

MAJOR ARCS IN THE FOUR CUBES PROBLEM

GEORGE SZEKERES

To Kurt Mahler for his seventy-fifth birthday

(Received 14 December 1977)

Communicated by J. H. Coates

Abstract

There is an old conjecture that every integer can be decomposed into four (positive or negative) perfect cubes. More specifically one would like to know the asymptotic number of solutions of

$$n = \pm m_1^3 \pm m_2^3 \pm m_3^3 \pm m_4^3$$

when a large bound N is placed on the parts m_i . Using the circle method it is shown that the number of such representations of n when $N \rightarrow \infty$ is asymptotically equal to $C(n) \cdot N$ for a certain positive constant $C(n)$, provided that the contribution of the minor arcs can be neglected.

The dependence of $C(n)$ on n is exhibited explicitly by expressing $C(n)$ as an infinite product. The formula is of heuristic value only since the minor arcs cannot be handled at present.

Subject classification (Amer. Math. Soc. (MOS) 1970): 10 J 10.

1. Introduction

Consider representations of integers $n \neq 0$ as a sum of signed r th powers of non-negative integers

$$(1) \quad n = \pm m_1^r \pm m_2^r \pm \dots \pm m_s^r.$$

What is the least value $v(r)$ of s such that every n can be expressed in this form? Obviously $v(r) \leq G(r) + 1$ where $G(r)$ is the smallest number of non-negative r th powers into which all but a finite number of $n > 0$ can be decomposed. The existence of $v(r)$ itself is a much more elementary fact than the existence of $G(r)$. E. M. Wright (1934), who first obtained elementary estimates for $v(r)$, called it an “easier”

Waring’s problem, presumably because of the greater ease with which n can be expressed by perfect r -th powers when both signs are allowed.

In spite of being an “easier” Waring problem, the precise value of $v(r)$ is not known for any $r > 2$. It is quite easy to show that $v(2) = 3$, but already $v(3)$ is something of a mystery; numbers of the form $n = 9m \pm 4$ require at least four cubes and five cubes suffice for any n (see Hardy and Wright, 1938, p. 327) so that $v(3)$ is either 4 or 5, but which of these two alternatives is true (notably for numbers $9m \pm 4$) is still not known. It seems likely that four cubes suffice for all integers. A similar situation prevails for decompositions into fourth powers (Hunter, 1941): ten fourth powers always suffice and there are numbers which cannot be decomposed into eight (signed) fourth powers, hence $v(4)$ is either 9 or 10.

Practically all work on Wright’s problem and on the much older four cubes problem has been done through algebraic identities, for example, Richmond (1922), Mordell (1936), Fuchs and Wright (1939), Schinzel and Sierpinski (1958). The circle method which has been so effective in Waring’s problem has not played an appreciable role in Wright’s problem. The reason for this is not hard to guess: the complementary integral, or “minor arcs” in Hardy and Littlewood’s terminology, become rather unmanageable when s is as low as the estimated $v(r) \leq G(r) + 1$.

Irrespective of the unruly behaviour of the minor arcs it is of some interest to calculate the contribution of the major arcs to the number of solutions of

$$n = \pm m_1^r \pm m_2^r \pm \dots \pm m_s^r, \quad 0 \leq m_i \leq N, \quad i = 1, \dots, s,$$

when s is near the suspected value of $v(r)$ and in particular when $r = 3, s = 4$, since this contribution is likely to determine the general character of the asymptotic behaviour of the number of solutions. The principal purpose of this paper is to carry out these calculations explicitly for the case of the four cubes problem.

The separation of the Farey arcs of the circle of integration into “major” and “minor” arcs is of course a matter of convention, or convenience, and depends on such things as the generating function employed and the circle along which one wishes to integrate. With the selection of an obvious generating function, the unit circle as the path of integration and an appropriate order for the Farey dissection, we shall find that the contribution of the major arcs to the number of solutions of

$$(2) \quad n = m_1^3 + m_2^3 + m_3^3 + m_4^3, \quad -N \leq m_i \leq N, \quad i = 1, 2, 3, 4,$$

when $N \rightarrow \infty$ is asymptotically equal to $C(n) \cdot N$ for a positive constant $C(n) = J \cdot S(n)$ where J is given by the integral (13) and $S(n)$ is given by the expressions (28) and (29). $S(n)$ is in fact the singular series of Hardy and Littlewood for cubes and has been previously determined by Barrucand (1960), but in a far less explicit form.

The present formulae are quite explicit; for instance when $n = 1$, the value of $C(1)$ is

$$(3) \quad C(1) = \frac{1}{9} J \prod_{p \equiv 1 \pmod{6}} \left(1 + \frac{5a-6}{p^2} \right),$$

where the infinite product runs through all primes $p \equiv 1 \pmod{6}$ and a is determined from

$$4p = a^2 + 27b^2, \quad a \equiv 1 \pmod{3}.$$

Numerical evaluation of J and the infinite product gives the value 17.3 for $C(1)$. Clearly this is far too low since already the trivial solutions

$$\{m_1, m_2, m_3, m_4\} = \{0, 1, m, -m\}, \quad 1 \leq m \leq N \quad \text{of } 1 = m_1^3 + m_2^3 + m_3^3 + m_4^3, \quad |m_i| \leq N$$

yield $24N - 12$ solutions. It should be noted, however, that if in (2) we restrict the m_i by $M \leq |m_i| \leq N$ where M is a fixed positive number, the major arcs supply exactly the same asymptotic expression as when $M = 0$, and it is conceivable that the asymptotic expression is correct when $M = M(n)$ is a sufficiently large number (perhaps tends slowly to ∞ with N).

It would be good to have experimental data on the number of cubic decompositions for a few low values of n and compare them with values obtained from the asymptotic formula. A list of (approximate) computed values of $C(n)$ for $1 \leq n \leq 10$ is given at the end of the paper.

2. The major arcs

Let $P(N; n)$ denote the number of solutions of (2). There is no loss in generality if we assume that $n > 0$. Then

$$\sum_{n=-\infty}^{\infty} P(N; n) z^n = \left(1 + \sum_{m=1}^N (z^{m^3} + z^{-m^3}) \right)^4,$$

where of course the sum on the left is finite. Hence

$$P(N; n) = \frac{1}{2\pi i} \int \left(1 + \sum_{m=1}^N (z^{m^3} + z^{-m^3}) \right)^4 z^{-(n+1)} dz,$$

the integral taken in the positive sense along any circle with centre 0. Because of the presence of an equal number of positive and negative powers in the (rational) generating function, the unit circle appears to be the most appropriate path of integration.

For fixed n and large N consider therefore the integral

$$\int_0^1 \left(1 + \sum_{n=1}^N [\exp(2\pi i t m^3) + \exp(-2\pi i t m^3)] \right)^4 \exp(-2\pi i n t) dt.$$

Dissect the interval of integration into Farey arcs $I_{h,k}$ of order $N^{2+1/3}$ with centres h/k , $1 \leq k \leq N^{2+1/3}$, $1 \leq h \leq K$, $(h, k) = 1$. The ‘‘major arcs’’ will be those with $k \leq K = N^{1/9}$. Thus we set

$$(4) P(N; n) = \sum_{\substack{1 \leq h \leq k \leq K \\ (h,k)=1}} \int_{I_{h,k}} \left(1 + \sum_{m=1}^N \left\{ \exp \left[2\pi i \left(\frac{h}{k} + \theta \right) m^3 \right] + \exp \left[-2\pi i \left(\frac{h}{k} + \theta \right) m^3 \right] \right\} \right)^4 \exp \left[-2\pi i n \left(\frac{h}{k} + \theta \right) \right] d\theta + \int_{\Gamma},$$

where Γ is the union of the complementary (minor) Farey arcs with centres h/k , $N^{1/9} < k \leq N^{2+1/3}$. Note that if $I_{h,k} = [(h/k) - \delta_1, (h/k) + \delta_2]$ then

$$(5) \quad \frac{1}{2k} N^{-7/3} < \delta_i < \frac{1}{k} N^{-7/3}, \quad i = 1, 2$$

(see Hardy and Wright, 1938, p. 30).

What follows is well known. As a first step we replace

$$\exp \left[2\pi i \left(\frac{h}{k} + \theta \right) m^3 \right] + \exp \left[-2\pi i \left(\frac{h}{k} + \theta \right) m^3 \right]$$

by

$$\frac{1}{k} S_{h,k} (e(\theta m^3) + e(-\theta m^3))$$

where $S_{h,k}$ is the cubic Gaussian sum

$$(6) \quad S_{h,k} = \sum_{\mu \pmod k} e \left(\frac{h}{k} \mu^3 \right), \quad e(x) = \exp(2\pi i x).$$

We have for $s \geq 0$

$$(7) \quad \sum_{0 \leq \mu < k} e \left[\left(\frac{h}{k} + \theta \right) (sk + \mu)^3 \right] - S_{h,k} \frac{1}{k} \sum_{0 \leq \mu < k} e[\theta (sk + \mu)^3] \\ = \sum_{0 \leq \mu < k} e \left(\frac{h}{k} \mu^3 \right) \left(e(\theta (sk + \mu)^3) - \frac{1}{k} \sum_{\nu=0}^{k-1} e[\theta (sk + \nu)^3] \right).$$

Now if $k(s+1) \leq N$ then

$$e[\theta (sk + \mu)^3] - e[\theta (sk + \nu)^3] = O(|\theta| N^2 k) = O(N^{-1/3})$$

by (5) and hence the expression in (7) is $O(|\theta| N^2 k)$. All O and o symbols refer to $N \rightarrow \infty$, with constants depending on n but not on k . Thus

$$\sum_{m=1}^N e \left[\left(\frac{h}{k} + \theta \right) m^3 \right] = \frac{1}{k} S_{h,k} \sum_{m=1}^N e(\theta m^3) + O(|\theta| N^3 + k),$$

and similarly

$$\sum_{m=1}^N e\left[-\left(\frac{h}{k} + \theta\right)m^3\right] = \frac{1}{k} S_{h,k} \sum_{m=1}^N e(-\theta m^3) + O(|\theta|N^3 + k).$$

Here

$$|\theta|N^3 + k = O\left(\frac{1}{k}N^{2/3} + K\right) = O(N^{2/3})$$

by (5) and by $K = O(N^{1/9})$, hence by (4)

$$(8) \quad P(N; n) = \sum_{\substack{1 \leq h \leq k \leq K \\ (h,k)=1}} \int_{I_{h,k}} \left(\frac{1}{k} S_{h,k} \sum_{m=-N}^N \cos(2\pi\theta m^3) + O(N^{2/3})\right)^4 \\ \times \cos\left(2\pi\frac{h}{k}n\right) (1 + O(1)) d\theta + \int_{\Gamma}.$$

To evaluate $\sum_{m=-N}^N \cos(2\pi\theta m^3)$ we use Euler–Maclaurin in its simplest form:

$$\sum_{m=-N}^N \cos(2\pi\theta m^3) = \int_{-N}^N \cos(2\pi\theta m^3) dm + O(1).$$

Setting this into (8) and observing that

$$\int_{-N}^N \cos(2\pi\theta m^3) dm = \frac{2}{3|\theta|^{1/3}} \int_0^{N|\theta|^{1/3}} u^{-2/3} \cos(2\pi u) du = O\left(\frac{N}{1 + N|\theta|^{1/3}}\right)$$

(namely $O(N)$ when $|\theta| \leq N^{-1/3}$, $O(|\theta|^{-1/3})$ when $|\theta| > N^{-1/3}$) we get

$$\left(\frac{1}{k} S_{h,k} \sum_{m=-N}^N \cos(2\pi\theta m^3) + O(N^{2/3})\right)^4 = \left(\frac{1}{k} S_{h,k}\right)^4 \left(\int_{-N}^N \cos(2\pi\theta m^3) dm\right)^4 \\ + O\left(\frac{N^{4-1/3}}{(1 + |\theta|^{1/3}N)^3}\right)$$

hence from (8) (with $u = (m/N)^3$, $\varphi = \theta N^3$)

$$P(N; n) = N \sum_{\substack{1 \leq h \leq k \leq K \\ (h,k)=1}} (1 + o(1)) \cos\left(2\pi\frac{h}{k}n\right) \left(\frac{2}{3k} S_{h,k}\right)^4 \\ \times \int_{-\delta_1 N^3}^{\delta_2 N^3} d\varphi \left(\int_0^1 u^{-2/3} \cos(2\pi\varphi u) du\right)^4 + O\left(K^2 N^{2/3} \int_{-N}^N \frac{d\varphi}{(1 + |\varphi|^{1/3})^3}\right) + \int_{\Gamma}.$$

Here $\delta_i N^3 > (1/K)N^{2/3} > N^{1/3}$ by (5), hence $\delta_i N^3 \rightarrow \infty$, $i = 1, 2$, and

$$K^2 N^{2/3} \int_{-N}^N \frac{d\varphi}{(1 + |\varphi|^{1/3})^3} = O(N^{8/9} \log N) = o(N).$$

Therefore

$$(9) \quad P(N; n) = J.S(n).N + R(N) + o(N),$$

where

$$(10) \quad J = 2 \cdot \left(\frac{2}{3}\right)^4 \int_0^\infty d\varphi \left(\int_0^1 u^{-2/3} \cos(2\pi\varphi u) du \right)^4,$$

$$(11) \quad S(n) = \sum_{\substack{1 \leq h \leq k < \infty \\ (h,k)=1}} \left(\frac{1}{k} S_{h,k}\right)^4 \cos\left(2\pi \frac{h}{k} n\right)$$

and

$$(12) \quad R(N) = \int_{\Gamma} \left(\sum_{m=-N}^N \exp(2\pi i t m^3) \right)^4 \exp(-2\pi i t) dt.$$

The sum in (11) is the singular series of Hardy and Littlewood; its absolute convergence is well known from Waring’s problem (Satz 319 in Landau, 1927, p. 300). The convergence of the integral for J is obvious since

$$\int_0^1 u^{-2/3} \cos(2\pi\varphi u) du = \varphi^{-1/3} \int_0^\varphi v^{-2/3} \cos \cos(2\pi v) d\varphi = O(\varphi^{-1/3})$$

when $\varphi \rightarrow \infty$. We would of course like to conclude from (9) that

$$P(N; n) \simeq C(n) \cdot N = J \cdot S(n) \cdot N$$

and this depends on whether the remainder term (RN) is $o(N)$. There is no hope that it should be generally so, as we have already mentioned in the introduction. It could well be that it is $o(N)$ if $\sum_{m=-N}^N$ in the integrand of (12) is replaced by $\sum_{M \leq |m| \leq N}$ where M is sufficiently large, perhaps tending to infinity with N such that $M = o(N)$.

3. Evaluation of C(n)

The evaluation of J causes no problem except a numerical one. From (10)

$$(13) \quad J = \int_0^\infty d\psi \left(\frac{2}{3\psi^{1/3}} \int_0^\psi v^{-2/3} \cos(\pi v) dv \right)^4 \simeq 12.09,$$

the last value being obtained by numerical integration.

For $S(n)$ we obtain

$$S(n) = \sum_{k=1}^\infty \sum_{\substack{h \pmod{k} \\ (h,k)=1}} \cos\left(2\pi \frac{h}{k} n\right) \left(\frac{1}{k} S_{h,k}\right)^4$$

where $S_{1,1} = 1$ and

$$S_{h,k} = \sum_{\mu \pmod{k}} e\left(\frac{h}{k} \mu^3\right) = \sum_{\mu \pmod{k}} \cos\left(2\pi \frac{h}{k} \mu^3\right) \text{ for } k > 1.$$

Let $G_k^{(0)}, G_k^{(1)}, \dots, G_k^{(k-1)}$ be the cosets of the subgroup $G_k^{(0)}$ of cubic residues in the multiplicative group G_k of co-prime residues modular k . If r_1 is the number

of distinct prime factors $p \equiv 1 \pmod{6}$ of k then the number of cosets is

$$t_k = 3^{r_1} \text{ if } 9 \nmid k, \quad t_k = 3^{r_1+1} \text{ if } 9 \mid k.$$

Note that each coset contains

$$(14) \quad \psi(k) = \varphi(k)/t_k$$

residues, $\varphi(k)$ the Euler function. The value of $S_{h,k}$ depends only on the coset $G_k^{(i)}$ (or the corresponding element γ of the quotient group $G_k/G_k^{(0)}$) to which h belongs; if $h \in \gamma = G^{(i)} \in G_k/G_k^{(0)}$, we write $S_k^{(\gamma)}$ or $S_k^{(i)}$ (whichever is more convenient) for $S_{h,k}$. We also write

$$(15) \quad T_k^{(\gamma)}(n) = \sum_{h \in \gamma} \cos\left(2\frac{h}{k}n\right) = \sum_{h \in \gamma} e\left(\frac{h}{k}n\right) = \frac{1}{t_k} \sum_{\substack{\mu \pmod{k} \\ (\mu,k)=1}} e\left(\frac{h}{k}\right) \mu^3 n.$$

Then $S(n) = \sum_{k=1}^{\infty} A(k; n)$ where $A(1; n = 1$ and

$$(16) \quad A(k; n) = \sum_{\gamma \in G_k/G_k^{(0)}} \left(\frac{1}{k} S_k^{(\gamma)}\right)^4 T_k^{(\gamma)}(n) \text{ for } k > 1.$$

LEMMA 1. For $(k_1, k_2) = 1$,

$$A(k_1 k_2; n) = A(k_1; n) A(k_2; n).$$

This is essentially Satz 282 in Landau (1927, p. 278); it follows without much trouble from Landau's Satz 281. As a corollary we obtain as in Landau's Satz 284 (p. 279):

$$(17) \quad S(n) = \prod_p \sum_{\lambda=0}^{\infty} A(p^\lambda; n),$$

the product taken over all primes p . Henceforth p will always denote a prime. We need not worry about the sum over λ ; it will be seen that it is finite for all p .

Formula (17) reduces the problem to the calculation of $A(k; n)$ when k is a prime power. For that we have to know $S_k^{(\gamma)}$ and $T_k^{(\gamma)}(n)$ when $k = p^\lambda$. It will be convenient to write

$$T_k^{(\gamma)} = \sum_{h \in \gamma} \cos\left(2\pi\frac{h}{k}\right)$$

for $T_k^{(\gamma)}(1)$; the symbol assumes that $\gamma \in G_k/G_k^{(0)}$. Suppose that $(n, k) = 1$; then

$$(18) \quad T_k^{(\gamma)}(n) = \sum_{k \in \gamma} \cos\left(2\pi\frac{h}{k}n\right) = T_k^{(\gamma n)},$$

where γn denotes natural action of n on the coset γ .

LEMMA 2. Let $k = p^\lambda$. Then $T_k^{(\gamma)} = 0$ for $\lambda \geq 2$ and $p \neq 3$, $T_{3^\lambda}^{(\gamma)} = 0$ for $\lambda \geq 3$.
 Furthermore

$$T_p^{(\gamma)} = -1 \text{ for } p \not\equiv 1 \pmod{6}, \quad T_p^{(\gamma)} = \frac{1}{3}(S_p^{(\gamma)} - 1) \text{ for } p \equiv 1 \pmod{6},$$

$$T_9^{(0)} = 2 \cos \frac{2\pi}{9}, \quad T_9^{(1)} = 2 \cos \frac{4\pi}{9}, \quad T_9^{(2)} = 2 \cos \frac{8\pi}{9}.$$

PROOF. If $p = 2$ or $p \equiv 5 \pmod{6}$ then μ^3 runs with μ through all co-prime residues $k = p^\lambda$ and the result is obvious. If $p \equiv 1 \pmod{6}$ then μ^3 runs exactly three times through all residues of p^λ congruent to a given (non-zero) cubic residue mod p and if $\lambda \geq 2$ then $\sum_{r=r_0 \pmod{p}} e(hr/p^\lambda) = 0$ when $r_0 \not\equiv 0 \pmod{p}$. The same is true for $p = 3$ when $\lambda \geq 3$. The statement concerning $T_9^{(i)}$ can be verified directly. We agree to number the cosets in $G_9/G_9^{(0)}$ so that $2 \in G_9^{(1)}$, $4 \in G_9^{(2)}$.

Lemma 2 enables us to calculate $T_k^{(\gamma)}$ for all $k = p^\lambda$ provided that $S_p^{(\gamma)}$ is known for $p \equiv 1 \pmod{6}$. We now calculate $S_k^{(\gamma)}$; whenever h and γ appear in an equation it will be assumed that $h \in \gamma$.

LEMMA 3. If $\lambda > 3$ and $k = p^\lambda$, $k' = p^{\lambda-3}$ then

$$S_k^{(\gamma)} = p^2 S_{k'}^{(\gamma)},$$

where on the right-hand side γ denotes the coset in $G_{k'}/G_{k'}^{(0)}$ induced by γ .

PROOF. Using Lemma 2,

$$\begin{aligned} \sum_{\mu \pmod{k}} e\left(\frac{h}{k} \mu^3\right) &= \sum_{\substack{\mu \pmod{k} \\ \mu \neq 0 \pmod{p}}} e\left(\frac{h}{k} \mu^3\right) = \sum_{\mu' \pmod{(k/p)}} e\left(\frac{h}{k'} \mu'^3\right) \\ &= p^2 \sum_{\mu' \pmod{k'}} e\left(\frac{h}{k'} \mu'^3\right) = p^2 S_{k'}^{(\gamma)}. \end{aligned}$$

The lemma reduces the evaluation of $S_{p^\lambda}^{(\gamma)}$ to the cases $\lambda = 1, 2, 3$.

LEMMA 4.

- (i) $S_2^{(\gamma)} = 0$, $S_4^{(\gamma)} = 2$, $S_8^{(\gamma)} = 4$.
- (ii) $S_3^{(\gamma)} = 0$, $S_9^{(\gamma)} = 3(1 + 2 \cos \frac{2}{9}\pi h)$, $S_{27}^{(\gamma)} = 9$.
- (iii) If $p \equiv 5 \pmod{6}$ then $S_p^{(\gamma)} = 0$, $S_{p^2}^{(\gamma)} = p$, $S_{p^3}^{(\gamma)} = p$, $S_{p^3}^{(\gamma)} = p^2$.
- (iv) If $p \equiv 1 \pmod{6}$ then $S_{p^2}^{(\gamma)} = p$, $S_{p^3}^{(\gamma)} = p^2$.

PROOF. The results (i) and (ii) are immediate. The results (iii) and (iv) follow from Lemma 2, noting that for $\lambda = 1, 2$

$$\sum_{\mu \equiv 0 \pmod{p}} e\left(\frac{h}{p^\lambda} \mu^3\right) = \sum_{\mu \equiv 0 \pmod{p}} 1.$$

Of course in cases (i) and (iii) there is a single coset $\gamma = G_k^{(0)} = G_k$.

The only remaining case is $S_p^{(\gamma)}$ when $p \equiv 1 \pmod{6}$.

LEMMA 5. *If $p \equiv 1 \pmod{6}$ then $G_p/G_p^{(0)}$ has three cosets and the values $S^{(0)}, S_p^{(1)}, S_p^{(2)}$ of $S_p^{(\gamma)}$ are roots of the cubic equation*

$$(19) \quad S^3 = 3pS + ap$$

where a is uniquely determined from

$$(20) \quad 4p = a^2 + 27b^2, \quad a \equiv 1 \pmod{3}.$$

For proof see Hasse (1964, p. 488). The equation for $S_9^{(0)}, S_9^{(1)}, S_9^{(2)}$ corresponding to (19) is $S^3 = 9S^2 - 81$. Later (in Lemma 8) we shall agree on a standard numbering for the $S_p^{(i)}$ (hence for the cosets $G_p^{(i)}$).

We are now in a position to compute $A(k; n)$ for $k = p^\lambda, \lambda > 0$. Let

$$(21) \quad n = \prod_p p^{\nu(p)}$$

and consider first a prime p for which $\nu(p) = 0$.

LEMMA 6. *Let $(3, n) = 1$. Then*

$$(22) \quad \begin{aligned} A(9; n) &= 7/9 \quad \text{if } n \equiv \pm 1 \pmod{9} \\ &= 1/9 \quad \text{if } n \equiv \pm 2 \pmod{9} \\ &= -8/9 \quad \text{if } n \equiv \pm 4 \pmod{9}. \end{aligned}$$

All other $A(3^\lambda; n), \lambda > 0$ are zero.

PROOF. The last statement follows directly from Definition (16) and Lemmas 2 and 4. To prove (22), let

$$U_0 = 1 + 2 \cos \frac{2\pi}{9}, \quad U_1 = 1 + 2 \cos \frac{4\pi}{9}, \quad U_2 = 1 + 2 \cos \frac{8\pi}{9}$$

be the roots of the equation

$$(23) \quad U^3 = 3U^2 - 3.$$

Then by (16) and Lemmas 2 and 4

$$\begin{aligned}
 A(9; 1) &= \frac{1}{81} \sum_{i=0}^2 U_i^4(U_i - 1), \\
 A(9; 2) &= \frac{1}{81}(U_0^4(U_1 - 1) + U_1^4(U_2 - 1) + U_2^4(U_0 - 1)), \\
 A(9; 4) &= \frac{1}{81}(U_0^4(U_2 - 1) + U_1^4(U_0 - 1) + U_2^4(U_1 - 1)),
 \end{aligned}$$

and the formulae in (22) follow by straightforward calculation, making use of equation (23).

LEMMA 7. *Let $p \equiv 1 \pmod{6}$, $(p, n) = 1$. Then*

$$\begin{aligned}
 (24) \quad A(p; n) &= \frac{1}{p^2}(5a - 6) \quad \text{if } n \in G_p^{(0)} \\
 &= -\frac{1}{2p^2}(12 + 5a - 27b) \quad \text{if } n \in G_p^{(1)} \\
 &= -\frac{1}{2p^2}(12 + 5a + 27b) \quad \text{if } n \in G_p^{(2)}
 \end{aligned}$$

where a, b are determined from (20) with the proviso $b > 0$, and the numbering of the cosets $G_p^{(1)}, G_p^{(2)}$ is according to Lemma 8 below. $A(p^\lambda; n) = 0$ for $p \equiv 1 \pmod{6}$, $\lambda > 1$ and for $p = 2$ or $p \equiv 5 \pmod{6}$, $\lambda \geq 1$.

Again the last statements follow directly from (16) and Lemmas 2 and 4; only the case of $A(p; n)$, $p \equiv 1 \pmod{6}$ needs elaboration. Suppose that in some way we have already fixed the numbering of the cosets. By (16) and Lemmas 2 and 4, if S_0, S_1, S_2 are the roots of equation (19) then

$$\begin{aligned}
 A(p; n) &= \frac{1}{3p^4} \sum_i S_i^4(S_i - 1) \quad \text{if } n \in G_p^{(0)} \\
 &= \frac{1}{3p^4}(S_0^4(S_1 - 1) + S_1^4(S_2 - 1) + S_2^4(S_0 - 1)) \quad \text{if } n \in G_p^{(1)} \\
 &= \frac{1}{3p^4}(S_0^4(S_2 - 1) + S_1^4(S_0 - 1) + S_2^4(S_1 - 1)) \quad \text{if } n \in G_p^{(2)}.
 \end{aligned}$$

Expressing S^4 from (19) and using the first two of the relations

$$(25) \quad \sum S_i = 0, \quad \sum_{i < j} S_i S_j = -3p, \quad S_0 S_1 S_2 = ap$$

one can verify immediately that $\frac{1}{3} \sum_i (S_i^5 - S_i^4) = p^2(5a - 6)$ which proves the first formula (24). The last two expressions of (24) are proved similarly, by means of

LEMMA 8. *If $G_p^{(1)}, G_p^{(2)}$ are suitably numbered then*

$$(26) \quad S_0^2 S_1 + S_1^2 S_2 + S_2^2 S_0 = \frac{1}{2}p(27b - 3a) \quad \text{with } b > 0.$$

The left-hand side of (26) is not a symmetric expression of the S_i , yet it is a rational integer. To see this, set

$$V_1 = S_0^2 S_1 + S_1^2 S_2 + S_2^2 S_0, \quad V_2 = S_0^2 S_2 + S_1^2 S_0 + S_2^2 S_1.$$

Then by (19), (20) and (25), $V_1 + V_2 = -3ap$ and

$$V_1 V_2 = 9a^2 p^2 - 27p^3 = \frac{1}{4}p^2(9a^2 - 27b^2)$$

from which the statement of the lemma follows.

Suppose next that p is a prime divisor of n , that is, $\nu(p) > 0$ in (21), and let $0 < \lambda \leq \nu(p)$. Then by definition (15) $T_k^{(\gamma)}(n)$ for the $k = p^\lambda$ is equal to the number of elements in $\gamma \in G_k/G_k^{(0)}$, that is,

$$(27) \quad \begin{aligned} T_k^{(\gamma)}(n) &= \psi(p^\lambda) = (p-1)p^{\lambda-1} \quad \text{if } p = 2 \text{ or } p \equiv 5 \pmod{6} \\ &= \frac{1}{3}(p-1)p^{\lambda-1} \quad \text{if } p \equiv 1 \pmod{6} \\ &= 2 \quad \text{if } k = 3 \\ &= 2 \times 3^{\lambda-2} \quad \text{if } k = 3^\lambda, \lambda > 1 \end{aligned}$$

by (14). Hence we obtain from (16), (19), (25), (27) and Lemmas 3, 4 and 5, by lengthy but trivial calculation:

LEMMA 9. *Let $p^\lambda | n, \lambda > 0$. Then*

(i) *for $p = 2$ or $p \equiv 5 \pmod{6}$*

$$\begin{aligned} A(p^\lambda; n) &= 0 \quad \text{if } \lambda = 3s - 2 \\ &= (p-1)p^{-(2+s)} \quad \text{if } \lambda = 3s - 1 \\ &= (p-1)p^{-(1+s)} \quad \text{if } \lambda = 3s; \end{aligned}$$

(ii) *for $p \equiv 1 \pmod{6}$*

$$\begin{aligned} A(p^\lambda; n) &= 6(p-1)p^{-(1+s)} \quad \text{if } \lambda = 3s - 2 \\ &= (p-1)p^{-(2+s)} \quad \text{if } \lambda = 3s - 1 \\ &= (p-1)p^{-(1+s)} \quad \text{if } \lambda = 3s; \end{aligned}$$

(iii) *for $p = 3$*

$$\begin{aligned} A(3^\lambda; n) &= 0 \quad \text{if } \lambda = 3s - 2 \\ &= 10 \times 3^{-(1+s)} \quad \text{if } \lambda = 3s - 1 \\ &= 2 \times 3^{-(1+s)} \quad \text{if } \lambda = 3s, s \geq 1. \end{aligned}$$

Finally suppose that $\lambda > \nu = \nu(p) > 0$ and let $n = p^\nu n'$, $(n', p) = 1$. Then

$$T_{p^\lambda}^{(\gamma)}(n) = \sum_{h \in \lambda} \cos\left(2\pi \frac{h}{p^{\lambda-\nu}} n'\right) = \frac{\psi(p^\lambda)}{\psi(p^{\lambda-\nu})} T_{p^{\lambda-\nu}}^{(\gamma n')}$$

hence by Lemma 2 the only non-vanishing $T_{p^\lambda}^{(\gamma)}(n)$ are

$$\begin{aligned} T_{p^{\nu+1}}^{(\gamma)}(n) &= -p^\nu \quad \text{if } p = 2 \text{ or } p \equiv 5 \pmod{6} \\ &= \frac{1}{2} p^\nu (S_p^{(\gamma n')} - 1) \quad \text{if } p \equiv 1 \pmod{6} \\ &= -3^{\nu-1} \quad \text{if } p = 3, \\ T_{3^{\nu+2}}^{(\gamma)}(n) &= 3^{\nu-1} (S_9^{(\gamma n')} - 3). \end{aligned}$$

Using these expressions, we obtain from (16), (25) and Lemmas 3, 4 and 5:

LEMMA 10. Let $\nu = \nu(p) > 0$ be the exponent in (21) and set $n = p^\nu n'$. Then

(i) for $p = 2$ or $p \equiv 5 \pmod{6}$

$$\begin{aligned} A(p^{\nu+1}; n) &= -p^{-(r+2)} \quad \text{if } \nu = 3r - 2 \\ &= -p^{-(r+1)} \quad \text{if } \nu = 3r - 1 \\ &= 0 \quad \text{if } \nu = 3r; \end{aligned}$$

(ii) for $p \equiv 1 \pmod{6}$

$$\begin{aligned} A(p^{\nu+1}; n) &= -p^{-(r+2)} \quad \text{if } \nu = 3r - 2 \\ &= -p^{-(r+1)} \quad \text{if } \nu = 3r - 1 \\ &= p^{-r} A(p; n') \quad \text{if } \nu = 3r \end{aligned}$$

where $A(p; n')$ is given by (24) in Lemma 7;

(iii) for $p = 3$,

$$\begin{aligned} A(3^{\nu+1}; n) &= -5 \times 3^{-(r+1)} \quad \text{if } \nu = 3r - 2 \\ &= -3^{-(r+1)} \quad \text{if } \nu = 3r - 1 \\ &= 0 \quad \text{if } \nu = 3r; \end{aligned}$$

$$\begin{aligned} A(3^{\nu+2}; n) &= 0 \quad \text{if } \nu = 3r - 2 \text{ or } 3r - 1 \\ &= 3^{-r} A(9; n') \quad \text{if } \nu = 3r, r \geq 1, \end{aligned}$$

where $A(9; n')$ is given by (22) in Lemma 6. All other $A(p^\lambda; n)$ with $\lambda > \nu$ are zero.

Collecting all results from Lemmas 6, 7, 9 and 10 we obtain for the factors $F_p(n) = \sum_{\lambda} A(p^\lambda; n)$ which appear in the product (17):

(i) If $p = 2$ or $p \equiv 5 \pmod{6}$ then

$$\begin{aligned}
 (28.1) \quad F_p(n) &= 1 + \left(\frac{1}{p} + \frac{1}{p^2}\right) \left(1 - \frac{1}{p^r}\right) \quad \text{for } \nu(p) = 3r, r \geq 0 \\
 &= \left(1 + \frac{1}{p} + \frac{1}{p^2}\right) \left(1 - \frac{1}{p^r}\right) \quad \text{for } \nu(p) = 3r-1 \text{ or } 3r-2, r \geq 1.
 \end{aligned}$$

(ii) If $p \equiv 1 \pmod{6}$ then

$$\begin{aligned}
 (28.2) \quad F_p(n) &= \left(1 + \frac{7}{p} + \frac{1}{p^2}\right) \left(1 - \frac{1}{p^r}\right) \quad \text{for } \nu(p) = 3r-1 \text{ or } 3r-2, r \geq 1 \\
 &= 1 + \left(\frac{8}{p} + \frac{1}{p^2}\right) \left(1 - \frac{1}{p^r}\right) + \frac{1}{p^{r+1}}(5a-6) \quad \text{for } \nu(p) = 3r, n/p^{3r} \in G_p^{(0)} \\
 &= 1 + \left(\frac{8}{p} + \frac{1}{p^2}\right) \left(1 - \frac{1}{p^r}\right) - \frac{1}{2p^{r+1}}(12 + 5a + (-1)^j 27b) \\
 &\quad \text{for } \nu(p) = 3r, n/p^{3r} \in G_p^{(j)}, j = 1, 2.
 \end{aligned}$$

(iii) If $p = 3$ then

$$\begin{aligned}
 (28.3) \quad F_3(n) &= 3 - \frac{23}{3^{r+1}} \quad \text{for } \nu(p) = 3r-2 \\
 &= 3 - \frac{1}{3^{r-1}} \quad \text{for } \nu(p) = 3r-1 \\
 &= 3 - \frac{11}{3^{r+2}} \quad \text{for } \nu(p) = 3r, n/3^{3r} \equiv \pm 1 \pmod{9} \\
 &= 3 - \frac{17}{3^{r+2}} \quad \text{for } \nu(p) = 3r, n/3^{3r} \equiv \pm 2 \pmod{9} \\
 &= 3 - \frac{26}{3^{r+2}} \quad \text{for } \nu(p) = 3r, n/3^{3r} \equiv \pm 4 \pmod{9}.
 \end{aligned}$$

We have now all the required factors in (17) and the calculations can be summarized as follows:

THEOREM. Let $n = \prod_p p^{\nu(p)}$. Then

$$(29) \quad S(n) = \prod_p F_p(n)$$

where the $F_p(n)$ are given by equations (28.1), (28.2) and (28.3) with $a = a(p)$, $b = b(p)$ in (28.2) determined from

$$4p = a^2 + 27b^2, \quad a \equiv 1 \pmod{3}, \quad b > 0$$

and the $G_p^{(j)}$, $j = 1, 2$ numbered according to Lemma 8.

In particular if $(p, n) = 1$ then

$$F_p(n) = 1 \quad \text{for } p = 2 \text{ or } p \equiv 5 \pmod{6},$$

$$F_p(n) = 1 + \frac{1}{p^2}(5a - 6) \quad \text{for } p \equiv 1 \pmod{6}, n \in G_p^{(0)}$$

$$= 1 - \frac{1}{2p^2}(12 + 5a + (-1)^j \cdot 27b) \quad \text{for } p \equiv 1 \pmod{6}, n \in G_p^{(j)}, j = 1, 2,$$

$$F_3(n) = 16/9 \quad \text{for } n \equiv \pm 1 \pmod{9}$$

$$= 10/9 \quad \text{for } n \equiv \pm 2 \pmod{9}$$

$$= 1/9 \quad \text{for } n \equiv \pm 4 \pmod{9}.$$

If $n = 1$ then $n \in G_p^{(0)}$ for all $p \equiv 1 \pmod{6}$ and we obtain formula (3) mentioned in the introduction.

The infinite product in the theorem converges to a positive value since $|a| < 2\sqrt{p}$, $b < (2/3\sqrt{3})\sqrt{p}$ and each $F_p(n)$ in (28) is positive. The comparatively low value of $F_3(n)$ when $n \equiv \pm 4 \pmod{9}$ makes it qualitatively understandable why numbers of the form $9m \pm 4$ are the most difficult to decompose into four cubes.

We list the computed values of $C(n)$ for the first ten values of n :

| | | | | | | | | | | |
|--------|------|------|-----|-----|-----|-----|------|------|------|-----|
| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $C(n)$ | 17.3 | 11.1 | 2.6 | 0.7 | 1.0 | 4.9 | 28.1 | 23.8 | 28.5 | 8.8 |

References

P. Barrucand (1960), "Sommes de Gauss et séries singulières de Hardy pour les cubes", *C. R. Acad. Sci. Paris* **250**, 4249–4251.
 W. H. J. Fuchs and E. M. Wright (1939), "The easier Waring problem", *Quart. J. Math. Oxford Ser.* **10**, 190–209.
 G. H. Hardy and E. M. Wright (1938), *An Introduction to the Theory of Numbers*, 4th ed. (Oxford University Press).
 H. Hasse (1964), *Vorlesungen über Zahlentheorie*, 2nd ed. (Springer, Berlin).
 W. Hunter (1941), "The representation of numbers by sums of fourth powers", *J. London Math. Soc.* **16**, 177–179.
 E. Landau (1927), *Vorlesungen über Zahlentheorie* (Chelsea, New York).
 L. J. Mordell (1936), "On the four integer cubes problem", *J. London Math. Soc.* **11**, 208–218.

H. W. Richmond (1922), "An elementary note upon Waring's problem for cubes, positive or negative", *Messenger Math.* **51**, 177–186.

A. Schinzel and W. Sierpinski (1958), "Sur les sommes de quatre cubes", *Acta Arithm.* **4**, 20–30.

E. M. Wright (1934), "An easier Waring's problem", *J. London Math. Soc.* **9**, 267–272.

The University of New South Wales
Kensington, N.S.W. 2033
Australia