SUR LES SOMMES DE QUATRE CUBES

Autor(en): **Revoy, Philippe**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **29 (1983)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **19.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-52980

L'Enseignement Mathématique, t. 29 (1983), p. 209-220

SUR LES SOMMES DE QUATRE CUBES

par Philippe REVOY

In this note, we do a systematic study of first degree identities $\sum_{i=1}^{4} P_i(x)^3 = Px + Q$, $P_i \in \mathbf{Z}[x]$, occuring in the four cube problem over $\mathbf{Z}$; we try to explain the difficulties to get identities for numbers $18k + 2$ which were found by Demjanenko and we show we can get a lot of similar identities, so that most integers of that residue class are sum of four cubes unless they are divisible by certain prime numbers, possibly an infinity, and we settle the question using second degree identities.

On sait que tout nombre rationnel est somme de trois cubes de rationnels. Il est conjecturé que tout entier est somme de quatre cubes d'entiers et cela a été montré pour de nombreuses progressions arithmétiques, si bien que depuis [2] on sait que le résultat est vrai pour tout entier n non congru à ± 4 modulo 9. Ces résultats se montrent à l'aide des identités ([3]):

$$(k+1)^3 + (k-1)^3 - 2k^3 = 6k\,,$$

$$k^3 + (-k+4)^3 + (2k-5)^3 + (-2k+4)^3 = 6k + 3\,,$$

$$(3k+30)^3 + (-3k-26)^3 + (-2k-23)^3 + (2k+14)^3 = 18k + 1\,,$$

$$(k+2)^3 + (6k-1)^3 + (8k-2)^3 + (-9k+2)^3 = 18k + 7\,,$$

$$(k-5)^3 + (-k+14)^3 + (3k-30)^3 + (-3k+29)^3 = 18k + 8\,.$$

Cela vérifie la conjecture pour $n \not\equiv \pm 4 \bmod 9$ et $n \not\equiv \pm 2$ mod. 18. Pour les entiers de la forme $9h \pm 4$, il a été montré ([1], [5]) qu'il n'existe pas d'identités du type ci-dessus: $\sum_{i=1}^{4} P_i(k)^3 = Pk + Q$ avec P, Q entiers, $P_i \in \mathbf{Z}[k]$ et $Q \equiv \pm 4$ modulo 9 si $\sup d^\circ P_i \leqslant 6$. Dans [2], V. A. Demjanenko montre qu'il existe des identités convenables pour les nombres de la forme $18h \pm 2$.

Nous voulons ici montrer comment on peut obtenir des identités analogues à celles de [2] et rendre explicite la démarche de cet article. L'auteur remercie A. Proscynski pour la traduction de [2] qui a permis ce travail. Nous noterons $\Sigma x_i = \sum_{i=1}^{4} x_i$ et $\mathbf{x}$ le vecteur (x_1, x_2, x_3, x_4) de $\mathbf{Z}^4$.

1. Nous voulons d'abord chercher systématiquement les identités du premier degré du type:

$$\Sigma(a_i k + b_i)^3 = Pk + Q$$

On doit avoir $\Sigma a_i^3 = \Sigma a_i^2 b_i = 0$. Alors $P = 3\Sigma a_i b_i^2$ et $Q = \Sigma b_i^3$ (des congruences élémentaires montrent que P est pair donc multiple de 6). On est amené à étudier la forme bilinéaire symétrique $\varphi_{\mathbf{a}}: \mathbf{Z}^4 \times \mathbf{Z}^4 \to \mathbf{Z}^4$, $(\mathbf{x}, \mathbf{y}) \to \Sigma a_i x_i y_i$ dont le vecteur $\mathbf{a}$ est un vecteur isotrope qu'on pourra supposer unimodulaire (les a_i sont premiers entre eux dans leur ensemble). De plus $\varphi_{\mathbf{a}}(\mathbf{a}, \mathbf{b}) = 0$; il s'agit donc de partir d'une solution entière de l'équation $\Sigma X_i^3 = 0$; ces solutions sont bien connues car c'est l'équation d'une surface cubique dont les 27 droites sont définies sur $Q[\sqrt{-3}]$. A chaque solution $\mathbf{a}$, on associe une forme $\varphi_{\mathbf{a}}$: l'orthogonal de $\mathbf{a}$ dans $\mathbf{Z}^4$ est un sous-groupe de rang 3 contenant $\mathbf{a}$. Soit $\mathbf{a}'$ un vecteur de $\mathbf{Z}^4$ tel que $\varphi(\mathbf{a}, \mathbf{a}') = 1$ (il en existe car les a_i^2 sont premiers entre eux). Le plan $H = \mathbf{Z}\mathbf{a} \oplus \mathbf{Z}\mathbf{a}'$ est métabolique pour $\varphi_{\mathbf{a}}$ et la restriction de $\varphi_{\mathbf{a}}$ à ce plan est non dégénérée. Il s'ensuit que $\mathbf{Z}^4$ est somme orthogonale de H et d'un plan H': l'orthogonal de $\mathbf{a}$ est donc le groupe $H' \oplus \mathbf{Z}\mathbf{a}$. On voit donc que si $\{\alpha, \beta\}$ est une base de H', $\mathbf{b} = \lambda\mathbf{a} + x\alpha + y\beta$: quitte à remplacer k par $k + \lambda$, on voit qu'à une solution $\mathbf{a}$ de l'équation $\Sigma X_i^3 = 0$, est associée une famille d'identités:

$$\Sigma(a_i k + \alpha_i x + \beta_i y)^3 = P(x, y)k + Q(x, y)$$

où $P(x, y) = 3\,\Sigma a_i(\alpha_i x + \beta_i y)^2$ est la forme quadratique $3\,\varphi_{\mathbf{a}}(x\alpha + y\beta, x\alpha + y\beta)$ et $Q(x, y)$ une forme cubique. On remarquera encore que $P(x, y)$ est divisible par 6 car $\Sigma a_i \alpha_i^2 \equiv \Sigma a_i \beta_i^2 \equiv 0 \bmod 2$.

2. Deux types d'identités sont obtenus suivant que l'on prend pour $\mathbf{a}$ une solution triviale de l'équation $\Sigma X_i^3 = 0$, c'est-à-dire après permutation des indices telle que $a_1 + a_2 = a_3 + a_4 = 0$, ou bien une solution qui ne se trouve pas sur une génératrice rectiligne de la surface. Dans tous les cas, remarquons que le discriminant de $\varphi_{\mathbf{a}}$ sur $\mathbf{Z}^4$ est le produit des discriminants de $\varphi_{\mathbf{a}}$ sur H et sur H'. En conséquence le discriminant de la forme bilinéaire symétrique $\varphi_{\mathbf{a}}$ sur H' est égal à $-a_1 a_2 a_3 a_4$ et $P(x, y)$ est définie si trois des a_i sont de même

signe ; P sera indéfini dans le cas contraire : 2 des a_i sont positifs, les deux autres négatifs. Ainsi à partir d'une solution triviale avec $a_1 = a$, $a_3 = b$, on obtient une forme quadratique indéfinie de discriminant $-a^2b^2$: ce sera le produit de deux formes linéaires en x et y. Supposons a et b premiers entre eux et soit (u_0, v_0) tel que $a^2u_0 + b^2v_0 = 1$. On peut prendre pour α et β les vecteurs $(bv_0, -bv_0, -au_0, au_0)$ et $(0, b^2, 0, -a^2)$, d'où l'identité

$$(ak+bv_0x)^3 + (-ak-bv_0x+b^2y)^3 + (bk-au_0x)^3 + (-bk+au_0x-a^2y)^3$$
$$= 3k[aby(2x-(a^3+b^3)y)] + Q(x, y)$$

Comme le coefficient de k est un produit, on obtient seulement un nombre fini d'identités de second membre $Pk + Q$ avec $|P|$ borné, car alors a, b et y sont bornés et donc aussi x. Quatre des cinq identités de l'introduction sont cependant obtenues ainsi.

Regardons le cas où P est définie positive : les deux plus petites solutions non triviales de $\Sigma X_i^3 = 0$ proviennent de

$$6^3 = 5^3 + 4^3 + 3^3 \quad \text{et} \quad 9^3 = 8^3 + 6^3 + 1^3 .$$

De la seconde on obtient :

$$(k-2x-5y)^3 + (6k+x-6y)^3 + (8k+2x-13y)^3 + (-9x-2x+13y)^3$$
$$= 18k(x^2+12y^2) - 7(x+y)(x^2-7xy+13y^2),$$

d'où l'identité de l'introduction pour $18k + 7$ avec le couple $(-1, 0)$. De la première solution, on tire :

$$(5k+x-y)^3 + (4k-x+y)^3 + (3k-x+5y)^3 + (-6k-y)^3$$
$$= 18k(2x^2+5y^2) - (x-4y)(x^2-7xy+31y^2).$$

Ces identités ne donnent chacune qu'un nombre fini d'identités pour une raison P donnée multiple de 18, la meilleure étant pour les nombres de la forme $36k \pm 1$. Il reste à trouver des identités pour les nombres congrus à 2 modulo 18. On peut déjà chercher, P étant divisible par 18, à quelles conditions $Q(x, y)$ sera congru à 2 modulo 18. Ainsi pour $(1, 6, 8, -9)$, on trouve $y \equiv 0(3)$, $x \equiv 1(3)$ et $x \equiv y(2)$ modulo 6, cela donne les couples suivants $(-2, 0)$ et $(1, 3)$ d'où des identités pour $72k + 56 = 18(4k+3) + 2$ et $18(109k-151) + 2$.

3. Supposons maintenant que $a_1a_2a_3a_4 > 0$, c'est-à-dire que $P(x, y)$ est indéfinie. Les cas les plus simples sont

$$12^3 + 1^3 = 10^3 + 9^3 ; 16^3 + 2^3 = 15^3 + 9^3 ,$$
$$\text{puis} \quad 27^3 + 10^3 = 24^3 + 19^3 .$$

On en déduit les identités :

(1) $(12k+5x-6y)^3 + (k+4x-3y)^3 + (-10k-4x+3y)^3 + (-9k-4x+7y)^3$
$= 18k(2x^2-15y^2) + (x+y)(61x^2-175xy+127y^2)$,

(2) $(15k+x+3y)^3 + (9k+7x+y)^3 + (-16k-3x-3y)^3 + (-2k-6x+3y)^3$
$= 18k(40x^2-3y^2) + 101x^3 + 399x^2y - 195xy^2 + 28y^3$,

(3) $(27k-26x+9y)^3 + (10k-63x-16y)^3 + (-24k+10x-13y)^3$
$+ (-19k+54x+7y)^3 = 9k[19(3x)^2 - 5(5x+4y)^2] + Q(x, y)$.

C'est en utilisant l'identité (3) que Demjanenko a résolu le problème pour les nombres de la forme $18h + 2$. Il faut tout d'abord chercher pour quelles valeurs de x et de y, $Q(x, y) \equiv 2 \bmod 18$. Cela donne en changeant les noms des variables et en supposant x non divisible par 3, les seconds membres suivants :

(1) $18k[2(2x-3y)^2-135y^2] + 2x(244x^2-1782xy+3267y^2)$

(2) $18k[160x^2-27y^2] + 808x^3 + 4788x^2y - 3510xy^2 + 756y^3$

(3) $9k[19(3x)^2-5(7x-24y)^2] + Q'(x, y)$.

Etudions le cas (1) : le phénomène important est que la forme quadratique $P(x, y)$ possède une infinité d'automorphismes ; ainsi la forme quadratique $2(2x-3y)^2 - 135y^2$ représente d'une *infinité* de façon les entiers qu'elle représente. Si N est un tel entier, supposé premier et plus grand que 3, on obtient une infinité d'identités dont le second membre est $18Nk + F_n$ où l'on sait que $F_n \equiv 2(18)$. Pour en déduire que tout entier de la forme $18h + 2$ est somme de 4 cubes, il suffirait de montrer que F_n parcourt un système *complet* de résidus modulo N. En fait cela n'est pas vrai, mais pour des choix convenables de N, on va montrer qu'on obtient tous les résidus modulo N possibles à l'exception d'un seul, qui est 0, c'est-à-dire que tout entier de la forme $18h + 2$ non divisible par N est de ce fait somme de quatre cubes par l'identité (1).

4. Soit N un nombre premier supérieur à 5 représenté par la forme quadratique $2(2x-3y)^2 - 135y^2$; on a alors une infinité de représentations de N données par $(x, y) = (x_n, y_n)$ avec $x_n = a\varepsilon^n + b\varepsilon'^n$, $y_n = c\varepsilon^n + d\varepsilon'^n$ où ε est

l'unité fondamentale de $\mathbf{Z}[\sqrt{270}]$ et $\varepsilon\varepsilon' = 1$. Il s'agit de regarder les résidus modulo N des nombres $Q(x_n, y_n)$. L'unité fondamentale de $\mathbf{Z}[\sqrt{270}]$ est

$$\varepsilon = \eta^3 \quad \text{avec} \quad \eta = 11 + 2\sqrt{30} : \varepsilon = 5291 + 966\sqrt{30}\,.$$

On pose $\eta^{3n} = A_n + 3B_n\sqrt{30}$, d'où les valeurs de A_n et de B_n: portant dans $2(2x_n - 3y_n)^2 - 135y_n^2 = N$, on trouve

$$\begin{cases} y_n = A_n y_0 + 2B_n(2x_0 - 3y_0)\,, \\ 2x_n - 3y_n = (2x_0 - 3y_0)A_n + 135B_n y_0\,. \end{cases}$$

$$\text{Soit } y_n = \frac{[3\sqrt{30}y_0 + 2(2x_0 - 3y_0)]\eta^{3n} + [3\sqrt{30}y_0 - 2(2x_0 - 3y_0)]\eta^{-3n}}{6\sqrt{30}},$$

$$x_n = \frac{(2+\sqrt{30})\,[3\sqrt{30}y_0 + 2(2x_0 - 3y_0)]\eta^{3n} + (2-\sqrt{30})\,[3\sqrt{30}y_0 - 2(2x_0 - 3y_0)]\eta^{-3n}}{8\sqrt{30}}.$$

Mais comme $2(2x_0 - 3y_0)^2 - 135y_0^2 = N$ est premier, l'idéal (N) se décompose dans $\mathbf{Z}[\sqrt{30}]$ en produit de deux idéaux premiers distincts qui contiennent l'un $3\sqrt{30}\,y_0 + 2(2x_0 - 3y_0)$ et l'autre son conjugué. On trouve donc que modulo N, on a l'un des deux systèmes

$$\begin{cases} x_n \equiv \alpha\eta^{3n} \\ y_n \equiv \beta\eta \end{cases} \qquad \text{ou bien} \qquad \begin{cases} x_n \equiv \alpha\eta^{-3n} \\ y_n \equiv \beta\eta^{-3n} \end{cases}$$

où α et β sont des entiers. Ceci montre que, modulo N,

$$Q(x_n, y_n) = \eta^{\pm 9n} Q(\alpha, \beta)\,.$$

Si $Q(\alpha, \beta)$ est nul, cela signifie qu'on obtient ainsi les multiples de N qui sont de la forme $18h + 2$. Si $Q(\alpha, \beta) \neq 0$, on ne peut jamais obtenir ces nombres, mais on peut obtenir tous les nombres de la forme $18h + 2$ qui sont congrus à C modulo N si la congruence $\eta^{\pm 9n} \equiv CQ(\alpha, \beta)^{-1}$ mod. N a une solution. Si $N \equiv 1(3)$, on ne peut obtenir tous les nombres car tout élément de $\mathbf{Z}/N\mathbf{Z}$ n'est pas une puissance neuvième. Par contre si $N \not\equiv 1(3)$ et si η est racine primitive modulo N, on obtient tous les résidus non nuls C possibles. On a donc démontré le

THÉORÈME. *Pour tout nombre premier* $N \equiv 2(3)$ *représenté par la forme quadratique* $2(2x-3y)^2 - 135y^2$ *tel que* $\eta = 11 + 2\sqrt{30}$ *est racine pri-*

mitive modulo N, la formule (1) fournit une représentation en somme de 4 cubes de tout entier de la forme $18h + 2$ non divisible par N.

Ce théorème a la conséquence suivante:

COROLLAIRE. *S'il existe une infinité de nombres premiers vérifiant les hypothèses du théorème, l'identité (1) permet d'écrire tout entier de la forme $18h + 2$ comme somme de 4 cubes.*

Remarquons que Demjanenko utilise (3) avec $N = 3323$: on a avec $x = 11$ et $y = 1$: $19(33)^2 - 5(53)^2 = 2 \times 3323$. L'unité fondamentale de $\mathbf{Z}[\sqrt{95}]$ est $39 + 4\sqrt{95}$. De plus, comme on peut prendre pour x_n et y_n: $(x_n, y_n) = \pm \varepsilon^n(x_0, y_0)$, il apparaît que si ε n'est pas racine primitive modulo n, on peut encore trouver le résultat analogue si $-\varepsilon$ l'est. Ainsi si $\varepsilon^2 \neq 1$ modulo N et si $\varphi(N) = 2p$, p nombre premier, alors ε ou $-\varepsilon$ est racine primitive modulo N. On a ainsi la

PROPOSITION. *Soit N un nombre premier $\equiv 2(3)$ représenté par la forme quadratique $2(2x-3y)^2 - 135y^2$ et tel que $\varphi(N) = 2p$ avec p premier: la formule (1) fournit une représentation en somme de quatre cubes de tout entier de la forme $18h + 2$ non divisible par N.*

Comme $N \equiv 2(3)$, $\pm \eta$ et $\pm \eta^3$ sont simultanément racines primitives modulo N; comme $\varphi(N) = 2p$ et que $\eta^2 \not\equiv 1(N)$, $\mathbf{F}_N^* \simeq \mathbf{Z}/2 \times \mathbf{Z}/p$ et l'image de $\pm \eta$ dans $\mathbf{Z}/p$ est non nulle. Il suffit donc que $\pm \eta$ ait son image non nulle dans $\mathbf{Z}/2$ ce qui équivaut à dire que $\pm \eta$ n'est pas résidu modulo N. Comme $N - 1 = 2p$, $N \equiv 3(4)$ de sorte que $\left(\frac{-1}{N}\right) = -1$: alors η ou $-\eta$ est non résidu quadratique, ce qui démontre la proposition. La proposition s'applique à:

$$N = 107, \quad (x_0, y_0) = (7,1), \quad p = 53,$$

$$N = 347, \quad (x_0, y_0) = (40,7), \quad p = 173,$$

$$N = 923, \quad (x_0, y_0) = (52,9), \quad p = 461,$$

$$N = 1883, \quad (x_0, y_0) = (127,15), \quad p = 941.$$

Ainsi tout entier non divisible par $107 \times 347 \times 923 \times 1883$, de la forme $18h + 2$ est somme de 4 cubes par l'identité (1).

Notons enfin que 3323 est représenté par la forme quadratique $2(2x-3y)^2 - 135y^2$ par le couple (220,39). Comme $\varphi(3323) = 3322 = 2 \times 11 \times 151$, pour vérifier que $\pm \varepsilon$ est racine primitive modulo 3323, il suffit de vérifier que

ε^{11} et ε^{151} sont différents de ± 1 modulo 3323. On a $\sqrt{30} = 1312$ mod. 3323 et donc $11 + 2\sqrt{30} = \varepsilon = -688$ mod. 3323. Ainsi on montre que tout non-multiple de 3323, qui est de la forme $18k + 2$ est somme de 4 cubes. Il reste les multiples de 3323, pour lesquels V. A. Demjanenko ([2]) utilise plusieurs identités dont deux du second degré, i.e. $\Sigma P_i(k)^3 = Pk + Q$ avec $d^\circ P_i = 2$.

5. Il reste à obtenir des identités pour les nombres de la forme $18h + 2$ qui sont multiples de l'un des nombres auxquels s'appliquent le théorème et la proposition du paragraphe 4, par exemple 107, 347, 923, ... Nous obtiendrons ce résultat par des identités du second degré que je vais décrire ici.

Nous cherchons des identités de la forme:

$$P_1^3(k) - P_2^3(k) + P_3^3(k) - P_4^3(k) = S(k)$$

où les P_i sont des polynômes du second degré et où:

$$P_2(k) = A(k),\ P_4(k) = B(k),\ P_1(k) = A(k) + pk + q \quad \text{et} \quad P_3(k) = B(k) - \alpha^2(pk+q),\ p, q \quad \text{et} \quad \alpha$$

étant des entiers. De plus, pour que $S(k)$ soit du premier degré, on suppose que $\alpha B(k) - A(k) = \varepsilon k + \varepsilon'$, ε et ε' étant entiers. Alors $P_1^3 - P_2^3$ et $P_3^3 - P_4^3$ sont divisibles par $pk + q$ si bien qu'en général $S(k)$ est le produit de $pk + q$ et d'un polynôme du troisième degré. On pose $B(k) = ak^2 + bk + c, a, b, c \in \mathbf{Z}$ de sorte que $S = S(k)$ dépend des huit paramètres a, b, c, α, p, q, ε et ε'. Il suffit maintenant d'annuler les coefficients de k^3, k^2 et k dans le quotient de S par $pk + q$ pour obtenir les trois relations entre les paramètres qui fourniront les identités voulues.

On obtient les trois équations suivantes:

$$2\varepsilon = p(1+\alpha^3),$$

$$a\alpha[2\varepsilon' - q(1+\alpha^3)] = \frac{p^2(1-\alpha^6)}{12},$$

$$b\alpha[2\varepsilon' - q(1+\alpha^3)] = p\varepsilon'\alpha^3 + \frac{pq(1+\alpha^3)(1-4\alpha^3)}{6}.$$

On remarquera que c n'intervient pas et que par contre $\dfrac{S}{pk+q}$ est fonction linéaire de c. Résolvant les deux dernières équations en ε' et q, on a

$$2aq = bp - \frac{p^2\alpha^2}{2} \quad \text{et} \quad a\varepsilon' = bp\frac{1+\alpha^3}{4} - p^2\frac{(1+\alpha^3)(4\alpha^3-1)}{24\alpha}.$$

Alors

$$S = (pk+q)\,[3c\alpha(q(1+\alpha^3)-2\varepsilon') + 3\varepsilon'^2 - 3q\varepsilon' + q^2(1-\alpha^6)]\,,$$

c'est-à-dire que S est de la forme $(pk+q)\,(rc+s)$, où

$$r = 3\alpha[q(1+\alpha^3)-2\varepsilon'] \quad \text{et} \quad s = 3\varepsilon'^2 - 3q\varepsilon' + q^2(1-\alpha^6)\,.$$

6. *Exemples.* Cherchons des identités avec $q = 0$; comme p est non nul, on a $b = \dfrac{p\alpha^2}{2}$ et $a\varepsilon' = \dfrac{p^2(1-\alpha^6)}{24\alpha}$. Il faut alors que p soit pair: $p = 2p_0$ et cela donne $\varepsilon = p_0(1+\alpha^3)$, $b = p_0\alpha^2$ et $6a\alpha\varepsilon' = p_0^2(1-\alpha^6)$. Prenant $\varepsilon' = 1$ et $c = 0$, on obtient $S = 6p_0k$ et la relation $6a\alpha = p_0^2(1-\alpha^6)$: on peut prendre $p_0 = \alpha =$ tout nombre impair car cela donne $a = \dfrac{\alpha - \alpha^7}{6}$, ce qui donne des identités pour les nombres de la forme $18k$, $30k$, $42k$, etc. On peut aussi prendre $p_0 = 2\alpha$ d'où $a = \dfrac{2(\alpha-\alpha^7)}{3}$, ce qui donne des identités pour $12k$, $24k$, $36k$, ... par exemple

$$12k = (42k^2+2k+1)^3 - (42k^2-2k+1)^3 + (21k^2-8k)^3 - (21k^2+8k)^3$$

([4] p. 218).

Supposons maintenant $q = 1$ et prenons $\alpha = 2$; p est pair, égal à $2p_0$. On obtient $\varepsilon = 9p_0$ et $a = bp_0 - 8p_0$; comme $4a\varepsilon' = 18bp_0 - 93p_0^2$, p_0 lui-même est pair et $a\varepsilon' = 9b\left(\dfrac{p_0}{2}\right) - 93\left(\dfrac{p_0}{2}\right)^2$. Avec $p_0 = 2p_1$, cela donne $\varepsilon = 18p_1$, $a = 2bp_1 - 32p_1^2$ et $a\varepsilon' = 9bp_1 - 93p_1^2$. On prend alors $\varepsilon' = 4$ et $p_1 = 1$, ce qui donne a et b: $a = -102$ et $b = -35$ et $S = (4k+1)\,(6c-27)$; avec $c = 5$, on obtient

$$(204k^2 \pm 84k - 7)^3 - (204k^2 \pm 88k - 6)^3 + (102k^2 \pm 51k - 1)^3 - (102k^2 \pm 35k - 5)^3$$
$$= \pm\, 12k - 3\,.$$

Cela donne tous les multiples impairs de 3.

Ces identités ne donnent rien de bien neuf; pour obtenir à l'aide de cela des nombres non multiples de 3, il est nécessaire que s ne soit divisible par 3, puisque r l'est. Il faut donc que $q(1-\alpha^6) \not\equiv 0(3)$ c'est-à-dire que $q \not\equiv 0(3)$ et $\alpha \equiv 0(3)$.

Comme $\dfrac{p^2(1+\alpha^3)\,(1-4\alpha^3)}{24\alpha}$ doit être entier, il faut que p soit divisible par 3; si α est pair, p doit être pair aussi pour la même raison; si α est impair,

p doit être pair car $p^2\alpha^2$ doit l'être. Il faut donc que $p = 6p_0$; on trouve donc $aq = 3bp_0 - 18p_0^2\alpha^2$ et, comme $q \not\equiv 0(3)$, on a $a \equiv 0(3)$. On en déduit que $a\varepsilon' - bp\dfrac{1+\alpha^3}{4}$ est divisible par 3. On en conclut que $\dfrac{p^2}{24\alpha}$ est lui aussi divisible par 3 ; comme $\alpha \equiv 0(3)$, il faut que p soit divisible par 9 et donc par 18.

A partir de maintenant, on cherche des nombres $S \equiv 2$ modulo 18 ; il faut donc que $q(rc+s)$ soit pair et congru à 2 modulo 9. La première condition donne q pair ou, comme r est toujours pair, α impair. Comme α est divisible par 3, $r \equiv 0(9)$, et la seconde congruence s'écrit

$$qs \equiv 3q\varepsilon'^2 - 3q^2\varepsilon' + q^3 \equiv (q-\varepsilon')^3 + \varepsilon'^3 \equiv 2(9)\,.$$

Cela donne $q - \varepsilon' \equiv 1(3)$ et $\varepsilon' \equiv 1(3)$. En fait comme en changeant k (ou $-c$) en $-k$, on peut négliger le signe, on voit qu'il suffit que q et ε' soient non divisibles par 3 et non congrus modulo 3. On a donc $q - 2\varepsilon' \equiv 0(3)$ et $q(1+\alpha^3) - 2\varepsilon'$ doit être divisible par 3. En conséquence $r = 3\alpha[q(1+\alpha^3)-2\varepsilon']$ est divisible par 3^3 et par 2, donc multiple de 54. On trouve, en utilisant les relations donnant $a\varepsilon'$ et $2aq$, que p lui aussi doit être divisible par 54 et on a, en prenant $\alpha = 3$: $S = (54p_1k+q)\left(54c\dfrac{14q-\varepsilon'}{3} + 3\varepsilon'^2 - 3q\varepsilon' - 728q^2\right)$ où $p = 54p_1$. Posons $14q - \varepsilon' = 3h$; on a alors

$$\varepsilon = 756p_1\,,\quad a = \frac{9828}{h}p_1\,,\quad b = 243p_1 + \frac{3276}{h}p_1q\,,$$

p_1 et h pouvant être choisis arbitrairement, pourvu que a et b soient entiers. Prenons pour simplifier $p_1 = h = 1$: on a donc $p = 54$, $\varepsilon' = 14q - 3$, $\varepsilon = 756$, $a = 9828$ et $b = 243 + 3276q$ et une identité dont le second membre est $(54k+q)(54c+3\varepsilon'^2-3q\varepsilon'-728q^2)$. Faisant parcourir à q toutes les valeurs entières 1, 2, ..., 26 non divisibles par 3 et inférieures à 27, on obtient une famille d'identités

$$S = (54k+q)\,(54c+s(q))\,,$$

dans laquelle, quitte à faire une translation sur c, on peut supposer $s(q) \in \{1, ..., 53\}$. Pour calculer $s(q)$, il suffit de calculer modulo 54 le polynôme :

$$3(14q-3)^2 - 3q(14q-3) - 728q^2 = 34q^2 + 27q + 27\,.$$

On obtient alors le tableau suivant, avec une colonne pour le produit $qs(q)$ modulo 54, que nous utiliserons plus tard.

q	$s(q)$	$qs(q)$	q	$s(q)$	$qs(q)$
1	34	34	14	49	38
2	1	2	16	37	52
4	31	16	17	52	20
5	40	38	19	16	34
7	46	52	20	19	2
8	43	20	22	13	16
10	25	34	23	4	38
11	10	2	25	28	52
13	22	16	26	7	20

Choisissant q, on pourra obtenir des identités, soit en fixant k, soit en fixant c: ainsi fixant k égal à 0 et q égal à 1, on obtient une identité du premier degré déjà connue, pour les nombres $54n + 34 = 18(3n+2) - 2$. Ensuite, choisissons $q = 2$ et c de sorte que $54c + s = 1$ et changeons de signe, on obtient une identité quadratique pour les nombres $54n - 2 = 18(3n) - 2$. En ce qui concerne les nombres congrus à ± 2 modulo 18, il ne reste plus que ceux de la forme $18(3n+1) - 2$ et leurs opposés, c'est-à-dire les nombres de la forme $54n + 16$ ou $54n + 38$. Le tableau nous indique qu'il faut prendre pour q l'une des six valeurs suivantes: 4, 5, 13, 14, 22 ou 23. Choisissant pour q l'une de ces six valeurs, on voit que suivant la valeur que l'on donne à c, on va obtenir une famille d'identités. On obtient ainsi la proposition:

PROPOSITION. *Soit N un entier congru à ± 13, ± 31 ou ± 49 modulo 54. Alors tout multiple de N de la forme $18n \pm 2$ est somme de 4 cubes.*

En effet, il suffit de s'intéresser à ceux qui sont de la forme $18n - 2$ et donc de la forme $54n - 2$, $54n + 16$ ou $54n + 34$. Les deux extrêmes sont donnés par les identités vues plus haut:

(1) $(3c+14)^3 - (3c+13)^3 + (c-1)^3 - (c+8)^3 = 54c + 34$,

(2) $(29484k^2-2157k+4)^3 - (29484k^2-2211k+43)^3$
$+ (9828k^2-971k+22)^3 - (9828k^2-485k+4)^3 = 54k - 2.$

Pour les nombres de la forme $54n + 16$, il suffit tout d'abord de choisir $q = 4$ pour $N \equiv \pm 31$, $q = 14$ si $N \equiv \pm 49$ et $q = 22$ si $N \equiv \pm 13$ modulo 54. Alors on choisit c de sorte que $54c + s(q) = N$ ou $-N$ suivant le cas et on obtient une identité

$\pm N(54k+q)$ est somme de quatre cubes avec
$\pm N(54k+q) = 54(Nk+t) \pm 16$ ce qui achève la démonstration.

COROLLAIRE 1. *Tout multiple de* 347 *resp.* 923 *de la forme* $18n \pm 2$ *est somme de quatre cubes.*

En effet $347 = 7.54 - 31$ et $923 = 18 \times 54 - 49$ et la proposition précédente s'applique à ces nombres.

COROLLAIRE 2. *Tout entier de la forme* $18n \pm 2$ *est somme de quatre cubes.*

En effet, c'est vrai s'il est multiple de 347 (ou de 923) d'après le corollaire 1; c'est vrai s'il n'est pas divisible par 347 (ou 923) d'après la partie 4.

Remarques. 1) Les identités pour $q = 5,13$ ou 23 sont moins intéressantes pour nous car le facteur de $54k + q$ est $54c + s(q)$ avec $s(q)$ pair. En conséquence, on obtient des identités avec des progressions arithmétiques de raison $N \times 108$, avec N impair; ainsi $3323 \times 2 = 54c + 4$ avec $c = 123$ d'où l'identité indiquée par Demjanenko mais elle ne rend compte que pour la moitié des entiers multiples de 3323 et de la forme $54n \pm 16$. Il faut donc des identités supplémentaires:

2) L'identité pour $N = 347$ s'obtient ainsi:

$$P_1(k) = 29484k^2 + 39339k + 3c - 49;$$
$$P_2 = 29484k^2 + 39285k + 3c - 53;$$
$$P_3 = 9828k^2 + 12861k + c - 36;$$
$$P_4 = 9828k^2 + 13347k + c.$$

On trouve $S(k) = (54k+4)(54c-3857)$; prenant $c = 65$, on trouve une identité pour les nombres $-347(54k+4) = 54(-347k-26) + 16$.

3) Dans [4], Mordell donne des identités où les P_i sont du second degré:

$$(k^2+5k-l^2+6l-4)^3 + (-k^2+3k+l^2-14l+12)^3$$
$$+ (2k^2+2k-2l^2+22l-10)^3 + (-2k^2-4k+2l^2-20l+10)^3 = Pk + Q\,.$$

Pour de petites valeurs de l, il en déduit des identités où P est relativement petit; il remarque ensuite que si l et k sont pairs, tous les cubes sont pairs et on peut en déduire d'autres identités en divisant par 8. En fait, il suffit que l soit pair car $k^2 + 5k$ et $k^2 - 3k$ sont pairs quel que soit k: posons $l = 2h$

$$\left(\frac{k(k+5)}{2} - 2h^2+6h-2\right)^3$$
$$+ \left(-\frac{k(k-3)}{2} + 2h^2-14h+6)^3 + (k^2+k-4h^2+22h-5\right)^3$$
$$+ (-k^2-2k+4h^2-20h+5)^3 = 3k(84h^2-132h+39) + P(h)\,,$$

où $P(h) = -504h^3 + 2244h^2 - 1290h + 208$.
Ainsi pour $h = 0$, on a une identité de second membre

$$13(9k+16) = 9(13k+23) + 1;$$

pour $h = 1$: $27(-k+24) + 10$;

pour $h = 2$: $37(9k+69) + 19 = 9(37k+285) + 7$;

pour $h = 3$: $9(113k+325) + 1$, etc.

BIBLIOGRAPHIE

[1] Cohn, J. H. E. and L. J. Mordell. On sums of four cubes of polynomials. *J. London. Math. Soc. 5* (1972), 74-78.
[2] Demjanenko, V. A. On sums of four cubes (Russian). *Izv. Vyss. Učebn. Zaved. Mathematika 5 (54)* (1966), 63-69.
[3] Mordell, L. J. *Diophantine equations.* Academic Press, London and New York (1968), Ch. XXI.
[4] —— On the four integer cubes problem. *J. London. Math. Soc. 11* (1936), 208-218.
[5] Schinzel, A. On the sums of cubes of polynomials. *J. London. Math. Soc. 43* (1963), 143-145.

(Reçu le 14 octobre 1982)

Philippe Revoy

U.E.R. de Mathématiques
Université des Sciences et Techniques du Languedoc
Place Eugène-Bataillon
F-34060 Montpellier Cedex