ALGÈBRE - LEÇON 120 : ANNEAUX $\mathbb{Z}/n\mathbb{Z}$. APPLICATIONS

SIMON RICHE

1. Commentaires du jury (rapport 2024)

Il est attendu de construire rapidement $\mathbf{Z}/n\mathbf{Z}$, puis d'en décrire les éléments inversibles, les diviseurs de zéro et les idéaux. Ensuite, le cas où l'entier n est un nombre premier doit être étudié. La fonction indicatrice d'Euler ainsi que le théorème chinois et sa réciproque sont incontournables. Il est naturel de s'intéresser à la résolution de systèmes de congruences.

Les applications sont très nombreuses. Les candidates et candidats peuvent, par exemple, choisir de s'intéresser à la résolution d'équations diophantiennes (par réduction modulo n bien choisi) ou bien au cryptosystème RSA. Si des applications en sont proposées, l'étude des morphismes de groupes de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/m\mathbf{Z}$ ou le morphisme de Frobenius peuvent figurer dans la leçon.

Pour aller plus loin, les candidates et candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, s'intéresser au calcul effectif des racines carrées dans $\mathbf{Z}/n\mathbf{Z}$, au logarithme discret, ou à la transformée de Fourier rapide.

2. Plan

2.1. **Ce qui doit apparaître.** Construction de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Description des diviseurs de 0.

Description des éléments inversibles, fait que ces éléments sont aussi les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$. Calcul de l'inverse via l'algorithme d'Euclide.

Lien avec les automorphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Description des sous-groupes, des idéaux. Lesquels sont premiers, maximaux.

Cas n premier.

Théorème chinois (et sa réciproque).

Calcul explicite de l'isomorphisme inverse.

Indicatrice d'Euler, formule pour la calculer.

Description [1] des groupes $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ puis $(\mathbb{Z}/n\mathbb{Z})^\times$.

Petit théorème de Fermat.

Théorème d'Euler.

Théorème de Wilson.

Critères d'irréductibilité de polynômes par réduction modulo n (notamment Eisenstein).

Date: Année 2024–2025.

1. Rappelons que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$ si p est impair ou $p = 2$ et $\alpha \in \{1, 2\}$, et que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$ si $\alpha \geq 3$, cf. [Pe, Chap. I, §7]. La preuve de ces résultats permet de rendre ces isomorphismes relativement explicites, ce qui peut s'avérer utile également.

Résolution d'équations $ax + by = c$.
Résolution de systèmes de congruences.

Système de cryptographie RSA.

2.2. **Ce qui peut apparaître.** Exemples d'équations diophantiennes.

Classification des groupes abéliens finis.

Description des éléments nilpotents dans $\mathbb{Z}/n\mathbb{Z}$.
Description des idempotents dans $\mathbb{Z}/n\mathbb{Z}$. [2]

Morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/m\mathbb{Z}$.

Symbole de Legendre.
Loi de réciprocité quadratique.

Polynômes cyclotomiques.

Théorème de Wedderburn sur les sous-groupes finis de $\mathbb{K}^\times$.

Théorème de Sophie Germain.

Test de primalité de Miller–Rabin.

Transformation de Fourier rapide [3].

3. Quelques questions bêtes auxquelles il faut absolument savoir répondre rapidement

(1) Déterminer les entiers n tels que 17 est inversible dans $\mathbb{Z}/n\mathbb{Z}$.
(2) Quels sont les quotients du groupe $\mathbb{Z}/n\mathbb{Z}$?
(3) Expliquer les critères de divisibilité par 9 et par 11.
(4) À quelle condition existe-t-il un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/m\mathbb{Z}$? Dans ce cas, combien en existe-t-il ?
(5) Calculer l'inverse de 17 dans $\mathbb{Z}/36\mathbb{Z}$.

4. Exercices

4.1. **Quelques exercices faciles ou classiques.**

Exercice 1. Montrer que dans un anneau fini, un élément non nul est soit inversible, soit diviseur de 0. (*Indication* : on pourra considérer le morphisme de multiplication par cet élément.)

Exercice 2. Décrire les représentations complexes du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Même chose pour le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$.

Exercice 3. Combien existe-t-il de morphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$ vers le groupe des racines n-ièmes de l'unité dans $\mathbb{C}$? Combien sont des isomorphismes ?
Même question avec un corps algébriquement clos de caractéristique $p > 0$.

Exercice 4. (1) Soit G un groupe, et Z son centre. Montrer que si G/Z est cyclique, alors G est abélien.

2. Voir l'Exercice 5.
3. Voir par exemple [CG, Chap. XIII, Exercice E.10].

(2) En déduire que si p est premier, un groupe d'ordre p^2 est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$, soit à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. (Indication : on pourra considérer l'action de G sur lui-même par conjugaison pour vérifier qu'un tel groupe a un centre non trivial.)

Référence : [Pe, Chap. I, Ex. A.4].

4.2. **Inversibles de $\mathbb{Z}/n\mathbb{Z}$.**

Exercice 5. Déterminer les idempotents de l'anneau $\mathbb{Z}/n\mathbb{Z}$. (*Indication* : on pourra utiliser le théorème chinois pour se ramener au cas où n est une puissance d'un nombre premier.)

Référence : voir la fiche de J. Germoni citée à la partie 6.

Exercice 6. (1) Si $n, m \geq 1$, rappeler à quelle condition le groupe $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ est cyclique.

(2) En déduire les valeurs de n pour lesquelles le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est cyclique.

Exercice 7. On fixe $n, m \geq 1$ avec $m \mid n$.

(1) Montrer que le morphisme naturel $f_{n,m} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ induit un morphisme de groupes *surjectif* $g_{n,m} : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$. (*Indication* : on pourra se ramener au cas où n est une puissance d'un nombre premier.)

(2) Montrer qu'il existe n_1, n_2 tels que $n = n_1 n_2$, les diviseurs premiers de n_1 sont les mêmes que ceux de m, et $\mathrm{pgcd}(n_1, n_2) = 1$. Montrer qu'on a alors $m \mid n_1$, et que

$$\ker(g_{n,m}) \cong \ker(g_{n_1,m}) \times (\mathbb{Z}/n_2\mathbb{Z})^\times,$$

où $g_{n_1,m}$ est le morphisme similaire à $g_{n,m}$ pour n_1 et m.

(3) On suppose que tout diviseur premier de n divise également m, et on note $q = n/m$. Montrer que

(a) si $8 \nmid n$ ou $4 \mid m$, alors $\ker(g_{n,m}) \cong \mathbb{Z}/q\mathbb{Z}$;

(b) si $8 \mid n$ et $4 \nmid m$, alors $\ker(g_{n,m}) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/(q/2)\mathbb{Z}$.

(*Indication* : on pourra se ramener au cas où n est une puissance d'un nombre premier, puis utiliser la description de $(\mathbb{Z}/n\mathbb{Z})^\times$ dans ce cas, cf. [Pe, Chap. I, §7].)

Cet exercice est copié de `https://perso.univ-rennes1.fr/matthieu.romagny/agreg/exo/reduction_des_inversibles_modulo_n.pdf` (qui malheureusement ne contient pas de correction).

Exercice 8. Soient $k, n \geq 2$ deux entiers.

(1) On suppose n impair. Montrer que l'application $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ donnée par $x \mapsto x^k$ est bijective si et seulement si pour tout facteur premier p de n on a $\mathrm{pgcd}(k, p(p-1)) = 1$ si $p^2 \mid n$, et $\mathrm{pgcd}(k, p-1) = 1$ sinon.

(2) Montrer que l'application $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ donnée par $x \mapsto x^k$ est bijective si et seulement si pour tout facteur premier p de n on a $p^2 \nmid n$ et $\mathrm{pgcd}(k, p-1) = 1$.

Référence : pour (2), voir le §2.1 dans la fiche de M. Romagny citée dans la partie 6.

Exercice 9 (Nombres de Carmichael)**.** Un entier n non premier est dit *nombre de Carmichael* si l'application $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ donnée par $x \mapsto x^n$ est l'identité, c'est-à-dire si n divise $a^n - a$ pour tout $a \in \mathbb{Z}$ premier à n. [4]

(1) Montrer qu'aucun entier pair (non premier) n'est un nombre de Carmichael. (*Indication* : on pourra considérer l'entier $a = -1$.)
(2) Dans cette question on veut montrer que si n est un nombre de Carmichael alors pour tout facteur premier impair p de n on a $p^2 \nmid n$ et $p - 1 \mid n - 1$. On suppose donc que n est un nombre de Carmichael, et on fixe un tel facteur premier, et on note r la valuation p-adique de n.
   (a) Montrer qu'il existe $a \in \mathbb{Z}$ que a engendre $(\mathbb{Z}/p^r\mathbb{Z})^\times$ et a est premier à n. (*Indication* : théorème chinois.)
   (b) En déduire que $(p-1)p^r$ divise $n - 1$.
   (c) Conclure.
(3) Réciproquement, supposons maintenant que $n = p_1 \cdots p_r$ où les p_i sont des nombres premiers impairs distincts, que de plus $p_i - 1$ divise $n - 1$ pour tout i. Dans cette question on va montrer que pour tout $a \in \mathbb{Z}$ l'entier n divise $a^n - a$ (ce qui montrera en particulier que n est un nombre de Carmichael si $r \geq 2$). On fixe donc $a \in \mathbb{Z}$.
   (a) Montrer que p_i divise $a^n - a$ pour tout $i \in \{1, \dots, r\}$.
   (b) Conclure.
(4) Montrer qu'aucun produit de 2 nombres premiers n'est un nombre de Carmichael. (*Indication* : on pourra utiliser la formule $pq - 1 = p(q-1) + (p-1)$.)

Le plus petit entier qui est un nombre de Carmichael est $561 = 3 \times 11 \times 17$. Pour d'autres exemples, on pourra consulter Wikipédia.

4.3. **Matrices à coefficients dans $\mathbb{Z}/n\mathbb{Z}$.** Si A est un anneau commutatif, et $n \in \mathbb{Z}_{\geq 1}$, on note $\mathrm{M}_n(A)$ l'ensemble des matrices carrées de taille n à coefficients dans A. On rappelle que cet ensemble est une A-algèbre pour les lois définies comme suit :

— si $B = (b_{i,j})_{1 \leq i,j \leq n}$ et $\lambda \in A$, la matrice $\lambda \cdot B$ a pour coefficient d'indice (i,j) l'élément $\lambda b_{i,j}$;
— si $B = (b_{i,j})_{1 \leq i,j \leq n}$ et $C = (c_{i,j})_{1 \leq i,j \leq n}$, la matrice $B + C$ a pour coefficient d'indice (i,j) l'élément $b_{i,j} + c_{i,j}$;
— si $B = (b_{i,j})_{1 \leq i,j \leq n}$ et $C = (c_{i,j})_{1 \leq i,j \leq n}$, la matrice $B + C$ a pour coefficient d'indice (i,j) l'élément $\sum_{k=1}^n b_{i,k} \cdot c_{k,j}$.

L'élément neutre est la matrice identité I_n. On note $\mathrm{GL}_n(A)$ le groupe des inversibles de l'anneau $\mathrm{M}_n(A)$.

math On rappelle les faits suivants. [5]

4. Notons que tout nombre premier p vérifie la propriété que $p \mid a^p - a$ pour tout $a \in \mathbb{Z}$ premier à p (et même pour tout $a \in \mathbb{Z}$ en fait), par le théorème de Lagrange. Un nombre de Carmichael est donc un entier non premier "qui se comporte comme s'il était premier" en un certain sens. Notons également que cette condition revient à se demander quand, dans le cas $k = n$ du contexte de l'Exercice 8, l'application considérée est l'identité.

5. Pour des détails, voir les notes du cours de Julien Bichon. La preuve des propriétés (2) et (3) peuvent également se ramener au cas (bien connu) où A est un corps de la façon suivante. On commence par les vérifier d'abord dans le cas où A est un anneau de polynômes (à plusieurs variables) à coefficients entiers, en utilisant l'inclusion de cet anneau (intègre) dans son corps des fractions. Puis on utilise le fait que si A est un anneau commutatif et $a_1, \dots, a_r$ sont des éléments de A, il existe un unique morphisme d'anneaux $\mathbb{Z}[X_1, \dots, X_r] \to A$ envoyant chaque X_i sur a_i.

(1) Si A et A' sont des anneaux commutatifs et $\varphi : A \to A'$ est un morphisme d'anneaux, alors pour tout $n \geq 1$ il existe un morphisme natural d'anneaux $\mathrm{M}_n(A) \to \mathrm{M}_n(A')$, qui envoie la matrice $(b_{i,j})_{1\leq i,j\leq n}$ sur la matrice $(\varphi(b_{i,j}))_{1\leq i,j\leq n}$.

(2) Pour tout anneau commutatif A et tout $n \geq 1$ il existe un morphisme d'anneau $\det : \mathrm{M}_n(A) \to A$, qui envoie la matrice $(b_{i,j})_{1\leq i,j\leq n}$ sur l'élément $\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^n b_{\sigma(i),i}$.

(3) Si $B \in \mathrm{M}_n(A)$, on définit la comatrice $\mathrm{Com}(B)$ de B comme la matrice dont le terme d'indice (i, j) est $(-1)^{i+j} \det(B_{i,j})$ où $B_{i,j}$ est la matrice obtenue à partir de B en supprimant la i-ème ligne et la j-ème colonne. Alors on a

$$B \cdot {}^t\mathrm{Com}(B) = {}^t\mathrm{Com}(B) \cdot B = \det(B) \cdot \mathrm{I}_n.$$

Exercice 10. Soit A un anneau commutatif et $n \geq 1$.

(1) Rappeler pourquoi une matrice $M \in \mathrm{M}_n(A)$ appartient à $\mathrm{GL}_n(A)$ si et seulement si $\det(M)$ est inversible dans A.

(2) Soit p un nombre premier, et $\alpha \geq 1$.

(a) On considère le morphisme d'anneaux

$$\varphi : \mathrm{M}_n(\mathbb{Z}/p^\alpha\mathbb{Z}) \to \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$$

induit par le morphisme naturel $\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Montrer que si $M \in \mathrm{M}_n(\mathbb{Z}/p^\alpha\mathbb{Z})$, M est inversible si et seulement si $\varphi(M)$ est inversible.

(b) En déduire que

$$\#\mathrm{GL}_n(\mathbb{Z}/p^\alpha\mathbb{Z}) = p^{(\alpha-1)n^2}(p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}).$$

(*Indication* : on pourra montrer que le morphisme

$$\mathrm{GL}_n(\mathbb{Z}/p^\alpha\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$$

induit par φ est surjectif, puis décrire son noyau.)

(3) Montrer que si $m = \prod_i p_i^{\alpha_i}$ est la décomposition de m en produit de facteurs premiers, on a un isomorphisme de groupes

$$\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z}) \cong \prod_i \mathrm{GL}_n(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}).$$

En déduire $\#\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$.

Référence : voir le §3.1 dans la fiche de M. Romagny citée dans la partie 6. Le cas très similaire du groupe $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ est traité également (de manière similaire) dans [FGN2, Correction de l'Ex. 3.23, p. 207].

Exercice 11. On rappelle que pour un anneau A, $\mathrm{GL}_n(A)$ est le groupe des matrices $n \times n$ de déterminant inversible dans A (cf. Exercice 10), et $\mathrm{SL}_n(A)$ est le sous-groupe des matrices de déterminant 1.

(1) Montrer que pour tout $m \geq 2$, le morphisme naturel $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ induit des morphismes de groupes $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$ et $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$.

(2) Montrer que si $m \geq 5$, le morphisme $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$ n'est pas surjectif. (*Indication* : on pourra remarquer que sous notre hypothèse on a $\{\pm 1\} \subsetneq (\mathbb{Z}/m\mathbb{Z})^\times$.)

(3) Le but de cette question est de montrer que si $m \geq 2$, toute matrice de $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ est produit de matrices de la forme

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

(a) Soit $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. En considérant le produit

$$\begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix} \begin{pmatrix} 1 & -1+a^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

montrer le résultat pour la matrice $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$.

(b) Considérons une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ avec a inversible. En considérant le produit

$$\begin{pmatrix} 1 & 0 \\ -a^{-1}c & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

montrer le résultat pour la matrice M.

(c) On considère finalement une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ avec a non inversible. Soit α un entier dont la classe dans $\mathbb{Z}/m\mathbb{Z}$ est a, soient $p_1, \cdots, p_r$ les diviseurs premiers communs à α et m, et soient $q_1, \cdots, q_s$ les autres diviseurs premiers de m. Montrer que l'image de c dans $\mathbb{Z}/p_i\mathbb{Z}$ est non nulle pour tout i, puis que $a + (\prod_j q_j)c$ est inversible dans $\mathbb{Z}/m\mathbb{Z}$. En considérant le produit

$$\begin{pmatrix} 1 & \prod_j q_j \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

montrer le résultat pour M.

(4) En utilisant la question précédente, montrer que le morphisme $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ est surjectif.

Référence : [FGN2, Ex. 3.23]. Pour une généralisation de la dernière propriété à $\mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$ pour tout n, voir le §3.2 dans la fiche de M. Romagny citée dans la partie 6.

4.4. **Équations diophantiennes.**

Exercice 12. Montrer que l'équation

$$x^3 + 5 = 117y^3$$

n'a pas de solutions entières. (*Indication* : on pourra réduire modulo 9.)

Exercice 13. Montrer que l'équation

$$6n^2 + 5n + 1 = 0$$

admet une solution dans chaque $\mathbb{Z}/p\mathbb{Z}$ (p premier), mais pas dans $\mathbb{Z}$. (*Indication* : on pourra utiliser la méthode habituelle de résolution des équations de degré 2, qui est valable dans tout corps de caractéristique $\neq 2$.)

Référence : [FGN1, Ex. 4.7].

Exercice 14. Déterminer les entiers k tels que

$$39k^2 + 3k - 77 = 0 \mod 385.$$

(*Indication* : on pourra écrire 385 comme produit de puissances de nombres premiers, puis utiliser le théorème chinois.)

Référence : [Co, Ex. 12-13, Solution p. 284-285].

Exercice 15. (1) Montrer que l'équation

$$n^2 - 23m = 329$$

n'a pas de solution entière. (Indication : on pourra réduire modulo 23.)

(2) Montrer que pour tout $a \in \mathbb{Z}$, l'équation

$$n^3 - 23m = a$$

admet des solutions entières. (*Indication* : on pourra étudier l'application de $\mathbb{Z}/23\mathbb{Z}$ dans lui-même donnée par $x \mapsto x^3$.)

Référence : [Co, Ex. 12-10, Solution p. 283].

Exercice 16. Soit p un entier premier congru à 3 modulo 4.

(1) Montrer que si $x, y, z \in \mathbb{Z}$ vérifient

$$x^2 + y^2 = pz^2,$$

alors x, y et z sont divisibles par p. (Indication : on rappelle que -1 n'est pas un carré modulo p.)

(2) En déduire que l'équation

$$x^2 + y^2 = pz^2$$

n'a pas de solution entière.

Référence : [Co, p. 275].

5. Complément : tests de primalité

Référence : [De, §§2.4.6, 2.4.7, 3.3.6].

5.1. **Tests "stupides".** On dit qu'un entier est *composé* s'il n'est pas premier. Pour tester si un entier est premier ou composé, on peut procéder des façons suivantes :

(1) Tester, pour tout entier $1 \leq a \leq \sqrt{n}$, si a et n sont premiers entre eux (en utilisant par exemple l'algorithme d'Euclide). (En effet n est composé si et seulement si il existe un tel entier.) Problème : si par exemple $n = pq$ avec p et q premiers, il existe "peu" d'entiers non premiers avec n.

(2) Tester s'il existe a avec $1 \leq a \leq n$ tel que $a^{n-1} \not\equiv 1 \mod n$. (En effet, le petit théorème de Fermat garantit que n est composé si et seulement si il existe un tel entier.) Dans la pratique il y a souvent de tels entiers "a" qui sont petits. Mais il peut aussi arriver que seuls les entiers non premiers à n satisfont ces conditions ; ce test n'est pas meilleur que le précédent dans ces cas-là.

(3) Supposons que n est impair. Tester s'il existe a avec $1 \leq a \leq n$ tel que $a^{\frac{n-1}{2}} \not\equiv \pm 1 \mod n$. (Encore une fois, cette condition est satisfaite si et seulement si n est composé.) Ce test résoud parfois les problèmes du précédent, mais pas toujours.

5.2. **Le critère de Miller–Rabin.** Ce test est basé sur le résultat suivant.

Proposition 1. Soit $n > 1$ un entier impair, et écrivons $n = 1 + 2^s t$ avec t impair. Alors n est composé si et seulement si il existe un entier $a \in \{2, 3, \cdots, n-1\}$ tel que

$$a^t \not\equiv 1 \mod n \quad \text{et} \quad a^{2^i t} \not\equiv -1 \mod n \text{ pour tout } i \in \{0, \cdots, s-1\}.$$

Démonstration. Si n est composé et a est un diviseur non trivial de n, alors aucune des puissances de a ne peut être congrue à ± 1 modulo n, puisque a n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Supposons maintenant que n est premier, et montrons qu'il n'existe pas d'entier a qui vérifie les conditions ci-dessus. Supposons donc $1 < a < n$, et pour $i \in \{0, \cdots, s\}$ notons a_i la classe de $a^{2^i t}$ modulo n. On sait que $a_s = a^{n-1} = 1$ par le petit théorème de Fermat. Donc soit $a_0 = 1$ (auquel cas on a gagné), soit il existe $i \in \{0, \cdots, s-1\}$ tel que $a_{i+1} = 1$ et $a_i \neq 1$. Alors on a $(a_i)^2 = a_{i+1} = 1$, d'où $a_i = -1$ puisque $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

Un entier a qui vérifie les conditions précédentes est appelé un *témoin de Miller*. On a donc démontré qu'un entier n est composé si et seulement si il admet un témoin de Miller. L'intérêt de cette notion est que si n est composé il admet *beaucoup* de témoins de Miller, comme expliqué dans le Théorème 1 ci-dessous, de sorte que si un entier choisi au hasard n'est pas un témoin de Miller, on a de bonnes chances que n soit premier. On obtient ainsi un test "probabiliste" de primalité. (Dans la pratique, on prendra *plusieurs* entiers au hasard entre 1 et n, dont on regardera s'ils sont des témoins de Miller ou non, pour déterminer "avec une bonne probabilité" si l'entier est premier ou non.)

Théorème 1. Si n est un entier impair composé, au moins $3/4$ des entiers a tels que $1 < a < n$ sont des témoins de Miller de n.

En fait, si on écrit $n = 1 + 2^s t$ avec t impair, il existe au plus $\varphi(n)/4$ entiers a tels que $1 < a < n$ et qui vérifient

$$a^t \equiv 1 \mod n \quad \text{ou} \quad a^{2^i t} \equiv -1 \mod n \text{ pour un } i \in \{0, \cdots, s-1\}.$$

Comme $\varphi(n) \leq n - 2 = \#\{a \in \mathbb{Z} \mid 1 < a < n\}$ pour n composé, la deuxième affirmation implique bien la première.

5.3. **Préliminaires sur les groupes cycliques.** On commence par deux lemmes.

Lemme 1. Soit G un groupe cyclique d'ordre r. Si $m \in \mathbb{Z}$ et $g \in G$, l'équation $x^m = g$ a des solutions si et seulement si $g^{r/\mathrm{pgcd}(m,r)} = e$. Si cette condition est satisfaite, le nombre de solutions est $\mathrm{pgcd}(m, r)$.

Démonstration. On peut supposer que $G = \mathbb{Z}/r\mathbb{Z}$. Si g est la classe de l'entier q, on cherche alors à quelle condition il existe un entier y tel que

$$m \cdot y \equiv q \mod r,$$

c'est-à-dire à quelle condition il existe des entiers y, z tels que

$$my + zr = q.$$

Il est bien connu que de tels entiers existent si et seulement si $\mathrm{pgcd}(m, r) \mid q$, c'est-à-dire si et seulement si r divise $rq/\mathrm{pgcd}(m, r)$, ce qui revient à dire que $g^{r/\mathrm{pgcd}(m,r)} = e$.

Si cette condition est satisfaite, on peut écrire

$$m = \mathrm{pgcd}(m,r)m', \quad r = \mathrm{pgcd}(m,r)r', \quad q = \mathrm{pgcd}(m,r)q'.$$

Alors notre équation devient

$$\mathrm{pgcd}(m,r)m'y \equiv \mathrm{pgcd}(m,r)q' \mod \mathrm{pgcd}(m,r)r',$$

c'est-à-dire

$$m'y \equiv q' \mod r'.$$

Puisque m' est inversible modulo r', cette équation détermine la classe de y dans $\mathbb{Z}/r'\mathbb{Z}$. Il reste à relever cette classe dans $\mathbb{Z}/r\mathbb{Z}$, ce qui peut se faire de $\mathrm{pgcd}(m,r)$ façons différentes. □

Lemme 2. Soit G un groupe cyclique d'ordre $r = 2^u v$ avec v impair et $u \geq 1$, et soit $t \geq 1$ impair.

(1) Le nombre de solutions de l'équation $x^t = e$ dans G est $\mathrm{pgcd}(t,v)$.
(2) Soit $s \geq 1$, soit $\alpha \in G$ un élément d'ordre 2, soit $j \leq s$, et notons $k = \min(u,s)$. Si $1 \leq j \leq k$, alors le nombre de solutions de l'équation $x^{2^{j-1}t} = \alpha$ est $2^{j-1} \cdot \mathrm{pgcd}(t,v)$. Si $j > k$, cette équation n'a pas de solution.

Démonstration. (1) Notre équation admet au moins une solution ($x = e$). D'après le Lemme 1, le nombre de solutions est $\mathrm{pgcd}(t,r) = \mathrm{pgcd}(t,v)$.

(2) D'après le Lemme 1, l'équation admet une solution si et seulement si on a $\alpha^{r/\mathrm{pgcd}(2^{j-1}t,r)} = 1$, c'est-à-dire si et seulement si $2 \mid r/\mathrm{pgcd}(2^{j-1}t,r)$, c'est-à-dire si et seulement si $j \leq u$. Si cette condition est satisfaite le nombre de solutions est $\mathrm{pgcd}(2^{j-1}t,r) = 2^{j-1} \cdot \mathrm{pgcd}(t,v)$. □

5.4. **Démonstration du Théorème.** On peut finalement démontrer le Théorème 1.

Preuve du Théorème 1. Si $n = 9$, seul $a = 8$ vérifie les conditions du théorème, ce qui permet de conclure puisque $\varphi(9) = 6$. On suppose maintenant que $n > 9$.

On veut majorer le nombre d'entiers a tels que

$$a^t \equiv 1 \mod n \quad \text{ou} \quad a^{2^i t} \equiv -1 \mod n \text{ pour un } i \in \{0, \cdots, s-1\}.$$

Ces entiers sont nécessairement inversibles modulo n, donc il suffit de considérer les équations

$$a^t = 1 \quad \text{et} \quad a^{2^i t} = -1 \ (i \in \{0, \cdots, s-1\})$$

dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Considérons la décomposition de n en produit de facteurs premiers distincts :

$$n = \prod_{i=1}^{N} p_i^{a_i}.$$

Alors on a, d'après le théorème chinois,

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{N} (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times.$$

Un élément a de $(\mathbb{Z}/n\mathbb{Z})^\times$ satisfait l'une des équations ci-dessus si et seulement si son image dans chacun des $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ satisfait la même équation. De plus, on sait que chacun des $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ est cyclique, d'ordre $(p_i - 1)p_i^{a_i - 1}$.

Posons, pour tout $i \in \{1, \cdots, N\}$,

$$(p_i - 1)p_i^{a_i - 1} = 2^{u_i} v_i \quad \text{avec } v_i \text{ impair.}$$

Alors on a $u_i \geq 1$ et $p_i^{a_i-1} \mid v_i$. On pose également $u = \min(u_1, \cdots, u_N)$.

En utilisant le Lemme 2(1) on obtient que le nombre de solutions de l'équation

$$a^t = 1$$

dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est

$$\prod_{i=1}^{N} \mathrm{pgcd}(t, v_i).$$

De même, d'après le Lemme 2(2), si $j \in \{1, \cdots, s\}$, l'équation $a^{2^{j-1}t} = -1$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ admet des solutions si et seulement si $j \leq \min(s, u)$, et dans ce cas le nombre de solutions est

$$\prod_{i=1}^{N} 2^{j-1}\mathrm{pgcd}(t, v_i) = 2^{N(j-1)} \prod_{i=1}^{N} \mathrm{pgcd}(t, v_i).$$

En conclusion, le nombre total d'éléments qui vérifient l'une de ces équations est au plus

$$A := \left(1 + 1 + 2^N + \cdots + 2^{N\cdot(\min(s,u)-1)}\right) \cdot \prod_{i=1}^{N} \mathrm{pgcd}(t, v_i).$$

Considérons le cas où $N = 1$, de sorte que $n = p^a$ pour un nombre premier p et $a \geq 2$. (On a exclu le cas $p = 3$ et $a = 2$, puisque $n > 9$.) On a $n - 1 = p^a - 1 = 2^s t$, et si on écrit $p - 1 = 2^u w$ avec w impair alors $\varphi(n) = (p-1)p^{a-1} = 2^u(wp^{a-1})$ avec wp^{a-1} impair. Comme $p - 1 \mid n - 1$ on a $u \leq s$ et $w \mid t$. De la première observation on déduit que $\min(s, u) = u$, et de la deuxième que $\mathrm{pgcd}(t, wp^{a-1}) = w$ puisque p^{a-1} est premier à $n - 1$, donc à t. On obtient finalement que

$$A = (1 + 1 + 2 + \cdots + 2^{u-1}) \cdot w = 2^u \cdot w = p - 1 = \frac{\varphi(n)}{p^{a-1}} \leq \frac{\varphi(n)}{4}.$$

On suppose maintenant que $N > 1$. On remarque alors que

$$A \leq 2^{N\cdot(\min(s,u)-1)+1} \cdot \prod_{i=1}^{N} \mathrm{pgcd}(t, v_i).$$

Puisque $\varphi(n) = \prod_i (p_i - 1)p_i^{a_i-1}$, on a

$$\varphi(n) = 2^{\sum_i u_i} \cdot \prod_i v_i,$$

d'où on tire que

$$\frac{\varphi(n)}{A} \geq 2^{\sum_i u_i - N\cdot\min(s,u)+N-1} \cdot \prod_i \frac{v_i}{\mathrm{pgcd}(t, v_i)}.$$

Ici, pour tout i on a $u_i \geq \min(s, u)$, d'où

$$\sum_i u_i - N \cdot \min(s, u) + N - 1 \geq N - 1.$$

Si $N \geq 3$, ou si $u_i > \min(s,u)$ pour un i, alors cette majoration suffit pour conclure que $\varphi(n)/A \geq 4$. On suppose donc maintenant que $N = 2$ et $u_1 = u_2 \leq s$. (On a alors $u = u_1 = u_2$). Dans ce cas l'inégalité précédente s'écrit

$$\frac{\varphi(n)}{A} \geq 2 \cdot \frac{v_1}{\mathrm{pgcd}(t, v_1)} \cdot \frac{v_2}{\mathrm{pgcd}(t, v_2)}.$$

On remarque que $t \mid n-1$, donc t est premier avec p_1 et p_2. Si $a_i > 1$ pour un i, comme $p_i^{a_i-1} \mid v_i$ on en déduit que $p_i^{a_i-1} \mid \frac{v_i}{\mathrm{pgcd}(t,v_i)}$. Le terme

$$2 \cdot \frac{v_i}{\mathrm{pgcd}(t, v_i)}$$

vaut alors au moins 6, ce qui permet de conclure.

Enfin on suppose que $\frac{v_1}{\mathrm{pgcd}(t,v_1)} = \frac{v_2}{\mathrm{pgcd}(t,v_2)} = 1$, ce qui implique en particulier (comme on l'a vu ci-dessus) que $a_1 = a_2 = 1$. On a alors

$$n = p_1 p_2, \quad n - 1 = 2^s t, \quad p_1 - 1 = 2^u v_1, \quad p_2 - 1 = 2^u v_2$$

avec $u \leq s$, $v_1 \mid t$, $v_2 \mid t$. Alors $p_1 - 1$ et $p_2 - 1$ divisent $n - 1$; mais on a

$$n - 1 = p_1 p_2 - 1 = (p_1 - 1)(p_2 - 1) + (p_1 - 1) + (p_2 - 1),$$

ce qui implique que $p_1 - 1 \mid p_2 - 1$ et $p_2 - 1 \mid p_1 - 1$, ce qui est absurde vu que $p_1 \neq p_2$. □

6. Autres ressources sur cette leçon

`http://math.univ-lyon1.fr/~germoni/agreg/ZsurnZ.pdf`.
`https://perso.univ-rennes1.fr/matthieu.romagny/agreg/theme/z_sur_n_z.pdf`

Références

[CG] P. Caldero, J. Germoni, *Nouvelles histoires hédonistes de groupes et de géométries, Tome II*, Calvage & Mounet, 2018.

[Co] F. Combes, *Algèbre et géometrie : Agrégation, CAPES, licence, maîtrise*, Bréal, 1998.

[De] M. Demazure, *Cours d'algèbre : primalité, divisibilité, codes*, Cassini, 1997.

[FGN1] S. Francinou, H. Gianella, S. Nicolas, *Oraux X-ENS, algèbre 1*, Cassini, 2007.

[FGN2] S. Francinou, H. Gianella, S. Nicolas, *Oraux X-ENS, algèbre 2*, Cassini, 2006.

[Pe] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.