# Nombres premiers en seconde : visite d'un site anglophone

Jean-François Kentzel

Jean François Kentzel
enseigne au Lycée Pardailhan à Auch (32)
jkentzel@ac-toulouse.fr

J'aborde souvent sans enthousiasme excessif le premier chapitre de la classe de seconde (Nombres) qui me semble être une collection disparate (et nécessaire) de notions de base. Alors même qu'à cette époque de l'année, les classes sont elles-mêmes des collections de visages disparates, tous inconnus…

Cette année, pour rompre avec cette mauvaise habitude, j'ai approfondi la notion de nombre premier avec ma classe (un des thèmes facultatifs du programme est intitulé : problèmes historiques sur les nombres). Lorsqu'on dresse la liste des nombres premiers inférieurs à 100, leur « raréfaction » saute aux yeux et la question « en existe-t-il une infinité ? » (je préfère dire aux élèves : « en trouve-t-on toujours ? ») devient naturelle. Elle l'est encore plus si on parle du crible d'Erastothène.

J'ai donc demandé aux élèves de calculer le pourcentage (arrondi à l'unité) des nombres premiers parmi les nombres inférieurs à $x$ pour $x$ valant 10, 100,…$10^7$ (voir l'annexe 1).

Après une autre question qui était une preuve (très guidée) de l'infinitude des nombres premiers, la dernière question posée au devoir était un comptage approximatif du nombre de chiffres du nombre premier $2^{20996011} - 1$ (record du plus grand nombre premier connu en 2003) à l'aide de l'égalité $2^{10} = 1024$. Ici on obtient une approximation intéressante (on se trompe de « seulement » 21627 chiffres) et on montre facilement que le nombre obtenu est en fait un nombre plus petit que le nombre cherché.

Pour voir si ce record de 2004 était encore valide en 2006, je suis allé sur le site « The prime pages » de Chris Caldwell (Université du Tennessee), facile à trouver avec un moteur de recherche. J'y ai ensuite emmené mes élèves à l'aide d'un vidéo-projecteur.

Mon propos n'est pas de dire ici qu'il convient de multiplier ces visites, durant lesquelles les élèves sont seulement spectateurs, mais seulement de raconter une expérience qui m'a semblé intéressante, ainsi qu'aux élèves (un questionnaire anonyme en atteste).

Toutes les pages de ce site sont en anglais ; ça m'a permis, d'une part de dire aux élèves qu'il s'agit de la langue la plus courante pour les sciences (afin de montrer à certains d'entre eux que son étude n'est pas utile seulement à ceux qui veulent se diriger vers le commerce ou le tourisme) et, d'autre part, que les mathématiques en anglais sont tout à fait abordables (il faut aller voir ce site si on n'en est pas convaincu[1]).

Nous avons visité les rares pages de ce site qui sont à leur portée. La plus intéressante est probablement « The largest known prime by year : a brief history » qui divise l'historique en question en deux périodes : « before electronic computers » et « the age of electronic com-

[1] Je suis moi-même très mauvais en anglais et la présence à mes côtés de mon collègue d'anglais m'a rassuré, mais la visite aurait été possible sans lui. Pour les cas graves, il existe sur internet des traducteurs automatiques, très rapides (et parfois si mauvais que c'en est comique !).
Présenter aux élèves ces traducteurs comme des outils intéressants me semble être une mauvaise idée…

puters », la charnière se situant en 1951 : cette année-là, un record de Lucas ($2^{127} - 1$, formé de 39 chiffres), tenant depuis 75 ans, a été battu par un record de 44 chiffres (($2^{148} + 1$) /17) obtenu à l'aide d'un calculateur mécanique, ancêtre de nos ordinateurs, puis presque aussitôt par un autre de 79 chiffres, obtenu cette fois à l'aide d'un calculateur électronique. Cette page n'est vraiment compréhensible que si on sait ce qu'est un nombre de Mersenne (c'est un nombre premier qui est de la forme $2^n - 1$, noté alors $M_n$) dont l'histoire est, elle aussi, intéressante et figure sur une autre page du site.
Le nombre $2^{20996011} - 1$, « connu » des élèves, leur a fourni un repère rassurant ! La page « why do people find these big primes ? » de la Foire Aux Questions donne des réponses à cette inévitable (et saine) question des élèves : en bref, c'est le respect d'une tradition et ce n'est pas plus idiot que de chercher à établir des records sportifs ; un peu plus sérieusement, certaines personnes utilisent ces recherches pour tester du matériel informatique. Il n'y est pas du tout question de cryptographie car dans ce domaine on se contente (actuellement) de nombres premiers comportant « seulement » quelques centaines de chiffres.
Le site de Chris Caldwell comporte de nombreux liens dont deux m'ont semblé intéressants à visiter en compagnie des élèves.

Le premier est une page du site de Dario Alpern (Université de Buenos Aires) consacrée à la spirale d'Ulam.
Pour la petite histoire, Ulam était un ingénieur (très bon ami de Paul Erdös…) qui, s'ennuyant au cours d'une conférence en 1963, s'amusa à écrire les nombres en spirale comme le montre le schéma ci-après.

| | | | | | |
|---|---|---|---|---|---|
| 31 | 30 | 29 | 28 | 27 | 26 |
| 32 | 13 | 12 | 11 | 10 | 25 |
| 33 | 14 | 3 | 2 | 9 | 24 |
| 34 | 15 | 4 | 1 | 8 | 23 |
| 35 | 16 | 5 | 6 | 7 | 22 |
| 36 | 17 | 18 | 19 | 20 | 21 |

Sur le site de Dario Alpern, les nombres premiers de la spirale d'Ulam sont marqués en couleur. On peut constater quelques alignements intrigants qui semblent indiquer « une certaine régularité ». En cliquant plusieurs fois sur la commande (-) on obtient des spirales de plus en plus grandes (jusqu'à 350 000 nombres environ) ; c'est beau comme un ciel étoilé et ça a plutôt tendance à montrer l'infinitude des nombres premiers que leur raréfaction. Il semble que la spirale d'Ulam ait suscité quelques espoirs (pour la connaissance de la répartition des nombres premiers) mais qu'elle ne soit plus qu'une aimable curiosité.

Voir les images page 25

Le deuxième lien visité a été une page d'Otto Forster (Université de Munich) montrant plus clairement la raréfaction des nombres premiers (ce qui était mon but initial).
Chacun des quatre dessins de la page 25 est un tableau de $2^7 = 128$ lignes et 128 colonnes. Chaque tableau contient donc $2^{14}$ cases et permet donc de représenter $2^{15}$ nombres successifs en se limitant aux nombres impairs. La n-ième case est noire si le (2n + 1)-ième nombre représenté est premier. Cette présentation rend particulièrement visibles les nombres premiers jumeaux[2] qui, sauf exception en fin de ligne, sont représentés par deux carrés accolés.

[2] Deux nombres premiers qui ne diffèrent que de 2 sont appelés jumeaux.

## ANNEXE 1 : TEXTE DU DEVOIR DONNÉ AUX ÉLÈVES

**Seconde 2 - Mathématiques - Devoir à la maison à rendre le 22 septembre 2006.**

Il est permis de rendre une seule copie pour deux ou trois élèves. Il est permis de rendre un devoir incomplet.

### La raréfaction des nombres premiers

| Nombre $x$ | 10 | $10^2$ | $10^3$ | $10^4$ | $10^5$ | $10^6$ | $10^7$ |
|---|---|---|---|---|---|---|---|
| Nombre de nombres premiers inférieurs à $x$ | 4 | 25 | 1229 | 1229 | 9592 | 78498 | 664579 |

Vérifier les deux premières colonnes de ce tableau
(punition pour ceux qui bavardent en classe : vérifier aussi la troisième colonne, sans l'aide d'internet).
Calculer le pourcentage (à 0.1 % près) des nombres premiers parmi les 10, puis les 100… premiers nombres et compléter le tableau suivant :

| Nombre $x$ | 10 | $10^2$ | $10^3$ | $10^4$ | $10^5$ | $10^6$ | $10^7$ |
|---|---|---|---|---|---|---|---|
| Pourcentage des nombres premiers parmi les nombres inférieurs à $x$ | 40 % | | | | | | |

*On voit qu'il y en a « de moins en moins ». Se demander s'il y en a une infinité ou bien si « ça s'arrête » est alors une question naturelle. C'est la question suivante.*

### Preuve de l'infinitude des nombres premiers

Il faut bien comprendre ici que la division (euclidienne, c'est-à-dire sans virgule) de a par b donnant un quotient q et un reste r signifie que a = bq + r.
Par exemple, ci-contre, 32 = 6 x 5 + 2.

| a | b |
|---|---|
| r | q |

| 32 | 6 |
|---|---|
| 2 | 5 |

La preuve qu'on va donner est une preuve « par l'absurde » :
on suppose (un instant !) le contraire de ce qu'on voudrait prouver et on démontre qu'on arrive alors à une absurdité ; la preuve est alors terminée !

Supposons (un instant !) qu'on peut compter les nombres premiers et écrire leur liste :
2 ; 3 ; 5…d' ; d. (on appelle d' l'avant-dernier et d le dernier).
Soit N le nombre : produit de tous ces nombres premiers augmenté de 1, c'est à dire que :
N = 2 x 3 x 5… d' x d + 1.
Calculer le reste de la division de N par 2, puis par 3, …puis par d (poser les divisions !).
Qu'obtient-on à chaque fois ?
Que peut-on alors dire de N ?
N est-il dans la liste donnée au départ ? (Pourquoi ?)
Conclure.

### Le plus grand nombre premier connu (en 2003)

Pour un nombre X, on désigne par N(X ) le nombre de ses chiffres, par exemple N(2006) = 4.
Le nombre A = $2^{20996011} - 1$ était le plus grand nombre premier connu en 2003.
On demande ici de trouver une valeur approchée (grossière, c'est à dire imprécise) de ce nombre N ( A ) à l'aide de l'égalité : $2^{10} = 1024$.
En effet on a $2^{10} \approx 10^3$ et donc, par exemple, $2^{400} = (2^{10})^{40} \approx (10^3)^{40} = 10^{120}$…(qui est un nombre comportant ? chiffres et donc N($2^{400}$) …).
Le nombre que vous avez trouvé est-il plus grand ou plus petit que N(A) ? (Pourquoi ?)

**ANNEXE 2 : COMMENTAIRES SUR CE DEVOIR destinés aux enseignants**

### La raréfaction des nombres premiers

J'aurais aimé parvenir au pourcentage 0 % mais la formule, connue sous le terme de théorème de raréfaction des nombres premiers, indiquant que le nombre de nombres premiers inférieurs à $x$ (souvent noté $\pi(x)$) est approximativement, si $x$ est grand, $\frac{x}{\ln x}$, donne la proportion approximative des nombres premiers dans l'intervalle $[1 ; x]$ : $\frac{1}{\ln x}$. Pour obtenir un pourcentage arrondi à 0 %, il faut prendre $x$ vérifiant $\frac{1}{\ln x} < 0.005$, soit $\ln x > 200$ et $x > e^{200}$, ce dernier nombre valant environ $7 \times 2 \times 10^{86}$. Pour avoir des chiffres exacts, avec $x \approx 7 \times 2 \times 10^{86}$ et $\ln x \approx 200$, il faudrait pouvoir connaître $\frac{x}{\ln x} \approx 3 \times 6 \times 10^{84}$ nombres premiers. C'est très lentement que $\ln x$ tend vers l'infini quand $x$ tend vers l'infini. Rien n'empêche cependant d'ajouter dans le devoir une colonne du type : si $x = 10^{87}$, le nombre de premiers inférieurs à $x$ est environ $4 \times 9 \times 10^{84}$. Donner la valeur exacte de $\pi(10^{87})$, quand bien même elle serait connue, n'aurait pas de sens mais l'approximation $\frac{x}{\ln x}$ de $\pi(x)$ est assez bonne (faire des essais pour s'en convaincre !) pour que la valeur approchée $4 \times 9 \times 10^{84}$ soit correcte.

Un autre argument en faveur de cette raréfaction est l'existence de plages « lacunaires » (en termes de nombres premiers) arbitrairement grandes. J'ai été déçu de voir la question suivante résolue (à la maison) par une seule élève : montrer qu'il n'y a aucun nombre premier dans l'intervalle $[1001 ! + 2 ; 1001 ! + 1001]$ qui contient 1000 entiers consécutifs[3].

### Preuve de l'infinitude des nombres premiers

Les élèves savaient que, si N n'est divisible par aucun nombre premier, alors N est premier.

La preuve demandée ici est une preuve par l'absurde, type de raisonnement déroutant pour les élèves ; il convient de commencer par la pratiquer en classe avec des questions simples, par exemple du type : admettant que $\sqrt{2}$ n'est pas rationnel, prouver que $\sqrt{2} + 5$ ne l'est pas (avec $\sqrt{2} + n$ pour n entier quelconque, on obtient ensuite une infinité d'irrationnels et une image moins déformée de la réalité que celle consistant à fournir $\sqrt{2}$ et $\pi$ comme seuls exemples d'irrationnels ; je l'ai fait pendant des années mais ça me paraît maintenant intellectuellement gênant quand on pense que l'ensemble des rationnels est dénombrable).

[3] La formule de Stirling, si $n$ est grand, $n! \approx \sqrt{2\pi n}\,(n/e)^n$ montre que de tels nombres sont inaccessibles et que 1000 ! est de l'ordre de $10^{2570}$.

## ANNEXE 3 : QUELQUES COMPLEMENTS SUR LA SPIRALE D'ULAM

### Ce que l'on peut montrer aux élèves d'une bonne classe

J'avais demandé à mes élèves d'écrire ainsi en spirale les nombres jusqu'à cent et d'y repérer les carrés. On les voit apparaître sur deux « diagonales ».

Les élèves avaient aussi été invités à programmer la fonction suivante sur leur calculatrice et à chercher les f(n) qui sont premiers pour n entier entre 0 et 16.

| n | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| $f(n) = n^2 - n + 17$ | | 17 | 17 | 19 | 23 | 29 | 37 | 47 | 59 |
| | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| | 73 | 89 | 107 | 127 | 149 | 173 | 199 | 227 | 257 |

| | | | | |
|---|---|---|---|---|
| 2 | 2 | 2 | 2 | 2 |
| 2 | 1 | 1 | 1 | 2 |
| 2 | 1 | 0 | 1 | 2 |
| 2 | 1 | 1 | 1 | 2 |
| 2 | 2 | 2 | 2 | 2 |

On désigne par t le le rang du tour autour de 1 dans une spirale d'Ulam (t = 0 étant le nombre 1), voir ci-contre les tours 0, 1 et 2.

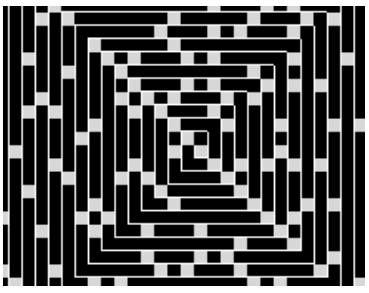
On peut alors montrer que chaque « diagonale » (ce mot désigne ici une demi-droite quelconque de « pente » 1 ou –1, c'est à dire orientée Sud-Ouest / Nord-Est ou bien Sud-Est / Nord-Ouest et d'origine située sur une des deux diagonales principales ou sur une case contiguë à une case d'une de ces diagonales principales) a une « équation » du type $n = 4t^2 + at + b$ où a et b sont des entiers fixés, $a \in \{-4;-2;0;2;4\}$ et b est quelconque ; au sens où le nombre de la diagonale situé dans le t-ième tour est $n = 4t^2 + at + b$ (ce point est détaillé et prouvé dans le dernier paragraphe).

Sur la page de Dario Alpern, lorsqu'on se déplace sur la spirale à l'aide de la souris, ces équations sont actualisées en permanence et on comprend mieux ce qui se passe. On a une petite idée de ce phénomène en considérant les deux diagonales donnant les carrés des entiers ; elles ont pour « équations » :

$n = (2t + 1)^2$, carrés des nombres impairs, et $n = (2t)^2$, carrés des nombres pairs.

Ce phénomène explique la présence des bandes bleues (sans aucun nombre premier) qui sont obtenues quand on clique sur la commande ( )( ), elles correspondent à des expressions $4t^2 + at + b$ factorisées, et il explique aussi certains alignements constatés sur la spirale (voir ce qui suit).

Dans les deux dessins, extraits de la page de Dario Alpern, qui suivent, les nombres premiers sont représentés par des petits carrés plus clairs. Par ailleurs, sur cette page, on peut faire démarrer la spirale du nombre qu'on veut. Les quatre alignements qu'on voyait au départ deviennent plus spectaculaires en partant de 17 ou de 41 :

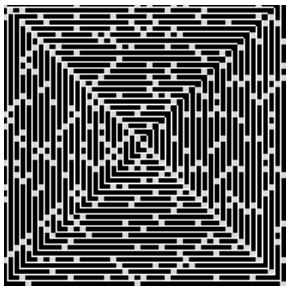


16 points alignés

*Le nombre central est 17. Les diagonales intéressantes ont pour équations :*

$n = 4t^2 + 2t + 17$

*et* $n = 4t^2 - 2t + 17$.



40 points alignés

*Le nombre central est 41. Les diagonales intéressantes ont pour équations :*
$n = 4t^2 + 2t + 41$
*et* $n = 4t^2 - 2t + 41$.

Le plus étonnant est que ces résultats étaient connus d'Euler qui avait remarqué, probablement en cherchant une formule donnant tous les nombres premiers ou tout au moins en donnant beaucoup, que $f(p) = p^2 - p + 17$ est premier si p est entre 0 et 16 (et le même résultat en remplaçant 17 et 16 par 41 et 40).

En remplaçant p par 2t + 1 et par 2t on retrouve les « équations » données dans l'encadré ci-contre.

| n | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $4n^2 + 2n + 17$ | 17 | 23 | 37 | 59 | 89 | 127 | 173 | 227 | 289 | 359 | 437 | 523 | 617 | 719 | 829 | 947 | 1073 |
| $4n^2 - 2n + 17$ | 17 | 19 | 29 | 47 | 73 | 107 | 149 | 199 | 257 | 323 | 397 | 479 | 569 | 667 | 773 | 887 | 1009 |
| $n^2 - n + 17$ | 17 | 17 | 19 | 23 | 29 | 37 | 47 | 59 | 73 | 89 | 107 | 127 | 149 | 173 | 199 | 227 | 257 |

Ce qui précède n'explique rien… : on a rendu plus visible le résultat d'Euler (en alignant les 16 nombres marqués en couleur dans le tableau ci-dessus) mais on ne l'a pas prouvé et on n'a pas non plus compris « d'où il sort » ni comment il l'avait trouvé. **Cette visite n'a été qu'une récréation : on a mis en lumière un phénomène étonnant mais on ne sait pas l'expliquer.**

## Ce qu'on peut montrer au professeur : les équations des demi-droites de la spirale d'Ulam

On distingue :
- les diagonales Nord-Ouest / Sud-Est (de « pente » -1)
- les diagonales Sud-Ouest / Nord-Est (de « pente » 1).

Dans ce qui suit, c est une constante entière quelconque.

Les demi-droites ont une équation du type :
Marque X : $n = 4t^2 + 2t + c$
Marque Y : $n = 4t^2 - 2t + c$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Y | | | | | | * |
| Y | | | Y | | | | * | |
| | Y | | | Y | | * | | |
| | | Y | | | * | | | |
| | | | Y | 1 | X | | | |
| | | | * | | | X | | |
| | | * | | X | | | X | |
| | * | | | | X | | | X |
| * | | | | | | X | | |

Diagonales NO / SE

Diagonales SO / NE

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| * | | | | A | | | | * |
| | * | | A | | | | * | |
| | | * | | | | * | | |
| | | | * | | * | | | B |
| | | | C | 1 | | | B | |
| | | C | | | * | B | | |
| | C | | | | | * | | |
| C | | | | | C | | * | |
| | | | | C | | | | * |

Les demi-droites ont une équation du type
Marque A : $n = 4t^2 - 4t + c$
Marque B : $n = 4t^2 + 4t + c$
Marque C : $n = 4t^2 + c$

On donne par exemple l'équation d'une demi-droite de marque X :
$n = 4t^2 + 2t + c$.
On va montrer que $b = u_p = 4p^2+2p+c$.

Pour passer de a à b, on parcourt d'abord k cases X, puis (2p -1) cases Y, puis (2p+1) cases Z, puis (2p) cases T et k' cases X.
$k + k' = 2p - 2$ donc $b = a + 8p - 2$, c'est-à-dire : $u_p = u_{p-1} + 8p - 2$.
La suite $(u_p)$ démarre à un certain rang r ; $u_r$ est situé sur une diagonale principale ou sur une case contiguë à deux cases de cette diagonale.

En sommant la relation obtenue pour p variant de r + 1 à n on obtient :

$$\sum_{p=r+1}^{p=n} u_p = \sum_{p=r+1}^{p=n} u_{p-1} + 8\sum_{p=r+1}^{p=n} p - 2(n-r),$$

$$\text{soit : } u_n = u_r + 8\frac{(n+r+1)(n-r)}{2} - 2(n-r),$$

$$\text{soit : } u_n = u_r + 4(n^2+n-r) - 2(n-r),$$

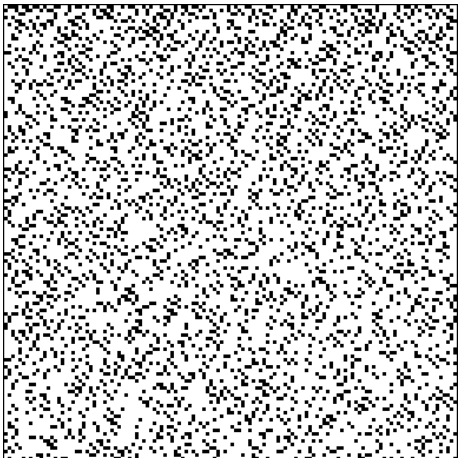
$$\text{soit : } u_n = 4n^2 + 2n + c \text{ en posant } c = u_r - 2r.$$

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | Y | Y | Y | Y | Y | Y | Y | Y | |
| Z | * | | | | | | | | X | |
| Z | | * | | | | | | * | X | |
| Z | | | * | | | | * | | X | |
| Z | | | | * | 3 | 2 | $u_r$ | | X | |
| Z | | | | | 4 | 1 | | | X | |
| Z | | | | * | | * | | | a | |
| Z | | | * | | | | * | | | b |
| Z | | * | | | | | | * | | X |
| Z | * | | | | | | | | * | X |
| Z | T | T | T | T | T | T | T | T | T | T |

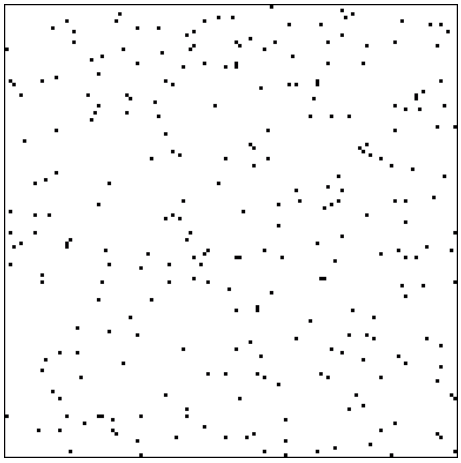
*Ci-dessus on a marqué en « couleur » les cases du p-ème tour. Elles sont situées sur un carré dont le côté comporte (2p + 1) cases. $a = u_{p-1}$ est situé sur le (p-1)-ème tour et $b = u_p$ est situé sur le p-ème tour.*

Il doit y avoir un moyen adroit d'en déduire les quatre autres équations. On peut aussi refaire à chaque fois un calcul du type ci-dessus : on a alors des relations différentes entre a et b suivant qu'on passe de a à b en suivant plutôt le p-ème tour ou le (p -1)-ème tour. Je n'ai pas compris pourquoi il y a trois cas à droite et seulement deux à gauche.

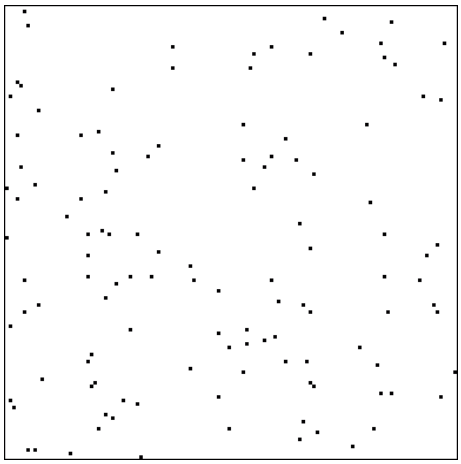
$0 < 2n+1 < 2^{16}$



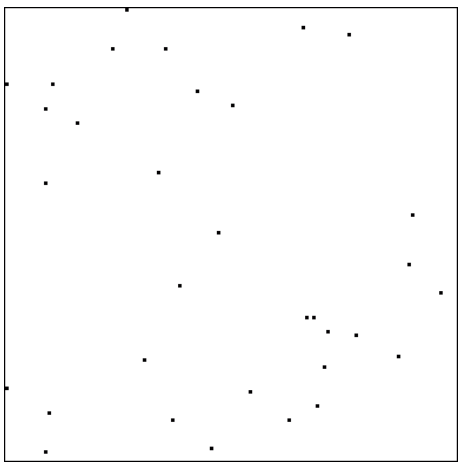
$10^{50} < 2n+1 < 10^{50} + 2^{15}$



$10^{100} < 2n+1 < 10^{100} + 2^{15}$



$10^{400} < 2n+1 < 10^{400} + 2^{15}$



La raréfaction des nombres premiers… comme vous ne l'avez jamais vue !