

---

Feuille n° 2  
*Arithmétique.*

---

Dans toute la suite, on convient de noter  $a \wedge b$  le PGCD de deux entiers  $a$  et  $b$ , et  $a \vee b$  leur PPCM.

**Exercice 1.** Par combien de « 0 » se termine « 1000! » ?

**Exercice 2.** Montrer que pour tout entier naturel  $n$  :

- 111 divise  $10^{6n} + 10^{3n} - 2$ .
- 288 divise  $7^{2n+1} - 48n - 7$ .
- 7 divise  $4^{2^n} + 2^{2^n} + 1$ .
- 9 divise  $2^{2^n} + 15n - 1$ .

**Exercice 3.**

1. Quel est le dernier chiffre de  $7^{7^7}$  ?
2. Quel est le reste de la division euclidienne par 7 de  $10^{10^n}$  ( $n \in \mathbb{N}$ ) ?

**Exercice 4.** Est-ce que 13 divise  $2^{70} + 3^{70}$  ?

**Exercice 5.** Montrer que pour tout entier naturel  $k$  impair, et tout entier naturel  $n \geq 1$ ,  $2^{n+2}$  divise  $k^{2^n} - 1$ .

**Exercice 6.**

1. Déterminer tous les entiers naturels ayant exactement 1789 diviseurs.
2. Pour  $n \in \mathbb{N}^*$ , on note  $N$  le nombre de ses diviseurs et  $P$  leur produit. Établir l'identité  $P^2 = n^N$ .

**Exercice 7.** Quels sont les nombres premiers  $p$  tels que  $p$  divise  $2^p + 1$  ?

**Exercice 8.**

1. Soient  $a, b$  et  $c$  trois entiers naturels. Montrer que
  - (a) Si 5 divise  $a^2 + b^2 + c^2$  alors 5 divise  $abc$ .
  - (b) Si 7 divise  $a^3 + b^3 + c^3$  alors 7 divise  $abc$ .
  - (c) Trouver une généralisation en observant que 5 et 7 sont premiers.

**Exercice 9.**

1. Soit  $m$  et  $n$  deux entiers naturels premiers entre eux,  $a$  et  $b$  deux entiers  $> 1$ . Montrer que  $a^m = b^n$  si et seulement si il existe un entier naturel  $x$  tel que  $a = x^n$  et  $b = x^m$ .
2. Que peut-on dire si l'on omet l'hypothèse «  $m$  et  $n$  premiers entre eux » ?
3. Étant donnés deux entiers naturels  $> 1$   $a$  et  $b$ , à quelle condition le réel  $\log_b a$  est-il rationnel ?

**Exercice 10.** Le produit de trois entiers naturels consécutifs peut-il être un carré ? un cube ? une puissance  $k$ ème ? [remarquer que le produit de 3 entiers consécutifs s'écrit sous la forme  $n(n^2 - 1)$  et que  $n$  et  $n^2 - 1$  sont premiers entre eux]

**Exercice 11.** Soit  $n$  un entier naturel  $\geq 2$ . Montrer que parmi  $n + 1$  entiers distincts entre 2 et  $2n$ , deux au moins sont tels que l'un divise l'autre [on pourra écrire chacun de ces entiers sous la forme  $a = 2^k b$  avec  $b$  impair].

**Exercice 12.** Soient  $1 < n \leq m$  deux entiers naturels et  $S_{n,m} = \sum_{k=n}^m \frac{1}{k}$ . On veut montrer que  $S_{n,m}$  n'est pas un entier. Pour  $n \leq k \leq m$ , on pose  $k = 2^{a_k} q_k$  avec  $q_k$  impair.

1. Montrer que  $a := \max \{a_k, n \leq k \leq m\}$  est atteint pour un unique entier  $k_0$  entre  $n$  et  $m$ .
2. En déduire que  $S_{n,m}$  n'est pas entier.

**Exercice 13. Triplets pythagoriciens** On appelle *triplet pythagorien* tout triplet d'entiers naturels non nuls  $(x, y, z)$  vérifiant la relation  $x^2 + y^2 = z^2$ . Un tel triplet est dit *primitif* si les trois entiers  $x, y, z$  sont premiers entre eux.

1. Montrer que si  $(x, y, z)$  est un triplet pythagorien primitif, alors  $x$  et  $y$  sont de parités différentes.
2. Montrer que les deux assertions suivantes sont équivalentes
  - (a)  $(x, y, z)$  est un triplet pythagorien primitif avec  $x$  impair.
  - (b) Il existe  $(p, q) \in \mathbb{N}^{*2}$  avec  $p > q$ ,  $p$  et  $q$  premiers entre eux et de parités différentes tels que
    - i.  $x = p^2 - q^2$ .
    - ii.  $y = 2pq$ .
    - iii.  $z = p^2 + q^2$ .

**Exercice 14.** Soient  $a$  et  $b$  deux entiers naturels,  $d = a \wedge b$  leur PGCD,  $m = a \vee b$  leur PPCM. Montrer que  $dm = ab$

**Exercice 15.** Démontrer que pour  $a \geq 2$ ,  $m \in \mathbb{N}^*$  et  $n \in \mathbb{N}^*$

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

où  $d = m \wedge n$ .

**Exercice 16.** Soient  $a, b, c, d$  quatre entiers tels que  $ad - bc = 1$ . Montrer que

$$(am + bn) \wedge (cm + dn) = m \wedge n.$$

**Exercice 17. Théorème de Lamé.** Le but de cet exercice est de montrer le théorème suivant :

Soient  $a$  et  $b$  deux entiers naturels non nuls, avec  $a > b$ . Alors, le nombre d'étapes de l'algorithme d'Euclide appliqué au couple  $(a, b)$  est majoré par

$$5 \times (\text{nombre de chiffres de l'écriture en base 10 de } b).$$

Écrivons les premières (et les dernières) étapes de l'algorithme d'Euclide :

$$r_0 := a = bq_1 + r_2, \quad 0 \leq r_2 < b \tag{1}$$

$$r_1 := b = r_2q_2 + r_3, \quad 0 \leq r_3 < r_2 \tag{2}$$

$$\vdots \tag{3}$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1} \tag{4}$$

$$r_{n-1} = r_nq_n \tag{5}$$

1. Montrer que pour tout  $0 \leq i \leq n$  on a

$$r_{n-i} \geq f_{i+2}$$

où  $f_k$  désigne le  $k$ ième terme de la suite de Fibonacci  $f_1 = f_2 = 1, f_k = f_{k-1} + f_{k-2}$  pour  $k \geq 3$ .  
[remarquer que  $q_k \geq 1$  pour tout  $k$  et  $q_n \geq 2$ ].

2. En déduire que  $b \geq \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}$ .
3. Montrer que  $\log_{10} \left(\frac{1+\sqrt{5}}{2}\right) \geq \frac{1}{5}$ .
4. Conclure.

**Exercice 18.** Soit  $\phi_n$  la suite de Fibonacci définie par  $\phi_0 = 0, \phi_1 = 1$  et  $\phi_{n+2} = \phi_n + \phi_{n+1}$  pour tout  $n \geq 0$ .

1. Établir que  $\forall n \in \mathbb{N}^*, \phi_{n+1}\phi_{n-1} - \phi_n^2 = (-1)^n$ . En déduire que  $\forall n \in \mathbb{N}^*, \phi_n$  et  $\phi_{n-1}$  sont premiers entre eux.
2. Montrer, pour tout  $n \in \mathbb{N}^*$ , les égalités suivantes :

$$\sum_{i=1}^n \phi_i = \phi_{n+2} - 1, \quad \sum_{i=1}^n \phi_i^2 = \phi_n \phi_{n+1}, \quad \sum_{i=1}^{2n-1} \phi_i \phi_{i+1} = \phi_{2n}^2, \quad \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n-i}{i} = \phi_{n+1}.$$

3. Montrer que  $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}^*, \phi_{n+m} = \phi_m \phi_{n+1} + \phi_{m-1} \phi_n$ . En déduire que  $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}^*, \phi_{n+m} \wedge \phi_m = \phi_n \wedge \phi_m$ .
4. Montrer que si  $r$  est le reste de la division euclidienne de  $a \in \mathbb{N}$  par  $b \in \mathbb{N}^*$ , alors  $\phi_a \wedge \phi_b = \phi_b \wedge \phi_r$ . En déduire que  $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}^*, \phi_n \wedge \phi_m = \phi_{n \wedge m}$ .

**Exercice 19.** *Algorithme d'Euclide étendu.*

Soient  $a$  et  $b$  deux entiers naturels non nuls. On reprend les notations de l'exercice précédent pour l'algorithme d'Euclide (1), et à côté de la suite des restes  $(r_i)_{i \in \mathbb{N}}$  on définit deux suites  $(u_i)_{i \in \mathbb{N}}$  et  $(v_i)_{i \in \mathbb{N}}$  de la façon suivante :

1.  $u_0 = 1, v_0 = 0, u_1 = 0, v_1 = 1$ .
2. pour  $i \geq 2, u_i = u_{i-2} - u_{i-1}q_{i-1}$  et  $v_i = v_{i-2} - v_{i-1}q_{i-1}$ .

Montrer que le couple  $(u_n, v_n)$  que l'on obtient à la sortie de l'algorithme fournit une relation de Bezout, c'est-à-dire

$$au_n + bv_n = a \wedge b.$$

Montrer en outre que  $|u_n| \leq b$  et  $|v_n| \leq a$ .

**Exercice 20.** *Le problème des scores.* Soient  $a$  et  $b$  deux entiers naturels non nuls et premiers entre eux. Pour tout entier relatif  $c$  fixé, on considère l'équation

$$ax + by = c, \quad (x, y) \in \mathbb{Z}^2 \tag{6}$$

1. Montrer que quel que soit l'entier  $c$ , l'équation (6) admet des solutions dans  $\mathbb{Z}^2$ .
2. Montrer que si le couple  $(x, y)$  est solution de (6), alors pour tout  $k \in \mathbb{Z}$ , le couple  $(x + kb, y - ka)$  est également solution. En déduire que pour tout entier  $c$ , l'équation (6) admet une solution  $(x, y) \in \mathbb{Z}^2$  avec  $0 \leq y \leq a - 1$ .

3. En déduire que si  $c > ab - a - b$ , il existe (au moins) un couple  $(x, y)$  d'entiers *positifs ou nuls* solution de l'équation (6).
4. Montrer enfin que si  $c = ab - a - b$ , l'équation (6) n'a pas de solution avec  $x$  et  $y$  entiers naturels.
5. Application : quels sont les scores réalisables au rugby ? On rappelle qu'une pénalité ou un drop rapportent 3 points, un essai 5 et un essai transformé 7.

**Exercice 21.** Montrer que 1996 a un multiple qui ne s'écrit qu'avec des 4.

**Exercice 22.** *Test de Lucas - Nombres de Fermat*

1. On rappelle que si  $p$  est un nombre premier, le groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^\times$  des éléments inversibles modulo  $p$  est cyclique d'ordre  $p - 1$ . On se propose de montrer dans cette question qu'un entier  $n$  est premier si et seulement si il existe  $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$  tel que

- $\alpha^{n-1} \equiv 1 \pmod{n}$
- $\alpha^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$  pour tout diviseur premier  $p$  de  $n - 1$ .

Ce critère est souvent appelé *test de Lucas* dans la littérature.

- (a) Montrer que si  $n$  est premier, tout générateur  $\alpha$  du groupe (cyclique)  $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$  convient.
  - (b) Inversement, montrer qu'un élément  $\alpha$  satisfaisant les conditions ci-dessus est nécessairement d'ordre  $n - 1$  dans  $(\mathbb{Z}/n\mathbb{Z})^\times$  et conclure.
2. Soit  $a$  un entier  $\geq 2$ , et  $n$  un entier  $\geq 1$ . Montrer que si  $a^n + 1$  est premier, alors  $a$  est pair et  $n$  est une puissance de 2.
  3. On définit pour  $n \in \mathbb{N}$  le nombre  $F_n = 2^{2^n} + 1$  ("n<sup>ième</sup> nombre de Fermat").
    - (a) Montrer que si  $n \neq m$ ,  $F_n$  et  $F_m$  sont premiers entre eux.
    - (b) En utilisant le test de Lucas, montrer que  $F_n$  est premier si et seulement si il existe  $k \in \mathbb{Z}$  tel que  $k^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$

**Exercice 23.** Soit  $x = \frac{p}{q}$  un rationnel **non décimal** avec  $p$  et  $q$  étrangers. On pose  $q = 2^\alpha 5^\beta q_1$ , avec  $q_1$  étranger à 10, et l'on note  $\gamma := \max(\alpha, \beta)$  et  $\nu :=$  l'ordre de 10 dans le groupe multiplicatif  $(\mathbb{Z}/q_1\mathbb{Z})^\times$ , c'est-à-dire le plus petit entier naturel non nul tel que  $10^\nu \equiv 1 \pmod{q_1}$ .

1. Montrer que

$$x = a_0, a_1 \cdots a_\gamma \overline{a_{\gamma+1} \cdots a_{\gamma+\nu}},$$

la notation  $\overline{a_{\gamma+1} \cdots a_{\gamma+\nu}}$  signifiant que le motif  $a_{\gamma+1} \cdots a_{\gamma+\nu}$  se répète à l'infini.

2. Montrer en outre que  $\nu$  est le plus petit entier vérifiant cette propriété, c'est-à-dire que tout entier  $m$  tel que le développement de  $x$  se termine par un motif récurrent de longueur  $m$  est un multiple de  $\nu$ .
3. Déterminer, pour tout entier naturel  $k$ , un rationnel dont le développement décimal est périodique de période  $k$ .