THE REPRESENTATION OF INTEGERS BY BINARY ADDITIVE FORMS

M. A. Bennett[1], N. P. Dummigan and T. D. Wooley[2]

Abstract. Let a, b and n be integers with $n \geq 3$. We show that, in the sense of natural density, almost all integers represented by the binary form $ax^n - by^n$ are thus represented essentially uniquely. By exploiting this conclusion, we derive an asymptotic formula for the total number of integers represented by such a form. These conclusions augment earlier work of Hooley concerning binary cubic and quartic forms, and generalise or sharpen work of Hooley, Greaves, and Skinner and Wooley concerning sums and differences of two nth powers.

1. Introduction

The problem of determining which integers are represented by a given binary form, and the number of such representations, is one with a long and distinguished history extending back beyond the seminal work of Gauss concerning quadratic forms. In 1909, Thue [23] proved that when $F(x, y) \in \mathbb{Z}[x, y]$ is a binary form of degree $k \geq 3$, and F is irreducible over $\mathbb{Q}$, then there are only finitely many integral solutions to the equation $F(x, y) = n$. Evertse [6], and Bombieri and Schmidt [2], have sharpened this conclusion, and thus the latter number of solutions is now known to be $O(k^{1+\omega(n)})$, where $\omega(n)$ denotes the number of distinct prime divisors of n (see [22] for later developments). When the degree of F is large, and n is not too small in terms of F, it is conjectured that whenever n is represented in the form $n = F(x, y)$, with $x, y \in \mathbb{Z}$, then this representation is essentially unique, in the sense that all primitive representations of n are generated from a single solution by the group of automorphisms of F. Such numerical evidence as is available supports this conjecture. Moreover Hooley [11] has shewn that in the sense of natural density, almost all integers represented by an irreducible binary cubic form are thus represented essentially uniquely, with a similar conclusion [14] holding for a class of quartic forms. With the exception of the examples provided by sums of two kth powers (see [13, 21]), no such conclusion has hitherto been available for binary forms of higher degree. Our purpose in the present paper is to establish this conclusion for binary additive forms, which is to say, forms of the shape $ax^k - by^k$, thereby lending credibility to the aforementioned conjecture, and augmenting the extensive body of literature on such forms (see, in particular, [1, 7, 16, 17, 19, 20]).

In order to describe our main conclusions we require some notation. When k is a positive integer, and α and β are non-zero integers, let $F_{\alpha\beta} = F_{\alpha\beta}(x, y)$ denote the binary additive form $F_{\alpha\beta}(x, y) = \alpha x^k - \beta y^k$. Denote by $\mathcal{A}_{\alpha\beta}$ the group of automorphisms of the form $F_{\alpha\beta}$ lying in $SL_2(\mathbb{Z})$, and write $A(\alpha, \beta)$ for the cardinality of $\mathcal{A}_{\alpha\beta}$. We say that $F_{\alpha\beta}$ represents the integer n *essentially uniquely* if there exist integers x and y with $F_{\alpha\beta}(x, y) = n$ such that if u and v are integers with $F_{\alpha\beta}(u, v) = n$, then (u, v) is generated from (x, y) by the action of $\mathcal{A}_{\alpha\beta}$. Finally, when X is a positive real number, let $\mu_k(X; \alpha, \beta)$ denote the number of integers with absolute value not exceeding X that are represented by $F_{\alpha\beta}$, but are not represented essentially uniquely.

Theorem 1. *Let k be an integer exceeding 4, and let α and β be non-zero integers. Then for each positive number X,*

$$\mu_k(X; \alpha, \beta) \ll X^{\frac{3}{2k} + \eta_k + \varepsilon},$$

1991 *Mathematics Subject Classification.* 11D41, 11P05, 11D85.

Key words and phrases. Binary forms, representation problems, higher degree equations, Diophantine approximation, Waring's problem and variants.

[1]Supported in part through the David and Lucile Packard Foundation, and by a Rackham Faculty Fellowship at the University of Michigan

[2]Packard Fellow and supported in part by NSF grant DMS-9622773

where the implicit constant depends at most on k, ε, α, β, and where

$$\eta_k = \frac{7k-9}{2k(2k^2-3k+3)}.$$

Moreover when $k = 5$, the exponent η_k may be replaced by $29/470$.

For comparison, the aforementioned work of Hooley [11, 14] shows that

$$\mu_3(X;\alpha,\beta) \ll \frac{X^{2/3}}{(\log\log X)^{1/600}}, \quad \text{and} \quad \mu_4(X;\alpha,\beta) \ll_\varepsilon X^{\frac{18}{37}+\varepsilon}, \tag{1.1}$$

where the implicit constants may depend on α and β. Hooley [14] shews, in fact, that when α and β have opposite signs, then the exponent $18/37$ in the latter estimate may be replaced by $9/19$.

When $F(x,y) \in \mathbb{Z}[x,y]$ is a binary form of degree $k \geq 3$, Mahler [15] has shown that the number, $N_F(m)$, of integral solutions of the inequality $|F(x,y)| \leq m$ satisfies

$$N_F(m) = \Delta_F m^{2/k} + O_{k,F}(m^{1/(k-1)}), \tag{1.2}$$

where Δ_F denotes the area of the set $\big\{(\xi,\eta) \in \mathbb{R}^2 : |F(\xi,\eta)| \leq 1\big\}$. Theorem 1, on the other hand, shows that when the form F is additive, the number of integers with absolute value not exceeding X, which are represented by F in more than one essentially distinct way, is $o(X^{2/k})$. Consequently, in the sense of natural density, almost all integers represented by F are thus represented essentially uniquely. This observation contrasts sharply with the corresponding situation for binary quadratic forms, where it is well known that most integers which are represented have many representations. A more concrete formulation of these deliberations is provided by the following immediate corollary of Theorem 1 and the asymptotic formula (1.2).

Corollary. *Suppose that the hypotheses of the statement of Theorem 1 hold. Let $S(X;\alpha,\beta)$ denote the number of integers, with absolute value not exceeding X, which are represented by the binary form $\alpha x^k - \beta y^k$. Also, let $\Delta(\alpha,\beta)$ denote the area of the set $\big\{(\xi,\eta) \in \mathbb{R}^2 : |\alpha\xi^k - \beta\eta^k| \leq 1\big\}$. Then*

$$S(X;\alpha,\beta) = \frac{\Delta(\alpha,\beta)}{A(\alpha,\beta)} X^{2/k} + O\left(X^{\frac{3}{2k}+\eta_k+\varepsilon}\right), \tag{1.3}$$

where the implicit constant depends at most on $k, \varepsilon, \alpha, \beta$.

By employing Hooley's estimates (1.1), a similar conclusion can also be inferred for binary additive forms of degree 3 and 4. We note that in this additive situation, the conclusion (1.3) provides a significant sharpening of a theorem of Erdős and Mahler [4] to the effect that $S(X;\alpha,\beta) \gg X^{2/k}$. Perhaps it is opportune, before leaving this topic, to characterise the possible automorphism groups for binary additive forms. It plainly suffices to consider forms $\alpha x^k - \beta y^k$ with α and β restricted to be k-free integers (so that neither is divisible by any kth power of a prime number). One may easily verify that the following are the only possible automorphisms: (i) when k is even, the maps $(x,y) \to \pm(x,\pm y)$; (ii) when $\alpha = -\beta$, the map $(x,y) \to (y,x)$; (iii) when $\alpha = \beta$ and k is odd, the map $(x,y) \to (-y,-x)$. Consequently $A(\alpha,\beta)$ is characterised as follows.

$$A(\alpha,\beta) = \begin{cases} 1, & \text{when } k \text{ is odd and } \alpha \neq \pm\beta, \\ 2, & \text{when } k \text{ is odd and } \alpha = \pm\beta, \\ 4, & \text{when } k \text{ is even and } \alpha \neq -\beta, \\ 8, & \text{when } k \text{ is even and } \alpha = -\beta. \end{cases}$$

In circumstances where $\alpha = \pm\beta$, the investigation of integers represented by the form $\alpha x^k - \beta y^k$ simplifies to the study of sums and differences of two kth powers. In this situation a modification of the argument used to establish Theorem 1 yields a somewhat sharper conclusion. Write, for the sake of concision, $\nu_k^{\pm}(X)$ for $\mu_k(X;1,\pm 1)$.

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

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

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

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

For comparison, Hooley [12] has shewn that $\nu_3^{\pm}(X) \ll_{\varepsilon} X^{5/9+\varepsilon}$, and has also established (in [13]) that when $k \geq 5$ is odd one has $\nu_k^{\pm}(X) \ll X^{5/(3k-1)+\varepsilon}$. Also, when $k \geq 4$ is even the estimate provided by Theorem 2 for $\nu_k^{-}(X)$ is identical with that provided by Skinner and Wooley [21, Theorem 1.1] (see Greaves [9, 10] when $k = 4$). However, Theorem 2 provides bounds for $\nu_k^{+}(X)$ which are new and non-trivial for all even k with $k \geq 6$, and provides bounds superior to those of Hooley [13, 14] when $k = 4$, and when $k \geq 5$ is odd.

Our proofs of Theorems 1 and 2 depend on a bound for the number of solutions of a certain auxiliary equation. We establish this estimate in §4, following the trail laid down in [21] for a simpler situation in which less precision was required. It transpires that our argument employs a slicing procedure which entails counting the number of points on certain affine plane curves. We bound the latter number by appealing to an estimate of Bombieri and Pila [3], the successful application of which requires us to establish a criterion for the absolute irreducibility of the polynomial $f(x, y) = f(x, y; \alpha, \beta, b_1, b_2)$, defined by

$$f(x, y) = \alpha((x + b_1)^k - (x - b_1)^k) - \beta((y + b_2)^k - (y - b_2)^k). \tag{1.4}$$

In Theorem 2.2 we completely classify the situations in which the polynomial $f(x, y)$ is, or is not, absolutely irreducible. Having obtained our absolute irreducibility criterion in §2, and recorded further technical preliminaries in §3, we are able in §4 to establish the desired auxiliary estimates. The proofs of Theorems 1 and 2, in §§6 and 5 respectively, are fairly immediate consequences of the estimates provided in §4, the proof of Theorem 1 entailing the application of Roth's theorem to bound the domains of the variables.

In the remainder of this paper, constants implied by the Vinogradov symbols $\ll$ and $\gg$, and those relating to Landau's notation, unless otherwise stated, depend at most on a positive number ε and upon the degree of a given binary form.

The authors are grateful to the referee for useful comments.

2. An Absolute Irreducibility Criterion

In this section we investigate the absolute irreducibility of the polynomial $f(x, y)$ defined in (1.4). Our strategy is to show that if this polynomial is reducible over $\mathbb{C}[x, y]$, then the corresponding curve must possess many singular points. Meanwhile, by exploiting the arithmetic of the number fields defined by the latter singular points, one finds that $f(x, y)$ has few singular points unless $\alpha = \pm\beta$ and $b_1 = \pm b_2$. But in the latter circumstance $f(x, y)$ is plainly reducible over $\mathbb{Q}[x, y]$. We start our investigations in $\mathbb{C}$.

Lemma 2.1. *Let α, β, b_1 and b_2 be non-zero complex numbers, let k be an integer exceeding 2, and let $f(x, y) = f(x, y; \alpha, \beta, b_1, b_2)$ be the polynomial defined in (1.4). Then the projective closure, $\mathcal{C}$, of the affine plane curve over $\mathbb{C}$ defined by the equation $f(x, y) = 0$, has the following properties.*

(i) The points at infinity on $\mathcal{C}$ are non-singular.

(ii) If $f(x, y)$ factors non-trivially over $\mathbb{C}$ as $f = f_1 f_2$, and if $\mathcal{C}_1$ and $\mathcal{C}_2$ are the projective closures of the curves defined by $f_1 = 0$ and $f_2 = 0$ respectively, then all the intersection points of $\mathcal{C}_1$ and $\mathcal{C}_2$ have intersection multiplicity one.

(iii) If $f(x, y)$ is reducible over $\mathbb{C}$ then $\mathcal{C}$ possesses at least $k - 2$ distinct singular points over $\mathbb{C}$.

Proof. (i) The homogenization of $f(x, y)$ has the shape

$$h(x, y, z) = 2b_1\alpha x^{k-1} - 2b_2\beta y^{k-1} + z^2 g(x, y, z),$$

where $g(x, y, z)$ is a homogeneous polynomial of degree $k - 3$. At infinity one has $z = 0$, and thus if the first partial derivatives vanish, then necessarily $x = y = 0$. But $x = y = z = 0$ does not define a

point in the projective plane, whence there are no singular points on $\mathcal{C}$ at infinity. Part (i) of the lemma follows immediately.

(ii) By hypothesis f splits non-trivially over $\mathbb{C}$ as $f = f_1 f_2$, and $\mathcal{C}_1$ and $\mathcal{C}_2$ are the respective projective closures of the curves defined by $f_1 = 0$ and $f_2 = 0$. Suppose that $\mathcal{C}_1$ and $\mathcal{C}_2$ intersect at a point P. Then necessarily P is a singular point of $\mathcal{C}$, whence from (i) one has that P is a finite point. If $\mathcal{C}_1$ and $\mathcal{C}_2$ have intersection multiplicity exceeding one at P, then without loss of generality one has

$$\left(\frac{\partial f_1}{\partial x}, \frac{\partial f_1}{\partial y}\right) = \lambda \left(\frac{\partial f_2}{\partial x}, \frac{\partial f_2}{\partial y}\right) \tag{2.1}$$

at P. Note that the equation (2.1) covers the case where P is a singular point of $\mathcal{C}_1$, in which case one has $\lambda = 0$. Consequently, on making use of the fact that $f_1 = f_2 = 0$ at P,

$$\frac{\partial^2 f}{\partial x^2} = 2\lambda \left(\frac{\partial f_2}{\partial x}\right)^2, \quad \frac{\partial^2 f}{\partial y^2} = 2\lambda \left(\frac{\partial f_2}{\partial y}\right)^2 \quad \text{and} \quad \frac{\partial^2 f}{\partial x \partial y} = 2\lambda \left(\frac{\partial f_2}{\partial x}\right)\left(\frac{\partial f_2}{\partial y}\right).$$

But in view of (1.4) the polynomial $\partial^2 f/\partial x \partial y$ is identically zero, and hence at least one of $\partial^2 f/\partial x^2$ and $\partial^2 f/\partial y^2$ vanishes at P. Moreover, because P is a singular point of $\mathcal{C}$, one also has $\partial f/\partial x = \partial f/\partial y = 0$ at P, and thus a simple calculation reveals that at least one of b_1 and b_2 is zero, contrary to our assumptions. It follows that whenever $\mathcal{C}_1$ and $\mathcal{C}_2$ intersect, they do so with multiplicity one, and this completes the proof of part (ii) of the lemma.

(iii) Suppose that $f(x, y)$ is reducible over $\mathbb{C}$, so that it splits non-trivially, let us say as $f = f_1 f_2$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ denote the projective closures of the curves defined by $f_1 = 0$ and $f_2 = 0$, respectively. Since the product of the degrees of f_1 and f_2 is at least as large as $\deg f - 1$, which is $k - 2$, we find from Bezout's theorem that $\mathcal{C}_1$ and $\mathcal{C}_2$ intersect in at least $k-2$ points in the complex projective plane, when counted according to multiplicity. But by (i), none of these points is at infinity, and by (ii), the intersection multiplicity at each of these points is one. Thus there are at least $k-2$ distinct intersection points, and all of these points are singular points of $\mathcal{C}$. This completes the proof of part (iii) of the lemma.

Theorem 2.2. *Let k be an integer exceeding 2, let b_1 and b_2 be non-zero integers, and suppose that α and β are non-zero k-free integers. If $\alpha = \pm\beta$ and $b_1 = \pm b_2$, then the polynomial f defined by (1.4) is reducible in $\mathbb{Q}[x, y]$, and otherwise f is absolutely irreducible in $\mathbb{C}[x, y]$.*

Proof. If f is not absolutely irreducible then by Lemma 2.1 there exist at least $k - 2$ distinct singular points $P = (x, y)$ on the affine curve defined by $f(x, y) = 0$. Since

$$\partial f/\partial x = \alpha k((x + b_1)^{k-1} - (x - b_1)^{k-1})$$

and

$$\partial f/\partial y = -\beta k((y + b_2)^{k-1} - (y - b_2)^{k-1}),$$

it follows that at a singular point P we have

$$x + b_1 = \omega_1(x - b_1) \quad \text{and} \quad y + b_2 = \omega_2(y - b_2), \tag{2.2}$$

where ω_1 and ω_2 are $(k-1)th$ roots of unity, not necessarily distinct. Notice that since the b_i are non-zero, one has $\omega_i \neq 1$ $(i = 1, 2)$. Thus, on solving for x and y and substituting into the equation $f(x, y) = 0$, we obtain the relation

$$\frac{\alpha}{\beta}\left(\frac{b_1}{b_2}\right)^k = \left(\frac{1 - \omega_1}{1 - \omega_2}\right)^{k-1}. \tag{2.3}$$

Moreover, in view of (2.2), the values ω_1 and ω_2 uniquely determine x and y, and hence the equation (2.3) must hold for at least $k - 2$ distinct pairs (ω_1, ω_2) of non-trivial $(k-1)$th roots of unity.

Suppose next that ω_1 and ω_2 satisfy (2.3), and let r_1 and r_2 be the exact multiplicative orders of ω_1 and ω_2 respectively. Necessarily each of r_1 and r_2 divides $k - 1$. When $m > 1$, let ζ_m denote a primitive mth root of unity. It is well-known (see for example, [8, Theorem 45]) that if m is divisible by at least two distinct primes, then $1 - \zeta_m$ is a unit. If $1 - \omega_1$ and $1 - \omega_2$ are both units then the

right hand side of (2.3) is a unit. But then, since the left hand side of (2.3) is rational, we must have $(\alpha/\beta)(b_1/b_2)^k = \pm 1$. Our hypotheses concerning α and β therefore lead to the conclusion that $\alpha = \pm\beta$ and $b_1 = \pm b_2$, in which case f is plainly reducible in $\mathbb{Q}[x, y]$. Henceforth, therefore, we may suppose without loss of generality that α and β are coprime, and that $r_1 = p^r$, a prime power. We can also assume that $r_2 \neq r_1$, since otherwise the right hand side of (2.3) again becomes a unit.

Our strategy is now to show that there are fewer than $k-2$ singular points by considering the possibilities for r_1 and r_2. If such can be established, then in view of Lemma 2.1 it follows that f is absolutely irreducible, and the proof of Theorem 2.2 will be complete.

Case 1. Suppose that $r_2 = p^s$ and, without loss of generality, $r < s$. The prime p is totally ramified in the cyclotomic field $\mathbb{Q}(\omega_2)$. Let $\mathfrak{p}$ be the prime ideal dividing (p) in the latter field, and let $d = \mathrm{ord}_p((\alpha/\beta)(b_1/b_2)^k)$. We know that $\mathrm{ord}_{\mathfrak{p}}(1-\omega_2) = 1$ and $\mathrm{ord}_{\mathfrak{p}}(1-\omega_1) = p^{s-r}$ (see [8, Theorem 45]). Using the fact $\mathrm{ord}_{\mathfrak{p}}(p) = [\mathbb{Q}(\omega_2) : \mathbb{Q}] = \phi(p^s)$, and equating orders at $\mathfrak{p}$ in (2.3), we find that

$$dp^{s-1}(p-1) = (p^{s-r}-1)(k-1).$$

It follows that the power of p dividing dp^{s-1} must be the same as that dividing $k-1$, and so this uniquely determines s, and thus r as well. Also, p is uniquely determined as the only prime dividing α or β, since $\mathfrak{p}$ is the only prime ideal of $\mathbb{Q}(\omega_2)$ occurring in the factorisation of the right hand side of (2.3).

If $r_2 = 4$ and $r_1 = 2$ then there are only two possible choices for (ω_1, ω_2), and this is insufficient, since there must be at least $k-2$, and $k-1$ is divisible by $r_2 = 4$. Therefore we may suppose that $r_2 > 4$. But then there is an automorphism of $\mathbb{Q}(\omega_2)/\mathbb{Q}$ which fixes ω_1 but does not fix ω_2 or send it to its complex conjugate. This automorphism fixes the left hand side of (2.3) but changes the absolute value of the right hand side. This again is impossible.

Case 2. Suppose now that r_2 is a power of some prime different from p, or is divisible by at least two distinct primes. Then $1-\omega_2$ is either a unit or does not divide p in any cyclotomic field. It follows that r is uniquely determined by the equation $dp^{r-1}(p-1) = k-1$. For each of the $\phi(p^r)$ possible choices of ω_1, there are at most two (complex conjugate) possibilities for ω_2, for otherwise the absolute value of the right hand side of (2.3) changes. Hence there are at most $2\phi(p^r) < 2p^r - 1$ choices for (ω_1, ω_2). Since both r_1 and r_2 must divide $k-1$, we deduce that there are fewer than $k-2$ choices for (ω_1, ω_2), and once more this provides a contradiction.

3. Preliminary Lemmata

Before advancing to the main body of our argument, we pause in order to record several preliminary lemmata.

Lemma 3.1. *For $i = 1, 2, 3$, suppose that Q_i is a positive number, and that x_i is an integer with $1 \leq x_i \leq Q_i$. Then the equation $a_1x_1 + a_2x_2 + a_3x_3 = 0$ is soluble in integers a_1, a_2, a_3 with $(a_1, a_2, a_3) = 1$ and*

$$|a_i| \leq Q_i^{-1}\,(3Q_1Q_2Q_3)^{1/2} \quad (1 \leq i \leq 3).$$

Proof. This is the case $s = 3$ of [21, Lemma 2.1].

Lemma 3.2. *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 $0 \leq x, y \leq X$, satisfies $N(X; p, q) \ll X^{1/k+\varepsilon}$.*

Proof. This is [21, Corollary 2.3.1].

Lemma 3.3. *Let k be an integer exceeding 2, let a_1, a_2, b_1 and b_2 be fixed positive integers, and suppose that α and β are non-zero k-free integers. Let $f(x, y) = f(x, y; \alpha, \beta, b_1, b_2)$ be the polynomial defined in (1.4). Also, let $M(X)$ denote the number of solutions of the Diophantine equation $f(a_1u, a_2v) = 0$ with $1 \leq u, v \leq X$, subject, in the cases in which $\alpha = \pm\beta$, to the additional condition $a_1u + b_1 \neq a_2v + b_2$. Then $M(X) \ll X^{1/(k-1)+\varepsilon}$.*

Proof. Suppose either that $\alpha \neq \pm\beta$, or else that $\alpha = \pm\beta$ but $b_1 \neq \pm b_2$. Then by Theorem 2.2 the polynomial $f(u, v)$ is absolutely irreducible of degree $k-1$. Thus Bombieri and Pila [3, Theorem 5] implies that in this case $M(X) \ll X^{1/(k-1)+\varepsilon}$. Meanwhile, if $\alpha = \pm\beta$ and $b_1 = \pm b_2$, then any solution u, v counted by $M(X)$ satisfies the equation $g(a_1u; b_1) = \pm g(a_2v; \pm b_1)$, 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 solutions to the latter equation must satisfy $a_1u = \pm a_2v$. Consequently, in this second case, there are no solutions counted by $M(X)$ with $a_1u + b_1 \neq a_2v + b_2$. This completes the proof of the lemma.

Notice that in the conclusions of Lemmata 3.2 and 3.3, the implicit constants depend at most on k and ε, but are independent of the coefficients of the polynomials defining the respective equations.

4. An Auxiliary Equation

It transpires that our arguments in §§5 and 6 below depend for their success on certain estimates for the number of solutions of the Diophantine equation

$$\alpha u_1^k - \beta v_1^k = \alpha u_2^k - \beta v_2^k, \tag{4.1}$$

with variables restricted to a suitable region. By defining new variables x, y, z, w by

$$x = u_1 - u_2, \quad y = u_1 + u_2, \quad z = v_1 - v_2, \quad w = v_1 + v_2, \tag{4.2}$$

the equation (4.1) may be brought into the shape

$$\alpha \Upsilon_k(x, y) = \beta \Upsilon_k(z, w), \tag{4.3}$$

where the polynomial $\Upsilon_k(s,t)$ is defined by

$$\Upsilon_k(s,t) = (t+s)^k - (t-s)^k. \tag{4.4}$$

The object of this section is to obtain estimates for the number, $M_k(\mathbf{Q}, \mathbf{H}) = M_k(\mathbf{Q}, \mathbf{H}; \alpha, \beta)$, of solutions of the equation (4.3) with $1 \leq x \leq H_1$, $1 \leq y \leq Q_1$, $1 \leq z \leq H_2$, $1 \leq w \leq Q_2$, subject, in the cases where $\alpha = \pm\beta$, to the additional condition $x + y \neq z + w$. We divide our argument into two parts, according to the parity of k, following closely the argument of [21, §3].

Lemma 4.1. *Let k be an even integer with $k \geq 4$, and let α and β be non-zero k-free integers. Let H_1, H_2, Q_1, Q_2 be positive numbers, and write*

$$\mathcal{M} = \min\{|\alpha|, |\beta|\} \max\{H_1, H_2, Q_1, Q_2\}.$$

Then

$$M_k(\mathbf{Q}, \mathbf{H}; \alpha, \beta) \ll \mathcal{M}^{\varepsilon} \left(H_1H_2Q_2 + H_1^2\right)^{1/2} (H_2 + Q_1 + Q_2)^{1/(k-1)}.$$

Proof. We begin by noting that by relabelling variables, we may suppose without loss of generality that $|\alpha| \geq |\beta|$. Next, for each solution x, y, z, w of (4.3) counted by $M_k(\mathbf{Q}, \mathbf{H}; \alpha, \beta)$, we have

$$\alpha xy U_k(x, y) = \beta zw U_k(z, w), \tag{4.5}$$

where we write

$$U_k(s,t) = \sum_{0 \leq r < k/2} \binom{k}{2r+1} s^{2r} t^{k-2r-2}. \tag{4.6}$$

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 $s = t = 0$. 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 (4.5), we obtain

$$\alpha x_1 y U_k(dex_1, y) = \beta z_1 w_1 U_k(dz_1, ew_1). \tag{4.7}$$

For ease of handling, let us define

$$\Delta = (3H_1H_2Q_2)^{1/2}, \quad A = \Delta/(dQ_2), \quad B = \Delta/(eH_2), \quad C = \Delta/H_1. \tag{4.8}$$

Let $T_1(d, e)$ denote the number of solutions (x_1, y, z_1, w_1) of equation (4.7) with

$$\max\{A, B\} < x_1 \leq H_1/(de), \tag{4.9}$$

$$1 \le y \le Q_1, \tag{4.10}$$

$$1 \le z_1 \le H_2/d, \quad (x_1, z_1) = 1, \tag{4.11}$$

$$1 \le w_1 \le Q_2/e, \quad (x_1, w_1) = 1, \tag{4.12}$$

and subject, in the cases where $\alpha = \pm\beta$, to the additional condition

$$dex_1 + y \ne dz_1 + ew_1. \tag{4.13}$$

Also, let $T_2(d, e)$ denote the corresponding number of solutions with the condition (4.9) replaced by

$$1 \le x_1 \le \max\{A, B\}. \tag{4.14}$$

Then it follows from the preceding paragraph that

$$M_k(\mathbf{Q}, \mathbf{H}) \le \sum_{1 \le d \le H_1} \sum_{1 \le e \le H_1/d} \left(T_1(d, e) + T_2(d, e)\right). \tag{4.15}$$

We first estimate T_1. By Lemma 3.1, for each x_1, z_1, w_1 satisfying (4.9), (4.11) and (4.12), there exist integers a, b and c, not all zero, with $(a, b, c) = 1$, $0 \le |a| \le A$, $0 \le |b| \le B$, $0 \le |c| \le C$ and satisfying the equation

$$aw_1 + bz_1 = cx_1. \tag{4.16}$$

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 $|x_1| = |b| \le B$, contradicting (4.9). Similarly, if $b = 0$, then necessarily $|x_1| = |a| \le A$, again contradicting (4.9). Thus we may assume that neither a nor b is zero. We substitute from (4.16) for w_1 into (4.7) to deduce that

$$T_1(d, e) \le \sum_{0 < |a| \le A} \sum_{0 < |b| \le B} \sum_{0 \le c \le C} U(d, e; a, b, c), \tag{4.17}$$

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

$$\alpha a^{k-1} x_1 y U_k(dex_1, y) = \beta z_1 (cx_1 - bz_1) U_k(adz_1, e(cx_1 - bz_1)), \tag{4.18}$$

with x_1, y, z_1 satisfying (4.9)-(4.11). Observe that, in view of the coprimality condition $(x_1, z_1) = 1$ of (4.11), for each such solution (x_1, y, z_1) counted by $U(d, e; a, b, c)$ the equation (4.18) implies that x_1 divides $\beta b U_k(ad, -be)$. Furthermore, since neither a nor b is zero, we have $bU_k(ad, -be) \ne 0$. Thus, by using standard estimates for the divisor function, there are at most $O(\mathcal{M}^\varepsilon)$ possible choices for x_1. Fixing any one such choice, the equation (4.18) takes the shape $p(z_1) = q(y)$, where $p(z_1)$ has degree k and $q(y)$ has degree $k - 1$. Then Lemma 3.2 implies that the number of possible choices for y and z_1 is $O\left((H_2 + Q_1)^{1/k+\varepsilon}\right)$. Thus $U(d, e; a, b, c)$ is $O(\mathcal{M}^\varepsilon (H_2 + Q_1)^{1/k})$, and hence by (4.8) and (4.17),

$$T_1(d, e) \ll \mathcal{M}^\varepsilon (de)^{-1} \left(H_1 H_2 Q_2 + H_1^2\right)^{1/2} (H_2 + Q_1)^{1/k}. \tag{4.19}$$

Next we estimate $T_2(d, e)$. Let $V_1(d, e)$ denote the number of the solutions x_1, y, z_1, w_1 counted by $T_2(d, e)$ in which $x_1 \le B$, and let $V_2(d, e)$ denote the corresponding number of solutions with $x_1 \le A$. Then in view of (4.14), we have

$$T_2(d, e) \le V_1(d, e) + V_2(d, e). \tag{4.20}$$

First we bound $V_1(d, e)$. For each fixed choice of x_1 and z_1, we solve the equation (4.7) for y and w_1. On recalling (4.6), equation (4.7) implies that

$$\alpha \left((a_1 y + b_1)^k - (a_1 y - b_1)^k\right) = \beta \left((a_2 w_1 + b_2)^k - (a_2 w_1 - b_2)^k\right), \tag{4.21}$$

where $a_1 = 1$, $b_1 = dex_1$, $a_2 = e$ and $b_2 = dz_1$. Then by Lemma 3.3, the number of possible choices for y and w_1 satisfying (4.10), (4.12) and (4.13) is $O\left((Q_1 + Q_2)^{1/(k-1)+\varepsilon}\right)$. Consequently,

$$V_1(d, e) \ll \sum_{1 \le x_1 \le B} \sum_{1 \le z_1 \le H_2/d} (Q_1 + Q_2)^{1/(k-1)+\varepsilon},$$

whence by (4.8),

$$V_1(d,e) \ll (de)^{-1}(H_1H_2Q_2)^{1/2}(Q_1+Q_2)^{1/(k-1)+\varepsilon}. \tag{4.22}$$

A similar argument bounds $V_2(d,e)$ in like manner, on interchanging the roles of d and e, and w_1 and z_1. In this way we obtain

$$V_2(d,e) \ll \sum_{1\le x_1\le A}\ \sum_{1\le w_1\le Q_2/e} (Q_1+H_2)^{1/(k-1)+\varepsilon},$$

and thus by (4.8),

$$V_2(d,e) \ll (de)^{-1}(H_1H_2Q_2)^{1/2}(Q_1+H_2)^{1/(k-1)+\varepsilon}. \tag{4.23}$$

On recalling (4.15), (4.19) and (4.22), we therefore deduce that

$$M_k(\mathbf{Q},\mathbf{H}) \ll \mathcal{M}^{\varepsilon} \sum_{1\le d\le H_1}\ \sum_{1\le e\le H_1/d} (de)^{-1}\left(H_1H_2Q_2+H_1^2\right)^{1/2}(Q_1+Q_2+H_2)^{\frac{1}{k-1}},$$

and the desired conclusion follows immediately.

Lemma 4.2. *Let k be an odd integer with $k\ge 3$, and let α and β be non-zero k-free integers. Let H_1,H_2,Q_1,Q_2 be positive numbers, and define $\mathcal{M}$ as in the statement of Lemma* 4.1. *Then*

$$M_k(\mathbf{Q},\mathbf{H};\alpha,\beta) \ll \mathcal{M}_k^{\varepsilon}\left(H_1H_2Q_2+H_1^2\right)^{1/2}(Q_1+Q_2+H_2)^{\delta_k},$$

where $\delta_k=1/k$ and $\mathcal{M}_k=|\alpha|\mathcal{M}$ when $k=3,5$, and $\delta_k=1/(k-1)$ and $\mathcal{M}_k=\mathcal{M}$ otherwise.

Proof. As in the proof of Lemma 4.1, we may plainly suppose that $|\alpha|\ge|\beta|$. For each solution x,y,z,w of (4.3) counted by $M_k(\mathbf{Q},\mathbf{H};\alpha,\beta)$, we have

$$\alpha x V_k(x,y) = \beta z V_k(z,w), \tag{4.24}$$

where we write

$$V_k(s,t) = \sum_{0\le r<k/2}\binom{k}{2r+1}s^{2r}t^{k-2r-1}. \tag{4.25}$$

We again note for future reference that for real values of s and t, the polynomial $V_k(s,t)$ is zero if and only if $s=t=0$. Write $d=(x,z)$, and put $x_1=x/d$ and $z_1=z/d$. Thus $(x_1,z_1)=1$. On substituting into (4.24), we obtain

$$\alpha x_1 V_k(dx_1,y) = \beta z_1 V_k(dz_1,w). \tag{4.26}$$

We now estimate $M_k(\mathbf{Q},\mathbf{H};\alpha,\beta)$ using an argument strikingly similar, though simpler, than that used in the proof of Lemma 4.1. In order to curtail our deliberations, we adopt the convention throughout the remainder of the proof of this lemma that $e=1$, $w_1=w$, that the coprimality condition $(x_1,w_1)=1$ is to be ignored, and that occurrences of $\max\{A,B\}$ are to be replaced simply by B. Let $T_1(d)$ denote the number of solutions (x_1,y,z_1,w) of the equation (4.26) satisfying (4.9)-(4.13), and let $T_2(d)$ denote the corresponding number of solutions with the condition (4.9) replaced by (4.14). Then it follows from the above discussion that

$$M_k(\mathbf{Q},\mathbf{H}) \le \sum_{1\le d\le H_1}\left(T_1(d)+T_2(d)\right). \tag{4.27}$$

We first observe that from (4.4) and (4.25) the equation (4.26) implies that (4.21) is satisfied. Thus the argument leading to (4.22) remains valid, and we deduce that

$$\sum_{1\le d\le H_1} T_2(d) \ll \mathcal{M}^{\varepsilon}(H_1H_2Q_2)^{1/2}(Q_1+Q_2)^{1/(k-1)}. \tag{4.28}$$

We estimate $T_1(d)$ when $1\le d\le H_1$ as in the argument used to estimate $T_1(d,e)$ in the proof of Lemma 4.1. Let $U(d;a,b,c)$ denote the number of solutions (x_1,y,z_1,w) of the equation (4.26) satisfying (4.9)-(4.13) and (4.16). Then it follows, as in the argument leading to (4.17), that

$$T_1(d) \le \sum_{0<|a|\le A}\ \sum_{0<|b|\le B}\ \sum_{0\le c\le C} U(d;a,b,c). \tag{4.29}$$

On substituting from (4.16) for w into (4.26), we deduce that $U(d;a,b,c)$ is bounded above by the number of solutions of the equation

$$\alpha a^{k-1}x_1V_k(dx_1,y)=\beta z_1V_k(adz_1,cx_1-bz_1),\tag{4.30}$$

with x_1,y,z_1 satisfying (4.9)-(4.11). Moreover on this occasion one may assume that a is non-zero. Observe that for each solution (x_1,y,z_1) counted by $U(d;a,b,c)$, the equation (4.30) implies that x_1 divides $\beta V_k(ad,-b)$. Furthermore, since a is non-zero, we have $V_k(ad,-b)\neq 0$. Then by again using standard estimates for the divisor function, it follows that there are at most $O(\mathcal{M}^\varepsilon)$ possible choices for x_1. Fixing any one such choice, the equation (4.30) takes the shape $p(z_1)=q(y)$, where $p(z_1)$ has degree k and $q(y)$ has degree $k-1$. Then Lemma 3.2 implies that the number of possible choices for y and z_1 is $O((H_2+Q_1)^{1/k+\varepsilon})$, whence $U(d;a,b,c)$ is $O(\mathcal{M}^\varepsilon(H_2+Q_1)^{1/k})$. Consequently we deduce from (4.29) the bound

$$T_1(d)\ll \mathcal{M}^\varepsilon d^{-1}\left(H_1H_2Q_2+H_1^2\right)^{1/2}(Q_1+Q_2+H_2)^{1/k}.\tag{4.31}$$

On combining (4.27), (4.28) and (4.31), we arrive at the desired conclusion in the cases where $k\geq 7$. When $k=3$, we proceed as in the above argument, save for the treatment of T_2. In this case the equation (4.21) becomes

$$\alpha(3a_1^2b_1y^2+b_1^3)=\beta(3a_2^2b_2w_1^2+b_2^3).$$

Then provided that $\alpha b_1^3\neq\beta b_2^3$, standard estimates (see, for example, Estermann [5]) show that the number of possible choices for y and w_1 is $O(\mathcal{M}_k^\varepsilon)$. Meanwhile, since α and β are cube-free in this case, if $\alpha b_1^3=\beta b_2^3$, then necessarily $\alpha=\pm\beta$ and $b_1=b_2$, whence $a_1y=a_2w_1$, and thus $a_1y+b_1=a_2w_1+b_2$, contradicting (4.13). We therefore deduce that when $k=3$, one has $T_2(d)\ll\mathcal{M}_k^\varepsilon d^{-1}(H_1H_2Q_2)^{1/2}$, and the desired refinement follows immediately. The case $k=5$ may be disposed of similarly once we observe that in this case the equation (4.21) becomes

$$\alpha(5b_1Y^2-4b_1^5)=\beta(5b_2W^2-4b_2^5),$$

where $Y=a_1^2y^2+b_1^2$ and $W=a_2^2w_1^2+b_2^2$. This completes the proof of the lemma.

5. Sums and Differences of kth Powers

In this section we apply the conclusions of §4 to establish Theorem 2. We first make some simplifying observations. First note that when k is even $\nu_k^-(X)$ is the number of non-negative integers not exceeding X which are represented as the sum of two kth powers of non-negative integers in more than one essentially distinct way. Thus Skinner and Wooley [21, Theorem 1] shows that when $k\geq 4$ is even,

$$\nu_k^-(X)\ll X^{\frac{3}{2k}+\frac{1}{k(k-1)}+\varepsilon}.$$

In all other cases under consideration, on taking account of the underlying automorphism group and noting that zero has multiple representations, one finds that $\nu_k^\pm(X)\ll 1+\nu_k^*(X)$, where $\nu_k^*(X)$ denotes the number of positive integers not exceeding X that are represented as the difference of two integral kth powers in more than one essentially distinct way.

Next we observe that if a positive integer n is represented as the difference of two integral kth powers, say $n=u^k-v^k$, then on taking account of the underlying automorphism group one may suppose that $u\geq|v|$ and $u\neq v$. Thus, by a suitable rearrangement of variables, we deduce that $\nu_k^*(X)$ is bounded above by the number of integral solutions of the system

$$0<u_1^k-v_1^k=u_2^k-v_2^k\leq X,\tag{5.1}$$

with

$$-u_i\leq v_i<u_i\quad(i=1,2)\quad\text{and}\quad u_1\neq u_2.\tag{5.2}$$

For each solution $\mathbf{u},\mathbf{v}$ of (5.1) satisfying (5.2), we define integers x,y,z,w by $x=u_1-v_1$, $y=u_1+v_1$, $z=u_2-v_2$ and $w=u_2+v_2$. On recalling the definition of $\Upsilon_k(s,t)$ given by (4.4), the above discussion leads to the conclusion

$$\nu_k^*(X)\ll N_k(2^kX),\tag{5.3}$$

where $N_k(Q)$ denotes the number of solutions of the system

$$0 < \Upsilon_k(x,y) = \Upsilon_k(z,w) \le Q, \tag{5.4}$$

in non-negative integers x, y, z, w satisfying $x \neq 0$, $z \neq 0$ and $x + y \neq z + w$. Moreover, when k is even we may use the symmetry of $\Upsilon_k(s,t)$ to impose the additional conditions $y \ge x$ and $w \ge z$.

On recalling the definitions (4.6) and (4.25), we note that (4.4) implies that

$$\Upsilon_k(s,t) = \begin{cases} 2stU_k(s,t), & \text{when } k \text{ is even,} \\ 2sV_k(s,t), & \text{when } k \text{ is odd.} \end{cases}$$

Consequently, if x, y, z, w is a solution of (5.4) counted by $N_k(Q)$, then

$$0 < x \le \min\{Q^{1/k}, Qy^{1-k}\} \quad \text{and} \quad 0 < z \le \min\{Q^{1/k}, Qw^{1-k}\}. \tag{5.5}$$

We note that the contribution to $N_k(Q)$ from those solutions with $y = 0$ or $w = 0$ is $O(Q^{1/k+\varepsilon})$. For when $y = 0$, on assigning any permissible choice of x one finds from (5.4) that z is a divisor of a fixed non-zero integer. Having determined x and z, the variable w is determined by a non-trivial polynomial from (5.4), and thus the desired conclusion follows from (5.5). A similar argument disposes of the solutions with $w = 0$ in like manner. Next, on dividing into dyadic intervals, we deduce that

$$N_k(Q) \ll Q^{1/k+\varepsilon} + Q^{\varepsilon} \max_{1 \le Y \le Q^{1/(k-1)}} \max_{1 \le W \le Q^{1/(k-1)}} N_k^*(Q; Y, W), \tag{5.6}$$

where $N_k^*(Q; Y, W)$ denotes the number of integral solutions of the system (5.4) satisfying $Y \le y \le 2Y$, $W \le w \le 2W$ and (5.5). Moreover, on recalling the definition of $M_k(\mathbf{Q}, \mathbf{H}; \alpha, \beta)$ from §4 , one has

$$N_k^*(Q; Y, W) \le M_k(2Y, 2W, \min\{Q^{1/k}, QY^{1-k}\}, \min\{Q^{1/k}, QW^{1-k}\}; 1, 1). \tag{5.7}$$

Write δ_k for $1/k$ when $k = 3, 5$, and for $1/(k-1)$ otherwise. Then when $Y \le Q^{1/k}$, $W \le Q^{1/k}$ and $k \ge 3$, we may combine the conclusions of Lemmata 4.1 and 4.2 with (5.7) to obtain

$$N_k^*(Q; Y, W) \ll \left(WQ^{2/k}\right)^{1/2} \left(Q^{1/k} + Y + W\right)^{\delta_k+\varepsilon} \ll (Q^{1/k})^{3/2+\delta_k+\varepsilon}.$$

When instead $Y \le Q^{1/k}$ and $Q^{1/k} < W \le Q^{1/(k-1)}$ one similarly obtains

$$N_k^*(Q; Y, W) \ll \left(Q^{1+1/k}W^{2-k}\right)^{1/2} \left(Y + W + QW^{1-k}\right)^{\delta_k+\varepsilon} \ll (Q^{1/k})^{3/2+\delta_k+\varepsilon}.$$

On interchanging the roles of Y and W, a similar argument yields the same bound when $Q^{1/k} < Y \le Q^{1/(k-1)}$ and $W \le Q^{1/k}$. Finally, when $Q^{1/k} < Y \le Q^{1/(k-1)}$ and $Q^{1/k} < W \le Q^{1/(k-1)}$ we find that

$$N_k^*(Q; Y, W) \ll \left(Q^2W^{2-k}Y^{1-k}\right)^{1/2} \left(Y + W + QW^{1-k}\right)^{\delta_k+\varepsilon} \ll \left(Q^{1/k}\right)^{3/2+\delta_k+\varepsilon}.$$

Thus in any case $N_k^*(Q; Y, W) \ll (Q^{1/k})^{3/2+\delta_k+\varepsilon}$, and so Theorem 2 follows immediately from (5.3) and (5.6).

6. Binary Additive Forms

Our way is now clear to establish Theorem 1. We begin by discussing some simplifications. First, by multiplying the form through, if necessary, by -1, we may restrict attention to non-negative integers represented by $\alpha x^k - \beta y^k$. Next we note that there is no loss of generality in supposing α and β to be non-zero k-free integers. Moreover the conclusions of Theorem 2 permit us to suppose further that $\alpha \neq \pm\beta$. In particular, therefore, zero is represented by $\alpha x^k - \beta y^k$ precisely when $x = y = 0$, and so it suffices henceforth to consider only positive integers represented by the form in question.

Now we bound the domains of the variables. Suppose that n is a positive integer represented by $\alpha x^k - \beta y^k$. If k is even and $\alpha x^k - \beta y^k$ is definite, so that $\alpha > 0$ and $\beta < 0$, then plainly $|x| \le n^{1/k}$ and $|y| \le n^{1/k}$. If k is even and $\alpha x^k - \beta y^k$ is indefinite, meanwhile, one has that α/β is positive. Let

$\theta = (\beta/\alpha)^{1/k}$. Then no matter what the parity of k, on recalling that α and β are k-free and $\alpha \neq \pm\beta$, we have that θ is a real irrational algebraic number. Let ε be a small positive number. Then it follows from Roth's theorem (see [18]) that for each pair of non-zero integers p and q, one has

$$|p - \theta q| \gg |q|^{-1-\varepsilon} \quad \text{and} \quad |p\theta^{-1} - q| \gg |p|^{-1-\varepsilon},$$

where here the (ineffective) implicit constants depend at most on α, β and ε. We thus conclude that for each integer pair (u, v) one has

$$|\alpha u^k - \beta v^k| \gg (\max\{|u|, |v|\})^{k-2-\epsilon},$$

and so in all cases under consideration, if $\alpha x^k - \beta y^k = n$ then there exists a number $A = A(k, \varepsilon, \alpha, \beta)$ such that

$$|x| \leq An^{1/(k-2)+\varepsilon} \quad \text{and} \quad |y| \leq An^{1/(k-2)+\varepsilon}. \tag{6.1}$$

An upper bound for $\mu_k(X; \alpha, \beta)$ is provided by the number of integral solutions of the system

$$0 < \alpha u_1^k - \beta v_1^k = \alpha u_2^k - \beta v_2^k \leq X, \tag{6.2}$$

with $u_1 \neq u_2$, and subject in the cases where k is even to the additional condition $u_1 \neq -u_2$. We apply different arguments to bound the latter number according to the size of $\max_{i=1,2}\{|u_i|, |v_i|\}$. Thus, on dividing the range for the latter maximum into dyadic intervals, one deduces from (6.1) that for any number V satisfying $1 \leq V \leq AX^{1/(k-2)+\varepsilon}$, one has

$$\mu_k(X; \alpha, \beta) \ll T(V) + X^{\varepsilon} \max_{V \leq W \leq AX^{1/(k-2)+\varepsilon}} S(W), \tag{6.3}$$

where $T(V)$ denotes the number of solutions of (6.2) with $u_1 \neq u_2$ (and when k is even, with $u_1 \neq \pm u_2$), satisfying

$$\max_{i=1,2}\{|u_i|, |v_i|\} \leq V, \tag{6.4}$$

and where $S(W)$ denotes the corresponding number of solutions satisfying instead

$$W < \max_{i=1,2}\{|u_i|, |v_i|\} \leq 2W. \tag{6.5}$$

We first bound $S(W)$. Let us estimate the number of solutions of (6.2) counted by $S(W)$ in which

$$|u_1| = \max_{i=1,2}\{|u_i|, |v_i|\}. \tag{6.6}$$

Plainly one may argue similarly when one of the remaining variables is in fact maximal. In view of (6.5), the hypothesis (6.6) implies that $W < |u_1| \leq 2W$. But from (6.2) one has $|\alpha u_1^k - \beta v_1^k| \leq X$, and hence $|u_1\theta^{-1} - v_1| \ll X|u_1|^{1-k}$. Thus we deduce that given u_1 with $W < |u_1| \leq 2W$, the number of possible choices for v_1 is $O(1 + XW^{1-k})$. Further, given u_1 and v_1, the variables u_2 and v_2 satisfy an equation of the shape $\alpha u_2^k - \beta v_2^k = n$, so that there are $O(X^{\varepsilon})$ possible choices for u_2 and v_2 (see, for example, [2], although earlier references would suffice in this case). Consequently, on combining these bounds we conclude that

$$S(W) \ll X^{\varepsilon}\left(W + XW^{2-k}\right). \tag{6.7}$$

Next we observe that an upper bound for $T(V)$ is provided by the number of integral solutions of the equation

$$\alpha(u_1^k - u_2^k) = \beta(v_1^k - v_2^k), \tag{6.8}$$

with $u_1 \neq u_2$ (and when k is even, with $u_1 \neq \pm u_2$), and satisfying $|u_i| \leq V$ and $|v_i| \leq V$ $(i = 1, 2)$. We are therefore able to bound $T(V)$ by using Lemmata 4.1 and 4.2, following some simplifying observations. Note first that by interchanging indices, it suffices to consider only those solutions in which $|u_1| > |u_2|$ and $|v_1| > |v_2|$. Also, when k is even we may plainly suppose that the variables are all non-negative. When k is odd, moreover, we may adjust the signs of α and β, if necessary, so that it suffices to consider the situation in which u_1 and v_1 are restricted to be positive numbers. Now define new variables

x, y, z, w according to (4.2). Then we find that the solution $\mathbf{u}, \mathbf{v}$ of (6.8) corresponds to a solution x, y, z, w of the equation (4.3). On recalling (6.4), we are led by this discussion to the conclusion

$$T(V) \ll M_k(2V, 2V, 2V, 2V; \alpha, \beta),$$

and hence, by Lemmata 4.1 and 4.2, we have

$$T(V) \ll V^{3/2+\delta_k+\varepsilon}, \tag{6.9}$$

where $\delta_k = 1/k$ when $k = 3, 5$, and $\delta_k = 1/(k-1)$ otherwise.

On combining (6.3), (6.7) and (6.9), we finally obtain

$$\mu_k(X; \alpha, \beta) \ll V^{3/2+\delta_k+\varepsilon} + X^{\varepsilon}\left(X^{1/(k-2)} + XV^{2-k}\right),$$

and the conclusion of Theorem 1 follows with a modicum of computation on taking $V^{k-1/2+\delta_k} = X$.

References

1. M. A. Bennett and B. M. M. de Weger, *On the Diophantine equation* $|ax^n - by^n| = 1$, Math. Comp. (to appear).
2. E. Bombieri and W. M. Schmidt, *On Thue's equation*, Invent. Math. **88** (1987), 69–81.
3. E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. **59** (1989), 337–357.
4. P. Erdős and K. Mahler, *On the number of integers that can be represented by a binary form*, J. London Math. Soc. **13** (1938), 134–139.
5. T. Estermann, *Einige Sätze über quadratfreie Zahlen*, Math. Ann. **105** (1931), 653–662.
6. J.-H. Evertse, *Upper Bounds for the Numbers of Solutions of Diophantine Equations*, PhD Thesis, Leiden, 1983.
7. J.-H. Evertse, *On the equation* $ax^n - by^n = c$, Compositio Math. **47** (1982), 289–315.
8. A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1991.
9. G. Greaves, *On the representation of a number as a sum of two fourth powers*, Math. Z. **94** (1966), 223–234.
10. G. Greaves, *On the representation of a number as a sum of two fourth powers, II*, Mat. Zametki **55** (1994), 47–58. (Russian)
11. C. Hooley, *On binary cubic forms*, J. Reine Angew. Math. **226** (1967), 30–87.
12. C. Hooley, *On the numbers that are representable as the sum of two cubes*, J. Reine Angew. Math. **314** (1980), 146–173.
13. 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.
14. C. Hooley, *On binary quartic forms*, J. Reine Angew. Math. **366** (1986), 32–52.
15. K. Mahler, *Zur Approximation algebraischer Zahlen III*, Acta Math. **62** (1934), 91–166.
16. M. Mignotte, *A note on the equation* $ax^n - by^n = c$, Acta Arith. **75** (1996), 287–295.
17. J. Mueller, *Counting solutions of* $|ax^r - by^r| \leq h$, Quart. J. Math. Oxford (2) **38** (1987), 503–513.
18. K. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20.
19. W. M. Schmidt, *Diophantine Approximations and Diophantine Equations, Lecture Notes in Mathematics*, vol. 1467, Springer-Verlag, New York, 1991.
20. C. L. Siegel, *Die Gleichung* $ax^n - by^n = c$, Math. Ann. **114** (1937), 57–68.
21. C. M. Skinner and T. D. Wooley, *Sums of two kth powers*, J. Reine Angew. Math. **462** (1995), 57–68.
22. C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc. **4** (1991), 793–835.
23. A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. **135** (1909), 284–305.

MAB: Mathematics Department, University of Michigan, Ann Arbor, Michigan 48109-1003
E-mail address: mabennet@math.lsa.umich.edu

NPD: Mathematics Department, University of Michigan, Ann Arbor, Michigan 48109-1003
Current address: Mathematics Department, Northern Illinois University, De Kalb, Illinois 60115-2888
E-mail address: dummigan@math.niu.edu

TDW: Mathematics Department, University of Michigan, Ann Arbor, Michigan 48109-1003
E-mail address: wooley@math.lsa.umich.edu