DÉMONSTRATION
D'UN THÉORÈME NOUVEAU
CONCERNANT LES NOMBRES PREMIERS[1].

(*Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin*, année 1771[2].)

1. Je viens de trouver, dans un excellent Ouvrage de M. Waring que j'ai reçu depuis peu[3], un très-beau Théorème d'Arithmétique, que voici :

Si n est un nombre premier quelconque, le nombre

$$1.2.3.4.5\ldots(n-1)+1$$

sera toujours divisible par n;

c'est-à-dire que le produit continuel des nombre 1, 2, 3,... jusqu'à $n-1$ inclusivement; étant augmenté de l'unité, sera divisible par n, ou bien, que si l'on divise ce même produit par le nombre premier n, on aura -1, ou, ce qui est la même chose, $n-1$ pour reste.

Par exemple,

soit	$n=3$,	on aura	$1.2+1=3$,
	$n=5$,		$1.2.3.4+1=25$,
	$n=7$,		$1.2.3.4.5.6+1=721=7.103$,
	$n=11$,		$1.2.3\ldots10+1=3628801=11.329891$,
	$n=13$,		$1.2.3\ldots12+1=479001601=13.36846277$,
	.....,		.....

M. Waring fait honneur de ce Théorème à M. Jean Wilson, mais il n'en donne point la démonstration, et il paraît même insinuer que personne ne l'a encore trouvée; du moins il semble qu'il la regarde comme extrêmement difficile; car, après avoir rapporté ce Théorème avec quelques autres qui en dépendent, il ajoute : *Demonstrationes vero hujusmodi propositionum eo magis difficiles erunt, quod nulla finge potest notatio, quæ primum numerum exprimat.*

Cette raison, jointe à l'élégance et à l'utililté du Théorème dont it s'agit, m'a engagé à en chercher une démonstration, et celle que j'ai trouvée m'a paru mériter l'attention des Géomètres, tant par elle-même que parce qu'elle fait connaître en même temps quelques autres propriétés des nombres premiers, qui n'avaient pas encore, ce me semble, été remarquées.

Lemme.

2. *Étant donné le produit continuel*

$$(x+1)(x+2)(x+3)(x+4)\ldots(x+n-1),$$

on propose de le développer suivant les puissances de x.

Il est visible qu'on aura

$$\begin{aligned}&(x+1)(x+2)(x+3)(x+4)\ldots(x+n-1)\\&\quad=x^{n-1}+A'x^{n-2}+A''x^{n-3}+A'''x^{n-4}+\ldots+A^{(n-1)},\end{aligned}$$

et pour déterminer facilement les coefficients A', A'', A''',..., on remarquera que l'équation précédente devant être identique subsistera également en y mettant $x+1$ à la place de x; c'est pourquoi on aura aussi

$$\begin{aligned}&(x+2)(x+3)(x+4)(x+5)\ldots(x+n)\\&\quad=(x+1)^{n-1}+A'(x+1)^{n-2}+A''(x+1)^{n-3}+A'''(x+1)^{n-4}+\ldots+A^{(n-1)};\end{aligned}$$

donc, multipliant toute cette équation par $x+1$, et la comparant ensuite à la précédente multipliée par $x+n$, on en tirera celle-ci

$$\begin{aligned}&(x+n)(x^{n-1}+A'x^{n-2}+A''x^{n-3}+A'''x^{n-4}+\ldots+A^{(n-1)})\\&\quad=(x+1)^n+A'(x+1)^{n-1}+A''(x+1)^{n-2}+A'''(x+1)^{n-3}+\ldots+A^{(n-1)}(x+1),\end{aligned}$$

[1] Lu à l'Académie le 13 juin 1771.

[2] *Œuvres de Lagrange*, t. III, pp. 425–438.

[3] *Meditationes algebraïcæab Eduardo Waring, Matheseos Professore Lucasiano, etc.* Cantabrigiæ, 1770; *voyez* page 218.

c'est-à-dire, en développant les termes et les ordonnant par rapport à x,

$$\begin{aligned}
&x^n + (n + A')x^{n-1} + (nA' + A'')x^{n-2} + (nA'' + A''')x^{n-3} + \dots \\
=&x^n + (n + A')x^{n-1} + \left[\frac{n(n-1)}{2} + (n-1)A' + A''\right] x^{n-2} \\
&+ \left[\frac{n(n-1)(n-2)}{2.3} + \frac{(n-1)(n-2)}{2}A' + (n-2)A'' + A'''\right] x^{n-2} + \dots .
\end{aligned}$$

Donc, puisque cette équation est identique, on aura, en comparant terme à terme,

$$\begin{aligned}
n+A' =&n + A', \\
nA'+A'' =&\frac{n(n-1)}{2} + (n-1)A' + A'', \\
nA''+A''' =&\frac{n(n-1)(n-2)}{2.3} + \frac{(n-1)(n-2)}{2}A' + (n-2)A'' + A''', \\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots ,
\end{aligned}$$

d'où l'on tire

$$\begin{aligned}
A' &= \frac{n(n-1)}{2}, \\
2A'' &= \frac{n(n-1)(n-2)}{2.3} + \frac{(n-1)(n-2)}{2}A', \\
3A''' &= \frac{n(n-1)(n-2)(n-3)}{2.3.4} + \frac{(n-1)(n-2)(n-3)}{2.3}A' + \frac{(n-2)(n-3)}{2}A'',
\end{aligned}$$

et ainsi de suite.

COROLLAIRE.

3. Il est clair, par la théorie des équations, que les coefficients A', A'', A''', ... ne sont autre chose que les sommes des nombres naturels 1, 2, 3, ... jusqu'à $n-1$ inclusivement, des produits de ces nombres multipliés deux á deux, trois à trois, etc.; en sorte que le dernier coefficient $A^{(n-1)}$ sera égal au produit $1.2.3.4\dots(n-1)$; ainsi tous les nombres A', A'', A''', ... seront nécessairement entiers.

THÉORÈME.

4. *Les mêmes choses étant posées que dans le Lemme précédent, je dis que, si n est un nombre premier, les nombres A', A'', A''', ... jusqu'à $A^{(n-2)}$ inclusivement, sont tous divisibles par n, et que le dernier nombre $A^{(n-1)}$ sera divisible par n, étant augmenté de l'unité.*

On sait que les expressions

$$\frac{n(n-1)}{2}, \quad \frac{n(n-1)(n-2)}{2.3}, \dots, \quad \frac{(n-1)(n-2)}{2}, \quad \frac{(n-1)(n-2)(n-3)}{2.3}, \dots$$

dénotent toujours des nombres entiers, tant que n est un nombre entier; puisque ce sont les coefficients du binôme élevé à la puissance n, ou $n-1$, ou, etc. De plus il est clair que, si n est un nombre premier, les nombres

$$\frac{n(n-1)}{1.2}, \quad \frac{n(n-1)(n-2)}{1.2.3}, \dots$$

seront tous divisibles par n, à l'exception seulment du dernier nombre

$$\frac{n(n-1)(n-2)\dots 1}{1.2.3\dots n}$$

qui est égal à l'unité; car il est visible que le numérateur de chacun de ces nombres est divisible par n, et que le dénominateur ne l'est pas, tant que n est premier; d'où il s'ensuit qu'après avoir divisé le numérateur par le dénominateur, il restera nécessairement dans le quotient le facteur n.

De là et des formules du Lemme précédent il est facile de conclure :

1° Que A' sera divisble par n, que $2A''$ le sera aussi, et de même $3A'''$, $4A^{\text{iv}}$, ... jusqu'à $(n-2)A^{(n-2)}$; et que par conséquent les nombres A', A'', A''', ..., $A^{(n-2)}$ que nous avons vu devoir être toujours entiers (**3**), seront eux-mêmes toujours divisible par n, au moins tant que n sera premier;

2° Que le nombre $A^{(n-1)}$ étant augmenté de l'unité sera divisible par n; car la formule qui servira à déterminer sa valeur sera

$$(n-1)A^{(n-1)} = \frac{n(n-1)(n-2)\dots 1}{1.2.3\dots n} + \frac{(n-1)(n-2)\dots 1}{1.2\dots(n-1)}A' + \frac{(n-2)(n-3)\dots 1}{1.2\dots(n-2)}A'' + \dots,$$

c'est-à-dire

$$(n-1)A^{(n-1)} = 1 + A' + A'' + A''' + \dots + A^{(n-2)};$$

donc

$$A^{n-1} + 1 = nA^{(n-1)} - A' - A'' - A''' - \dots - A^{(n-2)};$$

donc, puisque A', A'', $\dots$, $A^{(n-2)}$ sont tous divisibles par n, il s'ensuit que $A^{(n-1)} + 1$ sera toujours divisible par n.

COROLLAIRE I.

5. Donc (**3**) le nombre

$$1.2.3.4\dots(n-1) + 1$$

sera toujours divisible par n, lorsque n sera un nombre premier, ce qui est le Théorème qu'il s'agissait de démontrer.

En général, il s'ensuit de la formule du n° **2** que, quel que soit le nombre entier x, on aura toujours

$$(x+1)(x+2)(x+3)\dots(x+n-1) - x^{n-1} + 1$$

divisible par n, tant que n sera un nombre premier.

Donc :

1° Si x^{n-1} est divisible par n, ce qui ne peut arriver que lorsque x est égal à zéro ou égal à un multiple de n, le nombre

$$(x+1)(x+2)(x+3)\dots(x+n-1) + 1$$

sera toujours divisible par n; ce qui donne le Théorème de M. Wilson en faisant $x = 0$.

2° Si x n'est ni nul ni divisible par n, ce qui arrive lorsque $x = \mu n + \rho$, ρ étant un nombre quelconque entier moindre que n, il est clair que quelqu'un des nombres

$$x+1, \quad x+2, \quad x+3, \dots, \quad x+n-1$$

sera nécessairement divisible par n, et que le produit

$$(x+1)(x+2)(x+3)\dots(x+n-1)$$

sera par conséquent toujours divisible par n; donc $-x^{n-1}+1$, ou bien $x^{n-1}-1$ sera dans ce cas toujours divisible par n; ce qui est le fameux Théorème de Fermat dont M. Euler a donné plusieurs démonstrations dans les *Commentaires de Pétersbourg*. La nôtre a, comme on voit, l'avantage de faire voir la liaison et la dépendance mutuelle des deux Théorèmes dont il s'agit.

COROLLAIRE II.

6. Puisque

$$n-1, \quad n-2, \quad n-3, \dots$$

étant divisés par n donnent pour restes

$$-1, \quad -2, \quad -3, \dots,$$

on pourra mettre ces restes à la place des nombres $n-1$, $n-2$, $\dots$ dans la formule

$$1.2.3\dots(n-1);$$

et l'on aura les formules suivantes

$$\begin{array}{l} 1.2.3\ \dots\ (n-1)+1, \\ 1.2.3\ \dots\ (n-2)-1, \\ 1.2^2.3\ \dots\ (n-3)+1, \\ 1.2^2.3^2.4...(n-4)-1, \\ \dots\dots\dots\dots\dots\dots\dots, \end{array}$$

qui seront toutes divisibles par n; donc aussi

$$\left[1.2.3\ldots\left(\frac{n-1}{2}\right)\right]^2 \pm 1$$

sera divisible par n, le signe supérieur ayant lieu lorsque $\frac{n-1}{2}$ est un nombre pair, et l'inférieur lorsque $\frac{n-1}{2}$ est impair.

1° *Soit* $\frac{n-1}{2} = 2m$, *et par conséquent* $n = 4m+1$; *dans ce cas* $(1.2.3\ldots 2m)^2+1$ *sera divisible par* n.

Ainsi l'on aura une somme de deux carrés qui sera divisible par $4m+1$ lorsque ce nombre sera premier; c'est ce qu'on n'avait pu trouver jusq'à présent d'une manière générale; seulment on avait pu prouver, d'une manière même assez indirecte, qu'il existait toujours une pareille somme divisible par n lorsque n était de la forme $4m+1$ (*voyez* le tome V des *Nouveaux Mémoires de Pétersbourg*).

2° *Soit* $\frac{n-1}{2} = 2m-1$, *et par conséquent* $n = 4m-1$; *dans ce cas* $[1.2.3\ldots(2m-1)]^2-1$ *sera divisible par* n.

Mais

$$[1.2.3\ldots(2m-1)]^2-1 = [1.2.3\ldots(2m-1)+1][1.2.3\ldots(2m-1)-1];$$

donc, puisque n est un nombre premier, il faudra que l'un ou l'autre des deux facteurs

$$1.2.3\ldots(2m-1)+1 \quad \text{ou} \quad 1.2.3\ldots(2m-1)-1,$$

soit divisible par n; donc

$$1.2.3\ldots(2m-1)\pm 1$$

sera nécessairement divisible par n.

Remarque I.

7. Les propositions des Corollaires précédents sont d'autant plus remarquables que, si n n'était pas premier, les nombres que nous avons vu devoir être divisibles par n, dans l'hypothèse de n premier, ne le seraient plus. Car, si n n'est pas un nombre premier, il sera donc divisible par quelqu'un des nombres 2, 3, ..., $n-1$ moindres que n; donc, si

$$1.2.3\ldots(n-1)+1$$

était divisible par n, il faudrait qu'il le fût aussi par quelqu'un des nombres 2, 3, 4, ..., $n-1$; or c'est ce qui ne se peut; car le nombre $1.2.3\ldots(n-1)$ étant divisible par chacun de ces nombres, il est clair qu'en divisant par un quelconque d'eux le nombre

$$1.2.3\ldots(n-1)+1$$

on aura toujours l'unité pour reste.

On peut donc tirer de là une méthode directe pour reconnaître si un nombre quelconque impair n est premier ou non; il n'y aura qu'à voir si le produit continuel des nombres 2, 3, 4, ..., $n-2$, étant divisé par n, donne 1 pour reste, alors le nombre sera premier; sinon, il ne le sera pas. On peut encore simplifier cette règle en distinguant les deux cas où n est de la forme $4m+1$ ou de la forme $4m-1$; dans le premier cas, le nombre n sera premier, si le carré du produit continuel des nombres 2, 3, 4 ..., $2m$ étant divisé par n donne -1 ou $n-1$ pour reste; et dans le second, si le produit continuel des nombres 2, 3, 4, ..., $2m-1$ étant divisé par n donne 1 ou -1 pout reste; sinon, n ne sera pas premier.

J'avoue au reste que cette méthode devient extrêmement laborieuse, et presque impracticable, lorsque n est un très-grand nombre; mais il peut y avoir des moyens d'en simplifier la pratique, et c'est une recherche à laquelle nous invitons les Géomètres.

Remarque II.

8. On pourrait déduire du Théorème de M. Fermat une autre démonstration de celui de M. Wilson beaucoup plus simple que celle que nous en avons donnée ci-dessus.

Car, si l'on considère la suite des nombres naturels 1, 2, 3, ..., n, élevés à la puissance $(n-1)^{ième}$, et qu'on cherche la différence $(n-1)^{ième}$ des termes de cette suite, il est facile de voir, par la théorie des différences, qu'elle sera

$$n^{n-1} - (n-1)(n-1)^{n-1} + \frac{(n-1)(n-2)}{2}(n-2)^{n-1}$$
$$- \frac{(n-1)(n-2)(n-3)}{2.3}(n-3)^{n-1} + \ldots + 1;$$

d'autre part, comme la série

$$1, \quad 2^{n-1}, \quad 3^{n-1}, \ldots$$

est une série algébrique de l'ordre $(n-1)^{ième}$, on sait que la différence du même ordre sera exprimée par le produit continuel des nombres 1, 2, $3 \ldots$, $n-1$; ainsi l'on aura l'équation

$$\begin{aligned} 1.2.3.4 \ldots (n-1) =& n^{n-1} - (n-1)(n-1)^{n-1} + \frac{(n-1)(n-2)}{2}(n-2)^{n-1} \\ & - \frac{(n-1)(n-2)(n-3)}{2.3}(n-3)^{n-1} + \ldots + 1. \end{aligned}$$

Supposons maintenant qu'on divise le second membre de cette équation par n, et qu'on ne veuille tenir compte que du reste qui en proviendra; il est d'abord clair que le terme n^{n-1} donnera pour reste 0, et que les termes $(n-1)^{n-1}$, $(n-2)^{n-2}, \ldots$ donneront tous l'unité pour reste, par le Théorème de M. Fermat; donc, mettant à la place de ces termes leurs restes 0, 1, 1, …, on aura le reste total

$$-(n-1) + \frac{(n-1)(n-2)}{2} - \frac{(n-1)(n-2)(n-3)}{2.3} + \ldots,$$

ou bien

$$(1-1)^{n-1} - 1, \quad \text{c'est-à-dire} \quad -1;$$

ainsi le reste de la division de $1.2.3 \ldots (n-1)$ par n sera -1, et par conséquent

$$1.2.3 \ldots (n-1) + 1$$

sera toujours divisible par n, pourvu que n soit premier; condition nécessaire pour l'exactitude du Théorème de M. Fermat.

Remarque III.

9. Avant de quitter cette matière, nous croyons devoir démontrer encore quelques autres Théorèms sur les nombres premiers, qu'on trouve aussi sans démonstrations dans le même Ouvrage de M. Waring, et qui peuvent être de quelque utilité dans la construction des Tables des nombres premiers.

1° *Si trois nombres premiers sont en progression arithmétique, leur différence doit être divisible par* 6, *à moins que l'un de ces trois nombres ne soit égal à* 3.

Tout nombre entier quelconque peut être représenté par l'une de ces formules

$$6m, \quad 6m \pm 1, \quad 6m \pm 2, \quad 6m \pm 3;$$

les deux formules $6m$ et $6m \pm 2$ donnent tous les nombres pairs, et les deux autres $6m \pm 1$, $6m \pm 3$ donnent tous les nombres impairs; mais la dernière, étant divisible par 3, ne peut représenter d'autres nombres premiers que le seul nombre 3; donc tout nombre premier sera ou 3 ou $6m \pm 1$.

Cela posé, soient

$$p - a, \quad p, \quad p + a$$

les trois nombres en progression arithmétique qu'on suppose premiers; et en excluant d'abord le nombre 3 de la progression, il faudra que chacun de ces nombres soit de la forme $6m \pm 1$; d'autre part, il est clair que la différence a doit être un nombre pair, et par conséquent d'une de ces deux formes $6n$ ou $6n \pm 2$; soit donc, s'il est possible, $a = 6n \pm 2$, et prenons d'abord $p = 6m + 1$, on aura

$$p + a = 6(m+n) + 3 \text{ ou } = 6(m+n) - 1$$

et

$$p - a = 6(m-n) - 1 \text{ ou } = 6(m-n) + 3;$$

ainsi il est impossible que $p + a$ et $p - a$ soient à la fois de la forme $6\mu \pm 1$; prenons ensuite $p = 6m - 1$, on aura

$$p + a = 6(m+n) + 1 \text{ ou } = 6(m+n) - 3$$

et

$$p - a = 6(m-n) - 3 \text{ ou } = 6(m-n) + 1;$$

d'où l'on voit que $p + a$ et $p - a$ ne pourront pas être à la fois de la forme $6\mu \pm 1$; donc il est impossible que a soit de la forme $6n \pm 2$; par conséquent il faudra que a soit toujours de la forme $6n$, c'est-à-dire divisible par 6.

Si l'on voulait admettre le nombre 3 pour un des termes de la progression, alors la différence pourrait être de la forme $6n \pm 2$. Supposons d'abord que 3 soit le premier terme de la progression; le second se trouvera de la forme $6n \pm 2 + 3$ ou $6n \pm 1$, et la troisième de la forme $12n \pm 4 + 3$ ou $6n \pm 1$; ainsi ils pourront être tous les trois premiers; mais si l'on y en ajoutait un quatrième, celui-ci ne pourrait jamais être premier, car sa forme serait $18n \pm 6 + 3$, qui est divisible par 3. On pourra, par exemple, former ces progressions de trois terme 3, 5, 7, ou 3, 7, 11, ou 3, 11, 19, etc.; donc les différences ne seront pas divisbles par 6; mais ces progressions ne pourront jamais aller au delà de trois termes.

Si l'on prend 3 pour le second terme de la progression, alors le premier ne pourra être que 1, et le troisième sera 5; dans ce cas, on y pourra ajouter un quatrième terme qui sera 7; mais on ne pourrait pas aller au delà, parce que le suivant 9 ne serait plus premier.

On ne pourrait pas prendre 3 pour le troisième terme, car les deux premiers ne pourraient être alors que 1 et 2; or celui-ci peut n'être pas regardé comme un nombre premier à cause qu'il est pair.

2° *Si cinq nombres premiers sont en progression arithmétique, leur différence doit être divisible par* 30, *à moins que* 5 *ne soit l'un des termes de cette progression.*

Nous avons déjà vu que tout nombre premier doit être 3 ou $6m \pm 1$; nous avons vu de plus que, si 3 est un des termes de la progression arithmetique, il est impossible qu'elle ait plus de quatre termes qui soient nombres premiers; donc il faudra que les cinq termes de la progression proposée soient chacun de la forme $6m \pm 1$. Or, m pouvant être un nombre quelconque entier, il sera nécessairement d'une de ces formes

$$5\mu, \quad 5\mu \pm 1, \quad 5\mu \pm 2,$$

qui renferment évidemment tous les nombres possible; donc, substituant ces formules à la place de m, on aura les suivantes

$$30\mu \pm 1, \quad 30\mu \pm 5, \quad 30\mu \pm 7, \quad 30\mu \pm 11, \quad 30\mu \pm 13,$$

dont la seconde ne peut donner d'autres nombres premiers que 5; de sorte qu'en faisant abstraction, suivant l'hypothèse, du nombre 5, il faudra que les cinq termes de la progression soient renfermés dans ces quatres formules

$$30\mu \pm 1, \quad 30\mu \pm 7, \quad 30\mu \pm 11, \quad 30\mu \pm 13.$$

Maintenant nous avons déjà vu que la différence de la progression ne peut être que la forme $6n$; or n peut être aussi de ces formes

$$5\nu, \quad 5\nu \pm 1, \quad 5\nu \pm 2;$$

donc la forme $6n$ se réduira à celles-ci

$$30\nu, \quad 30\nu \pm 6, \quad 30\nu \pm 12.$$

Donc, si l'on désigne par

$$p - 2a, \quad p - a, \quad p, \quad p + a, \quad p + 2a,$$

les cinq termes en progression arithmétique qu'on suppose être premiers entre eux, ces termes devront être tous de ces formes

$$30\mu \pm 1, \quad 30\mu \pm 7, \quad 30\mu \pm 11, \quad 30\mu \pm 13,$$

et la différence a ne pourra être que de celles-ci

$$30\nu, \quad 30\nu \pm 6, \quad 30\nu \pm 12.$$

Supposons d'abord p de la forme $30\mu + 1$, et soit, s'il est possible, a de la forme $30\nu \pm 6$, on aura

$$\begin{array}{lll} p + a = 30(\mu + \nu) + 7 & \text{ou} & 30(\mu + \nu) - 5, \\ p + 2a = 30(\mu + 2\nu) + 13 & \text{ou} & 30(\mu + 2\nu) - 11, \\ p - a = 30(\mu - \nu) - 5 & \text{ou} & 30(\mu - \nu) + 7, \\ p - 2a = 30(\mu - 2\nu) - 11 & \text{ou} & 30(\mu - 2\nu) + 13; \end{array}$$

d'où l'on voit qu'il est impossible que les cinq nombres

$$p, \quad p + a, \quad p + 2a, \quad p - a, \quad p - 2a$$

aient à la fois les forme requises.

On trouvera la même impossibilité en prenant les autres formes de p; d'où l'on conclura d'abord que a ne saurait être de la forme $30\nu \pm 6$; on supposera ensuite $a = 30\nu \pm 12$, et, examinant successivement toutes les formes de p, on verra aussi qu'aucune d'elles ne pourra donner pour les autres nombres

$$p + a, \quad p + 2a, \quad p - a, \quad p - 2a,$$

les formes requises; d'où il s'ensuit que la différence a ne pourra jamais être ni de la forme $30\nu \pm 6$, ni de celle-ci $30\nu \pm 12$; par conséquent elle devra être nécessairement de la forme 30ν, c'est-à-dire divisible par 30.

Si l'on ne veut pas exclure le nombre 5 de la progression, il est d'abord clair que ce nombre ne pourra être pris que pour le premier terme, puisque la différence des termes devant être divisible par 6 ne pourra pas être moindre que 6; or, prenant 5 pour le premier terme, et faisant d'abord la différence égale à $30\nu \pm 6$, on aura pour le second terme la forme $30\nu \pm 6 + 5$, ou bien $30\nu + 11$ ou $30\nu - 1$; pour le troisième terme les formes $60\nu \pm 12 + 5$, ou bien $30\nu - 13$, ou $30\nu - 7$; pour le quatriéme, les formes $90\nu \pm 18 + 5$, ou bien $30\nu - 7$, ou $30\nu - 13$; et pour le cinquième, $120\nu \pm 24 + 5$, ou bien $30\nu - 1$, ou $30\nu + 11$. Ainsi tous les cinq termes auront les formes requises et pourront par conséquent être premiers; mais si l'on voulait y en joindre un sixième, alors on aurait la forme $150\nu \pm 30 + 5$, qui, étant divisible par 5, ne peut pas donner des nombres premiers. On trouverait des résultats semblables en adoptant la forme $30\nu \pm 12$ pour la différence de la progression : d'où l'on doit conclure que si 5 est le premier terme de la progression, alors il pourra y avoir cinq nombres premiers en progression arithmétique, et dont la différence ne soit pas divisible par 30, mais qu'il ne pourra jamais y en avoir plus de cinq.

On aura, par exemple, les nombres 5, 11, 17, 23, 29, ou 5, 17, 29, 41, 53, etc.; mais les sixièmes termes 35, 65, etc., ne seraient plus premiers.

3° On peut démontrer par une analyse semblable que, *si sept nombres premiers sont en progression arithmètique, leur différence sera nécessairement divisible par* 2.3.5.7, *à moins que* 7 *ne soit le premier terme de la progression, auquel cas il ne pourra jamais y avoir plus de sept termes dans une progression dont la différence ne serait pas divisible par* 2.3.5.7, et ainsi de suite.