

des répunits, mais, là encore, on attend une démonstration complète. En regroupant cette conjecture et celle sur les répunits en base 10, on conjecture donc tout simplement qu'il n'existe qu'un nombre fini de nombres premiers permutables et que ce sont les vingt-deux jusqu'à 991 et les dix répunits supérieurs à 991 connus.

DANS LES AUTRES BASES

La notion de nombre premier permutable est liée à la base de numération décimale et peut donc être envisagée dans d'autres bases. Convenons de nommer «nombres premiers b -permutables» les nombres premiers qui, quand on permute les chiffres de leur écriture en base b , restent premiers.

Une petite exploration numérique avec un ordinateur nous donne des débuts de listes pour ces nombres b -permutables.

Pour la base 2, en calculant par exemple jusqu'à 10000, on trouve quatre nombres premiers 2-permutables :

- 3, dont l'écriture en base 2 est 11_2 , (l'indice derrière un nombre précise la base dans laquelle on l'écrit quand ce n'est pas la base 10)

- $7 = 111_2$
- $31 = 11111_2$
- $127 = 1111111_2$
- $8191 = 1111111111111_2$

La situation est plus simple que pour la base 10: en base 2, les nombres trouvés sont tous, sans exception, des répunits. On formule donc la conjecture que tous les nombres premiers 2-permutables sont des répunits pour la base 2. La conjecture se démontre facilement: s'il y a un chiffre autre que 1 dans un nombre écrit en base 2, c'est un 0, donc en permutant les chiffres de ce nombre, ce 0 peut être mis à la fin, ce qui donne un nombre pair... qui n'est pas premier.

Les nombres premiers 2-permutables sont donc des répunits en base 2. Un répunit en base 2 qui s'écrit avec n fois le 1 vaut $2^n - 1$. Les nombres premiers de cette forme sont très recherchés et portent le nom de «nombres premiers de Mersenne» en l'honneur de Marin Mersenne (1588-1648), un moine savant de l'ordre des Minimes qui aurait énoncé que si $2^n - 1$ est premier, alors n est premier. Le plus grand nombre premier connu est un nombre premier de Mersenne; il s'écrit en base 2 avec 82589933 fois le 1 et, quand on l'écrit en base 10, il comporte 24862048 chiffres. Il a été découvert en décembre 2018 par Patrick Laroche en utilisant un programme du projet GIMPS (Great Internet Mersenne Prime Search, <https://www.mersenne.org>).

Au total, on connaît aujourd'hui 51 nombres premiers de Mersenne, qui sont donc aussi les

2

LES NOMBRES PREMIERS ET LE CALCUL

Un nombre est premier s'il a exactement deux diviseurs, 1 et lui-même. Les plus petits nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

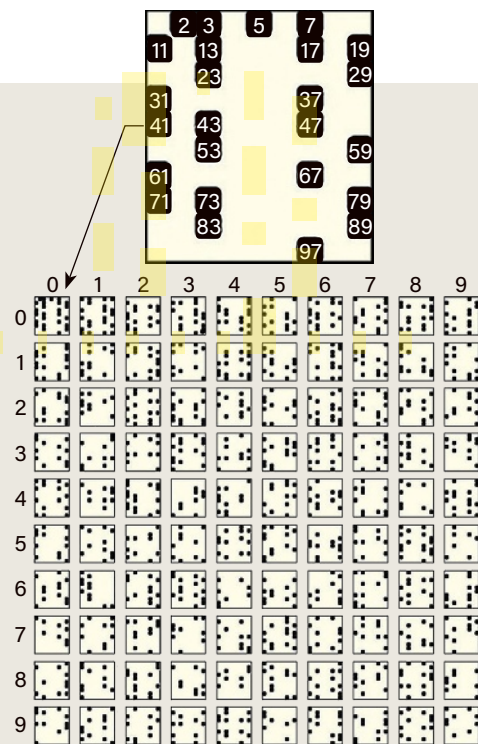
Le tableau à droite représente les nombres premiers jusqu'à 10 000. Chaque carré représente 100 entiers en 10 lignes de 9 petits carrés (les multiples de 10 ne sont pas représentés). Les nombres premiers sont dans une petite case noire. En examinant par exemple le carré de la ligne 9 et de la colonne 5, on voit qu'il y a sept nombres premiers entre 9 500 et 9 599, qui sont 9 511, 9 521, 9 533, 9 539, 9 547, 9 551 et 9 587.

On constate sur ce graphique que la densité des nombres premiers décroît lentement. Le théorème d'Hadarnard et de la Vallée Poussin de 1896 indique que la densité des nombres premiers autour de n est d'environ $1/\log(n)$.

Autour de 10 000, cette densité est donc $1/\log(10\,000) \approx 1/9,21$, ce qui

est compatible avec le fait qu'on trouve 9 nombres premiers dans la dernière centaine avant 10 000 de notre tableau et un peu plus dans la centaine précédente.

Les nombres premiers sont étudiés depuis l'Antiquité. Euclide savait démontrer qu'il y en a une infinité. Parmi les mathématiciens qui s'y sont intéressés, citons Ératosthène, Marin Mersenne, Pierre de Fermat, Leonhard Euler, Carl Friedrich Gauss, etc. On connaît des algorithmes rapides pour tester la primalité d'un nombre, y compris quand il comporte plusieurs milliers de chiffres. En revanche, pour décomposer un entier en facteurs premiers, les seuls algorithmes rapides qu'on connaît sont quantiques et sont donc inutilisables aujourd'hui faute d'ordinateurs quantiques de puissance suffisante. Personne ne sait aujourd'hui factoriser n'importe quel nombre de 300 chiffres décimaux.



3

RAISONNEMENTS HEURISTIQUES

Les raisonnements heuristiques utilisés en théorie des nombres déterminent des propriétés presque certaines concernant les entiers ou les familles d'entiers. La densité des nombres premiers étant $1/\log(n)$ pour les nombres autour de n , on en déduit que la densité des nombres premiers jumeaux (nombres premiers séparés de deux unités, comme 11-13, 17-19, 821-823) autour de n est, en ordre de grandeur, probablement $1/(\log(n))^2$. L'argument heuristique est : « La probabilité que p et que $p + 2$ soient simultanément premiers est le produit de la probabilité que p soit premier par celle que $p + 2$ le soit, donc le $1/\log(n)$ du théorème des nombres premiers fournit un $1/(\log(n))^2$. »

Bien sûr, l'argument n'est pas totalement satisfaisant, puisque même si la densité des nombres premiers est un résultat sûr, le fait pour un entier d'être premier ne résulte pas d'un tirage aléatoire : il est donc abusif de parler de probabilité. De plus, les événements concernant la primalité de p et de $p + 2$ ne sont pas indépendants, ce qui serait nécessaire pour multiplier les probabilités.

Le raisonnement heuristique donne une affirmation probable, mais qui ne peut être considérée comme rigoureusement prouvée.

Pour les nombres premiers permutablement, on peut mener le raisonnement heuristique suivant. La « probabilité » pour qu'un entier p formé de n chiffres décimaux soit premier ainsi que les $n!$ nombres qu'on obtient en permutant ses chiffres est, en ordre de grandeur, $(1/\log(p))^{n!}$. Puisqu'il y a environ 10^n nombres de n chiffres et que leur taille est environ 10^{n-1} , le nombre d'entiers premiers permutablement à n chiffres sera environ $10^n / (\log(10^{n-1}))^{n!}$.

Le calcul donne 18,9 pour $n = 2$, $1/10$ pour $n = 3$, 7×10^{-17} pour $n = 4$ et 2×10^{-111} pour $n = 5$. Ces évaluations sont grossièrement compatibles avec ce que l'on sait des nombres permutablement trouvés, mais surtout, la décroissance de l'évaluation heuristique est tellement rapide, quand n augmente, que le calcul appuie la conjecture qu'il n'y a qu'un nombre fini de nombres premiers permutablement. Pour les nombres premiers circulaires, un raisonnement du même type appuie aussi la conjecture qu'il n'y en a qu'un nombre fini.



51 nombres premiers 2-permutablement connus. On ignore s'il en existe une infinité, mais cette fois on conjecture plutôt que oui.

Pour la base 3, en calculant jusqu'à 50000, les nombres premiers 3-permutablement sont : $2=2_3$, $5=12_3$, $7=21_3$, $13=111_3$, $1093=111111_3$. Mis à part 2, 5 et 7, ce sont tous des répunits de la base 3. En base 4, les nombres premiers 4-permutablement sont, jusqu'à 50000 : $2=2_4$, $3=3_4$, $5=11_4$, $7=13_4$, $13=31_4$, $23=113_4$, $29=131_4$, $53=311_4$.

Pour la base 5, en calculant jusqu'à 50000, on a : $2=2_5$, $3=3_5$, $7=12_5$, $11=21_5$, $13=23_5$,

$17=32_5$, $19=34_5$, $23=43_5$, $31=111_5$, $1249=14444_5$, $2749=41444_5$, $3049=44144_5$, $3109=44414_5$, $3121=44441_5$, $19531=111111_5$.

D'autres listes de nombres premiers b -permutablement sont à la portée de votre ordinateur ou données sur Wikipédia, le tout conduisant à la conjecture générale : dans toute base b supérieure ou égale à 2, à l'exception du début de leur liste, les nombres premiers b -permutablement sont les répunits premiers de la base b .

Envisager toutes les permutations est très exigeant et cela a eu pour conséquence que nous