$2^{74\,207\,281} - 1$ est premier !

Mots-clefs.

Niveau. Quatrième, Troisième, Première S, Supérieur

Un nouveau très grand nombre premier vient d'être découvert ! La nouvelle n'est peut-être pas aussi sensationnelle que l'annonce de l'officialisation de quatre nouveaux éléments chimiques ou que la découverte potentielle d'une nouvelle planète dans le système solaire, mais elle a quand même été relayée par la presse générale.

En général, ces articles évoquent le nombre de chiffres du fameux nombre premier, et donnent parfois les premiers ou les derniers. Il arrive même qu'ils se trompent ! Revenons brièvement sur $2^{74\,207\,281} - 1$.

300376418084606182052986
098359166050056875863030
148484394169334554772321
906799429689365530077268
832044821488239942672783529
...
851607177740147629124621
136468794258014451073931
002129271816293359314942390
001821387921767116495628719
104986870100733910864363511

Quelques mots sur le projet GIMPS

La recherche des grands nombres premiers se concentre sur des nombres d'une forme très particulière, les *nombres de Mersenne*. Il s'agit de nombres de la forme $2^n - 1$. Ces nombres ne peuvent d'ailleurs être premiers que si l'exposant n est lui-même premier. En effet, si $n = pq$, avec $p, q \geq 2$, on peut utiliser la formule $a^r - 1 = (a-1)(a^{r-1} + a^{r-2} + \cdots + a^2 + a + 1)$ pour obtenir la factorisation non triviale

$$2^n - 1 = (2^p)^q - 1 = (2^p - 1)(2^{p(q-1)} + 2^{p(q-2)} + \cdots + 2^{2p} + 2^p + 1).$$

La raison de cette importance est que l'on dispose, pour les nombres de Mersenne, d'un test de primalité particulièrement efficace, le *test de Lucas-Lehmer*. Le plus grand nombre premier connu a très souvent été un nombre de Mersenne, comme l'indique par exemple cette table récapitulative.

Notons cependant que bien que l'on sache au moins depuis Euclide qu'il y a une infinité de nombre premiers, personne ne sait à l'heure actuelle s'il en va de même de la classe plus restreinte des nombres premiers de Mersenne, dont on ne connaît pour l'instant que 49 exemples.

Le projet GIMPS (*Great Internet Mersenne Prime Search*), lancé en 1996, est un projet collaboratif visant à déterminer quels nombres de Mersenne sont premiers. On pourra consulter le site du projet pour obtenir plus d'informations sur algorithmes utilisés et sur la manière dont les calculs sont répartis entre les ordinateurs des participants, voire pour participer à cette quête collective !

Le 21 janvier 2016, GIMPS a annoncé que le nombre de Mersenne $2^{74\,207\,281} - 1$ était effectivement premier, devenenant ainsi le plus grand nombre premier jamais découvert. Si vous voulez en connaître tous les chiffres, vous pouvez toujours télécharger un fichier texte contenant le nombre. Attention à l'ouverture : cet entier pèse 22 méga-octets...

Combien vaut (environ) $2^{74\,207\,281} - 1$?

Quel est l'ordre de grandeur de $2^{74\,207\,281} - 1$? Par exemple, combien de chiffres a-t-il ?

Remarquons déjà que $2^{74\,207\,281} - 1$ et son successeur $2^{74\,207\,281}$ ont exactement les mêmes chiffres, à l'exception du tout dernier. En effet, $2^{74\,207\,281}$, qui est un nombre pair non divisible par 5, doit se terminer par 2, 4, 6 ou 8, et il n'y a donc aucune retenue à faire dans la soustraction $2^{74\,207\,281} - 1$. Il s'agit donc de déterminer les premiers chiffres de la puissance de 2 correspondante, ici $2^{74\,207\,281}$.

Estimer $2^{74\,207\,281} - 1$ est en fait un exercice sur les logarithmes : en effet, 10^ℓ est le plus petit nombre à $\ell + 1$ chiffres donc le nombre ℓ de chiffres de $2^{74\,207\,281}$ est l'unique entier ℓ tel que $10^{\ell-1} \leq 2^{74\,207\,281} < 10^\ell$. On a alors

$$\begin{aligned} 10^{\ell-1} \leq 2^{74\,207\,281} < 10^\ell &\iff \ln\left(10^{\ell-1}\right) \leq \ln\left(2^{74\,207\,281}\right) < \ln\left(10^{\ell+1}\right) \\ &\iff (\ell-1)\ln(10) \leq 74\,207\,281\ln(2) < \ell\ln(10) \\ &\iff \ell = 1 + \left\lfloor 74\,207\,281\,\frac{\ln(2)}{\ln(10)} \right\rfloor, \end{aligned}$$

où $\lfloor x \rfloor$ désigne la partie entière de x.

Une calculatrice fournit le résultat $74\,207\,281\,\dfrac{\ln(2)}{\ln(10)} \approx 22\,338\,617,477\,665$, d'où l'on déduit que le nouveau plus grand nombre premier connu a 22 338 618 chiffres.

En revenant en sens inverse, on obtient donc que

$$\begin{aligned} 74\,207\,281\,\frac{\ln(2)}{\ln(10)} \approx 22\,338\,617,477\,665 &\iff 2^{74\,207\,281} \approx 10^{22\,338\,617,477\,665} \\ &\iff 2^{74\,207\,281} \approx 10^{0,477\,665} \times 10^{22\,338\,617} \\ &\iff 2^{74\,207\,281} \approx 3,003\,764 \times 10^{22\,338\,617}, \end{aligned}$$

ce qui donne effectivement les premiers chiffres de $2^{74\,207\,281} - 1$.

Les derniers chiffres

Évidemment, ce que l'on vient d'expliquer ne donne qu'un ordre de grandeur de $2^{74\,207\,281} - 1$. Il est en fait facile d'obtenir ses derniers chiffres. Expliquons par exemple comment en trouver les trois derniers chiffres en quelques secondes et quelques lignes de code.

Le point important est que si l'on connaît les trois derniers chiffres de deux entiers, on connaît également les trois derniers chiffres de leur produit. En effet, un nombre dont les trois

derniers chiffres forment le nombre $a < 1000$ s'écrit sous la forme $1000\,n + a$. Si l'on multiplie deux tels nombres, on obtient

$$(1000\,n + a)\,(1000\,m + b) = 1000\,(1000\,nm + nb + ma) + ab,$$

donc les trois derniers chiffres du produit sont les trois derniers chiffres de ab, et ils ne dépendent en particulier pas du tout de n et de m. C'est le principe de la multiplication **modulo 1000**.

En particulier, pour déterminer les trois derniers chiffres de $2^{74\,207\,281}$, il n'est pas besoin de multiplier 2 par lui-même 74 207 281 fois, on peut jeter à chaque fois tous les chiffres à part les trois derniers. Cela simplifie considérablement les calculs : par exemple, une fois que l'on sait que $2^{10} = 1024$, on peut déjà déduire que les trois derniers chiffres de $2^{20} = 2^{10} \times 2^{10}$ seront 576 (car $24 \times 24 = 576$), sans effectuer la multiplication complète. Cette simple remarque permet d'ailleurs déjà de calculer les derniers chiffres en un temps raisonnable. Par exemple le programme Python suivant nous apprend en quelques secondes que $2^{74\,207\,281}$ se termine par les trois chiffres 352 (et donc $2^{74\,207\,281} - 1$ par 351).

```
n=1
for i in range(74207281):
    n = (2*n) % 1000
print n
```

Il est en fait possible de calculer ces derniers chiffres beaucoup plus rapidement mais cette méthode rudimentaire illustre déjà l'importance de l'arithmétique modulaire : il n'est pas besoin de calculer entièrement $2^{74\,207\,281} - 1$ pour savoir qu'il se termine par

$$\ldots 364687942580144510739310021292718162933593149423901821387921767116495628719049868701007339108643635 1.$$