JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

J. LIOUVILLE

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

Journal de mathématiques pures et appliquées 2e série, tome 4 (1859), p. 399-400.

<http://www.numdam.org/item?id=JMPA_1859_2_4__399_0>

THÉORÈME

CONCERNANT

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

PAR M. J. LIOUVILLE.

Soit p un nombre premier de la forme $24\mu + 7$: considérons son double $2p$. Je me suis assuré par une démonstration assez simple que l'on peut poser au moins une fois, et toujours un nombre impair de fois, l'équation

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

où x et y sont des entiers positifs impairs et q un nombre premier de la forme $24\nu + 13$ qui ne divise pas y. Bien entendu, on peut avoir $l = 0$, $4l + 1 = 1$.

Comme pour chaque valeur de q l'équation

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

ne peut avoir lieu qu'une seule fois, notre théorème revient à dire qu'il y a un nombre impair de valeurs de q convenables.

En d'autres termes, si du double $2p$ d'un nombre premier donné $24\mu + 7$, on retranche les carrés impairs de grandeur moindre 1, 9, 25, 49,..., on pourra mettre au moins un des restes, et toujours un nombre impair de restes, sous la forme

$$q^{4l+1} \cdot y^2,$$

q étant un nombre premier $24\nu + 13$.

L'exemple le plus simple est 7. Or on a

$$2.7 = 1^2 + 13.1^2.$$

Vient ensuite 31 dont le double est 62. En retranchant de 62 les carrés 1, 9, 25, 49, on a ces restes

$$61,\ 53,\ 37,\ 13,$$

qui sont tous les quatre des nombres premiers. Mais trois d'entre eux seulement sont de la forme $24\nu + 13$ et donnent lieu à des expressions de 62 du type voulu

$$1^2 + 61.1^2,\quad 5^2 + 37.1^2,\quad 7^2 + 13.1^2.$$

On pouvait, au surplus, se dispenser d'essayer le carré de 3; car les formes linéaires assignées à p et q dans notre équation

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

ne permettent pas que x (ni y) soit divisible par 3.