NOUVELLES ANNALES DE MATHÉMATIQUES

LEBESGUE

Sur les racines primitives de l'équation $x^n - 1 = 0$

Nouvelles annales de mathématiques 1re série, tome 11 (1852), p. 417-424

<http://www.numdam.org/item?id=NAM_1852_1_11__417_0>

SUR LES RACINES PRIMITIVES DE L'ÉQUATION

$$x^n - 1 = 0;$$

PAR M. LEBESGUE.

1. L'équation

$$x^n = 1 \tag{1}$$

a n racines données par la formule

$$x_i = \cos\frac{2i\pi}{n} + \sin\frac{2i\pi}{n}\sqrt{-1},$$

dans laquelle il faut faire successivement

$$i = 0,\ 1,\ 2,\ 3,\ \ldots,\ n-1.$$

On tire de là

$$x_i^k = \cos\frac{ik}{n}2\pi + \sin\frac{ik}{n}2\pi\sqrt{-1}.$$

Pour réduire x_i^k à l'unité, il faut rendre $\frac{ik}{n}$ entier ; d'où il suit qu'en prenant d pour plus grand commun diviseur de i et n, il faut que k soit multiple de $\frac{n}{d}$. La plus petite valeur de k est donc $\frac{n}{d}$. On dit que la racine x_i *appartient* à l'exposant $\frac{n}{d}$.

Les racines primitives sont celles qui appartiennent à l'exposant n; il y en a autant que de nombres premiers à n et moindres que n; représentons ce nombre de nombres premiers à n par $\varphi(n)$.

2. Soit $n = a^\alpha b^\beta c^\gamma \ldots$, a, b, c, $\ldots$ étant des nombres premiers différents ; les racines non primitives de $x^n = 1$

appartiennent nécessairement à un exposant diviseur d'un des nombres $\frac{n}{a}$, $\frac{n}{b}$, $\frac{n}{c}$, ...

De sorte que, si l'on cherchait le plus petit multiple des binômes $x^{\frac{n}{a}} - 1$, $x^{\frac{n}{b}} - 1$, $x^{\frac{n}{c}} - 1$, ..., ce plus petit multiple étant X, l'équation aux racines primitives serait

$$\frac{x^n - 1}{X} = 0,$$

équation du degré $\varphi(n)$, ayant pour racines précisément toutes les racines primitives de $x^n = 1$.

Quant à la règle pour trouver le plus petit multiple de plusieurs fonctions entières $f(x)$, $F(x)$, etc., elle est précisément la même que celle qui sert à trouver le plus petit multiple de plusieurs nombres entiers. Je l'ai donnée et démontrée au commencement de l'année 1829, à peu près comme le fait ci-dessus M. Serret (*Bulletin du Nord*, journal scientifique publié à Moscou); j'ai rappelé ce théorème et son application à la recherche de l'équation aux racines primitives dans mes Recherches sur les nombres (*Journal de Mathématiques*, tome II, page 258).

Si l'on observe que $x^{\frac{n}{a}} - 1$, $x^{\frac{n}{b}} - 1$ ont $x^{\frac{n}{ab}} - 1$ pour plus grand commun diviseur, que $x^{\frac{n}{a}} - 1$, $x^{\frac{n}{b}} - 1$, $x^{\frac{n}{c}} - 1$ ont $x^{\frac{n}{abc}} - 1$ pour plus grand commun diviseur, et ainsi des autres; en posant

$$\Pi_1 = \Pi\left(x^{\frac{n}{a}} - 1\right) = \left(x^{\frac{n}{a}} - 1\right)\left(x^{\frac{n}{b}} - 1\right)\left(x^{\frac{n}{c}} - 1\right)\ldots,$$

$$\Pi_2 = \Pi\left(x^{\frac{n}{ab}} - 1\right) = \left(x^{\frac{n}{ab}} - 1\right)\left(x^{\frac{n}{ac}} - 1\right)\ldots\left(x^{\frac{n}{bc}} - 1\right)\ldots,$$

$$\Pi_3 = \Pi\left(x^{\frac{n}{abc}} - 1\right) = \left(x^{\frac{n}{abc}} - 1\right)\ldots\left(x^{\frac{n}{bcd}} - 1\right)\ldots,$$

.....

en prenant pour dénominateur de n dans Π_1 les nombres a, b, c, ..., dans Π_2 les combinaisons deux à deux, ou plutôt les produits ab, ac, ..., dans Π_3 les combinaisons ou produits trois à trois, tels que abc, abd, ..., le plus petit multiple des binômes $x^{\frac{n}{a}}-1$, $x^{\frac{n}{b}}-1$, ..., sera

$$X=\frac{\Pi_1.\Pi_3.\Pi_5\ldots}{\Pi_2.\Pi_4.\Pi_6\ldots},$$

et, par suite, l'équation aux racines primitives sera

$$(2)\quad \varphi_n(x)=\frac{(x^n-1).\Pi\left(x^{\frac{n}{ab}}-1\right).\Pi\left(x^{\frac{n}{abcd}}-1\right)\ldots}{\Pi\left(x^{\frac{n}{a}}-1\right).\Pi\left(x^{\frac{n}{abc}}-1\right)\ldots}=0\ (*).$$

Cette équation a été aussi donnée par M. Cauchy, en 1826, dans ses *Exercices de Mathématiques*.

3. Les remarques suivantes facilitent le calcul de la fonction $\varphi_n(x)$. Il suffit de les énoncer, la démonstration étant sans difficulté :

1°.
$$\varphi_{a^\alpha}(x)=\frac{x^{a^\alpha}-1}{x^{a^{\alpha-1}}-1}=x^{a^{\alpha-1}(a-1)}+x^{a^{\alpha-1}(a-2)}+\ldots+x^{a^{\alpha-1}}+1;$$

2°.
$$\varphi_{a^\alpha b^\beta}(x)=\frac{\varphi_{a^\alpha}\left(x^{b^\beta}\right)}{\varphi_{a^\alpha}\left(x^{b^{\beta-1}}\right)}=\frac{\varphi_{b^\beta}\left(x^{a^\alpha}\right)}{\varphi_{b^\beta}\left(x^{a^{\alpha-1}}\right)};$$

3°.
$$\varphi_{a^\alpha b^\beta c^\gamma}(x)=\frac{\varphi_{a^\alpha b^\beta}\left(x^{c^\gamma}\right)}{\varphi_{a^\alpha b^\beta}\left(x^{c^{\gamma-1}}\right)};\ \text{etc.}$$

(*) On lit en plusieurs endroits que l'equation aux racines primitives est irréductible ; la demonstration est bien connue pour le cas de n premier ou de $x^n=1$; $x^{n-1}+x^{n-2}+\ldots+x+1=0$ est alors l'équation aux racines primitives.

Il serait bon d'indiquer d'une manière précise la démonstration générale relative au cas de n nombre compose

et ainsi de suite,

$$4^{\circ}. \quad \varphi_{a^{\alpha}b^{\beta}c^{\gamma}}(x) = \varphi_{abc\ldots}\left(a^{\alpha-1}.b^{\beta-1}.c^{\gamma-1}\ldots\right);$$

5°. Pour $n = 2m$,

$$\frac{(x^m+1).\Pi\left(x^{\frac{m}{ab}}+1\right)\Pi\left(x^{\frac{m}{abcd}}+1\right)\ldots}{\Pi\left(x^{\frac{m}{a}}+1\right)\Pi\left(x^{\frac{m}{abc}}+1\right)\ldots} = 0, \quad n = 2^{\lambda}a^{\alpha}b^{\beta}c^{\gamma}\ldots.$$

Cette dernière s'obtient au moyen de

$$\frac{x^{2k}-1}{x^k-1} = x^k+1.$$

Sur les racines primitives de l'équation $x^{p-1}-1 = py$, *le nombre p supposé premier.*

4. Cette équation est satisfaite par $x = 1, 2, 3, \ldots, p-1$. Si la racine a est telle que a^k-1 soit la moindre puissance de a, qui, diminuée de l'unité, donne un reste divisible par p, la racine a appartiendra à l'exposant k, diviseur de $p-1$. Les *racines primitives* sont celles qui appartiennent à l'exposant $p-1$.

L'équation aux racines primitives est

$$\varphi_{p-1}(x) = py,$$

la fonction $\varphi_{p-1}(x)$ étant formée comme il a été dit plus haut. La démonstration s'établit facilement au moyen des propriétés communes aux équations

$$x^{p-1}-1 = 0, \quad x^{p-1}-1 = py.$$

Ces propositions d'algèbre supérieure, ces curiosités de la science, si l'on veut, n'appartenant point à l'enseignement des lycées, devraient naturellement trouver leur place dans l'enseignement des facultés; car l'expérience a prouvé que les curiosités de la science en deviennent assez souvent un jour des nécessités.

Les Tables de racines primitives, ou plutôt les Tables

d'indices correspondant aux nombres, et de nombres correspondant aux indices, pour un nombre premier donné, sont tellement utiles pour la résolution des équations numériques indéterminées, que l'illustre Jacobi s'est occupé de leur formation. Ces Tables ont été publiées à Berlin (*Impensis Academiæ litterarum regiæ Borussiæ*) (*).

Dans un ouvrage assez récent, M. Desmarest a donné quelques règles pour trouver, presque sans calcul, une racine primitive pour certaines classes de nombres premiers. Il est fâcheux que son ouvrage renferme, au sujet des *Recherches arithmétiques* de M. Gauss, des assertions qui ne seront point acceptées par ceux qui auront lu avec attention cet ouvrage si justement célèbre.

Pour démontrer ces règles, il suffit de se rappeler les théorèmes suivants :

I. *L'équation* $x^{\frac{p-1}{2}} + 1 = py$ *est l'équation aux non-résidus quadratiques.*

II. *Si* $p = 4q + 1$, -1 *est résidu quadratique ;*
Si $p = 4q + 3$, -1 *est non-résidu quadratique ;*
Si $p = 8k \pm 1$, 2 *est résidu quadratique ;*
Si $p = 8k \pm 3$, 2 *est non-résidu quadratique.*

III. *Si p est résidu quadratique de q, q sera résidu quadratique de p ;*

Si p est non-résidu quadratique de q, q sera non-résidu quadratique de p.

On suppose ici p et q premiers impairs, l'un au moins étant de forme $4k + 1$.

IV. *Les nombres premiers p et q étant tous deux de forme* $4k + 3$,

---

(*) L'arithmologie a subi une nouvelle perte, cruelle, irréparable. EISENTEIN est mort, jeune d'années, vétéran de la science Nous y reviendrons.

Si p est résidu quadratique de q, q sera non-résidu quadratique de p, et réciproquement.

Ceci posé, on a ces théorèmes :

A. *Si $p = 2^t + 1$ est premier, tout non-résidu est racine primitive.* 3 *est toujours racine primitive.*

L'équation aux racines primitives est

$$x^{2^{t-1}} + 1 = py,$$

qui est aussi l'équation aux non-résidus

$$p = (3 - 1)^t + 1 = 3k + 2,$$

car

$$t = 2^m;$$

donc p non-résidu de 3, et 3 non-résidu de p.

B. *Si $p = 2^t a + 1$, l'équation aux racines primitives est*

$$\frac{x^{2^{t-1}a} + 1}{x^{2^{i-1}} + 1} = py;$$

les non-résidus sont racines primitives, en exceptant seulement ceux qui donneraient

$$x^{2^{i-1}} + 1 = py.$$

Application :

$$t = 1, \quad p = 2a + 1.$$

Tous les non-résidus sont racines primitives, sauf -1, qui satisfait à l'équation

$$x + 1 = py.$$

Pour

$$a = 4k + 1, \quad p = 8k + 3,$$

2 est non-résidu et racine primitive.

Pour

$$a = 4k + 3, \quad p = 8k + 7,$$

-2 est racine primitive.

Pour

$$t = 2, \quad p = 4a + 1,$$

$a = 2k + 1$ donnant

$$p = 8k + 5,$$

2 est racine primitive.

Si

$$2^2 + 1 = 5 = py,$$

il y a exception; cela arrive pour

$$p = 5;$$

si

$$i = 3, \quad p = 8a + 1;$$

pour

$$a = 3, \quad a = 6k + 1,$$

p n'est plus nombre premier; pour

$$a = 6k - 1, \quad p = 3k + 2 = (48k - 7),$$

p étant non-résidu de 3, 3 sera non-résidu de p, et, par suite, racine primitive; à moins que l'on n'ait

$$3^4 + 1 = 82 = 2.41 = py,$$

l'exception tombe sur

$$p = 41.$$

Il serait facile de multiplier les exemples.

Le théorème A est de M. Richelot. Les théorèmes pour

$$p = 2a + 1,$$

ou d'autres analogues, ont été donnés par M. Proubet; les autres se trouvent dans l'ouvrage de M. Desmarest. Bien que je n'aie plus cet ouvrage entre les mains, je crois pouvoir assurer que la marche ici tracée peut faire trouver les règles que l'auteur y a données, et bien d'autres de même nature. On détermine un non-résidu quadratique du nombre premier p, et l'on fait voir qu'il est racine de l'équation aux racines primitives. Soient

$$R = py$$

l'équation aux racines primitives,

$$N = py$$

l'équation aux non-résidus quadratiques ; on a

$$N = RQ.$$

Le non-résidu n, qui est racine de $N = py$, le sera aussi de $R = py$, si $Q = py$ n'a pas n pour racine.