

# BULLETIN DE LA S. M. F.

LAGUERRE

## Sur quelques théorèmes d'arithmétique

*Bulletin de la S. M. F.*, tome 1 (1872-1873), p. 77-81

<[http://www.numdam.org/item?id=BSMF\\_1872-1873\\_\\_1\\_\\_77\\_0](http://www.numdam.org/item?id=BSMF_1872-1873__1__77_0)>

© Bulletin de la S. M. F., 1872-1873, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>*

## MÉMOIRES ET COMMUNICATIONS

---

*Sur quelques théorèmes d'arithmétique ; par M. LAGUERRE.*

(Séance du 22 janvier 1875)

1. On connaît la proposition suivante : «  $\varphi(m)$  désignant combien il y a de nombres premiers à  $m$  et non supérieurs à  $m$ , on a

$$m = \varphi(d) + \varphi(d') + \varphi(d'') + \dots,$$

$d, d', d''$  désignant la suite des diviseurs de  $m$ , parmi lesquels figurent 1 et  $m$  lui-même (\*). »

Cette proposition peut se généraliser ainsi qu'il suit :

Désignons en général par  $\left(m, \frac{m}{k}\right)$ , où  $m$  désigne un nombre entier et  $k$  une quantité réelle quelconque commensurable ou incommensurable, le nombre des entiers premiers avec  $m$  et non supérieurs à  $\frac{m}{k}$ ; on voit que, si  $k = 1$ , on a  $(m, m) = \varphi(m)$ .

(\*) Voy. SERRET, *Algèbre supérieure*, t. II, p. 13.

Cela posé, je dis que l'on a  $m$  désignant un nombre entier et  $\left(\frac{m}{k}\right)$  la partie entière du quotient  $\frac{m}{k}$ ,

$$(1) \quad \left(\frac{m}{k}\right) = \left(1, \frac{1}{k}\right) + \left(d, \frac{d}{k}\right) + \left(d', \frac{d'}{k}\right) + \dots + \left(m, \frac{m}{k}\right),$$

la somme contenue dans le second membre s'étendant à tous les diviseurs  $1, d, d', \dots, m$  du nombre  $m$ .

Pour le démontrer, je vais faire voir que si la proposition est vraie pour une valeur quelconque de  $k$ , elle est vraie pour toute autre valeur.

Soit  $k_0$  la valeur de  $k$  pour laquelle la formule est supposée vérifiée; concevons, par exemple, que  $k_0$  diminue d'une façon continue, le premier membre de la relation (1) ne pourra changer que si  $k$  passe par une valeur qui donne à  $\frac{m}{k}$  une valeur entière; dans ce passage,  $\left(\frac{m}{k}\right)$  augmentera d'une unité; le second membre ne peut changer que si l'une ou plusieurs des quantités  $\frac{d}{k}$  acquièrent une valeur entière, et, comme alors  $\frac{m}{k}$  a aussi une valeur entière, puisque  $m$  est un multiple de  $d$ , on voit que la solution de la question consiste à examiner ce qui se passe quand  $\frac{m}{k}$  est un entier.

Or, quand  $\frac{m}{k}$  est un entier, il peut se faire qu'un certain nombre d'expressions de la forme  $\frac{d}{k}$  soient aussi des entiers; supposons-les rangées par ordre décroissant de grandeur, en sorte qu'elles forment la série

$$\frac{m}{k}, \frac{m_1}{k}, \frac{m_2}{k}, \dots, \frac{\mu}{k},$$

$\frac{\mu}{k}$  désignant la plus petite de ces fractions (il est clair d'ailleurs que  $\mu$  peut être égal à  $m$ ).

Cela posé,  $\frac{\mu}{k}$  est nécessairement premier avec  $\mu$ ; car, si  $\alpha$  désignait un diviseur commun,  $\frac{\mu}{\alpha}$  et  $\frac{\alpha}{k}$  seraient des nombres entiers et  $\frac{\mu}{k}$  ne serait pas le dernier terme de la série. Il n'en est pas de même relativement aux termes précédents; en effet, si l'on pose  $\frac{\mu}{k} = e$ ,  $\mu$  et  $e$  étant premiers entre eux, on en déduit  $\left(\frac{m'}{k}\right)$  désignant un quelconque des termes qui précè-

dent  $\frac{\mu}{k}$ )  $e' = \frac{m'}{k} = \frac{m'e}{\mu}$ , d'où  $\frac{e'}{m'} = \frac{e}{\mu}$ ; et, comme la fraction  $\frac{e}{\mu}$  est irréductible, on en conclut que  $e'$  et  $m'$  sont respectivement des multiples de  $e$  et de  $m$  et ont par conséquent un facteur commun.

2. Voyons maintenant quels changements subit le second membre quand  $\frac{m}{k}$  prend une valeur entière.

Les différentes expressions telles que  $(m', \frac{m'}{k})$  ne changent pas de valeur; la série des nombres non supérieurs à  $\frac{m'}{k}$  renferme en plus, il est vrai, le nombre  $e'$ ; mais, comme il n'est pas premier avec  $m'$ , la somme n'est pas changée; l'expression  $(\mu, \frac{\mu}{k})$  seule change, et augmente précisément d'une unité, puisque  $\mu$  et  $\frac{\mu}{k}$  sont premiers entre eux.

La proposition est donc vraie, si elle est vraie pour une valeur quelconque de  $k$ ; et comme elle l'est évidemment pour une valeur de  $k$  supérieure à  $m$ , puisque les deux termes de la relation (1) se réduisent à zéro, elle est démontrée.

3. Je veux maintenant tirer de la relation  $m = \Sigma \varphi(d)$ , que j'ai rappelée au commencement de cette note, et dont je viens de donner une nouvelle démonstration indépendante de la formule qui exprime  $\varphi(m)$  au moyen de ses facteurs premiers (\*), une démonstration de cette formule elle-même.

M. Dedekind (*Théorie des nombres* de DIRICHLET, p. 594) a, il est vrai, donné un théorème remarquable qui permet de résoudre cette question.

Ce théorème s'énonce ainsi qu'il suit : «  $\lambda(n)$  désignant un nombre égal à 0, si  $n$  est divisible par un carré, dans le cas contraire, égal à  $\pm 1$  suivant que le nombre des facteurs de  $n$  est pair ou impair, si deux fonctions  $f(m)$  et  $\varphi(m)$  sont liées par la relation suivante

$$(2) \quad f(m) = \Sigma \lambda(d),$$

où, dans le second membre, la sommation s'étend à tous les diviseurs du nombre entier  $m$ , on a réciproquement

$$(3) \quad \psi(m) = \Sigma \lambda\left(\frac{m}{d}\right)f(d),$$

la sommation s'étendant également à tous les diviseurs de  $m$ .

De la formule (3), on déduit facilement l'expression connue de  $\varphi(m)$ ,

(\*) On connaît d'autres démonstrations indépendantes également de cette formule; voir, notamment, DIRICHLET, *Théorie des nombres*, p. 25.

mais il est à remarquer que la démonstration de cette formule indiquée par M. Dedekind s'appuie précisément sur cette expression; pour éviter un cercle vicieux, il faudrait donc établir directement la relation (3), ce qui serait du reste facile en développant les considérations qui suivent.

4. Pour obtenir l'expression de  $\vartheta(m)$ , je considérerai une série de la forme

$$f(1) \frac{x}{1-x} + f(2) \frac{x^2}{1-x^2} + f(3) \frac{x^3}{1-x^3} + \dots$$

Soit

$$\vartheta(1)x + \vartheta(2)x^2 + \vartheta(3)x^3 + \dots$$

son développement effectué suivant les puissances croissantes de  $x$ ; il est clair que les coefficients d'une des séries déterminent ceux de l'autre, en particulier on a évidemment

$$\vartheta(m) = \sum f(d),$$

la sommation s'étendant à tous les diviseurs du nombre entier  $m$ .

Supposons en particulier la fonction  $f$  tellement choisie que,  $m$  étant décomposé en facteurs premiers, en sorte que  $m = a^\alpha b^\beta c^\gamma \dots$ , on ait  $f(m) = f(a^\alpha) f(b^\beta) \dots$ . La fonction  $f$  reste du reste arbitraire; ainsi  $f(a^\alpha)$  et  $f(a'^\alpha)$  peuvent n'avoir aucune relation entre elles, si  $a$  et  $a'$  sont différents; il en est de même de  $f(a^\alpha)$  et  $f(b^\beta)$ , si les facteurs  $a$  et  $b$  ne sont pas les mêmes.

Cela posé, dans ces hypothèses, les différents diviseurs du nombre  $m = a^\alpha b^\beta \dots$  étant les différents termes du produit

$$(1 + a + \dots + a^{\alpha-1})(1 + b + \dots + b^{\beta-1}) \dots$$

il est clair que l'on aura

$$(4) \quad \vartheta(m) = [1 + f(a) + \dots + f(a^{\alpha-1})][1 + f(b) + \dots + f(b^{\beta-1})] \dots$$

5. Cette formule offre un grand nombre d'applications.

Supposons, par exemple, que l'on ait  $f(a) = f(b) = \dots = -1$ , et  $f(a^\alpha) = f(b^\beta) = \dots = 0$ , pour toutes les valeurs de  $\mu$  supérieures à l'unité. On déduira évidemment de la formule (4), pour toute valeur de  $m$  supérieure à l'unité,  $\vartheta(m) = 0$ ; on a d'ailleurs  $\vartheta(1) = 1$ , et il est facile de voir que  $f(m) = \lambda(m)$ ,  $\lambda$  désignant la même fonction numérique dont j'ai parlé ci-dessus (n° 3) (\*); on a donc l'expression suivante, due à Möbius (*loc. cit.*) :

$$(5) \quad x = \frac{x}{1-x} - \frac{x^2}{1-x^2} + \frac{x^3}{1-x^3} - \frac{x^5}{1-x^5} + \frac{x^6}{1-x^6} + \dots$$

(\*) Cette remarquable fonction numérique, qui se présente dans la formule de M. Dedekind, a aussi été étudiée par Möbius (*Sur un nouveau mode de réversion des séries*; *CRELLE*, t. IX), et par M. Tchebichef (*Note sur différentes séries*; *LIOUVILLE*, 1<sup>re</sup> série, t. XVI).

6. Supposons maintenant que l'on fasse,  $n$  désignant un entier quelconque,  $\theta(a) = \theta(b) = \dots = -1$ ,  $\theta(a^n) = \theta(b^n) = \dots = 1$ ,  $\theta(a^{n+1}) = \theta(b^{n+1}) = \dots = -1$ , en sorte que  $\theta(a^n)$  soit, quel que soit le facteur  $a$ , égal à  $+1$  si  $n$  est divisible par  $n$ , égal à  $-1$  si  $n$  est congru à  $+1$  suivant le module  $n$ , et dans tous les autres cas égal à zéro.

De la formule (4) il résulte que  $\theta(m)$  est nul, à moins que  $m$  ne soit une puissance  $n^{\text{ème}}$  exacte, auquel cas  $\theta(m) = 1$ ; d'ailleurs  $f(m)$  est toujours égal à  $-1$ ,  $0$  ou  $+1$ ; on déduit de là que, quel que soit l'entier  $n$ , la série

$$x + x^{2^n} + x^{3^n} + x^{4^n} + \dots$$

peut se mettre sous la forme

$$\frac{x}{1-x} + \epsilon_2 \frac{x^2}{1-x^2} + \epsilon_3 \frac{x^3}{1-x^3} + \epsilon_4 \frac{x^4}{1-x^4} + \dots,$$

les coefficients  $\epsilon$  étant toujours égaux à  $-1$ ,  $0$  ou  $+1$ , et se déterminant d'ailleurs facilement d'après ce qui précède.

Pour  $n = 2$ , on a en particulier la formule suivante, donnée par M. Liouville (*Journal de math.*, 2<sup>e</sup> série, t. II),

$$(6) \quad x + x^4 + x^9 + x^{16} + \dots = \frac{x}{1-x} - \frac{x^2}{1-x^2} - \frac{x^5}{1-x^5} + \frac{x^4}{1-x^4}.$$

7. Pour revenir à l'objet principal de cette note, je ferai remarquer que, de la propriété fondamentale de la fonction  $\varphi$ ,

$$(7) \quad m = \Sigma \varphi(d),$$

résulte le développement suivant :

$$(8) \quad \varphi(1) \frac{x}{1-x} + \varphi(2) \frac{x^2}{1-x^2} + \varphi(3) \frac{x^3}{1-x^3} + \dots = x + 2x^2 + 5x^3 + \dots$$

Posons maintenant, quel que soit le nombre premier  $a$ ,  $f(a^n) = a^{n-1}(a-1)$ , il est clair que, d'après la formule (4), on aura

$$\theta(m) = a^n b^3 \dots = m, \quad \text{et} \quad f(m) = a^{n-1} b^{3-1} \dots (a-1)(b-1).$$

D'où, en se reportant à la formule (7),

$$\varphi(m) = a^{n-1} b^{3-1} \dots (\alpha-1)(\beta-1).$$

Telle est l'expression que je voulais déduire de la relation (7) (\*).

(\*) Depuis que cette note a été écrite, j'ai reconnu que la proposition attribuée à M. Dedekind appartenait en réalité à M. Liouville. (Voy. *Journal de math.*, 2<sup>e</sup> série, t. II, p. 410.)