Un nombre premier de 157 chiffres

Michel Lafond(*)

Voici ce nombre :

M = 68 64797 66013 06097 14981 90079 90813 93217 26943 53001 43305 40939 44634 59185 54318 33976 56052 12255 96406 61454 55497 72963 11391 48085 80371 21987 99971 66438 12574 02829 11150 57151.

[*les tranches de 5 chiffres sont séparées*]

Si vous lisez la presse scientifique (Pour la Science, Science et Vie etc.), vous avez remarqué que tous les ans environ, on bat le record du plus grand nombre premier connu.

Le dernier record date de septembre 2006, et le nombre en question : $2^{32\,582\,657} - 1$ possède plus de 9 millions de chiffres.

Lorsque les 10 millions de chiffres seront atteints, ce qui ne saurait tarder, un prix de 100 000 dollars sera décerné par « Electronic Frontier Foundation ».

Quand on raconte autour de soi qu'on vient de trouver un nombre premier à plus de 9 millions de chiffres, 99% des gens rétorquent : « À quoi ça sert ? ». C'est exactement la même chose avec les 10 milliards de décimales de π. Quand on me demande « À quoi ça sert ? », je réponds en général « À la même chose que la course cycliste Paris-Roubaix ».

Ces résultats ne s'obtiennent qu'à l'aide de très beaux théorèmes de la théorie des nombres (et d'ordinateurs surpuissants qui sont d'ailleurs testés à cette occasion), et, quand vous aurez lu cet article, vous verrez comment les spécialistes de la théorie des nombres utilisent des outils taillés sur mesure pour arriver à leurs fins. C'est très instructif et fascinant. Bien entendu il faut se remuer les cellules grises, et c'est plus fatigant que de regarder à la télé des gens rouler à vélo sur des pavés.

1. Examen du monstre.

Vous avez reconnu M, il s'agit du nombre de Mersenne $M_{521} = 2^{521} - 1$.
Rappel : le p-ième nombre de Mersenne est par définition $M_p = 2^p - 1$.

On connaît aujourd'hui 44 nombres de Mersenne premiers, à savoir tous les M_p pour les valeurs de p appartenant à {2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, **521**, 607, 1 279, 2 203, 2 281, 3 217, 4 253, 4 423, 9 689, 9 941, 11 213, 19 937, 21 701, 23 209, 44 497, 86 243, 110 503, 132 049, 216 091, 756 839, 859 433, 1 257 787, 1 398 269, 2 976 221, 3 021 377, 6 972 593, 13 466 917, 20 996 011, 24 036 583, 25 964 951, 30 402 457, 32 582 657}.

Remarque : lorsque l'indice p n'est pas premier, le problème de la primarité de M_p ne se pose pas puisque $M_{qr} = 2^{qr} - 1$ est divisible par $2^q - 1$ et par $2^r - 1$.

(*) mlafond001@yahoo.fr

Le dernier et le plus grand : $M_{32\,582\,657}$ a été découvert en septembre 2006 et c'est le record actuel. La course ne s'arrêtera jamais ; d'abord un record est fait pour être battu : de plus, on ne sait pas s'il existe ou non une infinité de nombres de Mersenne premiers. Donc, cela ne peut qu'être intéressant de dresser la liste des premiers termes pour voir… Il y a des conjectures sur la suite des « bons exposants » : {2, 3, 5, 7, 13, 17, 19, 31, …} qui semblent être approximativement en suite géométrique.

Notre héros, l'entier $\mathbf{M = M_{521}}$, lui, a été découvert par un nommé ROBINSON en 1952 à l'aide d'un calculateur SWAC.

Ce qui est étonnant et qui fait l'objet de cet article est ceci :
1) Nous allons démontrer la primarité de M.
2) Le niveau de la démonstration est BAC + 1.
3) Les calculs nécessaires peuvent être entièrement et rapidement réalisés sur une simple calculatrice.

II. La préhistoire.

Du temps de l'âge de Pierre (Pierre Fermat bien sûr), pour tester la primarité de M, on n'avait pas tellement le choix, il fallait tester tous les diviseurs jusqu'à la racine carrée de M. Bien entendu, seuls les diviseurs premiers sont à tester et, par ailleurs, les diviseurs premiers q éventuels du nombre du Mersenne $M_p = 2^p - 1$ lorsque p est premier (c'est le cas de 521) ne peuvent être que de la forme $2kp + 1$ et congrus à 1 ou 7 modulo 8. Ce dernier résultat était connu de Legendre qui l'a démontré autour de 1800.
Exemples :
$2^{11} - 1 = 2\,047 = 23 \times 89$ deux facteurs de la forme $22k + 1$.
$2^{29} - 1 = 536\,870\,911 = 233 \times 1\,103 \times 2\,089$ trois facteurs de la forme $58k + 1$.
Mais même si on connaissait la liste des nombres premiers jusqu'à la racine carrée de M (il y en a de l'ordre de 10^{76}) et qu'on ne teste que ceux de la forme $2 \times 521\ k + 1$ et congrus à 1 ou 7 modulo 8 (il en reste de l'ordre de 10^{73}), avec une batterie de 10^{15} ordinateurs testant chacun 10^{15} diviseurs par seconde, il faudrait de l'ordre de 10^{33} siècles pour en venir à bout ! Oublions cette idée farfelue !
Nous allons ramener ces 10^{33} siècles à 3 minutes en utilisant le test de Lucas-Lehmer dont la démonstration date d'environ 1930.
Comme le microprocesseur a été fabriqué vers 1950, on comprend pourquoi, jusque là, on ne connaissait que 12 nombres premiers de Mersenne, le plus grand étant

$M_{127} = 2^{127} - 1 = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727$

et pourquoi les découvertes se multiplièrent par la suite.

III. L'énoncé du test de Lucas-Lehmer est :

Soit p un nombre premier supérieur ou égal à 3, et soit la suite L définie par :

$L_1 = 4$ et pour $n \geq 2$: $L_n = L_{n-1}^2 - 2$.

Alors : M_p est premier si et seulement si L_{p-1} est multiple de M_p.

Exemples :
$p = 5$, $M_5 = 2^5 - 1 = 31$.
La suite L calculée modulo 31, est ici :
$L_1 = 4$, $L_2 = 4^2 - 2 = 14$, $L_3 = 14^2 - 2 = 194 \equiv 8 \bmod 31$,
$L_4 = 8^2 - 2 = 62 \equiv 0 \bmod 31$.
D'après le test, $L_4 = L_{5-1}$ étant multiple de $M_5 = 31$, il s'ensuit que 31 est premier.

Par contre, si on essaie $p = 11$, $M_{11} = 2^{11} - 1 = 2\,047$ alors, la suite L est :
$L_1 = 4$, $L_2 = 4^2 - 2 = 14$, $L_3 = 14^2 - 2 = 194$,
$L_4 = 194^2 - 2 = 37\,634 \equiv 788 \bmod 2\,047$,
$L_5 = 788^2 - 2 = 620\,942 \equiv 701 \bmod 2\,047$,
$L_6 = 701^2 - 2 = 491\,399 \equiv 119 \bmod 2\,047$,
$L_7 = 119^2 - 2 = 14\,159 \equiv 1\,877 \bmod 2\,047$,
$L_8 = 1\,877^2 - 2 = 3\,523\,127 \equiv 240 \bmod 2\,047$,
$L_9 = 240^2 - 2 = 27\,598 \equiv 282 \bmod 2\,047$,
$L_{10} = 282^2 - 2 = 79\,522 \equiv 1\,736 \bmod 2\,047$.
$L_{10} = L_{11-1}$ n'étant pas multiple de $M_{11} = 2\,047$, il s'ensuit que 2 047 n'est pas premier.

IV. Démonstration de l'énoncé du test.

On n'a pas besoin ici de démonter complètement le test, tout ce qu'il nous faut est la démonstration de la partie directe : Si L_{p-1} est multiple de M_p, alors M_p est premier.

Pour cela, on part de l'hypothèse :
p est un nombre premier supérieur ou égal à 3.
La suite L est définie par : $L_1 = 4$ et pour $n \geq 2$: $L_n = L_{n-1}^2 - 2$.
L_{p-1} est multiple de M_p.
Et il faut démontrer que M_p est premier.

Nous raisonnerons par l'absurde :
Si M_p n'était pas premier, il existerait un diviseur premier d de M_p inférieur à la racine carrée de M_p : $1 < d \leq \sqrt{M_p}$ et d divise M_p.

Soit **K** le corps des entiers modulo d. [On s'intéresse aux multiples de d, et comme on a impérativement besoin d'une structure de corps commutatif par la suite, il est naturel de faire intervenir **K**]. Selon l'usage, on fera l'abus de notation consistant à noter 0, 1, 2, …, $d - 1$ les éléments de **K**.
Le nombre 3 (de **K**) va jouer un rôle spécial, et il faudra distinguer deux cas selon que, dans **K**, 3 est ou non un carré.

Exemples :
Si $d = 7$, dans **K** qu'on note abusivement {0, 1, 2, 3, 4, 5, 6}, les carrés (modulo 7) sont respectivement {0, 1, 4, 2, 2, 4, 1} et on constate que 3 n'est pas un carré.
Alors que si $d = 11$, on a $5^2 = 25 \equiv 3$ (modulo 11) et cette fois 3 est un carré.

IV-1. Premier cas : 3 n'est pas un carré dans K.

Nous allons procéder à une extension de corps (de la même manière qu'on étend le corps des réels $\mathbb{R}$ en posant $i^2 = -1$ pour obtenir le corps des complexes).
Soit α un élément « imaginaire » tel que $\alpha^2 = 3$.

Si vous pensez en ce moment à $\sqrt{3} \approx 1,732\ldots$, chassez vite cette mauvaise pensée.
D'après notre hypothèse, α n'est pas dans **K** sans quoi $3 = \alpha^2$ serait un carré dans **K**, et on étend **K** en définissant l'ensemble qu'on note **K**[α] des « nombres » de la forme $a + b\alpha$ avec a et b quelconques dans **K**.
La démonstration de la structure de corps de **K**[α] ne pose pas de problème, sauf lorsqu'il s'agit de démontrer que tout élément non nul de **K**[α] possède un inverse.

La voici :
Soit $a + b\alpha$ non nul de **K**[α].
On cherche dans **K**[α] un élément $x + y\alpha$ tel que $(a + b\alpha)(x + y\alpha) = 1$.
Cela équivaut au système

$$\begin{cases} ax + 3by = 1 \\ ay + bx = 0 \end{cases} \qquad \text{(S)}$$

$a + b\alpha$ est non nul donc <u>a et b ne sont pas tous deux nuls</u>.
Si a est non nul, il est inversible dans **K**, et alors la seconde équation de (S) donne $y = -ba^{-1}x$. Si on reporte dans la première équation, on obtient

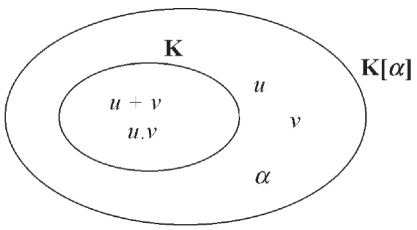
$$ax + 3b(-ba^{-1}x) = 1$$

ou encore : $x(a^2 - 3b^2)a^{-1} = 1$.
Or $a^2 - 3b^2$ n'est pas nul, sinon $3 = a^2 b^{-2} = (a b^{-1})^2$ serait un carré dans **K**.
Donc $x = a(a^2 - 3b^2)^{-1}$ et $y = -ba^{-1}x$ définissent l'inverse unique de $a + b\alpha$.
[On ferait une démonstration analogue si c'est b qui n'est pas nul].

Selon l'usage, on identifie **K** avec la partie de **K**[α] pour laquelle $b = 0$, et on peut donc dire que **K**[α] contient **K**.

C'est le moment d'utiliser nos hypothèses : L_{p-1} est multiple de M_p et M_p admet le diviseur $d > 1$.
Donc L_{p-1} est multiple de d et, par conséquent, si on reconsidère la suite L, mais modulo d, sans rien changer à sa définition, et en gardant la même lettre pour simplifier (encore un abus de notation), on aura $L_{p-1} = 0$ dans **K** (entiers modulo d).
Dans **K**[α] introduisons $u = 2 + \alpha$ et $v = 2 - \alpha$ de sorte que α, u, v vérifient les deux égalités ci dessous dont l'utilité apparaîtra dans la suite (L_i) :

$$u + v = 4 \text{ et } u \cdot v = (2 + \alpha) \cdot (2 - \alpha) = 4 - \alpha^2 = 4 - 3 = 1.$$



Posons donc dans **K**, $L_1 = 4$ et pour $n \geq 2$: $L_n = L_{n-1}^2 - 2$.
La suite (L_i) est toute entière dans **K** puisque les deux opérations sont internes [au corps]. Donc tout se passe dans $\mathbf{K}[\alpha]$. Les calculs ci-dessous montrent bien pourquoi il nous fallait un corps commutatif, et deux éléments u, v tels que $u + v = 4$ et $u \cdot v = 1$ [u, v sont inverses et $v = u^{-1}$]
Comme on est dans un corps commutatif, les règles ou conventions usuelles sur les puissances s'appliquent comme, par exemple, $x^0 = 1$; $u^4 \cdot v^4 = (u \cdot v)^4 = 1^4 = 1$; $\left(x^m\right)^n = x^{mn}$; etc.

$L_1 = 4 = u + v$ implique $L_2 = L_1^2 - 2 = (u + v)^2 - 2 = u^2 + v^2 + 2\,u{\cdot}v - 2 = u^2 + v^2$.

Puis $L_3 = L_2^2 - 2 = (u^2 + v^2)^2 - 2 = u^4 + v^4 + 2\,u^2{\cdot}v^2 - 2 = u^4 + v^4$.

Puis $L_4 = L_3^2 - 2 = (u^4 + v^4)^2 - 2 = u^8 + v^8 + 2\,u^4{\cdot}v^4 - 2 = u^8 + v^8$.
Une récurrence immédiate montre que pour tout entier naturel n on a :

$$L_n = u^{2^{n-1}} + v^{2^{n-1}}.$$

Mais $v = u^{-1}$ implique :

$$L_{p-1} = u^{2^{p-2}} + v^{2^{p-2}} = u^{2^{p-2}}\left(1 + u^{-2^{p-2}} v^{2^{p-2}}\right) = u^{2^{p-2}}\left(1 + v^{2^{p-2}} v^{2^{p-2}}\right) = u^{2^{p-2}}\left(1 + v^{2^{p-1}}\right).$$

Puisque $L_{p-1} = 0$ dans **K**, il s'ensuit que $u^{2^{p-2}}\left(1 + v^{2^{p-1}}\right) = 0.$ [Le 0 de **K**]

L'un des deux facteurs est nul, et ce n'est pas $u^{2^{p-2}}$ car si on avait $u = 2 + \alpha = 0$, on aurait $\alpha = -2$ et α serait dans **K**.

Le second facteur est donc nul, ou encore $1 + v^{2^{p-1}} = 0$, soit $v^{2^{p-1}} = -1$ (on est toujours dans $\mathbf{K}[\alpha]$).

En élevant au carré, on obtient $v^{2^p} = 1$.
Appelons ω l'ordre de v dans le groupe multiplicatif de $\mathbf{K}[\alpha]$, c'est-à-dire le plus petit entier strictement positif tel que $v^\omega = 1$. La théorie des groupes nous dit que ω divise 2^p et que ω divise le cardinal du groupe.
Il faut connaître le cardinal m de ce groupe. Puisque $\mathbf{K}[\alpha]$ est l'ensemble des « nombres » de la forme $a + b\alpha$ avec a et b quelconques dans **K**, le groupe multiplicatif du corps (tous les éléments sauf 0) contient $m = d^2 - 1$ éléments. Ceux-ci sont bien tous distincts, car, si $a + b\alpha = a' + b'\alpha$, alors $(a - a') + (b - b')\alpha = 0$ qui n'est possible que si $a = a'$ et $b = b'$, sans quoi α serait dans **K**.
Puisque ω divise 2^p, ω est une puissance de 2, disons $\omega = 2^t$.

Or t n'est pas inférieur ou égal à $p - 1$, sinon, partant de $v^{2^t} = 1$ et, par élévations au carré successives, on arriverait à $v^{2^{p-1}} = 1$, ce qui est contradictoire avec $v^{2^{p-1}} = -1$.
t est donc supérieur ou égal à p. Mais alors, $2^t = \omega$ est supérieur ou égal à 2^p.
C'est clair, $\omega = 2^p$.

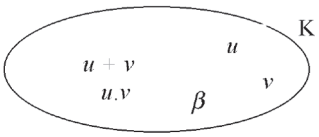
Mais ω divise le cardinal $m = d^2 - 1$ du groupe, donc on arrive enfin à la contradiction :

$$2^p \leq d^2 - 1 < d^2 \leq M_p < 2^p$$

(on rappelle que $d \leq \sqrt{M_p}$).

IV-2. Deuxième cas : 3 est un carré dans K.

Il existe dans **K** un élément β tel que $\beta^2 = 3$.
C'est beaucoup plus simple dans ce cas, aucune extension de corps n'étant à prévoir :



On pose $u = 2 + \beta$ et $v = 2 - \beta$. Et la démonstration est identique à celle du cas IV-1 sauf pour le cardinal du groupe (ici **K** − {0}) qui vaut $m = d - 1$ au lieu de $d^2 - 1$.

La contradiction est la même : $2^p \leq d^2 - 1 < d^2 \leq M_p < 2^p$.

V. Application du test à M = M_{521}.

521 est premier, le test s'applique et dit que si on pose $L_1 = 4$ et pour $n \geq 2$: $L_n = L_{n-1}^2 - 2$, alors il suffit de vérifier que L_{520} est multiple de M pour garantir la primarité de M.
519 multiplications sont nécessaires, et le calcul modulo M suffit (heureusement !).
Je n'ai pas mieux à la maison que la calculatrice TI 92 qui peut opérer exactement sur des entiers ayant jusqu'à 614 chiffres, mais voir à ce sujet la remarque de Claude Morin en fin d'article.
La TI 92 calcule exactement factorielle (299) qui a 613 chiffres (avec sa ribambelle de 72 zéros à la fin) mais on voit bien qu'elle peine !
Par contre pour factorielle (300) il faut se contenter du résultat

$$3.06057512216 \times 10^{614}.$$

$M = M_{521}$ possède 157 chiffres, et nous pouvons donc calculer des carrés (et même des cubes) modulo M sur la TI 92. Le test, qui ne nécessite que des élévations au carré, va pouvoir s'appliquer.

Auparavant, une remarque : on peut se dire « Pourquoi tout ça alors que la TI 92 a la fonction " factor " qui décompose les entiers en facteurs premiers ». Oui, mais si on lit la brochure, il est dit que le programme ne teste que les facteurs premiers jusqu'à 65 537 (c'est à dire $2^{16} + 1$).
Ainsi, elle trouve factor (4295098369) = 65537^2 en 40 secondes, mais elle ne trouve pas factor (4295622677) = 65539 × 65543.
C'est d'ailleurs piégeant, car elle affiche factor (4295622677) = 4295622677 laissant croire que ce nombre est premier [moralité : toujours lire les brochures].

Bref ! Vérifions que $y = L_{520}$ est bien nul modulo M et notre cauchemar prendra fin. Voici le programme valable sur TI 92 et sur bon nombre de ses petites soeurs :

```
lucas (p)
Prgm
Local n, y, i
2^p-1 → n: 4→ y
For i, 1, p-2
 mod (y*y-2,n) → y
EndFor
Output 18, 12, "y =": Output 18, 40, y
EndPrgm
```

Ce programme est traduisible dans n'importe quel langage.

(18, 12 et 18, 40 sont simplement des coordonnées écran pour l'affichage final)

On tape lucas(521) et au bout d'un peu moins de 3 minutes on voit s'afficher $y = 0$, ce qui prouve que $2^{521} - 1$ est premier.

Vous pouvez faire encore mieux, vérifiez avec la TI 92 que le nombre de Mersenne M_{607} qui a 183 chiffres est premier (il faut quatre bonnes minutes).

Si on essaye lucas (523) on voit s'afficher après quatre bonnes minutes :
y = 146802564739567965714618952671279944018627770337022406239699029841167563052656661820506839733340283359191284268802067755366616185543299501130238954950095 2495
Cela prouve que $2^{523} - 1$ n'est pas premier (on utilise la réciproque du test, non démontrée ici).

Quant à trouver les facteurs de $2^{523} - 1$, c'est un autre cauchemar, et il faut beaucoup plus que le test de Lucas-Lehmer pour les obtenir :

$2^{523} - 1 =$
27 459190 640522 438859 927603 196325 572869 077741 200573 221637 577853 836742 172733 590624 208490 238562 645818 219909 185245 565923 432148 487951 998866 575250 296113 164460 228607 =
160 188778 313202 118610 543685 368878 688932 828701 136501 444932 217468 039063
$\times$
171417 691861 249198 128317 096534 322116 476165 056718 630345 094896 620367 860006 486977 101859 504089

comme je l'ai vérifié avec ma vieille TI 92 !

VI. Pour tout savoir sur les nombres de Mersenne, aller sur :

http://primes.utm.edu/mersenne/index.html

Pour la manière dont s'y prennent concrètement les spécialistes pour battre les records, ainsi que des détails sur la fondation qui offre le prix de 100 000 dollars, aller sur :

http://www.mersenne.org

Pour une vue d'ensemble sur les nombres premiers un excellent site :

http://primes.utm.edu/top20/index.php

Enfin un site à partir duquel on peut factoriser en ligne des nombres de plusieurs dizaines de chiffres (que vous entrez au clavier) en un temps qui laisse rêveur (l'algorithme ECM utilisé est basé sur l'utilisation massive des courbes elliptiques) :

http://www.alpertron.com.ar/ECM.HTM

Remarque de Claude Morin :

La TI-92 (qui date de 1995) ne se fait plus ; elle est remplacée par la TI89, la Voyage 200 et la TI NSPIRE CAS. Le langage de programmation est le même pour toutes ces calculatrices. Mais la TI factorise maintenant 1234547G1234577 en dix secondes et isprime($2^{61} - 1$) donne « true » dans le même temps (la nouvelle TI NSPIRE est encore plus rapide). Les durées de calcul indiquées ci-dessus sont à diviser par 2 (au moins).