JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

LÉOPOLD KRONECKER

Démonstration d'un théorème de M. Kummer

Journal de mathématiques pures et appliquées 2^e série, tome 1 (1856), p. 396-398.
<http://www.numdam.org/item?id=JMPA_1856_2_1__396_0>

gallica NUMDAM

Article numérisé dans le cadre du programme Gallica de la Bibliothèque nationale de France
http://gallica.bnf.fr/

et catalogué par Mathdoc dans le cadre du pôle associé BnF/Mathdoc
http://www.numdam.org/journals/JMPA

DÉMONSTRATION

D'UN

THÉORÈME DE M. KUMMER;

PAR M. LÉOPOLD KRONECKER.

Dans son Mémoire sur la Théorie des nombres complexes composés de racines ($\lambda^{ièmes}$) de l'unité et de nombres entiers, M. Kummer a donné le théorème important que voici [*] :

La condition nécessaire et suffisante pour que le premier facteur du nombre des classes H *soit divisible par* λ, *consiste en ce qu'un quelconque des* $\frac{\lambda-3}{2}$ *premiers nombres bernoulliens soit divisible par* λ.

On peut démontrer ce théorème d'une manière très-simple. En effet, si l'on conserve les notations de M. Kummer [**], tout se réduit à examiner si la congruence

$$\psi(\gamma^{2n-1}) = b_0 + b_1\gamma^{2n-1} + \ldots + b_{\lambda-2}\cdot\gamma^{(\lambda-2)(2n-1)} \equiv 0 \pmod{\lambda},$$

est ou n'est pas satisfaite pour une quelconque des valeurs de

$$n = 1, 2, 3, \ldots, \mu.$$

Donc, puisqu'on a [***]

$$\lambda b_k = \gamma\cdot\gamma_{k-1} - \gamma_k,$$

il s'agit d'examiner la congruence

$$(I) \qquad \lambda.\psi(\gamma^{2n-1}) = \Sigma(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k} \equiv 0 \pmod{\lambda^2},$$

où le signe de sommation s'étend à toutes les valeurs de

$$k = 0, 1, 2, 3, \ldots, (\lambda-2).$$

---

[*] *Voir* ce Journal, tome XVI, page 479.

[**] *Voir* ce Journal, tome XVI, page 475.

[***] *Voir* ce Journal, tome XVI, page 474.

Partons de l'égalité identique

$$\gamma^k - (\gamma^k - \gamma_k) = \gamma_k .$$

En élevant cette égalité à la puissance $2n$ et en observant que le nombre entier $(\gamma^k - \gamma_k)$ est un multiple de λ, on obtient la congruence

$$\gamma^{2nk} - 2n\gamma^{(2n-1)k}(\gamma^k - \gamma_k) \equiv \gamma_k^{2n} \pmod{\lambda^2},$$

ou

$$(1 - 2n)\gamma^{2nk} + 2n.\gamma_k.\gamma^{(2n-1)k} \equiv \gamma_k^{2n} \pmod{\lambda^2}.$$

En remplaçant k par $(k-1)$ et en multipliant par γ^{2n}, il vient

$$(1 - 2n)\gamma^{2nk} + 2n\gamma_{k-1}\gamma^{(2n-1)k+1} \equiv \gamma^{2n}\gamma_{k-1}^{2n} \pmod{\lambda^2}.$$

En retranchant cette congruence de celle qui précède, on obtient

$$2n(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k} \equiv \gamma^{2n}\gamma_{k-1}^{2n} - \gamma_k^{2n} \pmod{\lambda^2}.$$

Donc on aura de même

$$2n.\Sigma(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k} \equiv \gamma^{2n}\Sigma\gamma_{k-1}^{2n} - \Sigma\gamma_k^{2n} \pmod{\lambda^2}.$$

Or, comme les nombres $\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_{\lambda-2}$ et les nombres $1, 2, 3, \ldots, (\lambda - 1)$ sont les mêmes à l'ordre près, on a enfin

$$\text{(II)} \qquad \left\{ \begin{array}{c} 2n.\Sigma(\gamma\gamma_{k-1} - \gamma_k).\gamma^{(2n-1)k} \\ \equiv (\gamma^{2n} - 1)[1^{2n} + 2^{2n} + \ldots + (\lambda - 1)^{2n}] \pmod{\lambda^2}. \end{array} \right.$$

Le nombre $2n$ est moindre que λ. On voit donc que la discussion de la congruence (I) se réduit à la question si le second membre de la congruence (II) est divisible par λ^2. Cela n'a pas lieu pour la valeur

$$2n = 2\mu = \lambda - 1.$$

Car, suivant l'hypothèse (faite par M. Kummer) que le nombre $\gamma^\mu + 1$ ne soit pas divisible par λ^2, le nombre $\gamma^{2\mu} - 1$ ne contiendra qu'*une* fois le facteur λ, et, en vertu du théorème de Fermat, la somme

$$1^{\lambda-1} + 2^{\lambda+1} + \ldots + (\lambda - 1)^{\lambda-1}$$

sera congrue à -1 suivant le module λ. Ensuite, pour décider si le produit

$$(\gamma^{2n}-1)\left[1^{2n}+2^{2n}+\ldots+(\lambda-1)^{2n}\right]$$

est divisible par λ^2 pour une des valeurs de $n=1, 2, \ldots, (\mu-1)$, observons que, dans ces cas, le nombre $(\gamma^{2n}-1)$ n'est pas divisible par λ, et que l'expression connue de la somme

$$1^{2n}+2^{2n}+\ldots+(x-1)^{2n}$$

en fonction rationnelle entière de x, fournit la congruence

$$1^{2n}+2^{2n}+\ldots+(\lambda-1)^{2n}\equiv\pm B_n.\lambda \pmod{\lambda^2},$$

B_n désignant le nombre bernoullien $n^{ième}$. Donc, pour que la congruence (1) ait lieu pour une quelconque des valeurs de

$$n=1, 2, 3, \ldots, \mu,$$

il faut et il suffit que la congruence

$$B_n\equiv 0 \pmod{\lambda}$$

soit satisfaite pour une quelconque des valeurs de $n=1, 2, \ldots, (\mu-1)$; ce qu'il fallait démontrer.