JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

J. LIOUVILLE

Théorèmes concernant les nombres premiers contenus dans la formule $4A^2 + 5B^2$, en Y prenant A impair

Journal de mathématiques pures et appliquées 2e série, tome 11 (1866), p. 41-48.

<http://www.numdam.org/item?id=JMPA_1866_2_11__41_0>

THÉORÈMES

CONCERNANT

LES NOMBRES PREMIERS

CONTENUS DANS LA FORMULE $4A^2+5B^2$, EN Y PRENANT A IMPAIR;

PAR M. J. LIOUVILLE.

1. Les nombres premiers contenus dans la formule quadratique

$$4A^2+5B^2,$$

en y prenant A impair, sont de deux espèces; les uns appartiennent à la forme linéaire

$$40\mu+1,$$

les autres à la forme linéaire

$$40\mu+9.$$

Nous donnerons pour chacune de ces deux espèces de nombres premiers un théorème distinct.

2. Considérons d'abord les nombres premiers m qui sont à la fois de la forme linéaire

$$40\mu+1$$

et de la forme quadratique

$$4A^2+5B^2$$

où la valeur de A sera naturellement impaire. Je dis que pour chacun d'eux on pourra poser au moins une fois (et toujours un nombre impair de fois) l'équation

$$m = 2(10x + 3)^2 + p^{4l+1}y^2,$$

x étant un entier pair ou impair, positif, nul ou négatif, y un entier impair et positif, enfin p un nombre premier qui ne divise pas y : on admet pour l la valeur zéro.

Les nombres contenus dans la formule

$$2(10x + 3)^2,$$

en y prenant pour x un entier quelconque (positif, nul ou négatif) sont, par ordre de grandeur,

$$2.3^2,\quad 2.7^2,\quad 2.13^2,\quad 2.17^2,\quad 2.23^2,\quad \text{etc.},$$

c'est-à-dire

$$18,\quad 98,\quad 338,\quad 578,\quad 1058,\quad \text{etc.}$$

Notre théorème revient donc à dire que si d'un nombre premier m appartenant en même temps à la forme linéaire

$$40\mu + 1$$

et à la forme quadratique

$$4A^2 + 5B^2$$

on retranche tant que faire se peut les termes de la suite

$$18,\ 98,\ 338,\ 578,\ 1058,\ \text{etc.},$$

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.

Nous n'exigeons rien *à priori* au sujet du nombre premier p; mais il est aisé de voir que, d'après les conditions où nous nous plaçons, on ne peut pas manquer d'avoir $p \equiv 7$ (mod. 8) et p non-résidu quadratique de 5. Donc p sera toujours de l'une ou de l'autre des deux formes linéaires

$$40\nu + 7, \quad 40\nu + 23.$$

3. Prenons, par exemple, les nombres premiers

$$41, \ 241, \ 281, \ 601, \ 641, \ 881,$$

qui sont tous de la forme

$$40\mu + 1.$$

Comme ils remplissent aussi la seconde condition imposée par notre théorème, attendu que l'on a

$$\begin{aligned}
41 &= 4.3^2 + 5.1^2, \\
241 &= 4.7^2 + 5.3^2, \\
281 &= 4.3^2 + 5.7^2, \\
601 &= 4.7^2 + 5.9^2, \\
641 &= 4.3^2 + 5.11^2, \\
881 &= 4.3^2 + 5.13^2,
\end{aligned}$$

nous devrons trouver pour chacun d'eux un nombre impair de restes canoniques.

Or, pour 41, il n'y a qu'un reste, et ce reste est canonique comme le prouve l'identité

$$41 - 18 = 23.1^2.$$

Pour chacun des deux nombres premiers

$$241, \ 281,$$

il y a un reste canonique et un reste non canonique. On a, en effet, d'une part

$$241 - 18 = 223.1^2$$

et

$$241 - 98 = 143 = 11.13;$$

d'autre part,

$$281 - 18 = 263.1^2$$

et

$$281 - 98 = 183 = 3.61.$$

Pour 601, il y a quatre restes, dont trois canoniques et un non canonique. Celui-ci s'offre immédiatement, car

$$601 - 18 = 583 = 11.53.$$

Les restes suivants sont canoniques; c'est d'abord

$$601 - 98 = 503.1^2,$$

puis

$$601 - 338 = 263.1^2,$$

enfin

$$601 - 578 = 23.1^2.$$

Pour chacun des deux nombres premiers

$$641,\ 881,$$

il y a aussi quatre restes; mais un seul d'entre eux est canonique. Relativement à 641, on a d'abord trois restes non canoniques, savoir :

$$641 - 18 = 623 = 7.89,$$
$$641 - 98 = 543 = 3.181,$$
$$641 - 338 = 303 = 3.101;$$

mais le quatrième reste est canonique, car

$$641 - 578 = 7.3^2.$$

Relativement à 881, c'est au contraire le premier reste qui est canonique, puisque

$$881 - 18 = 863.1^2;$$

les trois autres restes sont non canoniques : on a d'abord

$$881 - 98 = 783 = 3^3.29,$$

ensuite

$$881 - 338 = 543 = 3.181,$$

enfin

$$881 - 578 = 303 = 3.101.$$

On voit que notre théorème est vérifié partout.

4. Considérons maintenant les nombres premiers m qui sont à la fois de la forme linéaire

$$40\mu + 9$$

et de la forme quadratique

$$4A^2 + 5B^2$$

où la valeur de A sera naturellement impaire. Je dis que pour chacun d'eux on pourra toujours poser au moins une fois (et toujours un nombre impair de fois) l'équation

$$m = 2(10x + 1)^2 + p^{4l+1}y^2,$$

x étant un entier pair ou impair, positif, nul ou négatif, y un entier impair et positif, enfin p un nombre premier qui ne divise pas y : on admet pour l la valeur zéro.

Les nombres contenus dans la formule

$$2(10x + 1)^2,$$

en y prenant pour x un entier quelconque (positif, nul ou négatif), sont par ordre de grandeur

$$2.1^2,\quad 2.9^2,\quad 2.11^2,\quad 2.19^2,\quad 2.21^2,\quad \text{etc.},$$

c'est-à-dire

$$2,\quad 162,\quad 242,\quad 722,\quad 882,\quad \text{etc.}$$

Notre théorème revient donc à dire que si d'un nombre premier m, appartenant à la fois à la forme linéaire

$$40\mu + 9$$

et à la forme quadratique

$$4A^2 + 5B^2,$$

on retranche tant que faire se peut les termes de la suite

$$2, \ 162, \ 242, \ 722, \ 882, \text{ etc.},$$

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.

Nous n'exigeons rien *à priori* au sujet du nombre premier p; mais cette fois encore il est visible que, dans les conditions où nous nous plaçons, p ne peut manquer d'être de l'une des deux formes linéaires

$$40\nu + 7, \quad 40\nu + 23.$$

5. Commençons par les deux exemples de

$$m = 409$$

et de

$$m = 449.$$

Les deux nombres premiers 409 et 449 étant en effet de la forme linéaire

$$40\mu + 9,$$

et aussi de la forme quadratique

$$4A^2 + 5B^2$$

puisque l'on a

$$409 = 4.1^2 + 5.9^2$$

et

$$449 = 4.9^2 + 5.5^2,$$

notre théorème doit avoir lieu pour eux.

Or je trouve respectivement pour 409 et pour 449 les restes canoniques

$$409 - 242 = 167.1^2$$

et

$$449 - 242 = 23.3^2.$$

Les autres restes sont non canoniques; car on a d'une part

$$409 - 2 = 407 = 11.37$$

et

$$409 - 162 = 247 = 13.19,$$

puis, d'autre part,

$$449 - 2 = 447 = 3.149$$

et

$$449 - 162 = 287 = 7.41.$$

Notre théorème a donc réellement lieu pour les nombres premiers cités.

Nous pouvons faire ensuite

$$m = 569,$$

attendu qu'en vertu des deux identités

$$569 = 40.14 + 9$$

et

$$569 = 4.9^2 + 5.7^2$$

le nombre premier 569 remplit les conditions voulues.

Cette fois encore il faudra retrancher de 569 les trois nombres

$$2,\ 162,\ 242.$$

Or le premier reste ainsi obtenu est canonique; car

$$569 - 2 = 567 = 7.9^2.$$

Mais les deux autres restes sont non canoniques. On a en effet

$$569 - 162 = 407 = 11.37,$$

où 11 et 37 sont des nombres premiers, puis

$$569 - 242 = 327 = 3.109,$$

où 3 et 109 sont de même premiers. Notre théorème a donc lieu comme plus haut.

Nous ne pensons pas qu'il soit utile de pousser plus loin ces vérifications numériques.