JOURNAL

DE

# MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

J. LIOUVILLE

**Théorèmes concernant l'octuple 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 9 (1864), p. 137-144.

<http://www.numdam.org/item?id=JMPA_1864_2_9__137_0>

# THÉORÈMES

CONCERNANT

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

### PAR M. J. LIOUVILLE.

---

**1.** Dans l'article précédent, comme déjà dans un article inséré au cahier de mars 1863, nous nous sommes occupés du quadruple des nombres premiers $m$ qui appartiennent à l'une ou à l'autre des deux formes linéaires

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

et dont la propriété commune est d'être $\equiv 3 \pmod{4}$ et non résidus quadratiques de 5. Il s'agira ici de leur octuple $8m$.

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

$$8m = 5x^2 + p^{4l+1}y^2,$$

» $x$ et $y$ étant des entiers impairs positifs, et $p$ un nombre premier » qui ne divise pas $y$. »

En d'autres termes, si de l'octuple $8m$ d'un nombre premier $m$ provenant de l'une des deux expressions $20k+3$ ou $20k+7$, on retranche, tant que faire se peut, les termes de la suite

$$5.1^2,\ 5.3^2,\ 5.5^2,\ 5.7^2,\ 5.9^2,\ \text{etc.},$$

savoir,

$$5,\quad 45,\quad 125,\ 245,\ 405,\ \text{etc.},$$

il y aura un nombre impair de restes susceptibles d'être mis sous la forme

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

$p$ désignant un nombre premier non diviseur de $y$.

On admet pour $l$ la valeur zéro. Quant au nombre premier $p$, nous ne lui imposons aucune condition; mais comme $x$ et $y$ sont impairs, l'équation

$$8m = 5x^2 + p^{4l+1}y^2$$

entraînera nécessairement la congruence

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

D'un autre côté, $m$ étant non résidu quadratique de 5, $8m$ est résidu, et par suite $p$ aussi sera résidu. Le nombre premier $p$ ne peut donc être que de l'une des deux formes

$$40g + 11, \quad 40g + 19.$$

**2**. Les plus petits nombres premiers fournis par les expressions

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

sont

$$3, \ 7, \ 23, \ 43, \ 47, \ \text{etc.}$$

Voyons comment notre théorème se vérifie pour eux.

Soit d'abord $m = 3$, d'où $8m = 24$. On a l'équation canonique

$$24 = 5.1^2 + 19.1^2.$$

Pour $m = 7$, on n'a également qu'une seule équation canonique

$$56 = 5.3^2 + 11.1^2,$$

car le reste 51, obtenu en retranchant 5 de 56, est le produit de 3 par 17 et n'a pas la forme voulue.

Mais pour $m = 23$, c'est-à-dire pour $8m = 184$, il y a trois équations canoniques, savoir

$$184 = 5.1^2 + 179.1^2,$$
$$184 = 5.3^2 + 139.1^2,$$
$$184 = 5.5^2 + \ 59.1^2.$$

Pour $m = 43$ (d'où $8m = 344$), on ne trouve plus qu'une équation canonique :

$$344 = 5.7^2 + 11.3^2.$$

Les restes

$$339, \ 299, \ 219,$$

que l'on obtient en retranchant de 344 les entiers 5, 45, 125 sont égaux respectivement à

$$3.113, \ 13.23, \ 3.73;$$

ils n'ont donc pas la forme demandée.

Enfin, pour $m = 47$ (d'où $8m = 376$), on retrouve trois équations canoniques. L'équation

$$376 = 5.1^2 + 371 = 5.1^2 + 7.53$$

n'est pas de ce genre. Mais on a celles-ci :

$$376 = 5.3^2 + 331.1^2,$$
$$376 = 5.5^2 + 251.1^2,$$
$$376 = 5.7^2 + 131.1^2,$$

où

$$331, \ 251, \ 131$$

sont des nombres premiers. On voit donc que partout notre théorème est vérifié.

**3.** L'analyse qui m'a conduit à ce premier théorème en donne un second tout aussi simple.

**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

$$8m = x^2 + 5.p^{4l+1}y^2,$$

» $x$ et $y$ étant des entiers impairs et $p$ un nombre premier qui ne » divise pas $y$. »

On admet pour $l$ la valeur zéro. Quant au nombre premier $p$, nous ne lui imposons aucune condition. Mais puisque $x$ et $y$ sont impairs, l'équation

$$8m = x^2 + 5.p^{4l+1}y^2$$

entraînera nécessairement la congruence

$$5p \equiv -1 \pmod{8}$$

d'où

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

Ainsi $p$ ne peut être que de la forme $8\mu + 3$.

Nous avons compris dans un énoncé commun les nombres premiers $m$ des deux formes $20k+3$, $20k+7$; mais pour faciliter les vérifications numériques qu'on voudra entreprendre au sujet du théorème II, il est bon de considérer séparément le cas de

$$m = 20k+3$$

et celui de

$$m = 20k+7.$$

C'est ce que nous allons faire.

4. Soit d'abord

$$m = 20k+3.$$

On aura alors

$$8m \equiv -1 \pmod{5}.$$

Pour que

$$8m - x^2$$

soit divisible par 5, il faudra donc que l'entier impair et positif $x$ soit de la forme

$$10l + 3$$

ou de la forme

$$10l + 7.$$

Les valeurs de $x$ convenables ne peuvent donc être fournies que par la suite

$$3,\ 7,\ 13,\ 17,\ 23,\ \text{etc.}$$

Les carrés $x^2$ sont dès lors fournis par celle-ci :

$$9,\ 49,\ 169,\ 289,\ 529,\ \text{etc.}$$

Quand il s'agit d'un nombre premier $m$ de la forme $20k + 3$, notre théorème II consiste donc en ce que si du produit $8m$ on retranche, tant que faire se peut, les termes de la suite

$$9,\ 49,\ 169,\ 289,\ 529,\ \text{etc.}$$

on trouvera un nombre impair de restes susceptibles d'être mis sous la forme

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

$p$ désignant un nombre premier $(8\mu + 3)$ qui ne divise pas $y$.

Par cet énoncé, on abrége la recherche des équations canoniques propres à chaque valeur donnée de $m$.

Pour $m = 3$ (d'où $8m = 24$), on a immédiatement l'équation canonique

$$24 = 3^2 + 5.3.1^2.$$

Pour $m = 23$ (c'est-à-dire pour $8m = 184$), on a trois restes à examiner, savoir

$$175,\ 135,\ 15.$$

Le dernier conduit à l'équation canonique

$$184 = 13^2 + 5.3.1^2.$$

Les deux autres doivent être rejetés; car, divisés par 5, ils donnent respectivement le quotient $35 = 5.7$, qui n'a pas la forme voulue $p^{4l+1}y^2$, et le quotient $27 = 3^3$ qui ne l'a pas davantage, l'exposant 3 n'étant pas de la forme $4l+1$.

Pour $m = 43$ (d'où $8m = 344$), notre théorème est également vérifié. Le nombre des équations canoniques s'élève alors à trois. Les voici :

$$344 = 3^2 + 5.67.1^2,$$
$$344 = 7^2 + 5.59.1^2,$$
$$344 = 17^2 + 5.11.1^2.$$

5. Passons aux nombres premiers $m$ de la forme

$$20k + 7.$$

Pour qu'avec un tel nombre, la différence

$$8m - x^2$$

soit divisible par 5, il faut que l'entier impair et positif $x$ soit de la forme

$$10l + 1$$

ou de la forme

$$10l + 9.$$

Les valeurs de $x$ convenables ne peuvent donc être fournies que par la suite

$$1,\ 9,\ 11,\ 19,\ 21,\ \text{etc.}$$

Les carrés $x^2$ sont dès lors fournis par celle-ci :

$$1,\ 81,\ 121,\ 361,\ 441,\ \text{etc.}$$

Quand il s'agit d'un nombre premier $m$ de la forme $20k + 7$, notre théorème II consiste donc en ce que si du produit $8m$ on retranche, tant que faire se peut, les termes de la suite

$$1,\ 81,\ 121,\ 361,\ 441,\ \text{etc.},$$

il y aura un nombre impair de restes susceptibles d'être mis sous la forme

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

$p$ désignant un nombre premier $(8\mu + 3)$ qui ne divise pas $y$.

Avec cet énoncé, on trouve aisément les équations canoniques propres aux diverses valeurs de $m$.

Pour $m = 7$ (d'où $8m = 56$), on a immédiatement l'équation canonique

$$56 = 1^2 + 5.11.1^2.$$

Notre théorème est donc vérifié.

Il l'est également pour $m = 47$ (c'est-à-dire pour $8m = 376$). On trouve alors trois équations canoniques. Des quatre restes obtenus en retranchant de 376 les entiers

$$1,\ 81,\ 121,\ 361,$$

le troisième seul doit être rejeté; il est égal à $255 = 5.51$ et 51 (produit de 17 par 3) n'est pas de la forme

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

Les trois autres restes conduisent aux équations canoniques ci-après :

$$\begin{aligned}
376 &= \phantom{1}1^2 + 5.\ 3.5^2,\\
376 &= \phantom{1}9^2 + 5.59.1^2,\\
376 &= 19^2 + 5.\ 3.1^2.
\end{aligned}$$

Enfin, soit $m = 67$, d'où $8m = 536$. Les nombres à retrancher de 536 sont

$$1,\ 81,\ 121,\ 361,\ 441.$$

Les restes sont respectivement

$$535,\ 445,\ 415,\ 175,\ 95.$$

En les divisant par 5, on obtient les quotients

$$107,\ 91,\ 83,\ 35,\ 19,$$

dont deux n'ont pas la forme voulue, puisque l'on a

$$91 = 7.13$$

et

$$35 = 7.5.$$

Mais les autres donnent lieu, conformément à notre théorème, à un nombre impair d'équations canoniques :

$$536 = 1^2 + 5.107.1^2,$$
$$536 = 11^2 + 5.\ 83.1^2,$$
$$536 = 21^2 + 5.\ 19.1^2.$$

Je ne pousserai pas plus loin ces calculs.