

Objectif : démontrer que la conjecture de Goldbach est une variante du crible d'Ératosthène
Mais dans les congruences.

Goldbach indique que tout nombre pair est la somme de 2 nombres premiers. On veut utiliser la décomposition des multiples de 30 en deux nombres premiers selon les principes d'un crible. L'objectif est de montrer que ces nombres premiers particuliers forment l'ensemble des nombres premiers > 5 .

La méthode du crible à utiliser suit la méthode d'Ératosthène, en utilisant les congruences de multiples de 30 (ci-dessous appelé $30k$) modulo p , $p \leq \sqrt{2n}$ étant les nombres premiers définis ci-dessous qui vont cribler.

On crible de 1 à n et non de 1 à $2n$

⇒ cinq parties à expliciter :

1/ : comment on construit ce crible, algorithme de Goldbach.

2/ : prouver que les nombres premiers ainsi trouvés forment l'ensemble des nombres premiers

3/ : montrer que quelque soit un $30k$, il est toujours décomposable en somme de deux premiers en utilisant une des 8 familles $30k + 2i$, $i \in \{1, 7, 11, 13, 17, 19, 23, 29\}$ avec $30k \geq 300$. *Note*: on peut montrer en utilisant simplement les entiers non nul ≥ 1 .

4/ : montrer que l'on peut utiliser ce crible, à l'ensemble des entiers pairs en progression arithmétique de raison 30, selon des conditions particulières; afin d'obtenir une estimation minorée de couples premiers, qui décomposent un entier pair > 4 en somme de deux premiers.

5/ : on montrera que ce crible a une propriété récurrente, le décalage d'un rang des congruences sur leur successeur, lorsque la limite $2n$ augmente de 2, ou en utilisant une famille pour la limite $30(k+1) + 2i$; en la choisissant par rapport à la forme de $n = 15k + i$, la limite du criblage. «Ce crible dans les congruences fera ressortir la famille complémentaire par rapport à $2n$. Les nombres premiers q ont pour antécédent les entiers $A \neq 2n[p]$ »

6/ : pour **3/** et **4/**, on utilisera le Théorème des nombres premiers noté TNP et son corollaire, conséquence directe du TNP; où on en déduira une troisième fonction.

1/ : Le crible.

Le **périmètre** de travail du crible par famille: on travaille sur les entiers circonscrits aux familles suivantes qui seront appelé fam (i): («en fonction de la forme de $n=15k+i \rightarrow 2n = 30k + 2i$, on fixe la famille.» Ce qui donnera la famille complémentaire par rapport à $2n$, pas forcément la même. Par exemple si $n = 15k + 1$ on a $2n = 30k + 2$ on a que trois fam(i) possible $\{1, 13, 19\}$, $1+31=32$ et $13+19 = 32$. En fixant la **fam 13** on obtient les complémentaires $q \in \text{fam 19}$ et pour la **fam 1**; $q \in \text{fam 1}$ qui est la même.»)

fam(i) - $30k+1$
- $30k+7$
- $30k+11$
- $30k+13$
- $30k+17$
- $30k+19$

- $30k+23$
- $30k+29$

L'intérêt de travailler avec ces huit familles est qu'elles permettent de réduire le nombre d'entiers naturels avec lesquels on travaille, puisque tout entier de forme $30k+x$ avec x n'appartenant pas à $\{1,7,11,13,17,19,23,29\}$ n'est pas premier.

L'objectif est d'extraire de ces suites arithmétiques de raison 30, les nombres premiers supérieurs à 5 congrus à 1 [30] ou à p [30] avec p appartenant à $\{7,11,13,17,19,23,29\}$, et de décomposer les multiples de 30 en somme de deux nombres premiers par l'utilisation des congruences.

Construction de l'algorithme, crible de Goldbach:

[«Note: On peut construire directement le crible en partant de 1 et faire ressortir ses propriétés, en utilisant les nombres impairs représenté par des 1, les nombres pairs représenté par 0. Ainsi que les entiers qui seront congrus à $2n[p]$ noté $A \equiv 2n[p]$.

ex: 0,1,0,3,0,5,0,7,0,9,0,11...etc et avec $p \geq 3$. lorsqu'un nombre sera congru à $2n[p]$ il sera remplacé par 0 ou marqué en rouge suivant les cas ci-dessous par pas de p

ex: limite $n = 15$, $2n = 30$ et $p \leq \sqrt{2n} = 3$ et 5 le reste R de $2n$ par $p = 0$ et 0.

On part toujours de l'indice du reste: (ici) 0 avec $p = 3$ et on marque les entiers de 1 à 15 congruents à p d'un 0; suivant le principe d'Ératosthène **modulo** p ou par pas de p .

Si le reste $R \% 2 = 0$ on part de p puis $\pm 2p$.

(Ce qui est équivalent à marquer les multiples de $p \in [n; 2n]$, si ce n'est que l'on marque les entiers A congrus à $2n[p]$ de 1 à n)

ex: liste à cribler **limite** $n = 15$ [0,1,0,3,0,5,0,7,0,9,0,11,0,13,0,15]

résultat (mod 3) ou (mod $2*3$) [0,1,0,0,0,5,0,7,0,0,0,11,0,13,0,0]

résultat (mod 5) ou (mod $2*5$) [0,1,0,0,0,0,0,7,0,0,0,11,0,13,0,0]

Soit 3 couples $p'+q$ qui décomposent 30. On en déduit directement une conséquence du TNP:

Comme on crible avec les nombres premiers $p \leq$ racine de $2n$, la fonction du nombre d'entiers A non congrus à $2n[p]$ noté $A \neq 2n[p]$; devient $[n / \log 2n] \Rightarrow$ le nombre de nombres premiers $q \in [n; 2n]$.

Montrons le décalage d'un rang des congruences sur leur successeurs impair en progression arithmétique de raison 2, permettant d'affirmer que la conjecture sera vérifiée pour la limite $n+1$ suivante.

Propriété récurrente si un entier $A \neq 2n[p]$ précède un nombre premier $p'=A+2$, alors p' qui sera donc **non congru à $2n[p]$** vérifiera la conjecture pour la limite suivante $2n+2$ suivant l'égalité ci après: $30 - A \Leftrightarrow (30+2) - (A+2)$

Montrons:

Lorsque la limite n augmente de 1, et donc $2n$ augmente de 2, cela n'a pas d'influence sur les nombres de premiers $< (15+1)$ qui ne bougent pas.

Seul les congruences vont se décaler sur leur successeur $A+2$.

ex: liste à cribler $n+1$ [0,1,0,3,0,5,0,7,0,9,0,11,0,13,0,15,0]

les restes de 32 par 3 et 5, augmente de 2. Donc l'égalité $30 - A \Leftrightarrow (30+2) - (A+2)$.

Par conséquent, 1 qui était $\neq 2n[p]$ se reporte sur $(1+2) \neq (2n+2)[p]$ car 29 qui était un nombre premier q tel que $30 - 1 = 29$, sera toujours le même le contraire serait absurde.

D'où 3 sera $\neq (2n+2)[p]$ et tel que $32 - 3 = 29$ donnera pour $2n+2$ un couple $p'+q = 32$! On

vérification $n = 15$, $p = 3$, $R = 0$: $[0,1,0,0,0,5,0,7,0,0,11,0,13,0,0]$

résultat $n+1=16$, $p=3$ et $R=2$: $[0,1,0,3,0,0,0,7,0,9,0,0,13,0,0]$

a) la non congruence de 1 se reporte sur 3, celle de 3 qui était congru se reporte sur 5, celle de 7 se reporte sur 9 et celle de 9 se reporte sur 11.

b) vérification $n = 15$, $p=5$, $R = 0$: $[0,1,0,0,0,0,0,7,0,0,11,0,13,0,0]$

résultat $n+1=16$, $p=5$ et $R=2$: $[0,1,0,3,0,0,0,0,9,0,0,13,0,0]$

la non congruence de 1 se reporte sur 3, celle de 5 c'est reporté sur 7 **fin du crible.**

On a 2 couples $3+29$ et $13+19$ qui décomposent 32 et on constate bien que 23 qui est premier à pour antécédent $9 \neq (2n+2) [p]$, si les congruences ne se décalaient pas d'un rang, il serait resté congru à $(2n+2) [p]$ ce qui est absurde, car contraire au TFA et au TNP, ce qui garanti aussi la famille complémentaire!

Cela permet de garder la propriété des entiers $B \in [n; 2n]$; si $2n - A = B$ est un multiple de p , $(2n+2) - (A+2) = B$ sera toujours multiple de p ; et inversement si $2n - A = q$ premier $(2n+2) - (A+2) = q$ sera toujours premier.

Autre constat, 9 qui n'est pas premier mais qui précède 11 un nombre premier, **sa non** congruence se reportera sur 11 lors de la limite suivante $n+1$. Ce qui permet d'affirmer que pour $2n+2+2$ la conjecture sera encore vérifiée avec au minimum $34 - 11 = 23$.

On peut donc en déduire dès lors une troisième fonction caractérisée par cet algorithme, relative au TNP par rapport aux deux fonctions $[n / \log n]$ indique $\sim$ le nombre de premiers $\leq n$ et $G(n)$ qui vaut $\sim [n / \log 2n]$ indique le nombre d'entiers $A \neq 2n[p] \leq n \Leftrightarrow$ nombre de premiers $q \in [n; 2n]$ $[G(n) / \log G(n)]$ **qui indiquera le nombre minimum de couples $p+q = 2n$ lorsque $2n \rightarrow +\infty$**

Ce sont les même nombres premiers qui criblent, selon le même principe et ces deux algorithmes caractérisent les fonctions asymptotiques du TNP.

Pour $n=15$ on avait 4 entiers non congruent $[p]$ et 3 couples de premiers:

C'est à dire : pour $n-1$; $G(14)$ vaut $14/\ln 28 = 4,2$ $A \neq 2n[p]$ qui est le nombres de $A \neq 2n[p]$, **premiers ou pas, précédent un entier $A+2 = p'$** , ce qui implique par conséquent et suivant la propriété **b)** ci-dessus, le résultat du nombre de couples pour la limite suivante $2n+2=30$, que l'on vient de vérifier: on aura $4/\ln 4 = 2$ couples $p'+q < 3$ réels

Pour $n+1 = 16$ on 2 couples de premiers vérifieront 32 (« $15 / \ln 30 = 4,...$ et $4/\ln 4 = 2, ... \leq 2$.»)

pour $n+2=17$, $p = 3$ et 5; $R = 1$ et 4: donnera $[0,1,0,3,0,5,0,7,0,9,0,11,0,13,0,15,0,17]$ 4 couples de premiers $p'+q=34$. (« $16 / \ln 32 = 4,...$ et $4/\ln 4 = 2, ... \leq 4$.»)

pour $n+3 = 18$, sans vérifier, il est clair que l'on aura 4 couples $p'+q = 36$ car on a bien 4 $A \neq 2n[p]$ **qui précèdent p' . {3, 5, 11 et 15} et 15 n'est pas un P'** ; la fonction d'estimation aurait donnée 2 couples !

Ce qui permet avec cette propriété du décalage des congruences de ne pas tenir compte de la primalité des A qui précèdent p' ; mais simplement **du fait qu'ils sont non congruent à p .**

Cette fonction caractérisée par le crible de Goldbach et aussi caractérisé par le TNP, car cela revient à cribler avec Ératosthène uniquement les entiers $A \neq 2n[p]$ pour la même limite !

Elle sera bien inférieur au nombre réel de couples qui décomposent $2n$ en somme de deux premiers lorsque la limite du crible $n \rightarrow +\infty$.

Comme on peut le vérifier le décalage des congruences se produit sur plusieurs limite $n+k$ successives qui vérifieront la conjecture.

En fin de document on construit le programme pour cribler les entiers A impairs de 1 à n.
 Fin pour cette partie avec le crible dans les entiers A impairs en progression arithmétique de raison $2 \leq n$. »]

On va cribler dans les familles en progression arithmétique de raison 30:

On va utiliser le même principe, mais en calculant l'index de départ des nombres premiers p qui cribleront suivant la famille $30k+(i)$ noté fam(i) utilisé par rapport à $n \geq 150$, en progression arithmétique de raison 15. Les entiers A de 1 à n sont en progression arithmétique de raison 30. Sont exclu les multiples de 2, 3 et 5.

Avec Ératosthène en début de programme on extrait les premiers $p \leq \sqrt{2n}$

On établit un tableau de $1^* (n//30)$.

On calcul le reste R de $30k + 2i$ par p.

puis si $R \% 2 = 0$ on ajoute p tel que $R + p = j$; puis $+ 2p$ tant que $j \% 30$ est différent de fam (i) si $j \% 30 = \text{Fam}(i)$ on calcul l'index tel que $j // 30 = \text{idx}$.

Puis on crible de l'idx qui sera marqué 0, par pas de p $\rightarrow n // 30$ en remplaçant les 1 par 0. les 0 seront les entiers $A \equiv 2n[p]$; à la fin on compte les 1 qui sont les $A \not\equiv 2n[p]$.

Ex: on fixe la limite $n=15k+i=300$, la fam(i) = 7 progression arithmétique de raison 30 ; les A seront représenté par des 1: $A \in [7, 37, 67, 97, 127, \dots, 277 < 300]$

tableau du crible $n//30$ [1,1,1,1,1,1,1,1,1] p = 7,11,13,17 le R de 600 par p = 5, 6, 2, 5 on calcule $j = R + p$ si $R \% 2 = 0$, sinon $R += 2p \rightarrow j \% 30 = \text{fam}(i) = 7$

$p=7$, $R=5$ va donner $\rightarrow 5+14, 19+14 \rightarrow 33, 47, 61, 75, 89, 103, 117, 131, 145, 159, 173, 187 \equiv 7 \% 30$,

on calcul l'index : $\text{idx} = j // 30$, $187 // 30 = 6$. et on va cribler en partant de idx, « attention on compte en commençant par 0, 1, 2, ..., $n // 30$ » on remplace le 1 par 0 puis par pas de 7 .

ce qui va donner $\rightarrow [1, 1, 1, 1, 1, 1, 0, 1, 1]$ puis on réitère avec $p = 11$, $R = 6$

$127 \equiv j \% 30 \rightarrow [1, 1, 1, 1, 0, 1, 0, 1, 1]$ puis on réitère . $p = 13$, $R = 2$,

$67 \equiv j \% 30 \rightarrow [1, 1, 0, 1, 0, 1, 0, 1, 1]$ puis on réitère . $p = 17$, $R = 5$ donnera 187 qui est déjà marqué,

$187 \equiv j \% 30 \rightarrow [1, 1, 0, 1, 0, 1, 0, 1, 1]$ fin on fait la somme des 1 = 7 $A \not\equiv 2n[p] = 7$ premiers $q \in [n; 2n]$.

Ératosthène pour la même limite et la même fam(i) donnera les nombres $1 = p' \in [1, 1, 1, 1, 1, 0, 0, 0, 1]$.

En criblant le tableau d'Ératosthène avec le crible (G) $\rightarrow 0 = A \equiv 2n [p] \in : [1, 1, 0, 1, 0, 1, 0, 1, 1]$;

ce qui donne le résultat suivant : nombre de couples $p'+q = 600$; 5 couples $\in : [1, 1, 1, 1, 1, 0, 0, 0, 1]$

La propriété récurrente est la même, lorsque n ou $n+i$ augmente de 15 les congruences se décalent d'un rang sur leur successeur $A+30$. «On a nul besoin de se soucier de la fam i complémentaire pour vérifier la conjecture, car l'algorithme utilise les congruences et q a pour antécédent A.»

Cela donnera par obligation le tableau suivant pour $2n = 630$; 4 couples, sans même avoir besoin de cribler:

..... [x, 1, 1, 1, 1, 0, 0, 0, 1] seul le premier élément x est inconnu .

résultat réel pour $n=315$; vérifié :

Donnez N: 315; crible EG_2n_mod30: [1, 1, 1, 1, 1, 0, 0, 0, 1, 1] 4 couples $p+q = 2n$. Et ~ autant pour $2n = 660$

[1, 1, 1, 1, 1, 0, 0, 0, 1, 1] réel 6 couples

Ce qui permet de prédire formellement que la conjecture sera vérifiée pour la limite $2n = 30(k+1) + 2i$; sans avoir besoin de cribler cette limite $n = 15(k+1)+i$.

En effet: si $A \neq 2n[p]$ premier ou pas précèdent $A+30$ premier p' , congru ou pas à $2n [p]$ alors ce dernier, qui par obligation sera **non congruent à p**, il formera un couple: $p' + q$ qui décompose $2n = 30(k+1) + 2i$ en somme de deux premiers !

Il devient donc avec d'autres raisonnements à l'appui, **impossible d'infirmer la conjecture** pour la limite $2n = 30(k+1) + 2i$.

La fonction 2 du théorème de Goldbach est une conséquence directe du TNP: (log = logarithme naturel)

$G(n)$: la fonction de compte du nombre de nombres premiers $q \in [n; 2n]$

Corollaire: $G(n)$ vaut $\sim \lim_{n \rightarrow +\infty} \frac{n}{(\log 2n)}$

Le TNP dit que $\pi(n) = \frac{n}{(\log n)} + o(\frac{n}{\log n})$, donc le nombre de nombres premiers dans $]n, 2n]$ vaut

$$\begin{aligned} \pi(2n) - \pi(n) &= \left(\frac{2n}{\log(2n)} - \frac{n}{\log n} \right) + o\left(\frac{n}{\log n}\right) \\ &= n \times \left(\frac{2}{\log 2n} - \frac{1}{\log n} \right) + o\left(\frac{n}{\log n}\right) \\ &= n \times \frac{2\log n - \log(2n)}{\log(2n)\log n} + o\left(\frac{n}{\log n}\right) \\ &= \frac{n}{(\log 2n)} + o\left(\frac{n}{\log n}\right) \end{aligned}$$

Tout nombre pair $2n \geq 180$ peut s'écrire comme la somme de deux nombres premiers ($P' + q$) appartenant à une famille $Fam(i)$ tel que définie en début de document.

Mais plus précisément pour $n \geq 3000$: $C_2 \frac{G(n)}{\ln G(n)}$; où $C_2 \approx 1,320323...$ constante premiers jumeaux.

* Un autre document explicite ce fonctionnement et sa résolution, avec les programmes relatif à ces deux algorithmes.

Suite du crible pas à pas à partir de 30:

Soit $p \leq \sqrt{30k}$ un nombre premier. Tout nombre premier $p' < 30k/2$ qui n'est pas congru à $30k$ modulo p est un décomposant de Goldbach : admettons que p' soit congru à $30k$ modulo p , le reste R de $30k/p$ et le R de p'/p est le même, donc p divise $30k - p'$ qui est un multiple de p .

Démonstration : (pour $30k > 30$, il existe y/y' tels que $30k = p*y + R$ et $p' = p*y' + R \Rightarrow 30k - p' = p*(y - y')$ donc p divise $30k - p'$).

Il vient donc que si p' n'est pas congru à $30k$ modulo p , p' et $30k$ ne partagent pas le même R , et donc p ne divise pas $30k - p' = q$. Il est donc un nombre premier et par conséquent ils forment un couple de nombres premiers, qui décomposent $2n$ en la somme de deux nombres premiers.

Conséquence directe, q dépend de la congruence des entiers de 1 à n .

Soit p_n l'ensemble des nombres premiers appartenant à $[7 ; \sqrt{30k}]$, soit p'_n l'ensemble des nombres premiers appartenant à $[7 ; 30k/2]$ qui ne sont pas congrus à $30k$ modulo p (quelque soit $p \in p_n$), leurs complémentaires q par rapport à $30k$ sont premiers ($q = 30k - p'$).

On se moque de la décomposition via les nombres premiers 2,3,5 puisque tous les multiples de 30 sont congrus à 0 [2], 0 [3], 0 [5] et aucun p' appartenant à $[7 ; 30k/2]$ n'est congru à 0 [2], 0 [3], 0 [5].

Note pour : Si $30k - p'$ est divisible par 3 alors p' est congru à 0 [3], soit p' est divisible par 3 et n'est donc pas premier, ce qui est une contradiction.

Par conséquent :

1. On détermine ainsi en suivant la progression du crible les nombres premiers $p \in p_n$ inférieurs à $\sqrt{30k}$.
2. On détermine les nombres premiers $\leq 30k/2$ qui ne sont pas congrus à $30k$ modulo p : les $p' \in p'_n$
3. Comme les complémentaires $q = 30k - p'$ sont premiers, on peut ainsi connaître les couples de Goldbach pour la valeur $30k = (p' + q)$ en criblant uniquement jusqu'à n .

a) : On part de $30k$ avec $k=1$

Les premiers appartenant à $[7 ; 30]$ sont $\{7 ; 11 ; 13 ; 17 ; 19 ; 23 ; \text{et } 29\}$;

30 est congru à 0 [3] et 0 [5] la racine carrée de 30 est inférieure à $p = 7$, ainsi les nombres premiers ci dessus qui ne sont pas congrus à 0 [3] et 0 [5] sont des décomposant de Goldbach pour $30/2$. Il y a trois couples $p' + q$: 7/23, 11/19, 13/17.

Reste le nombre premier 29 qui ne peut former un couple, car 1 n'est pas un nombre premier.

Ces premiers, vont servir de base pour construire le crible.

b) : décomposition de $30k$ avec $k=2$ (60)

Je me sers des nombres premiers déterminés pour $k=1$, afin de décomposer $30k$ avec $k=2$ ($30k=60$)

Je détermine les $p < \sqrt{60}$ (<8) soit : $p = 7$

Je détermine les p' appartenant à $[7 ; 60/2]$ qui vont être criblés, ils ont été extrait par la décomposition de 30 avec 29 en plus, et forment la base de nombres premiers p' à utiliser pour ce crible : $\{7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29\}$

Je détermine ceux parmi ces nombres premiers p' qui ne sont pas congruents à 60 modulo 7, le reste R de 60 par p étant $R = 4 \dots$

Le principe est le même que selon la méthode d'Ératosthène, qui serait de supprimer parmi les nombres entiers considérés les multiples de p (ici 7), ici en considérant également le reste : on supprime les nombres premiers $p' = p + R$ (ici 4), jusque $60/2 = 30$, soit $p'=11$.

Ainsi, on supprime parmi l'ensemble des $p' \in p'_n$ les nombres de la forme $R + n \cdot p$ avec n entier naturel appartenant à $[1; (30k/2)/p]$, n étant ainsi défini et borné puisque l'on cherche à éliminer les $p' \equiv 30k[p]$ appartenant à $[7; 30k/2]$.

Ici : la limite n est borné par $30k/2/p = 30/7$ a pour quotient 4 qui sera la limite de n ; à ne pas confondre avec le reste $R = 4$ de 60 par 7

$$R + 1 \cdot p = 4 + 1 \cdot 7 = \underline{11}$$

$$R + 2 \cdot p = 4 + 2 \cdot 7 = 18$$

$$R + 3 \cdot p = 4 + 3 \cdot 7 = 25$$

$$R + 4 \cdot p = 4 + 4 \cdot 7 = 32 > 30$$

Parmi la liste des $p' \{7; \underline{11}; 13; 17; 19; 23; 29\}$ on supprime donc le 11 qui n'est pas un décomposant de Goldbach.

En fonction de la parité de R , et du fait que l'on crible des impairs, on aura au départ soit : $(R + p)$ ou $(R + 2 \cdot p)$: puis $+ 2 \cdot p \dots + 2 \cdot p$; dans la limite de $60/2$.

Tous les autres sont des décomposant de Goldbach, soit :

7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29. leurs complémentaires q par rapport à 60 sont :

53 ; ; 47 ; 43 ; 41 ; 37 ; 31 .

L'ensemble des premiers appartenant à $[7; 60 - 1]$: $\pi(60)$ vaut 14 à une unité près, soit 13 pour ce cas présent.

Car si $60 - 1$ est premier, il ne peut être extrait qu'à l'itération suivante tel que :

$31 + (60 - 1) = 60 + 30$; et de façon générale : $31 + (30k - 1)$ avec $30k - 1$ premier.

$1 + 59$ n'est pas un couple $(p' + q)$.

L'ensemble des premiers appartenant à $[7; 30]$: $\pi(30)$ vaut 7.

On peut donc estimer le nombre de p' qui sont des décomposant de Goldbach, donc le nombre de couples $(p' + q = 2n)$ selon deux méthodes les fonctions d'estimation $\pi(n)$ ou $G(n)$:

- 1) Pour 30, on n'a pas eu à cribler, mais on a 7 premiers : $7 / \ln 7 = 3,59 \dots$
- 2) Pour 60, on a 7 p' à cribler : $7 / \ln 7 = 3,59 \dots$

Dans le crible d'Ératosthène, et son principe de criblage, on aurait estimé pour un nombre d'entiers criblés: 30 ; puis pour 60, pour connaître environ le nombre de premiers. Selon la formule du TNP, et en déduisant les 3 premiers 2, 3 et 5.

Dans ce crible, on connaît le nombre d'entier que l'on va cribler, et surtout le nombre de premiers p' à cribler parmi ces mêmes entiers.

Et selon le TNP, on peut donc estimer: le nombre de premiers p' à cribler pour ces deux premiers cas; mais aussi le nombre d'entiers non congrus à $30k[P]$, $P \leq \sqrt{30k}$. Selon la fonction du TNP modifiée : $15k / \ln 30k$: du fait que l'on utilise les $P \leq \sqrt{30k}$ et non les $P \leq \sqrt{(30k / 2)}$.

On va donc obtenir une estimation minorée, selon le principe suivant en trois étapes: afin de détailler ce principe. En déduisant les trois premiers 2, 3 et 5.

c) : $((30k / 2) / \ln(30/2)) - 3 = 2,532....$ p' à cribler

d) : $2,53 / \ln 2,53 = 2,71...p'$ non congru à 30 modulo 7 ; décomposant de Goldbach.

e) : Minoration selon le TNP : $(30k / 2) / \ln(30/2)^2 = 2,04....$ décomposant de Goldbach.

f) : pour 60, estimation minorée : $(60k / 2) / \ln(60/2)^2 = 2,59...p'$ non congrus à 60 (mod 7) soit 2,59...couples (p'+q).

g) : Pour 90 on obtiendra $(90k / 2) / \ln(90/2)^2 = 3,10...p'$ non congrus à 90 (mod p).

On crible pour 90, on connaît $\pi(45)$ qui vaut 11, et l'estimation de p' non congru 90 (mod 7) vaut $11/\ln 11 = 4,58..$

soit les p' à cribler :

{7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43}

les $p_i < \sqrt{90} (< 9)$ soit : 7

la congruence R (« le reste R de 90 par p_i ») : $90/7$ donne R = 6

On fixe le départ du crible pour 90, Soit : $6+7 = 13$; $+14 = 27$; $+14 = 41$; $+14 = 55 > 45$; fin du crible pour 90.

On relève les p' congru à 90 [7] , on a **13 et 41**.

Les décomposant de Goldbach sont :

7 ; 11 ; ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; ; 43. Soit 9 couples :
83 ; 79 ; ; 73 ; 71 ; 67 ; 61 ; 59 ; 53 ; ; 47.

L'estimation minorée du nombre de décomposant de Goldbach, vaut : $45 / (\ln 45)^2 = 3,10.. < (11 / \ln 11) < 9$.

Ce qui fait rajouter à la base de donnée premières, les nouveaux premiers $q > (60 - 1)$
83 ; 79 ; ; 73 ; 71 ; 67 ; 61 ; 59 .

Puis on réitère pour $30(k+1)...$ etc.

$\pi(90)$ appartenant à [7 ; 90] = $\pi(60 - 1) + 7 = 20$ à l'unité près, car $89 + 1 \neq (p' + q)$.

Le nombre de p' à cribler pour $30(k+1)$ sera égal à $\pi(60) = 14$ et bien entendu le nombre de p' non congru $30(k+1) \pmod{p}$ vaudra $\approx 14 / \ln 14 = 5,304...$

Les 14 premiers p' à cribler sont ceux de $90/2 + 47, 53, 59$ soit :
{7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43 ; 47 ; 53 ; 59}.

Pour 120, le modulo p_i sera toujours 7, et le reste R de 120 par 7 = 1.

On partira donc de $(1 + 2*7) = 15$; $+14 = 29$; $+14 = 43$; $+14 = 57$ fin du crible.

29 et 43, sont barrés, on obtient 12 couples (p'+q) pour 120.

Estimation minorée de (p' + q) : $60 / (\ln 60)^2 = 3,57....$

Les premiers q appartenant à [60 ; 120] sont :

{ 61, 67, 73, 79, 83 ; **89, 97, 101, 103, 107, 109, 113.**} et on rajoute à la base de donnée première, les premiers [90-1 ; 120].

On vient donc de voir, que quelque soit $30k$, on recommence toujours un nouveau criblage pour $30(k+1)$, en repartant de p_i et $p' = 7$ pour :
 p_i appartenant à $[7 ; \sqrt{30(k+1)}]$; et p' appartenant à $[7 ; (30(k+1)) / 2]$.

2/ : On a fait qu'utiliser le principe et la méthode du crible Ératosthène, dire que tous les nombres premiers ne seraient pas extraits, revient à dire que le crible d'Ératosthène, est faux.

[En résumé avec A un entier non nul de 1 à n :

*Suivant le principe du crible d'Ératosthène il suffit d'utiliser P pour dire, que si B n'est pas divisible par $P \leq \sqrt{2n}$, il est alors un nombre premier q , en effet si $2n \neq A[P]$, $2n - A = B$ qui n'est pas un multiple de P ; car A et $2n$ sont dit **non congruent mod P** , ie : ils ne sont pas égaux modulo P .*

Le crible G est donc une variante du crible d'Ératosthène, mais qui utilise les congruences :

Pour dans un premier temps marquer les entiers A congrus à $2n$ modulo P où A et $2n$ partagent le même reste dans la division par P et par conséquence, indirectement dans un deuxième temps, indiquer les multiples de P tel que $2n - A = B = Py$

(1) rappelons : si est seulement si $2n$ et A sont égaux modulo P , il existe y et y' tel que :

*$2n = P*y + R$ et $A = P*y' + R \Rightarrow 2n - A = P*(y - y')$; donc P divise $2n - A$.]*

On supprime tout simplement les entiers qui sont congrus à $30k$ modulo p , soit $p + R$ et on indique par la même, les multiples de p appartenant à $[n ; 2n]$ et tel que $2n - n \neq q$.

Ce qui n'enlève aucune perte de généralité, par rapport à Ératosthène ; c'est tout simplement un corollaire d'Ératosthène .

L'utilisation du TNP dans ce cas, est parfaitement justifiée de par la propriété du décalage des congruences que l'on a vue en début de document.

Ce qui permet de dire que le point **3/ :** est vrai ; **a) :** car quel que soit $30k$, $(30k/2) / (\ln 30k / 2)$ donnera bien parmi les entiers criblés appartenant à $[7 ; 30k/2]$ une estimation de premiers p' à cribler.

Et en **b) :** en ré-estimant une deuxième foi, on obtient pour les premiers p' criblés, les p' non congrus à $30k$ modulo p , car on utilise le même principe et les même nombres premier p qui criblent.

Ce qui dans le cas contraire, revient exactement à dire que dans Ératosthène pour une limite $30k / 2$ criblée, il n'y a pas de nombre premiers entre $\sqrt{30k}$ et $30k/2$.

Ce qui est absurde car la fonction $G(n)$ a été démontrée !

Exemple pour 30 et 15 , $15 > \sqrt{30}$; puis entre 15 et $7,5 > \sqrt{30}$. il y aurait au minimum deux premiers, il existe tout autant deux p' non congrus à 30 modulo 5 , ou modulo 3 . Ce que confirme le TNP dans sa formule minorée.

L'estimation minorée du TNP, donne : $15 / (\ln 15)^2 = 2,04...$

Le nombre de couples $(p' + q) = 30$, vaut 3 .

On ne peut pas avoir $(30k/2) / (\ln 30k/2)^2 = 0$; du fait que l'on crible les congruences des entiers de 1 à n et où q dépend de la congruence de P et du décalage obligatoire d'un rang des congruences pour la limite $n = 15(k+1)$ ou simplement $n+1$ ce que l'on a vu.

Le point **4/ :** sera tout simplement une réplique de ce que l'on vient de voir pour les multiples des 30 avec certaines conditions.

Note : (« le modulo 30 permet de cribler par pas de 30, par conséquent de cribler tous les multiples de 30. Un autre modulo comme 60, 90 ou autre ..etc, laisserait des trous, et ne permettrait pas d'utiliser ce crible pour les autres suites arithmétiques de raison 30, suivant le point 4/ :

La fonction de compte des nombres premiers, $\pi(n)$ ne pourrait être utilisée avec précision.»)

4/ : on vient de voir pour les 30k, on va cribler et décomposer les entiers pairs non multiple de 30, comme précédemment.

Ils se répartissent selon 14 suites arithmétiques de raison 30 ; et leur décomposition en somme de deux premiers, va utiliser qu'un nombre restreint parmi les 8 suites de premiers du point 1/ : . La cause est due aux deux nombre premier 3 et 5.

Car comme précédemment, on n'utilisera pas ces deux nombres premiers dans les premiers p qui criblent sans perte de généralité.

4.1 :

Pour les multiples de 6, on distingue 4 suites arithmétiques qui sont congrues à 1,2,3 ou 4 modulo 5:

- $30k+6$
- $30k+12$
- $30k+18$
- $30k+24$

Pour chacune de ces suites arithmétiques, on criblera toujours selon le même principe et la même méthode, les premiers p' appartenant à 6 suites de premiers du point 1/ , en fonction du premier terme : 6, 12, 18 ou 24.

Ce qui donne un coefficient multiplicateur dans la formule de minoration, utilisé pour les 30k, égal à 0,75.

Soit par exemple, pour la suite $30k + 18$:

$$((18/2) / (\ln 18/2)^2) * 0,75 = 1,39..$$

$$((48/2) / (\ln 48/2)^2) * 0,75 = 1,78.....$$

$30k + 18$ se décompose avec les premiers > 5 , $(p'+q)$ en progression arithmétique de raison 30:

(7 et 11) ; (19 et 29) et (17 et 31).

La suite de premiers $\equiv 13 [30]$, utilise les multiples de 5, ainsi que les premiers $\equiv 23 [30]$.

Cette suite $30k+18 \equiv 3 [5]$, comme les deux suites de premiers.

On pourra vérifier qu'il en est de même pour les trois autres suites $30k + 6$, ou $+12$, ou $+24$.

$30k+6 \equiv 1[5]$ ce qui supprime les p' appartenant aux suites $30k+1$ et $30k+11$.

$30k+12 \equiv 2 [5]$, supprime les premiers p' appartenant aux suites $30k+7$ et $30k + 17$.

$30k+24 \equiv 4 [5]$, supprime les premiers p' appartenant aux suites $30k+19$ et $30k + 29$.

4.2 :

Les deux suites arithmétiques :

$$30k+10$$

$$30k+20$$

Elles se décomposent en somme de deux premiers $(p' + q)$ appartenant a 4 suites du point 1/ : .

Ce qui donne un coefficient multiplicateur dans la formule de minoration égal à 0,5.

Par exemple pour $30k+10$

$$((40/2) / (\ln 40/2)^2) * 0,5 = 1,11...$$

$30k+10 \equiv 1[3]$ ce qui supprime les p' appartenant aux suites $30k+1$; $30k+7$; $30k+13$ et $30k+19$
 $30k+20 \equiv 2[3]$ ce qui supprime les p' appartenant aux suites $30k+11$; $30k+17$; $30k+23$ et $30k+29$

4.3 :

Les huit suites arithmétiques qui ne sont que celle du point **1/** , où on multiplie le premier terme par 2.
 La décomposition de ces entiers pairs, utilise uniquement les p' appartenant a trois suites de premiers, du point **1/** :

- $30k+ 2*1$
- $30k+ 2*7$
- $30k+ 2*11$
- $30k+ 2*13$
- $30k+ 4$
- $30k+ 8$
- $30k+ 16$
- $30k+ 28$

Le coefficient multiplicateur de la formule de minoration, sera donc : 0,375.

Par exemple pour $30k+(2*7)$, soit $30k+14$.

$$(14/2) / (\ln 14/2)^2 * 0,375 = 0,753... ;$$

On a vérifié que 14 se décompose avec $7+7$, ou $3+11$ mais on se borne aux premiers > 5 . On peut cribler les $2n$, à partir de 18, dans ces suites d'entiers pairs. Car $12=5+7$, $16=5+11$ ou $3+13$

$$(44/2) / (\ln 44/2)^2 * 0,375 = 1,15...$$

4.3 :

On va montrer différentes décompositions de ces entiers pairs illustré par des tableaux, et 3 annexes en fin de dossier ; notamment l'annexe 3, qui est simplement le crible d'Ératosthène dans les entiers des 8 suites du point **1/**.

Un début du crible est effectué avec l'entier $9550 \equiv 10 [30]$

Tableau des premiers < 120 dans Eratosthène modulo 30.

(7).	(11).	(13)	(17).	(19)	(23)	(29)	(31).
37	41	43	47	0	53	59	61
67	71	73	0	79	83	89	0
97	101	103	107	109	113	0	0

Annexe 1:

Pour programmer l'algorithme dans les entiers impairs , on utilise le principe suivant «résumé»:

a) on crible avec Ératosthène les nombres premiers $p \geq \sqrt{2n}$ qui vont intervenir: **def eratosthene (n):**

b) on va rappeler ces premiers qui vont être utilisé par la fonction :

def G_crible (premiers,n):

On génère un tableau de N/2 cases rempli de 1

crible = n//2*[1]

```
# On calcule les restes: ri = 2*n/pi
nbpremiers = len(premiers)
n2 = 2*n
```

```
for i, premier in enumerate(premiers):
    reste = n2 % premier
```

```
if reste % 2 == 0:
```

```
    reste += p puis on crible modulo p à partir de ce (ri+ p) sans oublier de remplacer le 1 par 0 et on
    remplace tous les 1 par 0 modulo p, on sort du programme et on réitère avec p suivant et son ri
```

```
else si le reste est impair on crible directement à partir du 1 = ri, que l'on remplace par 0 et on crible
    modulo p
```

Exemple : avec $n = 26$, $2n = 52$ les premiers $p < \text{racine de } 52$, sont $\{3, 5 \text{ et } 7\}$ les ri sont $\{1, 2 \text{ et } 3\}$

tableau à cribler qui serait représenté uniquement par des 1 : $[1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25]$

on crible avec $p=3$ à partir de son $ri=1$: $[0, 3, 5, 0, 9, 11, 0, 15, 17, 0, 21, 23, 0]$ fin pour 3

on crible avec $p=5$ à partir de son $ri=2$ donc $2+5=7$ qui est marqué : $[0, 3, 5, 0, 9, 11, 0, 15, 0, 21, 23, 0]$ fin pour 5

on crible avec $p=7$ à partir de son $ri=3$ puis 17 qui est déjà marqué : $[0, 0, 5, 0, 9, 11, 0, 15, 0, 21, 23, 0]$ fin pour 7

```
print(f"Nombres non congru 2n[pi] {1} à {n}, premiers de {n} à {n2}: {total} ----- {int((time()-
start_crible)*100)/100}")
```

Résultat: 6 nombres premiers q entre 26 et 52 {47,43,41,37, 29 et 31}

3 couples de premiers qui décompose 52: 5+47; 11+41 et 23+29 .

(« attention: ligne de programme python copier dans le crible mod 30 GTY ainsi que la suite, la fin du programme ci-dessous ne devrait pas changer beaucoup... mais je ne suis pas programmeur »)

```
def main():
```

```
    # On demande N a l'utilisateur
```

```
    n = demander_N()
```

```
    # On récupère les premiers entre 3 et  $\sqrt{2N}$ 
```

```
    premiers = eratostene(n)
```

```
    #lprint("premiers:", premiers)
```

```
    #print(f"nombres premiers entre 3 et {int((2*n)**0.5)}: {len(premiers)}")
```

```
    start_time = time()
```

```
    # On crible
```

```
    GCrible(premiers, n)
```

```
    temps = time()-start_time
```

```
    print(f"--- Temps total: {int(temps*100)/100} sec ---")
```

```
    et
```

```
    main()
```

```
    system("pause")
```

Annexe 2 autre exemple :

Avec la suite arithmétique $30k+10 = 9550$: Selon le même principe et la même méthode que pour les multiples de 30.

On ne va donc cribler que les p' des 4 familles 11 et 29 de raison 30 ; ainsi que 17 et 23 appartenant à $[7 ; 9550 / 2]$.

Par contre, on va bien utiliser pour ce faire, la totalité des $P_i[7 ; < \sqrt{9550}]$ pour cribler les p' de ces quatre suites ; Pour déterminer les p' non congrus à 9550 $[P_i]$. On a par supposition, déjà extrait la totalité des premiers $< 9550 - 30$, et appartenant à ces 4 suites arithmétiques.

On connaît par conséquent : $\pi(9520)$ à une unité près, sans les 3 premiers 2, 3 et 5, et à plus forte raison :
 $\pi(9550/2) = 323$ p' dans ces 4 familles. (« Estimation directe connaissant la valeur du nombre de p' pour $\pi(4775)$ que l'on a extraits avec le crible : $323 / \ln 323 = 55,90$...non congrus à 9550 $[p_i]$ »)

Le TNP donne l'estimation de p' à cribler : $(4775 / \ln 4775) * 0,5 = 281,83$...

Et l'estimation de couples p' non congrus à 9550 $[p_i]$:

$281 / \ln 281 = 49,83$... (« Sans avoir besoin de s'occuper du nombre de nombre premiers q appartenant à $[15k; 30k]$ »)

L'estimation minorée de p' ou de couple $(p+q) = 9550$, vaut :

$(4775 / (\ln 4775)^2) * 0,5 = 33,27$...

Le tableau illustre les entiers de ces 4 familles, qui vont être criblé et on ne s'occupe que des premiers p'.

Les 0 représentent les entiers non premiers dans ces 4 familles.

7	11	13	17	19	23	29	31
37	41	43	47	0	53	59	61
67	71	73	0	79	83	89	0
97	101	103	107	109	113	0	0
	131		137		0	149	151
	0		167		173	179	181
	191		197		0	0	211
	0		227		233	239	

On calcule la racine carrée de 9550 pour déterminer les p_i , soit $p_i \leq 97$.

On va utiliser les p_i appartenant à $[7; 97]$ des 8 suites de premiers 1/.

Soit 22 modulus p_i :

9550 à pour reste R par 7 : 2

9550 à pour reste R par 11 : 2

9550 à pour reste R par 13 : 8

....etc jusqu'à 97.

9550 par 97 donne R = 44.

On commence avec 7 : pour barrer les $p' = 2 + n*7$.

$2+7 = 9$; $+14 = 23$; $+14 = 37$; $+3*14 = 79$; $+2*14 = 107$; $+14 = 121$; $+2*14 = 149$; $+14 = 163$; $+2*14 = 191$; $+3*14 = 233$.

On note qu'ensuite, et par colonne : on progresse modulo 210, ce qui fait que $23 + 210 = 233$; il est congru à 9550 [7]. ..etc ; pour les autres p' de ces 4 familles, où on rajoute le modulo 210, jusqu'à la limite 4775.

Par grille de crible on ne peut barrer qu'un entiers p' ou pas : par colonne, et tous les $p_i * 8$ entiers d'une grille de crible. Dans cet exemple, la grille de crible avec $p_i = 7$, comporte 8 termes, et parcourt 56 entiers par itération. Pour $p_i = 11$ la grille va parcourir 88 entiers dans les 8 familles ...etc

Les 8 termes d'une grille de cribles peuvent être remplacés par des 0, un tableau en annexe, donne une illustration, pour 9540, ainsi que la construction ; qui est programmable.

A partir des 8 termes, de ces 8 familles, on progresse par colonne modulo $p_i * 30$ pour marquer les p' congruent à $30k + 10$ modulo p_i .

Autrement dit et comme on ne s'intéresse qu'à 4 familles, on progressera modulo $p_i * 30$ dans ces 4 familles, et pour cette exemple jusqu'à 4775, on va barrer tous les p' congrus à 9550 [7] ; depuis :

$23 + n*210$; $107 + n*210$; $149 + n*210$; et $191 + n*210$.

Tableau ci-dessous, qui illustre le crible des p' par $p_i = 11$ avec R = 2

Soit le départ : $2+11 = 13$; $+3*22 = 79$; $+22 = 101$; $+3*22 = 167$; $+2*22 = 211$; $+22 = 233$; $+2*22 = 277$; $+22 = 299$; $+2*22 = 343$etc on réitère.

On a illustré en jaune clair les cellules congrues à 9550 [11] des 8 familles, pour la première itération, et le départ de la deuxième itération modulo 330 ; soit $13 + 330 = 343$, en notant le fait que l'on ne s'occupe que des p' ; appartenant à 4 familles.

7	11	13	17	19	23	29	31
	41		47		53	59	
	71		0		83	89	
	101		107		113	0	
	131		137		0	149	
	0		167		173	179	
	191		197		0	0	
	0		227		233	239	
	251		257		263	269	
	281		0		293	0	
	311		317		0	0	
	0		347		353	359	

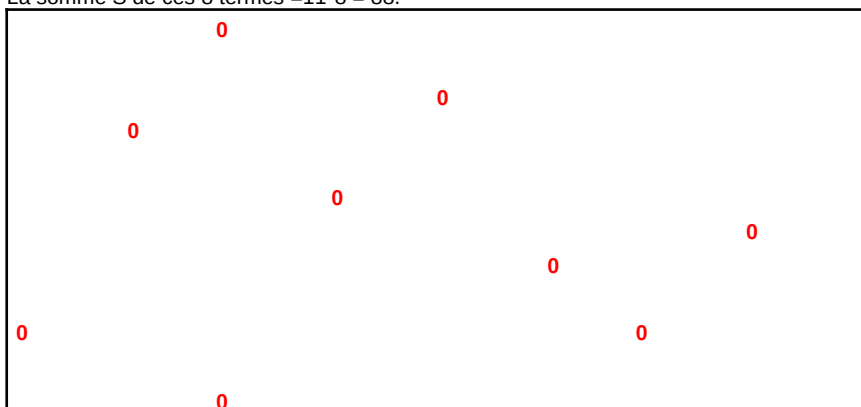
Exemple de ce que donne une table de crible, avec des 0 : méthode et principe Eratosthène.

table de crible (T,11) pour $9550 \equiv 2 [11]$, départ : cellule 13, puis on duplique : A partir de la onzième cellule même colonne.

EX:

raison 330 entre chaque 0 de chaque colonne et on peut compter les cellules, depuis la première jusqu'à la deuxième...etc → à la dernière avec 8 termes : 18,5,18,12,6,11,6,12. puis on réitère.

La somme S de ces 8 termes $= 11 \times 8 = 88$.



Cette table montre parfaitement, que les entiers des 8 familles sont criblés uniformément, quand bien même on ne prend en compte : que les p' des 4 familles arithmétiques ; 11, 29, 17, et 23 de raison 30.

Pour $p_i = 13$ et $R = 8$; on partira de $(8+13 + 2*13) = 47$; $+26 = 73$; $+3*26 = 151$; $+ 2*26 = 203$; $+ 26 = 229$;
 $+ 2*26 = 281$; $+26 = 307$; $+2*26 = 359$; $+ 3*26 = 437...$ *etc, on progresse modulo $(13*30)$ par famille.*