Devoir à la maison n°5
CORRECTION

Exercice 1 - Nombres parfaits

On note, comme dans le cours, $\mathcal{D}^+(c) = \{h \in \mathbb{N} \mid h|c\}$, l'ensemble des diviseurs positifs de c.

1. Pour tout $(h_1, h_2) \in \mathcal{D}^+(a) \times \mathcal{D}^+(b)$, il existe $k_1, k_2 \in \mathbb{Z}$ tel que $a = k_1 h_1$ et $b = k_2 h_2$.
   Donc $ab = (k_1k_2)(h_1h_2)$, donc $h_1h_2|ab$. Et donc $h_1h_2 \in \mathcal{D}^+(ab)$.
   Réciproquement, considérons $h \in \mathcal{D}(ab)$, un diviseur de ab.
   Notons $\delta_1 = h \wedge a$ et donc il existe $\delta_2 \wedge a = 1$ tel que $\delta_1\delta_2 = h$.
   Puis, $\delta_2|h|ab$, donc $\delta_2|ab$.
   mais $\delta_2 \wedge a = 1$, ainsi $\delta_2|b$.
   Ainsi, pour tout $h \in \mathcal{D}^+(ab)$, $\exists\ (\delta_1, \delta_2) \in \mathcal{D}^+(a) \cap \mathcal{D}^+(b)$ tel que $h = \delta_1\delta_2$.
   Enfin, notons que ce couple est unique. Si $h = \delta_1\delta_2 = \delta_1'\delta_2'$,
   alors $\delta_1'|h$ et $\delta_1'|a$, donc $\delta_1'|\delta_1$;
   alors $\delta_2'|h$ et $\delta_2'|b$, donc $\delta_2'|\delta_2$;
   Et comme $\delta_1\delta_2 = \delta_1'\delta_2'$,
   nécessairement δ_1 et δ_1' sont associées, de même δ_2 et δ_2'.
   Or tous ces nombres sont positifs : donc $\delta_1 = delta_1'$ et $\delta_2 = \delta_2'$ Bilan :

   $$\boxed{\forall\ h \in \mathcal{D}^+(ab), \exists\ !(\delta_1, \delta_2) \in \mathcal{D}^+(a) \cap \mathcal{D}^+(b) \text{ tel que } h = \delta_1\delta_2.}$$

   Et donc

   $$s(ab) = \sum_{h|ab} h = \sum_{\delta_1|a, \delta_2|b} \delta_1\delta_2 = \sum_{\delta_1|a}\left(\delta_1 \sum_{\delta_2|b}\delta_2\right) = \sum_{\delta_1|a}(\delta_1 \times s(b)) = s(b)\sum_{\delta_1|a}\delta_1 = s(b) \times s(a)$$

   $$\boxed{\text{Pour tout } a, b \in \mathbb{N}^*. \text{ Si } a \wedge b = 1, \text{ alors } s(ab) = s(a)s(b).}$$

2. Soit p un nombre premier tel que $M_p = 2^p - 1$ soit premier.
   On pose $N = 2^{p-1}M_p$. Comme M_p est premier, impair, alors $2^{p-1} \wedge M_p = 1$.
   On applique le résultat précédent : $s(N) = s(2^{p-1})s(M_p)$.
   Or M_p est premier donc $h|M_p \iff h = 1$ ou $h = M_p$. Ainsi : $S(M_p) = 1 + M_p = 1 + 2^p - 1 = 2^p$.
   Et les diviseurs de 2^{p-1} sont les 2^k, avec $k \in [\![0, p-1]\!]$, $S(2^{p-1}) = \displaystyle\sum_{k=0}^{p-1} 2^k = \frac{2^p - 1}{2 - 1} \times 1 = 2^p - 1$.
   Donc

   $$\boxed{s(N) = s(2^{p-1})s(M_p) = M_p \times 2^p = 2 \times 2^{p-1}M_p = 2N}$$

3. Réciproquement, soit $N > 0$, un entier pair tel que $s(N) = 2N$ (nombre parfait).
   (a) On écrit $N = 2^r m$ où m est un entier impair et $r \in \mathbb{N}^*$.
   Alors comme $2^r \wedge m = 1$ (sinon m serait pair, car divisible par 2), $s(N) = s(2^r)s(m)$.
   Or, avec le même calcul que la question précédente, on trouve $s(2^r) = 2^{r+1} - 1$.
   Et par ailleurs, N étant parfait : $s(N) = 2N = 2 \times 2^r m$. Ainsi $2^{r+1}m = (2^{r+1} - 1)s(m)$.
   Enfin, comme $2^{r+1} - 1$ est impair, $2^{r+1} \wedge 2^{r+1} - 1 = 1$,
   donc d'après le lemme de Gauss : $2^{r+1} - 1|m$.
   Et il existe $t \in \mathbb{N}$ tel que $m = (2^{r+1} - 1)t$.
   En reprenant l'égalité : $2^{r+1}m = (2^{r+1} - 1)s(m)$, on a $2^{r+1}(2^{r+1} - 1)t = (2^{r+1} - 1)s(m)$.
   C'est-à-dire : $s(m) = 2^{r+1}t$.

   $$\boxed{\text{Il existe un entier } t \text{ tel que } m = (2^{r+1} - 1)t \text{ et } s(m) = 2^{r+1}t.}$$

   (b) Si $t \neq 1$, alors on trouve trois diviseurs distincts de m :
   $1|m$, $t|m$, $(2^{r+1} - 1)t|m$, donc $s(m) \geqslant 1 + t + (2^{r+1} - 1)t = 2^{r+1}t + 1$.
   Ce qui est faux, donc $t = 1$ et ainsi $m = 2^{r+1} - 1$.
   Ensuite, si $\delta|r + 1$, avec $\delta \notin \{-1, 1, -r - 1, r + 1\}$, alors $r + 1 = \delta d$

   $$m = 2^{r+1} - 1 = ((2^d)^\delta - 1^\delta) = (2^d - 1)(\sum_{k=0}^{\delta-1} 2^d k)$$

Et donc $s(m) \geqslant 1+m+(2^d-1) = 1+(2^{r+1}+1)+(2^d-1) > 2^{r+1}$.
Ce qui est faux ; donc $p=r+1$ est premier

$$\boxed{\text{Ainsi } t=1 \text{ et que } p=r+1 \text{ est premier et } m=M_{r+1}=M_p.}$$

(c) Notons que si $m=M_{r+1}$ n'est pas premier, on reprend le même calcul qu'en 2, mais avec d'autres diviseurs à m. Et donc $s(N)>2N$. Impossible, donc m, premier.
Par double implication :

$$\boxed{N \text{ est parfait si et seulement si } N=2^r(2^{r+1}-1) \text{ avec } r+1 \text{ et } 2^{r+1}-1, \text{ nombres premiers}}$$

Exercice 2 - Formule de Legendre

Soient $n \geqslant 1$ et p un nombre premier. On se propose de calculer $m=v_p(n!)$.
On suppose que n s'écrit en base p,

$$n = a_rp^r + a_{r-1}p^{r-1}+\cdots+a_1p+a_0 \qquad a_r\neq 0, \quad a_r, a_{r-1},\ldots a_0 \in \{0,1,\ldots p-1\}$$

1. Soit $k\in\{0,1,\ldots r\}$. Comme pour tout k, $a_k\in\{0,1,\ldots p-1\}$, $p^k \leqslant a_kp^k < p^{k+1}$.
   Puis, pour tout $h\leqslant r$, (télescopage)

$$\sum_{k=0}^{h} a_kp^k \leqslant \sum_{k=0}^{h}(p-1)p^k = \sum_{k=0}^{h} p^{k+1}-p^k = p^{h+1}-1 < p^{h+1}$$

   Donc pour tout $h \leqslant r$,

$$\frac{n}{p^h} = \underbrace{\sum_{k=h}^{r} a_kp^{k-h}}_{\in\mathbb{N}^*} + \underbrace{\frac{\overbrace{\sum_{k=0}^{h-1}a_kp^k}^{<p^h}}{p^h}}_{\in[0,1[} \Longrightarrow \left\lfloor \frac{n}{p^h}\right\rfloor = \sum_{k=h}^{r} a_kp^{k-h}$$

   Donc

$$\boxed{\left\lfloor \frac{n}{p^h}\right\rfloor - p\left\lfloor \frac{n}{p^{h+1}}\right\rfloor = \sum_{k=h}^{r} a_kp^{k-h} - p\sum_{k=h+1}^{r} a_kp^{k-h-1} = \sum_{k=h}^{r} a_kp^{k-h} - \sum_{k=h+1}^{r} a_kp^{k-h} = a_hp^0 = a_h}$$

2. $n! = n(n-1)(n-2)\ldots 2\times 1 = \displaystyle\prod_{k\leqslant n} k$.

Remarques !

Si l'on demande d'étudier les diviseurs de 226! et en particulier de savoir combien sont divisibles par 10, il suffit de compter le nombre de nombres divisibles par 10, il y en a 22 : 10, 20, 30, ...220, mais dans ceux-ci 2 sont divisibles par 100 : 100 et 200.
Si l'on s'intéresse à un nombre N écrit $a_ra_{r-1}\cdots a_0$ en base 10, il y en a $a_ra_{r-1}\cdots a_1$ divisible par 10 et parmi ceux-ci, il y en a $a_ra_{r-1}\cdots a_2$ divisibles par 100 et parmi ceux-ci $a_ra_{r-1}\cdots a_3$ divisibles par 1000. ...
On suit ici la même idée.

On considère donc $n = a_rp^r + a_{r-1}p^{r-1}+\cdots+a_1p+a_0$.
Soit $k\leqslant n$, retrouvé dans le produit $n!$.
On peut supposer que k s'écrit également en base p : $k = b_rp^r+b_{r-1}p^{r-1}+\cdots+b_1p+b_0$.
Pour tout $i\leqslant r$, $p^i|k$ si et seulement si $b_0=b_1=\cdots=b_{i-1}=0$. Ainsi :

$$\begin{aligned} V_i := & \ \{k\leqslant n \text{ tq} p^i|k\} = \{k = b_rp^r+b_{r-1}p^{r-1}+\cdots+b_ip^i \mid k\leqslant n\} \\ = & \ \{p^i(b_rp^{r-i}+b_{r-1}p^{r-1-i}+\cdots+b_i) \mid b_rp^{r-i}+b_{r-1}p^{r-1-i}+\cdots+b_i \leqslant a_rp^{r-i}+a_{r-1}p^{r-1-i}+\cdots+a_i\} \end{aligned}$$

$$\text{card}V_i = \text{card}(\{k\leqslant n \text{ tq } p^i|k\}) = a_rp^{r-i}+a_{r-1}p^{r-1-i}+\cdots+a_i = \left\lfloor\frac{n}{p^i}\right\rfloor$$

d'après un calcul précédent. Puis, on a la somme :

$$\begin{aligned} m &= v_p(n!) = v_p\left(\prod_{k\leqslant n}\right) = \sum_{k\leqslant n} v_p(k) = \sum_{i=0}^{r}\left(\sum_{k \mid v_p(k)=i} i\right) = \sum_{i=0}^{r}\left(\sum_{k\in V_i, k\notin V_{i+1}} i\right) \\ &= \sum_{i=0}^{r}\left(i\sum_{k\in V_i,k\notin V_{i+1}} 1\right) = \sum_{i=0}^{r} i\,(\text{card}V_i - \text{card}V_{i+1}) = \sum_{i=0}^{r} i\text{card}V_i - \sum_{i=0}^{r} i\text{card}V_{i+1} \\ &= \sum_{i=0}^{r} i\text{card}V_i - \sum_{i=1}^{r+1}(i-1)\text{card}V_i = 0 + \sum_{i=1}^{r}[i-(i-1)]\text{card}V_i - 0 = \sum_{i=1}^{r}\text{card}V_i \end{aligned}$$

$$\boxed{m = \sum_{k=1}^{r}\left\lfloor \frac{n}{p^k}\right\rfloor}$$

3. Soit $k \in [\![1, r]\!]$. On a déjà répondu à cette question là :

$$\boxed{\left\lfloor \frac{n}{p^k}\right\rfloor = \sum_{i=k}^{r} a_i p^{i-k}}$$

4. On a alors :

$$\begin{aligned} m &= \sum_{k=1}^{r}\left\lfloor \frac{n}{p^k}\right\rfloor = \sum_{k=1}^{r}\left(\sum_{i=k}^{r} a_i p^{i-k}\right) = \sum_{1\leqslant k\leqslant i\leqslant r} a_i p^{i-k} = \sum_{i=1}^{r}\left(a_i\sum_{k=1}^{i} p^{i-k}\right) \underbrace{=}_{j=i-k} \sum_{i=1}^{r}\left(a_i\sum_{j=0}^{i-1} p^j\right) \\ &= \sum_{i=1}^{r}\left(a_i\frac{p^i-1}{p-1}\right) = \frac{1}{p-1}\left(\sum_{i=1}^{r} a_i p^i - \sum_{i=1}^{r} a_i\right) = \frac{1}{p-1}\left(\left[\sum_{i=1}^{r} a_i p^i + a_0p^0\right] - \left[\sum_{i=1}^{r} a_i + a_0\right]\right) \end{aligned}$$

$$\boxed{m = \frac{n-S}{p-1}, \text{ avec } S := \sum_{k=0}^{r} a_k \qquad\qquad \text{(formule de Legendre)}}$$

5. On a la décomposition de 1000 en base 2 :

$$1\,000 = 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3 = [11\,1110\,1000]_2$$

Et donc $S_2(1\,000) = 6$, et ainsi

$$\boxed{m = \frac{1000-6}{2-1} = 994}$$

Exercice 3

1. Soient $a < b$ et φ dérivable sur $[a, b]$ vérifiant $\varphi(b) > \varphi(a)$.

Piste de recherche...

Selon la remarque (analyse) donnée dans le complément de cours, on a besoin ici d'élaguer l'intervalle $[a, b]$.
Cela nous motive à appliquer le principe de dichotomie selon la seconde façon.
Il faut se débarrasser des intervalles $[c, d]$ où $f(c) > f(a)$ ou $f(d) < f(a)$. Car dans ce cas là, il pourrait ne pas y avoir de solution ℓ à notre problème...

Notons, pour tout $[c, d] \subset [a, b]$, $\mathcal{P}_{[c,d]}$: « $\varphi(c) > \varphi(a)$ ou $\varphi(d) < \varphi(a)$ ».
Alors, pour tout $[c, d], [d, e] \subset [a, b]$,
$\mathcal{P}_{[c,d]}$ et $\mathcal{P}_{[d,e]} \Longrightarrow [\varphi(c) > \varphi(a)$ ou $\varphi(d) < \varphi(a)]$ et $[\varphi(d) > \varphi(a)$ ou $\varphi(e) < \varphi(a)]$.
Alors ou bien $\varphi(c) > \varphi(a)$,
ou bien $\varphi(c) \leqslant \varphi(a)$ et donc nécessairement : $\varphi(d) < \varphi(a)$ puis $\varphi(e) < \varphi(a)$.
Donc $\mathcal{P}_{[c,e]}$ est vraie.
Puis comme $\mathcal{P}_{[a,b]}$ est faux, par hypothèse $\varphi(b) > \varphi(a)$ et $\varphi(a) \leqslant \varphi(a)$,
on peut appliquer le principe de dichotomie :

$$\exists\ (I_n)_{n\in\mathbb{N}} \qquad \text{telle que } \forall\ n \in \mathbb{N}, I_{n+1} \subset I_n\ ;\ \mathcal{P}_{I_n} \text{ faux et } \ell(I_n) \to 0$$

Notons $I_n = [c_n, d_n]$, donc pour tout $n \in \mathbb{N}$, $\varphi(c_n) \leqslant \varphi(a)$ et $\varphi(d_n) \geqslant \varphi(a)$.
Notons $\ell = \bigcap_{n\in\mathbb{N}} I_n$, alors $(c_n) \nearrow\nearrow \ell$ et $(d_n) \searrow\searrow \ell$.
Alors $\ell = \lim(c_n) = \lim(d_n)$ et donc par continuité de φ :

$\varphi(\ell) = \lim \varphi(c_n) \leqslant \varphi(a)$ et $\varphi(\ell) = \lim \varphi(d_n) \geqslant \varphi(a)$. Nécessairement : $\varphi(\ell) = \varphi(a)$.

Puis φ est dérivable donc $\varphi'(\ell) = \lim_{n\to\infty} \dfrac{\varphi(c_n) - \varphi(\ell)}{c_n - \ell}$.

Or $\varphi(c_n) - \varphi(\ell) = \varphi(c_n) - \varphi(a) < 0$ et $c_n - \ell < 0$, donc pour tout $n \in \mathbb{N}$, $\frac{\varphi(c_n)-\varphi(\ell)}{c_n-\ell} \geqslant 0$, et nécessairement : $\varphi'(\ell) \geqslant 0$.

$$\boxed{\text{Il existe au moins un réel } \ell \in [a,b] \text{ vérifiant } \varphi(\ell) = \varphi(a) \text{ et } \varphi'(\ell) \geqslant 0.}$$

2. Soit f une fonction non constantes et dérivable, de dérivée nulle.
   Considérons alors $a < b$ tel que $f(a) \neq f(b)$. On note $m = \dfrac{f(b) - f(a)}{b - a}$.
   Considérons $\varphi : x \mapsto -x + \frac{2}{m} f(x)$.
   Alors $\varphi(b) - \varphi(a) = -b + a + \frac{2}{m}(f(b) - f(a)) = b - a > 0$. Donc $\varphi(b) > \varphi(a)$.
   Et ainsi d'après la question précédente : il existe $\ell \in [a,b]$ tel que $\varphi(\ell) = \varphi(a)$ et $\varphi'(\ell) \geqslant 0$.
   Or pour tout $x \in [a,b]$, $\varphi'(x) = -1 + \frac{2}{m} f'(x) = -1$ car $f' = 0$.
   Donc $\varphi'(\ell) = -1 < 0$. Impossible.
   Réciproquement, si f est constante, f est dérivable de dérivée nulle.

$$\boxed{\text{Donc les fonctions constantes sur un intervalle sont les seules à posséder une fonction dérivée nulle.}}$$

Remarques !

La fonction φ est choisie le plus simple possible pour le calcul de dérivée donc proportionnelle à f. On ajoute une partie affine afin de passer de $f(a)$ à $f(b)$ de manière décroissante...

3. C'est la même stratégie.
   Soit f une fonction dérivable, de dérivée positive ou nulle et non croissantes.
   Considérons alors $a < b$ tel que $f(a) > f(b)$. On note $m = \dfrac{f(b) - f(a)}{b - a} < 0$.
   Considérons $\varphi : x \mapsto -x + \frac{2}{m} f(x)$.
   Alors $\varphi(b) - \varphi(a) = -b + a + \frac{2}{m}(f(b) - f(a)) = b - a > 0$. Donc $\varphi(b) > \varphi(a)$.
   Et ainsi d'après la première question : il existe $\ell \in [a,b]$ tel que $\varphi(\ell) = \varphi(a)$ et $\varphi'(\ell) \geqslant 0$.
   Or pour tout $x \in [a,b]$, $\varphi'(x) = -1 + \frac{2}{m} f'(x)$ car $f' = 0$.
   Donc $\varphi'(\ell) = -1 + \frac{2}{m} f'(\ell) \geqslant 0$. Ainsi $f'(\ell) \leqslant \frac{m}{2} < 0$ (car $m < 0$).
   C'est impossible, car f est dérivée positive ou nulle. Donc nécessairement f est croissante.
   Réciproquement, si f est croissante, f est dérivable de dérivée positive ou nulle.

$$\boxed{\begin{array}{c}\text{Les fonctions croissantes (respectivement décroissantes) sur un intervalle sont les seules}\\ \text{à posséder une fonction dérivée positive ou nulle (resp. négative ou nulle).}\end{array}}$$