1 DIVISIBILITÉ, DIVISION EUCLIDIENNE ET CONGRUENCES

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) Pour tous $p, q \in \mathbb{P}$, si : $q - p = 3$, alors : $p = 2$ et $q = 5$.
5) Si : $d | n^2$, alors : $d | n$.
6) Si : $a^2 \equiv 1\ [n]$, alors : $a \equiv \pm 1\ [n]$.
7) Si : $4a \equiv 4b\ [13]$, alors : $a \equiv b\ [13]$.
8) Si : $4a \equiv 4b\ [6]$, alors : $a \equiv b\ [6]$.
9) Si tout diviseur premier de n est congru à ± 1 modulo 8, alors : $n \equiv \pm 1\ [8]$. Et la réciproque ?

---

2 Montrer que $2^{123} + 3^{121}$ est divisible par 11.

---

3 Montrer que $n(n+2)(7n-5)$ est divisible par 6 pour tout $n \in \mathbb{Z}$.

---

4 Calculer le reste de la division euclidienne :

1) de 3^{2189} par 25. 2) de 55^{970321} par 8.
3) de $1234^{4321} + 4321^{1234}$ par 7.

5

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

---

6 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 de ses chiffres l'est.
3) Déterminer une condition nécessaire et suffisante sur $a_0, \ldots, a_r$ pour que n soit divisible par 11.

---

7 Montrer que pour tout $p \in \mathbb{P} \setminus \{2, 3\}$:
$$p^2 \equiv 1\ [24].$$

---

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

---

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

---

10 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, alors x, y ou z aussi.

---

11 Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle *sous-additive*, i.e. telle que pour tous $m, n \in \mathbb{N}$: $u_{m+n} \leqslant u_m + u_n$.
On pose : $A = \left\{ \dfrac{u_n}{n} \right\}_{n\in\mathbb{N}^*}$.

1) On suppose A minoré et on pose : $a = \inf A$.
   a) Soient $n, N \in \mathbb{N}^*$. On introduit la division euclidienne de n par N : $n = Nq + r$ avec $q \in \mathbb{N}$ et $r \in [\![0, N-1]\!]$. Montrer qu'alors :
   $$\frac{u_n}{n} \leqslant \frac{u_N}{N} + \frac{u_r}{n}.$$
   c) En déduire l'égalité : $\displaystyle\lim_{n\to+\infty} \frac{u_n}{n} = a$.
2) Montrer que : $\displaystyle\lim_{n\to+\infty} \frac{u_n}{n} = -\infty$ dans le cas où A n'est pas minoré.

En résumé, la limite : $\displaystyle\lim_{n\to+\infty} \frac{u_n}{n}$ existe toujours. Ce résultat est appelé le (*lemme sous-additif de Fekete*).

---

2 PGCD, PPCM ET NOMBRES PREMIERS ENTRE EUX

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 $n+1$ divise $\dbinom{2n}{n}$ pour tout $n \in \mathbb{N}$.

13

1) Montrer que $\dfrac{\ln 6}{\ln 7}$ est irrationnel.
2) Montrer que $\dfrac{\ln a}{\ln b}$ est irrationnel pour tous $a, b \geqslant 2$ premiers entre eux.

14

1) Calculer : $(n^3 + 3n^2 - 5) \wedge (n+2)$ pour tout $n \in \mathbb{Z}$.

2) Montrer que pour tout $n \in \mathbb{Z}$, les rationnels $\frac{21n-3}{4}$ et $\frac{15n+2}{4}$ ne peuvent pas être simultanément entiers.

15

1) Soient $a, b, n \in \mathbb{Z}$. On suppose que : $a \wedge n = 1$. Montrer qu'alors : $(ab) \wedge n = b \wedge n$.
2) Montrer que pour tout $n \in \mathbb{Z}$:

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

3) Simplifier : $(a+b) \wedge (a \vee b)$ pour tous $a, b \in \mathbb{Z}$.

---

16 Montrer que pour tous $a, b \in \mathbb{N}^*$:

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

---

17 Soient $a, b \in \mathbb{N}^*$ premiers entre eux.

1) Pour tout $k \in \mathbb{N}$, on note r_k le reste de la division euclidienne de a^k par b. Pourquoi l'application $k \longmapsto r_k$ n'est-elle pas injective de $\mathbb{N}$ dans $\mathbb{N}$?
2) En déduire que pour un certain $n \in \mathbb{N}^*$:

$$a^n \equiv 1 \; [b].$$

---

18 Pour tout $n \in \mathbb{N}^*$, on note $\operatorname{div}^+(n)$ l'ensemble des diviseurs positifs de n.
Soient $a, b \in \mathbb{N}^*$ premiers entre eux. Montrer que l'application $\left\{\begin{array}{ccc} \operatorname{div}^+(a) \times \operatorname{div}^+(b) & \longrightarrow & \mathbb{N} \\ (k,l) & \longmapsto & kl \end{array}\right.$ est bijective de $\operatorname{div}^+(a) \times \operatorname{div}^+(b)$ sur $\operatorname{div}^+(ab)$.

---

19 Soient $a_1, \ldots, a_r \in \mathbb{N}^*$ premiers entre eux deux à deux et $b \in \mathbb{Z}$.

1) Montrer que les entiers $\prod_{\substack{1 \leqslant i \leqslant r \\ i \neq k}} a_i$, k décrivant $[\![1, r]\!]$, sont premiers entre eux dans leur ensemble.
2) En déduire qu'il existe une et une seule famille d'entiers $(y, x_1, \ldots, x_r)$ telle que :

$$\frac{b}{a_1 \ldots a_r} = y + \sum_{k=1}^{r} \frac{x_k}{a_k}$$

avec : $0 \leqslant x_i < a_i$ pour tout $i \in [\![1, r]\!]$.

---

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

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.
On pose : $m = \min E \setminus \{2\}$.
 a) Montrer que m est impair.
 b) Montrer que E contient tous les entiers impairs plus grands que m.
 c) Montrer que E contient $2\mathbb{N}^*$.
 d) En déduire E.

---

3 VALUATIONS p-ADIQUES

21 Soient $a, b \in \mathbb{Z} \setminus \{0\}$. 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 pour tous $a, b, n \in \mathbb{N}^*$:

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

24

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 pour tout $k \in \mathbb{N}^*$: $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ dès que $p^k > n$.
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 $3^n - 1$.

---

4 NOMBRES PREMIERS

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

---

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

1) Proposer une factorisation non triviale de $a^n - 1$ en produit de deux entiers, puis montrer que : $a = 2$.

2) Montrer de même que n est premier.

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

29

1) a) Factoriser $a^{2n+1} + b^{2n+1}$ par $a + b$ pour tous $n \in \mathbb{N}$ et $a, b \in \mathbb{C}$.

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

Pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$ est appelé le $n^{ème}$ *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. Les nombres de Fermat premiers jouent un rôle étonnant dans le problème de la constructibilité à la règle et au compas des polygones réguliers.

2)

a) Montrer que pour tout $n \in \mathbb{N}$:

$$F_{n+1} = F_0 \dots F_n + 2.$$

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.

---

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

1) Montrer que :

$$\forall y \in [\![1, p-1]\!], \quad \exists\,!\, x \in [\![1, p-1]\!] / \quad xy \equiv 1\ [p].$$

2) En déduire le *théorème de Wilson* :

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

3) On suppose p impair. Montrer que :

$$\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}}\ [p].$$

---

5 ÉQUATIONS DIOPHANTIENNES

32 Résoudre les équations suivantes 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) $x \vee y = x + y - 1$.

---

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

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.

34

1)

a) Déterminer un entier $n \in \mathbb{Z}$ pour lequel : $5n \equiv 1\ [28]$.

b) Résoudre l'équation : $5x \equiv 3\ [28]$ d'inconnue $x \in \mathbb{Z}$.

2) Résoudre l'équation : $14x \equiv 6\ [34]$ d'inconnue $x \in \mathbb{Z}$.

3) Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On s'intéresse à l'équation : $ax \equiv b\ [n]$ $\bigstar$ d'inconnue $x \in \mathbb{Z}$.

a) Montrer que $\bigstar$ n'a pas de solution si b n'est pas un multiple de $a \wedge n$.

b) Résoudre $\bigstar$ dans le cas où $a \wedge n$ divise b.

---

35 Soient $a, b, c \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. On s'intéresse à l'équation : $ax + by = c$ $\bigstar$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

1) Montrer que $\bigstar$ 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 $\bigstar$ possède une solution (x_0, y_0).

b) Résoudre alors $\bigstar$.

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

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

---

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

---

37 On veut résoudre l'équation : $x^2 + y^2 = 3z^2$ $\bigstar$ d'inconnue $(x, y, z) \in \mathbb{N}^3$.

1) En raisonnant modulo 4, montrer que pour toute solution (x, y, z) de $\bigstar$, x, y et z sont pairs.

2) En déduire les solutions d'$\bigstar$.

---

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

---

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, après l'avoir factorisé, que y^2+1 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 $x, y \in \mathbb{N}^*$. On suppose que : $x \leqslant y$ 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 $p \in \mathbb{P}$.
