SUMS OF TWO KTH POWERS

C. M. Skinner[1] and T. D. Wooley[2]

1. Introduction

An important desideratum, in the additive theory of numbers, is a general understanding of the representation of positive integers as the sum of two kth powers of non-negative integers to match the theory of sums of two squares. Such knowledge would surely have profound and far reaching consequences. Yet at present even the widely held conjecture that when $k \geq 5$, no positive integer can be represented as the sum of two kth powers in two essentially different ways, remains open. Indeed, no value of k is known for which this conjecture holds, nor even is it known that such a value of k necessarily exists (see [7], §21.11 for an overview of what is known concerning this problem). In order to provide quantitative information concerning the latter conjecture, in this paper we consider $\nu_k(x)$, which we define to be the number of positive integers not exceeding x that can be expressed as the sum of two non-negative kth powers in more than one way. Thus the estimate $\nu_k(x) = O(x^{2/k})$ is trivial, and the conjecture above is equivalent to the assertion that $\nu_k(x)$ is zero when $k \geq 5$. In a formidable series of papers, Hooley [8], [9], [10], [11] has shewn that for odd k one has $\nu_k(x) = O_{\varepsilon,k}(x^{5/3k+\varepsilon})$ through the use of a delicate sieve method, utilising estimates deriving from Deligne's resolution of the Riemann hypothesis for varieties over finite fields. Greaves [4] has also made contributions to the subject, and recently has described a very elegant and flexible argument (see [5], [6]), again employing sieve methods, which shows that when $k \geq 3$ one has $\nu_k(x) = O_{\varepsilon,k}(x^{11/6k+\varepsilon})$. In contrast to Hooley's treatment, Greaves requires only Weil's proof of the Riemann hypothesis for finite fields, and for small k a wholly elementary estimate suffices for this aspect of his argument.

In this paper, through an essentially elementary method (avoiding, in particular, any use of sieves or reference to the Riemann hypothesis for finite fields), we establish the following estimate for $\nu_k(x)$.

[1] Supported by an N.S.F. Graduate Fellowship, and, during a visit to the University of Michigan, through the David and Lucile Packard Foundation.

[2] Research supported in part by NSF grant DMS-9303505, an Alfred P. Sloan Research Fellowship, and a Fellowship from the David and Lucile Packard Foundation.

J. Reine Angew. Math. 462 (1995), 57–68

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Theorem 1.1. *Let k be an integer exceeding 2, and let x be a positive real number. Then*

$$\nu_k(x) \ll_{\varepsilon,k} x^{\frac{3}{2k}+\frac{1}{k(k-1)}+\varepsilon}.$$

Moreover, when $k=3$ or 5, one has

$$\nu_k(x) \ll_{\varepsilon,k} x^{\frac{3}{2k}+\frac{1}{k^2}+\varepsilon}.$$

We note that Theorem 1.1 provides estimates superior to those of Greaves and Hooley when $k \geq 6$. In order to establish Theorem 1.1, we consider the non-trivial solutions of the diophantine equation

$$u_1^k + u_2^k = v_1^k + v_2^k. \tag{1.1}$$

Let $S_k(P)$ denote the number of solutions of the equation (1.1) with $1 \leq u_i, v_i \leq P$ $(i=1,2)$. Also, let $T(P)$ denote the corresponding number of trivial solutions of (1.1), which is to say, the number of solutions with $u_1 = v_1$ or $u_1 = v_2$. Then $T(P) = 2P^2 + O(P)$. In §3 we establish the following non-trivial estimate for $S_k(P) - T(P)$.

Theorem 1.2. *Let k be an integer exceeding 2, and let P be a positive real number. Then*

$$S_k(P) - T(P) \ll_{\varepsilon,k} P^{\frac{3}{2}+\frac{1}{k-1}+\varepsilon}. \tag{1.2}$$

Consequently,

$$S_k(P) = 2P^2 + O_{\varepsilon,k}(P^{\frac{3}{2}+\frac{1}{k-1}+\varepsilon}).$$

Moreover, when $k=3$ or $k=5$, one may replace the term $1/(k-1)$ in each of the above estimates by $1/k$.

For comparison, we note that in line with the estimates described in the first paragraph above, it follows from Hooley [10], [11] that an estimate similar to (1.2) holds when k is odd, but with the exponent $\frac{3}{2}+\frac{1}{k-1}$ replaced by $\frac{5}{3}$. Also, Greaves [5], [6] has indicated how to obtain such a conclusion for every $k \geq 3$, save that $\frac{3}{2}+\frac{1}{k-1}$ is replaced by 11/6 (which he refines to 7/4 when $k=4$). Thus, once again, our conclusions are stronger than those obtained hitherto for $k \geq 6$. Perhaps it is also worth noting that the conjecture mentioned in the first paragraph plainly implies that when $k \geq 5$, the only solutions of (1.1) are trivial, whence $S_k(P) = T(P) = 2P^2 + O(P)$. Moreover, the existence of just one non-trivial solution of (1.1) suffices to establish that $S_k(P) - T(P) \gg P$, for whenever $\mathbf{u}, \mathbf{v}$ satisfies (1.1), then so does $t\mathbf{u}, t\mathbf{v}$ for any integer t. Consequently the estimate $S_k(P) - T(P) = o(P)$ is tantamount to the truth of the conjecture. Of course, the truth of a suitable generalisation of the *abc*-conjecture (see [13], Epilogue, or [17], §8) would suffice to establish that the conjecture holds when k is sufficiently large.

In the interests of curtailing our discussion, we refer the reader to [11] for an overview of the many corollaries of the above theorems (but see also work of

Vaughan [14], [15] and Boklan [2] for applications to Waring's problem). We remark, by way of allusion to possible generalisations, that a conclusion similar to Theorem 1.2 may be obtained for the number of solutions of (1.1) with the variables satisfying $|u_i| \le P$ and $|v_i| \le P$ $(i = 1, 2)$, and also for the number of solutions of the equation

$$au_1^k + bu_2^k = av_1^k + bv_2^k,$$

where a and b are fixed integers bounded by a power of P. In each case the number of trivial solutions must be adjusted in an obvious manner.

Our argument depends for its success on an estimate of Bombieri and Pila ([3], Theorem 5) for the number of integral points on a plane affine curve. The crucial feature of their estimate is that it is independent of the coefficients of the polynomial defining the curve. In order to bring the polynomial implicit in (1.1) into a form suitable for the application of the latter result, we are forced in §3 to develop an efficient slicing argument which exploits the special form of our polynomial. Moreover, we also require that the resulting polynomial be absolutely irreducible. In §2, therefore, we establish criteria for absolute irreducibility sufficient for our purposes.

We are grateful to Professor Neil Dummigan for supplying an idea which enabled us to somewhat shorten the argument associated with Lemma 2.4.

2. Preliminary lemmata

We begin by proving an inhomogeneous version of a well-known lemma on solutions of linear equations (compare, for example, A. Baker [1], Chapter 2, Lemma 1). In §3 we apply the case $s = 3$ of this lemma within our slicing argument.

Lemma 2.1. *Suppose that $s \ge 2$, and that $Q_1, \dots, Q_s$ are positive real numbers. Let $x_1, \dots, x_s$ be integers with $1 \le x_i \le Q_i$ $(1 \le i \le s)$. Then the equation $a_1x_1 + \dots + a_sx_s = 0$ is soluble in integers $a_1, \dots, a_s$ with $(a_1, \dots, a_s) = 1$, and*

$$|a_i| \le Q_i^{-1}(sQ_1 \dots Q_s)^{1/(s-1)} \quad (1 \le i \le s).$$

Proof. Write $\mathcal{Q} = (sQ_1 \dots Q_s)^{1/(s-1)}$. Then for fixed $x_1, \dots, x_s$ satisfying the hypotheses of the lemma, each of the integers $b_1x_1 + \dots + b_sx_s$, with the b_i satisfying $0 \le b_i \le \mathcal{Q}/Q_i$ $(1 \le i \le s)$, is bounded above by $\sum_{j=1}^s Q_j[\mathcal{Q}/Q_j]$. Moreover the number of such linear expressions is

$$\prod_{i=1}^s ([\mathcal{Q}/Q_i] + 1) > \sum_{j=1}^s Q_j\,([\mathcal{Q}/Q_j] + 1) > \sum_{j=1}^s Q_j[\mathcal{Q}/Q_j] + 1.$$

Consequently there exist distinct such s-tuples, $\mathbf{b}^{(1)}$ and $\mathbf{b}^{(2)}$, such that

$$\sum_{i=1}^s b_i^{(1)}x_i = \sum_{i=1}^s b_i^{(2)}x_i.$$

We put $a_i = b_i^{(1)} - b_i^{(2)}$ $(1 \le i \le s)$, and observe that the lemma follows immediately on removing the common factor $(a_1, \dots, a_s)$.

The remainder of this section will be taken up with the derivation of estimates for the number of integral points on certain families of curves. Our basic tool, in establishing such results, is the following result of Bombieri and Pila.

Lemma 2.2. *Let C be a curve defined by $F(x,y) = 0$, where $F(x,y) \in \mathbb{R}[x,y]$ is an absolutely irreducible polynomial of degree $d \ge 2$. Also, let $N \ge \exp(d^6)$. Then the number of integral points on C, and inside a square $[0,N] \times [0,N]$, does not exceed*

$$N^{1/d} \exp\left(12\,(d \log N \log\log N)^{1/2}\right).$$

Proof. This is Theorem 5 of Bombieri and Pila [3].

In order to apply Lemma 2.2, we require criteria for a polynomial $f(x,y)$ to be absolutely irreducible. Our first criterion deals with the situation in which $f(x,y)$ has differing degrees with respect to x and y.

Lemma 2.3. *Let*

$$f(x,y) = g_0 y^d + g_1(x) y^{d-1} + \cdots + g_d(x),$$

where g_0 is a non-zero constant, be a polynomial with coefficients in a field K. Put

$$\psi(f) = \max_{1 \le i \le d} \frac{1}{i} \deg(g_i),$$

and suppose that $\psi(f) = m/d$ with $(m,d) = 1$. Then $f(x,y)$ is absolutely irreducible.

Proof. This is Theorem III.1B of Schmidt [12].

Corollary 2.3.1. *Let $p(x)$ and $q(x)$ be polynomials with integral coefficients, of respective degrees k and r. Suppose also that $k > r$ and $(k,r) = 1$. Then the number, $N(X;p,q)$, of solutions of the diophantine equation $p(y) = q(x)$, with $0 \le x, y \le X$, satisfies*

$$N(X;p,q) \ll_{k,\varepsilon} X^{1/k+\varepsilon}.$$

Proof. We apply Lemma 2.3 with $f(x,y) = p(y) - q(x)$. Thus, since $\psi(f) = r/k$ with $(r,k) = 1$, we find that $p(y) - q(x)$ is absolutely irreducible. It therefore follows from Lemma 2.2 that

$$N(X;p,q) \ll_k X^{1/k} \exp\left(12(k \log X \log\log X)^{1/2}\right),$$

and the corollary follows immediately.

We note that the estimate supplied by Corollary 2.3.1 is independent of the coefficients of p and q. This observation is crucial in our later application.

Lemma 2.4. *Let a_1, a_2, b_1 and b_2 be fixed non-zero integers, and define the polynomial $f(u,v) = f(u,v;\mathbf{a},\mathbf{b})$ by*

$$f(u,v) = (a_1u + b_1)^k - (a_1u - b_1)^k - (a_2v + b_2)^k + (a_2v - b_2)^k.$$

Then when $k \geq 2$, the polynomial $f(u,v)$ is absolutely irreducible in $\mathbb{Q}[u,v]$ provided that $b_1 \neq \pm b_2$.

Proof. Let $g_\alpha(\xi_1, \xi_2)$ denote the polynomial defined by

$$g_\alpha(\xi_1,\xi_2) = (\xi_1 + 1)^k - (\xi_1 - 1)^k - \alpha\left((\xi_2 + 1)^k - (\xi_2 - 1)^k\right).$$

Then on making the change of variable $\xi_1 = a_1u/b_1$ and $\xi_2 = a_2v/b_2$, and writing $\alpha = (b_2/b_1)^k$, it follows that $f(u,v)$ is absolutely irreducible in $\mathbb{Q}[u,v]$ if and only if $g_\alpha(\xi_1,\xi_2)$ is absolutely irreducible in $\mathbb{Q}[\xi_1,\xi_2]$. We write

$$h(\xi_1,\xi_2,\xi_3) = \xi_3^{k-1} g_\alpha(\xi_1/\xi_3, \xi_2/\xi_3),$$

and consider the curve $\mathcal{C}$ defined by $h(\xi_1,\xi_2,\xi_3) = 0$ in $\mathbb{P}^2$. If $g_\alpha(\xi_1,\xi_2)$ fails to be absolutely irreducible, then h splits, say as $h = h_1h_2$, with h_1 and h_2 non-trivial polynomials in $\mathbb{C}[\xi_1,\xi_2,\xi_3]$. By Bezout's Theorem, the two curves defined by $h_1 = 0$ and $h_2 = 0$ intersect at least once. Suppose that (η_1,η_2,η_3) is any such point. Then necessarily $\boldsymbol{\eta}$ is a singular point of $\mathcal{C}$, and consequently when $\boldsymbol{\xi} = \boldsymbol{\eta}$ we have

$$h = \frac{\partial h}{\partial \xi_1} = \frac{\partial h}{\partial \xi_2} = 0. \tag{2.1}$$

It follows easily that when $\eta_3 = 0$, then the equations (2.1) imply that $\eta_1 = \eta_2 = 0$, whence there are no singular points with $\eta_3 = 0$. Otherwise we may take $\eta_3 = 1$ in (2.1), and then the equations $\partial h/\partial \xi_i = 0$ $(i = 1,2)$ of (2.1) imply that $(\eta_i + 1)^{k-1} = (\eta_i - 1)^{k-1}$ $(i = 1,2)$. Thus for $i = 1,2$, it follows that $\eta_i = (\omega_i + 1)/(\omega_i - 1)$ for some $(k-1)$th root of unity ω_i with $\omega_i \neq 1$. On substituting into the equation $h = 0$ of (2.1), and recalling the definition of α, we therefore deduce that

$$(b_2/b_1)^k = ((\omega_2 - 1)/(\omega_1 - 1))^{k-1}. \tag{2.2}$$

We now execute an argument outlined to us by Professor Neil Dummigan. Let ω be a primitive $(k-1)$th root of unity, and write $K = \mathbb{Q}(\omega)$. Letting $N = N_{K/\mathbb{Q}}$ denote the norm map from K to $\mathbb{Q}$, and taking norms in equation (2.2), we obtain

$$(N(\omega_2 - 1)/N(\omega_1 - 1))^{k-1} = (N(b_2)/N(b_1))^k = (b_2/b_1)^{k\phi(k-1)}, \tag{2.3}$$

where $\phi(\cdot)$ denotes the Euler ϕ-function. But for $i = 1,2$, each conjugate of $\omega_i - 1$ has absolute value at most 2, and consequently $|N(\omega_i - 1)| \leq 2^{\phi(k-1)}$. We let $n_i = N(\omega_i - 1)$ $(i = 1,2)$, put $d = (n_1,n_2)$, and write $m_i = n_i/d$ $(i = 1,2)$. Also, we put $e = (b_1,b_2)$, and write $c_i = b_i/e$ $(i = 1,2)$. Then from (2.3) we have

$$(m_2/m_1)^{k-1} = (c_2/c_1)^{k\phi(k-1)}, \tag{2.4}$$

with $|m_i| \leq 2^{\phi(k-1)}$ $(i = 1, 2)$, and $(m_1, m_2) = (c_1, c_2) = 1$. We consider the canonical prime factorisation of c_2/c_1, which we write in the form $c_2/c_1 = \pm \prod_p p^{r(p)}$. Suppose that $r(p)$ is non-zero for some prime p. Then without loss of generality we may suppose that $r(p) > 0$. Thus from (2.4) we obtain $p^{k\phi(k-1)r(p)} | m_2^{k-1}$, whence

$$p^{k\phi(k-1)r(p)} \leq m_2^{k-1} \leq 2^{(k-1)\phi(k-1)} < 2^{k\phi(k-1)r(p)}.$$

We have obtained a contradiction, and so $f(u, v)$ fails to be absolutely irreducible only when $b_2/b_1 = \pm 1$, which completes the proof of the lemma.

Corollary 2.4.1. *Let a_1, a_2, b_1 and b_2 be fixed positive integers, and define $f(u, v; \mathbf{a}, \mathbf{b})$ as in the statement of Lemma 2.4. Then the number, $M(X; f)$, of solutions of the diophantine equation $f(u, v; \mathbf{a}, \mathbf{b}) = 0$ with $1 \leq u, v \leq X$, and such that $a_1u + b_1 \neq a_2v + b_2$, satisfies*

$$M(X; f) \ll_{\varepsilon,k} X^{1/(k-1)+\varepsilon}.$$

Proof. Suppose first that $b_1 \neq b_2$. Then $f(u, v)$ has degree $k - 1$, and moreover, by Lemma 2.4 and positivity, $f(u, v)$ is absolutely irreducible. Thus Lemma 2.2 implies that in this case $M(X; f) \ll_{\varepsilon,k} X^{1/(k-1)+\varepsilon}$. Meanwhile, if $b_1 = b_2$ then any solution u, v counted by $M(X; f)$ satisfies the equation $g(a_1u; b_1) = g(a_2v; b_1)$, where $g(z; w) = (z + w)^k - (z - w)^k$. But when z and w are positive, $g(z; w)$ is a strictly increasing function of z, and thus the only solutions of the latter equation must satisfy $a_1u = a_2v$. Consequently, in this case there are no solutions counted by $M(X; f)$ with $a_1u + b_1 \neq a_2v + b_2$. This completes the proof of the corollary.

3. The proof of Theorems 1.1 and 1.2

We first observe that Theorem 1.1 follows almost immediately from Theorem 1.2. For by a suitable rearrangement of variables, it follows that $\nu_k(x)$ is bounded above by the number of integral solutions of the simultaneous inequalities

$$0 < u_1^k + u_2^k = v_1^k + v_2^k \leq x \quad \text{and} \quad 0 \leq u_2 < v_1 \leq v_2 < u_1 \leq x^{1/k}.$$

However, the latter is bounded above by the number of solutions of the diophantine equation (1.1) subject to $0 \leq u_i, v_i \leq x^{1/k}$ and $u_1 \neq v_i$ $(i = 1, 2)$. But the number of such solutions in which one or more variables are zero is $O_{\varepsilon,k}(x^{1/k+\varepsilon})$, by using standard estimates for the divisor function. Thus our initial assertion follows from the consequent inequality

$$\nu_k(x) \leq S_k(x^{1/k}) - T(x^{1/k}) + O_{\varepsilon,k}(x^{1/k+\varepsilon}).$$

Next, when $k \geq 3$, we let $N_k^*(P)$ denote the number of solutions of (1.1) with

$$1 \leq u_2 < v_1 \leq v_2 < u_1 \leq P \quad \text{and} \quad (u_1, u_2, v_1, v_2) = 1. \tag{3.1}$$

Then by rearranging variables, and extracting common factors, it is apparent that

$$S_k(P) - T(P) \ll \sum_{1 \le d \le P} N_k^*(P/d). \tag{3.2}$$

For each solution $\mathbf{u}$, $\mathbf{v}$ counted by $N_k^*(Q)$, we define integers x, y, z, w by $z = v_2 - u_2$, $w = v_2 + u_2$, $x = u_1 - v_1$ and $y = u_1 + v_1$. Then by (3.1) we have $x + y \neq w + z$, and since $(x, y, z, w) | (x + y, w - z, y - x, w + z)$, we have also $(x, y, z, w) = 1$ or 2. Thus we obtain

$$N_k^*(Q) \ll M_k^*(2Q) + M_k^*(Q), \tag{3.3}$$

where $M_k^*(Q)$ denotes the number of solutions of the equation

$$(y + x)^k - (y - x)^k = (w + z)^k - (w - z)^k, \tag{3.4}$$

with

$$1 \le x < y \le Q, \quad 1 \le z < w \le Q, \quad (x, y, z, w) = 1, \quad x + y \neq z + w. \tag{3.5}$$

On collecting together (3.2) and (3.3), we find that Theorem 1.2 follows from Lemmata 3.1 and 3.2 below, according to whether k is odd or even.

Lemma 3.1. *Let k be an odd integer with $k \ge 3$, and define α_k to be $1/k$ when $k = 3$ or $k = 5$, and to be $1/(k - 1)$ otherwise. Then $M_k^*(Q) \ll_{\varepsilon,k} Q^{3/2+\alpha_k+\varepsilon}$.*

Proof. For each solution x, y, z, w of (3.4) counted by $M_k^*(Q)$, we have

$$xP_k(x, y) = zP_k(z, w), \tag{3.6}$$

where we write

$$P_k(s, t) = \sum_{0 \le r < k/2} \binom{k}{2r + 1} s^{2r} t^{k-2r-1}. \tag{3.7}$$

We note for future reference that for real values of s and t, the polynomial $P_k(s, t)$ is zero if and only if $s = t = 0$. We write $d = (x, z)$, and put $x_1 = x/d$ and $z_1 = z/d$. Thus $(x_1, z_1) = 1$. On substituting into (3.6) we obtain

$$x_1 P_k(dx_1, y) = z_1 P_k(dz_1, w). \tag{3.8}$$

Let $S_1(d)$ denote the number of solutions (x_1, y, z_1, w) of the equation (3.8) with

$$(3Q)^{1/2} < x_1 \le Q/d, \tag{3.9}$$

$$1 \le y \le Q, \quad 1 \le z_1 \le Q/d, \quad (x_1, z_1) = 1, \tag{3.10}$$

$$1 \le w \le Q, \quad \text{and} \quad dx_1 + y \neq dz_1 + w. \tag{3.11}$$

Also, let $S_2(d)$ denote the corresponding number of solutions with the condition (3.9) replaced by

$$1 \le x_1 \le (3Q)^{1/2}. \tag{3.12}$$

Then it follows from the preceding paragraph that

$$M_k^*(Q) \le \sum_{1\le d\le Q} \left(S_1(d) + S_2(d)\right). \tag{3.13}$$

We first estimate $S_1(d)$. By Lemma 2.1, for each x_1, z_1 and w satisfying (3.9), (3.10) and (3.11), there exist integers a, b, c with $(a, b, c) = 1$,

$$0 \le |a| \le d^{-1}(3Q)^{1/2}, \quad 0 \le |b|, |c| \le (3Q)^{1/2},$$

and satisfying the equation

$$aw = bz_1 - cx_1. \tag{3.14}$$

Moreover a is non-zero, for otherwise $bz_1 = cx_1$ with $(x_1, z_1) = (b, c) = 1$, whence $x_1 = \pm b$ and $z_1 = \pm c$. The latter implies that $|x_1| = |b| \le (3Q)^{1/2}$, contradicting (3.9), and establishing our assertion. Since $a \ne 0$, we may substitute from (3.14) for w into (3.8) to deduce that

$$S_1(d) \le \sum_{0<|a|\le d^{-1}(3Q)^{1/2}} \sum_{0\le|b|,|c|\le(3Q)^{1/2}} T(d; a, b, c), \tag{3.15}$$

where $T(d; a, b, c)$ denotes the number of solutions of the equation

$$a^{k-1}x_1P_k(dx_1, y) = z_1P_k(adz_1, bz_1 - cx_1), \tag{3.16}$$

with x_1, y, z_1 satisfying (3.9) and (3.10). Observe that for each solution (x_1, y, z_1) counted by $T(d; a, b, c)$, the equation (3.16) implies that $x_1|z_1P_k(adz_1, bz_1)$. Furthermore, since $a \ne 0$ we have $P_k(ad, b) \ne 0$. Then it follows from (3.10) that $x_1|P_k(ad, b)$, so that by using standard estimates for the divisor function, there are at most $O_{\varepsilon,k}(Q^\varepsilon)$ possible choices for x_1. Fix any one such choice. Then the equation (3.16) takes the shape $p(z_1) = q(y)$, where $p(z_1)$ is a polynomial of degree k, and $q(y)$ is a polynomial of degree $k - 1$. Then Corollary 2.3.1 implies that the number of possible choices for y and z_1 is $O_{\varepsilon,k}(Q^{1/k+\varepsilon})$. Thus

$$T(d; a, b, c) \ll_{\varepsilon,k} Q^{1/k+2\varepsilon},$$

and hence, by (3.15),

$$S_1(d) \ll_{\varepsilon,k} d^{-1}Q^{\frac{3}{2}+\frac{1}{k}+2\varepsilon}. \tag{3.17}$$

Next we estimate $S_2(d)$. For each fixed choice of x_1 and z_1, we may solve the equation (3.8) for y and w. On recalling (3.7), the equation (3.8) implies that

$$(a_1y + b_1)^k - (a_1y - b_1)^k = (a_2w + b_2)^k - (a_2w - b_2)^k, \tag{3.18}$$

where $a_1 = a_2 = 1$, $b_1 = dx_1$ and $b_2 = dz_1$. Then by Corollary 2.4.1, the number of possible choices for y and w satisfying (3.10) and (3.11) is $O_{\varepsilon,k}(Q^{1/(k-1)+\varepsilon})$. Consequently,

$$S_2(d) \ll_{\varepsilon,k} \sum_{1\le x_1\le (3Q)^{1/2}} \sum_{1\le z_1\le Q/d} Q^{1/(k-1)+\varepsilon} \ll_{\varepsilon,k} d^{-1}Q^{\frac{3}{2}+\frac{1}{k-1}+\varepsilon}. \qquad (3.19)$$

By (3.13), (3.17) and (3.19), we finally obtain

$$M_k^*(Q) \ll_{\varepsilon,k} \sum_{1\le d\le Q} d^{-1}Q^{\frac{3}{2}+\frac{1}{k-1}+\varepsilon} \ll_{\varepsilon,k} Q^{\frac{3}{2}+\frac{1}{k-1}+2\varepsilon},$$

which establishes the lemma when $k \neq 3, 5$.

When $k = 3$ we proceed as in the above argument, save for the treatment of S_2. In this case the equation (3.18) becomes

$$3a_1^2b_1y^2 + b_1^3 = 3a_2^2b_2w^2 + b_2^3. \qquad (3.20)$$

Then provided that $b_1 \neq b_2$, standard estimates (see, for example, [16, Lemma 3.5]) show that the number of possible choices for y and w is $O_{\varepsilon,k}(Q^\varepsilon)$. Meanwhile, if $b_1 = b_2$, then (3.20) implies that $a_1y = a_2w$, whence $a_1y + b_1 = a_2w + b_2$, which contradicts (3.11). We therefore deduce that when $k = 3$,

$$S_2(d) \ll_{\varepsilon,k} d^{-1}Q^{3/2+\varepsilon},$$

and the desired refinement follows immediately. The case $k = 5$ may be disposed of similarly once we observe that in this case the equation (3.18) becomes

$$5b_1Y^2 - 4b_1^5 = 5b_2W^2 - 4b_2^5,$$

where $Y = a_1^2y^2 + b_1^2$ and $W = a_2^2w^2 + b_2^2$. This completes the proof of the lemma.

When k is even, our argument is necessarily a little more elaborate, since the equation analogous to (3.6) involves two linear factors on each side of the equation. We feel that there are sufficiently many differences to warrant a complete exposition.

Lemma 3.2. *Let k be an even integer with $k \ge 4$. Then*

$$M_k^*(Q) \ll_{\varepsilon,k} Q^{\frac{3}{2}+\frac{1}{k-1}+\varepsilon}.$$

Proof. For each solution x, y, z, w of (3.4) counted by $M_k^*(Q)$, we have

$$xyU_k(x, y) = zwU_k(z, w), \qquad (3.21)$$

where we write

$$U_k(s, t) = \sum_{0\le r<k/2} \binom{k}{2r+1} s^{2r}t^{k-2r-2}. \qquad (3.22)$$

We note for future reference that for real values of s and t, the polynomial $U_k(s,t)$ is zero if and only if $s=t=0$. We write $d=(x,z)$ and $e=(x/d,w)$, and put $x_1=x/(de)$, $z_1=z/d$ and $w_1=w/e$. Then $(x_1,z_1w_1)=1$. On substituting into (3.21), we obtain

$$x_1yU_k(dex_1,y)=z_1w_1U_k(dz_1,ew_1). \tag{3.23}$$

Let $T_1(d,e)$ denote the number of solutions (x_1,y,z_1,w_1) of the equation (3.23) with

$$(3Q)^{1/2}\max\{d^{-1},e^{-1}\}<x_1\le Q/(de), \tag{3.24}$$

$$1\le y\le Q, \tag{3.25}$$

$$1\le z_1\le Q/d, \quad (x_1,z_1)=1, \tag{3.26}$$

$$1\le w_1\le Q/e, \quad (x_1,w_1)=1, \tag{3.27}$$

and

$$dex_1+y\ne dz_1+ew_1. \tag{3.28}$$

Also, let $T_2(d,e)$ denote the corresponding number of solutions with the condition (3.24) replaced by

$$1\le x_1\le (3Q)^{1/2}\max\{d^{-1},e^{-1}\}. \tag{3.29}$$

Then it follows from the preceding paragraph that

$$M_k^*(Q)\le \sum_{1\le d\le Q}\sum_{1\le e\le Q/d}\left(T_1(d,e)+T_2(d,e)\right). \tag{3.30}$$

We first estimate T_1. By Lemma 2.1, for each x_1, z_1, w_1 satisfying (3.24), (3.26) and (3.27), there exist integers a, b, c with $(a,b,c)=1$,

$$0\le |a|\le d^{-1}(3Q)^{1/2},\quad 0\le |b|\le e^{-1}(3Q)^{1/2},\quad 0\le |c|\le (3Q)^{1/2},$$

and satisfying the equation

$$aw_1+bz_1=cx_1. \tag{3.31}$$

We note that both a and b are non-zero. For suppose that $a=0$. Then we have $bz_1=cx_1$ with $(x_1,z_1)=(b,c)=1$, whence $|x_1|=|b|\le e^{-1}(3Q)^{1/2}$, contradicting (3.24). Similarly, if $b=0$ then necessarily $|x_1|=|a|\le d^{-1}(3Q)^{1/2}$, contradicting (3.24). Thus we may assume that neither a nor b are zero. We substitute from (3.31) for w_1 into (3.23) to deduce that

$$T_1(d,e)\le \sum_{0<|a|\le d^{-1}(3Q)^{1/2}}\ \sum_{0<|b|\le e^{-1}(3Q)^{1/2}}\ \sum_{0\le c\le (3Q)^{1/2}} U(d,e;a,b,c), \tag{3.32}$$

where $U(d,e;a,b,c)$ denotes the number of solutions of the equation

$$a^{k-1}x_1yU_k(dex_1,y)=z_1(cx_1-bz_1)U_k(adz_1,e(cx_1-bz_1)), \tag{3.33}$$

with x_1, y, z_1 satisfying (3.24), (3.25) and (3.26). Observe that for each solution (x_1, y, z_1) counted by $U(d, e; a, b, c)$, the equation (3.33) implies that

$$x_1 | bz_1^2 U_k(adz_1, -bez_1).$$

Furthermore, since neither a nor b are zero, we have $bU_k(ad, -be) \neq 0$. Then it follows from (3.26) that $x_1 | bU_k(ad, -be)$, so that by using standard estimates for the divisor function, there are at most $O_{\varepsilon,k}(Q^{\varepsilon})$ possible choices for x_1. Fixing any one such choice, the equation (3.33) takes the shape $p(z_1) = q(y)$, where $p(z_1)$ has degree k and $q(y)$ has degree $k-1$. Then Corollary 2.3.1 implies that the number of possible choices for y and z_1 is $O_{\varepsilon,k}(Q^{1/k+\varepsilon})$. Thus

$$U(d, e; a, b, c) \ll_{\varepsilon,k} Q^{1/k+2\varepsilon},$$

and hence, by (3.32),

$$T_1(d, e) \ll_{\varepsilon,k} (de)^{-1} Q^{\frac{3}{2}+\frac{1}{k}+2\varepsilon}. \tag{3.34}$$

Next we estimate $T_2(d, e)$. Let $V_1(d, e)$ denote the number of solutions x_1, y, z_1, w_1 counted by $T_2(d, e)$ with $x_1 \leq d^{-1}(3Q)^{1/2}$, and let $V_2(d, e)$ denote the corresponding number of solutions with $x_1 \leq e^{-1}(3Q)^{1/2}$. Then in view of (3.29), we have

$$T_2(d, e) \leq V_1(d, e) + V_2(d, e). \tag{3.35}$$

First we bound $V_1(d, e)$. For each fixed choice of x_1 and w_1, we solve the equation (3.23) for y and z_1. On recalling (3.22) (noting that k is even), the equation (3.23) implies that

$$(a_1 y + b_1)^k - (a_1 y - b_1)^k = (a_2 z_1 + b_2)^k - (a_2 z_1 - b_2)^k,$$

where $a_1 = 1$, $b_1 = dex_1$, $a_2 = d$ and $b_2 = ew_1$. Then by Corollary 2.4.1, the number of possible choices for y and z_1 satisfying (3.25), (3.26) and (3.28) is $O_{\varepsilon,k}\left(Q^{1/(k-1)+\varepsilon}\right)$. Consequently,

$$V_1(d, e) \ll_{\varepsilon,k} \sum_{1 \leq x_1 \leq d^{-1}(3Q)^{1/2}} \sum_{1 \leq w_1 \leq Q/e} Q^{1/(k-1)+\varepsilon} \ll_{\varepsilon,k} (de)^{-1} Q^{\frac{3}{2}+\frac{1}{k-1}+\varepsilon}.$$

A similar argument bounds $V_2(d, e)$ in like manner, on interchanging the rôles of d and e, and w_1 and z_1. Thus, by (3.30), (3.34) and (3.35), we have

$$M_k^*(Q) \ll_{\varepsilon,k} \sum_{1 \leq d \leq Q} \sum_{1 \leq e \leq Q/d} (de)^{-1} Q^{\frac{3}{2}+\frac{1}{k-1}+\varepsilon} \ll_{\varepsilon,k} Q^{\frac{3}{2}+\frac{1}{k-1}+2\varepsilon}.$$

This completes the proof of the lemma.

References

1. A. Baker, *Transcendental number theory. Second edition*, Cambridge University Press, Cambridge, 1990.
2. K. D. Boklan, *The asymptotic formula in Waring's problem*, Mathematika **41** (1994), 329–347.
3. E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. **59** (1989), 337–357.
4. G. Greaves, *On the representation of a number as a sum of two fourth powers*, Math. Z. **94** (1966), 223–234.
5. G. Greaves, *On the representation of a number as a sum of two fourth powers. II (Russian)*, Mat. Zametki **55** (1994), 47–58.
6. G. Greaves, *Some diophantine equations with almost all solutions trivial*, Mathematika (to appear).
7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers, fifth edition, fourth reprint*, Clarendon Press, Oxford, 1989.
8. C. Hooley, *On the representation of a number as a sum of two cubes*, Math. Z. **82** (1963), 259–266.
9. C. Hooley, *On the representation of a number as a sum of two hth powers*, Math. Z. **84** (1964), 126–136.
10. C. Hooley, *On the numbers that are representable as the sum of two cubes*, J. Reine Angew. Math. **314** (1980), 146–173.
11. 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.
12. W. M. Schmidt, *Equations over finite fields. An elementary approach. Lecture Notes in Mathematics, Vol. 536*, Springer-Verlag, Berlin-New York, 1976.
13. W. M. Schmidt, *Diophantine approximations and diophantine equations. Lecture Notes in Mathematics, Vol. 1467*, Springer-Verlag, Berlin-New York, 1991.
14. R. C. Vaughan, *On Waring's problem for cubes*, J. Reine Angew. Math. **365** (1986), 122–170.
15. R. C. Vaughan, *On Waring's problem for smaller exponents. II*, Mathematika **33** (1986), 6–22.
16. R. C. Vaughan and T. D. Wooley, *Further improvements in Waring's problem*, Acta Math. (to appear).
17. T. D. Wooley, *Quasi-diagonal behaviour in certain mean value theorems of additive number theory*, J. Amer. Math. Soc. **7** (1994), 221–245.

CMS: Department of Mathematics, Princeton University, Princeton, New Jersey 08544

E-mail address: `cmcls@phoenix.princeton.edu`

TDW: Mathematics Department, University of Michigan, Ann Arbor, Michigan, 48109-1003

E-mail address: `wooley@math.lsa.umich.edu`