DIVISIBILITÉ, DIVISION EUCLIDIENNE ET CONGRUENCES

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

1) $2^m 3^n$ possède mn diviseurs positifs.
2) $[\![1, 1000]\!]$ contient 140 entiers divisibles par 7.
3) Si a et b divisent d, alors ab aussi.
4) d divise ab si et seulement si d divise a ou b.
5) L'ensemble $\{p - q \mid p, q \in \mathbb{P}\}$ contient 19.
6) d divise n^2 si et seulement si d divise n.
7) $a^2 \equiv 1\ [n]$ si et seulement si $a \equiv \pm 1\ [n]$.
8) Si $4a \equiv 4b\ [13]$, alors $a \equiv b\ [13]$.
9) Si $4a \equiv 4b\ [6]$, alors $a \equiv b\ [6]$.
10) Si $a \equiv b\ [n]$, alors $d^a \equiv d^b\ [n]$.
11) Si $a \equiv b\ [6]$, alors $2^a \equiv 2^b\ [9]$.
12) Si tout diviseur premier de n est congru à ± 1 modulo 8, alors $n \equiv \pm 1\ [8]$. Et la réciproque ?

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

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 $a_0 + \dots + a_r$ l'est.
3) Déterminer une condition nécessaire et suffisante sur $a_0, \dots, a_r$ pour que n soit divisible par 11.

4

1) Montrer que $n(n+2)(7n-5)$ est divisible par 6 pour tout $n \in \mathbb{Z}$.
2) Déterminer tous les entiers $n \in \mathbb{Z}$ pour lesquels $n+1$ divise $n+7$.
3) Déterminer tous les entiers $n \in \mathbb{Z}$ pour lesquels $n^2 + (n+1)^2 + (n+3)^2$ est divisible par 10.
4) Déterminer tous les nombres premiers p pour lesquels $3p + 4$ est un carré parfait.
5) Déterminer tous les entiers $n \in \mathbb{N}$ pour lesquels $n(n+2)$ est une puissance de 2. Et si $n \in \mathbb{Z}$?

---

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 $a, b \in \mathbb{Z}$:

$$a \equiv b\ [n] \implies a^n \equiv b^n\ \left[n^2\right].$$

---

8 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 $m, n \in \mathbb{N}$. Montrer le *lemme sous-additif de Fekete* : $\dfrac{u_n}{n} \xrightarrow[n\to+\infty]{} \inf_{k\in\mathbb{N}^*} \dfrac{u_k}{k}$, où la borne inférieure est calculée dans $\overline{\mathbb{R}}$.

NOMBRES PREMIERS ET VALUATIONS p-ADIQUES

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

10

1) Soient $a \geqslant 2$ et $n \geqslant 2$.
a) Montrer que si $a^n - 1$ premier, alors $a = 2$ et n est premier.
b) Montrer que si $a^n + 1$ est premier, alors a est pair et n est une puissance de 2.
Les nombres premiers de la forme $2^p - 1$ avec $p \in \mathbb{P}$ sont dit *de Mersenne*. On ignore s'il en existe une infinité, mais on conjecture que oui.
2) Pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$ est appelé le $n^{ème}$ *nombre de Fermat*. On conjecture que parmi ces entiers, seul $F_0, \dots, F_4$ sont premiers.
a) Montrer que $F_{n+1} = F_0 \dots F_n + 2$ pour tout $n \in \mathbb{N}$.
b) En déduire que $F_m \wedge F_n = 1$ pour tous $m, n \in \mathbb{N}$ distincts.

11

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.

---

12 Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Montrer que si a^n divise b^n, alors a divise b.

---

13 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.

---

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

15

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 $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ pour tout $k \in \mathbb{N}^*$ pour lequel $p^k > n$.

2) Par combien de zéros l'entier 1000! s'achève-t-il ?

16

1) Montrer que pour tout $n \in \mathbb{N}^*$, n divise $(n-1)!$ si et seulement si n n'est ni égal à 4, ni premier.

2) Soit $p \in \mathbb{P}$ supérieur à 7. Montrer que $(p-1)!+1$ n'est pas une puissance de p.

---

17 Montrer que pour tout $n \geqslant 2$, $\sum_{k=1}^{n} \frac{1}{k}$ n'est pas un entier.

---

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

---

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

1) On note $\mathscr{M}$ l'ensemble des mots de p lettres sur l'alphabet $\{A, B\}$ et τ l'application de $\mathscr{M}$ dans $\mathscr{M}$ qui translate chaque lettre d'une unité vers la droite et ramène la dernière en première position. Par exemple, $\tau(AABBA) = AAABB$ pour $n = 5$. Montrer que l'ensemble $\{\tau^k(M) \mid k \in \mathbb{N}\}$ est de cardinal 1 ou p pour tout $M \in \mathscr{M}$. Pour quel(s) mot(s) M est-il de cardinal 1 ?

2) En déduire que pour tous $A, B \in \mathscr{M}_n(\mathbb{Z})$:

$$\mathrm{tr}\big((A+B)^p\big) \equiv \mathrm{tr}\big(A^p\big) + \mathrm{tr}\big(B^p\big) \ [p].$$

3) En déduire que pour tout $A \in \mathscr{M}_n(\mathbb{Z})$:

$$\mathrm{tr}\big(A^p\big) \equiv \mathrm{tr}(A) \ [p].$$

PGCD, PPCM

ET NOMBRES PREMIERS ENTRE EUX

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

21

1) Montrer que $n+1$ et $2n+1$ sont premiers entre eux pour tout $n \in \mathbb{N}$.

2) En déduire, grâce à $\binom{2n+1}{n+1}$, que $\binom{2n}{n}$ est divisible par $n+1$ pour tout $n \in \mathbb{N}$.

---

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

1) Montrer que p divise $\binom{p}{k}$ pour tout $k \in [\![1, p-1]\!]$.

2) En déduire que pour tout $k \in [\![0, p-1]\!]$:

$$\binom{p-1}{k} \equiv (-1)^k \ [p].$$

---

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

---

24 Soient $a, b, n \in \mathbb{Z}$.

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

2) Montrer que $\frac{21n-3}{4}$ et $\frac{15n+2}{4}$ ne sont pas tous les deux entiers.

3) Montrer que si $a \wedge n = 1$, alors :

$$(ab) \wedge n = b \wedge n.$$

4) Montrer que :

$$\big(n^4 + 3n^2 - n + 2\big) \wedge \big(n^2 + n + 1\big) = (n-2) \wedge 7.$$

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

6) Montrer que si a et b sont strictement positifs et premiers entre eux, l'application $(x, y) \longmapsto xy$ est bijective de $\mathrm{div}^+(a) \times \mathrm{div}^+(b)$ sur $\mathrm{div}^+(ab)$, où $\mathrm{div}^+(k)$ est l'ensemble des diviseurs positifs de k pour tout $k \in \mathbb{N}^*$.

---

25 Soient $a, b \in \mathbb{N}^*$. À quelle condition nécessaire et suffisante existe-t-il deux entiers $x, y \in \mathbb{N}^*$ pour lesquels $x \vee y = a$ et $xy = b$?

26

1) Soient $x \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ premiers entre eux.

a) Pourquoi l'application qui associe à tout entier $k \in [\![0, n]\!]$ le reste de la division euclidienne de x^k par n n'est-elle pas injective ? En déduire que pour un certain $N \in [\![1, n]\!]$: $x^N \equiv 1 \ [n]$.

b) Montrer qu'on peut choisir N inférieur à l'entier $\varphi(n) = \Big|\big\{k \in [\![0, n-1]\!] \mid k \wedge n = 1\big\}\Big|$.

La fonction φ est appelée l'*indicatrice d'Euler*.

2) Soit $p \in \mathbb{P}$.

a) Montrer que p divise $\binom{p}{k}$ pour tout $k \in [\![1, p-1]\!]$.

b) En déduire que $(x+y)^p \equiv x^p + y^p \ [p]$ pour tous $x, y \in \mathbb{Z}$.

c) En déduire que pour tout $x \in \mathbb{Z}$:

$$x^p \equiv x \ [p] \qquad \textit{(petit théorème de Fermat)},$$

puis que si $x \wedge p = 1$, alors $x^{p-1} \equiv 1 \ [p]$.

d) Montrer que pour tous $y \in \mathbb{Z}$ et $k \in \mathbb{N}$:

$$y \equiv 1 \ \big[p^k\big] \implies y^p \equiv 1 \ \big[p^{k+1}\big].$$

e) En déduire que pour tous $x \in \mathbb{Z}$ premier à p et $k \in \mathbb{N}^*$: $x^{p^{k-1}(p-1)} \equiv 1 \ \big[p^k\big]$.

3) Soit $n \in \mathbb{N}^*$. On pose $N_n = \prod_{p \mid n} p^{v_p(n)-1}(p-1)$ où l'indice p est un nombre premier. Montrer que pour tous $x \in \mathbb{Z}$ premier à n : $x^{N_n} \equiv 1 \ [n]$ (*théorème d'Euler*). Nous montrerons au chapitre « Groupes et anneaux » qu'en réalité, $N_n = \varphi(n)$.

---

27 Déterminer toutes les parties non vides E de $\mathbb{N}^*$ pour lesquelles $\dfrac{x+y}{x\wedge y}\in E$ pour tous $x,y\in E$.

ÉQUATIONS DIOPHANTIENNES

28 Résoudre les équations d'inconnue $(x,y)\in\mathbb{N}^2$:

1) $\begin{cases} x\wedge y=3\\ x+y=18.\end{cases}$ **2)** $x\vee y=x+y-1$.

3) $(x\wedge y)+(x\vee y)=2x+3y$.

---

29 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.

---

30 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 qu'★ n'a pas de solution si c n'est pas un multiple de $a\wedge b$.

2) On suppose que $a\wedge b=1$.

a) Montrer qu'★ possède au moins une solution.

b) En déduire toutes les solutions d'★ et interpréter le résultat géométriquement.

3) Résoudre les équations d'inconnue $(x,y)\in\mathbb{Z}^2$:

a) $7x-12y=3$. **b)** $20x-53y=3$.

---

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

---

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

33

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 $(x,y,z)\in\left(\mathbb{N}^*\right)^3$.

---

34 Résoudre l'équation $x^y=y^x$ d'inconnue $(x,y)\in\left(\mathbb{N}^*\right)^2$.

---

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