► MINES 1 **Une divisibilité par** 19

Montrer que pour tout $n \in \mathbb{N}$, 19 divise $2^{2^{6n+2}} + 3$.

▷ **Réponse**

Pour $n \in \mathbb{N}$, on pose $p_n = 2^{2^{6n+2}} + 3$ et $\mathscr{P}(n)$ la propriété : « 19 divise p_n ». Procédons par récurrence sur $\mathbb{N}$.

• *Initialisation :* $p_0 = 19$ donc $\mathscr{P}(0)$ est vraie.

• *Hérédité :* supposons $\mathscr{P}(n)$ vraie pour un $n \in \mathbb{N}$ et montrons $\mathscr{P}(n+1)$. On écrit,

$$\begin{aligned} p_{n+1} &= 2^{2^{6n+8}} + 3 = 2^{2^{6n+2} \times 2^6} + 3 \\ &= \left(2^{2^{6n+2}}\right)^{2^6} + 3 = (p_n - 3)^{2^6} + 3 \end{aligned}$$

Comme $p_n \equiv 0\,[19]$, on a $p_n - 3 \equiv -3\,[19]$ ainsi, $(p_n - 3)^{2^6} \equiv 3^{2^6}\,[19]$. Cependant, $3^4 \equiv 5\,[19]$ donc $3^{2^3} \equiv 6\,[19]$ puis $3^{2^4} \equiv -2\,[19]$, et $3^{2^5} \equiv 4\,[19]$, enfin $3^{2^6} \equiv -3\,[19]$. On en déduit que $(p_n - 3)^{2^6} + 3 \equiv 0\,[19]$ donc $p_{n+1} \equiv 0\,[19]$. La récurrence est établie.

► X 2 **Nombres de Fermat**

Soient $n \in \mathbb{N}$ et $F_n = 2^{2^n} + 1$. Montrer que les éléments de la suite $(F_n)_{n\in\mathbb{N}}$ sont premiers entre eux deux à deux, en déduire l'existence d'une infinité de nombres premiers.

▷ **Réponse**

• Soit $(m, n) \in \mathbb{N}^2$ tel que $m \neq n$. On suppose, par exemple, que $m > n$. Alors :

$$\begin{aligned} F_m &= (2^{2^n})^{2^{m-n}} + 1 \\ &= (F_n - 1)^{2^{m-n}} + 1 \\ &= \sum_{k=1}^{2^{m-n}} \binom{2^{m-n}}{k} F_n^k (-1)^{2^{m-n}-k} + 2. \end{aligned}$$

Il existe donc un entier relatif q tel que $F_m = qF_n + 2$. Un diviseur commun à F_n et F_m divise donc 2 et F_m (qui est impair), donc le plus grand diviseur commun à F_n et F_m est 1 : on a donc F_n et F_m premiers entre eux.

• Pour tout $m \in \mathbb{N}$, on note p_m un diviseur premier de F_m. La suite $(p_m)_{m\in\mathbb{N}}$ est une suite de nombres premiers, qui sont premiers entre eux par le point précédent, donc deux à deux distincts : on a bien prouvé l'existence d'une infinité de nombres premiers.

► CLASSIQUE 3 **Racines n-ème d'un rationnel**

Soit q un rationnel positif différent de 0 et de 1. Montrer que la suite $(q^{1/n})_{n\in\mathbb{N}^*}$ est constituée d'irrationnels à partir d'un rang que l'on explicitera.

Remarque : en corollaire de la preuve qui suit, $\sqrt{p}$ est irrationnel si p est un entier premier.

▷ **Réponse**

On décompose q en puissances relatives de facteurs premiers suivant : $q = \prod_{i=1}^{r} p_i^{m_i}$, où $r \in \mathbb{N}^*$ puisque $q \neq 1$, chaque $m_i \in \mathbb{Z}^*$ et $p_1, \ldots, p_r$ sont des nombres premiers deux à deux distincts. Quitte à permuter les p_i, on peut supposer que $|m_1| = \min_{i \in [\![1\ ;\ r]\!]} |m_i|$. Soit $n \in \mathbb{N}^*$ tel que $n > |m_1|$, notons $I = \left\{ i \in [\![1\ ;\ r]\!], m_i > 0 \right\}$ et $I' = [\![1\ ;\ r]\!] \backslash I$. Quitte à raisonner sur q^{-1} puisque $q \neq 0$, on peut supposer que $1 \in I$. Supposons par l'absurde que $q^{\frac{1}{n}} \in \mathbb{Q}$, on le note alors $q^{\frac{1}{n}} = \dfrac{a}{b}$, avec (a, b) un couple d'entiers naturels premiers entre eux, a est non nul. Alors :

$$b^n . p_1^{m_1} . \prod_{i \in I \backslash \{1\}} p_i^{m_i} = a^n . \prod_{j \in I'} p_j^{-m_j} \qquad (*)$$

les facteurs de cette égalité sont tous des entiers relatifs : comme $m_1 \in \mathbb{N}^*$, p_1 divise le terme de droite, donc divise a^n par le théorème de Gauss, donc divise a par le lemme d'Euclide. On peut écrire $a = p_1 a'$, avec $a' \in \mathbb{N}^*$. En revenant à $(*)$, on a alors :

$$b^n \prod_{i \in I \backslash \{1\}} p_i^{m_i} = p_1^{n - m_1} . (a')^n . \prod_{j \in I'} p_j^{-m_j}$$

Comme $n - m_1 \in \mathbb{N}^*$, p_1 divise le terme de gauche, donc p_1 divise b par le lemme d'Euclide : p_1 est alors un facteur premier commun à a et b, alors qu'ils sont supposés premiers entre eux : c'est absurde, d'où le résultat : $q^{1/n}$ est irrationnel dès que n excède la valuation d'un facteur premier du numérateur ou du dénominateur.

► X 4 — *Congruence de matrices*

Soient $A \in \mathscr{M}_n(\mathbb{Z})$ et p un entier non nul tels que $A^p = I_n$. On suppose qu'il existe un entier $m \geqslant 3$ tel que $A \equiv I_n\,[m]$. Montrer : $A = I_n$.

▷ **Réponse**

• Tout d'abord, le polynôme $P = X^p - 1$ est scindé à racines simples dans $\mathbb{C}$ et annule la matrice A donc celle-ci est diagonalisable sur $\mathbb{C}$. De plus on a $\mathrm{Sp}(A) \subset \mathbb{U}_p$: ensemble des racines p-ème de l'unité. Pour prouver que $A = I_n$, il suffit maintenant de montrer que la seule valeur propre de A est 1.

• Notons λ_1, ..., λ_n les valeurs propres de A. Par hypothèse, il existe une matrice B dans $\mathscr{M}_n(\mathbb{Z})$ telle que $A = I_n + mB$ où m est un entier supérieur ou égal à 3, donc $B = \dfrac{1}{m}(A - I_n)$. Le spectre de B est donc

$$\mathrm{Sp}(B) = \left\{ \mu_j = \frac{\lambda_j - 1}{m}\ ;\ j \in [\![1, n]\!] \right\}.$$

Montrons que les valeurs propres de B sont nulles. Soit $j \in [\![1\ ;\ n]\!]$, comme $|\lambda_j| = 1$:

$$|\mu_j| = \left| \frac{\lambda_j - 1}{m} \right| \leqslant \frac{|\lambda_j| + 1}{m} \leqslant \frac{2}{3} < 1 \qquad (*)$$

Le polynôme caractéristique de B est à coefficients dans $\mathbb{Z}$ car $B \in \mathscr{M}_n(\mathbb{Z})$ et s'écrit

$$\chi_B(X) = (-1)^n \left[X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \cdots + (-1)^n \sigma_n \right]$$

où σ_1, ..., σ_n désignent les fonctions symétriques élémentaires portant sur $\mu_1, \ldots, \mu_n$.

D'après $(*)$, on a $|\sigma_n| = \left| \prod_{j=1}^{n} \mu_j \right| < 1$, or $\sigma_n \in \mathbb{Z}$ donc $\sigma_n = 0 = \det(B)$. Ainsi, il existe $j_1 \in [\![1, n]\!]$ tel que $\mu_{j_1} = 0$. Mais alors, on a $\sigma_{n-1} = \sum_{j=1}^{n} \prod_{k \neq j} \mu_k = \prod_{k \neq j_1} \mu_k$, et à nouveau $|\sigma_{n-1}| < 1$ puis

$\sigma_{n-1} = 0$ car $\sigma_{n-1} \in \mathbb{Z}$. On en déduit qu'il existe $j_2 \in [\![1, n]\!] \setminus \{j_1\}$ tel que $\mu_{j_2} = 0$. On peut encore écrire

$$\sigma_{n-2} = \sum_{1 \leqslant k_1 < k_2 \leqslant n} \prod_{k \neq k_1, k \neq k_2} \mu_k = \prod_{k \neq j_1, k \neq j_2} \mu_k$$

puis à nouveau $\sigma_{n-2} = 0$. On itère ce procédé pour obtenir finalement, $\chi_B(X) = (-1)^n X^n$, donc les valeurs propres de B sont toutes nulles, donc les valeurs propres de A valent toutes 1. Comme A est diagonalisable sur $\mathbb{C}$, on déduit que $A = I_n$.

▶ X 5 — *Une divisibilité grâce aux déterminants.*

Soient $n \in \mathbb{N}^*$ et A, B dans $\mathscr{M}_n(\mathbb{R})$. On suppose que $AB - BA$ est inversible et que $A^2 + B^2 = \sqrt{3}(AB - BA)$. Montrer que n est un multiple de 6.

▷ **Réponse**
Commençons par remarquer que

$$(A + iB) \times (A - iB) = A^2 + B^2 - i\,(AB - BA) = \left(\sqrt{3} - i\right)(AB - BA)\,.$$

De plus, comme A et B sont à coefficients réels, l'expression du déterminant en fonction des coefficients donne $\overline{\det(A + iB)} = \det(\overline{A + iB}) = \det(A - iB)$. Mais alors on peut écrire :

$$\det\left[(A + iB)(A - iB)\right] = \det(A+iB)\det(A-iB) = \det(A+iB) \times \overline{\det(A + iB)} = |\det(A + iB)|^2\,.$$

En utilisant le déterminant dans l'égalité trouvée plus haut, on obtient

$$|\det(A + iB)|^2 = \left(\sqrt{3} - i\right)^n \det(AB - BA)\,.$$

Comme $AB - BA$ est inversible dans $\mathscr{M}_n(\mathbb{R})$, $\det(AB - BA) \in \mathbb{R}^*$, cependant $|\det(A + iB)|^2$ est aussi un réel donc $\left(\sqrt{3} - i\right)^n \in \mathbb{R}^*$. C'est à dire, $\left(\sqrt{3} - i\right)^n = 2^n \left(e^{-i\frac{\pi}{6}}\right)^n = 2^n e^{-i\frac{n\pi}{6}} \in \mathbb{R}^*$ donc $\dfrac{n\pi}{6} \equiv 0[\pi]$ ou encore $n \equiv 0[6]$.

▶ X 6 — *Dichotomie radicale*

Soit X une partie de $\mathbb{R}_+^*$ contenant au moins deux éléments, et telle que :

$$\forall (a, b) \in X^2, \quad \sqrt{ab} \in X.$$

Montrer que les irrationnels de X sont denses dans $]\inf X, \sup X[$, le sup est envisagé dans $\overline{\mathbb{R}}$.

Remarque : on pourra utiliser l'exercice 3 page 14.

▷ **Réponse**
• *Remarque :* l'inf est licite puisque X est non vide et minoré par 0. Il diffère de $\sup(X)$ puisque X contient au moins deux éléments.
• Voici le plan de la preuve :
(i) pour tout $y \in]\inf X, \sup X[$, on construit deux suites $(x_n^+)_n$ et $(x_n^-)_n$ constituées d'éléments de X, qui sont adjacentes, de limite y ;
(ii) on montre qu'il existe toujours un irrationnel de X entre deux éléments distincts de X ;
(iii) on conclut.

• *Preuve de (i).* Soit $y \in]\inf X, \sup X[$: il existe x^- et x^+ dans X tel que $x^- < y < x^+$. Par une dichotomie classique, on construit une suite d'éléments de l'intervalle $[\ln(x^-), \ln(x^+)]$ convergeant vers $\ln(y)$ en définissant les suites $(u_n)_n$ et $(v_n)_n$ par :

➢ $u_0 = \ln(x^-)$ et $v_0 = \ln(x^+)$,

➢ pour tout $n \in \mathbb{N}$ tel que u_n et v_n sont définis, alors :

  ➢ si $\ln(y) \in \left[u_n, \dfrac{u_n + v_n}{2}\right]$ alors on pose $u_{n+1} = u_n$ et $v_{n+1} = \dfrac{u_n + v_n}{2}$;

  ➢ sinon on pose $u_{n+1} = \dfrac{u_n + v_n}{2}$ et $v_{n+1} = v_n$.

On construit ainsi deux suites adjacentes $(u_n)_n$ et $(v_n)_n$ de limite commune $\ln(y)$. On définit maintenant :

$$\forall n \in \mathbb{N}, \quad x_n^- = \exp(u_n) \text{ et } x_n^+ = \exp(v_n).$$

Les suites $(x_n^-)_n$ et $(x_n^+)_n$ sont adjacentes, de limite commune y. De plus, on peut montrer par récurrence que tous les x_n^+ et x_n^- sont dans X, avec $x_n^- < x_n^+$: c'est vrai pour $n = 0$, et si (x_n^-, x_n^+) est dans X^2 alors :

➢ soit $x_{n+1}^+ = x_n^+$ et $x_{n+1}^- = \sqrt{x_n^- x_n^+} \in X$ avec $x_{n+1}^- < x_{n+1}^+$;

➢ soit $x_{n+1}^- = x_n^-$ et $x_{n+1}^+ = \sqrt{x_n^- x_n^+} \in X$ avec $x_{n+1}^- < x_{n+1}^+$.

Ceci achève la preuve du (i).

• *Preuve de (ii).* Soient $0 < a < b$ deux éléments de X. Si l'un d'entre eux est irrationnel, l'intervalle $[a, b]$ contient bien un irrationnel de X. Si a et b sont rationnels, alors on définit la suite $(x_n)_n$ par $x_0 = b$ et : $\forall n \in \mathbb{N}, \quad x_{n+1} = \sqrt{a x_n}$. C'est une suite d'éléments de $X \cap [a, b]$ et l'on peut montrer par récurrence que $x_n = a \left(\dfrac{b}{a}\right)^{\frac{1}{2^n}}$ pour tout $n \in \mathbb{N}$. Comme dans l'exercice 3 page 14, on montre que $\left(\dfrac{b}{a}\right)^{\frac{1}{2^n}}$ est irrationnel à partir d'un certain rang, ce qui implique l'irrationalité de x_n et le (ii).

• *Preuve de (iii).* Considérons les suites $(x_n^-)_n$ et $(x_n^+)_n$ du (i). Pour tout $n \in \mathbb{N}$, $x_n^- < x_n^+$ dans X, donc par le (ii) : il existe $x_n \in [x_n^-, x_n^+]$ tel que $x_n \in X \backslash \mathbb{Q}$. La suite $(x_n)_n$ ainsi construite est une suite d'éléments de $X \backslash \mathbb{Q}$, de limite y quelconque dans $]\inf X, \sup X[$: d'où le résultat.

▶ MINES 7 — *Maximisation sur les permutations*

Déterminer, pour $n \geqslant 2$, les permutations $\sigma \in \mathscr{S}_n$ telles que $S(\sigma) = \sum_{k=1}^{n} k\sigma(k)$ est maximal.

▷ **Réponse**

Soit σ dans $\mathscr{S}_n$, différente de l'identité donc l'ensemble : $X = \left\{ j \in [\![1\ ;\ n]\!], j > \sigma(j) \right\}$ est non vide, on note i son plus petit élément, donc

$$\sigma(i) < i. \qquad (*)$$

En particulier, $\sigma(i) \notin X$ donc on a $\sigma(\sigma(i)) \geqslant \sigma(i)$. L'égalité est impossible, sinon $\sigma(i) = i$ par injectivité de σ, d'où :

$$\sigma(\sigma(i)) > \sigma(i). \qquad (**)$$

Soit $\tau = (i, \sigma(i))$ la transposition échangeant i et $\sigma(i)$, ainsi que $\widetilde{\sigma} = \sigma \circ \tau$, qui ne diffère de σ qu'en i et $\sigma(i)$. On a donc :

$$\begin{aligned} S(\widetilde{\sigma}) - S(\sigma) &= i(\widetilde{\sigma}(i) - \sigma(i)) + \sigma(i)(\widetilde{\sigma}(\sigma(i)) - \sigma(\sigma(i))) \\ &= i(\sigma(\sigma(i)) - \sigma(i)) + \sigma(i)(\sigma(i) - \sigma(\sigma(i))) \\ &= (\sigma(\sigma(i)) - \sigma(i))\,(i - \sigma(i)) \\ &> 0 \end{aligned}$$

par $(*)$ et $(**)$. Une permutation différente de l'identité ne peut maximiser S. Le maximum de S n'est donc réalisé qu'en l'identité.

▶ CENTRALE 8 **Partie entière et arithmétique**

Ici, la notation $E[X]$ désigne la partie entière d'un réel X.

a) Montrer que $\mathrm{E}\left[\left(2+\sqrt{3}\right)^n\right]$ *est impair pour tout* $n \in \mathbb{N}$.

b) Montrer que $\mathrm{E}\left[\left(1+\sqrt{3}\right)^{2n+1}\right]$ *est divisible par* 2^{n+1} *pour tout* $n \in \mathbb{N}$.

a) Pour $n \in \mathbb{N}$, on pose $p_n = \left(2+\sqrt{3}\right)^n$ et $q_n = \left(2-\sqrt{3}\right)^n$. Remarquons que (p_n) et (q_n) sont solutions de l'équation récurrente linéaire d'ordre 2 :

$$\forall n \in \mathbb{N}, \quad u_{n+2} - 4u_{n+1} + u_n = 0 \qquad (*)$$

Cherchons à exprimer $\mathrm{E}[p_n]$ grâce à p_n et à q_n. Pour tout $n \in \mathbb{N}$, on a $0 < q_n < 1$ donc $p_n < p_n + q_n < p_n + 1$ ainsi

$$\forall n \in \mathbb{N}, \quad p_n + q_n - 1 < p_n < p_n + q_n \qquad (**)$$

Pour tout $n \in \mathbb{N}$, posons $v_n = p_n + q_n$, par linéarité (v_n) est solution de $(*)$, avec les conditions initiales $v_0 = p_0 + q_0 = 2$, $v_1 = p_1 + q_1 = 4$ qui sont des entiers pairs. Par une récurrence à deux pas immédiate, v_n est un entier pair pour tout $n \in \mathbb{N}$. Par définition de la partie entière et grâce à $(**)$, on peut donc affirmer que $v_n - 1 = p_n + q_n - 1 = \mathrm{E}[p_n]$. On en déduit que $\mathrm{E}\left[\left(2+\sqrt{3}\right)^n\right]$ est impair pour tout $n \in \mathbb{N}$.

b) Utilisons la même méthode et posons pour $n \in \mathbb{N}$, $p_n = \left(1+\sqrt{3}\right)^n$ et $q_n = \left(1-\sqrt{3}\right)^n$ son conjugué : (p_n) et (q_n) sont solutions de l'équation récurrente linéaire d'ordre 2 suivante :

$$\forall n \in \mathbb{N}, \quad u_{n+2} - 2u_{n+1} - 2u_n = 0 \qquad (***)$$

Comme $-1 < 1 - \sqrt{3} < 0$, pour tout $n \in \mathbb{N}$, on a $-1 < q_{2n+1} < 0$, ainsi :

$$\forall n \in \mathbb{N}, \quad p_{2n+1} - 1 < p_{2n+1} + q_{2n+1} < p_{2n+1}.$$

On pose alors $v_n = p_n + q_n$ et on obtient

$$\forall n \in \mathbb{N}, \quad v_{2n+1} < p_{2n+1} < v_{2n+1} + 1 \qquad (****)$$

Comme (v_n) est solution de $(***)$ avec $v_0 = 2$ et $v_1 = 2$, on montre par une récurrence à deux pas immédiate que v_n est un entier pour tout $n \in \mathbb{N}$ donc il en va de même pour v_{2n+1}. Enfin grâce à $(****)$,

$$\forall n \in \mathbb{N}, \quad \mathrm{E}[p_{2n+1}] = v_{2n+1}.$$

Montrons par récurrence que pour tout $n \in \mathbb{N}$, 2^{n+1} divise v_{2n+1} et 2^{n+1} divise v_{2n+2}.

• *Initialisation :* pour $n = 0$, $v_1 = 2$, $v_2 = 8$ donc 2 divise v_1 et v_2.

• *Hérédité :* supposons que 2^{n+1} divise v_{2n+1} et v_{2n+2} alors par $(***)$,

$$v_{2n+3} = 2(v_{2n+2} + v_{2n+1})$$

$$v_{2n+4} = 2(v_{2n+3} + v_{2n+2})$$

donc 2^{n+2} divise v_{2n+3} puis 2^{n+2} divise v_{2n+4}. La récurrence est établie.

• En conclusion : pour tout $n \in \mathbb{N}$, 2^{n+1} divise $\mathrm{E}\left[\left(1+\sqrt{3}\right)^n\right]$.

► CLASSIQUE 9 — *Sous-groupes additifs de* $\mathbb{R}$

Soit H un sous-groupe du groupe $(\mathbb{R},+)$. Montrer qu'on a l'alternative :

(i) il existe $a\in\mathbb{R}$ tel que $H=a\mathbb{Z}$ (on parle de **sous-groupe discret***) ;*

(ii) ou alors H est dense dans $\mathbb{R}$.

Application : *en déduire que, pour $\alpha\in\mathbb{R}$ donné, la suite $\big(\cos(n\alpha)\big)_n$ est périodique ou dense dans $[-1,1]$.*

▷ **Réponse**

• *Remarque :* soit $(a,b)\in\mathbb{N}^*\times\mathbb{N}$. On notera a/b pour signifier que a divise b dans $\mathbb{Z}$.

• Si $H=\{0\}$, alors on est dans la situation (i) en posant $a=0$. Nous supposerons par la suite que $H\neq\{0\}$, donc $H\cap\mathbb{R}_+^*$ est non vide puisque H contient h et $-h$ pour tout $h\in H\backslash\{0\}$. On note alors $a=\inf\{H\cap\mathbb{R}_+^*\}$.

• *Cas 1 : $a>0$*, nous allons montrer que dans ce cas $H=a\mathbb{Z}$.

➢ On montre tout d'abord que $a\in H$; en effet, $2a$ n'est pas un minorant de $H\cap\mathbb{R}_+^*$ puisque $a>0$ donc il existe $h\in H$ tel que $a\leqslant h<2a$. Si $h=a$, on a bien $a\in H$. Sinon, $a<h$ et h n'est pas un minorant de $H\cap\mathbb{R}_+^*$ donc il existe $h'\in H$ tel que $a\leqslant h'<h<2a$. Alors $0<h-h'\leqslant a$ avec $h-h'\in H\cap\mathbb{R}_+^*$, donc $h-h'=a$: on retrouve que $a\in H$.

➢ Puisque $a\in H$, on montre par récurrence que $(ap,-ap)\in H^2$ pour tout $p\in\mathbb{Z}$ en utilisant que H est stable par addition et inversion dans $(\mathbb{R},+)$; ceci prouve $a\mathbb{Z}\subset H$.

➢ On prouve l'inclusion réciproque : soit $h\in H$. Notons n la partie entière de h/a, on a l'encadrement $an\leqslant h<a(n+1)$, donc $0\leqslant h-an<a$. Remarquons que $h-na\in H$ puisque $(a,h)\in H^2$: $h-na\in H\cap\mathbb{R}_+$ donc $h-na=0$ sinon la définition de a est contredite. Finalement, $h=na\in a\mathbb{Z}$ et on a l'égalité d'ensembles $H=a\mathbb{Z}$.

• *Cas 2 : $a=0$*, nous allons montrer que dans ce cas H est dense dans $\mathbb{R}$. Soit $(x,y)\in\mathbb{R}^2$ tel que $x<y$. Le réel $y-x\in\mathbb{R}_+^*$ n'est donc pas un minorant de $H\cap\mathbb{R}_+^*$, ce qui veut dire qu'il existe $h\in H\cap\mathbb{R}_+^*$ tel que $0<h<y-x$. Soit n le plus petit entier relatif tel que $x<nh$, on a :

$$(n-1)h\leqslant x\ \text{ donc }\ nh\leqslant x+h<x+y-x=y$$

donc $x<nh<y$, donc $H\cap]x,y[\neq\emptyset$ pour tout intervalle $]x,y[$ non vide de $\mathbb{R}$: ceci exprime la densité de H dans $\mathbb{R}$.

• *Application :* soit $\alpha\in\mathbb{R}$, on note

$$u_n=\cos(n\alpha)$$

pour tout $n\in\mathbb{N}$. Si $\alpha=0$, la suite $(u_n)_n$ est constante donc 1-périodique. On suppose maintenant $\alpha\neq0$.

➢ *Cas 1 :* $\dfrac{\pi}{\alpha}\in\mathbb{Q}$, on note $\dfrac{2\pi}{\alpha}=\dfrac{a}{b}$ avec $(a,b)\in\mathbb{N}^*\times\mathbb{Z}^*$. Alors :

$$\forall n\in\mathbb{N},\quad u_n=\cos\left(n\frac{2\pi b}{a}\right).$$

La suite $(u_n)_n$ est alors a-périodique.

➢ *Cas 2 :* $\dfrac{\pi}{\alpha}\notin\mathbb{Q}$. On considère l'ensemble :

$$H=\alpha\mathbb{Z}+2\pi\mathbb{Z}=\Big\{\alpha k+2\pi l,(k,l)\in\mathbb{Z}^2\Big\}.$$

On vérifie rapidement qu'il s'agit d'un sous-groupe de $(\mathbb{R},+)$. Supposons qu'il soit de la forme $a\mathbb{Z}$ pour a nécessairement non nul. Alors $\alpha\in a\mathbb{Z}$ et $2\pi\in a\mathbb{Z}$ donc $\alpha=ap$ et $2\pi=aq$ pour deux entiers p et q nécessairement non nuls. Alors $\dfrac{2\pi}{\alpha}\in\mathbb{Q}$, ce qui est exclu. Donc H est dense dans $\mathbb{R}$ et, par continuité de cos, l'ensemble $\cos(H)$ est dense dans l'image de $\mathbb{R}$ par cos, qui est $[-1,1]$. Il suffit maintenant pour conclure d'observer que $(u_n)_n=\cos(H)$ par 2π-périodicité et parité de cos.

► MAPLE 10 **Fonction et inversion de Möbius**

La **fonction** $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ **de Möbius** *est définie suivant* $\mu(1) = 1$ *et, pour tout* $n \geqslant 2$ *:* $\mu(n) = (-1)^r$ *si* n *est un produit de* r *nombres premiers deux à deux distincts,* $\mu(n) = 0$ *si* n *est divisible par le carré d'un nombre premier.*

a) Montrer que μ *est une fonction multiplicative, c'est-à-dire :* $\mu(1) = 1$ *et, si* a *et* b *sont premiers entre eux,* $\mu(ab) = \mu(a)\mu(b)$.

b) On note d/n *pour signifier que l'entier naturel* $d \in \mathbb{N}^*$ *divise* $n \in \mathbb{N}^*$. *Montrer que :*

$$\forall n \geqslant 2, \quad \sum_{d/n} \mu(d) = 0.$$

c) Calculer les $\mu(n)$ *pour* $n \in [\![1\ ;\ 20]\!]$ *à l'aide de MAPLE — sans utiliser de commande MAPLE détectant les nombres premiers (de type* `isprime` *par exemple).*

d) Soient $f : \mathbb{N}^* \to \mathbb{C}$ *une application, on définit pour tout* $n \in \mathbb{N}^*$ *:* $g(n) = \sum_{d/n} f(d)$.

Prouver la **formule d'inversion de Möbius** *:*

$$\forall n \in \mathbb{N}^*, \quad f(n) = \sum_{d/n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d/n} \mu(d) g\left(\frac{n}{d}\right).$$

▷ **Réponse**

a) Par définition, $\mu(1) = 1$. Soient a et b deux entiers premiers entre eux.
- ➢ **Cas 1 :** Si l'un des deux est divisible par le carré d'un nombre premier, leur produit l'est aussi et alors $\mu(ab) = 0 = \mu(a)\mu(b)$ est triviale.
- ➢ **Cas 2 :** L'égalité reste triviale si $a = 1$ ou $b = 1$.
- ➢ **Cas 3 :** Dans le cas restant, on note $\mu(a) = (-1)^r$ et $\mu(b) = (-1)^s$, provenant de factorisations $a = p_1 \dots p_r$ et $b = q_1 \dots q_s$ écrites avec des premiers deux à deux distincts, on obtient donc $\mu(ab) = (-1)^{r+s} = \mu(a)\mu(b)$.

b) Nous allons montrer cette relation par récurrence forte sur n. La relation est vraie pour $n = 2$ puisque $\mu(1) + \mu(2) = 1 - 1 = 0$. Soit $n \geqslant 2$, supposons que ces relations soient vraies pour tous les rangs compris entre 2 et n. Si $n+1$ est de la forme p^r pour p premier et $r \in \mathbb{N}^*$. Alors les diviseurs de $n+1$ sont les p^k, pour $k \in [\![0\ ;\ r]\!]$, par définition :

$$\sum_{d/n+1} \mu(d) = \mu(1) + \mu(p) + 0 = 1 - 1 = 0.$$

Sinon, $n+1$ est de la forme rs, où r et s sont premiers entre eux et r et s sont supérieurs ou égaux à 2. Notons $D(r), D(s)$ et $D(rs)$ les ensembles respectifs des diviseurs de r, s, rs dans $\mathbb{N}^*$. L'application

$$\left| \begin{array}{ccc} D(r) \times D(s) & \longrightarrow & D(rs) \\ (d, d') & \longmapsto & dd' \end{array} \right.$$

est une bijection, on peut donc écrire :

$$\sum_{d/n+1} \mu(d) = \sum_{d \in D(rs)} \mu(d) = \sum_{(d,d') \in D(r) \times D(s)} \mu(dd') = \sum_{d \in D(r)} \sum_{d' \in D(s)} \mu(dd').$$

Dans cette somme, $\mu(dd') = \mu(d)\mu(d')$ puisque d et d' sont premiers entre eux. Donc

$$\sum_{d/n+1} \mu(d) = \left(\sum_{d \in D(r)} \mu(d) \right) \times \left(\sum_{d' \in D(s)} \mu(d') \right) = \left(\sum_{d/r} \mu(d) \right) \times \left(\sum_{d'/s} \mu(d') \right)$$

On a r, s dans $[\![2\ ;\ n]\!]$, donc les deux sommes sont nulles par hypothèse, d'où le résultat au rang $n+1$ et la conclusion par récurrence.

c) Nous allons utiliser la relation du b) pour calculer $\mu(n)$:

$$\forall n \geqslant 2, \quad \mu(n) = -\sum_{d/n, d\neq n} \mu(d) \qquad (*)$$

La commande `irem(i,j)`, qui renvoie le reste de la division de l'entier i par j permet de tester si j/i, auquel cas le terme $-\mu(i)$ fait partie du membre de droite de $(*)$.

```
> mu[1]:=1:for i from 2 to 20 do
> mu[i]:=0;
> for j from 1 to i-1 do
> if irem(i,j)=0 then mu[i]:=mu[i]-mu[j]:fi:
> od:
> od:
> seq(mu||`[`||i||`]`=mu[i],i=1..20);
```

$mu[1] = 1,\ mu[2] = -1,\ mu[3] = -1,\ mu[4] = 0,\ mu[5] = -1,\ mu[6] = 1,$
$mu[7] = -1, mu[8] = 0,\ mu[9] = 0,\ mu[10] = 1,\ mu[11] = -1,$
$mu[12] = 0,\ mu[13] = -1, mu[14] = 1,\ mu[15] = 1,\ mu[16] = 0,$
$mu[17] = -1,\ mu[18] = 0,\ mu[19] = -1, mu[20] = 0$

d) La seconde égalité provient du fait que l'application $d \mapsto \dfrac{n}{d}$ est une bijection de l'ensemble des diviseurs de n dans lui-même. On calcule ensuite pour tout $n \in \mathbb{N}^*$:

$$\sum_{d/n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d/n} \mu(d) \sum_{k/\frac{n}{d}} f(k)$$

L'équivalence : $\left\{ \begin{array}{l} d/n \\ k/\dfrac{n}{d} \end{array} \right. \iff \left\{ \begin{array}{l} k/n \\ d/\dfrac{n}{k} \end{array} \right.$ permet de permuter les sommations :

$$\sum_{d/n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{k/n} f(k) \sum_{d/\frac{n}{k}} \mu(d).$$

➢ **Cas 1 :** $k = n$. Alors $f(k) \displaystyle\sum_{d/\frac{n}{k}} \mu(d) = f(n)\mu(1) = f(n)$.

➢ **Cas 2 :** k/n et $k \neq n$. Alors $\dfrac{n}{k} \geqslant 2$ donc par b) : $f(k) \displaystyle\sum_{d/\frac{n}{k}} \mu(d) = 0$.

Il reste donc $\displaystyle\sum_{d/n} \mu(d) g\left(\frac{n}{d}\right) = f(n)$.

► X 11 *Elément idempotent dans un magma associatif fini.*

Soit E un ensemble fini, non vide, muni d'une loi de composition interne associative ; montrer qu'il existe dans E un élément x tel que $x^2 = x$.

▷ **Réponse**

• Puisque E est non vide, considérons a élément de E et l'application

$$\varphi : \left| \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & E \\ n & \longmapsto & a^n \end{array} \right. .$$