Les étranges régularités des nombres premiers

Trouver les nombres premiers

Dans ce document on ne considérera que des nombres entiers positifs. Ainsi, on pourra utiliser “entier” pour dire “entier positif”.
Un **nombre premier** est un entier qui a exactement 2 diviseurs : 1 et lui-même. Ainsi, 2, 3, 5, 7 et 11 sont premiers, mais pas 4, 6 ou 9. On remarque que le nombre 1 n’est pas premier vu qu’il n’a qu’un seul diviseur : lui-même.
Les nombres premiers ont été beaucoup étudiés en Grèce antique, même s’ils étaient connus avant.

Érathostène a notamment mis en place une méthode pour les détecter, appelée **crible d’Érathostène** :

- Faire la liste de tous les entiers de 2 à n.
- On commence avec 2.
- On l’entoure et on barre tous ses multiples.
- On prend le plus petit entier non barré et on recommence l’étape précédente.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Exercice 1 : En utilisant le crible d’Érathostène, déterminer tous les nombres premiers inférieurs à 100.

On peut remarquer qu’à partir de 11, plus aucun nombre n’est barré. Nous y reviendrons.

Exercice 2 : À l’aide du tableau, donner des contre-exemples aux propositions suivantes :

1) Tous les nombres premiers sont impairs.
2) Tous les nombres premiers impairs se terminent par 1, 3, 7 ou 9.
3) Il n’y a pas 2 nombres premiers qui sont des entiers consécutifs.

Pour déterminer si un entier n est premier, on peut vérifier qu’il n’a pas de diviseur entre 2 et $n-1$. Si le nombre n est très grand, cela fait beaucoup de vérifications à faire. Pour optimiser, on peut juste vérifier que n n’est pas pair et ensuite diviser uniquement par les nombres impairs.
On dit qu’un entier est **composé** s’il n’est pas premier. Tout nombre composé n peut s’écrire comme le produit de deux entiers a et b, tous deux, strictement compris entre 1 et n. Par conséquent, tout nombre composé n a au moins un diviseur premier qui est inférieur ou égal à $\sqrt{n}$. Ainsi, pour savoir si 101 est premier, il suffit de tester les diviseurs potentiels inférieurs à $\sqrt{101}$.
Quand on cherche les diviseurs d’un nombre, on peut donc s’arrêter à sa racine carrée. Pour déterminer si un nombre n est premier, on peut donc utiliser la méthode suivante :

- On vérifie qu’il n’est pas pair.
- On vérifie qu’il n’est divisible par aucun nombre impair compris entre 3 et $\sqrt{n}$.

Si on a la liste des nombres premiers inférieurs à $\sqrt{n}$, on peut essayer de diviser par ces nombres au lieu de le faire avec tous les nombres impairs.

Exercice 3 : Déterminer si les nombres suivants sont premiers ou non.

1) 101 2) 129 3) 2023 4) 9973

C'est pas bientôt fini ?

Quand on regarde le crible d'Érathostène, on peut se dire qu'à partir d'un certain seuil, tous les nombres seront barrés et qu'il ne restera plus de nombres premiers à découvrir. Ce n'est pas le cas. En effet, il y a une infinité de nombres premiers et Euclide l'a démontré il y a 2300 ans. Pour comprendre sa démonstration, il faut utiliser la propriété suivante :

Si un nombre n divise a et $a+b$, alors n divise b.

Exercice 4 : Compléter la démonstration de cette propriété.
Si n est un diviseur de a, alors il existe un entier k_1 tel que $a = \ldots$.
De même, si n est un diviseur de $a+b$, alors il existe un entier k_2 tel que $a+b = \ldots$.
Donc $b = (a+b) - a =$ .... Donc ....

Attention, ce n'est pas parce que n divise $a+b$, qu'il divise a et b.

Exercice 5 : Donner un contre exemple à l'énoncé précédent.

Exercice 6 : Faisons une preuve par l'absurde du Théorème d'Euclide. Supposons qu'il y a un nombre fini de nombres premiers, notés $p_1, p_2, \ldots, p_k$. Aucun autre nombre ne peut être premier.
On note $\mathrm{N} = p_1 \times p_2 \times \cdots \times p_k + 1$.

1) Expliquer pourquoi il existe au moins un nombre premier p_i qui divise N.
2) En déduire que p_i doit diviser 1.
3) Expliquer pourquoi c'est une absurdité et conclure.

Attention, cette construction ne permet pas d'obtenir des nombres premiers arbitrairement grands. Ajouter 1 au produit des k premiers nombres premiers ne donne pas toujours un nombre premiers. En effet, il peut y avoir d'autres nombres premiers entre le dernier utilisé dans le produit et la racine carrée du nombre obtenu.

Chaos ou régularité

Il y a donc une infinité de nombres premiers. Mais comment sont-ils répartis ?
En regardant dans le tableau on peut remarquer qu'initialement, les nombres premiers sont assez rapprochés. On dit que deux nombres premiers p et $p' = p+2$ sont jumeaux. C'est le cas de 3 et 5 ou de 11 et 13.

Exercice 7 : Déterminer toutes les paires de nombres premiers jumeaux inférieurs à 100.

Plus on se rapproche de 100, moins il y a de premiers jumeaux. Pourtant, la **conjecture des nombres premiers jumeaux** suppose qu'il y a un nombre infini de nombres premiers jumeaux. Cela veut dire que pour tout entier n, aussi grand soit-il, il y a une infinité de nombres premiers jumeaux supérieurs à n.
Les paires de nombres premiers de la forme $(p;p+4)$ sont dit **cousins** et ceux de la forme $(p;p+6)$ sont **sexy**. La **conjecture de Polignac** suppose qu'il existe une infinité de paires de nombres premiers $(p;p+n)$ pour tout n pair. Aucune de ces deux conjectures n'a été démontrée.
Un résultat de 2014, de Yitang Zhang, montre qu'il existe un entier $\mathrm{N} < 7 \times 10^7$ tel qu'il y a une infinité de paires de nombres premiers de la forme $(p;p+\mathrm{N})$.
À l'inverse de ces résultats, qui montrent que même sur les nombres extrêmement grands, il y a des nombres premiers très proches les uns des autres, il peut y avoir un grand écart entre deux nombres premiers consécutifs. On appelle **factorielle de** n, ou n **factorielle**, le produit de tous les entiers de 1 à n. Ainsi : $n! = 1 \times 2 \times 3 \times \cdots \times n$.

Exercice 8 : On considère le nombre $N = 100!$.

1) Expliquer pourquoi $N+2$ et $N+3$ ne peuvent pas être premiers.
2) Combien d'entiers consécutifs, à partir de $N+2$, ne peuvent pas être premiers ?
3) Donner une façon de trouver un intervalle de k nombres consécutifs qui ne sont pas premiers.

Il y a donc de très grands écarts entre 2 nombres premiers consécutifs, mais aussi de très petits écarts, même lorsqu'on considère des nombres infiniment grands.
Peut-on en déduire que la répartition des nombres premiers est totalement chaotique ? Pas vraiment.
À la fin du 18^{e} siècle, Gauss, alors qu'il n'avait que 15 ou 16 ans, et Legendre ont tous les deux conjecturé de façon indépendante le **théorème des nombres premiers** qui n'a été démontré que 100 ans plus tard : pour tout entier n, le nombre de nombres premiers inférieurs à n est environ $\dfrac{n}{\ln n}$, où $\ln n$ est le **logarithme népérien**. Cette approximation devient plus précise lorsque n devient très grand. Il faut la considérer comme un ordre de grandeur.

Exercice 9 :

1) Calculer le nombre de nombres premiers devant être inférieurs à 100 d'après cette formule. Comparer ce résultat avec la réalité.
2) Calculer le nombre de nombres premiers devant être inférieurs à 1 000 000 d'après cette formule.
3) Calculer le nombre de nombres premiers devant être inférieurs à 1 000 000 000 d'après cette formule.

Il y a deux corollaires à ce théorème :

- L'écart moyen entre tous les nombres premiers inférieurs à n est d'environ $\ln n$.
- Le n-ième nombre premier est environ $n \times \ln n$.

Pour l'écart moyen, cette valeur n'est pas forcément très précise puisque, comme nous l'avons vu, l'écart entre deux nombres premiers peut être très variable. Ces résultats donnent au moins une idée de la densité des nombres premiers parmi les entiers.

Exercice 10 :

1) Calculer l'écart moyen entre les nombres premiers inférieurs à n, avec :
   a) $n = 1000$ b) $n = 1\,000\,000$ c) $n = 1\,000\,000\,000$
2) Calculer une valeur approchée du n-ième nombre premier avec :
   a) $n = 1000$ b) $n = 1\,000\,000$ c) $n = 1\,000\,000\,000$

On connait, depuis, des formules plus précises. Par exemple, le n-ième nombre premier est environ égal à $n(\ln(n) + \ln(\ln n) - 1)$.
Le **Théorème de Tchébycheff** (1850) dit également que pour tout entier $n > 2$, il y a au moins un nombre premier entre n et $2n$.
On peut aussi observer une forme de régularité si on se concentre sur le dernier chiffre des nombres premiers. Si on met de côté 2 et 5, tous les nombres premiers se terminent par 1, 3, 7 ou 9. La proportion de nombres premiers se terminant par chacun de ces chiffres est d'environ 25 %. Ils sont donc relativement équitablement distribués.
Par contre, étant donné un nombre premier, les probabilités que le chiffre des unités du prochain soit 1, 3, 7 ou 9 ne sont pas les mêmes. En effet, la probabilité que le nombre premier suivant ait le même chiffre des unités est inférieure à 25 %. La probabilité de chacun des autres chiffres est, au contraire, supérieure à 25 %. Par exemple, si un nombre premier se termine par 1, le nombre premier suivant a moins de chances de se terminer par 1 que par 3, par 7 ou par 9. Ces résultats récents (2016) n'ont pas été démontrés mais observés sur 400 milliards de nombres premiers.

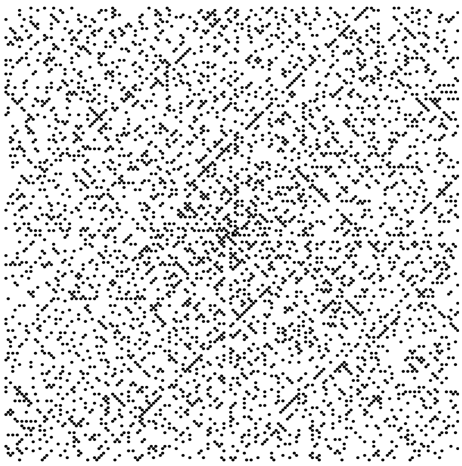
La spirale d'Ulam

Alors qu'il était forcé d'assister à un exposé très long qui ne le passionnait pas vraiment, le mathématicien Stanislaw Ulam s'est mis à gribouiller sur une feuille de papier. Il a mis un 1 au centre et a ensuite écrit les entiers suivants en tournant dans le sens inverse des aiguilles d'une montre. Il a ensuite entouré les nombres premiers. On appelle cela une **spirale d'Ulam**.

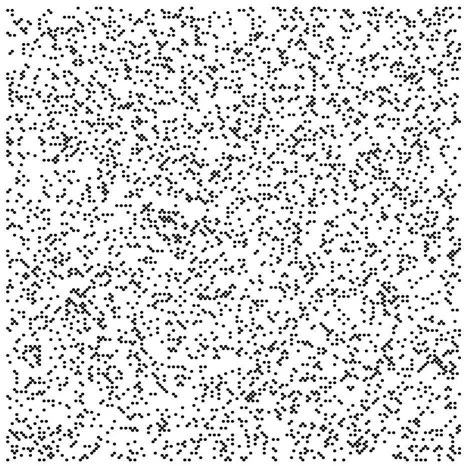
100	99	98	97	96	95	94	93	92	91
65	64	63	62	61	60	59	58	57	90
66	37	36	35	34	33	32	31	56	89
67	38	17	16	15	14	13	30	55	88
68	39	18	5	4	3	12	29	54	87
69	40	19	6	1	2	11	28	53	86
70	41	20	7	8	9	10	27	52	85
71	42	21	22	23	24	25	26	51	84
72	43	44	45	46	47	48	49	50	83
73	74	75	76	77	78	79	80	81	82

Exercice 11 : Entourer les nombres premiers dans la spirale ci-contre.

On peut remarquer que les nombres premiers semblent dessiner des segments en diagonale. En effet, dans la grille, les nombres alternent entre pair et impair, comme les cases blanches et noires sur un échiquier.
Les nombres premiers, à part 2, étant tous impairs, il est normal de retrouver ces regroupements sur les diagonales. Mais cela ne suffit pas à expliquer ces formes. On peut comparer la spirale d'Ulam formée des 40 000 premiers nombres, avec les nombres premiers marqués par un point, et une autre grille où des nombres impairs ont été marqués au hasard, avec la même densité.



Spirale d'Ulam jusqu'à 40 000



Nombres impairs aléatoires

On peut noter que les alignements en diagonale sont plus marqués dans la spirale d'Ulam que dans la grille aléatoire.
On peut obtenir les valeurs alignées sur une demi-droite en diagonale à l'aide de formules quadratiques de la forme $4n^2 + 2bn + c$, pour tout $n \in \mathbb{N}$, avec b et c des entiers naturels.

Exercice 12 : Identifier les demi-droites déterminées par ces formules en calculant les premières valeurs.

1) $4n^2 + 2n + 1$ 2) $4n^2 + 4n + 2$ 3) $4n^2 + 6n + 3$ 4) $4n^2 + 8n + 4$

La valeur de b définit la direction et le sens, alors que c permet de définir la valeur de départ. Par contre, il se peut que les premières valeurs ne soient pas alignées.

Exercice 13 : Déterminer à partir de quelle valeur de n la formule $4n^2 + 2n + 5$ génère une demi-droite.

On remarque que dans les 4 formules de base, c vaut 1, 2, 3 ou 4. Ce sont les 4 premières valeurs de la spirale. Si on commence la spirale par c au lieu de 1, les valeurs suivantes sont $c+1$, $c+2$ et $c+3$. Les formules $4n^2+2n+c$, $4n^2+4n+c+1$, $4n^2+6n+c+2$ et $4n^2+8n+c+3$ permettent d'obtenir les valeurs sur les 4 demi-droites partant du centre de cette nouvelle spirale.

Exercice 14 :

1) Dessiner les premières valeurs de la spirale d'Ulam en mettant 41 au centre.
2) Déterminer les formules donnant les 4 demi-droites partant de 41, 42, 43 et 44.
3) Vérifier que les premières valeurs générées par ces formules sont bien alignées dans votre spirale.

En fait, la formule n^2+n+c permet même de générer toutes les valeurs de la diagonale allant du coin bas gauche au coin haut droite dans la spirale dont la valeur centrale est c.

Exercice 15 : On considère la formule n^2+n+41.

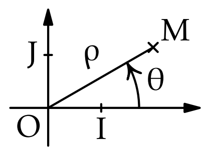
1) Cette formule célèbre a été découverte par Euler.
   a) Calculer les valeurs de n^2+n+41 inférieure à 100.
   b) Qu'est-ce qui rend cette formule si spéciale ?
2) Sur la spirale commençant en 41, les valeurs correspondent aux deux demi-droites partant de 41 et de 43. Une des demi-droites est générée par les valeurs paires de n et l'autre par les valeurs impaires.
   a) En prenant $n=2k$, retrouver la formule permettant de générer les valeurs d'une des demi-droites.
   b) En prenant $n=2k+1$, retrouver la formule permettant de générer les valeurs de l'autre demi-droite.

Cette formule n'est pas miraculeuse et ne donne pas que des nombres premiers, même s'il faut un n assez grand pour trouver un contre-exemple.
La spirale d'Ulam permet ainsi de visualiser les nombres premiers générés par cette formule.
Les autres points alignés qui apparaîssent dans la spirale peuvent aussi être obtenus en utilisant d'autres formules, comme $4n^2+2n+59$ ou n^2+n+17.

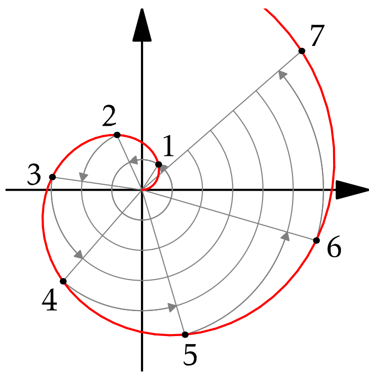
La spirale d'Archimède

La spirale d'Ulam n'est pas la seule façon de placer les entiers naturels sous la forme d'une spirale. On peut aussi, entre autres, faire une **spirale d'Archimède** en utilisant les **coordonnées polaires**.

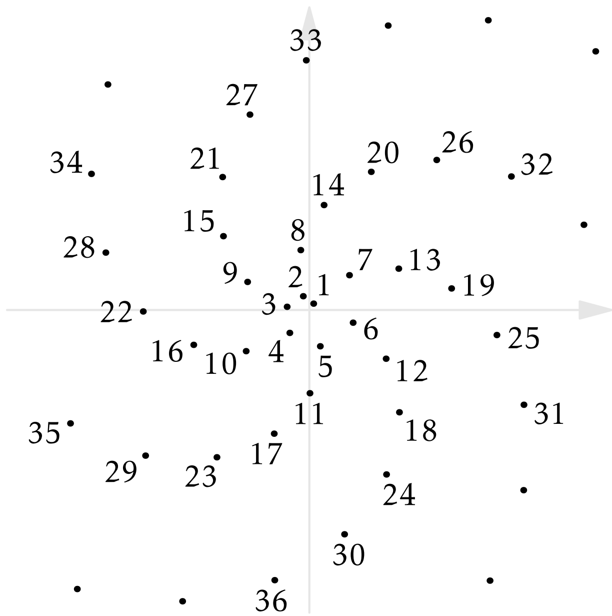
En général, on associe à un point du plan ses coordonnées cartésienne $(x;y)$. Mais on peut aussi définir un point M dans un repère orthonormé (O; I,J) à l'aide de la distance $\rho = \text{OM}$ et de l'angle orienté $\theta = \widehat{\text{IOM}}$ mesuré en radians. Les coordonnées polaires du point M sont alors $(\rho;\theta)$.



Pour faire une spirale d'Archimède en coordonnées polaires, on associe à chaque entier naturel n le point de coordonnées polaires $(n;n)$. C'est-à-dire qu'on place le point à la distance n de l'origine du repère et on tourne de n radians dans le sens inverse des aiguilles d'une montre en partant de l'axe des abscisses. En reliant les points avec des courbes, on dessine une spirale.



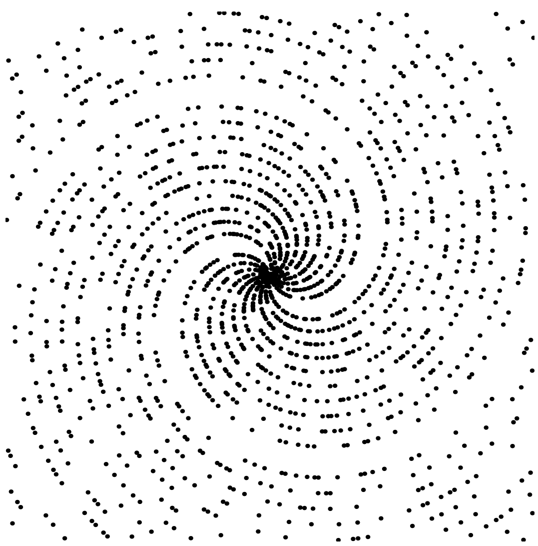
On peut voir sur la figure ci-contre se former 6 spirales dont seules deux contiennent des nombres premiers, à l'exception de 2 et de 3. Il y a 6 spirales parce que l'angle 6 radians est proche de 2π, donc d'un tour complet. L'angle 12 radians fait presque un tour de plus que 6 radians, et ainsi de suite. Une des spirales est formée par les nombres 6, 12, 18, 24… Ce sont des multiples de 6. La spirale suivante est formée par les nombres 1, 7, 13, 19… Si on fait une division euclidienne de ces nombres par 6, le reste est toujours 1. On dit que deux nombres a et b sont **congrus modulo** n s'ils ont le même reste dans la division euclidienne par n. Les nombres de chaque spirale sont tous congrus modulo 6.



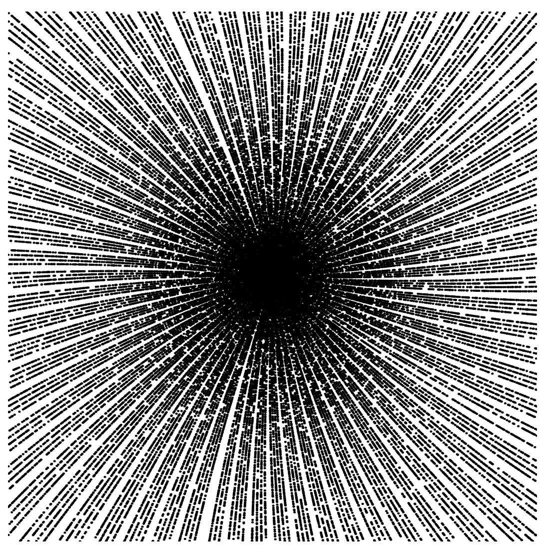
Exercice 16 :

1) Entourer les points correspondant à des nombres premiers sur la figure ci-dessus.
2) Expliquer pourquoi il y a 6 restes possibles dans la division euclidienne par 6.
3) Les nombres congrus à r modulo 6, avec $r < 6$, peuvent se noter $6k + r$, avec $k \in \mathbb{N}$.
   a) Expliquer pourquoi les nombres correspondant à $6k$ ne peuvent pas être premiers.
   b) Expliquer pourquoi les nombres correspondant à $6k+3$ ne peuvent pas être premiers, à l'exception de 3.
   c) En procédant de la même manière, déterminer les formules ne permettant pas d'obtenir plus d'un nombre premier et celles qui peuvent, au contraire, générer un nombre infini de nombres premiers.
4) On dit que deux nombres sont **premiers entre eux** si 1 est leur seul diviseur commun.
   a) Déterminer les entiers naturels $r < 6$ qui sont premiers avec 6.
   b) Que remarquez vous ?

En fait, il n'y a pas que le nombre 6 qui génère des spirales, dont certaines contiennent un nombre infini des nombres premiers. Voici deux autres exemples, à des échelles différentes, en ne gardant que les nombres premiers. Par contre, pour identifier les nombres générant ces spirales, il vaut mieux utiliser un ordinateur…



Jusqu'à $n \approx 16\,500$



Jusqu'à $n \approx 1\,000\,000$