EFFICIENT CONGRUENCING IN ELLIPSEPHIC SETS: THE QUADRATIC CASE

KIRSTI D. BIGGS

Abstract. In this paper, we bound the number of solutions to a quadratic Vinogradov system of equations in which the variables are required to satisfy digital restrictions in a given base. Certain sets of permitted digits, namely those giving rise to few representations of natural numbers as sums of elements of the digit set, allow us to obtain better bounds than would be possible using the size of the set alone. In particular, when the digits are required to be squares, we obtain diagonal behaviour with 12 variables.

1. Introduction

Vinogradov's mean value theorem seeks to bound the number of solutions, for a fixed integer $k \geq 2$, to the system of Diophantine equations

$$x_1^j + \cdots + x_s^j = y_1^j + \cdots + y_s^j, \quad (1 \leq j \leq k), \tag{1.1}$$

where $1 \leq x_i, y_i \leq X$ for all i. In this paper, we investigate variants of this problem in which the variables are restricted to certain subsets of the natural numbers which give us significantly stronger control over the associated mean value estimates. Specifically, the subsets of interest to us are defined by digital restrictions—further discussion requires some definitions.

Fix a prime $p > 2$ and a subset $A \subset \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ with the property that

$$\#\{(a_1, \ldots, a_t) \in A^t \mid a_1 + \cdots + a_t = n\} \ll n^\delta \tag{1.2}$$

for some $t \geq 2$ and some $\delta > 0$, and let

$$\mathcal{E} = \mathcal{E}_p^A = \{n \in \mathbb{N} \mid n = \textstyle\sum_i a_i p^i, a_i \in A \cap [0, p-1] \text{ for all } i\} \tag{1.3}$$

be the set of natural numbers whose base p expansion includes only digits from A. Write A_p for $A \cap [0, p-1]$, and assume that $2 \leq \#A_p \leq p-1$. Let $I_s(X) = I_{s,2}(X)$ be the number of solutions to (1.1) in the case $k = 2$ with $x_i, y_i \in \mathcal{E}(X) = \mathcal{E} \cap [1, X]$ for all i, and write Y for $\#\mathcal{E}(X)$.

Theorem 1.1. *We have*

$$I_s(X) \ll X^{3\delta+\epsilon}(Y^s + Y^{2s-3t}).$$

2010 *Mathematics Subject Classification.* 11A63, 11D45, 11L07, 11P55.

Key words and phrases. Hardy–Littlewood method, efficient congruencing, missing digits.

This paper is based on work appearing in the author's PhD thesis [3] at the University of Bristol, and supported by EPSRC Doctoral Training Partnership EP/M507994/1.

An estimate for the count of solutions to the Vinogradov system (1.1) in the case $k = 2$ follows from the quadratic identity

$$(a + b - c)^2 - (a^2 + b^2 - c^2) = 2(a - c)(b - c)$$

and a standard bound for the divisor function, while recent progress has led to an optimal upper bound in the case of general k. When $k = 3$, this bound was proved by Wooley in [14], and when $k \geq 4$, by Bourgain, Demeter and Guth in [6], using the l^2-decoupling method, and subsequently by Wooley in [15], using the nested efficient congruencing method. These two methods are held to be, respectively, real and p-adic analogues of each other—see [12] for further discussion of this.

We call our set (1.3)—or, interchangeably, its elements—ellipsephic. This terminology mimics the word *ellipséphique*, used in the French mathematical literature to denote integers with missing digits—for example, by Aloui in [1], and by Aloui, Mauduit and Mkaouar in [2]. The term was coined by Mauduit (see the discussion on page 12 of [7]), although such integers were already studied prior to its introduction.

Writing $r = \#A_p$ for the number of permitted digits, we observe that the cases $r = 0$ and $A_p = \{0\}$ are trivial, and the case $r = p$ reduces to the classical case, while when $r = 1$ (and $A_p \neq \{0\}$), we see that $\mathcal{E}$ has different behaviour, with $\#\mathcal{E}(X) \approx \log_p X$. Consequently, we implement the restriction mentioned above that $2 \leq r \leq p - 1$, and note that

$$\#\mathcal{E}(X) \ll r^{\log_p X + 1} = rX^{\log_p r},$$

and consequently that $\mathcal{E}$ is a thin subset of the integers, in the sense that

$$\lim_{X \to \infty} \frac{\#\mathcal{E}(X)}{X} = 0.$$

We observe that ellipsephic sets have a self-similar, fractal-like structure, with the digital restrictions seen here reminiscent of those in the classical Cantor set. They bear a resemblance to certain real fractal subsets studied by Łaba and Pramanik in [9], for which those authors study maximal operators.

The bounds we obtain in this paper are heavily dependent on the additive structure of the digit set A, in a way which we expand on here. A generalised Sidon set, or $B_h[g]$-set, is a subset of the natural numbers in which there are at most g representations of a given $n \in \mathbb{N}$ as the sum of h elements of the set, where representations are counted up to permutation. The sets we are interested in, as suggested earlier in this section by the condition (1.2), can be considered as a further generalisation of this concept.

For $t \geq 2$ an integer, we call a set $A \subset \mathbb{N}_0$ an $E_t(\delta)$-set if (1.2) holds for $\delta > 0$ a real number, and we call A an E_t^*-set if (1.2) holds for all $\delta > 0$. Hypothesis K, formulated by Hardy and Littlewood in [8], states that for all $k \geq 2$, the set of kth powers should be an E_k^*-set. This is known to be true for $k = 2$ (Landau, in [10]), known to be false for $k = 3$ (Mahler, in [11]), and open for $k \geq 4$. The set of squares forms a key motivating example for this work, and

in discussing our results below, we present the special case of square digits as a corollary.

In [13], Vu showed that for fixed k, there exists a subset S_k of the set of kth powers and an integer t_k such that S_k is an $E^*_{t_k}$-set. This proves the existence of infinitely many sets of the form we are interested in, although the argument is probabilistic, so does not exhibit such sets directly.

We refer to a set $\mathcal{E} = \mathcal{E}_p^A$ as a (p,t,δ)-ellipsephic set if A is an $E_t(\delta)$-set, and as a $(p,t)^*$-ellipsephic set if A is an E_t^*-set. We now introduce some further notation to allow us to state the more general case of our main result. For a sequence $\mathfrak{a} = (\mathfrak{a}_x)_{x\in\mathcal{E}}$ of complex weights, we let

$$J_s(X) = J_{s,2}(X;\mathfrak{a}) = \oint \Big| \sum_{x\in\mathcal{E}(X)} \mathfrak{a}_x e(\alpha_1 x + \alpha_2 x^2)\Big|^{2s} d\boldsymbol{\alpha},$$

where $e(z)$ is shorthand for $e^{2\pi iz}$, and $\oint$ denotes the integral over the unit square $[0,1]^2$. Then $J_s(X)$ counts the solutions, in positive integers $x_i, y_i \in \mathcal{E}(X)$, to the system

$$x_1^j + \cdots + x_s^j = y_1^j + \cdots + y_s^j, \quad (1 \le j \le 2), \tag{1.4}$$

where each solution is counted with weight $\mathfrak{a}_{\boldsymbol{x}}\overline{\mathfrak{a}_{\boldsymbol{y}}} = \mathfrak{a}_{x_1}\dots\mathfrak{a}_{x_s}\overline{\mathfrak{a}_{y_1}\dots\mathfrak{a}_{y_s}}$. We adopt the convention throughout that statements involving ϵ hold for any suitably small choice of $\epsilon > 0$, and as such the exact value may change from line to line. The vector notation $\boldsymbol{x} \equiv \xi \pmod q$ means that $x_i \equiv \xi \pmod q$ for all i, and $\boldsymbol{x} \equiv \boldsymbol{y} \pmod q$ means that $x_i \equiv y_i \pmod q$ for all i.

Our main theorem provides the following upper bound for $J_s(X)$.

Theorem 1.2. *For $t \ge 2$ an integer, $\delta > 0$ a real number, and $p > 2$ a prime, let $\mathcal{E}$ be a (p,t,δ)-ellipsephic set and let $Y = \#\mathcal{E}(X)$. Then for $s \ge 3t$, we have*

$$J_s(X) \ll Y^{s-3t}X^{3\delta+\epsilon}\bigg(\sum_{x\in\mathcal{E}(X)} |\mathfrak{a}_x|^2\bigg)^s.$$

When $\mathcal{E}$ is a $(p,t)^*$-ellipsephic set, we therefore have

$$J_s(X) \ll Y^{s-3t}X^{\epsilon}\bigg(\sum_{x\in\mathcal{E}(X)} |\mathfrak{a}_x|^2\bigg)^s.$$

Note that it follows from a standard application of Hölder's inequality that for $s \le 3t$, we have

$$J_s(X) \ll X^{\delta s/t+\epsilon}\bigg(\sum_{x\in\mathcal{E}(X)} |\mathfrak{a}_x|^2\bigg)^s.$$

Corollary 1.3. *Theorem 1.1 is true.*

Proof. This is the case where $\mathfrak{a}_x = 1$ for all $x \in \mathcal{E}(X)$. □

Corollary 1.4. *In the case where $\mathcal{E} = \mathcal{E}_p^{A_2}$, with $A_2 = \{n^2 \mid n \in \mathbb{N}_0\}$, we have that for $s \geq 6$,*

$$J_s(X) \ll Y^{s-6}X^{\epsilon}\bigg(\sum_{x\in\mathcal{E}(X)} |\mathfrak{a}_x|^2\bigg)^s,$$

and in the unweighted case,

$$J_s(X) \ll Y^{2s-6}X^{\epsilon} \ll Y^{2s-6+\epsilon}.$$

At the critical case $s = 6$, this yields

$$J_6(X) \ll Y^{6+\epsilon}. \tag{1.5}$$

Proof. As mentioned above, A_2 is an E_2^*-set, and the result follows from Theorem 1.2. □

The best upper bound which could previously be obtained for $J_s(X)$ is a consequence of a result of Bourgain in [5]. Taking $\mathfrak{a}_x = 0$ for $x \notin \mathcal{E}$ in that theorem yields, for $s \geq 3$,

$$J_s(X) \ll Y^{s-3}X^{\epsilon}\bigg(\sum_{x\in\mathcal{E}(X)} |\mathfrak{a}_x|^2\bigg)^s,$$

and in the particular case of square digits, this corresponds, in the unweighted case, to

$$J_6(X) \ll Y^{9+\epsilon},$$

so, by comparison with (1.5), we see that a power saving in Y has been obtained by accounting for the specific structure of our ellipsephic sets, rather than just their density.

The proof of Theorem 1.2 uses a version of Wooley's efficient congruencing method which we outline briefly here. We begin by postulating that $J_s(X)$ is significantly larger than the bound asserted in Theorem 1.2, and proceed to derive a contradiction. We partition our variables into congruence classes modulo powers of the base p, and apply Hölder's inequality to restrict our variables to lie in certain common congruence classes. The binomial theorem allows us to convert our equations into congruences featuring a subset of our variables, and using their ellipsephic nature and the $E_t(\delta)$ property, we can "lift" solutions to these congruences, at a small cost, to diagonal solutions in which each pair of variables is mutually congruent modulo the relevant power of p. Iterating this process, we strengthen the congruences satisfied by these variables—this may be viewed as a "p-adic concentration" argument, since our variables become closer p-adically. By iterating sufficiently many times, we find that our initial assumption on $J_s(X)$ is untenable, which leads us to a contradiction.

We would expect the full nested efficient congruencing method, as presented in [15], to deliver appropriate bounds for the ellipsephic version of any other system to which these techniques apply. In particular, the author has recently obtained the equivalent result, in the case of E_t^*-sets, for the number of ellipsephic solutions to (1.1) in the general case $k \geq 3$, which appears in [4].

Nevertheless, we believe that the level of detail included in this paper, as well as the treatment of the more general $E_t(\delta)$-sets, merits a full and separate presentation.

Theorem 1.2 has potential applications to a number of Diophantine problems, most notably Waring's problem, in which we attempt to write all natural numbers as sums of a bounded number of squares of ellipsephic integers. A more tractable form of this problem is to seek solutions to

$$n = x_1^2 + \cdots + x_s^2 + y^2,$$

with $x_1, \dots, x_s \in \mathcal{E}$ and $y \in \mathbb{N}_0$, which will form a subject for our future work.

As a corollary of Theorem 1.2, we provide a lower bound on the number of integers representable in the form required by Waring's problem. We would expect to need the set $\mathcal{E}(X)$ to be sufficiently large to give any chance of being able to represent a significant proportion of the integers up to X, and as such we incorporate this as an extra condition in the below result.

Let $N_s(X) = N_{s,2}^{\mathcal{E}}(X)$ be the number of integers n with $1 \le n \le X$ which have a representation as a sum of s squares of integers from $\mathcal{E}$.

Corollary 1.5. *For $t \ge 2$ an integer and $p > 2$ a prime, let $\mathcal{E}$ be a (p, t, δ)-ellipsephic set for some $\delta > 0$. Assume that $Y = \#\mathcal{E}(X) \gg X^{1/t}$. Then for $s \ge 3t$ we have*

$$N_s(X) \gg X^{1-3\delta/2-\epsilon}.$$

In the case where $\mathcal{E}$ is a $(p,t)^*$-ellipsephic set, such as in the case of square digits described in Corollary 1.4, we therefore have $N_s(X) \gg X^{1-\epsilon}$.

Proof. Using Cauchy's inequality, and writing $R(n) = R_{s,2}^{\mathcal{E}}(n)$ for the number of representations of an integer n as a sum of s squares of integers from $\mathcal{E}$, we have

$$\begin{aligned}\Big(\sum_{1\le n\le X} R(n)\Big)^2 &\le \Big(\sum_{\substack{1\le n\le X\\ R(n)>0}} 1\Big)\Big(\sum_{1\le n\le X} R(n)^2\Big)\\ &= N_s(X)\Big(\sum_{1\le n\le X} R(n)^2\Big). \qquad (1.6)\end{aligned}$$

We note that

$$\begin{aligned}\Big(\sum_{1\le n\le X} R(n)\Big)^2 &\ge \big(\#\mathcal{E}(\sqrt{X/s})^s\big)^2\\ &\gg Y^s,\end{aligned}$$

and, using Theorem 1.2, that

$$\begin{aligned}\Big(\sum_{1\le n\le X} R(n)^2\Big) &\ll X^{1/2} J_s(X^{1/2})\\ &\ll X^{1/2}(Y^{1/2})^{2s-3t}(X^{1/2})^{3\delta+\epsilon}\\ &= Y^{s-3t/2}(X^{1/2})^{1+3\delta+\epsilon}.\end{aligned}$$

Combining these bounds with (1.6), we see that

$$N_s(X) \gg Y^{3t/2}(X^{-1/2})^{1+3\delta+\epsilon},$$

and our additional assumption on the size of Y allows us to conclude that

$$N_s(X) \gg X^{1-3\delta/2-\epsilon},$$

as required. □

In Section 2 of this paper, we provide a series of preliminary results which form the basis of our iteration process, and in Section 3 we complete the proof of Theorem 1.2.

The author would like to thank Trevor Wooley for his supervision and for suggesting this line of research.

2. Preliminaries

We recall that we are interested in the integral

$$J(X) = J_{s,2}(X; \mathfrak{a}) = \oint \Big| \sum_{x \in \mathcal{E}(X)} \mathfrak{a}_x e(\alpha_1 x + \alpha_2 x^2) \Big|^{2s} d\boldsymbol{\alpha},$$

which counts the number of solutions to (1.4) where each solution is counted with weight $\mathfrak{a}_{\boldsymbol{x}}\overline{\mathfrak{a}_{\boldsymbol{y}}} = \mathfrak{a}_{x_1} \dots \mathfrak{a}_{x_s}\overline{\mathfrak{a}_{y_1} \dots \mathfrak{a}_{y_s}}$. We first observe that the case $s > 3t$ of Theorem 1.2 follows directly from the case $s = 3t$, and so we work only in this latter case throughout. We also note that it suffices to prove Theorem 1.2 for X a power of p because, for $p^{C-1} < X < p^C$, we then have

$$J(X) \ll J(p^C) \ll (pX)^{3\delta+\epsilon}\bigg(\sum_{x \in \mathcal{E}(p^C)} |\mathfrak{a}_x|^2 \bigg)^s$$

for any choice of $\mathfrak{a}$, and so

$$J(X) \ll X^{3\delta+\epsilon}\bigg(\sum_{x \in \mathcal{E}(X)} |\mathfrak{a}_x|^2 \bigg)^s,$$

since we may assume that $\mathfrak{a}_x = 0$ for $x > X$.

We apply the following normalisation. Let

$$\rho_0 = \bigg(\sum_{x \in \mathcal{E}(X)} |\mathfrak{a}_x|^2 \bigg)^{1/2},$$

and for any $\boldsymbol{\alpha} \in [0,1]^2$, let

$$f(\boldsymbol{\alpha}) = f(\boldsymbol{\alpha}; \mathfrak{a}) = \rho_0^{-1} \sum_{x \in \mathcal{E}(X)} \mathfrak{a}_x e(\alpha_1 x + \alpha_2 x^2),$$

and define the normalised mean value

$$\mathfrak{J}(X) = \mathfrak{J}_{s,2}(X; \mathfrak{a}) = \oint \big| f(\boldsymbol{\alpha}; \mathfrak{a}) \big|^{2s} d\boldsymbol{\alpha} = \rho_0^{-2s} J(X).$$

Note that this normalisation allows us to assume that $|\mathfrak{a}_x| \leq 1$ for all $x \in \mathcal{E}$. We may also restrict ourselves to the situation in which our weights are real

and non-negative, as follows. Let $\mathfrak{a}_x = \mathfrak{b}_x^+ - \mathfrak{b}_x^- + i\mathfrak{c}_x^+ - i\mathfrak{c}_x^-$, where $\mathfrak{b}_x^+, \mathfrak{b}_x^-, \mathfrak{c}_x^+$ and $\mathfrak{c}_x^-$ are non-negative real numbers, with at most one of $\mathfrak{b}_x^+$ and $\mathfrak{b}_x^-$ non-zero, and at most one of $\mathfrak{c}_x^+$ and $\mathfrak{c}_x^-$ non-zero. Write

$$g_1(\boldsymbol{\alpha}) = \sum_{x\in\mathcal{E}(X)} \mathfrak{b}_x^+ e(\alpha_1 x + \alpha_2 x^2), \qquad g_2(\boldsymbol{\alpha}) = \sum_{x\in\mathcal{E}(X)} \mathfrak{b}_x^- e(\alpha_1 x + \alpha_2 x^2),$$
$$g_3(\boldsymbol{\alpha}) = \sum_{x\in\mathcal{E}(X)} \mathfrak{c}_x^+ e(\alpha_1 x + \alpha_2 x^2), \qquad g_4(\boldsymbol{\alpha}) = \sum_{x\in\mathcal{E}(X)} \mathfrak{c}_x^- e(\alpha_1 x + \alpha_2 x^2),$$

and observe that

$$\sum_{x\in\mathcal{E}(X)} \mathfrak{a}_x e(\alpha_1 x + \alpha_2 x^2) = g_1(\boldsymbol{\alpha}) - g_2(\boldsymbol{\alpha}) + ig_3(\boldsymbol{\alpha}) - ig_4(\boldsymbol{\alpha}) = \sum_{j=1}^{4} \epsilon_j g_j(\boldsymbol{\alpha}),$$

where we have chosen $\epsilon_j \in \{\pm 1, \pm i\}$ appropriately. By Hölder's inequality, we now split up the integrals we are interested in into the parts corresponding to each of these weights, to see that

$$\oint \Big| \sum_{x\in\mathcal{E}(X)} \mathfrak{a}_x e(\alpha_1 x + \alpha_2 x^2) \Big|^{2s} d\boldsymbol{\alpha} = \oint \Big| \sum_{j=1}^{4} \epsilon_j g_j(\boldsymbol{\alpha}) \Big|^{2s} d\boldsymbol{\alpha} \ll \max_j \oint \big|g_j(\boldsymbol{\alpha})\big|^{2s} d\boldsymbol{\alpha},$$

and that since $|\mathfrak{b}_x^\pm|, |\mathfrak{c}_x^\pm| \le |\mathfrak{a}_x|$, we obtain the required bounds for general weights from those for real, non-negative weights as claimed. We let

$$\mathbb{D} = \{\mathfrak{a} \mid \mathfrak{a}_x \in [0,1] \text{ for all } x \in \mathcal{E}\},$$

and from now on we work with $\mathfrak{a} \in \mathbb{D}$.

With the above normalisation, we see that an estimate of the desired form

$$J(X) \ll X^{\Delta} \Big(\sum_{x\in\mathcal{E}(X)} |\mathfrak{a}_x|^2 \Big)^s,$$

for some $\Delta > 0$, follows directly from one of the form

$$\mathfrak{J}(X) \ll X^{\Delta}.$$

We define

$$\lambda = \sup_{\mathfrak{a}\in\mathbb{D}} \limsup_{X\to\infty} \frac{\log \mathfrak{J}(X;\mathfrak{a})}{\log X}.$$

An application of the Cauchy–Schwarz inequality gives us the trivial bound $\lambda \le s$. Taking into account the expected value of λ, we define $\Lambda = \lambda - 3\delta$ for ease of notation.

We introduce a series of interdependent constants which come into play during the proof of Theorem 1.2 and the results of this section. Let $\epsilon_0 > 0$, and suppose $\Lambda > \epsilon_0$. This is the assumption which we ultimately contradict in Section 3.

Let $n = \lceil 16t/\Lambda \rceil$, which will be the number of iterations of the main process in Section 3, and note that the existence and size of n is dependent on our assumption that Λ is bounded away from zero. While we would usually expect it to be significantly larger, we certainly have $n \ge 5$. Let $\iota = \lambda/2^{2n+3}$, and observe that by the definition of λ, there exists a sequence $(X_m)_{m=1}^{\infty}$ tending

to infinity with the property that for some $\mathfrak{a} \in \mathbb{D}$, and for large enough m, we have

$$\mathfrak{J}(X_m; \mathfrak{a}) > X_m^{\lambda-\iota}.$$

Henceforth, we work with a choice of $\mathfrak{a} \in \mathbb{D}$ satisfying this condition. In addition, for any $\mathfrak{b} \in \mathbb{D}$, we have

$$\mathfrak{J}(X; \mathfrak{b}) \ll X^{\lambda+\iota}.$$

Suppose that $X = p^B$, where $B \in \mathbb{N}$ is a large parameter which satisfies $B \geq 2^{n+3}$ and also ensures that X is sufficiently large with regards to the sequence (X_m). The proof of our main theorem features ν preliminary steps to handle solutions in which variables are congruent modulo small powers of p, as well as an initialisation step of size p^u, where ν and u are large in some respects, but small in relation to B. Specifically, let $\nu = \lceil B/2^{2n+2} \rceil$ and $u = \lceil B/2^{n+2} \rceil$. We record two further bounds which will come into play in Section 3. We have

$$\begin{aligned} 2^n(u+1) + \nu - 1 &\leq B/4 + 2^{n+1} + B/2^{2n+2} \\ &\leq B/2 + B/2^{2n+2} < B, \end{aligned} \tag{2.1}$$

and

$$\begin{aligned} 2tu - \nu &\geq 2tB/2^{n+2} - B/2^{2n+2} - 1 \\ &\geq (2^{n+1}t - 1 - 2^{n-1})B/2^{2n+2} \\ &> \lambda B/2^{2n+2} = 2\iota B. \end{aligned} \tag{2.2}$$

Our work is heavily dependent on the partition of our variables into congruence classes modulo various powers of the base prime p, and we therefore wish to define the restriction of $f(\boldsymbol{\alpha})$ to such classes. For $a \in \mathbb{N}$ and $\xi \in \mathcal{E}(p^a)$, let

$$\rho_a(\xi) = \bigg(\sum_{\substack{x \in \mathcal{E}(X) \\ x \equiv \xi \ (\mathrm{mod}\ p^a)}} \mathfrak{a}_x^2 \bigg)^{1/2}$$

and

$$f_a(\boldsymbol{\alpha}, \xi) = \rho_a(\xi)^{-1} \sum_{\substack{x \in \mathcal{E}(X) \\ x \equiv \xi \ (\mathrm{mod}\ p^a)}} \mathfrak{a}_x e(\alpha_1 x + \alpha_2 x^2).$$

For convenience, we let $\rho_0(\xi) = \rho_0$ and $f_0(\boldsymbol{\alpha}, \xi) = f(\boldsymbol{\alpha})$ for any ξ. We observe that for any $a \in \mathbb{N}$, we have

$$\sum_{\xi \in \mathcal{E}(p^a)} \rho_a(\xi)^2 = \rho_0^2, \tag{2.3}$$

and more generally, for $a, b \in \mathbb{N}$ with $a \leq b$,

$$\sum_{\substack{\xi' \in \mathcal{E}(p^b) \\ \xi' \equiv \xi \ (\mathrm{mod}\ p^a)}} \rho_b(\xi')^2 = \rho_a(\xi)^2.$$

Our first lemma provides a useful upper bound required for completion of the proof of Theorem 1.2.

Lemma 2.1. *For $a \in \mathbb{N}$ with $p^a < X$, we have*

$$\oint |f_a(\boldsymbol{\alpha}, \xi)|^{6t}\, d\boldsymbol{\alpha} \ll (X/p^a)^{\lambda+\iota}.$$

Proof. The above integral counts solutions to the system

$$\sum_{i=1}^{3t}(x_i^2 - y_i^2) = 0 = \sum_{i=1}^{3t}(x_i - y_i)$$

with $x_i, y_i \in \mathcal{E}(X)$ for $1 \le i \le 3t$ and $\boldsymbol{x} \equiv \boldsymbol{y} \equiv \xi \pmod{p^a}$, where solutions are counted with weight $\mathfrak{a}_{\boldsymbol{x}}\mathfrak{a}_{\boldsymbol{y}}\rho_a(\xi)^{-6t}$. Writing $x_i = p^a z_i + \xi$ and $y_i = p^a w_i + \xi$ for $1 \le i \le 3t$, and defining a new set of weights $\mathfrak{b}_z = \rho_a(\xi)^{-1}\mathfrak{a}_{p^a z+\xi}$, we can reinterpret the above system in the form

$$\sum_{i=1}^{3t}(z_i^2 - w_i^2) = 0 = \sum_{i=1}^{3t}(z_i - w_i)$$

with $z_i, w_i \in \mathcal{E}\big((X-\xi)/p^a\big)$ for $1 \le i \le 3t$ and solutions counted with weight $\mathfrak{b}_{\boldsymbol{z}}\mathfrak{b}_{\boldsymbol{w}}$. By definition, this is $\mathfrak{J}\big((X-\xi)/p^a; \mathfrak{b}\big)$, and consequently we have

$$\oint |f_a(\boldsymbol{\alpha}, \xi)|^{6t}\, d\boldsymbol{\alpha} \ll \mathfrak{J}(X/p^a; \mathfrak{b}) \ll (X/p^a)^{\lambda+\iota}. \qquad \square$$

We want to count solutions to congruences modulo some power p^c in the way that we count solutions to equations, via orthogonality, and as such, we make use of Wooley's notation

$$\oint_{p^c} F(\alpha)\, d\alpha = p^{-c} \sum_{1 \le u \le p^c} F(u/p^c),$$

and observe that $\oint_{p^c} |f(\boldsymbol{\alpha})|^{2s}\, d\boldsymbol{\alpha}$ counts the number of solutions to the system

$$\sum_{i=1}^{s}(x_i^j - y_i^j) \equiv 0 \pmod{p^c}, \quad (j = 1, 2)$$

with $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}(X)^s$, weighted by $\mathfrak{a}_{\boldsymbol{x}}\mathfrak{a}_{\boldsymbol{y}}\rho_0^{-2s}$.

The next lemma provides the key "lifting" step of the process, in which we make use of the $E_t(\delta)$ property of our digit set to raise the power of p used in our congruences. In preparation for this, for $c, d \in \mathbb{N}_0$ with $c \le d$, weights $\mathfrak{b} = (\mathfrak{b}_x)_{x \in \mathcal{E}}$ with $|\mathfrak{b}_x| \le 1$ for all $x \in \mathcal{E}$, and $\boldsymbol{z} \in \mathcal{E}(p^c)^t$, we define

$$G_{c,d}(\boldsymbol{z}) = G_{c,d}(\boldsymbol{z}, \mathfrak{b}) = \oint_{p^d} \Bigg| \sum_{\substack{\boldsymbol{x} \in \mathcal{E}(X)^t \\ \boldsymbol{x} \equiv \boldsymbol{z} \pmod{p^c}}} \mathfrak{b}_{\boldsymbol{x}} e\big(\beta(x_1 + \cdots + x_t)\big) \Bigg|^2 d\beta,$$

which counts solutions to the congruence

$$\sum_{i=1}^{t} x_i \equiv \sum_{i=1}^{t} y_i \pmod{p^d} \tag{2.4}$$

with $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}(X)^t$ and $\boldsymbol{x} \equiv \boldsymbol{y} \equiv \boldsymbol{z} \pmod{p^c}$, with weight $\mathfrak{b}_{\boldsymbol{x}}\overline{\mathfrak{b}_{\boldsymbol{y}}}$.

We now show that, up to a small cost, the number of such solutions is essentially controlled by the case in which $\boldsymbol{x} \equiv \boldsymbol{y} \pmod{p^d}$.

Lemma 2.2. *We have*

$$G_{c,d}(\boldsymbol{z}) \ll p^{\delta(d-c)} \sum_{\substack{\boldsymbol{u} \in \mathcal{E}(p^d)^t \\ \boldsymbol{u} \equiv \boldsymbol{z} \ (mod\ p^c)}} \Big| \sum_{\substack{\boldsymbol{x} \in \mathcal{E}(X)^t \\ \boldsymbol{x} \equiv \boldsymbol{u} \ (mod\ p^d)}} \mathfrak{b}_{\boldsymbol{x}} \Big|^2.$$

Proof. For $1 \le i \le t$, let

$$x_i = z_i + \sum_{r \ge c} x_i^{(r)} p^r$$

and

$$y_i = z_i + \sum_{r \ge c} y_i^{(r)} p^r,$$

with $x_i^{(r)}, y_i^{(r)} \in A_p$ for $1 \le i \le t$ and $r \ge c$. We bound the number of solutions to (2.4) by considering each base p digit in turn. Let

$$\mathcal{A}_t(h) = \left\{ \boldsymbol{u} \in A_p^t \;\middle|\; \sum_{i=1}^{t} u_i = h \right\},$$

and

$$\widetilde{\mathcal{A}}_t(h) = \left\{ (\boldsymbol{u}, \boldsymbol{v}) \in A_p^{2t} \;\middle|\; \sum_{i=1}^{t} (u_i - v_i) = h \right\}.$$

Summing the lowest digits which interest us (namely, those corresponding to the p^c term in the base p expansion of our variables), we see that a solution of (2.4) satisfies

$$(\boldsymbol{x}^{(c)}, \boldsymbol{y}^{(c)}) \in \widetilde{\mathcal{A}}_t(\lambda_c p)$$

for some $1 - t \le \lambda_c \le t - 1$. Accounting for this carry-over, and moving on to the next highest digits, we then see that

$$(\boldsymbol{x}^{(c+1)}, \boldsymbol{y}^{(c+1)}) \in \widetilde{\mathcal{A}}_t(\lambda_{c+1} p - \lambda_c)$$

for some $1 - t \le \lambda_{c+1} \le t - 1$. Continuing this process, and setting $\lambda_{c-1} = 0$ for convenience, we obtain the system

$$(\boldsymbol{x}^{(r)}, \boldsymbol{y}^{(r)}) \in \widetilde{\mathcal{A}}_t(\lambda_r p - \lambda_{r-1}), \quad (c \le r \le d-1).$$

For brevity, we use the notation $\underline{\boldsymbol{u}}$ to denote the tuple $(\boldsymbol{u}^{(c)}, \dots, \boldsymbol{u}^{(d-1)})$—this represents a regrouping of our variables by digit—and similarly we use $(\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}})$ for $\Big((\boldsymbol{u}^{(c)}, \boldsymbol{v}^{(c)}), \dots, (\boldsymbol{u}^{(d-1)}, \boldsymbol{v}^{(d-1)}) \Big)$.

We write

$$\mathcal{A}_t(\boldsymbol{h}) = \left\{ \underline{\boldsymbol{u}} \in A_p^{t(d-c)} \;\middle|\; \boldsymbol{u}^{(r)} \in \mathcal{A}_t(h_r) \text{ for } c \le r \le d-1 \right\}$$

and

$$\widetilde{\mathcal{A}}_t(\boldsymbol{h}) = \left\{ (\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}}) \in A_p^{2t(d-c)} \;\middle|\; (\boldsymbol{u}^{(r)}, \boldsymbol{v}^{(r)}) \in \widetilde{\mathcal{A}}_t(h_r) \text{ for } c \le r \le d-1 \right\},$$

and observe that these are the sets of all possible variables with given digit sums. By convention, we suppose that for any $\underline{\boldsymbol{u}} = (\boldsymbol{u}^{(c)}, \dots, \boldsymbol{u}^{(d-1)}) \in \mathcal{A}_t(\boldsymbol{h})$, we have $u_i = z_i + \sum_{c \le r \le d-1} u_i^{(r)} p^r$ and write $\boldsymbol{u} = (u_1, \dots, u_t)$, and similarly for $(\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}}) \in \widetilde{\mathcal{A}}_t(\boldsymbol{h})$.

For $\boldsymbol{\lambda} = (\lambda_c, \dots, \lambda_{d-1}) \in \{1-t, \dots, t-1\}^{d-c}$, we write

$$\boldsymbol{\lambda}' = (\lambda_c p - \lambda_{c-1}, \dots, \lambda_{d-1} p - \lambda_{d-2}).$$

We are now in a position to observe that

$$G_{c,d}(\boldsymbol{z}) = \sum_{\boldsymbol{\lambda} \in \{1-t,\dots,t-1\}^{d-c}} \sum_{(\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}}) \in \widetilde{\mathcal{A}}_t(\boldsymbol{\lambda}')} \sum_{\substack{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}(X)^t \\ (\boldsymbol{x}, \boldsymbol{y}) \equiv (\boldsymbol{u}, \boldsymbol{v}) \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}} \overline{\mathfrak{b}_{\boldsymbol{y}}}.$$

Writing

$$\mathfrak{B}(\boldsymbol{u}) = \sum_{\substack{\boldsymbol{x} \in \mathcal{E}(X)^t \\ \boldsymbol{x} \equiv \boldsymbol{u} \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}}$$

and

$$\phi_{\boldsymbol{u}}(\boldsymbol{\gamma}) = \gamma_c \sum_{i=1}^{t} u_i^{(c)} + \cdots + \gamma_{d-1} \sum_{i=1}^{t} u_i^{(d-1)}$$

for brevity, and encoding the condition $(\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}}) \in \widetilde{\mathcal{A}}_t(\boldsymbol{\lambda}')$ in integral form, we see that

$$\begin{aligned}
\sum_{(\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}}) \in \widetilde{\mathcal{A}}_t(\boldsymbol{\lambda}')} \mathfrak{B}(\boldsymbol{u}) \overline{\mathfrak{B}(\boldsymbol{v})} &= \sum_{(\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}}) \in A_p^{2t(d-c)}} \mathfrak{B}(\boldsymbol{u}) \overline{\mathfrak{B}(\boldsymbol{v})} \oint e\big(\phi_{\boldsymbol{u}}(\boldsymbol{\gamma}) - \phi_{\boldsymbol{v}}(\boldsymbol{\gamma})\big) e(-\boldsymbol{\gamma} \cdot \boldsymbol{\lambda}') \, d\boldsymbol{\gamma} \\
&= \oint e(-\boldsymbol{\gamma} \cdot \boldsymbol{\lambda}') \sum_{(\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}}) \in A_p^{2t(d-c)}} \mathfrak{B}(\boldsymbol{u}) \overline{\mathfrak{B}(\boldsymbol{v})} e\big(\phi_{\boldsymbol{u}}(\boldsymbol{\gamma}) - \phi_{\boldsymbol{v}}(\boldsymbol{\gamma})\big) \, d\boldsymbol{\gamma} \\
&\le \oint \left| \sum_{(\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}}) \in A_p^{2t(d-c)}} \mathfrak{B}(\boldsymbol{u}) \overline{\mathfrak{B}(\boldsymbol{v})} e\big(\phi_{\boldsymbol{u}}(\boldsymbol{\gamma}) - \phi_{\boldsymbol{v}}(\boldsymbol{\gamma})\big) \right| d\boldsymbol{\gamma}.
\end{aligned}$$

The expression on the right-hand side is now independent of our choice of $\boldsymbol{\lambda}$, so we conclude that

$$\begin{aligned} G_{c,d}(\boldsymbol{z}) &\leq (2t-1)^{d-c} \oint \Big| \sum_{\underline{\boldsymbol{u}} \in A_p^{t(d-c)}} \mathfrak{B}(\boldsymbol{u}) e(\phi_{\boldsymbol{u}}(\boldsymbol{\gamma})) \Big|^2 \, d\boldsymbol{\gamma} \\ &\ll \sum_{(\underline{\boldsymbol{u}},\underline{\boldsymbol{v}}) \in \widetilde{\mathcal{A}}_t(\mathbf{0})} \sum_{\substack{\boldsymbol{x},\boldsymbol{y} \in \mathcal{E}(X)^t \\ (\boldsymbol{x},\boldsymbol{y}) \equiv (\boldsymbol{u},\boldsymbol{v}) \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}} \overline{\mathfrak{b}_{\boldsymbol{y}}} \\ &= \sum_{0 \leq \boldsymbol{n} \leq t(p-1)} \Big| \sum_{\underline{\boldsymbol{u}} \in \mathcal{A}_t(\boldsymbol{n})} \sum_{\substack{\boldsymbol{x} \in \mathcal{E}(X)^t \\ \boldsymbol{x} \equiv \boldsymbol{u} \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}} \Big|^2. \end{aligned}$$

Using Cauchy's inequality, we see that

$$G_{c,d}(\boldsymbol{z}) \ll \sum_{0 \leq \boldsymbol{n} \leq t(p-1)} \Big(\sum_{\underline{\boldsymbol{u}} \in \mathcal{A}_t(\boldsymbol{n})} \Big| \sum_{\substack{\boldsymbol{x} \in \mathcal{E}(X)^t \\ \boldsymbol{x} \equiv \boldsymbol{u} \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}} \Big|^2 \Big) \Big(\sum_{\underline{\boldsymbol{u}} \in \mathcal{A}_t(\boldsymbol{n})} 1 \Big).$$

From our initial assumption that $\mathcal{E}$ is a (p,t,δ)-ellipsephic set, we know that for $\boldsymbol{n} = (n_c, \dots, n_{d-1})$ with $0 \leq \boldsymbol{n} \leq t(p-1)$, we have

$$\#\mathcal{A}_t(\boldsymbol{n}) = \#\Big\{ \underline{\boldsymbol{u}} \in A_p^{t(d-c)} \; \Big| \; \sum_{i=1}^{t} u_i^{(r)} = n_r \text{ for } c \leq r \leq d-1 \Big\} \ll \prod_{r=c}^{d-1} n_r^{\delta} \ll p^{\delta(d-c)},$$

and consequently

$$\begin{aligned} G_{c,d}(\boldsymbol{z}) &\ll p^{\delta(d-c)} \sum_{0 \leq \boldsymbol{n} \leq t(p-1)} \sum_{\underline{\boldsymbol{u}} \in \mathcal{A}_t(\boldsymbol{n})} \Big| \sum_{\substack{\boldsymbol{x} \in \mathcal{E}(X)^t \\ \boldsymbol{x} \equiv \boldsymbol{u} \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}} \Big|^2 \\ &= p^{\delta(d-c)} \sum_{\substack{\boldsymbol{u} \in \mathcal{E}(p^d)^t \\ \boldsymbol{u} \equiv \boldsymbol{z} \pmod{p^c}}} \Big| \sum_{\substack{\boldsymbol{x} \in \mathcal{E}(X)^t \\ \boldsymbol{x} \equiv \boldsymbol{u} \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}} \Big|^2, \end{aligned}$$

as claimed. □

We are interested in the following expressions, the first of which represents the weighted number of solutions to our system of equations in which the variables fall into certain congruence classes modulo powers of p. For $a, b \in \mathbb{N}$, we let

$$I_{a,b}(\xi, \eta) = \oint |f_a(\boldsymbol{\alpha}, \xi)|^{2t} \, |f_b(\boldsymbol{\alpha}, \eta)|^{4t} \, d\boldsymbol{\alpha},$$

and observe that this expression counts the number of solutions to the system

$$\sum_{i=1}^{t} (x_i^j - y_i^j) = \sum_{l=1}^{2t} (u_l^j - v_l^j), \quad (j = 1, 2) \tag{2.5}$$

with $x_i, y_i, u_l, v_l \in \mathcal{E}(X)$ for $1 \leq i \leq t$ and $1 \leq l \leq 2t$, satisfying $\boldsymbol{x} \equiv \boldsymbol{y} \equiv \xi \pmod{p^a}$ and $\boldsymbol{u} \equiv \boldsymbol{v} \equiv \eta \pmod{p^b}$, and with each solution being counted

with weight $\rho_a(\xi)^{-2t}\rho_b(\eta)^{-4t}\mathfrak{a}_{\boldsymbol{x}}\mathfrak{a}_{\boldsymbol{y}}\mathfrak{a}_{\boldsymbol{u}}\mathfrak{a}_{\boldsymbol{v}}$. We also assume that $I_{0,0}(\xi,\eta)=\mathfrak{J}(X)$ for any ξ and η.

Next, a weighted sum over the possible values of ξ and η in the above definition will simplify later computations. For $h\in\mathbb{N}$, we define

$$K_{a,b}^h=\rho_0^{-4}\sum_{\xi\in\mathcal{E}(p^a)}\sum_{\substack{\eta\in\mathcal{E}(p^b)\\ p^{h-1}\|(\xi-\eta)}}\rho_a(\xi)^2\rho_b(\eta)^2 I_{a,b}(\xi,\eta), \tag{2.6}$$

where the notation $p^c\|d$ means that $p^c\mid d$ and $p^{c+1}\nmid d$.

The next lemma allows us to apply Lemma 2.2 as the key ingredient in an iterative process which we use in Section 3 to complete the proof of Theorem 1.2.

Lemma 2.3. *For $a,b,h\in\mathbb{N}$ satisfying $h\le a<b\le 2a-h+1$ and $p^b<X$, we have*

$$K_{a,b}^h\ll p^{\delta(2b-a-h+1)}(X/p^b)^{(\lambda+\iota)/2}(K_{b,2b-h+1}^h)^{1/2}.$$

Proof. We begin by considering $I_{a,b}(\xi,\eta)$, and note that by the definition of $K_{a,b}^h$, we may assume that we are working in the situation in which $p^{h-1}\|(\xi-\eta)$.

Writing $x_i=p^a\tilde{x}_i+\xi$ and $u_l=p^b\tilde{u}_l+\eta$, and similarly for $\boldsymbol{y}$ and $\boldsymbol{v}$, we apply the binomial theorem to (2.5) to see that

$$\sum_{i=1}^{t}\left((p^a\tilde{x}_i+\xi-\eta)^j-(p^a\tilde{y}_i+\xi-\eta)^j\right)=p^{jb}\sum_{l=1}^{2t}(\tilde{u}_l^j-\tilde{v}_l^j),\quad (j=1,2),$$

and consequently that we have the congruences

$$\sum_{i=1}^{t}\left((p^a\tilde{x}_i+\xi-\eta)^j-(p^a\tilde{y}_i+\xi-\eta)^j\right)\equiv 0\ (\mathrm{mod}\ p^{jb}),\quad (j=1,2).$$

In other words, we have

$$\sum_{i=1}^{t}(\tilde{x}_i-\tilde{y}_i)\equiv 0\ (\mathrm{mod}\ p^{b-a}), \tag{2.7}$$

and

$$p^a\sum_{i=1}^{t}(\tilde{x}_i^2-\tilde{y}_i^2)+2(\xi-\eta)\sum_{i=1}^{t}(\tilde{x}_i-\tilde{y}_i)\equiv 0\ (\mathrm{mod}\ p^{2b-a}). \tag{2.8}$$

We fix the weights appearing in the definition of $G_{c,d}(\boldsymbol{z})$ to be

$$\mathfrak{b}_x=\rho_a(\xi)^{-1}\mathfrak{a}_x e(\alpha_1 x+\alpha_2 x^2).$$

Encoding (2.7) as part of our integral, and writing $\boldsymbol{\xi}=(\xi,\dots,\xi)$, we have

$$I_{a,b}(\xi,\eta)=\oint G_{a,b}(\boldsymbol{\xi})\,|f_b(\boldsymbol{\alpha},\eta)|^{4t}\,d\boldsymbol{\alpha}.$$

By Lemma 2.2, we may conclude that

$$I_{a,b}(\xi,\eta) \ll p^{\delta(b-a)} \sum_{\substack{\boldsymbol{z}\in\mathcal{E}(p^b)^t\\ \boldsymbol{z}\equiv\xi \pmod{p^a}}} \oint \Big| \sum_{\substack{\boldsymbol{x}\in\mathcal{E}(X)^t\\ \boldsymbol{x}\equiv\boldsymbol{z} \pmod{p^b}}} \mathfrak{b}_{\boldsymbol{x}} \Big|^2 |f_b(\boldsymbol{\alpha},\eta)|^{4t}\, d\boldsymbol{\alpha}.$$

We have therefore introduced, at a cost of $p^{\delta(b-a)}$, the additional condition

$$x_i \equiv y_i \pmod{p^b}, \quad (1\le i\le t),$$

or equivalently

$$\tilde{x}_i \equiv \tilde{y}_i \pmod{p^{b-a}}, \quad (1\le i\le t).$$

Substituting this back into (2.8), and using the facts that $p^{h-1}\|(\xi-\eta)$ and $h-1<a<b$, we see that

$$\sum_{i=1}^{t}(\tilde{x}_i-\tilde{y}_i)\equiv 0 \pmod{p^{b-h+1}}.$$

Encoding this congruence as before, we obtain

$$I_{a,b}(\xi,\eta) \ll p^{\delta(b-a)} \sum_{\substack{\boldsymbol{z}\in\mathcal{E}(p^b)^t\\ \boldsymbol{z}\equiv\xi \pmod{p^a}}} \oint G_{b,a+b-h+1}(\boldsymbol{z})\, |f_b(\boldsymbol{\alpha},\eta)|^{4t}\, d\boldsymbol{\alpha}.$$

We now apply Lemma 2.2 again to see that

$$I_{a,b}(\xi,\eta) \ll p^{\delta(b-h+1)} \sum_{\substack{\boldsymbol{z}\in\mathcal{E}(p^{a+b-h+1})^t\\ \boldsymbol{z}\equiv\xi \pmod{p^a}}} \oint \Big| \sum_{\substack{\boldsymbol{x}\in\mathcal{E}(X)^t\\ \boldsymbol{x}\equiv\boldsymbol{z} \pmod{p^{a+b-h+1}}}} \mathfrak{b}_{\boldsymbol{x}} \Big|^2 |f_b(\boldsymbol{\alpha},\eta)|^{4t}\, d\boldsymbol{\alpha},$$

and we have introduced the additional condition

$$\tilde{x}_i \equiv \tilde{y}_i \pmod{p^{b-h+1}}, \quad (1\le i\le t).$$

Repeating this process, we reach the situation in which

$$\sum_{i=1}^{t}(\tilde{x}_i-\tilde{y}_i)\equiv 0 \pmod{p^{2b-a-h+1}},$$

and a final application of Lemma 2.2 allows us to conclude that

$$I_{a,b}(\xi,\eta) \ll p^{\delta(2b-a-h+1)} \sum_{\substack{\boldsymbol{z}\in\mathcal{E}(p^{2b-h+1})^t\\ \boldsymbol{z}\equiv\xi \pmod{p^a}}} \oint \Big| \sum_{\substack{\boldsymbol{x}\in\mathcal{E}(X)^t\\ \boldsymbol{x}\equiv\boldsymbol{z} \pmod{p^{2b-h+1}}}} \mathfrak{b}_{\boldsymbol{x}} \Big|^2 |f_b(\boldsymbol{\alpha},\eta)|^{4t}\, d\boldsymbol{\alpha}.$$

Using the definition of the weights $\mathfrak{b}$, and writing $b'=2b-h+1$, we deduce that

$$I_{a,b}(\xi,\eta) \ll p^{\delta(b'-a)} \oint \Big(\sum_{\substack{\xi'\in\mathcal{E}(p^{b'})\\ \xi'\equiv\xi \pmod{p^a}}} \rho_a(\xi)^{-2}\rho_{b'}(\xi')^2\, |f_{b'}(\boldsymbol{\alpha},\xi')|^2 \Big)^t |f_b(\boldsymbol{\alpha},\eta)|^{4t}\, d\boldsymbol{\alpha},$$

and note that our assumption that $p^{h-1}\|(\xi-\eta)$ implies that we also have $p^{h-1}\|(\xi'-\eta)$. An application of Hölder's inequality gives

$$\begin{aligned} I_{a,b}(\xi,\eta) &\ll p^{\delta(b'-a)}\rho_a(\xi)^{-2} \sum_{\substack{\xi'\in\mathcal{E}(p^{b'})\\ \xi'\equiv\xi \pmod{p^a}}} \rho_{b'}(\xi')^2 \oint |f_{b'}(\boldsymbol{\alpha},\xi')|^{2t}\,|f_b(\boldsymbol{\alpha},\eta)|^{4t}\,d\boldsymbol{\alpha} \\ &= p^{\delta(b'-a)}\rho_a(\xi)^{-2} \sum_{\substack{\xi'\in\mathcal{E}(p^{b'})\\ \xi'\equiv\xi \pmod{p^a}}} \rho_{b'}(\xi')^2 I_{b',b}(\xi',\eta). \end{aligned}$$

Using Cauchy's inequality and Lemma 2.1, we see that

$$\begin{aligned} I_{b',b}(\xi',\eta) &= \oint |f_{b'}(\boldsymbol{\alpha},\xi')|^{2t}\,|f_b(\boldsymbol{\alpha},\eta)|^{4t}\,d\boldsymbol{\alpha} \\ &\le \Big(\oint |f_b(\boldsymbol{\alpha},\eta)|^{2t}\,|f_{b'}(\boldsymbol{\alpha},\xi')|^{4t}\,d\boldsymbol{\alpha}\Big)^{1/2} \Big(\oint |f_b(\boldsymbol{\alpha},\eta)|^{6t}\,d\boldsymbol{\alpha}\Big)^{1/2} \\ &\ll I_{b,b'}(\eta,\xi')^{1/2}(X/p^b)^{(\lambda+\iota)/2}. \end{aligned}$$

Substituting this into (2.6), we see that

$$\begin{aligned} K_{a,b}^h &= \rho_0^{-4} \sum_{\xi\in\mathcal{E}(p^a)} \sum_{\substack{\eta\in\mathcal{E}(p^b)\\ p^{h-1}\|(\xi-\eta)}} \rho_a(\xi)^2\rho_b(\eta)^2 I_{a,b}(\xi,\eta) \\ &\ll p^{\delta(b'-a)}(X/p^b)^{(\lambda+\iota)/2}\rho_0^{-4} \sum_{\eta\in\mathcal{E}(p^b)} \sum_{\substack{\xi'\in\mathcal{E}(p^{b'})\\ p^{h-1}\|(\xi'-\eta)}} \rho_b(\eta)^2\rho_{b'}(\xi')^2 I_{b,b'}(\eta,\xi')^{1/2}. \end{aligned}$$

By Cauchy's inequality and (2.3), we conclude that

$$\begin{aligned} K_{a,b}^h &\ll p^{\delta(b'-a)}(X/p^b)^{(\lambda+\iota)/2}\rho_0^{-2}\Bigg(\sum_{\eta\in\mathcal{E}(p^b)} \sum_{\substack{\xi'\in\mathcal{E}(p^{b'})\\ p^{h-1}\|(\xi'-\eta)}} \rho_b(\eta)^2\rho_{b'}(\xi')^2 I_{b,b'}(\eta,\xi')\Bigg)^{1/2} \\ &= p^{\delta(b'-a)}(X/p^b)^{(\lambda+\iota)/2}(K_{b,b'}^h)^{1/2}, \end{aligned}$$

as claimed. □

Finally, the following lemma provides a key step in the iterative process of Section 3.

Lemma 2.4. *For $h\in\mathbb{N}$, and for $\xi\in\mathcal{E}(p^{h-1})$, we have*

$$I_{h-1,h-1}(\xi,\xi) \ll \rho_{h-1}(\xi)^{-4}\Bigg(\sum_{\substack{\eta\in\mathcal{E}(p^h)\\ \eta\equiv\xi \ (mod\ p^{h-1})}} \rho_h(\eta)^4 I_{h,h}(\eta,\eta) + p^{2s-2}\rho_0^4\,K_{h,h}^h\Bigg).$$

Proof. We observe that

$$\begin{aligned} I_{h-1,h-1}(\xi,\xi) &= \oint |f_{h-1}(\boldsymbol{\alpha},\xi)|^{2t} \, |f_{h-1}(\boldsymbol{\alpha},\xi)|^{4t} \, d\boldsymbol{\alpha} \\ &= \oint |f_{h-1}(\boldsymbol{\alpha},\xi)|^{2s} \, d\boldsymbol{\alpha}, \end{aligned}$$

which counts the number of solutions to (1.4) with $x_i, y_i \in \mathcal{E}(X)$ for $1 \le i \le s$ and $\boldsymbol{x} \equiv \boldsymbol{y} \equiv \xi \pmod{p^{h-1}}$, each solution being counted with weight $\rho_{h-1}(\xi)^{-2s}\mathfrak{a}_{\boldsymbol{x}}\mathfrak{a}_{\boldsymbol{y}}$.

We partition the solutions based on the congruence classes in which the variables lie modulo p^h, letting $\mathfrak{J}_h(X,\xi)$ denote the contribution from solutions in which all variables are congruent modulo p^h, and $\mathfrak{J}_h^*(X,\xi)$ the contribution from the remaining solutions, so that

$$I_{h-1,h-1}(\xi,\xi) = \mathfrak{J}_h(X,\xi) + \mathfrak{J}_h^*(X,\xi). \tag{2.9}$$

We have

$$\begin{aligned} \mathfrak{J}_h(X,\xi) &= \sum_{\substack{\eta \in \mathcal{E}(p^h) \\ \eta \equiv \xi \pmod{p^{h-1}}}} \rho_{h-1}(\xi)^{-2s} \rho_h(\eta)^{2s} I_{h,h}(\eta,\eta) \\ &\le \rho_{h-1}(\xi)^{-4} \sum_{\substack{\eta \in \mathcal{E}(p^h) \\ \eta \equiv \xi \pmod{p^{h-1}}}} \rho_h(\eta)^4 I_{h,h}(\eta,\eta), \end{aligned} \tag{2.10}$$

since $\rho_h(\eta)^2 \le \rho_{h-1}(\xi)^2$ for $\eta \equiv \xi \pmod{p^{h-1}}$.

When estimating $\mathfrak{J}_h^*(X,\xi)$, we may assume, up to a combinatorial factor, that $x_1 \not\equiv x_2 \pmod{p^h}$, and observe that $\mathfrak{J}_h^*(X,\xi)$ is bounded above by at most a constant multiple of

$$\begin{aligned} &\rho_{h-1}(\xi)^{-2} \sum_{\substack{\eta \ne \eta' \in \mathcal{E}(p^h) \\ \eta \equiv \eta' \equiv \xi \pmod{p^{h-1}}}} \rho_h(\eta)\rho_h(\eta') \oint f_h(\boldsymbol{\alpha},\eta) f_h(-\boldsymbol{\alpha},\eta') \, |f_{h-1}(\boldsymbol{\alpha},\xi)|^{2s-2} \, d\boldsymbol{\alpha} \\ &\le \rho_{h-1}(\xi)^{-2} \sum_{\substack{\eta \ne \eta' \in \mathcal{E}(p^h) \\ \eta \equiv \eta' \equiv \xi \pmod{p^{h-1}}}} \rho_h(\eta)\rho_h(\eta') I_{h,h}(\eta,\eta')^{1/2s} I_{h,h}(\eta',\eta)^{1/2s} I_{h-1,h-1}(\xi,\xi)^{1-1/s}, \end{aligned}$$

by Hölder's inequality. If $\mathfrak{J}_h^*(X,\xi) = \max\{\mathfrak{J}_h(X,\xi), \mathfrak{J}_h^*(X,\xi)\}$, we have

$$I_{h-1,h-1}(\xi,\xi) \ll \mathfrak{J}_h^*(X,\xi),$$

and may rearrange to obtain

$$\begin{aligned} I_{h-1,h-1}(\xi,\xi) &\ll \rho_{h-1}(\xi)^{-2s}\bigg(\sum_{\substack{\eta\neq\eta'\in\mathcal{E}(p^h)\\ \eta\equiv\eta'\equiv\xi \pmod{p^{h-1}}}} \rho_h(\eta)\rho_h(\eta')I_{h,h}(\eta,\eta')^{1/s}\bigg)^s \\ &\ll \rho_{h-1}(\xi)^{-2s}\bigg(\sum_{\substack{\eta\neq\eta'\in\mathcal{E}(p^h)\\ \eta\equiv\eta'\equiv\xi \pmod{p^{h-1}}}} \rho_h(\eta)^s\rho_h(\eta')^s I_{h,h}(\eta,\eta')\bigg)\bigg(\sum_{\substack{\eta\neq\eta'\in\mathcal{E}(p^h)\\ \eta\equiv\eta'\equiv\xi \pmod{p^{h-1}}}} 1\bigg)^{s-1} \\ &\ll \rho_{h-1}(\xi)^{-4}p^{2s-2}\rho_0^4\,K_{h,h}^h. \end{aligned} \tag{2.11}$$

Substituting (2.10) and (2.11) into (2.9), we deduce that

$$I_{h-1,h-1}(\xi,\xi) \ll \rho_{h-1}(\xi)^{-4}\bigg(\sum_{\substack{\eta\in\mathcal{E}(p^h)\\ \eta\equiv\xi \pmod{p^{h-1}}}} \rho_h(\eta)^4 I_{h,h}(\eta,\eta) + p^{2s-2}\rho_0^4\,K_{h,h}^h\bigg),$$

as claimed. □

3. Proof of Theorem 1.2

We first wish to handle those solutions in which all of our variables are congruent modulo some small power of p, since these should contribute neglibly to the total, but would prevent some of the mechanisms of the previous section from working smoothly.

Applying Lemma 2.4 twice, we have

$$\begin{aligned} \mathfrak{J}(X) &\ll \rho_0^{-4}\sum_{\xi\in\mathcal{E}(p)} \rho_1(\xi)^4 I_{1,1}(\xi,\xi) + p^{2s-2}K_{1,1}^1 \\ &\ll \rho_0^{-4}\sum_{\xi\in\mathcal{E}(p)}\bigg(\sum_{\substack{\eta\in\mathcal{E}(p^2)\\ \eta\equiv\xi \pmod{p}}} \rho_2(\eta)^4 I_{2,2}(\eta,\eta) + p^{2s-2}\rho_0^4\,K_{2,2}^2\bigg) + p^{2s-2}K_{1,1}^1 \\ &= \rho_0^{-4}\sum_{\eta\in\mathcal{E}(p^2)} \rho_2(\eta)^4 I_{2,2}(\eta,\eta) + p^{2s-1}K_{2,2}^2 + p^{2s-2}K_{1,1}^1. \end{aligned}$$

Repeated application of Lemma 2.4 therefore yields

$$\mathfrak{J}(X) \ll \rho_0^{-4}\sum_{\omega\in\mathcal{E}(p^\nu)} \rho_\nu(\omega)^4 I_{\nu,\nu}(\omega,\omega) + \sum_{1\leq h\leq\nu} p^{2s-3+h}K_{h,h}^h.$$

We have

$$\begin{aligned} I_{\nu,\nu}(\omega,\omega) &= \oint |f_\nu(\boldsymbol{\alpha},\omega)|^{2t}\,|f_\nu(\boldsymbol{\alpha},\omega)|^{4t}\,d\boldsymbol{\alpha} \\ &= \oint |f_\nu(\boldsymbol{\alpha},\omega)|^{6t}\,d\boldsymbol{\alpha} \ll (X/p^\nu)^{\lambda+\iota}, \end{aligned}$$

by Lemma 2.1. Consequently, by the definitions of ν and ι, we have

$$\begin{aligned}\rho_0^{-4}\sum_{\omega\in\mathcal{E}(p^\nu)}\rho_\nu(\omega)^4 I_{\nu,\nu}(\omega,\omega) &\ll (X/p^\nu)^{\lambda+\iota}\rho_0^{-4}\sum_{\omega\in\mathcal{E}(p^\nu)}\rho_\nu(\omega)^4\\ &\ll X^{\lambda+\iota}p^{-(\lambda+\iota)B/2^{2n+2}}\\ &= X^{\lambda+\iota-(\lambda+\iota)/2^{2n+2}} = o(X^{\lambda-\iota}).\end{aligned}$$

By our choice of $\mathfrak{a}\in\mathbb{D}$, and the discussions at the beginning of Section 2, there is consequently some value of h with $1\le h\le\nu$ with the property that

$$\mathfrak{J}(X)\ll \nu p^{2s-3+h}K_{h,h}^h.$$

By Hölder's inequality, we have

$$K_{h,h}^h\le p^{(u-1)(2t-1)+u(4t-1)}K_{h+u-1,h+u}^h,$$

and consequently

$$\mathfrak{J}(X)\ll \nu p^{4t+6tu-2u+h}K_{h+u-1,h+u}^h. \tag{3.1}$$

We define a sequence of indices by the following recurrence relations:

$$a_0=h+u-1,\quad b_0=h+u,\quad a_m=b_{m-1},\quad b_m=2b_{m-1}-h+1.$$

For convenience we note that $b_m=2^m(u+1)+h-1$. By Lemma 2.3, while $p^{b_m}<X$, which is assured by (2.1) for $m\le n$, we have

$$K_{a_m,b_m}^h\ll p^{\delta(2b_m-a_m-h+1)}(X/p^{b_m})^{(\lambda+\iota)/2}(K_{a_{m+1},b_{m+1}}^h)^{1/2},$$

which gives

$$K_{a_0,b_0}^h\ll p^{\delta(u+2)}(X/p^{b_0})^{(\lambda+\iota)/2}(K_{a_1,b_1}^h)^{1/2},$$

and, for $m\ge 1$,

$$K_{a_m,b_m}^h\ll p^{3\cdot 2^{m-1}(u+1)\delta}(X/p^{b_m})^{(\lambda+\iota)/2}(K_{a_{m+1},b_{m+1}}^h)^{1/2}.$$

By iterating this relation, we see that

$$\begin{aligned}K_{h+u-1,h+u}^h &\ll p^{\delta(u+2+3(u+1)(n-1)/2)-n(\lambda+\iota)(u+1)/2}X^{(\lambda+\iota)(1-1/2^n)}(K_{a_n,b_n}^h)^{1/2^n}\\ &\ll p^{-\delta(u-1)/2+3\delta n(u+1)/2-\lambda n(u+1)/2}X^{(\lambda+\iota)(1-1/2^n)}(K_{a_n,b_n}^h)^{1/2^n},\end{aligned}$$

and using the definitions of Λ and n, we deduce that

$$\begin{aligned}K_{h+u-1,h+u}^h &\ll p^{-n\Lambda(u+1)/2}X^{(\lambda+\iota)(1-1/2^n)}(K_{a_n,b_n}^h)^{1/2^n}\\ &\ll p^{-8t(u+1)}X^{(\lambda+\iota)(1-1/2^n)}(K_{a_n,b_n}^h)^{1/2^n}.\end{aligned}$$

Substituting this into (3.1), we see that

$$\begin{aligned}\mathfrak{J}(X) &\ll \nu p^{-4t-2tu-2u+h}X^{(\lambda+\iota)(1-1/2^n)}(K_{a_n,b_n}^h)^{1/2^n}\\ &\ll p^{\nu-2tu-2u}X^{(\lambda+\iota)(1-1/2^n)}(K_{a_n,b_n}^h)^{1/2^n}\log X.\end{aligned} \tag{3.2}$$

A trivial bound gives us $K^h_{a_n,b_n} \ll X^{\lambda+\iota}$. Combining this with (3.2), and using (2.2), we obtain

$$\begin{aligned}\mathfrak{J}(X) &\ll p^{\nu-2tu-2u}X^{\lambda+\iota+\epsilon}\\ &\ll p^{-2\iota B-2u}X^{\lambda+\iota+\epsilon}\\ &\ll X^{\lambda-\iota-1/2^{n+1}+\epsilon} = o(X^{\lambda-\iota}),\end{aligned}$$

which provides the required contradiction and completes the proof of Theorem 1.2. □

References

[1] K. Aloui. Sur les entiers ellipséphiques: somme des chiffres et répartition dans les classes de congruence. *Period. Math. Hungar.* **70** (2015), no. 2, 171–208.

[2] K. Aloui, C. Mauduit, and M. Mkaouar. Somme des chiffres et répartition dans les classes de congruence pour les palindromes ellipséphiques. *Acta Math. Hungar.* **151** (2017), no. 2, 409–455.

[3] K. D. Biggs. *On additive problems involving shifted integers and ellipsephic sets.* Ph.D. thesis, University of Bristol, 2019.

[4] K. D. Biggs. Efficient congruencing in ellipsephic sets: the general case, arXiv:1912.04351.

[5] J. Bourgain. Fourier transform restriction phenomena for certain lattice subsets and applications to nonlinear evolution equations. I. Schrödinger equations. *Geom. Funct. Anal.* **3** (1993), no. 2, 107–156.

[6] J. Bourgain, C. Demeter, and L. Guth. Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three. *Ann. of Math. (2)* **184** (2016), no. 2, 633–682.

[7] S. Col. *Propriétés multiplicatives d'entiers soumis à des conditions digitales.* Ph.D. thesis, Université Henri Poincaré, 2006.

[8] G. H. Hardy and J. E. Littlewood. Some problems of 'Partitio numerorum' (VI): Further researches in Waring's Problem. *Math. Z.* **23** (1925), no. 1, 1–37.

[9] I. Łaba and M. Pramanik. Maximal operators and differentiation theorems for sparse sets. *Duke Math. J.* **158** (2011), no. 3, 347–411.

[10] E. Landau. Über die Anzahl der Gitterpunkte in geweissen Bereichen. *Nachr. Ges. Wiss. Goettingen, Math.-Phys. Kl.* **1912** (1912), 687–770.

[11] K. Mahler. Note on Hypothesis K of Hardy and Littlewood. *J. London Math. Soc.* **11** (1936), no. 2, 136–138.

[12] L. B. Pierce. The Vinogradov mean value theorem [after Wooley, and Bourgain, Demeter and Guth]. *Astérisque* (2019), no. 407, Exp. No. 1134, 479–564. Séminaire Bourbaki. Vol. 2016/2017. Exposés 1120–1135.

[13] V. H. Vu. On a refinement of Waring's problem. *Duke Math. J.* **105** (2000), no. 1, 107–134.

[14] T. D. Wooley. The cubic case of the main conjecture in Vinogradov's mean value theorem. *Adv. Math.* **294** (2016), 532–561.

[15] T. D. Wooley. Nested efficient congruencing and relatives of Vinogradov's mean value theorem. *Proc. London Math. Soc. (3)* **118** (2019), no. 4, 942–1016.

School of Mathematics, University of Bristol, Fry Building, Woodland Road, Bristol, BS8 1UG, United Kingdom, and the Heilbronn Institute for Mathematical Research, Bristol, United Kingdom

E-mail address: kirsti.biggs@bristol.ac.uk