ASIAN J. MATH.
Vol. 4, No. 4, pp. 885–904, December 2000

010

ON WARING'S PROBLEM FOR THREE SQUARES AND AN ℓTH POWER*

C. HOOLEY†

1. Introduction. Professor Loo Keng Hua was probably most renowned for his important contributions to the theory of Waring's problem. It is therefore fitting that this dedicatory article should be devoted to the proof of the hitherto elusive asymptotic formula for the number $\nu(n)$of representations of a large number n as the sum of three squares of integers of either sign and a non-negative (non-linear) ℓth power. Of the form that the Hardy-Littlewood circle method would presage, our asymptotic formula does not, however, seem to fall within the current ambit of that method for $\ell > 2$ and is therefore treated by other means that include the theories of Dirichlet's L-functions with real characters and the representation of numbers as the sum of three squares. All the same, as the proof develops, we encounter some of the familiar ancillary apparatus of the circle method, for details of which we most aptly direct the reader to Hua's compendium on number theory ([7], to which we refer later as H).

The situation under examination is one of those in additive number theory where the establishment of an asymptotic formula for the number of representations of an integer in a proposed form lies much deeper than any consequential criterion for deciding which integers possess such a representation. The latter question, indeed, has been settled by Churchhouse [2] in this case and does not cause undue difficulty owing to the familiar simple condition for the representability of a number as a sum of three squares. Nevertheless, conditions of the Churchhouse type emerge so naturally in the course of our proof that they are embodied explicitly in our final theorems.

We should mention that this article represents the final phase of work that was announced in our address to the I. C. M. Congress of 1983 in Warsaw [6]. Our earlier researches had, indeed, advanced the situation from Jacobi's exact formula for the case $\ell = 2$ (see H, p 216) to asymptotic formulae for exponents as large as $\ell = 7$ but had until then failed to deal with the general case.

2. Notation. Although the meaning of most of the notation is self evident from the content, the following guide may be helpful. The letters n and n_1 are usually positive integers and will be regarded as tending to infinity in the later parts of the work; X_i, X_i' are integers; ε is an arbitrarily small number that is not necessarily the same at each occurrence; the given exponent ℓ is assumed to exceed 1; B_i is a positive constant that depends at most on ℓ; $B_i(\varepsilon)$ is a positive constant depending at most on ℓ and ε; the constants implied by the O-notation are of type B_i save when there is an ε occurring as exponent, in which case they are of type $B_i(\varepsilon)$.

The highest common factor of integers X_1, X_2, X_3, X_4 is $(X_1, ..., X_4)$ when it is defined; $\sigma_{-\alpha}(n) = \sum_{d|n} d^{-\alpha}$ and $d(n) = \sigma_0(n)$.

For odd k, $\left(\frac{m}{k}\right) = (m|k)$ is the Jacobi symbol of quadratic residuacity.

3. Formulae regarding the representation of a number as a sum of

*Received July 19, 2000; accepted for publication September 19, 2000.
†Rushmoor Grange, Backwell, Bristol, BS48 3BN, England (MillsME@Cardiff.ac.uk).

three squares. There are at least two classical ways of deriving formulae for the number $r(n_1)$ of representations of a positive number n_1 as the sum of three squares of integers of either sign. The first has its origin in Gauss's Disquisitiones Arithmeticae and expresses the number $r^*(n_1)$ of primitive representations of n_1 as a sum of three squares in terms of the number of classes in the principal genus of properly primitive classes of binary quadratic forms of determinant $-n_1$, whence flows, for example, the expression for $r(n)$ in H,p 232, via Dirichlet's class number formula and the relation

$$r(n_1) = \sum_{d^2|n_1} r^*\left(\frac{n_1}{d^2}\right).$$

The second method - conceived by Hardy and Littlewood [4] during their researches on sums of squares and implemented by Estermann [3] in the hardest case of three squares - uses the Gauss sum

$$S_2(h,k) = \sum_{0<m\leq k} e^{2\pi i h m^2/k} \tag{1}$$

to construct the arithmetical function

$$\theta(n_1) = \sum_{k=1}^{\infty} \frac{1}{k^3} \sum_{\substack{0<h\leq k \\ (h,k)=1}} S_2^3(h,k) e^{-2\pi i h n_1/k} = \sum_{k=1}^{\infty} A_3(h_1,k), \text{ say,} \tag{2}$$

and shews that

$$r(n_1) = 2\pi n_1^{\frac{1}{2}} \theta(n_1) \tag{3}$$

by an identification of the function

$$1 + \sum_{n_1=1}^{\infty} r(n_1) z^{n_1}$$

with

$$1 + 2\pi \sum_{n_1=1}^{\infty} n_1^{\frac{1}{2}} \theta(n_1) z^{n_1}$$

for $|z| < 1$. Thence, if required, the formula for $r(n_1)$ in terms of the number $\rho_3(n_1,d)$ of incongruent solutions of the congruence

$$X_1^2 + X_2^2 + X_3^2 \equiv n_1, \text{ mod } d, \tag{4}$$

emerges because, being in the singular series[1] $\theta(n_1)$, the term $A_3(n_1,k)$ equals[2]

$$\sum_{d|k} \mu\left(\frac{k}{d}\right) \frac{\rho_3(n_1,d)}{d^2} \tag{5}$$

[1] One should note the diverse meanings that have been attributed to the term 'singular series'. In the original paper [4] it meant $2\pi n_1^{\frac{1}{2}} \theta(n_1)$ but according to later usage it would mean $\theta(n_1)$.

[2] Although the primary meaning attached to n_1 is that it is a positive integer, (5) is equally valid when n_1 is zero or negative. A similar comment applies to (8).

by the familiar theory of Waring's problem developed some time later than [4]. In particular, this line of development can end in the formula for $r(n_1)$ given in H at the beginning of §8.9 on p 215. But neither of these two approaches directly yields a representation of $r(n_1)$ that is suitable for our purpose here. Instead, we shall produce a hybrid formula by a method that would in fact serve to confirm directly the identity of the expressions derived for $r(n_1)$ by the above described procedures.

The source of our analysis being a comparison of (2) with the purely formal singular series

$$\sum_{k=1}^{\infty} \frac{1}{k} \sum_{\substack{0<h\leq k \\ (h,k)=1}} S_2(h,k) e^{-2\pi i h n_2/k} = \sum_{k=1}^{\infty} A_1(n_2,k), \text{ say,} \tag{6}$$

associated with the equation $X^2 = n_2$ we let $\rho_1(n_2,k)$ denote the number of incongruent solutions of the congruence

$$X^2 \equiv n_2, \text{ mod } k, \tag{7}$$

and deduce first that

$$A_1(n_2,k) = \sum_{d|k} \mu\left(\frac{k}{d}\right) \rho_1(n_2,d) \tag{8}$$

by analogy with (5). Then, since for *odd numbers* denoted by k_1 we have

$$S_2^2(h,k_1) = (-1)^{\frac{1}{2}(k_1-1)} k_1 = \left(\frac{-1}{k_1}\right) k_1$$

and

$$S_2(h,k_1) = \left(\frac{h}{k_1}\right) S_2(1,k_1),$$

by H, p 166, equations (2) and (6) imply that[3]

$$\begin{aligned} A_3(n_1,k_1) &= \frac{1}{k_1^2} \sum_{\substack{0<h\leq k_1 \\ (h,k_1)=1}} \left(\frac{-1}{k_1}\right) S_2(h,k_1) e^{-2\pi i h n_1/k_1} \\ &= \frac{1}{k_1^2} \sum_{\substack{0<h\leq k_1 \\ (h,k_1)=1}} S_2(-h,k_1) e^{-2\pi i h n_1/k_1} \\ &= \frac{1}{k_1^2} \sum_{\substack{0<h\leq k_1 \\ (h,k_1)=1}} S_2(h,k_1) e^{2\pi i h n_1/k_1} = \frac{1}{k_1} A_1(-n_1,k_1), \end{aligned} \tag{9}$$

which equality is best expressed here in terms of the formal identity

$$\sum_{k_1} \frac{A_3(n_1,k_1)}{k_1^s} = \sum_{k_1} \frac{A_1(-n_1,k_1)}{{k_1}^{1+s}} = \frac{(1-2^{-1-s})^{-1}}{\zeta(1+s)} \sum_{2\nmid q} \frac{\rho_1(-n_1,q)}{q^{1+s}}$$

[3]Here n_1 need not be positive; see footnote 2 .

between Dirichlet's series. This, by the formulae of §4 of our paper [5] that were merely deduced from the elementary properties of the congruence (7), evaluates $A_3(n_1,k)$ as the coefficient of k_1^{-s} in the formal series

$$\frac{1}{\zeta_1(2+2s)} \sum_{\substack{d^2|n_1 \\ (d,2)=1}} \frac{d}{d^{2s+2}} L_{(-n_1/d^2)}(1+s), \tag{10}$$

where

$$\zeta_1(s) = \sum_{\substack{a=1 \\ a \text{ odd}}}^{\infty} \frac{1}{a^s} \quad \text{and} \quad L_{(-n_1/d^2)}(s) = \sum_{\substack{b=1 \\ b \text{ odd}}}^{\infty} \left(\frac{-n_1/d^2}{b}\right) \frac{1}{b^s}. \tag{11}$$

In particular, we infer the well-known relation

$$\rho_3(n_1,p) = p^2\{1 + A_3(n_1,p)\} = p^2\left(1 + \frac{1}{p}A_1(-n_1,p)\right) = p^2\left\{1 + \left(\frac{-n_1}{p}\right)\right\} \tag{12}$$

for odd primes p.

To profit from this portrayal of $A_3(n,k_1)$ we shall need amongst other things to interpret the symbol $\left((-n_1/d^2)|b\right)$ as a Dirichlet character with the aid of §6 of [5], setting for any odd square divisor d^2 of n_1

$$\chi_{d_1}(b) = \begin{cases} ((-n_1/d^2)|b), & \text{if } b \text{ odd}, \\ 0, & \text{if } b \text{ even}, \end{cases}$$

where we write $d_1 = n_1/d^2$ for convenience in the subscript to χ. Accordingly, after scrutinizing [5] and slightly changing the notation therein by now writing $n_1 = D\Omega^2$ where D is square-free, we see that:

(i) since n_1 is positive, $\chi_{d_1}(b)$ is a non-principal character to a modulus not exceeding $4n_1$;

(ii) $\chi_{d_1}(b)$ is associated with a primitive character, the modulus of which is $2D$, $4D$, or $4D$ according as $D \equiv 3$, mod 4, $D \equiv 1$, mod 4, or D is even; consequently, the real primitive character associated with $\chi_{d1}(b)$ determines the value of D;

(iii) since d is odd, a unique primitive character is associated with all the characters $\chi_{d_1}(b)$ for a given value of n_1.

As those familiar with the theory will foresee, the connection between $A_1(n_1,k)$ and $A_3(n_1,k)$ is more diffuse when k is a power of 2. However, there is no need here to elucidate it, since it will suffice to have the relation

$$A_3(n_1,2^\alpha) = O\left(\frac{1}{2^{\frac{1}{2}\alpha}}\right) \tag{13}$$

that stems from (2) and inequalities for the Gauss sum.

In conclusion, for values of n_1 not exceeding n, we shall choose a parameter $N = N(n)$ to suit the problem under consideration and shall then substitute for (2) the formula

$$\theta(n_1) = \sum_{k \le N} A_3(n_1,k) + \sum_{k>N} A_3(n,k) = \theta_1(n_1) + \theta_2(n_1), \quad \text{say}, \tag{14}$$

in which the terms in $\theta_1(n_1)$ are expressed as (5) but in which those in $\theta_2(n_1)$ are handled by means of (10) and (13).

4. The singular series for three squares and an ℓth power. Although the Hardy-Littlewood circle method is not being used, some properties appertaining to the singular series $\mathfrak{S}(n)$ for $\nu(n)$ will participate in the analysis before its appearance in the final asymptotic formula. We must therefore summarize the features immediately needed, bearing in mind that some explanation is needed because the background theory of Waring's problem is only fully documented for the case where all powers have the same exponent.

First, the kth term in the singular series pertaining to $\nu(n)$ being

$$A(n,k) = \frac{1}{k^4} \sum_{\substack{0<h\le k \\ (h,k)=1}} S_2^3((h,k) S_\ell(h,k) e^{-2\pi i h n/k} \tag{15}$$

where

$$S_\ell(h,k) = \sum_{0<m\le k} e^{2\pi i h m^\ell/k} \tag{16}$$

in conformity with (1), we let $\tau(h,d)$ denote the number of incongruent solutions of the congruence

$$X_1^2 + X_2^2 + X_3^2 + W^\ell \equiv n, \mod d, \tag{17}$$

and deduce in the customary way that $A(n,k)$ is a multiplicative function of k and that

$$A(n,k) = \sum_{d|k} \mu\left(\frac{k}{d}\right) \frac{\tau(n,d)}{d^3}. \tag{18}$$

From this, its counterpart (5), and then (9), it follows for odd p that

$$\begin{aligned} p^3 A(n,p) = \tau(n,p) - p^3 &= \sum_{0<W\le p} \{\rho_3(n - W^\ell, p) - p^2\} \\ &= p^2 \sum_{0<W\le p} A_3(n - W^l, p) = p \sum_{0<W\le p} A_1(W^\ell - n, p) \\ &= p \sum_{0<W\le p} \left(\frac{W^\ell - n}{p}\right), \end{aligned}$$

in which the sum is (i) $O(p^{\frac{1}{2}})$ by a theorem due to Weil when $p \nmid n$, (ii) is never more than p in absolute value, and (iii) is not more than $p-1$ in absolute value when $p|n$. Hence, first not excluding the trivial case $p = 2$, we have

$$A(n,p) = O\left(\frac{1}{p^{\frac{3}{2}}}\right) \quad (p \nmid n), \qquad A(n,p) = O\left(\frac{1}{p}\right) \quad (p|n), \tag{19}$$

while also

$$\tau(n,p) \ge p^3 - p^2 \quad (p > 2), \quad \tau(n,p) > p^3 - p^2 \quad (p > 2,\ p|n). \tag{20}$$

When $\alpha > 1$ estimates for $A(n, p^\alpha)$ of comparable keenness to (19)are neither essential at this point nor so easy to come by, although the discussion in the later §7 will give some idea of what is possible. We are therefore content to gain the upper bound

$$A(n, p^\alpha) = O\left(p^{-\frac{1}{2}\alpha - 1}\right) \qquad (\alpha > 1) \tag{21}$$

by incorporating in (15) for $k = p^\alpha$ the familiar bounds (see Vinogradov [10], Chapter II, Lemmata 4 and 5; the case $\alpha \geq \ell$ also arises in H, §7.10.)

$$S_2(h, p^\alpha) = O\left(p^{\frac{1}{2}\alpha}\right), S_\ell(h, p^\alpha) = O\left(p^{\alpha - 1}\right) \qquad (\alpha > 1, (h, p) = 1).$$

Also, by (18),(19), and (21), we have

$$\begin{aligned} \frac{\tau(n, p^\alpha)}{p^{3\alpha}} &= 1 + \sum_{1 \leq \beta \leq \alpha} A(n, p^\beta) \leq 1 + \sum_{\beta \geq 1} |A(n, p^\beta)| \\ &< 1 + \frac{B_1(p, n)^{\frac{1}{2}}}{p^{\frac{3}{2}}} + B_1 \sum_{\beta \geq 2} \frac{1}{p^{\frac{1}{2}\beta + 1}} \\ &< 1 + \frac{B_2(p, n)^{\frac{1}{2}}}{p^{\frac{3}{2}}}. \end{aligned} \tag{22}$$

Thus not only do we deduce that[4]

$$\tau(n, \ell) = O\left\{\ell^3 \prod_{p \mid \ell} \left(1 + \frac{B_2}{p}\right)\right\} = O\left\{\ell^3 \sigma_{-\frac{1}{2}}(\ell)\right\} \tag{23}$$

but also confirm incidentally through Euler's multiplicative principle that the singular series $\mathfrak{S}(n)$ is absolutely convergent.

5. Decomposition of $\nu(n)$ and estimation of $\nu_1(n)$. Being ready to embark on the main analysis, we form the equation

$$\nu(n) = \sum_{X_1^2 + X_2^2 + X_3^2 + W^\ell = n} = \sum_{0 \leq W < n^{\frac{1}{\ell}}} r(n - W^\ell) + O(1)$$

and transform it by (3) and (14) into

$$\begin{aligned} \nu(n) &= 2\pi \sum_{W < n^{\frac{1}{\ell}}} (n - W^\ell)^{\frac{1}{2}} \theta_1(n - W^\ell) + 2\pi \sum_{W < n^{\frac{1}{\ell}}} (n - W^\ell)^{\frac{1}{2}} \theta_2(n - W^\ell) + O(1) \\ &= 2\pi\nu_1(n) + 2\pi\nu_2(n) + O(1), \text{ say,} \end{aligned} \tag{24}$$

for

$$N = n^{\delta_1}, \tag{25}$$

[4] Although the full force of (22) is not needed here, a close analogy of this estimate will be needed shortly.

where $\delta_1 = \delta_1(\ell)$ is a small positive constant to be selected later. From this the explicit term in the asymptotic formula will arise through $\nu_1(n)$, upon which therefore we first concentrate our attention.

By (24) and (5),

$$\begin{aligned}(26)\qquad \nu_1(n) &= \sum_{W<n^{\frac{1}{\ell}}} (n-W^\ell)^{\frac{1}{2}} \sum_{k\le N} A_3(n-W^\ell,k)\\ &= \sum_{W<n^{\frac{1}{\ell}}} (n-W^\ell)^{\frac{1}{2}} \sum_{k\le N} \sum_{d|k} \mu\left(\frac{k}{d}\right)\frac{\rho_3(n-W^\ell,d)}{d^2}\\ &= \sum_{k\le N}\sum_{d|k}\mu\left(\frac{k}{d}\right)\frac{1}{d^2}\sum_{W<n^{\frac{1}{\ell}}}(n-W^\ell)^{\frac{1}{2}}\rho_3(n-W^\ell,d)\\ &= \sum_{k\le N}\sum_{d|k}\mu\left(\frac{k}{d}\right)\frac{1}{d^2}\sum\nolimits_{d'}, \text{ say.}\end{aligned}$$

Here

$$\sum\nolimits_d = \sum_{0<a\le d} \rho_3(n-a^\ell,d) \sum_{\substack{W<n^{\frac{1}{\ell}}\\ W\equiv a,\mathrm{mod}\, d}} (n-W^\ell)^{\frac{1}{2}},$$

in which, since

$$s_u = s_u(a,d) = \sum_{\substack{0\le W<u\\ W\equiv a,\mathrm{mod}\ d}} 1 \qquad (u>0)$$

is estimated by

$$s_u = \frac{u}{d} + O(1),$$

we see the inner sum equals[5]

$$\begin{aligned}(27)\qquad \int_0^{n^{1/\ell}} (n-u^\ell)^{\frac{1}{2}}\,ds_u &= \frac{1}{d}\int_0^{n^{1/\ell}}(n-u^\ell)^{\frac{1}{2}}\,du + \left[O\{(n-u^\ell)^{\frac{1}{2}}\}\right]_0^{n^{1/\ell}}\\ &\quad + O\left\{\int_0^{n^{1/\ell}}\left(-\frac{d}{du}(n-u^\ell)^{\frac{1}{2}}\right)du\right\}\\ &= \frac{1}{d}\int_0^{n^{1/\ell}}(n-u^\ell)^{\frac{1}{2}}\,du + O(n^{\frac{1}{2}})\\ &= \frac{n^{\frac{1}{2}+\frac{1}{\ell}}}{d\ell}\int_0^1 (1-v)^{\frac{1}{2}}v^{\frac{1}{\ell}-1}\,dv + O(n^{\frac{1}{2}})\\ &= \frac{\Gamma(\frac{3}{2})\Gamma(\frac{1}{\ell}+1)}{d\Gamma(\frac{3}{2}+\frac{1}{\ell})}n^{\frac{1}{2}+\frac{1}{\ell}} + O(n^{\frac{1}{2}}).\end{aligned}$$

[5]This procedure affords the easiest way of avoiding a tedious appeal to summation formulae of the Euler-MacLaurin type.

Thus

$$\sum_d = \left(\frac{\Gamma(\frac{3}{2})\Gamma(\frac{1}{\ell}+1)}{\Gamma(\frac{3}{2}+\frac{1}{\ell})} \cdot \frac{n}{d} + O(n^{\frac{1}{2}})\right) \sum_{0<a\le d} \rho_3(n-a^\ell, d)$$
$$= \frac{\Gamma(\frac{3}{2})\Gamma(\frac{1}{\ell}+1)n^{\frac{1}{2}+\frac{1}{\ell}}}{\Gamma(\frac{3}{2}+\frac{1}{\ell})} \cdot \frac{\tau(n,d)}{d} + O\{n^{\frac{1}{2}}\tau(n,d)\}$$

by the definition of $\tau(n,d)$ in (17), and we deduce from (26) and (18) the equation

$$\nu_1(n) = \frac{\Gamma(\frac{3}{2})\Gamma(\frac{1}{\ell}+1)n^{\frac{1}{2}+\frac{1}{\ell}}}{\Gamma(\frac{3}{2}+\frac{1}{\ell})} \sum_{k\le N} \sum_{d|k} \mu\left(\frac{k}{d}\right)\frac{\tau(n,d)}{d^3} \tag{28}$$
$$+O\left(n^{\frac{1}{2}} \sum_{k\le N} \sum_{d|k} \frac{\tau(n,d)}{d^2}\right)$$
$$= \frac{\Gamma(\frac{3}{2})\Gamma(\frac{1}{\ell}+1)n^{\frac{1}{2}+\frac{1}{\ell}}}{\Gamma(\frac{3}{2}+\frac{1}{\ell})} \sum_{k\le N} A(n,k)$$
$$+O\left(n^{\frac{1}{2}} \sum_{d\le N} \frac{\tau(n,d)}{d^2} \sum_{\substack{k\le N \\ k\equiv 0, \bmod d}} 1\right)$$
$$= \frac{\Gamma(\frac{3}{2})\Gamma(\frac{1}{\ell}+1)n^{\frac{1}{2}+\frac{1}{\ell}}}{\Gamma(\frac{3}{2}+\frac{1}{\ell})} \sum_{k\le N} A(n,k) + O\left(n^{\frac{1}{2}} N \sum_{d\le N} \frac{\tau(n,d)}{d^3}\right)$$

that represents the virtual conclusion of the first phase of the estimations.

We take (23) to estimate the remainder term above as

$$O\left(n^{\frac{1}{2}} N \sum_{d\le N} \sigma_{-\frac{1}{2}}(d)\right) = O\left(n^{\frac{1}{2}} N^2\right) \tag{29}$$

and then tidy up (28) further by estimating the tail

$$\sum_{k>N} A(n,k) \tag{30}$$

of the singular series $\mathfrak{S}(n)$. This,[6] much as in (22) and (23), is majorized by

$$\sum_{k>N} |A(n,k)| \le \frac{1}{N^{\frac{1}{2}-\varepsilon}} \sum_{k=1}^{\infty} k^{\frac{1}{2}-\epsilon} A(n,k)$$
$$\le \frac{1}{N^{\frac{1}{2}-\varepsilon}} \prod_p \left(1 + \frac{B_1(p,n)^{\frac{1}{2}}}{p^{1+\varepsilon}} + \frac{B_1}{p} \sum_{\alpha=2}^{\infty} \frac{1}{p^{\alpha\epsilon}}\right)$$
$$\le \frac{1}{N^{\frac{1}{2}-\epsilon}} \prod_p \left\{1 + \frac{B_1(p,n)^{\frac{1}{2}}}{p^{1+\epsilon}} + \frac{B_1}{p^{1+2\epsilon}} \left(1 - \frac{1}{2^\epsilon}\right)^{-1}\right\}$$

[6] see footnote 4

$$< \frac{1}{N^{\frac{1}{2}-\epsilon}} \prod_p \left(1 + \frac{B_2(\epsilon)}{p^{1+\epsilon}}\right) \prod_{p|n} B_3(\epsilon)$$

$$< \frac{B_4(\epsilon)\{B_3(\epsilon)\}^{\omega(n)}}{N^{\frac{1}{2}-\epsilon}} \quad < \quad \frac{B_5(\epsilon)}{N^{\frac{1}{2}-\epsilon}}$$

by (19), (21), (25), and the multiplicativity of $A(n,k)$, whence (30) is $O\left(N^{-\frac{1}{2}+\epsilon}\right)$. Therefore, summing up the effects of this, (29), and (28), we conclude that

$$(31)\quad 2\pi\nu_1(n) = \frac{2\pi\Gamma\left(\frac{3}{2}\right)\Gamma\left(\frac{1}{\ell}+1\right)}{\Gamma\left(\frac{3}{2}+\frac{1}{\ell}\right)} n^{\frac{1}{2}+\frac{1}{\ell}} \mathfrak{S}(n) + O\left(n^{\frac{1}{2}+\frac{1}{\ell}} N^{-\frac{1}{2}+\epsilon}\right) + O\left(n^{\frac{1}{2}} N^2\right)$$

$$= \frac{2\pi\Gamma\left(\frac{3}{2}\right)\Gamma\left(\frac{1}{\ell}+1\right)}{\Gamma\left(\frac{3}{2}+\frac{1}{\ell}\right)} n^{\frac{1}{2}+\frac{1}{\ell}} \mathfrak{S}(n) + O\left(n^{\frac{1}{2}+\frac{4}{5\ell}+\epsilon}\right)$$

after we choose N in (25) to be $n^{\frac{2}{5\ell}}$.

6. Estimates for $\nu_2(n)$and $\nu(n)$. In treating $\nu_2(n)$ through the series (10) we encounter the theory of Dirichlet's L-functions, the first needed result in which is the classical

LEMMA 1. *Let $L(s,\chi_k)$ denote the Dirichlet's L -function formed with the non-principal character χ_k,* modulo k. *Then*

$$L(1,\chi_k) \quad = \quad O(\log\ 2k)$$

and

$$\sum_{m>y} \frac{\chi_k(m)}{m} \quad = \quad O(\log 2k).$$

These bounds suffice for only a minor part of our work. For most of the analysis, we shall require a result that substantially improves the second estimate above for characters associated with most primitive characters χ_q^*, modulo q, and that we embody in

LEMMA 2. *Let η_1,η_2 be any positive constants (less than* 1*) and suppose that $\eta_3 = \eta_3(\eta_1,\eta_2)$ is a sufficiently small positive constant. Then, save when the non-principal character χ_k,* mod *k, is associated with at most $O(Y^{\eta_1})$ exceptional primitive characters χ_q^* ,* mod *q , we have*

$$\sum_{m>y} \frac{\chi_k(m)}{m} = O\left(\frac{1}{Y^{\eta_3}}\right)$$

for $k \le 4Y$ and[7] $Y^{\eta_2} \le y \le Y$.

We only outline the proof because it depends on an order of ideas that is by now familiar to practitioners in this part of the subject.

Letting $N(\sigma_1,T,\chi_q^*)$ denote the number of zeros of $L(s,\chi_q^*)$ lying in the region $\sigma \ge \sigma_1 \ge \frac{4}{5}, |t| \le T$, we start with Montgomery's estimate

$$\sum_{q\le Q} \sum_{\chi_q^*} N(\sigma_1,T,\chi_q^*) = O\{(Q^2T)^{2(1-\sigma_1)/\sigma_1} \log^{14} QT\} \quad (T > 2)$$

[7]The imposition of the upper bound Y for k is clearly unnecessary but makes the exposition a little easier.

that he stated and proved in his monograph [8]. If in this we set

$$Q = 4Y, \quad T = 2Y^3, \quad \sigma_1 = 1 - \frac{1}{12}\eta_1 > \frac{11}{12}$$

for large Y, its right-hand side becomes

$$O\left(Y^{\frac{10}{11}\eta_1} \log^{14} Y\right) = O\left(Y^{\eta_1}\right)$$

so that $L(s, \chi_q^*)$ and all associated functions $L(s, \chi_k)$ have no zeros in the region R

$$\sigma > 1 - \frac{1}{12}\eta_1, \quad |t| < T$$

unless q belong to an exceptional set of cardinality $O(Y_1^{\eta})$. Then, excluding consideration of the L-functions appertaining to the aberrant set, we apply the Borel-Carathéodory theorem and Hadamard's three circles theorem in the usual way (see, for example, the argument in Titchmarsh [9], Chapter XIV, §14.2) to the function $\log L(s, \chi_k)$, which is regular in R and is subject there to the inequality

$$\Re \log L(s, \chi_k) < B_6 \log Y$$

in view of the basic relation $L(s, \chi_k) = O\{k|s| + 1)\}$ that is valid for $\sigma \geq \frac{1}{2}$. From the former theorem it follows that

$$|\log L(s, \chi_k)| < B_7 \log Y$$

for $\sigma > 1 - \frac{1}{13}\eta_1, |t| < T - 1$ and then from the latter that

$$|\log L(s, \chi_k)| < \log^{\eta_4} Y$$

for $\sigma \geq 1 - \frac{1}{14}\eta_1, |t| \leq \frac{1}{2}T$,and some positive absolute constant η_4 less than 1; hence in the last region

$$L(s, \chi_k) = O(Y^{\epsilon}). \tag{32}$$

Next, if y be equal to $\frac{1}{2}$ plus an integer in the first place, the usual contour integral methods shew that, for $c > 0$,

$$\sum_{m>y} \frac{\chi_k(m)}{m} = L(1, \chi_k) - \sum_{m \leq y} \frac{\chi_k(m)}{m} = L(1, \chi_k) - \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} L(1+s, \chi_k) \frac{y^s}{s} ds$$

and then that

$$\begin{aligned} &\sum_{m>y} \frac{\chi_k(m)}{m} \\ &= \frac{1}{2\pi i} \int_{-\frac{1}{14}\eta_1 - \frac{1}{2}iT}^{-\frac{1}{14}\eta_1 + \frac{1}{2}iT} L(s, \chi_k) \frac{y^s}{s} ds + O\left(\frac{y^2}{T} \max_{-\frac{1}{14}\eta_1 \leq \sigma \leq 2} |L(1 + \sigma + \frac{1}{2}iT, \chi_k)|\right) \\ &+ O\left(\frac{y^2}{T} \sum_{m=1}^{\infty} \frac{|\chi_k(m)|}{m^3 |\log y/m|}\right) \end{aligned}$$

$$= \frac{1}{2\pi i}\int_{-\frac{1}{14}\eta_1-\frac{1}{2}iT}^{+\frac{1}{14}\eta_1+\frac{1}{2}iT} L(s,\chi_k)\frac{y^s}{s}ds + O\left(\frac{y^2}{T}\max_{-\frac{1}{14}\eta_1\le\sigma\le 2}|L(1+\sigma+\frac{1}{2}iT,\chi_k)|\right)$$
$$+O\left(\frac{y^2}{T}\sum_{m=1}^{\infty}\frac{1}{m^2}\right),$$

from which, by (32), we deduce that

$$\sum_{m>y}\frac{\chi_k(m)}{m} = O\left(Y^{\epsilon}y^{-\frac{1}{14}\eta_1}\int_0^T\frac{dt}{\eta_1+t}\right)+O\left(\frac{Y^{\epsilon}}{Y}\right)$$
$$= O\left(Y^{\epsilon-\frac{1}{14}\eta_1\eta_2}\right) = O\left(Y^{-\frac{1}{15}\eta_1\eta_2}\right).$$

This establishes the lemma with the value $\frac{1}{15}\eta_1\eta_2$ for η_3, since the initial restriction on y is now seen to be irrelevant.

From the multiplicativity of $A_3(n_1,k)$ and the representation of $A(n_1,k_1)$ through (10) we first express the term $A_3(n-W^\ell,k)$ in $\theta_2(n-W^\ell)$ as

$$\sum_{\substack{a^2 2^\alpha d^2 b=k\\(ab,2)=1;d^2|(n-W^\ell)}}\frac{\mu^2(a)}{a^2}\frac{A_3(n-W^\ell,2^\ell)}{2^\alpha}\frac{1}{d}\left(\frac{-(n-W^\ell)/d^2}{b}\right)\frac{1}{b} \tag{33}$$

and then dissect it by writing the sum as

$$\sum_{a^2 2^\alpha d^2>N^{\frac{1}{2}}} + \sum_{a^2 2^\alpha d^2\le N^{\frac{1}{2}}} = A_3'(n-W^\ell,k)+A_3''(n-W^\ell,k),\ \text{say,} \tag{34}$$

letting the respective contributions of these two portions to $\theta_2(n-W^\ell)$ be indicated by $\theta_2'(n-W^\ell)$ and $\theta_2''(n-W^\ell)$. Next

$$\theta_2'(n-W^\ell) \tag{35}$$
$$= \sum_{\substack{a^2 2^\alpha d^2>N^{\frac{1}{2}}\\(a,2)=1;d^2|(n-W^\ell)}}\frac{\mu^2(a)}{a^2}\frac{A_3(n-W^\ell,2^\alpha)}{2^\alpha}\frac{1}{d}\sum_{\substack{b>N/a^2 2^\alpha d^2\\(b,2)=1}}\left(\frac{-(n-W^\ell)/d^2}{b}\right)\frac{1}{b},$$

wherein $A_3(n-W^\ell,2^\alpha)$ is $O(2^{\frac{1}{2}\alpha})$ by (13) and wherein the inner sum is either $L_{-(n-W^\ell)d^2}(1)$ or a tail of the series representing it. Hence, by Lemma 1 and a crude calculation that suffices in current circumstances,

$$\theta_2'(n-W^\ell) = O\left(\log n\sum_{\substack{a^2 2^\alpha d^2>N^{\frac{1}{2}}\\d^2|(n-W^\ell)}}\frac{1}{a^2 2^{\frac{1}{2}\alpha}d}\right) = O\left(\frac{\log n}{N^{\frac{1}{8}}}\sum_{\substack{a,\alpha\\d^2|(n-W^\ell)}}\frac{1}{a^{\frac{3}{2}}2^{\frac{1}{4}\alpha}d^{\frac{1}{2}}}\right)$$
$$= O\left(\frac{\log n\, d(n-W^\ell)}{N^{\frac{1}{8}}}\right) = O\left(\frac{1}{N^{\frac{1}{9}}}\right),$$

the contribution to $\nu_2(n)$ in (24) being

$$O\left(\frac{1}{N^{\frac{1}{9}}}\sum_{W<n^{\frac{1}{\ell}}}(n-W^\ell)^{\frac{1}{2}}\right) = O\left(n^{\frac{1}{2}+\frac{1}{\ell}-\frac{2}{45\ell}}\right) = O\left(n^{\frac{1}{2}+\frac{43}{45\ell}}\right) \tag{36}$$

by the choice of N in (31).

Parallel with (35), there is the equation

$$\theta_2''(n-W^\ell) = \sum_{\substack{a^2 2^\alpha d^2 \le N^{\frac{1}{2}} \\ (a,2)=1; d^2 | (n-W^\ell)}} \frac{\mu^2(a)}{a^2} \frac{A_3(n-W^\ell, 2^\alpha)}{2^\alpha} \frac{1}{d} \sum_{\substack{b > N/a^2 2^\alpha d^2 \\ (b,2)=1}} \left(\frac{-(n-W^\ell)/d^2}{b}\right) \frac{1}{b}, \tag{37}$$

for whose application we use Lemmata 1 and 2. In the latter lemma let us take $Y = n, \eta_1 = 1/3\ell, \eta_2 = 1/5\ell$, and set $\eta = \eta_3(1/3\ell, 1/5\ell)$. Then, since the lower bound above for b lies between $N^{\frac{1}{2}} = n^{\frac{1}{5\ell}}$ and N, the inner sum in (37) is

$$O\left(\frac{1}{n^\eta}\right)$$

when the unique primitive character associated with all the characters $(-(n-W^\ell)/d^2|b)$ for given W does not belong to an exceptional set with $O\left(n^{\frac{1}{3\ell}}\right)$ members. In this situation, by (13) again,

$$\begin{aligned} \theta_2''(n-W^\ell) &= O\left(\frac{1}{n^\eta} \sum_{\substack{a^2 2^\alpha d^2 \le N^{\frac{1}{2}} \\ (a,2)=1; d^2 | (n-W^\ell)}} \frac{\mu^2(a)}{a^2} \cdot \frac{1}{2^{\frac{1}{2}\alpha}} \cdot \frac{1}{d}\right) \\ &= O\left(\frac{1}{n^\eta} \sum_{\substack{a,\alpha \\ d^2 | (n-W^\ell)}} \frac{1}{a^2 2^{\frac{1}{2}\alpha} d}\right) \\ &= O\left(\frac{d(n-W^\ell)}{n^\eta}\right) = O\left(\frac{1}{n^{\frac{1}{2}\eta}}\right), \end{aligned} \tag{38}$$

and the effect of this on $\nu_2(n)$ due to the relevant values of W is

$$O\left(\frac{1}{n^{\frac{1}{2}\eta}} \sum_{W < n^{\frac{1}{\ell}}} (n-W^\ell)^{\frac{1}{2}}\right) = O\left(n^{\frac{1}{2}+\frac{1}{\ell}-\frac{1}{2}\eta}\right). \tag{39}$$

On the other hand, by Lemma 1 and similar reasoning, we always have

$$\theta_2''(n-W^\ell) = O\left(\log n \; d(n-W^\ell)\right) = O(n^\epsilon), \tag{40}$$

to which we must have recourse when $(-(n-W^\ell)|b)$ is associated with an exceptional primitive character. In this case, if

$$(n-W^\ell) = D\Omega^2 \tag{41}$$

as in the exposition in §3, the primitive character connected with $(-(n-W^\ell)|b)$ has modulus $2D$ or $4D$, this being unique for each value of D. Thus here the number of positive integers D that can occur in (41) is $O(n^{1/3\ell})$, to each of which there appertain the positive integers W satisfying (41). But, since (41) is an absolutely irreducible

equation in W and Ω in which we require that $0 < W, \Omega \leq n^{\frac{1}{2}}$, an important theorem due to Bombieri and Pila [1] shews that the number of relevant solutions has cardinality[8] $O(n^{(1/2\ell+\epsilon)})$. Consequently the set of W for which we must employ (40) has cardinality $O(n^{\frac{5}{6\ell}+\epsilon})$ and we deduce that their effect on $\nu_2(n)$ by way of (24) is

$$O\left(n^{\frac{1}{2}+\frac{6}{7\ell}}\right). \tag{42}$$

To sum up what has so far been achieved we let $\delta = \delta(\ell)$ denote a suitable positive constant that is not necessarily the same at all times. Then, gathering up (36), (39), and (42), we get

$$\nu_2(n) = O\left(n^{\frac{1}{2}+\frac{1}{\ell}-\delta}\right), \tag{43}$$

which combined with (31) and (24) leads us to the first form

$$\nu(n) = \frac{8\Gamma^3\left(\frac{3}{2}\right)\Gamma\left(\frac{1}{\ell}+1\right)}{\Gamma\left(\frac{3}{2}+\frac{1}{\ell}\right)} n^{\frac{1}{2}+\frac{1}{\ell}}\mathfrak{S}(n) + O\left(n^{\frac{1}{2}+\frac{1}{\ell}-\delta}\right) \tag{44}$$

of the asymptotic formula we were seeking.

It would be premature to attempt to read off conclusions from this formula until the singular series has been studied in more detail, since it is possible that the explicit term might not dominate even when $\mathfrak{S}(n) \neq 0$. Indeed, as we shall see, there is a clearly defined set of circumstances in which this situation occurs, it then being necessary to rehabilitate the asymptotic formula by a further analysis.

7. The singular series revisited. We look back at the final paragraph in §4 and see that

$$\begin{aligned} \mathfrak{S}(n) &= \prod_p \left(1 + A(n,p) + A(n,p^2) + \cdots\right) \\ &= \prod_p \lim_{\alpha\to 0} \frac{\tau(n,p^\alpha)}{p^{3\alpha}} = \prod_p \Theta(h,p), \text{ say,} \end{aligned} \tag{45}$$

which equation will be the source for lower bounds for $\mathfrak{S}(n)$ based on a study of $\tau(n,p^\alpha)$. In the interests of simplicity we avoid any appeal to the fact that $\tau(n,p^\alpha)/p^{3\alpha}$ is independent of α for $\alpha > \alpha_0(n,p)$ because, in contrast to the classical case of unmixed powers, the proof of this is not entirely straightforward and is probably best founded on the properties of the sums $S_2(h,k)$ and $S_\ell(h,k)$. Instead, we shall usually merely lean heavily on the simply proved Principal A to the effect that *a contribution of* $p^{3(\alpha-1)}$ *to* $\tau(n,p^\alpha)$ *is due from each solution,* mod p, *of*

$$X_1'^2 + X_2'^2 + X_3'^2 + W'^\ell \equiv n, \text{ mod } p, \tag{46}$$

for which either $X_i' \not\equiv 0, \text{mod} p$, *for some* i *when* $p \neq 2$ *or* $W' \not\equiv 0, \text{mod } p$, *when* $p \nmid \ell$, all such solutions being *primitive* in the sense that $p \nmid (X_1', X_2', X_3', W')$.

First let us consider the case $p \neq 2$, for which we examine separately the situations where (i) $p \nmid n$, $p \nmid \ell$, (ii) $p|n$, and (iii) $p \nmid n$, $p|\ell$. In the first instance, since all

[8] If ℓ be even, the properties of the Pellian equation imply more easily that the exponent of n in the estimate may be replaced by ϵ.

$\tau(n,p)$ incongruent solutions of (46) are primitive and therefore adhere to the data in Principle A,

$$\frac{\tau(n,p^\alpha)}{p^{3\alpha}} = \frac{\tau(n,p)}{p^3} = 1+O\left(\frac{1}{p^{\frac{3}{2}}}\right)$$

and

$$\frac{\tau(n,p^\alpha)}{p^{3\alpha}} \geq 1-\frac{1}{p} > 0$$

by (19) and (20). In the second instance there are

$$\tau(n,p)-1 \geq p^3-p^2+1-1 = p^3-p^2$$

incongruent primitive solutions of (46), of which all satisfy the conditions in Principle A because at least two components in a primitive solution are incongruent to 0, mod p, when $p|n$; thus here

$$\frac{\tau(n,p^\alpha)}{p^{3\alpha}} \geq 1-\frac{1}{p}.$$

Lastly, in the third instance, there are not less than p^3-p^2 incongruent primitive solutions of (46), the number satisfying $X_1' \equiv X_2' \equiv X_3' \equiv 0$, mod p, being obviously less than p; hence

$$\frac{\tau(n,p^\alpha)}{p^{3\alpha}} \geq \frac{1}{p^3}\left(p^3-p^2-p\right) > 1-\frac{2}{p}.$$

Thus, gathering what we have so far obtained, we conclude that

$$\prod_{p>2}\Theta(n,p) > B_6 \prod_{\substack{p|n \\ p\nmid 2}}\left(1-\frac{1}{p}\right) > B_7\frac{\phi(n)}{n} \tag{47}$$

for some positive absolute constant B_7.

Let us now suppose that $p=2$. If ℓ be odd, we confirm that there is a solution of the congruence

$$X_1'^2+X_2'^2+X_3'^2+W'^{\ell} \equiv n, \text{ mod } 8 \tag{48}$$

for which $W' \equiv 1$, mod 2, whence

$$\frac{\tau(n,2^\alpha)}{2^{3\alpha}} \geq \frac{1}{2^9} \qquad (\ell \text{ odd}) \tag{49}$$

for $\alpha \geq 3$. But, if ℓ be even, we have more difficulty with the treatment, which will often depend on the principle B to the effect that, *if the congruence* $Y^2 \equiv H$, mod 8, *with odd* H *have a solution* U, mod 8, *then the congruence* $Y_1^2 \equiv H_1$, mod 2^α, *with* $H_1 \equiv H$, mod 8, *has a solution* Y_1 *congruent to* Y, mod 8, *when* $\alpha > 3$. This criterion is, of course, a reflection of the fact that the necessary and sufficient condition for the solubility of $Y_1^2 \equiv H_1$, mod 2^α, for $\alpha \geq 3$ and odd H_1 is that $H_1 \equiv 1$, mod 8.

We write $2^\beta || n$ so that $n = 2^\beta n_1$ where n_1 is odd. Then first, if $\beta \leq 2$, the congruence (48) is seen to have a solution in which X_1' is odd because $X_i'^2 \equiv W'^2 \equiv 1$, mod 8, when X_1' and W' are odd. Hence, by Principle B,

$$\tau(n, 2^\alpha) \geq 2^{3(\alpha-3)}$$

and

$$\frac{\tau(n, 2^\alpha)}{2^{3\alpha}} \geq \frac{1}{2^9} \qquad (\alpha \geq 3). \tag{50}$$

If, however, $\beta > 2$, the situation becomes more complicated because of a phenomenon that is already familiar in connection with Lagrange's theorem for four squares. Since ℓ is even, the solutions of the underlying congruence

$$X_1^2 + X_2^2 + X_3^2 + W^\ell \equiv 2^\beta n_1, \text{ mod } 2^\alpha, \tag{51}$$

are contained in an obvious way in those of

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 \equiv 2^\beta n_1, \text{ mod } 2^\alpha, \tag{52}$$

in which, if $2^\gamma || (X_1, \cdots, X_4)$ so that $X_i = 2^\gamma X_i'$ and (X_1', X_2', X_3', X_4') is odd, then

$$2^{2\gamma}(X_1'^2 + X_2'^2 + X_3'^2 + X_4'^2) \equiv 2^\beta n_1, \text{ mod } 2^\alpha, \tag{53}$$

where we may assume that $\alpha > \beta$. Certainly $2\gamma \geq \beta$, while the inequality $2\gamma \leq \beta - 3$ would imply the impossible congruence $X_1'^2 + X_2'^2 + X_3'^2 + X_4'^2 \equiv 0$, mod 8. Hence, writing $\beta = 2r + 1$ or $\beta = 2r + 2$ for $r \geq 1$ according as β is odd or even, we infer that $\gamma = r$ if β be odd but that $\gamma = r$ or $r + 1$ if β be even.

Scrutinizing the former situation, we see that for $\alpha \geq 2r + 3$ the congruence (52) is equivalent to

$$X_1'^2 + X_2'^2 + X_3'^2 + X_4'^2 \equiv 2n_1, \text{ mod } 2^{\alpha-2r},$$

when X_4' therein is specialized by writing X_4 in (52) as $W^{\ell'}$ where $\ell' = \frac{1}{2}\ell$. Now X_4 is divisible by 2^r if and only if W be divisible by 2^s, where s is the least integer not less than r/ℓ' and where therefore

$$s = \frac{r}{\ell'} + \frac{\theta}{\ell} \tag{54}$$

for a suitable *even* integer θ between 0 and $\ell - 2$ inclusive; thus (51) is tantamount to the condition

$$X_1'^2 + X_2'^2 + X_3'^2 + 2^\theta W'^\ell \equiv 2n_1, \text{ mod } 2^{\alpha-2r}, \tag{55}$$

which surely implies that $(X_1', X_2', X_3', 2^\theta W')$ is odd and which, for $\alpha = 2r+3$, is always soluble with a solution X_1', X_2', odd $W' \equiv 0$, mod 8, $X_3' \equiv 0$ or 2, according as $n_1 \equiv 1$ or 3, mod 4. Hence, by Principle B, the solutions of (55) for $\alpha > 2r + 3$ belong to not less than $2^{3(\alpha-2r-3)}$ residue classes, each one that is represented by X_1', X_2', X_3', W', say, giving rise to residue class solutions $X_i \equiv 2^r X_i'$, mod $2^{\alpha-r}$, $W \equiv 2^s W'$, mod $2^{\alpha-2r+s}$, of (50) where s is given in (54) and $s \leq r$. Thus when $\beta > 2$ is odd we infer that for $\alpha > 2r + 3$

$$\tau(n, 2^\alpha) \geq 2^{3(\alpha-2r-3)} 2^{3r} 2^{2r-s} = 2^{3\alpha-r-s-9}$$

and

$$\frac{\tau(n,2^\alpha)}{2^{3\alpha}} \geq \frac{1}{2^{2r+9}} = \frac{1}{2^8 2^\beta} = \frac{n_1}{2^8 n}, \tag{56}$$

which remains true for $\beta = 1$ by (50)

Let now β be even so that $\gamma = r$ or $r+1$, the congruences springing from (52) being respectively

$$X_1'^2 + X_2'^2 + X_3'^2 + X_4'^2 \equiv 4n_1, \mod 2^{\alpha-2r}, \quad (\alpha \geq 2r+3)$$
$$X_1'^2 + X_2'^2 + X_3'^2 + X_4'^2 \equiv n_1, \mod 2^{\alpha-2r}, \quad (\alpha \geq 2r+5).$$

In the first instance, by the previous argument, $X_4' = 2^{\frac{1}{2}\theta} W'^{\ell'}$ where θ is still defined by (54), while in the second $X_4' = 2^{\frac{1}{2}\theta_1} W'^{\ell'}$ where θ_1 is the even integer between 0 and $\ell - 2$ for which $(2r+\theta_1)/\ell$ is an integer. Hence we obtain the congruences

$$X_1'^2 + X_2'^2 + X_3'^2 + 2^\theta W'^\ell \equiv 4n_1, \mod 2^{\alpha-2r}, \tag{57}$$

and

$$X_1'^2 + X_2'^2 + X_3'^2 + 2^{\theta_1} W'^\ell \equiv n_1, \mod 2^{\alpha-2r-1}, \tag{58}$$

the primitivity of solutions corresponding to the condition that (X_1', X_2', X_3', X_4') be odd being assured in (58) but needing the stipulation that $(X_1', X_2', X_3', 2^\theta W')$ be odd in (57). Next, if $\alpha = 2r+3$, the first congruence (57) is seen to have the solution $X_1' \equiv X_2' \equiv X_3' \equiv W' \equiv 1, \mod 8$, when $\theta = 0$ but has no appropriate solutions when $\theta > 0$. Similarly, if $\alpha = 2r+5$, the congruence (58) is soluble when $\theta_1 = 0$ or 2 but is otherwise only soluble if $n_1 \not\equiv 7, \mod 8$. Consequently, by following the later reasoning in the previous paragraph with the aid of Principle B, we conclude that

$$\frac{\tau(n,2^\alpha)}{2^{3\alpha}} > \frac{B_8}{2^{2r}} > \frac{B_8 n_1}{n} \tag{59}$$

whenever the above conditions for the solubility of (57) for $\alpha = 2r+3$ or (58) for $\alpha = 2r+5$ are met. Furthermore, although unnecessary here, we could with a little more effort produce a numerical value for B_8.

It is helpful to look a little further at the conditions of solubility for even ℓ before we return to the singular series and asymptotic formula. By (54) the equation $\theta = 0$ is tantamount to $2r \equiv 0, \mod \ell$, while similarly each requirement $\theta_1 = 0$, $\theta_1 = 2$ means respectively that $2r+2 \equiv 0, \mod \ell$, $2r+4 \equiv 0, \mod \ell$. Hence, since $\beta = 2r+2$, one or other of the congruences (57) and (58) is soluble in the appropriate sense if and only

$$\left.\begin{array}{c}\text{either one of } \beta-2, \beta, \beta+2 \text{ is congruent to } 0, \mod \ell, \\ \text{or} \qquad n_1 \not\equiv 7, \mod 8,\end{array}\right\} \tag{60}$$

the condition being certainly also fulfilled in the special cases $\beta = 0$ and $p = 2$ for which (59) is implied by (48).

Thus, for example, (60) is certainly always valid for $\ell \leq 6$ but must be replaced by $\tau(n,2^\alpha) = 0$ for some values of n when $\ell \geq 8$. In the latter case, of course, $\nu(n)$ is obviously zero, as is the singular series $\mathfrak{S}(n)$.

In summation, starting from (45) and (47), for odd $\ell > 2$ we deduce from (49) that

$$\mathfrak{S}(n) > \frac{B_9}{\log\log n} \tag{61}$$

but for even $\ell \geq 2$ can only deduce from (56) and (59) that

$$C(n) > \frac{B_9 n_1}{n \log\log n} \tag{62}$$

when

$$\text{either } \beta \text{ is odd or (60) holds;} \tag{63}$$

otherwise $\mathfrak{S}(n) = 0$.

The final theorems

Having completed our study of the singular series, we are ready to enunciate the first version of our theorem, which, as we shall see, does not yet represent all we would wish. We infer first from (61) that the explicit term in the right side of the asymptotic formula (44) is certainly dominant when ℓ is odd; on the other hand, if ℓ be even and the necessary condition (63) for the non-vanishing of $\nu(n)$ be in place, then we can only depend on the dominance of the explicit term when the power $2\beta = n/n_1$ in n does not exceed $n^{\delta-\epsilon}$, the asymptotic formula becoming nugatory when (63) fails. We consequently have arrived at

THEOREM 1. *If $\nu(n)$ be the number of representations of a (large) number n as the sum of three squares and an ℓ-th power, we have*

(i) *if $\ell > 2$ be odd, then*

$$\nu(n) \sim \frac{8\Gamma^3\left(\frac{3}{2}\right)\Gamma\left(\frac{1}{\ell}+1\right)}{\Gamma\left(\frac{3}{2}+\frac{1}{\ell}\right)} n^{\frac{1}{2}+\frac{1}{\ell}} \mathfrak{S}(n) \tag{64}$$

as $n \to \infty$:

(ii) *let $\ell > 2$ be even and $n = 2^\beta n_1$, where n_1 is odd and $2^\beta < n^\delta$ for some small positive number δ; then the asymptotic formula* (64) *is still valid when condition* (63) *above holds:*

(iii) *in the situations outlined above a large number n is representable as the sum of three squares and an ℓ-th power; but, if* (63) *fail, there are no such representations and the asymptotic formula is trivial.*

As it stands, this theorem suffers from the imperfection that a limitation has been placed on the size of the power of 2 in n when ℓ is even. This restriction, however, is not essential and would not have appeared had we adopted a more indirect approach in preference to one that made the principles behind the method more transparent. We therefore now briefly sketch what is needed to gain a superior result, confining ourselves for the sake of brevity to the case where β is odd

The most important change arises at the beginning when the given indeterminate equation

$$X_1^2 + X_2^2 + X_3^2 + W^\ell = 2^\beta n_1 \tag{65}$$

is forthwith transformed into

$$X_1^2 + X_2^2 + X_3^2 + 2^\theta W'^\ell = 2n_1 \tag{66}$$

by the method used to develop the congruence (55) from (51). From this we proceed to express $\nu(n)$ as

$$\sum_{0<W<2^{(1-\theta)/\ell}} r(2n_1 - 2^\theta W^\ell) + O(1),$$

to which representation the processes of §5 are applied as before save that now (i) $\tau(n,d)$ and $A(n,k)$ are respectively replaced by the number $\gamma'(m,d)$ of incongruent solutions of

$$X_1^2 + X_2^2 + X_3^2 + 2^\theta W^\ell \equiv 2n_1, \bmod d,$$

and

$$A'(n_1,k) = \sum_{d|k} \mu\left(\frac{k}{d}\right) \frac{\tau'(n_1,d)}{d^3}$$

(ii) the bound $n^{\frac{1}{\ell}}$ is superseded by $2^{(1-\theta)/\ell} n_1^{\frac{1}{\ell}}$ so that the analogue of the right-side of (27) has $2^{\frac{1}{2}+(1-\theta)/\ell} n_1^{\frac{1}{2}+\frac{1}{\ell}}$ in place of $n^{\frac{1}{2}+\frac{1}{\ell}}$ in the main term and has remainder term $O(n_1^{\frac{1}{2}})$. Our first deduction therefore is that, if $\mathfrak{S}'(n)$ formed from $A'(n,k)$ be the singular series associated with (67) and if the number $N_1 = n_1^{\frac{2}{5\ell}}$ be used instead of N, then a valid formula for $\nu_1(n)$ is retained when the entries $n^{\frac{1}{2}+\frac{1}{\ell}}\mathfrak{S}(n)$ and $n^{\frac{1}{2}+\frac{4}{5\ell}+\epsilon}$ in (31) are replaced by $2^{\frac{1}{2}+\frac{(1-\theta)}{\ell}} n_1^{\frac{1}{2}+\frac{1}{\ell}} \mathfrak{S}'(n_1)$ and $n_1^{\frac{1}{2}+\frac{4}{5\ell}+\epsilon}$. Also, since the consequential changes in the treatment of §6 due to the new approach are of a minor nature, we assess $\nu_2(n)$ as in (43) but with n_1 replacing n in the estimate. Thus, in all, we infer that

$$\nu(n) = \frac{8\Gamma^3\left(\frac{3}{2}\right)\Gamma\left(\frac{1}{\ell}+1\right)}{\Gamma\left(\frac{3}{2}+\frac{1}{\ell}\right)} 2^{\frac{1}{2}+\frac{(1-\theta)}{\ell}} \mathfrak{S}(n_1) n_1^{\frac{1}{2}+\frac{1}{\ell}} + O\left(n_1^{\frac{1}{2}+\frac{1}{\ell}-\delta}\right) \tag{67}$$

in parallel with the original formula (45).

To judge the significance of the new formula we must examine the singular series

$$\mathfrak{S}'(n_1) = \prod_p \lim_{\alpha\to\infty} \frac{\tau'(n_1,p^\alpha)}{p^{3\alpha}} = \prod_p \Theta'(n_1,p), \text{ say,} \tag{68}$$

noting immediately that for $p \neq 2$ we have $\tau'(n_1,p^\alpha) = \tau(n,p^\alpha)$ and hence

$$\Theta'(n,p) = \Theta(n,p) \qquad (p \neq 2) \tag{69}$$

because of the way (66) arose from (65). It is thus only the prime 2 that affects the scene, in which first $\tau'(n_1,2^\alpha) \geq 2^{3(\alpha-3)}$ for $\alpha \geq 3$ and hence $\Theta'(n_1 p) \geq \frac{1}{2^9}$ by the reasoning following (55). Therefore, by this, (69), (68) and (47), we confirm that (67) supplies a genuine asymptotic formula in which the explicit term preponderates.

Furthermore, a slight gloss on the argument after (55) shews that

$$\frac{\tau(n,2^\alpha)}{2^{3\alpha}} = \frac{1}{2^{r+s}} \cdot \frac{\tau'(n,2^{\alpha-2r})}{2^{3(\alpha-2r)}} \qquad (\alpha > 2r+3)$$

by way of the equation $\tau(n, 2^\alpha) = 2^{5r-s}\tau'(n, 2^{\alpha-2r})$ so that, letting $\alpha \to \infty$, we infer that

$$\Theta(n, 2) = \frac{1}{2^{r+s}}\Theta'(n_1, 2),$$

while, by (54) and the stated equality $\beta = 2r + 1$, we also have that

$$\frac{n^{\frac{1}{2}+\frac{1}{\ell}}}{2^{\ell+s}} = 2^{\{(\frac{1}{2}+\frac{1}{\ell})\beta-r-s\}}n_1^{\frac{1}{2}+\frac{1}{\ell}} = 2^{\{(\frac{1}{2}+\frac{1}{\ell})(2r+1)-r-\frac{2r}{\ell}-\frac{\theta}{\ell}\}}n_1^{\frac{1}{2}+\frac{1}{\ell}} = 2^{\frac{1}{2}+\frac{(1-\theta)}{\ell}}n_1^{\frac{1}{2}+\frac{1}{\ell}}.$$

Added to (69), these facts demonstrate that the main terms in (44) and the substitute formula (67) are the same, and we conclude therefore that $\nu(n)$ is asymptotic to the first provided only that $n_1 \to \infty$.

As similar, but more complicated, thinking is successful in the other case where ℓ and β are both even, we reach our second inference in the form of

THEOREM 2. *The conclusion in part* (ii) *of Theorem 1 is yet valid when it is only assumed that* $n_1 \to \infty$, *there being no other condition on* β *required save* (63); *part* (iii) *is then to be interpreted in the light of the revised part* (ii).

Thus we have achieved our goal of obtaining an asymptotic formula for $\nu(n)$ in all cases where the odd part n_1 of n tends to infinity. The missing situation when $2^\alpha \to \infty$ and n_1 is bounded is of no significance except when $\ell = 2$, in which event there is Jacobi's exact formula for $\nu(n)$ (H,p 216).

REFERENCES

[1] E. BOMBIERI AND J. PILA, *The number of integral points on arcs and ovals*, Duke Math. J., 59 (1989), pp. 337–357.

[2] R. F. CHURCHHOUSE, *Representation of integers by sums of mixed powers*, Proceedings of the third Caribbean Conference on Combinatorics and Computing (Bridgetown, 1981), Univ. West Indies, Cave Hill Campus, Bridgetown, Barbados, pp. 15–22, 1981.

[3] T. ESTERMANN, *On the representations of a number as a sum of three squares*, Proc. London Math. Soc. (3), 9 (1959), pp. 575–594.

[4] G. H. HARDY, *On the representation of a number as the sum of any number of squares, and in particular of five,* Transactions of the American Mathematical Society, 21 (1920), pp. 255–284.

[5] C. HOOLEY, *On the representation of a number as the sum of a square and a product,* Math. Zeitschr., 69 (1958), pp. 211–227.

[6] C. HOOLEY, *Some recent advances in analytical number theory,* Proc. of the International Congress of Mathematicians, August 16–24, 1983, Warsaw.

[7] LOO KENG HUA, *Introduction to Number Theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1982.

[8] H. L. MONTGOMERY, *Topics in Multiplicative Number Theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1982.

[9] E. C. TITCHMARSH, *The Theory of the Riemann Zeta-Function*, Oxford, 1951.

[10] I. M. VINOGRADOV, *The Method of Trigonometrical Sums in the Theory of Numbers*, Interscience Publishers Ltd.