Recherche de suites les plus longues de nombres respectant certaines contraintes

Denise Vella-Chemla

Janvier 2013

Dans le tome II de sa Théorie des nombres (cf paragraphe 9 de la partie *IV* en annexe 1), Legendre fournit un théorème dans l'article 410 qui énonce que :

"Soit donnée une progression arithmétique quelconque $A-C, 2A-C, 3A-C, etc.$*, dans laquelle* A *et* C *sont premiers entre eux ; soit donnée aussi une suite* $\theta, \lambda, \mu \ldots \psi, \omega$*, composée de* k *nombres premiers impairs, pris à volonté et disposés dans un ordre quelconque ; si on appelle en général* $\pi^{(z)}$ *le* $z^{ième}$ *terme de la suite naturelle des nombres premiers* $3, 5, 7, 11, etc.$*, je dis que sur* $\pi^{(k-1)}$ *termes consécutifs de la progression proposée, il y en aura au moins un qui ne sera divisible par aucun des nombres premiers* $\theta, \lambda, \mu \ldots \psi, \omega$*."*

Desboves analyse et critique la démonstration de ce théorème de Legendre en 1855 dans les Nouvelles annales de mathématiques (cf annexe 2).

On aimerait ici utiliser un raisonnement similaire à celui utilisé par Legendre en positionnant en quelque sorte l'origine de la droite numérique en $2n$ pour montrer qu'on peut toujours trouver entre n et $2n$ un nombre qui soit à la fois premier et non congru à $2n$ selon tout module premier inférieur à $\sqrt{2n}$, ce qui garantirait que ce nombre p est un décomposant de Goldbach de $2n$. On aimerait utiliser le théorème à prouver suivant :

"Soit donnée une progression arithmétique quelconque $A-C, 2A-C, 3A-C, etc.$*, dans laquelle* A *et* C *sont premiers entre eux ; soit donnée aussi la suite* $3, 5, 7, \ldots \psi, \omega$*, composée des* k *premiers nombres premiers impairs ; si on appelle en général* p_z *le* $z^{ième}$ *terme de la suite naturelle des nombres premiers* $3, 5, 7, 11, etc.$*, je dis que sur* p_{k-1} *termes consécutifs de la progression proposée, il y en aura au moins un qui ne sera divisible par aucun des nombres premiers* $3, 5, 7 \ldots \psi, \omega$ *et qui sera congru à* $2n$ *selon aucun des nombres premiers* $3, 5, 7 \ldots \psi, \omega$*."*

Mais même si on arrive à trouver que pour 2 nombres premiers la longueur maximale de la suite est 8 (article 403) en envisageant tous les cas possibles (i.e. le double de ce qui était nécessaire en éliminant les divisibles), on n'arrive pas à mener le raisonnement au-delà. Si on note θ les divisibles par 3, $\bar{\theta}$ les congrus à $2n$ modulo 3, λ les divisibles par 5, $\bar{\lambda}$ les congrus à $2n$ modulo 5, on obtient par exemple les deux possibilités de suites les plus longues possible suivantes :

$$(\bar{\theta})\ (\theta)\ (\bar{\lambda})\ (\bar{\theta})\ (\theta)\ (\lambda)\ (\bar{\theta})\ (\theta)$$

ou bien

$$(\bar{\theta})\ (\theta)\ (\lambda)\ (\bar{\theta})\ (\theta)\ (\bar{\lambda})\ (\bar{\theta})\ (\theta)$$

Annexe 1 : Extrait du tome II de la Théorie des nombres d'Adrien-Marie Legendre.

Tome II, Partie IV , § IX, page 71, *Démonstration de divers théorèmes sur les progressions arithmétiques*

(402) Soit proposée la progression arithmétique

$$A-C,\ \ 2A-C,\ \ 3A-C \quad \ldots \quad nA-C \qquad (Z)$$

dans laquelle A et C sont des nombres quelconques premiers entre eux ; soit θ un nombre premier non-diviseur de A ; si l'on détermine x de manière que $Ax - C$ soit divisible par θ, la valeur de x sera généralement de la forme $x = \alpha + \theta z$, d'où l'on voit que les termes divisibles par θ dans la progression proposée forment eux-mêmes la progression arithmétique

$$A\alpha - C, \quad A(\alpha + \theta) - C, \quad A(\alpha + 2\theta) - C, \quad etc.$$

et qu'ainsi sur θ termes consécutifs, pris partout où l'on voudra dans la progression (Z), il y en a toujours un divisible par θ, lequel est suivi et précédé d'une suite d'autres termes également divisibles par θ, et distants entre eux de l'intervalle θ.

Cela posé, soit $\theta, \lambda, \mu \ldots \psi, \omega$, une suite de nombres premiers, pris à volonté, dans un ordre quelconque, mais dont aucun ne divise A. Nous allons chercher quel est, dans la progression (Z), le plus grand nombre de termes consécutifs qui seraient divisibles par quelqu'un des nombres de la suite $\theta, \lambda, \mu \ldots \psi, \omega$ que nous appellerons (a). Il faut pour cet effet examiner d'abord les cas les plus simples.

(403) I°) Si l'on ne considère que deux nombres premiers θ, λ, il ne peut y avoir plus de deux termes consécutifs divisibles l'un par θ, l'autre par λ, et ces termes peuvent être désignés par $(\theta), (\lambda)$. Le terme qui suit (λ) ne peut être divisible par θ, car l'intervalle avec (θ) n'étant que de deux termes, il faudrait qu'on eût $\theta = 2$; mais ce cas est exclu, et nous ne considérons dans la suite (a) que des nombres premiers impairs. Par la même raison, le terme qui précède (θ) ne saurait être divisible par λ et encore moins par θ ; donc dans ce premier cas le *maximum* cherché $M = 2$.

(404) Soient les trois nombres premiers θ, λ, μ ; on pourra concevoir trois termes consécutifs divisibles par ces nombres, lesquels seront $(\theta), (\lambda), (\mu)$. Pour que le terme qui suit (μ) soit divisible par θ, il faut que θ soit 3, et pareillement pour que le terme qui précède θ soit divisible par μ, il faut que μ soit 3. Mais comme les nombres premiers que nous considérons sont nécessairement différents entre eux, il n'y a qu'une de ces deux suppositions qui puisse avoir lieu. Dans le cas donc de $\theta = 3$, on pourrait avoir quatre termes consécutifs $(3), (\lambda), (\mu), (3)$, divisibles chacun par l'un des nombres premiers $3, \lambda, \mu$. A la suite de ces quatre termes on n'en peut pas mettre un cinquième ; car la moindre valeur que puisse avoir (λ) étant 5, le premier terme divisible par 5, après (λ), serait le septième et non le cinquième. Donc dans le cas où la suite (a) est composée de trois nombres premiers, on a au plus $M = 4$, encore faut-il que l'un de ces nombres premiers soit 3.

(405) Supposons maintenant que la suite (a) soit composée de quatre nombres premiers $\theta, \lambda, \mu, \nu$. Si l'on considère quatre termes consécutifs divisibles par ces nombres, savoir : $(\theta), (\lambda), (\mu), (\nu)$; pour en ajouter un cinquième, il faudra que λ soit 3 ; alors on aura les cinq termes consécutifs $(\theta), (3), (\mu), (\nu), (3)$. Si l'on veut ajouter à ceux-ci un sixième terme, cela ne se pourra que lorsque $\theta = 5$, car alors on aurait les six termes $(5), (3), (\mu), (\nu), (3), (5)$. La progression ne peut plus être continuée ni vers la droite, ni vers la gauche, car μ et ν devant être plus grands que 5, les termes divisibles par μ ou par ν vont beaucoup au-delà. Donc dans le cas où la suite (a) est composée de quatre termes, il n'y a au plus que six termes consécutifs de la progression (Z) qui soient divisibles par quelqu'un des termes de la suite (a). On a donc alors $M = 6$, mais ce *maximum* n'a lieu que lorsque deux des quatre nombres premiers sont 3 et 5.

(406) On conçoit en effet que les nombres premiers les plus petits sont les plus propres à donner la plus grande valeur de M, toutes choses d'ailleurs égales, puisque de plus grands nombres premiers rendent plus grands les intervalles des termes dont ils sont diviseurs.

En vertu de cette observation, on peut considérer tout d'un coup la suite naturelle des nombres premiers $3, 5, 7 \ldots \psi, \omega$, en en laissant seulement deux indéterminés, tels qu'ils sont restés dans les cas précédents ; et le *maximum* trouvé pour cette suite aura lieu à plus forte raison pour la suite (a), composée d'un pareil nombre de termes $\theta, \lambda, \mu \ldots \psi, \omega$.

Soient donc les cinq nombres premiers $3, 5, 7, \psi, \omega$; on a déjà trouvé qu'avec les quatre seuls $3, 5, \psi, \omega$, on pouvait former les six termes consécutifs $(5), (3), (\psi), (\omega), (3), (5)$. Si à la place de ψ ou ω on prenait 7, alors on ne pourrait former au plus que les huit termes $(5), (3), (7), (\omega), (3), (5), (\psi), (3)$, car leur continuation à droite exigerait que ω fût 5, et à gauche que ψ fût 7. On obtiendra un résultat plus grand en laissant (ψ) et (ω), comme dans le premier arrangement, et en ajoutant (7) d'un côté, ce qui permettra de l'ajouter en même temps de l'autre, puisque l'intervalle des deux termes (7) et (7) sera de sept termes, comme il doit être : on aura ainsi les huit termes consécutifs $(7), (5), (3), (\psi), (\omega), (3), (5), (7)$. Mais de plus on voit que (3) peut être ajouté de chaque côté, à cause de l'intervalle requis entre les (3) les plus proches ; et de cette manière on aura une combinaison de dix termes, savoir : $(3), (7), (5), (3), (\psi), (\omega), (3), (5), (7), (3)$. Elle ne peut être prolongée ni d'un côté ni de l'autre, parce qu'il faudrait pour cela que ω ou ψ fût 5, ce

qui n'a pas lieu, 5 étant déjà employé. Donc dans le cas où la suite (a) est composée de cinq termes, le *maximum* cherché est $M = 10$.

(407) On aurait pu, par une simple observation, arriver immédiatement à ce résultat. Puisque les termes divisibles par 3 et représentés par (3) se succèdent à un intervalle de 3 rangs, que les termes divisibles par 5 se succèdent à un intervalle de cinq rangs, et ainsi de suite, la série des termes consécutifs qu'on veut former au plus grand nombre possible, a cette propriété commune avec la série des nombres impairs, commençant à un terme quelconque, puisque dans cette dernière les termes divisibles par 3, par 5, etc., se succèdent pareillement à à des intervalles de 3 termes, de 5 termes, etc. Mais le moyen d'obtenir le plus grand nombre de termes consécutifs de cette suite, qui soient divisibles par quelqu'un des nombres premiers $3, 5, 7, 11, etc.$ est de considérer la suite des nombres impairs dans ses moindres termes, c'est-à-dire dès l'origine de cette suite. Car à une distance plus grande on ne manquerait pas d'être arrêté par des nombres premiers plus grands que les nombres premiers donnés, et qui empêcheraient la continuité des termes qu'on veut former. Il faut donc tout simplement considérer la série $1, 3, 5, 7, 9, 11, etc.$, qu'on peut également prolonger dans l'autre sens, ce qui donnera

$$\ldots -9, -7, -5, -3, -1, 1, 3, 5, 7, 9 \ldots$$

ou parce que les signes des nombres sont indifférents, lorsqu'on a égard seulement à leur propriété d'être divisibles ou non-divisibles par un nombre donné, on pourra considérer la double suite

$$\ldots 15, 13, 11, 9, 7, 5, 3, 1, 1, 3, 5, 7, 9, 11, 13, 15 \ldots$$

dans laquelle les termes divisibles par $3, 5, 7, etc.$ se succèdent toujours à des intervalles de $3, 5, 7, etc.$ termes, et cette suite aura l'avantage d'être composée des moindres nombres possibles. Désignant comme ci-dessus chaque terme par le moindre nombre premier qui en est diviseur, on pourra la représenter ainsi :

$$\ldots (3), (13), (11), (3), (7), (5), (3), (1), (1), (3), (5), (7), (3), (11), (13), (3) \ldots$$

(408) Maintenant si les nombres premiers sont $3, 5, 7, \psi, \omega$, on mettra dans la suite précédente les indéterminées $(\psi), (\omega)$, à la place des deux termes (1) et (1) qui occupent le milieu, et on prendra dans les termes précédents et suivants tous ceux qui n'excèdent pas (7). De cette manière, on a immédiatement pour le cas dont il s'agit la suite

$$(3), (7), (5), (3), (\psi), (\omega), (3), (5), (7), (3),$$

qui est composée de dix termes et donne le *maximum* $M = 10$, comme on l'a déjà trouvé.

Rien de plus facile ensuite que de généraliser le résultat pour tant de nombres premiers qu'on voudra. Si on a, par exemple, les six nombres premiers $3, 5, 7, 11, \psi, \omega$, on voit que la combinaison qui produit le plus grand nombre de termes consécutifs divisibles par quelqu'un de ces nombres premiers, est

$$(11), (3), (7), (5), (3), (\psi), (\omega), (3), (5), (7), (3), (11),$$

ce qui donne le *maximum* $M = 12$.

En admettant encore un nombre premier de plus, de sorte que la suite (a) fût composée des sept termes $3, 5, 7, 11, 13, \psi, \omega$, on aurait la combinaison

$$(3), (13), (11), (3), (7), (5), (3), (\psi), (\omega), (3), (5), (7), (3), (11), (13), (3),$$

laquelle est composée de seize termes et donne $M = 16$. Elle ne peut être prolongée plus loin, parce que le terme qui viendrait à la suite, d'un côté ou de l'autre, est (17) ; or quand même ψ ou ω serait égal à 17, on ne peut l'employer pour continuer la suite, puisqu'il laisserait vers le milieu une place vide.

(409) Maintenant j'observe que le nombre 16 qui satisfait à la question précédente n'est autre chose que $17 - 1$, 17 étant le nombre premier qui suit immédiatement 13 ; et il est aisé de voir que ce résultat, ainsi généralisé, est exact ; car la progression dont nous venons de faire usage n'est autre chose que la progression des nombres impairs $1, 3, 5, 7, 9, etc.$ répétée dans deux sens différents, et dans laquelle on a désigné chaque terme par le plus petit nombre premier qui en est diviseur ; de sorte qu'on peut établir ainsi la correspondance de ces deux progressions :

$\overset{*}{17}$,	15,	13,	11,	9,	7,	5,	3,	1,	1,	3,	5,	7,	9,	11,	13,	15,	$\overset{*}{17}$,
	(3),	(13),	(11),	(3),	(7),	(5),	(3),	(ψ),	(ω),	(3),	(5),	(7),	(3),	(11),	(13),	(3);	

or par cette disposition on voit évidemment que le nombre de termes compris entre les deux désignés par $\overset{*}{17}, \overset{*}{17}$ est $17-1$; donc on a $M = 17-1$.

Il n'est pas moins facile de voir en général, que si la suite (a) est composée de k nombres premiers, dont deux, ψ et ω, sont indéterminés, et les $k-2$ autres forment la suite naturelle $3, 5, 7, 11, 13, 17, etc.$ jusqu'à $\pi^{(k-2)}$; le *maximum* cherché sera

$$M = \pi^{(k-1)} - 1$$

$\pi^{(k-1)} - 1$ étant le terme de rang $k-1$ dans la suite des nombres premiers $3, 5, 7, 11, etc.$

Cette formule s'accorde avec les résultats particuliers que nous avons trouvés, et il en résulte le théorème général qui suit :

(410) *"Soit donnée une progression arithmétique quelconque $A-C, 2A-C, 3A-C, etc.$, dans laquelle A et C sont premiers entre eux ; soit donnée aussi une suite $\theta, \lambda, \mu \ldots \psi, \omega$, composée de k nombres premiers impairs, pris à volonté et disposés dans un ordre quelconque ; si on appelle en général $\pi^{(z)}$ le $z^{ième}$ terme de la suite naturelle des nombres premiers $3, 5, 7, 11, etc.$, je dis que sur $\pi^{(k-1)}$ termes consécutifs de la progression proposée, il y en aura au moins un qui ne sera divisible par aucun des nombres premiers $\theta, \lambda, \mu \ldots \psi, \omega$."*

En effet, on vient de prouver que dans la progression dont il s'agit, il ne peut y avoir au plus que $\pi^{(k-1)} - 1$ termes consécutifs qui soient divisibles par quelqu'un des nombres premiers $\theta, \lambda, \mu \ldots \psi, \omega$. Donc, sur $\pi^{(k-1)}$ termes consécutifs, il y en aura au moins un qui ne sera divisible par aucun de ces nombres.

Ce théorème très remarquable est susceptible de plusieurs belles applications. On en jugera par les deux conséquences que nous allons en tirer.

(411) La progression $A-C, 2A-C, 3A-C, etc.$ étant continuée jusqu'au $n^{ième}$ terme $nA-C$, soit L le plus grand entier compris dans $\sqrt{nA-C}$; soit en même temps ω le nombre premier immédiatement au-dessous de L, et ψ le nombre premier qui précède ω ; si dans la progression $A-C, 2A-C, 3A-C, etc$, on prend partout où l'on voudra ψ termes consécutifs, il faut, en vertu du théorème précédent, que sur ces ψ termes il y en ait au moins un qui ne soit divisible par aucun des nombres premiers $3, 5, 7, 11 \ldots \psi, \omega$, et qui sera par conséquent un nombre premier, la progression étant terminée au terme $nA-C$.

Le nombre des termes de la progression, depuis celui qui approche le plus de $\sqrt{nA-C}$ jusqu'au dernier terme $nA-C$, est à peu près $n - \sqrt{\frac{n}{a}}$; (car on suppose $C < A$, et on a $\psi < \sqrt{nA}$). Donc dans les n termes de la progression dont il s'agit, il y aura au moins autant de nombres premiers qu'il y a d'unités dans $\frac{n-\sqrt{\frac{n}{A}}}{\sqrt{nA}}$ ou à peu près dans $\sqrt{\frac{n}{A}}$. Ce nombre peut être aussi grand qu'on veut, en donnant à n la valeur convenable. Donc

"Toute progression arithmétique dont le premier terme et la raison sont premiers entre eux, contient une infinité de nombres premiers."

Cette proposition, qui est très utile dans la théorie des nombres, avait été indiquée dans les Mémoires de l'Académie des Sciences, an.1785 ; mais jusqu'à présent sa démonstration n'était point encore connue et paraissait offrir de grandes difficultés.

(412) On pourrait, s'il était nécessaire, resserrer graduellement les limites entre lesquelles doit se trouver un nombre premier ; car le nombre $\pi^{(k-1)}$ qui fixe l'étendue de ces limites, diminue en même temps que n, et à peu près en raison de $\sqrt{n}$; donc lorsque n est moindre, ou que la progression est moins avancée, il faut un moindre nombre de termes consécutifs pour trouver parmi eux un nombre premier, que lorsque la progression est plus avancée. Par cette raison on trouverait une quantité plus grande que $\sqrt{\frac{n}{A}}$ pour le nombre des termes de la progression qui sont des nombres premiers ; ce résultat augmenterait encore en excluant les nombres premiers impairs qui peuvent diviser A ; car si le nombre de ceux-ci est i, alors au lieu du nombre $\pi^{(k-1)}$ mentionné dans le théorème du n°410, on devrait prendre $\pi^{(k-1-i)}$. Mais ces observations sont peu importantes, et il suffit d'avoir démontré généralement que toute progression arithmétique, dans laquelle C et A sont premiers entre eux, contient une infinité de nombres premiers. Quant à la multitude des nombres premiers contenus dans n termes de la progression arithmétique, elle ne peut être déterminée que par d'autres considérations.

(413) Examinons plus particulièrement la progression des nombres impairs $1, 3, 5, 7, 9 \ldots 2n-1$, et proposons-nous de trouver combien de termes il faut ajouter à cette progression, pour que parmi ces termes il se trouve nécessairement un nombre premier.

Soit ψ le nombre premier qui satisfait à la question, et ω le nombre premier qui suit immédiatement ψ ; il faudra, suivant notre théorème, que ω soit le plus grand nombre premier contenu dans $\sqrt{2n+2\psi-1}$; donc $\omega^2 - 2\psi + 1 < 2n$. Mais $\omega - \psi$ ne saurait être moindre que 2, on aura donc $\omega^2 - 2\omega + 1 < 2n - 4$; d'où résulte $\omega - 1 < \sqrt{2n-4}$, et par conséquent $\psi < -1 + \sqrt{2n-4}$. Cette solution générale fournit le théorème suivant :
"Soit ψ le plus grand nombre premier contenu dans $\sqrt{2n-4}-1$; je dis que parmi les ψ nombres impairs qui suivent immédiatement $2n-1$, il y aura toujours au moins un nombre premier."

(414) Par exemple, soit $2n-1 = 113$, ou $n = 57$, le nombre premier le plus grand contenu dans $\sqrt{110}-1$ est 7. Donc parmi les sept nombres impairs qui suivent 113 et qui sont : $115, 117, 119, 121, 123, 125, 127$, il y a nécessairement un nombre premier ; c'est 127, qui est précisément le septième.

Ici la limite fixée à 7 ne s'est trouvée que de la grandeur nécessaire ; le plus souvent, et surtout lorsque n est très grand, elle est beaucoup trop étendue ; on l'agrandirait encore, mais on simplifierait l'énoncé du théorème, en disant que de L à $L + 2\sqrt{L}$, il doit nécessairement se rencontrer un nombre premier.

Ce théorème est au moins un premier pas vers la solution du problème regardé comme très difficile, de trouver un nombre premier plus grand qu'une limite donnée.

Remarque. Si on donnait à n des valeurs très petites, on trouverait que ce théorème est sujet à quelques exceptions ; mais comme on a supposé que ψ est un terme de la suite $3, 5, 7, 11,$ *etc.*, il faut que $\sqrt{2n-4}-1$ soit plus grand que 3, ainsi on doit faire $n > 10$, et alors il n'y a aucune exception.

Annexe 2 : Extrait de l'article *"Sur un théorème de Legendre"* de M. Desboves

Cet article de Desboves *"Sur un théorème de Legendre et son application à la recherche de limites qui comprennent entre elles des nombres premiers"* se trouve dans les Nouvelles annales de mathématiques, première série, tome 14 (1855), aux pages 281 à 295.

Dans l'un des chapitres de l'*Essai sur la Théorie des nombres*, Legendre s'est proposé de démontrer que toute progression arithmétique dont le premier terme et la raison sont premiers entre eux, contient une infinité de nombres premiers, et, subsidiairement, de trouver des limites qui comprennent nécessairement des nombres premiers. La solution des deux problèmes serait aussi simple qu'on peut le désirer, si malheureusement elle ne s'appuyait pas sur une proposition que Legendre croyait avoir démontrée, mais à laquelle, à vrai dire, il n'est arrivé que par une heureuse induction, comme l'a déjà remarqué depuis longtemps M. Lejeune-Dirichlet.

Je me propose dans le présent article 1° de discuter la prétendue démonstration de Legendre, c'est à dire de faire voir en quoi elle pèche et quelle est, au fond, la vraie difficulté ; 2° en admettant le théorème de l'illustre géomètre comme postulatum, d'en faire découler immédiatement de beaux théorèmes sur les limites des nombres premiers. Puissé-je, par là, car je n'ai d'autre but, engager les géomètres à faire de nouveaux efforts pour trouver une démonstration qui jusqu'ici a échappé aux plus habiles.

Première partie - *Discussion*

Avant d'énoncer le théorème de Legendre, quelques explications préliminaires sont indispensables.

Si, dans la progression arithmétique formée par la suite naturelle des nombres impairs, on se propose de trouver plusieurs termes consécutifs qui soient divisibles par quelqu'un des nombres premiers depuis 3 jusqu'à un nombre premier désigné γ, on voit que le nombre de ces termes est variable et dépend, en général, de l'ordre dans lequel sont placés les multiples des différents nombres premiers. Ainsi, par exemple, dans la suite des nombres impairs, on pourra obtenir des suites partielles dont les termes seront des multiples des nombres premiers $3, 5, 7, 11, 13$ et seront rangés suivant les différents ordres indiqués ci-dessous* :

$$\dot{3}, \dot{7}, \dot{5}, \dot{3}, \dot{11}, \dot{13}, \dot{3}, \dot{5}, \dot{7}, \dot{3},$$
$$\dot{3}, \dot{7}, \dot{5}, \dot{3}, \dot{13}, \dot{11}, \dot{3}, \dot{5}, \dot{7}, \dot{3},$$
$$\dot{5}, \dot{3}, \dot{11}, \dot{7}, \dot{3}, \dot{5}, \dot{13}, \dot{3},$$
$$\dot{3}, \dot{5}, \dot{7}, \dot{3}, \dot{11}, \dot{13}, \dot{3}, \ldots$$

*J'adopte la notation de M. Terquem, $\dot{m}$, pour désigner un multiple d'un nombre m.

Chaque nombre impair est ici considéré comme multiple du plus petit nombre premier qui le divise. La seule condition à remplir, c'est que les multiples de 3 viennent de trois en trois rangs, les multiples de 5 de cinq en cinq rangs, etc., et ce sera d'ailleurs un problème d'analyse indéterminée de la nature la plus simple que celui de trouver, dans la suite indéfinie des nombres impairs, des suites analogues aux précédentes. Si, par exemple, on se propose de trouver les nombres consécutifs impairs les plus petits possibles qui soient divisibles par quelqu'un des nombres $3, 5, 7, 11, 13$ et qui, de plus, soient rangés comme dans la première des suites données plus haut, il suffit de remarquer que le nombre pair compris entre 11 et 13 est nécessairement de la forme

$$2 \times 3 \times 5 \times 7 \times \gamma$$

et que ce même nombre divisé par 11 et 13 donne pour reste $+1$ et -1. On trouve ainsi la suite des dix nombres

$$9441, 9443, 9445, 9447, 9449,$$
$$9451, 9453, 9455, 9457, 9459,$$

On aura, d'ailleurs, une infinité d'autres suites pareilles, en ajoutant aux nombres précédents un multiple quelconque des nombres premiers $3, 5, 7, 11, 13$.

On peut se demander maintenant quel est le nombre maximum des termes d'une suite de nombres impairs consécutifs qui sont divisibles par quelqu'un des nombres premiers $3, 5, 7, \ldots, \alpha, \beta, \gamma$; α, β, γ étant les trois derniers nombres premiers considérés. Or le théorème de Legendre sur lequel nous appelons l'attention, a précisément pour but de répondre à la question. En voici l'énoncé :

Une suite de nombres impairs consécutifs, qui sont divisibles par quelqu'un des nombres premiers $3, 5, 7, 11, \ldots, \alpha, \beta, \gamma$, *a pour maximum du nombre de ses termes* $\beta - 1$. *Le nombre maximum des termes reste d'ailleurs toujours égal à* $\beta - 1$, *lorsque l'on remplace les deux derniers nombres* β *et* γ *de la suite naturelle des nombres impairs par deux nombres premiers plus grands.*

D'après le théorème précédent, il y aura, par exemple, au plus dix nombres premiers impairs consécutifs qui seront divisibles par quelqu'un des nombres premiers $3, 5, 7, 11, 13$, et nous avons vu comment on peut obtenir effectivement une telle suite.

Pour établir son théorème, Legendre écrit la suite

$$(1)(\beta - 2), \ldots, 7, 5, 3, 1, 1, 3, 5, 7, \ldots, (\beta - 2),$$

qui est composée évidemment de $\beta - 1$ termes et qu'il obtient en écrivant la suite des nombres impairs dans l'ordre direct et dans l'ordre inverse depuis 1 jusqu'au nombre impair $\beta - 2$ qui précède le nombre premier β. Il remplace ensuite les termes 1 et 1 par $\dot{\alpha}$, $\dot{\beta}$ et les autres nombres premiers par des multiples de ces nombres, ce qui donne la suite

$$(2)(\beta - 2), \ldots, \dot{3}, \dot{7}, \dot{5}, \dot{3}, \dot{\beta}, \dot{\gamma}, \dot{3}, \dot{5}, \dot{7}, \dot{3}, \ldots, (\beta - 2),$$

qu'on peut écrire aussi dans l'ordre inverse et qui contient, comme la précédente, $(\beta - 1)$ termes. L'illustre géomètre prétend ensuite démontrer que la suite (2) a le nombre maximum de termes par les raisons suivantes :

> "Le moyen d'obtenir le plus grand nombre de termes consécutifs de la suite des nombres impairs qui soient divisibles par quelqu'un des nombres premiers $3, 5, 7, 11$ est de considérer la suite des nombres impairs dans ses moindres termes, c'est-à-dire dès l'origine de cette suite, car, à une distance plus grande, on ne manquerait pas d'être arrêté par des nombres premiers plus grands que les nombres premiers donnés et qui empêcheraient la continuité des termes qu'on veut former. Il faut donc tout simplement considérer la suite des nombres impairs $1, 3, 5, 7, 9, \ldots$, qu'on peut également prolonger dans l'autre sens, ce qui donnera
>
> $$\ldots, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, \ldots,$$
>
> ou, parce que les signes des nombres sont indifférents ici,
>
> $$\ldots, 9, 7, 5, 3, 1, 1, 3, 5, 7, 9, \ldots,$$
>
> etc."

Legendre est ainsi conduit à écrire les suites (1) et (3) que nous avons données plus haut.

En admettant, pour un moment, l'exactitude du raisonnement par lequel notre auteur essaye d'établir que l'on doit considérer la suite des nombres premiers à l'origine, il semble que la conclusion devrait être que la suite maximum dérive de la suite naturelle des nombres

$$3, 5, 7, 9, \ldots, \alpha, \ldots, \beta, \ldots, \gamma, \ldots, (\delta - 2)$$

(δ est le nombre premier qui suit immédiatement γ), comme la suite (2) dérive de la suite (1). En un mot, malgré un habile artifice de langage, il est certain que Legendre ne donne aucune raison pour préférer la suite (2) à la suite

$$\dot{3}, \dot{5}, \dot{7}, \dot{3}, \ldots, \dot{\alpha}, \ldots, \dot{\beta}, \ldots, \dot{\gamma}, \ldots, (\delta - 2)$$

S'il la préfère cependant, c'est qu'il admet tacitement que la dernière suite contient moins de termes que la suite (2) ou bien que l'on a

$$\frac{\delta - 3}{2} < \beta - 1 \text{ ou } \delta < 2\beta + 1$$

c'est-à-dire qu'entre β et 2β il y a au moins deux nombres premiers. Lorsque les nombres premiers considérés sont $3, 5$ et 7, les suites (2) et (3) sont identiques, de sorte qu'en fait Legendre n'admet le théorème que pour les valeurs de β plus grandes que 5. On peut d'ailleurs évidemment écarter ici l'hypothèse de β nombre premier ; le théorème supposé vrai peut donc s'énoncer ainsi : *Entre un nombre plus grand que 6 et son double il y a toujours au moins deux nombres premiers.*

Le théorème connu de M. Bertrand est un corollaire évident du précédent. Il est curieux de retrouver ici le premier théorème relatif aux limites des nombres premiers que l'on a rencontré dans les recherches mathématiques et le premier aussi dont on a pu trouver la démonstration rigoureuse. Je ferai observer du reste que M. Tchebichef, qui a donné la démonstration du théorème de M. Bertrand, aurait pu, sans plus de difficulté, démontrer par sa méthode le théorème plus général précédemment cité.

Si maintenant nous considérons en elle-même cette raison donnée par Legendre : qu'on doit considérer la suite des nombres impairs dans ses moindres termes, nous voyons bien qu'il est vrai qu'à mesure que l'on prend dans la suite des nombres impairs des nombres plus élevés, on a la chance de rencontrer des nombres premiers plus grands que γ ; mais ces nombres premiers peuvent entrer dans la suite non pas par eux-mêmes, mais comme facteurs de certains termes simultanément avec quelqu'un des nombres premiers $3, 5, 7, \ldots, \alpha, \beta, \gamma$, et peut-être, en faisant un choix convenable, aura-t-on une suite dont le nombre de termes surpassera $\beta - 1$. Rien dans le raisonnement de Legendre n'établit le contraire.

Essayons maintenant de ramener le théorème de Legendre à quelque autre proposition plus simple, ou, si l'on aime mieux, de voir où gît principalement la difficulté.

On peut voir qu'un des caractères distinctifs des deux suites

$$3, 5, 7, \ldots, \alpha, \ldots, \beta, \ldots, \gamma, \ldots, (\delta - 2),$$
$$(\beta - 2), \ldots, \alpha, \ldots, 5, 3, 1, 1, 3, 5, \ldots, \alpha, \ldots, (\beta - 2),$$

c'est que la première ne contient qu'un seul multiple de l'antépénultième nombre premier α (supposé plus grand que 3), tandis que la seconde en contient deux ; car $\delta - 2$ est plus petit que 3α, ou, en d'autres termes, il y a au moins trois nombres premiers β, γ, δ entre α et 3α. On démontre effectivement, par la méthode de M. Tchebichef, qu'entre un nombre supposé plus grand que 3 et son triple il y a toujours trois nombres premiers.

En rapprochant ce qui précède des remarques faites plus haut, on peut admettre maintenant comme démontré qu'à l'origine des nombres, pour parler le langage de Legendre, la suite des nombres impairs qui ne contient qu'un seul multiple de α, a moins de termes que la suite des nombres impairs qui en renferme deux. Je dis maintenant, et c'est par là que je terminerai la présente discussion, que si l'on admettait que le même théorème a lieu quelque part que ce soit dans la suite naturelle des nombres impairs, le théorème de Legendre serait démontré.

En effet, admettons que le théorème de Legendre soit vrai lorsqu'on considère tous les nombres premiers $3, 5, \ldots, \alpha, \beta, \gamma$, les deux derniers β et γ pouvant être remplacés par des nombres premiers plus grands, c'est-à-dire admettons qu'alors la suite du nombre maximum de termes soit nécessaires la suite (2) qui contient $\beta - 1$ termes ; je dis que losqu'on prendra un nombre premier de plus δ, le nombre maximum deviendra $\gamma - 1$.

On peut remarquer d'abord que la nouvelle suite ne pourra contenir ni deux multiples de γ ni deux multiples de δ. Car si la nouvelle suite contenait deux multiples de γ, entre ces deux multiples il y aurait $\gamma - 1$ termes intermédiaires divisibles par quelqu'un des nombres $3, 5, 7, \ldots, \alpha, \beta, \delta$, ce qui est impossible, puisque le nombre des termes divisibles par quelqu'un des nombres $3, 5, 7, \ldots, \alpha, \beta, \delta$ est, par hypothèse, au plus égal à $\beta - 1$. Par la même raison, on n'aura pas deux multiples de δ, mais on pourra former une suite contenant deux multiples de β ; il suffira, pour cela, de remplacer au milieu de la suite (2) $\dot{\beta}$ par $\dot{\delta}$, de mettre $\dot{\beta}$ au commencement et à la fin de la même suite et de continuer d'écrire des termes autant que faire se pourra vers la droite et vers la gauche : on aura aini une suite contenant $\gamma - 1$ termes. Comme d'ailleurs cette suite est la seule qui, d'après l'hypothèse faite, puisse contenir deux multiples de β, elle sera, d'après le principe que nous avons admis, la suite du nombre de termes maximum. Le théorème de Legendre, se vérifiant directement pour les nombres premiers $3, 5, 7, 11$, peut être considéré maintenant comme vrai en général.

Quand les nombres premiers sont $3, 5$ et 7, les suites (2) et (3) sont identiques et contiennent chacune deux multiples de α, mais le théorème de Legendre n'en subsiste pas moins, puisque le nombre des termes de la suite est égal à 4.

En résumé, on voit qu'il résulte de la discussion précédente que les travaux de M. Tchebichef ont, en quelque sorte avancé la démonstration du théorème de Legendre, mais qu'il reste toujours à démontrer la proposition suivante : *Une suite de nombres impairs consécutifs divisibles par quelqu'un des nombres premiers* $3, 5, \ldots, \alpha, \beta, \gamma$ *étant prolongée autant que possible, aura plus de termes lorsqu'elle contiendra deux multiples de l'antépénultième nombre premier* α *que lorsqu'elle n'en contiendra qu'un seul.*