Sur une identité de Liouville généralisant la relation $1^3+2^3+\ldots+n^3= (1+2+\ldots+n)^2$

Notations

Pour n et p dans N^*, on pose $S_{n,p} = 1^p + 2^p + \ldots + n^p$.

Pour a dans N^*, on note $D(a)$ l'ensemble des diviseurs de a, et $d(a)$ **le nombre de diviseurs de** a.
Pour a et b dans Z avec $a \neq 0$, a divise b sera noté $a|b$.

1) $S_{n,1} = \dfrac{n(n+1)}{2}$; $S_{n,2} = \dfrac{n(n+1)(2n+1)}{6}$; $S_{n,3} = \dfrac{n^2(n+1)^2}{4}$ et donc $S_{n,3} = (S_{n,1})^2$

preuve :

Ces trois relations peuvent se montrer par récurrence sans difficulté.
Mais voici une méthode qui permet de calculer de proche en proche tous les $S_{n,p}$.

Calcul de $S_{n,1}$.

$(n+1)^2 = n^2 + 2n + 1$: on écrit cette égalité pour $n = 1, 2, \ldots n$ et on ajoute membres à membres les n égalités obtenues.

On obtient $(n+1)^2 = 1 + 2S_{n,1} + n$, soit $S_{n,1} = \dfrac{n(n+1)}{2}$.

Note : dans ce cas il existe une méthode astucieuse (due à Gauss?) qui consiste à ajouter membres à membres les deux égalités suivantes :

$S_{n,1} = 1 + 2 + 3 + \ldots\ldots\ldots\ldots\ldots\ldots + (n-2) + (n-1) + n$

$S_{n,1} = n + (n-1) + (n-2) + \ldots\ldots + 3 + 2 + 1,$

et on obtient $2S_{n,1} = (n+1) + (n+1) + (n+1) + \ldots + (n+1) + (n+1) + (n+1) = n(n+1)$

Calcul de $S_{n,2}$.

$(n+1)^3 = n^3 + 3n^2 + 3n + 1$: on écrit cette égalité pour $n = 1, 2, \ldots n$ et on ajoute membres à membres les n égalités obtenues.

On obtient $(n+1)^3 = 1 + 3S_{n,2} + 3S_{n,1} + n$,

soit $3S_{n,2} = (n+1)^3 - 3\dfrac{n(n+1)}{2} - (n+1) = (n+1)\dfrac{2n^2+4n+2-3n-2}{2} = \dfrac{(n+1)(2n^2+n)}{2}$

et $S_{n,2} = \dfrac{n(n+1)(2n+1)}{6}$

Calcul de $S_{n,3}$.

$(n+1)^4 = n^4 + 4n^3 + 6n^2 + 4n + 1$: on écrit cette égalité pour $n = 1, 2, \ldots n$ et on ajoute membre à membre les n égalités obtenues.

On obtient $(n+1)^4 = 1 + 4S_{n,3} + 6S_{n,2} + 4S_{n,1} + n$,

soit $4S_{n,3} = (n+1)((n+1)^3 - n(2n+1) - 2n - 1) = (n+1)(n^3+n^2)$

et $S_{n,3} = \dfrac{n^2(n+1)^2}{4}$ ■

2)

2.1) j étant un entier naturel, p un nombre premier, les diviseurs de p^j sont $1, p, p^2, \ldots, p^j$, donc le nombre de ses diviseurs est $d(p^j) = j+1$.

2.2) Si a et b sont deux entiers naturels non nuls, premiers entre eux, alors $c|ab \Leftrightarrow c = \alpha\beta$ avec $\alpha|a$ et $\beta|b$

2.3) L'application d de N^* dans N^* est **multiplicative**, cad si a et b sont premiers entre eux, $d(ab) = d(a)d(b)$,
ce qui implique que si $e_1, e_2, \ldots, e_k$ sont des entiers premiers entre eux deux à deux, $d(\prod e_i) = \prod d(e_i)$,
en particulier si $p_1, p_2, \ldots, p_k$ sont des nombres premiers distincts deux à deux, $d(\prod p_i^{n_i}) = \prod(n_i+1)$, avec $n_i \geq 1$.

preuve :

2.1 évident

2.2 il y a juste à montrer que $c|ab \Rightarrow c = \alpha\beta$ avec $\alpha|a$ et $\beta|b$ (l'autre sens étant évident).

Soient $a = \prod p_i^{n_i}$ et $b = \prod q_i^{m_i}$ les décompositions en nombre premiers de a et b : pour tout i et tout j on a $p_i \neq q_j$ puisque a et b sont premiers entre eux.

Si c divise ab, $ab = cq$: donc la décomposition en nombres premiers de c est $\prod p_i^{n'_i} \prod q_i^{m'_i}$ avec $n'_i \leq n_i$ et $m'_i \leq m_i$.
Cad $c = \alpha\beta$ avec $\alpha = \prod p_i^{n'_i} | a$ et $\beta = \prod q_i^{m'_i} | b$.
2.3 cf ce qui vient d'être montré, $d(ab)$ est le nombre de couples (α, β) tels que α divise a et β divise b, soit $d(ab) = d(a)d(b)$.
Maintenant si $e_1,\ e_2,\ ...,\ e_k$ sont des entiers premiers entre eux deux à deux,
$d(e_1e_2) = d(e_1)d(e_2)$ puisque e_1 et e_2 sont premiers entre eux.
Ensuite, pour $k \geq 3$, on remarque que pour tout $i \in \{2; 3; \ldots; k-1\}$, $\mathrm{pgcd}(e_1e_2\ldots e_i, e_{i+1}) = 1$
(cela se prouve facilement via Bezout : pour $j \in \{1; 2; \ldots; i\}$ il existe des entiers u_j, v_j tels que $u_je_j + v_je_{i+1} = 1$, ce qui donne par multiplication membres à membres de ces i égalités, l'existence d'entiers u et v tels que $ue_1e_2\ldots e_j + ve_{j+1} = 1$)
Donc
e_1e_2 et e_3 sont premiers entre eux et $d(e_1e_2e_3) = d(e_1e_2)d(e_3) = d(e_1)d(e_2)d(e_3)$,
$e_1e_2e_3$ et e_4 sont premiers entre eux et $d(e_1e_2e_3e_4) = d(e_1e_2e_3)d(e_4) = d(e_1)d(e_2)d(e_3)d(e_4)$,
Etc ■

3) La relation $S_{n,3} = (S_{n,1})^2$ revient à dire , en posant $e = p^{n-1}$, avec p nombre premier quelconque, que $\sum\limits_{c|e}(d(c))^3 = (\sum\limits_{c|e} d(c))^2$, leur valeur commune étant $S_{n,3} = (S_{n,1})^2$.
C'est ce aspect que qui va se généraliser à tout entier naturel e non nul.

preuve :
cf le 2.1), les diviseurs de e sont $1, p, p^2, \ldots, p^{n-1}$, donc
$\sum\limits_{c|e}(d(c))^3 = \sum\limits_{j=0}^{n-1}(d(p^j))^3$, soit, toujours cf le 2.1), $\sum\limits_{c|e}(d(c))^3 = \sum\limits_{j=0}^{n-1}(j+1)^3 = S_{n,3}$,
et, pour les mêmes raisons, $(\sum\limits_{c|e} d(c))^2 = (\sum\limits_{j=0}^{n-1} d(p^j))^2 = (\sum\limits_{j=0}^{n-1}(j+1))^2 = (S_{n,1})^2$,
d'où le résultat cf le **1)** ■

4) Pour tout réel r, les applications de N^* dans N^*
$f : n \longrightarrow \sum\limits_{c|n}(d(c))^r$ et $g : n \to (\sum\limits_{c|n} d(c))^r$
sont multiplicatives,
cad, si e et e' sont premiers entre eux, $f(ee') = f(e)f(e')$ et $g(ee') = g(e)g(e')$
Donc, si $e_1,\ e_2,\ ...,\ e_k$ sont premiers entre eux deux à deux, $f(\prod\limits_i e_i) = \prod\limits_i f(e_i)$ et $g(\prod\limits_i e_i) = \prod\limits_i g(e_i)$.

Note : si $r = 0$, $f(n) = d(n)$ et $g(n) = 1$.

preuve :
tout d'abord un "petit" lemme évident :
f et g étant deux fonctions à valeurs dans R et définies respectivement sur A et B (ensembles **finis**),
$\sum\limits_{(\alpha,\beta)\epsilon A\times B} f(\alpha)g(\beta) = (\sum\limits_{\alpha\epsilon A} f(\alpha))(\sum\limits_{\beta\epsilon B} g(\beta))$
Prouvons maintenant que f est effectivement multiplicative.
$f(ee') = \sum\limits_{c|ee'}(d(c))^r = \sum\limits_{(\alpha,\beta)\epsilon D(e)\times D(e')}(d(\alpha\beta))^r$, cf le 2.2),
$f(ee') = \sum\limits_{(\alpha,\beta)\epsilon D(e)\times D(e')}(d(\alpha))^r(d(\beta))^r$, cf le 2.3), puisque e et e' sont supposés premiers entre eux,
et $f(ee') = \sum\limits_{\alpha\epsilon D(e)}(d(\alpha))^r \sum\limits_{\beta\epsilon D(e')}(d(\beta))^r$, cf le lemme ci-dessus.
Ce qui donne $f(ee') = f(e)f(e')$.
Pour $f(\prod\limits_i e_i) = \prod\limits_i f(e_i)$, voir la preuve du 2.3).
Pour g, les justifications sont identiques ■

5)

Identité de Liouville : pour tout entier naturel n non nul, $\sum_{c|n}(d(c))^3 = (\sum_{c|n} d(c))^2$

Cette identité de Liouville généralise $S_{n,3} = (S_{n,1})^2$ car, cf le 3), si on remplace n par p^{n-1} (avec p premier, $n \geq 1$) on obtient $S_{n,3} = (S_{n,1})^2$.

On obtient d'autres types d'exemples pour des entiers n qui ne sont pas des puissances d'un seul nombre premier.
Par exemple, p et q étant deux nombres premiers distincts,
$n = pq$ donne $1^3 + 2^3 + 2^3 + 4^3 = (1+2+2+4)^2$, les quatre diviseurs de pq étant $1, p, q, pq$
$n = p^2q$ donne $1^3 + 2^3 + 3^3 + 2^3 + 4^3 + 6^3 = (1+2+3+2+4+6)^2$, les six diviseurs de p^2q étant $1, p, p^2, q, pq, p^2q$
$n = p^2q^2$ donne $1^3 + 2^3 + 3^3 + 2^3 + 4^3 + 6^3 + 3^3 + 6^3 + 9^3 = (1+2+3+2+4+6+3+6+9)^2$,
les neuf diviseurs de p^2q^2 étant $1, p, p^2, q, pq, p^2q, q^2, pq^2, p^2q^2$.

preuve :
on note $f(n) = \sum_{c|n}(d(c))^3$ et $g(n) = (\sum_{c|n} d(c))^2$: cf le **4**) ces deux applications sont multiplicatives.
La décomposition en nombres premiers de n s'écrit $n = \prod_i p_i^{n_i}$ et on note $e_i = p_i^{n_i}$.
Les e_i étant premiers entre eux deux à deux le 4) donne tout de suite $f(\prod_i e_i) = \prod_i f(e_i)$ et $g(\prod_i e_i) = \prod_i g(e_i)$.
Mais cf le **3**), pour tout i, on a $f(e_i) = g(e_i)$, et donc $f(n) = g(n)$ ■

6)

6.1) Une question : peut-on trouver des relations $\sum_{i=1}^{k} \alpha_i^3 = (\sum_{i=1}^{k} \alpha_i)^2$, avec k dans N^* et α_i dans N^* qui ne s'obtiennent pas via l'identité ci-dessus de Liouville, cad k n'est pas le nombre de diviseurs d'un entier n ou bien k est le nombre de diviseurs d'un entier n dont les diviseurs $c_1, c_2, \ldots, c_k$ ne sont pas tels que $d(c_1), d(c_2), \ldots, d(c_k)$ soit une permutation de $\alpha_1, \alpha_2, \ldots, \alpha_k$?
Evidemment si $k = 1$, la seule possibilité est $\alpha_1 = 1$ qui s'obtient avec Liouville ($n = 1$), mais si $k \geqslant 2$, il existe une possibilité qui ne provient pas de Liouville : c'est la relation $\sum_{i=1}^{k} k^3 = (\sum_{i=1}^{k} k)^2$.
En effet, cette relation vraie pour tout entier $k \geq 1$, ($k \times k^3 = (k \times k)^2$), ne peut provenir de Liouville pour $k \geq 2$, puisqu'il faudrait trouver n non nul ayant exactement k diviseurs tels que chacun de ces k diviseurs ait $k \geqslant 2$ diviseurs, ce qui est impossible, 1 étant un diviseur de n et ayant un seul diviseur.
Mais est-ce la seule relation qui ne provient pas de Liouville?

6.2) La réponse est oui pour $k = 2$ et $k = 3$, mais pour $k > 3$, je n'ai pas trouvé la réponse :
6.2.1 : les seuls couples d'entiers naturels (α, β) tels que $0 < \alpha \leqslant \beta$ et vérifiant $\alpha^3 + \beta^3 = (\alpha + \beta)^2$ sont $(1,2)$ et $(2,2)$, le premier couple venant de Liouville, pas le deuxième.
6.2.2 : les seuls couples d'entiers naturels (α, β, γ) tels que $0 < \alpha \leqslant \beta \leqslant \gamma$ et vérifiant $\alpha^3 + \beta^3 + \gamma^3 = (\alpha + \beta + \gamma)^2$ sont $(1,2,3)$ et $(3,3,3)$, le premier couple venant de Liouville, pas le deuxième.
6.2.3 : pour $k \geqslant 2$, notons E_k les k-uplets d'entiers naturels $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ tels que $1 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_k$ et $\sum_{i=1}^{k} \alpha_i^3 = (\sum_{i=1}^{k} \alpha_i)^2$

E_k contient le k-uplet $(1, 2, \ldots, k)$ provenant de Liouville : si k est premier, c'est le seul k-uplet de E_k provenant de Liouville.

Mais si k n'est pas premier, E_k contient d'autres triplets provenant de Liouville, par exemple :
si $k = 4$: $(1,2,2,4)$
si $k = 8$: $(1,2,2,3,4,4,6,8)$ et $(1,2,2,2,4,4,4,8)$.

E_k contient le k-uplet $(k, k, \ldots, k)$ ne provenant pas de Liouville.

Pour tout élément de E_k provenant de Liouville, $\alpha_k = k$.

Pour tout élément de E_k, $\alpha_k \leqslant k^2 - 1$.

preuve :

6.2.1

$1 \leqslant \alpha \leq \beta$ et $\alpha^3 + \beta^3 = (\alpha + \beta)^2$

La relation $\alpha^3 + \beta^3 = (\alpha + \beta)^2$ s'écrit $(\alpha + \beta)(\alpha^2 - \alpha\beta + \beta^2) = (\alpha + \beta)^2$ et se simplifie par $\alpha + \beta,$ ce qui donne

$\alpha^2 + \beta^2 - \alpha\beta - \alpha - \beta = 0 \Leftrightarrow (\alpha - \dfrac{\beta + 1}{2})^2 + \dfrac{3(\beta - 1)^2 - 4}{4} = 0.$

Or pour $\beta \geq 3,\ 3(\beta - 1)^2 - 4 > 0,$ donc nécessairement $\beta = 1$ ou 2.

Si $\beta = 1$ on obtient $\alpha = 0$ ou 2 donc cette valeur de β ne convient pas (cf $0 < \alpha \leq \beta$).

Mais $\beta = 2$ donne $\alpha = 1$ ou 2, et les couples $(1,2)$ et $(2,2)$ conviennent effectivement ; $(1,2)$ provient de Liouville ($n = p$ avec p premier), pas $(2,2)$ cf le 6.1).

6.2.2

$1 \leqslant \alpha \leq \beta \leqslant \gamma$ et $\alpha^3 + \beta^3 + \gamma^3 = (\alpha + \beta + \gamma)^2$

Cf le 2.3, les seuls entiers possédant exactement 3 diviseurs sont de la forme p^2 avec p premier, donc le seul triplet solution provenant de Liouville ($n = p^2,\ p$ premier) est $(1,2,3)$.

Et évidemment, cf 6.1), $(3,3,3)$ est un triplet solution ne provenant pas de Liouville.

En fait, il n'y a pas d'autres triplets solutions.

En effet $\alpha^3 + \beta^3 + \gamma^3 \geqslant 2 + \gamma^3$ et $(\alpha + \beta + \gamma)^2 \leqslant 9\gamma^2,$ donc $2 + \gamma^3 \leqslant 9\gamma^2,$ soit $\gamma^2(\gamma - 9) \leqslant -2$, ce qui exige $\gamma \leqslant 8.$

Il suffit alors de faire un petit programme avec une triple boucle calculant, pour $0 < \alpha \leqslant \beta \leqslant \gamma \leqslant 8,$ l'entier $\alpha^3 + \beta^3 + \gamma^3 - (\alpha + \beta + \gamma)^2$ et on constate que cet entier ne s'annulle que pour les triplets (1,2,3) et (3,3,3).

6.2.3

Un k-uplet de E_k provient de Liouville si et seulement si k est le nombre de diviseurs $(c_1, c_2, \ldots, c_k)$ d'un entier n et si les α_i sont les $d(c_i)$.

Or si $n = \prod p_i^{n_i}$ (décomposition en nombres premiers), cf le 2.3), son nombre de diviseurs est $\prod(n_i + 1),$ nombre qui doit être k.

D'où si k est premier, n doit posséder un seul facteur premier p_1 et donc être de la forme $p_1^{n_1} = p_1^{k-1},$ choix de n qui donne le k-uplet $(1, 2, \ldots, k)$

Donc si k est premier, le seul k-uplet de E_k provenant de Liouville est $(1, 2, \ldots, k)$ obtenu pour $n = p_1^{k-1}$.

Mais si k n'est pas premier, le choix $n = p_1^{k-1}$ conduit encore au k-uplet $(1, 2, .., k),$ mais on a d'autres choix pour n qui correspondent à toutes les écritures possibles de k en produit de facteurs tous distincts de 1.

Par exemple si $k = 4,$ on a $4 = 2 \times 2$ qui est le nombre de diviseurs de $n = p_1\, p_2$, d'où l'unique autre 4-uplet en provenance de Liouville $(1,2,2,4),$ déjà vu au 5.

Si $k = 8,$ on a deux décompositions (en facteurs tous distincts de 1) : 2×4 et $2 \times 2 \times 2$.

$k = 2 \times 4$ est le nombre de diviseurs de $n = p_1 p_2^3,$ ce qui donne le 8-uplet $(1,2,2,3,4,4,6,8)$

$k = 2 \times 2 \times 2$ est le nombre de diviseurs de $n = p_1 p_2 p_3,$ ce qui donne le 8-uplet $(1,2,2,2,4,4,4,8)$

Montrons que si $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ est un élément de E_k provenant de Liouville, $\alpha_k = k$:

k est alors le nombre de diviseurs d'un entier n et les α_i sont les nombres de diviseurs des diviseurs de n ; comme α_k est le plus grand des $\alpha_i,\ \alpha_k$ est le nombre de diviseurs d'un diviseur de n ayant le plus grand nombre de diviseurs, donc, puisque $c|n$ et $c < n$ impliquent (voir 2.3) $d(c) < d(n),$ c'est que $\alpha_k = d(n) = k.$

Montrons que si $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ est un élément de $E_k,\ \alpha_k \leqslant k^2 - 1$:

$\alpha_k^3 + k - 1 \leqslant \sum_{i=1}^{k} \alpha_i^3 = (\sum_{i=1}^{k} \alpha_i)^2 \leqslant (k\alpha_k)^2,$ et donc $\alpha_k^2(\alpha_k - k^2) \leqslant 1 - k < 0,$ soit $\alpha_k \leqslant k^2 - 1.$

Bien entendu, cette majoration n'est pas intéressante pour un k-uplet provenant de Liouville puisque dans ce cas $\alpha_k = k$ ■

7) Identité de Liouville et nombre de décompositions en deux carrés d'un entier naturel.

On peut donner un aspect "curieux" à la formule de Liouville du paragraphe 5.

Pour cela prenons $n = \prod_i p_i^{n_i}$ où les p_i sont des nombres premiers **congrus à 1 modulo 4** :

dans ce cas on démontre que si c (dans N) divise $n,$ alors $d(c)$ n'est autre que le nombre de couples $(a, b) \in N \times N$ tels que $a^2 + b^2 = 2c,$ $2c$ étant donc de la forme $2\prod_i p_i^{n_i'}$.

Cela se montre à partir de la formule suivante, que l'on peut trouver dans l'ouvrage Théorie des Nombres de Daniel Duverney chez Dunod :

m étant cette fois un entier naturel non nul quelconque,
le nombre de couples $(a, b) \in Z \times Z$ tels que $a^2 + b^2 = m$ est $4(d_1(m) - d_3(m))$, avec $d_1(m)$ le nombre de diviseurs de m tels que $m \equiv 1\ (4)$ et $d_3(m)$ le nombre de diviseurs de m tels que $m \equiv 3\ (4)$.
(511_10_4)
Par exemples,

si $c = 5 \times 13 = 65$, il posséde $d(c) = 4$ diviseurs et on peut vérifier que le nombre de décompositions en deux carrés (d'entiers naturels) de $2 \times 65 = 130$ est effectivement 4, les quatre couples correspondants étant $(3, 11), (11, 3), (7, 9), (9, 7)$

si $c = 5^2 \times 13 = 325$, il posséde $d(c) = 6$ diviseurs et on peut vérifier là aussi que le nombre de décompositions en deux carrés (d'entiers naturels) de $2 \times 325 = 650$ est effectivement 6, les six couples correspondants étant $(5, 25), (25, 5), (11, 23), (23, 11), (17, 19), (19, 17)$.

D'où l'énoncé suivant :

La somme des cubes des nombres de décompositions en deux carrés des diviseurs pairs de $2n$ est égale au carré de la somme de ces nombres de décompositions.

On peut rendre l'énoncé encore plus curieux :

La somme des cubes des nombres de décompositions en deux carrés impairs des diviseurs pairs de $2^k n$ (avec $k \geq 1$) est égale au carré de la somme de ces nombres de décompositions.

En effet, si un entier est divisible par 4, toute décomposition en deux carrés de ce nombre est constituée de deux carrés pairs, donc pour avoir des nombres de décompositions en deux carrés impairs qui soient non nuls, il faut se limiter aux diviseurs pairs de $2n$.