

G. MÉTROD

Démonstration de la formule de l'indicateur

Nouvelles annales de mathématiques 5^e série, tome 2
(1923), p. 378-383

http://www.numdam.org/item?id=NAM_1923_5_2__378_0

© Nouvelles annales de mathématiques, 1923, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » 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/>

[12c]

DÉMONSTRATION DE LA FORMULE DE L'INDICATEUR ;

PAR G. MÉTROD.

1. Dans la démonstration habituelle de la formule qui donne le nombre $\varphi(m)$ des entiers premiers avec l'entier m et non supérieurs à m , on part d'un système complet (mod m) dans lequel on supprime les entiers non premiers avec m .

On peut appliquer la méthode inverse, c'est-à-dire former directement le système des entiers premiers avec m ; on obtient ainsi une démonstration simple de la formule de l'indicateur de m .

2. Soit p^α une puissance du nombre premier p . Dans le système de numération de base p , tout entier inférieur à p^α peut s'écrire sous la forme

$$x_{\alpha-1}p^{\alpha-1} + x_{\alpha-2}p^{\alpha-2} + \dots + p x_1 + x_0,$$

dans laquelle les x sont des entiers égaux à $p - 1$ au plus. Quand on donne aux x toutes les valeurs entières de 0 à $p - 1$, l'expression précédente parcourt l'ensemble des p^α nombres inférieurs à p^α .

Parmi ces nombres, ceux qui sont premiers avec p sont ceux pour lesquels x_0 n'est pas nul; leur nombre est donc

$$\varphi(p^\alpha) = p^{\alpha-1}(p - 1).$$

3. Soit maintenant un entier quelconque m décomposé en ses facteurs premiers, dont le nombre est ν :

$$m = a^\alpha b^\beta \dots l^\lambda.$$

Considérons l'expression

$$\frac{m}{a^\alpha} x_1 + \frac{m}{b^\beta} x_2 + \dots + \frac{m}{l^\lambda} x_v;$$

si x_1 parcourt un système complet (mod a^α), x_2 un système complet (mod b^β), ..., x_v un système complet (mod l^λ), l'expression prend m valeurs formant un système complet (mod m).

En effet l'expression considérée ne peut être congrue à 0 (mod m) que si elle est congrue à 0 suivant chacun des modules a^α , b^β , ..., l^λ ce qui exige

$$\begin{aligned} x_1 &\equiv 0 \pmod{a^\alpha}, \\ x_2 &\equiv 0 \pmod{b^\beta}, \\ &\dots\dots\dots \\ x_v &\equiv 0 \pmod{l^\lambda}. \end{aligned}$$

Pour qu'un entier soit premier avec m il faut et il suffit qu'il soit premier séparément avec a^α , b^β , ..., l^λ , c'est-à-dire que x_1 soit premier avec a^α , x_2 avec b^β , ..., x_v avec l^λ . On obtient donc un système complet de nombres premiers avec m en faisant parcourir à x_1 un système complet de nombres premiers avec a^α , à x_2 un système complet de nombres premiers avec b^β , ..., à x_v un système complet de nombres premiers avec l^λ .

On a donc

$$\begin{aligned} \varphi(m) &= \varphi(a^\alpha) \varphi(b^\beta) \dots \varphi(l^\lambda), \\ &= m \left(1 - \frac{1}{a}\right) \left(1 - \frac{1}{b}\right) \dots \left(1 - \frac{1}{l}\right). \end{aligned}$$

4. La méthode peut être généralisée pour calculer l'indicateur de $k^{\text{ième}}$ ordre. On sait qu'on appelle indicateur de $k^{\text{ième}}$ ordre de l'entier m le nombre des arrangements k à k avec répétition des entiers 0, 1, ..., $m-1$ tels que ces k entiers et m soient premiers dans leur ensemble.

Considérons d'abord le cas d'une puissance p^α d'un nombre premier p . Un système de k entiers inférieurs à p^α peut être représenté par les k expressions

$$p^{\alpha-1} x_{\alpha-1}^{(1)} + p^{\alpha-2} x_{\alpha-2}^{(1)} + \dots + p x_1^{(1)} + x_0^{(1)}.$$

$$\dots \dots \dots$$

$$p^{\alpha-1} x_{\alpha-1}^{(k)} + p^{\alpha-2} x_{\alpha-2}^{(k)} + \dots + p x_1^{(k)} + x_0^{(k)},$$

dans lesquelles les x sont au moins 0 et au plus $p - 1$.

Les x parcourant séparément les entiers de 0 à $p-1$, ces expressions engendrent les $p^{\alpha k}$ systèmes de k entiers (mod p^{α}).

Pour que le plus grand commun diviseur des entiers d'un tel système soit premier avec p^α il faut et il suffit que les nombres x_0 ne soient pas tous nuls.

On a donc pour l'indicateur de k^{ieme} ordre la formule

$$\varphi_h(p^\alpha) = p^{(\alpha-1)h} (p^h - 1)$$

ou

$$\varphi_k(p^{\alpha}) = p^{\alpha} \left(1 - \frac{1}{p^k} \right).$$

3. Soit maintenant

$$m = a^\alpha b^\beta \dots l^\lambda.$$

Le nombre des arrangements complets k à k des entiers d'un système complet (mod m) est m^k . L'un quelconque de ces arrangements est représenté par les k expressions

$$\begin{aligned} & \frac{m}{\alpha^{\lambda}} x_1^{(1)} + \frac{m}{b^{\beta}} x_2^{(1)} + \dots + \frac{m}{l^{\lambda}} x_y^{(1)}, \\ & \dots\dots\dots, \\ & \frac{m}{\alpha^x} x_1^{(k)} + \frac{m}{b^{\beta}} x_2^{(k)} + \dots + \frac{m}{l^{\lambda}} x_y^{(k)}. \end{aligned}$$

Si les x_1 parcourent séparément un système complet $(\text{mod } a^x)$, les x_2 un système complet $(\text{mod } b^y)$, ...,

les x_i un système complet (mod l^k), l'ensemble des k expressions précédentes parcourt tous les arrangements complets k à k d'un système complet (mod m).

Pour que le plus grand commun diviseur d'un système de k entiers soit premier avec m , il faut et il suffit qu'il le soit avec $a^\alpha, b^\beta, \dots, l^\lambda$. Un système de k entiers possède cette propriété lorsque les x_i forment un système de k entiers dont le plus grand commun diviseur est premier avec $a^\alpha, \dots, l^\lambda$, les x_i un système de k entiers dont le plus grand commun diviseur est premier avec l .

On a donc pour l'indicateur de $k^{\text{ième}}$ ordre

$$\begin{aligned} \varphi_k(m) &= \varphi_k(a^\alpha) \varphi_k(b^\beta) \dots \varphi_k(l^\lambda) \\ &= m^k \left(1 - \frac{1}{a^\alpha}\right) \left(1 - \frac{1}{b^\beta}\right) \dots \left(1 - \frac{1}{l^\lambda}\right). \end{aligned}$$

6. La méthode peut aussi s'appliquer à la théorie des entiers et des idéaux d'un corps algébrique.

Soient P un idéal premier d'un corps algébrique, p un entier de ce corps divisible par P mais non par P^2 , l'expression

$$p^{\alpha-1} x_{\alpha-1} + p^{\alpha-2} x_{\alpha-2} + \dots + p x_1 + x_0$$

parcourt un système complet (mod P^α) lorsque les x parcourent séparément un système complet (mod P). On s'en assure en observant que l'expression ne peut être congrue à 0 que si tous les x sont congrus à 0 (mod P).

D'autre part, soit M un idéal composé

$$M = A^\alpha B^\beta \dots L^\lambda,$$

$A, B, \dots, L$ étant des idéaux premiers. Choisissons dans le corps algébrique un entier a divisible par A

mais non par A^2 et premier avec $\frac{M}{A^\alpha}$; un entier b divisible par B mais non par B^2 et premier avec $\frac{M}{B^\beta}$; ...; un entier l divisible par L mais non par L^2 et premier avec $\frac{M}{L^\lambda}$; puis posons

$$m = \alpha^\alpha b^\beta \dots l^\lambda.$$

Cet entier m est divisible par l'idéal M et le quotient $\frac{m}{M}$ est premier avec M .

On voit alors que l'expression

$$\frac{m}{\alpha^\alpha} x_1 + \frac{m}{b^\beta} x_2 + \dots + \frac{m}{l^\lambda} x_\nu$$

donne un système complet (mod M) lorsque x_1 parcourt un système complet (mod A^α), x_2 un système complet (mod B^β), ..., x_ν un système complet (mod L^λ). La démonstration se continue ensuite comme dans les nos 2 et 3. On raisonne de même pour l'indicateur de k^{iem} ordre.

7. La méthode que j'indique peut encore servir à résoudre d'autres questions analogues, par exemple la suivante qui constitue une extension de la notion de l'indicateur (LUCAS, *Théorie des nombres*, n° 221).

Trouver le nombre des entiers h de la suite

$$0, 1, 2, \dots, m-1$$

tels que

$$h - e_1, \quad h - e_2, \quad \dots, \quad h - e_k$$

soient premiers avec m ; $e_1, e_2, \dots, e_k$ étant des entiers donnés.

On trouvera facilement que ce nombre est :

$$m \left(1 - \frac{\mu_1}{a} \right) \left(1 - \frac{\mu_2}{b} \right) \dots \left(1 - \frac{\mu_\nu}{l} \right),$$

$a, b, \dots, l$ étant les facteurs premiers de m ; μ_1 le nombre des entiers e différents (mod a), μ_2 le nombre des entiers e différents (mod b), $\dots$, μ_ν le nombre des entiers e différents (mod l).