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 la forme $12\kappa + 5$

Journal de mathématiques pures et appliquées 2e série, tome 6 (1861), p. 93-96.

<http://www.numdam.org/item?id=JMPA_1861_2_6__93_0>

THÉORÈMES

CONCERNANT

LE QUADRUPLE D'UN NOMBRE PREMIER DE LA FORME $12k+5$;

Par M. J. LIOUVILLE.

Désignons par m un nombre premier donné, de la forme $12k+5$; considérons son quadruple $4m$, et posons de toutes les manières possibles l'équation

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

x et y étant des entiers impairs et p un nombre premier qui ne divise pas y : on admet pour l la valeur zéro. Nous trouvons tout de suite par nos *formules générales* que le nombre N des décompositions de $4m$ ainsi obtenues est essentiellement pair; mais comme on compte zéro parmi les nombres pairs, le cas de $N=0$ ne serait pas exclu. Or une analyse plus délicate fait voir que N est la somme de deux nombres impairs N_1, N_2, et dès lors on est sûr d'avoir soit $N=2$, soit $N>2$.

On peut, en effet, distinguer dans l'équation

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

deux genres de solutions, suivant que x est ou n'est pas divisible par 3. Dans le premier cas, on a, vu la forme donnée de m,

$$p \equiv 2 \pmod{3},$$

tandis que dans le second cas on a au contraire

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

D'ailleurs p vérifie toujours la congruence

$$p \equiv 3 \pmod{8}.$$

Il s'ensuit que p est de la forme

$$24g + 11$$

lorsque x est multiple de 3, mais de la forme

$$24g + 19$$

lorsque x est premier à 3. Quant à y, il n'est jamais divisible par 3.

Ceci expliqué, nous pouvons énoncer les deux théorèmes suivants, qui montreront comment N est la somme de deux entiers impairs N_1, N_2, respectivement relatifs aux deux genres de décompositions de $4m$ dont nous venons de parler.

Théorème I. — Pour chaque nombre premier m, de la forme $12k + 5$, on peut poser au moins une fois (et toujours un nombre impair de fois) l'équation

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

x et y étant des entiers impairs et p un nombre premier $24g + 11$ qui ne divise pas y.

En d'autres termes, si du quadruple d'un nombre premier donné, de la forme $12k + 5$, on retranche, tant que faire se peut, les carrés

$$9,\ 81,\ 225, \ldots,$$

des nombres impairs multiples de 3, il y aura un nombre impair de restes susceptibles d'être mis sous la forme

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

p étant un nombre premier non diviseur de y et naturellement de la forme $24g + 11$.

Théorème II. — Pour chaque nombre premier m, de la forme $12k + 5$, 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 non divisibles par 3, et p un nombre premier $24g + 19$ qui ne divise pas y.

En d'autres termes, si du quadruple d'un nombre premier donné, de la forme $12k + 5$, on retranche, tant que faire se peut, les carrés

$$1,\ 25,\ 49,\ 121, \ldots,$$

des nombres impairs premiers à 3, il y aura un nombre impair de restes susceptibles d'être mis sous la forme

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

p étant un nombre premier non diviseur de y et naturellement de la forme $24g + 19$. La condition relative de y (de ne pas être un multiple de 3) sera remplie d'elle-même.

Passons aux exemples, et d'abord soit

$$m = 5 :$$

nous aurons l'équation

$$4.5 = 9.1^2 + 11.1^2,$$

conformément au théorème I, et l'équation

$$4.5 = 1^2 + 19.1^2,$$

conformément au théorème II.

En prenant $k = 1$, la formule $12k + 5$ nous donne le nombre premier 17, et là encore nos théorèmes sont vérifiés, puisque l'on a d'une part

$$4.17 = 9.1^2 + 59.1^2,$$

et d'autre part

$$4.17 = 1^2 + 67.1^2,$$
$$4.17 = 5^2 + 43.1^2,$$
$$4.17 = 7^2 + 19.1^2.$$

Enfin, pour

$$m = 12.2 + 5 = 29,$$

même vérification; on n'a alors que les deux équations canoniques ci-après, une pour chaque genre :

$$4.29 = 9.1^2 + 107.1^2$$

et

$$4.29 = 7^2 + 67.1^2.$$

Ces exemples suffiront. Mais en terminant faisons observer que notre décomposition en deux entiers impairs N_1, N_2 du nombre complet (et essentiellement pair) N des solutions de l'équation

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

où l'on confondrait les deux espèces de valeurs de x^2 (mod. 3) ou de p (mod. 3), n'est pas sans quelque analogie avec la distinction des formes quadratiques en *genres*, qui joue un si grand rôle dans la théorie de ces formes.