Arithmétique

Divisibilité, décomposition en facteurs premiers

Autocorrection A.
Pour tous les couples (a, b) suivants, utiliser l'algorithme d'Euclide pour calculer le PGCD $a \wedge b$, puis l'algorithme d'Euclide étendu pour obtenir une relation de Bézout :

(i) $(a, b) = (438, 51)$; (iii) $(a, b) = (1320, 720)$; (v) $(a, b) = (120, 23)$;
(ii) $(a, b) = (151, 77)$; (iv) $(a, b) = (63, 17)$; (vi) $(a, b) = (8136, 492)$.

Autocorrection B.
Trouver tous les entiers $n \in \mathbb{N}$ vérifiant les conditions suivantes.

(i) $n + 1 \mid n + 3$; (ii) $n + 2 \mid n^2 + 3n + 5$.

Autocorrection C.
Montrer que pour tout $n \in \mathbb{N}$, l'entier $n^4 - n^2$ est un multiple de 12.

Exercice 1.
Se rappeler ou retrouver les critères de divisibilité par 2, 3, 4, 5, 6, 8, 9, 10 et 11 (en les démontrant).

Les utiliser pour obtenir (à la main !) la décomposition en facteurs premiers de 14 652.

Exercice 2.
Montrer que pour tout $n > 0$, n^2 divise $(n + 1)^n - 1$.

Exercice 3.
Résoudre dans $\mathbb{Z}^2$ les équations suivantes.

(i) $np = 3n + 2p$; (ii) $\dfrac{1}{n} + \dfrac{1}{p} = \dfrac{1}{5}$; (iii) $n^2 - p^2 - 4n - 2p = 5$.

Exercice 4.
Montrer que tout entier > 6 est la somme de deux entiers > 1 premiers entre eux.

Exercice 5.
Trouver tous les entiers $n > 0$ tels que $n^2 + 1$ est divisible par $n + 1$.

PGCD, PPCM

Exercice 6.
Soit $n \in \mathbb{N}^*$.

1. Montrer que $n^2 + n$ et $2n + 1$ sont premiers entre eux.
2. Montrer que $3n^2 + 2n$ et $n + 1$ sont premiers entre eux.

Exercice 7.
Soit $k \in \mathbb{N}$. Montrer que $2k + 1$ et $9k + 4$ sont premiers entre eux et calculer $(2k - 1) \wedge (9k + 4)$.

Exercice 8.
Déterminer $\{(2n + 4) \wedge (3n + 3) \mid n \in \mathbb{N}\}$.

Exercice 9.
Soit $m, d \in \mathbb{N}^*$. À quelle condition le système $\begin{cases} x \wedge y = d \\ x \vee y = m \end{cases}$ possède-t-il une solution dans $(\mathbb{N}^*)^2$?

Exercice 10.
Résoudre dans $(\mathbb{N}^*)^2$ l'équation $x \wedge y + x \vee y = x + y$.

Valuations

Exercice 11 (Formule de Legendre).
Pour tout $x \in \mathbb{R}$, on note $\lfloor x \rfloor$ la partie entière de x, c'est-à-dire le plus grand entier relatif $\leqslant x$. Montrer (en lui donnant un sens) la *formule de Legendre* (1830) : pour tout nombre premier p et tout $n \in \mathbb{N}$,

$$\nu_p(n!) = \sum_{k \in \mathbb{N}^*} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Exercice 12.

1. Soit p un nombre premier.
   (a) Prolonger la valuation p-adique en une fonction $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ vérifiant la propriété $\forall x, y \in \mathbb{Q}, \nu_p(xy) = \nu_p(x) + \nu_p(y)$.
   (b) Montrer que l'on conserve la propriété $\forall x, y \in \mathbb{Q}, \nu_p(x + y) \geqslant \min(\nu_p(x), \nu_p(y))$.
2. Pour $n \geqslant 1$, on note $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Calculer $\nu_2(H_n)$.
3. En déduire que pour tout $n > 1$, $H_n \notin \mathbb{Z}$ et que pour tous $m > n$, $H_m - H_n \notin \mathbb{Z}$.

Exercice 13$^+$.
Soit $n \geqslant 2$. Montrer que le produit de trois entiers > 0 consécutifs n'est jamais une puissance n-ième.

Exercice 14$^+$.
Si $n \in \mathbb{N}^*$, on note R_n le nombre s'écrivant en base 10 à l'aide de n chiffres « 1 ». Calculer $\nu_3(R_n)$.

Exercice 15^{++}.
Déterminer tous les entiers $n \in \mathbb{N}^*$ tels que 2^n divise $3^n - 1$.

Exercice 16^{+++}.
Trouver tous les entiers $n \in \mathbb{N}^*$ tels que n^2 divise $2^n + 1$.

Mélange

Exercice 17.
Un nombre $6666\ldots0000$ formé de six-cent-soixante-six « 6 » et éventuellement de quelques zéros à la fin peut-il être un carré parfait ?

Exercice 18$^+$.
Résoudre dans $(\mathbb{N}^*)^2$ l'équation $x^y = y^x$.

Exercice 19.
Soit $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci, c'est-à-dire la suite définie par

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

1. Montrer $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}^*, F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$.
2. En déduire $\forall n, m \in \mathbb{N}^*, F_n \wedge F_{n+m} = F_n \wedge F_m$.
3. En déduire que si n et m sont deux entiers non nuls et que r est le reste de la division euclidienne de m par n, alors $F_n \wedge F_m = F_n \wedge F_r$.
4. Montrer : $\forall m, n \in \mathbb{N}^*, F_n \wedge F_m = F_{n\wedge m}$.

Exercice 20.
Soit $n \in \mathbb{N}^*$. On note $\tau(n)$ le nombre de diviseurs (positifs) de n et $p(n)$ leur produit.

1. Quelles sont les inégalités liant n, $\tau(n)$ et $p(n)$?
2. Montrer que $\tau(n)$ est impair si et seulement si n est un carré parfait.
3. Exprimer $\tau(n)$ en fonction des valuations p-adiques de n.
4. Montrer que $p(n) = \sqrt{n^{\tau(n)}}$.

Exercice 21 (Nombres parfaits).
Pour tout $n \in \mathbb{N}^*$, on note $\sigma(n)$ la somme des diviseurs de n. On dit que n est *parfait* si $\sigma(n) = 2n$ (c'est-à-dire si n est égal à la somme de ses diviseurs différents de lui-même).

1. Montrer que 6 et 28 sont parfaits.
2. Soit $n \in \mathbb{N}^*$. En commençant par le cas où n est une puissance d'un nombre premier, établir une formule pour $\sigma(n)$ en fonction de la décomposition en facteurs premiers de n.
3. Montrer que si n et m sont des nombres premiers entre eux, alors $\sigma(mn) = \sigma(m)\sigma(n)$.
4. Soit p un nombre premier tel que $2^p - 1$ soit premier. Montrer que $2^{p-1}(2^p - 1)$ est parfait.
5. Soit n un entier pair parfait. Il existe $a \in \mathbb{N}^*$ et b entier impair tels que $n = 2^a b$.
   (a) Montrer : $\sigma(n) = (2^{a+1} - 1)\sigma(b)$.
   (b) En déduire qu'il existe un entier impair c tel que $b = (2^{a+1} - 1)c$ et $\sigma(b) = 2^{a+1}c$.
   (c) Montrer que $c = 1$ et que b est premier.
   (d) En déduire que n est de la forme $2^{k-1}(2^k - 1)$, avec $2^k - 1$ premier.

Autres résultats sur les nombres premiers

Autocorrection D.
Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un nombre premier compris entre $n+1$ et $n!+1$.

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

Exercice 22.
Soit p un nombre premier $\geqslant 5$. Montrer que p^2-1 est divisible par 24.

Exercice 23.
Montrer que la somme de deux nombres premiers consécutifs n'est jamais le produit de deux nombres premiers.

Exercice 24.
Soit $n \in \mathbb{N}^*$. Montrer qu'il existe n nombres composés consécutifs.

Exercice 25.
Déterminer les nombres premiers dont l'écriture en base 10 comporte en alternance des 0 et des 1.

Exercice 26$^+$.

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.

Exercice 27$^+$ (Théorème de Wilson).
Soit $n \geqslant 2$. Montrer que n est premier si et seulement si $(n-1)! \equiv -1 \pmod{n}$.

Exercice 28$^+$.
Soit p un nombre premier impair.

1. On suppose que l'équation $x^2 \equiv -1 \pmod{p}$ possède une solution dans $\mathbb{Z}$.
   Montrer que $p \equiv 1 \pmod{4}$.
2. **Application.** En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.
3. Réciproquement, montrer que si $p \equiv 1 \pmod{4}$, on a $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$.

Exercice 29^{++} (Identité de Sophie Germain).
Montrer que si $n > 1$, $n^4 + 4^n$ n'est pas premier.

Exercice 30 (Nombres de Mersenne).
Soit $a, b, n \geqslant 2$ trois entiers.

1. Montrer que $a^n - 1$ est divisible par $a-1$.
2. En déduire que si $a^n - 1$ est un nombre premier, alors $a = 2$ et n est un nombre premier.
3. On note r le reste de la division euclidienne de a par b. Montrer que $2^r - 1$ est le reste de la division euclidienne de $2^a - 1$ par $2^b - 1$.
4. Montrer que $\left(2^a-1\right) \wedge \left(2^b-1\right) = 2^{a \wedge b} - 1$.

Exercice 31 (Nombres de Fermat).

1. Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ soit premier. Montrer qu'il existe $n \in \mathbb{N}$ tel que $m = 2^n$.
2. Pour $n \in \mathbb{N}$, on note $F_n = 2^{2^n} + 1$. Calculer F_0, F_1, F_2, F_3, F_4.
3. Montrer que $\forall n \in \mathbb{N}, F_{n+1} - 2 = (F_n - 2)F_n$.
4. En déduire, pour $n \in \mathbb{N}^*$, une expression de F_n en fonction des $(F_k)_{k=1}^{n-1}$.
5. Montrer que si $m \neq n$ alors F_n et F_m sont premiers entre eux.
6. En déduire une nouvelle preuve de l'existence d'une infinité de nombres premiers.

Congruences

Autocorrection E. ☑
Trouver $\lambda, \mu, \nu, \xi \in \mathbb{Z}$ tels que, pour tous $a, b, c, d \in \mathbb{Z}$, le nombre $n = \lambda a + \mu b + \nu c + \xi d$ vérifie

$$\begin{cases} n \equiv a \pmod 2 \\ n \equiv b \pmod 3 \\ n \equiv c \pmod 5 \\ n \equiv d \pmod 7 \end{cases}$$

Autocorrection F. ☑
Montrer que 13 divise $2^{70} + 3^{70}$.

Exercice 32.
Soit $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$ tels que $a \equiv b \pmod n$. Montrer $a^n \equiv b^n \pmod{n^2}$.

Exercice 33.
Le plus grand nombre premier connu actuellement (depuis le 7 décembre 2018) est $2^{82\,589\,933} - 1$. Calculer son dernier chiffre.

Exercice 34. ☑
Résoudre dans $\mathbb{Z}^2$ les équations suivantes, d'inconnue (x, y) :

(i) $7x + 5y = 1$; (ii) $3x - 9y = 1$; (iii) $5x - 10y = 15$; (iv) $5x + 3y = 4$.

Exercice 35$^+$.
Résoudre l'équation $3x + 4y + 5z = 6$, d'inconnue $(x, y, z) \in \mathbb{Z}^3$.

Exercice 36. ☑
Résoudre dans $\mathbb{Z}$ les « équations » suivantes.

(i) $5x \equiv 1 \pmod 7$; (iii) $23x \equiv 0 \pmod{97}$; (v) $4x \equiv 8 \pmod{12}$;
(ii) $3x \equiv 4 \pmod{19}$; (iv) $8x \equiv 7 \pmod{105}$; (vi) $4x \equiv 6 \pmod{12}$.

Exercice 37.
Résoudre dans $\mathbb{Z}^2$ le système de congruences

$$\begin{cases} 4x + y \equiv 6 \pmod{12} \\ x + 4y \equiv 3 \pmod{12}. \end{cases}$$

Exercice 38$^+$.

1. Soit p un nombre premier impair. Montrer l'équivalence
$$\big(\exists x \in \mathbb{Z} : x^2 + x + 3 \equiv 0 \pmod{p}\big) \Leftrightarrow \big(\exists y \in \mathbb{Z} : y^2 \equiv -11 \pmod{p}\big).$$
2. Pour chaque entier $n \in \mathbb{N}^*$, on considère « l'équation »
$$x^2 + x + 3 \equiv 0 \pmod{n}. \qquad (E_n)$$
   (a) Résoudre (E_2) et (E_3).
   (b) En suivant le raisonnement de la première question, résoudre (E_n) dans les cas $n \in \{5, 7, 11\}$.
   (c) Déduire de ce qui précède une résolution de (E_n) dans les cas $n \in \{10, 15, 55, 105\}$.
   (d) Résoudre l'équation (E_n) dans le cas $n = 121$ puis dans les cas $n \in \{25, 125\}$.
   (e) Montrer que, pour tout $k \in \mathbb{N}^*$, il existe deux éléments distincts $a, b \in [\![0, 5^k - 1]\!]$ tels que les solutions de (E_{5^k}) soient exactement les entiers congrus à a ou b modulo 5^k.
   (Autrement dit, montrer que l'équation $x^2 + x + 3 = 0$ possède exactement deux solutions dans $\mathbb{Z}/5^k\mathbb{Z}$.)

Exercice 39.
Montrer qu'il existe une infinité d'entiers $n > 0$ tels que $4n^2 + 1$ est divisible par 5 et 13.

Exercice 40.
Montrer que l'ensemble $\{2^n - 3 \,|\, n \geqslant 2\}$ contient une infinité de multiples de 5, une infinité de multiples de 13, mais aucun multiple de 65.

Exercice 41.
Montrer que $\min\left\{\left|36^n - 5^m\right| \,\middle|\, n, m \in \mathbb{N}^*\right\} = 11$.

Exercice 42.
Déterminer les $n \in \mathbb{N}$ tels que $n\,3^n \equiv 1 \pmod{7}$.

Exercice 43$^+$.
Soit p un nombre premier. Montrer $\exists n \in \mathbb{N} : 2^n \equiv n \pmod{p}$.

Exercice 44 (Petit théorème de Fermat).
Soit p un nombre premier.

1. Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.
2. En déduire une nouvelle démonstration, par récurrence, de $\forall a \in \mathbb{Z}, a^p \equiv a \pmod{p}$.

Exercice 45.
Montrer que pour $k \geqslant 0$, on a $19 | 2^{2^{6k+2}} + 3$.

Exercice 46$^+$.
On appelle *repunit* un nombre entier dont l'écriture en base 10 ne contient que des 1.

Caractériser les nombres premiers qui divisent au moins un repunit.

Applications diverses

Exercice 47.

1. Soit $n \in \mathbb{N}$.
   Déterminer à quelle condition « l'équation » $x^3 \equiv n \pmod 9$ possède une solution dans $\mathbb{Z}$.
2. Montrer que $\forall a, b, c \in \mathbb{Z}, a^3 + b^3 + c^3 \neq 11\,111$.
3. En utilisant des propriétés fines du plus petit sous-corps de $\mathbb{R}$ contenant $\sqrt[3]{117}$, habituellement noté $\mathbb{Q}(\sqrt[3]{117})$, Finkelstein et London ont montré en 1971 que l'équation $x^3 + 117y^3 = 5$ n'avait pas de solution $(x, y) \in \mathbb{Z}^2$. Montrer leur résultat de façon plus élémentaire.

Exercice 48$^+$.
Soit $(x, y) \in (\mathbb{N}^*)^2$ une solution de $3^x = 8 + y^2$.

1. Déterminer les parités de x et y.
2. Conclure.

Exercice 49.
Le nombre 2^{29} possède neuf chiffres, tous distincts. Quel est le chiffre manquant ?

Exercice 50$^+$. *IMO 2017*
Soit $a_0 \in \mathbb{N}^*$. On définit la suite $(a_n)_{n\in\mathbb{N}}$ par

$$\forall n \in \mathbb{N}, a_{n+1} = \begin{cases} \sqrt{a_n} & \text{si } \sqrt{a_n} \in \mathbb{N}^* \\ a_n + 3 & \text{sinon.} \end{cases}$$

Déterminer les $a_0 \in \mathbb{N}$ tels que la suite $(a_n)_{n\in\mathbb{N}}$ prenne la même valeur une infinité de fois.

Exercice 51^{++}.
Soit $n \in \mathbb{N}^*$.

Montrer que n est impair si et seulement si n divise $\displaystyle\sum_{k=1}^{n} k^n$.

Exercice 52^{++}.
Soit $a, b > 1$ des entiers. Montrer que la suite

$$a, a^a, a^{a^a}, a^{a^{a^a}}, \ldots$$

est stationnaire modulo b.

Exercice 53^{+++} (Théorème de Leudesdorf). *Lyon*
Soit $p \geqslant 5$ un nombre premier. Quand $n \wedge p = 1$, on choisit un entier $n^\dagger$ tel que $n\, n^\dagger \equiv 1 \pmod{p^2}$.

Montrer

$$\sum_{k=1}^{p-1} k^\dagger \equiv 0 \pmod{p^2}.$$

Arithmétique et algèbre

Exercice 54 ($\mathbb{Z}$ est intégralement clos). ☑
Soit $a_0, \dots, a_{n-1}$ des nombres entiers et $x \in \mathbb{Q}$ tel que $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$.

Montrer que $x \in \mathbb{Z}$.

Exercice 55.
Soit $n, m \in \mathbb{N}^*$. Déterminer $\mathbb{U}_n \cap \mathbb{U}_m$.

Exercice 56$^+$.
Soit $n, m \in \mathbb{N}^*$. Combien y a-t-il de morphismes de groupes $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$?

Exercice 57^{++} (Groupe de Baer-Specker). *Lyon*
L'ensemble $\mathbb{Z}^{\mathbb{N}}$ des suites à valeurs entières est un groupe pour l'addition, et l'ensemble $\mathbb{Z}^{(\mathbb{N})}$ des suites nulles à partir d'un certain rang en est un sous-groupe. (On ne demande pas de le vérifier).

Soit $\varphi : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$ un morphisme de groupes tel que $\mathbb{Z}^{(\mathbb{N})} \subseteq \ker \varphi$. Montrer que $\varphi = 0$.

Exercice 58 (Convolution de Dirichlet).
On munit l'ensemble des fonctions $\mathbb{N}^* \to \mathbb{R}$ de l'addition et de la loi $*$ définie par

$$(f * g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right).$$

1. Montrer que cela définit un anneau commutatif.
2. En déterminer les inversibles.
3. On définit la *fonction de Möbius* μ par la formule

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n \text{ est le produit de } r \text{ premiers distincts} \\ 0 & \text{sinon.} \end{cases}$$

   Montrer que $\mu * 1$ est l'unité de l'anneau.
4. En déduire la formule $\varphi(n) = \sum_{d|n} d\, \mu\left(\frac{n}{d}\right)$.

Exercice 59.
Soit p un nombre premier et

$$A = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \,\middle|\, a \in \mathbb{Z}, b \in \mathbb{N}^*, b \wedge p = 1 \right\}.$$

1. Montrer que A (muni des opérations usuelles) est un anneau intègre.
2. Déterminer les éléments inversibles de A.
3. Montrer qu'il existe un unique morphisme d'anneaux $\varphi : A \to \mathbb{Z}/p\mathbb{Z}$, et que $A^\times = A \setminus \ker \varphi$. (On dit que $\mathbb{Z}/p\mathbb{Z}$ est le *corps résiduel* de l'anneau *local* A.)

Exercice 60$^+$.

1. Soit p un nombre premier impair.
   (a) Montrer par récurrence $\forall \ell \in \mathbb{N}, (p+1)^{p^\ell} \equiv 1 + p^{\ell+1} \pmod{p^{\ell+2}}$.
   (b) En déduire que, pour tout $k \geqslant 1$, $[p+1]_{p^k}$ est d'ordre p^{k-1} dans $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$.
   (c) En admettant le cas $k = 1$, montrer que le groupe $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ est cyclique.
2. Montrer que, pour tout $k \geqslant 3$, le groupe multiplicatif $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$ n'est pas cyclique.