JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

LE BESGUE

Extrait d'une Lettre de M. Le Besgue à M. Liouville

Journal de mathématiques pures et appliquées 2e série, tome 7 (1862), p. 417-420.

<http://www.numdam.org/item?id=JMPA_1862_2_7__417_0>

EXTRAIT D'UNE LETTRE DE M. LE BESGUE A M. LIOUVILLE.

« ... Le moyen que j'ai employé dans votre Journal, t. VIII, pour prouver qu'il y a une infinité de nombres premiers de la forme $2pz+1$, le nombre p étant premier, peut servir aussi à montrer qu'il y a une infinité de nombres premiers de la forme $2pz-1$.

» Soit

$$\varphi(x) = x^{p-1} + x^{p-2} + \ldots + x + 1,$$

$$\psi\left(x+\frac{1}{x}\right) = 1 + x + \frac{1}{x} + x^2 + \frac{1}{x^2} + \ldots + x^{\frac{p-1}{2}} + \frac{1}{x^{\frac{p-1}{2}}};$$

en posant

$$x + \frac{1}{x} = y,$$

on aura, en faisant $p = 2q+1$,

$$\psi(y) = y^q - (q-1)y^{q-2} + \frac{q-2.q-3}{1.2}y^{q-4} - \frac{q-3.q-4.q-5}{1.2.3}y^{q-6} + \ldots,$$
$$+ y^{q-1} - (q-2)y^{q-3} + \frac{q-3.q-4}{1.2}y^{q-5} - \frac{q-4.q-5.q-6}{1.2.3}y^{q-7} + \ldots.$$

(*Théorie des Nombres* de Legendre, t. II, p. 209.)

» Il est prouvé que la fonction $\varphi(x)$, quand on donne à x des valeurs entières, n'a pas d'autres diviseurs premiers que p et des nombres de la forme $2pz+1$. De même la fonction $\psi(y)$, pour y entier, n'a pas d'autres diviseurs premiers que p et des nombres des deux formes $2pz+1$, $2pz-1$. Pour la généralisation de ces théorèmes, il faut voir le Mémoire de M. Kummer sur les diviseurs de certaines formes de nombres qui résultent de la théorie de la division du cercle. (*Journal de M. Liouville*, 2[e] série, t. V.)

» Il est à remarquer que

$$\varphi(x) = \frac{x^p - 1}{x - 1}$$

donne, en faisant $x = 1 + u$,

$$\varphi(1+u) = \theta(u) = u^{p-1} + pu^{p-2} + \frac{p.p-1}{1.2} u^{p-3} + \ldots + \frac{p.p-1}{1.2} u + p.$$

» $\theta(u)$ ne peut être multiple de p que pour u multiple de p, et p^2 n'est jamais diviseur de $\theta(u)$.

» Comme pour une valeur entière de u non multiple de p, $\theta(u)$ est un nombre entier impair de la forme

$$pA + 1,$$

il aura nécessairement des facteurs premiers de la forme $2pz + 1$, car il n'en saurait avoir d'autres. Soient

$$p_1, \quad p_2, \ldots, \quad p_n,$$

de tels facteurs premiers; en posant

$$U = p_1 p_2 \ldots p_n,$$

il viendra

$$\theta(U) = pA + 1,$$

et ce nombre, qui ne saurait être divisible par p_1, $p_2, \ldots$, donnera nécessairement un ou plusieurs nouveaux nombres premiers de cette forme. Il y a donc un nombre infini de tels nombres premiers.

» Il faut remarquer également que si dans $\psi(y)$ on change y en $u + 2$, on aura pour

$$\psi(u+2) = \xi(u)$$

la valeur suivante

$$\xi(u) = (2q+1)\Big[1 + \frac{q+1.q}{1.2}\cdot\frac{u}{3} + \frac{q+2.q+1.q.q-1}{1.2.3.4}\frac{u^2}{5} + \ldots$$
$$+ \frac{(q+q-1)\ldots q.q-1\ldots 2}{1.2.3\ldots 2q-2}\frac{u^{q-1}}{2q-1}$$
$$+ \frac{q+q\ldots q+1.q\ldots 1}{1.2\ldots 2q}\cdot\frac{u^q}{2q+1}\Big];$$

le coefficient de u^q se réduit à l'unité, les coefficients des autres puissances de u sont des entiers multiples de $p = 2q + 1$.

» La vérification est plus longue que difficile; il suffira de dire ici que si l'on pose

$$x = \cos 2z + \sin 2z \sqrt{-1},$$

on aura

$$x + \frac{1}{x} = 2\cos 2z$$

et

$$\psi\left(x + \frac{1}{x}\right) = 1 + 2(\cos 2z + \cos 4z + \ldots + \cos 2qz) = \frac{\sin(2q+1)z}{\sin z}.$$

» La valeur de $\xi(u)$ donnée plus haut, en y changeant le signe de u, n'est autre que la formule (6) de la page 233 de l'*Analyse algébrique* de Cauchy, où l'on aurait remplacé m par $2q + 1$ et $(2\sin z)^2$ par u.

» Le nombre entier $\xi(u)$, répondant à une valeur entière de u, ne peut être divisible par p que pour u multiple de p, et il n'est jamais multiple de p^2. Quand u n'est pas multiple de p, comme l'on a

$$u^{\frac{p-1}{2}} = pQ \pm 1,$$

le nombre $\xi(u)$ aura la forme $pQ + 1$ ou $pQ - 1$, selon que u sera résidu ou non résidu quadratique de p.

» En prenant pour u un nombre entier non-résidu quadratique de p, le nombre entier impair

$$\xi(u) = pA - 1$$

donnera nécessairement un ou plusieurs diviseurs premiers de la forme $2pz - 1$, et ces nombres

$$p_1, \ p_2, \ p_3, \ \ldots, \ p_k$$

en fourniront d'autres. Si n est un non-résidu quadratique de p, on donnera pour valeur à u celui des deux nombres

$$p_1 p_2 \ldots p_k, \quad n p_1 p_2 \ldots p_k,$$

qui sera non-résidu quadratique de p, et l'on aura ainsi un nombre $pQ - 1$, non divisible par $p_1, p_2, \ldots p_k$, et qui aura nécessairement un ou plusieurs autres diviseurs premiers de la forme $2pz - 1$, d'où l'on doit conclure que ces diviseurs sont en nombre infini.

» *N. B.* — Pour $p = 3$, $\psi(y) = 1 + y$ peut avoir 2 pour diviseur. La démonstration de ce cas ne présente aucune difficulté et se trouve immédiatement en remarquant que tout nombre $6z - 1$, qui n'est pas premier, a nécessairement un nombre impair de diviseurs premiers de la forme $6y - 1$, puisque, à l'exception de 3 et 2, tous les nombres premiers sont contenus dans les formules $6x + 1$, $6x - 1$.

» Je reviendrai ailleurs sur le théorème de M. Kummer, propriété importante des équations que Gauss a nommées *auxiliaires* pour la résolution de l'équation $x^p = 1$. »