JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

J. LIOUVILLE

Théorèmes concernant le quadruple d'un nombre premier de l'une ou de l'autre des deux formes $20\kappa + 3$, $20\kappa + 7$

Journal de mathématiques pures et appliquées 2e série, tome 8 (1863), p. 85-88.

<http://www.numdam.org/item?id=JMPA_1863_2_8__85_0>

THÉORÈMES

CONCERNANT

LE QUADRUPLE D'UN NOMBRE PREMIER DE L'UNE OU DE L'AUTRE DES DEUX FORMES $20k+3$, $20k+7$;

PAR M. J. LIOUVILLE.

En considérant le nombre N des décompositions dont le quadruple d'un nombre premier $m \equiv 3$ (mod. 4) est susceptible sous la forme

$$x^2 + p^{4l+1} y^2,$$

x et y désignant des entiers impairs et p un nombre premier $8g+3$ qui ne divise pas y, on prouve sans peine que ce nombre N est essentiellement pair. Mais quand m est de l'une des deux formes spéciales

$$20k+3, \quad 20k+7,$$

c'est-à-dire quand m est à la fois $\equiv 3$ (mod. 4) et $\equiv \pm 3$ (mod. 5), on peut aller plus loin et démontrer que N est la somme de deux entiers impairs N_1, N_2, en sorte qu'on est assuré d'avoir au moins $N = 2$. Cela résulte de deux théorèmes que nous allons énoncer et qui sont fondés sur la distinction des nombres premiers p de la forme $8g+3$ en deux classes suivant qu'ils sont ou non résidus quadratiques de 5; l'une de ces classes contiendra donc les nombres premiers p de l'une ou de l'autre des deux formes

$$40h+11, \quad 40h+19,$$

et c'est à elle que se rapportera l'entier impair N_1 : l'autre contiendra les nombres premiers p de l'une ou de l'autre des deux formes

$$40h+3, \quad 40h+27,$$

et c'est à elle que se rapportera l'entier impair N_2. Nos deux théorèmes s'appliquent en effet à ces deux classes de nombres premiers prises successivement.

Théorème I. — « Pour tout nombre premier m de l'une ou de » l'autre des deux formes $20k+3$, $20k+7$, on peut poser au moins » une fois (et toujours un nombre impair de fois) l'équation

$$4m = x^2 + p^{4l+1}y^2,$$

» x et y étant des entiers impairs et p un nombre premier $40h+11$ » ou $40h+19$, qui ne divise pas y. »

Théorème II. — « Pour tout nombre premier m de l'une ou de » l'autre des deux formes $20k+3$, $20k+7$, on peut poser au moins » une fois (et toujours un nombre impair de fois) l'équation

$$4m = x^2 + p^{4l+1}y^2,$$

» x et y étant des entiers impairs et p un nombre premier $40h+3$ » ou $40h+27$, qui ne divise pas y. »

On peut réunir ces deux énoncés en un seul en disant que : « Si du » quadruple $4m$ d'un nombre premier donné, de l'une des deux » formes $20k+3$, $20k+7$, on retranche tant que faire se peut les » carrés impairs

$$1^2,\ 3^2,\ 5^2,\ 7^2,\ 9^2,\ 11^2,\ldots,$$

» il y aura un nombre pair N de restes susceptibles d'être mis sous la » forme

$$p^{4l+1}y^2,$$

» p étant un nombre premier (naturellement de la forme $8g+3$) qui » ne divise pas y. Mais ce nombre pair N sera la somme de deux » nombres impairs N_1, N_2 respectivement relatifs aux deux cas de » $p \equiv 11$ ou $19 \pmod{40}$ et de $p \equiv 3$ ou $27 \pmod{40}$. »

Soit, comme premier exemple, $m=3$, d'où $4m=12$. On aura

$$\begin{aligned} 12 - 1^2 &= 11.1^2, \\ 12 - 3^2 &= 3.1^2, \end{aligned}$$

d'où visiblement $N = 2$, $N_1 = 1$, $N_2 = 1$, conformément à ce que nous avons annoncé.

Prenons ensuite $m = 7$, d'où $4m = 28$. Il viendra d'abord

$$28 - 1^2 = 27 = 3^3 . 1^2,$$

ce qui ne fournit pas un reste canonique parce que l'exposant 3 n'est pas de la forme $4l + 1$; mais en continuant on a

$$\begin{aligned} 28 - 3^2 &= 19 . 1^2, \\ 28 - 5^2 &= 3 . 1^2, \end{aligned}$$

ce qui conduit encore à $N_1 = 1$, $N_2 = 1$.

Soit à présent $m = 23$, d'où $4m = 92$. Les restes seront

$$\begin{aligned} 92 - 1^2 &= 7 . 13, \\ 92 - 3^2 &= 83 . 1^2, \\ 92 - 5^2 &= 67 . 1^2, \\ 92 - 7^2 &= 43 . 1^2, \\ 92 - 9^2 &= 11 . 1^2. \end{aligned}$$

Il y a quatre restes canoniques, et le dernier seul appartient à la première classe des nombres p. On a, par suite, $N_1 = 1$, $N_2 = 3$, et cette fois encore notre théorème est confirmé.

Pour $m = 43$ (c'est-à-dire pour $4m = 172$) on a également $N_1 = 1$, $N_2 = 3$, les restes canoniques étant d'une part

$$172 - 1^2 = 19 . 3^2,$$

et d'autre part

$$\begin{aligned} 172 - 3^2 &= 163 . 1^2, \\ 172 - 5^2 &= 3 . 7^2, \\ 172 - 13^2 &= 3 . 1^2; \end{aligned}$$

les restes non canoniques sont

$$\begin{aligned} 172 - 7^2 &= 3 . 41, \\ 172 - 9^2 &= 7 . 13, \\ 172 - 11^2 &= 3 . 17. \end{aligned}$$

Enfin pour $m = 47$ (ou $4m = 188$) on trouve $N_1 = 3$ et $N_2 = 3$. Après avoir écarté le reste non canonique

$$188 - 1^2 = 11.17,$$

on obtient en effet ces deux classes de restes

$$\begin{aligned} 188 - 3^2 &= 179.1^2, \\ 188 - 7^2 &= 139.1^2, \\ 188 - 13^2 &= 19.1^2, \end{aligned}$$

puis

$$\begin{aligned} 188 - 5^2 &= 163.1^2, \\ 188 - 9^2 &= 107.1^2, \\ 188 - 11^2 &= 67.1^2. \end{aligned}$$

Je ne crois pas devoir pousser plus loin ces vérifications numériques.