

JOURNAL
DE
MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

HERMITE

**Démonstration élémentaire d'une proposition relative
aux diviseurs de $x^2 + Ay^2$**

Journal de mathématiques pures et appliquées 1^{re} série, tome 14 (1849), p. 451-452.

http://www.numdam.org/item?id=JMPA_1849_1_14__451_0



NUMDAM

Article numérisé dans le cadre du programme
Gallica de la Bibliothèque nationale de France
<http://gallica.bnf.fr/>

et catalogué par Mathdoc
dans le cadre du pôle associé BnF/Mathdoc
<http://www.numdam.org/journals/JMPA>

*Démonstration élémentaire d'une proposition relative aux
diviseurs de $x^2 + Ay^2$;*

PAR M. HERMITE.

Je dis que p désignant un diviseur de la formule $x^2 + Ay^2$, une puissance convenablement déterminée de p pourra toujours être représentée par cette forme, c'est-à-dire qu'on pourra toujours faire

$$p^\mu = X^2 + AY^2.$$

Soit pour une valeur entière quelconque de μ , α_μ une valeur de $\sqrt{-A} \pmod{p^\mu}$: l'expression

$$(xp^\mu - y\alpha_\mu)^2 + Ay^2$$

représentera toujours des nombres entiers divisibles par p^μ , et je dis en premier lieu qu'on pourra toujours déterminer x et y de telle manière qu'on ait

$$\frac{(xp^\mu - y\alpha_\mu)^2 + Ay^2}{p^\mu} < 2\sqrt{A}.$$

En effet, il suffira de développer en fraction continue $\frac{\alpha_\mu}{p^\mu}$, jusqu'à ce qu'on arrive à une réduite telle que son dénominateur étant moindre que $\frac{p^{\frac{1}{2}\mu}}{\sqrt{A}}$, cette limite soit atteinte ou surpassée par le dénominateur de la réduite suivante. Les valeurs de x et y seront respectivement le numérateur et le dénominateur de cette réduite. Cela posé, on voit que, par une infinité de valeurs de μ , on aura la représentation d'un même multiple de p^μ par la forme $x^2 + Ay^2$. Ainsi, en nommant k

ce multiple, on trouvera nécessairement deux équations

$$k p^{\mu} = x^2 + A y^2,$$

$$k p^{\mu'} = x'^2 + A y'^2,$$

dans lesquelles $x - x'$ et $y - y'$ seront à la fois divisibles par k . Sous cette condition il vient, en multipliant membre à membre les deux équations précédentes,

$$k^2 \cdot p^{\mu + \mu'} = (xx' + Ayy')^2 + A(xy' - yx')^2.$$

Or $xy' - yx'$ est divisible par k , puisqu'on a

$$x \equiv x', \quad y \equiv y' \pmod{k};$$

donc il en est de même de $xx' + Ayy'$, et finalement la puissance $\mu + \mu'$ de p se trouve bien représentée par la forme $x^2 + Ay^2$.

Il est facile de voir qu'une démonstration toute semblable s'applique au cas de A négatif; on a, au reste, un théorème plus général et dont voici l'énoncé :

« p étant un diviseur de la norme d'un nombre complexe quelconque, formé avec les racines $m^{\text{ièmes}}$ de l'unité, on pourra toujours déterminer une puissance entière de p , qui soit représentée précisément par cette norme. »

FIN DU QUATORZIÈME VOLUME.