Fonctions arithmétiques multiplicatives

Notations

– Dans ce problème, le mot « entier » (sans précision supplémentaire) désigne les éléments de $\mathbb{N}^*$.
On note respectivement $m \wedge n$ et $m \vee n$ le pgcd et le ppcm de deux entiers m et n.

– On appelle *fonction arithmétique* toute application f de $\mathbb{N}^*$ dans $\mathbb{C}$.
On dit que f est *multiplicative* si $f(1) = 1$ et si $m \wedge n = 1 \Rightarrow f(mn) = f(m)f(n)$.
L'objet de ce problème est d'étudier quelques fonctions arithmétiques multiplicatives classiques.

– On note $\mathbb{P}$ l'ensemble des entiers premiers.
Pour tout entier n, on désigne par $\mathcal{D}_n$ l'ensemble des entiers qui divisent n.
On note alors $\mathbb{P}_n$ l'ensemble des diviseurs premiers de n. Ainsi $\mathbb{P}_n = \mathbb{P} \cap \mathcal{D}_n$.

– Pour tout p de $\mathbb{P}$ et tout entier n, on note $v_p(n) = \max\{k \in \mathbb{N},\ p^k \mid n\}$.
On dit que $v_p(n)$ est la *valuation* de n pour l'entier premier p. Il est clair que $p \in \mathbb{P}_n \Leftrightarrow v_p(n) \geqslant 1$.
L'entier $v_p(n)$ représente l'exposant de p dans la décomposition de n en facteurs premiers.
Exemple : si $n = 56 = 2^3 7$ alors $v_2(n) = 3, v_7(n) = 1$ et $\forall\, p \in \mathbb{P} \setminus \{2, 7\},\ v_p(n) = 0$.

I. Généralités

On se propose d'établir ici quelques résultats arithmétiques portant ou non sur les fonctions arithmétiques, et qui s'avèreront utiles dans la suite du problème.

1. On se donne deux entiers m et n quelconques.
   (a) Justifier rapidement les égalités $\mathcal{D}_m \cap \mathcal{D}_n = \mathcal{D}_{m\wedge n}$ et $\mathbb{P}_m \cap \mathbb{P}_n = \mathbb{P}_{m\wedge n}$. [S]
   (b) Prouver l'égalité $\mathbb{P}_m \cup \mathbb{P}_n = \mathbb{P}_{m\vee n}$. [S]
   (c) Que dire de $\mathbb{P}_m$ et $\mathbb{P}_n$ si m, n sont premiers entre eux ? [S]
2. Soient a, b, c trois entiers tels que $a \wedge b = 1$. On veut prouver que $\begin{cases} a \wedge (bc) = a \wedge c \\ (ab) \wedge c = (a \wedge c)(b \wedge c) \end{cases}$
   Pour cela, on demande deux méthodes distinctes :
   (a) Poser $d = a \wedge c$, et considérer les entiers a', b' tels que $a = da'$ et $c = dc'$. [S]
   (b) Utiliser les valuations $v_p(a), v_p(b), v_p(c)$ pour tout p de $\mathbb{P}$. [S]
3. On se donne deux entiers m et n premiers entre eux.
   On considère l'application ψ définie de $\mathcal{D}_m \times \mathcal{D}_n$ dans $\mathcal{D}_{mn}$ par $\psi(d, \delta) = d\,\delta$.
   De même, soit ξ l'application de $\mathcal{D}_{mn}$ dans $\mathcal{D}_m \times \mathcal{D}_n$ définie par $\xi(q) = (m \wedge q, n \wedge q)$.
   Montrer que ψ et ξ sont deux bijections réciproques l'une de l'autre. [S]
4. Dans cette question, on se donne une fonction multiplicative f.
   (a) Si $m_1, \ldots, m_q$ sont premiers entre eux deux à deux montrer que $f\Big(\prod_{j=1}^{q} m_j\Big) = \prod_{j=1}^{q} f(m_j)$. [S]
   (b) Montrer que f est caractérisée par les $f(p^k)$, où $(p, k) \in \mathbb{P}\times\mathbb{N}^*$. [S]

II. Exemples de fonctions multiplicatives

Dans cette partie, on découvre quelques fonctions multiplicatives simples et classiques.

1. Pour tout $n \geqslant 1$, on note $\omega(n) = \operatorname{card} \mathbb{P}_n$: c'est le nombre de diviseurs premiers de n.
   (a) Montrer que pour tout z de $\mathbb{C}^*$, l'application $f : n \mapsto z^{\omega(n)}$ est multiplicative. [S]
   (b) Que valent les $f(p^k)$, pour tous p dans $\mathbb{P}$ et k dans $\mathbb{N}^*$? [S]
2. Pour tout $n \geqslant 1$, on note $\tau(n) = \operatorname{card} \mathcal{D}_n$: c'est le nombre d'entiers qui divisent n.
   (a) Montrer que l'application τ est multiplicative (utiliser I.3.) [S]
   (b) Que valent les $\tau(p^k)$, pour tous p dans $\mathbb{P}$ et k dans $\mathbb{N}^*$? [S]
   (c) En déduire que pour tout $n \geqslant 2$, on a $\tau(n) = \prod\limits_{p \in \mathbb{P}_n} (v_p(n) + 1)$. [S]
3. On définit la *fonction de Moëbius* $n \mapsto \mu(n)$ de la façon suivante :
   S'il existe p dans $\mathbb{P}$ tel que $v_p(n) \geqslant 2$, alors $\mu(n) = 0$. Sinon $\mu(n) = (-1)^{\omega(n)}$.
   Ainsi $\mu(n) = 0$ si n est divisible par le carré d'un entier premier, et sinon $\mu(n) = 1$ ou $\mu(n) = -1$ selon que les facteurs premiers de n (qui sont alors distincts) sont en nombre pair ou impair.
   (a) Montrer que l'application μ est multiplicative. [S]
   (b) Que valent les $\mu(p^k)$, pour tous p dans $\mathbb{P}$ et k dans $\mathbb{N}^*$? [S]

III. Produit de Dirichlet des fonctions arithmétiques

- On note $\mathcal{A}$ l'ensemble des fonctions arithmétiques, et $\mathcal{M}$ celui des fonctions multiplicatives.
- On note Id la fonction identité de $\mathbb{N}^*$, et $\mathbf{1}$ la fonction constante égale à 1 sur $\mathbb{N}^*$.
  On note $\mathbf{e}$ la fonction définie sur $\mathbb{N}^*$ par $\mathbf{e}(1) = 1$, et $\mathbf{e}(n) = 0$ si $n \geqslant 2$.
  Il est clair que les applications $\mathrm{Id}, \mathbf{1}, \mathbf{e}$ sont des éléments de $\mathcal{M}$.
- Pour toute fonction f de $\mathcal{A}$, on note $\sum\limits_{d|n} f(d)$ la somme des valeurs de f sur les éléments d de $\mathcal{D}_n$.
- Soient f et g deux éléments de $\mathcal{A}$. Pour tout entier n, on pose $(f \star g)(n) = \sum\limits_{d|n} f(d)\, g(\frac{n}{d})$.
  On définit ainsi une loi de composition sur $\mathcal{A}$, appelée *produit de Dirichlet*.
  Remarque : une écriture équivalente du produit de Dirichlet est $(f \star g)(n) = \sum\limits_{ab=n} f(a)g(b)$, où la somme est étendue aux couples d'entiers (a, b) tels que $ab = n$.

1. Dans cette question, on montre que $(\mathcal{A}, +, \star)$ est un anneau commutatif.
   (a) Montrer que $\mathcal{A}$ est un groupe commutatif pour l'addition des fonctions. [S]
   (b) Montrer que le produit de Dirichlet est commutatif. [S]
   (c) Vérifier que l'application $\mathbf{e}$ est élément neutre. [S]
   (d) Montrer que le produit de Dirichlet est associatif et conclure. [S]
2. Dans cette question, on en apprend un peu plus sur l'anneau $\mathcal{A}$.
   (a) Montrer qu'un élément f de $\mathcal{A}$ est inversible pour $\star$ si et seulement si $f(1) \neq 0$. [S]
   (b) Montrer que l'anneau $(\mathcal{A}, +, \star)$ est intègre. [S]
3. On va montrer que les fonctions multiplicatives forment un groupe pour la loi $\star$.
   (a) En utilisant (I.3), montrer que $\mathcal{M}$ est stable pour la loi $\star$. Le produit de Dirichlet de deux fonctions multiplicatives est donc encore une fonction multiplicative. [S]
   (b) Montrer que $\mathcal{M}$ est un sous-groupe du groupe des éléments inversibles de l'anneau $\mathcal{A}$. [S]

IV. La formule d'inversion de Moebius

On utilise ici les notations et les résultats de la partie III.

1. Soient f, g, h trois fonctions arithmétiques multiplicatives.
   Montrer que $h = f \star g$ équivaut à : $\forall\, p \in \mathbb{P},\ \forall\, k \in \mathbb{N}^*,\ h(p^k) = \sum_{j=0}^{k} f(p^j)g(p^{k-j})$. [S]
2. Montrer que les fonctions μ et $\mathbf{1}$ sont inverses l'une de l'autre dans le groupe $(\mathcal{M}, \star)$. [S]
3. Soit f une fonction arithmétique, et F définie sur $\mathbb{N}^*$ par $F(n) = \sum_{d|n} f(d)$.
   Montrer que pour tout n de $\mathbb{N}^*$, on a $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$.
   Cette égalité est connue sous le nom de *formule d'inversion de Moebius*. [S]
4. En déduire par exemple la valeur de la somme $\sum_{d|n} \mu(d)\, \tau(\frac{n}{d})$. [S]

V. La fonction « somme des diviseurs »

Pour tout $n \geqslant 1$, on note $\sigma(n)$ la somme des éléments de $\mathcal{D}_n$ (c'est-à-dire des diviseurs de n.)

1. (a) Montrer que σ est multiplicative en utilisant une question de la partie I. [S]
   (b) Montrer que σ est multiplicative en utilisant une question de la partie IV. [S]
   (c) Montrer que pour tout entier $n \geqslant 1$, on a $\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$. [S]
2. (a) Que valent les $\sigma(p^k)$, pour (p, k) dans $\mathbb{P} \times \mathbb{N}^*$? [S]
   (b) En déduire que pour tout $n \geqslant 2$, on a l'égalité $\sigma(n) = \prod_{p \in \mathbb{P}_n} \frac{p^{v_p(n)+1} - 1}{p - 1}$. [S]
   (c) A titre d'exemple, calculer $\sigma(10!)$. [S]
3. Pour tout m de $\mathbb{Z}$, on note $\sigma_m(n)$ la somme des puissances m-ièmes des diviseurs de n.
   (a) Comme dans (2b), exprimer $\sigma_m(n)$ en fonction de la factorisation de n. [S]
   (b) Calculer par exemple la somme des carrés des diviseurs de 2002. [S]
4. On dit qu'un entier n est *parfait* si $\sigma(n) = 2n$.
   Cela équivaut à dire qu'il est égal à la somme de ses diviseurs stricts.
   Exemple : $n = 28$ est parfait ; ses diviseurs sont $1, 2, 4, 7, 14, 28$ et $1+2+4+7+14+28 = 2n$.
   (a) Montrer que si $2^k - 1$ est premier, alors $n = 2^{k-1}(2^k - 1)$ est parfait et pair. [S]
   (b) Réciproquement, on suppose que n est un entier parfait pair.
   Montrer qu'il existe un entier k tel que $n = 2^{k-1}(2^k - 1)$, avec $2^k - 1$ premier.
   Indication : introduire $m \geqslant 1$ et q impair tel que $n = 2^m\, q$.
   Montrer que $q = (2^{m+1} - 1)\, r$ avec $r \geqslant 1$. Montrer que $\sigma(q) = q + r$. [S]
   NB : Le problème de l'existence d'entiers parfaits impairs est un problème ouvert.

VI. L'indicateur d'Euler

Pour tout entier n, on note $\mathcal{E}_n$ l'ensemble des entiers k de $\{1, \ldots, n\}$ tels que $k \wedge n = 1$.

On note alors $\varphi(n) = \operatorname{card} \mathcal{E}_n$. La fonction arithmétique φ est appelée *indicateur d'Euler*.

1. (a) On se donne un entier n, et on considère $f : \{1, \ldots, n\} \to \mathcal{D}_n$ définie par $f(k) = n \wedge k$.
   Montrer que chaque d de $\mathcal{D}_n$ possède exactement $\varphi(\frac{n}{d})$ antécédents par f. [S]
   (b) En déduire que pour tout n de $\mathbb{N}^*$, on a l'égalité $\sum_{d|n} \varphi(d) = n$. [S]
   (c) Montrer que $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$ pour tout $n \geqslant 1$, et que φ est multiplicative. [S]
2. (a) Préciser $\varphi(p^k)$ pour $(p, k) \in (\mathbb{P} \times \mathbb{N}^*)$. On donnera deux démonstrations distinctes. [S]
   (b) En déduire que pour tout $n \geqslant 1$, on a $\varphi(n) = n \prod_{k \in \mathbb{P}_n} \left(1 - \frac{1}{p}\right)$. Calculer par exemple $\varphi(10!)$. [S]

VII. Quelques formules asymptotiques

1. (a) Pour tout entier n, montrer qu'on a l'égalité $\sum_{k=1}^{n} \tau(k) = \sum_{d=1}^{n} \left[\frac{n}{d}\right]$.
   Indication : on écrira $\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \sum_{d|k} 1$ et on cherchera à intervertir les deux sommes. [S]
   (b) Avec $S_n = \sum_{d=1}^{n} \frac{1}{d}$, montrer que $\lim_{n\to\infty} S_n / \ln n = 1$. [S]
   (c) Déduire de ce qui précède qu'on a : $\lim_{n\to\infty} \frac{\tau(1) + \tau(2) + \cdots + \tau(n)}{n \ln n} = 1$
   Ainsi, quand $n \to \infty$, la somme $\tau(1) + \tau(2) + \cdots + \tau(n)$ est équivalente à $n \ln n$. [S]
2. (a) Pour tout entier n, montrer que $\sum_{k=1}^{n} \sigma(k) = \sum_{d=1}^{n} d \left[\frac{n}{d}\right]$ (même indication qu'en (1a).) [S]
   (b) Justifier les transformations suivantes :
   $$\sum_{k=1}^{n} \sigma(k) = \sum_{d=1}^{n} d \Big(\sum_{k=1}^{n/d} 1\Big) = \sum_{d=1}^{n} \Big(\sum_{k=1}^{n/d} d\Big) = \sum_{1 \leqslant dk \leqslant n} d = \sum_{k=1}^{n} \Big(\sum_{d=1}^{n/k} d\Big) = \frac{1}{2} \sum_{k=1}^{n} \left[\frac{n}{k}\right] \left(\left[\frac{n}{k}\right] + 1\right)$$ [S]
   (c) Pour tout entier n, on pose (comme dans (1b)) $S_n = \sum_{k=1}^{n} \frac{1}{k}$ et $T_n = \sum_{k=1}^{n} \frac{1}{k^2}$.
   Montrer que : $\frac{1}{2}\Big(n^2 T_n - n S_n\Big) \leqslant \sum_{k=1}^{n} \sigma(k) \leqslant \frac{1}{2}\Big(n^2 T_n + n S_n\Big)$. [S]
   (d) On admet que $\lim_{n\to\infty} T_n = \frac{\pi^2}{6}$. En déduire $\lim_{n\to\infty} \frac{\sigma(1) + \sigma(2) + \ldots + \sigma(n)}{n^2} = \frac{\pi^2}{12}$. [S]
3. On pose $U_n = \sum_{k=1}^{n} \frac{\mu(k)}{k^2}$ pour tout entier n. On admet que $\lim_{n\to\infty} U_n = \frac{6}{\pi^2}$.
   (a) Pour tout $n \geqslant 1$, montrer que $\sum_{k=1}^{n} \varphi(k) = \sum_{d=1}^{n} \mu(d) \Big(\sum_{d|k} \frac{k}{d}\Big) = \frac{1}{2} \sum_{d=1}^{n} \mu(d) \left[\frac{n}{d}\right] \left(\left[\frac{n}{d}\right] + 1\right)$. [S]
   (b) Montrer : $\left| \frac{n^2}{2} U_n - \sum_{k=1}^{n} \varphi(k) \right| \leqslant \frac{3n S_n}{2}$. En déduire $\lim_{n\to\infty} \frac{\varphi(1) + \varphi(2) + \ldots + \varphi(n)}{n^2} = \frac{3}{\pi^2}$. [S]
   (c) On se donne deux entiers a et b au hasard dans $\{1, \ldots, n\}$.
   Quelle est la probabilité p_n que $a \wedge b = 1$? Quelle est la limite de p_n quand $n \to \infty$?
   On peut interpréter ce résultat de la manière suivante :
   La probabilité que deux entiers a, b choisis au hasard soient premiers entre eux est $\frac{6}{\pi^2}$. [S]

Corrigé du problème

I. Généralités

1. (a) L'égalité $\mathcal{D}_m \cap \mathcal{D}_n = \mathcal{D}_{m\wedge n}$ ne fait qu'exprimer une des caractérisations de $m \wedge n$: les diviseurs positifs communs à m et n sont les diviseurs positifs de leur pgcd.

   Par intersection avec $\mathbb{P}$, l'égalité $\mathcal{D}_m \cap \mathcal{D}_n = \mathcal{D}_{m\wedge n}$ donne alors $\mathbb{P}_m \cap \mathbb{P}_n = \mathbb{P}_{m\wedge n}$. [Q]

   (b) Puisque m et n divisent $m \vee n$, on a $\mathbb{P}_m \subset \mathbb{P}_{m\vee n}$ et $\mathbb{P}_n \subset \mathbb{P}_{m\vee n}$ donc $\mathbb{P}_m \cup \mathbb{P}_n \subset \mathbb{P}_{m\vee n}$.

   Réciproquement, on sait que $(m \wedge n)(m \vee n) = mn$.

   Si p est premier et divise $m \vee n$, alors il divise mn, donc il divise m ou n (quand un entier premier divise un produit de facteurs, il divise l'un au moins de ces facteurs.)

   Autrement dit $\mathbb{P}_{m\vee n} \subset \mathbb{P}_m \cup \mathbb{P}_n$, ce qui assure l'égalité $\mathbb{P}_m \cup \mathbb{P}_n = \mathbb{P}_{m\vee n}$. [Q]

   (c) Si $m \wedge n = 1$, on a $\mathbb{P}_m \cap \mathbb{P}_n = \mathbb{P}_{m\wedge n} = \mathbb{P}_1 = \emptyset$ et $\mathbb{P}_m \cup \mathbb{P}_n = \mathbb{P}_{m\vee n} = \mathbb{P}_{mn}$.

   En d'autres termes, $\mathbb{P}_{mn}$ est l'union disjointe des ensembles $\mathbb{P}_m$ et $\mathbb{P}_n$. [Q]

2. (a) Posons $d = a \wedge c$. Il existe deux entiers a', c' tels que $a = da'$ et $c = dc'$ avec $a' \wedge c' = 1$.

   On peut alors écrire $a \wedge (bc) = (da') \wedge (dbc') = d(a' \wedge bc')$.

   Mais a' est premier avec c' et avec b (car $a' \mid a$ et $a \wedge b = 1$.)

   Il en résulte que $a' \wedge (bc') = 1$. Ainsi $a \wedge (bc) = d = a \wedge c$.

   Avec les mêmes notations, on écrit $(ab) \wedge c = (da'b) \wedge (dc') = d((a'b) \wedge c')$.

   En utilisant le début de cette question, l'égalité $a' \wedge c' = 1$ implique $(a'b) \wedge c' = b \wedge c'$.

   D'autre part $b \wedge c = b \wedge (dc') = b \wedge c'$ (en effet $b \wedge a = 1$ et $d \mid a$ donc $b \wedge d = 1$.)

   Finalement, on trouve l'égalité : $(ab) \wedge c = d(b \wedge c') = d(b \wedge c) = (a \wedge c)(b \wedge c)$. [Q]

   (b) L'hypothèse $a \wedge b = 1$ signifie qu'il n'y a pas d'entier premier divisant simultanément a et b, ou encore que pour tout p de $\mathbb{P}$ on a $v_p(a) = 0$ ou $v_p(b) = 0$.

   Pour montrer l'égalité de deux entiers m, n il suffit d'établir $v_p(m) = v_p(n)$ pour tout p de $\mathbb{P}$ (car m et n ont alors la même factorisation.)

   Enfin pour tous entiers m, n et tout p de $\mathbb{P}$, on a $\begin{cases} v_p(mn) = v_p(m) + v_p(n) \\ v_p(m \wedge n) = \min(v_p(m), v_p(n)) \end{cases}$

   Ainsi $a \wedge (bc) = a \wedge c \Leftrightarrow \min(v_p(a), v_p(b) + v_p(c)) = \min(v_p(a), v_p(c))$, pour tout p de $\mathbb{P}$.

   Or ce résultat est évident dans chacun des deux seuls cas possibles $v_p(a) = 0$ ou $v_p(b) = 0$.

   De même on a $\begin{cases} v_p((ab) \wedge c) = \min(v_p(a) + v_p(b), v_p(c)) \\ v_p((a \wedge c)(b \wedge c)) = \min(v_p(a), v_p(c)) + \min(v_p(b), v_p(c)) \end{cases}$

   Là encore, l'égalité de ces deux valuations est évidente si $v_a(p) = 0$ ou si $v_p(b) = 0$. [Q]

3. Bien sûr, si $d \mid m$ et $\delta \mid n$, alors $d\delta \mid mn$. Donc ψ est bien à valeurs dans $\mathcal{D}_{mn}$.

   De même, pour tout entier q, le couple $(m \wedge q, n \wedge q)$ est élément de $\mathcal{D}_m \times \mathcal{D}_n$.

   Ceci nous assure que ξ est bien à valeurs dans $\mathcal{D}_m \times \mathcal{D}_n$ (on n'a pas encore utilisé $m \wedge n = 1$.)

   On suppose donc que m et n sont premiers entre eux.

   – Soit (d, δ) dans $\mathcal{D}_m \times \mathcal{D}_n$. On note a, b les entiers tels que $m = da$ et $n = \delta b$.

     On a alors $\xi \circ \psi\,(d, \delta) = \xi(d\delta) = ((d\delta) \wedge m, (d\delta) \wedge n) = ((d\delta) \wedge (da), (d\delta) \wedge (\delta b))$.

     Mais $(d\delta) \wedge (da) = d\,(\delta \wedge a) = d$. En effet $\delta \wedge a = 1$ car il divise δ et a, donc n et m.

     De même : $(d\delta) \wedge (\delta b) = \delta(d \wedge b) = \delta$ car $d \wedge b = 1$ (il divise d et b donc m et n.)

     On a ainsi obtenu $\xi \circ \psi\,(d, \delta) = (d, \delta)$, pour tout élément (d, δ) de $\mathcal{D}_m \times \mathcal{D}_n$.

– Réciproquement, soit q un diviseur de l'entier mn.

On a $\psi\circ\xi(q)=\psi(q\wedge m,q\wedge n)=(q\wedge m)(q\wedge n)=q\wedge(mn)$, car $m\wedge n=1$ (cf I.3)

Mais q étant un diviseur de mn, on obtient $\psi\circ\xi(q)=q$.

Ainsi $\psi\circ\xi$ est l'application identité de $\mathcal{D}_{mn}$.

Ainsi $\begin{cases}\psi:\mathcal{D}_m\times\mathcal{D}_n\to\mathcal{D}_{mn}\\ \xi:\mathcal{D}_{mn}\to\mathcal{D}_m\times\mathcal{D}_n\end{cases}$ sont deux bijections réciproques l'une de l'autre. [Q]

4. (a) La propriété est évidente si $q=1$, et vraie si $q=2$ car f est multiplicative.

   On se donne alors $q\geqslant 3$ et on suppose que la propriété est vraie au rang $q-1$.

   Soit $m_1,m_2,\ldots,m_q$ une famille de q entiers premiers entre eux deux à deux.

   Puisque m_1 est premier avec $m_2,m_3,\ldots,m_q$, il est premier avec leur produit.

   On en déduit, puisque f est multiplicative, et en utilisant l'hypothèse de récurrence :

$$f\Big(\prod_{j=1}^{q}m_j\Big)=f(m_1)\,f\Big(\prod_{j=2}^{q}m_j\Big)=f(m_1)\prod_{j=2}^{q}f(m_j)=\prod_{j=1}^{q}f(m_j)$$

   Cela démontre la propriété au rang q et achève la récurrence. [Q]

   (b) Soit $n\geqslant 2$ un entier décomposé en produit de facteurs premiers : $n=\prod_{p\in\mathbb{P}_n}p^{v_p(n)}$.
   Les entiers $m_p=p^{v_p(n)}$ sont premiers entre eux deux à deux.
   On en déduit l'égalité $f(n)=f\Big(\prod_{p\in\mathbb{P}_n}m_p\Big)=\prod_{p\in\mathbb{P}_n}f(m_p)=\prod_{p\in\mathbb{P}_n}f(p^{v_p(n)})$.

   On voit que la connaissance des $f(p^k)$, avec p dans $\mathbb{P}$ et k dans $\mathbb{N}^*$ détermine entièrement les $f(n)$ pour $n\geqslant 2$, donc détermine entièrement f puisqu'on sait que $f(1)=1$. [Q]

II. Exemples de fonctions multiplicatives

1. (a) On suppose que les deux entiers m et n sont premiers entre eux.

   D'après I.1.c, on a $\operatorname{card}P_{mn}=\operatorname{card}P_m+\operatorname{card}P_n$ c'est-à-dire $\omega(mn)=\omega(m)+\omega(n)$.

   Pour tout z de $\mathbb{C}^*$, il en résulte $z^{\omega(mn)}=z^{\omega(m)}\,z^{\omega(n)}$. Enfin $\mathbb{P}_1=\emptyset\Rightarrow\omega(1)=0\Rightarrow z^{\omega(1)}=1$.

   On en déduit que la fonction $n\mapsto z^{\omega(n)}$ est multiplicative, pour tout z de $\mathbb{C}^*$. [Q]

   (b) On se donne p dans $\mathbb{P}$ et k dans $\mathbb{N}^*$.

   Le seul diviseur premier de p^k est p. Ainsi $\omega(p^k)=1$ et $f(p^k)=z$. [Q]

2. (a) On se donne deux entiers m et n premiers entre eux.

   D'après I.3, les ensembles finis $\mathcal{D}_{mn}$ et $\mathcal{D}_m\times\mathcal{D}_n$ sont en bijection, donc ont même cardinal.

   Ainsi $\tau(mn)=\operatorname{card}\mathcal{D}_{mn}=\operatorname{card}(\mathcal{D}_m\times\mathcal{D}_n)=(\operatorname{card}\mathcal{D}_m)(\operatorname{card}\mathcal{D}_n)=\tau(m)\tau(n)$.

   Enfin $\mathcal{D}_1=\{1\}$ donc $\tau(1)=\operatorname{card}\mathcal{D}_1=1$: l'application τ est multiplicative. [Q]

   (b) On se donne p dans $\mathbb{P}$ et k dans $\mathbb{N}^*$.

   Les diviseurs de p^k sont les p^j, avec $0\leqslant j\leqslant k$. On en déduit $\tau(p^k)=k+1$. [Q]

   (c) D'après I.4.b, et pour tout $n\geqslant 2$, on a $\tau(n)=\prod_{p\in\mathbb{P}_n}\tau(p^{v_p(n)})=\prod_{p\in\mathbb{P}_n}(v_p(n)+1)$. [Q]

3. (a) On a tout d'abord $\mathbb{P}_1 = \emptyset$ puis $\omega(1) = 0$ donc $\mu(1) = 1$.

   On se donne deux entiers m, n premiers entre eux. Si l'un d'eux est divisible par le carré d'un entier premier p, il en est de même de mn, donc $\mu(mn) = \mu(m)\mu(n) = 0$.

   On peut donc supposer que ni m ni n ne sont divisibles par le carré d'un entier premier.

   Puisque $m \wedge n = 1$, on sait que $\mathbb{P}_{mn}$ est l'union disjointe de $\mathbb{P}_m$ et de $\mathbb{P}_n$.

   Ainsi $\omega(mn) = \omega(m) + \omega(n)$ puis $\mu(mn) = (-1)^{\omega(mn)} = (-1)^{\omega(m)}(-1)^{\omega(n)} = \mu(m)\mu(n)$.

   On a donc prouvé que la fonction de Moëbius μ est multiplicative. [Q]

   (b) Par définition, pour tout p de $\mathbb{P}$, on a $\mu(p) = -1$, et $\mu(p^k) = 0$ si $k \geqslant 2$. [Q]

III. Produit de Dirichlet des fonctions arithmétiques

1. (a) $\mathcal{A}$ est l'ensemble des applications de $\mathbb{N}^*$ dans $\mathbb{C}$.

   C'est donc un groupe pour l'addition des fonctions (résultat du cours.)

   La loi + est définie par : $\forall\,(f,g) \in \mathcal{A}^2,\ \forall\, n \in \mathbb{N}^*,\ (f+g)(n) = f(n) + g(n)$.

   Le neutre additif est la fonction nulle ; l'opposé de la fonction f est la fonction $-f$. [Q]

   (b) La commutativité de $\star$ résulte immédiatement de l'écriture $(f \star g)(n) = \sum\limits_{ab=n} f(a)g(b)$.
   Cette écriture est en effet symétrique par rapport à f et g. [Q]

   (c) Pour f dans $\mathcal{A}$ et $n \geqslant 1$: $(f \star \mathbf{e})(n) = \sum\limits_{d|n} f(\frac{n}{d})\,\mathbf{e}\,(d) = f(n)\,\mathbf{e}\,(1) = f(n)$.

   Ainsi $f \star \mathbf{e} = f$: l'application $\mathbf{e}$ est neutre pour le produit de Dirichlet. [Q]

   (d) Soient f, g, h trois éléments de $\mathcal{A}$, et soit n un entier quelconque.

   On a $(f \star (g \star h))(n) = \sum\limits_{ab=n} f(a)(g \star h)(b) = \sum\limits_{ab=n} f(a) \Big(\sum\limits_{cd=b} g(c)h(d) \Big)$.

   Cette somme peut être développée et elle devient $(f \star (g \star h))(n) = \sum\limits_{acd=n} f(a)g(c)h(d)$.
   Cette somme est étendue aux triplets (a, c, d) tels que $acd = n$.

   On aboutit bien sûr au même développement quand on part de $((f \star g) \star h)(n)$.

   Il en découle que la loi $\star$ est associative sur $\mathcal{A}$.

   La seule chose qui reste à prouver pour établir que $(\mathcal{A}, +, \star)$ est un anneau commutatif est la distributivité de la loi $\star$ sur la loi +.

   Pour tous éléments f, g, h de $\mathcal{A}$ et pour tout entier n, on a effectivement :

$$\begin{aligned}(f \star (g+h))(n) &= \sum_{ab=n} f(a)(g+h)(b) = \sum_{ab=n} f(a)(g(b) + h(b)) \\ &= \sum_{ab=n} f(a)g(b) + \sum_{ab=n} f(a)h(b) = (f \star g)(n) + (f \star h)(n) = (f \star g + f \star h)(n)\end{aligned}$$

   Conclusion : muni des lois + et $\star$, l'ensemble $\mathcal{A}$ est un anneau commutatif. [Q]

2. (a) Soit f un élément de $\mathcal{A}$ tel que $f(1) = 0$.

   Alors pour tout g de $\mathcal{A}$, on a $(f \star g)(1) = f(1)g(1) = 0 \neq \mathbf{e}\,(1)$ donc $f \star g \neq \mathbf{e}$.

   On constate donc que les f de $\mathcal{A}$ tels que $f(1) = 0$ ne sont pas inversibles pour la loi $\star$.

   On se donne maintenant f dans $\mathcal{A}$ tel que $f(1) \neq 0$.

   On va montrer qu'il existe g dans $\mathcal{A}$ tel que $g \star f = \mathbf{e}$.

   L'égalité $g \star f = \mathbf{e}$ équivaut à $1 = (g \star f)(1) = g(1)f(1)$ et $(g \star f)(n) = 0$ pour tout $n \geqslant 2$.

   La condition $g(1)f(1) = 1$ détermine $g(1)$ de façon unique car $f(1) \neq 0$.

On se donne $n \geqslant 2$ et on suppose que $g(k)$ est connu pour tout k de $\{1, \ldots, n-1\}$.

L'égalité $0 = (g \star f)(n)$ s'écrit $0 = g(n)f(1) + \sum_{d|n,\, d<n} g(d)f(\frac{n}{d})$.

On en déduit $g(n) = -\frac{1}{f(1)} \sum_{d|n,\, d<n} g(d)f(\frac{n}{d})$, donnant $g(n)$ en fonction de quantités connues.

On a ainsi montré par récurrence que $g(n)$ est défini de manière unique pour tout entier n.

Cela prouve que l'application f est inversible pour $\star$ et que son inverse est g. [Q]

(b) Soient f et g deux éléments non nuls de $\mathcal{A}$. Il faut montrer que $f \star g$ est non nul.

Soit $m = \min\{k \in \mathbb{N}^*,\, f(k) \neq 0\}$ et $n = \min\{k \in \mathbb{N}^*,\, g(k) \neq 0\}$.

On peut alors écrire : $(f \star g)(mn) = \sum_{ab=mn} f(a)g(b) = f(m)g(n) + \sum_{ab=mn}^{(a,b)\neq(m,n)} f(a)g(b)$.

Or $\begin{cases} ab = mn \\ (a,b) \neq (m,n) \end{cases}$ implique $\begin{cases} a < m \text{ ou} \\ b < n \end{cases}$ puis $\begin{cases} f(a) = 0 \text{ ou} \\ g(b) = 0 \end{cases}$, donc $f(a)g(b) = 0$.

Il en résulte que $(f \star g)(mn) = f(m)g(n) \neq 0$ donc $f \star g \neq 0$.

Conclusion : l'anneau $(\mathcal{A}, +, \star)$ est intègre. [Q]

3. (a) On se donne deux éléments f, g de $\mathcal{M}$. Tout d'abord $(f \star g)(1) = f(1)g(1) = 1$.

Donnons-nous ensuite deux entiers m, n tels que $m \wedge n = 1$.

D'après I.3, tout d de $\mathcal{D}_{mn}$ s'écrit de manière unique $d = ab$ avec (a, b) dans $\mathcal{D}_m \times \mathcal{D}_n$.

Puisque $m \wedge n = 1$, on trouve $a \wedge b = 1$ et $\frac{m}{a} \wedge \frac{n}{b} = 1$. On peut donc écrire :

$$\begin{aligned}(f\star g)\,(mn) &= \sum_{d|mn} f(d)\,g(\frac{mn}{d}) = \sum_{a|m}\sum_{b|n} f(ab)\,g(\frac{m}{a}\,\frac{n}{b}) \\ &= \sum_{a|m}\sum_{b|n} f(a)f(b)\,g(\frac{m}{a})\,g(\frac{n}{b}) = \sum_{a|m} f(a)\,g(\frac{m}{a}) \sum_{b|n} f(b)\,g(\frac{n}{b}) = h(m)h(n)\end{aligned}$$

On a donc prouvé que l'application $f\star g$ est multiplicative.

Ainsi l'ensemble $\mathcal{M}$ est une partie stable de $\mathcal{A}$. [Q]

(b) On sait déjà que $\mathcal{M}$ est une partie (non vide) stable de $\mathcal{A}$.

D'autre part les éléments f de $\mathcal{M}$ sont inversibles car $f(1) = 1 \neq 0$.

Il reste à prouver que si f est dans $\mathcal{M}$, alors son inverse g est dans $\mathcal{M}$.

On a déja $1 = \mathbf{e}(1) = (f \star g)(1) = f(1)g(1) = g(1)$.

On se donne deux entiers m et n premiers entre eux. Montrons $g(mn) = g(m)g(n)$.

On va procéder par récurrence sur la valeur du produit mn.

Notons tout d'abord que la propriété est évidente si $mn = 1$, c'est-à-dire $m = n = 1$.

On suppose $mn > 1$, et on suppose que la propriété a été démontrée pour tous les couples d'entiers (a, b) tels que $a \wedge b = 1$ et $ab < mn$.

Dans la suite des calculs, on va noter $a\|b$ pour dire que a est un diviseur strict de b.

On sait que $g(mn) = -\sum_{d\|mn} g(d)f(\frac{mn}{d})$.

On sait aussi que tout d de $\mathcal{D}_{mn}$ s'écrit de façon unique $d = ab$, où $(a, b) \in \mathcal{D}_a \times \mathcal{D}_b$.

On en déduit $g(mn) = -\sum_{ab\|mn} g(ab)f(\frac{m}{a}\,\frac{n}{b})$.

Dans la somme précédente, on a toujours $a \wedge b = 1$ et $\frac{m}{a} \wedge \frac{n}{d} = 1$.

D'autre part f est arithmétique, et $g(ab) = g(a)g(b)$ par hypothèse de récurrence.

On obtient : $g(mn) = -\sum_{ab\|mn} g(a)g(b)\, f(\frac{m}{a})\, f(\frac{n}{b}) = -\sum_{ab\|mn} g(a)\, f(\frac{m}{a})\, g(b)\, f(\frac{n}{b})$

Dans cette somme, on a tous les couples (a, b) de $\mathcal{D}_m \times \mathcal{D}_m$, sauf le couple (m, n).

On en déduit finalement :

$$\begin{aligned} g(mn) &= -\sum_{ab|mn} g(a)\, f(\frac{m}{a})\, g(b)\, f(\frac{n}{b}) + g(m)f(1)g(n)f(1) \\ &= -\sum_{a|m} g(a)\, f(\frac{m}{a}) \sum_{b|n} g(b)\, f(\frac{n}{b}) + g(m)g(n) \\ &= -(g \star f)(m)(g \star f)(n) + g(m)g(n) = -\,\mathbf{e}\,(m)\,\mathbf{e}\,(n) + g(m)g(n) \end{aligned}$$

Mais $\mathbf{e}\,(m)\,\mathbf{e}\,(n) = 0$ car $m > 1$ ou $n > 1$. On en déduit $g(mn) = g(m)g(n)$.

Cela établit la propriété "au rang mn" et achève la récurrence. On a donc prouvé que l'inverse (pour $\star$) d'une fonction multiplicative est encore une fonction multiplicative.

Conclusion : $\mathcal{M}$ est un sous-groupe du groupe des éléments inversibles de l'anneau $\mathcal{A}$. [Q]

IV. La formule d'inversion de Moebius

1. On se donne f, g, h dans $\mathcal{M}$. On sait que $f \star g$ est dans $\mathcal{M}$.

   On sait d'autre part (cf I.4.b) que deux applications éléments de $\mathcal{M}$ sont égales si et seulement si elles coïncident sur les p^k avec p dans $\mathbb{P}$ et k dans $\mathbb{N}^*$.

   Or si $(p, k) \in (\mathbb{P}, \mathbb{N}^*)$, on a $\mathcal{D}_{p^k} = \{p^j, 0 \leqslant j \leqslant k\}$, donc $(f \star g)(p^k) = \sum_{j=0}^{k} f(p^j)\, g(p^{k-j})$

   Ainsi : $f \star g = h \Leftrightarrow \forall\,(p, k) \in \mathbb{P} \times \mathbb{N}^*,\ h(p^k) = \sum_{j=0}^{k} f(p^j)\, g(p^{k-j})$. [Q]

2. Il s'agit de montrer l'égalité $\mu \star \mathbf{1} = \mathbf{e}$.

   Pour tout (p, k) de $\mathbb{P} \times \mathbb{N}^*$: $(\mu \star \mathbf{1})(p^k) = \sum_{j=0}^{k} \mu(p^j)\, \mathbf{1}(p^{k-j}) = \mu(1) + \mu(p) = 0 = \mathbf{e}\,(p^k)$.

   On sait que ces égalités impliquent $\mu \star \mathbf{1} = \mathbf{e}$. En d'autre termes : $\sum_{d|n} \mu(n) = 0$ si $n \geqslant 2$. [Q]

3. Par définition, on a $F = f \star \mathbf{1}$. Or $\mathbf{1}^{-1} = \mu$ dans l'anneau $\mathcal{A}$.

   Ainsi $f = (f \star \mathbf{1}) \star \mathbf{1}^{-1} = F \star \mu$ puis $\forall\, n \in \mathbb{N}^*,\ f(n) = (F \star \mu)(n) = \sum_{d|n} \mu(n) F(\frac{n}{d})$. [Q]

4. On a $\tau = \sum_{d|n} 1 = \mathbf{1} \star \mathbf{1}$. Ainsi $\mu \star \tau = \mathbf{1}$ donc : $\forall\, n \geqslant 1,\ \sum_{d|n} \mu(d)\tau(\frac{n}{d}) = 1$. [Q]

V. La fonction « somme des diviseurs »

1. (a) Soient m et n deux entiers premiers entre eux.

   On sait que $\Psi : \mathcal{D}_m \times \mathcal{D}_n \to \mathcal{D}_{mn}$ définie par $\Psi(d, \delta) = d\delta$ est bijective.

   Autrement dit $\sigma(mn) = \sum_{a|mn} a = \sum_{d|m,\, \delta|n} d\delta = \sum_{d|m} d \sum_{\delta|n} \delta = \sigma(m)\sigma(n)$.

   L'application σ est donc multiplicative. [Q]

   (b) On a $\sigma(n) = \sum_{d|n} d = \sum_{d|n} \mathrm{Id}(d)$ pour tout $n \geqslant 1$. Or Id est dans $\mathcal{M}$. Donc $\sigma \in \mathcal{M}$. [Q]

   (c) Il suffit d'écrire $\sigma(n) = (\mathrm{Id} \star \mathbf{1})(n) = (\mathbf{1} \star \mathrm{Id})(n) = \sum_{d|n} \frac{n}{d} = n \sum_{d|n} \frac{1}{d}$. [Q]

2. (a) Soit $n = p^k$ avec $(p, k) \in \mathbb{P} \times \mathbb{N}^*$. On a $\mathcal{D}_n = \{1, p, p^2, \ldots, p^k\}$.

   On en déduit $\sigma(p^k) = \sum_{j=0}^{k} p^j = \dfrac{p^{k+1} - 1}{p - 1}$. [Q]

   (b) Pour $n \geqslant 2$, on a $n = \prod_{p \in \mathbb{P}_n} p^{v_p(n)}$ donc $\sigma(n) = \prod_{p \in \mathbb{P}_n} \sigma(p^{v_p(n)}) = \prod_{p \in \mathbb{P}_n} \dfrac{p^{v_p(n)+1} - 1}{p - 1}$. [Q]

   (c) On a $10! = 2^8 3^4 5^2 7$ donc $\sigma(10!) = \dfrac{2^9 - 1}{1} \dfrac{3^5 - 1}{2} \dfrac{5^3 - 1}{4} \dfrac{7^2 - 1}{6} = 15334088$. [Q]

3. (a) La fonction $n \mapsto n^m$ est multiplicative. Il en est donc de même de σ_m.

   Soit $n = p^k$ avec $(p, k) \in \mathbb{P} \times \mathbb{N}^*$. On a $\mathcal{D}_n = \{1, p, p^2, \ldots, p^k\}$.

   On en déduit $\sigma_m(p^k) = \sum_{j=0}^{k} p^{mj} = \dfrac{p^{m(k+1)} - 1}{p^m - 1}$. [Q]

   (b) On a $2002 = 2 \cdot 7 \cdot 11 \cdot 13$ donc $\sigma_2(2002) = \dfrac{2^4 - 1}{2^2 - 1} \dfrac{7^4 - 1}{7^2 - 1} \dfrac{11^4 - 1}{11^2 - 1} \dfrac{13^4 - 1}{13^2 - 1} = 5185000$. [Q]

4. (a) On se donne un entier k tel que $2^k - 1$ soit premier (nécessairement $k \geqslant 2$.)

   Posons $n = 2^{k-1}(2^k - 1)$. Les entiers 2^{k-1} et $2^k - 1$ sont premiers entre eux.

   On en déduit $\sigma(n) = \sigma(2^{k-1})\, \sigma(2^k - 1)$. Or $\sigma(2^{k-1}) = 2^k - 1$ (cf question 2.a)

   Par hypothèse $2^k - 1$ est premier donc $\sigma(2^k - 1) = 2^k$.

   Il en résulte $\sigma(n) = (2^k - 1)2^k = 2n$. Ainsi n est un entier parfait (pair car $k \geqslant 2$.) [Q]

   (b) On se donne un entier parfait pair n. Soit $m = v_2(n)$ (c'est un élément de $\mathbb{N}^*$.)

   Il existe donc un entier m impair tel que $n = 2^m q$.

   Par hypothèse $\sigma(n) = 2n$ donc $2^{m+1}q = 2n = \sigma(2^m)\, \sigma(q) = (2^{m+1} - 1)\, \sigma(q)$.

   Ainsi l'entier $2^{m+1} - 1$, qui est premier avec 2^{m+1}, divise $2^{m+1}q$.

   Il en résulte (théorème de Gauss) que $2^{m+1} - 1$ divise q. Posons $q = (2^{m+1} - 1)r$.

   Si on remplace dans $2^{m+1}q = (2^{m+1} - 1)\, \sigma(q)$, on trouve $2^{m+1}r = \sigma(q)$.

   Mais $2^{m+1}r = q + r$, alors que q et r sont des diviseurs de q.

   Cela signifie que q et r sont les seuls diviseurs de q.

   Autrement dit q est un entier premier et $r = 1$, donc $q = 2^{m+1} - 1$.

   Ainsi $n = 2^m q = 2^m(2^{m+1} - 1)$ ce qui s'écrit $n = 2^{k-1}(2^k - 1)$ avec $2^k - 1$ premier. [Q]

VI. L'indicateur d'Euler

Avec ces notations, on peut par exemple écrire $\varphi(n) = \sum\limits_{k\wedge n=1} 1$.

1. (a) Soit d un diviseur de n (un élément de $\mathcal{D}_n$) et soit k un élément de $\{1,\ldots,n\}$.
   On a $f(k) = d \Leftrightarrow n \wedge k = d \Leftrightarrow \exists\, n', k'$ tels que $n = n'd$, $k = k'd$ et $n' \wedge k' = 1$.
   Il y a autant de solutions k qu'il y a d'entiers k'.
   Or les conditions sur k' sont $1 \leqslant k' \leqslant n'$ (car $1 \leqslant k \leqslant n$) et $k' \wedge n' = 1$.
   Le nombre de solutions est donc égal à $\varphi(n')$, c'est-à-dire $\varphi(\frac{n}{d})$. [Q]

   (b) Les images réciproques par f des éléments de $\mathcal{D}_n$ forment une partition de $\{1,\ldots,n\}$.
   Autrement dit, en utilisant (1a) : $n = \sum\limits_{d|n} \operatorname{card} f^{-1}(\{d\}) = \sum\limits_{d|n} \varphi(\frac{n}{d}) = \sum\limits_{d|n} \varphi(d)$. [Q]

   (c) L'égalité précédente s'écrit $\varphi \star \mathbf{1} = \mathrm{Id}$.
   On trouve alors $\varphi = \mu \star \mathrm{Id}$ en remplaçant f par Id et F par φ dans la question (IV.3)
   Autrement dit, pour tout n de $\mathbb{N}^*$, on a $\varphi(n) = \sum\limits_{d|n} \mu(d)\dfrac{n}{d}$.
   Enfin $\varphi = \mu \star \mathbf{1}$ prouve que φ est multiplicative puisque μ et $\mathbf{1}$ le sont. [Q]

2. (a) Si p est premier, on a $\mathcal{E}_p = \{1,\ldots,p-1\}$, donc $\varphi(p) = p-1$.
   Plus généralement soit p dans $\mathbb{P}$, k dans $\mathbb{N}^*$ et $n = p^k$.
   – Première démonstration :
     Soit m un entier de $\{1,\ldots,n\}$. On a $n \wedge m > 1 \Leftrightarrow p \mid m$.
     Dans $\{1,\ldots,n = p^k\}$, il y a p^{k-1} multiples de p : ce sont les qp avec $1 \leqslant q \ldots \leqslant p^{k-1}$.
     Dans $\{1,\ldots,n = p^k\}$, il y a donc $p^k - p^{k-1}$ entiers premiers avec n.
     Autrement dit, pour tout p de $\mathbb{P}$ et tout k de $\mathbb{N}^*$, on a $\varphi(p^k) = p^k - p^{k-1}$.
   – Deuxième démonstration :
     On sait qu'on a l'égalité $\varphi(n) = \sum\limits_{d|n} \mu(d)\dfrac{n}{d}$, donc $\varphi(p^k) = \sum\limits_{j=0}^{k} \mu(p^j)p^{k-j}$.
     Or $\mu(1) = 1$, $\mu(p) = -1$ et $\mu(p^j) = 0$ pour tout $j \geqslant 2$.
     On en déduit $\varphi(p^k) = \mu(1)p^k + \mu(p)p^{k-1} = p^k - p^{k-1}$.
   On a donc obtenu $\varphi(p^k) = p^k - p^{k-1}$ pour tout p de $\mathbb{P}$ et tout k de $\mathbb{N}^*$. [Q]

   (b) Le résultat précédent s'écrit, pour tout p de $\mathbb{P}$ et tout n de $\mathbb{N}^*$: $\varphi(p^k) = p^k\Big(1 - \dfrac{1}{p}\Big)$.
   On se donne un entier $n \geqslant 2$, décomposé en $n = \prod\limits_{p\in\mathbb{P}_n} p^{v_p(n)}$.
   Puisque φ est multiplicative, on obtient :
   $$\begin{aligned}\varphi(n) &= \varphi\Big(\prod_{p\in\mathbb{P}_n} p^{v_p(n)}\Big) = \prod_{p\in\mathbb{P}_n} \varphi(p^{v_p(n)}) = \prod_{p\in\mathbb{P}_n} \Big[p^{v_p(n)}\Big(1-\frac{1}{p}\Big)\Big]\\ &= \prod_{p\in\mathbb{P}_n} p^{v_p(n)} \prod_{p\in\mathbb{P}_n}\Big(1-\frac{1}{p}\Big) = n\prod_{p\in\mathbb{P}_n}\Big(1-\frac{1}{p}\Big)\end{aligned}$$
   Par exemple : $\varphi(10!) = \varphi(2^8 3^4 5^2 7) = 10!\,\Big(1-\dfrac{1}{2}\Big)\Big(1-\dfrac{1}{3}\Big)\Big(1-\dfrac{1}{5}\Big)\Big(1-\dfrac{1}{7}\Big) = 829440$. [Q]

VII. Quelques formules asymptotiques

1. (a) On commence par écrire $\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \sum_{d|k} 1$.

   La somme est effectuée sur des couples (k, d) d'entiers, et la somme «externe» est sur k.

   Dans cette double somme, l'entier d peut prendre toutes les valeurs de 1 à n.

   Pour chaque valeur de d, l'entier k prend toutes les valeurs telles que $d \mid k$ et $k \leqslant n$.

   Mais les multiples de d dans $\{1, \ldots, n\}$ sont $d, 2d, \ldots, md$, avec $m = \left[\frac{n}{d}\right]$.

   Autrement dit : $\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \sum_{d|k} 1 = \sum_{d=1}^{n} \Big(\sum_{d|k,\, k \leqslant n} 1 \Big) = \sum_{d=1}^{n} \left[\frac{n}{d}\right]$. [Q]

   (b) Pour $d \geqslant 2$, on a $\int_{d}^{d+1} \frac{\mathrm{d}\,t}{t} \leqslant \frac{1}{d} \leqslant \int_{d-1}^{d} \frac{\mathrm{d}\,t}{t}$ donc $\ln(d+1) - \ln(d) \leqslant \frac{1}{d} \leqslant \ln(d) - \ln(d-1)$.

   Par sommation, $\ln(n+1) - \ln 2 \leqslant S_n - 1 \leqslant \ln n$ et il en résulte $\lim_{n\to\infty} \frac{S_n}{\ln n} = 1$. [Q]

   (c) On a évidemment $\sum_{d=1}^{n} \Big(\frac{n}{d} - 1\Big) \leqslant \sum_{d=1}^{n} \left[\frac{n}{d}\right] \leqslant \sum_{d=1}^{n} \frac{n}{d}$, donc $n(S_n - 1) \leqslant \sum_{k=1}^{n} \tau(k) \leqslant nS_n$.

   Il en résulte immédiatement $\lim_{n\to\infty} \frac{1}{n \ln n} \sum_{k=1}^{n} \tau(k) = 1$, ce qu'il fallait prouver. [Q]

2. (a) On procède par interversion de sommations, comme dans la question (1a) de cette partie.

   On trouve $\sum_{k=1}^{n} \sigma(k) = \sum_{k=1}^{n} \sum_{d|k} d = \sum_{d=1}^{n} \Big(\sum_{d|k,\, k \leqslant n} d \Big) = \sum_{d=1}^{n} d \Big(\sum_{d|k,\, k \leqslant n} 1 \Big) = \sum_{d=1}^{n} d\left[\frac{n}{d}\right]$ [Q]

   (b) Bien sûr $d\left[\frac{n}{d}\right] = d \sum_{k=1}^{n/d} 1 = \sum_{k=1}^{n/d} d$, donc $\sum_{k=1}^{n} \sigma(k) = \sum_{d=1}^{n} \sum_{k=1}^{n/d} d$.

   Cette double somme est étendue aux couples (d, k) tels que $1 \leqslant d \leqslant n$ et $1 \leqslant k \leqslant n/d$.

   Ce sont les couples d'entiers (d, k) tels que $1 \leqslant dk \leqslant n$.

   Ce sont donc les couples d'entiers (d, k) tels que $1 \leqslant k \leqslant n$ et $1 \leqslant d \leqslant n/k$.

   On en déduit $\sum_{k=1}^{n} \sigma(k) = \sum_{k=1}^{n} \Big(\sum_{d=1}^{n/k} d \Big) = \frac{1}{2} \sum_{k=1}^{n} \left[\frac{n}{k}\right] \Big(\left[\frac{n}{k}\right] + 1 \Big)$. [Q]

   (c) On utilise évidemment les encadrements $\frac{n}{k} - 1 \leqslant \left[\frac{n}{k}\right] \leqslant \frac{n}{k}$.

   On en déduit $\frac{1}{2} \sum_{k=1}^{n} \frac{n}{k} \Big(\frac{n}{k} - 1 \Big) \leqslant \sum_{k=1}^{n} \sigma(k) \leqslant \frac{1}{2} \sum_{k=1}^{n} \frac{n}{k} \Big(\frac{n}{k} + 1 \Big)$.

   Après développement : $\frac{1}{2}\Big(n^2 T_n - nS_n\Big) \leqslant \sum_{k=1}^{n} \sigma(k) \leqslant \frac{1}{2}\Big(n^2 T_n + nS_n\Big)$. [Q]

   (d) On divise par n^2 : $\frac{1}{2}\Big(T_n - \frac{S_n}{n}\Big) \leqslant \frac{1}{n^2} \sum_{k=1}^{n} \sigma(k) \leqslant \frac{1}{2}\Big(T_n + \frac{S_n}{n}\Big)$.

   On sait d'après (1b) que $\frac{S_n}{n} = \frac{S_n}{\ln n} \frac{\ln n}{n}$ tend vers 0 quand $n \to \infty$.

   Sachant que $\lim_{n\to\infty} T_n = \frac{\pi^2}{6}$, on trouve bien $\lim_{n\to\infty} \frac{\sigma(1) + \sigma(2) + \ldots + \sigma(n)}{n^2} = \frac{\pi^2}{12}$. [Q]

3. (a) On trouve $\sum_{k=1}^{n} \varphi(k) = \sum_{k=1}^{n} \Big(\sum_{d|k} \mu(d) \frac{k}{d} \Big) = \sum_{d=1}^{n} \mu(d) \Big(\sum_{d|k} \frac{k}{d} \Big)$

   Dans la dernière somme, à d fixé, le quotient $q = k/d$ parcourt l'ensemble $\{1, 2, \ldots, [n/d]\}$.

   Ainsi $\sum_{k=1}^{n} \varphi(k) = \sum_{d=1}^{n} \mu(d) \Big(\sum_{q=1}^{n/d} q \Big) = \frac{1}{2} \sum_{d=1}^{n} \mu(d) \left[\frac{n}{d}\right] \Big(\left[\frac{n}{d}\right] + 1 \Big) = \frac{1}{2} \sum_{k=1}^{n} \mu(k) \Big(\left[\frac{n}{k}\right]^2 + \left[\frac{n}{k}\right] \Big)$. [Q]

(b) On trouve tout d'abord :

$$\begin{aligned}\frac{n^2}{2}U_n - \sum_{k=1}^{n}\varphi(k) &= \frac{1}{2}\sum_{k=1}^{n}\mu(k)\left(\frac{n}{k}\right)^2 - \frac{1}{2}\sum_{k=1}^{n}\mu(k)\left(\left[\frac{n}{k}\right]^2 + \left[\frac{n}{k}\right]\right)\\ &= \frac{1}{2}\sum_{k=1}^{n}\mu(k)\left(\left(\frac{n}{k}\right)^2 - \left[\frac{n}{k}\right]^2\right) - \frac{1}{2}\sum_{k=1}^{n}\mu(k)\left[\frac{n}{k}\right]\end{aligned}$$

On majore les $\mu(k)$ par 1 en valeur absolue, et on utilise $\left[\frac{n}{k}\right] \leqslant \frac{n}{k}$.

On obtient $\left|\frac{n^2}{2}U_n - \sum_{k=1}^{n}\varphi(k)\right| \leqslant \frac{1}{2}\sum_{k=1}^{n}\left(\left(\frac{n}{k}\right)^2 - \left[\frac{n}{k}\right]^2\right) + \frac{1}{2}\sum_{k=1}^{n}\left[\frac{n}{k}\right]$.

Ensuite on a : $0 \leqslant \left(\frac{n}{k}\right)^2 - \left[\frac{n}{k}\right]^2 = \left(\frac{n}{k} - \left[\frac{n}{k}\right]\right)\left(\frac{n}{k} + \left[\frac{n}{k}\right]\right) \leqslant \frac{n}{k} + \left[\frac{n}{k}\right]$.

On en déduit $\left|\frac{n^2}{2}U_n - \sum_{k=1}^{n}\varphi(k)\right| \leqslant \frac{1}{2}\sum_{k=1}^{n}\left(\frac{n}{k} + 2\left[\frac{n}{k}\right]\right) \leqslant \frac{1}{2}\sum_{k=1}^{n}\frac{3n}{k} = \frac{3nS_n}{2}$.

Après division par n^2 : $\left|\frac{1}{2}U_n - \frac{1}{n^2}\sum_{k=1}^{n}\varphi(k)\right| \leqslant \frac{3S_n}{2n}$.

On sait que $\lim_{n\to\infty}\frac{S_n}{n} = 0$. On en déduit $\lim_{n\to\infty}\frac{1}{n^2}\sum_{k=1}^{n}\varphi(k) = \frac{1}{2}\lim_{n\to\infty}U_n = \frac{3}{\pi^2}$. [Q]

(c) Il y a n^2 façons de choisir le couple (a,b) dans $\{1,\ldots,n\}^2$, toutes équiprobables.

Cherchons le nombre de couples (a,b) tels que $a \wedge b = 1$.

A part le couple $(1,1)$, ce sont des couples (a,b) avec $1 \leqslant a < b$ ou $1 \leqslant b < a$, et il y en a autant d'une sorte que de l'autre. Pour calculer le nombre de couples (a,b) tels que $1 \leqslant a < b$ et $a \wedge b = 1$, on effectue un dénombrement suivant les valeurs de b. Pour chaque b (de $b = 2$ à $b = n$) il y a bien sûr $\varphi(b)$ valeurs possibles.

Ainsi le nombre de couples (a,b) tels que $a \wedge b = 1$ est $1 + 2\sum_{k=2}^{n}\varphi(k) = 2\sum_{k=1}^{n}\varphi(k) - 1$.

La probabilité demandée est donc $p_n = \frac{1}{n^2}\left(2\sum_{k=1}^{n}\varphi(k) - 1\right)$.

Puisque $\lim_{n\to\infty}\frac{1}{n^2}\sum_{k=1}^{n}\varphi(k) = \frac{3}{\pi^2}$, on trouve $\lim_{n\to\infty}p_n = \frac{6}{\pi^2}$. [Q]