JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

J.-A. SERRET

Note sur un théorème de la théorie des nombres

Journal de mathématiques pures et appliquées 1re série, tome 17 (1852), p. 186-189.
<http://www.numdam.org/item?id=JMPA_1852_1_17__186_0>

NOTE

SUR UN THÉORÈME DE LA THÉORIE DES NOMBRES;

PAR M. J.-A. SERRET.

(Communiquée à la Société Philomatique le 12 avril 1851.)

On sait par quelle brillante analyse M. Lejeune-Dirichlet est parvenu à démontrer que :

Toute progression par différence dont le premier terme et la raison sont premiers entre eux renferme une infinité de nombres premiers; ou, en d'autres termes, que :

La formule $ax + b$, où a et b sont des entiers donnés sans diviseurs communs, renferme une infinité de nombres premiers.

Peut-être n'est-il pas sans intérêt de remarquer que, dans le cas d'une progression dont la raison est 8 ou 12, le théorème de l'illustre géomètre allemand peut se déduire des principes les plus élémentaires de la théorie des nombres. C'est ce que je me propose de montrer dans cette Note.

Soient N un nombre quelconque, et

$$2,\ 3,\ 5,\ 7,\ 11,\ldots,\ p$$

les nombres premiers qui ne surpassent pas N : posons

$$\begin{aligned}
A &= (2.3.5.7.11\ldots p)^4 + 1,\\
B &= (3.5.7.11\ldots p)^2 + 2,\\
C &= (3.5.7.11\ldots p)^2 + 2^2,\\
D &= (3.5.7.11\ldots p)^2 - 2,\\
E &= (2.3.5.7.11\ldots p)^4 - (2.3.5.7.11\ldots p)^2 + 1,\\
F &= (2.5.7.11\ldots p)^2 + 1,\\
G &= (2.5.7.11\ldots p)^2 + 3,\\
H &= 3(2.5.7.11\ldots p)^2 - 1.
\end{aligned}$$

1°. A est de la forme $a^4 + 1 = (a^2 - 1)^2 + 2a^2$, c'est-à-dire de l'une et de l'autre des deux formes $t^2 + u^2$ et $t^2 + 2u^2$; il s'ensuit que les facteurs premiers de A ont ces mêmes formes quadratiques, et, par suite, qu'ils ont tous la forme linéaire $8x + 1$.

2°. B est de la forme $t^2 + 2u^2$; ses facteurs premiers ont, par suite, cette même forme et sont de l'une ou de l'autre des formes linéaires $8x + 1$ et $8x + 3$. D'ailleurs B est de la forme $8x + 3$; donc l'un au moins de ses facteurs premiers a cette même forme $8x + 3$.

3°. C est de la forme $t^2 + u^2$; ses facteurs premiers ont cette même forme et sont de l'une ou de l'autre des deux formes linéaires $8x + 1$ et $8x + 5$; mais comme C a la forme $8x + 5$, un au moins de ses facteurs premiers a aussi la forme $8x + 5$.

4°. D est de la forme $t^2 - 2u^2$; ses facteurs premiers ont cette même forme et sont de l'une ou de l'autre des deux formes linéaires $8x + 1$ et $8x + 7$; mais comme D a la forme $8x + 7$, un au moins de ses facteurs premiers a lui-même la forme $8x + 7$.

5°. E est de la forme $a^4 - a^2 + 1 = (a^2 - 1)^2 + a^2 = (a^2 + 1)^2 - 3a^2$, c'est-à-dire de l'une et de l'autre des deux formes $t^2 + u^2$ et $t^2 - 3u^2$; il s'ensuit que les facteurs premiers de E ont ces mêmes formes. Or ces formes quadratiques ne peuvent appartenir en même temps qu'aux nombres $12x + 1$; donc tous les facteurs premiers de E sont de la forme $12x + 1$.

6°. F est de la forme $t^2 + u^2$; ses facteurs premiers ont cette même forme et sont de l'une ou de l'autre des deux formes linéaires $12x + 1$, $12x + 5$. En outre, la première partie de F est le carré du produit de tous les nombres premiers jusqu'à p, 3 excepté, produit qui est de la forme $6x \pm 2$; il s'ensuit que F a la forme linéaire $12x + 5$ et que l'un au moins de ses facteurs premiers a cette même forme.

7°. G est de la forme $t^2 + 3u^2$; ses facteurs premiers ont cette même forme quadratique et sont de l'une ou de l'autre des deux formes linéaires $12x + 1$ et $12x + 7$; mais comme G est de la forme $12x + 7$, l'un de ses facteurs premiers a nécessairement cette même forme $12x + 7$.

8°. H est de la forme $3t^2 - u^2$; ses facteurs premiers sont de l'une ou de l'autre des deux formes $3t^2 - u^2$ et $t^2 - 3u^2$; ils sont, par suite, de l'une des formes linéaires $12x+1$ et $12x+11$. D'ailleurs H a la forme $12x + 11$; donc l'un de ses facteurs premiers a aussi cette forme.

De ce qui précède et de ce que les facteurs premiers des nombres A, B, C, D, E, F, G, H sont évidemment tous supérieurs à N, il résulte que chacune des huit formules

$$8x+1, \quad 8x+3, \quad 8x+5, \quad 8x+7,$$
$$12x+1, \quad 12x+5, \quad 12x+7, \quad 12x+11,$$

renferme un nombre premier plus grand que N; en d'autres termes. *chacune des huit formules dont il s'agit renferme une infinité de nombres premiers.*

Les considérations qui précèdent s'appliquent encore à la formule $10x + 9$. Conservons, en effet, nos notations et considérons le nombre

$$5.(2.3.7.11\ldots p)^2 - 1;$$

ses diviseurs sont de la forme quadratique $5t^2 - u^2$, et, par suite, de l'une des formes linéaires $10x+1$, $10x+9$: mais le nombre dont il s'agit est de la forme $10x+9$; donc l'un au moins de ses facteurs premiers a la même forme. On conclut de là que la formule $10x+9$ renferme un nombre premier plus grand que N, ou qu'elle renferme une infinité de nombres premiers.

M. Lebesgue a remarqué (tome VIII de ce Journal, page 51) que le théorème sur la progression par différence peut se déduire d'un théorème connu d'Euler, dans le cas particulier où la raison est un nombre premier et où le premier terme est l'unité. Par un raisonnement du même genre, on peut prouver plus généralement que :

Toute progression par différence qui commence par l'unité renferme une infinité de nombres premiers.

On sait, en effet (*voir* LEGENDRE, *Théorie des Nombres*, tome I^er^, page 222), que les diviseurs *propres* de $a^n + 1$ sont de la forme $2nx + 1$. J'appelle diviseurs propres de $a^n + 1$ ceux qui ne divisent

en même temps aucun nombre tel que $a^{n'}+1$ où n' désigne le quotient de n par un de ses diviseurs impairs. Cela posé, il est très-facile d'établir que a^n+1 a au moins un facteur premier propre. Il n'y a qu'une seule exception : c'est le cas de $a=2$ et $n=3$. On déduit facilement de là le théorème en question. Car soient

$$2,\ 3,\ 5,\ 7,\ \ 11,\ldots,\ p$$

les nombres premiers qui ne surpassent pas un nombre donné N; le nombre

$$(2.3.5.7.11\ldots p)^n+1$$

admet un facteur premier propre, lequel est de la forme $2nx+1$. D'ailleurs ce facteur est nécessairement plus grand que N; donc la formule $2nx+1$ renferme un nombre premier plus grand que N, et, par suite, elle renferme une infinité de nombres premiers.