1 Vrai ou faux ? Justifier. Soient $d, n, a \in \mathbb{Z}$.

1) 45 possède 12 diviseurs.
2) Si $n \equiv 1$ [35], alors n est impair.
3) Si a et b divisent d, alors ab aussi.
4) Si d divise ab, alors d divise a ou d divise b.
5) L'intervalle d'entiers $[\![1, 1000]\!]$ contient 140 entiers divisibles par 7.
6) Pour tous $p, q \in \mathbb{P}$, si $q - p = 11$, alors $p = 2$ et $q = 13$.
7) Si d divise n^2, alors d divise n.
8) Si $a^2 \equiv 1$ $[n]$, alors $a \equiv \pm 1$ $[n]$.
9) Si $4a \equiv 4b$ [13], alors $a \equiv b$ [13].
10) Si $4a \equiv 4b$ [6], alors $a \equiv b$ [6].
11) Si $a \equiv b$ $[n]$, alors $d^a \equiv d^b$ $[n]$.
12) Si $a \equiv b$ [6], alors $2^a \equiv 2^b$ [9].
13) Si tout diviseur premier de n est congru à ± 1 modulo 8, alors $n \equiv \pm 1$ [8]. Et la réciproque ?

DIVISIBILITÉ, DIVISION EUCLIDIENNE ET CONGRUENCES

2

1) Montrer que $2^{123} + 3^{121}$ est divisible par 11.
2) Calculer le reste de la division euclidienne :
   a) de 3^{2189} par 25. b) de 49^{90021} par 13.

3

1) Montrer que $n(n+2)(7n-5)$ est divisible par 6 pour tout $n \in \mathbb{Z}$.
2) Pour quels entiers $n \in \mathbb{Z}$ est-il vrai que $n+1$ divise $n+7$?
3) Pour quelles valeurs de $n \in \mathbb{Z}$ l'entier :
$$n^2 + (n+1)^2 + (n+3)^2$$
est-il divisible par 10 ?
4) Trouver tous les nombres premiers p pour lesquels $3p+4$ est un carré parfait.
5) Pour quels $n \in \mathbb{Z}$ le produit $n(n+2)$ est-il une puissance de 2 ?

4 Soit $n \in \mathbb{N}$. On note $a_0, \ldots, a_r$ les chiffres de la décomposition de n en base 10. Par exemple, pour $n = 156$: $a_0 = 6$, $a_1 = 5$ et $a_2 = 1$.

1) Montrer que n est divisible par 4 si et seulement si l'entier obtenu en ne conservant que les chiffres a_0 et a_1 l'est.
2) Montrer que n est divisible par 3 (resp. 9) si et seulement si la somme $a_0 + \ldots + a_r$ l'est.
3) Déterminer une condition nécessaire et suffisante sur $a_0, \ldots, a_r$ pour que n soit divisible par 11.

5 Soient $x, y, z \in \mathbb{Z}$.

1) Montrer que $x^2 + y^2$ est divisible par 7 si et seulement si x et y le sont.
2) Montrer que si $x^3 + y^3 + z^3$ est divisible par 7, l'un des entiers x, y ou z l'est aussi.

6 Montrer que $p^2 \equiv 1$ [24] pour tout $p \in \mathbb{P}$ supérieur ou égal à 5.

7 Montrer que pour tous $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$, si $a \equiv b$ $[n]$, alors $a^n \equiv b^n$ $\left[n^2\right]$.

8 Montrer que $a^{2^n} \equiv 1$ $\left[2^{n+1}\right]$ pour tous $a \in \mathbb{Z}$ impair et $n \in \mathbb{N}$.

9

1) Montrer que pour tout $n \geqslant 6$ pair, n divise $(n-1)!$.
2) Soit $p \in \mathbb{P}$ supérieur ou égal à 7. Montrer que $(p-1)! + 1$ n'est pas une puissance de p.

10 Soit $(u_n)_{n \in \mathbb{N}}$ une suite réelle *sous-additive*, i.e. pour laquelle $u_{m+n} \leqslant u_m + u_n$ pour tous $m, n \in \mathbb{N}$.
On note a la borne inférieure dans $\overline{\mathbb{R}}$ de $\left\{ \dfrac{u_n}{n} \;\middle|\; n \in \mathbb{N}^* \right\}$.

1) Soient $n, N \in \mathbb{N}^*$. On note q le quotient et r le reste de la division euclidienne de n par N. Montrer que : $\dfrac{u_n}{n} \leqslant \dfrac{Nq}{n} \times \dfrac{u_N}{N} + \dfrac{u_r}{n}$.
2) Montrer que $\displaystyle\lim_{n \to +\infty} \frac{u_n}{n} = \inf A$ (*lemme sous-additif de Fekete*).

PGCD, PPCM ET NOMBRES PREMIERS ENTRE EUX

11 Déterminer tous les couples $(x, y) \in \mathbb{Z}^2$ d'entiers premiers entre eux pour lesquels $xy = 150$.

12

1) Montrer que $n+1$ et $2n+1$ sont premiers entre eux pour tout $n \in \mathbb{N}$.
2) En déduire, grâce à $\dbinom{2n+1}{n+1}$, que $\dbinom{2n}{n}$ est divisible par $n+1$ pour tout $n \in \mathbb{N}$.

13 Soit $p \in \mathbb{P}$.

1) Montrer que p divise $\dbinom{p}{k}$ pour tout $k \in [\![1, p-1]\!]$.
2) En déduire que pour tout $k \in [\![0, p-1]\!]$:
$$\binom{p-1}{k} \equiv (-1)^k \; [p].$$

14 Montrer que pour tous $a,b \geqslant 2$ premiers entre eux, $\dfrac{\ln a}{\ln b}$ est irrationnel.

---

15 Soients $a,b,n \in \mathbb{Z}$.

1) Montrer que $\left(n^3+3n^2-5\right) \wedge (n+2) = 1$.

2) Montrer que si $a \wedge n = 1$: $\quad (ab) \wedge n = b \wedge n$.

3) Montrer que :
$$\left(n^4+3n^2-n+2\right) \wedge \left(n^2+n+1\right) = (n-2) \wedge 7.$$

4) Simplifier $(a+b) \wedge (a \vee b)$.

---

16 Soit $n \in \mathbb{Z}$. Montrer que $\dfrac{21n-3}{4}$ et $\dfrac{15n+2}{4}$ ne sont pas tous les deux entiers.

---

17 Montrer que $\mathbb{U}_a \cap \mathbb{U}_b = \mathbb{U}_{a \wedge b}$ pour tous $a,b \in \mathbb{N}^*$.

---

18 Soients $a,n \in \mathbb{N}^*$ premiers entre eux. Pour tout $k \in \mathbb{N}$, on note r_k le reste de la division euclidienne de a^k par n.

1) Pourquoi l'application $k \longmapsto r_k$ n'est-elle pas injective sur $[\![0,n]\!]$? En déduire que $a^N \equiv 1 \ [n]$ pour un certain $N \in [\![1,n]\!]$.

2) On pose :
$$\varphi(n) = \left|\left\{k \in [\![0,n-1]\!] \mid \quad k \wedge n = 1\right\}\right|.$$
Montrer qu'on peut choisir N inférieur ou égal à $\varphi(n)$. On peut montrer avec des outils différents que $N=\varphi(n)$ convient (*théorème d'Euler*).

---

19 Soients $a,b \in \mathbb{N}^*$ premiers entre eux. Montrer que l'application « produit » $(x,y) \longmapsto xy$ est bijective de $\mathrm{div}^+(a) \times \mathrm{div}^+(b)$ sur $\mathrm{div}^+(ab)$, où l'on a noté $\mathrm{div}^+(n)$ l'ensemble des diviseurs positifs de n pour tout $n \in \mathbb{N}^*$.

---

20 On dira qu'une partie non vide E de $\mathbb{N}^*$ est *sympathique* si pour tous $x,y \in E$: $\quad \dfrac{x+y}{x \wedge y} \in E$.

1) Montrer que toute partie sympathique contient 2 et que $\{2\}$ est une partie sympathique.

2) Déterminer toutes les parties sympathiques qui contiennent 1.

3) Soit E une partie sympathique non réduite à $\{2\}$ et ne contenant pas 1.

a) Montrer que le plus petit élément de $E \setminus \{2\}$ est impair.

b) Montrer que $E = \mathbb{N} \setminus \{0,1\}$.

Valuations p-adiques

21 Soients $a,b \in \mathbb{Z}$. Montrer que si a^2 divise b^2, alors a divise b.

---

22 Soit $n \in \mathbb{N}$. Montrer que si n est à la fois un carré parfait et un cube parfait, alors il est la puissance sixième d'un entier.

---

23 Montrer que $(a \wedge b)^n = a^n \wedge b^n$ pour tous $a,b \in \mathbb{Z}$ et $n \in \mathbb{N}$.

---

24 Le résultat de cet exercice est utile à la résolution de bon nombre d'équations diophantiennes, notamment de cette feuille d'exercices.

1) Soient $a,b \in \mathbb{N}^*$ et $k \geqslant 2$ entier. Montrer que si a et b sont premiers entre eux et si ab est la puissance $k^{\text{ème}}$ d'un entier, alors a et b sont eux-mêmes des puissances $k^{\text{èmes}}$ d'entiers.

2) Le résultat de la question **1)** est-il vrai pour des entiers $a,b \in \mathbb{Z}$?

25

1) Montrer que pour tous $p \in \mathbb{P}$ et $n \in \mathbb{N}$:
$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \qquad \textit{(formule de Legendre)},$$
où la somme est faussement infinie car $\left\lfloor \dfrac{n}{p^k} \right\rfloor = 0$ pour tout $k \in \mathbb{N}^*$ pour lequel $p^k > n$.

2) Par combien de zéros l'entier $100!$ s'achève-t-il ?

---

26 Déterminer tous les entiers $n \in \mathbb{N}^*$ pour lesquels 2^n divise 3^n-1.

Nombres premiers

27 Pour tout $n \in \mathbb{N}^*$, on note p_n le $n^{\text{ème}}$ nombre premier. Montrer que pour tout $n \geqslant 2$: $\quad p_{n+1} < p_1 \ldots p_n$.

---

28 Soient $a \geqslant 2$ et $n \geqslant 2$. On suppose a^n-1 premier.

1) Montrer que $a=2$.

2) Montrer que n est premier.

Pour tout $p \geqslant 2$, l'entier $M_p = 2^p-1$ est appelé le *$p^{\text{ème}}$ nombre de Mersenne*. Tous ne sont pas premiers, par exemple $M_{11} = 23 \times 89$.

29

1) Montrer que pour tout $n \in \mathbb{N}^*$, si 2^n+1 est premier, n est une puissance de 2.

Pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n}+1$ est appelé le *$n^{\text{ème}}$ nombre de Fermat*. Les nombres de Fermat F_0, F_1, F_2, F_3 et F_4 sont premiers et on conjecture que ce sont les seuls.

2) a) Montrer que $F_{n+1} = F_0 \ldots F_n + 2$ pour tout $n \in \mathbb{N}$.

b) En déduire que F_m et F_n sont premiers entre eux pour tous $m,n \in \mathbb{N}$ distincts.

30
1) a) Montrer que tout entier naturel congru à 3 modulo 4 possède au moins un diviseur premier congru à 3 modulo 4.
   b) 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.

ÉQUATIONS DIOPHANTIENNES

31 Résoudre les équations d'inconnue $(x,y)\in\mathbb{N}^2$:
1) $\begin{cases} x\wedge y=3 \\ x+y=21. \end{cases}$
2) $(x\wedge y)+(x\vee y)=2x+3y$.
3) $x\vee y=x+y-1$.

---

32 Résoudre les équations d'inconnue $(x,y)\in\mathbb{N}^2$ suivantes :
1) $x^2-y^2=7$. 2) $9x^2-y^2=32$.
3) $x^2-2y^2=3$ en raisonnant modulo 8.
4) $15x^2-7y^2=9$ en raisonnant modulo 3.

33
1) Soient $a,b,n\in\mathbb{Z}$ pour lesquels $a\wedge n=1$.
   a) Montrer que $aa'\equiv 1\,[n]$ pour un certain $a'\in\mathbb{Z}$.
   b) En déduire, en fonction de a', b et n, les solutions de l'équation $ax\equiv b\,[n]$ d'inconnue $x\in\mathbb{Z}$.
2) Résoudre les équations suivantes d'inconnue $x\in\mathbb{Z}$: a) $5x\equiv 3\,[28]$. b) $14x\equiv 6\,[34]$.
3) Résoudre l'équation $ax\equiv b\,[n]$ d'inconnue $x\in\mathbb{Z}$ pour tous $a,b,n\in\mathbb{Z}$.

---

34 Soient $a,b,c\in\mathbb{Z}$ avec $(a,b)\neq(0,0)$. On s'intéresse à l'équation : $ax+by=c$ ★ d'inconnue $(x,y)\in\mathbb{Z}^2$.
1) Montrer que ★ n'a pas de solution si c n'est pas un multiple de $a\wedge b$.
2) On suppose à présent que $a\wedge b$ divise c.
   a) Montrer, grâce à une relation de Bézout de a et b, que ★ possède une solution (x_0,y_0).
   b) Résoudre ★ et interpréter le résultat géométriquement.
3) Résoudre les équations d'inconnue $(x,y)\in\mathbb{Z}^2$:
   a) $7x-12y=3$. b) $20x-53y=3$.

---

35 Résoudre le système $\begin{cases} x\equiv 1 \mod 5 \\ x\equiv 2 \mod 11 \end{cases}$ d'inconnue $x\in\mathbb{Z}$.

---

36 Résoudre l'équation $x^2+y^2=3z^2$ d'inconnue $(x,y,z)\in\mathbb{N}^3$, notamment en raisonnant modulo 3.

---

37 Montrer que l'équation $2^n+1=m^3$ d'inconnue $(m,n)\in\mathbb{N}^2$ n'a pas de solution.

38
1) Soit $(x,y,z)\in\left(\mathbb{N}^*\right)^3$. On suppose que :
$$x^2+y^2=z^2 \qquad \text{et} \qquad x\wedge y=1.$$
   a) Montrer que $y\wedge z=1$.
   b) Montrer que x ou y est pair. Quitte à les permuter, on suppose désormais y pair.
   c) Montrer que $y+z$ et $z-y$ sont premiers entre eux, puis que $y+z=a^2$ et $z-y=b^2$ pour certains $a,b\in\mathbb{N}^*$ impairs et premiers entre eux.
   d) En déduire la forme du triplet (x,y,z).
2) Résoudre finalement l'équation $x^2+y^2=z^2$ d'inconnue $(x,y,z)\in\left(\mathbb{N}^*\right)^3$.

---

39 Pour montrer que l'équation $y^2=x^3+7$ d'inconnue $(x,y)\in\mathbb{Z}^2$ n'a pas de solution, on suppose par l'absurde qu'elle en possède une (x,y).
1) Montrer que $x\equiv 1\,[4]$.
2) Montrer que x^3+8 possède un facteur premier p congru à 3 modulo 4.
3) Calculer y^{p-1} modulo p de deux manières différentes, puis conclure.

---

40 On veut résoudre l'équation $x^y=y^x$ d'inconnue $(x,y)\in\mathbb{N}^*$.
1) Soient $x,y\in\mathbb{N}^*$ deux entiers pour lesquels $x\leqslant y$ et $x^y=y^x$. Montrer que x divise y en étudiant leur PGCD.
2) Conclure.

---

41 Résoudre l'équation $y^3=x^2+x$ d'inconnue $(x,y)\in\mathbb{Z}^2$.

---

42 Résoudre l'équation $x^2+px=y^2$ d'inconnue $(x,y)\in\mathbb{N}^2$ pour tout $p\in\mathbb{P}$.
