57.

SUR LES DIVISEURS DES FONCTIONS DES PÉRIODES DES RACINES PRIMITIVES DE L'UNITÉ.

[*Comptes Rendus,* XCII. (1881), pp. 1084—1086.]

SOIT p un nombre premier égal à $ef+1$; la fonction du $e^{\text{ième}}$ degré, dont les racines sont les e périodes entre lesquelles on peut distribuer les ef $p^{\text{ièmes}}$ racines primitives de l'unité, est ce que je désigne comme la fonction à e périodes par rapport à p.

On connaît bien que p et un $e^{\text{ième}}$ résidu quelconque par rapport à p sont toujours diviseurs de cette fonction. Tout autre diviseur se nomme *diviseur exceptionnel* de la fonction. On sait que tout diviseur exceptionnel d'une fonction de périodes doit être contenu comme facteur dans le discriminant de cette fonction et, de plus, que pour les cas où $f=1$, ou $f=2$, ou $e=2$, il n'y a pas de facteurs exceptionnels. Si l'on en connaît davantage au sujet de ces facteurs exceptionnels, je n'en suis pas instruit. On ne trouve rien de plus dans le Livre classique de Bachmann (*Kreistheilung*, 1872)*.

Or je trouve facilement, pour le cas de $e=3$, qu'il n'y a pas de facteurs exceptionnels, de sorte que tout diviseur premier de la fonction bien connue

$$\eta^3+\eta^2-\frac{p-1}{3}\eta+\cdots$$

est nécessairement ou p ou un résidu cubique de p. Pour $e=4$, la même chose n'a pas lieu.

* Dans cet excellent ouvrage, M. Bachmann démontre que, si Ω est la fonction à e périodes par rapport à p et q nombre premier qui est une $e^{\text{ième}}$ puissance résidu de p, la congruence $\Omega\equiv 0$ (mod. q) aura e racines réelles, mais, chose extraordinaire, omet de démontrer ou même de dire que la même chose a lieu pour la congruence $\Omega\equiv 0$ (mod. q^i), i étant un nombre entier positif quelconque. En effet, cette propriété de q (que *toutes* ses puissances sont diviseurs) est le *caractère distinctif* de la classe *principale* de diviseurs, non pas seulement pour les fonctions des périodes de racines d'unité par rapport à un nombre premier, mais aussi pour les fonctions cyclotomiques en général. Dans le cas que nous considérons, ni p ni aucun *diviseur exceptionnel* ne possède cette propriété.

Quand $p = f^2 + g^2$, où f est impair, si g est divisible par 4, mais non pas par 8, le nombre 2 divisera la fonction des quatre périodes, mais ne sera pas (comme on sait bien) un résidu biquadratique, mais seulement un résidu quadratique de p; de plus, si g n'est pas divisible par 4, tout nombre premier contenu dans $\frac{g}{2}$ sera un diviseur de la fonction des périodes, et, si ce nombre premier est de la forme $4i+3$, il sera seulement un résidu quadratique et non biquadratique de p. Pour $e=4$, il n'y a pas d'autres diviseurs exceptionnels au delà de ceux que j'ai donnés ci-dessus. En établissant ce fait, j'ai été amené à cette proposition curieuse, qu'il serait difficile (il me semble) d'établir par un autre genre de considérations, mais qui est indubitablement vraie, c'est-à-dire :

Si $p = f^2 + (2g)^2$ (p étant un nombre premier et g impair), *tout nombre contenu dans le nombre impair* $\frac{f^2 + 3g^2}{4}$ *est un résidu biquadratique de* p.

Mais je passe à un théorème général, qui me paraît très intéressant et que voici :

1°. *Si* e (le nombre des périodes) *est un nombre premier de la forme* $2^{2^x}+1$, *le nombre* 2 *ne peut pas être un diviseur exceptionnel de la fonction des* e *périodes.*

2°. *Si* e *est un nombre premier, un facteur exceptionnel* K (si un tel cas peut exister) *doit entrer à la seconde puissance au moins comme facteur dans* $e-1$, *de sorte qu'on sait que, pour* $e = 2, 3, 5, 7, 11, 17$, *il n'existe pas de diviseur de la fonction des* e *périodes en dehors de* p *et des résidus* $e^{\text{ièmes}}$ *de* p.

Quand $e=19$, puisque $19-1$ contient 3^2, le théorème n'exclut pas la possibilité que 3 soit un diviseur de la fonction à dix-neuf périodes sans être une dix-neuvième puissance résidu de p. De même, quand $e=13$, le théorème ne dit rien sur le caractère du diviseur 2, dont le carré 4 est contenu dans 13. Cependant, je n'ai pas la moindre raison pour conclure que les diviseurs exceptés sont vraiment des facteurs exceptionnels.

On doit regarder le cas où, e étant un nombre premier, $e-1$ contient K^2, non pas comme un cas exceptionnel, mais comme un cas réservé pour un examen ultérieur.