Plane Curves in Boxes and Equal Sums of Two Powers

T.D. Browning[1]
D.R. Heath-Brown[2]
Mathematical Institute, 24–29 St. Giles', Oxford OX1 3LB
[1]browning@maths.ox.ac.uk, [2]rhb@maths.ox.ac.uk

1 Introduction

Let $F \in \mathbb{Z}[x_1, x_2, x_3]$ be an absolutely irreducible form of degree d, producing a plane curve in $\mathbb{P}^2$. The central aim of this paper is to analyze the density of rational points on such curves, which are contained in boxes with unequal sides. We shall see below how such considerations may be used to obtain new paucity results for equal sums of two powers.

Suppose that $\mathbf{P} = (P_1, P_2, P_3)$ for fixed real numbers $1 \leq P_1 \leq P_2 \leq P_3$, say. Then we define

$$N(F; \mathbf{P}) = \#\{\mathbf{x} \in \mathbb{Z}^3 : \ F(\mathbf{x}) = 0, \ |x_i| \leq P_i, \ (1 \leq i \leq 3), \ \mathbf{x} \text{ primitive}\},$$

where $\mathbf{x} = (x_1, x_2, x_3)$ is said to be primitive if h.c.f.$(x_1, x_2, x_3) = 1$. Our starting point is the recent work of the second author [2], who has shown that $N(F; \mathbf{P}) = O(P^{2/d+\varepsilon})$ for any $\varepsilon > 0$, whenever $P_i = P$ for $1 \leq i \leq 3$. The implied constant in this bound depends at most upon the choice of ε and d, a convention that we shall follow throughout this paper. This is essentially best possible for curves of genus zero, and it is natural to ask what can be said about the quantity $N(F; \mathbf{P})$ when the P_i are of genuinely different sizes. With this in mind we define

$$T = \max\{P_1^{e_1} P_2^{e_2} P_3^{e_3}\}, \tag{1}$$

where the maximum is taken over all integer triples (e_1, e_2, e_3) for which the corresponding monomial $x_1^{e_1} x_2^{e_2} x_3^{e_3}$ occurs in $F(\mathbf{x})$ with non-zero coefficient. Then for any $\varepsilon > 0$, the second author's principal result for curves [2, Theorem 3] states that

$$N(F; \mathbf{P}) \ll \left(\frac{P_1 P_2 P_3}{T^{1/d}}\right)^{1/d+\varepsilon}. \tag{2}$$

This clearly reduces to the previous bound whenever $P_i = P$ for $1 \leq i \leq 3$. Turning to the case of unequal P_i, it is easy to construct examples for which (2) is not best possible. Indeed, let $F = x_1^{d-1} x_3 - x_2^d$ and $\mathbf{P} = (1, P, Q)$, say.

Then it follows from (2) that $N(F;\mathbf{P}) \ll P^{1/d}Q^{(d-1)/d^2+\varepsilon}$ whenever $P^d \le Q$, whereas in fact $N(F;\mathbf{P})$ has order of magnitude $\min\{P, Q^{1/d}\}$.

It transpires that in the case of unequal P_i there is scope for improvement within the proof of (2) itself. This has been demonstrated by the second author [3, Theorem 15] in the special case $P_1 = 1$. For any $\varepsilon > 0$, it is shown that

$$N(F; 1, P_2, P_3) \ll P_3^{\varepsilon} \exp\left(\frac{\log P_2 \log P_3}{\log T}\right), \tag{3}$$

where T is given by (1). In particular, this is always at least as sharp as (2) and is essentially best possible by our example above. Moreover, the formulation we have given obviously incorporates the corresponding problem for integral points on affine plane curves $F(1, x_2, x_3) = 0$.

We build upon these results by returning once again to the framework provided by the proof of (2). Our aim is to establish a sharper bound for the interim case in which $P_1 \ge 1$ and the region $|x_i| \le P_i$ is sufficiently lopsided. Unfortunately the statement of the bound is somewhat complicated, and it will be convenient to introduce the quantities

$$\alpha = \frac{\log P_1}{\log P_3}, \qquad \beta = \frac{\log P_2}{\log P_3}, \qquad \tau = \frac{\log T}{d \log P_3},$$

for given $1 \le P_1 \le P_2 \le P_3$ and T as in (1). With this in mind, we have the following result.

Theorem 1. *Suppose that $T \ge (P_1P_2)^d$, and let $\varepsilon > 0$ be given. Then we have*

$$N(F;\mathbf{P}) \ll P_3^{\varepsilon} \exp\left(\frac{\alpha\beta + (\alpha+\beta-\alpha\beta)(\tau-\alpha-\beta)}{d(\tau-\alpha)(\tau-\beta)} \log P_3\right).$$

In particular, Theorem 1 reduces to (3) in the case $P_1 = 1$. Indeed, we always have the lower bound $T \ge P_2^d$ whenever F is an absolutely irreducible form, and the bounds in Theorem 1 and (3) agree when $\alpha = 0$. On the face of it, one might think of the condition $T \ge (P_1P_2)^d$ as being unduly restrictive. In fact a straightforward calculation shows that this is precisely the region for which Theorem 1 is sharper than (2).

Turning to our application of Theorem 1, we fix a choice of $k \ge 4$ and consider the diagonal equation

$$w^k + x^k = y^k + z^k. \tag{4}$$

For any $X \ge 1$, we denote by $N_k(X)$ the number of positive integer solutions in the region $\max\{w, x, y, z\} \le X$. There are $2X^2 + O(X)$ trivial solutions in which y, z are a permutation of w, x, and so we write $N_k^{(0)}(X)$ for the number of non-trivial solutions. This quantity has received a great deal of attention lately, and we mention in particular the results of Hooley [4, 5] and the second author [2, Theorem 11]. Together, they comprise the best available estimates for values of k in the interval $4 \le k \le 12$. The first of these provides the bound

$$N_k^{(0)}(X) \ll X^{5/3+\varepsilon} \tag{5}$$

for any $k \geq 4$, whereas the second yields

$$N_k^{(0)}(X) \ll X^{1+\varepsilon} + X^{3/\sqrt{k}+2/(k-1)+\varepsilon} \tag{6}$$

for any such k, and supersedes Hooley's bound for $k \geq 6$.

The aim of the second part of this paper is to improve upon the previous bounds whenever $k = 5$ or 6. This will be done via a suitable application of Theorem 1. It is unfortunate that we shall only make use of the special case (3), and not of Theorem 1 *per se*. Nonetheless, it is our belief that the bound in Theorem 1 still merits a full presentation. We shall establish the following result in Section 3.

Theorem 2. *For any $k \geq 4$ and any $\varepsilon > 0$, we have*

$$N_k^{(0)}(X) \ll X^{3/2+1/(2k-2)+\varepsilon}.$$

We take this opportunity to remark that the proof of (6) may be modified slightly to give a sharper result. In fact it is possbile to establish the estimate

$$N_k^{(0)}(X) \ll X^{1+\varepsilon} + X^{3/\sqrt{k}+2/k+\varepsilon}, \tag{7}$$

for any $\varepsilon > 0$ and $k \geq 4$. At this point it is convenient to tabulate the various available bounds for $N_k^{(0)}(X)$, for k in the range $4 \leq k \leq 8$. Let $\varepsilon > 0$. Then we may write $N_k^{(0)}(X) = O(X^{\theta_k+\varepsilon})$, where the permissible values of θ_k are given in the following table. The rows in this table correspond to the estimates (5), (6), (7) and Theorem 2, respectively.

θ_4	θ_5	θ_6	θ_7	θ_8
1.666..	1.666..	1.666..	1.666..	1.666..
2.166..	1.841..	1.624..	1.467..	1.346..
2.000..	1.741..	1.558..	1.419..	1.310..
1.666..	1.625	1.600..	1.583..	1.571..

Thus we see that Hooley's bound (5) remains unbeaten only for $k = 4$. For $k = 5$ the exponent in Theorem 2 is the sharpest known, but (7) should be used for larger values of k.

We now indicate how (7) can be established. An inspection of the proof [2, §8] of (6), reveals that it suffices to offer an alternative treatment of the curves of degree $k-1$ which are contained in the non-singular projective surface (4). Our observed improvement rests upon a reformulation of Colliot-Thélène's result [2, Appendix], as used in the proof of (6). This states that any non-singular surface of degree k in $\mathbb{P}^3$ contains $O(1)$ curves of degree $\leq k-2$. In recent communications with the authors, Professor Colliot-Thélène has shown that any such non-singular surface actually contains $O(1)$ non-degenerate curves of degree $\leq 2(k-2)$. Here, a curve in $\mathbb{P}^3$ is said to be non-degenerate if it is not contained in any $\mathbb{P}^2 \subset \mathbb{P}^3$. Since any absolutely irreducible curve of degree d in

$\mathbb{P}^3$ contains $O(X^{2/d+\varepsilon})$ rational points of height at most X, by [2, Theorem 5], it remains to handle the plane curves of degree $k-1$ which are contained in (4). Such curves arise as the intersection of (4) with a plane

$$aw + bx + cy + dz = 0, \tag{8}$$

say, that contains one of the lines in (4). But we know that all of the lines contained in this surface are given by $\{|w|, |x|\} = \{|y|, |z|\}$ (for k even), or by $\{w, x\} = \{y, z\}$ or $w = -x$, $y = -z$ (for k odd). Hence it is trivial to deduce from (8) that the only available planes have $\{|a|, |b|\} = \{|c|, |d|\}$ (for k even), or $\{a, b\} = \{-c, -d\}$ or $a = b$, $c = d$ (for k odd). Thus there are relatively few planes (8) of low height that need to be considered. The proof may then be completed by counting points according to the height of the corresponding plane (8).

In the case $k = 4$, it is worthwhile remarking that the proof of Theorem 2 can readily be adapted to show that for any $\varepsilon > 0$ there are $O(X^{5/3+\varepsilon})$ positive integer solutions to the equation

$$w^4 + x^4 + y^4 = z^4,$$

in the region $\max\{w, x, y, z\} \le X$. This supersedes work of the first author [1], who has already obtained the exponent $7/4 + \varepsilon$.

Notation. We shall follow common practice in allowing the small positive quantity ε to take different values at different points in all that follows.

Acknowledgement. While working on this paper, the first author was supported by EPSRC Grant number GR/R93155/01.

2 Proof of Theorem 1

In this section we shall prove Theorem 1. If $P_1 = 1$, then Theorem 1 reduces to (3). Henceforth we assume that $P_1 > 1$. But then the condition $T \ge (P_1P_2)^d$ implies that $f_3 \ne 0$, where we suppose that (f_1, f_2, f_3) is the maximal triple taken in the definition (1) of T. We set

$$\kappa = (2f_1 + f_2)/f_3 + 3, \tag{9}$$

and note that $3 \le \kappa \le 3d$. During the course of our argument we will encounter difficulties if the values of $\log P_i$ are too close together. We therefore replace P_1, P_2, P_3 by

$$B_1 = P_1P_3^{\delta}, \qquad B_2 = P_2P_3^{2\delta}, \qquad B_3 = P_3^{1+\kappa\delta}. \tag{10}$$

Here κ is given by (9), and δ is defined to be

$$\delta = \frac{\varepsilon}{180d^3}. \tag{11}$$

Writing $B_1^{f_1}B_2^{f_2}B_3^{f_3} = T'$, say, we observe that

$$\log T' = \log T + 3d\delta \log P_3.$$

For any $x \geq 0$, define the functions

$$\alpha(x) = \frac{\alpha + x}{1 + \kappa x}, \qquad \beta(x) = \frac{\beta + 2x}{1 + \kappa x}, \qquad \tau(x) = \frac{\tau + 3x}{1 + \kappa x}, \tag{12}$$

where α, β, τ are the quantities appearing in the statement of Theorem 1. Then (10) implies that

$$\alpha(\delta) = \frac{\log B_1}{\log B_3}, \qquad \beta(\delta) = \frac{\log B_2}{\log B_3}, \qquad \tau(\delta) = \frac{\log T'}{d \log B_3}.$$

It will be convenient to record that for any $x \geq 0$ we have $0 < \alpha(x) \leq \beta(x)$ and

$$\alpha(x) + \beta(x) \leq \tau(x) \leq 1, \tag{13}$$

since $P_3^d \geq T \geq (P_1 P_2)^d$ and $\kappa \geq 3$. Finally, we define the function

$$g(x) = \frac{\alpha(x)^2}{\tau(x) - \beta(x)} \cdot \frac{\beta(x) - 1}{\tau(x) - \alpha(x)} + \frac{\alpha(x) + \beta(x) - \alpha(x)\beta(x)}{\tau(x) - \alpha(x)}. \tag{14}$$

With these notations, our task is to establish that

$$N(F; \mathbf{P}) \ll P_3^{\varepsilon} \exp\left(\frac{1}{d} g(0) \log P_3\right), \tag{15}$$

whenever $T \geq (P_1 P_2)^d$.

Our first step is to note that $N(F; \mathbf{P}) \leq N(F; \mathbf{B})$, and we proceed to estimate the latter. Fortunately we shall only need to make minor alterations to the second author's proof of (2) to do so. Let $\mathcal{P} \geq \log^2(\|F\| B_3)$, where $\|F\|$ denotes the maximum modulus of the coefficients of F. Then according to [1; Lemma 4] it suffices to consider the set of $\mathbf{x}$ counted by $N(F; \mathbf{B})$ for which $p \nmid \nabla F(\mathbf{x})$, for a fixed prime p in the range $\mathcal{P} \ll p \ll \mathcal{P}$. For each non-singular $\mathbf{t} = (t_1, t_2, t_3)$ on the projective variety $F(\mathbf{t}) \equiv 0 \pmod{p}$, we write $S(\mathbf{t})$ for the set of points counted by $N(F; \mathbf{B})$ for which $\mathbf{x} \equiv \lambda \mathbf{t} \pmod{p}$ for some integer λ. Clearly there are $O(\mathcal{P})$ possible values of $\mathbf{t}$. Let δ be given by (11). We plan to show that whenever

$$\mathcal{P} \gg B_3^{\varepsilon} \exp\left(\frac{1}{d} g(\delta) \log B_3\right) \log^2 \|F\|, \tag{16}$$

there is an auxiliary form $G(\mathbf{x})$ of degree $O(1)$, such that $F \nmid G$ and $G(\mathbf{x}) = 0$ for all $\mathbf{x} \in S(\mathbf{t})$. It turns out that we may only do this if

$$\log T' \geq d \log B_1 + d \log B_2. \tag{17}$$

Under this assumption we easily deduce the estimate

$$N(F; \mathbf{B}) \ll B_3^{\varepsilon} \exp\left(\frac{1}{d} g(\delta) \log B_3\right), \tag{18}$$

via an application of Bézout's Theorem and [1; Theorem 4], just as in the proof of (2). We now show how Theorem 1 can be derived from (18). We first observe that (17) holds in view of the first of the inequalities (13). Next we show how (15) follows from the corresponding estimate (18) for $N(F; \mathbf{B})$. This will require the following result.

Lemma 1. *Let δ be given by (11). Then we have*

$$g(\delta) \leq g(0) + \varepsilon.$$

Since F is absolutely irreducible we must have $T \geq P_3$, and hence (12) implies the lower bound $\tau(x) \geq 1/d$. Once combined with (13), we deduce that

$$\tau(x) - \alpha(x) \geq \max\{\beta(x), \frac{1}{d} - \alpha(x)\} \geq \max\{\alpha(x), \frac{1}{d} - \alpha(x)\} \geq \frac{1}{2d}. \qquad (19)$$

To prove Lemma 1 we shall also use the fact that for any $x \geq 0$ we have the trivial inequalities

$$0 < \alpha(x), \beta(x), \tau(x) \leq 1, \qquad |\alpha'(x)|, |\beta'(x)|, |\tau'(x)| \leq 6d. \qquad (20)$$

To see the last three inequalities we note that

$$|\tau'(x)| = \left| \frac{3}{1+\kappa x} - \frac{\kappa(\tau + 3x)}{(1+\kappa x)^2} \right| \leq 3 + \kappa \leq 6d,$$

for example, since $3 \leq \kappa \leq 3d$. If we write

$$h_1(x) = \frac{\alpha(x) + \beta(x) - \alpha(x)\beta(x)}{\tau(x) - \alpha(x)},$$

then there exists some $0 < \xi < \delta$ such that $h_1(\delta) - h_1(0) = \delta h_1'(\xi)$, by the mean value theorem. Using (13) it is easy to see that $0 \leq \alpha(x) + \beta(x) - \alpha(x)\beta(x) \leq 1$, and so (19) and (20) yield

$$|h_1'(x)| \leq 24d^2 + 48d^3 \leq 72d^3,$$

for any $x \geq 0$. Similarly, we write

$$h_2(x) = \frac{1 - \beta(x)}{\tau(x) - \alpha(x)},$$

and deduce that $|h_2(\delta) - h_2(0)| \leq 60d^3\delta$. Finally, we write

$$h_3(x) = \frac{\alpha(x)^2}{\tau(x) - \beta(x)},$$

and consider the derivative

$$h_3'(x) = \frac{2\alpha(x)\alpha'(x)}{\tau(x) - \beta(x)} - \left(\frac{\alpha(x)}{\tau(x) - \beta(x)} \right)^2 (\tau'(x) - \beta'(x)).$$

But (13) implies that $\alpha(x) \leq \tau(x) - \beta(x)$, and so we easily obtain the bound $|h_3(\delta) - h_3(0)| \leq 24d\delta$. Taken together with (14), it therefore follows that

$$\begin{aligned} |g(\delta) - g(0)| &\leq |h_3(\delta) - h_3(0)|h_2(\delta) + |h_2(\delta) - h_2(0)|h_3(0) + |h_1(\delta) - h_1(0)| \\ &\leq 2d|h_3(\delta) - h_3(0)| + |h_2(\delta) - h_2(0)| + |h_1(\delta) - h_1(0)| \\ &\leq \delta\{48d^2 + 60d^3 + 72d^3\} \\ &\leq \varepsilon, \end{aligned}$$

by (11). This completes the proof of Lemma 1.

We are now in a position to deduce (15) from (18) and Lemma 1. Using the same notation it is easy to deduce from (12), (13) and (14) that

$$g(0) = -h_3(0)h_2(0) + h_1(0) \leq 4d.$$

Recall that $\kappa \leq 3d$. Then (10), (11) and Lemma 1 yield

$$\begin{aligned} \frac{1}{d}g(\delta)\log B_3 - \frac{1}{d}g(0)\log P_3 &\leq \frac{1}{d}\log P_3\{\varepsilon + \kappa\delta(g(0)+\varepsilon)\} \\ &\leq 2\varepsilon \log P_3, \end{aligned}$$

whence (15).

We now show how the lower bound (16) suffices for the existence of a suitable auxiliary form $G(\mathbf{x})$. Let $D \geq d$ and $A > 0$, and consider the exponent set

$$\mathcal{E}(A) = \left\{ \mathbf{e} \in \mathbb{Z}^3 : e_i \geq 0,\ \sum_{i=1}^{3} e_i = D,\ \sum_{i=1}^{3} e_i \log B_i \leq A,\ \exists j \text{ s.t. } e_j < f_j \right\}.$$

Let $E = \#\mathcal{E}(A)$, and suppose for the moment that $E \leq \#S(\mathbf{t})$. If we choose any distinct vectors $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(E)} \in S(\mathbf{t})$, then it will actually suffice just to show that the determinant

$$\Delta = \det(\mathbf{x}^{(i)\mathbf{e}})_{1 \leq i \leq E,\ \mathbf{e} \in \mathcal{E}(A)}$$

vanishes whenever (16) occurs. Indeed, the construction of the auxiliary polynomial

$$G(\mathbf{x}) = \sum_{\mathbf{e} \in \mathcal{E}(A)} a_{\mathbf{e}} x_1^{e_1} x_2^{e_2} x_3^{e_3}$$

is then identical to that given in the proof of (2). We have written $\mathbf{w}^{\mathbf{e}} = w_1^{e_1} w_2^{e_2} w_3^{e_3}$ in the definition of Δ, in which rows correspond to the different vectors $\mathbf{x}^{(i)}$, and columns correspond to the various $\mathbf{e} \in \mathcal{E}(A)$. Furthermore, it is immediate from the proof of (2) that any such form G cannot be divisible by F. The advantage over the previous situation is that our new exponent set $\mathcal{E}(A)$ allows us to choose an optimal value of A, for which better control over the size of $|\Delta|$ is possible in certain situations.

Our proof now breaks into two parts. Firstly we must obtain an estimate for the real modulus of Δ, and then secondly show that its p-adic order is sufficiently large that Δ must in fact vanish. We begin with the first of these, and use the fact that $|x_j^{(i)}| \leq B_j$ for $1 \leq j \leq 3$ to deduce that the column corresponding to the exponent vector $\mathbf{e}$ consists of elements of modulus at most $B_1^{e_1} B_2^{e_2} B_3^{e_3}$. It therefore follows that

$$|\Delta| \leq E^E \prod_{\mathbf{e} \in \mathcal{E}(A)} B_1^{e_1} B_2^{e_2} B_3^{e_3}. \tag{21}$$

For any $\mathbf{e} \in \mathbb{Z}^3$ with $e_i \geq 0$, we henceforth set

$$\sigma(\mathbf{e}) = e_1 \log B_1 + e_2 \log B_2 + e_3 \log B_3.$$

For $1 \le i \le 3$, define $\mathcal{E}_i$ to be the subset of $\mathcal{E}(A)$ for which $e_i < f_i$. Then we have

$$\log \prod_{\mathbf{e}\in\mathcal{E}(A)} B_1^{e_1} B_2^{e_2} B_3^{e_3} = \sum_{\mathbf{e}\in\mathcal{E}(A)} \sigma(\mathbf{e}) \le \sum_{i=1}^{3} \sum_{\mathbf{e}\in\mathcal{E}_i} \sigma(\mathbf{e}), \tag{22}$$

since $\mathcal{E}(A) = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3$. Hence it suffices to estimate $\sum_{\mathbf{e}\in\mathcal{E}_i} \sigma(\mathbf{e})$, for which it will be convenient to write

$$b_i = \log B_i, \qquad 1 \le i \le 3.$$

Let $c = 1/\delta + \kappa$, where κ and δ are given by (9) and (11), respectively. Then it follows from our initial change of variables (10) that we have the inequalities

$$0 < b_1 < b_2 < b_3 \le cb_1, \qquad b_3 \le c(b_j - b_i), \tag{23}$$

for each $1 \le i < j \le 3$.

It is convenient at this point to make the assumption that A is contained in the interval

$$Db_2 < A \le Db_3. \tag{24}$$

Clearly our definition of $\mathcal{E}(A)$ would be rather pointless if we allowed $A > Db_3$, since then the condition $\sigma(\mathbf{e}) \le A$ is automatic and we retrieve the exponent set considered in the proof of (2). Similarly, $\mathcal{E}(A)$ is obviously empty for any $A \le Db_1$. Our motive for omitting any treatment of the interval $Db_1 < A \le Db_2$ is not so apparent. Indeed, it is possible to adjust our argument to take such values of A into account and actually achieve something new at the end of it. We have chosen not to do so simply because we would ultimately be led to a weaker result than Theorem 1. Moreover, we are able to simplify our work considerably under the hypothesis (24).

Henceforth let i, j, k denote distinct elements of the set $\{1, 2, 3\}$, and define

$$\mathcal{M}_{jk} = \left\{(m_j, m_k) \in \mathbb{Z}^2 : m_j, m_k \ge 0,\ m_j + m_k = D,\ \tau(m_j, m_k) \le A\right\},$$

where $\tau(m_j, m_k) = m_j b_j + m_k b_k$. We shall apply the following result to simplify our estimate for $\sum_{\mathbf{e}\in\mathcal{E}_i} \sigma(\mathbf{e})$.

Lemma 2. *For $1 \le i \le 3$ we have*

$$\sum_{\mathbf{e}\in\mathcal{E}_i} \sigma(\mathbf{e}) \le f_i \sum_{(m_j,m_k)\in\mathcal{M}_{jk}} \tau(m_j, m_k) + O(A),$$

provided that (24) holds.

We prove the result for $i = 3$, say, and consider values of $\mathbf{e} \in \mathcal{E}_3$ with a fixed component $e_3 < f_3$. If $m_1 = e_1$ and $m_2 = e_2 + e_3$ then $|\tau(m_1, m_2) - \sigma(\mathbf{e})| \le db_3$. In particular we either have $(m_1, m_2) \in \mathcal{M}_{12}$ or

$$A < \tau(m_1, m_2) \le A + db_3. \tag{25}$$

Let R_{12} denote the number of non-negative $m_1, m_2 \in \mathbb{Z}$ such that $m_1+m_2 = D$ and (25) holds. It follows that

$$\sum_{\mathbf{e}\in\mathcal{E}_3} \sigma(\mathbf{e}) \le \sum_{e_3<f_3} \left\{ AR_{12} + \sum_{(m_1,m_2)\in\mathcal{M}_{12}} (\tau(m_1,m_2)+db_3) \right\}.$$

Moreover, we observe that

$$A > Db_2 \gg Db_3, \tag{26}$$

by (23) and (24). Since $\#\mathcal{M}_{12} \le D+1$ and $D \ge d$, this yields

$$\sum_{\mathbf{e}\in\mathcal{E}_3} \sigma(\mathbf{e}) \le f_3 \sum_{(m_1,m_2)\in\mathcal{M}_{12}} \tau(m_1,m_2) + O(A+AR_{12}).$$

In order to estimate R_{12} we set $\nu = b_1D/(b_2-b_1)$. Then R_{12} is the number of non-negative integers $m_2 \le D$ for which

$$\frac{A}{b_2-b_1} < m_2+\nu \le \frac{A}{b_2-b_1} + \frac{db_3}{b_2-b_1}.$$

It follows from (23) that $db_3/(b_2-b_1) \ll 1$, whence $R_{12} = O(1)$. This suffices for the proof of Lemma 2.

Recall that $\{i,j,k\}$ is a permutation of $\{1,2,3\}$. Our next task is to establish the estimate

$$\sum_{(m_j,m_k)\in\mathcal{M}_{jk}} \tau(m_j,m_k) = \frac{1}{2}\sum_{g,h}{}^{*} \frac{A^2-D^2b_h^2}{b_g-b_h} + O(A), \tag{27}$$

where $\{g,h\}$ runs over permutations of $\{j,k\}$, and Σ^* denotes the condition $b_h < A/D$. Taking the case corresponding to $i=3$ first, we automatically have $\tau(m_1,m_2) < A$ since $Db_2 < A$, by (24). Therefore

$$\begin{aligned}
\sum_{(m_1,m_2)\in\mathcal{M}_{12}} \tau(m_1,m_2) &= \sum_{m_1+m_2=D} \tau(m_1,m_2) \\
&= \sum_{m_2=0}^{D} \{(b_2-b_1)m_2 + b_1D\} \\
&= (b_1+b_2)D(D+1)/2 \\
&= \frac{1}{2}\left\{ \frac{A^2-D^2b_1^2}{b_2-b_1} + \frac{A^2-D^2b_2^2}{b_1-b_2} \right\} + O(A).
\end{aligned}$$

In the case $i=1$, we find

$$\begin{aligned}
\sum_{(m_2,m_3)\in\mathcal{M}_{23}} \tau(m_2,m_3) &= \sum_{m_3=0}^{[\frac{A-Db_2}{b_3-b_2}]} \{(b_3-b_2)m_3 + b_2D\} \\
&= \frac{A^2-D^2b_2^2}{2(b_3-b_2)} + O(A),
\end{aligned}$$

on using (26). The treatment of the case $i = 2$ is similar. This completes the proof of (27).

Upon combining (21), (22), Lemma 2 and (27), we are therefore led to the following result.

Lemma 3. *We have*

$$\log|\Delta| \le \frac{1}{2}\sum_{i=1}^{3} f_i \sum_{g,h}{}^{*} \frac{A^2 - D^2 b_h^2}{b_g - b_h} + E\log E + O(A),$$

provided that (24) holds.

For our fixed prime p with order of magnitude $\mathcal{P}$, we must now determine a lower bound for $\nu_p(\Delta)$, the p-adic order of Δ. However it suffices to compute $E = \#\mathcal{E}(A)$, since [1; Lemma 6] implies that

$$\nu_p(\Delta) \ge \frac{1}{2}E^2\{1 + o(1)\}, \tag{28}$$

as $E \to \infty$. In fact a lower bound for E can easily be deduced by mimicking the previous calculation. Beginning with the analogue of (22), one obviously has

$$\left| \sum_{\mathbf{e}\in\mathcal{E}(A)} 1 - \sum_{i=1}^{3}\sum_{\mathbf{e}\in\mathcal{E}_i} 1 \right| \le \sum_{i<j}\sum_{\mathbf{e}\in\mathcal{E}_i\cap\mathcal{E}_j} 1 = O(1). \tag{29}$$

Moreover, the corresponding version of Lemma 2 is

$$\sum_{\mathbf{e}\in\mathcal{E}_i} 1 \ge f_i \sum_{(m_j,m_k)\in\mathcal{M}_{jk}} 1 + O(1), \tag{30}$$

under the same assumption that (24) holds. We prove this for $i = 3$, say. Recall that $m_1 + m_2 = D$ and $\tau(m_1, m_2) \le A$ whenever $(m_1, m_2) \in \mathcal{M}_{12}$. In particular, for each integer $0 \le k < f_3$ we either have $(m_1, m_2 - k, k) \in \mathcal{E}_3$ or $0 \le m_2 < k$ or $A - db_3 < \tau(m_1, m_2) \le A$. Hence an argument similar to that used in the proof of Lemma 2 yields the upper bound

$$\sum_{k<f_3}\sum_{(m_1,m_2)\in\mathcal{M}_{12}} 1 \le \sum_{\mathbf{e}\in\mathcal{E}_3} 1 + O(1),$$

which establishes (30). Combining (29) and (30), together with the corresponding version of (27), we obtain the lower bound

$$E \ge \sum_{i=1}^{3} f_i \sum_{g,h}{}^{*} \frac{A - Db_h}{b_g - b_h} + O(1), \tag{31}$$

provided that (24) holds.

Let A be contained in the interval (24). Then as $D \to \infty$ we will have both $E \to \infty$ and $A = o(D^2 b_2)$. It now follows from Lemma 3 that

$$\log|\Delta| \leq \frac{1}{2}\left\{f_1 \frac{A^2 - D^2 b_2^2}{b_3 - b_2} + f_2 \frac{A^2 - D^2 b_1^2}{b_3 - b_1} + f_3 D^2(b_1 + b_2)\right\}(1+o(1)) + o(E^2),$$

as $D \to \infty$. Moreover from (28) and (31) we also have

$$\nu_p(\Delta) \geq \frac{1}{2}\left\{f_1 \frac{A - Db_2}{b_3 - b_2} + f_2 \frac{A - Db_1}{b_3 - b_1} + f_3 D\right\}^2 (1 + o(1)).$$

We may therefore conclude that

$$\frac{\log|\Delta|}{\nu_p(\Delta)} \leq \frac{f_1 \frac{A^2 - D^2 b_2^2}{b_3 - b_2} + f_2 \frac{A^2 - D^2 b_1^2}{b_3 - b_1} + f_3 D^2(b_1 + b_2)}{\left\{f_1 \frac{A - Db_2}{b_3 - b_2} + f_2 \frac{A - Db_1}{b_3 - b_1} + f_3 D\right\}^2}(1 + o(1)),$$

as $D \to \infty$. Define the constants

$$\lambda = \frac{db_3 - \log T'}{(b_3 - b_1)(b_3 - b_2)}, \qquad \phi = \frac{db_1 b_2 + b_3(\log T' - db_1 - db_2)}{(b_3 - b_1)(b_3 - b_2)},$$

and

$$\gamma = \phi(b_1 + b_2) + \lambda b_1 b_2.$$

Then in particular $\lambda \geq 0$ and (17) implies that $\phi > 0$. We shall consider the behaviour of the real-valued function

$$f(A) = \frac{\lambda A^2 + \gamma D^2}{(\lambda A + \phi D)^2},$$

as A varies over the interval (24). We recall that Δ necessarily vanishes if $p^{\nu_p(\Delta)} > |\Delta|$. Using the identities $f_1 + f_2 + f_3 = d$ and $\sigma(\mathbf{f}) = \log T'$, a straightforward calculation reveals that Δ vanishes if $\log p > (1 + o(1))f(A)$ for any A in the interval (24).

It remains to choose a suitable value of A for which the function $f(A)$ is minimized. In fact, an easy calculation reveals that f has a turning point at $A = \gamma D/\phi$. Moreover, this value of A is contained in the interval (24) precisely when $\phi b_2 < \gamma \leq \phi b_3$. The lower bound here always holds, whereas it is not hard to see that the upper bound is true if and only if (17) holds. Hence it suffices to take

$$p > \exp\left(\frac{db_1 b_2 b_3 + (b_1 b_3 + b_2 b_3 - b_1 b_2)(\log T' - db_1 - db_2)}{(\log T' - db_1)(\log T' - db_2)}(1 + o(1))\right),$$

under this assumption. Therefore (16) is indeed satisfactory, provided that D is chosen to be sufficiently large in terms of ε and d.

3 Equal sums of two powers

Let $k \geq 4$ and $X \geq 1$. We now turn to our estimate for the number $N_k^{(0)}(X)$ of positive non-trivial integral solutions of the Diophantine equation (4), which are contained in the region $\max\{w, x, y, z\} \leq X$. It will suffice to count positive integers w, x, y, z such that $x < y \leq z < w$. For each such solution we define

$$v_1 = z - x, \qquad v_2 = z + x.$$

It follows that

$$1 \leq y < w \leq X, \qquad 1 \leq v_1 < v_2 \leq 2X. \tag{32}$$

Furthermore, under this transformation (4) takes the shape

$$2^{k-1}\{w^k - y^k\} = v_1 f(v_1, v_2), \tag{33}$$

where

$$f(v_1, v_2) = \sum_{0 \leq j < k/2} \binom{k}{2j+1} v_1^{2j} v_2^{k-2j-1} \tag{34}$$

is a binary form of degree $k - 1$. In order to estimate the number of integers w, y, v_1, v_2 such that (32) and (33) hold, we begin by considering the contribution corresponding to a fixed choice of v_1. For this we define

$$\xi = \xi(v_1) = \prod_{p \mid v_1, p > 2} p$$

to be the odd square-free kernel of v_1, and consider the set

$$S = \{(w, y) \in \mathbb{Z}^2 : \xi \mid w^k - y^k\}.$$

Let $(w, y) \in S$ and let p be any prime divisor of ξ. Then we see that either p divides y, or there exist at most k integers $\lambda_1, \ldots, \lambda_t$, say, such that

$$w \equiv \lambda_i y \pmod{p}$$

for some $1 \leq i \leq t$. Collecting these lattice conditions together via the Chinese Remainder Theorem, we therefore conclude that S is a union of $O(k^{\omega(\xi)})$ lattices in $\mathbb{Z}^2$, each of determinant ξ.

We henceforth fix our attention upon those w, y contained in the region (32), which lie in one such lattice Λ, say. By [2, Lemma 1, (iii)] there exist basis vectors $\mathbf{e}^{(1)}, \mathbf{e}^{(2)} \in \Lambda$ with

$$\xi \ll |\mathbf{e}^{(1)}||\mathbf{e}^{(2)}| \ll \xi, \tag{35}$$

and such that whenever we write

$$(w, y) = u_1 \mathbf{e}^{(1)} + u_2 \mathbf{e}^{(2)} \tag{36}$$

for appropriate integers u_1, u_2, we automatically have

$$u_1 \ll X/|\mathbf{e}^{(1)}|, \qquad u_2 \ll X/|\mathbf{e}^{(2)}|. \tag{37}$$

We assume without loss of generality that $|\mathbf{e}^{(1)}| \leq |\mathbf{e}^{(2)}|$, and so

$$|\mathbf{e}^{(1)}|^i |\mathbf{e}^{(2)}|^j \geq (|\mathbf{e}^{(1)}||\mathbf{e}^{(2)}|)^{(i+j)/2} \tag{38}$$

for any choice of $j \geq i \geq 0$.

For each v_1, it suffices to count the number of integers u_1, u_2, v_2 lying in the region defined by (32) and (37), for which

$$g(u_1, u_2) = v_1 f(v_1, v_2),$$

where $g(u_1, u_2)$ is obtained from $2^{k-1}\{w^k - y^k\}$ via the substitution (36). In fact we shall also fix a choice of u_2, and then count the number $M(X; u_2, v_1)$, say, of integers r, s for which $r \ll X/|\mathbf{e}^{(1)}|$, $1 \leq s \leq 2X$, and

$$p(r) = q(s), \tag{39}$$

where $p(r) = g(r, u_2)$ and $q(s) = v_1 f(v_1, s)$.

An important issue here is whether or not the polynomial $p - q$ is absolutely irreducible. But it is not hard to see that (39) is obtained from (4) via an appropriate affine plane section. We now distinguish the projective plane sections of (4) into three distinct types: those producing absolutely irreducible curves of degree k, those that produce a line and an absolutely irreducible curve of degree $k-1$, and finally those that produce a union of absolutely irreducible curves each of degree $\leq k-2$. In the first case it is clear that the corresponding affine plane section is absolutely irreducible. In the second case we may deduce that the polynomial defining the resulting affine curve (39) is either the product of a linear polynomial and an absolutely irreducible polynomial of degree $k-1$, or it is absolutely irreducible of degree $k-1$. The latter possibility is clearly satisfactory, whereas the former possibility implies that $p - q$ has degree k. But then $\deg p = k$ and $\deg q = k-1$, and a result of Schmidt [6, Theorem III.1B] tells us that $p(r) - q(s)$ should be absolutely irreducible.

In the final degenerate case, we may assume that the projective plane section of (39) produces at least two distinct absolutely irreducible curves. Indeed, the existence of any plane section producing precisely one line in (4) would imply the existence of a singular point on the surface. Now we know by the previously discussed result of Colliot-Thélène [2, Appendix] that (4) contains finitely many plane curves of degree $\leq k-2$. It follows that there can only be $O(1)$ projective plane sections which produce two distinct absolutely irreducible curves of degree $\leq k-2$. Recall from the introduction that any absolutely irreducible plane curve of degree d contains $O(X^{2/d+\varepsilon})$ rational points of height at most X. Since trivial integral solutions to (4) correspond to rational points lying on projective lines in the surface, we therefore conclude that there is a total contribution of $O(X^{1+\varepsilon})$ to $N_k^{(0)}(X)$, from those affine plane sections of (4) which lead to reducible curves

(39). This is clearly satisfactory for Theorem 2, and we may assume henceforth that $p-q$ is absolutely irreducible.

In order to estimate $M(X;u_2,v_1)$, we shall apply (3) to $p(r)-q(s)$. In view of the shape (34) that f takes, it is apparent that $q(s)$ contains the monomial s^{k-1} with non-zero coefficient. Taking $P_2 \ll X/|\mathbf{e}^{(1)}|$ and $P_3 = 2X$ in (3), we see that $T \gg X^{k-1}$ and hence

$$M(X;u_2,v_1) \ll X^{1/(k-1)+\varepsilon}|\mathbf{e}^{(1)}|^{-1/(k-1)}.$$

Summing over the values of $u_2 \ll X/|\mathbf{e}^{(2)}|$ in (37) we therefore obtain the contribution

$$\begin{aligned} &\ll \frac{X^{1+1/(k-1)+\varepsilon}}{|\mathbf{e}^{(1)}|^{1/(k-1)}|\mathbf{e}^{(2)}|} \\ &\ll (\xi^{-1/2}X)^{1+1/(k-1)+\varepsilon}, \end{aligned} \tag{40}$$

via (38) and (35). Let $Y \geq 1$, and write $A_\varepsilon = (1-2^{-\varepsilon})^{-1}$ for a fixed choice of $\varepsilon > 0$. Then for any $\theta \leq 1$ we have

$$\begin{aligned} \sum_{n\leq Y} \xi(n)^{-\theta} &\leq \sum_{n\leq Y} \xi(n)^{-\theta}\left(\frac{Y}{n}\right)^{1-\theta+\varepsilon} \\ &= Y^{1-\theta+\varepsilon}\sum_{n\leq Y}\xi(n)^{-\theta}n^{\theta-1-\varepsilon} \\ &\leq Y^{1-\theta+\varepsilon}\sum_{n=1}^{\infty}\xi(n)^{-\theta}n^{\theta-1-\varepsilon} \\ &\leq Y^{1-\theta+\varepsilon}\prod_p\left\{1+p^{-\theta}p^{\theta-1-\varepsilon}+p^{-\theta}p^{2\theta-2-2\varepsilon}+\ldots\right\} \\ &= Y^{1-\theta+\varepsilon}\prod_p\left\{1+p^{-\theta}\frac{p^{\theta-1-\varepsilon}}{1-p^{\theta-1-\varepsilon}}\right\} \\ &\leq Y^{1-\theta+\varepsilon}\prod_p\left\{1+p^{-1-\varepsilon}A_\varepsilon\right\} \\ &= c_\varepsilon Y^{1-\theta+\varepsilon}, \end{aligned}$$

say. Upon taking $\theta = \frac{1}{2}(1+1/(k-1))$, so that $\theta \leq 1$ for every $k \geq 2$, it therefore follows from (40) that

$$\begin{aligned} N_k^{(0)}(X) &\ll X^{1+1/(k-1)+\varepsilon}\sum_{v_1<2X}\xi(v_1)^{-\theta} \\ &\ll X^{3/2+1/(2k-2)+\varepsilon}. \end{aligned}$$

This completes the proof of Theorem 2.

References

[1] T.D. Browning, Sums of four biquadrates, *Math. Proc. Camb. Phil. Soc.,* 134 (2003), 385–395.

[2] D.R. Heath-Brown, The density of rational points on curves and surfaces, *Annals of Math.,* 155 (2002), 553-595.

[3] D.R. Heath-Brown, *C.I.M.E. Lecture Notes,* to appear.

[4] C. Hooley, On another sieve method and the numbers that are a sum of two h-th powers, *Proc. London Math. Soc. (3),* 43 (1981), 73-109.

[5] C. Hooley, On another sieve method and the numbers that are a sum of two h-th powers. II, *J. Reine Angew. Math.,* 475 (1996), 55-75.

[6] W.M. Schmidt, *Diophantine Approximations and Diophantine Equations,* Lecture Notes in Math., 1467 (Springer-Verlag, 1991).