenant montrer que $q \mid a$. Sinon le même paragraphe donnerait $a^p = \pm 1$ puis $0 = b^p + c^p - a^p = \pm 3, \pm 1$ ce qui est impossible. D'où $q \mid a$. Ainsi on peut écrire $y + z = a^p = 0$, c'est-à-dire $y = -z$. Ainsi, comme dans la relation (15), on a $\alpha^p = t = py^{p-1}$. Comme $y = \pm 1$, cela donne $\alpha^p = p(-1)^{p-1} = p$. Mais l'avant-dernier paragraphe montre que $p = \alpha^p = 0, \pm 1$, donc $p \mid q$ ou $q = 2p + 1 \mid p \mp 1$ ce qui est encore impossible.

Dans tous les cas, l'hypothèse du début conduit à une absurdité. Ainsi il ne peut exister de tel triplet $(x, y, z) \in \mathbf{Z}^3$. ◁

3.2. Interpolation et systèmes de congruences

Les énoncés suivants proviennent du livre [1] et leurs différents aspects algorithmique sont expliqués dans le livre [2].

3.2.1. *Le théorème des restes chinois*

Théorème 36 *(des restes chinois).* Soient A un anneau et $I_1, \dots, I_n \subset A$ des idéaux deux à deux étrangers, c'est-à-dire vérifiant

$$i \neq j \quad \Longrightarrow \quad I_i + I_j = A.$$

Pour chaque indice $i \in [\![1, n]\!]$, on considère la projection $\pi_i \colon A \longrightarrow A/I_i$. Alors l'application

$$\varphi \colon \left| \begin{array}{l} A \longrightarrow A/I_1 \times \cdots \times A/I_n, \\ x \longmapsto (\pi_1(x), \dots, \pi_n(x)) \end{array} \right.$$

est un morphisme d'anneaux surjectif de noyau $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.

Preuve Grâce à la condition d'étrangeté, on montre le théorème en effectuant une récurrence sur l'entier n. Il suffit alors de montrer le cas $n = 2$. C'est clairement un morphisme d'anneaux.

Son noyau est l'idéal $I_1 \cap I_2$. Il reste à vérifier que $I_1 \cap I_2 = I_1 I_2$. L'inclusion $\supset$ est toujours vérifiée. Réciproquement, soit $x \in I \cap J$. Notre hypothèse est $I_1 + I_2 = A$, donc il existe deux éléments $i_1 \in I_1$ et $i_2 \in I_2$ tels que $1 = i_1 + i_2$, donc $x = xi_1 + xi_2 \in I_1 I_2$. Ceci conclut $\operatorname{Ker} \varphi = I_1 I_2$.

Montrons que le morphisme φ est surjectif. Soient $u_1 \in A/I_1$ et $u_2 \in A/I_2$. Comme les projections sont surjectives, on note $\pi_1(x_1) = u_1$ et $\pi_2(x_2) = u_2$ pour deux éléments $x_1, x_2 \in A$. De la sorte, l'élément $x \coloneqq i_1 x_2 + i_2 x_1$ vérifie $\varphi(x) = (u_1, u_2)$. ◁

Corollaire 37 *(théorème des restes chinois pour les entiers).* Soient $m_1, \dots, m_n \in \mathbf{Z}$ des entiers deux à deux premiers entre eux et $v_1, \dots, v_n \in \mathbf{Z}$ d'autres entiers quelconques. Alors il existe un

unique entier $a \in [\![0, m_1 \cdots m_n - 1]\!]$ vérifiant le système

$$\begin{cases} a \equiv v_1 & \mod m_1, \\ \vdots & \\ a \equiv v_n & \mod m_n. \end{cases}$$

Preuve Il suffit d'appliquer le théorème 36 dans l'anneau $A = \mathbf{Z}$ avec les idéaux $I_i = m_i\mathbf{Z}$. ◁

3.2.2. Calcul effectif des solutions d'un système de congruences

On garde les mêmes notations que le corollaire 37. On suppose $m_1, \ldots, m_n \in \mathbf{N}$. On souhaite trouver explicitement les solutions entières du système de congruences

$$\begin{cases} x \equiv v_1 & \mod m_1, \\ \vdots & \\ x \equiv v_n & \mod m_n. \end{cases} \tag{17}$$

L'interpolation de Lagrange. On procède comme dans la preuve du théorème 36. Considérons l'entier $M \coloneqq m_1 \cdots m_n$. Soit $i \in [\![1, n]\!]$ un indice. Notons $M_i \coloneqq M/m_i$. Comme $\operatorname{pgcd}(M_i, m_i) = 1$, il existe un entier $N_i \in [\![0, m_i - 1]\!]$ tel que

$$N_i M_i \equiv 1 \mod m_i.$$

Ce dernier se trouve grâce à l'algorithme d'Euclide étendu. On pose ensuite $\ell_i \coloneqq M_i N_i$. Dès lors, l'unique solution du système est l'entier

$$a = \sum_{i=1}^{n} v_i \ell_i.$$

Entrée Un n-uplet $(m_1, \ldots, m_n)$ d'entiers deux à deux premiers entre eux et un n-uplet $(v_1, \ldots, v_n)$ d'entiers
Sortie L'unique solution $a \in [\![0, m_1 \cdots m_n - 1]\!]$ du système (17)

```
M ⟵ m_1 ··· m_n
a ⟵ 0
Pour i allant de 1 à n, faire
    M_i ⟵ M/m_i
    Trouver une relation de Bézout u M_i + v m_i = 1 avec l'algorithme 2
    N_i ⟵ reste(u, m_i)
    a ⟵ a + v_i M_i N_i
Retourner reste(a, M)
```

Algorithme 3 – L'interpolation de Lagrange pour les entiers

Exemple. On souhaite résoudre le système

$$\begin{cases} x \equiv 0 & \mod 2, \\ x \equiv 2 & \mod 3, \\ x \equiv -2 & \mod 7. \end{cases} \tag{18}$$

On calcul d'abord $M \coloneqq 2 \times 3 \times 7 = 42$. Les entiers 2, 3 et 7 étant premiers, ce système admet une unique solution dans l'intervalle $[\![0, 41]\!]$.

- L'élément $M_1 \coloneqq M/2 = 21 \equiv 1$ est d'inverse $N_1 = 1$ dans $\mathbf{Z}/2\mathbf{Z}$.
- L'élément $M_2 \coloneqq M/3 = 14 \equiv -1$ est d'inverse $N_2 = -1$ dans $\mathbf{Z}/3\mathbf{Z}$.
- L'élément $M_3 \coloneqq M/7 = 6 \equiv -1$ est d'inverse $N_2 = -1$ dans $\mathbf{Z}/7\mathbf{Z}$.

Finalement, l'unique solution est

$$0 \times 21 \times 1 + 2 \times 14 \times (-1) - 2 \times 6 \times (-1) = -16.$$

L'interpolation de Newton. Soient $\alpha_1, \dots, \alpha_n \in \mathbf{Z}$ des entiers vérifiant

$$0 \leqslant \alpha_i < m_i, \qquad i \in [\![1, n]\!]$$

et

$$\alpha_0 + \cdots + m_1 \cdots m_{i-1}\alpha_i \equiv v_i \mod m_i, \qquad i \in [\![1, n]\!]. \tag{19}$$

Alors l'entier

$$a \coloneqq \alpha_1 + m_1\alpha_2 + \cdots + m_1 \cdots m_{n-1}\alpha_n$$

vérifie le système (17). Il s'agit donc de savoir résoudre successivement les équations (19) : on utilisera l'algorithme d'Euclide étendu.

Entrée Un n-uplet $(m_1, \dots, m_n)$ d'entiers deux à deux premiers entre eux et un n-uplet $(v_1, \dots, v_n)$ d'entiers
Sortie L'unique solution $a \in [\![0, m_1 \cdots m_n - 1]\!]$ du système (17)

```
a ⟵ 0
Pour i allant de 1 à n, faire
    c_i ⟵ m_1 ··· m_{i-1}
    α_i ⟵ 0
    Tant que a + c_i α_i ≢ v_i mod m_i, faire
        α_i ⟵ α_i + 1
    a ⟵ a + c_i α_i
Retourner reste(a, m_1 ··· m_n)
```

Algorithme 4 – L'interpolation de Newton pour les entiers

Exemple. Soit $a \coloneqq \alpha_1 + 2\alpha_2 + 6\alpha_3$ un entier solution du système (18) avec

$$0 \leqslant \alpha_1 < 2, \qquad 0 \leqslant \alpha_2 < 3 \qquad \text{et} \qquad 0 \leqslant \alpha_3 < 7.$$

On cherche l'entier α_1. La congruence $a \equiv 0 \mod 2$ donne $\alpha_1 \equiv 0 \mod 2$, donc $\alpha_1 = 0$. On continue avec le même procédé pour trouver l'entier α_2. Comme $a \equiv 2 \mod 3$ et avec $\alpha_1 = 0$, on peut écrire $2\alpha_2 \equiv 2 \mod 3$, donc $\alpha_2 = 1$. La dernière congruence donne $2 + 6\alpha_3 \equiv -2 \mod 7$, c'est-à-dire $2\alpha_3 \equiv 1 \mod 7$. Pour résoudre cette dernière relation, on peut chercher une relation de Bézout reliant les entiers 2 et 7 : on trouve $1 = 7 - 3 \times 2$. On obtient alors $\alpha_3 \equiv -3 \mod 7$ ce qui donne $\alpha_3 = 4$. Finalement, on retrouve l'unique solution

$$a = 0 + 2 \times 1 + 6 \times 4 = 26$$

modulo $M = 42$.

L'avantage de l'interpolation de Newton est qu'il est facile de rajouter une équation au système : à partir d'une solution du système, on peut en déduire une solution du système avec une équation en plus. Par exemple, si on rajoute l'équation $x \equiv 2 \mod 5$ au système (18), on cherche alors une solution sous la forme $26 + 6 \times 7\alpha_4$ avec $0 \leqslant \alpha_4 < 5$.

Bibliographie

[1] Vincent Beck, Jérôme Malick et Gabriel Peyré. *Objectif Agrégation*. 2e édition. H&K, 2005.

[2] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy et Éric Schost. *Algorithmes Efficaces en Calcul Formel*. 2017.

[3] Serge Francinou, Hervé Gianella et Serge Nicolas. *Algèbre 1*. Cassini, 2001.

[4] Xavier Gourdon. *Algèbre*. 2e édition. Ellipses, 2009.

[5] Bertrand Hauchecorne et Daniel Suratteau. *Des mathématiciens de A à Z*. Ellipses, 2019.

[6] Pascal Ortiz. *Exercices d'algèbre*. Ellipses, 2004.

[7] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.

[8] Philippe Saux Picart. *Cours de calcul formel. Algorithmes fondamentaux*. Ellipses, 1999.