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 $p \in \mathbb{P}_n \Leftrightarrow v_p(n) \geq 1$.
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 $f\left(\prod_{j=1}^{q} m_j\right) = \prod_{j=1}^{q} f(m_j)$. [S]
   (b) Montrer que f est caractérisée par les $f(p^k)$, où $(p, k) \in \mathbb{P} \times \mathbb{N}^*$. [S]

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 13 pages.

II. Exemples de fonctions multiplicatives

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

1. Pour tout $n \geq 1$, 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 $n \geq 1$, 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 $n \geq 2$, 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 $v_p(n) \geq 2$, 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 $n \geq 2$.
  Il est clair que les applications 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]

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 13 pages.

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 $n \geq 1$, 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 $n \geq 1$, on a $\dfrac{\sigma(n)}{n} = \sum_{d|n} \dfrac{1}{d}$. [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 $n \geq 2$, on a l'égalité $\sigma(n) = \prod_{p \in \mathbb{P}_n} \dfrac{p^{v_p(n)+1} - 1}{p - 1}$. [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 $m \geq 1$ et q impair tel que $n = 2^m\, q$.
   Montrer que $q = (2^{m+1} - 1)\, r$ avec $r \geq 1$. Montrer que $\sigma(q) = q + r$. [S]
   NB : Le problème de l'existence d'entiers parfaits impairs est un problème ouvert.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 13 pages.

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 $\sum\limits_{d|n}\varphi(n)=n$. [S]

   (c) Montrer que $\varphi(n)=\sum\limits_{d|n}\mu(d)\dfrac{n}{d}$ pour tout $n\geq 1$, 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 $n\geq 1$, on a $\varphi(n)=n\prod\limits_{k\in\mathbb{P}_n}\Bigl(1-\dfrac{1}{p}\Bigr)$. Calculer par exemple $\varphi(10!)$. [S]

VII. Quelques formules asymptotiques

1. (a) Pour tout entier n, montrer qu'on a l'égalité $\sum\limits_{k=1}^{n}\tau(k)=\sum\limits_{d=1}^{n}\Bigl[\dfrac{n}{d}\Bigr]$.
   Indication : on écrira $\sum\limits_{k=1}^{n}\tau(k)=\sum\limits_{k=1}^{n}\sum\limits_{d|k}1$ et on cherchera à intervertir les deux sommes. [S]

   (b) Avec $S_n=\sum\limits_{d=1}^{n}\dfrac{1}{d}$, montrer que $\lim\limits_{n\to\infty}S_n/\ln n=1$. [S]

   (c) Déduire de ce qui précède qu'on a : $\lim\limits_{n\to\infty}\dfrac{\tau(1)+\tau(2)+\cdots+\tau(n)}{n\ln n}=1$
   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 $\sum\limits_{k=1}^{n}\sigma(k)=\sum\limits_{d=1}^{n}d\Bigl[\dfrac{n}{d}\Bigr]$ (même indication qu'en (1a).) [S]

   (b) Justifier les transformations suivantes :
   $$\sum_{k=1}^{n}\sigma(k)=\sum_{d=1}^{n}d\Bigl(\sum_{k=1}^{n/d}1\Bigr)=\sum_{d=1}^{n}\Bigl(\sum_{k=1}^{n/d}d\Bigr)=\sum_{1\leq dk\leq n}d=\sum_{k=1}^{n}\Bigl(\sum_{d=1}^{n/k}d\Bigr)=\frac{1}{2}\sum_{k=1}^{n}\Bigl[\frac{n}{k}\Bigr]\Bigl(\Bigl[\frac{n}{k}\Bigr]+1\Bigr)$$ [S]

   (c) Pour tout entier n, on pose (comme dans (1b)) $S_n=\sum\limits_{k=1}^{n}\dfrac{1}{k}$ et $T_n=\sum\limits_{k=1}^{n}\dfrac{1}{k^2}$.
   Montrer que : $\dfrac{1}{2}\Bigl(n^2T_n-nS_n\Bigr)\leq\sum\limits_{k=1}^{n}\sigma(k)\leq\dfrac{1}{2}\Bigl(n^2T_n+nS_n\Bigr)$. [S]

   (d) On admet que $\lim\limits_{n\to\infty}T_n=\dfrac{\pi^2}{6}$. En déduire $\lim\limits_{n\to\infty}\dfrac{\sigma(1)+\sigma(2)+\ldots+\sigma(n)}{n^2}=\dfrac{\pi^2}{12}$. [S]

3. On pose $U_n=\sum\limits_{k=1}^{n}\dfrac{\mu(k)}{k^2}$ pour tout entier n. On admet que $\lim\limits_{n\to\infty}U_n=\dfrac{6}{\pi^2}$.

   (a) Pour tout $n\geq 1$, montrer que $\sum\limits_{k=1}^{n}\varphi(k)=\sum\limits_{d=1}^{n}\mu(d)\Bigl(\sum\limits_{d|k}\dfrac{k}{d}\Bigr)=\dfrac{1}{2}\sum\limits_{d=1}^{n}\mu(d)\Bigl[\dfrac{n}{d}\Bigr]\Bigl(\Bigl[\dfrac{n}{d}\Bigr]+1\Bigr)$. [S]

   (b) Montrer : $\Bigl|\dfrac{n^2}{2}U_n-\sum\limits_{k=1}^{n}\varphi(k)\Bigr|\leq\dfrac{3nS_n}{2}$. En déduire $\lim\limits_{n\to\infty}\dfrac{\varphi(1)+\varphi(2)+\ldots+\varphi(n)}{n^2}=\dfrac{3}{\pi^2}$. [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 $\dfrac{6}{\pi^2}$. [S]

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 13 pages.

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.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 13 pages.