Ci-dessous, un extrait du tome II de la Théorie des nombres d'Adrien-Marie Legendre.

1 Quatrième partie, § IX, 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

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

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.