Arithmétique

Énoncés . . . 2
Petits calculs de restes de lycée . . . 2
Applications des valuations p-adiques . . . 3
Fonctions arithmétiques . . . 5
Quelques nombres remarquables . . . 6
Autour de la division euclidienne et de l'algorithme d'Euclide . . . 8
Factorielles et coefficients binomiaux . . . 10
PGCD et PPCM . . . 12
Congruences . . . 15
Un zeste de polynômes . . . 16
Outils avancés . . . 17
Équations diophantiennes: le cas linéaire . . . 20
Équations diophantiennes: méthodes “réelles« et majoration . . . 20
Équations diophantiennes: réduction modulo n . . . 22
Encore des équations diophantiennes . . . 23
Un peu d'informatique . . . 25
En vrac . . . 27
Indications . . . 29
Solutions . . . 43

Énoncés

Petits calculs de restes de lycée

Exercice 1 (◔☆ Premier petit calcul)
Calculer le reste de la division euclidienne de $2025^{2026^{2027}}$ par 19.

Indication p. 29 · Solution p. 43

Exercice 2 (◔☆ Un peu de repunit)
Soit $a \in \mathbb{N}^*$ un entier premier avec 10.

Montrer qu'il existe un multiple de a dont l'écriture en base 10 ne contient que des 1.

Indication p. 29 · Solution p. 43

Exercice 3 (◔☆ Encore des repunits en base 10)
Montrer qu'excepté 1 il n'existe pas de carré dont l'écriture en base 10 ne contienne que des 1.

Indication p. 29 · Solution p. 43

Exercice 4 (◔★ Critères de divisibilité)
Soit $n \in \mathbb{N}$ et $c_0, c_1, ..., c_r$ les chiffres de l'écriture en base 10 de n.

1. Montrer que n est divisible par 3 ssi $\sum_{k=0}^{r} c_k$ est divisible par 3.
2. Montrer que n est divisible par 11 ssi $\sum_{k=0}^{r} (-1)^k c_k$ est divisible par 11.
3. Déterminer un critère similaire pour la divisibilité par 7.
4. Soit $a \in \mathbb{N}$ premier avec 10.

   Montrer qu'il existe une suite $(\alpha_k)_{k\in\mathbb{N}}$ périodique et indépendante de n telle que n est divisible par a ssi $\sum_{k=0}^{r} \alpha_k c_k$ est divisible par a.

Indication p. 29 · Solution p. 44

Exercice 5 (◔☆ Encore un petit calcul)
Montrer que la somme des cubes de trois nombres consécutifs est toujours divisible par 9.

Indication p. 29 · Solution p. 46

Exercice 6 (◔☆ Juste faire un tableau)
Soit $n \in \mathbb{Z}$ qui n'est divisible ni par 2 ni par 3.

Montrer que 24 divise $n^2 - 1$.

Indication p. 29 · Solution p. 46

Exercice 7 (◔☆ Encore des tableaux peu passionnants)

1. Soit $n \in \mathbb{Z}$. Montrer que parmi n, $n+10$ et $n+14$ exactement un des nombres est divisible par 3.
2. Soit $n \in \mathbb{Z}$. Montrer que parmi n, $2n+1$, et $4n+1$ exactement un des nombres est divisible par 3.
3. Soit $n \in \mathbb{Z}$. Montrer que parmi n, $4n^2+1$ et $6n^2+1$ exactement un des nombres est divisible par 5.

Indication p. 29 · Solution p. 46

Exercice 8 (◔☆ Des trous aussi grands que l'on veut)
Montrer que pour tout $n \in \mathbb{N}$ il existe n entiers consécutifs qui ne sont pas premiers.

Indication p. 30 · Solution p. 47

Exercice 9 (◑☆ Somme des chiffres itérée)
On note pour tout entier $n \in N$, $s_{10}(n)$ la somme des chiffres de l'écriture décimale de n.

Déterminer $s_{10}(s_{10}(s_{10}(s_{10}(s_{10}(2^{2026})))))$.

Indication p. 30 · Solution p. 47

Applications des valuations p-adiques

Exercice 10 (◔★ Caractérisation des racines r-ièmes)
Soit $r \in \mathbb{N}^*$.

Soit $n \in \mathbb{N}^*$.

Montrer que

$$\exists x \in \mathbb{N}, x^r = n \Leftrightarrow \exists x \in \mathbb{Q}, x^r = n.$$

Indication p. 30

Exercice 11 (◔★ Divisibilité et puissances)
Soit $r \in \mathbb{N}^*$.

1. Soit $a \in \mathbb{N}$ et p un nombre premier.

Montrer l'équivalence

$$p \mid a \Leftrightarrow p \mid a^r \Leftrightarrow p^r \mid a^r.$$

2. Soient $a, b \in \mathbb{N}$ deux entiers.

Montrer l'équivalence

$$a \mid b \Leftrightarrow a^r \mid b^r.$$

Indication p. 30

Exercice 12 (◔★ Irrationnalité et logarithme)
Soient a et b deux entiers supérieurs à 2, et premiers entre eux.

Montrer que

$$\frac{\ln(a)}{\ln(b)} \notin \mathbb{Q}.$$

Indication p. 30

Exercice 13 (◔☆ Passage à la limite)
Soient $a, b \in \mathbb{N}^*$.

On suppose que pour tout $n \in \mathbb{N}$, $a^n \mid b^{n+2025}$.

Montrer que $a \mid b$.

Indication p. 30 · Solution p. 48

Exercice 14 (◔☆ Puissances multiples)
Soit $a \in \mathbb{N}$.

Soient $r_1, r_2 \in \mathbb{N}^*$. On suppose qu'il existe $b_1 \in \mathbb{N}$ tel que $a = b_1^{r_1}$ et $b_2 \in \mathbb{N}$ tel que $a = b_2^{r_2}$.

Montrer qu'il existe $b \in \mathbb{N}$ tel que $a = b^{r_1 \vee r_2}$.

Indication p. 30 · Solution p. 48

Exercice 15 (◔☆ Encore une caractérisation des puissances)
Soient $a, b \in \mathbb{N}^*$ premiers entre eux tels que ab est un carré.

Montrer que a et b sont des carrés.

Indication p. 30 · Solution p. 49

Exercice 16 (◑★ Majoration de valuation et combinatoire)
Soient $p_1, ..., p_r$ des nombres premiers distincts.

On note A l'ensemble des entiers dont les seuls facteurs premiers sont dans $\{p_1, ..., p_r\}$.

Montrer que pour tout $N \in \mathbb{N}^*$,

$$|A \cap [\![1, N]\!]| \leq \left(1 + \frac{\ln(N)}{\ln(2)}\right)^r.$$

En déduire une nouvelle preuve de l'existence d'une infinité de nombres premiers.

Indication p. 31

Fonctions arithmétiques

Exercice 17 (◑★♠ Somme de puissances de diviseurs ou décomposition des sigmas)
Pour tout $s \in \mathbb{R}$ on note

$$\begin{aligned} \sigma_s : \mathbb{N}^* &\to \mathbb{R}_+ \\ n &\mapsto \sum_{d|n} d^s. \end{aligned}$$

Par exemple, pour tout entier n, $\sigma_0(n)$ est le nombre de diviseurs de n tandis que $\sigma_1(n)$ est la somme des diviseurs de n.

1. Montrer que pour tous n et m **premiers entre eux**, pour tout $s \in \mathbb{R}$,
$$\sigma_s(nm) = \sigma_s(n)\sigma_s(m).$$
2. Soit $p \in \mathcal{P}$ et $k \in \mathbb{N}$. Exprimer pour tout $s \in \mathbb{R}$, $\sigma_s\left(p^k\right)$ en fonction de p, k et s.
3. Soit $n \in \mathbb{N}^*$. Montrer que
   - ▷ si $s = 0$ alors
   $$\sigma_0(n) = \prod_{p \in \mathcal{P}} \left(\nu_p(n) + 1\right)$$
   - ▷ si $s \neq 0$ alors
   $$\sigma_s(n) = \prod_{p \in \mathcal{P}} \frac{p^{(\nu_p(n)+1)s} - 1}{p^s - 1}$$

Indication p. 31 · Solution p. 49

Exercice 18 (◔★ Caractérisation des carrés par le nombre de diviseurs)
Soit $n \in \mathbb{N}^*$.

Montrer que n est un carré ssi $\sigma_0(n)$ est impair.

Indication p. 31

Exercice 19 (◑☆ Diviseurs et carrés)
Pour tout $n \in \mathbb{N}^*$ on note $\sigma_0(n)$ le nombre de diviseurs de n.

Montrer que

$$\sum_{d|n} \sigma_0(d^2) = \sigma_0(n)^2.$$

Indication p. 31

Quelques nombres remarquables

Exercice 20 (◔★▫ Un peu d'arithmétique des suites de Fibonacci)
On définit une suite $(F_n)_{n\in\mathbb{N}}$ par

$$F_0 = 0$$
$$F_1 = 1$$
$$\forall n \in \mathbb{N}, F_{n+2} = F_{n+1} + F_n.$$

1. ▫ Écrire en Python une fonction `fibo` prenant en argument un entier $n \in \mathbb{N}$ et renvoyant F_n. La complexité devra être linéaire en n.

   Expliquer très brièvement pourquoi pour tout $n \in \mathbb{N}$, $F_n \in \mathbb{N}$.
2. Montrer que

$$\forall n \in \mathbb{N}, F_{n+1} \wedge F_n = 1.$$

(Pour d'autres exercices sur la suite de Fibonacci regarder par exemple les exercices 30 et 83.)

Indication p. 31 · Solution p. 51

Exercice 21 (◔★▫ Nombres de Mersenne)
Soient $a \geq 2$ et $n \geq 2$ des entiers.

1. Montrer que **si** $a^n - 1$ est premier **alors** $a = 2$ et n est premier.
2. ▫ Que dire de la réciproque ?

Indication p. 31 · Solution p. 52

Exercice 22 (◑★▫ Nombres de Fermat)

1. Soit $b \in \mathbb{N}^*$.

Montrer que **si** $2^b + 1$ est premier **alors** il existe $n \in \mathbb{N}$ tel que $b = 2^n$.

Pour $n \in \mathbb{N}$ on pose $F_n = 2^{2^n} + 1$.

1. ▫ Étudier la primalité de F_n pour $n \in [\![0, 6]\!]$.

2. Montrer que

$$\forall (n, m) \in \mathbb{N}^2, n \neq m, F_n \wedge F_m = 1.$$

3. En déduire une nouvelle preuve de l'existence d'une infinité de nombres premiers.

Indication p. 31 · Solution p. 53

Exercice 23 (◔☆▫ Nombres de Carmichael)

Soit $n \geq 2$ un entier. On dit que n est un nombre de Carmichael ssi n est non-premier et pour tout $a \in [\![1, n-1]\!]$ premier avec n, $a^{n-1} \equiv 1[n]$.

1. Commenter l'appellation «pseudo-premier» utilisée parfois pour les nombres de Carmichael.

2. ▫ Écrire une fonction python prenant en argument un entier $n \geq 2$ et renvoyant la valeur de vérité de «n est un nombre de Carmichael».

Indication p. 31

Exercice 24 (◕☆▫ Nombres parfaits)

Un entier $n \in \mathbb{N}^*$ est dit *parfait* ssi il est égal à la somme de ses diviseurs stricts c'est à dire avec les notations de la question 17 ssi $\sigma_1(n) = 2n$.

1. ▫ Déterminer tous les nombres parfaits entre 1 et 10000.

2. Soit $p \in \mathbb{N}$ tel que $2^p - 1$ est premier (cf exercice 21).

Montrer que $2^{p-1}(2^p - 1)$ est parfait.

3. Soit n un nombre parfait pair.

Montrer qu'il existe $p \in \mathbb{N}$ tel que $2^p - 1$ est premier et $n = 2^{p-1}(2^p - 1)$.

Indication p. 32

Exercice 25 (◔★ Infinité de nombres premiers dans certaines progressions arithmétiques I)

1. Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

2. Montrer qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.

Indication p. 32 · Solution p. 55

Exercice 26 (◑★ Infinité de nombres premiers dans certaines progressions arithmétiques II)
Soit p un nombre premier impair.

Montrer que -1 est un carré modulo p ssi $p \equiv 1[4]$.

En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Indication p. 32 · Solution p. 56

Autour de la division euclidienne et de l'algorithme d'Euclide

Exercice 27 (◔★ Un exemple de suite à divisibilité)
Soit $a \in \mathbb{N}$ tel que $a \geq 2$.

On définit

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto a^n - 1 \end{aligned}$$

1. Montrer que

$$f : (\mathbb{N}, |) \to (\mathbb{N}, |)$$

est croissante, c'est à dire que

$$\forall (n, m) \in \mathbb{N}^2, m \mid n \Rightarrow f(m) \mid f(n).$$

2. Soit $(n, m) \in \mathbb{N}^2$ et $(q, r) \in \mathbb{N}^2$ tels que $n = mq + r$.

Montrer que

$$(a^n - 1) \wedge (a^m - 1) = (a^m - 1) \wedge (a^r - 1).$$

3. On munit $\mathbb{N}$ de l'opération $\wedge$.

Montrer que

$$f : (\mathbb{N}, \wedge) \to (\mathbb{N}, \wedge)$$

est un morphisme de monoïde c'est à dire que $f(0) = 0$ et

$$\forall (n, m) \in \mathbb{N}^2, f(n \wedge m) = f(n) \wedge f(m).$$

Indication p. 32 · Solution p. 56

Exercice 28 (◑★ XKCD 2835 - Décomposition en base factorielle)
Soit $n \in \mathbb{N}$.

Montrer qu'il existe une et unique suite $(a_k)_{k\in\mathbb{N}^*}$ nulle à partir d'un certain rang telle que

$$n = \sum_{k=1}^{+\infty} a_k k!$$

et

$$\forall k \in \mathbb{N}^*, a_k \in [\![0, k]\!]$$

Indication p. 32

Exercice 29 (◔★ Décomposition en fractions simples)
Soient $r \in \mathbb{N}^*$ et $(a_1, ..., a_r) \in (\mathbb{N}^*)^r$ des entiers deux à deux premiers entre eux. Soit b un entier.

Montrer qu'il existe $m \in \mathbb{Z}$ et $(x_1, ..., x_r) \in \mathbb{Z}^r$ tels que

$$\frac{b}{\prod_{k=1}^{r} a_k} = m + \sum_{k=1}^{r} \frac{x_k}{a_k}$$

et

$$\forall k \in [\![1, r]\!], \quad 0 \leq x_k \leq a_k - 1.$$

Commenter.

Indication p. 33

Exercice 30 (◑★ Encore de l'arithmétique des suites de Fibonacci)
On définit la suite $(F_n)_{n\in\mathbb{N}}$ comme à l'exercice 20.

1. Montrer que

$$\forall p \geq 1, \forall n \in \mathbb{N}, F_{n+p} = F_p F_{n+1} + F_{p-1} F_n.$$

2. Montrer que

$$\forall (n, m) \in \mathbb{N}^2, F_n \wedge F_m = F_{n\wedge m}.$$

Indication p. 33 · Solution p. 58

Exercice 31 (◕☆ Pleins de premiers entre eux)
Soient α, β deux entiers naturels non nuls premiers entre eux.

Soient n et m deux entiers naturels non nuls premiers entre eux.

- Si n et m sont impairs alors $(\alpha^n + \beta^n) \wedge (\alpha^m + \beta^m) = \alpha + \beta$,
- Sinon,
  - Si α et β sont impairs alors $(\alpha^n + \beta^n) \wedge (\alpha^m + \beta^m) = 2$
  - Sinon $(\alpha^n + \beta^n) \wedge (\alpha^m + \beta^m) = 1$.

Indication p. 33

Exercice 32 (◑☆ Une division euclidienne cachée)
Existe-t-il des $a, b \in \mathbb{N}$ tels que $2^a - 1 \mid 2^b + 1$ et $a > 1$. Si oui, les déterminer.

Indication p. 33

Exercice 33 (◕★ Suite récurrente et Euclide simultané)
Soit $P \in \mathbb{Z}[X]$ (c'est à dire un polynôme à coefficients entiers).

On définit une suite $(a_n)_{n\in\mathbb{N}}$ par

$$a_0 = 0$$
$$\forall k \in \mathbb{N}, a_{k+1} = P(a_k).$$

Montrer que pour tout $(n, m) \in \mathbb{N}^2$,

$$a_n \wedge a_m = |a_{n\wedge m}|.$$

Indication p. 33

Factorielles et coefficients binomiaux

Exercice 34 (◔★♠ Formule de Legendre)
Soit $n \in \mathbb{N}^*$ et p un nombre premier.

Montrer que

$$\nu_p(n!) = \sum_{k=1}^{\left\lfloor \frac{\ln(n)}{\ln(p)} \right\rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Indication p. 34

Exercice 35 (◔☆ Application directe de Legendre)
Par combien de zéros se termine l'écriture décimale de 2025! ?

Indication p. 34

Exercice 36 (◔☆ Un petit coefficient multinomial)
Soient n et m deux entiers naturels. Montrer que

$$\frac{(2n)!\,(2m)!}{n!\,m!\,(n+m)!}$$

est entier.

Indication p. 34

Exercice 37 (◔★♠ Divisibilité des coefficients binomiaux)
Soit p un nombre premier. Montrer que

$$\forall k \in [\![1, p-1]\!],\ p \mid \binom{p}{k}.$$

Indication p. 34

Exercice 38 (◔☆ Encore des coefficients binomiaux)
Soit p un nombre premier.

Montrer que

$$\forall k \in [\![0, p-1]\!], \binom{p-1}{k} \equiv (-1)^k [p].$$

Indication p. 34

Exercice 39 (◔★♠ Formule de Wilson)
Soit $n \geq 2$ un entier.

1. Si $n = p$ est premier alors $(p-1)! \equiv -1[p]$.
2. Si $n > 4$ est composé alors $(n-1)! \equiv 0[n]$.

Indication p. 34 · Solution p. 60

Exercice 40 (◕★▫ Wolstenholme)
Pour tout $n \in \mathbb{N}^*$ on pose

$$H_n = \sum_{k=1}^{n-1} \frac{1}{k} \in \mathbb{Q}$$
$$C_n = \sum_{k=1}^{n-1} \frac{1}{k^2} \in \mathbb{Q}$$

et on note

$$H_n = \frac{a_n}{b_n}, (a_n, b_n) \in \mathbb{Z} \times \mathbb{N}^*, a_n \wedge b_n = 1$$
$$C_n = \frac{c_n}{d_n}, (c_n, d_n) \in \mathbb{Z} \times \mathbb{N}^*, c_n \wedge d_n = 1$$

les représentations comme fractions irréductibles de H_n et C_n.

1. ▫ Déterminer le reste de la division euclidienne de a_p par p^2 pour tout nombre premier $p \in [\![2, 100]\!]$.

   Conjecturer un résultat.
2. ▫ Déterminer le reste de la division euclidienne de c_p par p pour tout nombre premier $p \in [\![2, 100]\!]$.

   Conjecturer un résultat.
3. Démontrer les résultats conjecturés.

Indication p. 34

PGCD et PPCM

Exercice 41 (◔★ Équations en PGCD et PPCM)
Déterminer l'ensemble des solutions de

$$\begin{cases} x \wedge y = 3 \\ x \vee y = 135 \end{cases}$$

d'inconnue $(x, y) \in \mathbb{N}^2$.

Indication p. 35

Exercice 42 (◑☆ Équations en PGCD et PPCM: cas général)
Soient $a, b \in \mathbb{N}$. Déterminer l'ensemble des solutions de

$$\begin{cases} x \wedge y = a \\ x \vee y = b \end{cases}$$

d'inconnue $(x, y) \in \mathbb{N}^2$.

Indication p. 35

Exercice 43 (◔★ Théorème de structure des couples de Bézout)
Soient a et b deux entiers non tous deux nuls. On pose $\tilde{a} = \frac{a}{a \wedge b}$ et $\tilde{b} = \frac{b}{a \wedge b}$.

Soit $n \in \mathbb{Z}$. On considère l'équation

$$au + bv = n \tag{1}$$

d'inconnue $(u, v) \in \mathbb{Z}^2$.

1. Pour $n = 0$ montrer que l'ensemble des solutions de l'équation «homogène» est
$$\mathbb{Z}(\tilde{b}, -\tilde{a}) = \{(k\tilde{b}, -k\tilde{a}), k \in \mathbb{Z}\}.$$
2. Montrer que (1) admet une solution ssi $n \in (a \wedge b)\mathbb{Z}$.
3. Dans le cas où $n \in (a \wedge b)\mathbb{Z}$, on note (u_0, v_0) une solution particulière de (1).

   Montrer que l'ensemble des solutions de (1) est
$$\{(u_0 + k\tilde{b}, v_0 - k\tilde{a}), k \in \mathbb{Z}\}.$$
4. Commenter.

Indication p. 35

Exercice 44 (◔★ Couple de Bézout sous contrainte)
Soient a et b deux entiers tels que $b \neq 0$.

Montrer que pour tout n divisible par $a \wedge b$, il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$\begin{cases} au + bv = n \\ 0 \leq u \leq |b| - 1 \end{cases}.$$

Indication p. 35

Exercice 45 (◔★♣ Quelques règles de calcul)
Soit $(a, b) \in \mathbb{Z}^2$.

1. Montrer que

$$(a \wedge b)(a \vee b) = |ab|.$$

2. Montrer que pour tout $k \in \mathbb{Z}$,

$$(ka) \wedge (kb) = |k|(a \wedge b)$$
$$(ka) \vee (kb) = |k|(a \vee b)$$

3. Montrer que pour tout $n \in \mathbb{N}$,

$$a^n \wedge b^n = (a \wedge b)^n$$
$$a^n \vee b^n = (a \vee b)^n$$

Indication p. 35

Exercice 46 (◔★♠ Distributivité)
Soit $(a, b, c) \in \mathbb{Z}^3$.

Montrer que

$$(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$$

et

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c).$$

Indication p. 35

Exercice 47 (◑☆ Toujours la même idée)
Soit $(a, b, c) \in (\mathbb{Z}^*)^3$.

Montrer que

$$\frac{(a \wedge b \wedge c)^2}{(a \wedge b)(b \wedge c)(c \wedge a)} = \frac{(a \vee b \vee c)^2}{(a \vee b)(b \vee c)(c \vee a)}$$

Indication p. 35

Exercice 48 (◑☆ Encore des règles de calculs peu utiles)
Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge b = 1$.

Montrer que

$$a \wedge (bc) = a \wedge c.$$

Indication p. 35

Congruences

Exercice 49 (◑★♠ Théorème des restes chinois)
Soient $(n_1, n_2) \in (\mathbb{N}^*)^2$ premiers entre eux.

Montrer que pour tout $(y_1, y_2) \in \mathbb{Z}^2$ le système

$$\begin{cases} x \equiv y_1 [n_1] \\ x \equiv y_2 [n_2] \end{cases}$$

admet une solution, et que cette solution est unique modulo $n_1 n_2$.

Indication p. 35

Exercice 50 (◔★ Formulation par les racines n-ièmes)
Soient a et b deux entiers strictement positifs.

1. Montrer que

$$a|b \Leftrightarrow \mathbb{U}_a \subset \mathbb{U}_b.$$

2. Montrer que

$$\mathbb{U}_a \cap \mathbb{U}_b = \mathbb{U}_{a \wedge b}.$$

3. Montrer que

$$\{z_1 \times z_2, (z_1, z_2) \in \mathbb{U}_a \times \mathbb{U}_b\} = \mathbb{U}_{a \vee b}.$$

Indication p. 36

Exercice 51 (◑★♠ Résidus quadratiques)
Soit p un nombre premier différent de 2.

Soit $a \in \mathbb{Z}$. On dit que a est un *résidu quadratique modulo* p ssi il existe $b \in \mathbb{Z}$ tel que $b^2 \equiv a[p]$.

Montrer que pour tout $a \not\equiv 0[p]$, on a

$$a \text{ est un résidu quadratique modulo } p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1[p].$$

Indication p. 36

Exercice 52 (◔★ RSA)
Soient p et q deux nombres premiers distincts.

Soient e et d deux entiers naturels tels que

$$ed \equiv 1[(p-1)(q-1)].$$

Montrer que pour tout entier M on a

$$(M^e)^d \equiv M[pq].$$

Solution p. 61

Exercice 53 (◑★ Théorème des restes chinois: version isomorphisme d'anneau)
Pour $n \in \mathbb{N}^*$ on rappelle que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence modulo n que l'on peut munir de $+$ et $\times$ formant ainsi un anneau commutatif.

Soient $r \in \mathbb{N}^*$ et $n_1, ..., n_r \in \mathbb{N}^*$ deux à deux premiers entre eux. Montrer que les anneaux $\mathbb{Z}/(n_1 n_2 \cdots n_r)\mathbb{Z}$ et $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ sont isomorphes.

Indication p. 36

Un zeste de polynômes

On note $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients entiers.

Exercice 54 (◔★♠ Bernoulli)
Soit $P \in \mathbb{Z}[X]$.

Montrer que

$$\forall (a,b) \in \mathbb{Z}^2, b-a \mid P(b) - P(a).$$

Indication p. 36

Exercice 55 (◔★ Évidemment pas de formule simple)
Déterminer l'ensemble des polynômes $P \in \mathbb{Z}[X]$ tels que

$$\forall n \in \mathbb{N}, P(n) \text{ est premier.}$$

Indication p. 36

Exercice 56 (◔★♠ Petit critère d'Eisenstein)
Soit

$$P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$$

un polynôme à coefficients entiers.

Soit $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $p \wedge q = 1$.

Montrer que

$$P\left(\frac{p}{q}\right) = 0 \Rightarrow (p \mid a_0 \text{ et } q \mid a_n).$$

Indication p. 36

Outils avancés

Exercice 57 (◑★ Convolution de Dirichlet)
On définit l'ensemble des fonctions arithmétiques par $A = \mathcal{F}(\mathbb{N}^*, \mathbb{C})$.

Pour $f, g \in A$ on définit leur convolution de Dirichlet $f * g$ par

$$\forall n \in \mathbb{N}^*, (f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Montrer que $(A, +, *)$ est un anneau commutatif.

Indication p. 37

Exercice 58 (◔☆ LTE light)
Soit $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$ tels que $n \mid a - b$.

Montrer que $n^2 \mid a^n - b^n$.

Indication p. 37

Exercice 59 (◕★ LTE)
Soit p un nombre premier différent de 2, x, y deux entiers tels que $x \neq \pm y$. On suppose de plus $\nu_p(x) = 0$, $\nu_p(y) = 0$ et $\nu_p(x-y) > 0$.

On cherche à démontrer que pour tout entier $n \in \mathbb{N}^*$

$$\nu_p(x^n - y^n) = \nu_p(x-y) + \nu_p(n) \tag{1}$$

1. Soit $n \in \mathbb{N}$ tel que $\nu_p(n) = 0$.

Montrer que pour tout $k \in [\![0, n-1]\!]$,

$$x^k y^{n-1-k} \equiv y^{n-1} [p].$$

En déduire l'égalité (1).

2. Soit $n \in \mathbb{N}$ tel que $\nu_p(n) = 1$.

Montrer que pour tout $k \in [\![1, n-1]\!]$,

$$x^k y^{n-1-k} \equiv y^{n-1} + k(x-y)y^{n-2} [p^2].$$

En déduire l'égalité (1).

3. Soit $n \in \mathbb{N}$.

Montrer l'égalité (1).

Indication p. 37

Exercice 60 (◕★ Formule d'inversion de Moebius)
On définit une fonction $\mu : \mathbb{N}^* \to \mathbb{Z}$ par

$$\forall n \in \mathbb{N}^*, \mu(n) = \begin{cases} 0 & \text{si } n \text{ admet un carré dans sa décomposition en facteurs premiers.} \\ (-1)^d & \text{si } n \text{ est produit de } d \text{ nombres premiers distincts.} \end{cases}$$

Autrement dit, pour $n \in \mathbb{N}^*$ en notant $\mathcal{P}_n = \{p \in \mathcal{P} \mid \nu_p(n) > 0\}$ l'ensemble des diviseurs premiers de n, on a $\mu(n) = 0$ si il existe $p \in \mathcal{P}_n$ tel que $\nu_p(n) \geq 2$, et $(-1)^{|\mathcal{P}_n|}$ sinon.

1. Soit $n \in \mathbb{N}^*$. Calculer $\prod_{p \in \mathcal{P}_n} (1-1)$.

En déduire que

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon.} \end{cases}$$

2. Montrer que la fonction μ est multiplicative, c'est à dire que pour tous $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$, on a $\mu(mn) = \mu(m)\mu(n)$.

3. Soit $f : \mathbb{N}^* \to \mathbb{C}$.

On définit la fonction $g : \mathbb{N}^* \to \mathbb{C}$ par

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} f(d).$$

Montrer la formule d'inversion de Moebius:

$$\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Indication p. 37

Exercice 61 (◕★ Division euclidienne dans les entiers de Gauss)
On rappelle que $\mathbb{Z}[i] = \{a + bi, (a,b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.

Soit $(a,b) \in \mathbb{Z}[i]^2$ tel que $b \neq 0$.

Montrer qu'il existe $(q,r) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ tels que

$$a = bq + r$$
$$|r|^2 < |b|^2$$

Indication p. 37 · Solution p. 62

Équations diophantiennes: le cas linéaire

Exercice 62 (◔★♣ Détermination explicite des couples de Bézout)
Soient a et b premiers entre eux et $n \in \mathbb{N}$. Déterminer l'ensemble des solutions de l'équation

$$ax + by = n$$

d'inconnue $(x, y) \in \mathbb{Z}^2$.

Indication p. 38

Exercice 63 (◔★ Un cas particulier de Bézout positif)
Déterminer l'ensemble des $n \in \mathbb{N}$ tels que l'équation

$$5x + 2y = n$$

admette au moins une solution avec x et y des entiers **positifs**.

Indication p. 38

Exercice 64 (◑★ Cas général)
Soient a et b deux entiers naturels premiers entre eux.

1. Montrer que pour tout $n \geq ab - a - b + 1$ l'équation

   $$ax + by = n$$

   admet au moins une solution $(x, y) \in \mathbb{N}^2$.
2. Montrer que pour $n = ab - a - b$ l'équation

   $$ax + by = n$$

   n'admet pas de solution avec $(x, y) \in \mathbb{N}^2$.

Équations diophantiennes: méthodes "réelles« et majoration

Exercice 65 (◔☆ Pourquoi réfléchir quand on peut trinomer)
Déterminer les entiers n tels que

$$7n^2 - n^4 = 12.$$

Indication p. 38 · Solution p. 64

Exercice 66 (◑★ Majorations successives)

1. Déterminer les couples $(a,b) \in (\mathbb{N}^*)^2$ solutions de

$$\frac{1}{a} + \frac{1}{b} = 1.$$

2. Déterminer les triplets $(a,b,c) \in (\mathbb{N}^*)^3$ solutions de

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1.$$

Indication p. 38 · Solution p. 64

Exercice 67 (◔★ Étude de fonction)

Déterminer tous les entiers strictement positifs a et b tels que

$$a^b = b^a.$$

Indication p. 38 · Solution p. 66

Exercice 68 (◔☆ Une identité de Sophie Germain)

Déterminer l'ensemble des $(n,m) \in (\mathbb{N}^*)^2$ tels que

$$n^4 + 4m^4$$

est premier.

Indication p. 38

Exercice 69 (◕★ Une question du CG 1990)

Déterminer les entiers $n \in \mathbb{N}^*$ tels que l'équation

$$\sum_{k=1}^{n} \frac{1}{x_k^2} = 1$$

admette une solution $(x_1, ..., x_n) \in (\mathbb{N}^*)^n$.

Indication p. 38 · Solution p. 68

Exercice 70 (◔☆ Équations en vrac)

1. Déterminer tous les entiers positifs n et m tels que

$$n^4 - m^4 = 42.$$

2. Déterminer l'ensemble des entiers naturels n tels que $5^n + 4$ est un carré.

Indication p. 39 · Solution p. 71

Équations diophantiennes: réduction modulo n

Exercice 71 (◑★ Réduction donc impossibilité)

1. Montrer que l'équation

$$a^2 + b^2 = 2023$$

n'admet pas de solution.

2. Montrer que l'équation

$$a^5 - 2b^2 = 528$$

n'admet pas de solutions.

3. Montrer que l'équation

$$a^5 - 2b^2 = 110007$$

n'admet pas de solutions.

Indication p. 39 · Solution p. 71

Exercice 72 (◔★ Une question du Bac 2003)

Déterminer tous les entiers positifs x, y et z solutions de

$$x^2 + y^2 = 7z^2.$$

Indication p. 39 · Solution p. 73

Exercice 73 (◕★ Lemme d'Hensel)

Soit $P \in \mathbb{Z}[X]$, $p \in \mathcal{P}$ un nombre premier.

Soit $a \in \mathbb{Z}$ tel que $P(a) \equiv 0[p]$ et $P'(a) \not\equiv 0[p]$ (c'est à dire une racine simple modulo p).

Montrer que pour tout $n \in \mathbb{N}$ il existe un entier $x \in \mathbb{Z}$ tel que $x \equiv a[p]$ et $P(x) \equiv 0[p^n]$.

Indication p. 39

Exercice 74 (●☆ Un contre-exemple au principe général de réduction modulaire)
On considère le polynôme

$$P = (X^2 - 2)(X^2 - 17)(X^2 - 34)$$

Montrer que P n'admet pas de racine entière mais que pour tout $n \in \mathbb{N}$ il existe $a \in \mathbb{Z}$ tel que $P(a) \equiv 0[n]$.

Indication p. 39

Encore des équations diophantiennes

Exercice 75 (◑★ Paramétrisation des triplets pythagoriciens)
On appelle *triplet pythagoricien* tout triplet $(a, b, c) \in (\mathbb{N}^*)^3$ tel que

$$a^2 + b^2 = c^2.$$

Montrer que, à l'échange de a et b près, l'ensemble des triplets pythagoriciens est

$$\Big\{(k(m^2 - n^2), 2kmn, k(m^2 + n^2)), (k, m, n) \in (\mathbb{N}^*)^3, m > n\Big\}.$$

Indication p. 39

Exercice 76 (◔☆ Petite translation)
Soit p un nombre premier.

Montrer que l'équation

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{p}$$

d'inconnue $(a, b) \in (\mathbb{N}^*)^2$ admet exactement 3 solutions.

Indication p. 40

Exercice 77 (◔☆ Petite puissance de 2)
Déterminer l'ensemble des entiers positifs a et b tels que

$$3^a = 2^b + 1.$$

Indication p. 40

Exercice 78 (◔☆ Petite division)
Déterminer l'ensemble des entiers positifs a et b tels que

$$a^2 + b^2 = (ab)^2.$$

Indication p. 40

Exercice 79 (◑☆ Encore des majorations)
Déterminer tous les entiers $n \in \mathbb{N}$ tels que $2^n \mid 3^n - 1$.

Indication p. 40

Exercice 80 (◉☆ L'exemple le plus connu de «saut de Viète»)

1. Pour $k \in \mathbb{N}$ on note E_k l'équation

$$x^2 - kxy + y^2 = k$$

d'inconnue $(x, y) \in \mathbb{N}^2$.

Soit $(a, b) \in \mathbb{N}^2$. Montrer que si (a, b) est solution de E_k alors $\left(b, \frac{b^2-k}{a}\right)$ est aussi solution de E_k.

2. Soient $a, b \in \mathbb{N}$. Montrer que

$$\frac{a^2+b^2}{ab+1} \text{ est entier } \implies \frac{(a^2+b^2)}{ab+1} \text{ est un carré parfait}$$

.

Indication p. 40

Un peu d'informatique

Exercice 81 (◑★□ Crible mystère I)
On considère la fonction `mystere1` suivante

```python
def mystere1(N):
    """Fonction mystere et donc sans documentation…"""
    lp = []  # Nom peu expressif, à éviter
    ppdp = [i for i in range(N + 1)]  # Nom peu expressif, à éviter
    i = 2
    while i <= N:
        if ppdp[i] == i:
            lp.append(i)
        j = 0
        while j < len(lp) and lp[j] <= ppdp[i] and i * lp[j] <= N:
            ppdp[i * lp[j]] = lp[j]
            j = j + 1
        i = i + 1
    return lp, ppdp

```

1. Étant donné un entier $N \geq 2$ que renvoie `mystere1`(N) ?
2. Déterminer en fonction de N la complexité de la fonction.
3. Commenter.

Indication p. 40 · Solution p. 74

Exercice 82 (◑☆□ Crible mystère II)
On considère la fonction `mystere2` suivante

```python
def mystere2(N):
    """Fonction mystere et donc sans documentation…"""
    lp = []  # Nom peu expressif, à éviter
    pgdp = [i for i in range(N + 1)]  # Nom peu expressif, à éviter
    i = 2
    while i <= N:
        if pgdp[i] == i:
            lp.append(i)
            k = 1
            while i * k <= N:
                pgdp[i * k] = i
                k = k + 1
        i = i + 1
    return lp, pgdp

```

1. Étant donné un entier $N \geq 2$ que renvoie `mystere2`(N) ?
2. Déterminer en fonction de N la complexité de la fonction.

Indication p. 40 · Solution p. 76

Exercice 83 (◔★▫ Complexité de l'algorithme d'Euclide)

1. Rappeler l'algorithme d'Euclide pour le calcul du pgcd de deux entiers naturels.
2. Pour $n \in \mathbb{N}$ on note F_n le n-ième nombre de Fibonacci (cf exercice 20).

   Déterminer la complexité (en fonction de n) du calcul de $F_{n+1} \wedge F_n$ par algorithme d'Euclide.
3. Commenter.

Indication p. 40

Exercice 84 (◔☆▫ Autour du Projet Euler 37)

Une suite finie de chiffres (en base 10) $c_1, c_2, ..., c_r$ est dite première par troncature à droite ssi pour tout $j \in [\![1, r]\!]$ le nombre $\overline{c_1 c_2 \cdots c_j}$ est premier.

Par exemple la suite de chiffres $7, 1, 9, 3, 3, 3$ est une suite première par troncature à droite car

- ▹ 7 est premier,
- ▹ 71 est premier,
- ▹ 719 est premier,
- ▹ 7193 est premier,
- ▹ 71933 est premier,
- ▹ 719333 est premier.
- ▹ (mais pour tout $c \in [\![0, 9]\!]$, $719333c$ n'est pas premier.)

Montrer qu'il n'existe qu'un nombre fini de suites de chiffres premières par troncature à droite.

Il est conseillé de s'aider des résultats d'un programme python.

Indication p. 41

Exercice 85 (◑☆▫ Projet Euler 72)

Pour $n \in \mathbb{N}^*$ on note $f(n)$ le nombre de fractions irréductibles strictement comprises entre 0 et 1 et de dénominateur inférieur ou égal à n.

Par exemple les fractions irréductibles dans $]0, 1[$ et de dénominateur inférieur ou égal à 8 sont $\frac{1}{8}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{3}{8}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{5}{8}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{7}{8}$ et donc $f(8) = 21$.

1. Écrire une fonction Python prenant en argument un entier n et renvoyant $f(n)$. La complexité devra être au plus en $O(n^2 \ln(n))$.
2. Écrire une fonction Python prenant en argument un entier n et renvoyant $f(n)$. La complexité devra être au plus en $O\left(n^{\frac{3}{2}}\right)$.

En vrac

Exercice 86 (◔★ De l'art de choisir ses tiroirs)
Soit $n \in \mathbb{N}$ et $(a_1, ..., a_{n+1}) \in [\![1, 2n]\!]^{n+1}$ deux à deux distincts.

1. Montrer qu'il existe $i, j \in [\![1, n+1]\!]$ distincts tels que $a_i \wedge a_j = 1$.
2. Montrer qu'il existe $i, j \in [\![1, n+1]\!]$ distincts tels que $a_i \mid a_j$.

Indication p. 41

Exercice 87 (◑★ Somme des puissances modulo p)
Soit p un nombre premier et $m \in \mathbb{N}$.

Montrer que **si** $m \not\equiv 0[p-1]$ alors

$$\sum_{k=0}^{p-1} k^m \equiv 0[p].$$

Indication p. 41

Exercice 88 (◔☆ Juste parité et moyenne)
Existe-t-il deux nombres premiers *consécutifs* dont la somme est le produit d'exactement deux nombres premiers ?

Indication p. 41

Exercice 89 (◔☆ Bernoulli itéré)
Montrer que pour tout entier $n \geq 1$ et tout entier a impair on a

$$a^{2^n} \equiv 1[2^{n+2}].$$

Indication p. 41 · Solution p. 76

Exercice 90 (◕☆ Travailler puis plein de disjonctions de cas)
Déterminer tous les entiers strictement positifs a, b, c tels que

$$a \mid bc - 1$$
$$b \mid ac - 1$$
$$c \mid ab - 1.$$

Indication p. 41

Exercice 91 (◕☆ P1 2017)
Soit $a_0 \in \mathbb{N}$.

On considère la suite $(a_n)_{n\in\mathbb{N}}$ définie par

$$a_0 = a_0$$
$$\forall n \in \mathbb{N}, a_{n+1} = \begin{cases} \sqrt{a_n} & \text{si } a_n \text{ est un carré parfait} \\ a_n + 3 & \text{sinon} \end{cases}.$$

Expliciter une partition (P, I) de $\mathbb{N}$ telle que
- ▷ Si $a_0 \in P$ alors $(a_n)_{n\in\mathbb{N}}$ est périodique à partir d'un certain rang.
- ▷ Si $a_0 \in I$ alors $a_n \sim 3n$ lorsque $n \to +\infty$ (c'est à dire $\lim_{n\to+\infty} \frac{a_n}{n} = 3$).

Indication p. 41

Indications

Indication 1 · Énoncé p. 2 (Premier petit calcul)
Remarquer que pour tous a, b entiers la suite des restes de la division euclidienne de a^n par b est périodique (à partir d'un certain rang).

Solution p. 43

Indication 2 · Énoncé p. 2 (Un peu de repunit)
Avec $r_n = \underbrace{111\cdots111}_{n \text{ fois}}$ on montre par tiroirs qu'il existe (n, m) tel que $r_n - r_m$ divisible par a.

Solution p. 43

Indication 3 · Énoncé p. 2 (Encore des repunits en base 10)
Face à un carré, au cas où, regarder modulo 4.

Solution p. 43

Indication 4 · Énoncé p. 2 (Critères de divisibilité)
Écrire $n = \sum_{k=0}^{r} c_k 10^k$ d'où en particulier $a \mid n$ ssi $\sum_{k=0}^{r} c_k 10^k \equiv 0[a]$.

Comme 10 est inversible modulo a, la suite 10^k est périodique modulo a.

Solution p. 44

Indication 5 · Énoncé p. 2 (Encore un petit calcul)
Développer et factoriser ou bien dresser la table des cubes modulo 9.

Solution p. 46

Indication 6 · Énoncé p. 3 (Juste faire un tableau)
Juste faire un tableau de congruence.

Solution p. 46

Indication 7 · Énoncé p. 3 (Encore des tableaux peu passionnants)
Juste faire des tableaux de congruences.

Solution p. 46

Indication 8 · Énoncé p. 3 (Des trous aussi grands que l'on veut)
Les construire, par exemple avec des factorielles.

Solution p. 47

Indication 9 · Énoncé p. 3 (Somme des chiffres itérée)
D'un point de vue algorithmique remarquer:

- un **invariant**: la congruence modulo 9,
- un **variant**: la «taille», a priori $s_{10}(n)$ est bien plus petit que n.

Solution p. 47

Indication 10 · Énoncé p. 3 (Caractérisation des racines r-ièmes)
Un sens est immédiat.

Dans l'autre sens, remarquer que si $x = \frac{a}{b}$ est une fraction irréductible (où $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$) alors $x^r = n$ ssi $a^r = nb^r$.

Passer aux valuations p-adiques pour un nombre premier p.

Indication 11 · Énoncé p. 4 (Divisibilité et puissances)
Lemme d'Euclide (ou de Gauss).

Ou bien plus simplement valuation p-adique.

Indication 12 · Énoncé p. 4 (Irrationnalité et logarithme)
Passer à l'exponentielle puis aux valuations p-adiques.

Indication 13 · Énoncé p. 4 (Passage à la limite)
Prendre les valuations p-adiques, diviser par n et passer à la limite.

Solution p. 48

Indication 14 · Énoncé p. 4 (Puissances multiples)
Passer aux valuations p-adiques.

Solution p. 48

Indication 15 · Énoncé p. 5 (Encore une caractérisation des puissances)
Une somme est divisible par 2 et l'un des termes vaut 0.

Solution p. 49

Indication 16 · Énoncé p. 5 (Majoration de valuation et combinatoire)
Remarque si $n \leq N$, alors pour tout p premier, $v_p(n) \leq \frac{\ln(N)}{\ln(p)} \leq \frac{\ln(N)}{\ln(2)}$.

Indication 17 · Énoncé p. 5 (Somme de puissances de diviseurs ou décomposition des sigmas)

1. Si n et m sont premiers entre eux alors tout diviseur de nm s'écrit de manière unique comme produit d'un diviseur de n et d'un diviseur de m.

   Écrire la somme sur $\mathcal{D}(nm)$ comme une somme double sur $\mathcal{D}(n) \times \mathcal{D}(m)$.
2. On a $\sigma_s(p^k) = \sum_{j \leq k} (p^j)^s$. Distinguer selon $s = 0$ ou $s \neq 0$.
3. Écrire n comme produit de ses facteurs premiers.

Solution p. 49

Indication 18 · Énoncé p. 6 (Caractérisation des carrés par le nombre de diviseurs)
Utiliser par exemple l'exercice 17.

Indication 19 · Énoncé p. 6 (Diviseurs et carrés)
Commencer par traiter l'exercice 17.

Au choix montrer la propriété pour $n = p^k$ puis utiliser la multiplicativité de σ_0 ou bien utiliser la formule de l'exercice 17 pour $s = 0$.

Indication 20 · Énoncé p. 6 (Un peu d'arithmétique des suites de Fibonacci)

1. Pour le script python travailler sur le couple (F_{n+1}, F_n).

   Par récurrence.
2. Par récurrence et algorithme d'Euclide.

Solution p. 51

Indication 21 · Énoncé p. 6 (Nombres de Mersenne)
Bernoulli.

Solution p. 52

Indication 22 · Énoncé p. 7 (Nombres de Fermat)
Écrire une relation de récurrence de la forme $F_n = \prod_{k=0}^{n-1} F_k + 2$ ou $F_{n+b} = (F_n - 1)^{2^b} + 1$.

Solution p. 53

Indication 23 · Énoncé p. 7 (Nombres de Carmichael)

1. Cf petit théorème de Fermat.
2. Pour vérifier les premiers nombres de Carmichael sont 561, 1105 et 1729..

Indication 24 · Énoncé p. 7 (Nombres parfaits)

1. On obtient 6, 28, 496 et 8128.
2. Utiliser la multiplicativité de σ_1 et le fait que $2^p - 1$ est premier.
3. Écrire $n = 2^{p-1}m$ avec m impair et $p \geq 2$.

   Constater que $(2^p - 1)\sigma_1(m) = 2^p m$.

   Par Gauss il existe q tel que $m = q(2^p - 1)$.

   Il reste ensuite à réinjecter pour montrer $q = 1$.

Indication 25 · Énoncé p. 7 (Infinité de nombres premiers dans certaines progressions arithmétiques I)

1. Remarquer qu'un nombre premier impair est congru à 1 ou 3 modulo 4 et que $1 \times 1 \not\equiv 3[4]$.
2. Remarquer qu'un nombre premier plus grand que 5 est congru à 1 ou 5 modulo 6 et que $1 \times 1 \not\equiv 5[6]$.

Solution p. 55

Indication 26 · Énoncé p. 8 (Infinité de nombres premiers dans certaines progressions arithmétiques II)
Il s'agit d'un cas particulier de l'exercice 51.

Adapter la preuve d'Euclide à $(2p_1 \cdots p_r)^2 + 1$.

Solution p. 56

Indication 27 · Énoncé p. 8 (Un exemple de suite à divisibilité)

1. Bernoulli
2. $a^n - 1 = a^r a^{mq} - a^r + a^r - 1$
3. faire simultanément l'algorithme d'Euclide sur (n, m) et $(a^n - 1, a^m - 1)$.

Solution p. 56

Indication 28 · Énoncé p. 9 (XKCD 2835 - Décomposition en base factorielle)
Raisonner par analyse-synthèse.

Comme pour une décomposition en base b, a_1 est le reste de la division euclidienne de n par 2.

Puis a_2 est le reste de la division euclidienne de $\frac{1}{2}(n - a_1)$ par 3, etc.

Remarque: lien vers la référence: https://xkcd.com/2835/

Indication 29 · Énoncé p. 9 (Décomposition en fractions simples)
On peut soit montrer que les $\prod_{j\neq k} a_j$ sont premiers entre eux et bézouter ou bien procéder par récurrence.

Dans ce dernier cas, à l'aide de l'exercice 44 montrer que si a_1, a_2 sont premiers entre eux alors pour tout b il existe $(x_1, s_2) \in \mathbb{Z}^2$ tels que

$$\frac{b}{a_1 a_2} = \frac{x_1}{a_1} + \frac{s_2}{a_2}$$
$$0 \leq x_1 \leq a_1 - 1$$

On peut commenter:
- ▹ L'unicité.
- ▹ La généralisation sous la forme

$$\frac{b}{\prod_{p\in\mathcal{P}} p^{\nu_p(a)}} = m + \sum_{p\in\mathcal{P}} \sum_{k=1}^{\nu_p(a)} \frac{x_{p,k}}{p^k}$$

  où les $x_{p,k}$ entre 0 et $p-1$.
- ▹ La généralisation à $\mathbb{K}[X]$ au lieu de $\mathbb{Z}$: il s'agit de la décomposition en éléments simples (cf SI ou cours de mathématiques dédié).

Indication 30 · Énoncé p. 9 (Encore de l'arithmétique des suites de Fibonacci)
1. Par récurrence sur p.
2. Par exemple reparamétrer en $F_{n+p} \wedge F_n = F_{n+p\wedge n}$ et procéder par récurrence.

Solution p. 58

Indication 31 · Énoncé p. 10 (Pleins de premiers entre eux)
Poser pour tout $n \in \mathbb{N}$, $a_n = \alpha^n + \beta^n$.

Constater que pour tout $m \geq 2n$, $a_n a_{m-n} = a_m + (\alpha\beta)^n a_{m-2n}$.

Procéder alors à un algorithme d'Euclide simultané.

Indication 32 · Énoncé p. 10 (Une division euclidienne cachée)
Avec la division euclidienne $b = aq + r$ constater que $2^b + 1 = 2^r(2^{aq} - 1) + (2^r + 1)$.

Indication 33 · Énoncé p. 10 (Suite récurrente et Euclide simultané)
S'inspirer des exercices précédents.

Par exemple pour $k \in \mathbb{N}$, pour tout n on a $a_{n+k} = \underbrace{P \circ P \circ \cdots \circ P}_{k \text{ fois}}(a_n)$ et en particulier (comme pour tout polynôme R à coefficients entiers $R(a_n) \equiv R(0)\,[a_n]$), on a une écriture de la forme

$$a_{n+k} = a_n q_{n,k} + a_k.$$

Procéder par algorithme d'Euclide simultané.

Indication 34 · Énoncé p. 10 (Formule de Legendre)
Faire un schéma.

Remarquer aussi qu'étant donné $a \in \mathbb{N}^*$ et $n \in \mathbb{N}$ le nombre d'entiers dans $[\![1, n]\!]$ divisibles par a est $\left\lfloor \frac{n}{a} \right\rfloor$.

Indication 35 · Énoncé p. 11 (Application directe de Legendre)
Il suffit de calculer $\min(\nu_2(2025!), \nu_5(2025!))$, et pour calculer ces valuations utiliser la formule de Legendre (exercice 34).

Indication 36 · Énoncé p. 11 (Un petit coefficient multinomial)
Réfléchir à une interprétation combinatoire, ou utiliser immédiatement la formule de Legendre (exercice 34).

Indication 37 · Énoncé p. 11 (Divisibilité des coefficients binomiaux)
Plusieurs méthodes possibles.

Par exemple formule de la capitaine puis Gauss.

Ou de manière plus abstraite remarquer que dans $\mathbb{Z}/p\mathbb{Z}[X]$ on a $(X+1)^p = X^p + 1$ et utiliser le binôme de Newton.

Indication 38 · Énoncé p. 11 (Encore des coefficients binomiaux)
Commencer par traiter l'exercice 37

Indication 39 · Énoncé p. 11 (Formule de Wilson)

1. Regrouper les termes deux à deux.
2. Si n n'est pas le carré d'un nombre premier, regrouper deux termes dont le produit est n.

   Si $n = p^2$ remarquer que $n \mid p \times (2p)$.

Solution p. 60

Indication 40 · Énoncé p. 12 (Wolstenholme)

1. On conjecture que, pour $p \geq 5$, $a_p \equiv 0[p^2]$.
2. On conjecture que, pour $p \geq 5$, $c_p \equiv 0[p]$.
3. Cela revient à étudier

$$\sum_{k=1}^{p-1} \prod_{j \neq k} j$$

modulo p^2 et

$$\sum_{k=1}^{p-1} \left(\prod_{j \neq k} j \right)^2$$

modulo p

Remarquer que cela ressemble très fortement à des relations coefficients racines pour le polynôme

$$(X-1)(X-2)\cdots(X-(p-1))$$

qui est égal dans $\mathbb{Z}/pZ$ à

$$X^{p-1}-1.$$

Indication 41 · Énoncé p. 12 (Équations en PGCD et PPCM)
Plusieurs méthodes. Par exemple regarder les valuations p-adiques. Ou encore poser $d = x \wedge y$ et écrire $x = d\tilde{x}$, $y = d\tilde{y}$ et l'équation sur $\tilde{x}, \tilde{y}$.

Indication 42 · Énoncé p. 13 (Équations en PGCD et PPCM: cas général)
De même que pour 41.

Indication 43 · Énoncé p. 13 (Théorème de structure des couples de Bézout)

1. Si $au + bv = 0$ en simplifiant par $a \wedge b$ on obtient $u\tilde{a} = -v\tilde{b}$. Utiliser ensuite Gauss.
2. Cours (définition du pgcd).
3. On a (u, v) solution de l'équation ssi $(u - u_0, v - v_0)$ solution de l'équation homogène.
4. Plein de commentaires possibles. Par exemple le lien avec tous les théorèmes de structures déjà étudiés. Ou que comme une solution est algorithmiquement calculable par algorithme d'Euclide étendu, toutes les solutions le sont.

   Ou encore une interprétation géométrique (intersection de droites et du réseau $\mathbb{Z}^2$).

Indication 44 · Énoncé p. 13 (Couple de Bézout sous contrainte)
Écrire l'ensemble des solutions de $au + bv = n$ à l'aide de l'exercice 43

Prendre celle minimisant u tout en étant positive.

Indication 45 · Énoncé p. 14 (Quelques règles de calcul)
Utiliser les valuations p-adiques.

Indication 46 · Énoncé p. 14 (Distributivité)
Utiliser les valuations p-adiques.

Indication 47 · Énoncé p. 14 (Toujours la même idée)
Passer aux valuations p-adiques.

Indication 48 · Énoncé p. 15 (Encore des règles de calculs peu utiles)
Utiliser par exemple les valuations p-adiques.

Ou bien se ramener à $a \wedge c = 1$.

Indication 49 · Énoncé p. 15 (Théorème des restes chinois)
Pour l'unicité étudier le système homogène.

Pour l'existence par exemple se ramener aux cas $(1,0)$ et $(0,1)$.

Indication 50 · Énoncé p. 15 (Formulation par les racines n-ièmes)
Comme tous les exercices de racines n-ièmes se rappeler qu'il y a **deux** définitions possibles: celles par extension et celle par compréhension.

Et comme tous les exercices de pgcd, se rappeler de Bézout.

Indication 51 · Énoncé p. 16 (Résidus quadratiques)
Commencer par remarquer que $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1[p]$ et donc par intégrité $a^{\frac{p-1}{2}} \equiv \pm 1[p]$.

Montrer ensuite une inclusion et conclure sur l'égalité par calcul des cardinaux.

Remarque: on définit souvent le symbole de Legendre $\left(\frac{a}{p}\right)$ par 0 si $p \mid a$, 1 si a est un résidu quadratique modulo p et -1 sinon. On a alors $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$.

Déterminer les résidus quadratiques modulo p est donc équivalent à déterminer les valeurs du symbole de Legendre.

Par exemple les règles des signes sont les règles usuelles.

La loi de réciprocité quadratique permet de plus de relier $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$. Si p et q sont deux nombres premiers impairs distincts, alors

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

Indication 53 · Énoncé p. 16 (Théorème des restes chinois: version isomorphisme d'anneau)
Par récurrence en utilisant l'exercice 49.

Indication 54 · Énoncé p. 16 (Bernoulli)
Bernoulli.

Indication 55 · Énoncé p. 17 (Évidemment pas de formule simple)
Les polynômes constants avec comme constante un nombre premier conviennent.

Montrons que ce sont les seuls. Soit P un tel polynôme.

On a a_0 est premier. De plus pour tout $k \in \mathbb{N}$, $a_0 \mid P(ka_0)$ et donc $P(ka_0) = a_0$.

Donc P coïncide avec a_0 une infinité de fois.

Indication 56 · Énoncé p. 17 (Petit critère d'Eisenstein)
Réécrire $P\left(\frac{p}{q}\right) = 0$ comme

$$\sum_{k=0}^{n} a_k p^k q^{n-k} = 0$$

c'est à dire

$$a_0 q^n + p\left(\sum_{k=1}^{n} a_k p^{k-1} q^{n-k}\right) = 0$$

ou encore

$$\left(\sum_{k=0}^{n-1} a_k p^k q^{n-k-1}\right) q + a_n p^n = 0.$$

Indication 57 · Énoncé p. 17 (Convolution de Dirichlet)
Les points non automatiques sont les suivants:

- ▷ Montrer que $*$ est commutatif.
- ▷ Montrer que $*$ est associatif.
- ▷ Montrer que $*$ admet un élément neutre.

Pour les deux premiers points constater que pour tout $n \in \mathbb{N}^*$,

$$(f * g)(n) = \sum_{\substack{p,q \\ pq=n}} f(p)g(q)$$

et pour le neutre considérer le Dirac $\delta_0 : n \mapsto \delta_{n,1}$.

Indication 58 · Énoncé p. 17 (LTE light)
Bernoulli. D'un côté $a - b$ est divisible par n. De l'autre côté une somme de n termes tous égaux modulo n.

Indication 59 · Énoncé p. 18 (LTE)

1. On a $x \equiv y[p]$, d'où $x^{n-1-k} \equiv y^{n-1-k}[p]$.

Utiliser Bernoulli et utiliser $\sum_{k=0}^{n-1} x^k y^{n-1-k} \equiv nx^{n-1}[p]$.

2. On a $x^k = (y + (x-y))^k = y^k + k(x-y)y^{k-1} + \cdots$ avec les termes suivants divisibles par $(x-y)^2$ donc par p^2.

D'où par $\sum_{k=0}^{n-1} x^k y^{n-1-k} \equiv 0[p]$ et $\sum_{k=0}^{n-1} x^k y^{n-1-k} \equiv ny^{n-1} + \frac{n(n-1)}{2}(x-y)y^{n-2} \equiv ny^{n-1} \not\equiv 0[p^2]$ car $p \mid \frac{n(n-1)}{2}$.

3. Procéder par récurrence sur $\nu_p(n)$, en remarquant que si $n = ab$ alors $x^n - y^n = \left((x^a)^b - (y^a)^b\right)$.

Indication 60 · Énoncé p. 19 (Formule d'inversion de Moebius)

1. Si $n = 1$ alors le produit est 1. Sinon, il est nul car il contient un facteur $1 - 1 = 0$.

2. Utiliser la question précédente ou constater que si n et m sont premiers entre eux alors $\mathcal{P}_{mn} = \mathcal{P}_m \sqcup \mathcal{P}_n$ (union disjointe).

3. Avec les notations de l'exercice 57, on a $g = \mathbf{1} * f$ et $\mathbf{1} * \mu = \delta_0$.

Indication 61 · Énoncé p. 19 (Division euclidienne dans les entiers de Gauss)
Remarquer que tout point de $\mathbb{C}$ est à distance au plus $\frac{\sqrt{2}}{2} < 1$ d'un point de $\mathbb{Z}[i]$.

Solution p. 62

Indication 62 · Énoncé p. 20 (Détermination explicite des couples de Bézout)
Exprimer l'ensemble des solutions sous la forme d'un théorème de structure (solution particulière et solutions homogènes).

On remarque qu'en pratique on peut utiliser l'algorithme d'Euclide étendu pour déterminer une solution particulière.

Indication 63 · Énoncé p. 20 (Un cas particulier de Bézout positif)
Cf l'exercice 64 ou bien faire tout simplement les petits cas en remarquant que l'ensemble est stable par addition.

Indication 65 · Énoncé p. 20 (Pourquoi réfléchir quand on peut trinomer)
Il s'agit d'une équation du second degré.

Solution p. 64

Indication 66 · Énoncé p. 21 (Majorations successives)
Raisonner par exemple par condition nécessaire pour majorer des solutions éventuelles et terminer par disjonction de cas.

Solution p. 64

Indication 67 · Énoncé p. 21 (Étude de fonction)
Étudier $x \mapsto \frac{\ln(x)}{x}$.

Solution p. 66

Indication 68 · Énoncé p. 21 (Une identité de Sophie Germain)
Remarquer que $X^4+4=(X^2-2X+2)(X^2+2X+2)$.

Par conséquent

$$n^4+4m^4=(n^2-2nm+2m^2)(n^2+2nm+2m^2)=((n-m)^2+m^2)((n+m)^2+m^2)$$

d'où la seule possibilité est $m=1$ et $n-m=0$.

Indication 69 · Énoncé p. 21 (Une question du CG 1990)
Faire de même que l'exercice 66, en raisonnant par majorations nécessaires.

On pourra aussi constater que si $(x_1,...,x_n)$ et $(y_1,...,y_m)$ conviennent, alors $(x_1y_1,x_1y_2,...,x_1y_m,x_2,...,x_n)$ convient.

Solution p. 68

Indication 70 · Énoncé p. 22 (Équations en vrac)
Plein d'options pour le premier, de l'identité remarquable $x^2 - y^2 = (x-y)(x+y)$ à l'étude d'un carré modulo un entier usuel.

Utiliser par exemple encore une identité remarquable pour le second.

Solution p. 71

Indication 71 · Énoncé p. 22 (Réduction donc impossibilité)
1. Modulo 4.
2. Encore modulo 4.
3. On a $11 - 1 = 10$ divisible par 2 et 5. Donc réduction modulo 11.

Solution p. 71

Indication 72 · Énoncé p. 22 (Une question du Bac 2003)
Étudier les carrés modulo 7.

Solution p. 73

Indication 73 · Énoncé p. 22 (Lemme d'Hensel)
Procéder par récurrence sur n (le cas $n = 0$ est trivial, le cas $n = 1$ donné par $x_1 = a$).

Pour l'hérédité à partir de $n \geq 1$, rechercher x_{n+1} sous la forme $x_{n+1} = x_n + p^n y_n$.

Remarquer qu'alors $P(x_{n+1}) \equiv P(x_n) + p^n y_n P'(x_n)[p^{n+1}]$.

Indication 74 · Énoncé p. 23 (Un contre-exemple au principe général de réduction modulaire)
Il faut donc montrer que parmi, 2, 17 et 34 au moins est toujours un carré modulo n.

Par théorème des restes chinois, il suffit de montrer que pour tout nombre premier p et tout entier k, au moins un des trois nombres $2, 17, 34$ est un carré modulo p^k.

Par le lemme d'Hensel, cf exercice 73, il y a trois cas à traiter:
- $p \notin \{2, 17\}$: le symbole de Legendre étant multiplicatif et $2 \times 17 = 34$ donc au moins l'un vaut 1,
- $p = 17$, on a $6^2 \equiv 2[17]$,
- $p = 2$, le cas restant à faire, utiliser $17 \equiv 1[8]$.

Indication 75 · Énoncé p. 23 (Paramétrisation des triplets pythagoriciens)
Une inclusion est immédiate.

Pour l'autre remarquer par exemple que déterminer un triplet pythagoricien revient à déterminer un point de $\mathbb{U} \cap \mathbb{Q}^2$. Le k correspond alors à la réduction en fraction irréductible et $\frac{n}{m}$ à la tangente de l'angle moitié.

Indication 76 · Énoncé p. 23 (Petite translation)
Avec $a = p + x$, $b = p + y$ on se ramène à $xy = p^2$

Indication 77 · Énoncé p. 23 (Petite puissance de 2)
Étudier modulo 4 : en déduire que $b = 1$ (ce qui donne $a = 1$) ou que a est pair.

Dans le cas a pair, factoriser $3^a - 1$ par Bernoulli en produit de deux puissances de 2.

Indication 78 · Énoncé p. 24 (Petite division)
Majorer ou diviser par $(ab)^2$ (dans le cas $\neq 0$) pour se ramener à 66.

Indication 79 · Énoncé p. 24 (Encore des majorations)
Vérifier que $n = 0$ et $n = 1$ conviennent ; pour $n \geq 2$, regarder modulo 4 pour déduire que n est pair.

Montrer que si $2^{2m} \mid (3^m - 1)(3^m + 1)$ alors $2^{2m-1} \mid 3^m - 1$ ou $2^{2m-1} \mid 3^m + 1$.

Se ramener à un nombre fini de cas.

Indication 80 · Énoncé p. 24 (L'exemple le plus connu de «saut de Viète»)
1. Utiliser les relations coefficients/racines.
2. Faire un principe de descente infinie.

Indication 81 · Énoncé p. 25 (Crible mystère I)
Les noms sont en fait légèrement expressifs: `lp` comme «Liste des nombres Premiers» et `ppdp` comme «liste du Plus Petit Diviseur Premier».

Solution p. 74

Indication 82 · Énoncé p. 25 (Crible mystère II)
Faire d'abord l'exercice 81.

Solution p. 76

Indication 83 · Énoncé p. 26 (Complexité de l'algorithme d'Euclide)
1. Cf cours.
2. Remarquer la division euclidienne suivante pour tout $n \in \mathbb{N}^*$:
$$F_{n+1} = \underbrace{1}_{\text{quotient}} \times F_n + \underbrace{F_{n-1}}_{\text{reste}}$$
et faire une récurrence.
3. On pourrait montrer à partir de ce résultat que, pour deux entiers de taille N, la complexité générale de l'algorithme d'Euclide est en $O(\ln(N))$, c'est à dire que l'algorithme d'Euclide est très efficace (complexité sous-linéaire) ; le couple (F_{n+1}, F_n) réalise précisément le pire cas de cette borne.

Indication 84 · Énoncé p. 26 (Autour du Projet Euler 37)
On peut déterminer l'arbre des préfixes des suites de chiffres premières par troncature à droite. En remarquant que le nombre est décroissant. En optimisant un peu les chiffres à rajouter voir que l'arbre est fini.

Indication 86 · Énoncé p. 27 (De l'art de choisir ses tiroirs)
1. Montrer en faisant des petits tiroirs de deux entiers consécutifs qu'il existe même i et j tels que a_i et a_j consécutifs.
2. Tout entier a_i s'écrit sous la forme $2^{r_i}q_i$ avec q_i impair.

   Si $q_i = q_j$ alors $a_i \mid a_j$ ou $a_j \mid a_i$.

Indication 87 · Énoncé p. 27 (Somme des puissances modulo p)
Constater que l'on peut se ramener à $m \in [\![0, p-2]\!]$.

Ensuite plusieurs options:

1. Une formule par récurrence sur les S_m,
2. une bijection astucieuse,
3. une relation coefficient/racines sur $X^n - 1$ et des sommes de Newton (plus compliqué).

Indication 88 · Énoncé p. 27 (Juste parité et moyenne)
Il y a peu de nombres premiers pairs.

Ensuite si p_n et p_{n+1} sont *consécutifs* alors $\frac{p_n+p_{n+1}}{2}$ n'est pas premier.

Indication 89 · Énoncé p. 27 (Bernoulli itéré)
Bernoulli.

Solution p. 76

Indication 90 · Énoncé p. 27 (Travailler puis plein de disjonctions de cas)
Supposer $a \leq b \leq c$.

Montrer que a, b, c sont deux à deux premiers entre eux puis que $abc \mid ab + bc + ac - 1$.

En déduire $a \leq 2$.

Traiter la disjonction de cas de manière similaire (majoration puis disjonction).

Indication 91 · Énoncé p. 28 (P1 2017)
Remarquer que la suite est autonome et travailler modulo 3.
- ▷ Si $a_0 \equiv 0[3]$ alors pour tout n, $a_n \equiv 0[3]$. Et si $a_0 \leq (3m)^2$ alors pour tout $n \in \mathbb{N}$, $a_n \leq (3m)^2$.
- ▷ Si $a_0 \equiv 2[3]$ alors pour tout n, $a_n \equiv 2[3]$ et $a_n = a_0 + 3n$.
- ▷ Il reste le cas $a_0 \equiv 1[3]$.

  Traiter à la main les petits cas.

Remarquer que si $a_0 = 3k+1$ alors comme $(3k-1)^2 = (3k+1) + 9(k^2-k)$, si $k \geq 9$ alors il existera un rang où $a_n < a_0$.

Si ce a_n est congru à 2 modulo 3 alors on a terminé.

Conclure par récurrence forte dans le cas de congruence à 1.

Solutions

Solution pour l'exercice 1 · Énoncé p. 2 · Indication p. 29 (Premier petit calcul)
On a $2025 \equiv 11[19]$.

Il reste donc à calculer $11^{2026^{2027}}$ modulo 19.

On regarde les premières congruences de 11^k modulo 19:
- $11^1 \equiv 11[19]$
- $11^2 \equiv 7[19]$
- $11^3 \equiv 1[19]$

Par conséquent avec $r \in [\![0, 2]\!]$ tel que $2026^{2027} \equiv r[3]$, on a $11^{2026^{2027}} \equiv 11^r[19]$.

Il reste donc à calculer 2026^{2027} modulo 3.

Or $2026 \equiv 1[3]$ donc $2026^{2027} \equiv 1^{2027} \equiv 1[3]$.

Par conséquent $r = 1$ et donc $\boxed{2025^{2026^{2027}} \equiv 11[19]}$.

Solution pour l'exercice 2 · Énoncé p. 2 · Indication p. 29 (Un peu de repunit)
Notons pour tout $n \in \mathbb{N}^*$, $r_n = \underbrace{111\cdots111}_{n \text{ fois}}$ c'est à dire $r_n = \sum_{k=0}^{n-1} 10^k$.

On cherche à montrer qu'il existe $n \in \mathbb{N}^*$ tel que $r_n \equiv 0[a]$.

On remarque que les restes de r_n dans leur division par a sont dans $[\![0, a-1]\!]$.

Comme il y a une infinité de valeurs possibles de n, par le principe des tiroirs (version infinité de chaussettes dans un nombre fini de tiroirs), il existe n, m distincts tels que r_n et r_m ont le même reste par la division par a.

Quitte à les intervertir on peut supposer que $n > m$.

On a alors comme $r_n \equiv r_m[a]$, la congruence $r_n - r_m \equiv 0[a]$.

Or

$$\begin{aligned} r_n - r_m &= \sum_{k=0}^{n-1} 10^k - \sum_{k=0}^{m-1} 10^k \\ &= \sum_{k=m}^{n-1} 10^k \\ &= 10^m \sum_{k=0}^{n-m-1} 10^k \\ &= 10^m r_{n-m}. \end{aligned}$$

Par conséquent $a \mid 10^m r_{n-m}$.

Donc, comme a et 10 sont premiers entre eux, par lemme de Gauss on en déduit que $\boxed{a \mid r_{n-m}}$.

Solution pour l'exercice 3 · Énoncé p. 2 · Indication p. 29 (Encore des repunits en base 10)
Notons pour tout $n \in \mathbb{N}^*$, $r_n = \underbrace{111\cdots111}_{n \text{ fois}}$ c'est à dire $r_n = \sum_{k=0}^{n-1} 10^k$.

On a $1 \equiv 1[4]$ et $10 \equiv 2[4]$ puis pour tout $k \geq 2$, $10^k \equiv 0[4]$.

Ainsi $r_1 \equiv 1[4]$ et pour tout $n \geq 2$, $r_n \equiv 1 + 2 \equiv 3[4]$.

Or on a le tableau des carrés modulo 4:

$x \bmod 4$	0	1	2	3
$x^2 \bmod 4$	0	1	0	1

et en particulier tout carré est congru à 0 ou 1 modulo 4.

D'où pour tout $n \geq 2$, r_n n'est pas un carré.

Comme $r_1 = 1 = 1^2$, le seul repunit qui soit un carré est $r_1 = 1$.

Remarque : l'idée de regarder modulo 4 pour un carré est un bon réflexe de condition nécessaire (mais non suffisante) à avoir.

Solution pour l'exercice 4 · Énoncé p. 2 · Indication p. 29 (Critères de divisibilité)
On a

$$n = \sum_{k=0}^{r} c_k 10^k.$$

1. On a $10 \equiv 1[3]$ donc pour tout $k \in \mathbb{N}$, $10^k \equiv 1[3]$.

Par conséquent

$$\begin{aligned} n \equiv \sum_{k=0}^{r} c_k 10^k &\equiv \sum_{k=0}^{r} c_k 1 \ [3] \\ &\equiv \sum_{k=0}^{r} c_k \ [3]. \end{aligned}$$

En particulier on obtient $n \equiv 0[3]$ ssi $\sum_{k=0}^{r} c_k \equiv 0[3]$. D'où le critère de divisibilité par 3.

2. On a $10 \equiv -1[11]$ donc pour tout $k \in \mathbb{N}$, $10^k \equiv (-1)^k[11]$.

Par conséquent

$$n \equiv \sum_{k=0}^{r} c_k 10^k \equiv \sum_{k=0}^{r} c_k (-1)^k [11].$$

En particulier on obtient $n \equiv 0[11]$ ssi $\sum_{k=0}^{r} (-1)^k c_k \equiv 0[11]$. D'où le critère de divisibilité par 11.

3. On a $10^6 \equiv 1[7]$ (par calcul ou petit théorème de Fermat).

Par conséquent en posant pour tout $k \in \mathbb{N}$,

$$\alpha_k = \begin{cases} 1 \text{ si } & k \equiv 0[6] \\ 3 \text{ si } & k \equiv 1[6] \\ 2 \text{ si } & k \equiv 2[6] \\ 6 \text{ si } & k \equiv 3[6] \\ 4 \text{ si } & k \equiv 4[6] \\ 5 \text{ si } & k \equiv 5[6] \end{cases}$$

on obtient pour tout $k \in \mathbb{N}$, comme

$$\begin{aligned} 10^k &\equiv 10^{6(k/\!\!/6)+(k\%6)} \ [7] \\ &\equiv \left(10^6\right)^{k/\!\!/6} 10^{k\%6} \ [7] \\ &\equiv 10^{k\%6} \ [7] \\ &\equiv \alpha_k \ [7]. \end{aligned}$$

D'où pour tout $n \in \mathbb{N}$,

$$\begin{aligned} n &\equiv \sum_{k=0}^{r} c_k 10^k \ [7] \\ &\equiv \sum_{k=0}^{r} c_k \alpha_k \ [7]. \end{aligned}$$

et donc n est divisible par 7 ssi $\sum_{k=0}^{r} \alpha_k c_k$ est divisible par 7.

D'où un critère de divisibilité par 7.

Remarques: comme pour tous les autres critères on a en fait mieux que juste la divisibilité:

- ▷ on a plus précisément une congruence modulo 7,
- ▷ on peut aussi itérer le processus sur l'écriture décimale de la somme pondérée obtenue.

4. Notons pour tout $k \in \mathbb{N}$, α_k le reste de la division euclidienne de 10^k par a.

Comme précédemment on a

$$n \equiv \sum_{k=0}^{r} c_k 10^k \equiv \sum_{k=0}^{r} c_k \alpha_k \ [a].$$

Il reste juste à montrer que la suite $(\alpha_k)_{k\in\mathbb{N}}$ est périodique.

Comme les α_k sont dans $[\![0, a-1]\!]$, par le principe des tiroirs (version une infinité de chaussettes dans un nombre fini de tiroirs), il existe $i < j$ tels que $\alpha_i = \alpha_j$ c'est à dire

$$10^i \equiv 10^j \ [a].$$

Comme 10 est inversible modulo a (car a et 10 sont premiers entre eux) on a donc

$$10^{j-i} \equiv 1 \ [a].$$

Notons $p = j - i$.

Alors pour tout $k \in \mathbb{N}$, on a

$$10^{k+p} \equiv 10^k 10^p \equiv 10^k \ [a].$$

Et donc $\boxed{\text{pour tout } k \in \mathbb{N},\ \alpha_{k+p} = \alpha_k}$.

Solution pour l'exercice 5 · Énoncé p. 2 · Indication p. 29 (Encore un petit calcul)
Première méthode

On peut tout simplement développer.

Soit n un entier. Par la formule du binôme

$$\begin{aligned}(n-1)^3 + n^3 + (n+1)^3 &= n^3 - 3n^2 + 3n - 1 + n^3 + n^3 + 3n^2 + 3n + 1\\ &= 3n^3 + 6n\\ &= 3n(n^2+2)\end{aligned}$$

et

- ▹ Si $n \equiv 0[3]$ alors $3 \mid n$
- ▹ sinon $n \equiv \pm 1[3]$ d'où $n^2 + 2 \equiv 0[3]$.

Dans tous les cas $3 \mid n(n^2+2)$ et donc $9 \mid (n-1)^3 + n^3 + (n+1)^3$.

Deuxième méthode On regarde la table des cubes modulo 9

$x \bmod 9$	0	1	2	3	4	5	6	7	8
$x^3 \bmod 9$	0	1	8	0	1	8	0	1	8

d'où la somme des cubes de trois nombres consécutifs est toujours congrue à 0 modulo 9.

Solution pour l'exercice 6 · Énoncé p. 3 · Indication p. 29 (Juste faire un tableau)
On regarde le tableau des carrés modulo 24, en retirant les entiers congrus à 0 modulo 2 ou 3:

$n \bmod 24$	1	5	7	11	13	17	19	23
$n^2 \bmod 24$	1	1	1	1	1	1	1	1

d'où dans tous les cas $n^2 \equiv 1[24]$ et donc $24 \mid n^2 - 1$.

Solution pour l'exercice 7 · Énoncé p. 3 · Indication p. 29 (Encore des tableaux peu passionnants)

1. On a le tableau de congruences modulo 3, comme $10 \equiv 1[3]$ et $14 \equiv 2[3]$:

$n \bmod 3$	0	1	2
$n + 10 \bmod 3$	1	2	0
$n + 14 \bmod 3$	2	0	1

Dans chaque colonne exactement un des trois nombres est congru à 0 modulo 3.

2. Comme $2 \equiv -1[3]$ et $4 \equiv 1[3]$ on a le tableau de congruence modulo 3:

$n \bmod 3$	0	1	2

$2n+1 \bmod 3$	1	0	2
$4n+1 \bmod 3$	1	2	0

Dans chaque colonne exactement un des trois nombres est congru à 0 modulo 3.

3. Comme $4 \equiv -1[5]$ et $6 \equiv 1[5]$ on a le tableau de congruence modulo 5:

$n \bmod 5$	0	1	2	3	4
$4n^2+1 \bmod 5$	1	0	2	2	0
$6n^2+1 \bmod 5$	1	2	0	0	2

Dans chaque colonne exactement un des trois nombres est congru à 0 modulo 5.

Solution pour l'exercice 8 · Énoncé p. 3 · Indication p. 30 (Des trous aussi grands que l'on veut)
Soit $n \in \mathbb{N}$.

On constate alors que $(n+1)!+2, (n+1)!+3, ..., (n+1)!+(n+1)$ sont n entiers consécutifs.

De plus pour tout $k \in [\![2, n+1]\!]$, $(n+1)!+k$ est divisible par k (car k divise $(n+1)!$). Et comme $(n+1)!+k > k > 1$ on en déduit que $(n+1)!+k$ n'est pas premier.

Solution pour l'exercice 9 · Énoncé p. 3 · Indication p. 30 (Somme des chiffres itérée)
Comme $10 \equiv 1[9]$ on a pour tout $n \in N$,

$$s_{10}(n) \equiv n[9].$$

De plus on a $2^3 \equiv -1[9]$ et donc $2^6 \equiv 1[9]$.

Comme $2026 = 6 \times 337 + 4$, on a

$$\begin{aligned} 2^{2026} &\equiv \left\{2^6\right\}^{337} \times 2^4[9] \\ &\equiv 2^4[9] \\ &\equiv 7[9]. \end{aligned}$$

et donc finalement

$$s_{10}(s_{10}(s_{10}(s_{10}(s_{10}(2^{2026}))))) \equiv 7[9].$$

De plus pour tout $n \in N$, on a n admet une écriture décimale de $\lfloor \log_{10}(n) \rfloor + 1$ chiffres, et donc on a

$$s_{10}(n) \leq 9(\lfloor \log_{10}(n) \rfloor + 1).$$

Par conséquent, comme $\log_{10}(2) < 1$, (c'est environ 0.3) on a

$$s_{10}(2^{2026}) \leq 9(\lfloor \log_{10}(2^{2026}) \rfloor + 1) = 9(\lfloor 2026 \log_{10}(2) \rfloor + 1) \leq 9 \times 2027 < 10^6$$

d'où

$$s_{10}(s_{10}(2^{2026})) \leq 9(\lfloor \log_{10}(s_{10}(2^{2026})) \rfloor + 1) \leq 9(\lfloor \log_{10}(9 \times 2027) \rfloor + 1) \leq 9(5+1) = 54.$$

Par conséquent

$$s_{10}(s_{10}(s_{10}(2^{2026}))) \leq 5 + 9 = 14.$$

Puis

$$s_{10}(s_{10}(s_{10}(s_{10}(2^{2026})))) \leq 9$$

et (l'énoncé est volontairement très «large»)

$$s_{10}(s_{10}(s_{10}(s_{10}(s_{10}(2^{2026}))))) \leq 9.$$

Le seul entier de $[\![0, 9]\!]$ congru à 7 modulo 9 est 7.

Par conséquent

$$\boxed{s_{10}(s_{10}(s_{10}(s_{10}(s_{10}(2^{2026}))))) = 7}.$$

Remarque: ici les bornes sont volontairement très «larges» pour que l'on puisse conclure facilement. Un petit script python montrer que l'on a

$$s_{10}(s_{10}(s_{10}(s_{10}(2^{2026})))) = 7.$$

Solution pour l'exercice 13 · Énoncé p. 4 · Indication p. 30 (Passage à la limite)
On a pour tout nombre premier p, pour tout $n \in \mathbb{N}$, comme $a^n \mid b^{n+2025}$,

$$v_p(a^n) \leq v_p(b^{n+2025})$$

c'est à dire

$$\forall n \in \mathbb{N}, n v_p(a) \leq (n + 2025) v_p(b)$$

ou encore (dans $\mathbb{R}$),

$$\forall n \in \mathbb{N}^*, v_p(a) \leq \frac{n + 2025}{n} v_p(b).$$

Par Passage à la Limite des Inégalités Larges, quand $n \to +\infty$, on a

$$v_p(a) \leq v_p(b).$$

Comme c'est le cas pour tout nombre premier p, on a donc

$$\boxed{a \mid b}.$$

Solution pour l'exercice 14 · Énoncé p. 4 · Indication p. 30 (Puissances multiples)
Si $a = 0$, alors $b = 0$ convient.

Supposons désormais $a \neq 0$, et donc b_1, b_2 non nuls.

On commence par montrer le résultat suivant

Il existe $b \in \mathbb{N}^*$ tel que $a = b^r$ **ssi** pour tout nombre premier p, $r \mid v_p(a)$.

En effet:

- ▷ $\boxed{\Rightarrow}$ Si il existe $b \in \mathbb{N}^*$ tel que $a = b^r$ alors pour tout nombre premier p, $v_p(a) = rv_p(b)$ et donc $r \mid v_p(a)$.
- ▷ $\boxed{\Leftarrow}$ Si pour tout nombre premier p, $r \mid v_p(a)$ alors pour tout $p \in \mathcal{P}$, $\frac{v_p(a)}{r} \in \mathbb{N}$ et donc $b = \prod_{p\in\mathcal{P}} p^{\frac{v_p(a)}{r}}$ est bien défini.

  Et on a bien $b^r = a$.

Une fois ce résultat montré, on a donc pour tout nombre premier p, $r_1 \mid v_p(a)$ et $r_2 \mid v_p(a)$.

Donc par définition du ppcm, pour tout nombre premier p, $r_1 \vee r_2 \mid v_p(a)$.

Par conséquent il existe $b \in \mathbb{N}$ tel que $a = b^{r_1 \vee r_2}$.

Solution pour l'exercice 15 · Énoncé p. 5 · Indication p. 30 (Encore une caractérisation des puissances)
Supposons qu'il existe $d \in \mathbb{N}^*$ tel que $ab = d^2$.

Soit p un nombre premier. On a

- ▷ $\nu_p(ab) = \nu_p(a) + \nu_p(b) = \nu_p(d^2) = 2\nu_p(d)$,
- ▷ $\nu_p(a \wedge b) = \min\big(\nu_p(a), \nu_p(b)\big) = 0$ car a et b sont premiers entre eux, c'est à dire $\nu_p(a) = 0$ ou $\nu_p(b) = 0$.

En particulier $\nu_p(a) + \nu_p(b)$ est pair et l'un des deux termes vaut 0 et donc est pair.

Ainsi $\nu_p(a)$ et $\nu_p(b)$ sont tous les deux pairs.

On a donc montré que pour tout nombre premier p, $\nu_p(a)$ et $\nu_p(b)$ sont pairs.

D'où $\boxed{a \text{ et } b \text{ sont des carrés}}$.

En effet

$$a = \left(\prod_{p\in\mathcal{P}} p^{\frac{\nu_p(a)}{2}}\right)^2$$

le produit étant bien défini et un entier car $\left(\frac{\nu_p(a)}{2}\right)_{p\in\mathcal{P}}$ est une famille à support fini d'entiers naturels.

Et de même pour b.

Solution pour l'exercice 17 · Énoncé p. 5 · Indication p. 31 (Somme de puissances de diviseurs ou décomposition des sigmas)
Notons dans la suite pour $n \in \mathbb{N}$, $\mathcal{D}(n)$ l'ensemble des diviseurs **positifs** de n.

Ainsi pour tout $s \in \mathbb{R}$ et $n \in \mathbb{N}^*$,

$$\sigma_s(n) = \sum_{d\in\mathcal{D}(n)} d^s.$$

1. Soient n, m premiers entre eux.

On a

$$\begin{aligned}\sigma_s(n)\sigma_s(m) &= \left(\sum_{d_1\in\mathcal{D}(n)} d_1^s\right)\left(\sum_{d_2\in\mathcal{D}(m)} d_2^s\right)\\ &= \sum_{(d_1,d_2)\in\mathcal{D}(n)\times\mathcal{D}(m)} d_1^s d_2^s\\ &= \sum_{(d_1,d_2)\in\mathcal{D}(n)\times\mathcal{D}(m)} (d_1d_2)^s\end{aligned}$$

De plus comme $n\wedge m = 1$ on a

$$\varphi : \begin{array}{l}\mathcal{D}(n)\times\mathcal{D}(m) \longrightarrow \mathcal{D}(nm)\\ (d_1,d_2) \qquad\quad \longmapsto d_1d_2\end{array}$$

est bijective.

On peut le voir sur la Décomposition en Produit de Facteurs Premiers, ou de manière équivalente en remarquant que

$$\psi : \begin{array}{l}\mathcal{D}(nm) \longrightarrow \mathcal{D}(n)\times\mathcal{D}(m)\\ d \qquad\quad \longmapsto (d\wedge n, d\wedge m)\end{array}$$

est une bijection réciproque de φ (encore une fois car n et m n'ont pas de facteurs premiers en commun).

D'où

$$\sum_{(d_1,d_2)\in\mathcal{D}(n)\times\mathcal{D}(m)} (d_1d_2)^s = \sum_{d\in\mathcal{D}(nm)} d^s = \sigma_s(nm).$$

Et donc $\boxed{\sigma_s(nm) = \sigma_s(n)\sigma_s(m)}$.

2. Comme p est premier, les diviseurs de p^k admettent p comme unique facteur premier, d'où les diviseurs de p^k sont les p^j pour $j\in[\![0,k]\!]$.

$$\mathcal{D}(p^k) = \{p^j \mid j\in[\![0,k]\!]\}.$$

En particulier, par somme géométrique,

$$\begin{aligned}\sigma_s(p^k) &= \sum_{j=0}^{k} (p^j)^s\\ &= \sum_{j=0}^{k} (p^s)^j\\ &= \begin{cases} k+1 & \text{si } s=0\\ \frac{p^{(k+1)s}-1}{p^s-1} & \text{si } s\neq 0\end{cases}.\end{aligned}$$

Ainsi

$$\boxed{\sigma_s(p^k) = \begin{cases} k+1 & \text{si } s=0\\ \frac{p^{(k+1)s}-1}{p^s-1} & \text{si } s\neq 0\end{cases}}.$$

3. On écrit n comme produit de ses facteurs premiers, $n = \prod_{p\in\mathcal{P}} p^{\nu_p(n)}$.

Comme pour deux nombres premiers distincts $p_1, p_2 \in \mathcal{P}$, $p_1^{\nu_{p_1}(n)}$ et $p_2^{\nu_{p_2}(n)}$ sont premiers entre eux, on a par la première question,

$$\sigma_s(n) = \prod_{p\in\mathcal{P}} \sigma_s\left(p^{\nu_p(n)}\right).$$

Et donc par la deuxième question

$$\boxed{\sigma_s(n) = \begin{cases} \prod_{p\in\mathcal{P}} (\nu_p(n)+1) & \text{si } s=0 \\ \prod_{p\in\mathcal{P}} \frac{p^{(\nu_p(n)+1)s}-1}{p^s-1} & \text{si } s\neq 0 \end{cases}}$$

Solution pour l'exercice 20 · Énoncé p. 6 · Indication p. 31 (Un peu d'arithmétique des suites de Fibonacci)

1. Une version itérative est

```
def fibo(n):
    """Prend en argument un entier n et renvoie le n-ième terme de la suite de Fibonacci"""
    a, b = 0, 1
    for i in range(n):
        a, b = b, a + b
    return a

```

et une version récursive est

```
def fibo_rec(n):
    """Prend en argument un entier n et renvoie récursivement (F_n,F_{n+1})"""
    if n == 0:
        return (0, 1)
    else:
        a, b = fibo_rec(n - 1)
        return (b, a + b)


def fibo(n):
    """Prend en argument un entier n et renvoie le n-ième terme de la suite de Fibonacci"""
    return fibo_rec(n)[0]

```

On peut montrer par récurrence forte sur $n \in \mathbb{N}$ que pour tout $n \in \mathbb{N}$, $F_n \in \mathbb{N}$.

2. On remarque que pour tout $n \in \mathbb{N}^*$,

$$F_{n+1} = F_n + F_{n-1}$$

et donc par invariance par transvection du pgcd,

$$F_{n+1} \wedge F_n = F_n + F_{n-1} \wedge F_n = F_{n-1} \wedge F_n.$$

On procède donc par récurrence sur $n \in \mathbb{N}$.

▷ **Initialisation**

Pour $n = 0$, $F_0 = 0$ et $F_1 = 1$ donc $F_0 \wedge F_1 = 1$.

▷ **Hérédité**

Soit $n \in \mathbb{N}$, supposons que $F_{n+1} \wedge F_n = 1$.

On a que

$$F_{n+2} \wedge F_{n+1} = F_{n+1} + F_n \wedge F_{n+1} = F_n \wedge F_{n+1} = 1.$$

▷ **Conclusion**

Par récurrence, on a donc

$$\forall n \in \mathbb{N}, \boxed{F_{n+1} \wedge F_n = 1}.$$

Remarque : on remarque qu'une preuve algorithmique est aussi possible, en suivant un algorithme d'Euclide, la propriété que pour tout $n \in \mathbb{N}$, $F_{n+1} \wedge F_n = 1$ étant un invariant de boucle.

Solution pour l'exercice 21 · Énoncé p. 6 · Indication p. 31 (Nombres de Mersenne)

1. On remarque que par formule de Bernoulli on a

$$a^n - 1 = (a-1)\left(\sum_{k=0}^{n-1} a^k\right).$$

et donc

$$a - 1 | a^n - 1.$$

D'où

- ▷ Si $a > 2$ alors $a - 1 > 1$ et (comme $n \geq 2$) $a - 1 < a^n - 1$ et donc $a^n - 1$ n'est pas premier.
- ▷ Si n est non premier, il existe $p, q \in \mathbb{N}$ tels que $n = pq$ avec $p, q > 1$. Alors $a^n - 1 = (a^p)^q - 1$ et est donc divisible par $a^p - 1$ différent de 1 et de $a^n - 1$ (car $p, q > 1$).

Par contraposée on a donc montré que $\boxed{\text{si } a^n - 1 \text{ est premier alors } a = 2 \text{ et } n \text{ est premier}}$.

2. On peut par exemple utiliser le programme suivant

```python
# Pour déterminer les nombres premiers on propose un algorithme de crible d'Ératosthène:
def crible(n):
    """Prend en argument un entier n.
    Renvoie un tuple (est_premier, premiers) où est_premier est un tableau de booléens de taille n indiquant si chaque entier inférieur à n est premier et premiers est la liste des nombres premiers inférieurs à n.
    """
    if n < 2:
        return []
    premiers = []  # La liste des nombres premiers
    est_premier = [True for _ in range(n)]  # est_premier[i] indique si i est premier
    est_premier[0] = False
    est_premier[1] = False
    for i in range(2, n):
        if est_premier[i]:
            premiers.append(i)
            for j in range(i * i, n, i):
                est_premier[j] = False
    return est_premier, premiers


```

```python
def mersenne(n):
    """Prend en argument un entier n et affiche la liste des nombres de Mersennes inférieurs à 2**n - 1 et leur primalité éventuelle"""
    N = 2**n
    est_premier, premiers = crible(N)
    for p in range(n + 1):
        if est_premier[p]:
            m = 2**p - 1
            print(f"2^{p} - 1 = {m} est {'premier' if est_premier[m] else 'composé'}")
    return None


# Affiche les nombres de Mersennes inférieurs à 2**23 - 1 et leur primalité éventuelle
mersenne(23)

```

On obtient

```
2^2 - 1 = 3 est premier
            2^3 - 1 = 7 est premier
            2^5 - 1 = 31 est premier
            2^7 - 1 = 127 est premier
            2^11 - 1 = 2047 est composé
            2^13 - 1 = 8191 est premier
            2^17 - 1 = 131071 est premier
            2^19 - 1 = 524287 est premier
            2^23 - 1 = 8388607 est composé
```

et $2^{11}-1 = 2047 = 23 \times 89$ et $2^{23}-1 = 8388607 = 47 \times 178481$ ne sont pas premiers.

Solution pour l'exercice 22 · Énoncé p. 7 · Indication p. 31 (Nombres de Fermat)

1. Supposons que b n'est pas une puissance de 2.

Il existe alors $\alpha \in \mathbb{N}$ et $q \in \mathbb{N}$ impair et $q \geq 3$ tels que $b = 2^\alpha q$.

On a alors par Bernoulli, comme q est impair,

$$\begin{aligned} 2^b + 1 &= 2^{2^\alpha q} + 1 \\ &= \left(2^{2^\alpha}\right)^q - (-1)^q \\ &= \left(2^{2^\alpha} - (-1)\right)\left(\sum_{k=0}^{q-1} \left(2^{2^\alpha}\right)^k (-1)^{q-1-k}\right) \end{aligned}$$

donc $2^{2^\alpha}+1$ divise 2^b+1 et est différent de 1 et de 2^b+1 car $q > 1$.

Donc 2^b+1 n'est pas premier.

Par contraposée, on a donc montré que $\boxed{\text{si } 2^b+1 \text{ est premier alors } b \text{ est une puissance de 2}}$.

2. On peut par exemple utiliser le programme suivant

```python
# Par exemple pour déterminer si un nombre est premier, plutôt qu'un crible d'Ératosthène, on peut tester les nombres plus petits que la racine carrée de ce nombre (un crible serait plus efficace pour tester plusieurs nombres).


def est_premier(n):
```

```python
    """Prend en argument un entier n et renvoie True si il est premier, False sinon"""
    # Pour gagner du temps on traite que les diviseurs impairs
    if n < 2 or n % 2 == 0:
        return False
    if n == 2:
        return True
    k = 3
    while k * k <= n:
        if n % k == 0:
            return False
        k = k + 2
    return True


def fermat(n):
    """Prend en argument un entier n et affiche la liste des n premiers nombres de Fermat et leur primalité éventuelle"""
    for p in range(n):
        f = 2 ** (2**p) + 1
        print(f"F_{p} = {f} est {'premier' if est_premier(f) else 'composé'}")
    return None


fermat(7)

```

On obtient

```
F_0 = 3 est premier
F_1 = 5 est premier
F_2 = 17 est premier
F_3 = 257 est premier
F_4 = 65537 est premier
F_5 = 4294967297 est composé
F_6 = 18446744073709551617 est composé
```

et $F_5 = 4294967297 = 641 \times 6700417$ et $F_6 = 18446744073709551617 = 274177 \times 67280421310721$ ne sont pas premiers.

3. Soient $n, m \in \mathbb{N}$ tels que $n \neq m$.

Quitte à intervertir n et m, on peut supposer que $n < m$.

On a alors

$$F_m - 1 = 2^{2^m} = \left(2^{2^n}\right)^{2^{m-n}} = (F_n - 1)^{2^{m-n}}$$

c'est à dire

$$F_m = (F_n - 1)^{2^{m-n}} + 1.$$

Par le binôme

$$F_m = 1 + \sum_{k=0}^{2^{m-n}} \binom{2^{m-n}}{k} F_n^k (-1)^{2^{m-n}-k}$$

i.e

$$F_m = 1 + 1 + \left(\sum_{k=1}^{2^{m-n}} \binom{2^{m-n}}{k} F_n^{k-1} (-1)^{2^{m-n}-k}\right) F_n$$

d'où par invariance du pgcd par transvection, et comme F_n est impair,

$$F_m \wedge F_n = F_n \wedge 2 = 1.$$

4. Pour tout $n \in \mathbb{N}$, $F_n > 1$ et donc admet au moins un diviseur premier.

Notons p_n un tel diviseur premier.

Alors pour tous $n, m \in \mathbb{N}$ tels que $n \neq m$, on a $F_n \wedge F_m = 1$ et donc $p_n \neq p_m$.

D'où il existe une infinité de nombres premiers.

Solution pour l'exercice 25 · Énoncé p. 7 · Indication p. 32 (Infinité de nombres premiers dans certaines progressions arithmétiques I)

1. La remarque clef est qu'un produit de nombres congrus à 1 modulo 4 est aussi congru à 1 modulo 4. Par conséquent (contraposée) si un produit de termes n'est pas congru à 1 modulo 4 alors l'un des facteurs n'est pas congru à 1 modulo 4.

Soient $p_1, ..., p_r$ des nombres premiers distincts de 3 et congrus à 3 modulo 4.

Posons

$$N = 4p_1 \times p_2 \times \cdots p_r + 3.$$

Alors N admet une décomposition en facteurs premiers. Par la remarque préliminaire, ces facteurs premiers (congrus à 1 ou 3 modulo 4 car N impair) ne peuvent pas tous être congrus à 1 modulo 4 (car $N \not\equiv 1[4]$) et il existe donc q premier tel que $q \equiv 3[4]$ et $q \mid N$.

De plus pour tout $i \in [\![1, r]\!]$, on a $N \equiv 3[p_i]$ et par conséquent (comme p_i ne divise pas 3), p_i ne divise pas N. Enfin $N \equiv 4p_1 \times \cdots p_r[3]$ et (par théorème de Gauss) 3 ne divise pas $4 \times p_1 \times \cdots p_r$.

On en déduit que $q \notin \{3, p_1, p_2, ..., p_r\}$.

On a donc montré qu'étant donné un ensemble fini de nombres premiers congrus à 3 modulo 4 on peut construire un nombre premier congru à 3 modulo 4 qui n'est pas dans cet ensemble (et différent de 3).

Par conséquent (par l'absurde ou par argument combinatoire) il existe une infinité de nombres premiers congrus à 3 modulo 4 (et plus grands que 3).

2. On procède de même. Soient $p_1, ..., p_r$ des nombres premiers congrus à 5 modulo 6 et distincts de 5.

Posons

$$N = 6p_1...p_r + 5.$$

Alors N admet une décomposition en produit de facteurs premiers.

- ▷ Comme $N \equiv 1[2]$, 2 n'est pas parmi ces facteurs.
- ▷ Comme $N \equiv 2[3]$, 3 n'est pas parmi ces facteurs.
- ▷ Comme 5 ne divise pas $6 \times p_1 \times \cdots p_r$ (Gauss), 5 n'est pas parmi ces facteurs.
- ▷ Pour tout i, $N \equiv 5[p_i]$ et donc p_i n'est pas parmi ces facteurs.

Or tout nombre premier plus grand que 3 est congru à 1 ou 5 modulo 6 (car sinon divisible par 2 ou 3).

Comme un produit de facteurs tous congrus à 1 modulo 6 est aussi congru à 1 modulo 6 au moins un des facteurs premiers est congru à 5 modulo 6.

On a donc exhibé un nombre premier congru à 5 modulo 6 et n'étant pas dans $\{2, 3, 5, p_1, ..., p_r\}$.

Comme précédemment cela permet de conclure sur l'existence d'une infinité de tels nombres premiers.

Remarque: cette méthode ne se généralise pas forcément, par exemple il existe une infinité de nombres premiers congrus à 1 modulo 4 (cf plus loin) mais une telle preuve ne peut pas s'adapter à ce cas.

Solution pour l'exercice 26 · Énoncé p. 8 · Indication p. 32 (Infinité de nombres premiers dans certaines progressions arithmétiques II)
Par l'exercice 51, on a -1 est un carré modulo p (premier impair) ssi $(-1)^{\frac{p-1}{2}} \equiv 1[p]$ donc ssi $\frac{p-1}{2}$ est pair i.e ssi $p \equiv 1[4]$.

Soient $p_1, ..., p_r$ des nombres premiers.

Posons

$$N = (2 \times p_1 \times p_2 \times \cdots \times p_r)^2 + 1.$$

Alors N admet une décomposition en produit de facteurs premiers.

Pour tout $i \in [\![1, r]\!]$, $N \equiv 1[p_i]$ et donc p_i ne divise pas N.

De plus N est impair, donc tout facteur premier q de N est impair ; alors $(2 \times p_1 \times p_2 \times \cdots \times p_r)^2 \equiv -1[q]$, autrement dit -1 est un carré modulo q, et donc (par ce qui précède) q est congru à 1 modulo 4.

Par conséquent il existe un nombre premier distinct de $p_1, ..., p_r$ et congru à 1 modulo 4.

Et donc il y a une infinité de nombres premiers congrus à 1 modulo 4.

Solution pour l'exercice 27 · Énoncé p. 8 · Indication p. 32 (Un exemple de suite à divisibilité)

1. Soient $n, m \in \mathbb{N}$ tels que $m \mid n$.

Soit $q \in \mathbb{N}$ tel que $n = mq$.

On a par la formule de Bernoulli,

$$\begin{aligned} a^n - 1 &= a^{mq} - 1 \\ &= (a^m)^q - 1^q \\ &= (a^m - 1)\left(\sum_{k=0}^{q-1} (a^m)^k\right) \end{aligned}$$

et en particulier $a^m - 1 \mid a^n - 1$.

D'où $\boxed{f \text{ est croissante pour la divisibilité}}$.

2. On a

$$\begin{aligned} a^n - 1 &= a^{mq+r} - 1 \\ &= a^{mq}a^r - a^r + a^r - 1 \\ &= a^r(a^{mq} - 1) + (a^r - 1). \end{aligned}$$

par la formule de Bernoulli,

$$a^{mq} - 1 = (a^m)^q - 1^q = (a^m - 1)\left(\sum_{k=0}^{q-1} (a^m)^k\right)$$

et donc en particulier

$$a^m - 1 \mid a^{mq} - 1.$$

Par invariance du pgcd par transvection on a donc

$$\boxed{(a^n - 1) \wedge (a^m - 1) = (a^r - 1) \wedge (a^m - 1)}.$$

3. On observe que lorsqu'on effectue un algorithme d'Euclide pour calculer le pgcd de $f(n)$ et $f(m)$ on effectue de manière simultanée un algorithme d'Euclide pour calculer le pgcd de n et m.

Une façon de rédiger cela est d'effectuer une preuve algorithmique, ou bien d'effectuer une récurrence forte sur le variant de boucle.

Procédons par récurrence forte.

Pour $m \in \mathbb{N}$, notons

$$\mathcal{P}_m : \forall n \in \mathbb{N}, f(n) \wedge f(m) = f(n \wedge m).$$

▷ **Initialisation**

Pour $m = 0$, comme $f(0) = 0$, on a bien

$$\forall n \in \mathbb{N}, f(n) \wedge f(0) = f(n) = f(n \wedge 0).$$

D'où $\mathcal{P}_0$.

▷ **Hérédité**

Soit $m \in \mathbb{N}^*$.

Supposons que pour tout $k \in [\![0, m-1]\!]$, $\mathcal{P}_k$ est vraie.

Soit $n \in \mathbb{N}$.

Effectuons la division euclidienne de n par m

$$\begin{aligned} n &= mq + r \\ r &\in [\![0, m-1]\!]. \end{aligned}$$

Par la question précédente,

$$f(n) \wedge f(m) = f(m) \wedge f(r).$$

Comme $r < m$, par $\mathcal{P}_r$ on a donc

$$f(m) \wedge f(r) = f(m \wedge r).$$

Et comme $n = mq + r$, on a $m \wedge r = m \wedge n$.

Ainsi

$$f(n) \wedge f(m) = f(m \wedge n).$$

D'où $\mathcal{P}_m$.

▷ **Conclusion**

On a donc montré par récurrence forte que

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, \boxed{f(n) \wedge f(m) = f(n \wedge m)}.$$

Solution pour l'exercice 30 · Énoncé p. 9 · Indication p. 33 (Encore de l'arithmétique des suites de Fibonacci)

1. Pour $p \in \mathbb{N}$ notons $\mathcal{R}_p$:

$$\mathcal{R}_p : \forall n \in \mathbb{N}, F_{n+p} = F_p F_{n+1} + F_{p-1} F_n$$

et montrons par récurrence sur $p \in \mathbb{N}$, que pour tout $p \in \mathbb{N}$, $\mathcal{R}_p$.

▷ **Initialisation**

Pour $p = 1$, on a bien

$$\forall n \in \mathbb{N}, F_{n+1} = \underbrace{1}_{F_1} F_{n+1} + \underbrace{0}_{F_{1-1}} F_n.$$

▷ **Hérédité**

Soit $p \in \mathbb{N}^*$. Supposons $\mathcal{R}_p$.

Soit $n \in \mathbb{N}$.

On a:

$$\begin{aligned}
F_{n+(p+1)} &= F_{(n+1)+p} && (\text{par } \mathcal{R}_p) \\
&= F_p F_{n+2} + F_{p-1} F_{n+1} && (\text{par définition de la suite } (F_n)_{n\in\mathbb{N}}) \\
&= F_p(F_{n+1} + F_n) + F_{p-1} F_{n+1} && (\text{développement et factorisation}) \\
&= (F_p + F_{p-1}) F_{n+1} + F_p F_n && (\text{par définition de la suite } (F_n)_{n\in\mathbb{N}}) \\
&= F_{p+1} F_{n+1} + F_p F_n
\end{aligned}$$

D'où on a bien montré

$$\forall n \in \mathbb{N}, F_{n+(p+1)} = F_{p+1} F_{n+1} + F_{(p+1)-1} F_n$$

ce qui est $\mathcal{R}_{p+1}$.

▷ **Conclusion**

On a montré $\mathcal{R}_1$ et $\forall p \in \mathbb{N}^*, \mathcal{R}_p \Rightarrow \mathcal{R}_{p+1}$.

Par récurrence, on a donc bien montré que

$$\forall p \in \mathbb{N}^*, \forall n \in \mathbb{N}, F_{n+p} = F_p F_{n+1} + F_{p-1} F_n.$$

2. Soient $(n,m) \in \mathbb{N}^2$, sans perte de généralité, $n \geq m$. Si $n = m$ il n'y a rien à faire.

Sinon comme $n = m + (n-m)$ on a par la question précédente

$$F_n = F_{m+(n-m)} = F_{n-m}F_{m+1} + F_{n-m-1}F_m$$

par conséquent (invariance du pgcd par transvection)

$$F_m \wedge F_n = F_m \wedge \left(F_{n-m}F_{m+1} + F_{n-m-1}F_m\right) = F_m \wedge \left(F_{n-m}F_{m+1}\right)$$

et comme $F_m \wedge F_{m+1} = 1$ (cf exercice 20) on a

$$F_m \wedge \left(F_{n-m}F_{m+1}\right) = F_m \wedge F_{n-m}.$$

On a donc montré

$$\boxed{\forall (n,m) \in \mathbb{N}^2, n \geq m, F_m \wedge F_n = F_m \wedge F_{n-m}}.$$

L'idée est ensuite d'effectuer un algorithme d'Euclide simultané sur (n,m) et (F_n, F_m).

Une rédaction possible (ce n'est pas la seule) est de procéder par récurrence forte.

(La récurrence peut porter sur $n-m$, $n+m$, le plus petit des deux ou tout simplement en fixant un paramètre.)

Pour $n \in \mathbb{N}$, on note $\mathcal{H}_n$: «$\forall m \leq n, F_m \wedge F_n = F_{n\wedge m}$».

- **Initialisation**

  Pour $n = 0$, on a bien

  $$\forall m \in \mathbb{N}, F_0 \wedge F_m = 0 \wedge F_m = F_m = F_{0\wedge m}$$

  et c'est donc bien le cas en particulier pour $m \leq 0$.

  Donc $\mathcal{H}_0$ est vraie.
- **Hérédité**

  Soit $n \in \mathbb{N}$. Supposons que pour tout $k \in [\![0, n-1]\!]$, $\mathcal{H}_k$.

  Soit $m \leq n$.

  - Si $m = 0$ on a bien $F_0 \wedge F_n = F_n = F_{0\wedge n}$. De même si $m = n$, on a bien $F_n \wedge F_n = F_n = F_{n\wedge n}$.
  - Sinon on a vu que

    $$F_m \wedge F_n = F_m \wedge F_{n-m}$$

    Il y a alors deux possibilités:
    - Si $m \leq n-m$ alors comme $n-m \leq n-1$, par hypothèse de récurrence forte, $\mathcal{H}_{n-m}$ est vraie et donc

      $$F_m \wedge F_{n-m} = F_{n-m\wedge m} = F_{n\wedge m}.$$
    - Si $n-m < m$ alors comme $m \leq n-1$, par hypothèse de récurrence forte, $\mathcal{H}_m$ est vraie et donc

      $$F_m \wedge F_{n-m} = F_{n-m} \wedge F_m = F_{n-m\wedge m} = F_{n\wedge m}.$$

Par conséquent on a dans tous les cas

$$F_m \wedge F_n = F_m \wedge F_{n-m} = F_{n-m\wedge m} = F_{n\wedge m}.$$

On a donc bien $F_m \wedge F_n = F_{n\wedge m}$.

▷ **Conclusion**

Par récurrence, on a donc bien montré que

$$\boxed{\forall n \in \mathbb{N}, \forall m \in [\![0, n]\!], F_n \wedge F_m = F_{n\wedge m}}$$

Remarque: d'autres méthodes étaient possibles.

Par exemple de $F_m \wedge F_n = F_m \wedge F_{n-m}$ on en déduit par récurrence sur $q \in \mathbb{N}$ immédiate que pour tout $q \in \mathbb{N}$ tel que $n - qm \geq 0$ on a

$$F_m \wedge F_n = F_m \wedge F_{n-qm}$$

ce qui simplifie la preuve algorithmique en prenant q le quotient de la division euclidienne de n par m.

Solution pour l'exercice 39 · Énoncé p. 11 · Indication p. 34 (Formule de Wilson)

1. Comme p est premier on a $x^2 \equiv 1[p]$ ssi $(x-1)(x+1) \equiv 0[p]$ ssi $x \equiv \pm 1[p]$, c'est à dire que les seuls éléments modulo p qui sont leurs propres inverses sont 1 et -1.

Ainsi tout élément entre 2 et $p-2$ est distinct de son inverse et dans le produit

$$2 \times 3 \times \cdots (p-2)$$

on peut regrouper chaque élément avec son inverse pour obtenir

$$2 \times 3 \times \cdots (p-2) \equiv 1[p].$$

Par exemple modulo 11 on effectue le regroupement

$$\begin{aligned} 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 &\equiv (2 \times 6) \times (3 \times 4) \times (5 \times 9) \times (7 \times 8)[p] \\ &\equiv 1 \times 1 \times 1 \times 1 \qquad [p] \end{aligned}$$

Et par conséquent en multipliant par $1 \times (p-1) \equiv -1[p]$ on en déduit

$$(p-1)! \equiv -1[p].$$

Remarque: Une autre méthode pour démontrer ce résultat est d'utiliser des polynômes dans $\frac{\mathbb{Z}}{p}\mathbb{Z}[X]$: comme les polynômes $X^{p-1} - 1$ et $(X-1)(X-2)\cdots(X-(p-1))$ coïncident en $p-1$ points (par le petit théorème de Fermat) et sont unitaires de degré $p-1$ on en déduit qu'ils sont égaux. Les relations de Viète entre coefficients et racines permettent alors de conclure.

Remarque: Pour formaliser ce regroupement le plus simple est de regrouper selon la relation d'équivalence $a \sim b$ ssi $a = b$ ou $ab \equiv 1[p]$. Alors toutes les classes d'équivalence contiennent deux éléments sauf celles de 1 et de -1.

2. On procède par disjonction de cas.

▷ Supposons que n n'est pas le carré d'un nombre premier.

Soit par exemple $a \geq 2$ le plus petit diviseur non trivial de n (qui est donc premier) et b tel que $n = ab$.

Comme n est composé, $a, b < n$, et comme n n'est pas le carré d'un nombre premier, $b \neq a$.

De plus dans le produit

$$(n-1)! = 1 \times 2 \times \cdots \times \cdots a \times \cdots \times b \times \cdots (n-1)$$

apparaît le facteur ab et donc $n \mid (n-1)!$.

Par exemple modulo 8 on a

$$\begin{aligned} 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 &\equiv (2 \times 4) \times \cdots [n] \\ &\equiv 0 \qquad\qquad [n]. \end{aligned}$$

▷ Supposons que n est le carré d'un nombre premier p.

On a $p \times (2p) = 2p^2 = 2n$ qui est divisible par n.

De plus comme $n > 4$, $p > 2$ et donc $2p < p^2 - 1$ (car $(p-1)^2 - 2 > 0$).

Donc dans le produit

$$(n-1)! = 1 \times 2 \times \cdots \times \cdots p \times \cdots \times 2p \times \cdots (n-1)$$

apparaît le facteur $p \times 2p$ et donc $n \mid (n-1)!$.

Par exemple modulo 9,

$$\begin{aligned} 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 &\equiv (3 \times 6) \times \cdots [n] \\ &\equiv 0 \qquad\qquad [n]. \end{aligned}$$

Remarque: il reste le cas $n = 4$ à traiter.

On a alors $(4-1)! \equiv 2[4]$.

Solution pour l'exercice 52 · Énoncé p. 16 (RSA)

Posons $a = ed$.

Comme $a \equiv 1[p-1]$: si $p \nmid M$, le petit théorème de Fermat donne $M^{p-1} \equiv 1[p]$, donc $M^{a-1} \equiv 1[p]$ (car $(p-1) \mid (a-1)$) et $M^a \equiv M[p]$; et si $p \mid M$, alors $M^a \equiv 0 \equiv M[p]$. Dans les deux cas $M^a \equiv M[p]$.

De même, si $q \nmid M$ on a $M^{a-1} \equiv 1[q]$ donc $M^a \equiv M[q]$, et si $q \mid M$ alors $M^a \equiv 0 \equiv M[q]$; dans tous les cas $M^a \equiv M[q]$.

Comme $p \mid M^a - M$ et $q \mid M^a - M$ et que p et q premiers entre eux on conclut que $pq \mid M^a - M$ c'est à dire $M^a \equiv M[pq]$.

Remarque: ce résultat est à la base de l'algorithme RSA très utilisé en cryptographie. En effet, en posant $n = pq$, pour chiffrer le message M la connaissance de e et de n suffit. Mais pour le déchiffrer la connaissance de d est nécessaire. Et pour retrouver d à partir de e et n il faut calculer p et q, ce qui est un problème complexe.

Solution pour l'exercice 61 · Énoncé p. 19 · Indication p. 37 (Division euclidienne dans les entiers de Gauss)
On propose deux preuves: une première adaptant la preuve usuelle dans $\mathbb{Z}$ ou $\mathbb{K}[X]$, et une seconde utilisant $\mathbb{Z}[i] \subset \mathbb{C}$ et une intuition géométrique.

▷ **Version 1**

Considérons

$$\{|a - b\gamma|^2, \gamma \in \mathbb{Z}[i]\} \subset \mathbb{N}$$

qui est un sous-ensemble non vide de $\mathbb{N}$.

Il existe alors $\boxed{q \in \mathbb{Z}[i]}$ tel que

$$|a - bq|^2 = \min_{\gamma \in \mathbb{Z}[i]} (|a - b\gamma|^2).$$

Posons $\boxed{r = a - bq}$. Il reste à montrer que $|r|^2 < |b|^2$.

Supposons par l'absurde que $|r| \geq |b|$.

Pour tout $\omega \in \{1, i, -1, -i\}$, on a

$$|a - b(q + \omega)|^2 = |r - b\omega|^2 = |r|^2 + |b|^2 - 2\,\mathrm{Re}(\overline{r}b\omega).$$

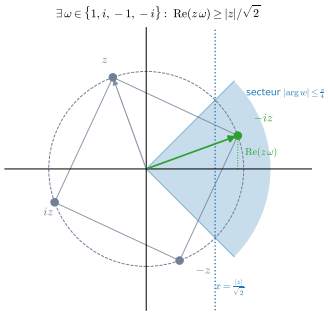
Mais pour tout $z \in \mathbb{C} \setminus \{0\}$ il existe $\omega \in \{1, i, -1, -i\}$ tel que $\mathrm{Re}(z\omega) \geq \frac{|z|}{\sqrt{2}}$.

En effet avec $z = |z|\ e^{i\theta}$, on a pour tout $k \in [\![0, 3]\!]$, comme $i^k \in \{1, i, -1, -i\}$,

$$\mathrm{Re}\big(zi^k\big) = |z| \cos\Big(\theta + k\frac{\pi}{2}\Big).$$

Or les quatre arguments $\theta + k\frac{\pi}{2}$, $k \in [\![0, 3]\!]$, étant espacés de $\frac{\pi}{2}$, l'un d'eux, disons $\theta + k_0\frac{\pi}{2}$, appartient à $\left[-\frac{\pi}{4}, \frac{\pi}{4}\right]$ modulo 2π. Sur cet intervalle $\cos(\theta + k_0\frac{\pi}{2}) \geq \cos(\frac{\pi}{4}) = \frac{1}{\sqrt{2}}$, d'où, en posant $\omega = i^{k_0}$,

$$\mathrm{Re}(z\omega) = |z| \cos\Big(\theta + k_0\frac{\pi}{2}\Big) \geq \frac{|z|}{\sqrt{2}}.$$



Par conséquent, en choisissant $\omega \in \{1, i, -1, -i\}$ tel que $\mathrm{Re}(\overline{r}b\omega) \geq \frac{|\overline{r}b|}{\sqrt{2}} = \frac{|r||b|}{\sqrt{2}}$, on a,

$$\begin{aligned}|a-b(q+\omega)|^2 &\leq |r|^2+|b|^2-2\frac{|r\|b|}{\sqrt{2}}\\ &\leq |r|^2+|b|^2-\sqrt{2}|b|^2\\ &< |r|^2\end{aligned}$$

ce qui contredit l'hypothèse de minimalité.

D'où

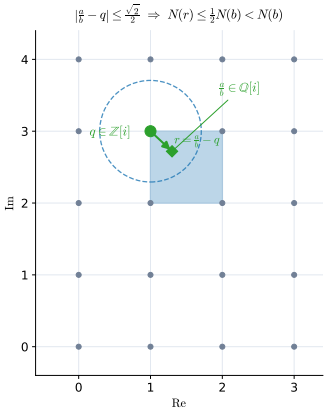
$$\boxed{|r|^2<|b|^2.}$$

▷ **Version 2**

On a

$$\frac{a}{b}\in\mathbb{C}$$

(c'est même un élément de $\mathbb{Q}[i]$).



Or pour tout $z\in\mathbb{C}$ il existe $q\in\mathbb{Z}[i]$ tel que $|z-q|\leq\frac{1}{\sqrt{2}}$.

En effet avec $x,y\in\mathbb{Z}$ tels que

$$|\operatorname{Re}(z)-x|\leq\frac{1}{2}$$
$$|\operatorname{Im}(z)-y|\leq\frac{1}{2}$$

on a alors

$$|z-(x+iy)|^2=|\operatorname{Re}(z)-x|^2+|\operatorname{Im}(z)-y|^2\leq\frac{1}{4}+\frac{1}{4}=\frac{1}{2}.$$

et donc $q=x+iy$ convient.

Par conséquent en posant $\boxed{q\in\mathbb{Z}[i]}$ tel que $|\frac{a}{b}-q|\leq\frac{1}{\sqrt{2}}$ et $\boxed{r=a-bq}$, on a

$$a=bq+r$$

et

$$|r|^2 = |a-bq|^2 = |b|^2\ |\frac{a}{b} - q|^2$$
$$\leq |b|^2\ \frac{1}{2}$$

et donc en particulier

$$\boxed{|r|^2 < |b|^2}.$$

Solution pour l'exercice 65 · Énoncé p. 20 · Indication p. 38 (Pourquoi réfléchir quand on peut trinomer)
Le plus simple est de reconnaître un **trinôme du second degré**.

Avec $x = n^2$, n est solution de l'équation ssi

$$x^2 - 7x + 12 = 0.$$

Il s'agit d'un trinôme du second degré de discriminant

$$\Delta = 7^2 - 4 \times 12 = 1 > 0$$

et donc ayant deux racines réelles

$$\frac{7 \pm 1}{2}.$$

Donc n est solution ssi $n^2 = 4$ ou $n^2 = 3$.

Or $n^2 = 4$ admet deux solutions entières: $n = 2$ et $n = -2$.

Et $n^2 = 3$ n'admet aucune solution entière (passer par exemple aux valuations 3-adiques pour montrer qu'il n'y a pas de solutions rationnelles ou majorer et remarquer que $\pm 1, \pm 2$ ne sont pas solutions).

On conclut donc que l'ensemble des solutions entières est

$$\boxed{\{-2, 2\}}.$$

Solution pour l'exercice 66 · Énoncé p. 21 · Indication p. 38 (Majorations successives)

1. Il y a plusieurs méthodes.

Première option: majoration

Soient a et b deux entiers strictement positifs vérifiant

$$\frac{1}{a} + \frac{1}{b} = 1.$$

Quitte à changer l'ordre on peut supposer que $0 < a \leq b$.

Dans ce cas on a

$$0 < \frac{1}{b} \leq \frac{1}{a}$$

et donc

$$\frac{1}{a}+\frac{1}{b}\leq\frac{2}{a}.$$

d'où on déduit

$$0<a\leq 2.$$

Il suffit alors de regarder $a=1$ et $a=2$.

- ▹ Pour $a=1$, $\frac{1}{b}+1=1$ n'admet pas de solution.
- ▹ Pour $a=2$, $\frac{1}{b}+\frac{1}{2}=1$ admet $b=2$ comme solution.

La seule solution est donc

$$\boxed{(a,b)=(2,2).}$$

Deuxième option: résolution dans $\mathbb{R}$

Si a et b sont solutions alors $a\neq 1$ et

$$b=\frac{a}{a-1}.$$

Donc comme a et b sont entiers $a-1\mid a$ et donc $a-1\mid a-(a-1)$.

On en déduit que $a-1=1$ donc $a=2$.

Et donc $b=2$.

La seule solution est donc

$$\boxed{(a,b)=(2,2).}$$

2. Soient a , b et c trois entiers strictement positifs vérifiant

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=1.$$

Quitte à changer l'ordre on peut supposer que $0<a\leq b\leq c$.

Dans ce cas on a

$$0<\frac{1}{c}\leq\frac{1}{b}\leq\frac{1}{a}$$

et donc

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\leq\frac{3}{a}.$$

d'où on déduit

$$0<a\leq 3.$$

Il suffit alors de regarder $a=1$, $a=2$ et $a=3$.

- ▹ Pour $a=1$, $1+\frac{1}{b}+\frac{1}{c}=1$ n'admet pas de solution.
- ▹ Pour $a=2$, $\frac{1}{2}+\frac{1}{b}+\frac{1}{c}=1$ revient à

$$\frac{1}{b}+\frac{1}{c}=\frac{1}{2}.$$

Comme $0<b\leq c$, par le même raisonnement que précédemment on a

$$\frac{1}{2}\leq\frac{2}{b}$$

c'est à dire $b\leq 4$. De plus $b\geq a=2$. Il suffit donc de regarder $b=2$, $b=3$ et $b=4$.

- Pour $b=2$,

$$\frac{1}{2}+\frac{1}{c}=\frac{1}{2}$$

n'admet pas de solution.

- Pour $b=3$,

$$\frac{1}{3}+\frac{1}{c}=\frac{1}{2}$$

admet $c=6$ comme solution.

- Pour $b=4$,

$$\frac{1}{4}+\frac{1}{c}=\frac{1}{2}$$

admet $c=4$ comme solution.

- Pour $a=3$, $\frac{1}{3}+\frac{1}{b}+\frac{1}{c}=1$ revient à

$$\frac{1}{b}+\frac{1}{c}=\frac{2}{3}.$$

Comme $0<b\leq c$, par le même raisonnement que précédemment on a

$$\frac{2}{3}\leq\frac{2}{b}$$

c'est à dire $b\leq 3$. De plus $b\geq a=3$. Il suffit donc de regarder $b=3$.

- Pour $b=3$,

$$\frac{1}{3}+\frac{1}{c}=\frac{2}{3}$$

admet $c=3$ comme solution.

Les solutions vérifiant $a\leq b\leq c$ sont donc $(2,3,6)$, $(2,4,4)$ et $(3,3,3)$.

En comptant les permutations de ces solutions, on obtient donc $6+3+1$ c'est à dire

10 triplets solutions.

Solution pour l'exercice 67 · Énoncé p. 21 · Indication p. 38 (Étude de fonction)
On observe que $a=b$ est toujours solution.

Fixons a et résolvons

$$a^x = x^a$$

d'inconnue $x \in \mathbb{R}$.

En passant au ln l'équation se réécrit

$$\frac{\ln(x)}{x} = \frac{\ln(a)}{a}.$$

Posons

$$\begin{aligned} f :]0, +\infty[&\to \mathbb{R} \\ x &\mapsto \frac{\ln(x)}{x} - \frac{\ln(a)}{a} \end{aligned}$$

et étudions la fonction f.

La fonction f est dérivable sur son ensemble de définition, et sa dérivée est, pour tout $x > 0$

$$f'(x) = \frac{\frac{1}{x} \times x - \ln(x) \times 1}{x^2} = \frac{1 - \ln(x)}{x^2}.$$

La fonction f est donc
- ▹ **croissante** sur $]0, e^1[$
- ▹ puis **décroissante** sur $]e^1, +\infty[$.

Comme de plus $f(a) = 0$,

- ▹ Si $a > e^1$ on a le tableau de variations

  et l'équation $f(x) = 0$ admet une unique solution dans $]0, a[$ et n'admet aucune solution dans $]a, +\infty[$.
- ▹ Si $1 < a < e^1$ on a le tableau de variations

  et l'équation $f(x) = 0$ n'admet aucune solution dans $]0, a[$ et admet une unique solution dans $]a, +\infty[$.

Retournons au problème initial.

Quitte à réordonner on peut supposer $a < b$.

Si $a > e^1$ il n'y a donc pas de solution.

Comme a est un entier strictement positif et que $e^1 < 3$ il suffit donc de regarder $a = 1$ et $a = 2$.

- ▹ Pour $a = 1$, $1^b = b^1$ n'admet pas de solution $b > 1$.
- ▹ Pour $a = 2$, $2^b = b^2$ admet $b = 4$ comme solution, et par l'étude précédente c'est la seule.

On conclut donc que la seule solution avec $a < b$ est $a = 2$ et $b = 4$.

Par conséquent l'ensemble des solutions est

$$\boxed{\{(n, n), n \in \mathbb{N}^*\} \cup \{(2, 4), (4, 2)\}}.$$

Remarque: il aurait été bien plus simple de, dès le début
- ▹ supposer $a < b$
- ▹ transformer le problème en

$$\frac{\ln(a)}{a} = \frac{\ln(b)}{b}$$

et étudier $\frac{\ln(x)}{x}$ sur $]0,+\infty[$. On en déduit directement que

$$a < e^1 < b.$$

Solution pour l'exercice 69 · Énoncé p. 21 · Indication p. 38 (Une question du CG 1990)
On remarque tout d'abord que si n et m conviennent alors avec

$$\frac{1}{x_1^2} + \cdots + \frac{1}{x_n^2} = 1$$

et

$$\frac{1}{y_1^2} + \cdots + \frac{1}{y_m^2} = 1$$

on a

$$\begin{aligned}\frac{1}{(x_1y_1)^2} + \cdots + \frac{1}{(x_1y_m)^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} &= \left(\frac{1}{y_1^2} + \cdots + \frac{1}{y_m^2}\right)\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} \\ &= \frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} = 1\end{aligned}$$

et donc $n+m-1$ convient aussi.

On cherche donc ce qui se passe pour les petits cas, en espérant ensuite reconstituer tous les entiers assez grands à partir de ces derniers.

- Pour $n = 1$ on a bien

$$\frac{1}{1^2} = 1$$

- Pour $n = 2$, si

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} = 1$$

alors en supposant $1 < x_1 \leq x_2$ on a

$$1 = \frac{1}{x_1^2} + \frac{1}{x_2^2} \leq \frac{2}{x_1^2} \leq \frac{2}{4} = \frac{1}{2} < 1$$

et donc pas de solutions.

- Pour $n = 3$, de même si

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} = 1$$

alors en supposant $1 < x_1 \leq x_2 \leq x_3$ on a

$$1 = \frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} \leq \frac{3}{x_1^2} \leq \frac{3}{4} < 1$$

et donc pas de solutions.

- ▷ Pour $n = 4$ on peut remarquer directement que

$$\frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^2} = 1.$$

Donc $n = 4$ convient.

- ▷ Pour $n = 5$, on majore comme dans les exercices précédents. Plus précisément si

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} + \frac{1}{x_4^2} + \frac{1}{x_5^2} = 1$$

, en se ramenant à $1 < x_1 \leq x_2 \leq x_3 \leq x_4 \leq x_5$ on obtient

$$1 \leq \frac{5}{x_1^2}$$

donc $1 < x_1 \leq \sqrt{5}$. Il suffit de regarder $x_1 = 2$.

Dans ce cas on obtient

$$\frac{1}{x_2^2} + \frac{1}{x_3^2} + \frac{1}{x_4^2} + \frac{1}{x_5^2} = \frac{3}{4}$$

et donc de même

$$\frac{3}{4} \leq \frac{4}{x_2^2}$$

d'où $x_1 = 2 \leq x_2 \leq \sqrt{\frac{16}{3}} < 3$. Il suffit donc de regarder $x_2 = 2$.

Dans ce cas on obtient

$$\frac{1}{x_3^2} + \frac{1}{x_4^2} + \frac{1}{x_5^2} = \frac{1}{2}$$

et donc de même

$$\frac{1}{2} \leq \frac{3}{x_3^2}$$

d'où $x_2 = 2 \leq x_3 \leq \sqrt{6} < 3$. Il suffit donc de regarder $x_3 = 2$.

Dans ce cas on obtient

$$\frac{1}{x_4^2} + \frac{1}{x_5^2} = \frac{1}{4}$$

et donc de même

$$\frac{1}{4} \leq \frac{2}{x_4^2}$$

d'où $x_3 = 2 \leq x_4 \leq \sqrt{8} < 3$. Il suffit donc de regarder $x_4 = 2$.

Dans ce cas on obtient

$$\frac{1}{x_5^2} = 0$$

qui n'admet pas de solution.

- Pour $n = 6$ on peut de même que précédemment effectuer des majorations en chaîne pour se ramener à un nombre fini de cas à traiter.

  Plus précisément, en ordonnant de même que précédemment $1 < x_1 \leq x_2 \leq x_3 \leq x_4 \leq x_5 \leq x_6$ on obtient successivement

  $$1 \leq \frac{6}{x_1^2}$$

  c'est à dire $1 < x_1 \leq \sqrt{6} < 3$ et il suffit donc de regarder $x_1 = 2$. On obtient alors

  $$\frac{3}{4} \leq \frac{5}{x_2^2}$$

  c'est à dire $x_1 = 2 \leq x_2 \leq \sqrt{\frac{20}{3}} < 3$ et il suffit donc de regarder $x_2 = 2$. On obtient alors

  $$\frac{1}{2} \leq \frac{4}{x_3^2}$$

  c'est à dire $x_2 = 2 \leq x_3 \leq \sqrt{8} < 3$ et il suffit donc de regarder $x_3 = 2$. On obtient alors

  $$\frac{1}{4} \leq \frac{3}{x_4^2}$$

  c'est à dire $x_3 = 2 \leq x_4 \leq \sqrt{12} < 4$ et il suffit donc de regarder $x_4 = 2$ ou $x_4 = 3$. Pour $x_4 = 2$ on obtiendrait que la somme restante est nulle, ce qui est impossible. Il suffit donc de regarder $x_4 = 3$. On obtient alors

  $$\frac{1}{4} - \frac{1}{9} \leq \frac{2}{x_5^2}$$

  c'est à dire $x_4 = 3 \leq x_5 \leq \sqrt{\frac{72}{5}} < 4$ il suffit donc de regarder $x_5 = 3$.

  On obtient alors

  $$\frac{1}{x_6^2} = \frac{5}{36} - \frac{1}{9}$$

  et $x_6 = 6$ convient.

  Par conséquent on obtient une solution qui est $(2, 2, 2, 3, 3, 6)$.
- Le cas $n = 7$ se construit à partir des précédents car $7 = 4 + 4 - 1$.
- Pour $n = 8$ après avoir effectué des majorations et regardé un nombre fini de cas on obtient que $(2, 2, 2, 3, 3, 9, 9, 18)$ est solution.
- Tous les entiers ≥ 9 conviennent. En effet par le cas $n = 4$, si m convient alors $m + 3$ convient. Et les cas $6, 7, 8$ conviennent.

En conclusion les entiers n qui conviennent sont $\boxed{\text{tous les entiers sauf 2, 3, 5}}$.

Solution pour l'exercice 70 · Énoncé p. 22 · Indication p. 39 (Équations en vrac)

1. On regarde modulo 4.

On a pour tous $n, m \in \mathbb{N}$, $n^4 = \left(n^2\right)^2$ est congru à 0 ou 1 modulo 4. Donc $n^4 - m^4$ est congru à 0, 1, -1.

Or

$$42 \equiv 2[4]$$

et par conséquent il n"y a pas de solution.

2. On cherche donc les n tels que l'équation

$$5^n + 4 = a^2.$$

Ce qui peut se réécrire

$$5^n = a^2 - 4.$$

En reconnaissant une identité remarquable, cela revient à

$$(a-2)(a+2) = 5^n.$$

Par conséquent, comme 5 est premier, on en déduit que $a-2$ et $a+2$ sont des puissances de 5, i.e il existe r et s entiers tels que

$$\begin{aligned} a+2 &= 5^r \\ a-2 &= 5^s. \end{aligned}$$

Leur différence est donc, en supposant quitte à changer l'ordre que $r \geq s$,

$$\begin{aligned} (a+2) - (a-2) = 4 &= 5^r - 5^s \\ &= 5^s(5^{r-s} - 1). \end{aligned}$$

La seule possibilité est donc $s = 0$ et $r - s = 1$.

On en déduit que si n est solution alors $5^n + 4 = 9$.

On vérifie que $5^1 + 4 = 9$.

Par conséquent il existe une unique solution qui est

$$\boxed{n = 1}$$

Solution pour l'exercice 71 · Énoncé p. 22 · Indication p. 39 (Réduction donc impossibilité)

1. On regarde modulo 4.

Comme un carré est congru à 0 ou 1 modulo 4 on a

$$a^2 + b^2 \equiv 0, 1 \text{ ou } 2 \bmod 4.$$

Mais

$$2023 \equiv 3 \bmod 4.$$

Donc il n"y a pas de solution.

2. On regarde modulo 4.

Tout d'abord comme a^5 est de même parité que a, on a a est pair. Soit $\tilde{a} \in \mathbb{Z}$ tel que $a = 2\tilde{a}$. Alors l'équation devient

$$2^5\tilde{a}^5 - 2b^2 = 528$$

et donc

$$b^2 = 16\tilde{a}^5 - 264$$

en particulier b est pair.

Soit $\tilde{b} \in \mathbb{Z}$ tel que $b = 2\tilde{b}$. Alors l'équation devient

$$4\tilde{a}^5 - \tilde{b}^2 = 66$$

et donc modulo 4 on obtient

$$-\tilde{b}^2 \equiv 2 \bmod 4$$

ce qui est impossible.

Donc | il n"y a pas de solution |.

3. On regarde modulo 11.

On a $110007 \equiv 7 \bmod 11$.

La table des carrés et des puissances 5-ièmes modulo 11 est

$x \bmod 11$	0	1	2	3	4	5	6	7	8	9	10
$x^2 \bmod 11$	0	1	4	9	5	3	3	5	9	4	1
$x^5 \bmod 11$	0	1	10	1	1	1	10	10	10	1	10

D'où le tableau de possibilités

	0	1	2	3	4	5	6	7	8	9	10
0	0	9	3	4	1	5	5	1	4	3	9
1	1	10	4	5	2	6	6	2	5	4	10
2	10	8	2	3	0	4	4	0	3	2	8
3	1	10	4	5	2	6	6	2	5	4	10
4	1	10	4	5	2	6	6	2	5	4	10
5	1	10	4	5	2	6	6	2	5	4	10
6	10	8	2	3	0	4	4	0	3	2	8
7	10	8	2	3	0	4	4	0	3	2	8
8	10	8	2	3	0	4	4	0	3	2	8
9	1	10	4	5	2	6	6	2	5	4	10
10	10	8	2	3	0	4	4	0	3	2	8

Et il est donc impossible d'avoir

$$a^5 - 2b^2 \equiv 7 \bmod 11.$$

L'équation n'admet donc $\boxed{\text{pas de solution}}$.

Remarque: Pourquoi modulo 11 ? On cherche un entier n pour lequel les puissances 2 et 5 sont simples modulo n. Comme le ppcm de 2 et 5 est 10 on cherche par exemple n tel que $\varphi(n) = 10$ ce qui permet de simplifier toutes les puissances 10ème. Ici 11 convient car 11 est premier et $11 - 1 = 10$.

Solution pour l'exercice 72 · Énoncé p. 22 · Indication p. 39 (Une question du Bac 2003)
On observe que $x = y = z = 0$ est solution.

Montrons que c'est la seule.

Soit $(x, y, z) \neq (0, 0, 0)$ une solution. Sans perte de généralité on peut supposer $x \neq 0$.

On peut écrire modulo 7

$$x^2 \equiv -y^2 \bmod 7.$$

Supposons que $7 \nmid x$. Comme $7 \nmid x$, comme 7 est premier, x est inversible modulo 7.

En notant ξ un inverse de x modulo 7, i.e un entier tel que

$$x\xi \equiv 1 \bmod 7$$

et en multipliant par ξ^2 on en déduit

$$(\xi y)^2 \equiv -1 \bmod 7.$$

Or la table des carrés modulo 7 est:

$x \bmod 7$	0	1	2	3	4	5	6
$x^2 \bmod 7$	0	1	4	2	2	4	1

et on aboutit donc à une contradiction.

Donc pour toute solution non nulle $7 \mid x$.

Si $7 \mid x$ alors $7 \mid y$ et donc en posant $x = 7\tilde{x}$ et $y = 7\tilde{y}$ on obtient

$$7\tilde{x}^2 + 7\tilde{y}^2 = z^2$$

donc on peut écrire $z = 7\tilde{z}$. Et obtient alors

$$\tilde{x}^2 + \tilde{y}^2 = 7\tilde{z}^2.$$

On obtient donc une solution $(\tilde{x}, \tilde{y}, \tilde{z})$ avec $0 < \tilde{x} < x$.

Par principe de descente infinie il n'existe pas de solution non nulle.

Remarque: ici le point clé est que -1 n'est pas carré modulo le nombre premier 7. Un résultat très classique est que -1 est un carré modulo le nombre premier impair p ssi $p \equiv 1 \bmod 4$.

Solution pour l'exercice 81 · Énoncé p. 25 · Indication p. 40 (Crible mystère I)

1. On note $\texttt{spf}(k)$ le plus petit diviseur premier d'un entier $k \geq 2$ (de sorte que $\texttt{spf}(p) = p$ lorsque p est premier). Les indices de `ppdp` vont de 0 à N. On montre par récurrence (forte) sur $i \in [\![2, N+1]\!]$ l'invariant suivant :

au début de l'itération de la boucle «`while i<=N:`» associée à la valeur i :

- `lp` contient, dans l'ordre croissant, tous les nombres premiers strictement inférieurs à i ;
- pour tout $k \in [\![2, i]\!]$ tel que $k \leq N$,

$$\texttt{ppdp}[k] = \begin{cases} \min(\{p \in \texttt{lp} \mid p \text{ divise } k\}) & \text{si } \exists p \in \texttt{lp}\ ,\ p \text{ divise } k \\ k & \text{sinon.} \end{cases}$$

Comme `lp` contient à cet instant tous les premiers $< i$, ce membre de droite vaut toujours $\texttt{spf}(k)$: le premier cas s'applique dès que $\texttt{spf}(k) < i$, et sinon $\texttt{spf}(k) = i = k$ (k est alors premier) et le second cas donne aussi $k = \texttt{spf}(k)$. Bref, l'invariant affirme que $\boldsymbol{\texttt{ppdp}[k] = \texttt{spf}(k) \text{ pour tout } k \in [\![2, \min(i, N)]\!]}$.

Initialisation ($i = 2$). Avant la première itération, `lp` est vide (aucun premier < 2) et `ppdp[k] = k` pour tout k ; comme $\texttt{spf}(2) = 2$, l'invariant est vrai.

Hérédité. Supposons l'invariant vrai au début de chaque itération $2, ..., i$ (avec $i \leq N$), et décrivons l'itération i.

- Par hypothèse $\texttt{ppdp[i]} = \texttt{spf}(i)$, qui vaut i si et seulement si i est premier. Le test `ppdp[i] == i` (ligne 7) ajoute donc i à `lp` exactement lorsque i est premier : après la ligne 8, `lp` contient tous les premiers $\leq i$, dans l'ordre croissant.
- La boucle interne (lignes 10–12) écrit `ppdp[i*lp[j]] = lp[j]`. Les indices modifiés $i \cdot \texttt{lp}[j] \geq 2i > i$ ne touchent aucune case $k \leq i$: l'invariant reste vrai sur $[\![2, \min(i, N)]\!]$.
- Reste la case $k = i+1$ (lorsque $i+1 \leq N$). Si $i+1$ est premier, il n'a jamais pu être marqué — un marquage écrit à un indice $i'' \cdot \texttt{lp}[j]$, produit d'au moins deux facteurs ≥ 2, donc composé — d'où $\texttt{ppdp[i+1]} = i+1 = \texttt{spf}(i+1)$. Si $i+1$ est composé, écrivons $i+1 = i'p$ avec $p = \texttt{spf}(i+1)$; comme p est le plus petit facteur premier du composé $i+1$, on a $p^2 \leq i+1$, donc $i' \geq p \geq 2$, et $2i' \leq i'p = i+1 \leq 2i$ donne $i' \leq i$. À l'itération $i' \leq i$, l'hypothèse de récurrence donne $\texttt{ppdp[i']} = \texttt{spf}(i')$; comme tout diviseur premier de i' est $\geq p$, on a $p \leq \texttt{spf}(i') = \texttt{ppdp[i']}$, et $p \in \texttt{lp}$ (p premier et $p \leq i'$, ajouté au plus tard au début de l'itération i' si $p = i'$), et $i'p = i+1 \leq N$. La boucle interne de l'itération i' atteint bien l'indice de p (les $\texttt{lp}[j] < p$ vérifient $\texttt{lp}[j] < p \leq \texttt{ppdp}[i']$ et $i'\ \texttt{lp}[j] < i'p \leq N$, donc elle ne s'arrête pas avant) et exécute donc `ppdp[i+1] =` $p = \texttt{spf}(i+1)$. Enfin, cette case n'est marquée qu'à cette seule itération : tout marquage $i''q = i+1$ (avec $q \in \texttt{lp}$ premier) vérifie $q \leq \texttt{ppdp}[i''] = \texttt{spf}(i'')$ par récurrence forte, puisque $i'' \leq (i+1)/2 \leq i$; or q divise $i+1$ donc $q \geq p$, et si $q > p$ alors p divise i'' (car p divise $i+1$ et $p \neq q$), d'où $\texttt{spf}(i'') \leq p < q$, contradiction ; donc $q = p$ et $i'' = i'$. Ainsi, au début de l'itération $i+1$, on a bien $\texttt{ppdp[i+1]} = p = \texttt{spf}(i+1)$.

L'invariant est donc vrai au début de l'itération $i+1$, ce qui achève la récurrence.

Conclusion. À la sortie de la boucle ($i = N + 1$), l'invariant donne : `lp` est la liste des nombres premiers $\leq N$, et `ppdp[k]` $=$ `spf`(k) pour tout $k \in [\![2, N]\!]$. Ainsi, pour tout entier $N \geq 2$, `mystere1`(N) renvoie un tuple constitué de
- ▷ la liste des nombres premiers inférieurs ou égaux à N
- ▷ une liste de longueur $N + 1$ dont le k-ième élément (pour tout k entre 2 et N) est le plus petit diviseur premier de k (et 0 en 0, 1 en 1, inchangés depuis l'initialisation).

2. Le corps de la boucle interne (ligne 11) effectue un marquage `ppdp[i*lp[j]] = lp[j]` en temps constant ; comptons le nombre total de tels marquages.

Soit $n \geq 2$ un nombre composé, $n \leq N$. Alors n s'écrit de manière unique $n = pQ$ avec p le plus petit diviseur premier de n et tous les diviseurs premiers de Q supérieurs ou égaux à p. Autrement dit, l'écriture de n sous la forme $n = i * \texttt{lp}[j]$ (ligne 11) où `lp[j] <= ppdp[i]` (et `j < len(lp)` pour la bonne définition, et `i * lp[j] <= N` car $n \leq N$) existe et est unique : elle correspond à $i = Q$ et $\texttt{lp}[j] = p$. Chaque entier composé $\leq N$ est donc marqué **exactement une fois**, et les nombres premiers ne sont jamais marqués.

Le nombre total d'exécutions du corps de la boucle interne est ainsi majoré par le nombre d'entiers composés $\leq N$, donc par N. En ajoutant, pour chacune des $N - 1$ valeurs de i, le coût $O(1)$ de l'itération externe et du test d'arrêt de la boucle interne, on effectue $O(N)$ opérations élémentaires au total : la complexité est en

$$\boxed{O(N)}.$$

(C'est la condition d'arrêt `lp[j] <= ppdp[i]`, qui interrompt la boucle interne dès le plus petit diviseur premier de i, qui garantit ce marquage unique et rend le crible linéaire.)

3. On peut effectuer plusieurs commentaires:
- ▷ Tout d'abord l'algorithme du crible d'Ératosthène peut **s'adapter** sans complexité supplémentaire pour non seulement renvoyer la liste des nombres premiers mais aussi déterminer les plus grands (ou plus petits) diviseurs premiers.
- ▷ A priori, par un raisonnement similaire à celui de la première question, la complexité de l'algorithme d'Ératosthène vu en cours est en $O(n \ln(\ln(n)))$. Il se trouve qu'avec l'algorithme légèrement modifié de la question 2 on obtient en fait une complexité en $O(n)$. On parle parfois de **crible linéaire** pour cet algorithme. Mais si en théorie $n \ll n \ln(\ln(n))$ quand $n \to +\infty$, en pratique cette différence est extrêmement faible.
- ▷ Enfin, on s'est intéressé ici à la complexité «temporelle» des algorithmes, c'est à dire au nombre d'opérations élémentaires nécessaires. Cette approche admet deux critiques:
  - ▷ en pratique les temps d'accès dans la liste `lp` mais surtout les calculs de produit ne sont plus nécessairement en temps constant si les entiers sont grands,
  - ▷ surtout, il faudrait dans de tels algorithmes considérer la complexité «**spatiale**», c'est à dire la taille utilisée en mémoire pour stocker les variables et liste.

Solution pour l'exercice 82 · Énoncé p. 25 · Indication p. 40 (Crible mystère II)

1. On montre par récurrence sur i (éventuellement à rédiger) qu'à l'étape i de la boucle «`while i<=N:`»:

- ▷ `lp` contient tous les nombres premiers inférieurs à i c'est à dire

$$\texttt{lp}_i = [p \in \mathcal{P} \mid p \leq i]$$

- ▷ `pgdp` est la liste telle que pour tout k (plus grand que 2), `pgdp[k]` est
  - ▷ le plus grand diviseur premier de k présent dans la liste `lp` si il y en a
  - ▷ k si il n'admet pas de diviseur dans cette liste

c'est à dire

$$\forall k \in [\![2, N]\!], \texttt{pgdp}_i[k] = \begin{cases} \max(\{p \in \texttt{lp}_i \mid p \text{ divise } k\}) & \text{si } \exists p \in \texttt{lp}_i \text{ , } p \text{ divise } k \\ k & \text{sinon.} \end{cases}$$

Et par conséquent pour tout entier $N \geq 2$, `mystere2`(N) renvoie un tuple constitué de

- ▷ la liste des nombres premiers inférieurs à N
- ▷ une liste de longueur $N+1$ dont le k-ième élément (pour tout k entre 2 et N) est le plus grand diviseur premier de k (et 0 en 0, 1 en 1).

2. À l'étape i de la boucle `while` on effectue dans tous les cas $O(1)$ opérations (le `if` et `i = i + 1`) et si i est premier on effectue ensuite $\left\lfloor \frac{N}{i} \right\rfloor$ (le nombre de k t.q $i \times k \leq N$) fois un nombre constant d'opérations (un produit, une affectation puis une somme).

La complexité est donc en

$$O(N) + O\left(\sum_{\substack{p \text{ premier} \\ p \leq N}} \left\lfloor \frac{N}{p} \right\rfloor \right).$$

En admettant l'équivalent (peut s'obtenir à partir d'un encadrement de $\pi(x)$, cf DM idoine), $\sum_{\substack{p \text{ premier} \\ p \leq n}} \frac{1}{p} \sim \ln(\ln(n))$ lorsque $n \to +\infty$, cela donne finalement une complexité en

$$\boxed{O(N \ln(\ln(N)))}.$$

Solution pour l'exercice 89 · Énoncé p. 27 · Indication p. 41 (Bernoulli itéré)

On procède par exemple par récurrence sur $n \in \mathbb{N}^*$.

- ▷ **Initialisation**

Pour $n = 1$ on a, pour tout entier a impair, $a^2 \equiv 1[8]$.

- ▷ **Hérédité**

Soit $n \in \mathbb{N}^*$ et supposons que pour tout entier a impair, $a^{2^n} \equiv 1[2^{n+2}]$ c'est à dire que

$$2^{n+2} \mid a^{2^n} - 1.$$

Soit $a \in \mathbb{Z}$ impair. Par identité remarquable on a la factorisation

$$a^{2^{n+1}} - 1 = (a^{2^n} - 1)(a^{2^n} + 1)$$

par hypothèse de récurrence, 2^{n+2} divise $a^{2^n} - 1$, et par imparité de a, 2 divise $a^{2^n} + 1$.

Par conséquent 2^{n+2+1} divise $a^{2^{n+1}}-1$.

▷ **Conclusion**

Par récurrence on a bien pour tout entier $n \geq 1$ et tout entier a impair

$$a^{2^n} \equiv 1 [2^{n+2}].$$

On remarque que la récurrence proposée correspond en fait à la factorisation directe.

$$a^{2^n}-1 = (a-1)(a+1)(a^2+1)(a^4+1)\cdots\left(a^{2^{n-1}}+1\right).$$