44.

SUR LES DIVISEURS DES FONCTIONS CYCLOTOMIQUES.

[*Comptes Rendus*, XC. (1880), pp. 287—289, 345—347.]

SOIT k un nombre quelconque ; formons la série

$$\cos \lambda_1 \frac{2\pi}{k}, \quad \cos \lambda_2 \frac{2\pi}{k}, \quad \ldots, \quad \cos \lambda_i \frac{2\pi}{k},$$

$\lambda_1, \lambda_2, \ldots, \lambda_i$ étant les $\frac{1}{2}\phi(k)$ nombres premiers à k et moindres que $\frac{1}{2}k$. Le produit de tous les facteurs $x - 2\cos\lambda\frac{2\pi}{k}$ est ce que l'on nomme une *fonction cyclotomique*, et k sera nommé son indice. En effet, la fonction cyclotomique en x à l'indice k est ce que devient le facteur primitif de $t^k - 1$ quand on le divise par $t^{\frac{1}{2}\phi(k)}$ et que l'on écrit $t + t^{-1} = x$. A l'indice 1 ou 2 ne correspond aucune fonction cyclotomique, et pour les indices 3, 4, 6, la fonction cyclotomique est linéaire, et conséquemment ne peut posséder aucune propriété arithmétique.

Je distingue les diviseurs de ces fonctions en deux classes. Les nombres qui divisent la fonction sans diviser l'indice se nomment *diviseurs extérieurs* ou *extrinsèques*, ceux qui divisent en même temps une fonction et son indice se nomment *diviseurs intérieurs* ou *intrinsèques*.

Voici les théorèmes que j'ai réussis à établir concernant ces diviseurs.

Quant à la première classe, je démontre :

1°. Que tout nombre dont les facteurs premiers diminués ou augmentés de l'unité sont divisibles par l'indice d'une fonction cyclotomique est diviseur de cette fonction. Je fais dépendre la démonstration de cette proposition du théorème suivant, qui est, pour ainsi dire, la clef de la théorie entière :

En posant $\quad J(\cos\vartheta) = \cos(p^i\vartheta) - \cos(p^{i-1}\vartheta),$

$J(\cos\vartheta)$, *regardé comme fonction algébrique de* $\cos\vartheta$, *est divisible par* p^i *pour toute valeur réelle et entière attribuée à* $\cos\vartheta$.

La proposition précédente est une conséquence immédiate de ce théorème, quand on met $2\cos\vartheta = x$ et qu'on substitue, pour la congruence

$$J(\cos\vartheta) \equiv 0 \quad [\text{mod. } p^i],$$

la congruence équivalente

$$(t^{p^i-p^{i-1}} - 1)(t^{p^i+p^{i-1}} - 1) \equiv 0 \quad [\text{mod. } p^i];$$

de sorte que, a étant un nombre réel quelconque, il faut que l'un ou l'autre des deux facteurs $a^{p^i-p^{i-1}} - 1$, $a^{p^i+p^{i-1}} - 1$ soit toujours divisible par p^i, car, si les deux facteurs contenaient p, on aurait $a^{2p^i} - 1$ divisible par p; c'est-à-dire, puisque $2p^i = 2 + \left(2\frac{p^i-1}{p-1}\right)(p-1)$, $a^2 - 1$ serait divisible par p, et conséquemment $a = \pm 1 + \lambda p$, auquel cas $a^{p^{i-1}} \equiv (\pm 1)$ mod. p^i, et les deux facteurs deviennent respectivement congrus à $(\pm 1)^{p^i \pm p^{i-1}} - 1$, c'est-à-dire tous les deux congrus à zéro par rapport à ce module, et par conséquent tous les deux divisibles par p^i et congrus à zéro. Avec l'exception de ces valeurs de a, c'est toujours l'un des deux facteurs exclusivement qui s'évanouit pour une valeur donnée de a.

2°. Je démontre, à l'aide du même théorème de forme trigonométrique, mais en faisant $i = 1$, que si un diviseur extérieur d'une fonction cyclotomique, disons ψ_k, est de la forme $mk \pm e$, k étant son indice, la congruence

$$\psi_k \equiv 0 \quad [\text{mod. } mk \pm e]$$

aura deux racines congrues l'une à l'autre, à moins que $e = 1$. On prouve facilement que cette équivalence est impossible avec l'aide du petit principe additionnel que, si ψ est congru à zéro selon un module quelconque, $\frac{d\psi}{dx}$ sera congru à zéro selon le même module.

Quant à la seconde classe des diviseurs, je démontre que, laissant à part les fonctions cyclotomiques linéaires $x+1$, x, $x-1$ appartenant aux indices 3, 4, 6 et la fonction quadratique qui répond à l'indice 12, il n'y a *au plus* qu'*un seul* diviseur intérieur (un nombre premier); bien entendu, la première puissance seulement de ce nombre. J'ai déjà dit que, pour que p^j soit un diviseur extérieur, il faut et il suffit que $p = mk + \epsilon$, k étant l'indice et $\epsilon = \pm 1$. Or, pour que p soit diviseur intérieur de la fonction cyclotomique à l'indice k, je démontre qu'il faut et qu'il suffit que k soit de la forme

$$\frac{p-\epsilon}{m} p^j.$$

En général, il n'y a *au plus* qu'une seule manière de mettre un indice k, donné sous la forme qui met en évidence un diviseur intérieur; mais, quand $k = 12$, on peut écrire $m = 1$, $j = 2$, $p = 2$, $\epsilon = -1$ ou bien $m = 1$, $j = 1$, $p = 3$, $\epsilon = -1$; c'est pourquoi ψ_{12} possède les *trois* diviseurs intérieurs 2, 3, 6. En démontrant que la condition donnée plus haut pour que p soit diviseur

intérieur est nécessaire et que la première puissance seulement de p est un diviseur de la fonction, je me sers du même théorème trigonométrique qu'auparavant et en même temps de la seconde proposition sur les facteurs extérieurs. Pour démontrer que cette condition est suffisante, j'ai recours à un théorème purement algébrique, savoir, que si $k = k_1 (mk_1 \pm 1)^j$, $mk_1 \pm 1$ étant un nombre premier p, le résultant des deux équations $\psi_k = 0$, $\psi_{k_1} = 0$ est égal à $p^{\frac{1}{2}\phi(k_1)}$, en me servant en même temps d'un second petit principe, qu'afin que deux congruences soient satisfaites simultanément par rapport au même module, le résultant algébrique de ces congruences transformées en équations doit être congru à zéro par rapport au module.

La fonction cyclotomique à l'indice 9, $x^3 - 3x + 1$, m'a amené à faire cette recherche ; car j'avais grandement besoin de démontrer apodictiquement (ce que j'avais établi par des épreuves numériques sans fin) que les diviseurs de cette fonction sont 3 et les nombres premiers de la forme $18n \pm 1$ exclusivement. C'est à l'aide de ce théorème que je démontre qu'aucun nombre A de la forme*

$$pq,\ p^2q^2,\ p_1p_2^2,\ q_1q_2^2;\quad 9pq,\ 9p^2q^2,\ 9p_1p_2^2,\ 9q_1q_2^2,$$

où chaque p désigne un nombre premier de la forme $18n - 5$ et chaque q un nombre premier de la forme $18n + 7$, ne peut être décomposé en une somme ou différence de deux cubes rationnels. En effet, je démontre facilement que, si cette décomposition était possible, l'équation

$$x^3 - 3xy^2 + y^3 = 3Az^3$$

serait résoluble en nombres entiers, ce qui est impossible, puisque $x^3 - 3x + 1$ ne contient aucun p ou q. La même équation, en mettant $A = 3$, devrait avoir lieu aussi si 3 était décomposable en deux cubes rationnels ; ainsi on voit (comme on sait déjà) que cette décomposition est impossible, puisque $x^3 - 3x + 1$ ne contient pas le diviseur intérieur 9.

Tout ce que j'ai pu trouver sur la question qui a fait le sujet de ma première Communication † est contenu dans le livre classique du professeur Bachmann, *Die Lehre von der Kreistheilung*‡, Leipzig, 1872, pp. 242, 243 ;

[* See below, p. 437.]

† *Comptes Rendus*, séance du 16 février [p. 428, above.]

‡ *Kreistheilung* = cyclotomie. La fonction à racines réelles qui sert à la division du cercle en parties égales est celle que j'ai nommée *fonction cyclotomique*. Il y a aussi des fonctions cyclotomiques à racines imaginaires ; je parle des facteurs primitifs de $x^k - 1$, qu'on pourrait nommer *fonctions cyclotomiques simples* ou *irréduites*, dont les diviseurs sont assujettis à des conditions parallèles, mais non identiques avec celles des fonctions cyclotomiques que j'ai traitées dans le texte. En effet, voici la règle pour les diviseurs des fonctions cyclotomiques non réduites. Afin qu'un nombre quelconque soit diviseur d'une fonction cyclotomique non réduite à l'indice k, il faut et il suffit que chaque facteur premier de ce diviseur soit de la forme $ki + 1$, avec exception d'un seul facteur premier p qui peut figurer aussi comme facteur du diviseur dans le cas, et

mais cela même ne me servait à rien, car cet excellent auteur s'est borné au cas où l'indice est un nombre premier, pour lequel cas il énonce et démontre " qu'en dehors des diviseurs premiers de la forme $2mp \pm 1$ " la fonction cyclotomique à l'indice p " contient seulement le diviseur premier p "; mais M. Bachmann n'a nullement démontré ni même affirmé, ce qui cependant est vrai, que tout nombre premier de la forme $2mp \pm 1$, et même un tel nombre élevé à une puissance quelconque *, est diviseur de la fonction cyclotomique à l'indice p.

Reste une remarque à faire. Si l'on prend le produit des facteurs $x - 2\cos\lambda\frac{2\pi}{k}y$, on obtient ce qu'on peut nommer une *forme* cyclotomique. Quand on prend l'indice égal à 5 ou à 10, à 8 ou à 12, de sorte que l'ordre de cette forme, disons $F(x, y)$, devient 2, si D est un diviseur quelconque de la fonction cyclotomique à ces indices, on sait, par la théorie ordinaire des

---

seulement dans le cas, que k admet de la représentation (nécessairement et sans exception unique) $\frac{p-1}{m}p^j$. Ainsi, si P, p désignent des nombres premiers, J, j des nombres indéfinis, et k l'indice d'une fonction cyclotomique de l'une ou de l'autre espèce, et si

$$P = mk + \epsilon \text{ et } k = \frac{p-\epsilon}{m}p^j,$$

P^J et p seront diviseurs de la fonction dans un cas et dans l'autre, avec la distinction que pour les fonctions cyclotomiques simples $\epsilon = 1$, tandis que pour les fonctions cyclotomiques à racines réelles $\epsilon = \pm 1$. En effet, le cours de la démonstration est précisément le même dans les deux cas, avec la seule exception que pour la première proposition, celle qui affirme que, p étant un nombre premier de la forme $mk+\epsilon$, p^j est diviseur de la fonction à indice k, pour les fonctions cyclotomiques d'une classe on se sert du théorème que la congruence $\cos p^j\vartheta - \cos p\vartheta \equiv 0$ [mod. p^j] a toutes ses racines réelles; pour les fonctions cyclotomiques de l'autre classe on se sert du théorème (mieux connu) que *la congruence*

$$x^{p^j} - x^{p^{j-1}} \equiv 0 \quad [\text{mod. } p^j]$$

a toutes ses racines réelles. Pour tout ce qui suit cette proposition, la méthode de démonstration pour les deux cas est absolument identique. Peut-être serait-il mieux de nommer les fonctions dont je parle spécialement dans le texte *fonctions cyclotomiques de la seconde*, et celles qui sont simplement facteurs primitifs de la forme binôme *fonctions cyclotomiques de la première espèce.* Il y a une raison qui me paraît assez grave pour ce changement de nomenclature, vu qu'il suggère l'idée d'une théorie de diviseurs des fonctions cyclotomiques dont le *rang de l'espèce* sera un nombre q quelconque, où figureront les racines $q^{\text{ièmes}}$ de l'unité, par rapport à l'indice comme module, de laquelle théorie je crois entrevoir assez distinctement et la haute probabilité de son existence et sa nature. J'espère développer cette théorie dans quelque futur Mémoire.

* Il est à peine nécessaire d'observer que la fonction cyclotomique de l'ordre ω [où $\omega = \frac{1}{2}\phi(k)$] étant divisible pour ω valeurs a de la variable incongrues par rapport à p^α, et ω autres valeurs b de la même variable incongrues par rapport à q^β, par p^α, q^β respectivement, on n'a qu'à combiner un a quelconque avec un b quelconque, et, en écrivant $p^\alpha u - a = t = q^\beta v - b$, on obtiendra une valeur réelle de t (et conséquemment ω valeurs réelles de t), qui substituée pour la variable rendra la fonction divisible par $p^\alpha q^\beta$; et de même on déduit que la fonction admettra comme diviseur un nombre quelconque dont les facteurs sont les nombres premiers de la forme $mk \pm 1$ accompagnés ou non (au choix) par le facteur intrinsèque, quand il y en a un, et par l'un ou l'autre ou tous les deux facteurs intrinsèques 2, 3, dans le cas où l'indice est le nombre 12.

formes quadratiques, qu'en écrivant $F(x, y) = Dz^2$ (les valeurs de F étant $x^2 \pm xy - y^2$, $x^2 - 2y^2$ ou $x^2 - 3y^2$), une telle équation est résoluble en nombres entiers.

Or une étude empirique très étendue sur le cas où l'indice est 9, qui mène à l'équation $x^3 - 3xy^2 + y^3 = Dz^3$, m'a donné lieu de croire qu'il y a une probabilité très considérable que cette équation est aussi toujours résoluble en nombres entiers. Si cela était établi, il deviendrait plus que probable que le théorème analogue est vrai pour toutes les formes cyclotomiques, et du cas de l'indice 9, si seulement la résolubilité de l'equation qui y appartient était démontrée, on tirerait la belle conséquence que tout nombre dont les facteurs premiers sont de la forme $18n \pm 1$, accompagné ou non accompagné (au choix) par le facteur 9, est décomposable en une somme de cubes de deux nombres rationnels. Car on démontre facilement qu'en substituant pour X, Y, Z, respectivement, certaines fonctions rationnelles et entières qu'on connaît, du neuvième degré en x, y, z, la fonction $X^3 + Y^3 + AZ^3$ contiendra

$$x^3 - 3xy^2 + y^3 - 3Az^3$$

comme facteur algébrique.

Voici, en quelques mots, le résumé des lois actuellement démontrées :

Tout diviseur de la fonction cyclotomique à l'indice k est de la forme $ik \pm 1$, excepté dans le cas que $k = \frac{p \mp 1}{m} p^j$, dans lequel cas p aussi (mais non pas p^2) sera un diviseur. Et réciproquement tout nombre dont les facteurs sont des puissances arbitraires de nombres premiers de la forme $ik \pm 1$ est diviseur de la fonction cyclotomique à l'indice k.

On peut y ajouter que, si l'ordre de la fonction cyclotomique [c'est-à-dire $\frac{1}{2}\phi(k)$] est nommé ω, et N un nombre quelconque qui ne divise pas k, il n'y aura aucune valeur ou ω valeurs de la variable, incongrues par rapport à N, qui rendront la fonction divisible par N. Mais si p, nombre premier, est un diviseur de k, le nombre des valeurs de la variable qui rendent la fonction divisible par p sera ou nul ou le quotient de k par la plus haute puissance qu'il contient de p.