ACTA ARITHMETICA
LXXIX.4 (1997)

On a problem of Hardy and Littlewood

by

Christopher Hooley (Cardiff)

1. Introduction. Amongst many important statements in their famous memoir *Some problems of 'Partitio numerorum'*; *III*, Hardy and Littlewood ([1]) [4] enunciated their Conjecture N to the effect that there are infinitely many prime numbers that are the sum of three non-negative cubes; indeed, defining $P(x)$ to be the number of primes not exceeding x that are of the form $X_1^3+X_2^3+X_3^3$ where primes susceptible of several representations are counted multiply, they furthermore expressed the belief that

$$P(x)\sim \Gamma^3\left(\frac{4}{3}\right)\frac{x}{\log x}\prod_{\varpi\equiv 1 \ (\mathrm{mod}\ 3)}\left(1-\frac{a_\varpi}{\varpi^2}\right) \tag{1}$$

as $x\to\infty$, in which a_ϖ is defined by the two conditions $4\varpi=a_\varpi^2+27b_\varpi^2$ and $a_\varpi\equiv 1 \pmod 3$. Yet, owing perhaps to its intrinsic difficulty, the problem thus raised has received scant subsequent attention compared with that given—successfully in some instances too well known to be enumerated here—to several other conjectures in that memoir. Indeed, following the advent of the modern sieve method initiated by Brun and transformed by Selberg, the most we can say about the state of knowledge about the problem is that there must have been a general awareness that $P(x)$ could be bounded above by some fixed multiple λ of the right-hand side of (1) and that a lower bound would be obtainable if primes were replaced by numbers having few prime factors. To be specific, leaving on one side the values of λ derivable by earlier versions of Brun's method, we can certainly assert in a situation lacking written references that any value of λ exceeding 6 can be quickly produced by Selberg's method; also that the number 4 can replace 6 here if

([1]) We have made some unimportant changes to Hardy and Littlewood's enunciation in preparation for our later work.

more attention be paid to the sum

$$N(d) = \sum_{\substack{0<X_1^3+X_2^3+X_3^3\le x \\ X_1^3+X_2^3+X_3^3\equiv 0 \,(\mathrm{mod}\, d)}} 1,$$

which is an inevitable concomitant of the application of any sieve method to $P(x)$. But, in obtaining these bounds, the Selberg method exhibits a characteristic and not unfamiliar weakness in that the effect of the remainder term R_d in the formula for $N(d)$ is estimated by a summation over d involving $|R_d|$, thus probably circumscribing to about $x^{1/2}$ the likely range of d over which the summation can be performed satisfactorily.

As a contribution to the further study of $P(x)$, we consider in this memoir the relevant effect of assuming the Riemann hypothesis for both the Riemann zeta-function and a certain class of Dedekind zeta-functions defined over cubic fields ([2]). Combined with a novel and elaborate treatment of R_d involving the use of multiplicative functions in d, the hypothesis permits the summation of R_d to be treated so sensitively that the effective range of d is increased from $x^{1/2}$ to almost $x^{2/3}$. We thereby conditionally enhance our knowledge by shewing that $P(x)$ does not essentially exceed thrice the bound that (1) would lead one to expect.

Finally, from a perusal of our analysis, it will become clear how our method of exponential sums can be adapted to give an unconditional bound for $P(x)$ that contains the multiplier $\lambda > 4$. For convenience, therefore, a theorem embodying this hitherto unrecorded result is stated at the end.

2. Notation. The meaning of most of the notation used should be clear from the context. But, in particular, we mention that p, ϖ denote positive prime numbers, while p' is a prime of either sign; X_1, X_2, X_3 are non-negative integers but X_1', X_2', X_3' are integers that are of either sign or zero; k and d (with or without subscripts) are positive square-free numbers (possibly 1).

The letter x is a positive real variable to be regarded as tending to infinity, all inequalities that are valid for sufficiently large x being assumed to hold; ε is an arbitrarily small positive number that is not necessarily the same on all occasions; ε_1 is a small positive number remaining fixed until the final Section 10, at which point it may become arbitrarily small and not necessarily the same at each occurrence. The constants implied by the O-notation depend at most on ε until equation (67) in Section 10, the constants in the two following O-terms being in fact absolute from their derivation from equation (3); B_i denotes an absolute constant.

([2]) But see footnote ([5]).

Ordered triplets are indicated by letters in bold type, their components being denoted by the same letters in italic font with subscripts; if $\mathbf{b} = (b_1, b_2, b_3)$, then $\|\mathbf{b}\| = \max |b_i|$; $\mathbf{bc}$ is the scalar product $b_1c_1 + b_2c_2 + b_3c_3$. If $\mathbf{a}$ have integral components, $(\mathbf{a})$ is the positive highest common factor of a_1, a_2, a_3, while $(k, \mathbf{a})$ is the highest common factor of k, a_1, a_2, a_3; also the notation $\mathbf{a} \le u$ means $a_i \le u$ for $i = 1, 2, 3$, a similar significance being attached to other symbols of inequality. Also, for brevity, we use the notation $\int f(\mathbf{w})\, d\mathbf{w}$ to denote $\int f(\mathbf{w})\, dw_1\, dw_2\, dw_3$.

The function $d_r(n)$ is the number of ways of expressing n as a product of r factors and $\sigma_\alpha(n)$ is the sum of the αth powers of the divisors of n.

3. The initial analysis of the sum. Defined as in the introduction, the sum $P(x)$ is initially prepared for the subsequent analysis by bringing in a parameter

$$\eta = \eta(x) = x^{1/3 - 2\varepsilon_1} \tag{2}$$

and by then removing the terms corresponding to primes $p \le \eta$ in order to form the truncated sum $P_\eta(x)$, between which and its predecessor there is the obvious relation

$$\begin{aligned} P(x) &= P_\eta(x) + O\Big(\sum_{0 < X_1^3 + X_2^3 + X_3^3 \le \eta} 1\Big) \\ &= P_\eta(x) + O(\eta) = P_\eta(x) + O(x^{1/3}). \end{aligned} \tag{3}$$

Since, however, we have not yet reached a sum that is an ideal study for our method, we next formulate associated sums $P_\eta^*(M, \mathbf{y})$ that count with associated weights the number of solutions of the conditions

$$p' = X_1'^3 + X_2'^3 + X_3'^3, \qquad |p'| > \eta,$$

for which p' and the components of $\mathbf{X}'$ are of either sign and for which $\mathbf{X}'$ lies in a cube

$$\|\boldsymbol{\xi} - \mathbf{y}\| \le M \tag{4}$$

having an appropriate centre $\mathbf{y}$. To be specific, let

$$w(t) = \begin{cases} \cos^2 \frac{1}{2}\pi t & \text{if } |t| \le 1, \\ 0 & \text{if } |t| > 1, \end{cases} \tag{5}$$

$$M = M(x) = x^{1/3 - \varepsilon_1}, \tag{6}$$

and then assume that the point $\mathbf{y}$ belongs to the solid body $\mathcal{B}_1$ of volume V_1', say, having the property that at least one point $\boldsymbol{\xi}$ in (4) lies in

$$\xi_1^3 + \xi_2^3 + \xi_3^3 \le x, \qquad \xi_1, \xi_2, \xi_3 \ge 0,$$

which is the solid body $\mathcal{B}$ of volume V, say, related to the definition of the primary sum $P(x)$. Then, since we accordingly let

$$P_\eta^*(M,\mathbf{y}) = \sum_{\substack{p'=X_1'^3+X_2'^3+X_3'^3\\ |p'|>\eta}} \prod_{1\le i\le 3} w\biggl(\frac{X_i'-y_i}{M}\biggr), \tag{7}$$

we obtain the inequality

$$\begin{aligned}\int\limits_{\mathbf{y}\in\mathcal{B}_1} P_\eta^*(M,\mathbf{y})\,d\mathbf{y} &= \int\limits_{\mathbf{y}\in\mathcal{B}_1} \sum_{\substack{p'=X_1'^3+X_2'^3+X_3'^3\\ |p'|>\eta}} \prod_{1\le i\le 3} w\biggl(\frac{X_i'-y_i}{M}\biggr)\,d\mathbf{y}\\ &\ge \sum_{\substack{p=X_1^3+X_2^3+X_3^3\le x\\ p>\eta}} \int\limits_{\mathbf{y}\in\mathcal{B}_1} \prod_{1\le i\le 3} w\biggl(\frac{y_i-X_i}{M}\biggr)\,d\mathbf{y}\\ &= \sum_{\substack{p=X_1^3+X_2^3+X_3^3\\ p>\eta}} \biggl(\prod_{1\le i\le 3} \int\limits_{X_i-M}^{X_i+M} w\biggl(\frac{y_i-X_i}{M}\biggr)\,dy_i\biggr)\\ &= M^3 P_\eta(x)\end{aligned}$$

by the definition of $\mathcal{B}_1$ and the equation

$$\int\limits_{-1}^{1} w(t)\,dt = 1. \tag{8}$$

Thus, by (3),

$$P(x) \le \frac{1}{M^3} \int\limits_{\mathbf{y}\in\mathcal{B}_1} P_\eta^*(M,\mathbf{y})\,d\mathbf{y} + O(x^{1/3}), \tag{9}$$

the application of which will depend in part on the equations

$$V = \Gamma^3\biggl(\frac{4}{3}\biggr)x, \qquad V_1 = V + O(x^{2/3}M) \tag{10}$$

and the obvious relation

$$\|\mathbf{y}\| = O(x^{1/3}) \tag{11}$$

that holds when $\mathbf{y}\in\mathcal{B}_1$.

The situation has been prepared for the entrance of an appropriate one-dimensional version of Selberg's upper bound sieve method, where throughout (2), (6), and (11) will be deemed to hold when necessary. Assuming that

$$(12)\qquad \lambda_d = \lambda_{d,\eta} = \begin{cases} \mu(d)\left(1 - \dfrac{\log d}{\log \eta}\right) & \text{if } d \le \eta, \\ 0 & \text{if } d > \eta, \end{cases}$$

for square-free values of d, we observe as usual that

$$(13)\qquad \begin{aligned} h(n) = h_\eta(n) &= \Big(\sum_{d\mid n} \lambda_d\Big)^2 = \sum_{[d_1,d_2]\mid n} \lambda_{d_1}\lambda_{d_2} \\ &= \sum_{k\mid n} \sum_{[d_1,d_2]=k} \lambda_{d_1}\lambda_{d_2} = \sum_{k\mid n} \varrho_k, \quad \text{say,} \end{aligned}$$

is a non-negative function of the integer n that equals 1 when n is a prime having modulus exceeding η. Thus, if in the definition of $P_\eta^*(M,\mathbf{y})$ we replace p' and the stipulation $|p'| > \eta$ by the integer n affected with the weight $h(n)$, we derive a sum $Q_\eta(M,\mathbf{y})$ that does not exceed $P_\eta^*(M,\mathbf{y})$, wherefore (3)

$$(14)\qquad \begin{aligned} P_\eta^*(M,\mathbf{y}) &\le Q_\eta(M,\mathbf{y}) \\ &= \sum_{X_1'^3+X_2'^3+X_3'^3=n} \prod_{1\le i\le 3} w\left(\frac{X_i'-y_i}{M}\right) \sum_{k\mid n} \varrho_k \\ &= \sum_{k\le \eta^2} \varrho_k \sum_{X_1'^3+X_2'^3+X_3'^3\equiv 0 \ (\mathrm{mod}\ k)} \prod_{1\le i\le 3} w\left(\frac{X_i'-y_i}{M}\right) \\ &= \sum_{k\le\eta^2} \varrho_k R(M,\mathbf{y};k), \quad \text{say,} \end{aligned}$$

with which equation the preliminary analysis of our problem ends.

4. Analysis of $R(M,\mathbf{y};k)$. Initiating the second phase of the analysis by evaluating $R(M,\mathbf{y};k)$ as a combination of products of three sums, we have

$$(15)\qquad \begin{aligned} R(M,\mathbf{y};k) &= \sum_{\substack{a_1^3+a_2^3+a_3^3\equiv 0 \ (\mathrm{mod}\ k) \\ 0\le \mathbf{a}<k}} \sum_{\mathbf{X}'\equiv\mathbf{a} \ (\mathrm{mod}\ k)} \prod_{1\le i\le 3} w\left(\frac{X_i'-y_i}{M}\right) \\ &= \sum_{\substack{a_1^3+a_2^3+a_3^3\equiv 0 \ (\mathrm{mod}\ k) \\ 0\le \mathbf{a}<k}} \prod_{1\le i\le 3} \sum_{X_i'\equiv a_i \ (\mathrm{mod}\ k)} w\left(\frac{X_i'-y_i}{M}\right) \end{aligned}$$

---

(3) Allowing n to take the value 0 has no adverse effect on the work because the contribution attributable to it is $O(x^{1/3}\eta^2)$ on the basis of the trivial $h(0) = (\sum_{d\le\eta}\lambda_d)^2 = O(\eta^2)$; if, as here, the Riemann hypothesis be assumed, then the contribution is $O(x^{1/3}\eta^{1+\varepsilon})$.

$$= \sum_{\substack{a_1^3+a_2^3+a_3^3\equiv 0 \,(\mathrm{mod}\, k) \\ 0\le \mathbf{a}<k}} \prod_{1\le i\le 3} \Upsilon(M, y_i; a_i, k),$$

where

$$\Upsilon(M,y;a,k) = \sum_{X'\equiv a \,(\mathrm{mod}\, k)} w\biggl(\frac{X'-y}{M}\biggr).$$

Next $\Upsilon(M,y;a,k)$ is evaluated by the Poisson summation formula in order to represent $R(M,\mathbf{y};k)$ in terms of exponential sums. First, changing the variable of summation from X' to $a+qk$, we have

$$\begin{aligned}\Upsilon(M,y;a,k) &= \sum_{|a-y+qk|\le M} w\biggl(\frac{a-y+qk}{M}\biggr) \\ &= \int_{|a-y+tk|\le M} w\biggl(\frac{a-y+tk}{M}\biggr)\,dt \\ &\quad + \sum_{m\ne 0} \int_{|a-y+tk|\le M} w\biggl(\frac{a-y+tk}{M}\biggr) e^{2\pi i m t}\,dt,\end{aligned}$$

whence, setting $u=(a-y+tk)/M$ and using (8), we get

$$\Upsilon(M,y;a,k) = \frac{M}{k} + \frac{M}{k}\sum_{m\ne 0} e^{2\pi i (y-a)m/k} W\biggl(\frac{mM}{k}\biggr) \tag{16}$$

in which

$$W(v) = \int_{-1}^{1} w(t) e^{2\pi i v t}\,dt.$$

Here, by (5),

$$W(v) = \int_{-1}^{1} w(t)\cos 2\pi v t\,dt = -\frac{\sin 2\pi v}{2\pi v(2v+1)(2v-1)}$$

and

$$W'(v) = -\frac{\cos 2\pi v}{2\pi v(2v+1)(2v-1)} + \frac{\sin 2\pi v(12v^2-1)}{2\pi v^2(2v+1)^2(2v-1)^2}$$

when $v\ne 0, 1/2, -1/2$, from which or integration by parts we have

$$W(v), W'(v) = \begin{cases} O(1) & \text{always,} \\ O(1/|v|^3) & \text{if } |v|>1,\end{cases} \tag{17}$$

since $|W(v)|\le W(0)$ and $|W'(v)|\le |W'(0)|$.

Therefore, by (15) and (16),

$$R(M,\mathbf{y};k)=\frac{M^3}{k^3}\sum_{\substack{a_1^3+a_2^3+a_3^3\equiv 0\ (\mathrm{mod}\ k)\\ 0\le \mathbf{a}<k}} 1 \tag{18}$$
$$+\frac{M^3}{k^3}\sum_{\substack{a_1^3+a_2^3+a_3^3\equiv 0\ (\mathrm{mod}\ k)\\ 0\le \mathbf{a}<k}}\sum_{\mathbf{m}\neq 0} e^{2\pi i(\mathbf{my}-\mathbf{ma})/k}$$
$$\times W\left(\frac{m_1M}{k}\right)W\left(\frac{m_2M}{k}\right)W\left(\frac{m_3M}{k}\right)$$
$$=\frac{M^3\nu(k)}{k^3}+\frac{M^3}{k^3}\sum_{\mathbf{m}\neq 0}e^{2\pi i\mathbf{my}/k}$$
$$\times W\left(\frac{m_1M}{k}\right)W\left(\frac{m_2M}{k}\right)W\left(\frac{m_3M}{k}\right)S(\mathbf{m},k)$$
$$=\frac{M^3\nu(k)}{k^3}+M^3R^{\dagger}(M,\mathbf{y};k),\quad \text{say,}$$

where $\nu(k)$ is the number of incongruent roots of the congruence

$$z_1^3+z_2^3+z_3^3\equiv 0\pmod k$$

and $S(\mathbf{m},k)=S(-\mathbf{m},k)$ is the important exponential sum

$$\sum_{\substack{a_1^3+a_2^3+a_3^3\equiv 0\ (\mathrm{mod}\ k)\\ 0\le \mathbf{a}<k}} e^{2\pi i\mathbf{ma}/k}$$

that is to be investigated in the next section but one.

But, in the meanwhile, we deduce from (14) and (18) that

$$Q_\eta(M,\mathbf{y})=M^3\sum_{k\le\eta^2}\frac{\varrho_k\nu(k)}{k^3}+M^3\sum_{k\le\eta^2}\varrho_kR^{\dagger}(M,\mathbf{y};k) \tag{19}$$
$$=M^3Q_\eta^*+M^3Q_\eta^{\dagger}(M,\mathbf{y}),\quad\text{say,}$$

the penultimate term in which we proceed to estimate at once.

5. Estimation of Q_η^*. The treatment of Q_η^* depends on the multiplicativity of $\nu(d)$ and the formula

$$\nu(p)=\begin{cases} p^2 & \text{if } p\equiv 2\pmod 3 \text{ or } p=3,\\ p^2+(p-1)a_p & \text{if } p\equiv 1\pmod 3,\end{cases} \tag{20}$$

where in the second instance a_p is determined by the conditions $4p=a_p^2+27b_p^2$, $a_p\equiv 1\pmod 3$. The non-trivial aspect of the result lies only in the second part, which follows from the theory of cyclotomy since then

$$\nu(p) = p^2 + \tfrac{1}{3}(p-1)(\eta_0^3 + \eta_1^3 + \eta_2^3)$$

in which η_0, η_1, η_2 are the $\frac{1}{3}(p-1)$-nomial periods satisfying the period equation

$$(3\eta+1)^3 - 3p(3\eta+1) - pa_p = 0.$$

Thus, in particular, we verify that $0 < \nu(p) < p^3$ (of course the falsity of the second inequality for some p would render our problem nugatory).

At first, setting

$$f(d) = d^3/\nu(d) > 1$$

and using (19) and (13) in a familiar manner, we have

$$\begin{aligned}
(21) \qquad Q_\eta^* &= \sum_{d_1, d_2 \le \eta} \frac{\lambda_{d_1}\lambda_{d_2}}{f([d_1, d_2])} = \sum_{d_1, d_2 \le \eta} \frac{\lambda_{d_1}\lambda_{d_2}}{f(d_1)f(d_2)} f\{(d_1, d_2)\} \\
&= \sum_{d_1, d_2 \le \eta} \frac{\lambda_{d_1}\lambda_{d_2}}{f(d_1)f(d_2)} \sum_{\varrho \mid d_1;\, \varrho \mid d_2} f_1(\varrho) \\
&= \sum_{\varrho \le \eta} f_1(\varrho) u_\varrho^2,
\end{aligned}$$

wherein as usual

$$f_1(\varrho) = \sum_{d \mid \varrho} \mu(d) f\left(\frac{\varrho}{d}\right) = f(\varrho) \prod_{p \mid \varrho} \left(1 - \frac{1}{f(p)}\right) > 0$$

and

$$u_\varrho = \sum_{\substack{d \le \eta \\ d \equiv 0 \ (\mathrm{mod}\ \varrho)}} \frac{\lambda_d}{f(d)}.$$

Here, however, we must depart from the basic form of Selberg's method because our choice of λ_d does not enable u_ϱ and Q_η^* to be quickly and exactly determined. Instead, by (12), we write

$$(22) \qquad u_\varrho = \frac{\mu(\varrho)}{f(\varrho)\log \eta} \sum_{\substack{d' \le \eta/\varrho \\ (d', \varrho) = 1}} \frac{\mu(d')}{f(d')} \log \frac{\eta/\varrho}{d'},$$

the sum in which is estimated through the generating function

$$F_\varrho(s) = \sum_{\substack{n=1 \\ (n, \varrho) = 1}}^{\infty} \frac{\mu(n)}{f(n) n^s}$$

that for $\sigma > 0$ equals

$$(23)\qquad \prod_{p\nmid\varrho}\left(1-\frac{1}{p^s f(p)}\right)=\prod_{p\mid\varrho}\left(1-\frac{1}{p^s f(p)}\right)^{-1}\prod_{p}\left(1-\frac{1}{p^{s+1}}\right)$$
$$\times\prod_{p}\left(1-\frac{1}{p^{s+1}}\right)^{-1}\left(1-\frac{1}{p^s f(p)}\right)$$
$$=\frac{E_\varrho(s)I(s)}{\zeta(s+1)},\quad \text{say.}$$

In this, being of the form $\prod_p\{1+O(1/p^{\sigma+3/2})\}$ because of (20), the function $I(s)$ is regular and bounded for $\sigma>\sigma_0>-1/2$ so that $F_\varrho(s)$ determines a regular function in any part of the same half-plane for which $\zeta(s+1)$ is zero-free. Thus, since

$$\sum_{\substack{d'\le u\\(d',\varrho)=1}}\frac{\mu(d')}{f(d')}\log\frac{u}{d}=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{E_\varrho(s)I(s)x^s}{\zeta(s+1)s^2}\,ds\qquad(c>0),$$

we obtain

$$\sum_{\substack{d'\le u\\(d',\varrho)=1}}\frac{\mu(d')}{f(d')}\log\frac{u}{d}=\frac{I(0)f(\varrho)}{f_1(\varrho)}+O\biggl(\frac{\sigma_{-1/2}(\varrho)}{\log^2 2u}\biggr)\qquad(u\ge 1)$$

by suitably moving the contour of integration and invoking well known properties of the Riemann zeta-function.

Going back to (22), we therefore get

$$u_\varrho=\frac{I(0)\mu(\varrho)}{f_1(\varrho)\log\eta}+O\biggl(\frac{\mu^2(\varrho)\sigma_{-1/2}(\varrho)}{f(\varrho)\log\eta\log^2(2\eta/\varrho)}\biggr)$$

and then

$$Q_\eta^*=\frac{I^2(0)}{\log^2\eta}\sum_{\varrho\le\eta}\frac{\mu^2(\varrho)}{f_1(\varrho)}+O\biggl(\frac{1}{\log^2\eta}\sum_{\varrho\le\eta}\frac{\mu^2(\varrho)\sigma_{-1/4}(\varrho)}{\varrho\log^2(2\eta/\varrho)}\biggr)$$
$$=\frac{I^2(0)}{\log^2\eta}\sum_{\varrho\le\eta}\frac{\mu^2(\varrho)}{f_1(\varrho)}+O\biggl(\frac{1}{\log^2\eta}\biggr)$$

from (21) and elementary properties of divisor-type functions. Finally, as

$$\sum_{\varrho\le\eta}\frac{\mu^2(\varrho)}{f_1(\varrho)}=\frac{\log\eta}{I(0)}+O(1),$$

we conclude that

$$(24)\qquad Q_\eta^*=\frac{I(0)}{\log\eta}+O\biggl(\frac{1}{\log^2\eta}\biggr),$$

it being opportune to deduce from (23) and (20) that

$$I(0) = \prod_{p\equiv 1\ (\mathrm{mod}\ 3)} \left(1-\frac{1}{p}-\frac{(p-1)a_p}{p^3}\right)\left(1-\frac{1}{p}\right)^{-1} \tag{25}$$

$$= \prod_{p\equiv 1\ (\mathrm{mod}\ 3)} \left(1-\frac{a_p}{p^2}\right) = A, \quad \text{say.}$$

It should be noted that as yet the Riemann hypothesis has not been brought into play.

6. Investigation of $S(\mathbf{m},k)$. The initially required properties of $S(\mathbf{m},k)$ are stated in the following lemma; they are similar to some results given in our previous memoirs [5] and [6] but are best given a brief direct demonstration below.

Lemma 1. (i) *$S(\mathbf{m},k)$ is properly multiplicative, i.e., if $(k_1,k_2)=1$, then $S(\mathbf{m},k_1k_2)=S(\mathbf{m},k_1)S(\mathbf{m},k_2)$;*

(ii) *if $\nu(\mathbf{m},p)$ denote the number of incongruent roots of the simultaneous congruences*

$$z_1^3+z_2^3+z_3^3\equiv 0 \pmod p; \quad \mathbf{mz}\equiv 0 \pmod p,$$

then

$$S(\mathbf{m},p)=\frac{p}{p-1}\nu(\mathbf{m},p)-\frac{\nu(p)}{p-1}.$$

The first part depends on the fact that $\mathbf{a}_3=k_2\mathbf{a}_1+k_1\mathbf{a}_2$ runs through a complete set of residue vectors, $\mathrm{mod}\, k_1k_2$, as $\mathbf{a}_1$, $\mathbf{a}_2$ run through complete sets of residue vectors, modulis k_1, k_2, respectively. Then, writing $g(\mathbf{a})=a_1^3+a_2^3+a_3^3$ without danger of confusion with regard to subscripts ([4]), we know the condition $g(\mathbf{a}_3)\equiv 0 \pmod{k_1k_2}$ is equivalent to the conjunction of $g(\mathbf{a}_1)\equiv 0 \pmod{k_1}$ and $g(\mathbf{a}_2)\equiv 0 \pmod{k_2}$, while the product of typical summands in $S(\mathbf{m},k_1)$ and $S(\mathbf{m},k_2)$ is a typical summand in $S(\mathbf{m},k_1k_2)$.

For $h\not\equiv 0 \pmod p$, the substitution $\mathbf{a}\equiv h\mathbf{a}' \pmod p$ shews that $S(\mathbf{m},p)$ $=S(h\mathbf{m},p)$, wherefore

$$S(\mathbf{m},p)=\frac{1}{p-1}\sum_{0<h<p}S(h\mathbf{m},p)=\frac{1}{p-1}\sum_{0\le h<p}S(h\mathbf{m},p)-\frac{1}{p-1}S(0,p)$$

$$=\frac{1}{p-1}\sum_{\substack{g(\mathbf{a})\equiv 0\ (\mathrm{mod}\ p)\\ 0\le \mathbf{a}<p}}\ \sum_{0\le h<p} e^{2\pi h\mathbf{ma}/k}-\frac{\nu(p)}{p-1}$$

([4]) I.e. by using double subscripts for the components of $\mathbf{a}_i$.

$$= \frac{p}{p-1} \sum_{\substack{g(\mathbf{a}) \equiv \mathbf{ma} \equiv 0 \, (\mathrm{mod}\, p) \\ 0 \le \mathbf{a} < p}} 1 - \frac{\nu(p)}{p-1} = \frac{p}{p-1} \nu(\mathbf{m}, p) - \frac{\nu(p)}{p-1},$$

as asserted in part (ii).

To treat $S(\mathbf{m}, p)$ by Lemma 1 we always suppose that $\mathbf{m} \neq 0$ and may limit serious consideration to the case $\mu = (\mathbf{m}) = 1$ because

$$\nu(\mathbf{m}, p) = \nu(\mathbf{m}/\mu, p) \tag{26}$$

when $\mathbf{m} \not\equiv 0 \pmod p$, the result in the contrary instance where $\mathbf{m} \equiv 0 \pmod p$, being the estimate

$$S(\mathbf{m}, p) = \nu(p) = p^2 + O(p^{3/2}) = O(p^2), \tag{27}$$

the final term in which supplies of course a bound of universal validity.

Assuming then that $\mu = 1$, we consider the *affine* variety $\mathcal{V}_{\mathbf{m}}$ defined over $\mathbb{Q}$ by the equations

$$\zeta_1^3 + \zeta_2^3 + \zeta_3^3 = 0, \qquad \mathbf{m}\boldsymbol{\zeta} = 0. \tag{28}$$

To derive a symmetric version of treating $\mathcal{V}_{\mathbf{m}}$ through obtaining a single equation with appropriate integral coefficients to represent it, we find by a method having its genesis in the *Disquisitiones Arithmeticae* ([3], art. 279) a substitution

$$\zeta_1' = \mathbf{m}\boldsymbol{\zeta}, \quad \zeta_2' = \mathbf{m}'\boldsymbol{\zeta}, \quad \zeta_3' = \mathbf{m}''\boldsymbol{\zeta}$$

having integral coefficients and modulus unity that transforms the equation of $\mathcal{V}_{\mathbf{m}}$ into

$$f_{\mathbf{m}}(\boldsymbol{\zeta}') = 0, \quad \zeta_1' = 0 \tag{29}$$

so that $\mathcal{V}_{\mathbf{m}}$ is represented by $g_{\mathbf{m}}(\zeta_2', \zeta_3') = f_{\mathbf{m}}(0, \zeta_2', \zeta_3')$. Discriminants being invariant with respect to unimodular transformations, those of $\mathcal{V}_{\mathbf{m}}$ and (29) are equal, from which fact it easily follows that the discriminant $\Delta_{\mathbf{m}}$ of $g_{\mathbf{m}}(\zeta_2', \zeta_3')$ is the eliminant

$$\prod (m_1^{3/2} \pm m_2^{3/2} \pm m_3^{3/2}) = m_1^6 + m_2^6 + m_3^6 - 2m_2^3 m_3^3 - 2m_3^3 m_1^3 - 2m_1^3 m_2^3 \tag{30}$$

of the conditions $\zeta_1^2 : \zeta_2^2 : \zeta_3^2 :: m_1 : m_2 : m_3, \mathbf{m}\boldsymbol{\zeta} = 0$ that express the condition that (28) have a non-zero singularity (i.e. not contain a repeated line).

Save for a few easily described determinations of $\mathbf{m}$, the binary cubic form $g_{\mathbf{m}}(\zeta_2', \zeta_3')$ is irreducible over $\mathbb{Q}$ with non-vanishing discriminant $\Delta_{\mathbf{m}}$ because the originating equation $\zeta_1^3 + \zeta_2^3 + \zeta_3^3 = 0$ has no rational solutions apart from the trivial ones $\zeta_1 = 0$, $\zeta_2 = -\zeta_3$; $\zeta_2 = 0$, $\zeta_3 = -\zeta_1$; $\zeta_3 = 0$, $\zeta_1 = -\zeta_2$. Since the only determinations of $\mathbf{m}$ for which $g_{\mathbf{m}}(\zeta_2', \zeta_3')$ is reducible over $\mathbb{Q}$ (i.e. has at least one non-trivial zero in $\mathbb{Q}$) are those for which $\mathbf{m}\boldsymbol{\zeta} = 0$ is satisfied by one of these special solutions, we extract the set $\mathcal{S}$ of (non-zero) $\mathbf{m}$ for which

$$m_2 = m_3 \quad \text{or} \quad m_3 = m_1 \quad \text{or} \quad m_1 = m_2; \tag{31}$$

the common value of two components here may indeed be zero provided the third one be not. The occurrence of this exceptional case where $\mathbf{m} \in \mathcal{S}$ is sufficiently rare for it to be enough to confine the thrust of our subsequent main analysis to the opposite case where $g_{\mathbf{m}}(\zeta_2', \zeta_3')$ is irreducible over $\mathbb{Q}$; appropriate modifications of this analysis are indeed available in the residual situation, which, however, is more expeditiously treated by a fairly crude method.

Considering $\nu(\mathbf{m}, p)$ in the main situation delineated above, we need the number of incongruent solutions of $g_{\mathbf{m}}(\zeta_2', \zeta_3') \equiv 0 \pmod{p}$, or what is the same, the number of such solutions of $\gamma_{\mathbf{m}}(\zeta_2'', \zeta_3'') \equiv 0 \pmod{p}$, where $\gamma_{\mathbf{m}}(\zeta_2'', \zeta_3'')$ is the reduced binary cubic to which $g_{\mathbf{m}}(\zeta_2', \zeta_3')$ is equivalent. Here, by theories as expounded by, say, Davenport ([1], [2]),

$$\gamma_{\mathbf{m}}(\zeta_2'', \zeta_3'') = A_0 {\zeta_2''}^3 + 3A_1 {\zeta_2''}^2 \zeta_3'' + 3A_2 \zeta_2'' {\zeta_3''}^2 + A_4 {\zeta_3''}^3,$$

where, writing $A_0 = D_{\mathbf{m}}$, we have

$$0 < |D_{\mathbf{m}}| = O(\Delta_{\mathbf{m}}^4); \tag{32}$$

consequently, if $\nu^{\dagger}(\mathbf{m}, p)$ be the number of incongruent roots of

$$h_{\mathbf{m}}(u) = u^3 + 3A_1 u^2 + 3D_{\mathbf{m}} A_2 u + D_{\mathbf{m}}^2 A_3 \equiv 0 \pmod{p},$$

then

$$\nu(\mathbf{m}, p) = (p-1)\nu^{\dagger}(\mathbf{m}, p) + 1 \tag{33}$$

when $p \nmid D_{\mathbf{m}}$. Thus, if $\theta = \theta_{\mathbf{m}}$ be a zero of $h_{\mathbf{m}}(u)$, then by a principle due to Dedekind $\nu^{\dagger}(\mathbf{m}, p)$ equals the number $\nu^*(\mathbf{m}, p)$ of linear prime ideal factors of p in the corpus $\mathbb{Q}(\theta) = \mathbb{Q}(\theta_{\mathbf{m}})$ when p is subject to the further restriction $p \nmid \Delta_{\mathbf{m}}$, the discriminant of $h_{\mathbf{m}}(u)$ being $D_{\mathbf{m}}^2 \Delta_{\mathbf{m}}$. In conclusion, by Lemma 1, (20), and (33), we therefore arrive at the determination

$$p\{\nu^*(\mathbf{m}, p) - 1\} + O(p^{1/2}) \tag{34}$$

for $S(\mathbf{m}, p)$ when $p \nmid D_{\mathbf{m}} \Delta_{\mathbf{m}}$, $(\mathbf{m}) = 1$, and $\mathbf{m} \notin \mathcal{S}$.

Having obtained (34), we now drop the temporary convention that $(\mathbf{m}) = 1$ and consequently extend $\mathcal{S}$ to the set $\mathcal{S}'$ of all *non-zero* triplets of type (31). To (27) and (34) we must then finally adjoin the estimate

$$S(\mathbf{m}, p) = O(p) \qquad (\mathbf{m} \not\equiv 0 \pmod{p}), \tag{35}$$

the truth of which for $p \neq 3$ follows from part (ii) of Lemma 1 and the irreducibility of $\zeta_1^3 + \zeta_2^3 + \zeta_3^3 \pmod{p}$; when $p = 3$ the result is trivial.

7. Estimation of $Q_\eta^{\dagger}(M,\mathbf{y})$; first stage. Going on to the hardest part of the analysis, we reverse the order of summation that is latent in (18) and (19) and first obtain

$$(36)\quad Q_\eta^{\dagger}(M,\mathbf{y}) = \sum_{\mathbf{m}\neq 0}\sum_{k\le\eta^2}\frac{\varrho_k e^{2\pi i\mathbf{m}\mathbf{y}/k}}{k^2}W\left(\frac{m_1M}{k}\right) \times W\left(\frac{m_2M}{k}\right)W\left(\frac{m_3M}{k}\right)\frac{S(\mathbf{m},k)}{k} = \sum_{\mathbf{m}\in\mathcal{S}'} + \sum_{\mathbf{m}\notin\mathcal{S}',\,\mathbf{m}\neq 0} = Q_\eta^{\ddagger}(M,\mathbf{y}) + Q_\eta^{\$}(M,\mathbf{y}),\quad\text{say,}$$

the final two constituents in which are to be estimated with the aid of the following deduction from (17).

Lemma 2. *We have*

$$\sum_{m\ge 0}|W(\alpha m)| = \begin{cases} O(1/\alpha) & \textit{if } 0<\alpha\le 1,\\ O(1) & \textit{if } \alpha>1.\end{cases}$$

Also, for any number δ such that $0\le\delta\le 3/2$,

$$\sum_{m>0} m^\delta|W(\alpha m)|,\ \sum_{m>0} m^\delta|W'(\alpha m)| = \begin{cases} O(1/\alpha^{1+\delta}) & \textit{if } 0<\alpha\le 1,\\ O(1/\alpha^3) & \textit{if } \alpha>1.\end{cases}$$

Assuming throughout that k is square-free in what follows in virtue of the definition of ϱ_k in (13), we first dispose of the easier sum $Q_\eta^{\ddagger}(M,\mathbf{y})$. Since $\varrho_k = O\{d_3(k)\} = O(x^\varepsilon)$ by (12) and (2) and since

$$(37)\qquad S(\mathbf{m},k) = O(B_1^{\omega(k)}k(k,\mathbf{m})) = O(x^\varepsilon k(k,\mathbf{m}))$$

by Lemma 1, (27), and (35), the summand in $Q_\eta^{\ddagger}(M,\mathbf{y})$ is

$$O\left(\frac{x^\varepsilon(k,\mathbf{m})}{k^2}\left|W\left(\frac{m_1M}{k}\right)\right|\cdot\left|W\left(\frac{m_2M}{k}\right)\right|\cdot\left|W\left(\frac{m_3M}{k}\right)\right|\right),$$

to which, by symmetry and positivity, attention may be confined in the situations where either $m_1=m_2=m>0$; $m_3\ge 0$; or $m_1=m_2=0$, $m_3>0$. Hence

$$(38)\quad Q_\eta^{\ddagger}(M,\mathbf{y}) = O\left(x^\varepsilon\sum_{m>0;\,m_3\ge 0}\sum_{k\le\eta^2}\frac{(k,m,m_3)}{k^2}W^2\left(\frac{mM}{k}\right)\left|W\left(\frac{m_3M}{k}\right)\right|\right) + O\left(x^\varepsilon\sum_{m_3>0}\sum_{k\le\eta^2}\frac{(k,m_3)}{k^2}\left|W\left(\frac{m_3M}{k}\right)\right|\right)$$

$$= O\bigg(x^{\varepsilon} \sum_{k \le \eta^2} \frac{1}{k^2} \sum_{d|k} d \sum_{\substack{m \equiv m_3 \equiv 0 \,(\mathrm{mod}\, d) \\ m>0;\, m_3 \ge 0}} \bigg|W\bigg(\frac{mM}{k}\bigg)\bigg| \cdot \bigg|W\bigg(\frac{m_3 M}{k}\bigg)\bigg|\bigg)$$

$$+ O\bigg(x^{\varepsilon} \sum_{k \le \eta^2} \frac{1}{k^2} \sum_{d|k} d \sum_{\substack{m_3 \equiv 0 \,(\mathrm{mod}\, d) \\ m_3>0}} \bigg|W\bigg(\frac{m_3 M}{k}\bigg)\bigg|\bigg)$$

with the aid of (17). In this, using part of the strength of Lemma 2, we see that the first innermost sum is

$$\bigg(\sum_{m'>0} \bigg|W\bigg(\frac{m'dM}{k}\bigg)\bigg|\bigg)\bigg(\sum_{m_3' \ge 0} \bigg|W\bigg(\frac{m_3'dM}{k}\bigg)\bigg|\bigg) = O\bigg(\frac{k^2}{d^2M^2}\bigg)$$

whatever be the value of dM/k, while the second such sum is

$$\sum_{m_3'>0} \bigg|W\bigg(\frac{m_3'dM}{k}\bigg)\bigg| = O\bigg(\frac{k}{dM}\bigg).$$

From these estimates and (38), we then conclude that

$$\begin{aligned} Q_\eta^{\ddagger}(M,\mathbf{y}) &= O\bigg(\frac{x^{\varepsilon}}{M^2} \sum_{k \le \eta^2} \sum_{d|k} \frac{1}{d}\bigg) + O\bigg(\frac{x^{\varepsilon}}{M} \sum_{k \le \eta^2} \frac{1}{k} \sum_{d|k} 1\bigg) \\ &= O\bigg(\frac{x^{\varepsilon}}{M^2} \sum_{k \le \eta^2} \sigma_{-1}(k)\bigg) + O\bigg(\frac{x^{\varepsilon}}{M} \sum_{k \le \eta^2} \frac{d(k)}{k}\bigg) \\ &= O\bigg(\frac{x^{\varepsilon}\eta^2}{M^2}\bigg) + O\bigg(\frac{x^{\varepsilon}}{M}\bigg) = O\bigg(\frac{x^{\varepsilon}\eta^2}{M^2}\bigg) \end{aligned} \tag{39}$$

in the light of (2) and (6).

8. Estimation of $\gamma(\mathbf{m}, u)$. We use partial summation to transform the inner sum in the formula for $Q_\eta^{\$}(M,\mathbf{y})$ given implicitly by (36), to which end we always assume that

$$\mathbf{m} \notin \mathcal{S}', \quad \mathbf{m} \ne 0, \quad \mathbf{m}' = \mathbf{m}/(\mathbf{m}) \tag{40}$$

and write

$$\begin{aligned} \psi(M,\mathbf{y};\mathbf{m},u) &= \psi(\mathbf{m},u) \\ &= \frac{e^{2\pi \mathbf{m}\mathbf{y}/u}}{u^2} W\bigg(\frac{m_1M}{u}\bigg) W\bigg(\frac{m_2M}{u}\bigg) W\bigg(\frac{m_3M}{u}\bigg) \end{aligned} \tag{41}$$

in order to get

$$T_\eta(M,\mathbf{y};\mathbf{m}) = \sum_{k \le \eta^2} \frac{\varrho_k S(\mathbf{m},k)}{k} \psi(\mathbf{m},k) \tag{42}$$

$$= \psi(\mathbf{m}, \eta^2)\gamma(\mathbf{m}, \eta^2) - \int_1^{\eta^2} \psi'(\mathbf{m}, u)\gamma(\mathbf{m}, u)\, du,$$

where

$$\gamma(\mathbf{m}, u) = \sum_{k \le u} \frac{\varrho_k S(\mathbf{m}, k)}{k} \tag{43}$$

for $1 \le u \le \eta^2$. As a direct estimation of $\gamma(\mathbf{m}, u)$ presents special difficulties when $u < \eta^2$, we approach it obliquely by a method that involves the Dirichlet's series

$$\Gamma(\mathbf{m}, s') = \Gamma_\eta(\mathbf{m}, s') = \sum_{k \le \eta^2} \frac{\varrho_k S(\mathbf{m}, k)}{k^{1+s'}} \qquad (s' = \sigma' + it'), \tag{44}$$

in which the presence of the exponent s' does not vitiate the phenomenon of multiplicativity that is present in a straight treatment of $\gamma(\mathbf{m}, u)$ for the individual case $u = \eta^2$.

The first stage in our journey here is to enunciate a generalization of one of Selberg's procedures in

LEMMA 3. *Let $\upsilon(q)$ be a multiplicative function for square-values of q. Then*, *writing*

$$\upsilon_2(l) = \prod_{p|l} (1 - \upsilon(p)),$$

we have

$$\upsilon([d_1, d_2]) = \sum_{ld_1' = d_1; ld_2' = d_2} \upsilon(l)\upsilon_2(l)\upsilon(d_1')\upsilon(d_2'). \tag{45}$$

In the general case where $\upsilon(2), \upsilon(3), \ldots$ are independent indeterminates $x_2, x_3, \ldots$, the lemma asserts that (45) is a polynomial identity in $x_2, x_3, \ldots$ In this instance, setting

$$\upsilon_1(l) = \sum_{\delta|l} \frac{\mu(\delta)}{\upsilon(l/\delta)} = \frac{1}{\upsilon(l)} \prod_{p|l} (1 - \upsilon(p)) = \frac{\upsilon_2(l)}{\upsilon(l)},$$

we deduce from the Möbius inversion formula that

$$\begin{aligned}\upsilon([d_1, d_2]) = \frac{\upsilon(d_1)\upsilon(d_2)}{\upsilon\{(d_1, d_2)\}} &= \upsilon(d_1)\upsilon(d_2) \sum_{ld_1' = d_1;\, ld_2' = d_2} \frac{\upsilon_2(l)}{\upsilon(l)} \\ &= \sum_{ld_1' = d_1;\, ld_2' = d_2} \upsilon(l)\upsilon_2(l)\upsilon(d_1')\upsilon(d_2'),\end{aligned}$$

as stated. Thus, by a specialization of $x_2, x_3, \ldots$ to any required numerical values, we obtain the lemma even in the case where $\upsilon(p)$ may be zero.

To apply this lemma to $\Gamma(\mathbf{m}, s')$ let us write

$$\Theta(\mathbf{m}, l, s') = \prod_{p|l}\left(1 - \frac{S(\mathbf{m}, p)}{p^{1+s'}}\right)$$

and note that

$$\Theta(\mathbf{m}, l, s') = O(B_2^{\omega(l)}(\mathbf{m}, l)) \quad (\sigma' > 0) \tag{46}$$

by (27) and (35). Then, using (13) and Lemma 1, we infer that

$$\Gamma(\mathbf{m}, s') = \sum_{d_1, d_2 \le \eta} \lambda_{d_1}\lambda_{d_2} \sum_{ld_1' = d_1;\, ld_2' = d_2} \frac{\Theta(\mathbf{m}, l, s')S(\mathbf{m}, l)S(\mathbf{m}, d_1')S(\mathbf{m}, d_2')}{l^{1+s'} d_1'^{1+s'} d_2'^{1+s'}},$$

from which and (12) it follows that

$$\begin{aligned} \Gamma(\mathbf{m}, s') &= \frac{1}{\log^2 \eta} \sum_{l \le \eta} \frac{\mu^2(l)\Theta(\mathbf{m}, l, s')S(\mathbf{m}, l)}{l^{1+s'}} \\ &\quad \times \Bigg(\sum_{\substack{d \le \eta/l \\ (d,l)=1}} \frac{\mu(d)S(\mathbf{m}, d)}{d^{1+s'}} \log \frac{\eta/l}{d}\Bigg)^2 \\ &= O\bigg(\sum_{l \le \eta} \frac{\mu^2(l)|\Theta(\mathbf{m}, l, s')| \cdot |S(\mathbf{m}, l)|}{l^{1+s'}} \Psi^2(\mathbf{m}, l, \eta/l, s')\bigg), \end{aligned} \tag{47}$$

where

$$\Psi(\mathbf{m}, l, v, s') = \sum_{\substack{d \le v \\ (d,l)=1}} \frac{\mu(d)S(\mathbf{m}, d)}{d^{1+s'}} \log \frac{v}{d}$$

and where we temporarily relinquish the condition $d \le \eta$ that has been implicit in some of our earlier work.

The sum $\Psi(\mathbf{m}, l, v, s')$ is studied through the agency of the Dirichlet's series

$$E(\mathbf{m}, l, s'') = \sum_{(d,l)=1} \frac{\mu(d)S(\mathbf{m}, d)}{d^{1+s''}} \quad (s'' = \sigma'' + it''),$$

which, being absolutely convergent for $\sigma'' > 1$ by (37), is expressible in this half-plane as

$$\prod_{p \nmid l}\left(1 - \frac{S(\mathbf{m}, p)}{p^{1+s''}}\right) \tag{48}$$

by Euler's theorem. This is used to find a formula for $E(\mathbf{m}, l, s'')$ in terms of the Riemann zeta-function and the Dedekind zeta-function

$$\zeta_{\mathbf{m}'}(s'') = \sum_{\mathfrak{m}} \frac{1}{(\mathrm{N}\mathfrak{m})^{s''}} = \prod_{\mathfrak{p}}\left(1 - \frac{1}{(\mathrm{N}\mathfrak{p})^{s''}}\right)^{-1}$$

taken over the corpus $\mathbb{Q}(\theta) = \mathbb{Q}(\theta_{\mathbf{m}'})$ defined as in Section 6. For this purpose, the infinite product (48) is split according to the three categories of estimations in (27), (34), and (35) so we obtain

$$(49)\qquad \begin{aligned} E(\mathbf{m}, l, s'') &= \prod_{p\nmid l;\, p\mid(\mathbf{m})} \ \prod_{\substack{p\nmid l(\mathbf{m}) \\ p\,\mid\, 210D_{\mathbf{m}'}\Delta_{\mathbf{m}'}}} \ \prod_{\substack{p\nmid l(\mathbf{m}) \\ p\nmid 210D_{\mathbf{m}'}\Delta_{\mathbf{m}'}}} \\ &= E_1(\mathbf{m}, l, s'')E_2(\mathbf{m}, l, s'')E_3(\mathbf{m}, l, s''), \quad \text{say}, \end{aligned}$$

where $E_1(\mathbf{m}, l, s'')$ and $E_2(\mathbf{m}, l, s'')$ are regular functions for all s'' having the properties

$$(50)\qquad \begin{aligned} E_1(\mathbf{m}, l, s'') &= O\Big\{\prod_{p\mid(\mathbf{m})}\Big(1+\frac{B_3}{p^{\sigma''-1}}\Big)\Big\}, \\ E_2(\mathbf{m}, l, s'') &= O\Big\{\prod_{p\mid 210D_{\mathbf{m}'}\Delta_{\mathbf{m}'}}\Big(1+\frac{B_4}{p^{\sigma''}}\Big)\Big\}. \end{aligned}$$

Also, since $|\nu^*(\mathbf{m}', p)|/p^{1/2} < 3/\sqrt{11} < 1$ when $p > 7$ and $p\nmid D_{\mathbf{m}'}\Delta_{\mathbf{m}'}$,

$$(51)\qquad E_3(\mathbf{m}, l, s'') = E_4(\mathbf{m}, l, s'')E_5(\mathbf{m}, l, s'')$$

for $\sigma'' > 1/2$, in which

$$(52)\qquad \begin{aligned} E_4(\mathbf{m}, l, s'') &= O\Big\{\prod_{p}\Big(1+\frac{B_5}{p^{\sigma''+1/2}}\Big)\Big\}, \\ E_5(\mathbf{m}, l, s'') &= \prod_{\substack{p\nmid l(\mathbf{m}) \\ p\nmid 210D_{\mathbf{m}'}\Delta_{\mathbf{m}'}}}\Big(1+\frac{1}{p^{s''}}\Big)\Big(1-\frac{\nu^*(\mathbf{m}', p)}{p^{s''}}\Big) \end{aligned}$$

by (34). Here, for $\sigma'' > 1$, the first product implicit in the above expression for $E_5(\mathbf{m}, l, s'')$ is

$$(53)\qquad \Big[O\Big\{\prod_{p\mid 210lD_{\mathbf{m}'}\Delta_{\mathbf{m}}}\Big(1+\frac{1}{p^{\sigma''}}\Big)\Big\}\Big]\frac{\zeta(s)}{\zeta(2s)},$$

while the second one is

$$(54)\qquad \begin{aligned} &\Big[O\Big\{\prod_{p}\Big(1+\frac{B_6}{p^{2\sigma''}}\Big)\Big\}\Big]\prod_{p\nmid 210lD_{\mathbf{m}'}\Delta_{\mathbf{m}}}\Big(1-\frac{1}{p^{s''}}\Big)^{\nu^*(\mathbf{m}', p)} \\ &\qquad = \Big[O\Big\{\prod_{p}\Big(1+\frac{B_6}{p^{2\sigma''}}\Big)\Big\}\Big]\prod_{\substack{p\nmid 210lD_{\mathbf{m}'}\Delta_{\mathbf{m}} \\ \mathrm{N}\mathfrak{p}=p}}\Big(1-\frac{1}{(\mathrm{N}\mathfrak{p})^{s''}}\Big) \\ &\qquad = \Big[O\Big\{\prod_{p}\Big(1+\frac{B_7}{p^{2\sigma''}}\Big)\Big\}\Big]\prod_{p\nmid 210lD_{\mathbf{m}'}\Delta_{\mathbf{m}}}\Big(1-\frac{1}{(\mathrm{N}\mathfrak{p})^{s''}}\Big) \end{aligned}$$

$$= \frac{1}{\zeta_{\mathbf{m}'}(s'')}\Big[O\Big\{\prod_p\Big(1+\frac{B_7}{p^{2\sigma''}}\Big)\prod_{p\mid 210lD_{\mathbf{m}'}\Delta_{\mathbf{m}}}\Big(1+\frac{B_8}{p^{\sigma''}}\Big)\Big\}\Big],$$

all the O-factors above being certainly regular for $\sigma'' > 1/2$. Hence, altogether in the half-plane $\sigma'' > 1$, using (49)–(54), we conclude that

$$E(\mathbf{m}, l, s'') = \frac{\zeta(s'')}{\zeta_{\mathbf{m}'}(s'')}E_6(\mathbf{m}, l, s''), \tag{55}$$

wherein $E_6(\mathbf{m}, l, s'')$ is regular for $\sigma'' > 1/2 + \varepsilon$ and subject to the estimate

$$|E_6(\mathbf{m}, l, s'')| = O(\{(\mathbf{m})\}^{1/2+\varepsilon}\|\mathbf{m}\|^{\varepsilon} l^{\varepsilon}) = O(\{(\mathbf{m})\}^{1/2}\|\mathbf{m}\|^{\varepsilon} l^{\varepsilon}) \tag{56}$$

in virtue of (30), (32), and elementary properties of divisor-type functions.

We have now reached the point at which we need to assume an

Extended Riemann Hypothesis (5). *The Riemann zeta-function $\zeta(s)$ and the Dedekind zeta-functions $\zeta_{\mathbf{m}'}(s)$ (defined over the corpora $\mathbb{Q}(\theta)$ introduced in Section 6) have no zeros in the half-plane $\sigma > 1/2$.*

From this supposition, since $\zeta(s)/\zeta_{\mathbf{m}'}(s)$ is regular and non-zero for $\sigma > 1/2$ and since the discriminant $\Box_{\mathbf{m}'}$ of $\mathbb{Q}(\theta_{\mathbf{m}'})$ divides $D^2_{\mathbf{m}'}\Delta_{\mathbf{m}'}$, the methods of Titchmarsh ([7], Chapter XIV) (see also the author [5]) yield

$$\zeta(s)/\zeta_{\mathbf{m}'}(s) = O\{|\Box_{\mathbf{m}'}|^{\varepsilon}(|t|+1)^{\varepsilon}\}$$

for $\sigma \ge 1/2 + \varepsilon$, wherefore

$$\zeta(s)/\zeta_{\mathbf{m}'}(s) = O\{\|\mathbf{m}\|^{\varepsilon}(|t|+1)^{\varepsilon}\} \tag{57}$$

because $|\Box_{\mathbf{m}'}| \le D^2_{\mathbf{m}'}\Delta_{\mathbf{m}'} = O(\Delta^9_{\mathbf{m}'}) = O(\|\mathbf{m}'\|^{54})$ by (30) and (32).

All preparations are in place for the estimation of $\Gamma(\mathbf{m}, s')$, it being assumed during the calculation that $l \le x$, $1 \le v \le x$, and $\sigma' \ge \varepsilon$. By a well-known formula and then by (55)–(57), we first infer that

$$\begin{aligned}\Psi(\mathbf{m}, l, v, s') &= \frac{1}{2\pi i}\int_{1/2+\varepsilon-i\infty}^{1/2+\varepsilon+i\infty} E(\mathbf{m}, l, s+s')\frac{v^s}{s^2}\,ds\\ &= O\Big(v^{1/2+\varepsilon}\{(\mathbf{m})\}^{1/2}\|\mathbf{m}\|^{\varepsilon} l^{\varepsilon}\int_{-\infty}^{\infty}\frac{(|t+t'|+1)^{\varepsilon}}{(|t|+1)^2}\,dt\Big)\\ &= O\Big(x^{\varepsilon} v^{1/2}\{(\mathbf{m})\}^{1/2}\|\mathbf{m}\|^{\varepsilon}\int_{-\infty}^{\infty}\frac{|t|^{\varepsilon}+(|t'|+1)^{\varepsilon}}{(|t|+1)^2}\,dt\Big)\\ &= O(x^{\varepsilon} v^{1/2}\{(\mathbf{m})\}^{1/2}\|\mathbf{m}\|^{\varepsilon}(|t'|+1)^{\varepsilon}).\end{aligned}$$

(5) It is enough to assume the hypothesis for the functions $\zeta_{\mathbf{m}'}(s)$, since all zeros of $\zeta(s)$ are zeros of $\zeta_{\mathbf{m}'}(s)$.

Therefore, deploying (47) and then (37) and (46), we conclude that

$$
\begin{aligned}
(58)\qquad & \Gamma(\mathbf{m}, s') \\
&= O\biggl(x^\varepsilon \eta(\mathbf{m})\|\mathbf{m}\|^\varepsilon(|t'|+1)^\varepsilon \sum_{l\le\eta} \frac{\mu^2(l)|\Theta(\mathbf{m}, l, s')|\cdot|S(\mathbf{m}, l)|}{l^{2+\sigma'}}\biggr) \\
&= O\biggl(x^\varepsilon \eta(\mathbf{m})\|\mathbf{m}\|^\varepsilon(|t'|+1)^\varepsilon \sum_{l\le\eta} \frac{\{(\mathbf{m}, l)\}^2}{l}\biggr) \\
&= O\biggl(x^\varepsilon \eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon(|t'|+1)^\varepsilon \sum_{l\le\eta} \frac{(\mathbf{m}, l)}{l}\biggr) \\
&= O(x^\varepsilon \eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon(|t'|+1)^\varepsilon d\{(\mathbf{m})\}\log\eta) \\
&= O(x^\varepsilon \eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon(|t'|+1)^\varepsilon) \qquad (\sigma' \ge \varepsilon)
\end{aligned}
$$

in virtue of a well known bound for the sum occurring in the antepenultimate line.

At last we can return to $\gamma(\mathbf{m}, u)$ in (43), noting that the coefficient of $k^{-s'}$ in its generating function $\Gamma(\mathbf{m}, s')$ is

$$\frac{\varrho_k S(\mathbf{m}, k)}{k} = O\{k^2 d_3(k)\}$$

by an utterly trivial estimation that suffices for one of our purposes here. Hence, utilizing the familiar result

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{v^s}{s}\,ds = \begin{cases} 1 + O(v^c/(T\log v)) & \text{if } v > 1, \\ O(v^c/(T|\log v|)) & \text{if } v < 1, \end{cases}$$

that is certainly valid for $c > 0$ and $T \ge 1$ and then supposing in the first place that $u - 1/2$ is a positive integer not exceeding η^2, we deduce in the usual way that

$$
\begin{aligned}
(59)\qquad \gamma(\mathbf{m}, u) &= \frac{1}{2\pi i}\int_{5-iT}^{5+iT} \Gamma(\mathbf{m}, s)\frac{u^s}{s}\,ds + O\biggl(\frac{u^5}{T}\sum_{k\le\eta^2}\frac{k^2 d_3(k)}{k^5|\log u/k|}\biggr) \\
&= \frac{1}{2\pi i}\int_{5-iT}^{5+iT} \Gamma(\mathbf{m}, s)\frac{u^s}{s}\,ds + O\biggl(\frac{u^5}{T}\sum_{k\le\eta^2}\frac{d_3(k)}{k^2}\biggr) \\
&= \frac{1}{2\pi i}\int_{5-iT}^{5+iT} \Gamma(\mathbf{m}, s)\frac{u^s}{s}\,ds + O\biggl(\frac{u^5}{T}\biggr),
\end{aligned}
$$

the integral in which is

$$\frac{1}{2\pi i}\int_{\varepsilon-iT}^{\varepsilon+iT}\Gamma(\mathbf{m},s)\frac{u^s}{s}\,ds+O\biggl(\frac{u^5x^\varepsilon\eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon}{T^{1-\varepsilon}}\biggr)\tag{60}$$
$$=O\biggl(u^\varepsilon x^\varepsilon\eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon\int_0^T\frac{dt}{(1+t)^{1-\varepsilon}}\biggr)+O\biggl(\frac{u^5x^\varepsilon\eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon}{T^{1-\varepsilon}}\biggr)$$
$$=O(u^\varepsilon T^\varepsilon x^\varepsilon\eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon)+O\biggl(\frac{u^5x^\varepsilon\eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon}{T^{1-\varepsilon}}\biggr)$$

by (58). The second term in (59) being accounted for by an expression like the second one in the last line of (60), we finally conclude that

$$\gamma(\mathbf{m},u)=O(x^\varepsilon\eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon)\qquad(1\le u\le\eta^2)\tag{61}$$

on choosing $T=u^5$ and then expunging the now irrelevant restriction that $u-1/2$ be an integer. In particular, we should observe that for $u=\eta^2$ the estimate (61) is the same as what a direct treatment of $\gamma(\mathbf{m},\eta^2)$ would yield.

9. Completion of the estimations of $Q_\eta^{\$}(M,\mathbf{y})$ and $Q_\eta^{\dagger}(M,\mathbf{y})$. Equipped with (61), we look back at (42) and obtain

$$T_\eta(M,\mathbf{y};\mathbf{m})=O(x^\varepsilon\eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon|\psi(\mathbf{m},\eta^2)|)+O\Bigl(x^\varepsilon\eta\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon\int_1^{\eta^2}|\psi'(\mathbf{m},u)|\,du\Bigr)$$

so that

$$Q_\eta^{\$}(M,\mathbf{y})=O\Bigl(x^\varepsilon\eta\sum_{\mathbf{m}\notin\mathcal{S}',\,\mathbf{m}\ne0}\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon|\psi(\mathbf{m},\eta^2)|\Bigr)+O\Bigl(x^\varepsilon\eta\int_1^{\eta^2}\sum_{\mathbf{m}\notin\mathcal{S}',\,\mathbf{m}\ne0}\{(\mathbf{m})\}^2\|\mathbf{m}\|^\varepsilon|\psi'(\mathbf{m},u)|\,du\Bigr)\tag{62}$$
$$=O(x^\varepsilon\eta\Xi_1(\eta))+O\Bigl(x^\varepsilon\eta\int_1^{\eta^2}\Xi_2(u)\,du\Bigr),\quad\text{say,}$$

because of (36).

Next, by (41) and symmetry and then by Lemma 2,

$$\Xi_1(\eta)=O\biggl(\frac{1}{\eta^4}\sum_{0\le m_1<m_2,m_3}m_2^\varepsilon m_3^\varepsilon\{(m_1,m_2,m_3)\}^2\times\biggl|W\Bigl(\frac{m_1M}{\eta^2}\Bigr)W\Bigl(\frac{m_2M}{\eta^2}\Bigr)W\Bigl(\frac{m_3M}{\eta^2}\Bigr)\biggr|\biggr)\tag{63}$$

$$= O\left\{\frac{1}{\eta^4}\sum_{r=1}^{\infty} r^{2+2\varepsilon}\left(\sum_{m_1'\geq 0}\left|W\left(\frac{m_1' rM}{\eta^2}\right)\right|\right)\right.$$
$$\left.\times\left(\sum_{m_4'>0} m_4'^{\varepsilon}\left|W\left(\frac{m_4' rM}{\eta^2}\right)\right|\right)^2\right\}$$
$$= O\left(\frac{\eta^{2+4\varepsilon}}{M^3}\sum_{r\leq \eta^2/M}\frac{1}{r}\right) + O\left(\frac{\eta^8}{M^6}\sum_{r>\eta^2/M}\frac{1}{r^{4-2\varepsilon}}\right)$$
$$= O\left(\frac{\eta^{2+\varepsilon}}{M^3}\right).$$

The estimation of $\Xi_2(u)$ is similar to that of $\Xi_1(\eta)$ but is considerably more complicated. First, by differentiation and (11),

(64) $\quad \psi'(\mathbf{m}, u)$

$$= O\left(\frac{1}{u^3}\prod_{1\leq i\leq 3}\left|W\left(\frac{m_i M}{u}\right)\right|\right) + O\left(\frac{\|\mathbf{m}\| x^{1/3}}{u^4}\prod_{1\leq i\leq 3}\left|W\left(\frac{m_i M}{u}\right)\right|\right)$$
$$+ O\left(\frac{M}{u^4}\sum_{(i_1,i_2,i_3)}|m_{i_1}|\left|W'\left(\frac{m_{i_1}M}{u}\right)\right|\cdot\left|W\left(\frac{m_{i_2}M}{u}\right)\right|\cdot\left|W\left(\frac{m_{i_3}M}{u}\right)\right|\right)$$
$$= O\{\psi_1(\mathbf{m}, u)\} + O\{\psi_2(\mathbf{m}, u)\} + O\{\psi_3(\mathbf{m}, u)\}, \quad \text{say,}$$

where (i_1, i_2, i_3) in the sum defining $\psi_3(\mathbf{m}, u)$ runs through all cyclic permutations of $(1, 2, 3)$. Next, limiting detailed attention to the effect of the third term in the last line of (64), we see that the contribution of $\psi_3(\mathbf{m}, u)$ to $\Xi_2(u)$ is

$$O\left(\frac{M}{u^4}\sum_{m_1>0;\, 0\leq m_2<m_3}(m_1, m_2, m_3)^2 m_1^{1+\varepsilon} m_3^{\varepsilon}\right.$$
$$\left.\times\left|W'\left(\frac{m_1 M}{u}\right)\right|\cdot\left|W\left(\frac{m_2 M}{u}\right)\right|\cdot\left|W\left(\frac{m_3 M}{u}\right)\right|\right)$$

because of (62), symmetry, and the definition of $\mathcal{S}'$. This equals

$$O\left\{\frac{M}{u^4}\sum_{r=1}^{\infty} r^{3+2\varepsilon}\left(\sum_{m_1'>0} m_1'^{\,1+\varepsilon}\left|W'\left(\frac{m_1' rM}{u}\right)\right|\right)\right.$$
$$\left.\times\left(\sum_{m_2'\geq 0}\left|W\left(\frac{m_2' rM}{u}\right)\right|\right)\left(\sum_{m_3'>0} m_3'^{\varepsilon}\left|W\left(\frac{m_3' rM}{u}\right)\right|\right)\right\},$$

which Lemma 2 tells us is

$$O\left(\frac{u^{2\varepsilon}}{M^3}\sum_{r\le u/M}\frac{1}{r}\right)+O\left(\frac{u^2}{M^5}\sum_{r>u/M}\frac{1}{r^{3-2\varepsilon}}\right)=O\left(\frac{x^{\varepsilon}}{M^3}\right) \tag{65}$$

through estimations that become partially trivial when $u < M$. Since parallel methods shew that the contributions of $\psi_1(\mathbf{m},u)$ and $\psi_2(\mathbf{m},u)$ are likewise

$$O\left(\frac{x^{\varepsilon}}{M^3}\right) \quad \text{and} \quad O\left(\frac{x^{1/3+\varepsilon}}{M^4}\right),$$

respectively, we end the estimation of $Q_\eta^{\$}(M,\mathbf{y})$ by deducing the relation

$$Q_\eta^{\$}(M,\mathbf{y})=O\left(\frac{x^{\varepsilon}\eta^3}{M^3}\right)+O\left(\frac{x^{1/3+\varepsilon}\eta^3}{M^4}\right)=O\left(\frac{x^{1/3+\varepsilon}\eta^3}{M^4}\right)$$

from (62)–(65) and (6).

Combining this with (39) in (36), we thus conclude that

$$Q_\eta^{\dagger}(M,\mathbf{y})=O\left(\frac{x^{1/3+\varepsilon}\eta^3}{M^4}\right)+O\left(\frac{x^{\varepsilon}\eta^2}{M^2}\right)=O\left(\frac{x^{1/3+\varepsilon}\eta^3}{M^4}\right) \tag{66}$$

in view of (2) and (6).

10. The final theorem. We are almost at our destination. From (19), (24), (25), and (66) we have

$$\begin{aligned} Q_\eta(M,\mathbf{y}) &= \frac{AM^3}{\log\eta}+O\left(\frac{M^3}{\log^2\eta}\right)+O\left(\frac{x^{1/3+\varepsilon}\eta^3}{M}\right) \\ &= \frac{AM^3}{\log\eta}+O\left(\frac{M^3}{\log^2\eta}\right)+O(M^3x^{\varepsilon-2\varepsilon_1}) \\ &< \frac{(A+\varepsilon_1)M^3}{\log\eta} \qquad (x>x_0(\varepsilon_1)) \end{aligned} \tag{67}$$

on choosing ε so that $\varepsilon=\varepsilon_1$. Thus, by (14),

$$P_\eta^*(M,\mathbf{y}) < \frac{(A+\varepsilon_1)M^3}{\log\eta}$$

and so, by (9) and (10), we arrive at

$$\begin{aligned} P(x) &\le \frac{(A+\varepsilon_1)}{\log\eta}\int_{\mathbf{y}\in\mathcal{B}_1} d\mathbf{y}+O(x^{1/3})=\frac{(A+\varepsilon_1)V_1}{\log\eta}+O(x^{1/3}) \\ &< (A+\varepsilon_1)\Gamma^3\left(\frac{4}{3}\right)\frac{x}{\log\eta} \\ &< 3(A+\varepsilon_1)\Gamma^3\left(\frac{4}{3}\right)\frac{x}{\log x} \qquad (x>x_0'(\varepsilon_1)) \end{aligned}$$

after taking (2) into consideration. We have thus obtained our main

THEOREM 1. *Let* $P(x)$ *be the number of positive primes* p *not exceeding* x *that are the sum of three non-negative cubes, multiple representations of any such* p *being counted according to multiplicity. Then, if the Riemann hypothesis be valid for the Riemann zeta-function and the Dedekind zeta-functions defined over the cubic fields* $\mathbb{Q}(\theta)$ *introduced in Section* 6 *above, we have*

$$P(x) < 3(A+\varepsilon)\Gamma^3\left(\frac{4}{3}\right)\frac{x}{\log x} \qquad (x > x_1(\varepsilon)),$$

where

$$A = \prod_{\varpi \equiv 1 \,(\mathrm{mod}\, 3)} \left(1 - \frac{a_\varpi}{\varpi^2}\right)$$

as in equation (25) *above.*

Also, as explained in the Introduction, we have the following unconditional

THEOREM 2. *With the notation of Theorem* 1, *we have*

$$P(x) < 4(A+\varepsilon)\Gamma^3\left(\frac{4}{3}\right)\frac{x}{\log x} \qquad (x > x_1'(\varepsilon)),$$

unconditionally.

References

[1] H. Davenport, *On the class-number of binary cubic forms* (*I*), J. London Math. Soc. 26 (1951), 183–192.

[2] —, *On the class-number of binary cubic forms* (*II*), ibid., 192–198.

[3] C. F. Gauss, *Disquisitiones Arithmeticae*, Fleischer, Leipzig, 1801.

[4] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio numerorum'*; *III*: *On the expression of a number as a sum of primes*, Acta Math. 44 (1923), 1–70.

[5] C. Hooley, *On Waring's problem*, ibid. 157 (1986), 49–97.

[6] —, *On nonary cubic forms*, J. Reine Angew. Math. 386 (1988), 32–98.

[7] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Clarendon Press, Oxford, 1951.

School of Mathematics
University of Wales College of Cardiff
Senghennydd Road
Cardiff CF2 4YH, Great Britain

Received on 2.4.1996 (2955)