Compléments d'arithmétique

Leçons concernées (2020)

(120) Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

(121) Nombres premiers. Applications.

(122) Anneaux principaux. Applications.

(123) Corps finis. Applications.

(125) Extensions de corps. Exemples et applications.

(126) Exemples d'équations en arithmétique.

Bibliographie

- Hindry, Arithmétique.
- Naudin, Quitté, Algorithmique algébrique.
- Perrin, Cours d'algèbre.
- Serre, Cours d'arithmétique.

Table des matières

Lorsqu'on se donne $P \in \mathbb{Z}[X_1, \dots, X_d]$, il est naturel de se demander s'il existe des solutions à l'équation $P(x_1, \dots, x_d) = 0$ pour $x = (x_1, \dots, x_d) \in \mathbb{Z}^d$. D'un côté, si on dispose d'une solution dans $\mathbb{Z}^d$, alors on a en particulier une solution dans $\mathbb{R}^d$ et une solution modulo n pour tout $n \in \mathbb{N}^*$ et on peut par exemple se poser la question d'une éventuelle réciproque.

Par des techniques de nature analytique, on peut chercher l'existence ou l'approximation de solutions dans $\mathbb{R}^d$. On peut notamment chercher à borner le domaine d'existence des solutions. Si on sait par exemple que l'ensemble des solutions est borné, contenu dans une boule centrée en 0 de rayon $M \in \mathbb{N}^*$, alors il suffit de raisonner modulo $2M$ pour trouver toutes les solutions. On voit alors qu'une application du Lemme des restes chinois permettra de réduire le problème.

En raisonnant modulo p, pour p premier, on peut chercher des solutions via des techniques de dénombrement ou des méthodes arithmétiques dans les corps finis. Dans certains cas favorables (Lemme de Hensel), une solution modulo p se relève en une solution modulo p^m (ou même dans $\mathbb{Z}_p$). Par le Lemme des restes chinois, une solution modulo p^m pour tout p premier, tout m entier donnera une solution modulo n pour tout n. Cependant, en général, il n'est pas toujours possible de relever une solution modulo n pour tout n en une solution dans $\mathbb{Z}$.

L'enjeu de ce cours est de présenter différentes techniques de résolution d'équations en arithmétiques qui peuvent être réinvesties dans de nombreuses leçons d'agrégation. Certaines d'entre elles sont cependant l'apanage de l'option C et ne seront pas détaillées mais seulement présentées ici.

Dans toute la suite, on désignera par A un anneau commutatif unitaire intègre et K un corps (commutatif) contenant A.

1 Entiers algébriques

De même que pour les polynômes sur un corps, on commence par introduire une notion de clôture intégrale permettant de fournir des domaines d'existence de solutions aux équations diophantiennes.

Définition 1.1. On dit qu'un élément $\alpha \in K$ est entier sur A s'il existe un polynôme unitaire $P \in A[X]$ tel que $P(\alpha) = 0$.

Remarque 1.2. On peut supposer que K est un anneau et non pas un corps dans cette définition et dans une bonne partie de la suite.

Exemple 1.3. L'élément $i \in \mathbb{C}$ est un entier algébrique sur $\mathbb{Z}$ car annulé par le polynôme irréductible unitaire $X^2 + 1 \in \mathbb{Z}[X]$.

Fait 1.4. *On suppose que A est factoriel et que K est algébriquement clos. Si P est un polynôme irréductible unitaire, alors pour toute racine α de P, on a un isomorphisme d'anneaux $A[X]/(P) \simeq A[\alpha]$.*

Démonstration. On a un morphisme d'anneaux surjectif canonique $A[X] \to A[\alpha]$ donné par propriété universelle des anneaux de polynômes via $P \mapsto P(\alpha)$. Soit I son noyau. Par construction $(P) = PA[X] \subset I$. Notons $k = \mathrm{Frac}(A)$ qui est un sous-corps de K. Comme P est unitaire et irréductible sur A, c'est un polynôme primitif irréductible sur A donc irréductible sur $k[X]$. En particulier $P = \mu_{\alpha,k}$ est le polynôme minimal de α sur k. Soit $R \in I$. Alors $R \in k[X]$ annule α, ce qui montre que $R \in Pk[X]$. On écrit $R = rPQ$ avec $r \in k$ et $Q \in A[X]$ primitif. Soit $a \in A$ tel que $ar \in A$. Alors $ac(R) = c(aR) = c(arPQ) = arc(P)c(Q) = ar$. Donc $c(R) = r \in A$. Ce qui montre que $R \in (P) = PA[X]$. Ainsi on a bien $(P) = PA[X] = I$, d'où l'isomorphisme. □

Théorème 1.5. *L'ensemble C des éléments de K qui sont entiers sur A est un sous-anneau de K.*

Démonstration. Soit $\alpha \in K$. On montre d'abord que s'équivalent :

(i) α est entier sur A ;

(ii) $A[\alpha]$ est un A-module de type fini ;

(iii) il existe un sous-anneau B de A contenant α qui est un A-module de type fini.

En effet, on a $(i) \Rightarrow (ii) \Rightarrow (iii)$ par définition. Supposons (iii). Soit f l'endomorphisme du A-module B donné par la multiplication par α. Alors le théorème de Cayley-Hamilton donne un polynôme unitaire qui annule α. D'où $(iii) \Rightarrow (i)$.

Soit $\alpha, \beta \in C$. Alors β est entier sur A et donc sur $A[\alpha]$ par définition. Donc $A[\alpha, \beta] = A[\alpha][\beta]$ est un $A[\alpha]$-module de type fini via $(i) \Rightarrow (ii)$. On en déduit que l'anneau $A[\alpha, \beta]$ est un A-module de type fini car $A[\alpha]$ l'est également et cet anneau contient $\alpha + \beta$ et $\alpha\beta$. Ainsi, par $(iii) \Rightarrow (i)$ on en déduit que $\alpha + \beta \in C$ et $\alpha\beta \in C$. Donc C est bien un sous-anneau de K. □

Définition 1.6. L'anneau C du théorème précédent s'appelle clôture intégrale de A dans K. On dira que A est intégralement clos dans K si $C = A$. Si $K = \mathrm{Frac}(A)$ et $C = A$, on dira plus simplement que A est intégralement clos.

Exercice 1. Un anneau factoriel est intégralement clos.
Indication : on dispose d'un pgcd *donc d'un contenu par exemple.*

Notation 1.7. Si K est une extension finie de $\mathbb{Q}$ (contenue dans $\mathbb{C}$) on notera $\mathcal{O}_K$ la clôture intégrale de $\mathbb{Z}$ dans K.

Exemple 1.8. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ car $\mathbb{Z}$ est factoriel donc intégralement clos.
$\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel mais est intégralement clos.

On verra tout au long de ce cours que certains anneaux d'entiers s'avèrent pratiques pour résoudre certaines équations arithmétiques.

2 Équations modulaires

Dans cette partie, on veut résoudre l'équation

$$P(x) \equiv 0 \mod n$$

pour $P \in \mathbb{Z}[X]$ et $n \in \mathbb{N}^*$. Voici quelques pistes pour aborder ce type de problèmes.

2.1 Relations de Bézout et lemme des restes chinois

On se place dans l'anneau $A = \mathbb{Z}$. La principalité, d'une part, et la factorialité, d'autre part, de cet anneau euclidien permettent de réinterpréter le lemme des restes chinois :

Théorème 2.1 (Restes chinois)**.** *Soit $n \in \mathbb{N}^*$ et $n = \prod_p p^{\alpha_p}$ une décomposition de n en produit de facteurs premiers. Alors on a un isomorphisme canonique d'anneaux :*

$$f : \mathbb{Z}/n\mathbb{N} \to \prod_p \mathbb{Z}/p^{\alpha_p}\mathbb{Z}$$

donné par $f(x \mod n) = (x \mod p^{\alpha_p})_p$.

On ne sait pas donner de formule explicite à l'inverse de f en général mais néanmoins, la principalité donne

Théorème 2.2 (Relations de Bézout)**.** *Soient $a, b \in \mathbb{N}^*$ et $d = \mathrm{pgcd}(a, b)$. Alors il existe des entiers relatifs $u, v \in \mathbb{Z}$ tels que $d = au + bv$.*

De plus, lorsque $d = 1$, l'isomorphisme canonique d'anneaux $f : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ admet la formule explicite suivante pour son inverse :

$$f^{-1}(x \mod a, y \mod b) = bvx + auy \mod ab$$

Démonstration. Le premier point est immédiat car $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ car $\mathbb{Z}$ est principal.

Pour le second point, on observe que

$$x = (au + bv)x = bvx \mod a$$

et que

$$y = (au + bv)y = auy \mod b$$

Par somme,

$$bvx + auy = bvx = x \mod a \qquad\qquad bvx + auy = auy = y \mod b$$

□

On peut alors définir un algorithme explicite (cf. cours d'option C) pour trouver le couple (u, v) en fonction de (a, b) en même temps que $d = \text{pgcd}(a, b)$.

Le principe est le suivant :

On effectue successivement les divions euclidiennes successives :

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ &\vdots \\ r_{n-1} &= r_n q_{n+1} + r_{n+1} \\ &\vdots \\ r_{m-1} &= r_m q_{m+1} + 0 \end{aligned}$$

Alors $d = \text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \cdots = \text{pgcd}(r_{m-1}, r_m) = r_m$.

Pour calculer u, v, on part de $u_0 = 1, u_1 = 0, v_0 = 0, v_1 = 1$ et on pose récursivement $u_n = u_{n-2} - q_n u_{n-1}$ et $v_n = v_{n-2} - q_n v_{n-1}$. On vérifie immédiatement que $au_n + bv_n = r_n$ pour tout n donc en particulier pour $n = m$.

Matriciellement, cela se réécrit également, pour :

$$X_n = \begin{pmatrix} u_{n-2} & v_{n-2} \\ u_{n-1} & v_{n-1} \end{pmatrix} \qquad X_2 = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$X_{n+1} = Q_n X_n \qquad Q_n = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix}$$

Les étudiants en option C savent très bien que le coût est un

$$O(\log \max(|a|, |b|)^3).$$

2.2 Le lemme de Hensel

Le lemme des restes chinois permet de réduire partiellement le problème : au lieu de raisonner modulo un entier n quelconque, on voit que l'équation $P(x) = 0 \mod n$ est équivalente au système d'équations $P(x) = 0 \mod p^{\alpha_p}$.

On se demande alors comment résoudre $P(x) = 0 \mod p^{\alpha_p}$. Cela n'est pas toujours évident mais, lorsque $\alpha_p = 1$, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps et le nombre de solutions est alors majoré par $\max\big(\deg(P), p\big)$. On ne traitera pas ici de la question de la résolution d'une équation polynômiale dans un corps (fini).

On observe qu'une solution modulo p^α donne toujours lieu à une solution modulo p (descente). On cherche alors à remonter les solutions, c'est-à-dire à répondre au problème suivant :

> Étant donné une solution à $P(\overline{x}) = 0 \mod p$, existe-t-il des solutions à $P(x) = 0 \mod p^\alpha$ telles que $\overline{x} = x \mod p$?

On observe que certains polynômes ne se comportent pas bien vis-à-vis de ce problème. Par exemple, le polynôme $P = X^2 - p$ admet une solution modulo p mais pas modulo p^2.

Une réponse partielle mais souvent utile à ce problème est le Lemme de Hensel, qu'on a déjà utilisé et démontré dans le cas particulier des résidus quadratiques. Ceci devrait certainement rappeler des souvenirs aux étudiants en option C :

Lemme 2.3 (Dérivée de Hasse)**.** *Pour $Q = a_d X^d + \cdots + a_0 \in \mathbb{Z}[X]$ et $i \in [\![0, d]\!]$, on définit la i-ème dérivée de Hasse de Q par :*

$$Q^{[i]} = a_d \binom{d}{i} X^{d-i} + \cdots + a_i \binom{i}{i} \in \mathbb{Z}[X]$$

On a alors l'égalité suivante dans $\mathbb{Z}[X, Y]$:

$$Q(X + Y) = Q(X) + YQ^{[1]}(X) + \cdots + Y^d Q^{[d]}(X)$$

où $d = \deg(Q)$.

Démonstration. Ceci est laissé en exercice au lecteur. Celui-ci pourra également observer que dans $\mathbb{Q}[X]$, on a $Q^{[i]}(X) = \frac{Q^{(i)}(X)}{i!}$. □

Proposition 2.4. *Soit P un polynôme dans $\mathbb{Z}[X]$ et $p \in \mathbb{N}$ un nombre premier. On suppose qu'il existe $x \in \mathbb{Z}$ et $\alpha \in \mathbb{N}$ tels que*

$$P(x) = 0 \mod p^\alpha \qquad \text{et} \qquad P'(x) \neq 0 \mod p$$

Alors, il existe un entier $y \in \mathbb{Z}$ tel que

$$P(y) = 0 \mod p^{2\alpha} \qquad \text{et } y = x \mod p^\alpha$$

De plus, cet entier y est alors uniquement déterminé modulo $p^{2\alpha}$ et on peut le choisir sous la forme $y = x - P(x)z$ où $z \in \mathbb{Z}$ vérifie $zP'(x) = 1 \mod p^\alpha$.

Démonstration. On cherche y sous la forme $y = x + tp^\alpha$. Le lemme précédent (ou une formule de Taylor si on justifie correctement) donne alors

$$P(x + tp^\alpha) = P(x) + tp^\alpha P'(x) + t^2 p^{2\alpha} Q(x)$$

pour un certain $Q \in \mathbb{Z}[X]$. Comme $P(x) = 0 \mod p^\alpha$, il existe $s \in \mathbb{Z}$ tel que $P(x) = p^\alpha s$. On a alors $P(x + tp^\alpha) = p^\alpha(s + tP'(x)) \mod p^{2\alpha}$. Comme $P'(x) \neq 0 \mod p$, on sait en particulier que $P'(x)$ est inversible modulo p^α. On note $z = (P'(x))^{-1} \mod p^\alpha$ son inverse. Il suffit de prendre $t = -zs \mod p^\alpha$ pour obtenir l'existence annoncée.

On observe de plus qu'on a trouvé y sous la forme $y = x - zsp^\alpha = x - P(x)z \mod p^{2\alpha}$.

On laisse au lecteur le soin de justifier l'unicité. □

Corollaire 2.5 (Lemme de Hensel – version 1)**.** *Soit P un polynôme dans $\mathbb{Z}[X]$, soit $p \in \mathbb{N}$ un nombre premier et $\alpha \in \mathbb{N}^*$. Toute solution $\overline{x} \in \mathbb{Z}/p^\alpha\mathbb{Z}$ telle que*

$$P(\overline{x}) = 0 \mod p^\alpha \qquad \text{et} \qquad P'(\overline{x}) \neq 0 \mod p$$

se relève de manière unique modulo p^n pour tout $n \geqslant \alpha$. Autrement dit, pour tout $n \geqslant \alpha$, il existe un unique $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ tel que

$$P(x_n) = 0 \mod p^n \qquad \text{et } x_n = \overline{x} \mod p^\alpha$$

Démonstration. Il suffit de définir par récurrence $x_\alpha = \overline{x}$ et pour $n \geqslant \alpha$

$$x_{n+1} = x_n - P(x_n)z \qquad \text{où} \qquad zP'(x_n) = 1 \mod p^n$$

En effet, la formule de Taylor

$$P'(x_n) = P'(\overline{x} + (x_n - \overline{x})) = P'(\overline{x}) + (x_n - \overline{x})Q(\overline{x}) = P'(\overline{x}) \mod p$$

pour un certain $Q \in \mathbb{Z}[X]$ permet de justifier l'inversibilité de $P'(x_n)$ pour tout n. □

Remarque 2.6. Formellement, on recopie ici une méthode de Newton où on part d'un certain x_0 qui n'est « pas trop loin » d'être solution puisque c'est le cas modulo p et on veut poser, comme pour une méthode de Newton classique

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

pour $f = P$ tant que $f'(x_n)$ ne s'annule pas, ce qui est en fait toujours le cas sous ces hypothèse. Le nombre $\varepsilon = p$ est, en topologie p-adique de norme strictement inférieure à 1, ce qui permet d'interpréter la congruence modulo p^n pour $n \to \infty$ comme une certaine convergence. Autrement dit, la suite de terme général p^n converge vers 0 lorsque n tend vers $+\infty$.

Il existe des versions plus générales de ce théorème. Par exemple, par convergence dans l'anneau des entiers p-adiques, une solution modulo p^α pour tout α, relevée de manière « compatible » est en fait un élément de $\mathbb{Z}_p$.

Voici par exemple un énoncé assez général qu'on laisse au lecteur le soin de le réécrire en termes de congruences modulo p^n pour tout n et de le démontrer.

Théorème 2.7 (Lemme de Hensel – variante 2)**.** *Si $P \in \mathbb{Z}_p[X]$ et $k \geqslant 1$ et $\overline{x} \in \mathbb{Z}_p$ sont tels que $P(\overline{x}) \in p^k Q'(\overline{x})^2 \mathbb{Z}_p$, alors il existe un unique $x \in \mathbb{Z}_p$ tel que $P(x) = 0$ et $x - \overline{x} \in p^k P'(\overline{x})\mathbb{Z}_p$.*

On notera que la première condition dit, en particulier, que $P(\overline{x}) = 0 \mod p^k$.

3 Équations diophantiennes linéaires

On a vu une première technique pour s'intéresser à des équations en 1 indéterminée. L'étape suivante est de s'intéresser à plusieurs indéterminer. Commençons par le cas le plus simple de 2 indéterminées et d'un polynôme de degré $d = 1$ (cas linéaire).

Comme souvent, la situation linéaire est simplifiée et permettra de se ramener à des méthodes d'algèbre linéaire et/ou des calculs matriciels.

3.1 Le cas de dimension 1 en 2 variables

Soient $a, b, c \in \mathbb{Z}$. On s'intéresse à l'équation diophantienne

$$ax + by = c$$

c'est-à-dire à l'équation $P(x, y) = 0$ pour $P = aX + bY - c \in \mathbb{Z}[X, Y]$.

La principalité de $\mathbb{Z}$ donne immédiatement une obstruction à l'existence de solutions : pour tous $x, y \in \mathbb{Z}$, $ax + by \in a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$. Si c n'est pas un multiplie du PGCD de a et b, alors il n'y a pas de solutions.

Dans la suite notons $d = \text{pgcd}(a, b)$. On peut alors poser $a_0 = \frac{a}{d}$, $b_0 = \frac{b}{d}$ et $c_0 = \frac{c}{d}$. Cela donne l'équivalence des problèmes

$$ax + by = x \quad \iff \quad a_0x + b_0y = c_0$$

On suppose donc dans la suite, sans restriction, que a et b sont premiers entre eux et on se donne alors une relation de Bézout :

$$au + bv = 1$$

Ainsi, par multiplication par c, on dispose d'une solution évidente

$$(x_0, y_0) = (uc, vc)$$

Soit $(x, y) \in \mathbb{Z}^2$ une autre solution. Par soustraction des équations $ax + by = c$ et $ax_0 + by_0 = c$, on a alors

$$a(x - x_0) + b(y - y_0) = 0$$

Comme a et b sont premiers entre eux, le lemme de Gauss donne

$$a|y - y_0 \qquad \text{et} \qquad b|x - x_0$$

Donc il existe $(k, \ell) \in \mathbb{Z}^2$ tels que

$$x = x_0 + bk \qquad \text{et} \qquad y = y_0 + a\ell$$

Réciproquement, on observe que $(x_0 + bk, y_0 + a\ell)$ est solution si, et seulement si, $\ell = -k$. On a ainsi démontré le :

Théorème 3.1. *Soient $a, b, c \in \mathbb{Z}$ trois entiers non tous nuls et $d = \text{pgcd}(a, b)$. Soit $(\mathcal{E})$ l'équation diophantienne $ax + by = c$. Soit $au + bv = d$ une relation de Bézout.*

Si $d \not| c$ alors $(\mathcal{E})$ n'admet pas de solutions entières.

Si $d|c$, alors $d \neq 0$ et les solutions entières de $(\mathcal{E})$ sont exactement les

$$\left\{(u\frac{c}{d} + k\frac{b}{d}, v\frac{c}{d} - k\frac{a}{d},\ k \in \mathbb{Z}\right\}$$

3.2 Le cas de dimension k en ℓ variables

Matriciellement, on a résolu l'équation diophantienne :

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c \end{pmatrix}$$

Plus généralement, pour $A \in \mathcal{M}_{k,\ell}(\mathbb{Z})$ et $C \in \mathcal{M}_{k,1}(\mathbb{Z})$, on cherche à résoudre

$$AX = C$$

pour $X \in \mathcal{M}_{\ell,1}(\mathbb{Z})$.

Un très mauvais réflexe serait de chercher à résoudre dans $\mathbb{Q}$ puis à chercher à éliminer les dénominateurs communs : on risque alors de « rater » des solutions comme le montre le contre-exemple suivant :

Exemple 3.2. L'espace des solutions sur $\mathbb{Q}$ de

$$2x + 3y + 5z = \begin{pmatrix} 2 & 3 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

est

$$\mathbb{Q}\left(-\frac{3}{2}, 1, 0\right) \oplus \mathbb{Q}\left(-\frac{5}{2}, 0, 1\right)$$

mais l'espace des solutions sur $\mathbb{Z}$ n'est pas

$$\mathbb{Z}\left(-3, 2, 0\right) \oplus \mathbb{Z}\left(-5, 0, 2\right)$$

En effet, l'élément $(0, 5, -3)$ n'est pas dans l'ensemble précédente puisque sa dernière coordonnée est impair alors que c'est effectivement une solution du système diophantien.

Revenons à la résolution de $AX = C$. Supposons qu'on puisse échelonner la matrice A suivant ses colonnes via des opérations élémentaires dans $\mathbb{Z}$, c'est-à-dire trouver $R \in \mathrm{GL}_k(\mathbb{Z})$ telle que $B = AR \in \mathcal{M}_{k,\ell}(\mathbb{Z})$ est échelonnée. Il devient alors facile de résoudre $BY = C$ comme suit :

> Supposons que B ait r colonnes $B_1, \ldots, B_r$ non nulles. Alors, grâce à l'échelonnement, on peut facilement vérifier s'il existe des entiers $u_1, \ldots, u_r$ (forcément uniques) tels que $C = u_1 B_1 + \cdots + u_r B_r$.* Si cette condition nécessaire et suffisante pour l'existence de solutions entières du système est remplie, alors les solutions entières du système $BY = C$ sont les $(u_1, \ldots, u_r, v_{r+1}, \ldots, v_\ell)$ pour $v_{r+1}, \ldots, v_\ell \in \mathbb{Z}$ quelconques.

On résout ainsi $AX = C$ en posant $X = RY$.

Exemple 3.3 (Le cas $k = 1$ et $\ell = 2$). Ce cas a fait l'objet de la section précédente. Voyons comment échelonner en colonnes la matrice $A = \begin{pmatrix} a & b \end{pmatrix}$. Si $au + bv = d = \mathrm{pgcd}(a, b)$ est une relation de Bézout, alors on observe en posant $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ qu'on a l'égalité matricielle :

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} u & -b' \\ v & a' \end{pmatrix} = \begin{pmatrix} d & 0 \end{pmatrix}$$

Cela donne un échelonnement suivant les colonnes de $A = \begin{pmatrix} a & b \end{pmatrix}$ en $B = \begin{pmatrix} d & 0 \end{pmatrix}$ via la matrice $R = \begin{pmatrix} u & -b' \\ v & a' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

L'équation $BY = c'd = c$ se résout très bien en $Y = \begin{pmatrix} c' \\ k \end{pmatrix}$ pour $k \in \mathbb{Z}$ quelconque. On retrouve alors les solutions

$$X = RY = \begin{pmatrix} u & -b' \\ v & a' \end{pmatrix} \begin{pmatrix} c' \\ k \end{pmatrix} = \begin{pmatrix} uc' - b'k \\ vc' + a'k \end{pmatrix}$$

de la section précédente.

3.3 Forme normale de Hermite et de Smith d'une matrice

On rappelle (voir cours d'algèbre linéaire de début d'année) la définition suivante :

Définition 3.4. Soit $A = (a_{i,j}) \in \mathcal{M}_{k,\ell}(\mathbb{Z})$ une matrice échelonnée suivant les lignes. Soit r le nombre de lignes non nulles de A et soit $p(i)$ (appelé pivot) tel que $a_{i,p(i)}$ est le premier coefficient non nul sur la i-ème ligne.

On dit que la matrice échelonnée A est *réduite* suivant les lignes si pour tout $i \in llbracket 1, r\rrbracket$ on a $a_{i,p(i)} > 0$ et $0 \leqslant a_{k,p(i)} < a_{i,p(i)}$ pour tout $k \in [\![1, i-1]\!]$.

Exercice 2. Donner une définition analogue pour les matrices échelonnées suivant les colonnes.

Pour échelonner une matrice à coefficients entiers suivant les colonnes, on utilise alors le théorème suivant :

Théorème 3.5 (Forme normale de Hermite)**.** *Soit $A \in \mathcal{M}_{k,\ell}(\mathbb{Z})$. Alors il existe une unique matrice $B \in \mathcal{M}_{k,\ell}(\mathbb{Z})$ échelonnée réduite suivant les lignes telle qu'il existe $L \in \mathrm{GL}_k(\mathbb{Z})$ satisfaisant $B = LA$.*

La matrice B ainsi obtenue est appelée la forme normale de Hermite *de A.*

∗. Ceci revient à dire que C appartient au $\mathbb{Z}$-module de A dont $(B_1, \ldots, B_r)$ est une base.

Esquisse de preuve. L'existence est en fait constructive : on commence par échelonner la matrice A pour obtenir B. On peut supposer que le premier coefficient non nul $b_{i,p(i)}$ de chaque ligne non nulle de B est positif, quitte à multiplier cette ligne par -1. On peut ensuite faire $0 \leqslant b_{k,p(i)} < b_{i,p(i)}$ pour $k < i$ en soustrayant à la k-ème ligne la i-ème multipliée par le quotient de la division euclidienne de $b_{k,p(i)}$ par $b_{i,p(i)}$; on le fait dans l'ordre pour $i = 1, 2, \ldots$ (de gauche à droite).

Supposons qu'on ait deux formes normales de Hermite B et B' pour une même matrice A. Les lignes non nulles de B et B' sont deux bases du même sous-module de $\mathbb{Z}^\ell$ de rang r. Notons ces lignes $B_1, \ldots, B_r$ et $B'_1, \ldots, B'_r$ respectivement. Par la condition d'échelonnement pour B et B', on a $B'_i = \sum_{\ell=i}^{r} \lambda_{i,\ell} B_\ell$ avec $\lambda_{i,i} \in \{\pm 1\}$. Le fait que B et B' sont réduites impose d'abord $\lambda_{i,i} = 1$ puis $\lambda_{i,\ell} = 0$ pour $\ell \in [\![i+1, r]\!]$. □

Remarque 3.6. Attention : le théorème statue l'unicité de la forme normale de Hermite mais pas de la matrice de transformation L.

Exercice 3. Proposer et démontrer un théorème analogue pour l'échelonnement suivant les colonnes d'une matrice.

Exercice 4. Soient $A, B \in \mathcal{M}_{k,\ell}(\mathbb{Z})$ deux matrices. Montrer que s'équivalent :

(i) il existe $L \in \mathrm{GL}_k(\mathbb{Z})$ telle que $B = LA$;

(ii) les lignes de A engendrent le même sous-$\mathbb{Z}$-module de $\mathbb{Z}^\ell$ que les lignes de B ;

(iii) les matrices A et B ont même forme normale de Hermite.

Bien que ceci ne soit pas utile dans la résolution de systèmes linéaires d'équations diophantiennes, indiquons tout de même l'existence de la forme normale de Smith, qui s'avère essentielle pour manipuler les $\mathbb{Z}$-modules de type fini.

Théorème 3.7 (Forme normale de Smith)**.** *Soit $A \in \mathcal{M}_{k,\ell}(\mathbb{Z})$. Il existe une matrice diagonale $B = \mathcal{M}_{k,\ell}(\mathbb{Z})$ dont les coefficients diagonaux $b_1, \ldots, b_r$ pour $r = \min(k, \ell)$ sont positifs ou nuls et vérifient $b_i | b_{i+1}$ pour tout $i \in [\![1, r-1]\!]$ et deux matrices inversibles $L \in \mathrm{GL}_k(\mathbb{Z})$ et $R \in \mathrm{GL}_\ell(\mathbb{Z})$ telles que $B = LAR$.*

De plus la matrice B vérifiant ces conditions est uniquement déterminée. On l'appelle la forme normale de Smith *de A.*

Remarque 3.8. Encore une fois, on prendra garde que les matrices L et R ne sont pas uniquement déterminées.

Contrairement à la forme normale de Hermite, il est possible de généraliser ce résultat à tout anneau principal comme vous l'aviez vu l'année dernière en M1.

4 Le problème des d carrés

On se pose le problème suivant :

> Étant donné un entier $d > 1$, à quelle(s) condition(s) un entier $n \in \mathbb{Z}$ s'écrit-il comme somme de d carrés ?

Les carrés entiers – donc réels – étant positifs, une condition nécessaire immédiate est $n \geqslant 0$. Est-elle suffisante ? Si $d = 2$, en raisonnant modulo 4 on observe qu'une somme de deux carrés est nécessairement congrue à 0, 1 ou 2 modulo 4.

4.1 L'anneau des entiers de Gauss

On appelle anneau des entiers de Gauss l'anneau $\mathbb{Z}[i]$.

Pour $z = a + ib \in \mathbb{Z}[i]$, on définit :

1. son conjugué $\overline{z} = a - ib$;
2. sa trace $\mathrm{Tr}(z) = \overline{z} + z = 2a$;
3. sa norme $\overline{z}z = a^2 + b^2$.

On observe en particulier que z est solution de l'équation entière $X^2 - \mathrm{Tr}(z)X + N(z)$.

L'application trace est $\mathbb{Z}$-linéaire et l'application norme est multiplicative.

4.2 Propriétés de l'anneau

Fait 4.1. *L'anneau $\mathbb{Z}[i]$ est intègre comme sous-anneau de $\mathbb{C}$.*

Proposition 4.2. *L'application norme définit un stathme euclidien qui fait de $\mathbb{Z}[i]$ un anneau euclidien.*

Démonstration. Tout d'abord, on constate que $N(\mathbb{Z}[i]) \subset \mathbb{N}$. Établissons l'existence d'une division euclidienne.

Si $x, y \in \mathbb{Z}[i]$, alors il existe des réels $\alpha, \beta \in \mathbb{R}$ tels que $\frac{x}{y} = \alpha + i\beta$. Il existe alors des entiers $a, b \in \mathbb{Z}$ tels que $|\alpha - a| < \frac{1}{2}$ et $|\beta - b| < \frac{1}{2}$. On pose $q = a + ib \in \mathbb{Z}[i]$ et $r = x - qy$. On a alors $\frac{N(r)}{N(y)} = \frac{|x-qy|^2}{|y|^2} = \left|\frac{x}{y} - q\right|^2 \leqslant |\alpha - a|^2 + |\beta - b|^2 < \frac{1}{2}$. En particulier, on a $N(r) = 0$ ou $N(r) < N(y)$, ce qui montre que N est bien un stathme. □

Remarque 4.3. Ici, on observe, en particulier, qu'il n'y a pas toujours unicité de la division euclidienne contrairement au cas $\mathbb{Z}$ ou $K[X]$.

Exercice 5. Effectuer une division euclidienne de $3-3i$ par 2. Quels sont les différents quotients et restes possibles ?

4.3 Éléments irréductibles

Avant de déterminer les éléments irréductibles de $\mathbb{Z}[i]$, il est utile de donner la liste de ses inversibles.

Fait 4.4. *On a $\mathbb{Z}[i]^\times = \{x \in \mathbb{Z}[i],\ N(x) = 1\} = \{\pm 1, \pm i\}$.*

Démonstration. Si $x \in \mathbb{Z}[i]$ est inversible, alors il existe $y \in \mathbb{Z}[i]$ tel que $xy = 1$. Comme la norme est multiplicative, on a $N(x)N(y) = 1$ dans $\mathbb{Z}$. Ceci impose que $N(x) \in \mathbb{Z}^\times \cap \mathbb{N} = \{1\}$. Donc $x = a + ib$ avec $a^2 + b^2 = 1$. Cette équation impose $a = \pm 1$ et $b = 0$ ou $a = 0$ et $b = \pm 1$ dans $\mathbb{Z}$ par un argument élémentaire de comparaison.

Réciproquement, on constate que les éléments ± 1 et $\pm i$ sont inversibles dans $\mathbb{Z}[i]$. □

Lemme 4.5. *Tout élément irréductible de $\mathbb{Z}[i]$ divise dans $\mathbb{Z}[i]$ un élément irréductible de $\mathbb{Z}$ (i.e. un nombre premier).*

Démonstration. Soit $x \in \mathbb{Z}[i]$ irréductible. Alors $\overline{x}$ est également irréductible car sinon x ne le serait pas en appliquant la conjugaison. Soit $p \in \mathbb{Z}$ premier divisant $a = N(x) = x\overline{x}$. Comme $\mathbb{Z}[i]$ est factoriel, on sait que $x|p$ ou $\overline{x}|p$ dans $\mathbb{Z}[i]$. Dans le premier cas, on a obtenu le résultat souhaité. On se ramène du second cas au premier par conjugaison. □

Lemme 4.6. *Si un nombre premier $p \in \mathbb{Z}$ est réductible dans $\mathbb{Z}[i]$, alors c'est le produit de deux irréductibles conjugués l'un de l'autre. De plus, ces irréductibles sont associés si, et seulement si, $p = 2$.*

Démonstration. On écrit $p = xy$ avec $N(x) \neq 1$ et $N(y) \neq 1$. Alors $N(p) = p^2 = N(x)N(y)$ donne $p = N(x) = N(y) = x\overline{x}$. D'où $y = \overline{x}$.

Écrivons $x = uv$ avec $u, v \in \mathbb{Z}[i]$. Alors $N(x) = p = N(u)N(v)$ est une égalité dans $\mathbb{Z}$. Donc $N(u) = 1$ ou $N(v) = 1$ par factorialité de $\mathbb{Z}$. Ceci montre que u ou v est inversible dans $\mathbb{Z}[i]$ et donc que x et $\overline{x}$ sont irréductibles.

Enfin, si $\overline{x} \in \mathbb{Z}[i]^\times \cdot x$, alors les cas $\overline{x} = \pm x$ sont exclus car $p = \pm x^2$ ne pourrait pas être un nombre premier. Si $\overline{x} = ix$, écrivons $x = a + ib$ et $\overline{x} = a - ib = ia - b$. On en déduit que $b = -a$ et $x = a(-1 + i)$. Donc $N(x) = p = 2N(a)$ est premier donne $N(a) = 1$ et $p = 2$. Il en est de même pour $\overline{x} = -ix$. □

Proposition 4.7. *À inversibles près, les irréductibles de $\mathbb{Z}[i]$ sont :*

$$\{1 + i\} \sqcup \{p \text{ premier},\ p \equiv 3 \mod 4\} \sqcup \{a + ib,\ p = a^2 + b^2 \text{ est premier et } p \equiv 1 \mod 4\}.$$

Démonstration. Soit $x = a + ib$ irréductible et $p \in \mathbb{Z}$ premier tel que $a + ib$ divise p dans $\mathbb{Z}[i]$.

Si p est irréductible dans $\mathbb{Z}[i]$, alors $a + ib = p$.

Sinon, $p = x\overline{x} = a^2 + b^2$ est somme de deux carrés. Donc $p \equiv 1$ ou $2 \mod 4$. Si $p \equiv 1 \mod 4$, montrons que p est réductible dans $\mathbb{Z}[i]$. Par double quotient, cela revient à montrer que $X^2 + 1$ est

réductible dans $\mathbb{F}_p$. Or

$$\begin{aligned} -1 \text{ est un carré dans } \mathbb{F}_p &\Leftrightarrow (-1) \in \operatorname{im} \begin{pmatrix} \mathbb{F}_p^\times & \to & \mathbb{F}_p^\times \\ x & \mapsto & x^2 \end{pmatrix} \\ &\Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \\ &\Leftrightarrow \frac{p-1}{2} \equiv 0 \mod 2 \\ &\Leftrightarrow p \equiv 1 \mod 4 \end{aligned}$$

Enfin, on conclut en observant que 2 est le seul nombre premier pair. □

4.4 Le théorème des 2 carrés

Théorème 4.8. *Un nombre entier positif $n \in \mathbb{N}$ est somme de deux carrés si, et seulement si, $v_p(n)$ est pair pour tout nombre premier $p \equiv 3 \mod 4$.*

Démonstration. Notons $\Sigma = N(\mathbb{Z}[i])$ l'ensemble des sommes de deux carrés d'entiers. Il est clair que Σ est stable par multiplication.

De plus, on a vu que $2 = 1^2 + 1^2 = N(1+i)$ et les nombres premiers $p \equiv 1 \mod 4$ sont des sommes de 2 carrés. Si pour tout $p \equiv 3 \mod 4$, on a $v_p(n)$ pair, alors on sait par multiplicativité de Σ que n est somme de deux carrés.

Réciproquement, supposons $n \in \Sigma$ et p premier tel que $p \equiv 3 \mod 4$. On a vu que p est alors irréductible dans l'anneau $\mathbb{Z}[i]$. On écrit $n = a^2 + b^2$ avec $a, b \in \mathbb{Z}$. Notons respectivement α et β les valuations p-adiques dans $\mathbb{Z}[i]$ de $a+ib$ et $a-ib$, ce qui est loisible puisque $\mathbb{Z}[i]$ est factoriel. La division $p^\alpha | a+ib$ donne alors $N(p^\alpha) = p^{2\alpha} | N(a+ib) = a^2+b^2 = n$. De même $p^{2\beta} | N(a-ib) = n$. Donc la valuation p-adique de n dans $\mathbb{Z}[i]$ est $\alpha + \beta \geqslant \max(2\alpha, 2\beta)$. Ce qui donne $\alpha = \beta$ et donc $\alpha + \beta$ est pair. □

4.5 Le théorème des 4 carrés

Si on augmente la quantités de carrés à prendre en compte, il est claire que les conditions suffisantes à une écriture en somme de d carrés est encore suffisante pour une écriture en somme de $d+1$ carrés puisque $0 = 0^2$ est un carré dans $\mathbb{Z}$. Le théorème suivant montre que le problème est en fait trivialisé dès la situation $d = 4$.

Théorème 4.9. *Tout entier positif $n \in \mathbb{N}$ s'écrit comme somme de 4 carrés $n = a^2 + b^2 + c^2 + d^2$ pour $a, b, c, d \in \mathbb{Z}$.*

Pour démontrer ce résultat, on introduit cette fois la $\mathbb{R}$-algèbre (non-commutative) des quaternions

$$\mathbb{H} = \left\{ \begin{pmatrix} u & -v \\ \overline{v} & \overline{u} \end{pmatrix} \in \mathcal{M}_2(\mathbb{C}),\ u, v \in \mathbb{C} \right\}$$

dont une $\mathbb{R}$ base est donnée par

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

On observe les relations $I^2 = J^2 = K^2 = -\mathbf{1}$ et $IJ = K$, $JK = I$, $KI = J$.

On appelle *quaternions purs* les éléments du sous-espace vectoriel de dimension 3, noté $\mathbb{H}_0$, engendré par I, J et K.

Si $z = a\mathbf{1} + w$ avec $a \in \mathbb{R}$ et $w = bI + cJ + dK \in \mathbb{H}_0$, on définit :

— son conjugué par $\overline{z} = a\mathbf{1} - w = a\mathbf{1} - bI - cJ - dK$;

— sa trace par $\operatorname{Tr}(z) = z + \overline{z} = 2a\mathbf{1}$;

— sa norme par $N(z) = z\overline{z} = (a^2 + b^2 + c^2 + d^2)\mathbf{1}$.

On observe en particulier que $\overline{z}z = N(z) = z\overline{z}$, que $N(z_1 z_2) = N(z_1)N(z_2)$ et que z est une racine dans $\mathbb{H}$ du polynôme $X^2 - \operatorname{Tr}(z)X + N(z) \in \mathbb{R}[X]$.

On définit $A_0 = \mathbb{Z}\mathbf{1} + \mathbb{Z}I + \mathbb{Z}J + \mathbb{Z}K$. On observe que A_0 est une sous-$\mathbb{Z}$-algèbre (non-commutative) de $\mathbb{H}$ et que l'ensemble $\mathcal{S}$ des sommes de 4 carrés entiers est exactement $\mathcal{S} = N(A_0)$.

Il est également commode d'introduire l'élément suivant $L = \frac{\mathbf{1}+I+J+K}{2}$.

Lemme 4.10. *L'ensemble $A = A_0 + \mathbb{Z}L$ est une sous-$\mathbb{Z}$-algèbre de $\mathbb{H}$.*

Démonstration. L'ensemble A est clairement stable par somme. L'ensemble A est stable par multiplication par les éléments $\mathbf{1}$, I, J, K. Enfin $\mathrm{Tr}(L) = 1$ et $N(L) = 1$ donnent $L^2 - L + 1 = 0$ donc A est stable par multiplication par L. □

Proposition 4.11. *On a $\mathcal{S} = N(A) = N(A_0)$.*

Démonstration. L'inclusion $N(A_0) \subset N(A)$ est claire. Pour $\alpha = \frac{a\mathbf{1}+bI+cJ+dK}{2} \in A$ avec $a, b, c, d \in \mathbb{Z}$, les entiers a, b, c, d sont de même parité. S'ils sont pairs, on a $\alpha \in A_0$. Sinon, il existe des nombres $\varepsilon_a, \varepsilon_b, \varepsilon_c, \varepsilon_d \in \{\pm 1\}$ et $a', b', c', d' \in \mathbb{Z}$ tels que $a = 4a' + \varepsilon_a$, $b = 4b' + \varepsilon_b$, $c = 4c' + \varepsilon_c$, $d = 4d' + \varepsilon_d$. On pose $\varepsilon = \frac{\varepsilon_a \mathbf{1} - \varepsilon_b I - \varepsilon_c J - \varepsilon_d K}{2} \in A$. Alors $N(\varepsilon) = 1$ donc $N(\alpha) = N(\alpha\varepsilon)$. De plus, $\alpha\varepsilon = 4\frac{a'\mathbf{1}+b'I+c'J+d'K}{2}\varepsilon + N(\varepsilon) = (a'\mathbf{1} + b'I + c'J + d'K)(2\varepsilon) + \mathbf{1} \in A_0$. D'où $N(\alpha) = N(\alpha\varepsilon) \in N(A)$. Ainsi $N(A) = N(A_0) = \mathcal{S}$. □

Démontrons à présent le théorème des 4 carrés.

Démonstration. De l'observation $N(z_1 z_2) = N(z_1)N(z_2)$ on tire qu'il suffit de démontrer que tout nombre premier p est somme de 4 carrés. C'est vrai si $p = 2$ et on suppose désormais que $p \geqslant 3$ est premier donc, en particulier, impair.

Le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$ est $\frac{p+1}{2}$ donc le polynôme $-1 - X^2$ prend au moins une fois pour valeur un carré modulo p. Autrement dit, il existe $a, b \in \mathbb{Z}$ tels que $1 + a^2 + b^2 \in p\mathbb{Z}$. Ainsi $(\mathbf{1} + aI + bJ)(\mathbf{1} - aI - bJ) \in p\mathbb{Z}\mathbf{1}$. Considérons l'idéal à gauche $\mathcal{I}$ de A engendré par p et $\mathbf{1} + aI + bJ$. Avec une technique analogue à celle utilisée pour l'anneau des entiers de Gauss, on définit un stathme sur A et on en déduit que l'idéal à gauche $\mathcal{I}$ est principal, engendré par un élément $\beta \in A$ de sorte que $\mathcal{I} = A\beta$. D'autre part, on observe que $pA = Ap \subset \mathcal{I} \subset A$. Ainsi, il existe $\alpha \in A$ tel que $p\mathbf{1} = \alpha\beta$. Donc $p^2 = N(p\mathbf{1}) = N(\alpha)N(\beta)$.

Montrons que α et β ne sont pas inversibles.

Si α était inversible, alors p diviserait $\mathbf{1} + aI + bJ$. Autrement dit, il existerait des entiers $a', b', c', d' \in \mathbb{Z}$ tels que $\mathbf{1} + aI + bJ = p\frac{a'\mathbf{1}+b'I+c'J+d'K}{2}$. En particulier, comme $\mathbf{1}, I, J, K$ est une $\mathbb{R}$-base, on a $\frac{p}{2} = 1$ ce qui contredit p impair. Ainsi α est inversible.

Si β était inversible, on aurait $\mathcal{I} = A$ donc $\mathbf{1} = z_1(\mathbf{1} + aI + bJ) + z_2 p \in \mathcal{I}$. En multipliant à droite par $\overline{\mathbf{1} + aI + bJ} = \mathbf{1} - aI - bJ$, on en déduit que $\mathbf{1} - aI - bJ \in Ap$, ce qui est absurde par le même raisonnement que précédemment.

Ainsi, on en déduit que $N(\alpha) \neq 1$ et $N(\beta) \neq 1$ donc $N(\alpha) = N(\beta) = p$ dans $\mathbb{Z}$ factoriel. En particulier, $N(\alpha) = p$ est une somme de quatre carrés. □

Corollaire 4.12. *Il existe une équation diophantienne qui admet une solution modulo n pour tout entier $n \in \mathbb{N}^*$ mais qui n'admet pas de solution dans $\mathbb{Z}$.*

Démonstration. Considérons $P = X_1^2 + X_2^2 + X_3^2 + X_4^2 + 1$. Alors $P(a, b, c, d) = 0 \iff a^2 + b^2 + c^2 + d^2 = -1$ n'a pas de solutions dans $\mathbb{Z}$ pour des raisons de signe. Mais $P(a, b, c, d) = 0 \mod n \iff a^2 + b^2 + c^2 + d^2 = n - 1 \mod n$ admet une solution dans $\mathbb{Z}/n\mathbb{Z}$ puisque $n - 1$ est somme de quatre carrés d'après le théorème précédent. □

4.6 Sommes de 3 carrés

La situation intermédiaire est celle des sommes de 3 carrés. Celle-ci utilise des techniques beaucoup plus avancées et nous nous contenterons d'observer ici le résultat suivant :

Théorème 4.13 (Admis !)**.** *Un entier n s'écrit comme somme de 3 carrés si, et seulement si, il n'est pas de la forme $n = 4^a(8m + 7)$ avec $m, a \in \mathbb{N}$.*

Pour une preuve complète du théorème, le lecteur qui s'ennuie pourra consulter le *Cours d'arithmétique* de Serre.

Remarque 4.14. On observera que l'énoncé laisse d'emblée penser que le résultat est plus technique puisque contrairement aux sommes de 2 carrés et 4 carrés, l'ensemble des sommes de 3 carrés n'est pas stable par multiplication.