Sous la direction de Jean-Pierre Ramis et André Warusfel
Xavier Buff · Josselin Garnier · François Moulin · Monique Ramis · Jacques Sauloy

# Mathématiques

## Tout-en-un pour la Licence 3

3e édition

DUNOD

**Jean-Pierre Ramis**, ancien élève de l'École Normale Supérieure de la rue d'Ulm, membre de l'Institut (Académie des Sciences), membre de l'Institut Universitaire de France, membre de l'Académie des Sciences, Inscriptions et Belles-Lettres de Toulouse, professeur émérite à l'Institut de Mathématique de Toulouse (Université Paul Sabatier), a été directeur de l'Institut de Recherches Mathématiques Avancées de Strasbourg et de l'Institut de Mathématiques de Toulouse.

**André Warusfel**, ancien élève de l'École Normale Supérieure de la rue d'Ulm, a été professeur de mathématiques spéciales au Lycée Louis-le-Grand à Paris et inspecteur général de Mathématiques.

**Xavier Buff**, ancien élève de l'École Normale Supérieure de la rue d'Ulm, professeur à l'Institut de Mathématiques de Toulouse, ancien directeur de l'Institut de Recherches sur l'Enseignement des Mathématiques de Toulouse.

**Josselin Garnier**, ancien élève de l'École normale supérieure de la rue d'Ulm, professeur à l'Uni-versité Paris Diderot, Laboratoire de Probabilités et Modèles Aléatoires & Laboratoire Jacques-Louis Lions.

**François Moulin**, ancien élève de l'École Normale Supérieure de la rue d'Ulm, professeur de chaires supérieures au Lycée sainte-Geneviève (spéciales MP*).

**Monique Ramis**, ancienne élève de l'École Normale Supérieure de Sèvres, a été professeur de chaires supérieures (à Paris, Strasbourg, Toulouse).

**Jacques Sauloy**, ancien élève de l'École Normale Supérieure de Saint-Cloud, maître de conférences à l'Institut de Mathématiques de Toulouse.

Les éditions Dunod remercient Jean-Marie Monier, professeur de mathématiques en classes préparatoires au lycée La Martinière-Monplaisir (Lyon), pour sa relecture attentive de l'ouvrage.

Création graphique et couverture : Elizabeth Riba


11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-087704-1

# Préface

Les mathématiques constituent l'ossature de la science moderne et sont une source intarissable de concepts nouveaux d'une efficacité incroyable pour la compréhension de la réalité matérielle qui nous entoure. Ainsi l'apprentissage des mathématiques est devenu indispensable pour la compréhension du monde par la science. Les nouveaux concepts eux-mêmes sont le résultat d'un long processus de distillation dans l'alambic de la pensée. Essayer de justifier les mathématiques par leurs applications pratiques n'a guère de sens, tant ce processus de création est sous-tendu par la soif de connaître et non l'intérêt immédiat.

Les mathématiques restent l'un des domaines dans lequel la France excelle et ceci malgré la mutilation des programmes dans le secondaire et l'influence néfaste d'un pédagogisme dont l'effet principal est de compliquer les choses simples.

Vues de loin les mathématiques apparaissent comme la réunion de sujets distincts comme la géométrie, qui a pour objet la compréhension du concept d'espace, l'algèbre, art de manipuler les symboles, l'analyse, science de l'infini et du continu, la théorie des nombres etc. Cette division ne rend pas justice à l'un des traits essentiels des mathématiques qui est leur unité profonde de sorte qu'il est impossible d'en isoler une partie sans la priver de son essence. En ce sens les mathématiques ressemblent à un être biologique qui ne peut survivre que comme un tout et serait condamné à périr si on le découpait en morceaux en oubliant son unité fondamentale.

L'une des caractéristiques de l'apprentissage des mathématiques, c'est la possibilité donnée à tout étudiant de devenir son propre maître et en ce sens il n'y a pas d'autorité en mathématiques. Seules la preuve et la rigueur y font la loi. L'étudiant peut atteindre par le travail une maîtrise suffisante pour pouvoir s'il le faut tenir tête au maître. La rigueur, c'est être sûr de soi, et à l'âge où l'on construit sa personnalité, se confronter au monde mathématique est le moyen le plus sûr de construire sur un terrain solide. Il faut, si l'on veut avancer, respecter un équilibre entre les connaissances qui sont indispensables et le « savoir-faire » qui l'est autant. On apprend les maths en faisant des exercices, en apprenant à calculer sans l'aide de l'ordinateur, en se posant des questions et en ne lâchant pas prise facilement devant la difficulté. Seule la confrontation réelle à la difficulté a une valeur formatrice, en rupture avec ce pédagogisme qui complique les choses simples et mélange l'abstraction mathématique avec le jeu qui n'a vraiment rien à voir. Non, les mathématiques ne sont pas un jeu et l'on n'apprend pas les mathématiques en s'amusant.

L'ouvrage qui suit est un cours soigné et complet idéal pour apprendre toutes les Mathématiques qui sont indispensables au niveau de la Licence. Il regorge d'exercices (350) qui

incitent le lecteur à réfléchir et ne sont pas de simples applications de recettes, et respecte parfaitement l'équilibre nécessaire entre connaissances et savoir-faire, permettant à l'étudiant de construire des images mentales allant bien au-delà de simples connaissances mémorisées. Il s'agit d'un ouvrage de référence pour la Licence, non seulement pour les étudiants en mathématiques mais aussi pour tous ceux qui s'orientent vers d'autres disciplines scientifiques. Il insiste sur la rigueur et la précision et va au fond des notions fondamentales les plus importantes sans mollir devant la difficulté et en respectant constamment l'unité des mathématiques qui interdit tout cloisonnement artificiel. Il répond à une demande de tant de nos collègues d'un ouvrage qui les aide à « redresser la barre », mais sera aussi un atout merveilleux pour l'étudiant travaillant seul par la cohérence et la richesse de son contenu.
Il est l'œuvre d'une équipe qui rassemble des mathématiciens de tout premier plan ayant une véritable passion pour l'enseignement. Il était grand temps !

Alain Connes,
Médaille Fields 1982,
Professeur au Collège de France.

# *Monique*

*Notre collègue et amie, Monique Ramis, l'épouse de Jean-Pierre,*
*nous a quittés le 3 février 2024, après une terrible maladie.*

*Monique avait une passion pour l'enseignement des mathématiques.*
*Elle a enseigné en classes préparatoires à Paris, Strasbourg et Toulouse,*
*et aussi quelques années aux Universités de Tunis et Strasbourg.*
*Elle a formé avec exigence de nombreuses générations d'étudiants.*
*Elle était très attachée à leur réussite. Élevée dans un milieu très modeste,*
*elle devait beaucoup au lycée de la République. Elle avait particulièrement admiré*
*son professeur de mathématiques spéciales au Lycée Fénelon, à Paris,*
*Marie-Odette Dubois-Violette. Le goût de Monique pour les mathématiques*
*devait beaucoup à l'enseignement de Marie-Odette,*
*mais aussi à la lecture des livres d'Edmond Ramis.*
*L'exemple de Mme Dubois-Violette a été crucial pour le choix de carrière*
*de Monique et sa volonté de transmettre le savoir.*

*Monique avait dès le début adhéré avec enthousiasme au projet*
*d'André Warusfel d'écrire une variante de la « série E. Ramis »*
*pour les étudiants des premières années de l'enseignement supérieur.*
*Elle y voyait en particulier un moyen de transmettre*
*sa grande expérience de l'enseignement des mathématiques.*
*Les rédactions des modules dont elle avait la charge sont remarquables.*
*Elle s'intéressait aussi au travail de chacun*
*et nous avons souvent bénéficié de ses remarques.*

*Après plusieurs rééditions et restructurations,*
*notre série de livres a maintenant atteint une forme « définitive ».*
*C'est pour nous une grande satisfaction, mais avec un fond de tristesse,*
*car quatre des membres de l'équipe initiale nous ont quittés.*

# Table des matières

# IV Probabilités

# Avant-propos

Cet ouvrage est le dernier d'une série de trois, conçue pour couvrir les programmes de mathématiques de la plupart des Licences scientifiques.
Il complète le précédent en traitant certains sujets habituellement enseignés au niveau de la deuxième année de Licence et couvre par ailleurs un « tronc commun » des programmes de mathématiques au niveau de la troisième année.

Ce cours est illustré d'exemples et applications, il propose de plus au fil du texte de nombreux exercices corrigés qui permettront à l'étudiant de s'entraîner au fur et à mesure de son apprentissage, des notices historiques et un index très complet. On trouvera aussi à la fin de chaque module des exercices supplémentaires[1] avec des indications de solutions. Une correction détaillée d'une grande partie de ces exercices est accessible sur le site de l'éditeur.

Nos livres sont conçus comme une aide à l'enseignement oral dispensé par nos collègues dans les cours et travaux dirigés. L'ordre de lecture n'est pas complètement imposé et chaque étudiant peut se concentrer sur tel ou tel aspect en fonction de son programme et de son travail personnel.
Ce livre peut aussi être utilisé par un enseignant comme ouvrage de base pour son cours, dans l'esprit d'une pédagogie encore peu utilisée en France, mais qui a largement fait ses preuves ailleurs. Nous avons aussi pensé à l'étudiant travaillant seul, sans appui d'un corps professoral.

Dans les mathématiques d'aujourd'hui, un certain nombre de théories puissantes sont au premier plan. Leur maniement, au moins à un certain niveau dépendant de la filière choisie, devra évidemment être acquis par l'étudiant à la fin de ses années de Licence. Mais celui-ci devra aussi avoir appris à calculer, sans s'appuyer exagérément sur les ordinateurs et les logiciels, et à savoir « se débrouiller » devant un problème abstrait ou issu des applications. Nous avons, à cette fin, mis en place une approche adaptée. Nous insistons aussi sur les exigences de rigueur (définitions précises, démonstrations rigoureuses), mais les choses sont mises en place de façon progressive et pragmatique, et nous proposons des exemples riches, dont l'étude met souvent en œuvre des approches multiples. Nous aidons progressivement le lecteur à acquérir le maniement d'un outillage abstrait puissant, sans jamais nous complaire dans l'abstraction pour elle-même, ni un formalisme sec et gratuit : le cœur des mathématiques n'est sans doute pas un corpus de théories, si profondes et efficaces soient-elles, mais

[1] Les plus difficiles sont marqués d'une ou deux étoiles.

un certain nombre de problèmes dans toute leur complexité, souvent issus d'une réflexion sur le monde qui nous entoure.

Historiquement, les mathématiques se sont développées pendant des siècles en relation avec les autres sciences. De nos jours, leurs interactions se poursuivent vigoureusement (avec la physique, l'informatique, la mécanique, la chimie, la biologie, l'économie...). Nous souhaitons accompagner ce mouvement au niveau de l'enseignement des premières années d'université et aider à la mise en place, ici ou là, de filières scientifiques pluridisciplinaires contenant une composante mathématique pure ou appliquée. En particulier, nous avons introduit dans nos ouvrages de solides initiations aux probabilités et statistique ainsi qu'à l'algorithmique.

Malgré tout le soin apporté à cet ouvrage il est inévitable que quelques erreurs subsistent. Nous prions le lecteur, qui pourra les signaler à l'éditeur ou à l'un d'entre nous pour correction lors d'un nouveau tirage, de nous en excuser.

Jean-Pierre Ramis, André Warusfel

*Vous pouvez accéder aux corrigés des exercices supplémentaires à partir de la page de présentation de l'ouvrage sur le site de l'éditeur* `www.dunod.com`*. Les corrigés sont au format pdf et permettent une recherche classique par mots clef. Ils peuvent être lus, enregistrés ou imprimés en partie comme en totalité.*

# Algèbre

Partie I

# Arithmétique I.1

On attribue à Gauß (lui-même surnommé « le prince des mathématiciens ») la phrase selon laquelle « les mathématiques sont la reine des sciences et la théorie des nombres est la reine des mathématiques ». C'est sans conteste le domaine où l'activité des mathématiciens a été le plus purement motivée par la beauté et le plaisir. Trois mutations ont progressivement changé le caractère de l'arithmétique (c'est l'autre nom de la théorie des nombres) telle que l'avait connue Gauß :

1. Sous son influence, puis sous celle d'autres mathématiciens du XIX$^{e}$ siècle (surtout allemands !), de profondes techniques d'algèbre puis d'analyse (et même, au XX$^{e}$ siècle, de géométrie algébrique) ont renforcé l'arsenal de l'arithméticien.
2. Au XX$^{e}$ siècle, des problèmes de pure théorie des nombres ont rencontré des échos en physique.
3. Encore au XX$^{e}$ siècle, des applications financières et même militaires lui sont tombées dessus ! Il s'agit bien entendu des questions de sécurité de communication : cryptographie, authentification ...

Ce chapitre commencera donc par un peu d'outillage algébrique (section 1, consacrée à une approche abstraite de la théorie de la divisibilité et de la factorisation), complété par la section 2, intermédiaire entre l'algèbre et l'arithmétique, et qui comportera des applications informatiques ; et il se terminera par un pont avec la théorie des fonctions spéciales (section 6), qui jouent un rôle essentiel en physique ; cet aspect sera développé dans le module III.4 de ce volume sur les polynômes orthogonaux ; les aspects proprement arithmétiques des fractions continues pourront être approfondis dans le livre [MPA1]. Entre ces limites, les sections 3, 4 et 5 permettront de jouer avec des problèmes remontant à Fermat, Euler, Lagrange, Gauß, Legendre... et dont certains (critères de primalité) jouissent d'un intérêt renouvelé depuis quelques années.

Nous avons proposé dans la bibliographie quelques livres qui vous permettront d'approfondir les sujets abordés dans ce module et d'en découvrir d'autres. Les ouvrages [HW] et [Serre] sont de grands classiques que tout mathématicien, même amateur, devrait posséder (le second est toutefois nettement plus avancé que le premier). [Demazure] fait le lien avec les applications informatiques, que [Knuth2] (qui est beaucoup plus ancien) développe de manière détaillée. [Baker] et [Hindry] sont très riches, mais d'un abord plus difficile.

Comme des notions plus générales vont apparaître, précisons que nous réservons l'appellation de *nombre premier* aux entiers naturels premiers : $2, 3, 5, 7 \ldots$ .

# 1 Divisibilité dans un anneau commutatif

Notre but est de généraliser autant que possible le *théorème fondamental de l'arithmétique* : existence pour tout entier d'une factorisation essentiellement unique en produit de nombres premiers. Le cadre est ici celui des anneaux commutatifs intègres (autrement, les difficultés techniques seraient trop grandes). Les éléments les plus caractéristiques de l'arithmétique d'un tel anneau sont ses *unités*, *i.e.* ses éléments inversibles (ce sont eux qui empêchent la décomposition d'être vraiment unique) ; et, bien entendu, ses éléments irréductibles et ses éléments premiers : nous verrons que ces deux termes ne désignent pas exactement la même chose, et c'est même là le cœur du problème !

## 1.1 Anneaux euclidiens et anneaux principaux

Résumons l'enchaînement logique des propriétés arithmétiques des anneaux intègres $\mathbb{Z}$ et $K[X]$ ($K$ un corps commutatif), telles qu'on les a établies dans le livre [L1] :

1. Dans $\mathbb{Z}$ et dans $K[X]$, on dispose d'une *division euclidienne*.
2. Les anneaux $\mathbb{Z}$ et $K[X]$ sont principaux. On en déduit le théorème de Bézout, le lemme de Gauß et le lemme d'Euclide.
3. Dans $\mathbb{Z}$ et dans $K[X]$, tout élément admet une factorisation essentiellement unique en produit de facteurs irréductibles.

Nous allons maintenant formaliser (ici et dans la section 1.2) les liens logiques entre ces propriétés en vue d'applications plus générales.

**Définition 1.** Un anneau (commutatif intègre) $A$ est dit *euclidien* s'il admet un *stathme euclidien*, c'est-à-dire une application $g : A \setminus \{0\} \to \mathbb{N}$ telle que, pour tout couple $(x, y)$ d'éléments de $A$ :

1. Si $x, y \neq 0$ et $x \mid y$, alors $g(x) \leqslant g(y)$. De manière équivalente, si $x, x' \neq 0$, alors $g(x) \leqslant g(xx')$.
2. Si $x \neq 0$, il existe $q, r \in A$ tels que $y = qx + r$ et : soit $r = 0$ ; soit $g(r) < g(x)$.

Les éléments $q$ et $r$ sont appelés *quotient* et *reste* de la *division euclidienne*. On ne requiert *pas* l'unicité de la division euclidienne.

L'exemple qui suit sera fondamental dans les applications arithmétiques de ce chapitre. On rappelle que $\mathbb{Z}[\mathrm{i}]$ désigne l'anneau des entiers de Gauß $a + b\mathrm{i}$, $a, b \in \mathbb{Z}$ et que la norme algébrique $N$ est définie par $N(z) := z\overline{z}$ (on approfondira ces notions en 4.1).

---

**Exercice 1.**

Démontrer que, pour tout complexe $z \in \mathbb{C}$, il existe un entier de Gauß $q$ tel que $N(z - q) < 1$, où $N$ est la norme algébrique sur $\mathbb{C}$. En déduire que $N$ est un stathme euclidien sur $\mathbb{Z}[\mathrm{i}]$.

***Solution.*** Si $z = a + \mathrm{i}b$, notons $a_0$ l'entier le plus proche de $a$ et $b_0$ l'entier le plus proche de $b$ (s'il y a ambiguïté, c'est-à-dire si $a$ ou $b$ est un entier plus $1/2$, on prend la partie entière) ; on a donc $|a - a_0|, |b - b_0| \leqslant 1/2$, d'où, en posant $q := a_0 + b_0\mathrm{i}$, $N(z - q) \leqslant 1/4 + 1/4 < 1$.

Soient maintenant $x, y \in \mathbb{Z}[\mathrm{i}]$, $x \neq 0$. En appliquant ce qui précède à $z := \dfrac{y}{x}$, on trouve $q \in \mathbb{Z}[\mathrm{i}]$ tel que, si $r := y - qx$, on ait $N(r) < N(x)$ et $y = qx + r$ : que $r$ soit nul ou pas, c'est bien une division euclidienne.
Par ailleurs, si $x, x' \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$, on a $N(x') \geqslant 1$, d'où $N(x) \leqslant N(xx')$.

---

**Théorème 1.** Tout anneau euclidien est principal.

***Démonstration.*** On rappelle (*cf.* le livre [L1], module « Groupes, anneaux, corps ») qu'un anneau principal est un anneau intègre dans lequel tout idéal est principal.
Soit $I$ un idéal de l'anneau euclidien $A$. Si $I = 0$, il n'y a rien à démontrer. Sinon, soit $x \in I \setminus \{0\}$ tel que l'entier $g(x)$ est minimum. Alors $Ax \subset I$. Pour tout $y \in I$, dans la division euclidienne $y = qx + r$, on a $r \in I$, donc $r = 0$ car $g(r) < g(x)$ est impossible (minimalité), donc $y \in Ax$ et $I = Ax$. ∎

***Exemples***. L'application $x \mapsto |x|$ est un stathme euclidien sur $\mathbb{Z}$.
L'application $P \mapsto \deg P$ est un stathme euclidien sur $K[X]$ ($K$ un corps). Ces anneaux sont donc principaux, ainsi que $\mathbb{Z}[\mathrm{i}]$. En revanche, l'anneau $\mathbb{Z}[X]$ n'est pas principal : si l'idéal $<2, X>$ était engendré par $u$, ce dernier diviserait 2 et $X$, donc vaudrait $\pm 1$ ; mais 1 et $-1$ n'appartiennent pas à l'idéal engendré par 2 et $X$, car tout élément $P$ de cet idéal est tel que $P(0)$ est pair.

Soient $x, y$ deux éléments de l'anneau principal $A$. Tout générateur $d$ de l'idéal $Ax + Ay$ est un diviseur commun à $x$ et $y$ (car $x, y \in Ad$); comme il s'écrit $d = ax + by$, tout diviseur commun à $x$ et $y$ divise $d$ : c'est donc un pgcd de $x$ et $y$.

**Proposition 2 (Algorithme d'Euclide).** Supposons $A$ euclidien. L'algorithme suivant permet de calculer un pgcd de $x$ et $y$. On admet l'existence d'une fonction **`reste(y,x)`** qui, si $x \neq 0$, rend le reste **`r`** d'une division euclidienne $y = qx + r$.
On suppose au départ que : $y \neq 0$, et que : $x = 0$ ou $g(x) < g(y)$ (on peut s'y ramener au prix d'une division euclidienne de $y$ par $x$). Voici le corps de l'algorithme :

```
pgcd(x,y)
si x = 0
    rendre y
sinon
    (r := reste(y,x); rendre pgcd(x,r));
```

***Démonstration.*** C'est un algorithme *récursif* (voir le module « Structures discrètes et récursivité » du livre [L2]). Dans le cas de sortie où $x = 0$, il n'y a pas de problème, on sait bien que $y$ est un pgcd de $x$ et $y$.
Si $x \neq 0$, et si $y = qx + r$, on sait qu'un pgcd de $x$ et $r$ est aussi un pgcd de $x$ et $y$ (même raisonnement que dans les versions de cet algorithme du livre [L1]). Pour calculer **`pgcd(x,y)`**, il suffit donc de calculer **`pgcd(x,r)`**. Est-ce plus simple ? *Oui*, car soit $r = 0$ (et le calcul est instantané), soit $g(r) < g(x) < g(y)$, et l'on est plus près de la *sortie* de l'algorithme qu'au premier appel de la fonction **`pgcd`**.

Si l'on préfère une version non récursive (boucle **`tant que`**), il suffit de calquer celle du livre [L1]. ∎

Le résultat suivant est donné sous une forme concrète dans le cas d'un anneau euclidien. Voir [MPA1] pour une extension (considérablement enrichie) au cas des anneaux principaux.

**Proposition 3 (Algorithme du pivot sur un anneau euclidien).** Soit $A$ un anneau euclidien et soit $M \in M_{m,n}(A)$ une matrice à coefficients dans $A$. On peut, par des permutations de lignes et de colonnes, et par des transvections (à coefficients dans $A$) sur les lignes et les colonnes, mettre $M$ sous la forme :

$$\begin{pmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & d_r & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \end{pmatrix} = \sum_{i=1}^{r} d_i E_{i,i} = \begin{pmatrix} D & 0_{r,n-r} \\ 0_{m-r,r} & 0_{m-r,n-r} \end{pmatrix},$$

pour un certain $r \in [\![0, \min(m,n)]\!]$ et des éléments $d_1, \dots, d_r$ de $A \setminus \{0\}$ tels que $d_1 \mid d_2 \mid \cdots \mid d_r$. Dans la dernière écriture, $D := \mathrm{Diag}(d_1, \dots, d_r)$, et $0_{p,q}$ désigne la matrice nulle de type $(p,q)$.

***Démonstration.*** Il s'agit bien sûr d'une adaptation de l'algorithme du pivot de Gauß sur un corps, mais en plus compliqué ; le lecteur est donc invité à se replonger dans l'algorithme classique (*cf.* le livre [L1], module sur les matrices). On peut supposer la matrice $M$ non nulle. Pour simplifier les notations, nous noterons ici $\gamma(M)$ le minimum des $g(m_{i,j})$ pour $m_{i,j}$ non nul (les $g(m_{i,j})$ sont des entiers).

Pour commencer, on choisit un coefficient $m_{i,j}$ (le « pivot ») tel que $g(m_{i,j}) = \gamma(M)$. Par permutation de lignes et colonnes, on le ramène en position $(1,1)$. C'est donc maintenant $g(m_{1,1})$ qui est minimal. Par divisions euclidiennes $m_{1,j} = q_j m_{1,1} + r_j$, on peut définir des transvections sur les colonnes : $C_j \leftarrow C_j - q_j C_1$, à l'issue desquelles chaque $m_{1,j}$ $(j > 1)$ est nul ou tel que $g(m_{1,j}) < g(m_{1,1})$. De même, par des transvections sur les lignes, on peut obtenir la propriété que chaque $m_{i,1}$ $(i > 1)$ est nul ou tel que $g(m_{i,1}) < g(m_{1,1})$.

Si l'un des $m_{1,j}$ $(j > 1)$ ou l'un des $m_{i,1}$ $(i > 1)$ n'est pas nul, $\gamma(M)$ a diminué strictement et l'on recommence tout le processus ci-dessus. Cela ne peut se produire une infinité de fois puisque l'entier $\gamma(M)$ diminue strictement chaque fois. On peut donc ramener $M$ à la forme $\begin{pmatrix} m_{1,1} & 0 \\ 0 & M' \end{pmatrix}$, où $M'$ a une ligne et une colonne de moins que $M$ (si $M$ n'avait qu'une ligne ou une colonne, l'algorithme est déjà terminé).

Supposons que $m_{1,1}$ ne divise pas tous les coefficients de $M'$. Soit $m_{i,j}$ $(i,j > 1)$ non multiple de $m_{1,1}$ ; on a donc une division euclidienne $m_{i,j} = q m_{1,1} + r$, $g(r) < g(m_{1,1})$.

On opère la transvection $C_j \leftarrow C_j + C_1$, puis la transvection $L_i \leftarrow L_i - qL_1$ et maintenant $m_{i,j} = r$, donc $\gamma(M)$ a diminué strictement. En itérant l'ensemble des deux processus décrits ci-dessus, on peut ramener $M$ à la forme $\begin{pmatrix} m_{1,1} & 0 \\ 0 & M' \end{pmatrix}$, où, de plus, $m_{1,1}$ divise tous les coefficients de $M'$. Ce $m_{1,1}$ est $d_1$.
On recommence maintenant l'ensemble de l'algorithme ci-dessus sur $M'$. ∎

Le lecteur courageux pourra tenter la programmation de cet algorithme : il constatera que la structure ne peut en être substantiellement simplifiée.

***Exemple***. Nous allons étudier le système à inconnues entières $\begin{pmatrix} -10 & 14 \\ -8 & 10 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$, ou encore $\begin{cases} -10x + 14y = a, \\ -8x + 10y = b. \end{cases}$ $(x, y, a, b \in \mathbb{Z})$. On effectue successivement les opérations $L_1 \leftrightarrow L_2$, $C_2 \leftarrow C_2 + C_1$, $L_2 \leftarrow L_2 - L_1$, $C_1 \leftrightarrow C_2$, $C_2 \leftarrow C_2 + 4C_1$ et $L_2 \leftarrow L_2 - L_1$, ce qui donne la matrice $\begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$. Du côté des systèmes, les transvections sur les colonnes se traduisent par les changements de variable $x' := x - y$ puis $y' := y - 4x'$. Le système final est $\begin{cases} 2y' = b, \\ 6x' = a - 2b. \end{cases}$
Il admet des solutions entières si, et seulement si, $2 \mid b$ et $6 \mid a - 2b$. On trouve alors les solutions du système de départ en inversant le changement de variables : $y := y' + 4x'$ et $x := x' + y = y' + 5x'$. Par exemple si $a := 10$ et $b := 2$, on trouve $(x', y') = (1, 1)$, puis $(x, y) = (6, 5)$.

## 1.2 Anneaux principaux et anneaux factoriels

Ces notions ont déjà reçu des applications dans le module sur les polynômes à plusieurs indéterminées du livre [L2]. Rappelons et complétons le vocabulaire sur la divisibilité dans un anneau *intègre*. Nous notons $A^*$ le groupe des unités (éléments inversibles) de $A$.

1. On dit que $x$ divise $y$, notation : $x \mid y$, s'il existe $a \in A$ tel que $y = ax$. Si $x = 0$, cela implique $y = 0$ et $a$ est quelconque ; si $x \neq 0$, un tel $a$ est unique (intégrité !), on le note $\dfrac{y}{x}$. On dit que $x$ et $y$ sont associés, ce que l'on notera $x \sim y$, si chacun divise l'autre. Si $x = 0$, cela implique $y = 0$ (et réciproquement) ; si $x$ et $y$ sont non nuls, cela équivaut à l'existence de $u \in A^*$ tel que $y = ux$, et donc $x = u^{-1}y$.
2. On dit que $x$ est *irréductible* s'il est non inversible et s'il n'admet aucune décomposition non triviale ; autrement dit, pour toute décomposition $x = yz$, on a $y$ inversible (et donc $z$ associé à $x$) ou bien $z$ inversible (et donc $y$ associé à $x$).
3. On dit que $x$ est *premier* s'il est non inversible et non nul et si l'idéal principal $Ax$ est premier ; de manière équivalente, $x \neq 0$, $x \notin A^*$ et :
$$\forall y, z \in A\ ,\ x \mid yz \Rightarrow (x \mid y \quad \text{ou} \quad x \mid z)\,.$$
Il est bien évident que tout élément premier est irréductible.

***Idéaux et divisibilité dans un anneau principal***. Soit $A$ un anneau principal qui n'est pas un corps (cette hypothèse sera désormais implicite). Outre l'idéal nul, ses idéaux sont de la forme $<x>$ avec $x \neq 0$. De plus, $<x> = <y>$ si, et seulement si, $x$ et $y$ sont associés. Il y a donc bijection entre les idéaux non nuls et les classes d'éléments non nuls de $A$ (pour la relation « être associé »). De plus, $x \mid y$ si, et seulement si, $<y> \subset <x>$. Ainsi, le plus grand idéal, $A$, correspond à la plus petite classe (pour la relation « diviser »), $A^*$ (la classe de $1$); et les idéaux maximaux correspondent aux classes des éléments irréductibles. Les idéaux premiers non nuls de $A$ sont donc les $<x>$, $x$ irréductible, et ils sont maximaux et ces $x$ sont premiers.

La situation n'est en général pas aussi simple. Commençons par quelques exemples motivants. Ceux-ci font appel aux propriétés de la norme algébrique des nombres complexes : $N(a+\mathrm{i}b) := a^2+b^2$ (pour $a, b \in \mathbb{R}$); rappelons que $N(uv) = N(u)N(v)$.

***Exemple***. Soit $d \in \mathbb{Z}$, $d > 0$. Rappelons que, par convention, nous notons $\sqrt{-d} := \mathrm{i}\sqrt{d}$. Si $u \in \mathbb{Z}[\sqrt{-d}] \setminus \{0\}$, alors $N(u) \in \mathbb{N}^*$ (si $a, b \in \mathbb{Z}$ sont non tous deux nuls, $N(a+b\sqrt{-d}) = a^2+db^2$ est un entier strictement positif). On en déduit que les éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{-d}]$ sont les éléments $u$ tels que $N(u) = 1$ : en effet, si $u$ a pour inverse $v$, on a $N(u)N(v) = N(uv) = 1$, d'où $N(u) = 1$ (c'est un entier positif); réciproquement, si $N(u) = 1$, le conjugué $\overline{u}$ est l'inverse de $u$. Pour des entiers, $a^2+db^2 = 1$ n'est possible que si $a = \pm 1$ et $b = 0$, sauf dans le cas où $d = 1$, pour lequel on a aussi les solutions $a = 0$ et $b = \pm 1$. Les éléments inversibles de $\mathbb{Z}[\sqrt{-d}]$ sont donc $\pm 1$ et $\pm\mathrm{i}$ si $d = 1$ et $\pm 1$ si $d \geqslant 2$.
Montrons maintenant que le nombre premier $p \in \mathbb{N}$ est réductible dans $\mathbb{Z}[\sqrt{-d}]$ si, et seulement s'il est de la forme $a^2+db^2$ avec $a, b \in \mathbb{Z}$. Supposons tout d'abord $p = uv$, avec $u, v \in \mathbb{Z}[\sqrt{-d}]$ non inversibles. Alors $p^2 = N(p) = N(u)N(v)$ et $N(u), N(v) > 1$, donc $N(u) = N(v) = p$. Comme $N(a+b\sqrt{-d}) = a^2+db^2$, $p$ est bien de la forme indiquée. Réciproquement, si $p = a^2+db^2$ avec $a, b \in \mathbb{Z}$, on a $p = uv$, avec $u := a+b\sqrt{-d} \in \mathbb{Z}[\sqrt{-d}]$ et $v := \overline{u} \in \mathbb{Z}[\sqrt{-d}]$ tous deux non inversibles.

## Exercice 2.

On prend maintenant $d := 5$. Montrer que $3$ est irréductible dans l'anneau $\mathbb{Z}[\sqrt{-5}]$. Vérifier que $3$ divise $(2+\sqrt{-5})(2-\sqrt{-5})$ mais qu'il ne divise ni $2+\sqrt{-5}$ ni $2-\sqrt{-5}$.

***Solution.*** On vérifie facilement que $3 = a^2+5b^2$ est impossible avec $a, b \in \mathbb{Z}$. Ainsi, $3$ est irréductible dans $\mathbb{Z}[\sqrt{-5}]$ (de même, du fait que $N(2+\sqrt{-5}) = N(2-\sqrt{-5}) = 9$, on peut déduire que $2+\sqrt{-5}$ et $2-\sqrt{-5}$ sont irréductibles). On a $(2+\sqrt{-5})(2-\sqrt{-5}) = 3^2$. Mais ni $\dfrac{2+\sqrt{-5}}{3}$, ni $\dfrac{2-\sqrt{-5}}{3}$, ne sont de la forme $a+b\sqrt{-5}$ avec $a, b \in \mathbb{Z}$, donc $3$ ne divise ni $2+\sqrt{-5}$ ni $2-\sqrt{-5}$. Ainsi, $3$ *est irréductible mais n'est pas premier*. C'est cette discordance qui est impossible dans un anneau factoriel.

## Exercice 3.

Soit $d \in \mathbb{Z}$ qui n'est pas un carré. Décrire les éléments de $\mathbb{Z}$ qui sont premiers dans $\mathbb{Z}[\sqrt{d}]$.

***Solution.*** Puisque, par construction, l'anneau $\mathbb{Z}[\sqrt{d}]$ est intègre, l'idéal $\{0\}$ est premier dans $\mathbb{Z}[\sqrt{d}]$ ; mais, par définition, l'élément $0$ n'est pas considéré comme premier.
Soit $p \in \mathbb{N}^*$ ($-p$ engendre le même idéal) ; par convention, $1$ n'est jamais premier (car l'anneau trivial n'est pas intègre), et l'on peut supposer $p \geqslant 2$. En vertu des résultats du module « Compléments d'algèbre » du livre [L2] (théorèmes d'isomorphisme pour les anneaux, et polynômes sur un anneau), l'anneau $\mathbb{Z}[\sqrt{d}]/<p>$ est isomorphe à l'anneau $\mathbb{Z}[X]/<X^2 - d, p>$, qui est lui-même isomorphe à l'anneau $\mathbb{F}_p[X]/<X^2 - \overline{d}>$, où $\overline{d}$ désigne la classe de $d$ modulo $p$ ; rappelons que l'on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. Cet anneau est intègre si, et seulement si, le polynôme $X^2 - \overline{d}$ est irréductible, *i.e.* (puisqu'il est de degré $2$) s'il n'a pas de racines. En conclusion, $p \geqslant 2$ est premier dans $\mathbb{Z}[\sqrt{d}]$ si, et seulement si, $d$ n'est pas un carré modulo $p$.

---

## 1.2.1 Divisibilité dans les anneaux factoriels

Les preuves des résultats qui vont suivre sont en tous points similaires à celles données dans le cas de $\mathbb{Z}$ et de $K[X]$, voire pour tout anneau principal, dans le livre [L1] : nous laissons au lecteur le soin d'en rédiger les détails.

**Théorème et définition 4.** Soit $A$ un anneau intègre (commutatif) dans lequel tout élément non nul et non inversible est produit d'éléments irréductibles. Les propriétés suivantes sont alors équivalentes :
(i) La décomposition en produit d'irréductibles est unique à l'ordre des facteurs près et à inversible près.
(ii) Tout élément irréductible est premier.
On dit alors que l'anneau $A$ est *factoriel*. Cette propriété équivaut encore à la suivante : tout élément non inversible de $A$ est produit d'éléments *premiers*.

La propriété (i) signifie que, si $p_1 \cdots p_r = q_1 \cdots q_s$, les $p_i$ et $q_j$ étant irréductibles, alors $r = s$ et, quitte à réordonner les facteurs, $q_i$ est associé à $p_i$ pour tout $i \in [\![1, r]\!]$.

**Point Méthode**

Il sera plus commode de procéder comme suit. Dans l'ensemble des éléments irréductibles de $A$, on fixe un ensemble de représentants $P$. Autrement dit, tous les éléments de $P$ sont irréductibles ; et, pour chaque $p \in A$ irréductible, il y a un unique $p' \in P$ tel que $p \sim p'$ (*i.e.* $p$ et $p'$ sont associés). Ce choix étant fait, les propriétés du théorème et de la définition se résument ainsi : tout $a \in A$ non nul admet une unique écriture $a = up_1^{r_1} \cdots p_k^{r_k}$ ($u \in A^*$, $k \in \mathbb{N}$ et les $r_i \in \mathbb{N}^*$, les $p_i \in P$).

***Exemple***. Si $A = \mathbb{Z}$, on prend pour $P$ l'ensemble des nombres premiers (dans $\mathbb{N}$). Si $A = K[X]$, on prend pour $P$ l'ensemble des polynômes unitaires irréductibles.

**Théorème 5.** Tout anneau principal est factoriel.

### 1.2.2 Valuations

Soit $a \in A$. On introduit les *valuations* $v_p$ par la formule :

$$a = u \prod_{p \in P} p^{v_p(a)},$$

où $u \in A^*$ et où les $v_p(a) \in \mathbb{N}$ sont presque tous nuls.
On convient par ailleurs que $\forall p \in P\ ,\ v_p(0) := +\infty$. On a alors les formules :

$$v_p(ab) = v_p(a) + v_p(b) \qquad \text{et} \qquad v_p(a+b) \geqslant \min\big(v_p(a), v_p(b)\big).$$

On vérifie immédiatement que $a \mid b$ équivaut à : pour tout $p \in P$, $v_p(a) \leqslant v_p(b)$.
Ainsi, $a \sim b$ équivaut à : pour tout $p \in P$, $v_p(a) = v_p(b)$.
Il en découle que le *plus grand commun diviseur* $a \wedge b$ de $a$ et $b$ se calcule ainsi :

$$a \wedge b = \prod_{p \in P} p^{\min\left(v_p(a), v_p(b)\right)};$$

les pgcd de $a$ et $b$ sont les éléments associés à $a \wedge b$. Les diviseurs communs à $a$ et $b$ sont les diviseurs de $a \wedge b$. On voit que $a$ et $b$ sont premiers entre eux (ou étrangers) si, et seulement si, $a \wedge b = 1$.

Dire que les éléments $a$ et $b$ sont étrangers n'est pas équivalent à dire que les idéaux $<a>$ et $<b>$ sont étrangers (c'est-à-dire, selon le module « Compléments d'algèbre » du livre [L2], que $<a> + <b> = A$) : voir l'exercice I.1.8 de la page 69.

**Proposition 6 (Lemme de Gauß).** Si $a$ et $b$ sont étrangers et si $a \mid bc$, alors $a \mid c$.

Plus généralement, on peut calculer :

$$pgcd(a_1, \ldots, a_n) := a_1 \wedge \cdots \wedge a_n := \prod_{p \in P} p^{\min\left(v_p(a_1), \ldots, v_p(a_n)\right)}$$

et dire que les éléments $a_1, \ldots, a_n \in A$ sont premiers entre eux (ou étrangers) *dans leur ensemble* si ce pgcd est égal à $1$. De même, on peut définir le ppcm par la formule : $ppcm(a_1, \ldots, a_n) := a_1 \vee \cdots \vee a_n := \prod_{p \in P} p^{\max\left(v_p(a_1), \ldots, v_p(a_n)\right)}$. Les multiples communs à $a_1, \ldots, a_n$ sont les multiples de leur ppcm.

---

**Exercice 4.**
On suppose que $a$ et $b$ sont étrangers et que $ab$ est de la forme $x^d$ pour un $d \geqslant 2$. Montrer qu'il existe $y, z \in A$ tels que $a \sim y^d$ et $b \sim z^d$.
***Solution.*** Puisque $a$ et $b$ sont étrangers, pour tout $p \in P$, $v_p(a)$ ou $v_p(b)$ est nul ; mais comme $v_p(a) + v_p(b) = v_p(x^d) = dv_p(x)$, $v_p(a)$ et $v_p(b)$ sont tous deux multiples de $d$. Or, la condition « il existe $y \in A$ tel que $a \sim y^d$ » est clairement équivalente à : « pour tout $p \in P$, $v_p(a)$ est multiple de $d$ ».

---

***Extension des $v_p$ au corps des fractions de $A$***

Soit $\dfrac{a}{b}$ un élément du corps des fractions $K$ de $A$. Quitte à simplifier le numérateur et le dénominateur par $a \wedge b$, on peut supposer que cette fraction est irréductible, c'est-à-dire que $a$ et $b$ sont premiers entre eux. Dans ce cas, pour toute égalité $\dfrac{a}{b} = \dfrac{c}{d}$, on a $c = am$ et $d = bm$ avec $m \in A$ : cela découle du lemme de Gauß. En particulier, si $\dfrac{c}{d}$ est également irréductible, alors $a$ et $c$ sont associés, ainsi que $b$ et $d$.
On peut étendre les valuations $v_p$ au corps des fractions de $A$ en posant :

$$\forall p \in P\ ,\ \forall a, b \in A \setminus \{0\}\ ,\ v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b).$$

Le lecteur vérifiera que cette définition n'est pas ambiguë et que les règles sur $v_p(ab)$ et $v_p(a+b)$ restent valides. De plus, tout élément $x \in K^*$ admet une unique écriture :

$$x = u \prod_{p \in P} p^{v_p(x)},$$

où $u \in A^*$ et où les $v_p(x) \in \mathbb{Z}$ sont presque tous nuls.

---

**Exercice 5.**
Démontrer que $\sqrt{2}$ est irrationnel.
***Solution.*** Si $x := \sqrt{2}$ était rationnel, de l'égalité $x^2 = 2$ on tirerait $2v_2(x) = 1$, ce qui est impossible puisque $v_2(x) \in \mathbb{Z}$.

---

***Remarque***. Notons $P^*$ le sous-groupe de $K^*$ engendré par $P$, autrement dit :

$$P^* := \{x \in K^* \mid x = \prod_{p \in P} p^{v_p(x)}\}.$$

Il résulte des conventions précédentes que *le* pgcd et *le* ppcm d'éléments de $A \setminus \{0\}$ sont des éléments de $P^*$.

La propriété suivante, bien que facile à démontrer, est très utile :

**Proposition 7.** Pour que $x \in K$ soit élément de $A$, il faut, et il suffit, que $v_p(x)$ soit positif ou nul pour tout $p \in P$.

---

**Exercice 6.**
Démontrer que $x = \sqrt{2} + \sqrt{3}$ est irrationnel.
***Solution.*** Si $x$ était rationnel, de l'égalité $(x^2-5)^2 = 24$, *i.e.* $x^4 - 10x^2 + 1 = 0$, on déduirait que $x^2 = 10 - x^{-2}$, donc que $v_p(x^2) \geqslant \min(v_p(10), -v_p(x^2))$, donc que $v_p(x) \geqslant 0$ pour tout $p \in P$, et $x$ serait entier. Mais c'est impossible car $1{,}4 + 1{,}7 < x < 1{,}5 + 1{,}8$.

---

## 1.3 Polynômes sur un anneau factoriel

Soit $A$ un anneau factoriel, de corps des fractions $K$. On choisit un ensemble de représentants $P$ de l'ensemble des irréductibles de $A$ (pour la relation « être associé »).

**Définition 2.** Un polynôme non nul $F \in A[X]$ est dit *primitif* si ses coefficients sont premiers entre eux dans leur ensemble.

**Proposition et définition 8.** Soit $F \in K[X]$ un polynôme non nul. Il existe alors un unique $c(F) \in P^*$ et un unique polynôme primitif $\tilde{F} \in A[X]$ tels que $F = c(F)\tilde{F}$. L'élément $c(F)$ est appelé *contenu* de $F$.

***Démonstration.*** Écrivons $F = \sum \frac{a_i}{b_i} X^i$, et soit $b$ le ppcm des dénominateurs des $b_i$. Alors $bF \in A[X]$, et l'on prend pour $c(F)$ le pgcd des coefficients de $bF$ divisé par $b$. Les propriétés indiquées (unicité, primitivité) sont alors immédiates. ∎

Il est clair que $F \in A[X]$ si, et seulement si, $c(F) \in A$.

**Théorème 9 (Gauß).**
(i) Le produit de deux polynômes primitifs est primitif.
(ii) Si $F, G \in K[X]$ sont non nuls, $c(FG) = c(F)c(G)$.

***Démonstration.*** Soient $F, G \in A[X]$. Si $FG \in A[X]$ n'est pas primitif, il existe $p \in P$ qui divise tous les coefficients de $FG$. Dans l'anneau intègre $A/<p>[X]$, le produit des images $\overline{F}$ et $\overline{G}$ est nul, donc l'un des deux, par exemple $\overline{F}$, est nul ; donc $p$ divise tous les coefficients de $F$, qui n'est donc pas primitif : on a prouvé (i) par contraposée.
L'assertion (ii) est alors immédiate en invoquant la proposition 8. ∎

**Lemme 10.** Les éléments suivants sont premiers dans $A[X]$ : d'une part, les irréductibles de $A$, d'autre part, les polynômes primitifs de $A[X]$ qui sont irréductibles dans $K[X]$.

***Démonstration.*** En ce qui concerne les irréductibles de $A$, cela résulte de la preuve du théorème 9. Soit $F$ un polynôme primitif de $A[X]$ irréductible dans $K[X]$. Supposons que $F \mid GH$ dans $A[X]$. Comme $F$ divise $GH$ dans $K[X]$, il divise (par exemple) $G$ dans $K[X]$ : on a donc $FE = G$ avec $E \in K[X]$. Alors $c(E) = c(G)$ (car $c(F) = 1$), donc $c(E) \in A$, donc $E \in A[X]$ et $F$ divise $G$ dans $A[X]$. ∎

**Théorème 11.** L'anneau $A[X]$ est factoriel. Ses irréductibles sont, d'une part, les irréductibles de $A$, d'autre part, les polynômes primitifs de $A[X]$ qui sont irréductibles dans $K[X]$.

***Démonstration.*** Soit $F$ un élément non inversible de $A[X]$. S'il est constant, c'est un

élément non inversible de $A$, donc, de manière essentiellement unique, un produit d'irréductibles de $A$ ; et il n'est pas multiple d'un polynôme non constant. Si $F$ est non constant, il est produit d'irréductibles de $K[X]$, ce que l'on écrit $F = F_1 \cdots F_r$. On a donc $c(F) = c(F_1) \cdots c(F_r)$, d'où $\tilde{F} = \tilde{F}_1 \cdots \tilde{F}_r$. Finalement, $F = c(F)\tilde{F}_1 \cdots \tilde{F}_r$, où $c(F) \in A$ et les $\tilde{F}_i$ primitifs dans $A[X]$ et irréductibles dans $K[X]$. Le lemme précédent et la remarque qui suit le théorème 4 de la page 9 permettent alors de conclure. ∎

Nous pouvons maintenant compléter la théorie du résultant (module sur les polynômes à plusieurs indéterminées du livre [L2]).

**Corollaire 12.** Soient $P, Q \in A[X]$. Si l'anneau $A$ est factoriel, pour que $\mathrm{Res}(P, Q)$ s'annule, il faut, et il suffit, que $P$ et $Q$ aient un facteur commun non constant dans $A[X]$.

# 2 Le groupe multiplicatif de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Cette section est surtout destinée à fournir des outils pour la suivante ; cependant, on y trouvera deux applications informatiques intéressantes en 2.4.

## 2.1 Rappels sur $(\mathbb{Z}/n\mathbb{Z})^*$

Pour tout $n \geqslant 1$ entier, on note $(\mathbb{Z}/n\mathbb{Z})^*$ le groupe multiplicatif de l'anneau $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire, en tant qu'ensemble :

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \mid a \in \{0, \ldots, n-1\}\ ,\ a \wedge n = 1\},$$

où l'on a noté $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ la classe de $a$ et $a \wedge n$ le pgcd de $a$ et de $n$ (choisi positif). L'indicatrice d'Euler $\varphi(n)$ est alors définie par la formule :

$$\varphi(n) := \mathrm{card}\,(\mathbb{Z}/n\mathbb{Z})^* = \mathrm{card}\,\{a \in \{0, \ldots, n-1\}\ ,\ a \wedge n = 1\}.$$

***Exemple***. Si $n = p^r$, $p$ premier, $r \geqslant 1$, les non inversibles de $\mathbb{Z}/p^r\mathbb{Z}$ sont les $\overline{a}$ tels que $p \mid a$, *i.e.* les $\overline{pb}$ avec $0 \leqslant b < p^{r-1}$. Il y en a donc $p^{r-1}$ et $\varphi(p^r) = p^r - p^{r-1}$.

Si $n = p_1^{r_1} \cdots p_k^{r_k}$ (décomposition en facteurs premiers), on déduit du lemme chinois l'isomorphisme d'anneaux puis l'isomorphisme de groupes :

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{r_k}\mathbb{Z} \Longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{r_k}\mathbb{Z})^*,$$

puisque pour deux anneaux $A, B$ quelconques $(A \times B)^* = A^* \times B^*$. On en tire les formules :

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k}) = (p_1^{r_1} - p_1^{r_1-1}) \cdots (p_k^{r_k} - p_k^{r_k-1}) = n(1 - 1/p_1) \cdots (1 - 1/p_k).$$

---

**Exercice 7.**

À quelle condition a-t-on $\varphi(n) = 1$ ? $\varphi(n) = 2$ ? $\varphi(n)$ impair ?

***Solution.*** Puisque $\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k})$, on ne peut avoir $\varphi(n) = 1$ que si $n = 1$ ou $2$. De plus, sauf dans le cas de $\varphi(2)$, chaque facteur $\varphi(p_i^{r_i})$ est pair ; donc on ne peut avoir $\varphi(n) = 2$ que si $n = 3$ ou $4$ et $\varphi(n)$ ne peut être impair que si $n = 1$ ou $2$.

---

Plus généralement, on voit que la fonction arithmétique $\varphi$ est *multiplicative*, ce qui, en arithmétique, exprime la propriété suivante :

$$\forall a, b \in \mathbb{N}\ ,\ a \wedge b = 1 \Longrightarrow \varphi(ab) = \varphi(a)\varphi(b).$$

Puisque le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ a $\varphi(n)$ éléments, on déduit du théorème de Lagrange le théorème d'Euler :

$$\forall a \in \mathbb{Z}\ ,\ a \wedge n = 1 \Longrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Le petit théorème de Fermat en est un cas particulier ; si $p$ est premier :

$$\forall a \in \mathbb{Z} \setminus p\mathbb{Z}\ ,\ a^{p-1} \equiv 1 \pmod{p},\ \text{d'où l'on déduit : } \forall a \in \mathbb{Z}\ ,\ a^p \equiv a \pmod{p}.$$

La relation $\forall a \in \mathbb{Z} \setminus p\mathbb{Z}\ ,\ a^{p-1} \equiv 1 \pmod{p}$ entraîne réciproquement que tout non multiple de $p$ est premier avec $p$, donc que $p$ est premier. Cependant, la deuxième relation, qui est conséquence immédiate de la première, n'implique pas la primalité de $p$ : les *nombres de Carmichael*, comme $561 = 3 \times 11 \times 17$ la possèdent (proposition 39 de la page 43).

***Application aux groupes cycliques***

On sait que tout groupe cyclique d'ordre $n$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ et que les générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ (section 2 du module « Groupes, anneaux, corps » du livre [L1]). On en déduit que tout groupe cyclique d'ordre $n$ admet exactement $\varphi(n)$ générateurs.

***Exemple***. Il découlera de la section 2.2 que $(\mathbb{Z}/5\mathbb{Z})^*$ et $(\mathbb{Z}/7\mathbb{Z})^*$ sont cycliques. Ils ont respectivement $\varphi(5) = 4$ et $\varphi(7) = 6$ éléments. Ils sont donc respectivement isomorphes à $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$. Le groupe $(\mathbb{Z}/5\mathbb{Z})^*$ a $\varphi(4) = 2$ générateurs (les classes de 2 et de 3) et le groupe $(\mathbb{Z}/7\mathbb{Z})^*$ en a $\varphi(6) = 2$ (les classes de 3 et de 5).

**Proposition 13.** Pour tout $n \in \mathbb{N}^*$, on a :

$$\sum_{d|n} \varphi(d) = n \qquad \text{(somme étendue aux diviseurs entiers naturels de } n\text{)}.$$

***Démonstration.*** Notons $E := \{0, \ldots, n-1\}$ et, pour $d \mid n$, $E_d := \{a \in E \mid a \wedge n = d\}$, de sorte que $E$ est la réunion disjointe des $E_d$. Soit $d \mid n$ et soit $n' := n/d$. L'application $a' \mapsto da'$ définit une bijection de $\{0, \ldots, n'-1\}$ sur $E_d$. On a donc $\operatorname{card} E_d = \varphi(n/d)$ et $n$ est la somme des $\varphi(n/d)$ pour $d \mid n$. Comme l'application $d \mapsto n/d$ permute l'ensemble des diviseurs de $n$, la formule voulue en découle. ∎

Une autre démonstration est proposée dans l'exercice I.1.23 de la page 70.

## 2.2 Le groupe multiplicatif d'un corps fini

Nous commencerons par un résultat un peu plus général que nécessaire.

**Proposition 14.** Soient $K$ un corps commutatif et $G$ un sous-groupe fini de $K^*$. Alors $G$ est cyclique.

***Démonstration.*** Notons $n := \operatorname{card} G$ et, pour tout diviseur $d$ de $n$, $\psi(d)$ le nombre d'éléments de $G$ qui sont d'ordre exactement $d$. Nous voulons démontrer que $\psi(n) \neq 0$.

D'après le théorème de Lagrange, l'ordre de tout élément de $G$ est un diviseur de $n$, et donc $\sum_{d|n} \psi(d) = n$.

Soit $d \mid n$ tel que $\psi(d) \neq 0$ et soit $x \in G$ un élément d'ordre $d$. Le sous-groupe $<x>$ qu'il engendre a exactement $d$ éléments, qui vérifient donc $x^d = 1$. En particulier, ils sont les racines du polynôme $X^d - 1$, qui en a au plus $d$ *puisque le corps* $K$ *est commutatif*. Ainsi $<x>$ est égal à l'ensemble de toutes les racines de ce polynôme. Tous les éléments d'ordre $d$ de $G$ sont donc dans $<x>$ et en sont des générateurs, d'où, en vertu de ce qui a été dit plus haut sur les groupes cycliques, l'égalité $\psi(d) = \varphi(d)$.
On a donc $\psi(d) = 0$ ou $\psi(d) = \varphi(d)$ pour tout $d \mid n$. Comme $\sum_{d|n} \psi(d) = \sum_{d|n} \varphi(d) = n$, on a en fait $\psi(d) = \varphi(d)$ pour tout $d \mid n$, d'où $\psi(n) = \varphi(n) \neq 0$. ∎

Ce résultat peut être en défaut si l'on ne suppose pas le corps commutatif (exercice I.1.24 de la page 70).

**Corollaire 15.** Soit $K$ un corps fini commutatif[1]. Alors $K^*$ est cyclique.

***Exemple***. Soit $p$ un nombre premier. Un entier $a \in \mathbb{Z}$ dont la classe dans $\mathbb{Z}/p\mathbb{Z}$ est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ est appelé *racine primitive modulo* $p$. Ces nombres sont utiles pour les tests de primalité (voir la section 5). On en trouve des tables, par exemple sur le site :

`http://fr.wikipedia.org/wiki/Racine_primitive_modulo_n`

## 2.3 Le groupe multiplicatif de l'anneau $\mathbb{Z}/p^r\mathbb{Z}$

Dans toute cette section, $p$ désignera un nombre premier impair. Pour le cas des groupes $(\mathbb{Z}/2^r\mathbb{Z})^*$, des informations partielles sont proposées en exercice ; le cas général est traité dans [Demazure].

**Lemme 16.** L'élément $\overline{1+p} \in (\mathbb{Z}/p^r\mathbb{Z})^*$ est d'ordre $p^{r-1}$.

***Démonstration.*** On va démontrer par récurrence sur $i$ que $(1+p)^{p^i} = 1 + p^{i+1}x_i$, où $x_i \in \mathbb{Z} \setminus p\mathbb{Z}$. Pour $i = 0$, on a $x_0 = 1$. Supposons la relation vérifiée au rang $i \geqslant 1$. Alors :

$$(1+p)^{p^{i+1}} = \left(1 + p^{i+1}x_i\right)^p = 1 + p^{i+2}x_{i+1},$$

où :

$$x_{i+1} = x_i + \sum_{k=2}^{p-1} \binom{p}{k} p^{k(i+1)-(i+2)} x_i^k + p^{p(i+1)-(i+2)} x_i^p \equiv x_i \pmod{p},$$

car $p \mid \binom{p}{k}$ pour $0 < k < p$ et $p(i+1) - (i+2) > 1$ puisque $p > 2$. La relation étant établie, on voit que $\left(\overline{1+p}\right)^{p^{r-2}} \neq \overline{1}$ (prendre $i = r-2$) et que $\left(\overline{1+p}\right)^{p^{r-1}} = \overline{1}$ (prendre $i = r-1$). ∎

[1] En fait, tout corps fini est commutatif (théorème de Wedderburn, voir le livre [MPA1]).

**Théorème 17.** Pour $p$ premier impair, le groupe $(\mathbb{Z}/p^r\mathbb{Z})^*$ est cyclique.

***Démonstration.*** Le morphisme surjectif d'anneaux $\mathbb{Z}/p^r\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induit un morphisme de groupes $(\mathbb{Z}/p^r\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ qui est lui aussi surjectif, puisqu'à la source comme au but on trouve les classes des éléments de $\mathbb{Z} \setminus p\mathbb{Z}$. Soit $x_0$ un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ (corollaire 15 de la page précédente) et soit $y_0 \in (\mathbb{Z}/p^r\mathbb{Z})^*$ un antécédent de $x_0$. Puisque $y_0^k = 1 \Rightarrow x_0^k = 1$, l'ordre $p-1$ de $x_0$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ divise l'ordre de $y_0$ dans $(\mathbb{Z}/p^r\mathbb{Z})^*$. Il existe donc une puissance $z_0$ de $y_0$ dont l'ordre est $p-1$. Alors l'ordre de $z_0\,\overline{1+p} \in (\mathbb{Z}/p^r\mathbb{Z})^*$ est $(p-1)p^{r-1} = \varphi(p^r)$ (exercice I.1.25 de la page 70) et $z_0\,\overline{1+p}$ est un générateur de $(\mathbb{Z}/p^r\mathbb{Z})^*$. ∎

**Exercice 8.**

Trouver un générateur de $(\mathbb{Z}/125\mathbb{Z})^*$.

***Solution.*** Puisque (par exemple) la classe de $3$ engendre $(\mathbb{Z}/5\mathbb{Z})^*$, on cherche l'ordre de $\overline{3} \in (\mathbb{Z}/125\mathbb{Z})^*$, qui doit être un multiple de $4$ et un diviseur de $\varphi(125) = 100$. On constate que le reste de $3^{20}$ modulo $125$ est $26$ et l'on a donc directement un générateur.

## 2.4 Deux applications informatiques

### 2.4.1 Première application : générateurs pseudo-aléatoires

L'un des pères fondateurs de l'informatique, John von Neumann, a dit : *« Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin. »*[2]. Nous tenterons donc plus modestement de *simuler* l'aléatoire et parlerons de « générateur pseudo-aléatoire ». Dans ce but, nous décrirons des moyens de produire de longues suites de nombres variés (en utilisant l'arithmétique modulaire, et en particulier la structure du groupe $(\mathbb{Z}/m\mathbb{Z})^*$). Il y a pour cela une théorie riche et compliquée (et amusante), que nous effleurerons à peine. Pour une étude approfondie, voir [Knuth2] qui traite de plus des tests permettant d'évaluer la qualité d'un générateur (son aptitude à simuler l'aléatoire). Vu de l'extérieur, un générateur pseudo-aléatoire est un programme qui rend un nombre chaque fois qu'on l'appelle. Vu de l'intérieur, ce programme calcule en fait les termes d'une suite numérique $(x_n)$. Chaque fois qu'on l'appelle, il renvoie un terme ; d'un appel sur l'autre, il passe au terme suivant. Autrement dit, entre deux appels, le programme garde trace du rang du dernier terme rendu : l'indice $n$ est une *variable rémanente*, et il faut donc savoir programmer de telles variables. Le plus souvent, il s'agit de suites définies par récurrence : $x_{n+1} = f(x_n)$. Dans ce cas, la variable rémanente contient la dernière valeur de $x_n$ qui a été rendue. Dans notre approche élémentaire, nous ne traiterons pas ce problème : nous considérerons simplement des programmes qui calculent $f(x)$, donc chaque nouveau terme en fonction du précédent. Il existe deux types principaux de générateurs aléatoires : ceux qui rendent des nombres réels entre $0$ et $1$ ; et ceux qui rendent des entiers entre $0$ et $m-1$, l'entier $m \geqslant 2$ ayant été passé en argument. Nous ne nous occuperons que du deuxième type.

[2] « Quiconque envisage des méthodes arithmétiques pour produire des nombres aléatoires est, bien entendu, en état de péché. »

### *Générateurs linéaires congruentiels*

Nous supposons fixé le *module* $m \geqslant 2$ (argument d'appel). Au lieu de considérer une suite d'entiers compris entre $0$ et $m-1$, nous considérerons une suite d'éléments de $\mathbb{Z}/m\mathbb{Z}$. Le format général de cette suite est donné par la relation de récurrence :

$$\forall n \in \mathbb{N}\ ,\ x_{n+1} := ax_n + b.$$

Un générateur pseudo-aléatoire basé sur ce principe est appelé *linéaire congruentiel*. Il faut, pour le spécifier choisir le module $m$, la « graine », ou « semence », (en anglais : the seed) $x_0 \in \mathbb{Z}/m\mathbb{Z}$ et les coefficients $a, b \in \mathbb{Z}/m\mathbb{Z}$. On ne prendra évidemment pas $a := \overline{0}$ car la suite serait constante à partir du rang $n = 1$ et n'aurait pas du tout l'air aléatoire. On ne prendra pas non plus en général $a := 1$ (nous employons cette notation simplifiée pour $\overline{1}$), car on aurait $x_n = x_0 + nb$, et l'on repérerait trop facilement une régularité. La théorie des générateurs linéaires congruentiels n'est vraiment développée que pour le cas d'un module premier ou primaire (*i.e.* puissance d'un nombre premier).

### *Cas d'un module premier*

Supposons $m$ premier. Puisque l'on a exclu le cas où $a = 1$, l'élément $1 - a$ est inversible dans $\mathbb{Z}/m\mathbb{Z}$ et l'on va pouvoir appliquer la méthode vue en terminale pour les suites arithmético-géométriques. On cherche un « point fixe » $u = au + b$, d'où $u = b(1-a)^{-1}$. La relation de récurrence devient alors : $(x_{n+1} - u) := a(x_n - u)$, et l'on en déduit $x_n - u = a^n(x_0 - u)$, donc :

$$\forall n \in \mathbb{N}\ ,\ x_n = a^n(x_0 - u) + u.$$

Finalement, à un décalage près de valeur $u$, tout se passe comme si la suite était géométrique. Pour la suite de ce paragraphe, nous supposons donc que $b = u = \overline{0}$ et donc que $x_n = a^n x_0$. On prendra évidemment $x_0 \neq \overline{0}$, sinon la suite serait constante et n'aurait pas du tout l'air aléatoire. Finalement, on est donc conduit à examiner la suite des $a^n x_0$. Pour savoir si elle a l'air aléatoire, on trouvera dans [Knuth2] des tests empiriques. On peut déjà se demander si elle ne boucle pas trop vite. En effet, le petit théorème de Fermat nous dit que $a^{m-1} = 1$ et donc que, si $n = q(m-1) + r$, on a $a^n = (a^{m-1})^q a^r = a^r$, d'où $x_n = x_r$ : cela signifie que la suite se reproduit avec une période $(m-1)$. Mais ce n'est pas nécessairement *la* période de cette suite.

***Exemple***. Prenons $m := 7$. Tout $a \in (\mathbb{Z}/7\mathbb{Z})^*$ vérifie $a^6 = \overline{1}$, donc la suite des $a^n x_0$ se reproduit à coup sûr avec une période $6$. Mais si l'on prend par exemple $a := \overline{2}$, on a $a^3 = \overline{1}$ et la période tombe à $3$. Il vaut mieux prendre $a := \overline{3}$ qui est tel que $a^0 = \overline{1}$, $a^1 = \overline{3}$, $a^2 = \overline{2}$, $a^3 = \overline{6}$, $a^4 = \overline{4}$, $a^5 = \overline{5}$ sont distincts et qui fournit donc une suite aussi longue que possible.

Dans tous les cas, il est raisonnable de choisir pour $a$ un générateur du groupe cyclique $(\mathbb{Z}/m\mathbb{Z})^*$.

***Cas d'un module primaire***

Supposons $m$ *primaire*, c'est-à-dire puissance d'un nombre premier : $n = p^r$, où $p$ est premier et $r \geqslant 2$. Dans ce cas, il n'est pas aussi facile d'étudier une suite arithmético-géométrique générale (car $a \neq 1$ n'entraîne pas que $1 - a$ est inversible), aussi prendrons nous d'emblée $b := \overline{0}$. Et, bien entendu, on suppose toujours $a \neq \overline{0}, \overline{1}$ et $x_0 \neq \overline{0}$.

Si $a$ est la classe d'un multiple de $p$, alors $a^r$ est la classe d'un multiple de $p^r$, donc $a^r = \overline{0}$. Dans ce cas, la suite est stationnaire en $\overline{0}$ et donc très peu aléatoire. Nous supposons donc que $a$ est la classe d'un entier non multiple de $p$. Mais un tel entier n'a pas de diviseur commun avec $p^r = m$, donc $a$ est inversible : on a encore $a \in (\mathbb{Z}/m\mathbb{Z})^*$. la situation est analogue à celle décrite plus haut : la suite aura pour longueur l'ordre de $a$. Si $p$ est impair, le groupe étant cyclique, on choisira donc pour $a$ un générateur.

***Exemple***. Avec $m := 27$, on a $\varphi(m) = 18$. Les générateurs de $(\mathbb{Z}/27\mathbb{Z})^*$ sont $\overline{2}$, $\overline{5}$, $\overline{11}$, $\overline{14}$, $\overline{20}$ et $\overline{23}$ (en fait, les puissances de $\overline{2}$ avec un exposant premier à $18$).

### 2.4.2 Deuxième application : cryptographie à clé publique

La méthode RSA de cryptographie à clé publique a été inventée en 1978 par Ron Rivest, Adi Shamir et Leonard Adleman du MIT. Sa mise en œuvre suppose le choix d'un *module* $n$, d'une *clé publique* $(e, n)$ et d'une *clé secrète* $(d, n)$. Les propriétés requises sont les suivantes :

1. L'entier naturel $n$ est assez grand pour que l'on puisse facilement *coder* (voir la remarque ci-dessous) tout message sous la forme d'une suite d'entiers de $\{0, \ldots, n-1\}$.
2. Les entiers naturels $d$ et $e$ vérifient la propriété :

$$\forall a \in \mathbb{Z}\ ,\ a^{de} \equiv a \pmod{n}.$$

Nous distinguons ici le *codage* du *cryptage*. Le codage est simplement la mise du texte sous une forme adaptée à l'algorithme. Par exemple, chaque caractère du message à transmettre est représenté par un octet et le message est tronçonné en paquets d'octets de tailles telles que l'on puisse les représenter par un entier $M \in \{0, \ldots, n-1\}$. Le problème du cryptage est alors, pour l'émetteur du message, de remplacer $M$ par un entier $M' := C(M) \in \{0, \ldots, n-1\}$ (la lettre $C$ est ici pour « cryptage »), que le destinataire du message saura reconvertir en $M := D(M')$ (la lettre $D$ est ici pour « décryptage »).

La clé publique $(e, n)$ et la clé secrète $(d, n)$ étant données, le principe est le suivant. Leur détenteur diffuse publiquement (!) la clé publique $(e, n)$ et garde par devers lui (!) la clé secrète $(d, n)$. Chaque fois que quelqu'un veut lui envoyer un message secret $M \in \{0, \ldots, n-1\}$ :

1. Il crypte $M$ selon la formule $M' := C(M) := M^e \pmod{n}$.
2. Le destinataire décrypte $M'$ selon la formule $M := D(M') := (M')^d \pmod{n}$.

Ici, par abus de notation, $M^e \pmod{n}$ désigne le reste de la division de $M^e$ par $n$, et similairement pour $(M')^d \pmod{n}$. En fait, ces calculs peuvent s'effectuer relativement vite par exponentiation rapide dans $\mathbb{Z}/n\mathbb{Z}$. La méthode RSA est correcte en vertu du calcul :

$$D(C(M)) = M^{de} \pmod{n} = M.$$

Cette relation est certainement vérifiée si $de \equiv 1 \pmod{\varphi(n)}$ (comme les choix ci-dessous l'impliquent) en vertu du théorème d'Euler (page 14) et si de plus $M$ est premier avec $n$. Pour le cas général, voir l'exercice I.1.31 de la page 70.
Il reste à voir comment on détermine les clés publique et secrète :

1. On choisit deux grands nombres premiers distincts $p$ et $q$, et l'on pose $n := pq$.
2. On choisit un entier $e$ premier avec $n' := \varphi(n) = (p-1)(q-1)$ ni trop grand ni trop petit.
3. On détermine un entier $d$ tel que $de \equiv 1 \pmod{n'}$ à l'aide de l'algorithme d'Euclide étendu.

***Exemple***. On choisit dans une table deux « grands » nombres premiers. Pour pouvoir effectuer les calculs à la main, nous nous contenterons de $p = 41$ et $q = 61$, d'où $n = 2501$ et $n' = 2400$. Les seuls facteurs premiers de $n'$ étant $2$, $3$ et $5$, on peut prendre (par exemple) $d = 7$. L'algorithme d'Euclide permet de trouver $e = 343$ (par miracle on est tombé sur l'égalité $n' = 7^4 - 1$ et donc ici $e = d^3$). Pour le codage, on décide d'accepter lettres (codées de $1$ à $26$) et chiffres (codés de $27$ à $36$). Donc chaque caractère isolé d'un texte alphanumérique est représenté par un nombre compris entre $1$ et $36$ (on ne tient pas compte de la différence majuscule-minuscule et l'on ne s'occupe pas des signes typographiques, etc.). Pour exploiter un peu mieux le grand nombre de codes disponibles, on décide enfin de découper le texte en paquets de deux caractères consécutifs. Quand deux tels caractères ont respectivement reçu les codes $a_1, a_2$ (compris entre $1$ et $36$) on attribue au paquet le code $a := 36a_1 + a_2 - 36$. On a appliqué à $(a_1 - 1, a_2 - 1)$ la bijection $(x_1, x_2) \mapsto 36x_1 + x_2$ de $\{0, \dots, 35\}^2$ sur $\{0, \dots, 36^2 - 1\}$. On voit donc que $a$ est compris entre $1$ et $1296$, et que l'on peut retrouver $a_1$ et $a_2$ à partir de $a$ en faisant la division euclidienne de $a-1$ par $36$ : on a en effet $a-1 = 36(a_1-1)+(a_2-1)$ avec de plus la condition $0 \leqslant a_2-1 \leqslant 35$, donc le quotient et le reste sont respectivement $a_1-1$ et $a_2-1$. Pour transmettre par exemple le paquet « 5t », on code le caractère '5' par l'entier $a_1 = 31$, le caractère 't' par l'entier $a_2 = 20$ et donc le paquet par $a = 36\times 31+20-36 = 1100$. C'est en fait l'entier $M$ dans la description générale donnée plus haut. Puis on calcule $C(M)$, c'est-à-dire le reste de la division euclidienne de $1100^{343}$ par $2501$. On n'est pas obligé pour cela de calculer $1100^{343}$, qui est très gros . On peut effectuer tous les calculs modulo $2501$, *i.e.* poser $a := \overline{1100} \in \mathbb{Z}/2501\mathbb{Z}$ et exécuter l'algorithme d'exponentiation dichotomique dans $\mathbb{Z}/2501\mathbb{Z}$. On pose donc $b_0 := b := \overline{1100}$, puis :

$$
\begin{array}{llll}
b_1 = b^2 & = b_0 \times b_0 & = \overline{1100} \times \overline{1100} & = \overline{1210000} \quad = \overline{2017}, \\
b_2 = b^5 & = b_1 \times b_1 \times b & = \overline{2017} \times \overline{2017} \times \overline{1100} & = \overline{4475117900} \quad = \overline{1069}, \\
b_3 = b^{10} & = b_2 \times b_2 & = \overline{1069} \times \overline{1069} & = \overline{1142761} \quad = \overline{2305}, \\
b_4 = b^{21} & = b_3 \times b_3 \times b & = \overline{2305} \times \overline{2305} \times \overline{1100} & = \overline{5844327500} \quad = \overline{704}, \\
b_5 = b^{42} & = b_4 \times b_4 & = \overline{704} \times \overline{704} & = \overline{495616} \quad = \overline{418}, \\
b_6 = b^{85} & = b_5 \times b_5 \times b & = \overline{418} \times \overline{418} \times \overline{1100} & = \overline{192196400} \quad = \overline{2053}, \\
b_7 = b^{171} & = b_6 \times b_6 \times b & = \overline{2053} \times \overline{2053} \times \overline{1100} & = \overline{4636289900} \quad = \overline{1126}, \\
b_8 = b^{343} & = b_7 \times b_7 \times b & = \overline{1126} \times \overline{1126} \times \overline{1100} & = \overline{1394663600} \quad = \overline{958}
\end{array}
$$

et l'on transmet donc $958$ (on a donc au total $13$ multiplications de nombres de quatre

chiffres et divisions euclidiennes de nombres de dix chiffres par $2501$, ce qui est faisable sur calculette …). Pour décrypter ce nombre, il faut calculer le reste de la division euclidienne de $958^7$ par $2501$ :

$\overline{958}\times\overline{958}\times\overline{958} = \overline{879217912} = \overline{1366}$, puis $\overline{1366}\times\overline{1366}\times\overline{958} = \overline{1787585848} = \overline{1100}$.

On retrouve bien le code de départ. Pour le décoder, on effectue la division euclidienne $1099 = 36 \times 30 + 19$, d'où $a_1 = 30 + 1 = 31$ et $a_2 = 19 + 1 = 20$, ce qui correspond aux caractères '5' et 't' donc au paquet « 5t ».

***Fiabilité de RSA***

Cette méthode est praticable parce qu'il est « plutôt facile » de trouver des grands nombres premiers (voir la section 5). Si l'on savait aussi facilement factoriser $n$, la méthode de cryptage serait facile à casser. Dans l'article original de Rivest, Shamir et Adleman sur RSA (1978), la table suivante est donnée ; elle indique le nombre $c(n)$ d'opérations nécessaires pour factoriser un entier de $n$ chiffres et le temps $t(n)$ correspondant, avec le meilleur algorithme de factorisation connu à l'époque et la technologie du moment :

| $n$ | 50 | 75 | 100 | 200 | 300 | 500 |
|---|---|---|---|---|---|---|
| $c(n)$ | $1{,}4.10^{10}$ | $9{,}0.10^{12}$ | $2{,}3.10^{15}$ | $1{,}2.10^{23}$ | $1{,}5.10^{29}$ | $1{,}3.10^{39}$ |
| $t(n)$ | 3,9 heures | 104 jours | 74 ans | $3{,}8.10^{9}$ ans | $34{,}9.10^{15}$ ans | $34{,}2.10^{25}$ ans |

Si l'on se fie à la « loi de Moore », selon laquelle la vitesse des machines double tous les dix-huit mois, il faudrait en 2014 plus de deux siècles pour factoriser un nombre de $200$ chiffres. La situation est bien différente. Dans le livre « Mathématiques et Technologie » de Christiane Rousseau et Yvan Saint-Aubin (Springer, collection SUMAT) on trouve (au chapitre 7, consacré à RSA) des informations plus récentes ; par exemple, des nombres de $130$ chiffres ont été factorisés en 1996, de $155$ chiffres en 1999, de $200$ chiffres en 2005. Le site `http://en.wikipedia.org/wiki/Integer_factorization` indique la factorisation en 2009 d'un entier de $232$ chiffres en deux ans à l'aide de centaines de machines ; et, en 2019, la factorisation en 2009 d'un entier de $240$ chiffres ayant coûté neuf cents années (cumulées) de calcul. Notons pour finir que factoriser $n$ n'est pas la seule attaque possible contre RSA, mais cela est une autre histoire …

## Exercice 9.

On tente d'attaquer RSA en factorisant $n$ de la manière suivante : on tire au hasard un entier $m \in \{1, \dots, n\}$ et l'on calcule (avec Bézout) le pgcd de $m$ et $n$. Que vaut cette méthode ?

***Solution.*** Le coût du calcul du pgcd n'est pas très élevé (voir [Knuth2]). Mais la probabilité d'obtenir un résultat est faible : en effet, il y a échec si $m \wedge n = 1$, donc avec probabilité $\dfrac{\varphi(n)}{n} = (1-1/p)(1-1/q)$. Si $p$ et $q$ sont grands, la probabilité de succès $1/p+1/q-1/pq$ est très faible. Il faudrait un très grand nombre d'essais pour avoir une chance de succès ; voir le calcul de l'espérance du temps de premier succès dans une suite de tirages de Bernoulli qui est ici :

$$\frac{1}{\frac{1}{p}+\frac{1}{q}-\frac{1}{pq}} = \frac{pq}{p+q-1}.$$

# 3 Résidus quadratiques

## 3.1 Carrés dans un corps fini

Soit $K$ un corps commutatif fini ; notons $p$ sa caractéristique et $q$ son cardinal. Nos applications concerneront uniquement le corps $\mathbb{Z}/p\mathbb{Z}$, (des corps finis plus généraux sont étudiés dans [MPA1]). Quelques propriétés élémentaires de $K$ sont démontrées à l'exercice I.1.32 de la page 71.

L'application $x \mapsto x^2$ définit un endomorphisme du groupe commutatif $K^*$, dont le noyau est $\{x \in K^* \mid x^2 = 1\}$, c'est-à-dire l'ensemble $\{+1, -1\}$ des racines du polynôme $X^2 - 1 = (X-1)(X+1)$. Si $K$ est de caractéristique $p = 2$, on a $+1 = -1$ et le noyau est trivial ; l'endomorphisme est alors injectif donc bijectif (puisque $K$ est fini). C'est un exemple d'« automorphisme de Frobenius », voir l'exercice I.1.32.

Nous supposerons désormais que la caractéristique $p$ de $K$ est un nombre premier impair. Le noyau $\{+1, -1\}$ de notre endomorphisme ayant 2 éléments, son image $K^{*2} := \{x^2 \mid x \in K^*\}$ est un sous-groupe d'indice 2 de $K^*$, donc a $(q-1)/2$ éléments ; on invoque le théorème d'isomorphisme $G/\operatorname{Ker} f \simeq \operatorname{Im} f$ (premier théorème d'isomorphisme pour les groupes, du module « Compléments d'algèbre » du livre [L2]).

D'après le théorème de Lagrange, tout $x \in K^*$ vérifie $x^{q-1} = 1$, donc $(x^2)^{(q-1)/2} = 1$. Donc les éléments de $K^{*2}$ sont tous racines du polynôme $X^{(q-1)/2} - 1$. Comme celui-ci admet au plus $(q-1)/2$ racines, $K^{*2}$ est exactement l'ensemble de ces racines.

**Proposition 18.**
L'endomorphisme $x \mapsto x^{(q-1)/2}$ de $K^*$ a pour noyau $K^{*2}$ et pour image $\{+1, -1\}$.

***Démonstration.*** L'assertion sur le noyau découle de la discussion précédente. Comme $(x^{(q-1)/2})^2 = x^{q-1} = 1$, on a $x^{(q-1)/2} = \pm 1$. Comme l'image a 2 éléments (encore en vertu du premier théorème d'isomorphisme), c'est $\{+1, -1\}$. ∎

---

**Exercice 10.**
Démontrer la proposition en utilisant seulement le fait que $K^*$ est cyclique.

***Solution.*** Cela revient à poser $n := q-1$, qui est pair : $n = 2m$, et à établir que dans $\mathbb{Z}/n\mathbb{Z}$ les endomorphismes $x \mapsto 2x$ et $x \mapsto mx$ ont chacun pour noyau l'image de l'autre, le premier noyau ayant 2 éléments et le deuxième $m$ éléments.

---

**Corollaire 19.** Pour tout $a \in K$, il existe $x, y \in K$ tels que $a = x^2 + y^2$.

***Démonstration.*** L'ensemble $K^2$ des $x^2$, $x \in K$, a $(q-1)/2 + 1 = (q+1)/2$ éléments (on compte ici le zéro). L'ensemble $a - K^2$ des $a - y^2$, $y \in K$, a donc également $(q+1)/2$ éléments. Comme $\operatorname{card} K^2 + \operatorname{card}(a - K^2) = q + 1 > \operatorname{card} K$, ces ensembles ne sont pas disjoints. ∎

***Exemple***. Les carrés de $(\mathbb{Z}/5\mathbb{Z})^*$ sont $\overline{1}$ et $\overline{4}$, ce sont également les éléments $x$ tels que $x^{(q-1)/2} = x^2 = 1$ (ici abréviation pour $\overline{1}$); alors que les non carrés $\overline{2}$ et $\overline{3}$ ont pour carré $-1$. Les carrés de $(\mathbb{Z}/7\mathbb{Z})^*$ sont $\overline{1}$, $\overline{2}$ et $\overline{4}$, ce sont également les éléments $x$ tels que $x^{(q-1)/2} = x^3 = 1$ ; alors que les non carrés $\overline{3}$, $\overline{5}$ et $\overline{6}$ ont pour cube $-1$.

## 3.2 Symbole de Legendre

**Définition 3.** Soit $p$ un nombre premier impair.
(i) On dit que $a \in \mathbb{Z} \setminus p\mathbb{Z}$ est *résidu quadratique modulo* $p$ s'il existe $b \in \mathbb{Z}$ tel que $a \equiv b^2 \pmod p$, autrement dit, si $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ est un carré.
(ii) Soit $a \in \mathbb{Z}$ quelconque. Le *symbole de Legendre* $\left(\frac{a}{p}\right) \in \mathbb{Z}$ est défini par les formules suivantes :

$$\left(\frac{a}{p}\right) := \begin{cases} 0 \text{ si } a \in p\mathbb{Z}, \\ +1 \text{ si } a \notin p\mathbb{Z} \text{ et } a \text{ résidu quadratique modulo } p, \\ -1 \text{ si } a \notin p\mathbb{Z} \text{ et } a \text{ non résidu quadratique modulo } p. \end{cases}$$

Il est clair que $\left(\frac{a}{p}\right)$ ne dépend que de la classe de $a$ modulo $p$ ; si $x \in \mathbb{Z}/p\mathbb{Z}$ désigne cette classe, on notera donc encore $\left(\frac{x}{p}\right) := \left(\frac{a}{p}\right)$.

***Exemple***. Pour que le nombre premier naturel $p \in \mathbb{N}^*$ reste premier dans $\mathbb{Z}[\sqrt{d}]$, il faut, et il suffit, que $\left(\frac{d}{p}\right) = -1$ (exercice 3 de la page 8).

**Théorème 20.** Soient $p$ premier impair et $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Alors :

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p.$$

***Démonstration.*** Soit $x \in (\mathbb{Z}/p\mathbb{Z})^*$ la classe de $a$. D'après la proposition 18 de la page précédente, $\left(\frac{x}{p}\right)$ vaut 1 si $x^{(p-1)/2} = 1$ et $-1$ si $x^{(p-1)/2} = -1$, autrement dit, $x^{(p-1)/2}$ est la classe de $\left(\frac{x}{p}\right)$ modulo $p$, ce qui équivaut à la relation à démontrer. ∎

**Corollaire 21.** Le symbole de Legendre est multiplicatif :

$$\forall a, b \in \mathbb{Z}\ ,\ \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

***Démonstration.*** Si $a, b \notin p\mathbb{Z}$ cela découle du théorème, sinon c'est immédiat. ∎

**Corollaire 22 (Euler).** On a $\left(\dfrac{-1}{p}\right) = (-1)^{(p-1)/2}$. Par conséquent, $-1$ est résidu quadratique, respectivement non résidu quadratique modulo $p$ si, et seulement si, $p \equiv 1 \pmod 4$, respectivement $p \equiv -1 \pmod 4$.

***Démonstration.*** Pour les nombres $\pm 1$, la congruence modulo $p \geqslant 3$ équivaut à l'égalité. Par ailleurs, la congruence $p \equiv \pm 1 \pmod 4$ traduit la parité de $(p-1)/2$.

Le corollaire dit que, pour que l'on puisse résoudre la congruence $a^2 + 1 \equiv 0 \pmod p$, il faut et il suffit que $p$ soit de la forme $4k+1$ ; mais il ne fournit pas de solution.

---

**Exercice 11.**
Si $p = 4k+1$, montrer que $a := (2k)!$ est solution. On rappelle le théorème de Wilson (module II.1 du livre [L1]) : si $p$ est premier, $(p-1)! \equiv -1 \pmod p$.

***Solution.*** Ici, $(p-1)! = (2k)!A$, où $A := \prod_{i=1}^{2k}(2k+i) \equiv \prod_{i=1}^{2k}(2k+i-p) \pmod p$ et $\prod_{i=1}^{2k}(2k+i-p) = \prod_{i=1}^{2k}(i-2k-1) = a$, d'où $(p-1)! \equiv a^2 \pmod p$, d'où $a^2 \equiv -1 \pmod p$ en vertu du théorème de Wilson.

---

Pour calculer $\left(\dfrac{2}{p}\right)$, nous ferons appel à un lemme dû à Gauß et qui nous servira aussi pour démontrer la loi de réciprocité quadratique. Écrivons $p = 2m+1$. Pour tout $a \in \mathbb{Z} \setminus p\mathbb{Z}$, le reste $b$ de la division euclidienne de $a$ par $p$ appartient à l'un des deux intervalles $E' := \{1, \dots, m\}$, $E'' := \{m+1, \dots, 2m\}$. Notons $r(a) := b$ si $b \in E'$ et $r(a) := b - p$ si $b \in E''$. L'entier $r(a)$ est caractérisé par les relations : $a \equiv r(a) \pmod p$ et $1 \leqslant |r(a)| \leqslant m$.

**Lemme 23 (Gauß).** Soient $a \in \mathbb{Z} \setminus p\mathbb{Z}$ et soit $\ell := \operatorname{card}\{i = 1, \dots, m \mid r(ia) < 0\}$. Alors :

$$\left(\frac{a}{p}\right) = (-1)^{\ell}.$$

***Démonstration.*** Le produit $\prod_{i=1}^{m}(ai)$ est égal à $m!a^m$, donc congru modulo $p$ à $m!\left(\dfrac{a}{p}\right)$ d'après le théorème 20 (puisque $m = (p-1)/2$). Mais $\prod_{i=1}^{m}(ai)$ est également congru modulo $p$ au produit $\prod_{i=1}^{m} r(ai)$, qui est égal à $(-1)^{\ell}\prod_{i=1}^{m}|r(ai)|$.

On remarque d'autre part que l'application $i \mapsto |r(ai)|$ de $E'$ dans lui-même est injective ; en effet, puisque $p$ ne divise pas $a$ :

$$r(ai) \equiv \pm r(aj) \pmod p \iff ai \equiv \pm aj \pmod p \iff i \equiv \pm j \pmod p \iff i = j,$$

pour $i, j \in E'$. Cette application est donc une permutation de $E'$ et $\prod_{i=1}^{m} |r(ai)| = m!$.

Des deux congruences ci-dessus, on déduit :

$$m!\left(\frac{a}{p}\right) \equiv (-1)^{\ell} m! \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) \equiv (-1)^{\ell} \pmod{p},$$

puisque $m!$ est inversible modulo $p$.

---

**Exercice 12.**

Calculer $\left(\frac{5}{7}\right)$ par cette méthode.

***Solution.*** Ici, $m = 3$. Les restes des divisions des $5i$ par $7$ pour $i = 1, \ldots, 6$ sont $5, 3, 1, 6, 4, 2$. Les $r(ai)$ sont $-2, 3, 1, -1, -3, 2$. Parmi les $m = 3$ premiers, *i.e.* ici les trois premiers, un seul est négatif, donc $\ell = 1$ et $\left(\frac{5}{7}\right) = -1$.

On le vérifie par la formule d'Euler : $5^{(7-1)/2} = 125 = 7 \times 18 - 1$, d'où $\left(\frac{5}{7}\right) = -1$.

---

On prend maintenant $a := 2$. On voit que $r(2i) = 2i$ si, et seulement si, $2i \leqslant m$, *i.e.* si $i \leqslant \lfloor m/2 \rfloor$ (partie entière de $m/2$). De même, $r(2i) = 2i - p$ si, et seulement si, $m < 2i \leqslant 2m$, *i.e.* si $\lfloor m/2 \rfloor < i \leqslant m$. Avec les notations du lemme, on a donc $\ell = m - \lfloor m/2 \rfloor = \lfloor (m+1)/2 \rfloor$ (le lecteur vérifiera sans peine que cette dernière égalité est vraie pour tout $m$).

**Corollaire 24 (Gauß).** On a $\left(\frac{2}{p}\right) = (-1)^{\lfloor (p+1)/4 \rfloor} = (-1)^{(p^2-1)/8}$ et les équivalences :

$$\left(\frac{2}{p}\right) = 1 \Longleftrightarrow p \equiv \pm 1 \pmod{8}, \quad \left(\frac{2}{p}\right) = -1 \Longleftrightarrow p \equiv \pm 3 \pmod{8}.$$

***Démonstration.*** Puisque $p = 2m + 1$, on a $(m+1)/2 = (p+1)/4$ et la première égalité résulte de l'étude précédente. Comme $(p^2 - 1)/8 = (m^2 + m)/2$, il reste à vérifier que cet entier et $\lfloor (m+1)/2 \rfloor$ ont même parité. Si $m = 2k$, leur différence vaut $2k^2$ ; si $m = 2k-1$, elle vaut $2k^2 - 2k$. La suite est alors immédiate par examen des quatre cas possibles.

## 3.3 Loi de réciprocité quadratique

Dans chacun des deux exemples traités complètement ($a = -1$ et $a = 2$), on voit que la condition $\left(\frac{a}{p}\right) = +1$, respectivement $\left(\frac{a}{p}\right) = -1$, organise l'ensemble des nombres premiers impairs en classes de congruence : modulo $4$ dans le premier cas, modulo $8$ dans le second cas. Voici un autre exemple, dans lequel nous répartissons les nombres premiers impairs (et non multiples de $3$) inférieurs à $100$ selon la valeur de $\left(\frac{3}{p}\right)$ :

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\left(\frac{3}{p}\right) = +1$ | 11 | 13 | 23 | 37 | 47 | 59 | 61 | 71 | 73 | 83 | 97 |
| $\left(\frac{3}{p}\right) = -1$ | 5 | 7 | 17 | 19 | 29 | 31 | 41 | 43 | 53 | 67 | 79 | 89 |

On constate que chacune des deux lignes s'organise en classes modulo $12$ : les classes $\pm\overline{1}$ dans la première ligne, les classes $\pm\overline{5}$ dans la deuxième.

**Un peu d'Histoire**

C'est ce genre d'observation qui conduisit Euler à formuler la loi de réciprocité quadratique, que démontra Gauß dans ses extraordinaires *Disquisitiones Arithmeticae*. Ce dernier y attachait tant d'importance qu'il en donna huit démonstrations. Cette importance fut confirmée par l'histoire ultérieure de la théorie des nombres : les « lois de réciprocité généralisées » donnèrent naissance à la théorie du corps de classes au début du XX$^{\text{e}}$ siècle, puis à une impressionnante extension non abélienne, le « programme de Langlands » qui est au cœur d'une grande partie des mathématiques contemporaines.

**Théorème 25 (Loi de réciprocité quadratique, Gauß).** Soient $p$, $q$ deux nombres premiers impairs distincts. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Notons que, chacun des trois facteurs présents valant $\pm 1$, on peut aussi bien écrire que le produit de deux quelconques d'entre eux est égal au troisième ou encore que le produit des trois vaut $+1$. De plus, $\frac{p-1}{2}\frac{q-1}{2}$ étant impair si, et seulement si, $p, q \equiv -1 \pmod 4$, la loi de réciprocité se traduit par :

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \qquad \text{sauf si } p, q \equiv -1 \pmod 4 \quad \text{auquel cas } \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Avant d'en donner la preuve, montrons comment ce théorème « explique » l'observation ci-dessus. Il nous dit que :

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}} \Longrightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

Le premier facteur $(-1)^{\frac{p-1}{2}}$ dépend de la classe de $p$ modulo $4$, le deuxième $\left(\frac{p}{3}\right)$ de sa classe modulo $3$ : le produit dépend donc bien de la classe modulo $12$.

**Exercice 13.**

Calculer $\left(\frac{3}{p}\right)$ dans tous les cas.

***Solution.*** Le facteur $(-1)^{\frac{p-1}{2}}$ vaut $+1$ si $p \equiv 1 \pmod 4$ et $-1$ si $p \equiv -1 \pmod 4$. Le facteur $\left(\frac{p}{3}\right) \equiv p^{(3-1)/2} \pmod 3$ vaut $+1$ si $p \equiv 1 \pmod 3$ et $-1$ si $p \equiv -1 \pmod 3$.

Ainsi $\left(\frac{3}{p}\right)$ vaut $+1$ si $p \equiv \pm 1 \pmod{12}$ et $-1$ dans les autres cas : c'est bien ce que nous avons observé.

---

***Démonstration de la loi de réciprocité quadratique***

Elle relève de la « géométrie des nombres » . Nous écrivons $p = 2k+1$, $q = 2l+1$ et :

$$m := \operatorname{card}\{i \in \{1,\dots,k\} \mid \exists r \in \{-k,\dots,-1\} \ : \ iq \equiv r \pmod{p}\},$$

$$n := \operatorname{card}\{j \in \{1,\dots,l\} \mid \exists s \in \{-l,\dots,-1\} \ : \ jp \equiv s \pmod{q}\},$$

de sorte que, d'après le lemme 23, $\left(\frac{q}{p}\right) = (-1)^m$ et $\left(\frac{p}{q}\right) = (-1)^n$.

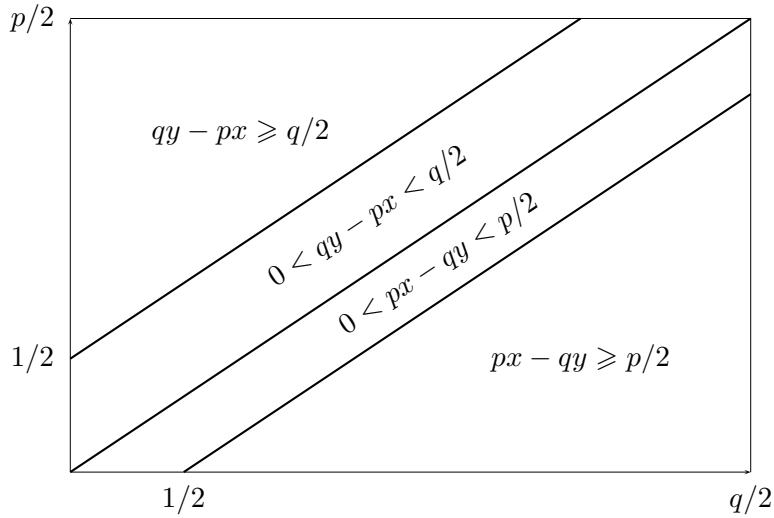
Si $i \in \{1,\dots,k\}$ appartient à l'ensemble à $m$ éléments ci-dessus, il existe un unique entier $j$ tel que $iq = jp + r$ et cet entier vérifie $1 \leqslant jp - iq \leqslant k$. Réciproquement, l'existence d'un tel $j$ garantit que $i$ est dans cet ensemble, qui est donc en bijection avec l'ensemble des couples $(i,j)$ d'entiers tels que $1 \leqslant i \leqslant k$, ce qui équivaut à $0 < i < p/2$ ; et $1 \leqslant jp - iq \leqslant k$, ce qui équivaut à $0 < jp - iq < p/2$. On déduit d'ailleurs de ces conditions que $0 < j < \frac{1}{p}(\frac{p}{2} + q\frac{p}{2}) = l+1$, donc que $0 < j < q/2$. Cela donne une nouvelle formule pour $m$ :

$$m = \operatorname{card}\{(i,j) \in \mathbb{N}^2 \mid 0 < i < p/2, 0 < j < q/2, 0 < jp - iq < p/2\}.$$

Symétriquement :

$$n = \operatorname{card}\{(i,j) \in \mathbb{N}^2 \mid 0 < i < p/2, 0 < j < q/2, 0 < iq - jp < q/2\}.$$

Le rectangle ouvert de $\mathbb{R}^2$ défini par les inégalités $0 < i < p/2$, $0 < j < q/2$ contient au total $kl$ points entiers. L'égalité à démontrer est $(-1)^m(-1)^n = (-1)^{kl}$ ; elle équivaut à la parité de $kl - (m+n)$, c'est-à-dire du nombre de points entiers du rectangle qui ne vérifient aucune des deux conditions $0 < jp - iq < p/2$, $0 < iq - jp < q/2$.



Comme, pour des points entiers, $jp - iq \geqslant p/2 \iff jp - iq \geqslant k+1$, etc, ceux de ces points qui sont situés hors des deux bandes jouxtant la première diagonale forment les deux triangles respectivement définis par les triples inégalités :

$$\big(jp - iq \geqslant k+1, i \geqslant 1, j \leqslant l\big) \text{ et } \big(iq - jp \geqslant l+1, j \geqslant 1, i \leqslant k\big).$$

Nous allons établir une bijection entre ces deux ensembles de points entiers, ce qui prouvera que leur réunion a un nombre pair d'éléments, donc que $kl - (m+n)$ est pair.

Pour cela nous introduisons l'involution $(i,j) \mapsto (i',j')$ de $\mathbb{R}^2$ (en fait une symétrie axiale) définie par $i + i' = k+1$, $j + j' = l+1$. Cette involution permute $\mathbb{Z}^2$ et transforme la première triple inégalité ci-dessus en la deuxième, et réciproquement ; en effet, il est évident que :

$$i \geqslant 1 \iff i' \leqslant k, \quad j \leqslant l \iff j' \geqslant 1, \quad jp - iq \geqslant k+1 \iff i'q - j'p \geqslant l+1,$$

cette dernière équivalence résultant de l'égalité :

$$(jp - iq) - (i'q - j'p) = (l+1)p - (k+1)q = k - l. \qquad \blacksquare$$

La loi de réciprocité quadratique peut fournir un moyen rapide de calculer les symboles de Legendre (la méthode sera encore perfectionnée plus loin grâce au symbole de Jacobi).

***Exemple***. On veut calculer $\left(\frac{37}{97}\right)$. Outre la loi de réciprocité, on utilisera la multiplicativité, le fait que $\left(\frac{a}{p}\right)$ ne dépend que de la classe de $a$ modulo $p$ et les valeurs spéciales $\left(\frac{-1}{p}\right)$ et $\left(\frac{2}{p}\right)$ :

$$\left(\frac{37}{97}\right) = (-1)^{\frac{37-1}{2}\frac{97-1}{2}}\left(\frac{97}{37}\right) = \left(\frac{97}{37}\right) = \left(\frac{60}{37}\right) = \left(\frac{4}{37}\right)\left(\frac{3}{37}\right)\left(\frac{5}{37}\right).$$

On a bien entendu $\left(\frac{4}{37}\right) = +1$ (tout carré est un résidu quadratique). On a déjà vu que $\left(\frac{3}{37}\right) = +1$. Il reste à calculer :

$$\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

pour conclure que $\left(\frac{37}{97}\right) = -1$.

## 3.4 Symbole de Jacobi

Le symbole de Jacobi est une généralisation du symbole de Legendre qui facilite les calculs, mais qui a de plus sa propre importance dans les tests de primalité, ce dont nous donnerons un exemple à la section 5. Soient $a \in \mathbb{Z}$ quelconque et $n = p_1^{r_1} \cdots p_k^{r_k}$ la décomposition

en facteurs premiers d'un entier naturel impair $n$. Le symbole de Jacobi est défini par la formule :

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{r_i}.$$

De manière équivalente : $\left(\frac{a}{1}\right) = 1$, $\left(\frac{a}{p}\right)$ est identique au symbole de Legendre quand $p$ est premier impair, et $\left(\frac{a}{nn'}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{n'}\right)$ quels que soient $n, n'$ impairs.
C'est donc un élément de $\{-1, 0, +1\}$ qui s'annule si, et seulement si, $a$ et $n$ ont un diviseur commun non trivial. Des propriétés analogues du symbole de Legendre, on déduit que $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ et que $a \equiv a' \pmod{n} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{a'}{n}\right)$.

**Proposition 26.**
(i) On a les formules :

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2} \qquad \text{et} \qquad \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}.$$

(ii) Si $m$ et $n$ sont tous deux impairs, on a la formule de réciprocité :

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

***Démonstration.*** (i) Chaque formule est vraie lorsque $n$ est premier. Il suffit donc de montrer que, si elle est vraie pour $n$ et $n'$, elle l'est encore pour $nn'$. Comme le membre gauche est multiplicatif en $n$, il suffit de vérifier que le membre droit l'est. Cela équivaut à la parité des expressions $(nn'-1)/2 - (n-1)/2 - (n'-1)/2$ et $(n^2n'^2-1)/8 - (n^2-1)/8 - (n'^2-1)/8$. Remplaçant $n$ par $2k+1$ et $n'$ par $2k'+1$, on voit que ces expressions valent respectivement $2kk'$ et $2(k^2+k)(k'^2+k')$, ce qui achève la preuve.

(ii) On utilise d'abord la multiplicativité en $n$ des deux fonctions $\left(\frac{m}{n}\right)$ et $\left(\frac{n}{m}\right)$ (à $m$ fixé) pour se ramener au cas où $n$ est premier. Pour cela, comme en (i), il suffit de vérifier la parité de $\frac{m-1}{2}\frac{nn'-1}{2} - \frac{m-1}{2}\frac{n-1}{2} - \frac{m-1}{2}\frac{n'-1}{2}$ lorsque $m, n, n'$ sont impairs. On écrit donc $n = 2k+1$ et $n' = 2k'+1$, et l'on trouve $(m-1)kk'$ qui est bien pair puisque $m$ est impair. De la même manière on se ramène ensuite au cas où $m$ est premier. On n'a plus alors qu'à invoquer la loi de réciprocité quadratique pour le symbole de Legendre. ∎

### *Lien du symbole de Jacobi avec les résidus quadratiques*

Si $m$ est résidu quadratique (c'est-à-dire congru à un carré) modulo $n$, on voit facilement que $\left(\frac{m}{n}\right) = 1$. La réciproque est évidemment vraie si $n$ est premier, mais pas en général.

**Exercice 14.**
Vérifier que $\left(\frac{20}{21}\right) = 1$ mais que $20$ n'est pas résidu quadratique modulo $21$.

***Solution.*** En utilisant toutes les multiplicativités :

$$\left(\frac{20}{21}\right) = \left(\frac{4}{21}\right)\left(\frac{5}{21}\right) = \left(\frac{5}{21}\right) = \left(\frac{5}{3}\right)\left(\frac{5}{7}\right) = 1,$$

par calcul direct de $\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$ et d'après un calcul antérieur de $\left(\frac{5}{7}\right) = -1$.

Cependant $\left(\frac{20}{3}\right) = \left(\frac{2}{3}\right) = -1$, donc $20$ n'est pas résidu quadratique modulo $3$ et *a fortiori* il ne l'est pas modulo $21$. De même $\left(\frac{20}{7}\right) = \left(\frac{-1}{7}\right) = -1$.

De la même manière, on n'a pas nécessairement $\left(\frac{m}{n}\right) \equiv m^{(n-1)/2} \pmod{n}$. En fait, $m^{(n-1)/2}$ n'est même pas nécessairement congru à $\pm 1$ modulo $n$, comme on le voit par exemple en prenant $m = 2$ et $n = 15$. Cependant, les cas d'égalité jouent un rôle crucial dans le test de primalité de Solovay-Strassen, que nous étudierons à la section 5, en vertu du résultat suivant :

**Théorème 27.** Si l'entier impair $n$ est tel que $\left(\frac{m}{n}\right) \equiv m^{(n-1)/2} \pmod{n}$ pour tout entier $m$ tel que $m \wedge n = 1$, alors $n$ est premier.

***Démonstration.*** En élevant la relation au carré, on voir que tout élément $x \in (\mathbb{Z}/n\mathbb{Z})^*$ vérifie $x^{n-1} = 1$ (autrement dit, $n$ est un nombre de Carmichael, voir la proposition 39 de la page 43). Si $p^2$ divisait $n$, alors la composante $(\mathbb{Z}/p^r\mathbb{Z})^*$ de $(\mathbb{Z}/n\mathbb{Z})^*$, qui a $p^{r-1}(p-1)$ éléments avec $r - 1 \geqslant 2$, admettrait un élément d'ordre $p$ ; or $p$ ne divise par $n - 1$, contredisant l'égalité ci-dessus.

Donc $n = p_1 \cdots p_k$ (premiers distincts). Si $k \geqslant 1$, à l'aide du lemme chinois, on peut trouver $a \in \mathbb{Z}$ tel que $a \equiv 1 \pmod{p_2 \cdots p_k}$ et $a$ non résidu modulo $p_1$.

Alors $\left(\frac{a}{p_1}\right) = -1$, $\left(\frac{a}{p_2 \cdots p_k}\right) = 1$, donc $\left(\frac{a}{n}\right) = -1$, donc (par l'hypothèse faite sur $n$) $a^{(n-1)/2} \equiv -1 \pmod{n}$, donc $a^{(n-1)/2} \equiv -1 \pmod{p_2 \cdots p_k}$, ce qui est impossible puisque $a \equiv 1 \pmod{p_2 \cdots p_k}$. ∎

# 4 Sommes de deux carrés

## 4.1 Rappels sur l'anneau des entiers de Gauß

C'est le sous-anneau de $\mathbb{C}$ engendré par $\mathrm{i}$ :

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}.$$