NOUVELLES ANNALES DE MATHÉMATIQUES

LEBESGUE

# Remarques diverses sur les nombres premiers

*Nouvelles annales de mathématiques 1re série*, tome 15 (1856), p. 130-134

<http://www.numdam.org/item?id=NAM_1856_1_15__130_0>

# REMARQUES DIVERSES SUR LES NOMBRES PREMIERS;

PAR M. LEBESGUE,
Professeur.

1. THÉORÈME. *On peut toujours trouver tant de nombres consécutifs qu'on voudra qui ne soient pas premiers.*

La démonstration est bien simple et bien connue; elle peut être présentée ainsi qu'il suit : Si l'on veut avoir au moins $2n$ nombres consécutifs non premiers, on représentera la suite complète des nombres premiers par

$$p_0 = 2, \quad p_1 = 3, \quad p_2 = 5, \ldots, \quad p_{i-1}, \; p_i, \; p_{i+1}.$$

Supposons que $n$ tombe entre $p_{i-1}$ et $p_i$, on fera

$$\mathrm{P} = p_0 \, p_1 \, p_2 \ldots p_{i-1}.$$

Comme P, $p_{i+1}$, $p_i$ sont premiers entre eux, on pourra toujours trouver des entiers $x$, $y$, $z$, tels, qu'on ait

$$\mathrm{P}x - 1 = p_i y,$$
$$\mathrm{P}x + 1 = p_{i+1} z,$$

et il en résultera que les

$$1 + 2(p_i - 1) = 2p_i - 1$$

nombres

$$\mathrm{P}x - (p_i - 1),$$
$$(a) \quad \ldots, \; \mathrm{P}x - 1, \; \mathrm{P}x, \; \mathrm{P}x + 1, \; \mathrm{P}x + 2, \ldots,$$
$$\mathrm{P}x + (p_i - 1),$$

sont composés, et que chaque terme est divisible par un des nombres

$$2, \; 3, \; 5, \ldots, \; p_{i-1}, \; p_i, \; p_{i+1}.$$

Cela résulte des équations données plus haut pour les trois termes moyens

$$Px - 1, \quad Px, \quad Px + 1.$$

D'ailleurs P est divisible par les nombres

$$2, \ 3, \ 5, \ p_{i-1},$$

et il en est de même des nombres consécutifs

$$2, \ 3, \ 4, \ 5, \ 6, \ 7, \ p_i - 1.$$

Ainsi les $2p_i - 1$ nombres $(a)$ sont composés. Comme

$$p_i > n, \quad 2p_i - 1 > 2n - 1,$$

on a plus de $2n$ nombres consécutifs non premiers. Si l'on supprimait dans les nombres $(a)$ les nombres pairs, il resterait $p_i - 1$ nombres impairs

$$Px - (p_i - 2),$$
$$\ldots, \ Px - 1, \quad Px + 1, \ldots,$$
$$Px + p_i - 2,$$

contenant

$$2 \times \frac{p_i - 1}{2} = p_i - 1 \text{ termes}.$$

De là ce théorème de Legendre :

*On peut trouver* $p_i - 1$ *nombres impairs consécutifs non premiers et divisibles chacun par quelques-uns des nombres*

$$3, \ 5, \ 7, \ldots, \ p_i, \ p_{i+1}$$

Quand on admet des diviseurs quelconques au lieu des diviseurs consécutifs, on obtient des solutions en nombres bien plus petits. On peut d'ailleurs en trouver à l'aide de la Table de Burckhardt. Entre les deux nombres premiers 3029867 et 3029947, dont la différence est 80, il n'y a pas de nombres premiers.

Legendre a cru avoir démontré qu'on ne saurait trouver plus de $p_i - 1$ nombres impairs consécutifs dont chacun fût divisible par quelqu'un des nombres

$$3,\ 5,\ 7,\ \ldots,\ p_{i+1}.$$

Il n'a fait que donner à la proposition une grande probabilité. Ainsi il n'a point prouvé que la formule

$$Ax + B,$$

où A et B sont premiers entre eux, ou encore que la progression arithmétique

$$B,\quad B+A,\quad B+2A,\quad B+3A,\ldots$$

renferme une infinité de nombres premiers. Cette importante proposition a été démontrée par M. Dirichlet dans un Mémoire extrêmement remarquable (dont M. Terquem a donné la traduction dans le *Journal de Mathématiques*, t. IV, p. 39), et sa méthode lui a donné par suite nombre d'importants théorèmes.

On peut voir dans un article de M. Desboves (*Nouvelles Annales*, t. XIV, p. 281) en quoi consiste l'imperfection de la démonstration de Legendre. Cependant comme il n'est pas prouvé que la proposition soit inexacte, et qu'on peut même l'établir rigoureusement pour un petit nombre de diviseurs consécutifs, par exemple pour

$$3,\ 5,\ 7,$$

on peut demander si la chose étant admise pour la suite de diviseurs

$$3,\ 5,\ 7,\ \ldots,\ p_{i+1},$$

est vraie aussi pour la suite

$$3,\ 5,\ 7,\ \ldots,\ p_{i+2}.$$

Ainsi M. Gauss ayant vérifié la loi de réciprocité de Legendre jusqu'à une certaine limite, a montré par une réduction à l'absurde que la limite pouvait être reculée, de sorte que la loi s'est trouvée généralement établie.

Cette démonstration très-compliquée a été notablement simplifiée par M. L. Dirichlet dans le tome XLVII du *Journal* de M. Crelle. Quelques propositions de ce Mémoire établissent très-simplement que les formules

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

renferment une infinité de nombres premiers. M. Serret en a déjà donné une démonstration élémentaire dans le *Journal de Mathématiques*, t. XVII, p. 186.

2. Théorème. *Les formules*

$$4x+1, \quad 4x+3$$

*renferment une infinité de nombres premiers.*

1°. On ne saurait avoir $y^2+1$ divisible par un nombre premier $4\alpha+3$, car en supposant que $4\alpha+3$ soit le moindre diviseur de cette forme, on aurait

$$y^2+1=(4\alpha+3)z.$$

Or on peut toujours poser

$$y=(4\alpha+3)n\pm r$$

de manière à avoir $r$ pair inférieur à $4\alpha+3$. De là

$$r^2+1=4k+1=(4\alpha+3)(4n+3),$$

$4n+3$ étant nécessairement inférieur à $4\alpha+3$; or $4n+3$ a nécessairement un diviseur premier de forme $4\beta+3$, inférieur à $4\alpha+3$, ce qui est contre l'hypothèse.

(Cette démonstration est dans le Mémoire cité plus haut.)

2°. Il y a une infinité de nombres premiers $4k+1$; car si $p_1, p_2, \ldots, p_i$ étaient les seuls de cette forme, on aurait

$$N = 4(p_1, p_2, \ldots, p_i)^2 + 1$$

composé et divisible par un nombre premier de forme $4k+1$ et nécessairement autre que l'un des nombres $p_1, p_2, \ldots, p_i$ qui ne divisent pas N.

3°. Il y a une infinité de nombres premiers de la forme $4k+3$, car si $p_1, p_2, \ldots, p_i$ étaient les seuls nombres de cette forme, on aurait

$$N = 4p_1, p_2, \ldots, p_i + 3$$

composé et ayant un diviseur $4k+3$, autre que l'un des nombres $p_1, p_2, \ldots, p_i$ qui ne divisent pas N. Cette démonstration est imitée d'Euclide.