La factorisation des grands nombres

Laboratoire de Mathématiques

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Université Blaise Pascal

Votre calculatrice est en panne. Sachant que

$$33\,398\,630\,137 \times 73 = 2\,438\,100\,000\,001,$$

pouvez-vous avec votre seul crayon trouver une factorisation de 33 398 630 137 ?

Les nombres de Fermat....

Les nombres de la forme

$$F_n = 2^{2^n} + 1,\ n = 0, 1, 2, 3, \ldots$$

s'appellent les **nombres de Fermat**. Cet illustre mathématicien **(1601-1665)** pensait que ces nombres étaient tous des nombres premiers. Est-ce vrai ?

... sont-il des nombres premiers ?

Cela commence plutôt bien :

$F_0 = 2^1 + 1 = 3$ est premier, $F_1 = 2^2 + 1 = 5$ est premier,
$F_2 = 2^4 + 1 = 17$ est premier, $F_3 = 2^8 + 1 = 257$ est premier,
mais que dire de $F_4 = 2^{16} + 1 = 65\,537$?....

Votre calculatrice est toujours en panne et 65 537 n'est pas un nombre si gros. On doit pouvoir décider "à la main" si celui-ci est premier.... *Avec un peu de patience et à l'aide de votre crayon, vous constatez que* **65 537 ne possède pas de diviseurs premiers inférieurs à $256 \simeq \sqrt{65\,537}$**. *Cette information vous permet-elle d'en déduire que* 65 537 *est un nombre premier ?*

De Pierre de Fermat...

Les cinq nombres F_0, F_1, F_2, F_3 et F_4 sont donc premiers, ce que Fermat avait bien sûr observé.

Les choses se gâtent avec

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297,$$

nombre de 10 chiffres pour lequel Fermat était incapable de décider s'il était premier ou pas. Il lui aurait fallu pour cela une table de nombres premiers inférieurs à 100 000, ce qui était impensable à l'époque.

... à Leonhard Euler

Au prix d'une virtuosité époustouflante, **Euler (1707-1783)** parvint à trouver un diviseur premier de F_5. Il s'agit d'un merveilleux tour de force pour un calcul à la main. Même en connaissant ce diviseur premier, il n'est pas si aisé de comprendre comment Euler a pu le trouver.

Le diviseur de $F_5 = 2^{32} + 1$ trouvé par Euler est 641.

Sans utiliser la valeur F_5, seriez-vous capable de retrouver comment Euler a pu montrer que 641 divise $2^{32} + 1$?

Une indication est sans doute nécessaire, la voici :

$$641 = 2^4 + 5^4 \text{ et } 640 = 2^7 \times 5.$$

Bon courage et surtout pas trop de calculs !

Les ordinateurs au secours de la factorisation

Malgré l'apparition de puissants ordinateurs, très peu de choses sont connues sur l'arithmétique des nombres de Fermat.

La factorisation de

$$F_9 = 2^{512} + 1$$

est un véritable exploit. Ce nombre possède 155 chiffres. Par chance, il possède un "petit" facteur premier de 7 chiffres, ce qui a facilité le début de la factorisation. Le plus dur restait évidemment à faire car diviser un nombre de 155 chiffres par un nombre de 7 chiffres conduit à un nombre ayant environ 148 chiffres...

La décomposition en facteurs premiers de $F_9 = 2^{512} + 1$ est

$$F_9 = 2^{512} + 1 = p \times q \times r$$

avec

$p = 24\,24833,$

$q = 7455\,60282\,56478\,84208\,33739\,57362\,00454\,91878\,33663\,42657,$

et r un nombre de 99 chiffres que nous renonçons à écrire.... mais que vous pourrez obtenir à partir de la divison de $2^{512} + 1$ par pq à l'aide d'une calculatrice !

La factorisation complète de $2^{512} + 1$ s'est achevée en 1993 après **une vingtaine d'années de travail** ; c'est un tour de force, tout comme le calcul d'Euler en son temps. Il a été nécessaire que 700 **ordinateurs** travaillent en parallèle dans le monde entier, à l'aide d'un **algorithme extrêmement sophistiqué**. Cela représente environ **80 années de temps de calculs**. Cela n'a pourtant pas suffi. Il a encore fallu 4 **mois de calcul sur un super-ordinateur** pour obtenir finalement le résultat.

Même aujourd'hui, la factorisation de nombres de 150 chiffres reste un exploit très exceptionnel, parfois accessible mais toujours avec **des moyens informatiques considérables et déraisonnables**.

Encore du pain sur la planche !...

À ce jour les seuls nombres de Fermat premiers que nous connaissons sont ceux que Fermat avait trouvés, c'est-à-dire F_0, F_1, F_2, F_3 et F_4.

- On ignore toujours s'il existe d'autres nombres de Fermat premiers.
  On pense que non, mais on ne dispose d'aucune démonstration ....
- On ignore tout autant s'il existe une infinité de nombres de Fermat qui ne sont pas premiers.
  On pense que oui, mais toujours pas de démonstration...

FÊTE DE LA SCIENCE