Présence d'un nombre premier entre deux carrés consécutifs

Legendre's Conjecture

(Réjean Labrie, juillet 2014**)**

Résumé : Le présent article constitue une démonstration de l'existence d'au moins un nombre premier entre deux carrés consécutifs.

Abstract: This article is a demonstration of the existence of at least one prime number between two consecutive squares.

1. Introduction

Cet article se veut une démonstration de la conjecture énoncée par Adrien-Marie Legendre et fait partie des quatre problèmes relatifs aux nombres premiers présentés par Edmund Landau lors du congrès international des mathématiciens de 1912 à Cambridge.

Afin de démontrer que pour tout entier n≥1, il existe au moins un nombre premier p tel que n^2<p< (n+1)^2 nous procéderons en deux étapes :

- Démonstration du lemme suivant : La plus longue suite de nombres composés consécutifs dont chacun des termes est divisible par au moins un des nombres premiers 2, 3, 5, …, p_i contient (2* p_{i-1}) – 1 nombres composés.
- Démonstration de la véracité de la conjecture affirmant que pour tout entier n≥1, il existe au moins un nombre premier p tel que n^2<p< (n+1)^2.

2. Démonstration du lemme

Lemme : La plus longue suite de nombres composés consécutifs dont chacun des termes est divisible par au moins un des nombres premiers 2, 3, 5, …, p_i contient (2* p_{i-1}) – 1 nombres composés.

Explication de l'algorithme de calcul

Désignons par Sp_i la suite de longueur maximum qui renferme uniquement des nombres composés consécutifs dont chacun des termes est divisible par au moins un des nombres premiers 2, 3, 5,…, p_i. Représentons la longueur de cette suite par Lp_i. Cette suite peut s'écrire comme ci-dessous :

$Sp_i = \{x+1, x+2, x+3, x+4, x+5, x+6\ldots, x+ Lp_i\}$

Certains termes peuvent être divisés par un ou plusieurs des diviseurs premiers 2, 3, 5,…, p_i. Autrement dit, ces termes sont divisibles par le produit d'une combinaison de plusieurs diviseurs premiers. On peut imaginer à titre d'exemple que x+1 est divisible à la fois par 2 et 3, ou plus simplement par leur produit qui est 6. Il découle de ce choix que les nombres x+3, x+5, x+7, etc. sont aussi divisibles par 2 puisque distants de x+1 par un multiple de 2. De même x+4, x+7, x+10, etc. sont divisibles par 3 car ils sont éloignés de x+1 par un multiple de 3. Si l'on considère aussi que x+2 est divisible à la fois par 5 et 7, on obtient ainsi une configuration de diviseurs qui ressemble au schéma ci-dessous. Les diviseurs 11, 13, …, p_i ne sont pas représentés ici. Nommons cette configuration Cp_i ou p_i représente le nombre premier de rang i, sachant que p_1=2. Il est évident que cette configuration est égale en longueur à la suite Sp_i puisqu'à chaque ensemble de diviseurs dans une colonne est associé le nombre divisé apparaissant au haut de cette colonne.

Sp_i	x+1	x+2	x+3	x+4	x+5	x+6	x+7	x+8	x+9	x+10	.....	$x+Lp_i$
Cp_i		7						7			.....	
		5				5					.....	
	3			3			3			3	.....	
	2		2		2		2		2		.....	2

Afin de bien fixer les idées examinons un cas concret soit la suite S_7 et une configuration de diviseurs possible C_7.

S_7	x+1	x+2	x+3	x+4	x+5	x+6	x+7	x+8	x+9
C_7						7			
				5					5
		3			3			3	
	2		2		2		2		2

Il ne peut y avoir un terme x+10 car il n'y a pas de diviseur parmi 2, 3, 5, 7 satisfaisant l'éloignement requis avec son homologue sur une ligne. En effet, 2 pourrait diviser x+11, 3 pourrait diviser x+11, 5 pourrait diviser x+14 et 7 pourrait diviser x+13. Donc aucun diviseur possible pour x+10 si l'on tente de prolonger cette configuration. On pourrait bien sûr essayer d'autres configurations parmi celles imaginables. Toutefois une seule autre peut être aussi longue, soit celle où l'on place le diviseur 7 comme diviseur de x+4 et 5 comme diviseur de x+6. Ainsi pour S_7 on a une longueur maximum L_7=9. À titre d'exemple la suite {212, 213, 214, 215, 216, 217, 218, 219, 220} est une suite S_7 dont les termes consécutifs sont divisibles respectivement par 2, 3, 2, 5, 6, 7, 2, 3 et 10.

Pour connaître la valeur de Lp_i il nous faut donc trouver la configuration Cp_i de longueur maximum. Un algorithme pour construire la plus longue configuration de diviseurs consiste à remplir d'abord les cases avec les diviseurs 2. Pour remplir un maximum de cases on inscrit 2 dans la première case et dans toutes les autres distantes de la première par un multiple de 2. Ce qui donne le schéma ci-dessous.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
2		2		2		2		2		2		2		2		2		2		2

Ensuite on place les diviseurs 3. Pour ce faire, on insère un premier 3 dans une case déjà occupée par un 2 le plus près possible du centre. Pour notre exemple choisissons la case 9 comme lieu de notre premier 3. Les autres 3 seront distribués à gauche et à droite de ce premier 3, à une distance égale à un multiple de 3. Voyons ci-dessous le nouvel état de notre configuration de diviseurs.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
2		3 2		2	3	2		3 2		2	3	2		3 2		2	3	2		3 2

Continuons la construction de la configuration de diviseurs, voulue la plus longue, en plaçant 5 dans la même case centrale que le premier 3, soit la case 9. Les autres 5 sont répartis à droite et à gauche de ce premier 5 à une distance égale à un multiple de 5. Supposons que la configuration cherchée est celle de C_{11}. Il reste donc seulement les diviseurs 7 et 11 à placer. Ces 2 derniers diviseurs doivent être positionnés respectivement à gauche et à droite de la case centrale numéro 9. Le diviseur 7 est répété dans les cases distantes par un multiple de 7, tandis que le diviseur 11 est reproduit dans les cases distantes par un multiple de 11. On aboutit ainsi au schéma ci-dessous.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
7 2		3 2	5	2	3	2	7	5 3 2	11	2	3	2	5	7 3 2		2	3	5 2		11 3 2

On observe qu'il n'y a pas de diviseur pour les cases 2, 16 et 20. Ainsi la plus longue configuration C_{11} s'étend de la case 3 à la case 15 inclusivement pour une longueur L_{11} =13.

Dans le cas de la suite C_{13}, construite avec le même algorithme, on a une longueur de L_{13}=21 comme on peut voir ci-dessous.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
5 2	3	2	7	3 2	5	2	3	2	11	7 5 3 2	13	2	3	2	5	3 2	7	2	3	11 5 2

Il découle de cet algorithme que les différents diviseurs s'accumulent au milieu de la configuration et que les autres se rangent symétriquement par rapport à la case centrale, sauf les deux derniers situés de part

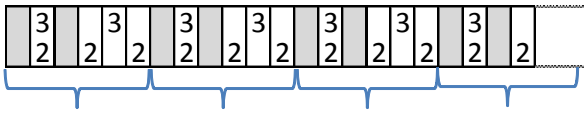
et d'autre de la case centrale. De plus l'avant-dernier diviseur tombe toujours dans la case qui précède la case centrale. Dans notre dernier exemple l'avant-dernier diviseur, en l'occurrence 11, arrive en position 10. La case suivante est la case centrale et se situe en position 11. Ainsi la valeur de l'avant dernier diviseur correspond à la position de la case centrale.

À partir de ces observations on déduit facilement une formule qui donne la longueur d'une configuration en fonction du plus grand diviseur utilisé. Ainsi pour la configuration $Cp_{i,}$ qui correspond aux diviseurs premiers 2, 3, 5,…, p_i, l'avant-dernier diviseur p_{i-1} nous dit que la case centrale est en position p_{i-1}. Pour déterminer la longueur de la configuration il suffit de multiplier p_{i-1} par 2 et soustraire 1. On a alors $Lp_i=(2*p_{i-1}) – 1$ qui nous donne la longueur de Cp_i mais également la longueur de Sp_i, soit la suite la plus longue de nombres composés dont chacun des termes est divisible par au moins un des diviseurs premiers 2, 3, 5,…, p_i.

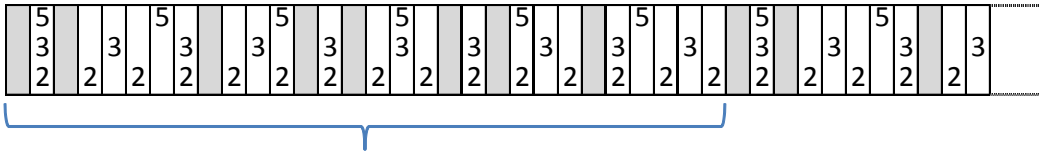
<u>Démonstration à l'effet que $Lp_n=(2*p_{n-1}) – 1$ pour tout entier n>1.</u>

On peut vérifier de façon empirique, pour les premières valeurs de n, que la formule $Lp_n =(2*p_{n-1}) – 1$ donne effectivement la longueur maximum de la configuration de diviseurs premiers.

Pour n=2 la suite des diviseurs se limite à $p_1=2$ et $p_2=3$. Pour construire les configurations possibles il suffit de distribuer les diviseurs 2 en laissant une case vide entre chacun d'eux. On fait la même chose avec les diviseurs 3 en laissant deux cases entre chacun d'eux. Nous constatons qu'il y a seulement deux configurations possibles délimitées par les cases vides et grisées, le tout englobé par l'accolade. Le reste de la construction montre une répétition sans fin de ces 2 configurations. La première à une longueur de 1 et la deuxième est la plus longue avec une longueur de 3, ainsi on a $Lp_2=3$. Cela correspond effectivement à la prédiction de la formule car $Lp_2 = (2*p_1) – 1 = (2*2) – 1 = 3$.



On peut de même vérifier la formule pour n=3 par une construction semblable avec le résultat suivant :



Cette fois nous identifions, séparées par des cases grisées, sept configurations dans l'accolade et le contenu de cette accolade se répète encore sans fin. Les plus longues d'entre elles sont d'une longueur égale à 5. Calculons maintenant avec la formule, $Lp_3 = (2*p_2) – 1 = (2*3) – 1 = 5$ aussi.

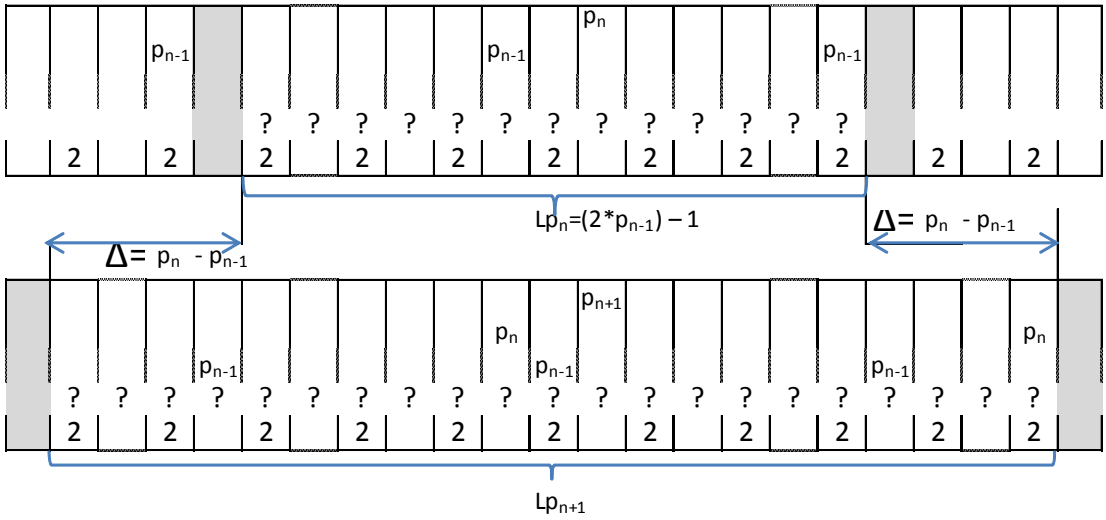
Nous allons maintenant démontrer par induction que cette formule est valide pour tout entier n>3. Pour ce faire, rappelons d'abord les règles de l'algorithme de calcul afin de construire la configuration de diviseurs la plus longue pour les diviseurs premiers 2, 3, 5, 7, …, p_n pour n>3:

1- Placer les diviseurs 2 en commençant par la première case et dans les cases successives espacées par un multiple de 2.
2- Insérer un premier diviseur 3 dans une case occupée par un 2 près du centre et répartir les autres 3 dans les cases à gauche et à droite du premier 3 à une distance multiple de 3.
3- Procéder avec chacun des autres diviseurs X en inscrivant chacun d'eux dans la case centrale (déjà occupée par les diviseurs 2 , 3,…) et les autres homologues de part et d'autre de la case centrale à une distance multiple de X.
4- Mettre l'avant-dernier diviseur p_{n-1} dans la case qui précède immédiatement la case centrale et le dernier diviseur p_n dans la case qui suit la case centrale.
5- La configuration de longueur maximum est confinée entre deux cases où il y a absence de diviseurs. En soustrayant 1 au produit de l'avant-dernier diviseur p_{n-1} multiplié par 2 nous obtenons la longueur de la configuration.

Dans les deux schémas ci-dessous construits selon les règles de l'algorithme nous voyons seulement les lignes de diviseurs qui présentent un intérêt pour la démonstration. Les autres lignes de diviseurs sont simplement évoquées par les points d'interrogation.

Le schéma du haut correspond à la configuration pour les diviseurs 2, 3, 5, …, p_n. Nous remarquons que l'avant-dernier diviseur p_{n-1} est positionné à gauche du 2 central tandis que le dernier diviseur est placé à droite du même 2. Aussi nous comprenons que les autres diviseurs p_{n-1} arrivent juste avant les cases grisées car le premier diviseur p_{n-1} est lui-même décalé d'une case avant le centre et ses homologues s'écartent de lui par une distance égale à p_{n-1}. Les cases grisées renferment aucun diviseur.

Le schéma du bas présente la configuration pour les diviseurs 2, 3, 5, …, p_{n+1}. Le diviseur p_{n-1} n'étant plus l'avant-dernier diviseur se retrouve maintenant dans la case centrale. Par contre p_n et p_{n+1}, respectivement avant-dernier et dernier diviseur, se logent à gauche et à droite de la case centrale.



Il ressort de ces 2 schémas que la configuration du bas est plus longue que celle du haut par une valeur équivalente à 2*Δ, où Δ est la différence entre p_n et p_{n-1}. Il en découle que $Lp_{n+1} = Lp_n + 2*\Delta$.

On a vu que la formule $Lp_i = (2 * p_{i-1}) - 1$ est valide pour i = 2 et 3. Supposons la formule valide pour i = n. On démontre qu'elle est valide également pour i =n+1. En effet,

$$Lp_{n+1} = Lp_n + 2*\Delta = ((2*p_{n-1}) -1) + (2 *(p_n - p_{n-1})) = 2 *p_n - 1 = (2 * p_{n+1\,-1}) - 1$$

Donc la formule est démontrée pour tout entier n>1.

3. Existence d'au moins un nombre premier entre deux carrés consécutifs

Théorème : Pour tout entier n≥1, il existe au moins un nombre premier p tel que n^2<p< (n+1)^2.

Démonstration

Pour n=1 nous constatons qu'il y a entre 1^2 et 2^2 les nombres premiers 2 et 3. De même pour n=2 il est visible qu'entre les carrés 2^2 et 3^2 il y a les nombres premiers 5 et 7.

La démonstration se poursuivra donc pour des valeurs de n>2. Nous verrons qu'il est impossible de trouver une suite de nombres composés suffisamment longue pour remplir l'espace entre les deux bornes n^2 et (n+1)^2 qui délimitent (n+1)^2 - n^2 - 1 = 2*n cases à remplir. Donc des nombres premiers doivent s'intercaler entre les nombres composés pour combler l'espace entre les deux carrés. Il y a deux situations à examiner selon que n est premier ou composé.

Cas où n est un nombre premier >2

Si un nombre entre n^2 et (n+1)^2 est divisible, alors il possède un diviseur plus petit que la racine carrée de (n+1)^2, donc inférieur à n+1. Les diviseurs considérés sont les nombres premiers 2, 3, 5,…, n. Nous incluons n car n est premier par hypothèse et il est plus petit que n+1.

Comme n est premier alors il est égal à un certain p_i. Alors notre liste de diviseurs premiers équivaut à 2, 3, 5,…, p_i. Par le lemme précédent on sait que la suite de nombres composés de longueur maximum pour une telle liste de diviseurs premiers est $(2*p_{i-1}) - 1$. Cette suite est trop courte pour saturer l'espace disponible entre les 2 carrés qui mesure $2*n = 2*p_i$. En effet, $(2*p_{i-1}) - 1 < 2*p_i$ pour toute valeur p_i. Donc il y a un ou plusieurs nombres premiers présents entre les deux carrés n^2 et (n+1)^2 pour tout nombre premier n supérieur à 2.

Cas où n est un nombre composé >2

Les nombres divisibles entre n^2 et (n+1)^2 disposent d'un diviseur premier plus petit que la racine carrée de (n+1)^2, donc inférieur à n+1. Comme n est un nombre composé par hypothèse, il s'ensuit que n est nécessairement compris entre deux nombres premiers consécutifs, ce qui se traduit par $p_i<n<p_{i+1}$. Ainsi $n+1 \leq p_{i+1}$ et puisqu'on se limite aux diviseurs premiers inférieurs à n+1 ceci signifie que les diviseurs sont inférieurs à p_{i+1}. Notre liste de diviseurs premiers devient 2, 3, 5,…, p_i puisque p_i est le nombre premier immédiatement inférieur à p_{i+1}. Pour cette liste de diviseurs le lemme précédent accorde à la suite de nombres composés de longueur maximum une mesure de $(2*p_{i-1}) - 1$. Puisque $(2*p_{i-1}) - 1 < 2*p_i$ on a

$(2*p_{i-1}) - 1 < 2*n$ car $p_i<n$. Nous constatons que la suite de nombres composés de longueur maximum est trop courte pour remplir les 2*n positions entre les deux carrés n^2 et (n+1)^2 et ceci pour tout nombre composé n supérieur à 2. Donc il y a un ou plusieurs nombres premiers entre les deux carrés en plus des nombres composés.

********** C.Q.F.D. **********