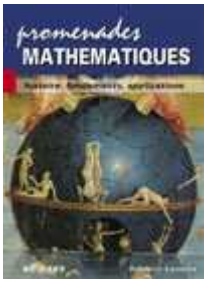

Nombres parfaits, nombres de Mersenne et test de Lucas-Lehmer

1. Nombres parfaits et nombres de Mersenne

Les nombres parfaits sont les nombres égaux à la somme de leurs diviseurs autres que eux-mêmes comme 6 ou 28. Euclide montre que si 2^p-1 et p sont premiers alors $2^{p-1}(2^p-1)$ est parfait. Euler a démontré la réciproque : un nombre parfait pair est de la forme $2^{p-1}(2^p-1)$.

Prenons un nombre quelconque constitué de r facteurs premiers à des puissances diverses : $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$; pour avoir un diviseur de n on peut choisir une puissance de p_1 de α_1+1 manières ($+1$ pour la puissance 0), une puissance de p_2 de α_2+1 manières … donc au final on a $\nu(n)=\prod_{i=1}^{r}(\alpha_i+1)$ diviseurs possibles. La somme des diviseurs est alors

$$\sigma(n)=(1+p_1+...+p_1^{\alpha_1})(1+p_2+...+p_2^{\alpha_1})...(1+p_r+...+p_r^{\alpha_r})=\prod_{i=1}^{r}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

puisque si on développe le membre de gauche on aura tous les produits possibles sans aucune répétition de tous les termes primaires de n. Remarquons que si $\text{pgcd}(m,n)=1$ alors

$$\nu(mn)=\nu(m)\nu(n) \text{ et } \sigma(mn)=\sigma(m)\sigma(n).$$

Ceci est facile à voir du fait que m et n n'ont aucun facteur commun autre que 1. Les fonctions ν et σ sont des fonctions *multiplicatives*. Montrer qu'un nombre P est parfait revient donc à montrer que

$$\sigma(P)=2P.$$

Revenons aux nombres parfaits en prenant $n=2^p-1$ premier ainsi que p :

$$\sigma(2^{p-1}(2^p-1))=\sigma(2^{p-1})\sigma(2^p-1)=(2^p-1)(2^p)$$

la somme des diviseurs de 2^{p-1} est la somme des termes 2^i et la somme des diviseurs de 2^{p-1} est $1+(2^p-1)=2^p$. En enlevant n, on a bien un nombre parfait.

Réciproquement prenons un nombre parfait pair P, de la forme $q2^{n-1}$ avec q impair et $n>1$; 2^{n-1} et q sont premiers entre eux donc

$$\sigma(P)=\sigma(2^{n-1}q)=\sigma(2^{n-1})\sigma(q)=(2^n-1)\sigma(q),$$

mais comme P est parfait, on doit avoir

$$\sigma(P)=2P=2^n q.$$

2^n-1 est impair donc divise q, soit $q=(2^n-1)r$ ou encore $q+r=2^n-1$ qui est inférieur ou égal à $\sigma(q)$.

On a donc

$$(2^n-1)\sigma(q)\geq(2^n-1)(q+r)=(2^n-1)(2^n r)=2^n q=\sigma(2^{n-1}q)=(2^n-1)\sigma(q) \ ;$$

l'inégalité du début est donc une égalité et $\sigma(q) = q + r$, par conséquent q et r sont les seuls diviseurs de q ; conclusion $r = 1$, q est premier, vaut $2^n - 1$ et $P = 2^{n-1}(2^n - 1)$ avec n et $2^n - 1$ premiers (en fait si $2^n - 1$ est premier, n l'est aussi mais la réciproque est fausse…trouvez un contre-exemple).

Ceci amène à plusieurs questions :

* y-a-t'il des nombres parfaits impairs ? on n'en connaît aucun alors qu'il n'y a à priori aucune raison qu'il n'y en ait pas… la conjecture est donc : « il n'y a pas de nombre parfait impair » !

* quels sont les nombres de la forme $2^n - 1$ premiers ? ce sont les nombres de Mersenne dont on a conjecturé qu'ils étaient une infinité et font l'objet d'actives recherches car ils permettent de produire les très grands nombres premiers indispensables en cryptographie.

Attention, les nombres de Mersenne ne sont pas tous premiers !

2. Test de Lucas-Lehmer

Edouard Lucas (1842 – 1891) a trouvé le test suivant permettant de vérifier si on a un nombre de Mersenne premier ; ce test a été amélioré par Derrick Lehmer dans les années 30 : on prend la suite définie par

$$s_{n+1} = (s_n)^2 - 2\,,\ s_0 = 4 \text{ (on peut changer la valeur initiale),}$$

alors

$$M_p = 2^p - 1 \text{ est premier si et seulement si } M_p \text{ divise } s_{p-1} \text{ (ou } s_{p-1} \equiv 0(2^p - 1)\text{).}$$

Quelques exemples réalisés avec Maple :

```
> restart;
> M := 2^n-1:seq(M,n=[2,3,5,7,11,13,17]);
# on calcule les premiers Mersenne
                    3, 7, 31, 127, 2047, 8191, 131071

> lucas := proc(n)
local M,L,k;
M := 2^n-1; L := 4;
for k from 2 to n-1 do L := (L^2 - 2) mod M; od;
evalb(L=0);
end;
#procédure de calcul, renvoie true si le test est bon, false
#sinon, calcule également le temps mis pour le calcul.

> n := 2281:length(M);debut:= time():lucas(n);time()-debut;
                              687
                             true
                            0.750

> n := 15281:length(M);debut:= time():lucas(n);time()-debut;
                             4601
                            false
                           93.016
```

Pour les détails sur les nombres de Mersenne, voir
http://fr.wikipedia.org/wiki/Nombre_premier_de_Mersenne
Le projet de recherche des nombres premiers de Mersenne, GIMPS
http://www.mersenne.org/french_prime.htm
Un cours assez complet
http://algo.inria.fr/banderier/Recipro/node1.html de http://www-lipn.univ-paris13.fr/~banderier/
Date un peu mais amusant http://www.fatrazie.com/nb_premiers.htm
Et évidemment http://mathworld.wolfram.com/MersennePrime.html
ainsi que http://mathworld.wolfram.com/Lucas-LehmerTest.html

La démonstration se fait en deux temps : si $s_{p-1} \equiv 0(2^p - 1)$ alors $M_p = 2^p - 1$ est premier, puis la réciproque.

Etape 1 : posons $u = 2 - \sqrt{3}$ et $v = 2 + \sqrt{3}$, alors $s_0 = 4 = u^1 + v^1$; supposons que $s_n = u^{t_n} + v^{t_n}$, t_n à déterminer avec $t_0 = 1$, on calcule : $s_{n+1} = u^{t_{n+1}} + v^{t_{n+1}} = (s_n)^2 - 2 = u^{2t_n} + v^{2t_n} + 2(uv)^{t_n} - 2$, or $uv = 4 - 3 = 1$ donc $s_{n+1} = u^{2t_n} + v^{2t_n}$ et $t_{n+1} = 2t_n$, soit $t_n = 2^n$.

On a donc $s_n = u^{2^n} + v^{2^n}$ (si on démarre avec une autre valeur de s_0, il suffit de prendre u et v de sorte que $uv = 1$).
Le raisonnement va consister à trouver une contradiction au fait que M_p n'est pas premier : supposons que $s_{p-1} = u^{2^{p-1}} + v^{2^{p-1}}$ soit divisible par M_p, lui-même divisible par q premier et $q < \sqrt{M_p}$, alors s_{p-1} est divisble par q.
Plaçons nous dans le corps $\mathrm{F}_q\left(\sqrt{3}\right) = \left\{ n \in \mathbb{R} / n = a + b\sqrt{3}, a, b \in \mathrm{F}_q \right\}$, $\mathrm{F}_q\left(\sqrt{3}\right)$ contient évidemment F_q, avec égalité lorsque $\sqrt{3}$ est un carré modulo q. Dans $\mathrm{F}_q\left(\sqrt{3}\right)$ il y a q^2 éléments ou q, et les éléments non-nuls sont au nombre de $q^2 - 1$ ou $q - 1$.
Soit x un élément non nul de $\mathrm{F}_q\left(\sqrt{3}\right)$, il existe un plus petit nombre positif d, appelé ordre de x, tel que $x^d = 1[q]$ et divise $q^2 - 1$ ou $q - 1$ (en fait comme $q - 1$ divise $q^2 - 1$, on peut ne pas s'occuper de ce cas et donc ne pas s'inquiéter de ce que $\sqrt{3}$ soit un carré modulo q ou non).
Continuons : s_{p-1} est divisible par q donc $s_{p-1} \equiv 0[q] \Leftrightarrow u^{t_{p-2}} + v^{t_{p-2}} \equiv 0[q] \Leftrightarrow u^{t_{p-2}}\left(1 + \dfrac{v^{t_{p-2}}}{u^{t_{p-2}}}\right) \equiv 0[q]$
mais comme $uv = 1$, on a $u^{t_{p-2}}\left(1 + v^{2t_{p-2}}\right) \equiv 0[q]$.
Mais u n'est pas nul modulo q, sinon on aurait $3 \equiv 4[q]$ ce qui est impossible sauf si $q = 1$, si bien que $u^{t_{p-2}}\left(1 + v^{2t_{p-2}}\right) \equiv 0[q] \Leftrightarrow 1 + v^{2t_{p-2}} \equiv 0[q] \Leftrightarrow v^{t_{p-1}} \equiv -1[q] \Rightarrow \left(v^{t_{p-1}}\right)^2 \equiv 1[q] \Leftrightarrow v^{t_p} \equiv 1[q]$. L'ordre de v doit donc diviser t_p qui est une puissance de 2 ; or tout nombre divisant strictement t_p divise t_{p-1} : si l'ordre de v était plus petit que t_p alors on aurait $v^{t_{p-1}} \equiv 1[q]$ et non $v^{t_{p-1}} \equiv -1[q]$, moralité l'ordre de v est bien t_p.

On a alors $t_p = 2^p = M_p + 1$ et t_p divise $q^2 - 1$, soit $M_p + 1 = t_p = 2^p < q^2 - 1 < M_p - 1$ puisqu'on avait supposé que $q < \sqrt{M_p}$; il y a bien contradiction.

Etape 2 : on suppose M_p premier ; si on montre que $v^{2t_{p-2}} = v^{t_{p-1}} \equiv -1 \left[M_p \right]$ alors on aura $s_{p-1} = u^{t_{p-2}} \left(1 + v^{2t_{p-2}} \right) \equiv 0 \left[M_p \right]$.

Nous avons besoin de plusieurs résultats dans le corps F_{M_p} :

* -1 n'est pas un carré modulo M_p : $M_p - 1 = 2^p - 2 = 2\left(2^{p-1} - 1 \right)$ est divisible par 2 mais pas par 4, $\dfrac{M_p - 1}{2}$ est impair et $(-1)^{\frac{M_p - 1}{2}} = -1$ ou -1 n'est pas un carré.

* 2 est un carré et une puissance quatrième modulo M_p : d'après le petit théorème de Fermat, $2^{M_p} = 2 \left[M_p \right] \Rightarrow 2^{M_p + 1} = 4 \left[M_p \right]$ et $M_p + 1 = 2^p$; on en tire $\sqrt{2} = 2^{\frac{1}{2}} = 2^{\frac{M_p + 1}{4}} \left[M_p \right]$ et $2^{\frac{1}{4}} = 2^{\frac{M_p + 1}{8}} \left[M_p \right]$ (à condition évidemment que $p \geq 3$).

* 3 n'est pas un carré modulo M_p : prenons les trois nombres consécutifs $M_p - 1$, M_p et $M_p + 1$; un des trois doit être divisible par 3 : M_p est premier et $M_p + 1$ est une puissance de 2 donc 3 doit diviser $M_p - 1$.

Soit g un générateur du groupe multiplicatif des éléments non-nuls de F_{M_p} : ce groupe est cyclique et a $M_p - 1$ éléments et les différentes puissances de g représentent tous les éléments de F_{M_p}.

Considérons $w = g^{\frac{M_p - 1}{3}}$, racine cubique[1] non-triviale de 1, soit une solution de l'équation $x^3 = 1 \left[M_p \right]$, et donc de $x^2 + x + 1 = 0 \left[M_p \right]$.

Calculons maintenant $z^2 = \left(w - w^2 \right)^2 = w^2 - 2w^3 + w^4 = w^2 - 2 + w = w^2 + w + 1 - 3 = -3 \left[M_p \right]$; -3 est donc un carré alors que -1 n'en est pas un, conclusion : 3 n'est pas un carré puisque $3 = (-1)(-3)$.

* $v = 2 + \sqrt{3}$ a une racine carrée mais pas de racine quatrième : comme 3 n'est pas un carré, nous avons $3^{\frac{M_p - 1}{2}} = -1 \left[M_p \right]$, ce qui donne $v^{M_p} = 2^{M_p} + 3^{\frac{M_p - 1}{2}} \sqrt{3} = 2 - \sqrt{3} = u \left[M_p \right]$ (dans le développement du binôme l'exposant apparaît dans tous les termes sauf le premier et le dernier, donc $(x + y)^{M_p} = x^{M_p} + y^{M_p} \left[M_p \right]$).

On cherche une racine carrée de v : soit

$$\left(a + b\sqrt{3} \right)^2 = 2 + \sqrt{3} \Leftrightarrow a^2 + 3b^2 + 2ab\sqrt{3} = 2 + \sqrt{3} \Leftrightarrow \begin{cases} a^2 + 3b^2 = 2 \\ 2ab = 1 \end{cases},$$

[1] Par exemple les racines cubiques de 1 dans F_{31} sont 5 et 25.

ce qui donne $a+b\sqrt{3}=\frac{3}{\sqrt{6}}+\frac{\sqrt{3}}{\sqrt{6}}=\pm\frac{1+\sqrt{3}}{\sqrt{2}}$; comme on a $2^{\frac{M_p+1}{4}}=\sqrt{2}\left[M_p\right]$ et $2^{M_p-1}=1\left[M_p\right]$, on peut écrire $\frac{1}{\sqrt{2}}=2^{M_p-1-\frac{M_p+1}{4}}\left[M_p\right]=2^{\frac{3M_p-5}{4}}\left[M_p\right]=2^{\frac{3\times 2^p}{4}-2}\left[M_p\right]$. De toutes manières comme 2 a une racine quatrième, pour que v en ait une, il faudrait que $1+\sqrt{3}$ ait une racine carrée et soit donc un carré. Comme précédemment on a le système $\begin{cases} a^2+3b^2=1 \\ 2ab=1 \end{cases}$ d'où l'on tire

$$a^2+3b^2=2ab\Rightarrow(a-b)^2+2b^2=0\Rightarrow\left(\frac{a-b}{b}\right)^2=-2\ ;$$

2 est un carré mais -1 n'en est pas un donc -2 n'est pas un carré et on ne peut trouver a et b.

* La démonstration maintenant : 3 n'est pas un carré mod M_p donc $\mathrm{F}_{M_p}\left(\sqrt{3}\right)$ a M_p^2 éléments (il est évidemment sous-entendu que $\sqrt{3}$ est ici une solution de l'équation $x^2=3\left[M_p\right]$). Les nombres u et v sont représentés dans $\mathrm{F}_{M_p}\left(\sqrt{3}\right)$ par $u=2-\sqrt{3}$ et $v=2+\sqrt{3}$ qui satisfont toujours $u+v=4$ et $uv=1$; par récurrence on a $v^{M_p}=2^{M_p}+\sqrt{3}^{M_p}=2^{M_p}+3^{\frac{M_p-1}{2}}\sqrt{3}$.

3 n'est pas un carré modulo M_p et $\left(3^{\frac{M_p-1}{2}}\right)^2=3^{M_p-1}=1\left[M_p\right]\Rightarrow 3^{\frac{M_p-1}{2}}=-1\left[M_p\right]$; avec Fermat, on a $2^{M_p}=2\left[M_p\right]$, on obtient donc $v^{M_p}=2^{M_p}+\sqrt{3}^{M_p}=2-\sqrt{3}\left[M_p\right]=u$, soit $v^{M_p+1}=uv=1\left[M_p\right]$.

Comme dans la première partie, l'ordre des éléments de $\mathrm{F}_{M_p}\left(\sqrt{3}\right)$ divise $M_p^2-1=\left(M_p-1\right)\left(M_p+1\right)=\left(M_p-1\right)2^p=\left(\frac{M_p-1}{2}\right)2^{p+1}$; $\frac{M_p-1}{2}=\frac{2^p-2}{2}=2^{p-1}-1$ est impair et l'ordre de v est une puissance de 2 divisant M_p+1 : on peut alors trouver un élément de $\mathrm{F}_{M_p}\left(\sqrt{3}\right)$ qui est une racine carrée de v mais qui n'a pas de racine carrée lui-même ; cet élément a alors pour ordre $2\left(M_p+1\right)$ et v a pour ordre M_p+1.

Concluons : $v^{\frac{M_p+1}{2}}=v^{t_p-1}=-1\left[M_p\right]$, ce qui achève la réciproque.