NOUVELLES ANNALES DE MATHÉMATIQUES

LEBESGUE

Extrait des exercices d'analyse numérique

Nouvelles annales de mathématiques 1re série, tome 8 (1849), p. 347-353

<http://www.numdam.org/item?id=NAM_1849_1_8__347_1>

EXTRAIT DES EXERCICES D'ANALYSE NUMÉRIQUE;

PAR M. LEBESGUE.

Dans un premier extrait (p. 87), j'ai pris un exemple propre à montrer qu'en développant un peu plus l'analyse indéterminée du premier degré, on simplifierait, quant aux démonstrations, l'analyse indéterminée du second degré.

Dans ce second extrait, je prendrai un exemple montrant l'usage de la théorie des nombres dans l'algèbre supérieure.

PROBLÈME. *Soient* $a, b, c, \ldots, k$ *des nombres premiers*

diviseurs de n, on demande combien de 1 *à n il y a de nombres premiers à* $a, b, c, \ldots, k$.

Solution. De 1 à a il y a $a-1$ nombres premiers à a; ce sont $1, 2, 3 \ldots a-1$; il y en a autant de a à $2a$, de $2a$ à $3a$, et généralement de ma à $(m+1)a$, car, pour que $ma+r\,(r<a)$ soit premier à a, il faut et il suffit que r le soit. Ainsi, puisque $n=\frac{n}{a}.a$, il y aura, de 1 à n, $\frac{n}{a}(a-1)$ nombres premiers à a. On les obtient en supprimant, dans la série $1, 2, 3 \ldots n$, tous les multiples de a.

Pour avoir les nombres premiers à a et b de 1 à n, il faut supprimer d'abord les multiples de a. On a vu qu'il reste $\frac{n}{a}(a-1)$ nombres; en supprimant les multiples de a on a, par là même, supprimé certains multiples de b de la suite $b, 2b, 3b, \ldots, hb, \ldots \frac{n}{b}.b$; mais on n'a pas supprimé ceux où le facteur h serait premier à a. Or de 1 à $\frac{n}{b}$ multiple de a, il y a $\frac{n}{ab}(a-1)$ nombres premiers à a; il faut donc diminuer $\frac{n}{a}(a-1)$ de $\frac{n}{ab}(a-1)$, et l'on aura $\frac{n}{ab}(a-1)(b-1)$, qui indiquera combien de 1 à n il y a de nombres premiers à a et b.

Pour avoir les nombres premiers à a, b et c, comme en supprimant les multiples de a et b on n'a supprimé qu'une partie des multiples de c, ou des nombres c, $2c, 3c, \ldots, \frac{n}{c}.c$; puisque $\frac{n}{c}$ est multiple de a et b, les multiples de c premiers à a et à b qui restent à supprimer sont en nombre $\frac{n}{abc}(a-1)(b-1)$, de sorte que la

différence

$$\frac{n}{ab}(a-1)(b-1) - \frac{n}{abc}(a-1)(b-1)$$
$$= \frac{n}{abc}(a-1)(b-1)(c-1)$$

indiquera combien de 1 à n il y a de nombres premiers à a, b, c diviseurs premiers de n.

En continuant de la même manière on trouvera, pour le nombre cherché,

$$\frac{n}{abc\ldots k}(a-1)(b-1)(c-1)\ldots(k-1).$$

PROBLEME. *Combien y a-t-il de nombres premiers à n et non plus grands?*

Solution. Soit $n = a^{\alpha} b^{\beta} c^{\gamma} \ldots m^{\mu}$; a, b, c, $\ldots$, m étant des nombres premiers différents, tout nombre premier à n doit nécessairement l'être aux nombres a, b, c, $\ldots$, m; et, réciproquement, tout nombre premier à chacun des nombres a, b, c, $\ldots$, m est premier à n. Il suit donc du problème précédent que le nombre cherché est

$$\frac{n}{abc\ldots m}(a-1)(b-1)(c-1)\ldots(m-1),$$

ou encore

$$n \cdot \frac{a-1}{a} \cdot \frac{b-1}{b} \cdot \frac{c-1}{c} \cdots \frac{m-1}{m}.$$

Remarque. Ce nombre est souvent représenté par $\varphi(n)$; on a donc

$$\varphi(a^{\alpha}) = a^{\alpha-1}(a-1),$$
$$\varphi(a^{\alpha} b^{\beta}) = a^{\alpha-1}(a-1)\, b^{\beta-1}(b-1) = \varphi(a^{\alpha})\,\varphi(b^{\beta}),$$

de même

$$\varphi(a^{\alpha} b^{\beta} c^{\gamma}) = \varphi(a^{\alpha}) . \varphi(b^{\beta}) . \varphi(c^{\gamma}),$$

et ainsi de suite.

Plus généralement, si m et n sont premiers entre eux, on aura

$$\varphi(m\ n) = \varphi(m) . \varphi(n);$$

propositions qu'il est facile de résoudre à priori.

Problème. *Trouver le plus petit multiple de plusieurs nombres donnés* $a, b, c, \ldots, k$.

On connaît deux solutions . l'une qui se tire de la décomposition des nombres $a, b, c, \ldots, k$ en facteurs premiers ; l'autre qui se déduit de cette proposition : « Le » plus petit multiple des nombres a et b est égal à leur » produit ab divisé par leur plus grand commun divi- » seur (ab). » Cette proposition peut être généralisée ainsi qu'il suit :

« Soit p_1 le produit des nombres $a, b, c, \ldots, k$; p_2 le » produit $(ab)\,(ac)\ldots(bc)\ldots$ des plus grands communs » diviseurs des nombres $a, b, \ldots, k$ pris deux à deux; » p_3 le produit des plus grands communs diviseurs des » nombres pris trois à trois, et ainsi de suite, jusqu'à ce » que l'on prenne tous les nombres; ce qui donne un » seul plus grand commun diviseur : le plus petit multiple » cherché sera

$$\frac{p_1 . p_3 . p_5 . \ldots}{p_2 . p_4 . p_6 \ldots} = \mathrm{M}$$

Soit θ un quelconque des nombres premiers, diviseur d'un des nombres $a, b, c, \ldots, k$. Comme l'ordre des nombres $a, b, c, \ldots, k$ est indifférent, on peut supposer que θ entre dans ces nombres avec les exposants $\alpha, \beta, \gamma, \ldots$ rangés par ordre de grandeur décroissante Il suit de là

que l'exposant de θ sera

$$\begin{aligned} &\alpha+\beta+\gamma+\delta+\ldots \text{ dans } p_1,\\ &\beta+2\gamma+3\delta+\ldots \text{ dans } p_2,\\ &\gamma+3\delta+\ldots \text{ dans } p_3,\\ &\delta+\ldots \text{ dans } p_4, \end{aligned}$$

et ainsi de suite, de sorte que dans $\frac{p_1 \cdot p_3 \cdot p_5 \cdots}{p_2 \cdot p_4 \cdot p_6 \cdots}$ l'exposant sera

$$\alpha+(1-1)\beta+(1-1)^2\gamma+(1-1)^3\delta+\ldots=\alpha.$$

D'ailleurs, le nombre M ne peut contenir que les diviseurs premiers de $a, b, c, \ldots, k$, et il les contient avec leur exposant maximum. M est donc le plus petit multiple demandé.

Application à l'algèbre.

Quand on aura décomposé un polynôme

$$P = x^n + ax^{n-1} + \ldots + px + q$$

en facteurs du premier degré

$$P = (x-\alpha)(x-\beta)(x-\gamma)\ldots,$$

on appellera P un polynôme composé de binômes simples, et tous les théorèmes sur la décomposition des nombres en facteurs premiers s'étendront aux polynômes. On pourra, par exemple, appliquer la règle précédente pour trouver le plus petit multiple de plusieurs polynômes.

Ceci posé, proposons-nous cette question :

PROBLÈME. *Trouver l'équation aux racines primitives de l'équation binôme* $x^m-1=0$.

On sait que r étant racine de $x^m-1=0$, il en est de

même de $r, r^2, r^3, \ldots, r^m - 1$. Une racine est dite *primitive*, quand la série $r, r^2, \ldots, r^m$ est composée de m expressions différentes, qui sont, par conséquent, les m racines. Y a-t-il des racines primitives? Combien y en a-t-il? La solution du problème précédent répondra à ces questions.

1°. Si r est une racine dans la série $1, r, r^2, \ldots$, le premier terme qui se répétera sera l'unité. Si l'on avait, par exemple, $r^\alpha = r^{\alpha+\beta}$, il en résulterait $r^\beta = 1$; donc l'unité se répète avant qu'on soit parvenu à $r^{\alpha+\beta}$.

2°. La série $1, r, r^2, \ldots r^{\alpha-1}$, $r^\alpha = 1$ donne α diviseur de m.

Démonstration connue. Cela posé, soit $m = a^\alpha b^\beta c^\gamma \ldots$. Les racines non primitives satisferont à quelques-unes des équations

$$x^{\frac{m}{a}} - 1 = 0, \quad x^{\frac{m}{b}} - 1 = 0, \quad x^{\frac{m}{c}} - 1 = 0, \quad \ldots,$$

qui ont toutes leurs racines communes avec

$$x^m - 1 = \left(x^{\frac{m}{a}}\right)^a - 1 = 0. \ \ldots$$

Il suffira donc de diviser $x^m - 1$ par le plus petit multiple des polynômes $x^{\frac{m}{a}} - 1$, $x^{\frac{m}{b}} - 1$, $x^{\frac{m}{c}} - 1$, etc. Or l'algèbre montre que le plus grand commun diviseur des polynômes $x^f - 1$, $x^g - 1$ est $x^{(fg)} - 1$, (fg) étant le plus grand commun diviseur des nombres f et g. Le quotient égalé à zéro sera l'équation aux racines primitives. Cette équation sera donc

$$\frac{(x^m-1)\times\left(x^{\frac{m}{ab}}-1\right)\left(x^{\frac{m}{ac}}-1\right)\ldots\times\left(x^{\frac{m}{abcd}}-1\right)\ldots}{\left(x^{\frac{m}{a}}-1\right)\left(x^{\frac{m}{b}}-1\right)\ldots\times\left(x^{\frac{m}{abc}}-1\right)\ldots} = 0,$$

et aura pour degré

$$m - m\left(\frac{1}{a}+\frac{1}{b}+\ldots\right)+m\left(\frac{1}{ab}+\frac{1}{ac}+\ldots\right)-m\left(\frac{1}{abc}\ldots\right)\ldots$$
$$= m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots$$
$$= m\,\frac{a-1}{a}\cdot\frac{b-1}{b}\cdot\frac{c-1}{c}\ldots = \varphi(m).$$

Il y a donc autant de racines primitives que de nombres premiers à m. C'est ce qu'il est facile de prouver sans passer par l'équation précédente.

On sait, en effet, que $x^m - 1 = 0$ est satisfaite par

$$x = \cos\frac{2\pi}{m} + \sin\frac{2\pi}{m}\sqrt{-1},$$

et comme

$$\left(\cos\frac{2\pi}{m} + \sin\frac{2\pi}{m}\sqrt{-1}\right)^t = \cos\frac{2\pi t}{m} + \sin\frac{2\pi t}{m}\sqrt{-1},$$

on reconnaît tout de suite que $\cos\frac{2\pi}{m} + \sin\frac{2\pi}{m}\sqrt{-1}$ est racine primitive. La formule des racines est donc

$$\cos\frac{2t\pi}{m} + \sin\frac{2t\pi}{m}\sqrt{-1}.$$

Il en est de même pour $\cos\frac{2h\pi}{m} + \sin\frac{2h\pi}{m}\sqrt{-1}$, si h est un nombre déterminé premier à m; mais cette racine ne serait pas primitive si h n'était pas premier à m. Chacun développera facilement ces propositions.

On peut consulter, à ce sujet, les *Exercices d'Analyse et de Physique mathématique*, de M. Cauchy, 1829.

La méthode donnée plus haut s'étend à l'équation $x^m - 1 = py$, le nombre p étant premier. C'est en cela, surtout, que consiste son utilité.