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

J. LIOUVILLE

Remarques nouvelles concernant les nombres premiers de la forme $24\mu + 7$

Journal de mathématiques pures et appliquées 2^e série, tome 6 (1861), p. 219-224.
<http://www.numdam.org/item?id=JMPA_1861_2_6__219_0>

REMARQUES NOUVELLES

CONCERNANT

LES NOMBRES PREMIERS DE LA FORME $24\mu + 7$;

PAR M. J. LIOUVILLE.

Déjà nous nous sommes occupés des nombres premiers de la forme $24\mu + 7$. On a vu en particulier (dans le cahier de novembre 1859) que si p désigne un tel nombre, on peut toujours poser (un nombre impair de fois) l'équation

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

x et y étant des entiers impairs et q un nombre premier de la forme $24\nu + 13$, qui ne divise pas y.

Avec la forme imposée à q, il est évident que x doit être premier à 3, et réciproquement dès que x est premier à 3, q ne peut avoir que la forme indiquée. Quant à y, on s'assurera sans peine qu'il n'est jamais divisible par 3. Mais en prenant x multiple de 3 et q de la forme $24\nu + 5$, on pourrait aussi représenter $2p$. De là un théorème nouveau qui complétera, pour ainsi dire, celui que nous venons de rappeler. Les nombres premiers de la forme $24\mu + 7$ donnent en outre lieu à plusieurs remarques intéressantes qu'on trouvera ci-après. J'entre en matière.

Théorème I. — « Pour tout nombre premier p, de la forme » $24\mu + 7$, on peut poser un nombre impair de fois l'équation

$$2p = 9x^2 + q^{4l+1} y^2,$$

» x et y étant des entiers impairs, et q un nombre premier qui ne di- » vise pas y. »

Cet énoncé n'impose aucune condition au nombre premier q; mais

comme, d'après la forme $24\mu + 7$ assignée à p, on a

$$2p \equiv 6 \pmod 8, \qquad 2p \equiv 2 \pmod 3,$$

il s'ensuit qu'on aura nécessairement

$$q \equiv 5 \pmod 8, \qquad q \equiv 2 \pmod 3.$$

Donc q sera toujours de la forme $24\nu + 5$, indiquée tout à l'heure.

Vérifions notre théorème sur quelques exemples. Et d'abord soit $p = 7$; nous aurons, comme il le faut, l'équation canonique

$$2.7 = 9.1^2 + 5.1^2.$$

Pour $p = 31$, on a de même

$$2.31 = 9.1^2 + 53.1^2.$$

Je trouve aussi une équation canonique pour $p = 79$, savoir

$$2.79 = 9.1^2 + 149.1^2.$$

Enfin on en a une pour $p = 103$. C'est

$$2.103 = 9.1^2 + 197.1^2.$$

L'équation

$$2.103 = 9.3^2 + 5^2.1^2$$

a dû être rejetée, bien que 5 soit un nombre premier, parce que l'exposant 3 n'est pas de la forme $4l + 1$.

Remarque. — Si, désignant toujours par p un nombre premier donné de la forme $24\mu + 7$, on posait

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

en prenant pour x et y des entiers impairs *quelconques* et en assujettissant le nombre premier q à la seule condition de ne pas diviser y, le nombre N des décompositions de $2p$ ainsi obtenues serait toujours

pair, mais au moins égal à 2, comme étant la somme de deux nombres impairs N_1, N_2 respectivement relatifs aux deux hypothèses de x premier à 3 (ou de $q = 24\nu + 13$) et de x multiple de 3 (ou de $q = 24\nu + 5$). Cela résulte du nouveau théorème que nous venons de donner, combiné avec celui que nous avions donné en 1859.

Théorème II. — « Pour tout nombre premier p, de la forme » $24\mu + 7$, on peut poser un nombre impair de fois l'équation

$$2p = 3x^2 + q^{4l+1} y^2,$$

» x et y étant des entiers impairs, et q un nombre premier non di- » viseur de y. »

Notre énoncé n'impose aucune condition au nombre premier q; mais il est évident qu'il ne pourra manquer de vérifier les deux congruences

$$q \equiv 3 \pmod 8, \qquad q \equiv 2 \pmod 3.$$

Il sera donc nécessairement de la forme $24\nu + 11$.

Passons aux vérifications numériques. D'abord pour

$$p = 7,$$

on a l'équation canonique

$$2.7 = 3.1^2 + 11.1^2.$$

On en a une également pour

$$p = 31,$$

savoir

$$2.31 = 3.1^2 + 59.1^2.$$

Soit à présent

$$p = 79.$$

Les équations canoniques seront alors au nombre de trois :

$$2.79 = 3.3^2 + 131.1^2,$$
$$2.79 = 3.5^2 + 83.1^2,$$
$$2.79 = 3.7^2 + 11.1^2.$$

J'en trouve aussi trois pour

$$p = 103.$$

Les voici :

$$2.103 = 3.3^2 + 179.1^2,$$
$$2.103 = 3.5^2 + 131.1^2,$$
$$2.103 = 3.7^2 + 59.1^2.$$

Toujours notre théorème a lieu, mais voilà assez d'exemples.

Théorème III. — « Pour tout nombre premier p, de la forme » $24\mu + 7$, on peut poser un nombre impair de fois l'équation

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

» x et y étant des entiers impairs, non divisibles par 3, et q un nombre » premier non diviseur de y. »

Puisque x est supposé premier à 3, on aura

$$2x^2 \equiv 2 \pmod 3.$$

Mais déjà on a

$$p \equiv 1 \pmod 3.$$

L'équation

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

entraîne donc la congruence

$$q^{4l+1} y^2 \equiv -1 \pmod 3.$$

La condition relative à y de ne pas être divisible par 3 sera donc remplie d'elle-même; mais de plus on voit que nécessairement

$$q \equiv -1 \pmod 3.$$

Il est d'ailleurs aisé de voir que l'équation

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

où l'on a

$$p \equiv 7 \pmod 8),$$

entraîne cette seconde congruence

$$q \equiv 5 \pmod 8.$$

Il suit de là que q ne peut être que de la forme $24\nu + 5$.

Soit d'abord

$$p = 7,$$

et nous aurons l'équation canonique

$$7 = 2.1^2 + 5.1^2.$$

On en a une également pour

$$p = 31,$$

savoir

$$31 = 2.1^2 + 29.1^2;$$

une aussi pour

$$p = 79,$$

car

$$79 = 2.5^2 + 29.1^2.$$

Notre théorème se vérifie aussi pour

$$p = 103;$$

mais alors il y a trois équations canoniques

$$103 = 2.1^2 + 101.1^2,$$
$$103 = 2.5^2 + 53.1^2,$$
$$103 = 2.7^2 + 5.1^2.$$

Nous ne pousserons pas plus loin les exemples.

Dans la forme

$$2x^2 + q^{4l+1} y$$

que nous venons d'employer pour représenter le nombre premier donné p, de la forme $24\mu + 7$, nous avons supposé x premier à 3. Prenons à présent x multiple de 3, ou plutôt remplaçons x par $3x$, et nous aurons la proposition nouvelle que voici :

Théorème IV. — « On désigne par p un nombre premier donné,

» de la forme $24\mu + 7$, et on pose de toutes les manières possibles l'é-
» quation

$$p = 18x^2 + q^{4l+1}y^2,$$

» x et y étant des entiers impairs, et q un nombre premier (naturelle-
» ment de la forme $24\nu + 13$) qui ne divise pas y. Le nombre N des
» décompositions de p ainsi obtenues est tantôt pair et tantôt impair;
» mais on a toujours $N \equiv \mu \pmod 2$. »

En d'autres termes N est pair quand μ est pair, mais impair quand μ est impair; ou ce qui revient au même, N est pair quand $p = 48k + 7$, mais impair quand $p = 48k + 31$.

Il suit de notre théorème que l'on doit trouver N pair pour

$$p = 7$$

et pour

$$p = 103,$$

mais impair pour

$$p = 31$$

et pour

$$p = 79.$$

Or je trouve en effet

$$N = 0$$

pour les deux premiers nombres 7 et 103, tandis que pour les deux autres, 31 et 17, on a

$$N = 1,$$

en vertu des équations canoniques

$$31 = 18.1^2 + 13.1^2$$

et

$$79 = 18 + 61.1^2.$$

Notre théorème est donc vérifié sur ces exemples, et il le sera également sur tous ceux qu'on pourra vouloir ajouter.