Les nombres premiers jusqu'à 1000000

Steven Pigeon Professeur Département de mathématiques, informatique et génie UQAR



Les nombres premiers, jusqu'à 1000000

par

Steven Pigeon, professeur

Département de mathématiques, informatique et génie \mathbf{UQAR}

Steven Pigeon
Département de mathématiques, informatique, et génie
Université du Québec à Rimouski
Rimouski, Québec
G5L 3A1
steven_pigeon@uqar.ca

Le document a été typographié par l'auteur avec la police libre URW-Garamond par Mathdesign et le système LATEX. Les illustrations, sauf indications contraires, sont de la main de l'auteur. Les autres illustrations sont libres de droits ou utilisées selon les dispositions de l'article 29 de la loi sur le droit d'auteur.

V 0.9 Mars 2022

005.7xxxs QA76.xx 2022 ISBN 978-0-0000-0000-2

© 2022 Steven Pigeon

Tous droits de traduction totale ou partielle réservés pour tous les pays. La reproduction d'un extrait quelconque de ce livre, sauf selon les dispositions prévue par la loi, par quelque procédé que ce soit, tant électronique que mécanique, en particulier par photocopie, est interdite sans l'autorisation écrite de l'auteur.

Chapitre 1

Comment lire la table?

Les nombres premiers n'ont comme facteurs qu'un et eux-mêmes. Sauf pour deux, qui est le seul nombre premier pair, tous les nombres premiers sont impairs. Une table qui listerait les nombres premiers pourrait alors ne contenir que les nombres impairs, marquant les nombres premiers avec et les autres avec , avec un « taux de compression » de 2, puisque nous listons deux fois moins de nombres. Cependant, dans cette liste, beaucoup seraient encore des nombres composés — c'est-à-dire avec des diviseurs autres que un et eux-mêmes. Nous pourrions de plus éliminer les nombres qui sont des multiples de trois, car, sauf pour trois, aucun nombre premier n'est un multiple de trois. Puis éliminer les multiples de cinq, de sept, etc.

Si nous éliminons tous les multiples de deux et de trois, nous cherchons des nombres tels que $pgcd(x, 2 \cdot 3) = pgcd(x, 6) = 1$, c'est-à-dire relativement premiers à 6. Cela ne nous laisse que des nombres potentiellement premiers de la forme $6j \pm 1$. Certes :

- Les nombres de la forme 6j sont divisibles par 2 et 3, ils ne peuvent donc pas être premiers;
- Les nombres de la forme 6j + 1 laissent un reste de 1 lorsqu'ils sont divisés par 2 ou 3, ils *pour-raient* être premiers;
- Les nombres de la forme 6j + 2 sont divisibles par 2;
- Les nombres de la forme 6j + 3 sont divisibles par 3;
- Les nombres de la forme 6j + 4 sont divisibles par 2;
- Les nombres de la forme 6j + 5 laissent un reste de 1 lorsqu'ils sont divisés par 2 et un reste de 2 lorsqu'ils sont divisés par 3, ils *pourraient* être premiers.

Cela nous laisse les nombres de la forme 6j + 1 ou 6j + 5; ou, de façon équivalente, de la forme $6j \pm 1$. Une table basée sur les diviseurs 2 et 3 pourrait n'avoir que des nombres de la forme $6j \pm 1$, en marquant \square ou \square ces positions, selon que les nombres soient premiers ou non. Mais en

n'utilisant que 2 et 3, nous obtenons un « taux de compression » de 3, puisque de tous les groupes de six nombres nous n'en retenons que deux.

On peut faire un peu mieux en incluant un troisième diviseur, 5. Nous cherchons alors des nombres tels que $pgcd(x, 2 \cdot 3 \cdot 5) = pgcd(x, 30) = 1$, c'est-à-dire relativement premiers à 2, 3 et 5. Avec le même type de raisonnement que pour $6j \pm 1$, nous trouvons que cela nous laisse avec les nombres de la forme $30j \pm 1$, $30j \pm 7$, $30j \pm 11$, ou $30j \pm 13$, c'est-à-dire, de façon équivalente, de la forme 30j + 1, 30j + 7, 30j + 11, 30j + 13, 30j + 17, 30j + 19, 30j + 23, ou 30j + 29.

La table qui suit inclut les colonnes pour 30j + 1, +7, +11, +13, +17, +19, +23, et +29. Le « taux de compression » est un peu plus intéressant, car nous ne conservons que 8 nombres sur 30, c'est un taux près de 4 (3.75, en fait). Ainsi, la colonne de gauche indique un nombre multiple de 30, par exemple 6030. Les 8 cases qui suivent représentent l'un des cas, +1,..., +29. Ainsi, la 6e case correspond à 6030 + 19 = 6049, qui n'est pas premier, marqué \square . Juste à coté, la 7e case, qui correspond à 6030 + 23 = 6053 est marquée d'un \square , puisque 6053 est premier.

* *

L'idée de faire une table pour $30j \pm 1,\pm 7,\ldots$ est venue après un gazouilli de Vincent Pantal du premier janvier $2022^{\,1}$, lui-même une réponse à un autre gazouilli 2 qui présentait une table semblable, mais sans élagage. Vincent proposait une table pour la forme $6j \pm 1$. Comme les $6j \pm 1$ incluent encore les multiples de 5 (puisque 24+1=25 et 36-1=35), cela me paraissait moins efficace que ç'aurait pu l'être. J'ai donc proposé d'utiliser les $30j \pm 1, \pm 7,\ldots$ dans une organisation un peu différente, et potentiellement plus compacte, si on dispose d'une façon d'entasser quatre points dans un quadrat 3 . Vincent propose une autre organisation 4 . Le 2 janvier, l'idée était finalisée. Un peu de temps libre, un programme C++, deux-trois scripts Bash, et voici le résultat.

^{1.} Tweet de départ de Vincent Pantal.

^{2.} Tweet d'Alex Freuman.

^{3.} Mon Tweet des quadrats.

^{4.} Tweet de Vincent sur la table organisée en rangées.

Chapitre 2

Nombres premiers

La table commence à 30, et donc omet les nombres premiers 2, 3, 5 (qui sont d'office exclus de la table, puisque ce sont nos diviseurs), mais aussi 7, 11, 13, 17, 19, 23 et 29. Il ne faudra pas les oublier.















































































































































































































































































































































