Progresser en arithmétique

Martin Rakovsky & *al*

2026

Ce polycopié s'adresse aux élèves du groupe senior ayant les connaissances dispensées dans le cours pour débutants de la POFM. Son ambition est de leur donner les outils nécessaires à la résolution de problèmes d'arithmétique de niveau 1/4 et 2/5 des Olympiades Internationales de Mathématiques.

Table des matières

1 Introduction

1.1 Pourquoi la théorie des nombres ?

La théorie des nombres, qui correspond à l'étude des nombres entiers, est l'un des quatre grands thèmes des Olympiades Internationales. Les entiers sont principalement reliés par trois types de liens : des liens « algébriques » (issus des relations de divisibilité), des liens « analytiques » (issus des comparaisons de taille) et des liens « combinatoires » (issus du caractère discret de $\mathbb{N}$). C'est la variété de ces liens qui fait la richesse du thème.

Au vu de ces trois liens, les arguments employés dans les problèmes seront souvent un mélange de ces trois idées : un peu de divisibilité, un peu de comparaison des tailles et éventuellement un peu de combinatoire, le tout en maniant des idées simples. C'est probablement ce principe un peu réducteur qu'il faut avoir en tête avant d'attaquer chaque problème d'arithmétique. Il est souvent suffisant pour résoudre les problèmes de niveau 1 et 4 des IMO, pour lesquels on attend généralement une idée originale utilisant les spécificités du problème combinée à des manipulations routinières. On ne s'avancera pas à catégoriser les problèmes de difficulté supérieure : certains problèmes d'Olympiades sont difficiles pour leur longueur et la quantité d'idées à combiner, d'autres se concentrent en une seule idée astucieuse mais salutaire.

A l'image des maths olympiques, l'arithmétique fascine par le contraste entre la simplicité des énoncés posées, la vaste technologie développée pour les aborder, et la stupéfiante complexité des liens qui émergent derrière ces technologies. Il n'est pas rare que les problèmes donnés en Olympiades, même élémentaires, puisent leur inspiration dans de la théorie très profonde. Tout comme les autres thèmes des olympiades, les attentes en arithmétique couvrent trois compétences : **de la connaissance théorique, des automatismes et de l'astuce**. L'arithmétique est sans doute le thème avec les parts les plus équilibrées de ces trois compétences. L'entraînement à fournir pour progresser en arithmétique doit donc être à l'image de cet équilibre : assimiler une grande quantité de théorie sans maîtriser les gestes d'hygiène est inefficace, et se borner à faire de la gymnastique sans développer plus d'astuce n'emmène pas très loin non plus. Ce polycopié a pour objectif de donner aux élèves les outils pour effectuer ce travail.

1.2 Comment utiliser le polycopié ?

Tout d'abord, on suppose acquises les notions d'arithmétique suivantes : lemme de Gauss, lemme d'Euclide, décomposition en facteurs premiers et les manipulations autour des congruences. On entend par là que les théorèmes sont connus parfaitement avec leurs hypothèses et que les élèves ont déjà pratiqué ces théorèmes sur au moins 10 exercices. Ce polycopié peut donc être attaqué par tout élève ayant suivi les cours du groupe A des stages de Valbonne, tels qu'ils ont été donnés entre 2020 et 2025. Toutefois, ce polycopié a été pensé pour les élèves seniors, et même s'il est accessible pour les élèves juniors, il n'est pas conçu pour aider à préparer les exercices de la JBMO.

Après cette introduction, ce polycopié est divisé en quatre section. **La section 2** veille à s'exercer sur les arguments de base de la théorie des nombres : divisibilité et taille, manipulation des nombres premiers, petit théorème de Fermat, théorie de l'ordre et théorème des restes chinois. Cette première partie est donc un outil pour pratiquer **les automatismes**.

La section 3 présente des outils plus avancés, dont on ne demande pas de connaître les preuves, et qui sont régulièrement utiles dans les problèmes d'olympiade. Les lemmes LTE, les théorèmes de Zsigmondy, le théorème de Dirichlet, le théorème de Schur et le postulat de Bertrand sont

énoncés dans une première sous-section. Dans la deuxième sous-section, on présente des théories plus techniques, qui ont assurément inspiré plusieurs exercices récents, et dont on espère que la compréhension permettra aux élèves de mieux appréhender ces problèmes. Cette section a donc pour but principal de renforcer **le bagage théorique** de l'élève.

La section 4 explore plusieurs sous-thèmes de l'arithmétique, comme les problèmes impliquant les suites ou les équations fonctionnelles entières. On aborde cinq tels sous-thèmes. Pour chacun, il ne s'agit pas d'apprendre de nouveaux théorèmes mais plutôt de détailler **les astuces** récurrentes et qui sont spécifiques à chaque thème.

Chaque sous-section contient d'abord sa part de théorie, avec des théorèmes et leur preuve et qui sont souvent accompagnés de remarques et de commentaires. On espère que ces commentaires éclaireront les élèves et leur permettront de prendre du recul sur le contenu des sections, et il est donc conseillé de lire en détail ces différents compléments, même pour les élèves qui connaîtraient déjà le contenu associé. On fournit aussi des exemples d'applications avec leurs solutions. Enfin, on conclut la sous-section par une batterie d'exercices, classés par difficulté croissante (les derniers exercices constituant souvent un véritable challenge).

Enfin, **la section 5** est un florilège d'exercices appelant ce qui a été vu dans les différentes sections. L'intérêt est de chercher des exercices en dehors du contexte d'application d'une notion spécifique et de se mettre dans les conditions des olympiades.

On recommande de commencer par lire la section 2. Une fois celle-ci maîtrisée, on peut s'attaquer aux deux sections suivantes. On ne recommande pas une lecture linéaire mais plutôt d'explorer et d'alterner entre les sections 3 et 4. La section 3, si elle est nouvelle pour l'élève, nécessitera sûrement plusieurs lectures approfondies. Les sous-sections de la section 4 sont dans un ordre assez quelconque en réalité, et les élèves peuvent les regarder dans l'ordre qui leur plaît.

En ce qui concerne les exercices, il n'est pas nécessaire de savoir faire tous les exercices d'une section avant d'attaquer la suivante. Au contraire, il est probablement mieux de commencer par les exercices d'application, de passer du temps sur les exercices suivants, puis, lorsqu'on sent que les exercices sont trop difficiles, de passer à la section suivante pour revenir plus tard sur les exercices sautés. La large gamme d'exercices a pour but de satisfaire tous les niveaux d'expérience, et il faudrait probablement plusieurs années pour maîtriser complètement tous les éléments du polycopié et pour venir à bout de tous les exercices. La vocation de ce polycopié est d'être un camarade de route pour ce long trajet.

Chaque exercice possède une solution rédigée dans le polycopié annexe de solutions. Des solutions alternatives sont même parfois ajoutées lorsqu'elles apportent des arguments différents.

Une nouveauté concernant les solutions, dont on espère qu'elle est une bonne nouveauté, est que **celles-ci sont parfois accompagnées de commentaires, en violet dans le texte**. Dans ces commentaires, on donne plusieurs informations que l'on juge pertinentes. Dans certains commentaires, on donne les intuitions derrière la solution, qui peut parfois sembler tombée du ciel. Dans d'autres commentaires, on donne les idées clées pour qu'elles ne soient pas noyées au milieu d'une solution technique, afin que les élèves lisant le commentaire identifient où se trouve la difficulté dans la solution qu'ils vont lire, difficulté qui n'est pas toujours reflétée par la longueur du texte. L'objectif de ces commentaires, c'est de pouvoir réserver une partie du texte à l'explication des idées, tout en gardant la satisfaction de fournir une solution nette.

Même s'ils se veulent détaillés, les corrigés sont rédigés pour être lus **après** avoir longuement cherché l'exercice. On ne sera pas surpris de voir certains raisonnements, arguments, calculs et

manipulations d'hypothèses abrégés lorsqu'ils sont supposés être limpides pour quiconque a déjà réfléchi à l'exercice.

Ainsi, même pour un élève qui a résolu l'exerice, il peut être intéressant de consulter la (parfois les) solution proposée dans le polycopié de solutions. Cela permet de vérifier sa solution mais aussi de regarder quels sont les autres arguments possibles et quelles sont les autres façons de les raconter. Nous sommes convaincus que voir d'autres arguments et d'autres rédactions que les siennes est plus efficace pour progresser que de s'en tenir aux idées qu'on a produites tout seul. La plupart du temps, les solutions proposées et leur rédaction ne sont pas celles de l'auteur du polycopié, mais sont celles qu'il a jugées les plus pertinentes.

1.3 Remerciements

Nombre des conseils, exercices, astuces, points de vue et même des sections entières sont largement inspirées des cours donnés lors de stages par d'autres animatheurs. J'aimerais citer Anatole Bouton, Thomas Budzinski, Maxime Chevalier, Gaëtan Dautzenberg, Antoine Derimay, Erik Desurmont, Aurélien Fourré, Eva Jacob, Vincent Jugé, Théo Lenoir, Arthur Léonard, Rémi Lesbats et Camille Pawlowski pour les cours et les exercices qu'ils ont préparés avec soin et dont ce polycopié a pu (parfois copieusement) s'inspirer. Plusieurs exercices proviennent d'envois et de tests de sélection donnés depuis 2016, dont j'ai souvent pu reprendre, au moins en partie, la solution des concepteurs de ces sujets, qui se reconnaîtront, et que je remercie donc également.

J'adresse enfin toute ma gratitude envers les différents bénévoles qui ont accepté, courageusement, de passer du temps à relire les différentes parties du polycopié. Merci pour leur vigilance et pour leurs (excellentes) suggestions : Anatole Bouton, Antoine Derimay, Erik Desurmont et Vincent Jugé.

1.4 Notations

On rappelle quelques notations et quelques appellations utilisées dans le polycopié.

- On note $\mathbb{N}$ l'ensemble des entiers positifs ou nuls, $\mathbb{N}^\star$ l'ensemble des entiers strictement positifs et $\mathbb{Z}$ l'ensemble des entiers relatifs.
- Pour tout entier n, on note parfois $[\![1, n]\!]$ l'ensemble $\{1, \dots, n\}$.
- Pour tout entier n, on appelle diviseur *propre* de n tout diviseur de n distinct de 1 et n.
- Étant donnés n entiers $a_1, \dots, a_n$, on appelle *plus grand commun diviseur* de ces entiers le plus grand entier qui divise chacun des a_i, et on le note $\mathrm{PGCD}(a_1, \dots, a_n)$. De même, on appelle *plus petit commun multiple* de ces entiers le petit entier strictement positif divisible par chacun des a_i, et on le note $\mathrm{PPCM}(a_1, \dots, a_n)$.
- Pour tout entier $n \geqslant 1$, on appelle *partie impaire* de n le plus grand diviseur impair de n. Il existe un unique couple (α, β) d'entiers tel que $\alpha \geqslant 0$, β est impair et $n = 2^\alpha \beta$. La partie impaire de n est précisément l'entier β.

2 Un peu de théorie

2.1 Divisibilité et taille, épisode 1 - les fondamentaux

Au tout début de l'apprentissage de la théorie des nombres, on découvre deux types d'arguments : les arguments de divisibilité, développés via la théorie des modulos ou le choix d'une bonne combinaison linéaire, et les arguments de taille. De **très** nombreux problèmes de théorie des nombres se ramènent à la maitrise de ces deux types d'arguments, éventuellement soutenus par les théorèmes élémentaires d'arithmétique (lemme de Gauss et d'Euclide, décomposition en facteurs premiers). Dans cette première sous-section, on propose de faire le tour de ces différents raisonnements à travers une collection d'exercices. Les premiers exercices sont des exercices visant à développer des automatismes, les exercices suivants ont pour objectif d'utiliser ces automatismes dans des contextes plus originaux et les derniers exercices représentent de plus gros challenges.

Voici les raisonnements très courants quand on cherche des arguments de divisibilité et taille :

- Si $a \mid b$, alors a divise toute combinaison linéaire de a et b. Pour tirer profit de cette information, on cherchera la combinaison linéaire dont la valeur est la plus petite possible puis on convertira cette divisibilité en une inégalité. La « bonne » combinaison linéaire peut être trouvée plus facilement en passant par les modulos, comme dans l'exemple suivant :

Exemple 1. Déterminer tous les entiers $n \geqslant 1$ tels que $n+2$ divise n^3+3n^2+3.

Solution. Plutôt que de chercher la combinaison linéaire adéquate, à savoir que si n est solution, alors $n+2 \mid n^3+3n^2+3-(n^2+n-2)(n+2)$, on peut directement dire que $n \equiv -2 \mod n+2$, et donc que

$$0 \equiv n^3+3n^2+3 \equiv (-2)^3+3\cdot(-2)^2+3 \equiv 7 \mod n+2,$$

ce qui implique que $n+2 \mid 7$. Comme les diviseurs positifs de 7 sont 1 et 7 et que $n+2 \geqslant 3$, on déduit que $n+2=7$ puis que $\boxed{n=5}$. Il reste à vérifier qu'on a bien $5+2 \mid 5^3+3\cdot 5^2+3=203$, ce qui est le cas car $203=29\times 7$. L'entier 5 est donc l'unique solution recherchée.

- Si $a \mid b$ et $b \neq 0$, alors $|a| \leqslant b$. Ainsi, si b est divisible par un très grand nombre, il sera sûrement nul. Une variante de cet argument est que, pour montrer une égalité entre deux expressions A et B, on peut montrer que $A-B$ admet un diviseur très grand ou une infinité de diviseurs. Trouver un grand diviseur peut parfois consister à trouver plusieurs petits diviseurs premiers entre eux deux à deux, car alors leur produit est un nouveau diviseur plus grand.
- Si $na \leqslant b < (n+1)a$ et si b est un multiple de a, alors $b=na$. Notons qu'à l'inverse, si $b > na$ et si b est un multiple de a, alors $b \geqslant (n+1)a$, ce qui donne une meilleure estimation de la taille de b.
- Travailler avec des diviseurs premiers plutôt qu'avec des entiers composés. L'avantage est qu'il est alors plus facile d'utiliser le lemme d'Euclide et le lemme de Gauss.

Exemple 2. Soient a et b des nombres premiers entre eux. Montrer que $a+b$ et ab sont premiers entre eux.

Solution. Soit p un éventuel diviseur premier de $\mathrm{PGCD}(ab, a+b)$. Alors $p \mid ab$, donc $p \mid a$ ou $p \mid b$. Mais si $p \mid a$, puisque $p \mid a+b$, on déduit que $p \mid b$, ce qui contredit que $\mathrm{PGCD}(a,b) = 1$. On montre de même que si $p \mid b$ alors $p \mid a$. Dans les deux cas, p divise a et b. Cette contradiction implique que $\mathrm{PGCD}(ab, a+b)$ n'admet pas de facteur premier. Il vaut donc 1, ce qui correspond au résultat demandé.

➢ Un carré parfait ne peut pas être compris entre deux carrés consécutifs. L'application très concrète se trouve dans les exercices faisant intervenir des expressions qui sont supposées être des carrés parfaits. Pour identifier ces expressions, on les encadre par des carrés parfaits plus simples, et proches. Si l'encadrement est réussi, on obtient la valeur exacte du carré parfait.

Exemple 3. *(Pan African Olympiad 2022, P2)* Déterminer tous les triplets (a,b,c) d'entiers strictement positifs avec $a \geqslant b \geqslant c$ tels que a^2+3b, b^2+3c et c^2+3a sont des carrés parfaits.

Solution. Notons que $a^2 < a^2+3b < a^2+4a+4 = (a+2)^2$. Pour que a^2+3b soit un carré parfait, il faut donc que $a^2+3b = (a+1)^2$, puisqu'il s'agit du seul carré parfait compris entre a^2 et $(a+2)^2$. On déduit après développement que $\boxed{3b = 2a+1}$. De la même façon, on obtient que $\boxed{3c = 2b+1}$. On déduit que $\boxed{9c = 4a+5}$. Il y a alors plusieurs façons de conclure à partir de l'hypothèse sur c^2+3a. On donne la suivante. L'égalité implique en particulier que $a < \dfrac{9}{4}c$. On a donc l'encadrement

$$c^2 < c^2+3a < c^2+\frac{27}{4}c < c^2+8c+16 = (c+4)^2,$$

dont on déduit que $c^2+3a \in \{(c+1)^2, (c+2)^2, (c+3)^2\}$. Il reste a distinguer les cas :

- Si $c^2+3a = (c+1)^2$, alors $3a = 2c+1$. Les deux équations $3a = 2c+1$ et $9c = 4a+5$ forment un système de deux équations à deux inconnues, dont la résolution aboutit à $a = c = 1$. On conclut que $b = 1$. Réciproquement, le triplet $\boxed{(1,1,1) \text{ est bien solution}}$ puisque chacun des nombres a^2+3b, b^2+3c et c^2+3a vaut 4.
- Si $c^2+3a = (c+2)^2$, alors $3a = 4c+4$. Les deux équations $3a = 4c+4$ et $9c = 4a+5$ forment un système de deux équations à deux inconnues, dont la résolution aboutit à $c = 31/11$, ce qui est absurde.
- Si $c^2+3a = (c+3)^2$, alors $3a = 6c+9$ et $a = 2c+3$. En combinant avec l'équation $9c = 4a+5$, on trouve $c = 17$ et $a = 37$. Puisque $3b = 2a+1$, on déduit que $b = 25$. Réciproquement, le triplet $\boxed{(37,25,17) \text{ est bien solution}}$ puisque $a^2+3b = 38^2$, $b^2+3c = 26^2$ et $c^2+3a = 20^2$.

Le problème a donc deux solutions, à savoir les deux triplets $(1,1,1)$ et $(17,25,37)$.

➢ Les croissances comparées d'expressions classiques sont un excellent outil pour des arguments de taille : si P est un polynôme, et $a \geqslant 2$ est un entier, alors pour n suffisamment grand, $P(n) < a^n < n!$. Ainsi, en présence d'inégalités inverses, on déduit que n prend un nombre fini de valeurs (qu'il ne reste plus qu'à tester).

- ➢ Il n'y a pas de suite strictement décroissante d'entiers strictement positifs. Ainsi, dans le cadre d'un problème de suite, si on trouve une suite auxiliaire décroissante d'entiers positifs, celle-ci est constante à partir d'un certain rang. C'est particulièrement pertinent dans les problèmes du type « considérons une suite infinie d'entiers telle que... ». Pour chercher la contradiction dans ce genre de problème, on peut chercher à encadrer les termes de la suite, jusqu'à encadrer un terme de la suite par deux entiers consécutifs. On peut aussi chercher à produire une suite décroissante d'entiers. Cela nécessite souvent de remanipuler algébriquement les suites.
- ➢ Pour montrer qu'un entier a divise un entier b, il peut être pertinent d'introduire la division euclidienne de b par a : en écrivant $b = aq + r$, avec $0 \leqslant r < a$, on se ramène à montrer que $r = 0$. Il s'agit alors généralement de raisonner autour de la taille de r.

Exemple 4. Soient a et b deux entiers strictement positifs et $n \geqslant 2$ un entier. Montrer que $n^a - 1 \mid n^b - 1$ si et seulement si $a \mid b$.

Solution. $\boxed{\Leftarrow :}$ Si a divise b, on pose $k = b/a$. Alors $n^a - 1 \mid n^b - 1$ en vertu de la factorisation

$$n^b - 1 = (n^a - 1)(n^{a(k-1} + n^{a(k-2)} + \ldots + n^a + 1)$$

ou encore de la congruence

$$n^b = (n^a)^k \equiv 1^k = 1 \mod n^a - 1.$$

$\boxed{\Rightarrow :}$ Supposons que $n^a - 1 \mid n^b - 1$. On effectue la division euclidienne de b par a en introduisant deux entiers q et r tels que $0 \leqslant r < a$ et $b = aq + r$. Puisque $n^a \equiv 1 \mod n^a - 1$, la relation $n^b - 1 \equiv 0 \mod n^a - 1$ implique

$$0 \equiv n^{aq+r} - 1 = (n^a)^q n^r - 1 \equiv n^r - 1 \mod n^a - 1.$$

Or $0 \leqslant n^r - 1 < n^a - 1$, donc $n^r = 1$ et $r = 0$, donc $\boxed{a \mid b}$.

On pourra pratiquer ces conseils à travers les exercices suivants.

Exercice 2.1. Soient a, b, n des entiers tels que pour tout $k > b$, on a $k - b \mid k^n - a$. Montrer que $a = b^n$.

Exercice 2.2. Soient p, m et n des entiers strictement positifs avec p premier impair tels que $p^2 + m^2 = n^2$. Montrer que $n = m + 1$.

Exercice 2.3. Soient $k, m, n \geqslant 1$ des entiers tels que $m^2 + n = k^2 + k$. Montrer que $m \leqslant n$.

Exercice 2.4. Soient a et b des entiers strictement positifs. Montrer que $2^a + 1$ divise $2^b + 1$ si et seulement si $a \mid b$ et b/a est impair.

Exercice 2.5. (APMO 2011 P1) Soient a, b et c des entiers strictement positifs. Montrer que les trois nombres $a^2 + b + c, b^2 + c + a$ et $c^2 + a + b$ ne peuvent pas être tous les trois des carrés parfaits.

Exercice 2.6. Soient a et b des entiers tels que $a > b$. On suppose que $a - b \mid a^2 + b$. Montrer que

$\frac{a+1}{b+1} \leqslant \mathrm{PGCD}(a,b)+1$.

Exercice 2.7. *(Baltic Way 2024)* Soit (a_n) une suite d'entiers supérieurs ou égaux à 2 telle que, pour tout $n \geqslant 1$, $a_{n+2} \mid a_n + a_{n+1}$. Montrer qu'il existe un nombre premier qui divise une infinité de termes de la suite.

Exercice 2.8. *(Nordic MO 2016)* Déterminer toutes les suites d'entiers $(a_1, \ldots, a_{2016})$ telles que les entiers sont tous bornés par 2016 et $i+j \mid ia_i + ja_j$ pour tout $i, j \in \{1, \ldots, 2016\}$.

Exercice 2.9. Déterminer les couples (m,n) d'entiers tels que $mn-1$ est non nul et $mn-1 \mid n^3-1$.

Exercice 2.10. Déterminer tous les entiers n tels que $2^n + n \mid 8^n + n$.

Exercice 2.11. On définit la suite $a_1, a_2, \ldots$ de la façon suivante : $a_1 = 63$ et, pour tout entier $n \geqslant 2$, a_n est le plus petit entier multiple de n qui soit supérieur ou égal à a_{n-1}. Montrer que les termes de la suite sont deux à deux distincts.

Exercice 2.12. *(Iran Round 2 2010)* Soient $a > b$ deux entiers strictement positifs. On suppose que $\mathrm{PGCD}(a-b, ab+1) = 1$ et que $\mathrm{PGCD}(a+b, ab-1) = 1$. Montrer que $(a-b)^2 + (ab+1)^2$ n'est pas un carré parfait.

Exercice 2.13. *(Iran MO 2025 Round 2)* Déterminer tous les entiers n tels que, pour tout diviseur premier p de n, $n+p$ est un carré parfait.

Exercice 2.14. *(OFM 2024)* Déterminer tous les entiers $n \geqslant 2$ pour lesquels il existe n entiers $a_1, \ldots, a_n$ supérieurs ou égaux à 2 et tels que $a_i \mid a_j^2 + 1$ lorsque $i \neq j$.

Exercice 2.15. *(IMO SL 2022 N2)* Déterminer tous les entiers $n > 2$ tels que

$$n! \mid \prod_{p<q\leqslant n} (p+q),$$

où le produit est pris sur l'ensemble des paires (p,q) telles que $p < q \leqslant n$ sont des nombres premiers.

Exercice 2.16. *(EGMO 2023 P5)* Soit $s \geqslant 2$ un entier. Pour tout entier k, on définit son *twist* k' de la façon suivante : si $k = as+b$ est la division euclidienne de k par s, alors $k' = bs+a$. Pour un entier strictement positif n, on définit la suite $(d_i)_i$ comme suit : $d_1 = n$, et d_{i+1} est le twist de d_i pour tout $i \geqslant 1$.
Montrer que la suite contient 1 si et seulement si le reste de la division de n par s^2-1 est 1 ou s.

Exercice 2.17. *(Balkan MO 2024 P3)* Soient a et b des entiers strictement positifs distincts tels que $3^b + 2 \mid 3^a + 2$. Montrer que $a > b^2$.

Exercice 2.18. *(IMO SL 2016 N4)* Soient n, m, k et ℓ des entiers strictement positifs tels que $n \neq 1$ et $n^k + mn^\ell + 1 \mid n^{k+\ell} - 1$. Montrer que

- soit $m = 1$ et $\ell = 2k$,
- soit $\ell \mid k$ et $m = \dfrac{n^{k-\ell}-1}{n^\ell - 1}$.

Exercice 2.19. (Envoi Pot Pourri 2019-2020 P8) Déterminer le plus petit entier $n \geqslant 2$ tel qu'il existe des entiers strictement positifs $a_1, \ldots, a_n$ tels que

$$a_1^2 + \ldots + a_n^2 \mid (a_1 + \ldots + a_n)^2 - 1.$$

Exercice 2.20. (IMO 2015 P2) Déterminer tous les triplets (a, b, c) d'entiers strictement positifs tels que les entiers

$$ab - c, \quad bc - a, \quad ca - b$$

sont des puissances de 2.

2.2 Valuation p–adique

Dans la sous-section précédente, on a (brièvement) évoqué l'intérêt d'effectuer les raisonnements de divisibilités sur les facteurs premiers de n plutôt que sur n lui-même. Toutefois, s'en tenir aux facteurs premiers est parfois insuffisant pour traiter les hypothèses à disposition. Par exemple, pour montrer que deux nombres sont égaux, il est insuffisant de montrer qu'ils ont les mêmes facteurs premiers. De même, pour montrer que d divise a, il est insuffisant de montrer que tout diviseur premier de d divise a.

Dans cette section, on s'entraîne donc à manipuler les divisibilités mêlant des puissances de nombres premiers. Encore une fois, la théorie donnée reste très élémentaire et l'on se concentre surtout sur ses applications dans des cadres de plus en plus originaux.

On rappelle la définition de valuation p-adique :

Définition 2.1. Soit n un entier relatif non nul et p un nombre premier. La valuation p-adique de n, notée $v_p(n)$, est le plus grand entier k tel que $p^k \mid n$.

Concrètement, si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ est la décomposition en facteurs premiers de n, alors $\alpha_i = v_{p_i}(n)$.

Démontrer soi-même les propriétés suivantes est un excellent exercice pour se familiariser avec la notion :

Proposition 2.2. Soient a et b deux entiers et p un nombre premier :

$$v_p(ab) = v_p(a) + v_p(b), \quad v_p(a+b) \geqslant \min(v_p(a), v_p(b)) \quad \text{avec égalité si } v_p(a) \neq v_p(b).$$

La caractérisation suivante donne une stratégie pour montrer qu'un entier en divise un autre à l'aide des valuations p-adiques, ainsi qu'une stratégie pour montrer qu'un entier est une puissance parfaite.

Proposition 2.3. Soient a et b des entiers strictement positifs. Alors on a l'équivalence :

$$a \mid b \quad \iff \quad v_p(a) \leqslant v_p(b) \text{ pour tout nombre premier } p.$$

En particulier, $a = b$ si et seulement si $v_p(a) = v_p(b)$ pour tout nombre premier p.

Soit $k \geqslant 1$. l'entier a est une puissance $k-$ème si et seulement si $k \mid v_p(a)$ pour tout nombre premier p.

Exemple 5. Soient a et b deux entiers. Montrer que si $d \mid a+b$ et $d^2 \mid ab$, alors $d \mid a$ et $d \mid b$.

Solution. Il suffit de montrer que, pour tout facteur premier p de d, le nombre $p^{v_p(d)}$ divise a et b ; autrement dit, que $v_p(d) \leqslant v_p(a)$ et $v_p(d) \leqslant v_p(b)$. On fixe dans la suite un tel facteur premier p.

D'après l'énoncé, $v_p(d) \leqslant v_p(a+b)$ et $2v_p(d) \leqslant v_p(ab) = v_p(a) + v_p(b)$. On déduit que $v_p(d) \leqslant v_p(a)$ ou $v_p(d) \leqslant v_p(b)$. Par symétrie des rôles de a et b, on peut supposer que $v_p(d) \leqslant v_p(a)$. Mais alors $p^{v_p(d)} \mid a$ et $p^{v_p(d)} \mid a+b$, donc $p^{v_p(d)} \mid b$ et $v_p(d) \leqslant v_p(b)$, ce qui conclut.

On peut retravailler cet exemple avec l'exercice suivant.

Exercice 2.21. Soit $a, b, c \geqslant 1$ des entiers tels que $a^b \mid b^c$ et $a^c \mid c^b$. Montrer que $a^2 \mid bc$.

Formules pour les PGCD et PPCM

La valuation p-adique intervient également dans les formules autour du PGCD et du PPCM d'entiers :

Proposition 2.4. Soient $a_1, \ldots, a_n$ des entiers. On dispose des formules suivantes :

$$\mathrm{PGCD}(a_1, a_2, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a_i), 1 \leqslant i \leqslant n\}}$$

$$\mathrm{PPCM}(a_1, a_2, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\max\{v_p(a_i), 1 \leqslant i \leqslant n\}}$$

Une conséquence fameuse est l'égalité

$$ab = \mathrm{PGCD}(a,b)\mathrm{PPCM}(a,b),$$

qui n'admet pas d'équivalent simple pour le produit de n entiers.

On rappelle à cette occasion qu'il ne faut pas confondre « premiers entre eux deux à deux », et « premiers entre eux dans leur ensemble ». Les nombres $2, 3, 4$ sont premiers entre eux dans leur ensemble, mais pas premiers entre eux deux à deux.

Cette deuxième formule pour $\mathrm{PGCD}(a,b)$ donne une deuxième façon d'aborder des problèmes de PGCD : la première était d'utiliser la divisibilité des combinaisons linéaires de a et b, la deuxième

est de raisonner avec les facteurs premiers de a et b.

Formule de Legendre

Dans un problème faisant intervenir des factorielles, il peut être utile de calculer $v_p(n!)$, à l'aide de la formule qui suit :

Proposition 2.5 (Formule de Legendre)**.** Soit p un nombre entier et $n \geqslant 1$ un entier. Alors

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

Notons que lorsque k est assez grand, $n < p^k$ et $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. Ainsi, la somme infinie ci-dessus contient en réalité un nombre fini de termes non nuls.

Démonstration. Considérons l'ensemble $A = \{(m, p^k), 1 \leqslant m \leqslant n, 1 \leqslant k \leqslant v_p(m)\}$. Si l'on fixe m, il y a exactement $v_p(m)$ éléments de A de la forme (m, p^k), ce qui veut dire que $\boxed{|A| = v_p(1) + \ldots + v_p(n) = v_p(n!)}$. Si l'on fixe k, le nombre d'entiers m tels que $(m, p^k) \in A$ est le nombre de multiples de p^k inférieurs ou égaux à n, c'est-à-dire $\lfloor n/p^k \rfloor$. On a donc aussi

$$|A| = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots .$$

Ceci donne la formule de Legendre.

Ce double comptage peut également se résumer par l'interversion de sommes suivante :

$$v_p(n!) = v_p(n) + \ldots + v_p(1) = \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \sum_{k=1}^{v_p(m)} 1 = \sum_{k \geqslant 1} \sum_{m \leqslant n, v_p(m) \geqslant k} 1 = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

On en déduit l'estimation suivante, déjà apparue dans plusieurs exercices de compétitions :

Corollaire 2.6. Soit $n \geqslant 1$ et p un nombre premier. Alors

$$v_p(n!) < \frac{n}{p-1}.$$

Démonstration. Soit r un entier tel que $p^r > n$. On utilise la majoration $\lfloor x \rfloor \leqslant x$ dans la formule de Legendre ainsi que l'expression d'une somme géométrique :

$$\begin{aligned} v_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots \\ &\leqslant \frac{n}{p} + \frac{n}{p^2} + \dots + \frac{n}{p^r} = n\left(\frac{1}{p} + \dots + \frac{1}{p^r}\right) \\ &= n \cdot \frac{1}{p} \cdot \frac{1 - \frac{1}{p^r}}{1 - \frac{1}{p}} < n \cdot \frac{1}{p} \cdot \frac{1}{1 - 1/p} = \frac{n}{p-1}. \end{aligned}$$

La formule de Legendre admet également une forme plus compacte, permettant notamment de retrouver immédiatement la majoration précédente et qu'on pourra utiliser librement.

Corollaire 2.7. Soit $n \geqslant 1$ un entier, p un nombre premier et $s_p(n)$ la somme des chiffres de n lorsqu'il est écrit dans la base p. On a

$$v_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Démonstration. On écrit $n = a_r p^r + \dots + a_1 p + a_0$ dans la base p, avec $0 \leqslant a_k \leqslant p-1$ pour tout $0 \leqslant k \leqslant r$. On a alors $\lfloor n/p^k \rfloor = a_r p^{r-k} + \dots + a_k$ pour tout $0 \leqslant k \leqslant r$, et $\lfloor n/p^k \rfloor = 0$ dès que $k \geqslant r+1$. La formule de Legendre et une interversion de sommes impliquent donc :

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{r} \left\lfloor \frac{n}{p^k} \right\rfloor \\ &= (a_r p^{r-1} + \dots + a_1) + \dots + (a_r p^{r-k} + \dots + a_k) + \dots + a_r \\ &= a_r(p^{r-1} + \dots + 1) + \dots + a_k(p^{k-1} + \dots + 1) + \dots + a_1 \\ &= \sum_{j=1}^{r} a_j \frac{p^j - 1}{p-1} \\ &= \frac{1}{p-1}\left(\sum_{j=1}^{r} a_j p^j - \sum_{j=1}^{r} a_j\right) = \frac{1}{p-1}\left(\sum_{j=0}^{r} a_j p^j - \sum_{j=0}^{r} a_j\right) \\ &= \frac{n - s_p(n)}{p-1}. \end{aligned}$$

On pourra appliquer la formule de Legendre sur les exemples suivants :

Exercice 2.22. Par combien de zéros termine 2025! ?

Exercice 2.23. Montrer que 2^n ne divise jamais $n!$ mais 2^{n-1} divise $n!$ pour une infinité de n.

Exercice 2.24. (IMO SL 2023 N3) Pour tout entier $k \geqslant 2$ et tout entier $n \geqslant 1$, on note $E_k(n)$ le plus grand entier r tel que $k^r \mid n!$. Montrer qu'il existe une infinité d'entiers n tels que $E_{10}(n) > E_9(n)$ et une infinité d'entiers n tels que $E_{10}(n) < E_9(n)$.

Exercices

Voici un petit résumé des conseils avant de passer aux exercices.

- Lorsqu'on regarde la divisibilité de a par n, on peut regarder plutôt la divisibilité de a par les facteurs premiers de n, mais aussi et surtout la divisibilité de a par $p^{v_p(n)}$.
- Il est intéressant d'être capable de construire des entiers dont la valuation p-adique est déterminée. Par exemple, si on sait que n est divisible par p^2, alors $n+p$ a pour valuation p-adique 1. Voici un exemple d'une telle gymnastique.

Exemple 6. Soit P un polynôme à coefficients entiers. On suppose qu'il existe un entier n_0 tel que $v_7(P(n_0)) = 3$. Montrer qu'il existe une infinité d'entiers n tels que $v_7(P(n)) = 3$.

Solution. On rappelle l'identité $a - b \mid P(a) - P(b)$.
L'identité implique en particulier que, pour tout entier $k \geqslant 1$, $7^4 \mid P(n_0+7^4k) - P(n_0)$.
On a alors, puisque $v_7(P(n_0)) \neq v_7(P(n_0 + 7^4k) - P(n_0))$,

$$\begin{aligned} v_7(P(n_0 + 7^4k)) &= v_7(P(n_0) + P(n_0 + 7^4k) - P(n_0)) \\ &= \min(v_7(P(n_0)), v_7(P(n_0 + 7^4k) - P(n_0))) = 3. \end{aligned}$$

On déduit que $\boxed{v_7(P(n_0 + 7^4k)) = 3}$, ce qui répond au problème.

- On n'oubliera pas d'appliquer tous ces raisonnements au plus petit facteur premier p divisant n, ou au plus grand, pour avoir encore plus d'informations.

Exercice 2.25. (Pologne MO 2023 Round 2) Déterminer tous les entiers b avec la propriété suivante : il existe un entier a et des entiers k et ℓ distincts tels que $b^{k+\ell}$ divise $a^k + b^\ell$ et $a^\ell + b^k$.

Exercice 2.26. (Caucase MO 2024 Junior) Soient 10 entiers strictement positifs de somme 1000. On suppose que le produit de leurs factorielles est une puissance 10−ème. Montrer que les 10 entiers sont égaux.

Exercice 2.27. (Roumanie TST 2007) Soit $n \geqslant 3$ un entier naturel et soient $a_1, a_2, \ldots, a_n$ des entiers naturels premiers entre eux dans leur ensemble tels que $\mathrm{PPCM}(a_1, a_2, \ldots, a_n)$ divise $a_1 + a_2 + \ldots + a_n$. Montrer que le produit $a_1 \times a_2 \times \ldots \times a_n$ divise $(a_1 + a_2 + \ldots + a_n)^{n-2}$.

Exercice 2.28. Soit $a_1, a_2, \ldots$ une suite d'entiers strictement positifs telle que, pour toute paire (i, j) d'entiers distincts, $\mathrm{PGCD}(a_i, a_j) = \mathrm{PGCD}(i, j)$. Montrer que, pour tout indice i, $a_i = i$.

Exercice 2.29. Rémi écrit n entiers strictement positifs $a_1, \ldots, a_n$ au tableau. Toutes les minutes, Rémi peut remplacer un entier a écrit au tableau par N/a, où N désigne le PPCM des entiers écrits au tableau. Montrer que Rémi peut faire en sorte que tous les nombres écrits au tableau soient des 1 après un nombre fini d'opérations.

Exercice 2.30. (EGMO 2020 P1) Les entiers $a_0, \ldots, a_{3030}$ satisfont la relation

$$2a_{n+2} = a_{n+1} + 4a_n$$

pour tout $n \in \{0, 1, 2, \ldots, 3028\}$. Montrer qu'au moins l'un des a_n est divisible par 2^{2020}.

Exercice 2.31. *(JBMO SL 2021 N4)* Alice et Bob jouent au jeu suivant : Alice choisit un ensemble infini S de nombres premiers qu'elle communique à Bob. Ensuite, Bob choisit une suite $x_1, x_2, \ldots$ infinie d'entiers strictement positifs qu'il communique à Alice. Alice choisit alors un entier M strictement positif et un nombre premier p de S, qu'elle communique à Bob.

Bob gagne si il existe un entier N tel que, pour tout $n \geqslant N$, x_n est divisible par p^M. Sinon, Alice gagne.

Quel joueur dispose d'une stratégie gagnante ?

Exercice 2.32. *(RMM 2019 P1)* Alice et Bob jouent au jeu suivant : Alice commence par écrire un entier au tableau. Ensuite, les joueurs jouent chacun à leur tour en commençant par Bob. Pendant son tour, Bob peut remplacer l'entier n écrit au tableau par n'importe quel entier de la forme $n - a^2$, où a est un entier positif. Alice, pendant son tour, peut remplacer l'entier n par n'importe quel entier de la forme n^ℓ, où ℓ est un entier positif. Bob gagne s'il parvient à écrire 0 au tableau.

Alice peut-elle empêcher Bob de gagner ?

Exercice 2.33. *(USAJMO 2022 P1)* Déterminer tous les entiers m pour lesquels il existe une suite arithmétique $a_1, a_2, \ldots$ et une suite géométrique $g_1, g_2, \ldots$ telles que $a_2 - a_1$ n'est pas divisible par m mais $a_n - g_n$ est divisible par m pour tout indice $n \geqslant 1$.

Exercice 2.34. *(IMO 2026 P1)* On considère 2026 entiers strictement plus grand ue 1 sur un tableau. Chaque minute, tant que cela est possible Alice choisit deux entiers m et n inscrits au tableau et tous les deux strictement plus grands que 1 et les remplace par les deux entiers

$$\mathrm{PGCD}(m, n) \quad \text{et} \quad \frac{\mathrm{PPCM}(m, n)}{\mathrm{PGCD}(m, n)}.$$

1. Montrer que, quels que soient les choix d'Alice, au bout d'un nombre fini de minutes, il y a exactement un entier M strictement plus grand que 1 parmi les entiers du tableau.
2. Montrer que la valeur de M est indépendante des choix d'Alice.

Exercice 2.35. *(2017 ELMO P1)* Soit n un entier positif impair, soient $a_1, \ldots, a_n$ des entiers strictement positifs et soit P leur produit. Montrer que

$$\mathrm{PGCD}(a_1^n + P, a_2^n + P, \ldots, a_n^n + P) \leqslant 2\mathrm{PGCD}(a_1, \ldots, a_n)^n.$$

Exercice 2.36. *(IMO SL 2007 N2)* Soient $b, n > 1$ des entiers. On suppose que pour tout entier k, il existe un entier a_k tel que $b - a_k^n$ est divisible par k. Montrer qu'il existe un entier A tel que $b = A^n$.

Exercice 2.37. *(Balkan MO SL 2025 N1)* Soit k un entier strictement positif et $n_1, \ldots, n_k$ des entiers strictement supérieurs à 1 et deux à deux distincts. On suppose qu'il existe un entier strictement positif a tel que

$$n_1! + \ldots + n_k! = a^{n_1}.$$

Montrer que l'un au moins des entiers $n_1, \ldots, n_k$ est premier.

2.3 Travailler modulo p, épisode 1 - état d'esprit

2.3.1 Rappels sur la notion d'inversible

Dans cette sous-section, on redonne la définition d'inverse modulo n et les premières propriétés de la fonction indicatrice d'Euler φ. Ces propriétés sont disponibles dans de nombreuses ressources de la POFM, et l'objectif de cette sous-section est uniquement de rendre le polycopié auto-contenu.

Après les arguments de divisibilité, l'autre idée principale que l'on apprend en mathématiques olympiques est la notion de congruence et de modulo. Cet outil est très puissant pour *simplifier* le problème : si l'équation n'a pas de solution modulo n, c'est qu'elle ne possède pas de solution. Il reste alors à choisir le bon entier n de sorte à simplifier la juste quantité de termes de l'équation. Une fois cette idée engagée, on se ramène donc à étudier un nombre fini d'entiers, à savoir les restes modulo n.

Un cours sur les modulos nous apprend les trois axiomes suivants :

- ☞ Si $a \equiv b \mod n$, alors $a + c \equiv b + c \mod n$,
- ☞ Si $a \equiv b \mod n$, alors $ac \equiv bc \mod n$,
- ☞ Si $a \equiv b \mod n$, alors $a^c \equiv b^c \mod n$.

Autrement dit, les opérations d'addition/soustraction, multiplication et passage à la puissance sont compatibles avec la congruence. Le même cours sur les modulos nous apprendra également que ce n'est pas aussi simple quand il s'agit de diviser : si $ac \equiv bc \mod n$, on ne peut pas toujours écrire $a \equiv b \mod n$.

Heureusement, la notion de division modulo n est loin d'être opaque, et on est capable non seulement de complètement caractériser les entiers c vérifiant « $ac \equiv bc \mod n \Rightarrow a \equiv b \mod n$ » (il s'agit des inversibles modulo n), mais en plus d'expliciter ce qu'il se passe pour des c non inversibles. C'est ce que l'on fait ici.

Définition 2.8 (Nombre inversible modulo n)**.** Soit $n \geqslant 1$ un entier. Un entier a est dit *inversible modulo* n s'il existe un entier c tel que $ac \equiv 1 \mod n$.

Cet entier c est appelé *inverse de* a *modulo* n et est parfois noté a^{-1}, notamment lorsqu'il n'y a pas d'ambiguïté.

Exemple 7. 2 est inversible modulo 5 car $2 \cdot 3 \equiv 1 \mod 5$, donc 3 est un inverse de 2 modulo 5. On vérifie que 8 est également un inverse de 2 modulo 5. En revanche, 2 n'est pas inversible modulo 10 : un entier de la forme $2c$ est pair et ne peut donc être congru à 1 modulo 10.

L'écriture a^{-1} doit être utilisée uniquement lorsque la situation est sans ambiguïté : il doit être clair, pour nous comme pour la personne qui nous lit, que a^{-1} désigne l'inverse de a modulo n, et non le nombre $1/a$ ou l'inverse de a modulo un autre entier.

Comme annoncé, les inversibles sont les éléments par lesquels on peut diviser modulo n :

Proposition 2.9. Soit n un modulo et a un entier inversible modulo n. Si deux entiers x et y vérifient $xa \equiv ya \mod n$, alors $x \equiv y \mod n$.

Démonstration. Soit c l'inverse de a modulo n. Il suffit de multiplier les deux côtés de la congruence par c :

$$x \underbrace{ac}_{\equiv 1} \equiv y \underbrace{ac}_{\equiv 1} \mod n \quad \text{soit} \quad x \equiv y \mod n.$$

La propriété suivante caractérise les entiers qui sont inversibles modulo n :

Proposition 2.10. Soit $n \geqslant 1$ un entier et a un entier. L'entier a est inversible modulo n si et seulement a est premier avec n.

Démonstration. On procède par double équivalence :
$\boxed{\Leftarrow :}$ on suppose que a est premier avec n. D'après le théorème de Bézout, il existe deux entiers u et v tels que $au + nv = 1$. En passant cette égalité modulo n, on déduit $au \equiv 1 \mod n$, donc a est inversible.
$\boxed{\Rightarrow :}$ on suppose que a est inversible modulo n. Soit c un inverse pour a modulo n. Comme $ac \equiv 1 \mod n$, il existe un entier v tel que $ac - 1 = nv$. Si on note $d = \mathrm{PGCD}(a, n)$, alors $d \mid ac - nv = 1$, donc $d = 1$ et a et n sont premiers entre eux.

Le cas où $n = p$ un est nombre premier est alors particulièrement intéressant :

Corollaire 2.11. Soit p un nombre premier. Alors tous les entiers de $\{1, \ldots, p-1\}$ sont inversibles modulo p.

Avec la preuve de la proposition 2.6, on comprend comment calculer l'inverse de a modulo n : il suffit de trouver un couple (u, v) de Bézout pour a et n, et l'entier u est un inverse pour a.

Exercice 2.38. Trouver un inverse pour 12 modulo 37.

On termine ce tour d'horizon en soulevant une ambiguïté : on a toujours parlé *d'un* inverse modulo n, ce qui laisse la question de savoir si un même entier peut avoir plusieurs inverses. Cette question est répondue dans le corollaire suivant, découlant de la Proposition 2.5 :

Corollaire 2.12. Soit $n \geqslant 1$ et a un entier. Si b et c sont deux inverses de a modulo n, alors $b \equiv c$.
Ainsi, si a est inversible, il a un unique inverse parmi les nombres $\{0, \ldots, n-1\}$.

On explique désormais comment se passe la division dans le cas des entiers a non inversibles. C'est résumé dans la propriété suivante :

Proposition 2.13. Soit $n \geqslant 1$ et a un entier. On note $d = \mathrm{PGCD}(a, n)$. Soient x et y deux entiers tels que $ax \equiv ay \mod n$. Alors $x \equiv y \mod \frac{n}{d}$.

Démonstration. Soient a' et n' des entiers tels que $a = da'$ et $n = dn'$. Comme $d = \mathrm{PGCD}(a, n)$, a' et n' sont premiers entre eux.

Puisque $ax \equiv ay \mod n$, il existe un entier k tel que $kn = a(x - y)$. En simplifiant par d, cette équation devient $kn' = a'(x - y)$. Comme n' est premier avec a', d'après le lemme de Gauss, n' divise $x - y$. Ceci donne $x \equiv y \mod n'$, ce qui correspond à la congruence annoncée.

La conclusion, c'est qu'il faut être vigilant lorsqu'on souhaite diviser modulo n.

On termine en rappelant les propriétés élémentaires de l'indicatrice d'Euler φ.

Définition 2.14. Soit $n \geqslant 1$. On note $\varphi(n)$ le nombre d'entiers de $\{1, \ldots, n-1\}$ premiers avec n.

La fonction φ qui à n associe le nombre $\varphi(n)$ est appelée *indicatrice d'Euler*.

On fait remarquer d'emblée que $\varphi(n)$ est le nombre d'éléments de $\{1, \ldots, n-1\}$ qui sont inversibles modulo n. On remarque également que si p est premier, $\varphi(p) = p - 1$.

On peut calculer explicitement $\varphi(n)$ en fonction de la décomposition en facteurs premiers de n.

Théorème 2.15. Soit $n \geqslant 1$ un entier et $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers.

Alors

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

Démonstration. Pour tout entier $k \geqslant 1$, on note A_k l'ensemble des entiers de l'intervalle $[\![1, n]\!]$ qui sont divisibles par k. On remarque que si $k \mid n$, alors $|A_k| = n/k$.

Si un entier $m \in [\![1, n]\!]$ n'est premier avec n, c'est qu'il appartient à l'un des ensembles A_{p_i}. D'après le principe d'inclusion exclusion, le nombre d'entiers de $[\![1, n]\!]$ qui ne sont pas premiers avec n vérifie donc

$$n - \varphi(n) = |A_{p_1} \cup \ldots \cup A_{p_r}| = \sum_{k=1}^{r} (-1)^{k+1} \sum_{i_1 < \ldots < i_k} \left|A_{p_{i_1}} \cap \ldots \cap A_{p_{i_r}}\right|.$$

Pour tout $k-$uplet $(i_1, \ldots, i_k)$ d'indices, le lemme de Gauss garantit que les éléments de $A_{p_{i_1}} \cap \ldots \cap A_{p_{i_k}}$ sont exactement les multiples de $p_{i_1} \ldots p_{i_k}$, autrement dit $\left|A_{p_{i_1}} \cap \ldots \cap A_{p_{i_r}}\right| = |A_{p_{i_1} \ldots p_{i_k}}| = n/p_{i_1} \ldots p_{i_k}$. On peut reprendre le calcul, et en factorisant on aboutit à

$$n - \varphi(n) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{i_1 < \ldots < i_k} \frac{n}{p_{i_1} \ldots p_{i_k}} = n - n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

On déduit que

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

Deux conséquences fameuses de cette formules sont rassemblées dans le corollaire suivant :

Corollaire 2.16. 1) Si m et n sont deux entiers premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.
2) Soit p un nombre premier et $\alpha \geqslant 1$ un entier. Alors $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Le calcul particulier de $\varphi(p^\alpha)$ est très utile pour les Olympiades et est à retenir.

Exercice 2.39. Calculer $\varphi(1001)$ et $\varphi(1111)$.

2.3.2 La structure des restes modulo p et le petit théorème de Fermat

Dans la suite, p désigne un nombre premier.

Imaginons que vous disposez d'une bibliothèque dans laquelle vous pouvez ranger des livres. Vous avez plusieurs rangements possibles : par ordre alphabétique, par auteur, par thème... l'objectif étant de trouver la méthode qui mettra en avant les liens entre les livres et pouvoir les retrouver rapidement.

De la même façon, il y a plusieurs façons de « ranger » les éléments de $[\![1, p-1]\!]$, et chaque « rangement » va mettre en avant un ou plusieurs liens entre les éléments et privilégier certaines informations. La *structure* de $[\![1, p-1]\!]$, c'est l'organisation qui régit tous ces liens entre ses éléments. Dans beaucoup de problèmes d'Olympiades en lien avec les nombres premiers, il s'agit d'être capable de trouver le bon rangement des éléments. Voyons quelques exemples de rangements et quelques conséquences, sans les preuves pour l'instant :

Les rangements par permutation :

- Selon leur reste modulo p : l'écriture la plus simple est $[\![1, p-1]\!] = \{1, \dots, p-1\}$. L'avantage est que cette écriture est simple, le désavantage est qu'elle ne donne pas spécialement de lien entre les objets.
- En privilégiant un élément : On fixe a un résidu non nul modulo p. On peut alors également écrire $[\![1, p-1]\!] = \{a \mod p, 2a \mod p, \dots, (p-1)a \mod p\}$. Cela vient du fait que la fonction $x \mapsto ax \mod p$ est une bijection de $[\![1, p-1]\!]$ sur lui-même (on verra pourquoi). L'avantage est que cela permet de décrire les nombres à partir d'un entier privilégié. Une utilisation de ce rangement est **le petit théorème de Fermat**.
- En décrivant l'ensemble à partir d'un générateur : On peut démontrer qu'il existe un élément g tel qu'on puisse écrire $[\![1, p-1]\!] = \{1, g \mod p, \dots, g^{p-2} \mod p\}$, ce fait sera prouvé dans la section 3. Cette écriture permet d'écrire tous les éléments en fonction d'un seul nombre. La multiplication de deux nombres se transforme donc en une addition d'exposants. En revanche, on perd de vue les valeurs des restes modulo p.

Les rangements par partition :

- En formant les paires (x, x^{-1}) : On peut décider de ranger les éléments de $[\![1, p-1]\!]$ par paire, en appariant x avec son inverse. Cela vient du fait que $x \mapsto x^{-1} \mod p$ est une bijection de $[\![1, p-1]\!]$ dans lui-même. Attention, 1 et -1 sont appariés avec eux-même. On exploite cet appariemment dans **le théorème de Wilson**.
- On peut également former les paires $(x, p-x)$ ou les paires $(x, x+(p-1)/2)$ pour apparier nos éléments. De tels appariemments sont intéressants par exemple pour appliquer des

stratégies miroir dans un jeu de stratégie gagnante ou pour partitionner $[\![1, p-1]\!]$ dans les problèmes à la frontière entre combinatoire et théorie des nombres.

- On peut trier les éléments selon s'ils sont des carrés modulo p ou non (c'est-à-dire s'il existe y tel que $x \equiv y^2 \mod p$). L'ensemble des carrés possède plusieurs propriétés notables : il est de cardinal $\frac{p+1}{2}$, le produit de deux carrés est un carré, le produit de deux non-carrés est un carré, le produit d'un carré et d'un non-carré est un non-carré. Les amateurs d'équations diophantiennes de type JBMO savent que connaître les nombres qui sont des carrés modulo p est fort utile. Les résidus quadratiques seront abordés dans la section 3.

Après ce tour d'ensemble, montrons les propriétés les plus saillantes de l'ensemble $[\![1, p-1]\!]$. On commence par l'une des propriétés qui permet le mieux de décrire la structure de $[\![1, p-1]\!]$.

Proposition 2.17. Soit a un entier premier avec p. La fonction

$$f_a : \left\{ \begin{array}{ccc} [\![1, p-1]\!] & \longrightarrow & [\![1, p-1]\!] \\ x & \longmapsto & ax \mod p \end{array} \right.$$

est une bijection de $[\![1, p-1]\!]$ dans lui-même.

Démonstration. On peut vérifier que $f_{a^{-1}}$ est la bijection réciproque, ce qui conclut la proposition. On peut également faire la preuve à la main pour voir ce qu'il se passe.

Injectivité : Soient x et y deux entiers tels que $ax \equiv ay$. Comme a est inversible modulo p, $x \equiv y \mod p$. La fonction f_a est donc injective sur $[\![1, p-1]\!]$.

Surjectivité : Soit $[\![1, p-1]\!]$. On cherche x tel que $ax = b$, c'est-à-dire tel que $x = a^{-1}b$. On vérifie bien que ce x vérifie $f_a(a^{-1}b) = aa^{-1}b = b$. Donc f_a est bien surjective.

On le redit, l'intérêt de cette bijection est d'exprimer tous les restes modulo p en fonction de a. Si, dans un exercice, on est confronté à une expression $f(1, 2, \ldots, p-1)$ qui fait intervenir tous les restes modulo p, on pourra, dans cette expression, remplacer chaque terme x par le terme ax, ce qui donne le nombre $f(a, 2a, \ldots, (p-1)a)$. Si f est symétrique, alors elle demeure inchangée par ce changement, et on obtient l'identité $f(1, 2, \ldots, p) = f(a, 2a, \ldots, pa)$. Un exemple non trivial est le petit théorème de Fermat, que l'on présente maintenant.

Théorème 2.18 (Petit théorème de Fermat)**.** Soit p un nombre premier et soit a un entier premier avec p. Alors

$$a^{p-1} \equiv 1 \mod p.$$

En conséquence, la congruence $a^p \equiv a \mod p$ est vraie pour tout entier a (même ceux divisibles par p).

Démonstration. Puisque $x \mapsto ax \mod p$ est une bijection de $[\![1, p-1]\!]$ dans lui-même, les éléments $a, 2a, \ldots, (p-1)a$ ont des restes deux à deux distincts modulo p. On déduit que le produit $1 \cdot \ldots \cdot (p-1)$ de tous les éléments de $[\![1, p-1]\!]$ est aussi congru à $a \cdot 2a \cdot \ldots \cdot (p-1)a$. On a donc l'égalité

$$(p-1)! = 1 \cdot \ldots \cdot (p-1) \equiv a \cdot 2a \cdot \ldots \cdot (p-1)a = (p-1)!a^{p-1} \mod p.$$

Puisque $(p-1)!$ n'est pas divisible par p, il est inversible modulo p. On peut donc simplifier la congruence ci-dessus par $(p-1)!$, ce qui donne $1 \equiv a^{p-1} \mod p$, comme voulu.

En ce qui concerne la conséquence, si $p \mid a$ alors $a^p \equiv a \equiv 0 \mod p$, tandis que si a est premier avec p, il suffit de multiplier la congruence précédente par a.

Le petit théorème de Fermat possède de nombreuses applications dans les exercices d'Olympiades. Il permet de facilement calculer le reste d'une grande puissance d'un entier lorsqu'on le divise par p, ce qui simplifie grandement l'équation. Il interviendra également dans la section 2.4. La rubrique des exercices inclut des applications plus ou moins directes de ce théorème dont il faut maîtriser l'énoncé et les hypothèses sans aucune faute.

Avant de passer aux exercices, on montre un autre résultat célèbre qui est une conséquence d'un bon choix de « rangement » des éléments de $[\![1, p-1]\!]$. Son utilisation est plus rare et apparaît dans des compétitions s'autorisant plus de culture (BMO, RMM...).

Théorème 2.19 (Théorème de Wilson)**.** Soit p un nombre premier. Alors

$$(p-1)! \equiv -1 \mod p.$$

Démonstration. Si $p = 2$, le résultat est bien vrai. On suppose maintenant que p est impair. Dans le produit $1 \cdot \ldots \cdot (p-1)$, on distingue 1 et $p-1$, dont le produit est congru à $-1 \mod p$. On regroupe les autres termes par paires de la forme (x, x^{-1}).

Il s'agit bien d'une partition de $\{2, \ldots, p-2\}$ car chaque élément admet un unique inverse, et que $(x^{-1})^{-1} = x$. D'autre part, pour tout x dans cet ensemble, on a bien $x \neq x^{-1}$. En effet, si $x = x^{-1} \mod p$, alors en multipliant par x^{-1} on trouve $x^2 = 1 \mod p$, soit $p \mid x^2 - 1 = (x-1)(x+1)$, ce qui donne $x = \pm 1 \mod p$ (ce que l'on a exclu).

On note $(x_1, x_1^{-1}), \ldots, (x_k, x_k^{-1})$, avec $k = \dfrac{p-3}{2}$ les paires de cette partition. Le produit s'écrit alors

$$(p-1)! \equiv 1 \cdot (p-1) \cdot (x_1 \cdot x_1^{-1}) \cdot \ldots \cdot (x_k \cdot x_k^{-1}) \equiv (-1) \cdot 1 \cdot \ldots \cdot 1 \equiv -1 \mod p.$$

On peut désormais passer aux exercices. Le premier exercice demande d'adapter la preuve du petit théorème de Fermat pour redémontrer le théorème d'Euler. Certains exercices concernent le petit théorème de Fermat, d'autres consistent à trouver la bonne façon de ranger les restes des entiers modulo un nombre premier. Il convient donc d'avoir bien en tête les différents exemples proposés en début de sous-section.

Exercice 2.40. *(Théorème d'Euler)* Soit n un entier et a un entier premier avec n. Montrer que

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Montrer également par un contre-exemple (a, n) **qu'on n'a pas nécessairement** $a^{\varphi(n)+1} \equiv a \mod n$ pour tout entier a.

Exercice 2.41. Soit n un entier. Montrer que $42 \mid n^7 - n$ et que n^{13} et n ont le même chiffre des

unités.

Exercice 2.42. *(Mexico Regional 2021)* Soit $n \geqslant 2021$ et $a_1 < \ldots < a_n$ une suite arithmétique telle que, pour tout indice i, le nombre a_i est un nombre premier strictement plus grand que 2021. Montrer que tout nombre premier p tel que $p < 2021$ divise la raison de la suite.

Exercice 2.43. Trouver les polynômes P à coefficients entiers tels que, pour tout entier $n \geqslant 1$, n divise $P(2^n)$.

Exercice 2.44. Soit $1 \leqslant k \leqslant p-2$. Montrer, sans utiliser de générateur, que p divise $1^k + 2^k + \ldots + (p-1)^k$.

Exercice 2.45. *(Balkan MO SL 2013 N4)* Soit $p \geqslant 5$ un nombre premier. Montrer que $1^{p+2} + 2^{p+2} + \ldots + (p-1)^{p+2}$ est divisible par p^2.

Exercice 2.46. *(Nordic MO 2022)* Soit $n \geqslant 5$ un entier impair, Alice et Bob jouent au jeu suivant : ils sélectionnent chacun leur tour, en commençant par Alice, un entier entre 1 et $n-1$ qui n'a pas déjà été pris à un tour précédent. On note A l'ensemble des entiers choisis par Alice et B l'ensemble de ceux choisis par Bob. Après cela, Alice donne deux entiers distincts $x_1, x_2 \in A$ à Bob, qui choisit ensuite deux entiers distincts $y_1, y_2 \in B$. Bob gagne si et seulement si :

$$\big(x_1x_2(x_1-y_1)(x_2-y_2)\big)^{\frac{n-1}{2}} \equiv 1 \pmod{n}.$$

Pour quels n Bob a-t-il une stratégie gagnante ?

Exercice 2.47. *(Envoi de TN 2025/2026)* Déterminer tous les entiers $n \geqslant 1$ tels qu'il existe un entier k tel que $n! + n = n^k$.

Exercice 2.48. *(Olympiade Francophone 2020)* Soit $a_1, a_2, \ldots$ une suite d'entiers strictement positifs et soit m un entier. On suppose que, pour tout ensemble S fini et non vide d'indices strictement positifs, le nombre

$$-1 + \prod_{k \in S} a_k$$

est un nombre premier.

Montrer que, parmi les entiers $a_1, a_2, \ldots$, seul un nombre fini de termes possède moins de m facteurs premiers distincts.

Exercice 2.49. *(Baltic Way 2025/Peru TST 2023 et* al.*)* Déterminer tous les entiers n tels qu'il existe une permutation $(a_1, \ldots, a_n)$ des entiers $(1, \ldots, n)$ telle que les nombres $a_1, 2a_2, \ldots, na_n$ forment des résidus distincts modulo n.

Exercice 2.50. *(Poland MO 2020 Round 2)* Soit p un nombre premier et S un ensemble de $p+1$ entiers. Montrer qu'il existe $a_1, \ldots, a_{p-1} \in S$ des entiers distincts tels que

$$p \mid a_1 + 2a_2 + 3a_3 + \ldots + (p-1)a_{p-1}.$$

Exercice 2.51. *(ELMO SL 2019 N3)* Soit S un ensemble non vide d'entiers vérifiant la propriété suivante : pour tous entiers a et b de S, l'entier $ab+1$ est également dans S.

Montrer qu'il n'existe qu'un nombre fini de nombres premiers ne divisant aucun élément de S.

Exercice 2.52. (IMO SL 2017 N2) Soit $p \geqslant 2$ un nombre premier. Alice et Bob jouent au jeu suivant. Chacun leur tour en commençant par Alice, ils choisissent un indice i dans $\{0, 1, \ldots, p-1\}$ qui n'a pas encore été choisi précédemment par l'un des deux joueurs, puis choisissent un nombre a_i dans $\{0, \ldots, 9\}$. Lorsque tous les indices sont choisis, on considère le nombre

$$M = a_0 \cdot 10^0 + a_1 \cdot 10^1 + \ldots + a_{p-1} \cdot 10^{p-1}.$$

Alice gagne si M est divisible par p, Bob gagne sinon. Montrer qu'Alice dispose d'une stratégie gagnante.

2.3.3 Imprégnation de la notion d'inverse - apprendre à écrire $\frac{1}{i}$ plutôt que i^{-1}

On pourrait se contenter de passer directement aux exercices. L'objectif de cette sous-section, à travers ses exercices, est d'illustrer à quel point la notion d'inverse modulo p et sa notation i^{-1} sont consistantes avec la notation pour les inverses des réels, au point qu'on propose d'accepter l'abus de notation qui consiste à noter $\frac{1}{i}$ l'inverse de i modulo p, et on tente d'en indiquer les avantages.

Puisque nous sommes habitués à manipuler les fractions (dans les rationnels) avec la notation $\frac{a}{b}$ plutôt qu'avec la notation ab^{-1}, adopter cette notation modulo p a de bonnes chances de rendre nos expressions plus parlantes.

Dans la suite, s'il n'y a pas d'ambiguïté sur le modulo, pour tout nombre i non nul modulo p, on notera $\frac{1}{i} = i^{-1}$ l'inverse de i modulo p. Les formules suivantes, auxquelles on s'attend, découlent de sa définition.

$$\frac{1}{i} \cdot i \equiv 1 \mod p, \qquad a \equiv bi \mod p \iff \frac{a}{i} \equiv b \mod p, \qquad i \equiv j \mod p \iff \frac{1}{i} \equiv \frac{1}{j} \mod p.$$

On notera la dernière équivalence, qui dit qu'on peut appliquer les congruences aux dénominateurs.

Exercice 2.53. Soit p un nombre premier. Soient i et j deux entiers premiers avec p. Avec ces notations, vérifier que $\frac{1}{i} + \frac{1}{j} \equiv \frac{i+j}{ij} \mod p$.

Exercice 2.54. Soit p un nombre premier et a un entier premier avec p.

- Montrer que $(p-3)! \equiv -\frac{1}{2} \mod p$.
- Remarquer que $a^{p-2} \equiv \frac{1}{a} \mod p$.

L'un des points conceptuellement moins évidents est le passage effectif d'égalités vraies dans $\mathbb{Q}$ vers les mêmes égalités modulo p. C'est ce qu'exprime la propriété suivante :

Proposition 2.20. Soient a, b, c, d et p des entiers tels que p est un nombre premier et b et d sont premiers avec p. Il existe un entier k et un entier q premier avec p tels que

$$\frac{a}{b} = \frac{c}{d} + k\frac{p}{q}$$

si et seulement si on a $ab^{-1} \equiv cd^{-1} \mod p$ ou autrement, si et seulement si $\frac{a}{b} \equiv \frac{c}{d} \mod p$.

Démonstration. On procède par double implication.

$\boxed{\Rightarrow}$ Après développement des dénominateurs, on trouve $q(ad-bc) = kpbd$. Puisque p est premier avec q, $p \mid ad-bc$. On a donc $0 \equiv ad-bc \equiv db(ab^{-1}-cd^{-1}) \mod p$. Comme p est premier avec bd, on déduit que $0 \equiv ab^{-1}-cd^{-1} \mod p$, ce qui est la congruence voulue.

$\boxed{\Leftarrow}$ On suppose que $ab^{-1} \equiv cd^{-1} \mod p$. Cette congruence implique que $p \mid ad-cb$. Comme p est premier avec b et d, le numérateur de la fraction $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$ écrite sous forme irréductible est divisible par p, ce qui implique l'existence de k et q.

Ce que dit cette propriété, c'est que, lorsque les différents termes ont un sens modulo p (les dénominateurs sont non nuls), on peut passer modulo p une égalité sur les rationnels.
L'exemple le plus célèbre est le suivant :

Exemple 8. Soit $p \geqslant 5$ un nombre premier. Soient a et b deux entiers premiers entre eux tels que

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} = \frac{a}{b}.$$

Montrer que p^2 divise a.

Solution. On peut commencer par montrer que p divise a. D'après la propriété, cela revient à montrer que

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \equiv 0 \mod p.$$

Or, $x \mapsto x^{-1}$ est une bijection modulo p, donc la somme précédente contient exactement une fois chaque élément $\{1, \ldots, p-1\}$. On a donc

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \equiv 1 + 2 + \ldots + (p-1) \equiv p \cdot \frac{(p+1)}{2} \equiv 0 \mod p.$$

Malheureusement, cela ne nous dit rien sur la divisibilité de a par p^2, et le même raisonnement ne s'adapte pas directement modulo p^2. On propose donc un autre raisonnement, qui sera en plus l'occasion de voir un autre rangement des éléments de $\{1, \ldots, p-1\}$.

On commence par regrouper $\frac{1}{x}$ et $\frac{1}{p-x}$. La somme devient

$$\left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \ldots + \left(\frac{1}{(p-1)/2} + \frac{1}{(p+1)/2}\right)$$
$$= \frac{p}{1(p-1)} + \frac{p}{2(p-2)} + \ldots + \frac{p}{x(p-x)} + \ldots + \frac{4p}{(p-1)(p+1)}.$$

Ceci remontre que p divise a (aucun des dénominateurs n'est divisible par p). Pour montrer que p^2 divise a, il suffit donc de montrer que

$$\frac{1}{1(p-1)} + \frac{1}{2(p-2)} + \ldots + \frac{1}{x(p-x)} + \ldots + \frac{4}{(p-1)(p+1)} \equiv 0 \mod p.$$

Or, pour tout x, on a $\dfrac{1}{x(p-x)} \equiv \dfrac{1}{-x^2} \mod p$. Ainsi,

$$\frac{1}{1(p-1)} + \ldots + \frac{1}{x(p-x)} + \ldots + \frac{4}{(p-1)(p+1)} \equiv -\left(1^{-2} + \ldots + \left(\frac{p-1}{2}\right)^{-2}\right) \mod p.$$

Afin d'apporter un peu de symétrie, on peut remarquer que $x^{-2} \equiv (p-x)^{-2} \mod p$. On a donc aussi

$$\frac{1}{1(p-1)} + \ldots + \frac{4}{(p-1)(p+1)} \equiv -\left((p-1)^{-2} + \ldots + \left(\frac{p+1}{2}\right)^{-2}\right) \mod p.$$

En sommant les deux congruences, on déduit

$$2\left(\frac{1}{1(p-1)} + \ldots + \frac{4}{(p-1)(p+1)}\right) \equiv -((1^{-1})^2 + (2^{-1})^2 + \ldots + ((p-1)^{-1})^2) \mod p.$$

Puisque $x \mapsto x^{-1}$ est une permutation de $\{1, \ldots, p-1\}$, la somme de droite n'est autre que la somme des carrés des éléments de $\{1, \ldots, p-1\}$. On a donc

$$1^{-2} + 2^{-2} + \ldots + (p-1)^{-2} \equiv 1^2 + \ldots + (p-1)^2 \equiv p\frac{(p-1)(2p-1)}{6} \equiv 0 \mod p.$$

La somme de départ est donc divisible par p, comme annoncé.

Concluons par un petit avertissement : manipuler des fractions modulo n fonctionne bien lorsque n est premier, mais lorsque n n'est pas premier, on peut avoir des entiers non nuls modulo n mais qui ne sont pas inversibles modulo n pour autant. L'écriture sous la forme de fraction n'a alors plus aucun sens. On fera donc attention à n'effectuer tous ces raisonnements que lorsqu'on travaille modulo p un nombre premier.

Un dernier exemple édifiant pour la route :

Exemple 9. *(IMO 2005 P4)* Déterminer tous les entiers strictement positifs qui sont premiers avec tous les termes de la suite (a_n) définie par

$$a_n = 2^n + 3^n + 6^n - 1$$

pour tout entier $n \geqslant 1$.

Solution. Il s'agit d'étudier les diviseurs des a_n. Le geste à avoir est de fixer un nombre premier p et de vérifier s'il existe un entier n tel que p divise a_n. Le deuxième geste à faire, en l'absence d'idées, est de regarder ce qu'il se passe pour des petites valeurs de p, comme $p = 7, p = 11$, pour lesquels on peut facilement calculer les termes a_n. On se convainc avec cette étude que tous les nombres premiers p vont diviser un terme de la suite. Un retour aux petits cas permet même de conjecturer la valeur de n tel que $p \mid a_n$. La preuve est alors aussi courte qu'inoubliable.

Notons que 2 (et 5) divisent a_1 tandis que $3 \mid a_2$. On choisit ensuite un nombre premier $p \geqslant 7$, qui est donc premier avec $2, 3, 6$ et 1. D'après le petit théorème de Fermat, $2^{p-1} \equiv 1 \mod p$,

donc $2^{p-2} \equiv 2^{-1}$. De même, $3^{p-2} \equiv 3^{-1}$ et $6^{p-2} \equiv 6^{-1} \mod p$. On a donc

$$a_{p-2} \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 1 - 1 = 0 \mod p$$

(où on a passé modulo p l'égalité entre rationnels $1/2 + 1/3 + 1/6 = 1$). Ainsi, tout nombre premier p divise au moins un terme de la suite (a_n), le seul entier recherché par l'énoncé est donc 1.

Exercice 2.55. Montrer que p et $p+2$ sont des nombres premiers si et seulement si $p(p+2)$ divise $4((p-1)!+1)+p$.

Exercice 2.56. *(Pays-Bas BXMO TST 2018)* Soit p un nombre premier. Montrer qu'il existe une permutation $a_1, \ldots, a_{p-1}$ de $1, \ldots, p-1$ telle que les nombres $a_1, a_1a_2, \ldots, a_1a_2 \ldots a_{p-1}$ donnent $p-1$ restes distincts modulo p.

Exercice 2.57. *(Thaïlande MO 2022 P7)* Soit p un nombre premier et $a_1, \ldots, a_p, b_1, \ldots, b_p$ des entiers de $\{1, \ldots, p-1\}$. Montrer qu'il existe deux indices $i \neq j$ tels que $a_ib_j - a_jb_i$ est divisible par p.

Exercice 2.58. *(ELMO SL 2010 N2)* Soit p un nombre premier. Montrer que

$$\left(1 + p\sum_{k=1}^{p-1} k^{-1}\right)^2 \equiv 1 - p^2 \sum_{k=1}^{p-1} k^{-2} \mod p^4,$$

où les inverses sont pris modulo p^4.

Exercice 2.59. *(Mexique 2012)* Soit p un nombre premier impair. Pour tout $i \in \{1, \ldots, p-1\}$, on note r_i le reste de i^p par p^2. Calculer $r_1 + \ldots + r_{p-1}$.

Exercice 2.60. *(inspiré de IMAR 2023)* Soit p un nombre premier. Montrer qu'il existe une permutation $(a_1, \ldots, a_{p-1})$ de $(1, \ldots, p-1)$ telle que, pour tout triplet (i, j, k) d'indices,

$$(i-j)a_k + (j-k)a_i + (k-i)a_j \neq 0 \mod p.$$

Exercice 2.61. *(IMC 2022 P6)* Soit p un nombre premier impair. Montrer qu'il existe une permutation $(a_1, \ldots, a_{p-1})$ de $(1, \ldots, p-1)$ telle que

$$a_1a_2 + a_2a_3 + \ldots + a_{p-2}a_{p-1} \equiv 2 \mod p.$$

Exercice 2.62. *(Entraînement groupe D 2022)* Soit $p \geqslant 5$ un nombre premier et $k \geqslant 2$. Théo et Vincent jouent au jeu suivant : Théo choisit une permutation $a_1, \ldots, a_k$ des entiers $1, \ldots, k$ et indique à Vincent ce que vaut $a_ia_j \mod p$ pour tous $i \neq j$. Vincent gagne s'il est capable de retrouver les valeurs des a_i. Pour quelles valeurs de k Vincent peut-il gagner à coup sûr quelle que soit la permutation choisie par Théo ?

Exercice 2.63. *(IMO SL 2020 N1)* Soit $k \geqslant 1$ un entier. Montrer qu'il existe un nombre premier p tel qu'on peut choisir des entiers $a_1, a_2, \ldots a_{k+3}$ distincts dans l'ensemble $\{1, 2, \ldots, p-1\}$ tels que, pour tout indice $i = 1, 2, \ldots, k$, l'entier p divise $a_ia_{i+1}a_{i+2}a_{i+3} - i$.

Exercice 2.64. *(Balkan MO 2016)* Déterminer tous les polynômes P à coefficients entiers et de coefficient dominant 1 vérifiant la condition suivante : il existe un entier $N \geqslant 1$ tel que, pour tout nombre premier $p > N$ vérifiant $P(p) > 0$, p divise $2 \cdot P(p)! + 1$.

Exercice 2.65. *(IMO 2024 P2)* Déterminer tous les couples (a, b) d'entiers strictement positifs pour lesquels il existe des entiers strictement positifs g et N tels que l'égalité

$$\mathrm{PGCD}(a^n + b, b^n + a) = g$$

soit vérifiée pour tout entier $n \geqslant N$.

Exercice 2.66. *(RMM 2026 P2)* Soit $p \geqslant 11$ un nombre premier. On suppose que, pour tous a, b entiers tels que $1 \leqslant a < b \leqslant p - 3$, le nombre $b! - a!$ n'est pas divisible par p. Montrer que 8 divise $p - 5$.

2.4 La théorie de l'ordre

Dans la section précédente, on a vu que, pour tout nombre premier p et tout entier a premier avec p, on a $a^{p-1} \equiv 1 \mod p$. Ce résultat appelle la question suivante :

- ☞ Quel est le plus petit entier k strictement positif tel que $a^k \equiv 1 \mod p$?

Dans ce chapitre, on répondra plutôt aux questions suivantes :

- ☞ Quelles sont les propriétés de ce plus petit entier ?
- ☞ Comment les exploiter dans les problèmes d'Olympiades ?

On a découpé ce chapitre en trois parties. Dans la première partie, on présente et on commente la partie théorique, dont la première lecture a des applications en équations diophantiennes. La deuxième partie consiste en un détour par une astuce très présente en contexte olympique et qui mérite notre attention. La troisième partie est tournée vers des utilisations qu'on identifie comme plus récentes dans les problèmes d'Olympiades. Les deux premières parties reprennent largement des contenus déjà présents dans les autres ressources de la POFM. Si la troisième partie semble tentante, nous recommandons de d'abord commencer par le commencement, pour bâtir une compréhension solide de l'objet.

2.4.1 Construction, divisibilité, périodicité

Commençons par définir l'ordre multiplicatif modulo un entier n.

Définition 2.21 (Ordre multiplicatif de a modulo n)**.** Soit n un entier non nul et a un entier **premier avec** n. On appelle *ordre de a modulo n*, noté $\omega_n(a)$, le plus petit entier strictement positif k tel que $a^k \equiv 1 \mod n$.

Remarque 1 : L'existence de l'ordre est garantie car l'ensemble

$$\{k \in \mathbb{N}^\star, a^k \equiv 1 \mod n\}$$

est non vide. En effet, d'après le théorème d'Euler, il contient $\varphi(n)$.

Remarque 2 : Dans le cas où a n'est pas premier avec n, a n'est pas inversible modulo n donc il n'existe pas d'entier b tel que $ab \equiv 1 \mod n$, et en particulier pas d'entier $k \geqslant 1$ tel que $a \cdot a^{k-1} \equiv 1 \mod n$.

On constate sur des petits exemples qu'il n'est pas aisé de calculer l'ordre d'un élément modulo n, et que cet ordre n'est pas nécessairement égal à $\varphi(n)$.

La minimalité de $\omega_n(a)$ lui confère la propriété suivante, à la base de nombreux arguments dans les exercices de théorie des nombres :

Proposition 2.22. Soit a un entier premier avec n et soit k un entier naturel tel que $a^k \equiv 1 \mod n$. Alors $\omega_n(a) \mid k$.

En particulier, $\omega_n(a) \mid \varphi(n)$, et si $n = p$ est un nombre premier, $\omega_p(a) \mid p - 1$.

Démonstration. Soit $k = q\omega_n(a) + r$ la division euclidienne de k par $\omega_n(a)$, avec $0 \leqslant r < \omega_n(a)$. Alors

$$a^r \equiv (a^{\omega_n(a)})^q a^r = a^k \equiv 1 \mod n.$$

Ainsi, r est un entier positif ou nul, strictement inférieur à $\omega_n(a)$, et vérifiant $a^r \equiv 1 \mod n$. Par minimalité de $\omega_n(a)$, on déduit que $r = 0$, ce qui signifie bien que $\omega_n(a) \mid k$.

Les relations $\omega_n(a) \mid \varphi(n)$ et $\omega_p(a) \mid p-1$ proviennent respectivement des théorèmes d'Euler et de Fermat.

Si cette proposition est celle que l'on utilisera le plus en pratique, elle cache un corollaire immédiat mais qui permet de complètement décrire la suite $(a^k)_{k\in\mathbb{N}}$, et qu'il vaut mieux garder dans un coin de sa tête.

Corollaire 2.23. Soit a un entier premier avec n. Alors la suite $(a^k)_{k\in\mathbb{N}}$ est périodique modulo n, de plus petite période $\omega_n(a)$.

Démonstration. Soit k un entier naturel. Alors

$$a^{k+\omega_n(a)} = a^k a^{\omega_n(a)} \equiv a^k \mod n,$$

de sorte que la suite est bien périodique de période $\omega_n(a)$.

D'autre part, si t est une période, alors $a_t = a_0 \equiv 1 \mod n$, donc $\omega_n(a) \mid t$, d'après la proposition précédente. Ainsi, $\omega_n(a)$ est bien la plus petite période.

Les lecteurs avertis sauront donner un sens à tous ces résultats en remplaçant l'hypothèse « $k \in \mathbb{N}$ » par « $k \in \mathbb{Z}$ ».

Voici l'utilisation de l'ordre pour les exercices qui suivent. Comme fréquemment en mathématiques, l'objectif est de combiner des relations entre les nombres pour en obtenir de nouvelles. L'ordre permet de déduire une relation de divisibilité dans les exposants à partir d'une relation de congruence. On peut s'en servir dans les deux sens : on a des informations sur les facteurs premiers de $p-1$ (la valeur explicite de $p-1$ par exemple) et on en déduit des propriétés de $\omega_n(a)$, ou alors, et c'est plus fréquent, on a des informations sur $\omega_n(a)$ (valeur explicite, diviseurs premiers) et on en déduit des propriétés sur $p-1$ et donc sur p. Une fois que l'on a obtenu des relations de divisibilités, on peut continuer avec les raisonnement des chapitres précédents. Signalons à ce titre une dernière conséquence des propriétés de divisibilité de l'ordre :

Corollaire 2.24. Soit a un entier premier avec n. Alors $\omega_n(a) \leqslant \varphi(n)$.

On donne tout de même un exemple d'application de cette théorie :

Exemple 10. Soit p un nombre premier. Montrer que tous les diviseurs premiers de $2^p - 1$ sont congrus à 1 modulo p.

Solution. Soit q un diviseur premier de $2^p - 1$. Cette divisibilité s'écrit $2^p \equiv 1 \mod q$. L'ordre ω de 2 modulo q est donc un diviseur de p. On a donc $\omega = 1$ ou $\omega = p$. Comme $q \geqslant 2$, $2^1 \neq 1 \mod q$ et ω est différent de 1, ce qui implique que $\omega = p$. Combiné à la divisibilité $\omega \mid q-1$, on trouve bien que $q \equiv 1 \mod p$.

Les exercices ci-après font travailler cette gymnastique. De façon élémentaire d'abord, puis progressivement de façon non triviale.

Exercice 2.67. Soit $n \geqslant 1$ un entier impair. Montrer que $n \mid 2^{n!} - 1$.

Exercice 2.68. *(Albanie TST 2011)* Montrer que les facteurs premiers du nombre $11\ldots1$ (avec 2011 chiffres 1) sont tous de la forme $4022k + 1$.

Exercice 2.69. Soit $n \geqslant 1$ un entier naturel et p un diviseur de $2^{2^n} + 1$. Montrer que $p \equiv 1 \mod 2^{n+1}$.

Exercice 2.70. Soient a et b deux éléments inversibles modulo n. On suppose que $\omega_n(a)$ et $\omega_n(b)$ sont premiers entre eux. Montrer que $\omega_n(ab) = \omega_n(a)\omega_n(b)$.

Exercice 2.71. Soient p et q des nombres premiers distincts et $a \in \mathbb{N}$ tel que $a \equiv 1 \mod (p-1)(q-1)$. Montrer que pour tout $n \in \mathbb{N}$, $n^a \equiv n \mod pq$.

Exercice 2.72. Soit $m, n \geqslant 2$ des entiers tels que $\mathrm{PGCD}(m, n) = \mathrm{PGCD}(m, n-1) = 1$. On définit la suite $(n_k)_{k\in\mathbb{N}}$ par $n_0 = m$ et $n_{k+1} = n \cdot n_k + 1$ pour $k \in \mathbb{N}$. Montrer que les entiers $n_1, \ldots, n_{m-1}$ ne peuvent pas tous être des nombres premiers.

Exercice 2.73. *(Nordic MO 2025)* Soit p un nombre premier. On suppose que $2^{2p} \equiv 1 \mod 2p+1$. Montrer que $2p + 1$ est un nombre premier.

Exercice 2.74. *(Balkan MO SL 2016 N1)* Déterminer tous les entiers $n \geqslant 1$ tels que $1^{\varphi(n)} + 2^{\varphi(n)} + \ldots + n^{\varphi(n)}$ est premier avec n.

Exercice 2.75. *(Pologne MO 2016 Round final)* Soient k et n des entiers positifs impairs différents de 1. On suppose qu'il existe un entier $a \geqslant 1$ tel que $k \mid 2^a + 1$ et $n \mid 2^a - 1$. Montrer qu'il n'existe pas d'entier b tel que $k \mid 2^b - 1$ et $n \mid 2^b + 1$.

Exercice 2.76. Trouver tous les couples (p, q) de nombres premiers tels que $pq \mid 2^p + 2^q$.

Exercice 2.77. *(JBMO SL 2024 N2)* Déterminer tous les couples (p, q) de nombres premiers tels que $p \neq q$ et q^p est un diviseur de $p + p^q + p^{(q^p)}$.

Exercice 2.78. *(IMO SL 2006 N2)* Soit x un rationnel de $]0, 1[$. On note y le nombre de $]0, 1[$ dont le n-ème chiffre après la virgule est le 2^n-ème chiffre après la virgule de x. Montrer que y est rationnel.

Exercice 2.79. Soient $a \geqslant 2$ et n deux entiers strictement positif. On note $a^{\uparrow k} = a^{(a^{\cdot^{a}})}$, où il y a $k-1$ termes dans l'exposant. Cette suite est également définie par $a_0 = 1$ et $a_{m+1} = a^{a_m}$ pour tout $m \geqslant 0$. Montrer que la suite $(a^{\uparrow k})_{k\in\mathbb{N}}$ est constante à partir d'un certain rang modulo n.

2.4.2 L'astuce du plus petit facteur premier

Dans le cas d'une relation de divisibilité impliquant un entier n (éventuellement composé), le seul outil à notre disposition jusqu'à présent est de comparer $\omega_n(a)$ avec $\varphi(n)$. Malheureusement, cette idée a ses limites puisqu'on dispose rarement d'une expression de $\varphi(n)$ directement en fonction de n qui soit malléable. Pour s'en sortir, il convient plutôt de revenir aux diviseurs premiers de n.

Si l'on entreprend de regarder $\omega_p(a)$ pour le plus petit diviseur premier p de n, on récupère (gratuitement) une hypothèse supplémentaire que l'on peut mélanger à notre raisonnement. Cette hypothèse se convertit généralement en argument de taille : on cherche en $\omega_p(a)$ un diviseur de $p-1$ et un diviseur de n, mais comme les diviseurs de $p-1$ sont tous strictement inférieurs à p, cela contredit la minimalité de p. Voyons avec l'exemple suivant :

Exemple 11. Déterminer tous les entiers $n \geqslant 1$ tels que $n \mid 2^n - 1$.

Solution. **Réponse :** la seule solution est $n = 1$.

Un tel entier n est manifestement impair et $n = 1$ est bien solution. Supposons désormais que $n \geqslant 2$ et prenons p le plus petit diviseur premier de n. La relation implique $2^n \equiv 1 \mod p$. Ainsi, $\omega_p(2)$ divise n. D'après le petit théorème de Fermat, on a également $\omega_p(2) \mid p-1$. En particulier, $\omega_p(2) \leqslant p-1 < p$. Donc il s'agit d'un diviseur de n strictement plus petit que p. Par minimalité de p, on déduit que $\omega_p(2) = 1$. On a donc $2^1 \equiv 1 \mod p$, ce qui est absurde. On déduit que n n'admet aucun facteur premier et que la seule solution est $n = 1$, ce qui est bien solution.

Exercice 2.80. Déterminer tous les entiers n impairs tels que $n \mid 3^n + 1$.

Exercice 2.81. Déterminer tous les couples d'entiers (n, a) avec $n \geqslant 1$ tels que n divise $(a+1)^n - a^n$.

Exercice 2.82. Soient $a_1, \ldots, a_n$ des entiers naturels non nuls tels que $a_1 \ldots a_n$ divise le produit

$$(2^{a_1-1} + 1) \ldots (2^{a_k-1} + 1).$$

Montrer que l'un des a_i vaut 1.

Exercice 2.83. Déterminer toutes les suites (u_n) telles que, pour tout entier n, $u_n \mid 2^{u_{n+1}} - 1$.

2.4.3 Application à la construction d'entiers

Lorsqu'on apprend la construction de l'ordre ω d'un entier a modulo p, la principale propriété mise en avant est la relation de divisibilité entre ω et tout entier n vérifiant $a^n = 1 \mod p$. Si cette propriété est très utile dans le contexte d'une équation diophantienne, elle produit moins de résultats dans des contextes plus originaux. Ces dernières années, les Olympiades font émerger des problèmes faisant intervenir l'ordre d'un élément modulo p en dehors du contexte primitif des équations diophantiennes. Le but de cette sous-partie est de voir des exemples de tels contextes et les astuces à exploiter (et il n'y en a pas tant que ça).

On regarde la propriété de l'ordre comme une propriété **d'existence** :

Proposition 2.25. Soit a un entier et p un nombre premier avec a. Alors il existe un entier N tel que $p \mid a^N - 1$.

Remarque : Les propriétés de l'ordre permettent de choisir un tel entier $N \leqslant p$.

Si cette proposition peut laisser sceptique (elle est plus faible que les propriétés que l'on connait sur l'ordre), c'est pourtant elle qu'on utilise le plus souvent dans les contextes originaux, notamment

dans des problèmes **de construction d'entier**. L'existence de l'ordre permet de **produire des multiples de** p avec une forme bien maitrisée. Voyons avec l'exemple suivant :

Exemple 12. Montrer qu'il existe un multiple de 2023 dont les chiffres en base 10 sont tous égaux à 1.

Solution. Un tel multiple est de la forme

$$10^k + 10^{k-1} + \ldots + 1 = \frac{10^{k+1} - 1}{10 - 1} = \frac{10^{k+1} - 1}{9}.$$

Ainsi, en prenant $k = \omega_{2023}(10) - 1$, le numérateur de la fraction ci-dessus est divisible par 2023. Comme en plus 2023 est premier avec 9, on déduit que le nombre ci-dessus est bien divisible par 2023, ce qui est le résultat voulu.

Exercice 2.84. Montrer que, pour toute paire d'entiers strictement positifs (a, b) premiers entre eux, il existe deux entiers $m, n \geqslant 1$ tels que

$$a^m + b^n \equiv 1 \mod ab$$

Exercice 2.85. Montrer qu'il existe un multiple de 2023 qui admet 2023 chiffres 1 dans son écriture décimale (et tous les autres chiffres sont des 0).

Exercice 2.86. (Arabie saoudite 2024) Montrer qu'il existe une infinité de nombres premiers divisant un terme de la forme $3^{3^n-1} + 2$.

Exercice 2.87. (Pologne 2025 round 2) Déterminer tous les entiers $n \geqslant 2$ vérifiant la propriété suivante : les nombres $2^k \cdot n - 1$ pour $k = 2, 3, \ldots, n$ sont des nombres premiers.

Exercice 2.88. (ELMO 2015 P4) Soit $a \geqslant 2$ un entier. Montrer qu'il existe un entier $n \geqslant 0$ tel que $2^{2^n} + a$ n'est pas un nombre premier.

Exercice 2.89. (Canada MO 2018 P5) Soit $k \geqslant 2$ un entier pair. Sarah choisit un entier $N \geqslant 2$ qu'elle écrit au tableau et le modifie de la façon suivante : à chaque minute, elle choisit un diviseur premier p du nombre n écrit au tableau et remplace l'entier n par $n(p^k - p^{-1})$.
Montrer qu'il existe une infinité d'entiers k pairs pour lesquels, quels que soient les choix de Sarah, au bout d'un certain temps, elle écrira au tableau un nombre divisible par 2018.

Exercice 2.90. (BXMO 2023) Un entier n strictement positif est dit *amical* si la différence entre deux chiffres voisins de son écriture en base 10 est toujours égale à 1 ou à -1. Par exemple, 6787 est amical mais 211 et 901 ne le sont pas.
Déterminer tous les entiers m tels qu'il existe un entier amical divisible par $64m$.

Exercice 2.91. (IMO SL 2019 N3) Un ensemble S est dit *enraciné* si, pour tout entier $n \geqslant 0$ et tout choix de $a_0, \ldots, a_n$ dans S, les racines entières du polynôme $a_0 + a_1X + \ldots + a_nX^n$ sont également dans S. Déterminer tous les ensembles S enracinés contenant tous les nombres de la forme $2^a - 2^b$ avec $a, b \in S$.

Exercice 2.92. (IMO SL 2020 N4) Soit p un nombre premier impair. Pour tout entier n, on

note $d_p(n)$ le reste de la division euclidienne de n par p. On appelle *p-suite* une suite $(a_0, a_1, \ldots)$ d'entiers telle que a_0 est premier avec p et $a_{n+1} = a_n + d_p(a_n)$ pour tout indice $n \geqslant 0$.

1) Existe-t-il une infinité d'entiers p tels qu'il existe deux p-suites $(a_0, \ldots)$ et $(b_0, \ldots)$ vérifiant $a_n > b_n$ pour une infinité d'indices n et $a_n < b_n$ pour une infinité d'indices n ?

2) Existe-t-il une infinité d'entiers p tels qu'il existe deux p-suites $(a_0, \ldots)$ et $(b_0, \ldots)$ vérifiant $a_0 < b_0$ et $a_n > b_n$ pour tout $n \geqslant 1$?

2.5 Le théorème des restes chinois

Dans cette sous-section, on présente un résultat permettant de généraliser le problème suivant :
Étant donnés deux nombres premiers entre eux n_1 et n_2, existe-t-il un entier m tel que

$$\begin{cases} m & \equiv & 3 & \mod n_1 \\ m & \equiv & 2 & \mod n_2 \end{cases} ?$$

Autrement dit, il s'agit de la résolution d'un système de congruences. Comme dans tout problème de résolutions d'équations, les questions qui émergent sont

- ☞ Existe-t-il une solution ?
- ☞ Combien y a-t-il de solutions ?

Concernant la deuxième question, on remarque d'emblée que si m est solution du système, alors $m + k \cdot n_1 n_2$ est également une solution du système pour tout entier k. Ainsi, s'il y a une solution au système, il y en a une infinité. La question plus intéressante est « y a-t-il unicité de la solution modulo $n_1 n_2$ » ?

Le théorème des restes chinois donne la réponse à ces deux questions, dans un cadre général de r équations :

Théorème 2.26. Soit $r \geqslant 2$ un entier. Soient $n_1, n_2, \ldots, n_r$ des entiers premiers entre eux **deux à deux**. Soient $a_1, \ldots, a_r$ des entiers.

1. *(Existence)* Il existe un entier m tel que

$$\begin{cases} m & \equiv & a_1 & \mod n_1 \\ m & \equiv & a_2 & \mod n_2 \\ \vdots & & \vdots & \\ m & \equiv & a_r & \mod n_r. \end{cases}$$

2. *(Unicité)* De plus, m est unique modulo $n_1 \ldots n_r$, c'est-à-dire que si m et m' sont deux solutions du système, alors $m \equiv m' \mod n_1 \ldots n_r$.

Remarque 1 : Le théorème dit que si m est solution du système, alors toutes les solutions sont de la forme $m + k \cdot n_1 \ldots n_r$ avec k un entier relatif.

Remarque 2 : On peut se demander ce qu'il se passe dans le cas où les n_i ne sont pas premiers entre eux deux à deux. Contentons-nous seulement de donner un contre-exemple, montrant qu'il est imprudent d'essayer d'appliquer le théorème en dehors des hypothèses données. On pourra vérifier que pour chacun des deux systèmes, il n'existe aucun entier m solution :

$$\begin{cases} m & \equiv & 1 & \mod 6 \\ m & \equiv & 2 & \mod 10 \end{cases} \qquad \begin{cases} m & \equiv & 2 & \mod 6 \\ m & \equiv & 2 & \mod 10 \\ m & \equiv & 3 & \mod 15. \end{cases}$$

On voit donc le caractère crucial de l'hypothèse « premiers entre eux deux à deux », car le théorème n'est en général pas vrai dans le cas où les entiers sont seulement premiers entre eux dans leur ensemble.

Le théorème des restes chinois possède plusieurs niveaux de lecture :

- *Résolution d'un système :* Le premier niveau, c'est bien-sûr d'être capable de résoudre un système de congruences et d'en caractériser les solutions.
- *Construction :* Le niveau de lecture qui nous intéresse est le suivant : **c'est un résultat d'existence.** Autrement dit, la partie intéressante du théorème, et qui va nous servir dans les Olympiades, est la partie stipulant qu'il existe une solution au système, c'est-à-dire un entier vérifiant plusieurs contraintes. L'expression de cette solution nous intéressera relativement peu.
- *Éclatement :* Le niveau de lecture suivant est heuristique : le théorème nous dit entre autre que pour comprendre m modulo $N = \prod_{i=1}^{r} p_i^{\alpha_i}$, il suffit de comprendre m modulo $p_i^{\alpha_i}$. Plus concrètement, il ne sert à rien de regarder une équation modulo 12, il vaut mieux regarder modulo 2^2 et modulo 3 : les informations modulo les $p_i^{\alpha_i}$ sont nécessaires et suffisantes pour reconstruire ce qu'il se passe modulo n. La bonne façon de le comprendre, inutile pour les Olympiades, est que le théorème décrit la structure de $\mathbb{Z}/mn\mathbb{Z}$ en fonction de la structure de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$ lorsque m et n sont premiers entre eux.

Démonstration. On commence par prouver l'unicité. Concernant l'existence, on présente deux preuves, qui sont en fait la même preuve mais racontée de deux façons différentes, puisque chaque approche présente ses qualités. La première preuve est naturelle : on comprend qu'il suffit de résoudre le cas $r = 2$ pour effectuer une récurrence. Le cas $r = 2$ est alors une application astucieuse du théorème de Bezout. La motivation derrière cette application est à comprendre dans la deuxième preuve, qui est plus ambitieuse mais constructive : elle donne directement la forme des solutions, ce qui donne une meilleure vue sur leur forme, .

Unicité : Soient m et m' deux solutions du système. Alors pour tout indice $1 \leqslant i \leqslant r$, $m \equiv a_i \equiv m' \mod n_i$. Il vient que $n_i \mid m - m'$ pour tout indice i. Puisque les n_i sont premiers entre eux deux à deux, on déduit que $n_1 \dots n_r$ divise $m - m'$, ce qui se réécrit comme $m \equiv m' \mod n_1 \dots n_r$, qui correspond à l'unicité annoncée.

Existence :

Preuve 1 : On procède par récurrence sur r.
Initialisation : Si $r = 1$, il y a bien une solution au système

$$\{m \equiv a_1 \mod n_1.$$

Hérédité : Supposons le théorème vrai pour un certain entier $r \geqslant 1$ fixé. Soient $a_1, \dots, a_r, a_{r+1}$ des entiers et $n_1, \dots, n_r, n_{r+1}$ des entiers premiers entre eux deux à deux. On cherche un entier m tel que

$$\begin{cases} m \equiv a_1 & \mod n_1 \\ m \equiv a_2 & \mod n_2 \\ \vdots \quad \vdots & \\ m \equiv a_r & \mod n_r \\ m \equiv a_{r+1} & \mod n_{r+1}. \end{cases} \qquad (\star)$$

D'après l'hypothèse de récurrence, il existe un entier m_0 vérifiant

$$\left\{\begin{array}{rcll} m_0 & \equiv & a_1 & \mod n_1 \\ m_0 & \equiv & a_2 & \mod n_2 \\ \vdots & & \vdots & \\ m_0 & \equiv & a_r & \mod n_r. \end{array}\right.$$

Posons $N = n_1 n_2 \dots n_r$. Il suffit désormais de trouver un entier m solution du système à deux équations

$$\left\{\begin{array}{rcll} m & \equiv & m_0 & \mod N \\ m & \equiv & a_{r+1} & \mod n_{r+1}, \end{array}\right.$$

puisqu'un tel entier sera également solution de ($\star$). Puisque n_{r+1} est premier avec $n_1, \dots, n_r$, n_{r+1} est premier avec N. D'après le théorème de Bezout, il existe deux entiers u et v tels que $uN + vn_{r+1} = 1$. On vérifie alors que l'entier $m = a_{r+1}uN + m_0 v n_{r+1}$ satisfait les deux équations, puisque

$$a_{r+1}uN + m_0 v n_{r+1} \equiv m_0 v n_{r+1} = m_0(1 - uN) \equiv m_0 \mod N\,;$$

$$a_{r+1}uN + m_0 v n_{r+1} \equiv a_{r+1}uN = a_{r+1}(1 - v n_{r+1}) \equiv a_{r+1} \mod n_{r+1}.$$

Ceci conclut l'existence d'un entier m solution de ($\star$) et achève la récurrence.

Preuve 2 : Remarquons que si m et m' vérifient respectivement

$$\left\{\begin{array}{rcll} m & \equiv & a_1 & \mod n_1 \\ m & \equiv & a_2 & \mod n_2 \\ \vdots & & \vdots & \\ m & \equiv & a_r & \mod n_r\,; \end{array}\right. \qquad \left\{\begin{array}{rcll} m' & \equiv & a'_1 & \mod n_1 \\ m' & \equiv & a'_2 & \mod n_2 \\ \vdots & & \vdots & \\ m' & \equiv & a'_r & \mod n_r\,, \end{array}\right.$$

alors $m + m'$ est solution du système d'inconnue x

$$\left\{\begin{array}{rcll} x & \equiv & a_1 + a'_1 & \mod n_1 \\ x & \equiv & a_2 + a'_2 & \mod n_2 \\ \vdots & & \vdots & \\ x & \equiv & a_r + a'_r & \mod n_r. \end{array}\right.$$

De cette observation, on déduit que, si l'on dispose, pour tout indice $1 \leqslant i \leqslant r$, d'un entier m_i tel que

$$\left\{\begin{array}{rcll} m_i & \equiv & 0 & \mod n_1 \\ \vdots & & \vdots & \\ m_i & \equiv & 1 & \mod n_i \\ \vdots & & \vdots & \\ m_i & \equiv & 0 & \mod n_r\,, \end{array}\right.$$

alors l'entier $m = a_1 m_1 + \ldots + a_r m_r$ sera solution du système voulu. Il suffit donc de justifier l'existence de l'entier m_i pour tout i.

Puisque $m_i \equiv 0 \mod n_j$ dès que $i \neq j$, on cherche un entier m_i de la forme $k \cdot n_1 \dots n_{i-1} n_{i+1} \dots n_r$, avec k un entier. Posons $N_i = n_1 \dots n_{i-1} n_{i+1} \dots n_r$. Puisque $m_i \equiv 1 \mod n_i$, l'entier k doit vérifier $k \cdot N_i \equiv 1 \mod n_i$. Puisque l'entier N_i est premier avec n_i,

il est inversible modulo n_i et il suffit alors de choisir k tel que $k \equiv N_i^{-1} \mod n_i$. Ainsi, si k_i est un entier dans la classe de l'inverse de N_i modulo n_i, l'entier $m_i = k_i \cdot N_i$ satisfait les conditions voulues et l'entier $m = k_1 N_1 + \ldots + k_r N_r$ est solution du système.

Remarque : Dans la preuve 2, on reconnaît dans la formule $m = k_1 n_1 + \ldots + k_r n_r$ la forme proposée dans la preuve 1, puisque les entiers u et v du théorème de Bezout correspondent respectivement aux inverses de N et n_{r+1} modulo n_{r+1} et N. En conclusion, résoudre un système de deux congruences avec le théorème des restes chinois revient à appliquer le théorème de Bezout (et vice-versa).

Pour comprendre ces deux preuves, on pourra chercher à résoudre les applications numériques suivantes :

$$\begin{cases} x \equiv 1 & \mod 25 \\ x \equiv 2 & \mod 51 \end{cases} \qquad \begin{cases} x \equiv 1 & \mod 5 \\ x \equiv 2 & \mod 7 \\ x \equiv 3 & \mod 11 \end{cases}$$

Enfin, on pourra résoudre l'exercice suivant :

Exercice 2.93. Un chef militaire possède un régiment avec un certain nombre de soldats compris entre 200 et 270. Il souhaite savoir combien de soldats il possède. Pour cela il fait se ranger les soldats par groupes de 10 et s'aperçoit que 8 soldats restent. Il fait ensuite se ranger les soldats par groupes de 7 et s'aperçoit que 5 soldats restent. Combien y a-t-il de soldats ?

Comme dit en début de sous-section, le principal usage qu'on fera du théorème des restes chinois est la partie « existence ». En général, on l'utilise pour montrer l'existence d'un entier vérifiant certaines contraintes que l'on traduit sous la forme de congruences. Ces contraintes peuvent être suggérées par l'exercice ou issues d'une démarche personnelle. La principale difficulté réside dans le fait de convoquer les différentes hypothèses en vue de l'application du théorème des restes chinois, comme c'est le cas de l'exemple suivant :

Exemple 13. Montrer que, pour tout entier $n \geqslant 1$, on peut trouver n entiers consécutifs tous divisibles par le cube d'un nombre premier.

Solution. Ici, c'est à nous de rajouter artificiellement des contraintes plausibles. Ainsi, si $p_1 = 2, p_2, \ldots, p_n$ sont les n premiers nombres premiers, on se propose de montrer l'existence d'un entier x tel que $p_1^3 \mid x$, $p_2^3 \mid x+1, \ldots, p_n^3 \mid x+n-1$. Cela revient à trouver un entier x vérifiant le système de congruences :

$$\begin{cases} x \equiv 0 & \mod p_1^3 \\ x \equiv -1 & \mod p_2^3 \\ \vdots \quad \vdots & \\ x \equiv -(n-1) & \mod p_n^3. \end{cases}$$

Les nombres $p_1^3, p_2^3, \ldots, p_n^3$ sont premiers entre eux, donc le théorème des restes chinois nous assure l'existence d'un entier x vérifiant le système, ce qui conclut l'exercice.

Quelques remarques avant d'attaquer les exercices :

- ➢ D'après la forme des solutions, il existe une infinité d'entiers m solution du système. Cette infinité peut être utilisée de façon forte (« il existe une infinité d'entiers m vérifiant une certaine propriété ») ou de façon faible (« il existe un entier m arbitrairement grand vérifiant la propriété »).
- ➢ On recommande de travailler un maximum avec des nombres premiers, ou des puissances de nombres premiers, plutôt qu'avec des entiers deux à deux premiers entre eux.
- ➢ Pour rejoindre la remarque précédente, dans le cas d'un exercice où l'on souhaite construire des entiers modulo n, on conseille de décomposer n en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, de construire l'entier recherché modulo $p_i^{\alpha_i}$ puis de revenir à l'entier n. Souvent, travailler modulo $p_i^{\alpha_i}$ apporte plus de possibilités, puisque, par exemple, on connait bien la forme des inversibles ou des ordres modulo p^{α}.

D'autres exercices sur le théorème des restes chinois seront présents dans la section 4, dans la partie réservée aux problèmes de construction d'entiers.

Exercice 2.94.

1. Montrer qu'une suite arithmétique de raison 5 et une suite arithmétique de raison 7 contiennent toujours un terme en commun.
2. Que dire d'une suite périodique à la fois de période 5 et de période 7 ?

Exercice 2.95. *(Inspiré de Caucase MO 2018)* Soit $n \geqslant 1$ un entier.

1. Soient $a_1, \ldots, a_k$ des entiers strictement positifs. Existe-t-il un entier n tel que, pour tout indice $1 \leqslant i \leqslant k$, il existe un entier x_i tel que $a_i n = x_i^{p_i}$, où p_i est le $i-$ème nombre premier ?
2. Soient $a_1, \ldots, a_k$ des entiers strictement positifs. Existe-t-il un entier n tel que, pour tout indice $1 \leqslant i \leqslant k$, il existe un entier x_i tel que $a_i n = x_i^i$?

Exercice 2.96. Prouver que pour tout entier positif n, il existe des entiers a et b tels que $9a^2+4b^2-1$ soit divisible par n.

Exercice 2.97. Soit p un nombre premier. Montrer qu'il existe un entier $n \geqslant 1$ tel que p divise $2025^n - n$.

Exercice 2.98.

1. Montrer que pour tout entier n, il existe n entiers consécutifs tels qu'aucun d'entre eux n'est un nombre premier.
2. *(IMO 1989)* Montrer que pour tout entier n, il existe n entiers consécutifs tels qu'aucun d'entre eux n'est une puissance d'un nombre premier.

Exercice 2.99. *(Belarus MO 2018)* Déterminer tous les entiers n strictement positifs ayant la propriété suivante : si l'on pose $a_k = \mathrm{PPCM}(k, k+1, \ldots, k+n-1)$ pour tout entier strictement positif k, alors la suite (a_k) est croissante.

Exercice 2.100. Un point du plan à coordonnées entières (a, b) est dit *invisible* depuis 0 si il existe un point (c, d) du plan, distinct de $(0, 0)$ et (a, b) et qui appartient au segment reliant $(0, 0)$ et (a, b).

Montrer qu'il existe un carré de taille 2026×2026 contenant 2026^2 points invisibles depuis 0.

Exercice 2.101.

1. Soit P un polynôme à coefficients entiers et non constant. On suppose qu'il existe n nombres premiers $p_1, \ldots, p_n$ divisant chacun au moins un entier de la forme $P(t)$. Montrer qu'il existe un entier t tel que $P(t)$ est divisible par $p_1 \ldots p_n$.
2. *(USAMO 2008 P1)* Soit $n \geqslant 2$. Montrer qu'il existe n entiers $k_1, \ldots, k_n$ premiers entre eux deux à deux tels que $k_1 \ldots k_n - 1$ est le produit de deux entiers consécutifs.

Exercice 2.102.

1. Montrer qu'il existe un ensemble A d'entiers strictement positifs de cardinal 2022 tel que, pour tout sous-ensemble B non vide de A, la moyenne arithmétique et la moyenne géométrique des éléments de B sont des entiers.
2. Montrer qu'il existe un sous-ensemble A d'entiers strictement positifs de cardinal 2022 tel que pour tout sous-ensemble B non vide de A, la moyenne arithmétique des éléments de B est une puissance parfaite.

Exercice 2.103. *(USA TSTST 2019 P7)* Une fonction f de $\mathbb{Z}$ dans $\{1, \ldots, 1000\}$ est dite *intéressante* si, pour tous les entiers x et y, on a

$$\mathrm{PGCD}(f(x), f(y)) = \mathrm{PGCD}(f(x), x - y)$$

Combien existe-t-il de fonctions intéressantes ?

Exercice 2.104. *(APMO 2009 P4)* Montrer que pour tout entier strictement positif k, il existe des entiers $a_1, \ldots, a_k, b_1, \ldots, b_k$ deux à deux distincts, tels que a_i et b_i sont premiers entre eux pour tout indice i, et tels que les entiers

$$\frac{a_1}{b_1}, \quad \frac{a_2}{b_2}, \quad \ldots, \quad \frac{a_k}{b_k},$$

forment une progression arithmétique.

Exercice 2.105. *(IMO 2016 P4)* On pose $P(n) = n^2 + n + 1$. On dit qu'un ensemble est *parfumé* s'il contient au moins deux éléments et si chaque élément possède un facteur premier en commun avec au moins un autre élément. Trouver le plus petit entier positif b tel qu'il existe un entier positif a tel que l'ensemble $\{P(a), \ldots, P(a + b - 1)\}$ soit parfumé.

Exercice 2.106. *(RMM 2021 P2)* Alice et Bob jouent au jeu suivant. Alice choisit un entier N tel que $1 \leqslant N \leqslant 5000$, qu'elle ne communique pas à Bob. Elle choisit 20 entiers distincts $a_1, \ldots, a_{20}$ tels que, pour tout $k = 1, \ldots, 20$, $a_k \equiv N \mod k$. Un coup consiste, pour Bob, à choisir un ensemble S d'indices, et Alice lui donne l'ensemble $\{a_k, k \in S\}$ sans lui dire quel nombre correspond à quel indice.

Déterminer le plus petit nombre de coups nécessaires à Bob pour déterminer l'entier N.

3 Beaucoup de théorie

La section précédente montre que l'on peut déjà résoudre beaucoup de problèmes d'Olympiades avec des théorèmes relativement élémentaires. Toutefois, certaines compétitions, comme le RMM, la Balkan MO et même plus récemment les Olympiades Internationales, peuvent proposer des problèmes dont les exigences sont plus avancées. Les exigences peuvent être de deux types. Certains problèmes nécessitent tout simplement la connaissance de théorèmes plus avancés. D'autres problèmes, même sans demander explicitement de connaissances supplémentaires, font intervenir des arguments qui, à notre opinion, puisqu'ils sont motivés par de la théorie plus avancée, demandent d'avoir un certain recul conceptuel sur les objets manipulés.

Il est facile de se préparer au premier type de problèmes. Il suffit d'apprendre les théorèmes plus avancés. C'est ce que nous faisons avec la sous-section sur le lemme Lifting the Exponent et le théorème de Zsigmondy, ou encore avec une partie sur les résidus quadratiques.

Il est un peu plus délicat d'anticiper le deuxième type de problème, et c'est pourtant notre ambition dans cette section, avec une présentations plus poussée de la structure des éléments de $\{1, \dots, p-1\}$ ou encore d'arguments dits « asymptotiques ».

Il va de soi que le niveau des exercices concernés par ces thèmes est très élevé, et on ne s'étonnera pas que les exercices proposés soient rapidement comparables aux niveaux des problèmes 1 (souvent) ou des problèmes 2 (fréquemment) des Olympiades Internationales, si ce n'est plus difficile parfois. On recommande donc d'avoir bien travaillé la section précédente avant de s'attaquer à celle-ci.

3.1 Lifting the Exponent, théorème de Zsigmondy et autres

3.1.1 LTE et Zsigmondy

Les lemmes Lifting the Exponent (abrégé en LTE) et les théorèmes de Zsigmondy permettent de prolonger les arguments développés dans les sous-sections sur la valuation p-adique, le travail modulo p et la théorie de l'ordre, puisqu'ils servent respectivement à calculer la valuation p-adique de nombres de la forme $a^n \pm b^n$ et à en construire des diviseurs premiers.

Ces théorèmes ont fait une apparition tardive dans les préparations olympiques, et se sont avérés retrospectivement très efficaces pour littéralement trivialiser quantité d'exercices des Olympiades des années 2000. L'*excellent* polycopié d'Igor Kortchemski sur le site de la POFM, que l'on ne prétend pas imiter, possède une large collection de tels exercices, qui sont bien souvent des équations diophantiennes. Dans les années 2010, les comités de sélection des problèmes des compétitions se sont montrés plus vigilants pour écarter les exercices qui seraient l'application directe de ces théorèmes (qui sont donc devenus moins centraux dans les préparations). Au bout de ce processus de sélection naturelle, qui nous amène aux années 2020, ces exercices ont été réintroduits dans les programmes et dans les compétitions, en les appliquant dans des contextes plus originaux (constructions d'entiers, monovariants dans des problèmes de suites, équations fonctionnelles...).

Après avoir présenté les résultats, on donne les raisonnements classiques issus de ces résultats, pour pouvoir les appliquer aux nouveaux contextes. On ne donnera donc pas beaucoup d'exercices d'application directe (on renvoie pour cela au polycopié d'Igor Kortchemski).

Commençons par les lemmes LTE. Il y en a deux.

Théorème 3.1 (Lemme LTE, cas $-$)**.** Soit p un nombre premier impair. Soient a et b deux entiers premiers avec p. On suppose que $p \mid a-b$. Alors, pour tout entier n,

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n).$$

Théorème 3.2 (Lemme LTE, cas $+$)**.** Soit p un nombre premier impair. Soient a et b deux entiers premiers avec p. On suppose que $p \mid a+b$. Alors pour tout entier n **impair**,

$$v_p(a^n + b^n) = v_p(a+b) + v_p(n).$$

La contrainte que n est impair dans le deuxième énoncé est naturelle : si n est pair, $a+b$ n'a pas de raisons de diviser $a^n + b^n$, donc on n'attend pas de lien entre $v_p(a+b)$ et $v_p(a^n+b^n)$.
Un énoncé similaire existe pour $p = 2$, mais il est légèrement plus délicat. Il est laissé en exercice.
Les deux lemmes, bien qu'assez spectaculaires, admettent une preuve relativement élémentaire.

Démonstration. **Preuve du lemme, cas** $-$ On fixe a et b et on procède par récurrence sur $v_p(n)$.
Initialisation : Si $v_p(n) = 0$, montrons que $v_p(a^n - b^n) = v_p(a-b)$. Comme $p \mid a-b$, $a \equiv b \mod p$, on a donc la congruence

$$\frac{a^n - b^n}{a-b} = a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1} \equiv a^{n-1} + a^{n-2}a + \ldots + a \cdot a^{n-2} + a^{n-1} \equiv na^{n-1} \mod p.$$

Comme p ne divise ni n ni a, ce nombre est non nul mod p. On déduit que $v_p(a^n - b^n) = v_p(a-b) + v_p\left(\frac{a^n-b^n}{a-b}\right) = v_p(a-b)$.
Hérédité : On va en fait se ramener à l'énoncé dans le cas $n = p$. On suppose que $v_p(a^\ell - b^\ell) = v_p(a-b) + v_p(\ell)$ pour tout entier ℓ tel que $v_p(\ell) = k$, avec $k \geqslant 0$ fixé. Soit n un entier tel que $v_p(n) = k+1$. On écrit $n = p\ell$ avec $v_p(\ell) = k$. Enfin, on pose $x = a^\ell$ et $y = b^\ell$. D'après l'hypothèse de récurrence, $v_p(x-y) = v_p(a^\ell - b^\ell) = v_p(a-b) + k$. Il s'agit donc de montrer que $v_p(x^p - y^p) = v_p(x-y) + 1$.
Comme $p \mid x-y$, on dispose d'un multiple δ de p tel que $x = y + \delta$. D'après l'identité du binôme de Newton,

$$(y+\delta)^p - y^p = \sum_{i=0}^{p} \binom{p}{i} \delta^i y^{p-i} - y^p = \binom{p}{1} \delta y^{p-1} + \sum_{i \geqslant 2}^{p-1} \binom{p}{i} \delta^i y^{p-i} + P^p.$$

On calcule alors la valuation p-adique de chaque terme.

- Comme p ne divise pas y, $v_p\left(\binom{p}{1}\delta y^{p-1}\right) = v_p(p\delta) = 1 + v_p(x-y)$.
- $v_p(\delta^p) = pv_p(\delta) = pv_p(x-y) > 1 + v_p(x-y)$ car $p \geqslant 3$.
- Lorsque $2 \leqslant i \leqslant p-1$, puisque $p \mid \binom{p}{i}$, on a

$$v_p\left(\binom{p}{i}\delta^i y^{p-i}\right) = v_p\left(\binom{p}{i}\right) + iv_p(\delta) > 1 + v_p(x-y).$$

La valuation p-adique de la somme correspond à la plus petite valuation sur l'ensemble des termes, c'est-à-dire la valuation du premier terme. On déduit que $v_p((y+\delta)^p - y^p) = v_p(x-y)+1$. En revenant aux notations initiales, on a bien $v_p(a^n-b^n) = v_p(a-b)+k+1 = v_p(a-b)+v_p(n)$, ce qui achève la récurrence.

Remarque : L'apparition de l'hypothèse « p impair » est assez discrète : elle est là pour garantir que $v_p(\delta^p) > v_p(p\delta)$, ce qui permet de conclure que la valuation p-adique de la somme est celle de $v_p(p\delta)$. Cette apparition n'en demeure pas moins éloquente sur ce qu'il se passe pour $p = 2$: la formule $v_2(x^2 - y^2) = v_2(x - y) + 1$ n'a pas de raison d'être vraie, donc on ne peut pas espérer que la formule $v_2(a^n - b^n) = v_2(a - b) + 1$ soit vraie. La bonne formule est donnée par l'exercice suivant (et n'est pas à retenir) :

Exercice 3.1. (LTE cas $p = 2$) Soient a et b des entiers impairs. Montrer que pour tout entier pair n,

$$v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1.$$

On peut facilement prouver le lemme LTE dans le cas + à partir du cas − :

Démonstration. **Preuve du lemme, cas** + Soit n un entier impair. On a alors d'après le lemme LTE,

$$v_p(a^n + b^n) = v_p(a^n - (-b)^n) = v_p(a - (-b)) + v_p(n) = v_p(a + b) + v_p(n).$$

On pourra éprouver la puissance de ces deux lemmes sur les exercices numériques suivants :

Exercice 3.2. Montrer que $3^{1000} \mid 2^{3^{999}} + 1$.

Exercice 3.3. (IMO SL 1991) Déterminer le plus grand entier k tel que 1991^k divise $1990^{1991^{1992}} + 1992^{1991^{1990}}$.

L'étude des diviseurs premiers de $a^n \pm b^n$ est complétée par le théorème de Zsigmondy, dont la preuve, extrêmement technique, est présentée dans le polycopié d'Igor Kortchemski.

Définition 3.3. Soit a et b deux entiers et $n \geqslant 1$ un entier. Un diviseur p de $a^n - b^n$ est appelé *facteur premier primitif* si p ne divise aucun des nombres de la forme $a^k - b^k$ pour $k = 1, \ldots, n-1$.

De même, un diviseur p de $a^n + b^n$ est appelé *facteur premier primitif* si p ne divise aucun des nombres de la forme $a^k + b^k$ pour $k = 1, \ldots, n-1$.

Théorème 3.4 (Zsigmondy, cas −)**.** Soient $a > b$ deux entiers distincts et $n \geqslant 1$. Alors $a^n - b^n$ admet au moins un facteur premier primitif, sauf dans les deux cas suivants :

(i) $(a, b, n) = (2, 1, 6)$,

(ii) $n = 2$ et $a + b$ est une puissance de 2.

Théorème 3.5 (Zsigmondy, cas +)**.** Soient $a > b$ deux entiers distincts et $n \geqslant 1$. Alors $a^n + b^n$ admet au moins un facteur premier primitif, sauf si $(a, b, n) = (2, 1, 3)$.

La puissance de ces deux théorèmes (surtout le deuxième, qui admet très peu d'exceptions) pour résoudre des équations diophantiennes difficiles peut se comprendre avec l'exemple suivant :

Exemple 14. Trouver tous les quadruplets d'entiers strictement positifs (a, b, c, p) avec p premier tels que $p^a = b^p + c^p$.

Solution. D'après le théorème de Zsigmondy, sauf exception à examiner plus tard, le nombre $b^p + c^p$ admet un facteur premier primitif q. Comme $q \mid p^a$, on déduit que $q = p$. Comme p est primitif, p ne divise pas $b + c$. Or, $b + c \mid b^p + c^p$, donc $b + c$ est une puissance de p (strictement plus grande que 1 de surcroît). Ceci est absurde, donc on est dans l'exception du théorème de Zsigmondy.

Cela signifie que $(b, c, p) = (2, 1, 3)$ ou $(b, c, p) = (1, 2, 3)$. Ces deux triplets donnent $a = 2$, ce qui conduit aux deux solutions $(2, 2, 1, 3)$ et $(2, 1, 2, 3)$.

Ce qu'il faut retenir dans le cadre des équations diophantiennes, c'est que le théorème de Zsigmondy implique que le nombre $a^n \pm b^n$ admet beaucoup de facteurs premiers, et ne peut donc pas être une puissance d'un nombre premier, sauf exception.

On pourra s'échauffer avec les exercices suivants, et éventuellement consulter les exercices du polycopié d'Igor.

Exercice 3.4. *(Korea final round 2023)* Déterminer tous les entiers n tels que les facteurs premiers de $2^n - 1$ sont inférieurs ou égaux à 7.

Exercice 3.5. Soient p et q des nombres premiers impairs distincts. Montrer que $2^{pq} - 1$ admet au moins trois diviseurs premiers distincts.

Exercice 3.6. *(BXMO 2010)* Déterminer tous les quadruplets (a, b, p, n) d'entiers strictement positifs tels que p est un nombre premier et

$$a^3 + b^3 = p^n.$$

Plus généralement, le théorème de Zsigmondy est un résultat *d'existence*, il produit des nombres premiers avec beaucoup de contraintes.

Présentons à présent les utilisations courantes de ces deux théorèmes :

- Comme le lemme LTE concerne aussi des nombres de la forme $a^n - 1$, il est fréquemment lié à des arguments d'ordre. En particulier, le lemme LTE est redoutable lorsqu'il est combiné avec l'astuce du plus petit facteur premier dans la théorie de l'ordre. L'exemple le plus fameux est sans doute le problème suivant :

  Exemple 15. *(IMO 1990 P3)* Déterminer tous les entiers $n \geqslant 1$ tels que $n^2 \mid 2^n + 1$.

Solution. Soit n un entier solution. Comme $n \geqslant 1$, $2^n + 1$ est impair donc n est également impair. On remarque que $n = 1$ est bien solution, on suppose donc par la suite que $n > 1$. On applique l'astuce du cours d'ordre, on considère p le plus petit facteur premier de n. On trouve que $2^n \equiv -1 \mod p$, ce qui veut dire que $2^{2n} \equiv 1 \mod p$. Soit ω l'ordre de 2 modulo p. On trouve que ω divise $2n$ et $p-1$.

Si ω est impair, il divise n, on a alors $-1 \equiv 2^n \equiv 1 \mod p$, ce qui implique que p divise 2, ce qui est absurde car n est impair. On peut donc écrire $\omega = 2\beta$, où β divise n et $p-1$. Mais alors $\beta \leqslant p-1 < p$. La minimalité de p implique donc que $\beta = 1$ et $\omega = 2$. Il vient que $p \mid 2^2 - 1$, ce qui donne que $p = 3$.

On écrit $n = 3k$. Si $k = 1$, on constate que $n = 3$ est bien solution et on suppose dans la suite que $k > 1$. L'idée est de recommencer la manipulation avec k. On note q le plus petit diviseur premier de k. On a que $q \mid 2^{3k} + 1 = 8^k + 1 \mid 8^{2k} - 1$. Si ω' est l'ordre de 8 modulo q, on déduit que ω' est un diviseur de $2k$ et de $q-1$. Le même raisonnement que ci-dessus conduit à ce que $3 \mid k$, soit $9 \mid n$.

C'est là que le lemme LTE intervient. D'après celui-ci et l'hypothèse de divisibilité,

$$2v_3(n) \leqslant v_3(2^n + 1) = v_3(2 + 1) + v_3(n),$$

ce qui donne $v_3(n) \leqslant 1$, donnant la contradiction au fait que $9 \mid n$. On conclut que les seules solutions sont $n = 1$ et $n = 3$.

➢ La construction d'entiers. Lorsqu'on veut construire des entiers respectant un certain cahier des charges, on peut retenir que choisir des nombres de la forme $a^k \pm b^k$ possède deux avantages.

1. D'après le théorème de Zsigmondy, ils possèdent des facteurs premiers intéressants. Le premier intérêt est qu'on connaît des nombres qui ne sont pas multiples de ces facteurs premiers. Le deuxième intérêt est lié à la théorie de l'ordre : si p est un facteur premier primitif de $a^n - 1$, alors l'ordre de a modulo p est exactement n, ce qui implique immédiatement que $n \mid p-1$. Régulièrement, choisir en plus n premier simplifie beaucoup les raisonnements.
2. D'après le lemme LTE, on peut moduler k pour que $a^k \pm b^k$ soit divisible par une grande puissance de nombre premier : si p est premier impair et divise $a + b$, alors le lemme LTE implique que $p^n \mid a^{p^{n-1}} + b^{p^{n-1}}$.

Donnons un premier exemple d'utilisation du théorème de Zsigmondy dans un problème de construction.

Exemple 16. *(USAMO 2017 P1)* Montrer qu'il existe une infinité de couples (a, b) d'entiers avec $a, b > 1$, a et b premiers entre eux et $a + b \mid a^b + b^a$.

Solution. Dans ce genre de problème, on commence par simplifier les choses. Pour cela, on propose de se rajouter une contrainte au final simplificatrice : on va chercher a et b tels que $a + b = p$ un nombre premier. On cherche désormais un entier b et un nombre premier p tel que $p \mid a^b + b^a$. L'effet est de gommer la variable a.

La deuxième chose est d'appliquer les procédures standards des divisibilités : comme $a \equiv -b \mod a+b$, on a $a^b + b^a \equiv (-b)^b + b^a = b^b(b^{a-b} + (-1)^b) \mod a+b$. Autrement

dit, il suffit de trouver b et p tels que $p \mid b^{p-2b} + (-1)^b$. D'après le petit théorème de Fermat, $b^{p-2b} + (-1)^b \equiv b^{1-2b} + (-1)^b \mod p$. En mutlipliant par b^{2b} et en se rajoutant la contrainte que b est impaire, cela revient à trouver b et p tels que $p \mid b^{2b-1} - 1$, avec b un entier impair et $p > b + 1$.

Des couples (p, b) tels que $p \mid b^{2b-1} - 1$, il y en a autant qu'on veut, la difficulté est de garantir l'inégalité $p > b + 1$. Pour cela, on combine un raisonnement sur l'ordre avec le théorème de Zsigmondy : on fixe $b \geqslant 3$ un nombre impair tel que $b + 1$ n'est pas une puissance de 2 et p un facteur premier primitif de $b^{2b-1} - 1$, qui existe d'après le théorème de Zsigmondy. L'intérêt est que l'ordre de b modulo p est exactement $2b - 1$, puisque p ne divise aucun des $b^k - 1$ avec $k \leqslant 2b - 1$. On a donc $2b - 1 \mid p - 1$, ce qui implique $p \geqslant 2b > b + 1$. Il va sans dire que b et $p - b$ sont premiers entre eux, car leur PGCD est un diviseur de p distinct de p. Ceci nous permet de conclure.

Les exercices suivants sont globalement de difficulté croissante, même si on s'est permis quelques interversions pour regrouper ensemble des exercices aux idées communes.

Exercice 3.7. *(Balkan MO 2015 N3)* Soit a un entier strictement positif. Pour tout entier n, on pose $a_n = 1 + a + a^2 + \ldots + a^{n-1}$. Soient s et t deux entiers strictement positifs tels que tout diviseur premier p de $s - t$ divise $a - 1$. Montrer que $s - t$ divise $a_s - a_t$.

Exercice 3.8. *(Thailand Fall Camp 2020)* Pour tout entier $n \geqslant 1$, on note $\rho(n)$ le nombre de diviseurs positifs de n avec exactement les mêmes facteurs premiers que n. Montrer que, pour tout entier m, il existe un entier n tel que $\rho(202^n + 1) \geqslant m$.

Exercice 3.9. *(BXMO 2024)* Pour tout entier $n \geqslant 1$, on note $\mathrm{rad}(n)$ le produit des facteurs premiers distincts de n. Par exemple, $\mathrm{rad}(20) = \mathrm{rad}(2^2 \cdot 5) = 2 \cdot 5 = 10$. Montrer qu'il existe des entiers $a, b > 1$ tels que $\mathrm{PGCD}(a, b) = 1$ et

$$\mathrm{rad}(ab(a + b)) < \frac{a + b}{2024^{2024}}.$$

Exercice 3.10. *(Test de sélection français 2016-2017)* Prouver qu'il existe un entier $n > 0$ tel que, parmi les 2016 chiffres de droite dans l'écriture décimale de 2^n, il y a au moins 1008 chiffres 9.

Exercice 3.11. Déterminer tous les entiers strictement positifs a et b supérieurs ou égaux à 1 tels que $b^a \mid a^b - 1$.

Exercice 3.12. *(IMO 1999 P4)* Déterminer tous les couples d'entiers (n, p) avec p premier et $0 < n \leqslant 2p$ tels que

$$n^{p-1} \mid (p - 1)^n + 1.$$

Exercice 3.13. *(USA TSTST 2018 P8)* Déterminer tous les entiers $b > 2$ tels qu'il existe une infinité d'entiers $n \geqslant 1$ tels que $n^2 \mid b^n + 1$.

Exercice 3.14. *(RMM 2012 P4)* Montrer qu'il existe une infinité d'entiers n tels que $2^{2^n+1} + 1$ est divisible par n mais pas par $2^n + 1$.

Exercice 3.15. (IMO SL 2014 N4) Soit $n > 1$ un entier. Montrer que, parmi les termes de la suite $(a_k)_{k\geqslant 1}$ définie par

$$a_k = \left\lfloor \frac{n^k}{k} \right\rfloor,$$

il y en a une infinité qui sont impairs.

Exercice 3.16. On note $\sigma(n)$ la somme de tous les diviseurs premiers distincts de l'entier n. Déterminer tous les entiers $n \geqslant 1$ tels que

$$\sigma(2^n + 1) = \sigma(n).$$

Exercice 3.17. (Balkan MO 2022) Soient a, b et n des entiers strictement positifs tels que $a > b$ et

- a^{2021} divise n,
- b^{2021} divise n,
- 2022 divise $a - b$.

Montrer que n admet des diviseurs positifs, deux à deux distincts, dont la somme est divisible par 2022 mais pas par 2022^2.

Exercice 3.18. (Iran TST 2022) Un ensemble $S \subset \mathbb{N}^\star$ est dit *magique* si pour tout choix de trois entiers a, b, c distincts, tous les diviseurs strictement positifs de $\dfrac{a^c - b^c}{a - b}$ sont dans S. Pour tout entier $n > 1$, montrer qu'il existe un ensemble magique ne contenant pas n.

Exercice 3.19. (France TST 2016-2017) Déterminer tous les entiers $a > 0$ pour lesquels il existe des entiers strictement positifs $r, s, m_1, \ldots, m_r, k_1, \ldots, k_s$ tels que

$$(a^{m_1} - 1) \ldots (a^{m_r} - 1) = (a^{k_1} + 1) \ldots (a^{k_s} + 1).$$

Exercice 3.20. (IMO 2022 P5) Déterminer tous les triplets d'entiers strictement positifs (a, b, p) tels que p soit premier et que

$$a^p = b! + p.$$

Exercice 3.21. (RMM 2025 P2) On considère une suite infinie d'entiers strictement positifs $a_1, a_2, \ldots$ telle que $a_1 > 1$ et $(2^{a_n} - 1)a_{n+1}$ est un carré parfait pour tout entier strictement positif n. Est-il possible que deux termes de la suite soient égaux ?

3.1.2 Dirichlet, Schur et Bertrand

Avec les lemmes LTE et les théorèmes de Zsigmondy, d'autres théorèmes plutôt avancés ont fait leur apparition dans les récentes Olympiades. On présente ici trois théorèmes d'existence permettant de construire des nombres premiers avec de bonnes propriétés.

Le **Postulat de Bertrand**, peu fréquent, a toutefois une conséquence notable pour étudier les diviseurs premiers des factorielles, et peut de façon plus générale **être combiné à des arguments de taille.**

Théorème 3.6 (Postulat de Bertrand)**.** Soit $n \geqslant 2$ un entier. Il existe un nombre premier p tel que $n < p < 2n$.

Bien que le résultat soit couramment appelé « postulat », il s'agit bien d'un théorème prouvé. On ne donne pas sa démonstration.

Corollaire 3.7. Soit $n \geqslant 2$. Il existe un nombre premier p tel que $v_p(n!) = 1$.

Démonstration. Si $n = 2$, alors $v_2(2!) = 1$. On suppose dans la suite que $n \geqslant 3$. Soit p le plus grand nombre premier inférieur ou égal à n. On a donc que $p \geqslant 3$. Si $2p \leqslant n$, alors il existe un nombre premier q tel que $p < q < 2p \leqslant n$, ce qui contredit la maximalité de p. Donc $2p > n$, ce qui implique que $v_p(n!) = 1$.

Le **Théorème de Dirichlet**, plus célèbre, est un théorème d'existence qui se combine très bien avec des équations fonctionnelles ou avec le théorème des restes chinois **pour des problèmes de construction** :

Théorème 3.8 (Théorème de Dirichlet)**.** Soient a et b des entiers premiers entre eux. Il existe une infinité de nombres premiers p de la forme $an + b$.

Ainsi, dans un problème de construction, si l'on a besoin d'un entier x vérifiant $x \equiv b \mod a$, on pourra en plus le choisir premier.

Le **Théorème de Schur** intervient dans des problèmes portant sur des **polynômes à coefficients entiers**. On peut l'utiliser pour des raisonnements de construction.

Théorème 3.9 (Théorème de Schur)**.** Soit P un polynôme non constant à coefficients entiers. Il existe une infinité de nombres premiers p divisant un entier de la forme $P(n)$.

Démonstration. La preuve de l'infinité est une adaptation des preuves classiques d'infinité de nombres premiers.

Si $P(0) = 0$, alors $P(0)$ est divisible par une infinité de nombres premiers. On suppose donc dans la suite que $P(0) \neq 0$.

Soient $p_1, \ldots, p_N$ des nombres premiers divisant un terme de la forme $P(n)$. On pose $M = p_1 \ldots p_N$. Comme P est non constant, il existe un entier k tel que $P(kMP(0)) \neq P(0)$ (sinon le polynôme $P(X) - P(0)$ aurait une infinité de racines, contredisant l'hypothèse que P est non constant).

L'identité $a - b \mid P(a) - P(b)$ implique que $MP(0) \mid P(kMP(0)) - P(0)$. Donc il existe un entier $\ell \neq 0$ tel que $P(kMP(0)) = P(0) + \ell MP(0) = P(0)(1 + \ell M)$. L'entier $1 + \ell M$ est strictement supérieur à 1, il admet donc un facteur premier, qui est de fait premier avec M. Ainsi, on a construit un nouveau nombre premier divisant un entier de la forme $P(n)$.

On peut combiner le théorème de Schur avec l'identité $a - b \mid P(a) - P(b)$ de la façon suivante : si $q \mid P(n)$, alors $q \mid P(n + kq)$. En modulant la valeur de k (par exemple $k = q^\alpha$) et en profitant de la divisibilité $q^\alpha \mid P(n + kq) - P(n)$, on peut même construire des entiers m dont on maitrise $v_q(P(m))$.

Une procédure régulière dans les problèmes de polynômes à coefficients entiers dont les solutions sont les monômes est la suivante : on décompose $P(X) = X^\alpha Q(X)$ avec $\alpha \geqslant 0$ et $Q(0) \neq 0$. Pour montrer que Q est constant, il suffit de montrer qu'il possède un nombre fini de diviseurs. Une dernière remarque utile dans ce contexte est que, si $p \mid Q(n)$ avec n entier et $p > |Q(0)|$ alors p ne divise pas n (sinon on aurait $p \mid n \mid Q(n) - Q(0)$, donc $p \mid Q(0)$, ce qu'on a exclu). Ces éléments permettent en général de démarrer.

Les exercices qui suivent utilisent l'un ou l'autre des trois théorèmes précédents, éventuellement combinés avec les résultats précédents.

Exercice 3.22. Soit $n \geqslant 3$ un entier. Alice souhaite placer n entiers naturels autour d'un cercle de sorte que les n produits de deux entiers voisins sont exactement les nombres $1, 2, \ldots, n$ (dans un certain ordre). Peut-elle y arriver ?

Exercice 3.23. Montrer qu'il existe une infinité de nombres premiers dont le premier chiffre (en partant de la gauche) en base 10 est 1.

Exercice 3.24. Pour tout entier $n \geqslant 2$, on pose $H_n = 1 + \dfrac{1}{2} + \ldots + \dfrac{1}{n}$. Montrer que H_n n'est pas un entier.

Exercice 3.25. Soit P un polynôme non constant à coefficients entiers. Montrer que pour tout entier $n \in \mathbb{N}^\star$, il existe un entier n tel que $P(n)$ admette au moins r facteurs premiers distincts.

Exercice 3.26. Trouver tous les $n \geqslant 1$ tels qu'il existe une bijection σ de $\{1, \ldots, n\}$ dans lui-même telle que $\sigma(k) + k$ est un nombre premier pour tout entier k de $\{1, \ldots, n\}$.

Exercice 3.27. (Ibero-American 2019 P6) Soient $a_1, \ldots, a_{2019}$ des entiers strictement positifs. Soit P un polynôme à coefficients entiers tel que, pour tout entier n,

$$P(n) \mid a_1^n + \ldots + a_{2019}^n.$$

Montrer que P est constant.

Exercice 3.28. (APMO 2025 P3) Soit P un polynôme non constant à coefficients entiers et tel que $P(0) \neq 0$. Soit $a_1, a_2, \ldots$ une suite infinie d'entiers telle que $P(i - j) \mid a_i - a_j$ pour tous indices i, j distincts. Montrer que la suite $a_1, a_2, \ldots$ est constante.

Exercice 3.29. (MEMO 2017 T8) Pour tout entier $n \geqslant 3$, la suite $\alpha_1, \ldots, \alpha_k$ désigne la suite des exposants dans la décomposition en facteurs premiers de $n! = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Déterminer tous les entiers $n \geqslant 3$ pour lesquels la suite $\alpha_1, \ldots, \alpha_k$ est géométrique.

Exercice 3.30. (RMM SL 2018 N1) Déterminer tous les polynômes f à coefficients entiers tels que, pour tout nombre premier $p \geqslant 3$, $f(p)$ divise $2^p - 2$.

Exercice 3.31. (Concours Mathraining 16) Soit P un polynôme non constant à coefficients

entiers. Soient a et b des entiers relatifs tels que, pour tout entier n non nul, le nombre $a^n + P(n)$ est non nul et

$$a^n + P(n) \mid b^n + P(n).$$

Montrer que $a = b$.

Exercice 3.32. *(Balkan MO 2023)* Soit $\omega(n)$ le nombre de diviseurs premiers distincts de n (par exemple $\omega(1) = 0, \omega(12) = 2$). Déterminer tous les polynômes P à coefficients entiers tels que, pour tout entier n tel que $\omega(n) > 2023^{2023}$, l'entier $P(n)$ est strictement positif et vérifie $\omega(n) < \omega(P(n))$.

Exercice 3.33. *(Envoi 2021-2022 P18)* Déterminer tous les polynômes $P \in \mathbb{Z}[X]$ tels que :

1. $P(n) \geqslant 1$ pour tout $n \geqslant 1$,
2. $P(mn)$ et $P(m)P(n)$ ont le même nombre de diviseurs premiers pour tous $m, n \geqslant 1$.

Exercice 3.34. *(ELMO SL 2014)* Déterminer tous les triplets (a, b, c) d'entiers strictement positifs tels que, pour tout entier n dont tous les facteurs premiers sont supérieurs à 2014, $n+c \mid a^n+b^n+n$.

3.2 Travailler modulo p, épisode 2 - concepts avancés

Dans la première partie sur les nombres premiers, nous avions évoqué, en raisonnant avec les mains sur $\{0, \ldots, p-1\}$, la « structure » de l'ensemble des restes modulo p. Pour ce qui suit, nous allons prolonger l'étude de cette structure, avec des résultats un peu plus conceptuels.

Dans la première section, on explore la théorie des polynômes modulo p. On explique d'abord quelles propriétés des polynômes à coefficients entiers sont conservées par le passage modulo p et lesquelles ne le sont pas. On voit quelques conséquences de ces résultats (existence d'un entier d'ordre $p-1$, lemme de Hensel) et des exemples d'applications des polynômes modulo p aux problèmes d'Olympiades. La théorie qui y est présente est probablement la plus subtile du polycopié, et nécessite une *très bonne* compréhension des polynômes, ainsi que *plusieurs* lectures minutieuses.

La deuxième sous-section étudie les carrés modulo p. La théorie reprend essentiellement le polycopié de la POFM consacré au sujet, qu'elle complète par une sélection d'exercices plus récents.

3.2.1 Polynômes modulo p

Voici la motivation que nous donnons pour nous intéresser aux polynômes modulo p. Considérons le petit théorème de Fermat, qui indique que $a^{p-1} \equiv 1 \mod p$ si a est un entier premier avec p. L'énoncé pourrait être reformulé de la façon suivante : l'entier a est racine du polynôme $X^{p-1}-1$ modulo p. Admettons momentanément que l'on arrive à donner un sens concret à cette reformulation. L'étude des entiers modulo p se transforme alors en l'étude des racines, modulo p, du polynôme $X^{p-1}-1$. De la même manière, déterminer les éléments d'ordre d revient à déterminer les racines modulo p du polynômes X^d-1. Voici que l'on peut alors espérer :

- ☞ Le nombre de solutions d'une équation polynomiale est majoré par le degré du polynôme associé. Par exemple, il y a au plus d éléments d'ordre d, car le polynôme X^d-1 est de degré d.
- ☞ Les solutions de l'équations sont liées par des relations algébriques, telles que les relations de Viète : la somme des éléments d'ordre d correspond, modulo p, au coefficient devant X^{d-1} dans le polynôme X^d-1, c'est-à-dire que cette somme est nulle.

Bref, l'idée de regarder les polynômes modulo p, c'est de transformer l'étude d'un entier solution d'une équation en l'étude du polynôme associé à cette équation.

Cette étude est très dangereuse, parce qu'elle nécessite de maîtriser complètement quelles propriétés des polynômes sont conservées par le passage modulo p. C'est ce que nous allons faire à présent. On commence par prolonger la notion de congruence aux polynômes.

Définition 3.10. Deux polynômes $P(X) = a_nX^n + \ldots + a_1X + a_0$ et $Q(X) = b_mX^m + \ldots + b_1X + b_0$ sont congruents modulo p, notés $P(X) \equiv Q(X) \mod p$, si les coefficients de $Q - P$ sont tous divisibles par p.

Exemple : Les polynômes $X^2 + pX + 1$ et $X^2 + 1$ sont congruents modulo p, les polynômes $pX^2 + X + 1$ et $X + 1$ sont également congruents, même s'ils n'ont pas le même degré.

En revanche, bien que $P(X) = X^p - X$ et le polynôme nul $Q(X) = 0$ vérifient $P(a) \equiv Q(a) \mod p$ pour tout entier a, **ils ne sont pas congruents**. Ce premier exemple peut paraître banal, mais il illustre le premier piège suivant :

Proposition 3.11. Soient P et Q deux polynômes tels que $P(x) \equiv Q(x) \mod p$ pour tout entier x. Alors **on n'a pas nécessairement** $P \equiv Q \mod p$.

Cette première déception illustre la différence, modulo p, entre l'objet *polynôme* $P(X)$, défini par une suite de coefficients $(a_n, \ldots, a_0)$, et l'objet *fonction polynomiale* $x \mapsto P(x)$.

Aparté : pourquoi ne pas étendre la définition et décréter que les polynômes $X^p - X$ et 0 sont égaux modulo p ? Si l'on ne devait donner qu'un seul intérêt, c'est par exemple pour pouvoir définir de façon consistante le degré d'un polynôme : le degré du polynôme $X^p - X$ est p tandis que celui du polynôme nul est $-\infty$. Garder une notion intrinsèque de degré permet de pouvoir affirmer un lien entre le degré et le nombre de racines d'un polynôme, ou encore pour pouvoir faire une division euclidienne. On pourra trouver une consolation dans la propriété suivante, appelée propriété de Frobenius :

Proposition 3.12 (Propriété de Frobenius)**.** Soit P un polynôme. Alors $P(X^p) \equiv P(X)^p \mod p$.

Démonstration. Rappelons que pour tout $1 \leqslant k \leqslant p-1$, on a $p \mid \binom{k}{p}$. Notons que d'après le binôme de Newton, si A et B sont deux polynômes,

$$(A+B)^p = \sum_{k=0}^{p} \binom{p}{k} A^k B^{p-k} \equiv A^p + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k}}_{\equiv 0} A^k B^{p-k} + B^p \equiv A^p + B^p \mod p.$$

Par récurrence immédiate, on trouve que pour d polynômes $A_1, \ldots, A_d$, $(A_1 + \ldots + A_d)^p \equiv A_1^p + \ldots + A_d^p$.

On décompose alors notre polynôme $P(X) = a_d X^d + \ldots + a_0$. On a donc

$$\begin{aligned} P(X)^p &\equiv (a_d X^d)^p + \ldots + (a_1 X)^p + a_0^p \\ &= a_d^p X^{dp} + \ldots + a_1^p X^p + a_0^p \\ &\equiv a_d X^{dp} + \ldots + a_1 X^p + a_0^p \qquad \text{d'après le petit Théorème de Fermat} \\ &= P(X^p) \end{aligned}$$

Exercice 3.35. Vérifier que $X^p - a \equiv (X-a)^p \mod p$.

La propriété importante que l'on va pouvoir mettre en place ici est le lien entre racine et factorisation :

Proposition 3.13. Soit P un polynôme et a un entier. On suppose que $P(a) \equiv 0 \mod p$. Alors il existe un polynôme Q à coefficients entiers et de degré $\deg P - 1$ tel que $P(X) \equiv (X-a)Q(X) \mod p$.

Démonstration. Soit (Q, R) le couple de polynômes entiers correspondant au quotient et au reste dans la division euclidienne (entière) de P par $X - a$. On a donc $P(X) = (X - a)Q(X) + R(X)$, avec $\deg Q = \deg P - 1$. Notons que comme $\deg R < 1$, R est constant égal à

r_0. On a alors $r_0 = P(a) \equiv 0 \mod p$. On a donc $R(X) \equiv 0 \mod p$ et $P(X) \equiv (X-a)Q(X) \mod p$.

On peut itérer ce résultat chaque fois qu'on trouve une nouvelle racine, pour obtenir le corollaire suivant, **qui n'est plus vrai si on travaille modulo n avec n composé** :

Corollaire 3.14. Soit P un polynôme et $a_1, \dots, a_d$ des entiers distincts tels que $P(a_i) \equiv 0 \mod p$ pour tout i. Alors il existe un polynôme Q de degré $\deg P - d$ tel que $P(X) \equiv (X-a_1)\dots(X-a_d)Q(X) \mod p$.

Démonstration. La preuve se fait par réccurence sur d. L'initialisation correspond à la propriété précédente. Pour l'hérédité, on suppose avoir $P(X) \equiv (X-a_1)\dots(X-a_d)Q(X) \mod p$ et que $P(a_{d+1}) \equiv 0 \mod p$, avec a_{d+1} distinct des a_i. On a alors la congruence $Q(a_{d+1})(a_{d+1}-a_1)\dots(a_{d+1}-a_d) \equiv 0 \mod p$. Comme les $(a_{d+1}-a_i)$ sont non nuls, on déduit que $Q(a_{d+1}) = 0$. On peut alors appliquer la proposition précédente pour trouver R de degré $\deg Q - 1$ tel que $Q(X) \equiv (X-a_{d+1})R(X) \mod p$, ce qui permet de conclure.

L'hypothèse que p est premier se traduit par le fait que si un produit est nul modulo p, alors l'un des facteurs est nul modulo p (ce qui permet d'avoir que $Q(a_{d+1}) \equiv 0$ dans la preuve précédente). Cette propriété n'étant plus vraie modulo n composé, on n'a plus le corollaire précédent. On pourra méditer les contre exemples suivants : le polynôme $X^2 - X$ modulo 6, qui a pour racines $0, 2, 3, 5$, et le polynôme $X^2 - 1$ modulo 8, qui a pour racines $1, 3, 5, 7$.

Cela permet par exemple d'obtenir la factorisation suivante, puisque tous les éléments de l'ensemble $\{1, \dots, p-1\}$ sont racines de $X^{p-1} - 1$ d'après le petit théorème de Fermat,

$$X^{p-1} - 1 \equiv (X-1)(X-2)\dots(X-(p-1)) \mod p.$$

On déduit alors la propriété fondamentale suivante, qui est l'analogue de la propriété qu'un polynôme de degré d admet au plus d racines.

Théorème 3.15. Soit P un polynôme entier de degré d. Alors il existe au plus d éléments a de $\{0, \dots, p-1\}$ tels que $P(a) \equiv 0 \mod p$.

Démonstration. Supposons avoir exhibé $d+1$ éléments distincts $a_1, \dots, a_{d+1}$ de $\{0, \dots, p-1\}$ tels que $P(a_i) \equiv 0 \mod p$. On dispose alors d'un polynôme Q de degré $\deg P - (d+1)$ tel que $P(X) \equiv (X-a_1)\dots(X-a_{d+1})Q(X) \mod p$, ce qui est absurde car $\deg P - (d+1) = -1$ n'est pas le degré d'un polynôme.

On insiste encore, cette propriété n'est vraie que parce que p est premier, et n'est plus vraie si on étudie les polynômes modulo un n composé.

Faisons une petite pause dans la théorie pour voir quelques applications de ce lien degré/racines. On commence par le théorème suivant, qui donne l'existence d'un entier $g \in \{1, \dots, p-1\}$ dont l'ordre modulo p vaut exactement $p-1$, de sorte que $\{1, \dots, p-1\} = \{g^0, g^1, \dots, g^{p-1}\}$ (où par g^k on sous-entend $g^k \mod p$) :

Théorème 3.16 (Existence d'un générateur modulo p)**.** Il existe un entier g dont l'ordre modulo p est exactement $p-1$.

Démonstration. **Étape 1 :** Notons $e = \text{PPCM}\{\omega(1), \omega(2), \ldots, \omega(p-1)\}$ le PPCM des ordres des éléments de $\{1, \ldots, p-1\}$. Comme $\omega(a) \mid p-1$ pour tout entier a, on déduit que $e \mid p-1$, et en particulier que $e \leqslant p-1$.

D'autre part, comme $\omega(a) \mid e$, on a $a^e \equiv 1 \mod p$ pour tout a. Ainsi, le polynôme $X^e - 1$ admet au moins $p-1$ racines modulo p, ce qui implique que $p-1 \leqslant e(p)$.

La combinaison de ces deux inégalités donne $e = p-1$.

Étape 2 : Construisons un élément g dont l'ordre est $p-1 = e$. Soit $e = q_1^{\alpha_1} \ldots q_r^{\alpha_r}$ la décomposition en facteurs premiers de e. Par définition du PPCM, pour tout indice $1 \leqslant k \leqslant r$, il existe un élément a_k tel que $v_{q_k}(\omega(a_k)) = v_{q_k}(e) = \alpha_k$. On écrit $\omega(a_{q_k}) = q_k^{\alpha_k}\ell$ avec ℓ entier. On vérifie alors que $\omega(a_{q_k}^{\ell}) = q_k^{\alpha_k}$. On pose alors $b_k = a_{q_k}^{\ell}$.

D'après l'exercice 2.70, on a alors

$$\omega(b_{q_1} \ldots b_{q_r}) = \omega(b_{q_1}) \ldots \omega(b_{q_r}) = q_1^{\alpha_1} \ldots q_r^{\alpha_r} = e,$$

donc $g = b_{q_1} \ldots b_{q_r}$ est d'ordre e, ce qui conclut.

Voici quelques exercices pour pratiquer ce premier pas avec les polynômes, ainsi que pour appliquer le théorème précédent :

Exercice 3.36. Soient P et Q deux polynômes entiers. On suppose que $p \mid P(a) - Q(a)$ pour tout entier $a = 0, \ldots, p-1$. Montrer qu'il existe un polynôme R à coefficients entiers tel que $X^p - X$ divise $P(X) - Q(X) + pR(X)$.

Exercice 3.37. Soit d un diviseur de $p-1$. Montrer qu'il y a exactement $\varphi(d)$ éléments de l'ensemble $\{1, \ldots, p-1\}$ d'ordre d. En particulier, il y a $\varphi(p-1)$ éléments d'ordre $p-1$.

Exercice 3.38. Soit $1 \leqslant k \leqslant p-2$. Montrer que $1^k + 2^k + \ldots + (p-1)^k \equiv 0 \mod p$.

Exercice 3.39. Déterminer le nombre de polynômes unitaires de degré $p-2$, admettant $p-2$ racines distinctes modulo p et dont les coefficients sont deux à deux distincts.

Exercice 3.40. *(Estonie TST 2020)* Soient p et q des nombres premiers et a un entier tel que q ne divise pas $a-1$ mais q divise $a^p - 1$. Montrer que

$$(1+a)(1+a^2)\ldots(1+a^{p-1}) \equiv 1 \mod q.$$

Exercice 3.41. *(Chine TST 2018 test 4 jour 2 Q4)* Soit p un nombre premier et k un entier strictement positif. On note S l'ensemble des éléments de $\{0, 1, \ldots, p-1\}$ pour lesquels il existe un entier x tel que $x^k \equiv a \mod p$.

On suppose que $3 \leqslant |S| \leqslant p-2$. Montrer que les éléments de S ne sont pas en progression arithmétique.

Exercice 3.42. *(Envoi d'arithmétique 2019-2020)* Déterminer tous les entiers n tels que la pro-

priété suivante est vraie : pour tout entier c, il existe un entier x tel que $x^x \equiv c \mod n$.

Permettons-nous un mot sur la notion de multiplicité de racines. Il peut être utile d'étudier si une racine est multiple, surtout si l'on compte les racines pour les comparer au degré du polynôme. Dans la théorie générale (polynômes réels), la notion de multiplicité est directement liée au polynôme dérivé. Pour les polynômes modulo p, c'est un peu plus subtil, dans la mesure ou certains polynômes de grand degré ont pour dérivée le polynôme nul (c'est le cas de $(X-2)^p$ et $(X-2)^{2p}$, pour lesquels 2 n'a pas la même multiplicité). Fort heureusement, pour les multiplicités inférieures à p, l'incertitude est levée via la propriété suivante.

Proposition 3.17. Soit P un polynôme et p un nombre premier impair.

1. Si $P'(X) \equiv 0 \mod p$, alors il existe un polynôme Q tel que $P(X) \equiv Q(X)^p \mod p$.
2. Soit $m \leqslant p-1$ et a un entier de $\{0, \ldots, p-1\}$. On suppose que $P(a) \equiv P'(a) \equiv P''(a) \equiv \ldots \equiv P^{(m)}(a) = 0 \mod p$. Alors il existe un polynôme Q de degré $\deg P - (m+1)$ tel que $P(X) \equiv (X-a)^{m+1}Q(X) \mod p$.

Démonstration. 1) Quitte à remplacer P par un polynôme qui lui est congru, on peut supposer que les coefficients non nuls de P ne sont pas divisibles par p. On écrit $P(X) = a_{n_1}X^{n_1} + \ldots + a_{n_r}X^{n_r} + a$. Puisque $P'(X) \equiv 0 \mod p$, on a $n_1 a_{n_1} X^{n_1-1} + \ldots + n_r a_{n_r} X^{n_r-1} \equiv 0 \mod p$. On déduit que $p \mid n_i a_{n_i}$ pour tout i et donc que $p \mid n_i$. En posant $n_i = pm_i$ et $Q(X) = a_{n_1}X^{m_1} + \ldots + a_{n_r}X^{m_r} + a$, on a d'après la propriété de Frobenius que

$$P(X) = Q(X^p) \equiv Q(X)^p \mod p.$$

2) Il s'agit d'une récurrence sur m.

Initialisation : Supposons que $m = 1$. On dispose d'un polynôme Q tel que $P(X) \equiv (X-a)Q(X) \mod p$. La dérivation passant modulo p (on vous laisse vérifier), on a

$$P'(X) \equiv (X-a)Q'(X) + Q(X) \mod p.$$

En évaluant en a, on trouve que $0 \equiv Q(a) \mod p$. On a donc un polynôme R tel que $\deg R = \deg Q - 1 = \deg P - 2$ et $Q(X) \equiv (X-a)R(X) \mod p$, donc $P(X) \equiv (X-a)^2 R(X) \mod p$.

Hérédité : On suppose la propriété vérifiée pour $m-1$. On a donc un polynôme Q de degré $\deg P - m$ tel que $P(X) \equiv (X-a)^m Q(X) \mod p$. Un calcul que l'on ne détaille pas et qui tient à la formule de Leibniz donne

$$0 \equiv P^m(a) \equiv m!Q(a) \mod p.$$

Comme $m \leqslant p-1$, on déduit que $Q(a) \equiv 0$, ce qui permet de factoriser Q par $X-a$ modulo p, et on retrouve que $P(X) \equiv (X-a)^{m+1}R(X) \mod p$ pour un polynôme R tel que $\deg R = \deg P - (m+1)$.

On présente désormais les relations de Viète. Tout comme dans la théorie générale, les polynômes modulo p admettent une forme développée et une forme factorisée. L'identification des coefficients dans la congruence de ces deux formes produit les relations de Viète, dont on souligne les deux relations les plus importantes :

Proposition 3.18 (relations de Viète)**.** Soit $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ un polynôme à coefficients entiers. On suppose que P admet n racines $x_1, \ldots, x_n$ (comptées avec multiplicité) modulo p. Alors

$$x_1 + \ldots + x_n \equiv -a_{n-1} \mod p \qquad \text{et} \qquad x_1 \ldots x_n \equiv (-1)^n a_0 \mod p.$$

Ces relations, appliquées au polynôme $X^{p-1} - 1 \equiv (X-1)\ldots(X-(p-1))$, impliquent en particulier que $1 + \ldots + (p-1) \equiv 0 \mod p$ (que l'on peut retrouver par le calcul) et que $1 \times \ldots \times (p-1) \equiv (-1)^p = -1 \mod p$, ce qui correspond au théorème de Wilson.

Dans le cas des polynômes réels, les relations de Viète expriment que les fonctions symétriques élémentaires de n nombres déterminent ces n nombres, dans le sens où, si les deux $n-$uplets $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_n)$ ont les mêmes fonctions symétriques élémentaires $\sigma_1, \ldots, \sigma_n$, alors ils sont égaux (à permutation près), puisqu'ils sont l'ensemble des racines du même polynôme, dont les coefficients sont les σ_i à signe près.

Une autre famille de fonctions symétriques déterminantes est la famille des sommes de Newton. Si on connaît $s_k = x_1^k + \ldots + x_n^k$ pour tout entier $k = 1, \ldots, n$, alors on peut retrouver $x_1, \ldots, x_n$. Cela vient du fait que l'on peut exprimer les σ_i en fonction des s_k, avec des formules que l'on ne retient pas en général.

Dans le cas des polynômes modulo p, c'est plus compliqué. Les fonctions symétriques élémentaires permettent effectivement de caractériser les racines de P s'il est scindé. En revanche, le résultat sur les sommes de Newton ne tient plus : par exemple les polynômes $(X-2)^p$ et $(X-3)^p$ vont avoir les mêmes sommes de Newton, qui sont toutes nulles. Cela vient du fait que, lorsqu'on établit les relations entre les sommes de Newton s_k et les fonctions symétriques élémentaires σ_i, des coefficients divisibles par p interviennent. L'exemple suivant donne une idée des résultats que l'on peut espérer, et comment les obtenir :

Exemple 17. *(Balkan MO SL 2014 N2)* Soit p un nombre premier et $x_1, \ldots, x_p$ des entiers. On suppose que, pour tout entier $n \geqslant 1$,

$$x_1^k + \ldots + x_p^k \equiv 0 \mod p$$

pour tout entier k strictement positif. Montrer que $x_1 \equiv \ldots \equiv x_p \mod p$.

Solution. Notons que la relation est également vraie pour $k = 0$ car $\underbrace{1 + \ldots + 1}_{p \text{ fois}} \equiv 0 \mod p$

Soit $Q(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients entiers. On a

$$Q(x_1) + \ldots + Q(x_p) = \sum_{\ell=1}^{p} \sum_{k=0}^{n} a_k x_\ell^k = \sum_{k=0}^{n} a_k \underbrace{\sum_{\ell=1}^{p} x_\ell^k}_{\equiv 0 \mod p} \equiv 0 \mod p$$

On suppose par l'absurde que les x_i ne donnent pas tous le même reste modulo p. Soit $\{y_1, \ldots, y_r\}$ l'ensemble des restes modulo p généré par l'ensemble $\{x_1, \ldots, x_p\}$, avec $y_1 \equiv x_1 \mod p$. On note a_1 le nombre d'éléments de l'ensemble $\{x_1, \ldots, x_p\}$ qui ont pour reste y_1. Soit $P(X) = (X - y_2)\ldots(X - y_r)$. P est nul en chacun des y_i pour $i \neq 0$. Notons que, comme $y_1 \neq y_i \mod p$, $P(y_1) \neq 0 \mod p$. La relation établie plus haut nous donne alors $a_1 P(y_1) \equiv 0$

mod p, ce qui implique que $a_1 = 0 \mod p$, c'est-à-dire que $a_1 = p$. Cela est en contradiction avec notre supposition de départ, donc les x_i sont tous égaux.

Exercice 3.43. *(IMO SL 1997)* Soit p un nombre premier et P un polynôme de degré d tel que $P(0) = 0, P(1) = 1$ et, pour tout entier n, soit $P(n) \equiv 0 \mod p$ soit $P(n) \equiv 1 \mod p$. Montrer que $d \geqslant p - 1$.

Exercice 3.44. Soient x, y, z et p quatre entiers tels que p est premier et $0 < x < y < z < p$. On suppose que x^3, y^3 et z^3 ont même reste modulo p. Montrer que $x + y + z$ divise $x^2 + y^2 + z^2$.

Exercice 3.45. *(Envoi 20219-2020)* Soient $m, n \geqslant 2$ des entiers tels que

$$a^n \equiv 1 \mod m$$

pour tout entier $a = 1, 2, \ldots, n$. Montrer que m est premier et que $n = m - 1$.

On termine cette sous-section avec quelques astuces pour employer les polynômes dans un contexte d'Olympiades :

- Pour chercher les racines d'un polynôme P modulo p, on peut regarder des multiples simples de P. Par exemple, si P divise $X^d - 1$, alors toute racine a de P vérifie $a^d \equiv 1 \mod p$, ce qui nous ramène à des considérations sur l'ordre.

  Exemple 18. Pour quels nombres premiers p existe-t-il un entier a tel que $a^4+a^2+1 = 0 \mod p$?

  Solution. **Réponse :** Il s'agit de $p = 3$ et des nombres premiers p tels que $p \equiv 1 \mod 6$.

  Comme a^4 et a^2 sont de même parité, $a^4 + a^2 + 1$ est toujours impair donc les p recherchés doivent l'être aussi.

  Soit p un tel nombre premier et a tel que $p \mid a^4 + a^2 + 1$. Si $a^2 = 1$, alors $p \mid 3$ et $p = 3$, qui est bien solution. Sinon, $p \mid a^4 + a^2 + 1 \mid a^6 - 1$. L'ordre de a divise donc 6 et vaut 3 ou 6 (le cas $a^2 = 1 \mod p$ ayant déjà été traité). D'après le petit théorème de Fermat, cela implique que $p \equiv 1 \mod 3$. Comme en plus $p \equiv 1 \mod 2$, on a $\boxed{p \equiv 1 \mod 6}$. Réciproquement, prenons g un élément d'ordre $p - 1$ modulo p. Alors le nombre $a = g^{(p-1)/6}$ vérifie $a^6 \equiv 1$ mais $a^2 \neq 1 \mod p$, donc $p \mid (a^6 - 1)/(a^2 - 1) = a^4 + a^2 + 1$.

- Dans le cas d'un polynôme de degré 2, on peut s'aider des relations de Viète : si on connaît une racine de P, on peut identifier la seconde.
- Il n'est pas rare que les contraintes d'un problèmes puissent se traduire par des équations polynomiales. Par exemple, si on cherche les points fixes d'une opération (idée salutaire dans de nombreuses situations), ceux-ci seront probablement solution d'une équation polynomiale, et il s'agit alors d'appliquer les conseils précédents.

Exercice 3.46. *(Iran MO 2024 Round 3)* Soit p un nombre premier et $k \geqslant 1$ un entier. Soit P un polynôme à coefficients dans $\{0, 1, \ldots, p - 1\}$. On suppose que P est le polynôme de plus petit degré vérifiant la propriété suivante : on peut placer les entiers $1, 2, \ldots, p-1$ dans un certain ordre autour d'un cercle de sorte que, pour tous k entiers consécutifs $a_1, \ldots, a_k$, on a

$$p \mid P(a_1) + \ldots + P(a_k).$$

Montrer qu'il existe un entier d, des entiers a et b et un polynôme Q à coefficients entiers de degré strictement inférieur à d tel que $P(X) = aX^d + b + pQ(X)$.

Exercice 3.47. (BXMO 2021) Une suite $a_1, a_2, \ldots$ d'entiers vérifie $a_1 > 5$ et $a_{n+1} = 5+6+\ldots+a_n$ pour tout entier positif n. Déterminer tous les nombres premiers p tels que, quelque soit la valeur de a_1, la suite contient un multiple de p.

Exercice 3.48. (IMO SL 2020 N2) Soit p un nombre premier. Le royaume de $p-$Land consiste en p îles numérotées de 1 à p. Deux îles distinctes de numéros n et m sont reliées par un pont si et seulement si p divise l'entier $(n^2 - m + 1)(m^2 - n + 1)$; les ponts ne peuvent pas se croiser, mais peuvent passer l'un en-dessous de l'autre). Montrer qu'il existe une infinité de nombres premiers p pour lesquels le royaume de $p-$Land contient deux îles qui ne sont pas reliées par une suite de ponts.

Exercice 3.49. (EMC 2020) Soit p un nombre premier. Alice et Bob jouent au jeu suivant. Alice écrit un entier strictement positif X au tableau et donne une suite $a_1, a_2, \ldots$ infinie à Bob. Bob effectue alors la suite d'opérations suivantes : lors de la $n-$ème opération, Bob remplace l'entier Y écrit au tableau par l'entier $Y + a_n$ ou par l'entier $Y \cdot a_n$.

Bob gagne si, au bout d'un nombre fini d'opérations, le nombre écrit au tableau est un multiple de p. Déterminer si Bob dispose d'une stratégie gagnante quelle que soit la suite d'Alice pour les nombres premiers suivants :

1. $p = 10^9 + 7$?
2. $p = 10^9 + 9$?

3.2.2 Résidus quadratiques

L'étude des carrés modulo p, aussi appelés pompeusement « résidus quadratiques », intervient la première fois lorsqu'on apprend à montrer qu'une équation comme $a^2 = 3b^2 + 2$ n'a pas de solution, puisque 2 n'est pas un carré modulo 3. Cette heureuse surprise, à savoir que, étant donné p, beaucoup d'entiers ne sont pas des carrés, n'est en fait pas un hasard, et on dispose en réalité d'une large théorie permettant de caractériser les carrés modulo p, théorie que l'on présente ici. Dans la suite, on fixe p un nombre premier, très certainement impair.

Définition 3.19 (Résidu quadratique)**.** Un entier y est appelé *carré modulo p* ou encore *résidu quadratique* s'il existe un entier $x \in \{0, 1, \ldots, p-1\}$ tel que $y \equiv x^2 \mod p$.

Les entiers qui ne sont pas des carrés sont appelés *non carrés* ou *non résidus quadratiques*.

Par exemple, 2 est un carré modulo 7 car $2 \equiv 3^2 \mod 7$. Souvent, on s'intéressera aux carrés non nuls modulo p. Il est possible de déterminer complètement ces carrés modulo p, via la proposition suivante.

Proposition 3.20. Il existe exactement $\dfrac{p+1}{2}$ résidus quadratiques modulo p, à savoir les nombres $0^2, 1^2, \ldots, \left(\dfrac{p-1}{2}\right)^2 \mod p$.

Démonstration. Soit y un résidu quadratique modulo p et $x \in \{0, \ldots, p-1\}$ tel que $y \equiv x^2 \mod p$. Comme on a aussi $(p-x)^2 \equiv x^2 \equiv y \mod p$, on peut supposer, quitte à prendre $p-x$, que $x \in \{0, 1, \ldots, (p-1)/2\}$.

D'autre part, les nombres $0^2, 1^2, \ldots, \left(\dfrac{p-1}{2}\right)^2$ sont deux à deux distincts : si on a deux tels nombres $i > j$ tels que $i^2 \equiv j^2$, alors $p \mid i^2 - j^2 = (i-j)(i+j)$, alors que les deux nombres $i-j$ et $i+j$ sont compris strictement entre 0 et p.

On a donc le nombre exact de résidus quadratiques et on sait tous les calculer. La preuve montre également que si $y \equiv x^2 \mod p$ est un carré modulo p, ses seules *racines carrés* sont x et $p-x$. On peut aussi s'en douter en voyant les racines carrés de y comme les racines du polynôme $X^2 - y$, qui a au plus deux racines modulo p et dont la somme vaut 0 modulo p d'après les relations de Viète.

On peut aller plus loin et comprendre *la structure* des résidus quadratiques, à l'aide du symbole de Legendre :

Définition 3.21 (Symbole de Legendre)**.** On adopte la notation suivante, appelée *symbole de Legendre* :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a \\ 1 & \text{si } a \text{ est un carré non nul modulo } p \\ -1 & \text{si } a \text{ n'est pas un carré modulo } p \end{cases}$$

Les liens entre les carrés et non carrés modulos p sont capturés par la formule suivante :

Proposition 3.22. Soient a et b deux entiers.

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Démonstration. Si a ou b est divisible par p, la formule est vraie. On suppose dans la suite que a et b sont non nuls. On distingue 3 cas :

- Si $a \equiv x^2 \mod p$ et $b \equiv z^2 \mod p$ sont des carrés, alors $ab \equiv (xz)^2 \mod p$ est également un carré, donc $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right) = 1 = \left(\dfrac{ab}{p}\right)$.
- Si $a \equiv x^2 \mod p$ est un carré et b n'est pas un carré, on a que ab n'est pas un carré : si on avait $ab \equiv z^2 \mod p$, on aurait $b \equiv (ba)a^{-1} \equiv (zx^{-1})^2 \mod p$, contredisant

l'hypothèse sur b. Ainsi, ab n'est pas un carré et $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -1 = \left(\frac{ab}{p}\right)$.

➢ On suppose que a et b ne sont pas des carrés. Puisque $x \mapsto ax \mod p$ est une bijection de $\{1, \dots, p-1\}$ dans lui-même, l'ensemble $\{a, 2a, \dots, (p-1)a\}$ contient exactement $(p-1)/2$ carrés et $(p-1)/2$ non-carrés. Or, si $x_1, \dots, x_{(p-1)/2}$ désignent les carrés modulo p, on a vu au cas précédent que $ax_1, \dots, ax_{(p-1)/2}$ sont des non-carrés. Comme ils sont distincts, il s'agit des $(p-1)/2$ non-carrés. Ainsi, ab n'est pas un non-carré, c'est donc bien un carré, et

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1 = \left(\frac{ab}{p}\right).$$

Le dernier cas illustre le comportement de la bijection $x \mapsto ax$. Si a est un carré, elle conserve les carrés et les non carrés, mais si a n'est pas un carré, elle échange les carrés et les non-carrés.

Les résidus quadratiques peuvent également être vus comme les racines du polynôme $X^{(p-1)/2} - 1$, ce qui donne le critère suivant :

Proposition 3.23 (Critère de Gauss)**.** Les carrrés modulo p non nuls sont exactement les racines modulo p du polynôme $X^{\frac{p-1}{2}} - 1$, ce qui se réécrit également comme

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

Démonstration. Soit $y \equiv x^2 \mod p$ un carré modulo p. On a par le petit théorème de Fermat

$$y^{\frac{p-1}{2}} \equiv x^{2\cdot\frac{p-1}{2}} = x^{p-1} \equiv 1 \mod p,$$

donc y est racine de $X^{\frac{p-1}{2}} - 1$. Comme ce polynôme admet au plus $\frac{p-1}{2}$ racines et que les $\frac{p-1}{2}$ carrés sont tous racines de ce polynôme, il s'agit des seules racines, ce qui prouve la première partie de la proposition.

Pour la deuxième partie, on constate que tous les nombres de $\{1, \dots, p-1\}$ sont racines de $X^{p-1} - 1 = (X^{(p-1)/2} - 1)(X^{(p-1)/2} + 1)$. Il vient que les non carrés a sont racines de $X^{(p-1)/2} + 1$, donc ils vérifient $a^{(p-1)/2} \equiv -1 \mod p$, ce qui conclut que $a^{(p-1)/2}$ et $\left(\frac{a}{p}\right)$ coïncident modulo p.

Corollaire 3.24. Soit p un nombre premier impair. Le nombre -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$.

Démonstration. D'après le critère d'Euler, $p \mid \left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}$. Or la différence des deux nombres est comprise entre -2 et 2, et $p > 3$. On a donc bien égalité. Comme $(-1)^{(p-1)/2} = 1$

si $p \equiv 1 \mod 4$ et $(-1)^{(p-1)/2} = -1$ si $p \equiv 3 \mod 4$, on déduit le critère annoncé.

Le corollaire suivant s'est montré utile dans de nombreuses situations et est donc à connaître :

Corollaire 3.25. Soit p un nombre premier tel que $p \equiv 3 \mod 4$. Soient a et b des entiers tels que $p \mid a^2 + b^2$. Alors $p \mid a$ et $p \mid b$.

Démonstration. Supposons que p ne divise pas b. La divisibilité devient $a^2 \equiv -b^2 \mod 4$, soit $(ab^{-1})^2 \equiv -1 \mod p$. Cela impliquerait que -1 est un carré modulo p, ce qui est impossible car $p \equiv 3 \mod 4$.

Pour les problèmes d'Olympiade, ce qui est attendu est d'avoir compris le comportement de $x \mapsto ax$ sur les carrés et les non carrés, d'avoir en tête que les deux éventuelles racines carrés de y sont x et $p - x$ et enfin et surtout de savoir à quelle condition sur p des nombres spécifiques sont des carrés, notamment -1. D'autres conditions sont obtenues par les lois suivantes, dont la troisième est appelée loi de réciprocité quadratique, dont les preuves dépassent le cadre de ce polycopié et ne sont donc pas présentées :

Théorème 3.26. Soient p et q des nombres premiers impairs. Alors

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \qquad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

En particulier, 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.

La troisième égalité, qui est donc la loi de réciprocité quadratique, permet de déterminer itérativement les carrés modulo p pour tout p (voir l'exercice 3.51).

On termine avec la résolution des équations de degré 2 modulo p, permettant de faire le lien entre les deux sous-sections :

Proposition 3.27 (Équations de degré 2 modulo p)**.** Soit p un nombre premier **impair** et a et b des entiers. On pose $P(X) = X^2 + aX + b$ et on note $\Delta = a^2 - 4b$. Alors :

- si $\Delta \equiv 0 \mod p$, le polynôme P admet une racine double modulo p,
- si Δ est un carré non nul modulo p, le polynôme P admet deux racines modulo p,
- si Δ n'est pas un carré modulo p, le polynôme P n'admet pas de racines modulo p.

Démonstration. Il s'agit de répliquer les calculs de la résolution d'une équation de degré 2 dans $\mathbb{R}$. Comme p est impair, 2 est inversible modulo p, donc on peut réécrire P sous sa forme canonique :

$$P(X) = \left(X + \frac{a}{2}\right)^2 - \frac{a^2 - 4b}{4} = \left(X + \frac{a}{2}\right)^2 - \frac{\Delta}{4}.$$

On voit d'emblée que s'il existe un entier x tel que $P(x) \equiv 0 \mod p$, alors

$$\Delta = \left[2\left(x + \frac{a}{2}\right)\right]^2 \mod p$$

donc Δ est un carré modulo p. En particulier, si Δ n'est pas un carré modulo p, le polynôme P n'admet pas de racines. Réciproquement :

- Si $\Delta \equiv 0 \mod p$, on a directement $P(X) \equiv \left(X + \frac{a}{2}\right)^2 \mod p$.
- Si Δ est un carré modulo p, on dispose d'un entier δ tel que $\Delta \equiv \delta^2 \mod p$. On a alors

$$P(X) \equiv \left(X + \frac{a}{2}\right)^2 - \left(\frac{\delta}{2}\right)^2 = \left(X + \frac{a-\delta}{2}\right)\left(X + \frac{a+\delta}{2}\right) \mod p,$$

ce qui donne bien que P admet les deux racines $\frac{-a+\delta}{2}$ et $\frac{-a-\delta}{2}$ modulo p.

Remarque : On a vu pourquoi les calculs précédents ne pouvaient se faire dans le cas $p = 2$. De fait, si $p = 2$, la proposition est fausse puisque le polynôme $X^2 + X + 1$ n'admet pas de racines modulo 2 (il est à valeurs impaires) bien que son discriminant soit un carré modulo 2.

Exercice 3.50. Que vaut le reste de la division par p de la somme des résidus quadratiques modulo p ?

Exercice 3.51. Pour quels nombres premiers p le nombre 3 est-il un carré modulo p ? Le nombre 5 ?

Exercice 3.52. Soit $p \equiv 1 \mod 4$. Montrer que $p \mid ((\frac{p-1}{2})!)^2 + 1$.

Exercice 3.53. (Autriche MO 2024) Déterminer les éléments x de $\{0, 1, \ldots, p-1\}$ tels qu'il existe deux entiers a et b tels que $x \equiv a^2 + b^2 \mod p$.

Exercice 3.54. (Olympiade Abel 2025, Norvège) Pour quels entiers positifs a existe-t-il une infinité d'entiers n tels que $n! - a$ est un carré parfait ?

Exercice 3.55. (Balkan MO SL 2024 N3) Montrer qu'il existe une infinité de nombres premiers divisant un nombre de la forme $2^n + 3^{n+2} + 5^{n+1}$ avec $n \geqslant 1$.

Exercice 3.56. (Iran MO 2015 Round 3/Entraînement D 2021) Soit $p > 5$ un nombre premier et $A = \{b_1, b_2, \ldots, b_{\frac{p-1}{2}}\}$ l'ensemble des résidus quadratiques non nuls modulo p. Montrer qu'il n'existe pas deux entiers a et c premiers avec p tels que les ensembles A et $B = \{ab_1 + c, \ldots, ab_{\frac{p-1}{2}} + c\}$ sont disjoints modulo p.

Exercice 3.57. (RMM 2013 P1) Soit a un entier strictement positif. On définit la suite $x_1, x_2, \ldots$ par $x_1 = a$ et $x_{n+1} = 2x_n + 1$ pour tout $n \geqslant 1$. On pose également $y_n = 2^{x_n} - 1$ pour tout $n \geqslant 1$. Déterminer le plus grand entier k tel qu'il existe un entier a pour lequel $y_1, \ldots, y_k$ sont premiers.

Exercice 3.58. (APMO 2014) Trouver les entiers $n \geqslant 1$ tels que pour tout entier k, il existe a tel que $n \mid a^3 + a - k$.

Exercice 3.59. (Balkan MO 2025 P1) Un entier $n \geqslant 1$ est dit *bon* s'il existe une permutation $a_1, a_2, \ldots, a_n$ des entiers $1, 2, \ldots, n$ telle que

- Les nombres a_i et a_{i+1} sont de parité différente pour tout $1 \leqslant i \leqslant n-1$.

➢ La somme $a_1 + \ldots + a_k$ est un carré modulo n pour tout indice $1 \leqslant k \leqslant n$.

Montrer qu'il existe une infinité d'entiers bons et une infinité d'entiers qui ne sont pas bons.

Exercice 3.60. *(Iran TST 2020)* Soit p un nombre premier impair. Déterminer tous les $\dfrac{p-1}{2}$−uplets $(x_1, \ldots, x_{(p-1)/2})$ d'éléments de $\{0, \ldots, p-1\}$ tels que

$$\sum_{i=1}^{\frac{p-1}{2}} x_i \equiv \sum_{i=1}^{\frac{p-1}{2}} x_i^2 \equiv \ldots \equiv \sum_{i=1}^{\frac{p-1}{2}} x_i^{\frac{p-1}{2}} \mod p.$$

Exercice 3.61. Soit n un entier (non nécessairement positif) qui est un carré modulo p pour tout nombre premier p. Montrer que n est un carré parfait.

On termine cette partie avec le lemme de Hensel, qui permet, à partir d'une racine de P modulo p, de construire une racine de P modulo p^α.

Théorème 3.28 (Lemme de Hensel)**.** Soit p un nombre premier, $n \geqslant 2$ un entier et P un polynôme à coefficients entiers. On suppose qu'il existe un entier x tel que $P(x) \equiv 0 \mod p$ et $P'(x) \neq 0 \mod p$. Alors il existe un entier y tel que $P(y) \equiv 0 \mod p^n$ et $x \equiv y \mod p$.

Démonstration. On procède par récurrence sur $n \geqslant 1$.

Initialisation : Si $n = 1$, il suffit de prendre $y \equiv x \mod p$.

Hérédité : On suppose que la propriété est vraie au rang n, avec $n \geqslant 1$ fixé : il existe un entier y_n tel que $P(y_n) \equiv 0 \mod p^n$ et $y_n \equiv x \mod p$, et on cherche un entier y_{n+1} vérifiant l'énoncé pour $n+1$. Comme y_{n+1} doit vérifier la même équation que y_n modulo p^n, il est raisonnable de chercher y_{n+1} sous la forme $y_n + kp^n$.

Notons que pour tout entier ℓ, la formule du binôme donne que

$$(y_n + kp^n)^\ell = y_n^\ell + \ell y_n^{\ell-1} kp^n + \sum_{i=2}^{\ell} \binom{\ell}{i} \underbrace{p^{ni}}_{p^{n+1}|} k^i y_n^{\ell-i} \equiv y_n^\ell + \ell y_n^{\ell-1} kp^n \mod p^{n+1}.$$

En notant $P(X) = a_d X^d + \ldots + a_1 X + a_0$, on trouve en sommant la congruence précédente

$$\begin{aligned} P(y_n + kp^n) &\equiv a_d(y_n + kp^n)^d + \ldots + a_1(y_n + kp^n) + a_0 \\ &\equiv a_d(y_n^d + d y_n^{d-1} kp^n) + \ldots + a_1(y_n + kp^n) + a_0 \equiv P(y_n) + kp^n P'(y_n) \mod p^{n+1}. \end{aligned}$$

Le but est alors de choisir k de sorte que ce dernier terme soit nul. Comme $P(y_n) \equiv 0 \mod p^n$, il existe un entier m tel que $P(y_n) = mp^n$. Comme $P'(y_n) \neq 0$, on peut trouver k tel que $kP'(y_n) \equiv -m \mod p$. Il vient alors, en posant $y_{n+1} = y_n + kp^n$, que $P(y_{n+1}) \equiv 0 \mod p^{n+1}$, ce qui achève la récurrence.

Il faut retenir que le lemme de Hensel est un résultat **d'existence** : il existe une solution à une équation modulo p^n. Il permet donc de construire des entiers spécifiques.

On notera la conséquence suivante :

Corollaire 3.29. Soit p un nombre premier impair et $n \geqslant 2$ un entier. Alors x est un carré non nul modulo p si et seulement si x est un carré inversible modulo p^n.

Démonstration. On procède par double implication :
$\boxed{\Leftarrow}$ Si x est un carré modulo p^n, alors il existe y tel que $x \equiv y^2 \mod p^n$, donc $x \equiv y^2 \mod p$.
$\boxed{\Rightarrow}$ Si x est un carré non nul modulo p, cela signifie que le polynôme $P(X) = X^2 - x$ admet une racine y non nulle. En particulier, comme p est impair, $P'(y) = 2y \neq 0 \mod p$. D'après le lemme de Hensel, il existe un entier z tel que $z \equiv y \mod p$ et $z^2 = P(z) \equiv x \mod p^n$, de sorte que x est un carré modulo p^n.

Exercice 3.62. (ELMO SL 2014 N1) Montrer qu'il existe une suite infinie (a_k) d'entiers telle que, pour tout entier $k \geqslant 1$, $13^k \mid a_k^2 + 1$.

Exercice 3.63. Soit p un nombre premier, $n \geqslant 1$ et k un entier non divisible par p. Montrer que x est une puissance $k-$ème modulo p si et seulement si x est une puissance $k-$ème modulo p^n.

Exercice 3.64. (Thailand TSTST 2021) Un nombre premier p impair est dit *incroyable* si il existe un entier n tel que p^{2022} divise $n^{2022} + 2022$. Montrer qu'il existe une infinité de nombres premiers incroyables.

Exercice 3.65. (IMO 1999 N3) Montrer qu'il existe deux suites strictement croissantes (a_n) et (b_n) telles que, pour tout entier n, $a_n(a_n + 1) \mid b_n^2 + 1$.

3.3 Divisibilité et taille, épisode 2 - arguments asymptotiques

Dans cette sous-partie, il s'agit d'appréhender la notion d'entiers arbitrairement grands pour s'en servir. Il y a deux savoir-faire à maîtriser :

- ☞ Transformer l'hypothèse « une infinité d'entiers vérifient $\mathcal{P}$ » en « des entiers arbitrairement grands vérifient $\mathcal{P}$ ».
- ☞ Pouvoir comparer des quantités arbitrairement grandes (souvent des suites dont les croissances sont différentes).

Pour se rendre compte de notre difficulté à appréhender des entiers très grands, on pourra essayer de se représenter mentalement une salle contenant une centaine de millions de personnes et une salle contenant une centaine de milliards de personnes. Malgré le fait qu'une salle contient mille fois plus de personnes que l'autre, les deux images que nous allons former seront probablement assez similaires. Si l'on cherche un exemple en termes de nombres, on pourra essayer de deviner le plus rapidement possible et sans calcul lequel des deux nombres $(n!)^{2^n}$ et $(2^n)^{n!}$ est le plus grand.

Un tel obstacle est généralement levé pendant la première année de post-bac, avec un cours d'introduction au calcul asymptotique. Pourtant des problèmes récents d'Olympiades, sans exiger concrètement de connaissances nouvelles, demandent une certaine aisance avec ces notions : comparer les ordres de grandeurs de deux suites qui tendent vers $+\infty$, exploiter une infinité d'entiers vérifiant une certaine propriété... des arguments qui nécessitent à la fois de la technique et un peu d'abstraction. On propose donc de présenter le nécessaire de la théorie relative à ces arguments.

Dans toute la suite, on gardera en tête le principe des tiroirs infini, que l'on utilisera de bien des façons différentes.

Proposition 3.30. Soit (u_n) une suite bornée d'entiers. Alors il existe un entier ℓ et une infinité de termes de la suite égaux à ℓ.

Lorsque plusieurs paramètres sont bornés, l'emploi répété de ce principe permet d'obtenir une sous-suite de (u_n) constante pour chacun de ces paramètres.

La suite de cette section se décline en deux idées. La première est d'employer le passage à la limite dans les exercices d'arithmétique. Pour certaines égalités, supposées vraies pour une infinité de n, on ne trouve pas de contradiction à n fixé, mais plutôt à la limite. Cet argument fonctionne bien pour des suites convergentes. Lorsque les suites sont divergentes, la contradiction peut venir de leur vitesse de croissance. Ce qui amène à la deuxième idée, qui est de revenir aux arguments de croissance comparée pour obtenir à nouveau une contradiction à la limite.

3.3.1 Passer à la limite

Pour attaquer cette partie, on suppose connus les éléments suivants :

- ☞ Définition d'une limite de suite, définition d'une suite qui tend vers $+\infty$.
- ☞ Les propriétés de base : unicité et linéarité de la limite.
- ☞ Le théorème des gendarmes.

On pourra trouver une introduction au sujet dans le polycopié du stage d'été 2025, dans le cours « Introduction aux réels » adressé au groupe D.

La spécificité, ici, est que les suites d'entiers possèdent des propriétés supplémentaires une fois passées à la limite.

Proposition 3.31. Soit (u_n) une suite d'entiers telle que u_n converge vers un réel ℓ. Alors ℓ est entier et il existe un rang N tel que, pour tout $n \geqslant N$, $u_n = \ell$.

Autrement dit : toute suite convergente d'entiers est constante à partir d'un certain rang (on dit qu'elle est stationnaire).

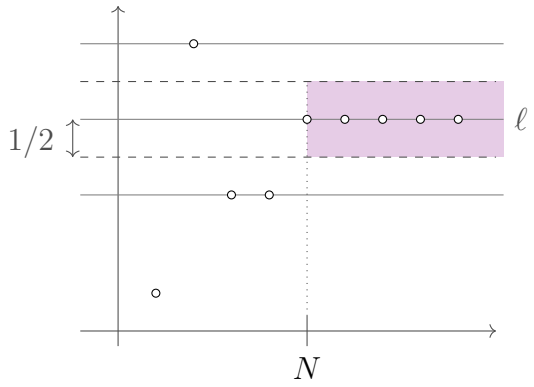
La version suivante de cette propriété apparaît très fréquemment.

Corollaire 3.32. Une suite décroissante d'entiers positifs est constante à partir d'un certain rang.

Démonstration. **Preuve de la propriété.** Puisque (u_n) converge vers ℓ, il existe un rang N tel que, pour tout $n \geqslant N$, $|u_n - \ell| < 1/2$. Ainsi, si $n \geqslant M$, on a d'après l'inégalité triangulaire

$$|u_n - u_N| \leqslant |u_n - \ell| + |u_N - \ell| < 1/2 + 1/2 = 1.$$

Comme u_n et u_N sont des entiers, on déduit que $u_n = u_N$. La suite (u_n) est donc constante à partir du rang N. Il vient que $\ell = \lim\limits_{n\to+\infty} u_n = u_N$, donc ℓ est entier.



L'emploi est le suivant : si on a une égalité vraie pour une infinité d'entiers n, passer à la limite cette égalité en faisant tendre n vers $+\infty$ fait souvent sortir des informations. Présentons deux exemples :

Exemple 19. Soient a et b deux réels strictement positifs tels qu'il existe une infinité d'entiers n tels que $\lfloor an \rfloor = \lfloor bn \rfloor$. Montrer que $a = b$.

Solution. Commençons par montrer que, pour tout réel x, $\lim\limits_{n\to+\infty} \dfrac{\lfloor xn \rfloor}{n} = x$. On a, en effet, pour tout entier n,

$$x - \frac{1}{n} = \frac{xn - 1}{n} < \frac{\lfloor xn \rfloor}{n} \leqslant \frac{xn}{n} = x.$$

Comme le membre de gauche tend vers x lorsque n tend vers $+\infty$ et que le membre de droite est constant égal à a, on a le résultat voulu d'après le théorème des gendarmes.

On revient désormais à l'exercice : notons (m_n) la suite (strictement croissante) des entiers tels que $\lfloor am_n \rfloor = \lfloor bm_n \rfloor$. On a alors en passant à la limite :

$$a = \lim_{n\to+\infty} \frac{\lfloor am_n \rfloor}{m_n} = \lim_{n\to+\infty} \frac{\lfloor bm_n \rfloor}{m_n} = b.$$

Cet exemple, bien qu'issu de l'algèbre, donne une façon de traiter des problèmes faisant intervenir des parties entières.

Exemple 20. *(Bulgarie MO 2021 P4)* Soit $a, b \in \mathbb{N}^*$ et $c, d \in \mathbb{N}$ tels qu'il y ait une infinité de paires (i, j) d'indices vérifiant $i \leqslant j \leqslant i + 2021$ et $ai + b \mid cj + d$. Montrez que pour tout indice i, il existe j tel que $ai + b$ divise $cj + d$.

Solution. Appelons *sympa* une paire (i, j) d'indices vérifiant la propriété de l'énoncé. Pour toute paire sympa (i, j), le nombre $j - i$ est dans $[\![0, 2021]\!]$. D'après le principe des tiroirs, il existe un entier $t \in [\![0, 2021]\!]$ et une infinité de paires (i, j) sympas vérifiant $j - i = t$. La paire (i, j) est donc $(i, i + t)$. On dit qu'un entier i tel que $(i, i + t)$ est sympa qu'il est *super sympa*.

Ainsi, on dispose d'une infinité d'entiers $i_0 < i_1 < \dots$ super sympas, qui vérifient donc $ai_n + b \mid c(i_n + t) + d$ pour tout indice n. Or on a

$$\lim_{i\to+\infty} \frac{c(i + t) + d}{ai + b} = \frac{c}{a}.$$

La suite $\left(\dfrac{c(i_n + t) + d}{ai_n + b}\right)_i$ est donc une suite d'entiers qui converge, elle est donc constante égale à c/a à partir d'un certain rang, ce qui implique en particulier que $\boxed{a/c \text{ est un entier}}$. On écrit $c = as$, avec s entier.

Mais alors, pour tout entier i sympa, $ai + b \mid sa(i + t) + d$ donc $ai + b \mid s(at - b) + d$. Le nombre $s(at - b) + d$ admet une infinité de diviseurs, il est donc nul et on a $\boxed{sb = ct + d}$. Mais alors $c(i + t) + d = s(ai + b)$ pour tout entier $i \geqslant 1$, donc en posant $j = i + t$,on obtient $ai + b \mid cj + t$ comme voulu.

Dans l'exemple précédent, on a

1. employé le principe des tiroirs pour avoir un entier t qui ne dépend pas de (i, j), permettant de supprimer j ;
2. passé une divisibilité à la limite pour obtenir une information à laquelle on n'avait pas accès à i fixé.

Il s'agit là des arguments typiques pour gérer un énoncé du type « il existe une infinité d'entiers tels que ».

Permettons-nous d'énoncer un autre principe général lisible dans l'exercice précédent : lorsqu'un énoncé décrit une quantité qui est supposée être un entier (dans l'exemple précédent, il s'agit du quotient $\dfrac{c(i + t) + d}{ai + b}$), il est intéressant d'introduire la suite (x_n) d'entiers associée. Dans l'exemple ci-dessus, cette suite converge. Parfois, ce n'est pas la suite (x_n) elle-même mais la suite $(x_{n+1} - x_n)$, ou d'autres variantes. Il est plus facile de deviner l'expression adéquate en introduisant explicitement la suite. Cette astuce d'introduire une suite auxiliaire bien choisie sera revue dans la sous-section 4.1 consacrée aux suites d'entiers.

On pourra s'exercer avec les problèmes suivants.

Exercice 3.66. (Thaïlande TSTST 2023) Soit $a \geqslant 2$ un entier. Montrer qu'il n'existe pas de fonction $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telle que

$$(m + f(n))^2 \geqslant af(m)^2 + n^2$$

pour tous entiers $m, n \in \mathbb{N}^\star$.

Exercice 3.67. Soient a et b des entiers tels que a est non nul et $an^2 + b$ est un carré parfait pour tout entier n. Montrer que $b = 0$ et que a est un carré parfait.

Exercice 3.68. Soient a et b des entiers tels que $a \cdot 2^n + b$ est un carré parfait pour tout entier $n \geqslant 1$. Montrer que $a = 0$.

Exercice 3.69. (Concours 18 MT P6/création de Gaëtan Dautzenberg) Trouver tous les polynômes P à coefficients entiers tels qu'il existe des entiers strictement positifs $a < b < c < d$ vérifiant la propriété suivante : pour tout entier $k \geqslant 1$, le nombre $P(ak) + P(bk)$ est non nul et

$$P(ak) + P(bk) \mid P(ck) + P(dk).$$

Exercice 3.70. (USA TSTST 2021 P4) Soient a et b des entiers strictement positifs. On suppose qu'il existe une infinité de couples (m, n) tels que $m^2 + an + b$ et $n^2 + am + b$ sont tous les deux des carrés parfaits. Montrer que a divise $2b$.

3.3.2 Croissances comparées

On passe à la deuxième partie de cette section, qui consiste à être en mesure de comparer des ordres de grandeur de suites de nombres. Donc contrairement à la sous-section précédente, où l'on regardait des suites convergentes et dont on comparait les limites, on regarde ici des suites divergentes dont on compare la vitesse de croissance.

L'idée n'a rien de nouvelle, on employait déjà les croissances comparées pour intuiter qu'une équation diophantienne telle que $n + 2 = 2^n$ n'a qu'un nombre fini de solutions. Ici, on utilisera les croissances comparées pour montrer qu'un problème n'a pas de solutions du tout, ou n'en a qu'un nombre fini.

C'est l'occasion d'introduire quelques notations nouvelles, propres au calcul asymptotique.

Définition 3.33 (Notations $o, O, \sim$)**.** Soient (a_n) et (b_n) deux suites réelles, telles que les termes de b_n sont non nuls. On dira que

- $a_n = o(b_n)$ si $a_n/b_n \to 0$ (on dit alors que a_n est négligeable devant b_n),
- $a_n = O(b_n)$ s'il existe une constante $C > 0$ telle que $|a_n| \leqslant C|b_n|$ pour tout indice n, autrement dit si la suite (a_n/b_n) est bornée,
- $a_n \sim b_n$ si $a_n/b_n \to 1$ (prononcé « a_n est équivalente à b_n »).

Quelques exemples pour manipuler :

1. $a_n \to 0$ se réécrit comme $a_n = o(1)$. Notons que cela se réécrit aussi $a_n = o(3)$, mais l'usage est de comparer (a_n) à la suite constante égale à 1.

2. Si $a_n \longrightarrow c$ avec $c \neq 0$ se réécrit comme $a_n \sim c$,
3. $n = o(n^2)$,
4. $n^4 + n^3 = O(n^4)$,
5. Si $P(X) = a_d X^d + \ldots + a_0$ est à coefficients réels, alors $P(n) \sim a_d n^d$,
6. Si $0 < a < b$ sont des réels, alors $a^n + b^n \sim b^n$,
7. $a_n \sim b_n$ si et seulement si $a_n = b_n + o(b_n)$,
8. Si $a_n = o(b_n)$ et $b_n = o(c_n)$, alors $a_n = o(c_n)$.
9. Si $a_n \leqslant b_n$ et $b_n = o(c_n)$, alors $a_n = o(c_n)$.
10. Si $a_n = o(b_n)$ et c_n est non nulle, alors $a_n c_n = o(b_n c_n)$ (le $o()$ absorbe)

On laisse l'exercice suivant en guise d'entraînement supplémentaire :

Exercice 3.71.

1. Soit $(a_n), (b_n), (c_n)$ et (d_n) des suites non nulles. On suppose que $a_n \sim b_n$ et $c_n \sim d_n$. Montrer que $a_n c_n \sim b_n d_n$.
2. Soit (a_n) et (b_n) deux suites non nulles qui tendent vers $+\infty$ et telles que $a_n \sim b_n$. Montrer que $\ln a_n \sim \ln b_n$.
3. Soit (a_n) et (b_n) deux suites telles que $a_n - b_n \longrightarrow 0$. Montrer que $2^{a_n} \sim 2^{b_n}$.
4. En prenant $a_n = n^2 + n$ et $b_n = n^2$, vérifier que l'implication de la question précédente est fausse si on remplace l'hypothèse $a_n - b_n \longrightarrow 0$ par l'hypothèse $a_n \sim b_n$.
5. Soient $(a_n), (b_n), (c_n)$ et (d_n) des suites à valeurs strictement positives. On suppose que $a_n \sim b_n$ et $c_n \sim d_n$. Montrer que $a_n + c_n \sim b_n + d_n$.

Au vu de cet exercice, permettons-nous un avertissement : les notations o, O et $\sim$ sont très capricieuses avec les opérations élémentaires. Par exemple, en général, on ne peut pas sommer des $\sim$. On ne peut pas non plus dire que si $a_n \sim b_n$, alors $c^{a_n} \sim c^{b_n}$. On déconseille donc de chercher à faire des opérations avec ces notations. On les présente ici parce qu'il serait bête d'omettre leur existence, mais on n'encourage pas leur utilisation.

Les croissances comparées se réécrivent de la façon suivante :

Théorème 3.34 (croissances comparées)**.** On a les comparaisons suivantes :

- Pour tout entier $k \geqslant 1$ et tout entier $a > 1$, $n^k = o(a^n)$,
- Pour tout entier $k \geqslant 1$ et tout entier $a < 1$, $a^n = o\left(\frac{1}{n^k}\right)$,
- Pour tout entier $k \geqslant 1$, tout entier $\ell \geqslant 1$, $(\ln n)^\ell = o(n^k)$.

On ajoute à ces résulats deux autres résultats assez courants : l'équivalent de la série harmonique et l'équivalent de $n!$, dont les preuves sont omises.

Proposition 3.35. Soit $H_n = 1 + \dfrac{1}{2} + \ldots + \dfrac{1}{n}$. Alors

$$H_n \sim \ln n.$$

Proposition 3.36 (Formule de Stirling)**.** Soit e la constante d'Euler (avec $e = 2.718...$). Alors

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}.$$

En conséquence, pour tout entier n suffisamment grand,

$$\left(\frac{n}{3}\right)^n \leqslant n! \leqslant \left(\frac{n}{2}\right)^n.$$

En pratique, c'est l'encadrement donné qui peut servir pour les Olympiades. Il est exigible pour les exercices difficiles, et il peut servir « d'intuition » pour des arguments de taille, sans forcément qu'il intervienne directement.

Montrons (à nouveau) par un exemple comment utiliser ces comparaisons dans un problème d'arithmétique.

Exemple 21. Soient a et b des entiers tels que $1 < a \leqslant b < a^2$. On suppose que $a^n - 1 \mid b^n - 1$ pour tout entier n. Montrer que $b = a$.

Solution. Posons $k_n = \dfrac{b^n - 1}{a^n - 1}$, qui est un entier. Supposons par l'absurde que $b > a$. Puisque $k_n \sim \left(\dfrac{b}{a}\right)^n$, on a $k_{n+1} \sim \dfrac{b}{a} k_n$. Ceci amène à considérer le nombre $ak_{n+1} - bk_n$ (dont il serait faux d'affirmer immédiatement qu'il tend vers 0, car $ak_{n+1} \sim bk_n$ ne signifie pas que $ak_{n+1} - bk_n \to 0$). On a alors

$$ak_{n+1} - bk_n = \frac{(1-a)b^{n+1} + (b-1)a^{n+1} + (a-b)}{(a^{n+1}-1)(a^n-1)}.$$

Or, le dénominateur vérifie $(a^{n+1}-1)(a^n-1) \sim a^{2n+1}$, tandis que, comme $a^{n+1} = o(b^n)$ et $a - b = o(b^n)$, le numérateur vaut

$$(1-a)b^{n+1} + (b-1)a^n + (a-b) = (1-a)b^{n+1} + o(b^n) \sim (1-a)b^{n+1}.$$

On déduit que

$$ak_{n+1} - bk_n \sim \frac{(1-a)b^{n+1}}{a^{2n+1}} = \frac{(1-a)b}{a}\left(\frac{b}{a^2}\right)^n \longrightarrow 0.$$

Comme la suite $(ak_{n+1} - bk_n)$ est une suite d'entiers qui converge vers 0, on déduit qu'elle vaut 0 pour n suffisamment grand. Cela signifie que le numérateur de la fraction ci-dessus est nul à partir d'un certain rang, alors qu'au vu de son équivalent, il est strictement négatif. Cette contradiction implique que $b = a$.

On pourra pratiquer également les exercices suivants :

Exercice 3.72. (RMM 2024 P4) Soient a et b des entiers strictement plus grands que 1. Pour tout entier $n \geqslant 1$, on note r_n le reste de la division euclidienne de b^n par a^n. On suppose qu'il

existe un entier $N \geqslant 1$ tel que $r_n < \dfrac{2^n}{n}$ pour tout entier $n \geqslant N$. Montrer que a divise b.

Exercice 3.73. *(IMO P4 2019)* Déterminer toutes les paires d'entiers (k, n) strictement positifs telles que

$$k! = (2^n - 1)(2^n - 2)(2^n - 4)\dots(2^n - 2^{n-1}).$$

Exercice 3.74. *(IMO SL 2011 A2)* Déterminer tous les 2011−uplets $(x_1, \dots, x_{2011})$ d'entiers strictement positifs tels que, pour tout entier n, il existe un entier a_n tel que

$$x_1^n + 2x_2^n + \dots + 2011x_{2011}^n = a_n^{n+1} + 1.$$

Exercice 3.75. Trouver les polynômes P à coefficients entiers tels que, pour tout entier n, le nombre $P(n)$ est un palindrome.

Exercice 3.76. *(P6 EGMO 2021)* Existe-t-il un entier $a \geqslant 0$ tel que l'équation

$$\left\lfloor \frac{m}{1} \right\rfloor + \left\lfloor \frac{m}{2} \right\rfloor + \left\lfloor \frac{m}{3} \right\rfloor + \dots + \left\lfloor \frac{m}{m} \right\rfloor = n^2 + a$$

admet plus de un million de solutions différentes (m, n) pour lesquelles m et n sont des entiers strictement positifs ?

Exercices

Les exercices suivants sont une sélections d'exercices utilisant des arguments de principe des tiroirs infinis, de passages à la limite et de croissance comparée. Certains d'entre eux, particulièrement difficiles, peuvent demander des connaissances en analyse plus poussées.

Exercice 3.77. *(EMC 2014/Mexico Regional 2021)* Soit $a_1, a_2, \dots$ une suite d'entiers strictement positifs telle que

- pour tous indices m et n, $a_{mn} = a_m a_n$.
- il existe une infinité d'entiers n tels que $(a_1, \dots, a_n)$ est une permutation de $(1, 2, \dots, n)$.

Montrer que $a_n = n$ pour tout indice n.

Exercice 3.78. *(IMO 2024 P1)* Déterminer tous les réels α tels que, pour tout entier n strictement positif, l'entier

$$\lfloor \alpha \rfloor + \lfloor 2\alpha \rfloor + \dots + \lfloor n\alpha \rfloor$$

soit un mutiple de n. (On rappelle que $\lfloor z \rfloor$ désigne le plus grand entier inférieur ou égal à z. Par exemple, $\lfloor -\pi \rfloor = -4$ et $\lfloor 2 \rfloor = \lfloor 2.9 \rfloor = 2$.)

Exercice 3.79. *(IMO SL 2011 N2)* Soient $d_1, \dots, d_9$ des entiers distincts et soit $P(x) = (x + d_1)(x + d_2) \cdot \dots \cdot (x + d_9)$. Montrer qu'il existe un entier $N \geqslant 1$ tel que pour tous les entiers $x \geqslant N$, le nombre $P(x)$ est divisible par un nombre premier plus grand que 20.

Exercice 3.80. *(OFM 2021 Senior)* Soient $a_1, a_2, \dots$ et $b_1, b_2, \dots$ deux suites satisfaisant respectivement, pour tout $n \geqslant 1$, $a_{n+2} = a_{n+1} + a_n$ et $b_{n+2} = b_{n+1} + b_n$. On suppose que a_n divise b_n pour une infinité d'indices n. Montrer qu'il existe un entier c tel que $a_n = cb_n$ pour tout entier $n \geqslant 1$.

Exercice 3.81. *(Iran 2024 round 3 P6)* Soit P un polynôme à coefficients entiers et positifs ou nuls. On suppose qu'il existe une suite (x_n) d'entiers strictement positifs telle que $x_1 = 1$ et, pour tout indice $n \geqslant 1$,

$$x_{n+1}^2 + P(n) = x_n x_{n+2}.$$

Montrer que P est un polynôme constant.

Exercice 3.82. *(Chine TST 2004 P2/France TST 2018-2019)* Soit u un entier strictement positif. Montrer qu'il n'existe qu'un nombre fini de triplets (n, α, β) d'entiers strictements positifs tels que $n! = u^\alpha - u^\beta$.

Exercice 3.83. *(ELMO 2017 N3)* Pour tout entier $C > 1$, déterminer s'il existe des entiers $a_1, a_2, \ldots$ deux à deux distincts tels que, pour tout indice $k \geqslant 1$, $a_{k+1}^k \mid C^k a_1 a_2 \ldots a_k$.

Exercice 3.84. *(USA 2022 TSTST P8)* Déterminer toutes les fonctions f allant de $\mathbb{N}^\star$ dans $\mathbb{Z}$ telles que, pour tout couple d'entiers strictement positifs (m, n) :

$$\left\lfloor \frac{f(mn)}{n} \right\rfloor = f(m)$$

On pourra admettre le théorème suivant : Soit (u_n) une suite telle que, pour tout $\varepsilon > 0$, il existe un rang N tel que

$$\text{pour tout } p, q \geqslant N, |u_p - u_q| < \varepsilon.$$

Alors la suite (u_n) converge.

Exercice 3.85. *(IMO SL 2021 N5)* Montrer que l'équation $n! = a^{n-1} + b^{n-1} + c^{n-1}$ admet un nombre fini de quadruplets solutions (a, b, c, n) d'entiers strictement positifs.

4 Exercices de style

4.1 L'arithmétique et les suites

Les problèmes d'arithmétique faisant intervenir les suites font partie des nouveaux jouets des créateurs de problèmes. Les arguments à savoir maîtriser sont variés, puisqu'ils combinent les réflexes d'hygiène en arithmétique (divisibilité, taille, étude des facteurs premiers) et les réflexes d'étude de suites (variations, comparaison d'un terme à l'autre, introduction de suites auxiliaires). Ces derniers réflexes sont en général un peu plus difficiles car moins enseignés en olympiades. Voici donc quelques conseils.

Parmi les astuces existantes sur les suites (pas forcément entières), on en retiendra principalement deux :

- ☞ Introduire des suites auxiliaires : la somme des n premiers termes de la suite, la somme des carrés des premiers termes de la suites, la différence entre deux termes consécutifs, la partie impaire... il est fréquent que, pour comprendre la suite présentée dans l'exercice, il faille plutôt étudier une autre suite cachée par l'exercice et rassemblant plus clairement les différentes hypothèses.
- ☞ Dans le cas où la suite est définie par une relation de récurrence, on peut comparer les relations de récurrence pour l'indice n et l'indice $n+1$ (soustraction/addition des deux relations, injection de l'une dans l'autre...). On peut également, dans le cas d'une suite périodique ou finie, considérer la somme des termes (ou la somme des carrés, ou le produit...), pour obtenir un effet moyennant (les termes « mauvais » de la suite ont alors moins d'importance). En résumé, il faut garder en tête l'idée d'essayer des raisonnements « locaux » (sur un terme et ses voisins) et des raisonnements « globaux » (sur l'ensemble des termes de la suite).

Dans la suite, en plus de développer ces astuces, on présente divers conseils sur les problèmes de suites d'entiers.

Variations d'une suite

Dans un problème de suite, notamment d'une suite infinie (u_n) définie récursivement, il est bon de commencer par déterminer quelques informations sur la suite (u_n). On cherchera notamment si la suite est bornée ou si elle est monotone. Il est fort possible que seule une sous-suite bien choisie possède cette propriété.

L'une des propriétés les plus importantes à garder à l'esprit dans ce cadre est la suivante :

Proposition 4.1. Soit (u_n) une suite d'entiers positifs qui est décroissante. Il existe un rang N et un entier c tels que, pour tout $n \geqslant N$, $u_n = c$.

Démonstration. Comme l'ensemble $\{u_n, n \in \mathbb{N}\}$ est un ensemble d'entiers positifs, il admet un plus petit élément c. Soit N un indice tel que $u_N = c$. Puisque la suite (u_n) est décroissante, pour tout entier $n \geqslant N$, on a $c \leqslant u_n \leqslant u_N = c$, donc $u_n = c$ comme annoncé.

Dans les exercices dont l'énoncé demande de prouver qu'une propriété est vraie à partir d'un certain rang, la clé est souvent d'appliquer cette propriété à une suite auxiliaire bien choisie, dont le caractère constant implique l'énoncé.

On en profite pour signaler que pour montrer qu'une suite est constante, on peut montrer qu'elle est constante à partir d'un certain rang et déduire qu'elle est constante en procédant par récurrence descendante.

Manipulations algébriques

Il s'agit d'une astuce inhérente aux problèmes de suites, et pas que les suites d'entiers, à savoir manipuler algébriquement la relation de récurrence qui est donnée. On peut chercher à factoriser, rééarranger, estimer un côté ou l'autre...

Une manipulation récurrente pour faire sortir des informations est de combiner l'expression pour un rang n et pour ses rangs voisins. Par exemple, si une relation est vraie pour tout n, il est intéressant d'étudier cette relation à l'indice n et à l'indice $n+1$. L'intérêt est de connecter plus de termes de la suite entre eux. Dans l'exemple suivant, ces manipulations sont très astucieuses mais nécessaires.

Exemple 22. *(Coupe Animath d'automne 2015)* Soit $a_1, a_2, \dots$ une suite d'entiers définie par $a_1 = 1, a_2 = 7$ et, pour tout $n \geqslant 1$,

$$a_{n+2} = \frac{a_{n+1}^2 - 1}{a_n}.$$

Montrer que $9a_n a_{n+1} + 1$ est le carré d'un entier pour tout indice $n \geqslant 1$.

Solution. On réécrit la relation de récurrence en supprimant les dénominateurs. Celle-ci devient $a_{n+2}a_n = a_{n+1}^2 - 1$. En combinant cette relation pour les indices n et $n+1$

$$\begin{cases} a_{n+2}a_n = a_{n+1}^2 - 1 \\ a_{n+3}a_{n+1} = a_{n+2}^2 - 1 \end{cases}$$

on trouve

$$a_{n+2}a_n - a_{n+3}a_{n+1} = a_{n+1}^2 - a_{n+2}^2.$$

Cette relation se réécrit

$$a_{n+2}(a_n + a_{n+2}) = a_{n+1}(a_{n+1} + a_{n+3})$$

ou encore

$$\frac{a_n + a_{n+2}}{a_{n+1}} = \frac{a_{n+1} + a_{n+3}}{a_{n+2}}.$$

Ainsi, la quantité $\dfrac{a_n + a_{n+2}}{a_{n+1}}$ est constante égale à $\dfrac{a_1 + a_3}{a_2} = \dfrac{1+48}{7} = 7$. En réinjectant l'égalité $a_{n+2} = 7a_{n+1} - a_n$ dans la relation initiale, on trouve $7a_{n+1}a_n - a_n^2 = a_{n+1}^2 - 1$, ce qui se réécrit $9a_n a_{n+1} + 1 = (a_n + a_{n+1})^2$, qui est bien un carré.

On pourra repratiquer ces conseils sur l'exercice suivant :

Exercice 4.1. (Baltic Way 2021 P3) Déterminer toutes les suites d'entiers strictement positifs $a_1, a_2, \dots$ telles que, pour tout $n \geqslant 1$,

$$a_{n+1}^2 = 1 + (n + 2021)a_n.$$

Le cas particulier des groupes de termes consécutifs

Dans le cas particulier où la relation porte sur un groupe de k termes consécutifs, appliquer l'énoncé aux indices n et $n+1$ permet souvent de connecter les nombres u_n et u_{n+k}. Par exemple, si l'énoncé dit que, pour tout entier n, $3 \mid u_n + u_{n+1} + u_{n+2}$, on déduit que $3 \mid (u_{n+1} + u_{n+2} + u_{n+3}) - (u_n + u_{n+1} + u_{n+2}) = u_{n+3} - u_n$. Cette nouvelle divisibilité possède moins de termes donc est plus facile à manipuler.

Dans l'ensemble si l'énoncé présente des propriétés vraie pour tout paramètre, on fait varier chacun des paramètres possibles. C'est ce qu'explore l'exemple suivant.

Exemple 23. *(USA TST 2014 P2)* Soit $a_1, a_2, \ldots$ une suite d'entiers vérifiant que pour tout entier k et tout indice n, la quantité

$$k(a_n + a_{n+1} + \ldots + a_{n+k-1})$$

est un carré parfait. Montrer que la suite est constante.

Solution. Dans cet exercice, il faut faire bouger n à k fixé et faire bouger k à n fixé.

Tout d'abord, l'énoncé appliqué à $k = 1$ indique que tous les a_n sont des carrés parfaits.

Soit p un nombre premier divisant au moins un terme de la suite. Nous allons montrer que p divise tous les termes de la suite. Puisque les termes sont des carrés, cela implique qu'ils sont tous divisibles par p^2. La suite (a_n/p^2) étant alors également solution du problème, on peut itérer le processus avec un nouveau nombre premier (éventuellement égal à p) divisant un terme de la suite (a_n/p^2). De proche en proche, on déduit que tous les termes de la suite admettent la même décomposition en facteurs premiers et sont donc égaux.

Ainsi, il suffit de montrer que $p \mid a_n$ pour tout entier n. On fixe désormais un indice i tel que $p \mid a_i$.

- On fixe k et on fait varier n : En appliquant la relation à $k = p$ et à n quelconque, on trouve que $p(a_n + \ldots + a_{n+p-1})$ est un carré divisible par p et donc par p^2 pour tout n. On a donc, en comparant cette divisibilité à l'indice n et à l'indice $n+1$, que $p \mid a_n + \ldots + a_{n+p-1}$ et $p \mid a_{n+1} + \ldots + a_{n+p}$ ce qui implique par différence que $p \mid a_{n+p} - a_n$, soit $\boxed{a_{n+p} \equiv a_n \mod p}$ pour tout indice n.
- On fixe n et on fait varier k : Soit k un nombre premier avec p. En appliquant l'énoncé à k et i, on trouve que $k(a_i + \ldots + a_{i+k-1})$ est un carré, et puisque $a_i \equiv 0 \mod p$, le nombre $k(a_{i+1} + \ldots + a_{i+k-1})$ est un carré modulo p. Or, en appliquant l'énoncé à $k-1$ et $i+1$, le nombre $(k-1)(a_{i+1} + \ldots a_{i+k-1})$ est aussi un carré modulo p. Il vient que si $a_{i+1} + \ldots + a_{i+k-1} \neq 0 \mod p$, les nombres k et $k-1$ sont tous les deux des carrés ou des non-carrés modulo p.

  Autrement dit, en appliquant nos résultats précédents au plus petit entier k_0 qui soit un non-carré modulo p, on déduit que $\boxed{a_{i+1} + \ldots + a_{i+k_0-1} \equiv 0 \mod p}$.

  En appliquant l'énoncé à k_0 et à $i+1$, on trouve que le nombre $k_0(a_{i+1} + \ldots + a_{i+k_0})$ est un carré modulo p. Or celui-ci est congru à $k_0 a_{i+k_0}$ modulo p. Si $a_{i+k_0} \neq 0 \mod p$, comme c'est un carré et k_0 un non-carré, on a une contradiction. Ainsi, $\boxed{p \mid a_{i+k_0}}$.

En résumé, on a obtenu que si $p \mid a_i$, alors $p \mid a_{i+k_0}$ et $p \mid a_{i+p}$. En itérant, on trouve que $p \mid a_{i+k_0 u}$ pour tout entier $u \geqslant 0$. En choisissant u l'inverse de k_0 modulo p, on dispose d'un entier $v \geqslant 0$ tel que $uk_0 = pv + 1$. On déduit que $p \mid a_{i+k_0 u} = a_{i+1+pv}$. en utilisant que $a_n \equiv a_{n+p} \mod p$ pour tout entier n, on déduit après itération que $a_{i+1} \equiv a_{i+1+pv} \equiv 0 \mod p$, donc $p \mid a_{i+1}$. De proche en proche, p divise tous les termes de la forme a_{i+n} avec $n \geqslant 0$. En utilisant que $a_{n-p} \equiv a_n \mod p$ pour tout indice $n \geqslant p+1$, on trouve que p divise tous les termes de la suite, ce qui conclut.

On pourra travailler ce réflexe avec les exercices suivants :

Exercice 4.2. (OFM 2025) Déterminer toutes les suites bornées d'entiers strictement positifs $(a_1, a_2, \ldots)$ vérifiant que, pour tout nombre premier p et tout indice $n \geqslant 1$, le nombre

$$a_n a_{n+1} \ldots a_{n+p-1} - a_{n+p}$$

est un multiple de p.

Exercice 4.3. (IMO SL 2024 N3) Déterminer toutes les suites infinies $a_1, a_2, \ldots$ d'entiers strictement positifs telles que, pour toute paire (m, n) d'entiers strictement positifs pour laquelle $m \leqslant n$, les nombres

$$\frac{a_m + a_{m+1} + \ldots + a_n}{n - m + 1} \quad \text{et} \quad (a_m a_{m+1} \ldots a_n)^{\frac{1}{n-m+1}}$$

sont tous les deux entiers.

Suites auxiliaires

Il est fréquent qu'il faille introduire une autre suite dépendant de la suite (u_n) d'étude, et que les hypothèses du problème et l'énoncé à démontrer s'expriment mieux sur cette suite auxiliaire. Il y a beaucoup de candidats possibles pour une bonne suite auxiliaire possible. Voici quelques exemples et indications pour trouver les plus pertinentes :

- Il y a les exemples classiques : la somme/le produit des n premiers termes, la différence de deux termes consécutifs (pour étudier la monotonie de la suite par exemple)... La pratique de nombreux exercices permet de consistituer sa propre banque.

Exemple 24. *(EGMO 2015 P4)* Déterminer s'il existe une suite infinie d'entiers strictement positifs $a_0, a_1, \ldots$ telle que pour tout entier $n \geqslant 0$:

$$a_{n+2} = a_{n+1} + \sqrt{a_n + a_{n+1}}.$$

Solution.
On introduit la suite auxiliaire (b_n) définie par $b_n = \sqrt{a_n + a_{n+1}}$ pour tout indice $n \geqslant 1$. Notons que, puisque $b_n = a_{n+2} - a_{n+1}$, b_n est entier pour tout indice $n \geqslant 1$. La suite (a_n) étant visiblement strictement croissante, il en est de même pour la suite (b_n). On vérifie que

$$b_{n+1}^2 = a_{n+1} + a_{n+2} = a_n + b_{n-1} + a_{n+1} + b_n = b_n^2 + b_{n-1} + b_n.$$

Cette égalité implique notamment que

$$b_{n-1}+b_n = b_{n+1}^2 - b_n^2 = (b_n+b_{n+1})\underbrace{(b_{n+1}-b_n)}_{\geqslant 1} \geqslant b_n + b_{n+1},$$

ce qui est absurde puisque la suite $(b_n + b_{n+1})_n$ est strictement croissante d'après la stricte croissance de (b_n).

Remarque : Cet exercice a été donné en dernier exercice de la coupe Animath d'automne 2019. Plusieurs élèves ont alors remarqué dans leur solution qu'en réalité, le nombre a_5 ne peut pas être entier. Cela vient de l'égalité $b_3^2 = b_2^2 + b_2 + b_1$, qui implique par croissance de la suite (b_n) que $b_2^2 < b_3^2 < (b_2+1)^2$, ce qui est impossible si b_3 est un entier.

- Dans le cadre d'une relation de récurrence faisant intervenir tous les termes précédents de la suite, par exemple $a_n = a_0 + a_1 + \ldots + a_{n-1}$, une bonne suite intermédiaire doit permettre de réécrire la relation en une relation faisant intervenir un nombre plus retreint de termes : dans l'exemple précédent, introduire $S_n = a_0 + \ldots + a_{n-1}$ permet de réécrire la relation comme $S_{n+1} = 2S_n$, de laquelle on récupère facilement l'expression explicite de S_n puis de a_n. La suite auxiliaire doit simplifier la relation.
- C'est un très bon signe si on peut réécrire l'intégralité des hypothèses et l'énoncé à démontrer uniquement en fonction des termes de la suite auxiliaire. De la même manière, il vaut mieux éviter de mélanger la suite de départ et la suite auxiliaire. Prenons l'exemple où l'on introduit $S_n = a_0 + \ldots + a_n$. Si on réécrit l'expression de l'énoncé en fonction de S_n, a_n et S_{n-1}, l'expression obtenue ne pourra pas à elle seule décrire le système de l'énoncé, puisqu'elle fait intervenir des variables liées par une autre relation (à savoir $S_n = a_n + S_{n-1}$).
- On peut chercher des suites auxiliaires de nature plus arithmétique : la suite $(v_p(a_n))$, la suite « partie impaire de a_n », la suite « quotient de a_n par b_n » sont des exemples de suites auxiliaires pertinentes, dont les variations sont peut-être tout à fait explicites, choses qui n'est pas évidente avec la seule expression de a_n.

Exemple 25. *(All Russia 2018)* Soit $a_1, a_2, \ldots$ une suite infinie d'entiers et $p_1, p_2, \ldots$ une suite de nombres premiers distincts telle que $p_n \mid a_n$ pour tout indice $n \geqslant 1$. On suppose que pour toute paire (n,k) d'indices, $a_n - a_k = p_n - p_k$. Montrer que la suite (a_n) est constituée exclusivement de nombres premiers.

Solution. Notons b_n l'entier tel que $a_n = p_n b_n$. On a donc

$$p_n - p_k = b_n p_n - b_k p_k,$$

ce qui se réécrit

$$p_k(b_k - 1) = p_n(b_n - 1)$$

pour tous indices k et n. On fixe à présent un indice n. Pour tout $k \neq n$, $p_k \neq p_n$ donc $p_k \mid b_n - 1$ (car les p_k sont deux à deux distincts). On déduit que $b_n - 1$ est divisible par une infinité de nombres premiers, ce qui implique que $b_n = 1$. On a donc $a_n = p_n$, ce qui implique le résultat voulu.

On pourra repratiquer ces idées dans l'exercice suivant :

Exercice 4.4. (Balkan MO 2019 SL A1) Soit a_0 un entier strictement positif. Soit (a_n) une suite dans laquelle $a_0 \geqslant 1$ est un entier et, pour tout $n \geqslant 1$, a_n est le plus petit entier strictement positif pour lequel $a_0 + a_1 + \ldots + a_n$ est divisible par n. Montrer qu'il existe un rang M tel que $a_n = a_{n+1}$ pour tout $n \geqslant M$.

Les systèmes à multi-choix

Certains problèmes de suites définissent la suite (u_n) de la façon suivante :

$$u_n = \begin{cases} a_n & \text{si condition } A \\ b_n & \text{si condition } B \end{cases}$$

où on a gardé une forme très générale pour l'énoncé. Les conditions A et B peuvent porter sur n, sur u_{n-1}, sur une autre suite, tandis que les suites (a_n) et (b_n) peuvent être explicites ou des fonctions de u_{n-1}.
Donnons un exemple concret d'un tel système, et commentons le avant de passer à sa résolution :

Exemple 26. *(APMO 2019 P2)* Soit m un entier strictement positif. On définit la suite (a_n) de la façon suivante : a_1 est un entier strictement positif et, pour tout indice $n \geqslant 1$,

$$a_{n+1} = \begin{cases} a_n^2 + 2^m & \text{si } a_n < 2^m \\ a_n/2 & \text{si } a_n \geqslant 2^m \end{cases}$$

Déterminer, en fonction de m, les valeurs de a_1 telles que la suite (a_n) ne contient que des entiers.

En général, le fait d'avoir plusieurs conditions possibles empêche la suite d'être monotone : l'une des deux conditions fait augmenter la suite, l'autre la fait diminuer. Les conseils pour approcher de tels problèmes sont les suivants :

- Chercher des variants et monovariants. En général, le système cache la monotonie d'une suite auxiliaire, ou d'une sous-suite de la suite considérée.
- S'intéresser à des blocs d'indices consécutifs pour lesquels la condition A (resp B) est remplie. En général, la suite du système ne peut pas passer trop de fois d'affilée par l'état A (resp B), à cause de la monotonie imposée par exemple. Arriver à quantifier ces affirmations, par exemple en prouvant que la suite ne peut pas passer k fois d'affilée par l'état A, avec k fixé, est l'une des clés du problème.

Solution. **Réponse :** Une telle valeur existe uniquement pour $m = 2$ et dans ce cas, les valeurs a_1 solutions sont $a_1 = 2^\alpha$ avec $\alpha \geqslant 1$.

On peut commencer par remarquer que, la suite ne peut pas contenir de terme impair. Par l'absurde prenons un terme a_n impair. Si $a_n > 2^m$, alors $a_{n+1} = a_n/2$ n'est pas entier. Si $a_n < 2^m$, alors a_{n+1} est impair et supérieur à 2^m, donc a_{n+2} n'est pas entier.

Ensuite, la valuation $2-$adique joue un rôle dans les opérations, donc elle va jouer un rôle dans le problème. On introduit donc les entiers α_n et β_n tels que $a_n = 2^{\alpha_n}\beta_n$. Les suites (α_n) et (β_n) sont alors des suites que l'on peut étudier. On peut notamment s'intéresser à la monotonie de (β_n).
Ce faisant, on constate que la suite (β_n) est croissante sauf dans le cas particulier $m = 2$, que l'on laisse pour la fin.

Soit $m \neq 2$ un entier quelconque et a_1 une valeur solution. Montrons que si $m \neq 2$, alors la suite (β_n) est croissante avec une sous-suite strictement croissante.

Prenons pour cela un indice n quelconque. Si $a_n > 2^m$, alors $a_{n+1} = a_n/2$ donc $\beta_{n+1} = \beta_n$. Supposons désormais que $a_n < 2^m$.

On a $a_{n+1} = a_n^2 + 2^m = 2^{2\alpha_n}\beta_n^2 + 2^m$. Pour identifier β_{n+1}, il faut alors distinguer trois cas :

- Si $2\alpha_n > m$, alors $a_{n+1} = 2^m(2^{2\alpha_n - m}\beta_n^2 + 1)$, donc $\beta_{n+1} = 2^{2\alpha_n - m}\beta_n^2 + 1 > \beta_n$.
- Si $2\alpha_n < m$, alors $a_{n+1} = 2^{2\alpha_n}(\beta_n^2 + 2^{m-2\alpha_n})$, donc $\beta_{n+1} = \beta_n^2 + 2^{m-2\alpha_n} > \beta_n$.
- Si $2\alpha_n = m$, alors $a_{n+1} = 2^m(\beta_n^2 + 1)$. Comme $\beta_n^2 + 1 \equiv 2 \mod 4$, on trouve $\beta_{n+1} = \dfrac{\beta_n^2 + 1}{2}$. D'après l'inégalité des moyennes, on a $\beta_{n+1} \geqslant \beta_n$, avec égalité seulement si $\beta_n = 1$. Mais dans ce cas, on a $a_{n+1} = 2^{m+1}$, $a_{n+2} = 2^m$ et $a_{n+3} = 2^{m-1}$. Si $m = 1$, alors la suite contient un terme impair, ce qui est exclu par la remarque plus haut. Sinon, $a_{n+4} = 2^m(2^{m-2} + 1)$. Comme $m \neq 2$, on trouve que $\beta_{n+4} > \beta_{n+3} = \ldots = \beta = 1$.

Dans tous les cas, on trouve que $\boxed{\text{la suite } (\beta_n) \text{ est croissante}}$ et admet une sous-suite strictement croissante. En particulier, lorsque n est assez grand, $a_n > \beta_n > 2^m$, donc la suite (a_n) ne fait ensuite que décroître strictement, ce qui est impossible. Plus précisément, d'après ce qu'on a montré plus haut, il existe un indice n tel que $\beta_n > 2^{m-1}$. Mais alors $a_n = 2^{\alpha_n}\beta_n \geqslant 2\beta_n > 2^m$. Il vient que pour tout $\ell \leqslant \alpha_n - 1$, $a_{n+\ell} = 2^{\alpha_n - \ell}\beta_n \geqslant 2\beta_n > 2^m$. Finalement, $a_{n+\alpha_n} = \beta_n$, ce qui est absurde car ce terme est impair. $\boxed{\text{Il n'y a donc pas de valeur } a_1 \text{ possible pour } m \neq 2}$.

Supposons maintenant que $m = 2$. Posons $a_1 = 2^\alpha\beta$. Si $\beta \geqslant 2$, de même que précédemment, on trouve $a_{1+\alpha} = \beta$ est impair, ce qui est exclu. Donc $\beta = 1$. Réciproquement, si $a_1 = 2^\alpha$, alors on vérifie que $a_{1+\ell} = 2^{\alpha-\ell}$ pour tout $\ell \leqslant \alpha - 1$, puis une récurrence sur k donne que $(a_{3k+\alpha}, a_{3k+\alpha+1}, a_{3k+\alpha+2}) = (2, 8, 4)$, donc la suite (a_n) ne prend que des valeurs entières et le nombre a_1 est bien solution du problème.

On pourra appliquer ces conseils pour résoudre l'exercice suivant :

Exercice 4.5. *(Taiwan IMOC 2021 N3)* Pour tout entier $x \geqslant 2$, on note $f(x)$ son plus grand facteur premier. Soient M et k des entiers strictement positifs. Une suite (a_n) d'entiers strictement positifs est définie par $a_1 = M > 1$ et

$$a_{n+1} = \begin{cases} a_n - f(a_n) & \text{si } a_n \text{ est composé} \\ a_n + k & \text{sinon} \end{cases}$$

Montrer que la suite (a_n) est bornée.

Derniers conseils

L'ensemble des conseils donnés ci-dessus ne représente qu'une petite partie des astuces applicables face aux problèmes de suite, et est loin de couvrir tous les types d'exercices, tant la variété des problèmes est grande. La meilleure façon de progresser est encore de se confronter le plus possible à des problèmes de suites pour y développer son style.

Les gestes les plus naturels restent bien sûr de tester des petits cas et des cas particuliers, calculer les premières valeurs de la suite et faire des conjectures. Les conseils donnés ci-dessus sont alors des outils pour prouver ces conjectures.

Exercices

Exercice 4.6. (BXMO 2012) Soit $a_1, a_2, \ldots$ une suite d'entiers positifs telle que, pour tout indice $n \geqslant 1$,

$$a_{n+1} = a_n + b_n,$$

où b_n est le dernier chiffre de a_n. Montrer que la suite (a_n) contient une infinité de puissances de 2 si et seulement si a_1 n'est pas divisible par 5.

Exercice 4.7. (St Petersbourg 2017) Soit (a_n) une suite d'entiers définie par $a_1 > 10$ et, pour tout entier $n \geqslant 2$,

$$a_n = a_{n-1} + \mathrm{PGCD}(n, a_{n-1}),$$

On suppose qu'il existe un indice k tel que $a_k = 2k$. Montrer qu'il existe une infinité d'indices k tels que $a_k = 2k$.

Exercice 4.8. (PAMO 2021 P3) Soit (a_n) une suite d'entiers définie par $a_1 \geqslant 2$ et, pour tout entier $n \geqslant 1$, $a_{n+1} = a_n + a_n/p_n$, où p_n est le plus petit diviseur premier de a_n.
Montrer qu'il existe un entier $N \geqslant 1$ tel que $a_{n+3} = 3a_n$ pour tout $n > N$.

Exercice 4.9. (Belarus Iran 2022) Pour tout entier $n \geqslant 1$, on note $d(n)$ est le nombre de diviseurs positifs de n. Existe-t-il une suite $a_1, a_2, \ldots$ d'entiers strictement positifs telle que pour tous indices i et j,

$$d(a_i + a_j) = i + j\,?$$

Exercice 4.10. (Dutch BXMO TST 2019) Existe-t-il un entier $k \geqslant 1$ et une suite non constante $a_1, a_2, \ldots$ telle que $a_n = \mathrm{PGCD}(a_{n+k}, a_{n+k+1})$ pour tout indice $n \geqslant 1$?

Exercice 4.11. (Iran 2017 Round 2)

1. Montrer qu'il n'existe pas de suites $a_1, a_2, \ldots$ d'entiers strictement positifs telles que pour toute pair (i, j) d'indices distincts, $\mathrm{PGCD}(a_i + j, a_j + i) = 1$.
2. Soit p un nombre premier impair. Montrer qu'il existe une suite $a_1, a_2, \ldots$ d'entiers strictement positifs telle que pour toute pair (i, j) d'indices distincts, $\mathrm{PGCD}(a_i + j, a_j + i)$ n'est pas divisible par p.

Exercice 4.12. (IMO 2017 P1) Pour tout entier $a_0 > 1$, on définit la suite $a_0, a_1, \ldots$ par

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{si } a_n \text{ est un carré parfait} \\ a_n + 3 & \text{sinon} \end{cases}$$

Déterminer toutes les valeurs de a_0 pour lesquelles il existe un nombre A tel que $a_n = A$ pour une infinité de valeurs de n.

Exercice 4.13. (ELMO 2019 P1) Soit P un polynôme à coefficients entiers tel que $P(0) = 1$ et soit $c > 1$ un entier. On définit la suite (x_n) par $x_0 = 0$ et $x_{n+1} = P(x_n)$ pour tout $n \geqslant 0$. Montrer qu'il existe une infinité d'entiers n tels que $\mathrm{PGCD}(x_n, n + c) = 1$.

Exercice 4.14. (Balkan MO SL 2021 N2) Pour tout $n > 1$, on note $\ell(n)$ le plus grand facteur premier de n. Soit (a_n) la suite définie par $a_1 = 2$ et $a_{n+1} = a_n + \ell(a_n)$ pour tout $n \geqslant 1$. Déterminer tous les entiers k tels qu'il existe au moins un indice n pour lequel $a_n = k^2$.

Exercice 4.15. (IMO SL 2008 N3) Soit $a_0, a_1, \ldots$ une suite d'entiers strictement positifs telle que $\mathrm{PGCD}(a_{i+1}, a_i) > a_{i-1}$ pour tout indice $i \geqslant 1$. Montrer que, pour tout entier $n \geqslant 0$, $a_n \geqslant 2^n$.

Exercice 4.16. (IMO SL 2015 N4) Soient $a_0, a_1, \ldots$ et $b_0, b_1, \ldots$ des suites d'entiers strictement positifs vérifiant $a_0, b_0 \geqslant 2$ et, pour tout entier $n \geqslant 0$,

$$a_{n+1} = \mathrm{PGCD}(a_n, b_n) + 1, \quad b_{n+1} = \mathrm{PPCM}(a_n, b_n) - 1.$$

Montrer qu'il existe un entier N et un entier t tels que, pour tout $n \geqslant N$, $a_{n+t} = a_n$.

Exercice 4.17. (Chine TST 2016) Soit $c, d \geqslant 2$ des entiers naturels. Soit (a_n) la suite définie par $a_1 = c$ et $a_{n+1} = a_n^d + c$. Montrer que pour tout $n \geqslant 2$, il existe un nombre premier p tel que $p \mid a_n$ et p ne divise aucun des a_i pour $i = 1, \ldots, n-1$.

Exercice 4.18. (IMO 2018 P5) Soit $a_1, a_2, \ldots$ une suite infinie d'entiers strictement positifs. On suppose qu'il existe un entier $N > 1$ tel que, pour tout entier $n \geqslant N$, le nombre

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \ldots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$$

est un entier. Montrer qu'il existe un entier M tel que $a_m = a_{m+1}$ pour tout entier $m \geqslant M$.

Exercice 4.19. (ELMO 2018 P2) Soit $a_1, a_2, \ldots$ une suite d'entiers strictement positifs telle que $a_1 = 1$ et, pour tous entiers $k, n \geqslant 1$,

$$a_n \mid a_k + a_{k+1} + \ldots + a_{n+k-1}.$$

Soit $m \geqslant 1$ un entier. Déterminer la plus grande valeur que peut prendre a_{2m}.

Exercice 4.20. (IMO 2005 P2) Soit $a_1, a_2, \ldots$ une suite d'entiers contenant une infinité de termes positifs et une infinité de termes négatifs. On suppose que pour tout entier $n \geqslant 1$, les nombres $a_1, \ldots, a_n$ donnent n restes distincts modulo n.
Montrer que chaque entier apparaît exactement une fois dans la suite.

Exercice 4.21. (France TST 2020-2021 P2) On dit qu'une suite $(u_n)_{n \geqslant 0}$ d'entiers naturels non nuls est *sicilienne* si

$$u_{n+1} \in \{u_n/2, u_n/3, 2u_n + 1, 3u_n + 1\}$$

pour tout $n \geqslant 0$. Démontrer que, pour tout entier $k \geqslant 1$, il existe une suite sicilienne $(u_n)_{n \geqslant 0}$ et un entier $\ell \geqslant 0$ tels que $u_0 = k$ et $u_\ell = 1$.

Exercice 4.22. (EGMO 2022 P3) Une suite infinie d'entiers strictement positifs $a_1, a_2, \ldots$ est dite *bonne* si

(1) a_1 est un carré parfait,

(2) pour tout entier $n \geqslant 2$, a_n est le plus petit entier strictement positif tel que

$$na_1 + (n-1)a_2 + \ldots + 2a_{n-1} + a_n$$

est un carré parfait.

Montrer que pour tout suite bonne $a_1, a_2, \ldots$, il existe un entier k tel que $a_n = a_k$ pour tout entier $n \geqslant k$.

Exercice 4.23. *(IMO SL 2023 N5)* Soit $a_1, a_2, a_3, \ldots$ une suite d'entiers strictement positifs, strictement croissante, telle que a_{k+1} divise $2(a_1 + a_2 + \cdots + a_k)$ pour tout entier $k \geqslant 1$. On suppose qu'il existe une infinité de nombres premiers p qui divisent au moins un terme parmi $a_1, a_2, a_3, \ldots$. Montrer que tout entier $n \geqslant 1$ divise au moins un terme parmi $a_1, a_2, a_3, \ldots$

Exercice 4.24. *(IMO SL 2025 N5)* La suite de triplets d'entiers strictement positifs (a_0, b_0, c_0), (a_1, b_1, c_1),..., $(a_{2025}, b_{2025}, c_{2025})$ vérifie

$$(a_{i+1}, b_{i+1}, c_{i+1}) = (a_i + \mathrm{PGCD}(b_i, c_i), b_i + \mathrm{PGCD}(c_i, a_i), c_i + \mathrm{PGCD}(a_i, b_i))$$

pour tout indice $0 \leqslant i \leqslant 2024$.

Déterminer la plus petite valeur que peut prendre a_{2025}.

Exercice 4.25. *(IMO SL 2021 N7)* Soit $(a_n)_{n \geqslant 1}$ une suite d'entiers naturels non nuls telle que a_{n+2m} divise $a_n + a_{n+m}$ pour tous les entiers $m \geqslant 1$ et $n \geqslant 1$. Démontrer que cette suite est ultimement périodique, c'est-à-dire qu'il existe deux entiers $N \geqslant 1$ et $d \geqslant 1$ tels que $a_n = a_{n+d}$ pour tout $n \geqslant N$.

4.2 Équations fonctionnelles en arithmétique

Les équations fonctionnelles en théorie des nombres rassemblent le meilleur des deux mondes : les raisonnements arithmétiques (divisibilité, étude des nombres premiers) sont utilisés pour enrichir les astuces de substitutions et d'étude de fonction propres aux équations fonctionnelles.

Le thème concerne en général des exercices assez difficiles et est assez rare dans les niveaux plus faciles des Olympiades. Le contexte est celui de l'étude d'une fonction $f : \mathbb{N}^\star \to \mathbb{N}^\star$ (parfois aussi de $\mathbb{Z}$ dans $\mathbb{N}^\star$). La fonction f peut vérifier plusieurs types de relations, les plus courantes étant :

- ☞ Une relation de divisbilité du type $A(n,m) \mid B(n,m)$ (par exemple $m^2+f(n) \mid mf(m)+n$).
- ☞ Une relation impliquant les fonctions PGCD ou PPCM (ce qui induit des relations de divisbilité).
- ☞ Une relation du type « $A(n,m)$ est un carré parfait ».

Une certaine forme de gymnastique permet d'envisager une large classe de ces équations fonctionnelles. Pour orienter la recherche, il est bon d'avoir une idée des résultats partiels auxquels on peut s'attendre pour une telle équation. En général, on peut chercher pour des inégalités entre $f(n)$ et n provenant d'hypothèses de divisibilité (il s'agit alors d'obtenir l'inégalité inverse) et/ou des valeurs spécifiques de f (notamment les valeurs de $f(p)$ ou de $f(p\pm 1)$ pour p premier) permettant de connaître f sur une large classe d'entiers. On détaille ci-après quelques astuces. Je remercie Thomas Budzinski pour son excellent cours sur le sujet, donné au groupe D lors du stage d'été 2022, dont les conseils, les exercices et les solutions sont un modèle d'efficacité et de concision, et dont le contenu a beaucoup enrichi les éléments qui suivent.

Substitutions de base :

Les substitutions $n = 1$ et $n = m$ sont toujours les bienvenues. Elles permettent de déterminer des petites valeurs de f ou des inégalités sur f. Dans le cas fréquent d'un énoncé du type « trouver les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que $A(n,m) \mid B(n,m)$ », il faut joindre à ces substitutions les gestes classiques devant une divisibilité :

- ➢ Chercher la meilleure combinaison linéaire entre $A(n,m)$ et $B(n,m)$ que peut diviser $A(n,m)$, pour simplifier un maximum de termes. Cette combinaison linéaire se trouve naturellement en traduisant la divisibilité comme $0 \equiv B(n,m) \mod A(n,m)$ et en utilisant que $A(n,m) \equiv 0$ pour simplifier $B(n,m)$.
- ➢ Chercher une substitution (n,m) telle que $A(n,m)$ est divisible par un entier bien choisi, divisant par conséquent $B(n,m)$. Autrement dit, au lieu de simplifier $A(n,m)$ ou $B(n,m)$, on cherche un diviseur simple de $A(n,m)$.

Exemple 27. Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tout $x, y \in \mathbb{N}^\star$,

$$f(y) + 2x \mid 2f(x) + y.$$

Solution. **Réponse :** $f(n) = n$ pour tout entier n.

En posant $x = y = 1$ dans la divisibilité, on trouve $f(1) + 2 \mid 2f(1) + 1$. Comme $f(1) \equiv -2 \mod f(1) + 2$, on déduit que

$$0 \equiv 2f(1) + 1 \equiv 2(-2) + 1 = -3 \mod 2f(1) + 1.$$

Comme $2f(1)+1 \geqslant 3$ et que ce nombre divise 3, on déduit que $2f(1)+1=3$, soit $\boxed{f(1)=1}$.

En posant $x=1$ dans la divisibilité, on trouve que pour tout entier y, $f(y)+2 \mid 2+y$, soit $\boxed{f(y) \leqslant y}$.

En posant $y=1$ dans la divisbilité, on trouve que $2x+1 \mid 2f(x)+1$, soit $\boxed{f(x) \geqslant x}$.

La combinaison de ces deux inégalités conduit à $\boxed{f(n)=n}$ pour tout entier n.

Réciproquement, la fonction identité est bien solution.

Pour pratiquer, on pourra directement réappliquer cette méthode pour l'exercice suivant :

Exercice 4.26. (IMO SL 2013 N1) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$m^2 + f(n) \mid mf(m) + n$$

pour tous $n, m \in \mathbb{N}^\star$.

Détermination de $f(a)$ pour une infinité d'entiers a :

Lorsque le problème est sous forme de relation de divisbilité (c'est également le cas lorsque le problème fait intervenir PGCD et PPCM), on peut raisonnablement chercher des valeurs spécifiques de f pour une large classe d'entiers avant de passer au cas général. Le plus fréquent est de parvenir à déterminer $f(p)$ ou $f(p \pm 1)$ pour p premier. Ces valeurs interviennent naturellement en cherchant à simplifier la relation de divisbilité :

- ➢ Rendre $B(n,m)$ ou $A(n,m)$ premier : Dans le cas d'une relation de la forme $A(n,m) \mid B(n,m)$, on peut chercher une substitution (n,m) telle que $B(n,m)$ soit premier ou une puissance d'un nombre premier. Il a alors peu de diviseurs, donc $A(n,m)$ peut prendre peu de valeurs possibles. De même, on peut chercher une substitution (m,n) pour laquelle $A(n,m)$ est premier ou divisible par un nombre premier spécifique.
- ➢ Simplifier $\mathrm{PGCD}(C(n,m), D(n,m))$: on peut chercher une substitution (n,m) pour laquelle $C(n,m)$ ou $D(n,m)$ est premier, vaut 1 ou pour laquelle l'un des nombres $C(n,m)$ ou $D(n,m)$ divise l'autre, afin de simplifier le terme $\mathrm{PGCD}(C(n,m), D(n,m))$.

Exemple 28. *(OFM 2021 Junior)* Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que pour tous entiers $a, b \geqslant 1$,

$$\mathrm{PGCD}(f(m), n) + \mathrm{PPCM}(m, f(n)) = \mathrm{PGCD}(m, f(n)) + \mathrm{PPCM}(f(m), n).$$

Solution. **Réponse :** La seule solution est l'identité.

En posant $m = f(n)$ dans l'équation de départ, on trouve que

$$\mathrm{PGCD}(f(f(n)), n) = \mathrm{PPCM}(n, f(f(n)))$$

ce qui implique $\boxed{f(f(n)) = n}$.

En posant $m = 1$ dans l'équation, on trouve

$$\mathrm{PGCD}(f(1), n) + f(n) = 1 + \mathrm{PPCM}(n, f(1)). \tag{1}$$

Soit p un nombre premier. En remplaçant $n = p$ dans cette équation, on trouve

$$\mathrm{PGCD}(f(1), p) + f(p) = 1 + \mathrm{PPCM}(p, f(1)).$$

Les termes sont plus simples si on rajoute la condition que p est premier avec $f(1)$. Dans ce cas, cette égalité devient

$$1 + f(p) = 1 + pf(1)$$

ce qui permet d'obtenir $\boxed{f(p) = pf(1)}$.

Pour p premier avec $f(1)$, on peut donc poser $n = pf(1)$ dans l'équation (1) pour trouver

$$1 + pf(1) = f(1) + f(pf(1)) = f(1) + f(f(p)) = f(1) + p.$$

On déduit que $(f(1) - 1)(p - 1) = 0$. Comme $p \neq 1$, on déduit que $\boxed{f(1) = 1}$.

En revenant à l'équation (1), on déduit que $1 + f(n) = 1 + n$, soit $\boxed{f(n) = n \text{ pour tout } n}$.

Réciproquement, la fonction identité est bien solution du problème.

Montrer que $f(n) - n$ admet une infinité de diviseurs :

Une fois que l'on a obtenu la valeur de f pour une infinité de valeurs, on essaye de transformer la divisibilité en une relation de la forme $A \mid f(a) - a$ avec a fixé et le nombre A qui peut prendre une infinité de valeurs, ce qui implique que $f(a) - a$ est nul. Un exemple vaut mieux qu'un beau discours.

Exemple 29. *(APMO 2019 P1)* Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$f(a) + b \mid a^2 + f(a)f(b)$$

pour tous $a, b \in \mathbb{N}^\star$.

Solution. On effectue les substitutions classiques puis on manipule la relation de divisbilité. Chaque action apporte une information supplémentaire. Il n'y a plus qu'à les combiner pour obtenir $f(p) = p$ lorsque p est premier, et conclure.

On commence par les substitutions habituelles : si $a = b = 1$, $1 + f(1) \mid 1 + f(1)^2$, donc $0 \equiv 1 + f(1)^2 \equiv 1 + (-1)^2 \equiv 2 \mod 1 + f(1)$, ce qui conduit à $\boxed{f(1) = 1}$.

Si $a = 1$, alors $1 + b \mid 1 + f(b)$ donc $\boxed{b \leqslant f(b)}$.

Si $a = b = p$ est un nombre premier impair, alors on a, en regardant modulo $f(p) + p$,

$$0 \equiv p^2 + f(p)^2 \equiv p^2 + (-p)^2 \equiv 2p^2 \mod p + f(p).$$

On déduit que $p + f(p)$ est un diviseur de $2p^2$. Comme en plus $2p \leqslant p + f(p)$, on a $f(p) \in \{2p, p^2, 2p^2\}$. En particulier, $p \mid f(p)$.

Si $a = p$ et $b = 1$, on trouve que $f(p) + 1 \mid p^2 + f(p)$. Comme $p \mid p^2 + f(p)$ et que p est premier avec $f(p) + 1$, on déduit que $p(f(p) + 1) \mid p^2 + f(p)$, soit $pf(p) + p \leqslant p^2 + f(p)$, ce qui se

simplifie en $f(p) \leqslant p$. Ainsi, $\boxed{f(p) = p \text{ pour tout nombre premier } p \text{ impair}}$.

Une fois qu'on a trouvé la valeur de f pour une infinité de valeurs p, le protocole est toujours le même : on fixe n quelconque, et on s'arrange pour que le RHS dépende de p et le LHS dépende de $f(n) - n$, pour que ce nombre admette une infinité de diviseurs et soit nul.

Ici, on pose $a = p$ et $b = n$. La relation implique que

$$0 \equiv p^2 + pf(n) \equiv (-n)^2 + (-n)f(n) \equiv n(n - f(n)) \mod n + p.$$

Ainsi, le nombre $n(n - f(n))$ admet une infinité de diviseurs, il est donc nul et $\boxed{f(n) = n \text{ pour tout } n}$.

Réciproquement, la fonction identité est bien solution du problème.

On pourra chercher à réappliquer ce principe dans l'exercice suivant :

Exercice 4.27. (TST Suisse 2017, P1) Trouver toutes les fonctions : $f\mathbb{Z} \to \mathbb{Z}$ telles que $f(p) > 0$ pour tout nombre premier p et, pour tout entier x et pour tout nombre premier p,

$$p \mid (f(x) + f(p))^{f(p)} - x.$$

Exercice 4.28. (IMO SL 2004 N3) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$(f(m)^2 + f(n)) \mid (m^2 + n)^2$$

pour tous $n, m \in \mathbb{N}^\star$.

Chercher les diviseurs premiers de $f(n+1) - f(n)$

Une stratégie se calquant sur plusieurs problèmes où f est linéaire est d'étudier les diviseurs premiers de $f(n+1) - f(n)$. Si on obtient une contradiction, cela donne $f(n+1) - f(n) = \pm 1$. Il suffit alors de montrer que $f(n+2) \neq f(n)$ pour tout n pour déduire que $f(n) = \pm n + c$ pour tout n. Merci à Thomas Budzinski qui m'a montré cette technique.

Exemple 30. *(Iran TST 2008 P11)* Soit $k \geqslant 1$ un entier. Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$f(m) + f(n) \mid (m + n)^k$$

pour tous $n, m \in \mathbb{N}^\star$.

Solution. **Réponse :** La seule solution est l'identité.

Montrons que $|f(n+1) - f(n)| = 1$ pour tout entier n. On fixe un entier $n \geqslant 1$. Pour tout entier m, on a les deux divisibilités suivantes d'après l'énoncé :

$$f(m) + f(n) \mid (m + n)^k, \quad f(m) + f(n+1) \mid (m + n + 1)^k.$$

Soit p un éventuel diviseur premier de $f(n+1) - f(n)$. Soit $\ell \geqslant 1$ tel que $p^\ell > n$. On pose $m = p^\ell - n$. Alors la première divisibilité ci-dessus implique que $f(n) + f(m) \mid p^{k\ell}$, donc il existe a tel que $f(n)+f(m) = p^a$. Comme en plus $f(n)+f(m) \geqslant 2$, $a \geqslant 1$ donc $p \mid f(n)+f(m)$. Mais alors

$$p \mid f(m)+f(n)+(f(n+1)-f(n)) = f(m)+f(n+1) \mid (m+n+1)^k = (p^\ell+1)^k.$$

Cette divisibilité étant absurde, on déduit que $f(n+1)-f(n)$ n'a pas de diviseurs premiers, donc $\boxed{|f(n+1)-f(n)|=1}$.

Montrons à présent qu'on ne peut jamais avoir $f(n+2)=f(n)$. Soit n un entier éventuel tel que $f(n+2)=f(n)$. En prenant $m=n+1$, on trouve les deux divisibilités

$$f(n+1)+f(n) \mid (2n+1)^k, \quad f(n+1)+f(n) = f(n+1)+f(n+2) \mid (2n+3)^k.$$

Or $2n+1$ et $2n+3$ sont premiers entre eux, on a donc une contradiction.

En conséquence, les deux nombres $f(n+2)-f(n+1)$ et $f(n+1)-f(n)$ ne peuvent jamais être opposés, sinon on aurait $f(n+2)-f(n+1) = -(f(n+1)-f(n))$ et donc $f(n+2)=f(n)$. On a donc soit $f(n+1)-f(n)=1$ pour tout n, soit $f(n+1)-f(n)=-1$ pour tout n.

Dans le premier cas, on déduit par récurrence immédiate que $\boxed{f(n)=n+f(1)-1 \text{ pour tout } n}$. Réciproquement, si la fonction définie par $f(n)=n+c$, avec $c \geqslant 0$, est solution, alors on a $m+n+2c \mid (m+n)^k$ pour toute paire (m,n) d'entiers. On a donc

$$0 \equiv (m+n)^k \equiv (-2c)^k \mod m+n+2c.$$

Le nombre $(-2c)^k$ admet donc une infinité de diviseur et est nul. La fonction identité est alors la seule solution.

Dans le second cas, on déduit que $f(n) = -n+f(1)+1$, pour tout n, ce qui est absurde car f ne peut pas prendre de valeurs négatives.

On pourra repratiquer cette astuce sur l'exercice suivant :

Exercice 4.29. Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que ; pour tout nombre premier p, on a $p \mid f(a)^{f(p)} - f(b)^p$ si et seulement si $p \mid a-b$.

Astuces en vrac

- Lorsque qu'une expression $A(n,m)$ est un carré parfait pour tout (n,m), on pourra comparer $A(n,m)$ avec des carrés proches et/ou penser à comparer la croissance supposée de $A(n,m)$ (qui doit croître de façon quadratique) avec la croissance effective de n et m dans l'expression $A(n,m)$.
- Après avoir obtenu $f(p)$ pour tout p, alors le fait que $p \mid n^{p-1}-1$ peut permettre de relier p à n, pour peu que l'équation fonctionnelle fasse intervenir de la divisibilité.
- Dans le cas d'équations fonctionnelles très difficiles, ne pas hésiter à déployer l'artillerie lourde des boîtes noires. Les théorèmes suivants ont déjà vu une équation fonctionnelles s'en servir : Dirichlet, LTE, Zsigmondy ou encore « un entier qui est un carré mod p pour tout p est un carré parfait » (voir résultat de l'exercice 3.61).

Remarque : Une erreur récurrente dans le cas d'un exercice de la forme $A(n,m) \mid B(n,m)$ est d'introduire à m et n fixés l'entier k tel que $B(n,m) = kA(n,m)$ et d'oublier que cet entier k dépend de m et n. Il n'est donc pas le même pour toutes les paires (n,m). On se gardera de produire des fausses preuves utilisant ce principe.

Exercices

Les exercices suivants reprennent les idées précédentes, et d'autres encore.

Exercice 4.30. (Taiwan IMOC 2017) Déterminer les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que :

$$f(x) + f(y) \mid x^2 - y^2 \quad \forall x, y \in \mathbb{N}^\star.$$

Exercice 4.31. (Canada MO 2017) Soit $f : \mathbb{N}^\star \to \mathbb{N}^\star$ une fonction telle que, pour tout entier $n \geq 1$, $f(f(n))$ soit égal au nombre de diviseurs positifs de n. Montrer que si p est un nombre premier, alors $f(p)$ est aussi un nombre premier.

Exercice 4.32. (Iran round 3 2023 P1) Soit $f : \mathbb{Z} \to \mathbb{N}^\star$ une fonction. Pour tout entier $n \geqslant 1$, on pose $P(n) = f(1) \cdot \ldots \cdot f(n)$. Déterminer toutes les fonctions f pour lesquelles

$$P(a) + P(b) \mid a! + b!$$

pour tous entiers $a, b \geqslant 1$.

Exercice 4.33. Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tout entier $n \in \mathbb{N}^\star$ et tout nombre premier p,

$$f(n)^p \equiv n \mod f(p).$$

Exercice 4.34. (Balkan MO 2017 P3) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$n + f(m) \mid f(n) + nf(m)$$

pour tous $n, m \in \mathbb{N}^\star$.

Exercice 4.35. (Balkan MO SL 2017 N2) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que $xf(x) + f(y)^2 + 2xf(y)$ est un carré parfait pour tous $x, y \in \mathbb{N}^\star$.

Exercice 4.36. (Canada MO 2021) Une fonction f de $\mathbb{N}^\star$ dans $\mathbb{N}^\star$ est dite *canadienne* si pour tous $x, y \in \mathbb{N}^\star$,

$$\mathrm{PGCD}(f(f(x)), f(x + y)) = \mathrm{PGCD}(x, y).$$

Déterminer tous les entiers m tels que $f(m) = m$ pour toute fonction canadienne.

Exercice 4.37. (Balkan MO SL 2020 N3) Soit $k \geqslant 2$. Trouver toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tous entiers strictements positifs $x_1, ..., x_k$, on ait

$$x_1! + ... + x_k! \mid f(x_1)! + ... + f(x_k)!$$

Exercice 4.38. (USAMO 2012 P4) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que $f(n!) = f(n)!$ pour tout entier $n \geqslant 1$ et $m - n \mid f(m) - f(n)$ pour tous entiers $m, n \in \mathbb{N}^\star$ distincts.

Exercice 4.39. (RMM 2020 P4) Un sous-ensemble A de $\mathbb{N}^\star$ est dit *sans somme* si, pour toute paire (x, y) d'entiers de A (pas forcément distincts), le nombre $x+y$ n'est pas dans A. Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ surjectives telles que, pour tout ensemble A sans somme, l'ensemble $\{f(a), a \in A\}$ est également sans somme.

Exercice 4.40. *(EGMO 2022 P2)* Déterminer toutes les fonctions de $\mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tous entiers a et b, on a

1. $f(ab) = f(a)f(b)$ et
2. au moins deux des entiers $f(a), f(b)$ et $f(a+b)$ sont égaux.

Exercice 4.41. *(USA TSTST 2022, P4)* Soit f une fonction de $\mathbb{N}^\star$ dans $\mathbb{N}^\star$ telle que, pour tout couple d'entiers strictement positifs m et n, exactement un des entiers

$$f(m+1), \ldots, f(m+f(n))$$

est divisible par n. Montrer que $f(n) = n$ pour une infinité d'entiers n.

Exercice 4.42. *(IMO SL 2011 N3)* Soit $n \geqslant 1$ un entier impair. Déterminer toutes les fonctions f de $\mathbb{Z}$ dans $\mathbb{Z}$ telles que, pour tous entiers x, y,

$$f(x) - f(y) \mid x^n - y^n.$$

Exercice 4.43. *(IMO SL 2019 N4)* Soit C un entier naturel non nul. Trouver toutes les fonctions $f\colon \mathbb{N}^* \to \mathbb{N}^*$ telles que, pour tous les entiers a et b de somme $a + b \geqslant C$, l'entier $a + f(b)$ divise $a^2 + bf(a)$.

Exercice 4.44. *(IMO 2011 P5)* Soit $f : \mathbb{Z} \to \mathbb{N}^\star$ une fonction. On suppose que pour tous entiers m, n, on a $f(m-n) \mid f(m) - f(n)$. Montrer que pour tous entiers m et n tels que $f(m) \leqslant f(n)$, on a $f(m) \mid f(n)$.

Exercice 4.45. *(IMO SL 2007 N5)* Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ surjectives telles que, pour tout nombre premier p et tous entiers $m, n \in \mathbb{N}^\star$, $f(m+n)$ est divisible par p si et seulement si $f(m) + f(n)$ est divisible par p.

Exercice 4.46. *(IMO SL 2016 N6)* Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tous $n, m \in \mathbb{N}^\star$, le nombre $f(m) + f(n) - mn$ est non nul et divise $mf(m) + nf(n)$.

Exercice 4.47. Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$xf(x) + yf(y) \mid (x^2 + y^2)^{2022}$$

pour tous $x, y \in \mathbb{N}^\star$.

Exercice 4.48. *(IMO SL 2008 N5)* Pour tout entier $n \in \mathbb{N}$, on pose $d(n)$ le nombre de diviseurs positifs de n. Déterminer toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que

(i) $d(f(x)) = x$ pour tout $x \in \mathbb{N}$.
(ii) $f(xy)$ divise $(x-1)y^{xy-1}f(x)$ pour tous $x, y \in \mathbb{N}$.

Exercice 4.49. *(IMO SL 2020 N5)* Trouver les fonctions $f\colon \mathbb{N}^\star \to \mathbb{N}$ vérifiant les deux conditions suivantes :

1. $f(xy) = f(x) + f(y)$ pour tous les entiers $x \geqslant 1$ et $y \geqslant 1$;
2. il existe une infinité d'entiers $n \geqslant 1$ tels que l'égalité $f(k) = f(n-k)$ est vraie pour tout entier k tel que $1 \leqslant k \leqslant n-1$.

Exercice 4.50. *(IMO 2010 P3)* Déterminer toutes les fonctions $g : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que le nombre

$$(g(m) + n)(g(n) + m)$$

est un carré parfait pour toute paire (m, n) d'entiers strictement positifs.

Exercice 4.51. *(IMO 2025 P3)* Une fonction $f : \mathbb{N}^\star \to \mathbb{N}^\star$ est dite *australienne* si

$$f(a) \mid b^a - f(b)^{f(a)}$$

pour tous entiers strictement positifs a et b.

Déterminer le plus petit réel $c > 0$ tel que $f(n) \leqslant cn$ pour toute fonction australienne et tout entier $n \geqslant 1$.

Exercice 4.52. *(EMC 2021 P3 senior)* Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$x^2 - y^2 + 2y(f(x) + f(y))$$

est un carré parfait pour tous $x, y > 0$.

Exercice 4.53. *(SL ELMO 2014 N8)* Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que :

(i) les entiers $f(1), f(2), \ldots$ sont premiers entre dans leur ensemble,

(ii) il existe un entier $N \geqslant 1$ tel que pour tout $n \geq N$, $f(n) \neq 1$ et pour tous $a, b \in \mathbb{N}^\star$,

$$f(a)^n \mid f(a + b)^{a^{n-1}} - f(b)^{a^{n-1}}.$$

4.3 Théorie des nombres et combinatoire

Voici là aussi un type de problème émergent dans les olympiades, à savoir les problèmes transverses, notamment à l'interface entre théorie des nombres et combinatoire.

Le domaine est trop vaste et trop récent pour pouvoir en identifier des catégories ou des recettes. On dira simplement qu'il s'agit d'avoir des idées combinatoires (principe des tiroirs, recherche d'invariants, principe de l'extremum) avec des objets de théories des nombres (nombres premiers, restes modulo n, diviseurs...). L'important pour s'y retrouver est de trouver la bonne façon de visualiser les différents objets et leurs liens combinatoires. Les représentations graphiques ne manquent heureusement pas : graphe, tableau, coloriage...

Les méthodes d'approche d'un problème de combinatoire restent valables pour cette catégorie : tests des petits cas, récurrence, algorithme glouton, double comptage... et bien sûr beaucoup de pratique pour avoir des exemples d'arguments et de construction en tête et savoir à quoi s'attendre sur ce genre de problème.

En guise d'amuse bouche, voici quelques exemples à méditer.

Exemple 31. *(Nordic 2021)* Soit $n \geqslant 1$ un entier. Alice et Bob jouent au jeu suivant : Alice choisit $n+1$ ensembles $A_1, \ldots, A_{n+1} \subseteq \{1, \ldots, 2^n\}$ chacun de taille 2^{n-1}. Ensuite, Bob choisit $n+1$ entiers $a_1, \ldots, a_{n+1}$. Bob gagne si, pour tout entier t, il existe un indice i et un élément $s \in A_i$ tel que $s + a_i \equiv t \mod 2^n$.

Déterminer, en fonction de n, lequel des deux joueurs possède une stratégie gagnante.

Solution. **Réponse :** Bob peut toujours s'arranger pour gagner.

On peut deviner la réponse en testant l'énoncé sur des petites valeurs. Dans la suite, tous les entiers sont considérés modulo 2^n. On note, pour tout ensemble A pour tout entier b, l'ensemble $A + b = \{a + b, a \in A\}$. Il s'agit de montrer que, quels que soient les ensembles $A_1, \ldots, A_{n+1}$, on peut trouver des entiers $a_1, \ldots, a_{n+1}$ tels que $\{0, 1, \ldots, 2^n - 1\}$ soit recouvert par les ensembles $A_1 + a_1, A_2 + a_2, \ldots, A_{n+1} + a_{n+1}$.

On va montrer que Bob peut gagner avec un algorithme « glouton », dans lequel Bob choisit les a_i un par un de sorte que, à chaque étape, l'ensemble $A_i + a_i$ recouvre au moins la moitié des restes de $\{0, \ldots, 2^n - 1\}$ qui ne sont pas encore recouverts.

Il s'agit donc de montrer le lemme suivant :

Lemme : Soit A un ensemble de restes de cardinal 2^{n-1} et X un ensemble d'entiers. Il existe un entier b tel que, pour au moins $|X|/2$ éléments x de X, on ait $x \in A + b$ (autrement dit, $|(A + b) \cup X| \geqslant |X|/2$.

Preuve : Il s'agit d'une méthode de la moyenne. On considère l'ensemble des couples (a, x) avec $a \in A$ et $x \in X$. Il y a $|A| \cdot |X| = 2^{n-1}|X|$ tels couples et 2^n valeurs possibles pour la différence $a - x$. D'après le principe des tiroirs, il existe un élément b de $\{0, \ldots, 2^n - 1\}$ et au moins $\dfrac{|A| \cdot |X|}{2^n}$ couples (a, x) partageant la même différence $x - a = b$.

Dans ces couples, les coordonnées x sont nécessairement deux à deux disjointes : si on a $x - a = b = x - a'$, alors $a = a'$ et $(x, a) = (x, a')$, ce qui est exclu. Ainsi, l'ensemble $A + b$ recouvre au moins $\dfrac{2^{n-1}|X|}{2^n} = |X|/2$ éléments distincts de X, ce qui est le résultat voulu. □

Ainsi, Bob procède de la façon suivante : il choisit a_1 tel que $A_1 + a_1$ recouvre la moitié des

restes de $\{0, \dots, 2^n - 1\}$ (c'est en fait toujours le cas quel que soit le choix de a_1), puis choisit a_2 de sorte que $A_2 + a_2$ contienne au moins la moitié des 2^{n-1} nombres qui ne sont pas dans $A_1 + a_1$ (c'est possible d'après le lemme), et continue ainsi. Lors de l'étape i, il choisit a_i de sorte que $A_i + a_i$ contiennent 2^{n-i} des 2^{n-i+1} nombres non encore contenus dans les précédents ensembles. Lors de l'étape $n+1$, il ne reste que $2^0 = 1$ nombre à recouvrir, et il choisit a_{n+1} de sorte que ce nombre soit dans $A_{n+1} + a_{n+1}$. Cela signifie bien que Bob peut gagner.

Dans l'exemple suivant, le point de vue des graphes est salutaire.

Exemple 32. *(USAMO 2018 P1)* Soit p un nombre premier impair et $a_1, \dots, a_p$ des entiers. Montrer qu'il existe un entier k tel que les nombres

$$a_1 + k, a_2 + 2k, \dots, a_p + pk$$

donnent au moins $\frac{p}{2}$ restes différents modulo p.

Solution. La première chose à faire est de regarder à quelle condition deux nombres $a_j + jk$ et $a_i + ik$ donnent le même reste modulo p. Cette condition se réécrit

$$a_j + jk \equiv a_i + ik \mod p \iff k \equiv -\frac{a_i - a_j}{i - j} \mod p$$

Considérons le graphe G complet dont les sommets sont les entiers $a_1, \dots, a_p$ et deux sommets a_i et a_j sont reliés par la couleur k si la congruence ci-dessus est satisfaite.

Ce graphe a $\binom{p}{2} = \frac{p(p-1)}{2}$ arêtes. D'après le principe des tiroirs, il existe une couleur k telle qu'au plus $\frac{p-1}{2}$ arêtes sont de cette couleur. On efface désormais toutes les autres arêtes.

On a donc un graphe avec au plus $\frac{p-1}{2}$ arêtes. Montrons que cela laisse au moins $\frac{p+1}{2}$ composantes connexes disjointes, c'est-à-dire que les $a_i + ik$ prennent au moins $\frac{p+1}{2}$ restes distincts.

Notons r le nombre de composantes connexes du graphe. Pour rendre le graphe connexe, il suffit d'ajouter $r-1$ arêtes. Le graphe obtenu possède alors au moins $p-1$ arêtes puisqu'il est connexe et possède $p-1$ sommets. Cela signifie que

$$r - 1 \geqslant p - 1 - \frac{p-1}{2} = \frac{p-1}{2}.$$

Cela implique que $r \geqslant \frac{p+1}{2}$, comme voulu.

Voici une gamme d'exercices pour s'entraîner.

Exercices

Exercice 4.54. *(OFM 2025 junior)* Charlotte écrit au tableau les entiers $1, \dots, 2025$. Charlotte dispose de deux opérations, l'opération *PGCD* et l'opération *PPCM*. L'opération *PGCD* consiste à choisir deux entiers a et b écrits au tableau, à les effacer et à écrire l'entier $\mathrm{PGCD}(a, b)$. L'opération *PPCM* consiste à choisir deux entiers a et b écrits au tableau, à les effacer et à écrire l'entier

PPCM(a, b). Un entier N est dit *gagnant* s'il existe une suite d'opérations à l'issue desquelles le seul entier encore écrit au tableau est l'entier N.
Déterminer tous les entiers gagnants parmi $\{1, \ldots, 2025\}$ et donner, pour chacun d'eux, le nombre minimum d'opérations *PGCD* que Charlotte doit utiliser.

Exercice 4.55. *(All Russia 2025)* Soit $n \geqslant 1$ un entier. On écrit les nombres $1, 2, \ldots, n$ en ligne dans un certain ordre. Pour toute paire de nombres adjacents, on calcule leur PGCD. Quel est le plus grand nombre de valeurs distinctes que l'on peut obtenir avec ces $n-1$ valeurs ?

Exercice 4.56. *(IZhO 2025 P4)* Au tableau, il y a 999 entiers consécutifs. Pour tout $i \in \{2, 3, \ldots 1000\}$, Alice écrit sur un papier la phrase « ce nombre n'est pas divisible par i ». Elle place ensuite les papiers sous les entiers écrits, de sorte qu'en dessous de chaque entier se trouve exactement un papier. Alice gagne un point chaque fois que l'information d'un papier est correcte. Combien de points, au maximum, Alice peut-elle s'assurer de gagner, quels que soient les 999 entiers consécutifs inscrits ?

Exercice 4.57. *(JBMO SL 2024 C1, Israël MO 2021)* Déterminer le plus petit entier strictement positif k vérifiant la propriété suivante : pour tout sous-ensemble S de $\{1, \ldots, 2024\}$ de taille k, il existe deux entiers distincts $a, b \in S$ tels que $ab + 1$ est un carré parfait.

Exercice 4.58. *(Balkan MO 2019 N2)* Soit $n \geqslant 1$ un entier et soit $S \subset \{1, \ldots, n\}$ un ensemble. On note s le PGCD des éléments de S. On suppose que $s \neq 1$ et on note d son plus petit diviseur strict. Soit $T \subset \{1, \ldots, n\}$ un ensemble tel que $S \subset T$ et $|T| \geqslant 1 + \left\lfloor \frac{n}{d} \right\rfloor$. Montrer que le plus grand commun diviseur des éléments de T est 1.

Exercice 4.59. *(Hong-Kong TST 2016 Test 2 P4)* Alice et Bob jouent au jeu suivant :

1. Alice commence par écrire sur une ligne 2015 nombres premiers dans l'ordre croissant. Son score correspond au produit de ces nombres premiers.
2. Bob écrit un entier strictement positif.
3. Alice dessine une barre verticale entre deux nombres premiers adjacents et calcule le produit de tous les nombres premiers à gauche de la barre verticale.
4. Bob ajoute ce produit à l'entier qu'il a inscrit. Son score correspond à cette somme.

Alice gagne si les scores d'Alice et Bob ont un facteur premier commun. Bob gagne sinon. Lequel des deux joueurs possède une stratégie gagnante ?

Exercice 4.60. *(France TST Novembre, Japan MO 2023)* Alice et Bob jouent au jeu suivant. Avant que le jeu ne commence, leur amie Clara a écrit les entiers $2, 3, 4, \ldots, 30$ au tableau. Puis, chacun à leur tour, Alice et Bob effacent certains entiers encore présents sur le tableau ; on note S_k l'ensemble des entiers effacés au $k^{\text{ème}}$ tour de jeu. Pour corser le jeu, Clara a elle-même choisi l'ensemble S_1 dont elle force Alice à effacer les éléments au premier tour.
De plus, pour tout entier $k \geqslant 2$, au moment de choisir l'ensemble S_k des nombres qu'il s'apprête à effacer, le joueur qui joue au $k^{\text{ème}}$ tour doit respecter la contrainte suivante : pour chaque élément x de S_k, il doit exister au moins un élément y de S_{k-1} tel que $\mathsf{PGCD}(x, y) \neq 1$.
Par exemple, si Clara choisit l'ensemble $S_1 = \{2, 5\}$, Bob peut choisir, au deuxième tour, l'ensemble $S_2 = \{14, 25, 26\}$; au troisième tour, Alice peut alors effacer les entiers 15 et 22, mais pas 27.
Le premier joueur qui choisit un ensemble vide perd la partie. Pour combien d'ensembles S_1 non vides Alice pourra-t-elle se débrouiller pour gagner quels que soient les choix de Bob ?

Exercice 4.61. (Polish MO Round 2 2023 P6) Soit $p \geqslant 5$ un nombre premier et soit $n = p - 1$. On considère un échiquier de $n \times n$ cases. Un ensemble de n cases est dit *tactique* si, après avoir placé une dame sur chacune des n cases, deux dames quelconques ne s'attaquent jamais. Montrer qu'il existe $n - 2$ ensembles tactiques disjoints n'ayant deux à deux aucune case en commun et ne contenant aucune case des deux diagonales principales.

Exercice 4.62. (Nordic 2021) Alice a écrit des entiers au tableau. Puis, à chaque minute, elle ajoute à la liste des nombres du tableau le plus petit entier supérieur aux entiers déjà écrits et non divisible par l'un d'entre eux. Montrer qu'à partir d'un certain temps, Alice n'écrit plus que des nombres premiers.

Exercice 4.63. (Canada MO 2018, Envoi TN 2021-2022) On dit que deux entiers $a, b \in \mathbb{N}^\star$ sont *reliés* s'il existe un nombre premier p tel que $a = pb$ ou $b = pa$.

Trouver tous les entiers $n \geqslant 1$ ayant la propriété suivante : on peut écrire tous les diviseurs positifs de n (1 et n compris) exactement une fois sur un cercle de sorte que tout diviseur soit relié avec chacun de ses deux voisins ?

Exercice 4.64. (IMO SL 2021 C1) Soit $\mathcal{S}$ un ensemble infini d'entiers naturels non nuls contenant quatre entiers a, b, c, d deux à deux distincts tels que $\mathrm{PGCD}(a, b) \neq \mathrm{PGCD}(c, d)$. Démontrer que $\mathcal{S}$ contient trois entiers x, y, z deux à deux distincts tels que $\mathrm{PGCD}(x, y) = \mathrm{PGCD}(y, z) \neq \mathrm{PGCD}(z, x)$.

Exercice 4.65. (IMO 2021 P1) Soit $n \geqslant 100$ un entier. On écrit les entiers $n, n+1, \ldots, 2n$ chacun sur une carte. On mélange ensuite les $n + 1$ cartes et on les divise en deux piles. Montrer qu'au moins une pile contient deux cartes dont la somme des numéros est un carré parfait.

Exercice 4.66. (Balkan MO 2024 N1) Soit $n \geqslant 1$ un entier. Existe-t-il deux entiers strictement positifs x et y distincts possédant chacun n chiffres, dont les chiffres sont chacun $1, 2, 3$ ou 4 et tels que $4^n \mid x - y$?

Exercice 4.67. (IMO SL 2009 N2) Un entier strictement positif N est dit joli si $N = 1$ ou si N s'écrit comme un produit d'un nombre pair de facteurs premiers (pas forcément distincts). Pour toute paire (a, b) d'entiers strictement positifs, on pose $P(x) = (x + a)(x + b)$.

a) Montrer qu'il existe des entiers strictement positifs distincts (a, b) tels que $P(1), P(2), \ldots, P(50)$ sont jolis.

b) Montrer que si $P(n)$ est joli pour tout entier $n > 0$, alors $a = b$

Exercice 4.68. (France EGMO TST 2019) Jean dispose de 503 pièces, qu'il a réparties dans deux saladiers, chaque saladier contenant au moins une pièce. Puis, tant que chacun des deux saladiers contient deux pièces ou plus, il effectue l'opération suivante : à chaque opération, il choisit le saladier qui contient un nombre pair de pièces, prend la moitié de ces pièces, et les met dans l'autre saladier ; si l'un des deux saladiers contient une pièce ou moins, il s'arrête.
Est-il possible que ce processus ne s'arrête jamais ?

Exercice 4.69. (BXMO 2017) Un $n-$carré est une grille $n \times n$ dans laquelle on inscrit n^2 entiers strictement positifs deux à deux distincts et vérifiant la propriété suivante :

Si on calcule le plus grand commun diviseur de chaque ligne et le plus grand commun diviseur de chaque colonne, les $2n$ nombres obtenus sont distincts.

1. Montrer qu'un $n-$carré contient au moins un nombre supérieur ou égal à $2n^2$.
2. On suppose que tous les nombres de la grilles sont majorés par $2n^2$. Trouver les valeurs possibles de n.

Exercice 4.70. *(IMO SL 2017 N3)* Déterminer tous les entiers $n \geqslant 2$ possédant la propriété suivante : pour tout choix de n entiers $a_1, a_2, \ldots, a_n$ dont la somme n'est pas divisible par n, il existe un indice $1 \leqslant i \leqslant n$ tel qu'aucun des nombres

$$a_i, \quad a_i + a_{i+1}, \quad \ldots, \quad a_i + a_{i+1} + \ldots + a_{i+n-1}$$

n'est divisible par n. (Ici, on adopte la convention $a_{i+n} = a_i$).

Exercice 4.71. *(EGMO 2026 P2)* Soit $n \geqslant 1$ un entier. Marie joue au jeu suivant. Elle commence par écrire l'entier 1 au tableau. Autant de fois qu'elle peut, elle peut choisir un entier j tel que $1 \leqslant j \leqslant n$ et remplacer l'entier V écrit au tableau par le nombre $j \cdot R(V/j)$, où $R(x)$ désigne l'entier le plus proche de V/j.

1. Montrer que, pour tout entier n, il existe un entier B strictement positif tel que Marie ne peut jamais écrire un entier strictement supérieur à B.
2. Pour tout entier n, on note $f(n)$ le plus grand entier que Marie peut écrire au tableau. Montrer qu'il existe un entier N strictement positif tel que, pour tout $n \geqslant N$, on a $2026 \mid f(n)$.

Exercice 4.72. *(BXMO 2025)* Soient $a_0, a_1, \ldots, a_{10}$ des entiers tels que, pour tout $i \in \{0, 1, \ldots, 2047\}$, il existe certains indices notés $i_1, \ldots, i_r$ tels que

$$a_{i_1} + \ldots + a_{i_r} \equiv i \mod 2048.$$

Montrer que pour tout $i \in \{0, 1, \ldots, 10\}$, il existe exactement un indice $j \in \{0, 1, \ldots, 10\}$ tel que a_j est divisible par 2^i mais pas par 2^{i+1}.

Exercice 4.73. *(France TST 2020-2021)* Morgane a écrit les trois entiers 3, 4 et 12 au tableau. Elle effectue ensuite des changements successifs en procédant comme suit : elle choisit deux nombres a et b écrits au tableau, les efface, et les remplace par $(3a + 4b)/5$ et $(4a - 3b)/5$.
Morgane peut-elle, après un nombre fini de tels changements,

1. parvenir à écrire le nombre 13 au tableau ?
2. parvenir à écrire le nombre -12 au tableau ?

Exercice 4.74. *(RMM 2024 P2)* Soit p un nombre premier impair et $N < 50p$ un entier. Soient $a_1, \ldots, a_N$ des entiers strictement inférieurs à p et tels que chaque entier apparaît au plus $\frac{51}{100}N$ fois parmi les entiers a_i. On suppose également que $a_1 + \ldots + a_N$ n'est pas divisible par p. Montrer qu'il existe une permutation $b_1, \ldots, b_N$ des entiers a_i telle que, pour tout $k = 1, 2, \ldots, N$, la somme $b_1 + b_2 + \ldots + b_k$ n'est pas divisible par p.

Exercice 4.75. *(IMO 2022 P3)* Soit $k \geqslant 1$ un entier et S un ensemble fini de nombres premiers impairs. Montrer qu'il existe au plus une façon (à rotation et symétrie près) de placer les éléments de S autour d'une cercle de sorte que le produit de deux nombres voisins soit de la forme $x^2 + x + k$, où x est un entier.

4.4 Problèmes de construction d'entiers

Le but de cette section est de se familiariser avec le processus de construction d'entiers vérifiant certaines propriétés. Elle est largement inspirée d'un cours donné avec Paul Cahen au stage de Valbonne 2022 et d'un cours donné par Rémi Lesbats en 2025.

Les problèmes de construction peuvent être des problèmes à part entière (« Montrer qu'il existe une infinité d'entiers avec la propriété suivante » ou « Montrer qu'il existe une suite infinie d'entiers vérifiant la propriété suivante » ou « Montrer que pour tout n, il existe un ensemble de n entiers vérifiant la propriété suivante »). Ils peuvent également être un peu mieux déguisés, comme dans le cas de problèmes avec une hypothèse de la forme « Pour tout entier n, on a la propriété suivante » et dans lesquels la clé est d'appliquer l'énoncé à des entiers n biens choisis qu'il faut construire.

Voici le protocole à adopter pour les problèmes de construction d'entiers :

1. Identifier le cahier des charges sur notre entier à partir de l'énoncé (ses facteurs premiers doivent suivre telle propriété, il doit diviser une expression...).
2. Exprimer les conditions du cahier des charges sous une forme plus simple, en général en trouvant une condition suffisante (et pas forcément nécessaire) pour que chaque condition soit remplie (par exemple « il suffit que n soit premier pour vérifier la première condition »).
3. Vérifier, si besoin est, l'existence d'entiers vérifiant le cahier des charges simplifié à l'aide de théorèmes d'existence.

Pour résoudre des problèmes de construction, il faut avoir dans sa valise des théorèmes d'existence, des méthodes générales et bien sûr, beaucoup d'exemples acquis avec la pratique.

Concernant les théorèmes d'existence, on rappelle les principaux, qui sont déjà évoqués dans le présent polycopié :

- ☞ Le théorème d'Euler-Fermat donnant l'existence d'un multiple de n de la forme $a^k - 1$ lorsque a et n sont premiers entre eux (voir la section dédiée).
- ☞ Le théorème des restes chinois : celui-ci donne l'existence d'une infinité de solutions (et donc d'entiers suffisamment grands) à un système de congruences bien posé. On peut donc construire à notre guise un entier vérifiant en même temps plusieurs contraintes de notre cahier des charges.
- ☞ Les théorèmes de Zsigmondy, le postulat de Bertrand, le théorème de Dirichlet et le théorème de Schur, qui permettent de construire des nombres premiers avec beaucoup de contraintes (voir la section dédiée).

On présente désormais plusieurs méthodes, stratégies et astuces.

Se simplifier la vie

Dans l'ensemble, il faut chercher des entiers avec une forme très simple : des puissances de nombres premiers (dont l'ensemble des diviseurs est bien maitrisé), des nombres de la forme $a^n - 1$, des puissances de 10... Commencer par chercher des entiers avec cette forme permet généralement de simplifier le cahier des charges, réduire le nombre d'inconnues ou de degrés de libertés et donc de faciliter les calculs, la mise en oeuvre et la rédaction.

Exemple 33. *(RMM 2020 SL N2)* Pour un entier $n \geqslant 1$, on note $\varphi(n)$ l'indicatrice d'Euler et $d(n)$ le nombre de diviseurs de n. Montrer qu'il existe une infinité d'entiers n tels que $\varphi(n)$ et $d(n)$ sont des carrés parfaits.

Solution. On commence par chercher du côté des entiers pour lesquels les fonctions $\varphi(n)$ et $d(n)$ sont faciles à calculer. C'est le cas des puissances de nombres premiers. Comme $\varphi(p^k) = p^{k-1}(p-1)$ et $d(p^k) = k+1$, il suffit que $k+1$ soit un carré parfait, que $k-1$ soit pair et que $p-1$ soit un carré parfait.

En particulier, on vérifie $\boxed{n = 5^{4k^2-1}}$ (ou même $n = 2^{4k^2-1}$) satisfait toutes ces conditions pour tout entier k, d'où l'infinité annoncée.

Les constructions par récurrence

Si n est solution, y a-t-il un autre entier solution que l'on peut exprimer en fonction de n ?

Pour montrer qu'il existe une infinité d'entiers vérifiant un énoncé, on peut les construire par récurrence : on trouve un premier entier simple, puis on suppose avoir construit un entier n générique et on construit le suivant à partir de n. Cela implique de chercher des propriétés de stabilités de la propriété étudiée (si n est solution, qui d'autre est solution ?).

Cette construction vaut également pour les ensembles : supposons que l'on cherche à construire un ensemble arbitrairement grand avec une certaine propriété. On peut procéder par récurrence, en construisant un ensemble de taille $1, 2, 3\ldots$, puis on suppose avoir construit un ensemble de taille $n-1$, et on l'adapte pour construire un ensemble de taille n.

Exemple 34. *(Autriche MO 2024)* Un entier n est dit puissant si tous les exposants dans sa décomposition en facteurs premiers sont $\geqslant 2$. Montrer qu'il existe une infinité d'entiers n tels que n et $n+1$ sont puissants.

Solution. Notons que $n = 8$ est puissant puisque $n = 2^3$ et $n+1 = 3^2$.

On cherche désormais, étant donné un entier puissant n, un autre entier puissant A que l'on peut exprimer en fonction de n. Dans l'idée de s'arranger pour que $A+1$ soit un carré parfait, ce qui le force à être puissant, on s'intéresse au nombre $A = 4n(n+1)$ qui est puissant car il est produit de deux nombres puissants. Alors $A+1 = 4n^2+4n+1 = (2n+1)^2$. Le nombre A est donc puissant. Comme en plus $A > n$, on construit ainsi par récurrence une infinité de nombres puissants.

On pourra pratiquer sur les exercices suivants :

Exercice 4.76. *(Extrait BXMO 2011)* Un couple d'entiers (m, n) vérifiant $1 < m < n$ est appelé *couple Benelux* si m a les mêmes diviseurs premiers que n et $m+1$ a les mêmes diviseurs premiers que $n+1$.

Montrer qu'il existe une infinité de couples Benelux.

Exercice 4.77. *(IMO 2013 P1)* Soient k et n deux entiers. Montrer qu'il existe des entiers $m_1, \ldots, m_k$ tels que

$$1 + \frac{2^k - 1}{n} = \left(1 + \frac{1}{m_1}\right) \ldots \left(1 + \frac{1}{m_k}\right).$$

Une variante : l'algorithme glouton

Lorsque l'on souhaite construire une permutation de $\mathbb{N}$ vérifiant certaines propriétés, une bonne stratégie est d'utiliser un algorithme glouton pour caser l'entier de votre choix. Cela se présente de la façon suivante : supposons que l'on a construit $a_1, \ldots, a_k$ les termes de notre suite. On note x le plus petit entier strictement positif qui n'apparaît pas parmi les a_k. On cherche alors à caser x parmi les prochains termes que l'on va construire.

Exemple 35. *(Russie MO 1995)* Existe-t-il une permutation $a_1, a_2, \ldots$ de $\mathbb{N}^\star$ telle que, pour tout entier $n \geqslant 1$, le nombre $a_1 + \ldots + a_n$ soit divisible par n ?

Solution. On montre que oui, on utilise pour cela un « algorithme glouton ».

On commence avec $a_1 = 1$. On suppose que $a_1, \ldots, a_k$ sont construits et on note x le plus petit entier strictement positif qui n'apparaît pas dans l'ensemble $\{a_1, \ldots, a_k\}$. On veut choisir a_{k+1} tel qu'on puisse poser $a_{k+2} = x$. Pour cela, on note $s = a_1 + \ldots + a_k$. Il faut que

$$\begin{cases} s + a_{k+1} & \equiv & 0 & \mod k+1 \\ s + a_{k+1} + x & \equiv & 0 & \mod k+2 \end{cases}$$

soit

$$\begin{cases} a_{k+1} & \equiv & -s & \mod k+1 \\ a_{k+1} & \equiv & -s - x & \mod k+2 \end{cases}$$

qui possède une infinité de solutions. On dispose donc d'un entier a_{k+1} qui n'est pas déjà dans la suite (a_i) et qui vérifie le système précédent.

On peut donc s'arranger pour placer x. Notre construction assure que les termes de la suite sont deux à deux distincts et que chaque entier y apparaît.

On pourra repratiquer avec :

Exercice 4.78. *(Envoi d'arithmétique 2020-2021)* Déterminer s'il existe une suite infinie d'entiers (a_n) d'entiers strictement positifs vérifiant les deux propriétés suivantes :

1. Tout entier strictement positif apparaît exactement une fois dans la suite (a_n).
2. Pour tout entier $n \geqslant 1$, $\prod_{i=1}^{n} a_i$ s'écrit comme une puissance $n-$ème d'un entier.

Exercice 4.79. *(France TST 2019/2020)* Soit $a_0, a_1, \ldots$ une suite d'entiers positifs, et soit (b_n) la suite définie par $b_n = \mathrm{PGCD}(a_n, a_{n+1})$ pour tout $n \geqslant 0$. Montrer qu'il est possible de choisir la suite (a_n) de sorte que tout entier naturel non nul soit égal à exactement un des termes $a_0, b_0, a_1, b_1, \ldots$.

Les problèmes sur les chiffres

Dans le cas de problèmes faisant intervenir les chiffres d'un entier, et bien souvent la somme des chiffres, les bons entiers à considérer sont bien souvent les entiers dont il est *très* facile de calculer la somme des chiffres, comme les puissances de 10 ou les nombres de la forme $10^k - 1$. Ces derniers possèdent de bonnes propriétés de divisibilité et peuvent être couplés avec les astuces données dans la théorie de l'ordre.

Exemple 36. *(Bundeswettbewerb 2021 Round 2 P1/4)* Pour tout entier $n \geqslant 1$, notons $S(n)$ la somme des chiffres de n. Montrer que tout entier k admet un multiple n tel que $S(n) = S(n^2)$.

Solution. On commence par le cas où k est premier avec 10. Dans ce cas, on prend $n = 10^{\varphi(k)} - 1$, qui est bien un multiple de k d'après le théorème d'Euler. On vérifie que

$$S(n^2) = S(10^{2\varphi(k)} - 2 \cdot 10^{\varphi(k)} + 1) = S(10^{\varphi(k)} - 2) + 1 = S(10^{\varphi(k)} - 1) = S(n).$$

Donc $\boxed{n = 10^{\varphi(k)} - 1}$ convient.

Le cas général n'est pas bien différent, dans la mesure où n et $10n$ partagent la même somme des chiffres. Posons donc $k = 2^\alpha 5^\beta k'$, avec k' premier avec 10. Alors $\boxed{n = (10^{\varphi(k')} - 1)10^{\max(\alpha,\beta)}}$ est bien un multiple de k et vérifie

$$S(n^2) = S((10^{\varphi(k')} - 1)^2) = S(10^{\varphi(k')} - 1) = S((10^{\varphi(k')} - 1)10^{\max(\alpha,\beta)}),$$

ce qui conclut.

On pourra repratiquer avec les exercices suivants :

Exercice 4.80. *(Polish MO round 2 2012)* Pour tout entier $n \geqslant 1$, notons $S(n)$ la somme des chiffres de n. Montrer qu'il existe une infinité d'entiers strictement positifs n tels que $S(2^n + n) < S(2^n)$.

Exercice 4.81. *(IMO SL 2016 N1)* Pour tout entier strictement positif k, on note $S(k)$ la somme de ses chiffres. Déterminer les polynômes P à coefficients entiers tels que, pour tout entier $n \geqslant 2016$, on a $P(n) > 0$ et

$$S(P(n)) = P(S(n)).$$

Exercices

Exercice 4.82. Montrer qu'il existe une infinité de paires (m, n) d'entiers distincts telles que $m!n!$ est un carré parfait.

Exercice 4.83. *(Roumanie MO SL 2023)* Montrer qu'il existe une infinité d'entiers x tels que $x + S(x)$ est un carré parfait, où $S(x)$ désigne la somme des chiffres de x.

Exercice 4.84. *(Estonie 2023 TST)* Deux entiers m et n distincts sont dits *amis* si $n - m$ divise m et n. Montrer que, pour tout entier $k \geqslant 1$, il existe k entiers distincts tels que deux quelconques d'entre eux sont toujours amis.

Exercice 4.85. *(Polish MO 2016 round 2 P4)* Soit $k \geqslant 1$ un entier. Montrer qu'il existe un entier $n \geqslant 1$ tels que les deux ensembles $A = \{1^2, 2^2, 3^2, \ldots\}$ et $B = \{1^2 + n, 2^2 + n, 3^2 + n, \ldots\}$ ont exactement k termes en commun.

Exercice 4.86. Soit $n \geqslant 1$ un entier. Dans une classe de n élèves numérotés de 1 à n, certains élèves sont amis de façon réciproque. Peut-on toujours trouver un entier $N \geqslant 1$ et n entiers $a_1, \ldots, a_n$ tels que les élèves numéros i et j sont amis si et seulement si N divise $a_i a_j$?

Exercice 4.87. (TST Suisse 2022) Soit n un entier strictement positif. Montrer qu'il existe une suite finie S de 0 et de 1 telle que, pour tout entier $d \geqslant 2$, le nombre dont l'écriture en base d correspond à la suite S est non nul et divisible par n.

Exercice 4.88. (RMM 2015 P1) Existe-t-il une suite infinie d'entiers strictement positifs $a_1, \ldots$ telle que a_m et a_n sont premiers entre eux si et seulement si $|m-n| = 1$?

Exercice 4.89. (Balkan MO 2018 SL N1) Pour tous entiers strictement positifs m et n, on note $d(m,n)$ le nombre de nombres premiers distincts divisant à la fois m et n. Par exemple $d(60,126) = d(2^2 \cdot 3 \cdot 5, 2 \cdot 3^2 \cdot 7) = 2$. Existe-t-il une suite (a_n) d'entiers strictement positifs telle que

- $a_1 \geqslant 2018^{2018}$,
- $a_m \leqslant a_n$ pour tous entiers $m \leqslant n$,
- $d(m,n) = d(a_m, a_n)$ pour tous entiers m et n distincts ?

Exercice 4.90. (OFM 2023 senior) Existe-t-il des entiers a et b tels que, parmi les entiers $a, a+1, \ldots, a+2023, b, b+1, \ldots, b+2023$, aucun entier n'en divise un autre, mais

$$a(a+1)\ldots(a+2023) \mid b(b+1)\ldots(b+2023).$$

Exercice 4.91. (Iran 2012 Round 2 P3) Soit $t > 0$ un entier. Montrer qu'il existe un entier $n > 1$, premier avec t tel qu'aucun des termes de la suite $n+t, n^2+t, n^3+t, \ldots$ ne soit une puissance parfaite.

Exercice 4.92. (MEMO 2021) Montrer qu'il existe une infinité d'entiers n tels que l'écriture de n^2 en base 4 ne contient que des 1 et des 2.

Exercice 4.93. (BXMO 2020) Existe-t-il un entier n admettant exactement 2020 diviseurs d tels que $\sqrt{n} < d < 2\sqrt{n}$?

Exercice 4.94. (Balkan MO SL 2025 N3) Étant donné un entier $k \geqslant 1$, on dit qu'un couple (a,b) d'entiers strictement positifs est $k-$sympa si $a \mid b^k + 1$ et $b \mid a^k + 1$.
Déterminer les entiers k pour lesquels il existe une infinité de couples $k-$sympas.

Exercice 4.95. (Iran TST 2021 P4) Pour tout entier $n \geqslant 2$, on note $\Omega(n)$ le plus grand facteur premier de n et $\omega(n)$ le plus petit facteur premier de n. Alice et Bob jouent au jeu suivant : Alice commence par choisir 1400 polynômes à coefficients entiers. Bob les répartit ensuite en deux ensembles A et B. Bob gagne le jeu si, pour tout entier $n \geqslant 2$,

$$\max_{P \in A}(\Omega(P(n))) \geqslant \min_{P \in B}(\omega(P(n))).$$

Lequel des deux joueurs possède une stratégie gagnante ?

Exercice 4.96. (USA TST 2015 Decembre P2) Montrer que, pour tout entier $n \geqslant 1$, il existe un ensemble S de n entiers strictement positifs, tel que, pour tous $a, b \in S$ distincts, $a-b$ divise a et b mais aucun autre élément de S.

Exercice 4.97. (IMO SL 2022 N5) Soit $n \geqslant 1$ un entier. Morgane écrit au tableau, en base 10, les nombres $2023, 2023 \times 2, \ldots, 2023 \times n$. Pour tout chiffre c compris entre 1 et 9, elle note alors $\mathsf{d}_c(n)$

le nombre d'apparitions du chiffre c sur le tableau. Par exemple, si $n = 3$, elle écrit les nombres 2023, 4046 et 6069, donc $\mathsf{d}_1(3) = \mathsf{d}_5(3) = \mathsf{d}_7(3) = \mathsf{d}_8(3) = 0$, $\mathsf{d}_3(3) = \mathsf{d}_9(3) = 1$, $\mathsf{d}_2(3) = \mathsf{d}_4(3) = 2$ et $\mathsf{d}_6(3) = 3$; ces neuf nombres prennent donc exactement quatre valeurs.
Démontrer qu'il existe une infinité d'entiers $n \geqslant 1$ pour lesquels les neuf nombres $\mathsf{d}_1(n), \mathsf{d}_2(n), \ldots, \mathsf{d}_9(n)$ prennent exactement deux valeurs.

Exercice 4.98. (IMO SL 2019 N7) Démontrer qu'il existe un réel $c > 0$ et une infinité d'entiers $n \geqslant 1$ ayant la propriété suivante :

> Il existe une infinité d'entiers naturels que l'on ne peut pas écrire comme une somme d'au plus $cn\ln(n)$ puissances $n^{\text{èmes}}$ deux à deux premières entre elles.

4.5 Problèmes de diviseurs

Les problèmes de diviseurs sont des problèmes de la forme « déterminer les entiers n vérifiant la condition suivante sur leur diviseurs... ». De tels problèmes sont apparus de plus en plus nombreux ces dernières années, au point de justifier une section à part entière. Cette section est inspirée du cours donné par Maxime Chevalier et Théo Lenoir au stage de Valbonne 2025.

On propose les conseils suivants pour réagir face aux problèmes de diviseurs.

Rassembler les diviseurs par groupe

Comme pour tout ensemble d'objets, il est toujours intéressant de chercher à mettre ces objets par paires ou par triplets pour faire ressortir des propriétés.

Exemple 37. *(Coupe Animath Automne 2022)* Soit n un entier positif impair et k un entier strictement positif. On suppose que le nombre de diviseurs positifs de $2n$ qui sont inférieurs ou égaux à k est impair. Montrer qu'il existe un diviseur d de $2n$ pour lequel $k < d \leqslant 2k$.

Solution. Puisque n est un entier impair, tous ses diviseurs sont également impairs. Notons $d_1, \ldots, d_r$ les diviseurs positifs de n qui sont inférieurs ou égaux à k et supposons par l'absurde que, pour tout i, on ait également $2d_i \leqslant k$.

Les paires $(d_i, 2d_i)$ forment alors une partition de l'ensemble des diviseurs de $2n$ inférieurs ou égaux à k. Mais alors cela signifie que le nombre de diviseurs positifs de $2n$ inférieurs ou égaux à k est pair, ce qui contredit l'hypothèse de l'énoncé.

Il existe donc un indice i tel que $2d_i > k$. Puisque $d_i \leqslant k$, on a $2d_i \leqslant 2k$. Ainsi, l'entier $2d_i$ est un diviseur de $2n$ tel que $k < 2d_i \leqslant 2k$, ce qui est le résultat voulu.

On pourra également regarder l'exercice suivant :

Exercice 4.99. *(OFM 2024 Senior)* Soit p un nombre premier. Déterminer tous les entiers $n \geqslant 1$ avec la propriété suivante : il est possible de partitionner l'ensemble des diviseurs de n en paires (d, d') telles que $d < d'$ et p divise $\left\lfloor \dfrac{d'}{d} \right\rfloor$.

Considérer d et n/d

Il s'agit d'une partition intéressante de l'ensemble des diviseurs. Une fois considéré le diviseur d, on peut effectuer un raisonnement sur le diviseur n/d, qui amène souvent plus d'information. On peut garder en tête que si d_1, d_2, d_3 sont des diviseurs consécutifs de n, alors $n/d_3, n/d_2$ et n/d_1 sont des diviseurs consécutifs de n.

Exemple 38. *(IMO 2023 P1)* Déterminer tous les entiers strictement positifs n composés avec la propriété suivante : si $1 = d_1 < d_2 < \ldots < d_k = n$ sont les diviseurs de n, alors $d_i \mid d_{i+1} + d_{i+2}$ pour tout $1 \leqslant i \leqslant k-2$.

Solution. Montrons qu'il s'agit des puissances de nombres premiers. On vérifie tout d'abord que ces entiers sont bien solutions du problème. En effet, si $n = p^k$ avec p un nombre premier et $k \geqslant 2$, on a $d_i = p^i$ pour $1 \leqslant i \leqslant k$. On vérifie que si $i \leqslant k-2$,

$$d_i = p^i \mid p^{i+1} + p^{i+2} = d_{i+1} + d_{i+2}.$$

Montrons à présent qu'il s'agit des seules solutions. L'idée est que si d_i, d_{i+1} et d_{i+2} sont trois diviseurs consécutifs de n, alors $n/d_{i+2}, n/d_{i+1}$ et n/d_i le sont également.
Plus concrètement, on observe que, comme d_{k-2} divise $d_{k-1} + d_k$ et $n = d_k$, il divise d_{k-1}, donc $d_2 = n/d_{k-1}$ divise $d_3 = n/d_{k-2}$. Ainsi, $d_2 = n/d_{k-1} \mid n/d_{k-2} = d_3$. A partir de là, on peut montrer de proche en proche que $d_2 \mid d_i$ pour tout $i \geqslant 2$, ce que nous faisons ci après par récurrence double.
Initialisation : Celle-ci a déjà été faite au paragraphe précédent, puisqu'on a montré que $d_2 \mid d_3$ et qu'on a déjà que $d_2 \mid d_2$.
Hérédité : Supposons que $d_2 \mid d_{i-1}$ et d_i pour un certain $i \geqslant 3$. D'après la condition de l'énoncé,

$$d_2 \mid d_{i-1} \mid d_i + d_{i+1}.$$

Mais alors puisque $d_2 \mid d_i$, $d_2 \mid d_i + d_{i+1} - d_i = d_{i+1}$. Ceci achève la réccurence.

On conclut que d_2, qui est égal au plus petit facteur premier de n, divise tous les diviseurs de n. Ainsi, n ne peut avoir d'autres facteurs premiers que d_2, sinon ceux-ci seraient divisibles par d_2, ce qui est absurde. Ainsi, n est une puissance de d_2.

On pourra pratiquer cette idée sur l'exercice suivant :

Exercice 4.100. (USAMO 2024 P1) Déterminer tous les entiers $n \geqslant 3$ tels que si l'on note $d_1 < \ldots < d_k$ les diviseurs de $n!$, alors $d_2 - d_1 \leqslant d_3 - d_2 \leqslant \ldots \leqslant d_k - d_{k-1}$.

Employer l'écriture $n = p^\alpha A$

Le conseil le plus surprenant par son efficacité est probablement le suivant. Lorsqu'un problème propose une propriété applicable à n'importe quel diviseur de n, il est bon d'isoler un facteur premier spécifique p et d'écrire n sous la forme $p^\alpha A$, avec A premier avec p. Cette écriture est même préférable à la décomposition complète de n en facteurs premiers, dans la mesure où elle est souvent beaucoup plus lisible. Il s'agit alors d'appliquer l'hypothèse de l'énoncé à des nombres comme p, p^α, A et pA. Bien sûr, on cherchera à distinguer un nombre premier p particulier, comme $p = 2$, $p = 3$ ou encore le plus petit diviseur premier de n.

Exemple 39. *(IMO SL 2024 N1)* Déterminer tous les entiers strictement positifs n vérifiant la propriété suivante : pour tout diviseur positif d de n, $d+1$ est soit un nombre premier, soit un diviseur de n.

Solution. **Réponse :** Les entiers solutions sont $1, 2, 4$ et 12.

Soit n un nombre solution. On dispose d'un entier a et d'un entier impair b tel que $n = 2^a b$. Comme b est un diviseur de n, $b+1$ est soit premier soit un diviseur de $n+1$.

- Si $b+1$ est premier, comme b est impair, $b+1$ est pair donc $b+1=2$ et $n=2^a$. Si $a \geqslant 3$, alors 2^3 est un diviseur de n mais tel que $2^3+1=9$ n'est pas premier et n'est pas un diviseur de n, ce qui contredit l'énoncé. Donc $a<3$, ce qui implique que $\boxed{n=1,2 \text{ ou } 4}$.

  Réciproquement, dans ce cas, tout diviseur d de n vaut 1, 2 ou 4, donc $d+1$ est premier, et n convient.

- Si $b+1$ est un diviseur de n, comme $b+1$ est premier avec b, c'est un diviseur de 2^a, donc on dispose de $c \leqslant a$ tel que $b=2^c-1$. Quitte à retourner au cas précédent, on peut supposer que $b \geqslant 2$ et donc que $c \geqslant 2$, ce qui donne $a \geqslant 2$.

  Si $a=2$, alors $c=2$ et $\boxed{n=12}$. Réciproquement les diviseurs de n étant $1,2,3,4,6,12$ et puisqu'on a $1+1, 2+1, 4+1, 6+1$ et $12+1$ premiers ainsi que $3+1 \mid 12$, 12 est bien solution du problème.

  Si $a \geqslant 3$, alors on montre que $2^{a-1}+1$ et 2^a+1 ne peuvent pas être des diviseurs de n. Puisqu'ils sont impairs, ils doivent diviser 2^c-1. Or $2^a+1>2^c-1$ donc 2^a+1 ne peut pas diviser 2^c-1.
  D'autre part, si $2^{a-1}+1 \mid 2^c-1$, alors $2^c \geqslant 2^{a-1}+2>2^{a-1}$ donc $c \geqslant a$ et $c=a$. Mais $2(2^{a-1}+1)>2^a-1>2^{a-1}+1$ pour $a \geqslant 3$, donc $2^{a-1}+1$ ne peut pas diviser 2^a-1 pour $a \geqslant 3$. Ainsi, 2^a+1 et $2^{a-1}+1$ ne divisent pas n.

  Ils sont donc tous les deux premiers. Or, l'un des deux entiers a et $a-1$ est impair. Notons le $2k+1$, avec $k \geqslant 1$ (puisque $a-1 \geqslant 2$). Mais alors $3=2+1 \mid 2^{2k+1}+1$, et $2^{2k+1}+1>3$ donc ce nombre n'est pas premier, ce qui contredit l'énoncé. Il n'y a donc $\boxed{\text{pas de solution dans ce cas}}$.

On pourra repratiquer cette idée sur les exercices suivants :

Exercice 4.101. (EGMO 2025 P1) Déterminer tous les entiers $N \geqslant 3$ tels que, si on note $c_1<\ldots<c_m$ les entiers strictement positifs premiers avec N et inférieurs à N, alors $\mathrm{PGCD}(N, c_i+c_{i+1}) \neq 1$ pour tout i tel que $1 \leqslant i \leqslant m-1$.

Exercices

Exercice 4.102. (Coupe Animath de Printemps 2020) Déterminer les triplets (m,n,k) d'entiers tels que $m \geqslant 2$, $n \geqslant 2$ et $k \geqslant 3$ et ayant la propriété suivante : m et n ont chacun k diviseurs positifs et, si l'on note $d_1<\ldots<d_k$ les diviseurs positifs de m (avec $d_1=1$ et $d_k=m$) et $d'_1<\ldots<d'_k$ les diviseurs positifs de n (avec $d'_1=1$ et $d'_k=n$), alors $d'_i=d_i+1$ pour tout entier i tel que $2 \leqslant i \leqslant k-1$.

Exercice 4.103. (Roumanie MO 2023) Soit n un entier composé et $1=d_1<d_2<\ldots<d_k=n$ ses diviseurs. On suppose que $d_{i+1}^2 \geqslant d_i d_{i+2}$ pour tout $i \leqslant k-2$.
Montrer que n est la puissance d'un nombre premier.

Exercice 4.104. (EMC 2020 junior) Un entier $k \geqslant 3$ est dit *sympa* s'il existe un entier n et k entiers strictement positifs $d_1<\ldots<d_k$ vérifiant :
- $d_{j+2}=d_j+d_{j+1}$ pour tout $1 \leqslant j \leqslant k-2$,
- les entiers $d_1,\ldots,d_k$ sont des diviseurs de n,
- tout diviseur positif de n autre que les d_i est soit inférieur à d_1 soit supérieur à d_k.

Déterminer tous les entiers sympas.

Exercice 4.105. *(BXMO 2014)* Déterminer tous les entiers n vérifiant la propriété suivante : pour tous diviseurs positifs k, ℓ de n vérifiant $k < n$ et $\ell < n$, l'un au moins des nombres $2k - \ell$ et $2\ell - k$ est également un diviseur (pas forcément positif) de n.

Exercice 4.106. *(BXMO 2016)* Soit n un entier strictement positif. On suppose que ses diviseurs positifs peuvent être répartis par paires de telle sorte que la somme de chaque paire est un nombre premier. Prouver que ces nombres premiers sont tous distincts et qu'aucun d'eux ne divise n.

Exercice 4.107. *(EMC 2025 senior)* Soit $k \geqslant 2$ un entier. Soient $m < n$ deux entiers strictement positifs, premiers entre eux et possédant tous les deux exactement k diviseurs positifs. Pour tout $1 \leqslant i \leqslant k$, on note respectivement f_i et d_i les $i-$èmes plus petits diviseurs de m et n. On suppose que, pour tout indice $i \geqslant 2$,

$$d_i - f_i \mid n - m.$$

Montrer que, pour tout $i \leqslant k/2$, on a $d_i \geqslant f_i$.

Exercice 4.108. *(IMO 2025 P4)* On considère une suite infinie $a_1, a_2, \ldots$ d'entiers strictement positifs telle que chaque a_i possède au moins trois diviseurs propres. Pour tout $n \geqslant 1$, on suppose que a_{n+1} est la somme des trois plus grands diviseurs propres de a_n.
Déterminer toutes les valeurs possibles de a_1.

Exercice 4.109. *(USAMO 2021 P4)* Un ensemble fini S d'entiers strictement positifs possède la propriété que pour tout entier $s \in S$ et tout diviseur d de s, il existe un unique élément t de S tel que $\text{PGCD}(s, t) = d$. Déterminer toutes les valeurs que peut prendre $|S|$.

Exercice 4.110. *(IMO SL 2021 N3)* Trouver tous les entiers $n \geqslant 1$ ayant la propriété suivante : il existe une permutation $d_1, d_2, \ldots, d_k$ des diviseurs positifs de n telle que, pour tout $i \leqslant k$, la somme $d_1 + d_2 + \ldots + d_i$ soit un carré parfait.

Exercice 4.111. *(IMO SL 2024 C2)* On considère une grille carrée de taille $n \times n$ composée de n^2 cases. Pour tout diviseur positif d de n, la *$d-$division* de la grille est définie comme la division de la grille en $(n/d)^2$ sous-grilles carrées, toutes de taille $d \times d$, de sorte que chaque case appartient à exactement une sous-grille.

On dit qu'un entier n est *régulier* s'il est possible d'écrire les entiers $1, 2, \ldots, n^2$ dans les cases de la grille en vérifiant les conditions suivantes :

- chaque case contient exactement un entier,
- chacun des entiers $1, 2, \ldots, n^2$ est écrit dans exactement une case,
- pour tout diviseur d de n tel que $1 < d < n$ et pour toute sous-grille de la $d-$division de la grille, la somme des entiers écrits dans les cases de la sous-grille n'est pas divisible par d.

Déterminer tous les entiers pairs réguliers.

Exercice 4.112. *(RMM SL 2021/France TST 2021-2022)* Étant donnés deux entiers naturels non nuls a et b, on dit que b est a-gréable si, pour toute liste $d_1, d_2, \ldots, d_k$ de diviseurs de b, non nécessairement distincts, telle que

$$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_k} > a,$$

il existe un ensemble I inclus dans $\{1, 2, \ldots, k\}$ tel que

$$\sum_{i \in I} \frac{1}{d_i} = a.$$

L'entier a étant fixé, quels sont les entiers a-gréables ?

Exercice 4.113. *(EMC 2022 senior)* On dit qu'un entier n est *joli* s'il existe un entier k et des entiers non nécessairement distincts $d_1, \ldots d_k$ tels que $n = d_1 d_2 \ldots d_k$ et $d_i^2 \mid n + d_i$ pour tout $1 \leqslant i \leqslant k$.
1) Existe-t-il une infinité d'entiers jolis ?
2) Existe-t-il un carré parfait joli différent de 1 ?

Exercice 4.114. *(EGMO 2024 P3)* Un entier $n \geqslant 1$ est dit *spécial* si, pour tout diviseur d de n, $d(d+1) \mid n(n+1)$. Montrer que si quatre entiers distincts A, B, C et D sont tous spéciaux, alors $\mathrm{PGCD}(A, B, C, D) = 1$.

Exercice 4.115. *(EMO 2026 J2)* Déterminer tous les entiers $n \geqslant 2$ vérifiant la propriété suivante : pour tout diviseur d de n, le produit de tous les autres diviseurs est une puissance parfaite.

5 Pratique

Exercice 5.1. *(St Pétersbourg 2016 grade 9 round 2)* Soient p et q des nombres premiers distincts tels que $p < 2q$ et $q < 2p$. Montrer qu'il existe deux entiers consécutifs tels que le plus grand diviseur premier de l'un d'entre eux est p et le plus grand diviseur premier de l'autre est q.

Exercice 5.2. *(Pologne MO 2010 Round final)* Soit p un nombre premier tel que $p \equiv 2 \mod 3$. Pour tout entier $k \geqslant 1$, on pose $a_k = k^2 + k + 1$. Montrer que $a_1 \dots a_{p-1} \equiv 3 \mod p$.

Exercice 5.3. *(BXMO 2022)* Un sous-ensemble A de $\mathbb{N}$ est dit *convenable* si chaque entier $n > 0$ admet au plus un facteur premier p tel que $n - p \in A$.

1. Montrer que l'ensemble des carrés parfaits est convenable.
2. Donner un ensemble convenable infini et ne contenant aucun carré parfait.

Exercice 5.4. *(Cyberspace Mathematical Competition P2)* On définit la fonction f par $f(x) = 3x^2 + 1$ pour tout entier x. Montrer que, pour tout entier n, le produit

$$f(1)f(2)\dots f(n)$$

possède au plus n diviseurs premiers distincts.

Exercice 5.5. *(Iran MO 2009 Round 2)* Soient $a_1 < \dots < a_n$ des entiers strictement positifs. On suppose que pour toute paire d'entiers (i, j) vérifiant $1 \leqslant i < j \leqslant n$, le nombre $\dfrac{a_i}{a_j - a_i}$ est un entier.
Montrer que pour tous indices $i < j$, $ia_j \leqslant ja_i$.

Exercice 5.6. *(IMO SL 2015 N1)* Déterminer tous les entiers M pour lesquels la suite $a_0, a_1, \dots$ définie par

$$a_0 = M + \frac{1}{2}, \quad \text{et} \quad a_{k+1} = a_k \lfloor a_k \rfloor \quad \text{pour } k = 0, 1, \dots$$

contient au moins un entier.

Exercice 5.7. *(Thaïlande TSTST 2025)* Soient a et b des entiers strictement positifs. Montrer qu'il existe une infinité d'entiers n tels que $a^n + b^n + n!$ n'est pas un carré parfait.

Exercice 5.8. *(MEMO 2018 T7)* Soit $a_1, \dots$ une suite d'entiers strictement positifs telle que $a_1 = 1$ et pour tout $k \geqslant 1$,

$$a_{k+1} = 1 + a_k^3.$$

Montrer que pour tout nombre premier p de la forme $3\ell + 2$, p divise un terme de la suite (a_k).

Exercice 5.9. *(Balkan MO 2018 N2)* Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tous entiers $m, n \geqslant 1$,

$$n! + f(m)! \mid f(n)! + f(m!).$$

Exercice 5.10. *(IMO SL 2024 N2)* Déterminer tous les ensembles $\mathcal{S}$ finis non vides d'entiers strictement positifs ayant la propriété suivante :
Pour tout choix de deux entiers a et b dans $\mathcal{S}$, il existe un entier c dans $\mathcal{S}$ tel que a divise $b+2c$.

Exercice 5.11. *(BXMO 2013)* 1) Déterminer tous les entiers g avec la propriété suivante : pour tout nombre premier p impair, il existe un entier strictement positif n tel que p divise les deux entiers

$$g^n - n \quad \text{et} \quad g^{n+1} - (n+1).$$

2) Déterminer tous les entiers g avec la propriété suivante : pour tout nombre premier p impair, il existe un entier strictement positif n tel que p divise les deux entiers

$$g^n - n^2 \quad \text{et} \quad g^{n+1} - (n+1)^2.$$

Exercice 5.12. *(EMC 2024 P1)* Une paire d'entiers distincts (a, b) est dite *binaire* si $ab+1$ est une puissance de 2. Quel est le plus grand nombre de paires binaires que peut contenir un ensemble S de n entiers strictement positifs ?

Exercice 5.13. *(Vietnam TST 2001)* Soit $a_0 < a_1 < \ldots$ une suite strictement croissante d'entiers strictement positifs. On suppose qu'il existe une constante $C > 0$ telle que, pour tout indice n, $a_{n+1} - a_n < C$. Montrer qu'il existe des indices i et j distincts tels que $a_i \mid a_j$.

Exercice 5.14. *(MEMO 2023 P8)* Soient A et B des entiers strictement positifs. Soit (x_n) la suite définie par

$$x_{n+1} = A \cdot \mathrm{PGCD}(x_n, x_{n-1}) + B.$$

Montrer que la suite (x_n) ne prend qu'un nombre fini de valeurs distinctes.

Exercice 5.15. *(EGMO 2017 P5)* Soit $n \geqslant 2$ un entier. Un $n-$uplet $(a_1, \ldots, a_n)$ d'entiers strictement positifs (pas forcément distincts) est dit *onéreux* s'il existe un entier strictement positif k tel que

$$(a_1 + a_2)(a_2 + a_3) \ldots (a_n + a_1) = 2^{2k-1}$$

1) Trouver tous les entiers $n \geqslant 2$ pour lesquels il existe un $n-$uplet onéreux.
2) Montrer que pour tout entier positif impair m, il existe un entier $n \geqslant 2$ tel que m appartient à un $n-$uplet onéreux.

Exercice 5.16. *(IMO 2020 P5)* On écrit un entier sur chaque carte d'un paquet de $n > 1$ cartes. On suppose que, pour chaque paire de cartes, la moyenne arithmétique des entiers inscrits est égale à la moyenne géométrique des entiers d'un certain nombre de cartes.
Pour quels entiers n les entiers inscrits sur les cartes sont-ils nécessairement égaux ?

Exercice 5.17. *(Chine TST 2019 Day 2 P4)* Existe-t-il un ensemble fini A d'entiers strictement positifs et un ensemble infini B d'entiers strictement positifs vérifiant la condition suivante : les entiers distincts de l'ensemble $S = \{a + b, a \in A, b \in B\}$ sont deux à deux premiers entre eux et, pour tous entiers m et n premiers entre eux, il existe une infinité d'entiers $x \in S$ tels que $x \equiv m \mod n$?

Exercice 5.18. *(N3 2015)* Soient m et n des entiers strictement positifs tels que $m > n$. On pose $x_k = \dfrac{m+k}{n+k}$ pour $k = 1, \ldots, n+1$. Montrer que si les nombres $x_1, \ldots, x_{n+1}$ sont tous entiers, alors $x_1 \ldots x_{n+1} - 1$ admet un diviseur premier impair.

Exercice 5.19. On note $\mathbb{N}^\star$ l'ensemble des entiers strictement positifs. Déterminer toutes les fonctions f de $\mathbb{N}^\star$ dans $\mathbb{Z}$ telles que, pour tout entier $n \in \mathbb{N}^\star$, et pour tout diviseur strictement positif d de n, il existe un diviseur strictement positif e de n tel que n divise $d + f(e)$.

Exercice 5.20. *(N5 2014)* Déterminer tous les triplets d'entiers (p, x, y) tels que p est premier et $x^{p-1} + y$ et $y^{p-1} + x$ sont des puissances de p.

Exercice 5.21. *(IMO SL 2022 N3)* Soit $a \geqslant 2$ et $d \geqslant 2$ deux entiers premiers entre eux. On pose $x_1 = 1$; puis, pour tout entier $k \geqslant 1$, on pose $x_{k+1} = x_k/a$ si a divise x_k, et $x_{k+1} = x_k + d$ sinon. Trouver, en fonction de a et de d, l'entier ℓ maximal pour lequel a^ℓ divise l'un des termes $x_1, x_2, x_3, \ldots$

Exercice 5.22. *(Iran TST 2019 P2, Envoi 2021 P17)* Soit n un entier strictement positif et soient $a, a_1, \ldots, a_n$ des entiers strictement positifs. On suppose que pour tout entier k pour lequel l'entier $ak + 1$ est un carré parfait, au moins l'un des entiers $a_1k + 1, \ldots, a_nk + 1$ est également un carré parfait.
Montrer qu'il existe un indice $1 \leqslant i \leqslant n$ tel que $a = a_i$.

Exercice 5.23. *(EGMO 2026 P6)* Soit p un nombre premier et n un entier strictement positif non divisible par p. On note k le nombre de diviseurs positifs de n et $1 = d_1 < d_2 < \ldots < d_k = n$ ses diviseurs. Pour tout indice $i = 1, 2, \ldots, k$, on note c_i le nombre de diviseurs strictement positifs ℓ de d_i^2 tels que $d_i - \ell$ est divisible par p. Montrer que

$$(p-1)(c_1 + c_2 + \ldots + c_k) \geqslant k^2.$$

Exercice 5.24. *(Chine TSTST 2012 P3)* Soit f une fonction de $\mathbb{N}^\star$ dans $\mathbb{N}^\star$ telle que :

1. si $\mathrm{PGCD}(m, n) = 1$, alors $\mathrm{PGCD}(f(m), f(n)) = 1$,
2. pour tout entier $n \in \mathbb{N}^\star$, $n \leqslant f(n) \leqslant n + 2012$.

Montrer que, pour tout entier $n \geqslant 1$, tout facteur premier de n divise $f(n)$.

Exercice 5.25. *(Entraînement groupe E Valbonne 2025, India IMO training camp 2025)* Soit $k \geqslant 1$, $a_1, \ldots, a_k$ des entiers strictement positifs et P leur produit. On suppose que l'équation

$$n = \sum_{i=1}^{k} \left\lfloor \frac{n}{a_i} \right\rfloor.$$

admet strictement plus de $P/2$ solutions strictement positives. Montrer qu'elle admet au moins P solutions positives.