Devoir Sur Table N°12

Arithmétique

1 Février 2019

Entiers parfaits pairs

Dans tout ce problème, les entiers sont naturels : on travaille donc dans $\mathbb{N}$.

Si n est un entier non nul, on note $S(n)$ la somme de ses diviseurs dans $\mathbb{N}^*$ (y compris 1 et n).

Ainsi, $S(1)=1$, $S(2)=3$, $S(833)=S(7^2\cdot 17)=1+7+17+49+119+833=1026$.

Un entier n est dit **parfait** lorsqu'il vérifie $S(n)=2n$.

Le but de ce problème est la recherche des nombres parfaits pairs.

On notera $\mathcal{D}(n)$ l'ensemble des diviseurs de n dans $\mathbb{N}^*$, de sorte que $S(n)=\sum_{k\in\mathcal{D}(n)} k$.

Question préliminaire : on note pour $n\in\mathbb{N}$, $M_n=2^n-1$.

Montrer que si $p,q\in\mathbb{N}$ alors M_p divise M_{pq}.

En déduire que pour que M_n soit premier, il est nécessaire que n soit premier.

Partie I

1. Ecrire sans ruser une prodécure Maple prenant en paramètre un entier n (que l'on supposera ≥ 1 sans le tester) et retournant `true` ou `false` suivant que n est parfait ou pas. On rappelle que `irem(n,k)` vaut le reste de la division euclidienne de n par k.
2. Expliquer (sans programmer) comment on pourrait améliorer l'efficacité de cette procédure.
3. Montrer que n est premier ssi $S(n)=n+1$.
4. Si p est premier et si $n\in\mathbb{N}^*$, déterminer $\mathcal{D}(p^n)$ et montrer que $S(p^n)=\dfrac{p^{n+1}-1}{p-1}$.

Partie II

On considère dans cette partie $a,b\in\mathbb{N}^*$ tels que $a\wedge b=1$.

Nous allons montrer que $S(ab)=S(a)S(b)$.

Soit f l'application définie sur $\mathcal{D}(a)\times\mathcal{D}(b)$ par $f(x,y)=xy$.

1. Montrer que f est à valeurs dans $\mathcal{D}(ab)$.
2. Montrer que si $u|a$ et $v|b$ alors $u\wedge v=1$.
3. En déduire que f est injective.
4. Montrer que f est surjective : on pourra prendre d dans $\mathcal{D}(ab)$ et considérer $x=d\wedge a$.
5. Etablir que $S(ab)=S(a)S(b)$.
6. Montrer que ceci fournit une nouvelle méthode pour calculer $S(n)$.
   Comparer avec la méthode utilisée dans la procédure Maple.

Partie III

On va montrer que n pair est parfait si et seulement si il est de la forme $2^{p-1}(2^p-1)$ avec 2^p-1 premier.

1. Soit p dans $\mathbb{N}^*$ tel que 2^p-1 est premier.
   Montrer que $2^{p-1}(2^p-1)$ est un nombre parfait pair.
   On considère désormais un nombre parfait pair n.
2. Montrer que n a au moins un facteur premier impair.
   Ainsi, on peut écrire : $n=2^a b$ avec $a\in\mathbb{N}^*$ et $b\geq 3$ impair.
3. Montrer qu'il existe c dans $\mathbb{N}^*$ tel que $\begin{cases} b=(2^{a+1}-1)c \\ S(b)=2^{a+1}c \end{cases}$
4. Montrer par l'absurde que $c=1$.
5. En déduire que b est premier puis que $a+1$ est premier. Conclure.
6. Donner trois nombres parfaits pairs.
7. On ne sait pas grand chose sur les nombres parfaits impairs : montrer tout de même que si n est parfait et impair alors il admet au moins trois diviseurs premiers distincts.

Corrigé

Question préliminaire :

Si $p, q \in \mathbb{N}$ alors $M_{pq} = 2^{pq} - 1 = (2^p)^q - 1 = (2^p - 1)((2^p)^{q-1} + \ldots + 1)$ ce qui prouve bien que $M_p \mid M_{pq}$.

Supposons que n ne soit pas premier. Alors on peut écrire $n = pq$ avec $p, q > 1$.

M_p divise M_n mais $M_p > 1$ car $p > 1$ et $M_p < M_n$ car $q > 1$ et donc $p < n$. Ainsi, M_n n'est pas premier.

Partie I

1.
```
est_parfait:=proc(n)
 local somme_div,k:
 somme_div:=1:
 for k from 2 to n do
  if irem(n,k)=0 then somme_div:=somme_div+k fi
 od:
 evalb(somme_div=2*n);
end:
```

2. Si d est un diviseur de n, n/d aussi. Ainsi, les diviseurs vont par deux et on peut les regrouper en ne cherchant que les diviseurs de 1 à $E(\sqrt{n})$.

3. n est premier ssi ses seuls diviseurs sont 1 et n ssi $S(n) = n + 1$.

4. Si a divise p^n alors tout diviseur premier de a est un diviseur premier de p^n donc est égal à p.
   Ainsi, a n'admet que p comme diviseur premier, il est donc de la forme p^k avec $k \leq n$.
   Ainsi, $\mathcal{D}(p^n) = \{p^k, k \in \{0, \ldots, n\}\}$. Donc $S(p^n) = 1 + p + p^2 + \ldots + p^n = \boxed{\dfrac{p^{n+1} - 1}{p - 1}}$.

Partie II

1. f est bien définie car si x divise a et y divise b alors xy divise ab.

2. Si $u|a$ et $v|b$ alors si $d = u \wedge v$, d divise u donc a et d divise v donc b.
   Ainsi, d divise $a \wedge b = 1$ donc $d = 1$. Ainsi, $\boxed{u \wedge v = 1}$.

3. Soient (x, y) et $(z, t) \in \mathcal{D}(a) \times \mathcal{D}(b)$ tels que $f(x, y) = f(z, t)$. Donc $xy = zt$.
   D'après la question précédente, $x \wedge t = 1$. Mais x divise zt donc x divise z.
   Par symétrie des couples (x, y) et (z, t), on a aussi z divise x et donc $z = x$ car on est dans $\mathbb{N}$.
   $x = z$ donne immédiatement $y = t$ et donc $(x, y) = (z, t)$. $\boxed{f \text{ est donc injective}}$.

4. Soit $d \in \mathcal{D}(ab)$. On cherche à écrire $d = xy$ avec x diviseur de a et y diviseur de b.
   Si ceci est possible, comme $a \wedge b = 1$, on aura $x = d \wedge a$.
   Après cette analyse inutile, faisons la synthèse.
   On pose $x = d \wedge a$. x est alors un diviseur de a et de d.
   On peut donc poser y tel que $d = xy$ et z tel que $a = xz$.
   On a alors $y \wedge z = 1$. Il ne reste plus qu'à montrer que y divise b.
   On sait que d divise ab donc xy divise xzb donc y divise zb.
   Mais y et z sont premiers entre eux donc y divise b.
   Résumons : $d = xy$, x est un diviseur de a, y un diviseur de b donc $d = f(x, y)$.
   Ainsi, $\boxed{f \text{ est surjective}}$.

5. $S(a) = \sum_{x \in \mathcal{D}(a)} x$, $S(b) = \sum_{y \in \mathcal{D}(b)} y$ donc $S(a)S(b) = (\sum_{x \in \mathcal{D}(a)} x)(\sum_{y \in \mathcal{D}(b)} y) = \sum_{(x,y) \in \mathcal{D}(a) \times \mathcal{D}(b)} xy$.

   Mais d'après la question précédente, tout diviseur de ab s'écrit de manière unique sous la forme xy avec $(x, y) \in \mathcal{D}(a) \times \mathcal{D}(b)$ donc $S(a)S(b) = \sum_{z \in \mathcal{D}(ab)} z$, c'est-à-dire $\boxed{\text{S(a)S(b)=S(ab)}}$.

6. Ainsi, pour calculer $S(n)$, on peut décomposer n en produit de puissances de nombres premiers $n = p_1^{a_1} \dots p_k^{a_k}$ puis utiliser la question précédente pour avoir $S(n) = S(p_1^{a_1}) \dots S(p_k^{a_k})$ et enfin appliquer la question 4 de la partie 1 pour avoir
$$S(n) = \frac{p_1^{a_1} - 1}{p_1 - 1} \dots \frac{p_k^{a_k} - 1}{p_k - 1}$$
Cependant, cette formule peut être intéressante de manière théorique mais pas de manière effective puisque pour l'appliquer, il faut connaître la décomposition de n en facteurs premiers, ce qui est plus couteux que d'avoir simplement les diviseurs puis de calculer leur somme !

Partie III

1. Notons $q = 2^p - 1$ et $a = 2^{p-1}(2^p - 1)$.
q est impair donc $2^{p-1} \wedge q = 1$ et donc $S(a) = S(2^{p-1}q) = S(2^{p-1})S(q)$.
On utilise la partie 1 qui nous dit que $S(2^{p-1}) = 2^p - 1$ et $S(q) = q + 1$.
Alors $S(a) = (2^p - 1)(q + 1) = (2^p - 1)2^p = 2a$. Donc a est parfait.
De plus, a est pair car $p \geq 2$ car $2^p - 1$ est premier donc $p \neq 1$.
Ainsi, $\boxed{2^{p-1}(2^p - 1) \text{ est un nombre parfait pair}}$ (résultat du à Euclide).

2. Si n n'a aucun facteur premier impair, c'est une puissance de 2 donc il existe $k \in \mathbb{N}$ tel que $n = 2^k$.
Mais alors $S(a) = 2^{k+1} - 1 \neq 2a$. Donc n n'est pas parfait ce qui est contradictoire.
Ainsi, $\boxed{n \text{ a au moins un facteur premier impair}}$.

3. $n = 2^a b$ et b est impair donc $S(n) = S(2^a)S(b)$. Or n est parfait donc $S(2^a)S(b) = 2n$.
Puis $S(2^a) = 2^{a+1} - 1$ donc $(2^{a+1} - 1)S(b) = 2^{a+1}b$.
Ainsi, 2^{a+1} divise $(2^{a+1} - 1)S(b)$ et 2^{a+1} et $2^{a+1} - 1$ sont premiers entre eux donc 2^{a+1} divise $S(b)$.
Ainsi, il existe $c \in \mathbb{N}^*$ ($c \neq 0$ car $S(b) \neq 0$) tel que $\boxed{S(b) = 2^{a+1}c}$.
Il suffit ensuite de reporter dans l'égalité $(2^{a+1} - 1)S(b) = 2^{a+1}b$ pour obtenir $\boxed{b = (2^{a+1} - 1)c}$

4. Des deux égalités précédentes on déduit que $S(b) = b + c$.
Mais $b = (2^{a+1} - 1)c$ et $2^{a+1} - 1 > 1$ car $a \geq 1$ donc c est un diviseur de b distinct de b.
Alors, si $c > 1$, $1, c, b$ sont trois diviseurs distincts de b et donc $S(b) \geq b + c + 1$ ce qui est absurde.
Ainsi, $\boxed{\text{c=1}}$.

5. Comme $S(b) = b + c$, on en déduit que $S(b) = b + 1$ et donc $\boxed{b \text{ est premier}}$ d'après la partie 1.
Ainsi, $2^{a+1} - 1$ est premier. La question préliminaire montre alors que $\boxed{a + 1 \text{ est premier}}$.
Posons $p = a + 1$ qui est donc premier.
On a $a = p - 1$ et $b = 2^{a+1} - 1 = 2^p - 1$ de sorte que $\boxed{n = 2^{p-1}(2^p - 1) \text{ avec } 2^p - 1 \text{ premier}}$ (résultat du à Euler).

6. Il s'agir de chercher les p premiers tels que $2^p - 1$ est premier.
$p = 2$ convient ce qui donne $\boxed{\text{n=6}}$.
$p = 3$ convient ce qui donne $\boxed{\text{n=28}}$.
$p = 5$ convient ce qui donne $\boxed{\text{n=496}}$.
Remarque : ça marche pour $p = 7$ mais pas pour $p = 11$. Les nombres M_n sont les nombres de Mersenne. Ils sont rarement premiers mais permettent de trouver de très grands nombres premiers.

7. On montre qu'un nombre impair ayant au plus deux diviseurs premiers distincts ne peut être parfait :
si n n'a qu'un diviseur premier p, on peut écrire $n = p^k$. Alors $S(n) = \dfrac{p^{k+1} - 1}{p - 1}$.
Si n était parfait, on aurait $\dfrac{p^{k+1} - 1}{p - 1} = 2p^k$ et donc $p^{k+1} = 2p^k - 1$ ce qui est absurde car p divise deux termes de cette égalité mais pas le troisième.
Utilisons un autre argument si n s'écrit $n = p^k q^{k'}$ avec p et q premiers impairs distincts.
On suppose par exemple $p < q$ et on a donc $p \geq 3$ et $q \geq 5$.

Si n était parfait, on aurait $S(p^k q^{k'}) = S(p^k)S(q^{k'}) = (1+p+\ldots+p^k)(1+q+\ldots+q^{k'}) = 2p^k q^{k'}$ d'où

$$(1+\frac{1}{p}+\ldots+\frac{1}{p^k})(1+\frac{1}{q}+\ldots+\frac{1}{q^{k'}}) = 2$$

Mais $p \geq 3$ donc $1+\frac{1}{p}+\ldots+\frac{1}{p^k} \leq 1+\frac{1}{3}+\ldots+\frac{1}{3^k} = \frac{1-(\frac{1}{3})^{k+1}}{1-\frac{1}{3}} \leq \frac{1}{1-\frac{1}{3}} = \frac{3}{2}$.

$q \geq 5$ donc on a de même $1+\frac{1}{q}+\ldots+\frac{1}{q^{k'}} \leq \frac{1}{1-\frac{1}{5}} = \frac{5}{4}$.

Ainsi, $(1+\frac{1}{p}+\ldots+\frac{1}{p^k})(1+\frac{1}{q}+\ldots+\frac{1}{q^{k'}}) \leq \frac{3}{2}\frac{5}{3} = \frac{15}{8} < 2$.

Il y a donc contradiction et n n'est donc pas parfait.

Remarque 1 : avec trois diviseurs, l'utilisation de telles inégalités ne marche plus car

$$\frac{1}{(1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7})} = \frac{35}{16} > 2$$

Remarque 2 : on ne sait pas s'il existe une infinité de nombres de Mersenne premiers (donc de nombres parfaits) et on ne connait aucun nombre parfait impair...