MATHEMATICA VOL. 13 (36), 2, 1971, pp. 271–279

SUR CERTAINES FONCTIONS ARITHMÉTIQUES MULTIPLICATIVES

par

TIBERIU POPOVICIU

à Cluj

I.

1. Une fonction arithmétique $f(n)$, donc une fonction (réelle) définie sur l'ensemble des nombres naturels, est dite *multiplicative* si nous avons

$$f(ab) = f(a)\,f(b) \tag{1}$$

quels que soient les nombres (naturels) a, b premiers entre eux.

Dans la suite nous désignerons par $(a_1, a_2, \ldots, a_n)$ le p.g.c.d. et par $[a_1, a_2, \ldots, a_n]$ le p.p.c.m. des nombres (naturels) $a_1, a_2, \ldots, a_n$. Les nombres $a_1, a_2, \ldots, a_n$ sont premiers entre eux si et seulement si $(a_1, a_2, \ldots, a_n) = 1$. Avec ces notations la propriété de multiplicativité de la fonction $f(n)$ s'écrit $(a, b) = 1 \Rightarrow f(ab) = f(a)\,f(b)$.

2. Dans le livre bien connu de G. PÓLYA et G. SZEGŐ [**3**, p. 126] on trouve énoncée et démontrée une intéressante propriété des fonctions arithmétiques multiplicatives. Sous une forme un peu modifiée nous pouvons énoncer cette propriété sous la forme du

THÉORÈME 1. *Si $f(n)$ est une fonction arithmétique multiplicative et $a_1, a_2, \ldots, a_n$ des nombres naturels quelconques, nous avons les formules*

$$f([a_1, a_2, \ldots, a_n]) = \prod_{k=1}^{n} \left(\prod_{(k)} f((a_{i_1}, a_{i_2}, \ldots, a_{i_k})) \right)^{(-1)^{k-1}} \tag{2}$$

$$f((a_1, a_2, \ldots, a_n)) = \prod_{k=1}^{n} \left(\prod_{(k)} f([a_{i_1}, a_{i_2}, \ldots, a_{i_k}]) \right)^{(-1)^{k-1}} \tag{3}$$

où $\prod_{(k)}$ *désigne un produit étendu à toutes les* $\binom{n}{k}$ *combinaisons* k *à* k, $i_1, i_2, \ldots, i_k$ *des indices* $1, 2, \ldots, n$.

Pour $n = 2$ la propriété revient à la formule

$$f((a, b))\, f([a, b]) = f(a)\, f(b) \tag{4}$$

où $f(n)$ est une fonction arithmétique multiplicative et a, b sont deux nombres naturels quelconques. Cette propriété est donnée comme exercice aussi dans mon cours d'algèbre supérieure (litographié) [**5**, p. 190].

La démonstration du théorème 1 dans [**3**] et aussi seulement du cas particulier $n = 2$ dans mon cours cité [**5**] est basée sur la décomposition unique, bien connue, d'un nombre naturel en facteurs premiers. Dans la suite nous donnerons une démonstration ne faisant pas appel à cette décomposition.

3. Pour commencer nous allons démontrer la propriété dans le cas particulier $n = 2$, donc nous allons établir la formule (4).

Nous allons d'abord démontrer le

Lemme 1. *a, b étant deux nombres premiers entre eux et d un troisième nombre naturel quelconque, il existe une décomposition $d = d'd''$ de d dans le produit de deux diviseurs complémentaires d', d'' tels que l'on ait*

$$(d', d'') = 1,\ (d', a) = 1,\ (d'', b) = 1. \tag{5}$$

Nous considérons seulement des diviseurs positifs des nombres.

Passons à la démonstration du lemme 1. Il existe des diviseurs de d qui sont premiers avec a. Par exemple le nombre 1 est un tel diviseur. Soit alors d' le plus grand des diviseurs de d qui est premier avec a et qui existe puisque tous les diviseurs de d, donc en particulier ceux qui sont premiers avec a, sont $\leq d$. Soit alors d'' le diviseur complémentaire de d'. Il suffit de démontrer la première et la troisième formule (5), la seconde étant vraie par construction.

Soit $e = (d', d'')$ et supposons que $e > 1$. Nous avons $e|d''$, d'où $ed'|d$, Ensuite de $e|d'$ et $(d', a) = 1$ il résulte que $(ed', a) = 1$. Enfin nous avons $d' < ed'$ ce qui est en contradiction avec la définition de d'. Il en résulte que $e = 1$, donc $(d', d'') = 1$.

Soit $f = (d'', b)$ et supposons que $f > 1$. Nous avons alors $f|b$, d'où $(f, a) = 1$. Ensuite de $f|d''$ et $(d', a) = 1$ il résulte que $fd'|d$ donc aussi que $(fd', a) = 1$. Nous avons enfin $d' < fd'$ ce qui est encore en contradiction avec la définition de d'. Il en résulte que $f = 1$, donc $(d'', b) = 1$.

Le lemme 1 est donc démontré.

Remarque 1. Tout diviseur d_1 de d et qui est premier avec a est un diviseur du plus grand diviseur d' de d qui jouit de la même propriété. En effet, de $d_1|d$, $d'|d$, $(d_1, a) = (d', a) = 1$ il résulte que $[d_1, d']|d$ et $([d_1, d'], a) = [(d_1, a), (d', a)] = 1$, donc $([d_1, d'], a) = 1$. Mais $d' \leq [d_1, d'] \leq d'$, en vertu de la définition de d'. Il en résulte que $[d_1, d'] = d'$, donc $d_1|d'$.

Remarque 2. Le diviseur d' a été utilisé aussi dans d'autres problèmes par W. SIERPINSKI [6, p. 17].

4. Passons à la démonstration de la formule (4). Posons $d = (a, b)$ et $a = da'$, $b = db'$. Alors $(a', b') = 1$. Appliquons le lemme 1 aux nombres a', b', d. Nous avons $a = d'd''a'$, $b = d''d'b'$, $(a, b) = d'd''$, $[a, b] = d'b'd''a'$.

Mais, de $(d', d'') = (d', a') = 1$ il résulte que $(d', d''a') = 1$. De même nous avons $(d'', d'b') = 1$. De la propriété (1) de multiplicativité il résulte alors que

$$f(a) = f(d')\, f(d''a'),\ f(b) = f(d'')\, f(d'b'). \tag{6}$$

De même de $(d', d''a') = (b', d''a') = 1$ il résulte que $(d''a', d'b') = 1$ et nous en déduisons

$$f((a, b)) = f(d')\, f(d''),\ f([a, b]) = f(d''a')\, f(d'b') \tag{7}$$

En comparant les formules (6) et (7) nous obtenons la formule cherchée (4).

5. Démontrons le théorème 1. Pour démontrer la formule (2) nous allons procéder par induction complète sur le nombre n des nombres a_i. Pour $n = 2$ la formule revient à (4) et est donc démontrée. Supposons que la propriété soit vraie pour $n - 1$ nombres et démontrons-la pour n nombres $a_1, a_2, \ldots, a_n$ $(n > 2)$. Pour simplifier l'écriture posons $E_k = \prod_{(k)} f((a_{i_1}, a_{i_2}, \ldots, a_{i_k}))$, $k = 1, 2, \ldots, n$ et désignons par E'_k, $k = 1, 2, \ldots, n - 1$ les nombres E_k correspondant aux $n - 1$ nombres $a_1, a_2, \ldots, a_{n-1}$ et par E^*_k, $k = 1, 2, \ldots, n - 1$ les mêmes nombres correspondant aux $n - 1$ nombres (a_1, a_n), (a_2, a_n), $\ldots$, (a_{n-1}, a_n). En tenant compte de (4) nous avons

$$f([[a_1, a_2, \ldots, a_{n-1}], a_n]) \cdot f(([a_1, a_2, \ldots, a_{n-1}], a_n)) = f([a_1, a_2, \ldots, a_n])\, f(a_n) \tag{8}$$

et on vérifie facilement que

$$E_k = E'_k E^*_{k-1},\ k = 1, 2, \ldots, n \tag{9}$$

en posant $E'_n = 1$, $E^*_0 = f(a_n)$. Par suite de la propriété de distributivité des opérations (a, b) et $[a, b]$, nous avons

$$([a_1, a_2, \ldots, a_{n-1}], a_n) = [(a_1, a_n), (a_2, a_n), \ldots, (a_{n-1}, a_n)]. \tag{10}$$

Par hypothèse nous avons

$$f([a_1, a_2, \ldots, a_{n-1}]) = \prod_{k=1}^{n-1} E_k'^{(-1)^{k-1}} \tag{11}$$

et en vertu de l'égalité (10) nous avons aussi

$$f([[a_1, a_2, \ldots, a_{n-1}], a_n)) = \prod_{k=1}^{n-1} E_k^{*(-1)^{k-1}} \tag{12}$$

Compte tenant de (8), (9), (11) et (12) on déduit la formule (2).

On démontre de la même manière la formule (3).

Le théorème 1 est donc démontré.

La fonction arithmétique $f(n) = n$ est bien multiplicative et la formule (4) devient $(a, b)[a, b] = ab$ qui peut se démontrer directement à l'aide de la relation de divisibilité. On peut facilement écrire les formules générales (2), (3) dans le cas de la fonction $f(n) = n$. Pour la formule (2) ceci est fait dans le livre cité de G. PÓLYA et G. SZEGŐ [3].

II.

6. La fonction arithmétique d'Euler $\varphi(n)$ (l'indicateur) est bien multiplicative et nous avons

$$\varphi(ab) = \varphi(a)\,\varphi(b) \tag{13}$$

si (et seulement si) $(a, b) = 1$.

On sait que $\varphi(n)$ est égale au nombre des nombres naturels $\leq n$ et premiers avec n.

Si la condition $(a, b) = 1$ n'est pas vérifiée la formule (13) n'est plus vraie. En général si $d = (a, b)$ nous avons la formule

$$d\varphi(a)\,\varphi(b) = \varphi(d)\,\varphi(ab). \tag{14}$$

On peut rencontrer cette formule, même si elle n'est pas explicitée assez clairement, dans divers traités. Il suffit de citer E. LUCAS [2, p. 398] et L. E. DICKSON [1, p. 13].

Les démonstrations de la formule (14) ont été toujours basées sur la décomposition en facteurs premiers des nombres. Il y a encore intérêt à nous passer de cette décomposition. C'est ce que nous allons faire dans la suite.

7. Nous allons d'abord démontrer le

Lemme 2. *Si $a|b$ nous avons*

$$\varphi(ab) = a\varphi(b). \tag{15}$$

Nous désignerons par $a|b$ le fait que le nombre b est divisible par le nombre a, notation que nous avons déjà utilisée dans la première partie de ce travail.

Nous pouvons donner une démonstration de ce lemme, analogue à la démonstration bien connue de la formule (13). Cette démonstration revient à dénombrer les termes de la suite des ab premiers nombres naturels qui sont premiers avec ab, les termes de cette suite étant rangés, pour plus de clarté, dans un tableau rectangulaire

$$\begin{array}{cccc} 1 & 2 & \ldots. & b \\ b+1 & b+2 & \ldots. & 2b \\ \ldots\ldots\ldots & \ldots\ldots\ldots & \ldots\ldots & \ldots\ldots \\ (a-1)b+1 & (a-1)b+2 & \ldots. & ab \end{array} \tag{16}$$

de a lignes et b colonnes de manière que l'élément de la $(i+1)^{\text{ème}}$ ligne et la $j^{\text{ème}}$ colonne soit $ib + j$. On peut trouver cette démonstration dans tous les traités de la théorie des nombres. Il suffit de citer le beau livre de W. SIERPINSKI [6, p. 229]. On peut aussi consulter mon cours déjà cité [5, p. 182].

Pour démontrer le lemme 2 considérons encore le tableau (16). Nous démontrerons que, dans les conditions du lemme nous avons

$$(ib + j, ab) = 1 \Leftrightarrow (j, b) = 1. \tag{17}$$

En effet, remarquons que nous avons en général $(\alpha, \beta\gamma) = 1 \Leftrightarrow (\alpha, \beta) = (\alpha, \gamma) = 1$ et $(\alpha, \beta) = (\alpha, \beta + \gamma\alpha)$, lorsque α, β, γ sont des nombres naturels. Si maintenant $(ib + j, ab) = 1$, il en résulte que $(ib + j, b) = 1$, donc aussi $(j, b) = 1$. Nous avons donc

$$(ib + j, ab) = 1 \Rightarrow (j, b) = 1. \tag{18}$$

Supposons maintenant que $(j, b) = 1$. Il en résulte que $(ib + j, b) = 1$ donc $(ib + j, a) = 1$, *puisque a est un diviseur de b*. Il en résulte que $(ib + j, ab) = 1$. Nous avons donc

$$(j, b) = 1 \Rightarrow (ib + j, ab) = 1. \tag{19}$$

De (18), (19) il résulte la formule (17). De la formule (17) il résulte que dans chaque ligne du tableau (16) il y a exactement $\varphi(b)$ nombres premiers avec ab. Le lemme 2 est donc démontré.

D'ailleurs la propriété exprimée par le lemme 2 est équivalente à celle exprimée par le

Lemme 3. *Nous avons*

$$\varphi(a^2 b) = a\varphi(ab). \tag{20}$$

Pour montrer que le lemme 3 résulte du lemme 2 il suffit d'appliquer la formule (15) aux nombres a, ab, le second étant visiblement divisible par le premier. Pour montrer que le lemme 2 résulte du lemme 3 soit $a|b$. Nous avons alors $b = ab'$ et en vertu du lemme 3 nous avons $\varphi(ab) = \varphi(a^2b') = a\varphi(ab') = a\varphi(b)$. Il en résulte la formule (15).

Une conséquence immédiate de (20) est la formule

$$\varphi(a^m b) = a^{m-1}\varphi(ab) \tag{21}$$

quels que soient les nombres naturels a, b, m.

8. Démontrons la formule (14). En posant $d = (a, b)$, nous avons $d[a, b] = ab$. Mais $d|[a, b]$, donc $\varphi(ab) = d\varphi([a, b])$. En tenant compte de la formule (4) il résulte que $\varphi(d)\,\varphi(ab) = d\varphi[(a, b])\,\varphi(d) = d\varphi(a)\,\varphi(b)$, d'où la formule (14).

9. La formule (14) peut être généralisée et nous pouvons énoncer le

THÉORÈME 2. *$a_1, a_2, \ldots, a_n$ étant des nombres naturels et en posant $d = (a_1, a_2, \ldots, a_n)$, nous avons*

$$\prod_{k=1}^{n}\Big(\prod_{(k)}\varphi(a_{i_1}a_{i_2}\ldots a_{i_k})\Big)^{(-1)^{k-1}} = \frac{\varphi(d)}{d} \tag{22}$$

où $\prod_{(k)}$ a la même signification que dans le théorème 1.

Nous allons faire la démonstration par induction complète sur le nombre n des nombres a_i. Pour $n = 2$ la formule (22) revient à (14) qui est déjà démontrée. Supposons maintenant que la propriété soit vraie pour $n - 1$ nombres et démontrons-la pour n nombres ($n > 2$).

Considérons les n nombres $a_1, a_2, \ldots, a_n$ et posons $d = (a_1, a_2, \ldots, a_n)$, $d' = (a_1, a_2, \ldots, a_{n-1})$. En désignant par $\prod'_{(k)}$ un produit étendu à toutes les $\binom{n-1}{k}$ combinaisons $i_1, i_2, \ldots, i_k$, k à k des indices $1, 2, \ldots, n-1$, nous avons, par hypothèse,

$$\frac{\varphi(d')}{d'} = \prod_{k=1}^{n-1}\Big(\prod'_{(k)}\varphi(a_{i_1}a_{i_2}\ldots a_{i_k})\Big)^{(-1)^{k-1}} \tag{23}$$

En remarquant que $(d', a_n) = d$ nous avons, d'après (14),

$$\frac{\varphi(d')\,\varphi(a_n)}{\varphi(a_n d')} = \frac{\varphi(d')}{d'}\cdot\frac{a_n d'}{\varphi(a_n d')}\cdot\frac{\varphi(a_n)}{a_n} = \frac{\varphi(d)}{d}. \tag{24}$$

En appliquant la formule générale aux $n - 1$ nombres $a_1 a_n, a_2 a_n, \ldots, a_{n-1}a_n$, dont le p.g.c.d. est égal à $a_n d'$ et en tenant compte de la formule (21), nous avons

$$\frac{a_n d'}{\varphi(a_n d')} = \prod_{k=2}^{n}\Big(a_n^{(k-2)\binom{n-1}{k-1}}\prod'_{(k-1)}\varphi(a_{i_1}a_{i_2}\ldots a_{i_{k-1}}a_n)\Big)^{(-1)^{k-1}}. \tag{25}$$

Compte tenant de (23), (25) et de

$$\Big(\prod'_{(1)}\varphi(a_{i_1})\Big)\varphi(a_n) = \prod_{(1)}\varphi(a_{i_1})$$

$$\Big(\prod'_{(k-1)}\varphi(a_{i_1}a_{i_2}\ldots a_{i_{k-1}}a_n)\Big)\Big(\prod'_{(k)}\varphi(a_{i_1}a_{i_2}\ldots a_{i_k})\Big) =$$

$$= \prod_{(k)}\varphi(a_{i_1}a_{i_2}\ldots a_{i_k}),\quad k = 2, 3, \ldots, n-1$$

$$\prod'_{(n-1)}\varphi(a_{i_1}a_{i_2}\ldots a_{i_{n-1}}a_n) = \prod_{(n)}\varphi(a_{i_1}a_{i_2}\ldots a_{i_n})$$

$$\sum_{k=2}^{n}(-1)^{k-1}(k-2)\binom{n-1}{k-1} = 1,$$

de la formule (24) nous déduisons la formule (22). Le théorème 2 est donc démontré.

J'ai d'ailleurs démontré l'égalité (22) d'une autre manière dans un autre travail [3]. Dans ce travail j'ai cherché à établir l'inégalité

$$\prod_{k-1}^{n}\Big(\prod_{(k)}\varphi(a_{i_1}a_{i_2}\ldots a_{i_k})\Big)^{(-1)^{k-1}} \leqq 1$$

l'égalité étant vraie si et seulement si les nombres $a_1, a_2, \ldots, a_n$ sont premiers entre eux.

10. Pour terminer reprenons le lemme 2 que nous allons généraliser et compléter par le

THÉORÈME 3. *Nous avons*

$$\varphi(ab) \leqq a\varphi(b) \tag{26}$$

l'égalité étant vraie si et seulement s'il existe une puissance entière positive de b qui soit divisible par a.

De la démonstration du lemme 2 il résulte que nous avons (18) sans aucune restriction sur a et b. Il en résulte que dans le tableau (16) chaque ligne contient au plus $\varphi(b)$ termes premiers avec ab. L'inégalité (26) en résulte.

Examinons le cas de l'égalité dans (26).

Remarquons d'abord que si $a|b^m$ nous avons bien l'égalité (26). En effet, d'après le lemme 2 et la formule (21), nous avons

$$\varphi(ab^m) = a\varphi(b^m), \quad \varphi(ab^m) = b^{m-1}\varphi(ab), \quad \varphi(b^m) = b^{m-1}\varphi(b)$$

et l'égalité (15) en résulte.

Supposons maintenant que l'on ait

$$\varphi(ab) = a\varphi(b). \tag{27}$$

De la formule

$$(a, b^m) = (a, b^{m-1})\left(\frac{a}{(a, b^{m-1})}, b\right) \tag{28}$$

on déduit que la suite $((a, b^m))_{m=1}^{+\infty}$ est non-décroissante. Mais $(a, b^m)) \leqq a$, $m = 1, 2, \ldots$, Il en résulte qu'on peut trouver un nombre naturel m tel que $(a, b^m) = (a, b^{m+1}) = c$. Nous allons démontrer que pour ce nombre m on a $a|b^m$. En effet, nous avons $a = ca'$, $b^m = cb'$, $b^{m+1} = cbb'$ et $(a', b'b) = 1$ d'où aussi $(a', b) = 1$. Il en résulte que $(a', b^m) = 1$. Compte tenant de (21) la formule (27) nous donne $\varphi(ab^m) = a\varphi(b^m)$, d'où $\varphi(a')\,\varphi(ab^m) = a\varphi(b^m)\,\varphi(a') = ca'\varphi(a'b^m)$. Mais ab^m est divisible par c^2, d'où il résulte que $\varphi(ab^m) = c\varphi(a'b^m)$. Nous obtenons l'égalité $\varphi(a') = a'$ qui ne peut être vraie que pour $a' = 1$. Nous avons donc $(a, b^m) = a$, d'où $a|b^m$.

Le théorème 3 est donc démontré.

11. Les démonstrations précédentes ne font pas appel à la décomposition en facteurs premiers des nombres, mais seulement aux propriétés de la relation de divisibilité et des opérations de p.g.c.d. et p.p.c.m. Ces propriétés sont l'associativité, la commutativité et la distributivité l'une par rapport à l'autre des opérations (a, b), $[a, b]$, les propriétés $c(a, b) = (ca, cb)$, $c[a, b] = [ca, cb]$, $a|b \Rightarrow ca|cb$, etc. Pour la démonstration de toutes ces propriétés on peut consulter, par exemple, mon cours cité [5].

Remarque 3. Si nous faisons appel à la décomposition unique en facteurs premiers des nombres naturels, la condition d'égalité dans la formule (26) est équivalente à la propriété suivante :

Tout facteur premier du nombre a divise le nombre b.

Supposons que $a|b^m$ où m est un nombre naturel. De la formule (28) il résulte que

$$(a, b^m) = \prod_{\nu=0}^{m-1}\left(\frac{a}{(a, b^\nu)}, b\right). \tag{29}$$

Soit maintenant p un facteur premier de a. Alors $p|a$ et il résulte que $p|b^m$, donc aussi que $p|(a, b^m)$. La formule (29) nous montre alors qu'il existe un k, $0 \leqq k \leqq m-1$ tel que $p\left|\left(\frac{a}{(a, b^k)}, b\right)\right.$. Il en résulte que $p|b$.

Supposons maintenant que $p|a \Rightarrow p|b$ si p est premier. Soit alors $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ la décomposition de a en facteurs premiers. Nous avons $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r} c$, où $\beta_1, \beta_2, \ldots, \beta_r$, c sont des nombres naturels. Si nous prenons un nombre naturel m tel que $m \geqq \max\left(\frac{\alpha_1}{\beta_1}, \frac{\alpha_2}{\beta_2}, \ldots, \frac{\alpha_r}{\beta_r}\right)$ nous avons $a|b^m$.

L'équivalence des deux propriétés examinées est donc démontrée.

BIBLIOGRAPHIE

[1] Dickson L. E., *Modern Elementary Theory of Nombers*, 1950.
[2] Lucas E., *Théorie des nombres*, 1891.
[3] Pólya G., Szegö G., *Aufgaben und Lehrsätze aus der Analysis* II, 1925.
[4] Popoviciu T., *Asupra unor inegalităţi*, Gazeta Matematică, **51**, 81–85 (1945).
[5] Popoviciu T., *Curs de Algebră superioară*, fascicola **1**, 1948.
[6] Sierpinski W., *Elementary Theory of Numbers*, 1964.

Reçu le 5. VIII. 1971.