Corrigé du Devoir à la Maison n°5

Partie A.

1. Comme $a-b$ est multiple de lui-même alors : $a \equiv b \ [a-b]$.
   Donc $a^n \equiv b^n \ [a-b]$, et $a-b$ divise $a^n - b^n$.
2. Si m divise n alors il existe un entier k tel que $n = km$.
   Alors $a^n = (a^m)^k$ et $b^n = (b^m)^k$.
   On pose $a' = a^m$ et $b' = b^m$. D'après la question précédente $(a'-b')$ divise $(a'^k - b'^k)$, ce qui montre que $(a^m - b^m)$ divise $(a^n - b^n)$.
3. On suppose que $a \geqslant 2$, $n \geqslant 2$, et $a^n - 1$ est premier.
   D'après la première question $a-1$ divise $a^n - 1$. Comme $a^n - 1$ est premier alors il admet exactement deux diviseurs : 1 et lui-même. Donc $a-1 = 1$ ou $a-1 = a^n - 1$.
   Si $a-1 = a^n - 1$ alors $a = a^n$ puis $n \ln a = \ln a$. Comme $a > 1$ alors $\ln a > 0$ donc $n = 1$. Ceci est une contradiction car n est supposé strictement supérieur à 1.
   Donc $a - 1 = 1$, et ainsi $a = 2$.
   Démontrons maintenant que n est premier.
   Soit m un diviseur de n. Alors d'après la question précédente $a^m - 1$ divise $a^n - 1$. Comme $a^n - 1$ est premier alors $a^m - 1$ est égal à 1 ou à $a^n - 1$.
   Si $a^m - 1 = 1$ alors $2^m = 2$ donc $m = 1$.
   Si $a^m - 1 = a^n - 1$ alors $m = n$ car $\ln a > 0$.
   Finalement si m divise n alors $m = 1$ ou $m = n$, donc n est premier.
   Nous avons démontré que si $a^n - 1$ est premier alors $a = 2$ et n est premier.
4. Les quatre premiers nombres de Mersenne sont obtenus pour $p = 2$, 3, 5 et 7, ce sont :

$$M_2 = 3 \qquad M_3 = 7 \qquad M_5 = 31 \qquad M_7 = 127$$

   Ces quatre entiers sont premiers. Pour le dernier il suffit de vérifier qu'il n'est pas divisible par 2, 3, 5, 7, 11, ni 13.
   Le nombre de Mersenne suivant est $M_{11} = 2\,047$. On vérifie que $2\,047 = 23 \times 89$, donc M_{11} n'est pas premier.
   On a donc bien donné quatre nombres de Mersenne premiers et un nombre de Mersenne non premier.
   On pourrait ajouter que le nombre de Mersenne suivant est $M_{13} = 8\,191$, il est premier.
   On connaît actuellement 52 nombres de Mersenne premiers, dont le plus grand nombre premier connu : $2^{136\,279\,841} - 1$ (12 octobre 2024), il comporte 41 024 320 chiffres.

Partie B.

Dans toute cette partie on appelle diviseur *strict* de n un diviseur de n autre que n.

1. (a) On écrit d'abord une fonction calculant la somme des diviseurs de n.
Il suffit ensuite de tester si cette somme est égale à n.

```
def SommeDiviseurs(n):
    """Calcule la somme des diviseurs stricts de l'entier n."""
    S=0
    for k in range(1, n//2+1):   # Inutile de tester n//2+1 ... n
        if n%k==0:
            S=S+k
    return S

def Parfait(n):
    """Teste si l'entier n est parfait."""
    return n==SommeDiviseurs(n)
```

(b) On écrit un programme comme le suivant :

```
n=1
NNP=0  # Nombre de nombres parfaits obtenus
while NNP<6:
    if Parfait(n):
        NNP=NNP+1
        print(n,'est parfait.')
    n=n+1
```

Les cinq premiers nombres parfaits sont 6, 28, 496, 8 128 et 33 550 336.

2. (a) Soit p un entier. On suppose que M_p est premier, ce qui implique d'après la première partie que p est premier.
Soit $n = 2^{p-1}M_p$. Comme M_p est premier alors cette écriture est la décomposition de n en facteurs premiers. Les diviseurs de n sont donc de la forme $d = 2^k M_p^\ell$ où $k \in \{0, \dots, p-1\}$ et $k \in \{0, 1\}$, et la liste ces diviseurs est :

$$1, \quad 2, \quad 2^2, \dots \quad 2^{p-1}, \qquad M_p, \quad 2M_p, \quad 2^2M_p, \dots \quad 2^{p-1}M_p.$$

Remarquons que le dernier est égal à n, il n'est pas diviseurs stricts de n.
La somme de diviseurs stricts de n est :

$$\sigma = \sum_{k=0}^{p-1} 2^k + \sum_{k=0}^{p-2} 2^k M_p$$

On calcule :

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

Comme $M_p = 2^p - 1$ alors :

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

Ainsi $\sigma = n$, et donc n est parfait.

(b) On sait que M_2, M_3, M_5 et M_7 sont premiers donc $2M_2$, 2^2M_3, 2^4M_5 et 2^6M_7 sont parfaits. On calcule ces nombres, on obtient :

$$2 \times 3 = 6 \qquad 4 \times 7 = 28 \qquad 16 \times 31 = 496 \qquad 64 \times 127 = 8\,128.$$

3. (a) Soit k la valuation 2-adique de m. Alors $m = 2^k u$ où u est impair, c'est le produit des facteurs premiers impairs de m.
Comme m est supposé pair alors $k \geqslant 1$.
Ceci montre bien qu'il existe deux entiers $k \in \mathbb{N}^*$ et $u \in \mathbb{N}$ impair tels que $m = 2^k u$.

(b) On note $d_1, \ldots, d_r$ les diviseurs de u.
Alors les diviseurs de $m = 2^k u$ sont les $2^j d_i$ où $j \in \{0, \ldots, k\}$ et $i \in \{1, \ldots, r\}$.
Les d_i sont supposés distincts, et ils sont impairs car ils divisent u qui est impair. Donc tous les diviseurs ci-dessus sont distincts.
La somme des diviseurs de m, stricts ou non, est : $\displaystyle\sum_{j=0}^{k}\sum_{i=1}^{r} 2^j d_i$
On calcule, sachant que $\sigma = \displaystyle\sum_{i=1}^{r} d_i$:

$$\sum_{j=0}^{k}\sum_{i=1}^{r} 2^j d_i = \left(\sum_{j=0}^{k} 2^j\right)\left(\sum_{i=1}^{r} d_i\right) = \left(2^{k+1}-1\right)\sigma$$

Comme m lui-même a été compté dans la liste de ses diviseurs alors la somme des diviseurs stricts de m est $\left(2^{k+1}-1\right)\sigma - m$.
Or m est supposé parfait donc cette somme est égale à m, et :

$$2m = \left(2^{k+1}-1\right)\sigma.$$

(c) Comme $m = 2^k u$ alors l'égalité démontrée ci-dessus donne : $2^{k+1}u = \left(2^{k+1}-1\right)\sigma$
Celle-ci implique que $2^{k+1}-1$ divise $2^{k+1}u$.
Or $k > 0$ donc 2^{k+1} est pair, puis $2^{k+1}-1$ est impair, et $2^{k+1}-1$ est premier avec 2^{k+1}.
Ainsi $2^{k+1}-1$ divise $2^{k+1}u$ et $2^{k+1}-1$ est premier avec 2^{k+1}, donc d'après le lemme de Gauss $2^{k+1}-1$ divise u.
Ceci montre qu'il existe un entier v tel que $u = (2^{k+1}-1)v$.

(d) Supposons que $v > 1$. Alors 1, v et u sont trois diviseurs distincts de u.

En effet $v \neq 1$ par hypothèse, et comme $k \geqslant 1$ alors $2^{k+1} - 1 \geqslant 3$, donc u est différent de v (car $u = (2^{k+1} - 1)v$).

Or σ est la somme des diviseurs de u. Cette somme contient au moins 1, v et u, donc :

$$\sigma \geqslant 1 + v + u$$

Comme $u = (2^{k+1} - 1)v$ alors $u + v = 2^{k+1}v$ donc :

$$\sigma \geqslant 1 + 2^{k+1}v \qquad \text{puis} \qquad \sigma > 2^{k+1}v$$

On multiplie cette inégalité par $2^{k+1} - 1$ qui est strictement positif, et on utilise les égalités $2m = (2^{k+1} - 1)\sigma$, $u = (2^{k+1} - 1)v$, et $m = 2^k u$:

$$(2^{k+1} - 1)\sigma > (2^{k+1} - 1)2^{k+1}v \qquad \text{donc} \qquad 2m > 2^{k+1}u = 2m$$

On a obtenu $2m > 2m$, ce qui absurde car m est positif.

(e) La contradiction obtenue dans la question précédente montre que $v = 1$.

Alors $u = 2^{k+1} - 1 = M_{k+1}$, et $m = 2^k M_{k+1}$.

De plus l'égalité $2m = (2^{k+1} - 1)\sigma$ montre que $\sigma = 2^{k+1}$.

Or σ est la somme des diviseurs de u. Cette somme contient au moins 1 et u. Comme $1 + u = 1 + (2^{k+1} - 1) = 2^{k+1} = \sigma$, alors elle ne contient aucun autre diviseur.

Ainsi 1 et u sont les seuls diviseurs de u, et donc u est premier.

Or $u = M_{k+1}$. D'après la partie précédente, si M_{k+1} est premier alors $k + 1$ est premier.

Notons $p = k + 1$. Ainsi p est premier et $m = 2^{p-1}M_p$.

On a donc démontré que tout nombre parfait pair est de la forme $2^{p-1}M_p$ où M_p est premier, et donc p est aussi premier.