Le 17.12.20

Devoir à la maison n°5
CORRECTION

Exercice 1 (n°259)

Pour tout entier n, on note $r(n) = \text{Card}\{(A,B) \in \mathbb{Z}^2 \mid A^2 + B^2 = n\}$.
On pose également $\chi(n) = (-1)^{(n-1)/2}$ si n est impair et $\chi(n) = 0$, sinon.

1. $5 = 2^2 + 1^2$. On ne peut pas chercher avec des nombres de valeurs absolues plus grandes.
   Puis, il y a toutes oppositions/permutations :

$$\boxed{\begin{array}{ll} 5 & = 2^2 + 1^2 = (-2)^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + (-1)^2 = 1^2 + 2^2 \\ & = 1^2 + (-2)^2 = (-1)^2 + 2^2 = (-1)^2 + (-2)^2 \qquad \Longrightarrow r(5) = 8 \end{array}}$$

$$\boxed{2 = 1^2 + 1^2 = (-1)^2 + (1)^2 = 1^2 + (-1)^2 = (-1)^2 + (-1)^2 \qquad \Longrightarrow r(2) = 4}$$

2. Si $n = A^2 + B^2$.
   Alors si $A = 2k$, alors $A^2 = 4k^2 \equiv 0[4]$ et si $A = 2k+1$, alors $A^2 = 4(k^2+k) + 1 \equiv 1[4]$.
   Donc si $r = (A^2 + B^2)\%4$, $r \in \{0, 1, 2\}$.

$$\boxed{\text{Par contraposée : si } n \equiv 3[4], \text{ alors } r(n) = 0.}$$

3. Soit $p \in \mathcal{P}$, un nombre premier tel que $p \equiv 1[4]$. On écrit $p = 4k+1$.
   (a) On rappelle le théorème de Wilson, démontré au DM précédent : $(p-1)! \equiv -1[p]$.

$$(p-1)! = \prod_{i=1}^{4k} i = \left(\prod_{i=1}^{2k} i\right) \times \left(\prod_{j=2k+1}^{4k} j\right)$$

   Dans le second produit, on fait le changement $j = p - i$ pour i de $p - 4k = 4k + 1 - 4k = 1$ à $p - (2k+1) = 2k$.
   Or $j \equiv -i[p]$, dans ce cas :

$$\boxed{(p-1)! \equiv \prod_{i=1}^{2k} i \times (-i) = (-1)^{2k} \left(\prod_{i=1}^{2k} i\right)^2 \qquad [p]}$$

   (b) Comme $(-1)^{2k} = 1$, on a donc (puisque $k = (p-1)/4$) :

$$\boxed{(-1) \equiv X^2[p], \text{ avec } X = \prod_{i=1}^{(p-1)/2} i}$$

   On note x, le reste de la division euclidienne de ce nombre par p.
   Puis on applique l'algorithme d'Euclide à ces nombres p et x. On note $r_0 = p$, $r_1 = x$ et r_{n+2} le reste de la division euclidienne de r_n par r_{n+1}.
   La suite (r_n) est une suite d'entiers naturels strictement décroissante. On note M l'indice tel que : $r_M > \sqrt{p} > r_{M+1}$.
   (c) Au rang $M+1$: $r_{M+1} = u_{M+1}p + v_{M+1}x$.
   On élève au carré :

$$r_{M+1}^2 = p(pu_{M+1}^2 + 2u_{M+1}v_{M+1}x) + v_{M+1}^2 x^2$$

   Et comme $x^2 = -1 + Ap$, on a donc :

$$r_{M+1}^2 + v_{M+1}^2 = p \times \underbrace{\left(pu_{M+1}^2 + 2u_{M+1}v_{M+1}x + Av_{M+1}^2\right)}_{:=K \in \mathbb{Z}} = Kp$$

   Or $0 < r_{M+1} < \sqrt{p}$, donc $r_{M+1}^2 < p$.
   On va démontrer que pour tout $n \in \mathbb{N}$:

$$r_n v_{n-1} - v_n r_{n-1} = (-1)^n p$$

En effet, on sait que pour tout n : $r_n = pu_n + xv_n$, donc pour tout $n \in \mathbb{N}$:

$$r_{n+1}v_n - v_{n+1}r_n = pu_{n+1}v_n + xv_{n+1}v_n - v_{n+1}pu_n - xv_{n+1}v_n = p(u_{n+1}v_n - u_nv_{n+1})$$

Et de même

$$r_nv_{n-1} - v_nr_{n-1} = p(u_nv_{n-1} - u_{n-1}v_n)$$

Alors que

$$u_{n+1}v_n - u_nv_{n+1} = (-q_nu_n + u_{n-1})v_n - (-q_nv_n + v_{n-1})u_n = u_{n-1}v_n - v_{n-1}u_n$$

Donc

$$r_{n+1}v_n - v_{n+1}r_n = (-1)[r_nv_{n-1} - v_nr_{n-1}]$$

La suite $(r_{n+1}v_n - v_{n+1}r_n)_n$ est géométrique de raison (-1) et de premier terme $r_1v_0 - v_1r_0 = x \times 0 - 1 \times p = -p$.
Donc pour tout $n \in \mathbb{N}$,

$$r_nv_{n-1} - v_nr_{n-1} = (-1)^{n-1}(-p) = (-1)^n p$$

L'expérience prouve que pour tout $n \in \mathbb{N}$, v_n est du signe de $(-1)^{n-1}$.
Notons, pour tout n, $x_n = \dfrac{(-1)^{n+1}v_n}{p} > 0$, on a alors

$$r_nx_{n-1} + x_nr_{n-1} = \frac{(-1)^n}{p}[r_nv_{n-1} - r_{n-1}v_n] = 1$$

Et comme x_k et $r_k > 0$, on a donc $0 \leqslant x_nr_{n-1} \leqslant 1$, donc $x_n \leqslant \frac{1}{r_{n-1}}$.
Ainsi,

$$\boxed{\forall\, n \in \mathbb{N}, \qquad |v_n| = px_n < \frac{1}{r_{n-1}}}$$

On a donc

$$v_{M+1}^2 \leqslant \frac{p^2}{r_M^2} < \frac{p^2}{p} = p$$

car $r_M > \sqrt{p}$.
Donc $0 < r_{M+1}^2 + v_{M+1}^2 < 2p$. Le seul nombre divisible par p dans $]0, 2p[$ est p.

$$\boxed{p = r_{M+1}^2 + v_{M+1}^2 \qquad \text{- Algorithme de Serret}}$$

(d) $37 = 4 \times 9 + 1$. On note donc $X = \prod_{i=1}^{18} i[37]$

$$\begin{aligned}
x &\equiv 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \cdots \times 18 \qquad [37] \\
&\equiv \underbrace{2 \times 18}_{\equiv -1} \times \underbrace{3 \times 12}_{\equiv -1} \times \underbrace{4 \times 9}_{\equiv -1} \times \underbrace{5 \times 8}_{\equiv 3} \times \underbrace{6 \times 7}_{\equiv 5} \times 10 \ldots \qquad [37] \\
&\equiv -15 \times \underbrace{10 \times 11}_{\equiv -1} \times 13 \times (2 \times 7) \times (3 \times 5) \times (2 \times 8) \times 17 \qquad [37] \\
&\equiv (3 \times 5) \times \underbrace{3 \times 13}_{\equiv 2} \times \underbrace{7 \times 5}_{\equiv -2} \times \underbrace{2 \times 17}_{\equiv -3} \times 2 \times 8 \qquad [37] \\
&\equiv 2^3 \times 3^2 \times 5 \times 8_{\equiv 3} \equiv 6^2{}_{\equiv -1} \times 6 \equiv -6 \equiv 31 \qquad 31[37]
\end{aligned}$$

(On peut vérifier : $31^2 = 961 = 29 \times 37 - 1$).
Ensuite, on fait l'algorithme d'Euclide à partir de 37 et 31 :

			n	r	u	v
			0	37	1	0
			1	31	0	1
$37 =$	1×31	$+6$	2	6	1	-1
$31 =$	5×6	$+1$	3	1	-5	6

On a ici $\sqrt{37} = 6, \ldots$ donc $r_2 = 6 < \sqrt{37} < r_1$ et donc $M = 1$ et $v_2 = -1$.

$$\boxed{\text{Alors } 37 = r_2^2 + (-1)^2 = 6^2 + 1^2.}$$

(e) Supposons que $p = a^2 + b^2$ (possible d'après la question (c)).
On peut supposer que a, b positifs (sinon, on prend l'opposé) et même $a \geqslant b$.
Si $a = b$, alors $p = 2a^2$ et donc $2|p$, impossible puisque $p \equiv 1[3]$.
Donc $a > b$.
On suppose alors que cette décomposition est unique On trouve 8 décomposition pour p :

$$p = a^2 + b^2 = (-a)^2 + b^2 = a^2 + (-b)^2 = (-a)^2 + (-b)^2$$

et les permutation $a \leftrightarrow b$.

$$\boxed{r(p) = 8}$$

Remarques !
Une démonstration classique de l'unicité consiste à se placer sur $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$.
Montrer qu'on a ainsi un anneau euclidien, donc soumis au même caractéristique que $\mathbb{Z}$ (décomposition unique en facteurs premiers, en considérant comme premier les éléments divisibles uniquement par les associés à p cf DS4 2016-2017).
On a alors si $p = a^2 + b^2 = c^2 + d^2 = (a + ib)(a - ib) = (c + id)(c - id)$
Si $z|a+ib$, alors $N(z) = z\overline{z} \in \mathbb{Z}|N(a+ib) = p$. Mais p est premier dans $\mathbb{Z}$. Donc $N(z) = 1$ ou $N(z) = p$.
Donc $a + ib$ est premier (dans $\mathbb{Z}[i]$), de même de $a - ib$.
Et donc $c + id = \epsilon(a + ib)$ ou $c + id = \epsilon(a - ib)$ car $a + ib$ et $a - ib$ est premier avec ϵ un inversible i.e. $N(\epsilon) = 1$ i.e. $\epsilon \in \{1, -1, i, -i\}$.

On a montré : pour p premier, $r(p) = 0$ si $p \equiv 3[4]$ ou $p = 2$ et $r(p) = 8$ si $p \equiv 1[4]$.

4. Si m ou n est pair, il en est de même de nm et $\chi(nm) = 0 = \chi(n)\chi(m)$
Si m et n sont impair, supposons $n = 2k + 1$ et $m = 2h + 1$, alors $nm = 2(2kh + k + h) + 1$

$$\chi(m)\chi(n) = (-1)^k(-1)^h = (-1)^{k+h} = (-1)^{2kh+k+h} = \chi(mn)$$

$$\boxed{\chi \text{ est complètement multiplicative.}}$$

5. On définit $\delta(n) = \sum_{d|n} \chi(d)$.
• Si $d \equiv 0[2]$, alors $\chi(d) = 0$,
• Si $d \equiv 1[4]$, i.e. $d = 4k + 1$, alors $\chi(d) = (-1)^{4k/2} = 1$
• Si $d \equiv 3[4]$, i.e. $d = 4k + 3$, alors $\chi(d) = (-1)^{(4k+2)/2} = -1$
Enfin, $\{d|n\} = \{d|n, d \equiv 0[2]\} \uplus \{d|n, d \equiv 1[4]\} \uplus \{d|n, d \equiv 3[4]\}$.
On peut sommer par paquets :

$$\boxed{\delta(n) = \sum_{\substack{d|n \\ d\equiv 0[2]}} \chi(d) + \sum_{\substack{d|n \\ d\equiv 1[4]}} \chi(d) + \sum_{\substack{d|n \\ d\equiv 3[4]}} \chi(d) = \sum_{\substack{d|n \\ d\equiv 1[4]}} 1 - \sum_{\substack{d|n \\ d\equiv 3[4]}} 1}$$

6. • Soit $n = 2^\alpha q$ avec q impair.
Les diviseurs non pairs de n sont exactement les diviseurs de q. Donc

$$d|n \text{ et } d \not\equiv 0[2] \iff d|q \text{ et } d \not\equiv 0[2]$$

Ainsi $\delta(n) = \sum_{\substack{d|n \\ d\equiv 1[4]}} 1 - \sum_{\substack{d|n \\ d\equiv 3[4]}} 1 = \sum_{\substack{d|q \\ d\equiv 1[4]}} 1 - \sum_{\substack{d|q \\ d\equiv 3[4]}} 1 = \delta(q)$.
Et notons que $\delta(1) = 1$
• Ensuite, on remarque que $\delta = \chi * 1$, donc comme χ et 1 sont multiplicatives, δ est également multiplicative.
• Si $p \equiv 3 \equiv -1[4]$ alors $p^2 \equiv 1[4]$.
Ainsi (par récurrence), $p^a \equiv (-1)^a[4]$,

$$\delta(p^\alpha) = \sum_{k=0}^{\alpha} \chi(p^k) = \sum_{k=0}^{\alpha} (-1)^k = \frac{1 - (-1)^{a+1}}{1 - (-1)} = \begin{cases} 0 & \text{si } a \text{ impair} \\ 1 & \text{si } a \text{ pair} \end{cases}$$

• Si $p \equiv 1[4]$, alors pour tout $a \in \mathbb{N}$ (récurrence), $p^a \equiv 1[4]$.

$$\delta(p^\alpha) = \sum_{k=0}^{\alpha} \chi(p^k) = \sum_{k=0}^{\alpha} 1 = \alpha + 1$$

En exploitant la multiplicativité de δ, pour $n = 2^{v_2(n)} \prod_{p\in\mathcal{P}\setminus\{2\}} p^{v_p(n)}$:

$$\delta(n) = \prod_{p\in\mathcal{P}\setminus\{2\}} \delta(p^{v_p(n)}) = \begin{cases} 0 & \text{si } \exists\ p \in \mathcal{P}, p \equiv 3[4] \text{ tel que } v_p(n) \equiv 1[2] \\ \sum_{p\in\mathcal{P}\&p\equiv 1[4]} (v_p(n)+1) & \text{si } \forall\ p \in \mathcal{P}, p \equiv 3[4] \text{ tel que } v_p(n) \equiv 0[2] \\ 1 & \text{si } n = 2^r \end{cases}$$

Ensuite, pour montrer l'égalité entre r et δ, on va montrer que r est également complément multiplicative comme δ et ont même image sur les nombres premiers.

• On a vu que si $p \in \mathcal{P}$,

$$r(p) = \begin{cases} 4 & \text{si } p = 2 \\ 0 & \text{si } p \equiv 3[4] \\ 8 & \text{si } p \equiv 1[4] \end{cases} = 4 \times \begin{cases} 1 & \text{si } p = 2 \\ 0 & \text{si } p \equiv 3[4] \\ 2 & \text{si } p \equiv 1[4] \end{cases} = 4\delta(p)$$

• On suppose que $n = a^2 + b^2$ $(a \geqslant b \geqslant 0)$ et $m = c^2 + d^2$ $(c \geqslant d \geqslant 0)$.
Alors, d'après l'identité de Lagrange (classique) :

$$nm = (a+ib)(a-ib)(c+id)(c-id) = \begin{cases} (a+ib)(c+id) \times (a-ib)(c-id) = (ac-bd)^2 + (ad+bc)^2 \\ \text{ou} \\ (a+ib)(c-id) \times (a-ib)(c+id) = (ac+bd)^2 + (-ad+bc)^2 \end{cases}$$

On se souvient qu'en fait si $a > b$, on a

$$n = a^2+b^2 = (-a)^2+b^2 = a^2+(-b)^2 = (-a)^2+(-b)^2 = b^2+a^2 = (-b)^2+a^2 = b^2+(-a)^2 = (-b)^2+(-a)^2$$

Alors, $(ac+bd)^2 + (-ad+bc)^2$ correspond au cas $(a'c-b'd)^2 + (a'd+b'c)^2$ avec $a' = -a$ et $b' = b$.
Donc pour chaque décomposition (à multiplier par 8 si $a > b$ ou 4 si $a = b$) de n et de m, on trouve une nouvelle décomposition de nm en somme de carrés.
Il est vrai qu'il n'y en a pas d'autres, mais ce n'est pas facile à montrer (cf DS 4 - 2015-2016)

Donc $r(nm) = r(n) \times r(m)$.
Finalement r et 4δ ont même expressions sur les nombres premiers, toutes les deux sont complètement multiplicatives.

$\forall\ n = 2^{v_2(n)} \prod_{p\in\mathcal{P}\setminus\{2\}} p^{v_p(n)} \in \mathbb{N}$,

$$\begin{aligned} r(n) &= 4\delta(n) = 4 \prod_{p\in\mathcal{P}\setminus\{2\}} \delta(p^{v_p(n)}) \\ &= \begin{cases} 0 & \text{si } \exists\ p \in \mathcal{P}, p \equiv 3[4] \text{ tel que } v_p(n) \equiv 1[2] \\ \sum_{p\in\mathcal{P}\&p\equiv 1[4]} (v_p(n)+1) & \text{si } \forall\ p \in \mathcal{P}, p \equiv 3[4] \text{ tel que } v_p(n) \equiv 0[2] \\ 1 & \text{si } n = 2^r \end{cases} \end{aligned}$$

Exercice 2 (n°230)

On dit qu'un groupe $(G, \star)$ opère sur un ensemble X, s'il existe une application $G \times X \to X$ $(s, x) \mapsto s \cdot x$ (ou une loi externe) vérifiant :

— $\forall\, s, t \in G,\ \forall\, x \in X,\ s \cdot (t \cdot x) = (s \star t) \cdot x$

— $\forall\, x \in X,\ e \cdot x = x$.

Enfin, pour tout $x \in X$, on note $O(x) = \{s \cdot x, s \in G\}$ (orbite ou trajectoire de x sous l'action de G).

1. Considérons l'application $S_n \times \mathbb{N}_n \to \mathbb{N}_n$, $(\varphi, k) \mapsto \varphi \cdot k = \varphi(k)$.
   Dans ce cas $(S_n, \circ)$ opère sur $\mathbb{N}_n$:
   — $\forall\, \varphi, \psi \in S_n,\ \forall\, k \in \mathbb{N}_n,\ \varphi \cdot (\psi \cdot k) = \varphi \cdot (\psi(k)) = \varphi(\psi(k)) = (\varphi \circ \psi) \cdot k$.
   — $\forall\, k \in \mathbb{N}_n,\ \mathrm{id} \cdot k = \mathrm{id}(k) = k$

   $\boxed{(S_n, \circ) \text{ opère (simplement = naturellement = canoniquement) sur } X = \mathbb{N}_n.}$

2. On note, pour tout $x \in X$, $S_x = \{s \in G \mid s \cdot x = x\}$ (stabilisateur de x).
   Soit $x \in X$. $S_x \subset G$.
   — $e \cdot x = x$, donc $e \in S_x$ et donc $S_x \neq \emptyset$.
   — Soient $s_1, s_2 \in S_x$. Alors

   $$(s_1 \star s_2) \cdot x = s_1 \cdot (\underbrace{s_2 \cdot x}_{=x\ -\ s_2 \in S_x}) = \underbrace{s_1 \cdot x}_{=x\ -\ s_1 \in S_x} = x$$

   Donc $s_1 \star s_2 \in S_x$.
   — Soit $s \in S_x$. Alors

   $$s^{-1} \cdot x = s^{-1} \cdot (s \cdot x) = (s^{-1} \star s) \cdot x = e \cdot x = x$$

   Donc $s^{-1} \in S_x$.
   Donc S_x est un sous-groupe de G.

   $\boxed{\text{Pour tout } x \in X,\ S_x \text{ est un sous-groupe de } G.}$

3. On suppose que G est fini. Soit $x \in X$.
   On considère la relation sur G $s \mathcal{R}_1 s' \iff s \cdot x = s' \cdot x$.
   Il n'est pas compliqué de voir qu'il s'agit d'une relation d'équivalence.
   Les classes d'équivalences forment une partition de G.
   Si $\mathcal{G}$ est un système de représentant des classes :

   $$G = \biguplus_{s \in \mathcal{G}} \overline{s}$$

   $\overline{e} = \{g \in G \mid g \cdot x = e \cdot x = x\} = S_x$.
   Par ailleurs, si $s \in \mathcal{G}$, un représentant d'une classes quelconque,
   Soit $\psi_s : S_x \to \overline{s}$, $g \mapsto s \star g$ est une bijection de S_x sur $\overline{s}$.
   En effet, pour tout $g \in S_x$, $(s \star g) \cdot x = s \cdot g \cdot x = s \cdot x$, donc $s \star g \mathcal{R}_1 s$.
   Donc $\psi_s(g) \in \overline{s}$. L'application réciproque est $\psi_{s^{-1}}$,

   $$\psi_{s^{-1}}(g) \cdot x = s^{-1} \cdot (g \cdot x) \underbrace{=}_{g \in \overline{s}} s^{-1} \cdot (s \cdot x) = (s^{-1} \star s) \cdot x = x$$

   Donc toutes les classes d'équivalence ont le même cardinal : $\mathrm{card}(S_x)$.
   Enfin, il existe une bijection de $\mathcal{G} \to \mathcal{O}(x)$, c'est l'application $s \mapsto s \cdot x$.

   $$\mathrm{card}(G) = \sum_{s \in \mathcal{G}} \mathrm{card}(\overline{s}) = \sum_{s \in \mathcal{G}} \mathrm{card}(S_x) = \mathrm{card}(S_x) \sum_{s \in \mathcal{G}} 1 = \mathrm{card}(S_x) \times \mathrm{card}(\mathcal{G})$$

   $\boxed{\mathrm{card}(G) = \mathrm{card}(S_x) \times \mathrm{card}(\mathcal{O}(x)) \quad \text{Formule des classes}}$

4. On suppose que G et X sont finis.
   On suppose que $X = \{x_1, \dots x_H\}$. Les orbites sont de les ensembles $\mathcal{O}(x_i)$, mais certains sont en double.
   En effet si $x_j \in \mathcal{O}(x_i)$, alors il existe $s \in G$ tel que $s \cdot x_i = x_j$ et donc $x_i = s^{-1} \cdots x_j$.
   Et par transitivité, tout élément $t \cdot x_j$ de $\mathcal{O}(x_j)$ est $(t \star s) \cdot x_i$ un élément de $\mathcal{O}(x_i)$.
   Finalement (double inclusion) : $\mathcal{O}(x_i) = \mathcal{O}(x_j)$.
   Donc l'ensembles des orbites forment une partition X. Si Θ est un système de représentant :

   $$X = \biguplus_{x \in \Theta} \mathcal{O}(x)$$

   Ainsi, en prenant les cardinaux :

   $$\boxed{\mathrm{card}(X) = \sum_{x \in \Theta} \mathrm{card}(\mathcal{O}(x)) = \mathrm{card}(G) \sum_{x \in \Theta} \frac{1}{\mathrm{card}(S_x)}}$$

   Θ *est un système de représentant*

Remarques !
En fait, on pourrait faire le parallèle entre cette démonstration et l'exploitation de la relation sur X :
$x\mathcal{R}_2 x' \iff \exists\ g \in G$ tel que $g \cdot x = x'$

5. Application. On note $\varphi : G \times G,\ (g,x) \mapsto g \cdot x := g \star x \star g^{-1}$.
Il s'agit d'une action de G sur $X = G$.
— $\forall\ s,t \in G,\ \forall\ x \in G,\ (s \star t) \cdot x = (s \star t) \star x (s \star t)^{-1} = stxt^{-1}s^{-1} = s \cdot (t \cdot x)$.
— $\forall\ x \in G,\ e \cdot x = e \star x \star e^{-1} = x$.

Donc G opère sur lui même par φ (on parle des automorphismes intérieurs)

Pour tout $g \in Z(G)$, comme g commute avec tout s :

$$S_g = \{s \in G \mid s \cdot g = g\} = \{s \in G \mid sgs^{-1} = g\} = \{s \in G \mid gss^{-1} = g\} = G$$

Alors que

$$\mathcal{O}(g) = \{s \cdot g; s \in G\} = \{sgs^{-1}; s \in G\} = \{gss^{-1} = g; s \in G\} = \{g\}$$

Donc $g \in \Theta$ et donc Θ contient tous les éléments de $Z(G)$.
On note Θ' tel que $Z(G) \uplus \Theta' = \Theta$ (Θ' comme Θ sont finis).

$$\sum_{g\in\Theta} \frac{\operatorname{card}(G)}{\operatorname{card}(S_g)} = \sum_{g\in Z(G)} \frac{\operatorname{card}(G)}{\operatorname{card}(S_g)} + \sum_{g\in\Theta'} \frac{\operatorname{card}(G)}{\operatorname{card}(S_g)} = \sum_{g\in Z(G)} \frac{\operatorname{card}(G)}{\operatorname{card}(G)} + \sum_{g\in\Theta'} \frac{\operatorname{card}(G)}{\operatorname{card}(S_g)} = \sum_{g\in Z(G)} 1 + \sum_{g\in\Theta'} \frac{\operatorname{card}(G)}{\operatorname{card}(S_g)}$$

$$\operatorname{card}(X) = \operatorname{card}(G) = \operatorname{card}(Z(G)) + \sum_{g\in\Theta'} \frac{\operatorname{card}(G)}{\operatorname{card}(S_g)}$$

On s'intéresse maintenant au $g \in \Theta'$.
S_g est un sous-groupe de G :
— $e \in S_g$ car $e \cdot g = g$. Donc S_g est non vide.
— Soient $s,t \in S_g$, $(s \star t) \cdot g = s \cdot (t \cdot g) = s \cdot g = g$;
donc $s \star t \in S_g$
— Soit $s \in S_g$, $s^{-1} \cdot g = s^{-1} \star g \star s$.
Or $s \star g \star s^{-1} = g$, donc en multipliant à gauche par s^{-1} et par s à droite : $g = s^{-1} \cdot g \cdot s$.
Donc $s^{-1} \in S_{g_i}$.
On peut donc associé pour tout $i \in I = \mathbb{N}_{\operatorname{card}(\Theta')}$, et $g_i \in \Theta'$, le groupe $H_i = S_g$.
Enfin, notons que $g_i \in H_i$: $g_i \cdot g_i = g_i \star g_i \star g_i^{-1} = g_i$, donc $H_i \neq \{e\}$
et $H_i = G$ signifie que pour tout $s \in G$, $s \star g_i s^{-1} = g_i$, donc $s \star g_i = g_i \star s$ donc $g_i \in Z(G)$.

Ainsi, il existe une famille (H_i) de sous-groupe de G, différents de G et $\{e\}$ telle que :

$$\operatorname{Card}(G) = \operatorname{Card}\big(Z(G)\big) + \sum_{i\in I} \frac{\operatorname{Card}(G)}{\operatorname{Card}(H_i)}$$