Nouvelles annales de mathématiques

Desboves

Sur un théorème de Legendre et son application à la recherche de limites qui comprennent entre elles des nombres premiers

Nouvelles annales de mathématiques 1re série, tome 14 (1855), p. 281-295.

<http://www.numdam.org/item?id=NAM_1855_1_14__281_1>

SUR UN THÉORÈME DE LEGENDRE
et son application à la recherche de limites qui comprennent entre elles des nombres premiers ;

Par M. DESBOVES,
Professeur au Lycée Bonaparte.

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 un postulatum, d'en faire découler immédiatement de beaux théorèmes sur les limites des nombres premiers. Puissé-je, par là, car je n'ai pas 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

$$\begin{matrix} 9441, & 9443, & 9445, & 9447, & 9449, \\ 9451, & 9453, & 9455, & 9457, & 9459, \end{matrix}$$

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,..., α, β, γ; 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,..., α, β, γ, *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 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

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

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

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

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 soit di- » visible 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 manque- » rait pas d'être arrêté par des nombres premiers plus » grands que les nombres premiers donnés et qui empê- » cheraient la continuité des termes qu'on veut former. Il

» faut donc tout simplement considérer la suite des nom-
» bres impairs 1, 3, 5, 7, 9,..., 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,

$$9,\ 7,\ 5,\ 3,\ 1,\ \dot{1},\ 3,\ 5,\ 7,\ 9,\ldots,$$

» 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

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

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

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

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 toujours 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 lorsque l'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 nécessairement la suite (2) qui contient $\beta-1$ termes ; je dis que lorsqu'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,..., α, β, δ, ce qui est impossible, puisque le nombre des termes divisibles par quelqu'un des nombres 3, 5, 7,..., α, β, δ 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 ainsi 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,..., α, β, γ *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.*

SECONDE PARTIE.

Nous allons maintenant déduire, comme conséquences du théorème de Legendre, divers théorèmes relatifs aux limites qui comprennent entre elles des nombres premiers.

THÉORÈME I. *Si l'on désigne par* n *un nombre entier plus grand que* 24, *par* a *sa racine par défaut à moins d'une unité près, par* α *et* β *les nombres premiers qui précèdent immédiatement* a (β *peut être égal à* a), *toutes les fois que* $a + 1$ *ne sera pas un nombre premier, on pourra assurer qu'entre* n *et* $n + 2\alpha + 1$ *il y a au moins un nombre premier, et qu'entre* n *et* $n + 2\beta + 1$ *il y en a au moins deux. Si* $a + 1$ *est premier, on sera seulement certain qu'il existe un nombre premier entre* n *et* $n + 2\beta + 1$.

Nous remarquons d'abord que $n + 2\alpha$, qui peut être plus grand que $(a + 1)^2$, est nécessairement plus petit que $(a + 2)^2$. Car n étant compris entre a^2 et $(a + 1)^2$, est au plus égal à $a^2 + 2a$, et $n + 2\alpha$ est inférieur à $a^2 + 4a$ et, à plus forte raison, à $(a + 2)^2$. Il en résulte que chacun des α nombres impairs consécutifs qui suivent n et sont compris dans tous les cas entre n et $n + 2\alpha + 1$, devra, s'il n'est pas premier, être divisible par quelqu'un des nombres premiers $3, 5, 7, \ldots, \alpha, \beta$. Le terme $(a + 1)^2$, le seul des termes de la suite qui pourrait n'admettre aucun facteur premier égal à β ou plus petit, n'échappera pas lui-même à cette loi, puisque $a + 1$ est d'abord supposé non premier. Mais, d'après le théorème de Legendre, il y a au plus $\alpha - 1$ nombres impairs consécutifs, divisibles par quelqu'un des nombres premiers précédemment cités; donc, entre n et $n + 2\alpha + 1$, il y a au moins un nombre premier lorsque $a + 1$ n'est pas lui-même premier.

Les limites n et $n+2\beta+1$ comprendront aussi, à plus forte raison, un nombre premier; mais je dis de plus maintenant qu'elles en contiendront au moins deux. En effet, s'il n'y avait qu'un nombre premier ω entre les limites indiquées, on aurait au moins β nombres impairs consécutifs, divisibles par $3, 5, \ldots, \alpha, \beta, \omega$, tandis qu'il y a au plus $\beta - 1$.

Si $a+1$ était un nombre premier, il devrait être joint à la suite $3, 5, \ldots, \alpha, \beta$, et dès lors on voit, en recommençant les raisonnements précédents, qu'on pourra seulement affirmer qu'il existe un nombre premier entre les limites n et $n+2\beta+1$.

Corollaire I. Il y a toujours un nombre premier entre n et $n+2\sqrt{n}+1$. La démonstration suppose n plus grand que 8, mais, pour les valeurs de n plus petites que 9, le corollaire se vérifie directement.

Corollaire II. Les carrés de deux nombres entiers consécutifs, comprennent toujours entre eux au moins un nombre premier.

Remarque. Le seul théorème relatif aux limites des nombres premiers que Legendre a déduit de son principe a de l'analogie avec le théorème I. Legendre donne aussi le premier corollaire.

THÉORÈME II. *Les carrés de deux nombres entiers consécutifs comprennent toujours entre eux au moins deux nombres premiers.*

Nous venons de voir que les carrés de deux nombres entiers consécutifs comprennent toujours entre eux au moins un nombre premier. Désignons ce nombre premier par ω. Si, parmi les a nombres impairs compris entre a^2 et $(a+1)^2$, il n'y avait qu'un seul nombre premier ω, on aurait a nombres impairs consécutifs divisibles par quelqu'un des nombres premiers $3, 5, 7, \ldots, \alpha, \beta, \omega$, tandis que, d'après le théorème de Legendre, il peut y en avoir au plus $\beta - 1$. Il y a donc au moins deux nombres premiers entre les limites indiquées.

La démonstration précédente suppose a au moins égal à 5, mais, pour les valeurs de a plus petites que 5, le théorème se vérifie directement.

Ici se présente naturellement la question de savoir si, à partir d'une valeur suffisamment grande, les carrés de deux nombres entiers consécutifs comprennent toujours un nombre déterminé de nombres premiers aussi grand que l'on veut, mais le théorème de Legendre ne paraît pas pouvoir fournir une réponse à la question. Nous allons, du reste, donner maintenant un théorème qui fera connaître des limites entre lesquelles on pourra comprendre autant de nombres premiers qu'on voudra.

Théorème III. *Si l'on désigne par* n *une variable qui peut prendre toutes les valeurs entières possibles, par* p *et* k *deux nombres entiers donnés, entre* 2n *et* 2n — k *il y aura toujours au moins* p *nombres premiers à partir d'une valeur de* n *suffisamment grande qu'on pourra déterminer en fonction de* p *et* k.

Soient a^2 et $(a+1)^2$ les carrés de deux nombres entiers consécutifs qui comprennent n, et supposons qu'à partir d'une valeur de n suffisamment grande on puisse toujours satisfaire à l'inégalité

$$2n - k > (a + l)^2,$$

l étant un nombre donné quelconque. Les nombres

$$(a+1)^2,\ (a+2)^2,\ .\ ,\ (a+l)^2$$

seront supérieurs à n et inférieurs à $2n - k$; d'après le théorème précédent, il y aura entre n et $2n - k$ au moins $2(l-1)$ nombres premiers. Si donc on pose

$$2(l-1) = p \quad \text{ou} \quad 2(l-1) = p + 1,$$

suivant que p est pair ou impair, on sera assuré qu'entre n et $2n-k$ il y a au moins p nombres premiers. On peut d'ailleurs, dans tous les cas, remplacer dans l'inégalité précédente l par sa valeur $1+\frac{p+1}{2}$ tirée de l'équation

$$2(l-1)=p+1,$$

puisque, dans le cas de p nombre pair, on ne ferait que remplacer, dans l'inégalité, l par une valeur trop grande: nous aurons ainsi

$$2n-k>\left(a+1+\frac{p+1}{2}\right)^2.$$

Cette inégalité sera évidemment satisfaite si nous pouvons déterminer n par la condition

$$2n-k>\left(\sqrt{n}+1+\frac{p+1}{2}\right)^2;$$

or cette dernière égalité ayant lieu pour toute valeur de n plus grande que

$$\frac{3(p+3)^2+4k+2(p+3)\sqrt{2(p+3)^2+4k}}{4},$$

le théorème est démontré.

En faisant

$$k=2,\quad p=1$$

dans la formule, nous trouvons que pour n plus grand que 27 il existe toujours un nombre premier compris entre n et $2n-2$. La même propriété se vérifiant directement pour tous les nombres plus grands que 3, on voit que l'on retombe sur le théorème de M. Bertrand, comme on devait d'ailleurs s'y attendre.

Corollaire. Entre n et pn, il y a toujours p nombres premiers à partir d'une valeur de n suffisamment grande. Je n'aurais pas donné ce corollaire si dans la discussion du théorème de Legendre, on n'avait pas rencontré les applications particulières $p=1$, $p=2$.

Le théorème de M. Bertrand a été seul démontré par M. Tchebichef; mais je me suis assuré que, par la discussion d'une équation transcendante, fournie par la méthode de l'habile géomètre, on pouvait démontrer le théorème III sans difficulté. C'est là, je crois, un utile exercice à recommander aux jeunes lecteurs des *Nouvelles Annales*.

THÉORÈME IV. *Entre un nombre et son carré il y aura toujours un nombre donné* p *de nombres premiers à partir d'une valeur suffisamment grande.*

Ce théorème est une conséquence évidente du théorème III. Comme cas particulier, on retrouve le théorème de M. de Polignac : *Entre un nombre et son carré il y a toujours un nombre premier.*

En terminant, je crois devoir faire observer que si la démonstration du théorème de Legendre ou du postulatum auquel je l'ai ramené doit encore résister aux investigations des géomètres, le théorème II, par son énoncé si simple, mérite d'appeler leurs efforts. MM. Tchebichef et de Polignac, par exemple, pourraient peut-être parvenir à le démontrer par leurs savantes méthodes.

NOTE SUR LE THÉORÈME DE GOLDBACH.

Tout nombre pair, excepté 2, *est la somme de deux nombres premiers au moins de deux manières, et lorsque le nombre pair est double d'un nombre impair, il est toujours simultanément la somme de deux nombres premiers de la forme* $4n+1$ *et la somme de deux nombres premiers de la forme* $(4n-1)$ (*vérifié jusqu'à* 10 000).

L'énoncé ainsi complété permet d'établir un certain lien entre le théorème de Goldbach et d'autres propositions connues.

Remarquons d'abord que la première partie de la proposition exige nécessairement la vérité du théorème que nous avons déjà trouvé au début de la discussion d'un théorème de Legendre, à savoir : qu'*entre un nombre plus grand que* 6 *et son double il y a toujours au moins deux nombres premiers*. En effet, la première partie du théorème, à partir de 14, est vraie, même en ne comptant pas la décomposition en deux nombres premiers égaux.

En second lieu, si l'on admettait la deuxième partie du théorème, en se rappelant que tout nombre premier de la forme $4n + 1$ est la somme de deux carrés, on en conclurait qu'un nombre quelconque est la somme de quatre carrés ou d'un nombre moindre de carrés. On peut même ajouter que si l'on voulait obtenir une décomposition d'un nombre en quatre carrés, par exemple, pour construire géométriquement la racine carrée de ce nombre, on aurait peut-être de cette manière le procédé le plus régulier et le plus simple. Je suppose, bien entendu, que l'on ait à sa disposition deux Tables, l'une de nombres premiers, l'autre de carrés.

Soit proposé, par exemple, de décomposer le nombre 327 en quatre carrés; en désignant par x^2, y^2, z^2, u^2 les quatre carrés inconnus, on écrira

$$2(x^2 + y^2 + z^2 + u^2) = 654,$$

et, en décomposant 654 en deux nombres premiers de la forme $4n + 1$,

$$2(x^2 + y^2 + z^2 + u^2) = 397 + 257.$$

Maintenant si l'on décompose chacun des nombres 397 et 257 en deux carrés, on a

$$2(x^2 + y^2 + z^2 + u^2) = 19^2 + 6^2 + 1^2 + 16^2,$$

ou encore

$$(x+y)^2+(x-y)^2+(z+u)^2+(z-u)^2$$
$$=19^2+1^2+16^2+6^2.$$

Or on peut satisfaire à cette équation en égalant chaque terme du premier membre au terme correspondant du second, ce qui détermine x, y, z et u.

On a ainsi finalement

$$327=10^2+9^2+11^2+5^2.$$