Arithmétique

1 Autour de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Rappelons le résultat suivant.

Proposition 1.1. *Soit $n \geq 2$ et $k \in \mathbb{Z}$. Les propositions suivantes sont équivalentes :*

1. *$\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.*
2. *$\overline{k}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.*
3. *k est premier avec n.*

Définition 1.2. *Soit $n \geq 1$. L'**indicatrice d'Euler** de n, notée $\varphi(n)$, est 1 si $n = 1$ et le nombre d'entiers $k \in \{1, \dots, n-1\}$ premiers avec n sinon.*

En vertu du théorème chinois, on a la propriété suivante.

Proposition 1.3. *Pour tout $m, n \geq 1$ premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$ (on dit que φ est **multiplicative**).*

Corollaire 1.4. *Soit $n \geq 2$. Alors*

$$\varphi(n) = n \prod_{\substack{p|n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right).$$

Démonstration. Si p est un nombre premier et $\alpha \geq 1$ alors les entiers entre 0 et $p^\alpha - 1$ premiers avec p^α sont ceux qui ne sont pas divisibles par p car p est premier. Il y en a donc $p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$. La formule générale s'en déduit par multiplicativité de φ. □

Proposition 1.5 (Théorème d'Euler)**.** *Soit $n \geq 2$ et $a \in \mathbb{Z}/n\mathbb{Z}^\times$. Alors $a^{\varphi(n)} = 1$.*

Théorème 1.6. *Soit $n \geq 2$. Le groupe $\mathbb{Z}/n\mathbb{Z}^\times$ est cyclique si et seulement si n est de la forme, $2, 4, p^\alpha$ ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$.*

Exercice 1. *Montrer que la condition est nécessaire.*

Remarque 1.7. Le caractère suffisant se montre en construisant un élément d'ordre $p-1$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}^\times$ à partir d'un élément d'ordre $p-1$ dans $\mathbb{F}_p$, et un élément d'ordre $p^{\alpha-1}$ (la classe de $1+p$ convient). Leur produit est alors d'ordre $p^{\alpha-1}(p-1)$ puisqu'ils commutent et leurs ordres sont premiers entre eux. La même méthode permet de montrer que $\mathbb{Z}/2^\alpha\mathbb{Z}$ est engendré par -1 et 5 dès que $\alpha \geq 3$. Ainsi, $\mathbb{Z}/2^\alpha\mathbb{Z}^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ pour $\alpha \geq 3$.

2 Nombres premiers

Théorème 2.1 (Euclide)**.** *Il existe une infinité de nombres premiers.*

Démonstration. Une des plus vieilles démonstrations de l'histoire (c'est un peu l'équivalent des peintures rupestres pour les maths) : Soit $p_1, \dots, p_r$ des nombres premiers distincts. Alors l'entier $1 + p_1 \dots p_r$ est supérieur ou égal à 2 donc admet un facteur premier p, distinct de $p_1, \dots, p_r$, sans quoi p diviserait 1. □

Remarque 2.2. Ce n'est **pas** un raisonnement par l'absurde ! On montre que toute liste finie d'entiers est incomplète, on n'a pas besoin de supposer que la liste complète l'est pour conclure à une absurdité.

On peut quantifier le caractère infini des nombres premiers avec le théorème culturel suivant.

Théorème 2.3 (des nombres premiers (malheureusement admis))**.** *Pour $x \geq 2$, notons $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x. Alors*

$$\pi(x) \underset{x \to +\infty}{\sim} \frac{x}{\ln x}.$$

Il faut savoir dire que la démonstration utilise l'analyse complexe et l'étude de la fonction ζ de Riemann.

Un autre théorème culturel à connaître (et dont la version faible avec $a = 1$ est abordable à l'agrégation) est le suivant.

Théorème 2.4 (de la progression arithmétique de Dirichlet (admis))**.** *Soit $a, q \in \mathbb{Z}$ premiers entre eux. Alors il existe une infinité de nombres premiers $p \equiv a \bmod q$.*

Exercice 2 (Nombres premiers de Fermat)**.** *Montrer que si $2^n + 1$ est un nombre premier alors n est une puissance de 2.*

Exercice 3 (Nombres premiers de Mersenne)**.** *Montrer que si $2^n - 1$ est un nombre premier alors n est un nombre premier.*

Définition 2.5. *Soit p un nombre premier. Le* ***symbole de Legendre*** *modulo p est la fonction*

$$\left(\frac{\cdot}{p}\right) : n \mapsto \begin{cases} 1 \text{ si } n \text{ est un carré non nul modulo } p, \\ -1 \text{ si } n \text{ n'est pas un carré modulo } p, \\ 0 \text{ si } p \text{ divise } n. \end{cases}$$

Proposition 2.6. *Le symbole de Legendre est multiplicatif : pour tout $a, b \in \mathbb{Z}$, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.*

Démonstration. Cela vient du fait que l'ensemble des carrés est un sous-groupe d'indice 2 de $\mathbb{F}_p^\times$. □

Théorème 2.7 (Loi de réciprocité quadratique)**.** *Soit p et q des nombres premiers impairs distincts. Alors*

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

Remarque 2.8. Autrement dit, la loi de réciprocité quadratique affirme que $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, sauf dans le cas où p et q sont tous les deux congrus à 3 modulo 4, auquel cas les deux symboles sont opposés.

On propose une démonstration dans les exercices inspirée du théorème de Wilson. Il y en a beaucoup d'autres abordables à l'agrégation (sommes de Gauss, comptage de points dans $\mathbb{F}_p$ et la classification des formes quadratiques, etc.) et on en connaît à ce jour plus de 300 !

Exercice 4. *Est-ce que* 713 *est un carré modulo* 1009 *?*

Exercice 5. *Soit p un nombre premier impair. Montrer que*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ si } p \equiv \pm 1 \bmod 8 \\ -1 \text{ si } p \equiv \pm 3 \bmod 8. \end{cases}$$

(Indication : Si ζ est une racine primitive 8-ième de l'unité dans $\overline{\mathbb{F}_p}$, alors $(\zeta + \zeta^{-1})^2 = 2$.)

Méthode : Pour tester si un petit nombre n est premier, on vérifie s'il est divisible par les nombres premiers inférieurs à $\sqrt{n}$. Cette méthode est hautement inefficace quand n devient grand, et on préfère des tests qui se basent sur des propriétés impliquées par le fait que $\mathbb{Z}/n\mathbb{Z}$ doit être un corps (tests de Fermat, Miller-Rabin, Solovay-Strassen, etc.).

Exercice 6. *Soit $n = 561$. Montrer que pour tout $a \in \mathbb{Z}$ premier avec n, $a^{n-1} \equiv 1 \bmod n$. En déduire qu'on ne peut pas assurer la primalité d'un entier à l'aide du petit théorème de Fermat.*

Définition 2.9. *Un entier n non premier tel que pour tout a premier avec n, $a^{n-1} \equiv 1 \bmod n$ est un* ***nombre de Carmichael****.*

Théorème 2.10 (Critère de Korselt)**.** *Un entier $n \geq 2$ est un nombre de Carmichael si et seulement si n est sans facteur carré, et pour tout diviseur premier p de n, $p - 1$ divise $n - 1$.*

3 Corps de nombres

Définition 3.1. *Un* ***corps de nombres*** *est une extension finie de $\mathbb{Q}$.*

Exemple 3.2.

1. Les corps quadratiques réels $\mathbb{Q}(\sqrt{d})$ avec $d \geq 2$ sans facteur carré.
2. Les corps quadratiques imaginaires $\mathbb{Q}(i\sqrt{d})$ avec $d \in \mathbb{N}^*$ sans facteur carré.
3. Les corps cyclotomiques $\mathbb{Q}(\zeta_n)$, avec ζ_n une racine primitive n-ième de l'unité.
4. Le corps de décomposition $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ de $X^3 - 2$ sur $\mathbb{Q}$.
5. $\overline{\mathbb{Q}}$ n'est pas un corps de nombres, mais les contient tous.

3.1 Corps cyclotomiques

Définition 3.3. *Soit $n \geq 1$. Le n-ième* ***polynôme cyclotomique*** *est*

$$\Phi_n = \prod_{\zeta \text{ racine primitive } n-\text{ième de l'unité}} (X - \zeta).$$

Exercice 7. *Soit p un nombre premier. Déterminer Φ_p et montrer que Φ_p est irréductible dans $\mathbb{Q}[X]$ en appliquant le critère d'Eisenstein au polynôme $\Phi_p(X + 1)$.*

Proposition 3.4. *Pour tout $n \in \mathbb{N}^*$,*

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Théorème 3.5. *Soit $n \geq 1$. Alors $\Phi_n \in \mathbb{Z}[X]$, est de degré $\varphi(n)$ et est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Le degré est clair. Au vu de l'égalité $X^n - 1 = \prod_{d|n} \Phi_d$, le fait que $\Phi_n \in \mathbb{Z}[X]$ se montre par récurrence sur n : le cas $n = 1$ est clair, et si le résultat est montré pour tous les $d < n$, on pose la division euclidienne de $X^n - 1$ par $\prod_{\substack{d|n \\ d \neq n}} \Phi_d$ dans $\mathbb{Z}[X]$, ce qui est possible car ce dernier est unitaire.

L'irréductibilité nécessite plus de travail. Soit ζ une racine primitive n-ième de l'unité et P son polynôme minimal sur $\mathbb{Q}$. Alors $P \in \mathbb{Z}[X]$ car il divise (dans $\mathbb{Q}[X]$) l'un des facteurs irréductibles dans $\mathbb{Z}[X]$ de Φ_n, et lui est donc égal car ils sont unitaires (lemme de Gauss).

Soit p un nombre premier ne divisant pas n. Alors ζ^p est encore une racine primitive n-ième de l'unité et on note Q son polynôme minimal sur $\mathbb{Q}$. Comme avant, il est dans $\mathbb{Z}[X]$ et on va montrer que $P = Q$. Si ce n'était pas le cas, on aurait $PQ \mid \Phi_n$ dans $\mathbb{Z}[X]$ puisque les deux sont irréductibles et $\mathbb{Z}[X]$ est factoriel. Mais on a aussi $P \mid Q(X^p)$ dans $\mathbb{Q}[X]$, puis dans $\mathbb{Z}[X]$ comme avant. Or, $\overline{Q(X^p)} = \overline{Q(X)}^p$ modulo p, et donc un facteur irréductible de $\overline{P}$ est également facteur irréductible de $\overline{Q}$, et donc un facteur multiple de $\overline{\Phi_n}$. Or un tel facteur n'existe pas car $\overline{X^n - 1}$ est sans facteur carré puisque premier avec sa dérivée $\overline{nX^{n-1}} \neq \overline{0}$. On a donc $P = Q$ et notamment $P(\zeta^p) = 0$.

Pour finir, si $m \in \{1, \ldots, n-1\}$ est premier avec n, on écrit $m = p_1 \ldots p_r$ avec les p_i des nombres premiers (pas forcément distincts) ne divisant pas n, et l'argument précédent montre par récurrence sur r que ζ^m est racine de P. Finalement, P divise Φ_n et a au moins autant de racines, ils sont donc associés (même égaux puisqu'ils sont unitaires) et Φ_n est bien irréductible dans $\mathbb{Q}[X]$. □

Corollaire 3.6. *Pour tout $n \geq 1$, Φ_n est le polynôme minimal de ζ_n. De plus, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*

3.2 Corps quadratiques

Proposition 3.7. *L'anneau $\mathbb{Z}[i] \subset \mathbb{Q}(i)$ est euclidien pour le stathme $N : a + ib \mapsto a^2 + b^2$.*

Démonstration. Puisque N est le carré du module, il est multiplicatif, et il est clair qu'il est à valeurs dans $\mathbb{N}$. Soit $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$. Pour trouver $q, r \in \mathbb{Z}[i]$ tels que $a = bq + r$ et $N(r) < N(b)$, il suffit de trouver $q \in \mathbb{Z}[i]$ de sorte que $N\left(\frac{a}{b} - q\right) < 1$. Or, si $\frac{a}{b} = u + iv$, avec $u, v \in \mathbb{Q}$, on prend $q_1, q_2 \in \mathbb{Z}$ avec $|u - q_1|, |v - q_2| \leq \frac{1}{2}$, et alors $N\left(\frac{a}{b} - (q_1 + iq_2)\right) = (u - q_1)^2 + (v - q_2)^2 \leq \frac{1}{2} < 1$. □

Proposition 3.8. *L'anneau $\mathbb{Z}[j] \subset \mathbb{Q}(j)$ est euclidien pour le stathme $N : a + jb \mapsto a^2 - ab + b^2$.*

Démonstration. Puisque N est le carré du module, il est multiplicatif, et il est clair qu'il est à valeurs dans $\mathbb{N}$. Soit $a, b \in \mathbb{Z}[j]$ avec $b \neq 0$. Pour trouver $q, r \in \mathbb{Z}[j]$ tels que $a = bq + r$ et $N(r) < N(b)$, il suffit de trouver $q \in \mathbb{Z}[j]$ de sorte que $N\left(\frac{a}{b} - q\right) < 1$. Or, si $\frac{a}{b} = u + jv$, avec $u, v \in \mathbb{Q}$, on prend $q_1, q_2 \in \mathbb{Z}$ avec $|u - q_1|, |v - q_2| \leq \frac{1}{2}$, et alors $N\left(\frac{a}{b} - (q_1 + jq_2)\right) = (u - q_1)^2 - (u - q_1)(v - q_2) + (v - q_2)^2 \leq \frac{1}{2} + \frac{1}{4} < 1$. □

Exercice 8. *Montrer que $\mathbb{Z}[\sqrt{2}]$ est euclidien pour le stathme $N : a + b\sqrt{2} \mapsto |a^2 - 2b^2|$.*

Remarque 3.9. Les anneaux $\mathbb{Z}[\zeta_n]$, $\mathbb{Z}[i\sqrt{d}]$ (pour $d \equiv 1 \bmod 4$) et $\mathbb{Z}\left[\frac{1+i\sqrt{d}}{2}\right]$ (pour $d \equiv 3 \bmod 4$[1]) sont euclidiens pour de petites valeurs de n et de d, mais ce n'est pas une généralité : il n'y a en fait qu'un nombre fini de valeurs de d et de n pour lesquelles ces anneaux peuvent être principaux. Nous allons voir ci-dessous que cette propriété peut être très précieuse pour la résolution de certaines équations. En ce qui concerne les anneaux de la forme $\mathbb{Z}[\sqrt{d}]$ et $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, la situation est beaucoup plus compliquée : on ne sait pas à ce jour s'il en existe une infinité qui sont principaux !

4 Équations diophantiennes

Définition 4.1. *Une **équation diophantienne** est une équation polynomiale à coefficients entiers dont on cherche les solutions entières (ou rationnelles).*

Exemple 4.2.

1. L'équation de Pell-Fermat $x^2 - dy^2 = 1$ avec $d \in \mathbb{N}$.
2. L'équation de Fermat $x^n + y^n = z^n$ avec $n \in \mathbb{N}^*$.
3. Les équations de Mordell $y^2 = x^3 + k$ avec $k \in \mathbb{Z}$.

Exercice 9. *Soit $a, b, c \in \mathbb{Z}$ non nuls. Déterminer quand l'équation diophantienne $ax + by = c$ admet des solutions dans $\mathbb{Z}$, et les déterminer.*

Exercice 10. *Résoudre l'équation diophantienne $103x + 78 = y^2$.*

Théorème 4.3 (Triplets pythagoriciens)**.** *Soit $x, y, z \in \mathbb{Z}$ premiers entre eux dans leur ensemble avec x impair. On a $x^2 + y^2 = z^2$ si et seulement s'il existe des entiers $u, v \in \mathbb{Z}$ premiers entre eux et de parités différentes tels que $x = u^2 - v^2, y = 2uv$ et $z = u^2 + v^2$.*

Démonstration. Un calcul montre que la condition est suffisante. Réciproquement, si $x^2+y^2 = z^2$ alors $x^2 = (z-y)(z+y)$. Ainsi, tout facteur premier p de x divise $z-y$ ou $z+y$, mais pas les deux. Dans le cas contraire, p diviserait $(z-y)+(z+y) = 2z$ et $(z-y)-(z+y) = -2y$ et donc y et z puisque $p \neq 2$, ce qui est absurde car x, y et z sont premiers entre eux dans leur ensemble. Ensuite, $p^{2v_p(x)}$ divise $z-y$ ou $z+y$, mais pas les deux. Réciproquement, tout facteur premier de $z-y$ et de $z+y$ est un facteur premier de x avec valuation paire. On en déduit que $z-y = a^2$ et $z+y = b^2$ avec $x = ab$ (a est le produit des puissances de nombres premiers divisant x et $z-y$, de même pour b avec $z+y$). Pour obtenir la décomposition voulue, on pose $u = \frac{a+b}{2}$ et $v = \frac{a-b}{2}$. □

Remarque 4.4. Ce résultat permet de trouver tous les triplets pythagoriciens en factorisant par le carré du PGCD de (x, y, z) et quitte à échanger les rôles de x et y pour que x soit impair (ils ne peuvent pas être tous les deux pairs, sinon z le serait aussi).

Exercice 11.
1. *Montrer que, pour trouver les triplets pythagoriciens, il suffit de trouver les points rationnels du cercle unité dans le plan.*
2. *Déterminer ces points rationnels, en utilisant la paramétrisation suivante : considérer le point d'intersection entre le cercle unité et la droite passant par $(-1, 0)$ et de pente un rationnel $t \in \mathbb{Q}$.*

1. Cette condition garantit que $\mathbb{Z}\left[\frac{1+i\sqrt{d}}{2}\right]$ est l'**anneau des entiers** de $\mathbb{Q}(i\sqrt{d})$, voir l'Exercice 23.

Corollaire 4.5. *L'équation de Fermat $x^4 + y^4 = z^4$ n'admet pas de solution non triviale, c'est-à-dire avec $xyz \neq 0$.*

Démonstration. On va même montrer qu'il n'y a pas de solution non triviale à l'équation $x^4 + y^4 = z^2$. Supposons par l'absurde l'existence d'une telle solution, avec $|z|$ minimal. Alors, quitte à factoriser et échanger x et y, on peut appliquer le critère des triplets pythagoriciens : il existe $u, v \in \mathbb{Z}$ premiers entre eux et de parités différentes tels que $x^2 = u^2 - v^2, y^2 = 2uv$ et $z = u^2 + v^2$. Alors $x^2 + v^2 = u^2$ constitue un triplet pythagoricien avec x impair et x, u, v premiers entre eux (car u et v le sont), et donc il existe à nouveau $a, b \in \mathbb{Z}$ premiers entre eux et de parités différentes tels que $x = a^2 - b^2$, $v = 2ab$ et $u = a^2 + b^2$. Les entiers u et v sont premiers entre eux, donc l'un au plus est pair, par exemple v, et alors u et $2v$ sont premiers entre eux. Puisque $2uv = y^2$, u et $2v$ sont des carrés. Comme $2v = 4ab$ est un carré, ab aussi et donc a et b sont des carrés. Si on note $u = k^2, a = m^2$ et $b = n^2$ alors on arrive finalement $m^4 + n^4 = k^2$ avec $|k| = |u|^{1/2} \leq |z|^{1/4} < |z|$. La minimalité de $|z|$ donne une contradiction. □

Remarque 4.6. On a utilisé la méthode de « descente infinie » de Fermat, qui est équivalente au principe de récurrence, ou encore au caractère bien ordonné de $\mathbb{N}$. Cette même méthode permet, avec (beaucoup) plus de travail, que l'équation de Fermat n'a pas de solution non triviales pour $n = 3, 5$ ou 7, en utilisant l'arithmétique des anneaux $\mathbb{Z}[j], \mathbb{Z}[\varphi]$ et $\mathbb{Z}[i\sqrt{7}]$.

Proposition 4.7. *L'équation diophantienne $y^2 = x^3 - 1$ a pour unique solution $(1, 0)$ dans $\mathbb{Z}^2$.*

Démonstration. Il est clair que $(1, 0)$ est solution. Réciproquement, supposons que (x, y) est solution dans $\mathbb{Z}^2$. On a alors $x^3 = y^2 + 1 = (y - i)(y + i)$ dans $\mathbb{Z}[i]$. Or $y + i$ et $y - i$ sont premiers entre eux dans $\mathbb{Z}[i]$. En effet, dans le cas contraire, il existerait un élément irréductible π divisant les deux, donc divisant notamment $2i$, qui est irréductible dans $\mathbb{Z}[i]$. Ainsi, π est associé à $2i$, mais il ne peut alors pas diviser $y + i$ (écrivez-le !). Comme $\mathbb{Z}[i]$ est factoriel (et comme ses inversibles sont des cubes), on en déduit que $y + i$ et $y - i$ sont des cubes dans $\mathbb{Z}[i]$. Si par exemple $y + i = (a + ib)^3 = (a^3 - 3ab^2) + i(3a^2b - b^3)$ alors $3a^2b - b^3 = (3a^2 - b^2)b = 1$ et donc $b = \pm 1$, puis $3a^2 = \pm 1 + 1$. La seule possibilité est que $a = 0$ et $b = -1$. Finalement, $y = a^3 - 3ab^2 = 0$ et donc $x^3 = 1$, ce qui implique que $x = 1$. □

Proposition 4.8. *L'équation diophantienne $y^2 = x^3 + 1$ a pour seules solutions $(-1, 0), (0, -1)$, $(0, 1), (2, 3), (2, -3)$ dans $\mathbb{Z}^2$.*

Démonstration. On vérifie immédiatement que les couples annoncés sont bien solutions.

Réciproquement, si (x, y) est une solution dans $\mathbb{Z}^2$, alors $y^2 = (x + 1)(x + j)(x + j^2)$ dans $\mathbb{Z}[j]$. Si l'un des deux derniers facteurs est premier avec le reste, on procède comme dans la résolution précédente : $\mathbb{Z}[j]$ étant factoriel, ce facteur est associé à un carré de $\mathbb{Z}[j]$. Les inversibles de $\mathbb{Z}[j]$ étant $\pm 1, \pm j$, et $\pm j^2$, et j lui-même étant un carré ($j = (j^2)^2$) on peut donc écrire $x + j = \pm(a + jb)^2$ et $x + j^2 = \pm(a + j^2 b)^2$ (puisque $x + j$ et $x + j^2$ sont conjugués). En prenant la différence on obtient $\pm b(2a - b) = 1$ ce qui mène aux couples $(-1, 0), (0, -1)$ et $(0, 1)$.

Sinon, $x + j$ n'est pas premier avec $(x + 1)(x + j^2)$ donc avec $x + 1$ ou $x + j^2$ et de même $x + j^2$ n'est pas premier avec $x + 1$ ou $x + j$. Dans tous les cas un facteur commun doit diviser la différence $1 - j, 1 - j^2$ ou $j - j^2$ qui est de norme 3 et est donc irréductible. Ainsi, un PGCD de $x + 1, x + j$ et $x + j^2$ est l'élément irréductible $\lambda = 1 - j$ (associé à chacun des trois éléments ci-dessus). Comme précédemment, on a donc $x + j = \pm(1 - j)(a + jb)^2$ et $x + j^2 = \pm(1 - j^2)(a + j^2 b)^2$. En ajoutant les deux, on obtient $2x - 1 = \pm 3(a^2 - b^2)$. Or, $x + 1$ étant réel, si λ divise $x + 1$ alors l'élément irréductible distinct $1 - j^2$ divise aussi $x + 1$, et donc a $x + 1 = \pm 3a^2$. Comme $y^2 \geq 0$ on doit avoir $x \geq -1$ et donc $x + 1 = 3a^2$. On a donc finalement $6a^2 - 3 = \pm 3(a^2 - b^2)$, ce qui mène aux couples $(2, -3)$ et $(2, 3)$. □

Remarque 4.9. Les équations précédentes, dites de Mordell, sont des exemples d'équations de **courbes elliptiques**, dont l'étude générale est plus que jamais d'actualité pour leurs applications en cryptographie et leur prépondérance dans la recherche en théorie des nombres contemporaine. Curieusement, la démonstration du dernier théorème de Fermat passe par celle d'une propriété profonde des courbes elliptiques définies sur $\mathbb{Q}$.

Théorème 4.10 (des deux carrés)**.** *Soit $n \in \mathbb{N}^*$. Alors l'équation $x^2 + y^2 = n$ est résoluble en nombres entiers si et seulement si pour tout facteur premier p de n congru à 3 modulo 4, la valuation p-adique de n est paire.*

Démonstration. Commençons par remarquer que $x^2 + y^2 = N(x + iy)$ dans l'anneau $\mathbb{Z}[i]$. Puisque la norme est multiplicative, on voit que la propriété d'être somme de deux carrés est multiplicative également. Ainsi, il suffit de déterminer les nombres premiers qui le sont. Il est clair que $2 = 1^2 + 1^2$, on va maintenant montrer que si p est un nombre premier impair, alors p est somme de deux carrés si et seulement si $p \equiv 1 \bmod 4$.

Les carrés modulo 4 étant 0 et 1, on voit que si $p \equiv 3 \bmod 4$ alors p ne peut s'écrire comme somme de deux carrés. Si $p \equiv 1 \bmod 4$, montrons que p est réductible dans $\mathbb{Z}[i]$, de sorte que $p = z_1 z_2$ avec $z_1, z_2 \in \mathbb{Z}[i]$ non inversibles, et donc de norme différente de 1. On aura alors $p^2 = N(p) = N(z_1)N(z_2)$ et donc $N(z_1) = N(z_2) = p$, et donc que p est somme de deux carrés. On a $\mathbb{Z}[i]/(p) = (\mathbb{Z}[X]/(X^2+1))/(p) \simeq \mathbb{Z}[X]/(p, X^2+1) \simeq \mathbb{F}_p[X]/(X^2+1)$ est intègre si et seulement si $X^2 + 1$ est irréductible dans $\mathbb{F}_p[X]$ si et seulement si $p \equiv 3 \bmod 4$. Comme $\mathbb{Z}[i]$ est factoriel, on en déduit que p est irréductible dans $\mathbb{Z}[i]$ si et seulement s'il est premier dans $\mathbb{Z}[i]$ si et seulement si $p \equiv 3 \bmod 4$.

On en déduit qu'un entier tel que dans l'énoncé est bien somme de deux carrés puisque c'est le produit de puissances de 2 et de premiers congrus à 1 modulo 4 et d'un carré (constitué de ses facteurs premiers congrus à 3 modulo 4).

Réciproquement, si $n = x^2 + y^2$ alors $n = d^2(a^2 + b^2)$ avec $d = \mathrm{PGCD}(x, y)$ et a et b premiers entre eux. Si p est un facteur premier impair de $a^2 + b^2$, alors p est nécessairement réductible dans $\mathbb{Z}[i]$, et donc congru à 1 modulo 4, ce qui permet ce conclure. En effet, si p était irréductible, il serait premier et diviserait $a + ib$ ou $a - ib$. Mais s'il divise l'un, il divise l'autre en passant au conjugué, donc il divise leurs somme et différence, soit $p \mid 2a$ et $p \mid 2ib$. Comme p est impair, $p \mid a$ et $p \mid b$, ce qui est absurde. □

5 Exercices

Exercice 12 (Échauffement)**.**

1. *Montrer que* 13 *divise* $3^{126} + 5^{126}$.
2. *Montrer de manière élémentaire qu'il n'existe pas d'entiers x et y tels que* $15x^2 - 8y^2 = 9$.
3. *Déterminer les entiers x vérifiant $x \equiv 7 \bmod 18$, $x \equiv 1 \bmod 30$ et $x \equiv 16 \bmod 45$.*

Exercice 13 (Règles de divisibilité)**.**

1. *Démontrer la règle de* 3 *: n est divisible par* 3 *si et seulement si la somme de ses chiffres l'est.*
2. *Donner des règles de* $2, 5, 9$ *et* 11.

Exercice 14. *Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers distincts et les α_i dans $\mathbb{N}$. Donner une formule pour le nombre de diviseurs (positifs) de n.*

Exercice 15 (Formule d'inversion de Möbius)**.** *On note $\mathcal{A}$ l'ensemble des fonctions arithmétiques, c'est-à-dire les fonctions de $\mathbb{N}^* \to \mathbb{C}$. Si $f, g \in \mathcal{A}$, on note*

$$f * g : n \mapsto \sum_{d|n} f(n)g(n/d)$$

leur ***convolution de Dirichlet****. On vérifie immédiatement qu'il s'agit d'une loi qui fait que $(\mathcal{A}, +, *)$ un anneau commutatif de neutre δ, la fonction indicatrice de $\{1\}$.*

1. *Donner une condition nécessaire et suffisante pour que $f \in \mathcal{A}$ soit inversible.*
2. *On dit que $f \in \mathcal{A}$ est* ***multiplicative*** *lorsque $f(ab) = f(a)f(b)$ pour a et b premiers entre eux. Soit $f \in \mathcal{A}^\times$ multiplicative. Montrer que f^{-1} est multiplicative. (Indication : Commencer par construire un inverse g sur les puissances de nombres premiers et vérifier que la fonction définie par $n = \prod_{i=1}^r p_i^{\alpha_i} \mapsto \prod_{i=1}^r g\left(p_i^{\alpha_i}\right)$ convient.)*
3. *On note μ l'inverse de la fonction constante égale à 1. Calculer $\mu(p^k)$ pour n'importe quel nombre premier p et $k \in \mathbb{N}$, et en déduire une formule pour $\mu(n)$ avec $n \in \mathbb{N}^*$.*
4. *Montrer la* ***formule d'inversion de Möbius*** *: Si $\forall n \geq 1, f(n) = \sum_{d|n} g(d)$ alors $\forall n \geq 1, g(n) = \sum_{d|n} f(d)\mu(n/d)$.*
5. *Montrer que, pour tout $n \geq 1$, $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$.*

Remarque. *La combinatoire sous-jacente montre qu'on a également $\Phi_n = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$ pour tout $n \in \mathbb{N}^*$.*

Exercice 16. *Soit q une puissance de nombre premier impair. Montrer que $\mathbb{Z}/q\mathbb{Z}^\times$ possède exactement $\frac{\varphi(q)}{2}$ carrés sans utiliser la cyclicité de ce groupe. (Indication : On pourra montrer que si $x^2 \equiv a \bmod p^n$ alors il existe $h \in \mathbb{Z}$ tel que $(x + hp)^2 \equiv a \bmod p^{n+1}$.) En déduire le nombre de carrés dans $\mathbb{Z}/n\mathbb{Z}^\times$ pour n'importe quel $n \geq 2$.*

Remarque. La méthode utilisée ici pour « remonter » une congruence modulo p^n en une congruence modulo p^{n+1} s'appelle le **lemme de Hensel**.

Exercice 17.
1. *Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4. (Indication : Si $p_1, \ldots, p_r$ sont de tels nombres premiers, considérer $4p_1 \ldots p_r - 1$.)*
2. *Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4. (Indication : Si $p_1, \ldots, p_r$ sont de tels nombres premiers, considérer $4(p_1 \ldots p_r)^2 + 1$.)*
3. *Montrer qu'il existe une infinité de nombres premiers congrus à 7 modulo 8. (Indication : Si $p_1, \ldots, p_r$ sont de tels nombres premiers, considérer $(4p_1 \ldots p_r)^2 - 2$.)*

Remarque. *En utilisant les polynômes cyclotomiques, on peut montrer à l'agreg que pour tout $q \geq 2$, il existe une infinité de nombres premiers congrus à 1 modulo q. Le cas général nécessite des outils algébriques et analytiques (caractères du groupe $(\mathbb{Z}/q\mathbb{Z})^\times$, séries de Dirichlet...).*

Exercice 18.
1. *Justifier que pour $x \geq 2$,*

$$P(x) = \prod_{\substack{p \leq x \\ p \text{ premier}}} \frac{1}{1 - \frac{1}{p}} \geq \ln(x).$$

2. *Montrer que*
$$\ln P(x) = \sum_{\substack{p \leq x \\ p \text{ premier}}} \frac{1}{p} + O(1).$$

3. *En déduire que* $\sum_{p \text{ premier}} \frac{1}{p}$ *diverge. (En particulier, il existe une infinité de nombres premiers...)*

4. *On suppose qu'il existe une mesure de probabilité* μ *sur* $\mathcal{P}(\mathbb{N})$ *telle que pour tout* $k \in \mathbb{N}^*, \mu(k\mathbb{N}) = \frac{1}{k}$.

   (a) *Montrer que si* $a, b \in \mathbb{N}$ *sont premiers entre eux, alors* $a\mathbb{N}$ *et* $b\mathbb{N}$ *sont indépendants.*

   (b) *En déduire que si* $k \in \mathbb{N}^*$ *alors pour tout* $n > k$,
$$\mu(\{k\}) \leq \prod_{\substack{k < p \leq n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right).$$

   (c) *Conclure.*

Exercice 19. *En admettant le théorème de la progression arithmétique, montrer qu'un entier* n *est un carré dans* $\mathbb{Z}$ *si et seulement si c'est un carré modulo tout nombre premier* p.

Exercice 20 (Inégalités de Tchebytchev)**.** *Pour tout* $x \geq 2$, *on note*
$$\pi(x) = \#\{p \leq x \mid p \text{ premier}\} \text{ et } \theta(x) = \sum_{\substack{p \leq x \\ p \text{ premier}}} \ln p.$$

On va montrer qu'il existe des constantes $c_1, c_2 > 0$ *telles que*
$$c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_2 \frac{x}{\ln x}.$$

1. *Pour tout entier* $n \in \mathbb{N}^*$, *montrer que*
$$\prod_{\substack{n < p \leq 2n \\ p \text{ premier}}} p \mid \binom{2n}{n} \leq 2^{2n}.$$

2. *En déduire que pour* $n \in \mathbb{N}^*$, $\theta(2n) - \theta(n) \leq n \ln 4$.

3. *Montrer que* $\theta(x) = O(x)$ *et en déduire que* $\pi(x) = O\left(\frac{x}{\ln x}\right)$.

4. *Montrer que pour* $n \in \mathbb{N}^*$,
$$\frac{2^{2n}}{2n} \leq \binom{2n}{n}.$$

5. *Montrer la formule de Legendre : Si* p *est premier et* $n \geq 2$ *est entier alors*
$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$
et en déduire que $\binom{2n}{n} \leq (2n)^{\pi(2n)}$. *On pourra constater que* $\lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$ *pour tout réel* x.

6. *En déduire que* $\frac{x}{\ln x} = O(\pi(x))$.

7. *Montrer le postulat de Bertrand faible : Il existe une constante* $t > 1$ *telle que pour tout entier* $n \geq 2$*, il existe un nombre premier entre* n *et* tn.

   Remarque. *Le* ***théorème des nombres premiers*** *permet de voir que tout réel de la forme* $1 + \varepsilon$ *avec* $\varepsilon > 0$ *convient, au moins quand* n *est assez grand en fonction de* ε.

Exercice 21. *Quels sont les nombres premiers* p *tels que* 7 *est un carré modulo* p *?*

Exercice 22. *Soit* p *un nombre premier et* $n \in \mathbb{N}^*$. *Montrer que* $\Phi_{p^n} = \Phi_p(X^{p^{n-1}})$.

Exercice 23. *On appelle* ***entier algébrique*** *tout nombre algébrique dont le polynôme minimal (sur* $\mathbb{Q}$*) est à coefficients dans* $\mathbb{Z}$*. On admet que la somme et le produit d'entiers algébriques sont des entiers algébriques*[2].

1. *Parmi les nombres suivants, lesquels sont des entiers algébriques ?*

$$\frac{1}{2}, \sqrt{2}, \frac{1+\sqrt{3}}{2}, \pi, \frac{1+i\sqrt{19}}{2}, e^{\frac{2i\pi}{n}}, \cos\left(\frac{2\pi}{n}\right)$$

2. *Montrer qu'un rationnel est un entier algébrique si et seulement si c'est un entier.*

3. *Si* K *est un corps de nombres, alors* $\{\alpha \in K \mid \alpha \text{ est un entier algébrique}\}$ *est un sous-anneau de* K*, noté* $\mathcal{O}_K$*. Pour tout* $d \in \mathbb{Z}$ *sans facteur carré, déterminer* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *(avec la convention* $\sqrt{d} = i\sqrt{|d|}$ *quand* $d < 0$*). On pourra se servir du fait suivant : si* $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ *avec* $b \neq 0$ *et* $\overline{\alpha} = a - b\sqrt{d}$ *alors* $\mathrm{tr}(\alpha) = \alpha + \overline{\alpha}$ *et* $N(\alpha) = \alpha\overline{\alpha}$ *sont les coefficients du polynôme minimal de* α *sur* $\mathbb{Q}$.

4. *On note* $\mathbb{A}$ *l'anneau des entiers algébriques. Montrer que c'est un anneau de Bézout non principal. (Indication : Pour le caractère non principal, raisonner sur les degrés en tant que nombres algébriques. Pour le caractère de Bézout, on pourra admettre que dans tout corps de nombres, tout idéal de son anneau d'entiers a une puissance principale.)*

Exercice 24 (Corps cyclotomiques)**.** *Dans tout l'exercice, on note* $\zeta_n = e^{\frac{2i\pi}{n}}$ *pour tout* $n \in \mathbb{N}^*$.

1. *Soit* n *un entier impair. Montrer que* $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$.

2. *Montrer que si* m *est pair et* r *est un multiple de* m *tel que* $\varphi(r) \leq \varphi(m)$*, alors* $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_r)$.

3. *Montrer que les seules racines de l'unité dans* $\mathbb{Q}(\zeta_m)$ *sont les puissances de* ζ_m *quand* m *est pair, et les puissances de* ζ_{2m} *quand* m *est impair. (Indication : Quand* m *est pair, si* ω *est une racine primitive* k*-ième de l'unité dans* $\mathbb{Q}(\zeta_m)$*, montrer qu'il existe* $u, v \in \mathbb{Z}$ *tels que* $\zeta_r = \zeta_m^u \omega^v$*, avec* $r = \mathrm{PPCM}(m, k)$*.)*

4. *En déduire une condition nécessaire et suffisante pour que* $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$.

5. *Soit* p *un nombre premier impair. Montrer que* $\mathbb{Q}(\zeta_p) \cap \mathbb{R} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$ *est une extension de degré* $\frac{p-1}{2}$ *de* $\mathbb{Q}$.

2. Cela se montre comme pour les nombres algébriques, à l'aide de la caractérisation suivante : $\alpha \in \mathbb{C}$ est un entier algébrique si et seulement le $\mathbb{Z}$-module $\mathbb{Z}[\alpha]$ est de type fini, et le fait qu'un sous-module d'un module de type fini sur un anneau principal (comme $\mathbb{Z}$) est également de type fini.

Exercice 25. *1. Soit $n \in \mathbb{N}^*$ et q une puissance du nombre premier p. Montrer que $\overline{\Phi_n}$ admet une racine dans $\mathbb{F}_q$ si et seulement si $\mathbb{F}_q$ contient une racine primitive n-ième de l'unité.*

2. Déterminer le nombre et le degré des facteurs irréductibles de $\overline{\Phi_n}$ dans $\mathbb{F}_p[X]$.

3. En déduire une démonstration alternative de l'irréductibilité de Φ_n dans $\mathbb{Q}[X]$ quand $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Exercice 26. *Montrer que les seules solutions de l'équation diophantienne $y^2 = x^3 - 2$ sont $(3, 5)$ et $(3, -5)$.*

Exercice 27. *On rappelle que $\mathbb{Z}[j]$ est un anneau euclidien.*

1. *Déterminer les inversibles de $\mathbb{Z}[j]$.*
2. *Montrer que $\lambda = 1 - j$ est un irréductible de $\mathbb{Z}[j]$.*
3. *Soit p un nombre premier différent de 3. Donner une condition nécessaire et suffisante pour qu'il soit irréductible dans $\mathbb{Z}[j]$ en termes de congruence modulo 3.*
4. *En déduire l'ensemble des entiers n qui s'écrivent sous la forme $x^2 - xy + y^2$.*

Remarque. *De la même manière, on peut déterminer à la main les nombres premiers (puis les entiers) s'écrivant sous la forme $x^2 + 2y^2$ ou encore $x^2 - 2y^2$. Quand vous aurez passé l'agreg, je vous recommande « Primes of the form $x^2 + ny^2$ » pour voir jusqu'où mène ce genre de questions !*

Exercice 28. *Soit $n = 4^a(8b + 7)$. Montrer que n ne peut s'écrire comme la somme de trois carrés d'entiers.*
Remarque. *La réciproque est vraie mais est beaucoup plus difficile.*

Exercice 29 (Théorème des quatre carrés de Lagrange)**.** *On va montrer que tout entier naturel n peut s'écrire comme somme de quatre carrés.*

1. *Montrer que si a et b sont sommes de quatre carrés, alors il en est de même de ab. (Indication : On pourra penser aux quaternions.) En déduire qu'il suffit de montrer que chaque nombre premier s'écrit comme somme de quatre carrés.*
2. *Montrer que 2 est somme de quatre carrés.*
3. *Soit p un nombre premier impair, montrer qu'il existe $a, b \in \{0, \dots, \frac{p-1}{2}\}$ tels que $p \mid a^2 + b^2 + 1$. (Indication : Compter les éléments de $\mathbb{Z}/p\mathbb{Z}$ de la forme a^2 et ceux de la forme $-b^2 - 1$.)*
4. *Soit k le plus petit entier entier naturel non nul tel que kp soit somme de quatre carrés. On va montrer que $k = 1$. Justifier, à l'aide de la question précédente, que $1 \leq k < p$.*
5. *Notons $kp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Pour $1 \leq i \leq 4$, notons y_i l'entier compris entre $\frac{(-k+1)}{2}$ et $\frac{m}{2}$ et congru à x_i. Justifier que $y_1^2 + y_2^2 + y_3^2 + y_4^2 = kq$ avec $0 \leq q < k$.*
6. *Montrer que $(kp)(kq)$ est une somme de quatre carrés et en déduire que qp également. Conclure.*

Remarque. *L'anneau des* ***quaternions de Hurwitz*** *de la forme* $\frac{a+ib+jc+kd}{2}$ *avec* $a, b, c, d \in \mathbb{Z}$ *de même parité est « principal » (il n'est pas commutatif). La question iii) montre qu'il existe un quaternion de Hurwitz* q *tel que* p *divise* $|q|^2$*. L'idéal engendré par* q *et* p *étant principal, il est engendré par un quaternion* q' *diviseur strict de* p*, et* $|q'|^2$ *est une somme de quatre carrés divisant strictement* p^2*, c'est donc* p*.*

Exercice 30 (Réciprocité quadratique)**.** *Soit* p *et* q *des nombres premiers impairs distincts.*

1. *Notons* $p = 2k + 1$*. Montrer que* $(k!)^2 \equiv (-1)^{n+1} \bmod p$ *(penser à la démonstration du théorème de Wilson).*

2. *On note* $G = \mathbb{F}_p^\times \times \mathbb{F}_q^\times / \langle (-1, -1) \rangle$ *et la classe de* (a, b) *est notée* $[a, b]$*. Montrer que tout élément de* G *s'écrit de manière unique* $[a, b]$ *avec* $1 \leq a \leq k$ *et* $1 \leq b \leq q - 1$*.*

3. *Notons* $E = \{m \in \mathbb{N} \mid 1 \leq a \leq \frac{pq-1}{2}$ *et* m *est premier avec* p *et* $q\}$*. A l'aide du théorème chinois, montrer que tout élément de* G *s'écrit de manière unique sous la forme* $[a, a]$ *avec* $a \in E$*.*

4. *Posons* $P = \prod_{a \in E} a$ *et* $Q = \prod_{a=1}^{k} qa$*. Calculer* $Q \bmod p$*,* $PQ \bmod p$ *et en déduire* $P \bmod p$*.*

5. *Calculer de deux manières différentes le produit des éléments de* G*, et en déduire la loi de réciprocité quadratique.*

Exercice 31. *On introduit le* ***symbole de Jacobi*** $\left(\frac{a}{n}\right)$ *pour* $a \in \mathbb{Z}$ *et* $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ *avec les* p_i *premiers impairs par*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i}.$$

1. *Montrer que si* a *est un carré non nul modulo* n *alors* $\left(\frac{a}{n}\right) = 1$*. Montrer que la réciproque est fausse.*

2. *Montrer que* $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ *et* $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$*.*

3. *Montrer que si* m *et* n *sont impairs et premiers entre eux alors* $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}}(-1)^{\frac{n-1}{2}}$*.*

4. *Soit maintenant* p *un nombre premier congru à* 1 *modulo* 4*. D'après le théorème des deux carrés, il existe* $a, b \in \mathbb{Z}$ *tels que* $p = a^2 + b^2$*. Justifier que l'un des deux est impair.*

5. *Sans perdre de généralité, supposons que* a *est impair. Montrer que* $\left(\frac{a}{p}\right) = 1$*.*

6. *En calculant* $(a + b)^2 + (a - b)^2$*, montrer que* $\left(\frac{a+b}{p}\right) = (-1)^{\frac{(a+b)^2-1}{2}}$ *puis que* $(a + b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} \bmod p$*.*

7. *Justifier qu'il existe* $c \in \mathbb{Z}$ *tel que* $b \equiv ac \bmod p$*. Montrer que* $c^2 \equiv -1 \bmod p$ *et que* $2^{\frac{p-1}{4}} \equiv c^{\frac{ab}{2}} \bmod p$*.*

8. *En déduire que* 2 *est une puissance quatrième modulo* p *si et seulement si* p *peut s'écrire sous la forme* $a^2 + 64b^2$*.*