ON THE REPRESENTATIONS OF A NUMBER AS THE SUM OF FOUR FIFTH POWERS

JOEL M. WISDOM

1. *Introduction*

It is known from Vaughan and Wooley's work on Waring's problem that every sufficiently large natural number is the sum of at most 17 fifth powers [13]. It is also known that at least six fifth powers are required to be able to express every sufficiently large natural number as a sum of fifth powers (see, for instance, [5, Theorem 394]). The techniques of [13] allow one to show that almost all natural numbers are the sum of nine fifth powers. A problem of related interest is to obtain an upper bound for the number of representations of a number as a sum of a fixed number of powers. Let $R(n)$ denote the number of representations of the natural number n as a sum of four fifth powers. In this paper, we establish a non-trivial upper bound for $R(n)$, which is expressed in the following theorem.

THEOREM 1.1.   *If $R(n)$ denotes the number of representations of n as a sum of four fifth powers, then*
$$R(n) \ll n^{(11/30)+\varepsilon}.$$

To consider the strength of this result, one can obtain $R(n) \ll n^{(2/5)+\varepsilon}$ by using standard estimates for the divisor function. In fact, if we let $r(n)$ denote the number of representations of n as the sum of two non-negative fifth powers, then we have

$$R(n) = \sum_{0 \leqslant m \leqslant n} r(m)\, r(n-m) \leqslant \sum_{0 \leqslant m \leqslant n} r^2(m) \ll n^{2/5},$$

where the last inequality follows from an asymptotic formula of Hooley given in [6]. For later developments concerning sums of two powers, see also Hooley [9, 10]. Therefore, Theorem 1.1 yields a saving of 1/30 over the first trivial estimate.

It is often easy to obtain close to square root cancellation, as we see above, but it is very difficult to achieve results which do better than square root cancellation when there are four or more variables. The only other such result we are aware of is due to Hooley, who showed in [8] that the number of representations of an integer n as the sum of four cubes is $O(n^{(11/18)+\varepsilon})$, which saves 1/18 from the trivial estimate. Our work carries Hooley's methods over to cover the case of fifth powers by using his work in [8] as a framework. Hooley's argument depended on transforming his original equation into

$$2r(h^6 r^2 + 3s^2) = m - Z^3 - W^3, \tag{1.1}$$

where h accounts for common factors of the original variables. Selberg's upper bound sieve is employed by creating a larger sequence of integers containing the terms $3s^2$,

and then bounding the number of solutions to congruential equations which must hold. If one makes the same transformations for the equation involving the sum of four kth powers, where k is odd, then the equation corresponding to (1.1) is of the form

$$2r\Psi(h^{2k}r^2, s^2) = m - Z^k - W^k, \tag{1.2}$$

where $\Psi(x, y)$ is a homogeneous polynomial of degree $(k-1)/2$. When $k = 5$, we are able to complete the square in (1.2) to obtain an equation of the form

$$2r(5U^2 - 4h^{20}r^4) = m - Z^5 - W^5,$$

which allows one to proceed in a similar manner to that of Hooley. However, when k is larger than 5, we cannot simply separate out all of the cross terms involving both r^2 and s^2, so that we cannot consider the congruential equations in the same manner. For this reason, we were only able to establish a result for fifth powers with the present techniques. Another important part of the argument is using exponential sums to represent the number of solutions to the resulting equations, and bounding the terms expected to be of lower order by estimates for these exponential sums.

For convenient reference, we make a few comments about the notation used in this paper. It should be noted that d always denotes an integer satisfying the description which follows (4.5), and that variables with a subscript of d are of the nature described in Section 4. Also, $\mathscr{P}(a_1, a_2, a_3, a_4)$ represents a condition on a_1, a_2, a_3, a_4 described at the beginning of Section 4. We use $\ll$ and $\gg$ to denote Vinogradov's familiar notation, where the constants depend at most on ε. As usual, the greatest common divisor of $u_1, \ldots, u_j$ is denoted by $(u_1, \ldots, u_j)$, the divisor function of n is denoted by $\tau(n)$, $\omega(u)$ denotes the number of prime factors of u, $\sigma_j(u)$ denotes the sum of the jth powers of the divisors of u, and $\|\varsigma\|$ denotes the distance of ς from the nearest integer; we denote $e(x) = e^{2\pi i x}$. The Legendre symbol is written as $(a \mid p)$ or (a/p).

2. Related results

Before beginning the proof of Theorem 1.1, we discuss what one might expect to be true about this problem. Basic counting arguments might lead one to conjecture that $R(n) \ll n^\varepsilon$. This would follow as a consequence of hypothesis K of Hardy and Littlewood [4], which would state that the corresponding statement is true for sums of five fifth powers. The failure of hypothesis K for cubes casts doubt on its validity for higher powers, but even if hypothesis K fails for fifth powers, the corresponding conjecture may hold in the case of sums of four fifth powers since there is one less summand. Lower bounds for the number of representations of an integer as the sum of five fifth powers are considered by Erdős and Szemerédi in [2, 3], where [2] obtains a lower bound of the form $\exp(c \log n / \log \log n)$, but there is little work on lower bounds in our case.

If we let $N(x)$ denote the number of integers $n \leqslant x$ for which $R(n)$ is non-zero, then we see that $N(x) \ll x^{4/5}$. To examine how many representations can usually arise, we can use Vaughan's work concerning exponential sums over smooth numbers [12] to easily obtain the following result.

THEOREM 2.1.   *For almost all natural numbers n with $n \leqslant x$, and such that n has at least one representation as a sum of four fifth powers, one has*

$$R(n) \ll n^\theta,$$

where $\theta = 0.08773126$.

Proof. Let n be a sufficiently large natural number. We consider representations of n as a sum of fifth powers of smooth numbers by defining

$$R^*(n) = \mathrm{card}\{u_1^5 + u_2^5 + u_3^5 + u_4^5 = n : u_i \in \mathscr{A}(n^{1/5}, n^\eta)\},$$

where

$$\mathscr{A}(X, Y) = \{m \leqslant X : p \mid m \Rightarrow p \leqslant Y\},$$

and η is a sufficiently small positive number. By noting that $\mathrm{card}\,\mathscr{A}(n^{1/5}, n^\eta) \gg n^{1/5}$, we see by the Cauchy–Schwarz inequality that

$$(x^{4/5})^2 \ll \left(\sum_{n \leqslant x} R^*(n)\right)^2 \leqslant \mathscr{D}(x)\left(\sum_{\substack{n \leqslant x \\ R^*(n) > 0}} 1\right), \tag{2.1}$$

where

$$\mathscr{D}(x) = \left(\sum_{n \leqslant x} R^*(n)^2\right).$$

If we note that $\mathscr{D}(n)$ is the number of solutions to

$$u_1^5 + u_2^5 + u_3^5 + u_4^5 = v_1^5 + v_2^5 + v_3^5 + v_4^5$$

with $u_i, v_i \in \mathscr{A}(n^{1/5}, n^\eta)$, then by [**12**],

$$\mathscr{D}(n) < (n^{1/5})^{\kappa_1}, \tag{2.2}$$

where $\kappa_1 = 4.438\,656\,3$, provided that η is sufficiently small. Noting that $R^*(n) \leqslant R(n)$, we now have from (2.1) and (2.2) that

$$N(x) \gg x^{\kappa_2}, \tag{2.3}$$

where $\kappa_2 = 0.712\,268\,74$. Suppose that some positive proportion of the numbers n represented as a sum of four fifth powers satisfy

$$R(n) \geqslant Cn^\theta, \tag{2.4}$$

where C is some constant and $\theta = 4/5 - \kappa_2 = 0.087\,731\,26$. However, we know that

$$\sum_{1 \leqslant n \leqslant x} R(n) \ll x^{4/5},$$

so that if C is too large, then (2.3) and (2.4) would lead to a contradiction. This gives the desired result. $\qquad\square$

3. *Initial transformations*

We now begin to prove Theorem 1.1, which will be completed in Section 14. Let $R(n)$ denote the number of solutions of the Diophantine equation

$$X^5 + Y^5 + Z^5 + W^5 = n, \tag{3.1}$$

in non-negative integers. We begin by transforming this equation into a form where we can obtain an upper bound for $R(n)$ by using a sieve method.

If we let $R'(n)$ denote the number of solutions in $R(n)$ when at least two of the variables are non-zero, then we obtain

$$R(n) = R'(n) + O(1). \tag{3.2}$$

For any representation arising in $R'(n)$, one of the non-zero variables must have the same parity as one of the other (not necessarily non-zero) variables, so that

$$R'(n) \ll \sum_{\substack{X^5+Y^5+Z^5+W^5=n \\ X>0,\, X\geqslant Y;\, X\equiv Y \,(\mathrm{mod}\,2)}} 1.$$

By substituting

$$X = r_1 + s, \quad Y = r_1 - s, \tag{3.3}$$

where r_1 is a positive integer and s is a non-negative integer, we see that

$$R'(n) \ll R''(n), \tag{3.4}$$

where

$$R''(n) = \sum_{2r_1(r_1^4+10r_1^2s^2+5s^4)=n-Z_1^5-W_1^5} 1, \tag{3.5}$$

where s also satisfies $0 \leqslant s < n^{1/5}$.

To examine $R''(n)$, consider solutions of the equation

$$2r_1(r_1^4 + 10r_1^2 s^2 + 5s^4) = n - Z_1^5 - W_1^5$$

for which

$$(n, r_1, Z_1^5, W_1^5) = h_1.$$

By writing

$$h_1 = h_2 h^5,$$

where h_2 is fifth power free, we have for these solutions

$$n = mh^5, \quad r_1 = rh^5, \quad Z_1 = Zh, \quad W_1 = Wh,$$
$$(m, r, Z^5, W^5) = h_2, \quad 2h^{25} \leqslant n,$$

so that

$$R''(n) = \sum_{\substack{h^5 \mid n \\ h \leqslant (n/2)^{1/25}}} v(n/h^5, h), \tag{3.6}$$

where for given values of m and h, we define $v(m, h)$ to be the number of solutions in r, s, Z, W of the equation

$$2r(h^{20}r^4 + 10h^{10}r^2s^2 + 5s^4) = m - Z^5 - W^5 \tag{3.7}$$

for which (m, r, Z^5, W^5) is fifth power free, and also $0 \leqslant s < hm^{1/5}$.

4. Introduction of the Selberg sieve

Most of our work involves estimating $v(m, h)$ for values of m and h which we can consider to be fixed until the completion of the proof in Section 14. For brevity of exposition, let the notation $\mathscr{P}(\mathbf{u})$ stand for the condition that (u_1, u_2, u_3, u_4) is fifth power free. Since the values of h which appear in (3.6) satisfy $h \leqslant (n/2)^{1/25}$, we only need to consider values of m and h where m is sufficiently large and $h \leqslant (m/2)^{1/20}$. We then have

$$v(m, h) = \sum_{r \leqslant M} \Xi(m, r, h), \tag{4.1}$$

where

$$M = M(m, h) = (m/2h^{20})^{1/5} < m^{1/5} \tag{4.2}$$

and where $\Xi(m, r, h)$ is the number of solutions in s, Z, and W of (3.7) for fixed values of m, r, and h, where the solutions must satisfy the condition $\mathscr{P}(m, r, Z^5, W^5)$. Note

that any solutions must have $Z, W \leqslant m^{1/5}$, since r is positive. To obtain an upper bound for $\Xi(m, r, h)$, we first complete the square in (3.7) by letting $U = s^2 + h^{10}r^2$, so that (3.7) becomes

$$2r(5U^2 - 4h^{20}r^4) = m - Z^5 - W^5. \tag{4.3}$$

Now we can replace the term $5U^2$ by a member of some larger set which includes all numbers of the form $5U^2$. To do this, let $\mathfrak{S} = \mathfrak{S}(m, r)$ be the set of all integers (positive or negative) that are not quadratic non-residues, modulo p, for all primes p such that

$$p \nmid r, \tag{4.4}$$

$$p \nmid m, \quad \left(\frac{5}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = -1, \quad p > D_1, \tag{4.5}$$

where D_1 is a suitable absolute constant greater than 5.

We are now in a position to use Selberg's upper bound sieve method as described in [7, Chapter 1] to obtain an upper bound for the characteristic function of $\mathfrak{S}$. Let d denote a square-free number (possibly 1) consisting entirely of prime factors p satisfying (4.4) and (4.5), and let $\mathfrak{h}(d)$ denote the set of all integers that are quadratic non-residues modulo each prime divisor of d (where $\mathfrak{h}(1)$ is the set of all integers). We now introduce real numbers $\lambda_d = \lambda_{d, m, r, h}$ which satisfy the conditions that $\lambda_1 = 1$ and $\lambda_d = 0$ for $d > \xi = m^\beta$, where β will be determined later to satisfy $0 < \beta < 2/5$. Then considering

$$\left(\sum_{u \in \mathfrak{h}(d)} \lambda_d\right)^2 = \sum_{u \in \mathfrak{h}(d)} \rho_d$$

as a function of u, we see that this function is non-negative and is equal to 1 when u is five times a square, and that this is an upper bound for the characteristic function of $\mathfrak{S}$. It is convenient to note that we can express ρ_d as

$$\rho_d = \sum_{[d_1, d_2] = d} \lambda_{d_1} \lambda_{d_2}, \tag{4.6}$$

so that $\rho_d = 0$ for $d > \xi^2 = m^{2\beta}$.

Combining this upper bound with the definition of $\Xi(m, r, h)$ and (4.3), and noting that solutions to (4.3) satisfy $Z, W \leqslant m^{1/5}$, we obtain

$$\Xi(m, r, h) \leqslant \sum_{Z, W, L} \sum_{\substack{d \\ L \in \mathfrak{h}(d)}} \rho_d,$$

where the first summation is over Z and W with $0 \leqslant Z, W \leqslant m^{1/5}$ and where $\mathscr{P}(m, r, Z^5, W^5)$ holds, and over L satisfying $2r(L - 4h^{20}r^4) = m - Z^5 - W^5$. This yields

$$\Xi(m, r, h) \leqslant \sum_{d \leqslant \xi^2} \rho_d \Phi(m, r, h, d) = \Theta(m, r, h), \tag{4.7}$$

say, where $\Phi(m, r, h, d)$ denotes the number of solutions in $\tilde{L}_d, Z, W$ of the conditions

$$2r(\tilde{L}_d - 4h^{20}r^4) = m - Z^5 - W^5; \quad Z, W \leqslant m^{1/5}; \quad \mathscr{P}(m, r, Z^5, W^5), \tag{4.8}$$

in which $\tilde{L}_d$ means that $\tilde{L}_d$ lies in $\mathfrak{h}(d)$. By looking back at (4.1), we see that

$$v(m, h) \leqslant \sum_{r \leqslant M} \Theta(m, r, h). \tag{4.9}$$

In order to estimate $\Theta(m, r, h)$, we need to transform $\Phi(m, r, h, d)$. Let l_d throughout refer to an integer belonging to any given complete set of incongruent representatives of $\mathfrak{h}(d)$, modulo d. Then the number of solutions to (4.8) is the same as the number of solutions in l_d, Z, W of

$$2r(l_d - 4h^{20}r^4) \equiv m - Z^5 - W^5 \pmod{2rd}, \quad \mathscr{P}(m, r, Z^5, W^5), \qquad (4.10)$$

where $Z, W \leqslant m^{1/5}$. Let $Y(m, r, h, d)$ denote the number of solutions in l_d, Z, W of (4.10) with $Z, W < 2rd$. Therefore, we can rewrite $\Phi(m, r, h, d)$ as

$$\Phi(m, r, h, d) = \frac{([m^{1/5}] + 1)^2}{4r^2 d^2} Y(m, r, h, d) + \Phi_2(m, r, h, d), \qquad (4.11)$$

where $\Phi_2(m, r, h, d)$ is defined by this relation. Since $(r, d) = 1$, then $Y(m, r, h, d)$ is the number of simultaneous solutions of the conditions

$$m - Z^5 - W^5 \equiv 0 \pmod{2r}, \qquad (4.12)$$

$$\mathscr{P}(m, r, Z^5, W^5), \qquad (4.13)$$

$$m - Z^5 - W^5 \equiv 2r(l_d - 4h^{20}r^4) \pmod{d}, \qquad (4.14)$$

for which $Z, W < 2rd$. Therefore we can write

$$Y(m, r, h, d) = \psi(m, r)\, \gamma(m, r, h, d),$$

where $\psi(m, r)$ is the number of incongruent solutions in Z and W, modulo $2r$, of (4.12) and (4.13), and where $\gamma(m, r, h, d)$ is the number of incongruent solutions in Z, W, l_d, modulo d, of (4.14). If we define

$$\Phi_1(m, r, h, d) = \frac{\gamma(m, r, h, d)}{d^2}, \qquad (4.15)$$

then (4.11) can be written as

$$\Phi(m, r, h, d) = \frac{([m^{1/5}] + 1)^2 \psi(m, r)}{4r^2} \Phi_1(m, r, h, d) + \Phi_2(m, r, h, d). \qquad (4.16)$$

Thus, if we let

$$\Theta_i(m, r, h) = \sum_{d \leqslant \xi^2} \rho_d \Phi_i(m, r, h, d) \qquad (4.17)$$

for $i = 1, 2$, then (4.7) yields

$$\Theta(m, r, h) = \frac{([m^{1/5}] + 1)^2 \psi(m, r)}{4r^2} \Theta_1(m, r, h) + \Theta_2(m, r, h). \qquad (4.18)$$

To conclude our preliminary work, let

$$v_1(m, h) = \frac{([m^{1/5}] + 1)^2}{4} \sum_{r \leqslant M} \frac{\psi(m, r)\, \Theta_1(m, r, h)}{r^2} \qquad (4.19)$$

and let

$$v_2(m, h) = \sum_{r \leqslant M} \Theta_2(m, r, h), \qquad (4.20)$$

so that by (4.9) and (4.18), we obtain

$$v(m, h) \leqslant v_1(m, h) + v_2(m, h). \qquad (4.21)$$

5. *Lemmas on congruences*

We next develop some lemmas which are useful in estimating $v_1(m, h)$ and $v_2(m, h)$, and which are the analogues of [**8**, Lemmas 1 and 2].

LEMMA 5.1.   *Let $g(u; v)$ be the multiplicative function of u defined on prime powers by*

$$g(p^\alpha; v) = \begin{cases} p^{\alpha-2} & \text{if } \alpha = 3 \text{ or } 4, \text{ and } p^\alpha | v \\ 1 & \text{otherwise.} \end{cases} \tag{5.1}$$

Then we have

$$\psi(m, r) \ll 11^{\omega(r)} r\, g(r; m).$$

Proof.   If p^α is any prime power, let $\psi_1(m, p^\alpha)$ denote the number of solutions in Z and W, modulo p^α, of

$$m - Z^5 - W^5 \equiv 0 \pmod{p^\alpha}, \tag{5.2}$$

such that $\mathscr{P}(m, p^\alpha, Z^5, W^5)$ also holds, and let $\psi_2(m, 2^b)$ for $b > 0$ denote the number of solutions, modulo 2^{b+1}, of

$$m - Z^5 - W^5 \equiv 0 \pmod{2^{b+1}} \quad \text{and} \quad \mathscr{P}(m, 2^b, Z^5, W^5).$$

Then if we write

$$r = 2^b \prod_{p>2} p^{\alpha_p},$$

it follows that $\psi(m, r)$ satisfies the inequality

$$\psi(m, r) \leqslant \psi_2(m, 2^b) \prod_{p>2} \psi_1(m, p^{\alpha_p}). \tag{5.3}$$

Also,

$$\psi_2(m, 2^b) \leqslant 4\psi_1(m, 2^b). \tag{5.4}$$

In the light of (5.3) and (5.4), we want to bound $\psi_1(m, p^\alpha)$, where p^α is any prime power, so we examine the possible values of α. If $\alpha = 1$, then for each given value of Z, there are at most five values of W, modulo p, satisfying (5.2), so that

$$\psi_1(m, p^\alpha) \leqslant 5p. \tag{5.5}$$

When $\alpha \geqslant 2$, we first examine solutions of (5.2) which do not satisfy the condition

$$Z \equiv W \equiv 0 \pmod{p}. \tag{5.6}$$

These solutions satisfy either $m - Z^5 \not\equiv 0$, mod p, or $m - W^5 \not\equiv 0$, mod p. In the first case, for each such Z, there are at most five values of W satisfying (5.2), and in the second case, for each appropriate W, there are at most five values of Z satisfying (5.2). Consequently there are at most $10p^\alpha$ solutions of (5.2) which do not satisfy (5.6).

It remains to consider the solutions of (5.2) satisfying (5.6) when $\alpha \geqslant 2$. Note that if $\alpha \geqslant 5$, then there are no solutions of this type contributing to $\psi_1(m, p^\alpha)$, because any solutions satisfying (5.2) and (5.6) would have $p^5 | (m, p^\alpha, Z^5, W^5)$, which is supposed to be fifth power free since $\mathscr{P}(m, p^\alpha, Z^5, W^5)$ holds. Thus when $2 \leqslant \alpha \leqslant 4$, there will be solutions satisfying (5.2) and (5.6) if and only if $p^\alpha | m$, and there will be $p^{2\alpha-2}$ such solutions.

Combining the conclusions of the previous two paragraphs, we see that if $\alpha = 2$ or $\alpha \geqslant 5$, we have

$$\psi_1(m, p^\alpha) \leqslant 11p^\alpha, \tag{5.7}$$

and if $\alpha = 3$ or 4, then

$$\psi_1(m, p^\alpha) \leqslant \begin{cases} 10p^\alpha & \text{if } p^\alpha \nmid m \\ 11p^{2\alpha-2} & \text{if } p^\alpha \mid m. \end{cases} \tag{5.8}$$

Upon combining (5.3), (5.4), (5.5), (5.7), and (5.8), we have

$$\psi_1(m, p^\alpha) \leqslant 11p^\alpha g(p^\alpha; m), \tag{5.9}$$

which leads to the desired result. $\qquad\square$

The next result which we need is given by the following lemma.

LEMMA 5.2. *Let $T(m, r, h, p)$ denote the number of solutions in a, Z, W, modulo p, of the congruence*

$$2r(a^2 - 4h^{20}r^4) \equiv m - Z^5 - W^5 \pmod{p}. \tag{5.10}$$

If $p \nmid 2r$, then we have

$$T(m, r, h, p) = p^2 + O(p^{3/2}).$$

Proof. Let

$$b(u) = \sum_{x=1}^{p} e(ux^5/p), \quad c(u) = \sum_{x=1}^{p} e(uq(x)/p),$$

where $q(x) = 2r(x^2 - 4h^{20}r^4)$. It is known that if $(u, p) = 1$, then $|b(u)| \leqslant 4p^{1/2}$; see, for instance, [11, Lemma 4.3]. Then we have

$$T(m, r, h, p) = \frac{1}{p} \sum_{u=1}^{p} c(u) b(u)^2 e(-um/p).$$

By applying the Cauchy–Schwarz inequality,

$$|T(m, r, h, p) - p^2| \leqslant \left(\max_{1 \leqslant v \leqslant p-1} |b(v)| \right) \frac{1}{p} \sum_{u=1}^{p-1} |b(u) c(u)|$$

$$\leqslant 4p^{1/2} \left(\frac{1}{p} \sum_{u=1}^{p} |b(u)|^2 \right)^{1/2} \left(\frac{1}{p} \sum_{u=1}^{p} |c(u)|^2 \right)^{1/2}. \tag{5.11}$$

By considering the number of solutions to the underlying congruences $u^5 \equiv v^5 \pmod{p}$ and $q(u) \equiv q(v) \pmod{p}$ of the sums in (5.11), it follows from orthogonality that

$$|T(m, r, h, p) - p^2| \leqslant (4p^{1/2})(5p)^{1/2}(2p)^{1/2} \leqslant 13p^{3/2},$$

which gives the desired result. $\qquad\square$

6. *Estimation of $v_1(m, h)$ by the Selberg sieve*

In order to achieve a bound for $v_1(m, h)$, we employ Selberg's sieve method to bound $\Theta_1(m, r, h)$, where the condition for each prime p which we are sieving out is the property of being a quadratic non-residue, modulo p.

Let p denote a prime satisfying (4.4) and (4.5). Recalling (4.14) and that if $d = p$, then l_p must lie in $\mathfrak{h}(p)$, we see that

$$\gamma(m, r, h, p) = p^2 - \frac{1}{2} T(m, r, h, p) - \frac{1}{2} \psi_1(m + 8h^{20}r^5, p),$$

because each of the p^2 choices of Z and W allows only one possible value, modulo p, for l_p, so that the latter two terms subtract off those values for which l_p is not in $\mathfrak{h}(p)$. (Here, $T(m, r, h, p)$ is defined as in Lemma 5.2, and $\psi_1(m + 8h^{20}r^5, p)$ as defined in Lemma 5.1 compensates for the solutions of (5.10) for which $p \mid a$.) Combining this result with (5.5) and Lemma 5.2 gives

$$\gamma(m, r, h, p) = \frac{1}{2}p^2 + O(p^{3/2}),$$

and from (4.15), this gives

$$\Phi_1(m, r, h, p) = \frac{1}{2} + O(p^{-1/2}). \tag{6.1}$$

Provided that D_1 is chosen sufficiently large, then since $p > D_1$ by (4.5), we have

$$0 < \Phi_1(m, r, h, p) < 1. \tag{6.2}$$

In order to utilize Selberg's sieve method, let

$$f(d) = f(m, r, h, d) = \frac{1}{\Phi_1(m, r, h, d)}, \tag{6.3}$$

and following Hooley's treatment in [7], let

$$f_1(d) = \sum_{k \mid d} \mu(k) f(d/k) = \prod_{p \mid d} (f(p) - 1),$$

where we recall that d is square-free, and observe that $f(d)$ is multiplicative by (4.15), and that since $f(p) > 1$, then $f_1(d) > 0$. From (4.6), (4.17), and (6.3), we see that

$$\Theta_1(m, r, h) = \sum_{d_1, d_2 \leqslant \xi} \frac{\lambda_{d_1} \lambda_{d_2}}{f([d_1, d_2])}. \tag{6.4}$$

Since this sum is the sum which appears in the main term of Selberg's method, then from [7], we see that $\Theta_1(m, r, h)$ has a minimum value of $1/V(\xi)$ subject to the constraints on λ_d, where

$$V(\xi) = V_{m, h, r}(\xi) = \sum_{d \leqslant \xi} \frac{\mu^2(d)}{f_1(d)}, \tag{6.5}$$

and where the λ_d which give this minimum are given by

$$\lambda_d = \frac{\mu(d)}{V(\xi)} \sum_{d_3 \mid d} \frac{\mu^2(d_3)}{f_1(d_3)} \sum_{\substack{d_4 \leqslant \xi/d \\ (d_4, d) = 1}} \frac{\mu^2(d_4)}{f_1(d_4)}. \tag{6.6}$$

From (6.1), we can deduce that for $p > D_1$, where D_1 is suitably large,

$$f_1(p) = 1 + O(p^{-1/2}) < 2 \quad \text{and} \quad f_1(p) > 1/2. \tag{6.7}$$

Then by (6.5) and recalling that primes dividing d must satisfy (4.4) and (4.5), we obtain

$$V(\xi) \geqslant 1 + \frac{1}{2} \sum_{D_1 < p \leqslant \xi} 1,$$

where the primes p in the sum must also satisfy $p \nmid rm$, $(5|p) = 1$, and $(-1|p) = -1$. Therefore,

$$V(\xi) > \frac{D_2 \xi}{\log \xi} \tag{6.8}$$

for some constant D_2, since $r \leqslant M < m$ by (4.2), and since $\xi = m^\beta$, where $0 < \beta < 1$. This gives

$$\Theta_1(m, r, h) \ll m^{-\beta+\varepsilon}.$$

With (4.19), this gives

$$v_1(m, h) \ll m^{(2/5)-\beta+\varepsilon} \sum_{r \leqslant M} \frac{\psi(m, r)}{r^2}. \tag{6.9}$$

To estimate the sum in (6.9), we see from Lemma 5.1 that

$$\sum_{r \leqslant M} \frac{\psi(m, r)}{r^2} \ll \sum_{r \leqslant M} r^{-1+\varepsilon} g(r; m).$$

By noticing that when $p \mid m$,

$$\sum_{j=0}^{\infty} \frac{g(p^j; m)}{p^j} \leqslant 2 \sum_{j=0}^{\infty} p^{-j},$$

and by recalling that $g(u; m)$ is multiplicative in u, we obtain

$$\sum_{r \leqslant M} \frac{\psi(m, r)}{r^2} \ll M^\varepsilon 2^{\omega(m)} \prod_{p \leqslant M} \left(1 - \frac{1}{p}\right)^{-1} \ll m^\varepsilon \log M \ll m^\varepsilon. \tag{6.10}$$

Finally, by using the estimate of (6.10) for the sum in (6.9), we see that

$$v_1(m, h) \ll m^{(2/5)-\beta+\varepsilon}. \tag{6.11}$$

7. Expression for $v_2(m, h)$ in terms of exponential sums

We now need to estimate $v_2(m, h)$. To achieve this bound we first express $\Phi(m, r, h, d)$ using exponential sums, and then appeal to (4.11). Let

$$\mathscr{N}(m, r, d, b, c) = \sum_{\substack{0 \leqslant Z, W \leqslant m^{1/5} \\ Z \equiv b \pmod{2rd} \\ W \equiv c \pmod{2rd}}} 1.$$

Then from (4.8) and (4.10), we have

$$\Phi(m,r,h,d) = \sum_{l_d} \sum_{0 \leqslant b,\,c < 2rd} \mathcal{N}(m,r,d,b,c), \tag{7.1}$$

where the inner sum is over b and c such that

$$2r(l_d - 4h^{20}r^4) \equiv m - b^5 - c^5 \quad (\mathrm{mod}\ 2rd) \tag{7.2}$$

and $\mathscr{P}(m,r,b^5,c^5)$ both hold. By orthogonality, one has

$$4r^2d^2\mathcal{N}(m,r,d,b,c) = \sum_{0 \leqslant Z,\,W \leqslant m^{1/5}} \sum_{0 \leqslant u,\,v < 2rd} e((u(b-Z)+v(c-W))/2rd)$$

$$= \tilde{m}^2 + \tilde{m} \sum_{0 < u < 2rd} \theta_u\, e(ub/2rd) + \tilde{m} \sum_{0 < v < 2rd} \theta_v\, e(vc/2rd)$$

$$+ \sum_{0 < u,\,v < 2rd} \theta_u\, \theta_v\, e((ub+vc)/2rd), \tag{7.3}$$

where $\tilde{m} = [m^{1/5}] + 1$, and

$$\theta_w = \theta_{w,\,2rd,\,m} = \sum_{0 \leqslant V \leqslant m^{1/5}} e(-wV/2rd) \leqslant \frac{1}{\|w/2rd\|}. \tag{7.4}$$

Therefore, by substituting (7.3) back into (7.1), and comparing this with (4.11), we see that

$$\Phi_2(m,r,h,d) = \frac{[m^{1/5}]+1}{2r^2d^2} \sum_{0 < u < 2rd} \theta_u\, S(m,r,h,d;u,0)$$

$$+ \frac{1}{4r^2d^2} \sum_{0 < u,\,v < 2rd} \theta_u\, \theta_v\, S(m,r,h,d;u,v), \tag{7.5}$$

where

$$S(m,r,h,d;u,v) = \sum_{l_d} \sum_{0 \leqslant b,\,c < 2rd} e((ub+vc)/2rd), \tag{7.6}$$

with the inner sum of (7.6) being over b and c such that (7.2) and $\mathscr{P}(m,r,b^5,c^5)$ both hold.

Let $S^*(m,r,h,d;u,v;l_d)$ be the inner sum of (7.6), so that

$$S(m,r,h,d;u,v) = \sum_{l_d} S^*(m,r,h,d;u,v;l_d). \tag{7.7}$$

From (7.4) and (7.5), we obtain

$$\Phi_2(m,r,h,d) \ll \frac{m^{1/5}}{rd} \sum_{0 < |u| < m} \frac{|S(m,r,h,d;u,0)|}{|u|}$$

$$+ \sum_{0 < |u|,\,|v| < m} \frac{|S(m,r,h,d;u,v)|}{|u|\,|v|}, \tag{7.8}$$

where the limits of summation are obtained from (4.2), (4.17), and (4.20), which give

$$rd \leqslant M\xi^2 < m^{(1/5)+2\beta} \leqslant m.$$

Next, from (4.17), (4.20), and (7.8), we obtain

$$v_2(m,h) \ll m^{1/5} \sum_{0<|u|<m} \frac{1}{|u|} \sum_{r \leqslant M} \frac{1}{r} \sum_{d \leqslant \xi^2} \frac{|\rho_{d,r}| \, |S(m,r,h,d;u,0)|}{d}$$

$$+ \sum_{0<|u|,|v|<m} \frac{1}{|u|\,|v|} \sum_{r \leqslant M} \sum_{d \leqslant \xi^2} |\rho_{d,r}| \, |S(m,r,h,d;u,v)|. \tag{7.9}$$

We now need to estimate the size of ρ_d which occurs in our expression for $v_2(m,h)$. To do this, we need to consider (6.6), which gives the optimal values for the λ_d. In examining the sums given in (6.6), if we recall (6.7) and that d_3 and d_4 are square-free, we see that

$$\sum_{d_3 | d} \frac{\mu^2(d_3)}{f_1(d_3)} \leqslant \tau(d) \, 2^{\omega(d)} \ll d^\varepsilon \ll (\xi^2)^\varepsilon \ll m^\varepsilon,$$

and that

$$\sum_{\substack{d_4 \leqslant \xi/d \\ (d_4,d)=1}} \frac{\mu^2(d_4)}{f_1(d_4)} \leqslant \sum_{d_4 \leqslant \xi/d} \frac{\mu^2(d_4)}{f_1(d_4)} \ll \sum_{d_4 \leqslant \xi/d} 2^{\omega(d_4)} \ll \frac{m^\varepsilon \xi}{d}.$$

By using (6.8) and these results in (6.6), we get

$$\lambda_d \ll \frac{m^\varepsilon}{d},$$

so that by (4.6), we have

$$\rho_d \ll m^\varepsilon \sum_{[d_1,d_2]=d} \frac{1}{d_1 \, d_2} \ll \frac{m^\varepsilon}{d} \sum_{[d_1,d_2]=d} 1 \ll \frac{m^\varepsilon \tau(d)^2}{d} \ll \frac{m^\varepsilon}{d}. \tag{7.10}$$

Our definition of d depends on r, since the prime factors of d must satisfy (4.4) and (4.5). If we want to remove this dependence of d on r, then we can equivalently require that d be a square-free integer whose prime factors satisfy (4.5), and then require that $(r,d)=1$. This allows us to change the order of summation of r and d by adding the condition that $(r,d)=1$. Therefore, if we use (7.10) in (7.9), we can change the order of summation in the second term of (7.9) to obtain

$$v_2(m,h) \ll m^{(1/5)+\varepsilon} v_3(m,h) + m^\varepsilon v_4(m,h), \tag{7.11}$$

where

$$v_3(m,h) = \sum_{0<|u|<m} \frac{1}{|u|} \sum_{r \leqslant M} \frac{1}{r} \sum_{d \leqslant \xi^2} \frac{|S(m,r,h,d;u,0)|}{d^2}, \tag{7.12}$$

and

$$v_4(m,h) = \sum_{0<|u|,|v|<m} \frac{1}{|u|\,|v|} \sum_{d \leqslant \xi^2} \frac{1}{d} \sum_{\substack{r \leqslant M \\ (r,d)=1}} |S(m,r,h,d;u,v)|. \tag{7.13}$$

In order to estimate $v_3(m,h)$ and $v_4(m,h)$, we first examine some results about exponential sums.

8. Some results on exponential sums

We now develop some results about exponential sums which we will use to estimate $S(m,h,r,d;u,v)$. The first lemma allows us to exhibit a multiplicative property of an exponential sum under suitable conditions.

Lemma 8.1. *Let* $\Psi(k;x,y)$ *indicate a condition on a positive integer k and integers x and y satisfying the following two properties:*

(1) *If* $x' \equiv x \pmod{k}$ *and* $y' \equiv y \pmod{k}$, *then* $\Psi(k;x,y)$ *is equivalent to* $\Psi(k;x',y')$.

(2) *If k_1 and k_2 are coprime, then $\Psi(k_1 k_2;x,y)$ holds if and only if $\Psi(k_1;x,y)$ and $\Psi(k_2;x,y)$ both hold.*

Let the exponential sum $P(k;u,v)$ be given by

$$P(k;u,v) = \sum_{\substack{\Psi(k;x,y) \\ 0 \leqslant x,y < k}} e((ux+vy)/k).$$

Then if $(k_1,k_2) = 1$, we have

$$P(k_1,k_2;u,v) = P(k_1;\bar{k}_2 u, \bar{k}_2 v)\, P(k_2;\bar{k}_1 u, \bar{k}_1 v),$$

where $\bar{k}_1$ and $\bar{k}_2$ are defined to the appropriate modulus so that

$$k_1 \bar{k}_1 \equiv 1 \pmod{k_2}, \quad k_2 \bar{k}_2 \equiv 1 \pmod{k_1}.$$

Proof. The proof relies on the Chinese remainder theorem, and Hooley gives a sketch of the proof following [**8**, Lemma 3]. □

This leads to the following useful lemma.

Lemma 8.2. *Let $P(k;u,v)$ be defined as in Lemma 8.1. If u and v are given and $(k_1,k_2) = 1$, then there exist integers u_1,v_1,u_2,v_2 such that*

$$P(k_1 k_2;u,v) = P(k_1;u_1,v_1)\, P(k_2;u_2,v_2),$$

and

$$(k_1 k_2, u, v) = (k_1, u_1, v_1)(k_2, u_2, v_2).$$

We also need a bound on exponential sums which comes from a result of Chalk and Smith [**1**], which they proved using algebraic geometry.

Lemma 8.3. *For given values of p,u,v,μ such that $p \nmid (u,v)\mu$, we have*

$$\left| \sum_{\substack{x^5 + y^5 \equiv \mu \pmod{p} \\ 0 \leqslant x,y < p}} e((ux+vy)/p) \right| \leqslant 20 p^{1/2} + 25.$$

Proof. The result is trivial for $p = 5$. For all other primes p, the result follows from [**1**, Theorem 2], because $x^5 + y^5 - \mu$ is absolutely irreducible when considered over the finite field with p elements. (One may verify that the curve defined by the equation $x^5 + y^5 = \mu$ has no singular points in the projective plane, from which the absolute irreducibility of $x^5 + y^5 - \mu$ follows as an immediate consequence of Bezout's theorem.) □

The estimate given in the preceding lemma allows us to bound an exponential sum arising from $S^*(m,r,h,d;u,v;l_d)$.

Lemma 8.4.   *Let $Q(k;u,v;\mu)$ be defined by*

$$Q(k;u,v;\mu) = \sum_{0 \leqslant x,y < 2k} e((ux+vy)/2k), \qquad (8.1)$$

where the sum is over x and y for which $x^5 + y^5 \equiv \mu \pmod{k}$ and $\mathscr{P}(\mu,k,x^5,y^5)$ both hold. Next, let $\nabla(k,\omega)$ be the multiplicative function of k defined on prime powers by

$$\nabla(p^\alpha,\omega) = \begin{cases} 1 & \text{if } \alpha = 1 \text{ and } p \nmid \omega \\ p^{\alpha/2} & \text{otherwise.} \end{cases} \qquad (8.2)$$

Also, let $\mathscr{H}(t;w_1,w_2;b)$ be the multiplicative function of t defined on prime powers by

$$\mathscr{H}(p^\alpha;w_1,w_2;b) = \begin{cases} g(p^\alpha;b) & \text{if } p^{\alpha-1} \mid (w_1,w_2) \\ 1 & \text{otherwise.} \end{cases} \qquad (8.3)$$

Then

$$Q(k;u,v;\mu) \ll 21^{\omega(k)} k^{1/2} \nabla(k,\mu(u,v)) \, \mathscr{H}(k;u,v;\mu).$$

Proof.   Let $k = 2^{\alpha_0} \prod_{j=1}^{t} p_j^{\alpha_j}$, where the primes p_j are distinct and exceed 2. Let $Q_1(k;u,v;\mu)$ be defined by

$$Q_1(k;u,v;\mu) = \sum_{0 \leqslant x,y < k} e((ux+vy)/k),$$

where the sum is over x and y for which $x^5 + y^5 \equiv \mu \pmod{k}$ and $\mathscr{P}(\mu,k,x^5,y^5)$ both hold. Then by repeated application of Lemma 8.2, for some integers u_j and v_j,

$$Q(k;u,v;\mu) = Q(2^{\alpha_0};u_0,v_0;\mu) \prod_{j=1}^{t} Q_1(p_j^{\alpha_j};u_j,v_j;\mu), \qquad (8.4)$$

where

$$(k,u,v) = \prod_{j=1}^{t} (p_j^{\alpha_j},u_j,v_j).$$

By (5.4) and (5.9), we see that

$$Q(2^{\alpha_0};u_0,v_0;\mu) \leqslant 11 \cdot 2^{\alpha_0+4},$$

which is sufficient for use in (8.4) when the prime dividing k is 2.

When $j \geqslant 1$, we consider the various possible values for α_j, and show that in each case we have

$$Q_1(p_j^{\alpha_j};u_j,v_j;\mu) \leqslant 21 p_j^{\alpha_j/2} \nabla(p_j^{\alpha_j},\mu(u,v)) \, \mathscr{H}(p_j^{\alpha_j};u,v;\mu), \qquad (8.5)$$

which will suffice to prove the lemma. When $\alpha_j = 1$ and $p_j \nmid \mu(u_j,v_j)$, then since $p_j \nmid \mu(u,v)$, we see from Lemma 8.3 that (8.5) will hold when p is sufficiently large. In the cases where $\alpha_j = 2$, $\alpha_j \geqslant 5$, or the case where $\alpha_j = 1$ and $p_j \mid \mu(u_j,v_j)$, we obtain (8.5) by applying the triangle inequality and (5.9).

It remains to consider the cases where $\alpha_j = 3$ or 4. We observe that the condition $\mathscr{P}(\mu,p_j^{\alpha_j},x^5,y^5)$ will hold automatically since $\alpha_j < 5$. From the argument in the proof of Lemma 5.1, there are at most $10 p_j^{\alpha_j}$ values of x and y appearing in the summation for $Q_1(p_j^{\alpha_j};u_j,v_j;\mu)$ which do not satisfy $x \equiv y \equiv 0 \pmod{p_j}$. On substituting $x = px'$ and $y = py'$ in the remaining terms, we observe that

$$Q_1(p_j^{\alpha_j};u_j,v_j;\mu) \leqslant 10 p_j^{\alpha_j} + \left| \sum_{0 \leqslant x',y' < p^{\alpha-1}} e((u_j x' + v_j y')/p^{\alpha-1}) \right|$$

$$\leqslant 10 p_j^{\alpha_j} + \left| \sum_{0 \leqslant x' < p^{\alpha-1}} e(u_j x'/p^{\alpha-1}) \sum_{0 \leqslant y' < p^{\alpha-1}} e(v_j y'/p^{\alpha-1}) \right|. \qquad (8.6)$$

Since the final term in (8.6) only occurs when $p_j^{\alpha_j} | \mu$, and is zero unless $p^{\alpha-1} | (u_j, v_j)$, we see that (8.5) holds in these cases as well, since $(p_j^{\alpha_j}, u, v) = (p_j^{\alpha_j}, u_j, v_j)$. The lemma now follows from (8.4) and (8.5). □

We have now laid the framework to obtain an expression for $S(m, r, h, d; u, v)$ that will be used to estimate $v_3(m, h)$ and $v_4(m, h)$. If $S^*(m, r, h, d; u, v; l_d)$ is as defined in (7.6) and (7.7), then by Lemma 8.1,

$$S^*(m, r, h, d; u, v; l_d) = Q(r; \bar{d}u, \bar{d}v; m)\, U^*(m, r, h, d; \overline{2r}u, \overline{2r}v; l_d), \qquad (8.7)$$

where $d\bar{d} \equiv 1 \pmod{2r}$, and $2r\overline{2r} \equiv 1 \pmod{d}$, and where

$$U^*(m, r, h, d; x, y; l_d) = \sum_{0 \leqslant b, c < d} e((xb + yc)/d),$$

in which the sum is over b, c such that

$$2r(l_d - 4h^{20}r^4) \equiv m - b^5 - c^5 \pmod{d}. \qquad (8.8)$$

(Recall that d is square-free, so that $\mathscr{P}(m, d, b^5, c^5)$ will always hold for solutions satisfying (8.8), and which also means we are justified in applying Lemma 8.2.) By (8.7) and (7.7),

$$S(m, r, h, d; u, v) = Q(r; \bar{d}u, \bar{d}v; m) \sum_{l_d} U^*(m, r, h, d; \overline{2r}u, \overline{2r}v; l_d)$$

$$= Q(r; \bar{d}u, \bar{d}v; m)\, U(m, r, h, d; \overline{2r}u, \overline{2r}v), \qquad (8.9)$$

where

$$U(m, r, h, d; x, y) = \sum_{l_d} \sum_{0 \leqslant b, c < d} e((xb + yc)/d), \qquad (8.10)$$

with the sum over l_d, b, c satisfying (8.8). Recalling that $(2r, \bar{d}) = 1$, we can use Lemma 8.4 to obtain the upper bound

$$S(m, r, h, d; u, v) \ll 21^{\omega(r)} r^{1/2} \nabla(r, m(u, v))\, \mathscr{H}(r; u, v; m)\, |U(m, r, h, d; \overline{2r}u, \overline{2r}v)|. \qquad (8.11)$$

9. Estimation of $v_3(m, h)$

We are now able to obtain a bound for $v_3(m, h)$. In order to do this, it is sufficient to use (8.11) to deduce the bound

$$S(m, r, h, d; u, v) \ll 21^{\omega(r)} r^{1/2} \nabla(r, m(u, v))\, g(r; m)\, d^2. \qquad (9.1)$$

Using this bound in (7.12), we see that

$$v_3(m, h) \ll m^\varepsilon \sum_{0 < |u| < m} \frac{1}{|u|} \sum_{r \leqslant M} \frac{\nabla(r, m(u, 0))\, g(r; m)}{r^{1/2}} \sum_{d \leqslant \xi^2} 1$$

$$\ll m^\varepsilon \xi^2 \sum_{0 < |u| < m} \frac{1}{|u|} \sum_{r \leqslant M} \frac{\nabla(r, mu)\, g(r; m)}{r^{1/2}}$$

$$\ll m^{(1/10) + 2\beta + \varepsilon} \sum_{0 < u < m} \frac{1}{u} \sum_{r \leqslant m^{1/5}} \frac{\nabla(r, mu)\, g(r; m)}{r}. \qquad (9.2)$$

By (5.1) and (8.2), the inner sum of (9.2) satisfies

$$\sum_{r \leqslant m^{1/5}} \frac{\nabla(r, mu)\, g(r; m)}{r} \leqslant \prod_{\substack{p \mid mu \\ p \leqslant m}} \left(1 + \frac{2}{p} + O(p^{-3/2})\right) \prod_{p \mid mu} \left(2 + \frac{2}{p^{1/2}} + O(p^{-1})\right)$$

$$\leqslant 2^{\omega(mu)} \prod_{p \leqslant m} \left(1 + \frac{1}{p}\right)^3 \prod_{p \mid mu} \left(1 + \frac{1}{p^{1/2}} + O(p^{-1})\right)$$

$$\leqslant m^\varepsilon \sigma_{-1/4}(mu) \leqslant m^\varepsilon \tau(mu) \leqslant m^\varepsilon,$$

since $0 < u < m$. Inserting this estimate into (9.2) yields

$$v_3(m, h) \ll m^{(1/10)+2\beta+\varepsilon} \sum_{0 < u < m} \frac{1}{u} \ll m^{(1/10)+2\beta+\varepsilon} \log m \ll m^{(1/10)+2\beta+\varepsilon}, \tag{9.3}$$

which proves to be a sufficient bound for $v_3(m, h)$.

10. *Preparations for estimating $v_4(m, h)$*

In order to estimate $v_4(m, h)$, we desire an estimate for the inner sum of the expression for $v_4(m, h)$ given by (7.13), which we denote by

$$\Omega(m, h, d; u, v) = \sum_{\substack{r \leqslant M \\ (r, d)=1}} |S(m, r, h, d; u, v)|. \tag{10.1}$$

Note that by virtue of the conditions on the summation in (7.13), we only need to consider values of m, h, d, u, v for which $0 < |u|, |v| < m$, d is square-free and primes dividing d satisfy (4.5), and $d < \xi^2$. Then by (8.11), we have

$$\Omega(m, h, d; u, v) \ll m^{(1/10)+\varepsilon}$$

$$\times \sum_{\substack{r \leqslant m^{1/5} \\ (r, d)=1}} \nabla(r, m(u, v))\, \mathscr{H}(r; u, v; m)\, |U(m, r, h, d; \overline{2ru}, \overline{2rv})|.$$

Next,

$$\Omega(m, h, d; u, v) \ll m^{(1/10)+\varepsilon} \sum_{\substack{0 \leqslant \Delta \leqslant d \\ (\Delta, d)=1}} |U(m, \Delta, h, d; \overline{2\Delta u}, \overline{2\Delta v})|$$

$$\times \sum_{\substack{r \leqslant m^{1/5} \\ r \equiv \Delta \,(\mathrm{mod}\, d)}} \nabla(r, m(u, v))\, \mathscr{H}(r; u, v; m)$$

$$= m^{(1/10)+\varepsilon} \sum_{\substack{0 \leqslant \Delta \leqslant d \\ (\Delta, d)=1}} |U(m, \Delta, h, d; \overline{2\Delta u}, \overline{2\Delta v})|$$

$$\times \Gamma(m^{1/5}, m(u, v); u, v, m; \Delta, d),$$

where

$$\Gamma(z, \omega; u, v, y; a, k) = \sum_{\substack{r \leqslant z \\ r \equiv a \,(\mathrm{mod}\, k)}} \nabla(r, \omega)\, \mathscr{H}(r; u, v; y), \tag{10.2}$$

and where $2\Delta \overline{2\Delta} \equiv 1 \,(\mathrm{mod}\, d)$. Then by the Cauchy–Schwarz inequality,

$$\Omega^2(m, h, d; u, v) \ll m^{(1/5)+\varepsilon} \Omega_1(m, h, d; u, v)\, G(m^{1/5}, m(u, v); u, v, m; d), \tag{10.3}$$

where

$$\Omega_1(m, h, d; u, v) = \sum_{\substack{0 \leqslant \Delta < d \\ (\Delta, d)=1}} |U(m, \Delta, h, d; \overline{2\Delta u}, \overline{2\Delta v})|^2, \tag{10.4}$$

and where

$$G(z, \omega; u, v, y; k) = \sum_{\substack{0 \leqslant a < k \\ (a, k)=1}} |\Gamma(z, \omega; u, v, y; a, k)|^2. \tag{10.5}$$

11. *Estimation of* $\Omega_1(m, h, d; u, v)$

In order to obtain an upper bound for Ω, we need bounds for Ω_1 and G, so in this section, we obtain an upper bound for $\Omega_1(m, h, d; u, v)$. To do this, we first consider $U(m, \Delta, h, d; \overline{2\Delta}u, \overline{2\Delta}v)$ by replacing the variables of summation l_d, b, c in (8.10) by L_d, B, C, where

$$l_d \equiv 16\Delta^4 L_d \pmod{d}, \quad b \equiv 2\Delta B \pmod{d}, \quad c \equiv 2\Delta C \pmod{d}.$$

Note that since l_d is in $\mathfrak{h}(d)$, then L_d is also in $\mathfrak{h}(d)$, because $(2\Delta, d) = 1$, and because $16\Delta^4$ is a quadratic residue modulo d. This change of variables causes the congruence condition in (8.8) to become

$$L_d + B^5 + C^5 \equiv (\overline{2\Delta})^5 m - \overline{4}h^{20} \pmod{d}, \tag{11.1}$$

so that

$$U(m, \Delta, h, d; \overline{2\Delta}u, \overline{2\Delta}v) = \sum_{L_d} \sum_{0 \leqslant B, C < d} e((uB + vC)/d), \tag{11.2}$$

where the summation is over L_d, B, C satisfying (11.1). Since all prime divisors of d must satisfy (4.5), then $(m, d) = 1$, so that the congruence

$$(\overline{2\Delta})^5 m - \overline{4}h^{20} \equiv \mu \pmod{d}$$

has at most $5^{\omega(d)} \ll d^\varepsilon$ solutions in Δ, modulo d. Then by (10.4) and (11.2),

$$\Omega_1(m, h, d; u, v) \ll d^\varepsilon \sum_{0 \leqslant \mu < d} \left| \sum_{L_d} \sum_{0 \leqslant B, C < d} e((uB + vC)/d) \right|^2,$$

where the inner sums are over L_d, B, C for which $L_d + B^5 + C^5 \equiv \mu \pmod{d}$. If we let

$$H(d; u, v) = \sum_{l_d, L_d} \sum_{0 \leqslant b, c, B, C < d} e((uB + vC - ub - vc)/d), \tag{11.3}$$

where the sum is over l_d, L_d, b, c, B, C satisfying

$$L_d + B^5 + C^5 \equiv l_d + b^5 + c^5 \pmod{d}, \tag{11.4}$$

then we have

$$\Omega_1(m, h, d; u, v) \ll d^\varepsilon H(d; u, v). \tag{11.5}$$

In order to estimate $H(d; u, v)$, we make use of the following multiplicative property.

LEMMA 11.1.   *If* $(k_1, k_2) = 1$, *then we have*

$$H(k_1 k_2; u, v) = H(k_1; u_1, v_1) H(k_2; u_2, v_2),$$

where $(k_1 k_2, u, v) = (k_1, u_1, v_1)(k_2, u_2, v_2)$.

Proof.   The proof is similar to those of Lemma 8.1 and Lemma 8.2   □

The following result about quadratic non-residues is also useful.

LEMMA 11.2.   *Let* $\kappa(p, \mu)$ *denote the number of solutions in* L_p *and* l_p, *modulo* p, *of the congruence*

$$L_p - l_p \equiv \mu \pmod{p}.$$

If $(-1 \,|\, p) = -1$, then

$$\kappa(p, \mu) = \begin{cases} (p-3)/4 & \text{if } p \nmid \mu \\ (p-1)/2 & \text{if } p \,|\, \mu. \end{cases}$$

Proof.   This is Lemma 8 in Hooley [**8**], in which there is a short proof.   □

We are now in a position to obtain a bound for $H(d; u, v)$ in the following result.

LEMMA 11.3.   *If $H(d; u, v)$ is defined as in* (11.3), *then*

$$H(d; u, v) \ll d^{3+\varepsilon}(d, u, v)^2,$$

for d which are square-free and whose prime factors satisfy (4.4) *and* (4.5).

Proof.   The proof of this lemma is essentially the same as that of [**8**, Lemma 9], which we include for the sake of completeness. Owing to the restrictions on d, it suffices to prove the lemma for $H(p; u, v)$ for primes p satisfying $(-1 \,|\, p) = -1$, from which the general result follows by Lemma 11.1. Note that if $(p, u, v) = p$, then the result is trivial, so we only need to prove it when $(p, u, v) = 1$.

If we rewrite (11.4) as

$$L_p - l_p \equiv b^5 + c^5 - B^5 - C^5 \pmod{p}, \tag{11.6}$$

then we can see from Lemma 11.2 that, if b, c, B, C are fixed, then (11.6) has $(p-3)/4$ solutions, modulo p, in L_p and l_p when

$$B^5 + C^5 \not\equiv b^5 + c^5 \pmod{p},$$

and that (11.6) has $(p-1)/2$ solutions when

$$B^5 + C^5 \equiv b^5 + c^5 \pmod{p}.$$

Combining these two contributions gives

$$H(p; u, v) = \frac{p+1}{4} \sum_{0 \leqslant \mu < p} \left| \sum_{B^5 + C^5 \equiv \mu \pmod{p}} e((uB + vC)/p) \right|^2$$

$$+ \frac{p-3}{4} \left| \sum_{0 \leqslant B < p} e(uB/p) \right|^2 \left| \sum_{0 \leqslant C < p} e(vC/p) \right|^2$$

$$= \frac{p+1}{4} \sum_{0 \leqslant \mu < p} \left| \sum_{B^5 + C^5 \equiv \mu \pmod{p}} e((uB + vC)/p) \right|^2,$$

where the second term in the first equation vanishes since $(p, u, v) = 1$. Thus, Lemma 8.3 gives

$$H(p; u, v) \ll p(p^2 + (p-1)p) \ll p^3,$$

which proves the result in the specialized case, and the general case follows by the preparatory remarks.   □

On substituting the bound for $H(d; u, v)$ from Lemma 11.3 into (11.5), we may conclude this section with the desired estimate

$$\Omega_1(m, h, d; u, v) \ll d^{3+\varepsilon}(d, u, v)^2. \tag{11.7}$$

12. *Estimation of* $G(z, \omega; u, v, y; k)$

We now require an estimate for $G(z, \omega; u, v, y; k)$ to use in (10.3).

LEMMA 12.1. *Let* $\mathscr{F}(t; a)$ *denote the multiplicative function of t defined on prime powers by*

$$\mathscr{F}(p^\alpha; a) = \begin{cases} p & \text{if } \alpha = 2 \text{ and } p \mid a \\ p^2 & \text{if } \alpha \geqslant 3 \text{ and } p \mid a \\ 1 & \text{otherwise.} \end{cases}$$

Then for $1 \leqslant \omega \leqslant z^{10}$, *we have*

$$G(z, \omega; u, v, y; k) \ll \mathscr{F}(u; y)^2 \left(\frac{z^{2+\varepsilon} k^\varepsilon}{k} + z^{1+\varepsilon} k^{2+\varepsilon} \right).$$

Proof. We first observe from (8.3) and (5.1) that for any values of r and v, we have

$$\mathscr{H}(r; u, v; y) \leqslant \mathscr{F}(u; y).$$

On noting that $\mathscr{H}(r; u, v; 1) = 1$, we have from (10.2)

$$\Gamma(z, \omega; u, v, y; a, k) \leqslant \mathscr{F}(u; y) \Gamma(z, \omega; u, v, 1; a, k). \tag{12.1}$$

Substituting (12.1) into (10.5) yields

$$G(z, \omega; u, v, y; k) \leqslant \mathscr{F}(u; y)^2 G(z, \omega; u, v, 1; k). \tag{12.2}$$

In [8], Hooley defines G and Γ which do not depend on the parameters u, v or y, and which only differ from our definitions in that they do not contain the factor of $\mathscr{H}(r; u, v; y)$ which appears in (10.2) in our definition of $\Gamma(z, \omega; u, v, y; a, k)$. (The function ∇ which appears in (10.2) is identical to that of Hooley.) From (8.3) and (5.1), we see that $\mathscr{H}(r; u, v; y) = 1$, so that when $y = 1$, our functions G and Γ are identical to those of Hooley. Therefore, by [8, Lemma 10], we have

$$G(z, \omega; u, v, 1; k) \leqslant \frac{z^{2+\varepsilon} k^\varepsilon}{k} + z^{1+\varepsilon} k^{2+\varepsilon}. \tag{12.3}$$

The lemma now follows from (12.2) and (12.3). $\qquad\square$

We can now apply Lemma 12.1 to the factor in (10.3) to obtain

$$G(m^{1/5}, m(u, v); u, v, m; d) \ll \mathscr{F}(u; m)^2 (m^{(2/5)+\varepsilon} d^{-1+\varepsilon} + m^{(1/5)+4\beta+\varepsilon}), \tag{12.4}$$

where $d \leqslant \xi^2 = m^{2\beta}$.

13. *Completion of the estimate for* $v_4(m, h)$

We have now laid the groundwork to obtain an upper bound for $v_4(m, h)$. From (10.3), (11.7), and (12.4), we have

$$\Omega(m, h, d; u, v) \ll (m^{(3/10)+\varepsilon} + m^{(1/5)+3\beta+\varepsilon}) d(d, u, v) \mathscr{F}(u; m).$$

Recalling (10.1), we see from (7.13) that

$$v_4(m, h) \ll (m^{(3/10)+\varepsilon} + m^{(1/5)+3\beta+\varepsilon}) \sum_{0 < |u|, |v| < m} \frac{\mathscr{F}(u; m)}{|u| \, |v|} \sum_{d \leqslant \xi^2} (d, u, v). \tag{13.1}$$

The inner sum of (13.1) satisfies

$$\sum_{0 < d \leqslant \xi^2} (d, u, v) \leqslant \sum_{\delta | (u, v)} \delta \sum_{\substack{0 < d \leqslant \xi^2 \\ \delta | d}} 1 \leqslant \xi^2 \sum_{\delta | (u, v)} 1 = \xi^2 \tau[(u, v)],$$

so that (13.1) becomes

$$v_4(m, h) \ll (m^{(3/10)+2\beta+\varepsilon} + m^{(1/5)+5\beta+\varepsilon}) \sum_{0 < u, v < m} \frac{\mathscr{F}(u; m)}{uv}. \tag{13.2}$$

Since $\mathscr{F}(u; m)$ is multiplicative in u, the sum in (13.2) satisfies

$$\sum_{0 < u, v < m} \frac{\mathscr{F}(u; m)}{uv} \leqslant \sum_{0 < u < m} \frac{\mathscr{F}(u; m)}{u} \sum_{0 < v < m} \frac{1}{v}$$

$$\ll m^\varepsilon \prod_{\substack{p < m \\ p | m}} \left(1 - \frac{1}{p}\right)^{-1} \prod_{\substack{p < m \\ p | m}} \left(1 + \frac{1}{p} + \frac{p}{p^2} + \sum_{j=3}^{\infty} \frac{p^2}{p^j}\right)$$

$$\ll m^\varepsilon 2^{\omega(m)} \prod_{p < m} \left(1 - \frac{1}{p}\right)^{-1} \ll m^\varepsilon \log m \ll m^\varepsilon.$$

Therefore, our bound for $v_4(m, h)$ is

$$v_4(m, h) \ll m^{(3/10)+2\beta+\varepsilon} + m^{(1/5)+5\beta+\varepsilon}. \tag{13.3}$$

14. *Completion of the proof*

We can now proceed to complete the proof of Theorem 1.1. By (7.11), (9.3), and (13.3), we have

$$v_2(m, h) \ll m^{(3/10)+2\beta+\varepsilon} + m^{(1/5)+5\beta+\varepsilon}. \tag{14.1}$$

Next, by (4.21), (6.11), and (14.1),

$$v(m, h) \ll m^{(2/5)-\beta+\varepsilon} + m^{(3/10)+2\beta+\varepsilon} + m^{(1/5)+5\beta+\varepsilon}. \tag{14.2}$$

If we set $\xi = m^{1/30}$, so that $\beta = 1/30$, then (14.2) yields the estimate $v(m, h) \ll m^{11/30}$. One should note that this definition could have been made in Section 4, but we delayed this choice until now to make more clear how the final result depends on our intermediate results. Thus, from (3.6), we have

$$R''(n) \ll n^{(11/30)+\varepsilon} \left(\sum_{h^5 | n} h^{-11/6}\right) \ll n^{(11/30)+\varepsilon}.$$

Finally, by (3.2) and (3.4), this proves Theorem 1.1. $\qquad \square$

References

1. J. CHALK and R. A. SMITH, 'On Bombieri's estimate for exponential sums', *Acta Arith.* 18 (1971) 191–212.
2. P. ERDŐS, 'On the representation of an integer as the sum of k kth powers', *J. London Math. Soc.* 11 (1936) 133–136.

3. P. Erdős and E. Szemerédi, 'On the number of solutions of $m = \sum_{i=1}^{k} x_i^k$', Proceedings of Symposia in Pure Mathematics 24 (ed. N. Diamond, American Mathematical Society, Providence, RI, 1973) 83–90.
4. G. H. Hardy and J. E. Littlewood, 'Some problems of "Partitio Numerorum": VI. Further researches in Waring's problem', *Math. Z.* 23 (1925) 1–37.
5. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th edn (Clarendon Press, Oxford, 1979).
6. C. Hooley, 'On the representation of a number as the sum of two hth powers', *Math. Z.* 84 (1964) 126–136.
7. C. Hooley, *Applications of sieve methods to the theory of numbers* (Cambridge University Press, Cambridge, 1976).
8. C. Hooley, 'On the representations of a number as the sum of four cubes: I', *Proc. London Math. Soc.* (3) 36 (1978) 117–140.
9. C. Hooley, 'On another sieve method and the numbers that are a sum of two hth powers', *Proc. London Math. Soc.* (3) 43 (1981) 73–109.
10. C. Hooley, 'On another sieve method and the numbers that are a sum of two hth powers: II', *J. Reine Angew. Math.* 475 (1996) 55–75.
11. R. C. Vaughan, *The Hardy–Littlewood method* (Cambridge University Press, Cambridge, 1981).
12. R. C. Vaughan, 'A new iterative method in Waring's problem II', *J. London Math. Soc.* (2) 39 (1989) 219–230.
13. R. C. Vaughan and T. D. Wooley, 'Further improvements in Waring's problem', *Acta Math.* 174 (1995) 147–240.

Department of Mathematics
University of Michigan
Ann Arbor
MI 48109-1109
USA

wisdom@math.lsa.umich.edu