# EFFICIENT CONGRUENCING IN ELLIPSEPHIC SETS: THE GENERAL CASE

KIRSTI D. BIGGS

Abstract. In this paper, we bound the number of solutions to a general Vinogradov system of equations

$$x_1^j + \cdots + x_s^j = y_1^j + \cdots + y_s^j, \quad (1 \le j \le k),$$

as well as other related systems, in which the variables are required to satisfy digital restrictions in a given base. Specifically, our sets of permitted digits have the property that there are few representations of a natural number as sums of elements of the digit set—the set of squares serving as a key example. We obtain better bounds using this additive structure than could be deduced purely from the size of the set of variables. In particular, when the digits are required to be squares, we obtain diagonal behaviour with $2k(k+1)$ variables.

## 1. Introduction

We consider, for a fixed integer $k \in \mathbb{N}$, the system of Diophantine equations

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

In [4], the author proved an upper bound, in the case $k = 2$, for the number of solutions to (1.1), with $1 \le x_i, y_i \le X$ for all $i$, where the variables are restricted to subsets of the natural numbers defined by digital restrictions. In this paper, we extend such results to the case of general $k$.

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

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

for some $t \ge 2$ and for all $\epsilon > 0$, and let

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

be the set of natural numbers whose expansion in base $p$ includes only digits from $A$. Write $A_p$ for $A \cap [0, p-1]$, and assume that $2 \le \#A_p \le p - 1$. Let $I_{s,k}(X)$ be the number of solutions to the Vinogradov system (1.1) 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*

$$I_{s,k}(X) \ll X^\epsilon (Y^s + Y^{2s - tk(k+1)/2}).$$

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.

We note that this bound is essentially optimal provided that $Y \gg X^{1/t}$, since one may apply a standard method, discussed later in this section, to see that

$$I_{s,k}(X) \gg Y^{2s} X^{-k(k+1)/2} \gg Y^{2s-tk(k+1)/2}, \tag{1.3}$$

by our assumption on the size of $Y$, and the bound $I_{s,k}(X) \gg Y^s$ comes from the diagonal solutions.

For historical reasons, upper bounds for the number of solutions to (1.1) go by the name of Vinogradov's mean value theorem—in [12], Wooley used the efficient congruencing method to prove an optimal upper bound for the number of solutions to this system in the case $k = 3$, the first time such a bound had been obtained for any $k > 2$. In [5], Bourgain, Demeter and Guth proved the equivalent statement for $k \geq 4$ using the harmonic analytic technique of $l^2$-decoupling, often seen as a real analogue of the $p$-adic efficient congruencing. Subsequently, Wooley developed the nested version of his method and used it to provide an alternative proof of the general case in [13]. The similarities between the two methods are analysed further in [10].

As discussed in [4], we call our sets with digital restrictions ellipsephic, after the French term *ellipséphique*, coined by Mauduit to refer to integers with missing digits, and used, for example, in [1] and [2]. We let $r = \#A_p$, and note that the restriction that $2 \leq r \leq p-1$ stems from the fact that the cases $r = 0$ and $A_p = \{0\}$ are trivial, and the case $r = p$ reduces to the classical case, while the case $r = 1$ (with $A_p \neq \{0\}$) is sufficiently unusual that we omit it from consideration. We observe that

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

and hence that $\mathcal{E}$ is a thin set, in the sense that

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

The effect of these digital restrictions is to give ellipsephic sets a fractal-like structure similar to those seen in the middle-third Cantor set and generalisations thereof. In [7], Łaba and Pramanik study maximal operators corresponding to certain real fractal subsets constructed in a similar manner.

We recall the details of the key additive property that we require of our digit set. For an integer $t \geq 2$, we refer to $A \subset \mathbb{N}_0$ as an $E_t^*$-set if (1.2) holds for all $\epsilon > 0$. As mentioned in [4], we can view such sets as a generalisation of Sidon sets, in which the number of representations of an integer as the sum of a fixed number of elements of our set is bounded by a constant.

Landau proved in [8] that the set of squares is an $E_2^*$-set, and Hardy and Littlewood conjectured in [6, Hypothesis K] that for all $k \geq 2$, the set of $k$th powers should be an $E_k^*$-set. However, in [9] Mahler proved that this conjecture is false for the set of cubes, and it remains open to date for $k \geq 4$. Nevertheless, in [11], Vu used a probabilistic argument to demonstrate that for any $k \geq 2$, there exists a subset $S_k$ of the set of $k$th powers and an integer $t_k$ such that

$S_k$ is an $E^*_{t_k}$-set, thus proving the existence of infinitely many sets of the form we are interested in.

We refer to $\mathcal{E} = \mathcal{E}_p^A$ as a $(p,t)^*$-ellipsephic set if $A$ is an $E^*_t$-set, and introduce some further notation to allow us to state the more general form of our main result. Consider a system of polynomials $\boldsymbol{\phi} \in \mathbb{Z}[z]^k$ which resemble those featuring in the Vinogradov system in the sense that, for some suitably large $c \in \mathbb{N}$, we have $\phi_j(z) \equiv z^j \pmod{p^c}$ for $1 \leq j \leq k$; we call such a system $p^c$-spaced. Note that it is crucial to our argument that the prime $p$ featured here is the same one used to define our digital restrictions. For a $p^c$-spaced system $\boldsymbol{\phi}$, and a sequence $\mathfrak{a} = (\mathfrak{a}_x)_{x\in\mathcal{E}}$ of complex weights, we let

$$J_{s,k}(X) = J_{s,k}(X; \mathfrak{a}, \boldsymbol{\phi}) = \oint \Big| \sum_{x\in\mathcal{E}(X)} \mathfrak{a}_x e\big(\alpha_1\phi_1(x) + \cdots + \alpha_k\phi_k(x)\big)\Big|^{2s} d\boldsymbol{\alpha},$$

where we write $e(z)$ for $e^{2\pi i z}$ and $\oint$ for the integral over the $k$-dimensional unit cube $[0,1]^k$. Then $J_{s,k}(X)$ counts the solutions $x_i, y_i \in \mathcal{E}(X)$ to the system

$$\phi_j(x_1) + \cdots + \phi_j(x_s) = \phi_j(y_1) + \cdots + \phi_j(y_s), \quad (1 \leq j \leq k),$$

with weights $\mathfrak{a}_{\boldsymbol{x}}\overline{\mathfrak{a}_{\boldsymbol{y}}} = \mathfrak{a}_{x_1}\dots\mathfrak{a}_{x_s}\overline{\mathfrak{a}_{y_1}\dots\mathfrak{a}_{y_s}}$. We adopt the convention that, unless previously fixed, statements involving $\epsilon$ 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 $J_{s,k}(X)$.

**Theorem 1.2.** *For natural numbers $k$ and $t$ with $t \geq 2$, and for $p > k$ an odd prime, let $\mathcal{E}$ be a $(p,t)^*$-ellipsephic set, and write $Y = \#\mathcal{E}(X)$. Let $\boldsymbol{\phi} \in \mathbb{Z}[z]^k$ be a $p^c$-spaced system of polynomials for some suitably large $c \in \mathbb{N}$. Then for $s \geq tk(k+1)/2$, we have*

$$J_{s,k}(X) \ll Y^{s-tk(k+1)/2} X^\epsilon \bigg( \sum_{x\in\mathcal{E}(X)} |\mathfrak{a}_x|^2 \bigg)^s.$$

A standard application of Hölder's inequality shows that for $s \leq tk(k+1)/2$, we have

$$J_{s,k}(X) \ll X^\epsilon \bigg( \sum_{x\in\mathcal{E}(X)} |\mathfrak{a}_x|^2 \bigg)^s,$$

whereas if we take $\mathfrak{a}_x = 0$ for $x \notin \mathcal{E}$ in the classical version of Vinogradov's mean value theorem, for $s = tk(k+1)/2$ we obtain

$$J_{s,k}(X) \ll Y^{(t-1)k(k+1)/2} X^\epsilon \bigg( \sum_{x\in\mathcal{E}(X)} |\mathfrak{a}_x|^2 \bigg)^s,$$

so we see that, as in the quadratic case, we have achieved a power saving in $Y$ by utilising the specific additive structure of our ellipsephic sets, rather than simply their density.

**Corollary 1.3.** *Theorem 1.1 is true.*

*Proof.* This is the case of Theorem 1.2 where $\phi_j(z) = z^j$ for $1 \leq j \leq k$, and $\mathfrak{a}_x = 1$ for all $x \in \mathcal{E}$. □

The lower bound (1.3) follows by integrating only over the portion of the unit cube for which we have $\alpha_j \ll X^{-j}$ for $1 \leq j \leq k$, as in the classical case of Vinogradov's mean value theorem, and using our additional assumption on the size of $Y$.

An important area for future consideration is the application of the results of this paper to Waring's problem, in which we seek to find $s = s(k)$ such that any $n \in \mathbb{N}$ may be written in the form

$$n = x_1^k + \cdots + x_s^k, \tag{1.4}$$

with $x_1, \ldots, x_s \in \mathcal{E}$. As in [4], we are able to prove a lower bound for $N_{s,k}(X) = N_{s,k}^{\mathcal{E}}(X)$, defined as the number of positive integers up to $X$ which have a representation in the form (1.4). We require the same condition on $Y$ as in the lower bound discussed above, without which we would not expect to represent a significant proportion of the integers up to $X$.

**Corollary 1.4.** *For natural numbers $k$ and $t$ with $t \geq 2$, and for $p > k$ an odd prime, let $\mathcal{E}$ be a $(p,t)^*$-ellipsephic set. Assume that $Y = \#\mathcal{E}(X) \gg X^{1/t}$. Then for $s \geq tk(k+1)/2$ we have*

$$N_{s,k}(X) \gg X^{1-\epsilon}.$$

*Proof.* As in [4, Corollary 1.5], we write $R(n) = R_{s,k}^{\mathcal{E}}(n)$ for the number of representations of an integer $n$ as a sum of $s$ $k$th powers of integers from $\mathcal{E}$ and apply Cauchy's inequality to see that

$$\bigg(\sum_{1 \leq n \leq X} R(n)\bigg)^2 \leq N_{s,k}(X)\bigg(\sum_{1 \leq n \leq X} R(n)^2\bigg).$$

Via Theorem 1.1, we obtain the bound

$$N_{s,k}(X) \gg Y^{t(k+1)/2} X^{(1-k)/2-\epsilon},$$

and then use our assumption on the size of $Y$to deduce that

$$N_{s,k}(X) \gg X^{1-\epsilon},$$

as required. □

The proof of Theorem 1.2 uses Wooley's nested efficient congruencing method and closely follows the argument of [13], with suitable adjustments for our ellipsephic situation. In Section 2 of this paper, we provide preliminary notation and formulate an alternative theorem (Theorem 2.1), which we prove by induction in the next four sections. Specifically, in Section 3, which is the main point of divergence from the work of Wooley, we use the additive properties of our $(p,t)^*$-ellipsephic sets to prove the base case $k = 1$ of Theorem 2.1, using a "lifting" argument similar to that in our previous paper [4]. In Section 4 we introduce a "hierarchy" of small constants to support the rest of the paper, and prove some basic results, and in Section 5 we use the inductive hypothesis to prove a series of lemmata which form the backbone of our iteration. In

Section 6 we complete the proof of Theorem 2.1, hypothesising that a certain quantity is strictly greater than zero and deriving a contradiction. Finally, in Section 7 we use Theorem 2.1 to deduce Theorem 1.2.

The author would like to thank Trevor Wooley for suggesting this problem and for his invaluable supervision and encouragement.

## 2. Preliminaries

For a sequence $\mathfrak{a} = (\mathfrak{a}_x)_{x\in\mathcal{E}}$ of complex weights with $\sum_{x\in\mathcal{E}}|\mathfrak{a}_x| < \infty$, we let

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

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

$$f(\boldsymbol{\alpha}) = f(\boldsymbol{\alpha};\mathfrak{a}) = \rho_0^{-1}\sum_{x\in\mathcal{E}} \mathfrak{a}_x e\big(\psi(x;\boldsymbol{\alpha})\big),$$

where $\psi(x;\boldsymbol{\alpha}) = \alpha_1\phi_1(x) + \cdots + \alpha_k\phi_k(x)$. Consequently, a bound of the form

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

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

$$\oint |f(\boldsymbol{\alpha})|^{2s}\, d\boldsymbol{\alpha} \ll X^{\Delta}.$$

As in [4], this normalisation allows us to assume that every $\mathfrak{a}_x$ is real, non-negative and at most one. We let

$$\mathbb{D} = \Bigg\{\mathfrak{a} \,\Bigg|\, 0 \le \mathfrak{a}_x \le 1 \text{ for all } x\in\mathcal{E} \text{ and } 0 < \sum_{x\in\mathcal{E}} \mathfrak{a}_x < \infty\Bigg\},$$

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

We also wish to define the restriction of $f(\boldsymbol{\alpha})$ to congruence classes modulo various powers of our chosen prime $p$. For $a \in \mathbb{N}$ and $\xi \in \mathcal{E}(p^a)$, let

$$\rho_a(\xi) = \Bigg(\sum_{\substack{x\in\mathcal{E}\\ x\equiv\xi \pmod{p^a}}} |\mathfrak{a}_x|^2\Bigg)^{1/2}$$

and

$$f_a(\boldsymbol{\alpha},\xi) = \rho_a(\xi)^{-1} \sum_{\substack{x\in\mathcal{E}\\ x\equiv\xi \pmod{p^a}}} \mathfrak{a}_x e\big(\psi(x;\boldsymbol{\alpha})\big). \tag{2.1}$$

For later convenience, for any $\xi$ we interpret $\rho_0(\xi)$ to be $\rho_0$ and $f_0(\boldsymbol{\alpha},\xi)$ to be $f(\boldsymbol{\alpha})$, and we observe that for $a \in \mathbb{N}$, we have

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

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

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

Our strategy for counting solutions to the system of equations we are interested in involves studying congruences modulo suitably large powers of $p$, and as such we make use of Wooley's notation

$$\oint_{p^B} F(\boldsymbol{\alpha})\, d\boldsymbol{\alpha} = p^{-kB} \sum_{1 \leq u_1 \leq p^B} \cdots \sum_{1 \leq u_k \leq p^B} F(\boldsymbol{u}/p^B),$$

and define

$$U^B_{s,k}(\mathfrak{a}) = \oint_{p^B} |f(\boldsymbol{\alpha})|^{2s}\, d\boldsymbol{\alpha},$$

which counts solutions to the system of congruences

$$\sum_{i=1}^{s} \big(\phi_j(x_i) - \phi_j(y_i)\big) \equiv 0 \pmod{p^B}, \quad (1 \leq j \leq k) \tag{2.2}$$

with $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}^s$, where each solution is counted with weight $\rho_0^{-2s} \mathfrak{a}_{\boldsymbol{x}} \mathfrak{a}_{\boldsymbol{y}}$. We also wish to count solutions to (2.2) with further congruence restrictions on our variables, so for $H \in \mathbb{N}$, we let

$$U^{B,H}_{s,k}(\mathfrak{a}) = \rho_0^{-2} \sum_{\xi \in \mathcal{E}(p^H)} \rho_H(\xi)^2 \oint_{p^B} |f_H(\boldsymbol{\alpha}, \xi)|^{2s}\, d\boldsymbol{\alpha}.$$

The integral on the right-hand side imposes the additional condition that $\boldsymbol{x} \equiv \boldsymbol{y} \equiv \xi \pmod{p^H}$, and the solutions are now counted with weight $\rho_H(\xi)^{-2s} \mathfrak{a}_{\boldsymbol{x}} \mathfrak{a}_{\boldsymbol{y}}$.

We observe that, for $H \in \mathbb{N}$, we have

$$f(\boldsymbol{\alpha}) = \rho_0^{-1} \sum_{\xi \in \mathcal{E}(p^H)} \rho_H(\xi) f_H(\boldsymbol{\alpha}, \xi),$$

so, by Hölder's inequality,

$$\begin{aligned} |f(\boldsymbol{\alpha})|^{2s} &\leq \rho_0^{-2s} \Big( \sum_{\xi \in \mathcal{E}(p^H)} 1 \Big)^s \Big( \sum_{\xi \in \mathcal{E}(p^H)} \rho_H(\xi)^2 \Big)^{s-1} \sum_{\xi \in \mathcal{E}(p^H)} \rho_H(\xi)^2 |f_H(\boldsymbol{\alpha}, \xi)|^{2s} \\ &\ll \rho_0^{-2} q^{sH} \sum_{\xi \in \mathcal{E}(p^H)} \rho_H(\xi)^2 |f_H(\boldsymbol{\alpha}, \xi)|^{2s}, \end{aligned}$$

where we have written $q = \#\mathcal{E}(p)$. Consequently, we have

$$U^B_{s,k}(\mathfrak{a}) \ll q^{sH} U^{B,H}_{s,k}(\mathfrak{a}). \tag{2.3}$$

We may now ask for the minimal value of $\lambda$ such that

$$U^B_{s,k}(\mathfrak{a}) \ll (q^H)^{\lambda + \epsilon} U^{B,H}_{s,k}(\mathfrak{a})$$

as uniformly as possible in the various parameters, and observe that the bound $\lambda \leq s$ follows from (2.3).

For $\tau > 0$, let $\Phi_\tau(B)$ denote the set of systems $\boldsymbol{\phi} \in \mathbb{Z}[z]^k$ which are $p^c$-spaced for some $c \geq \tau B$. We deduce from (2.3) that for $\boldsymbol{\phi} \in \Phi_\tau(B)$, we have

$$\sup_{\mathfrak{a} \in \mathbb{D}} \frac{\log \left(U^B_{s,k}(\mathfrak{a})/U^{B,H}_{s,k}(\mathfrak{a})\right)}{\log q^H} \leq s$$

for all $H \in \mathbb{N}$.

Now consider the particular choice of $\mathfrak{b} \in \mathbb{D}$ with $\mathfrak{b}_x = 0$ whenever $x \not\equiv 0 \pmod{p^H}$. We have $U^B_{s,k}(\mathfrak{b}) = U^{B,H}_{s,k}(\mathfrak{b})$, and consequently

$$\sup_{\mathfrak{a} \in \mathbb{D}} \frac{\log \left(U^B_{s,k}(\mathfrak{a})/U^{B,H}_{s,k}(\mathfrak{a})\right)}{\log q^H} \geq 0.$$

Given $s, k \in \mathbb{N}$ and $\tau > 0$, we let $H = \lceil B/k \rceil$ and let

$$\lambda^*(s,k;\tau) = \limsup_{B \to \infty} \sup_{\boldsymbol{\phi} \in \Phi_\tau(B)} \sup_{\mathfrak{a} \in \mathbb{D}} \frac{\log \left(U^B_{s,k}(\mathfrak{a})/U^{B,H}_{s,k}(\mathfrak{a})\right)}{\log q^H},$$

and

$$\lambda(s,k) = \limsup_{\tau \to 0} \lambda^*(s,k;\tau). \tag{2.4}$$

We then have $0 \leq \lambda^*(s,k;\tau) \leq s$ and consequently $0 \leq \lambda(s,k) \leq s$.

This leads us to the statement of a key result to be used in the proof of Theorem 1.2.

**Theorem 2.1.** *For natural numbers $k$ and $t$ with $t \geq 2$, and for $p > k$ an odd prime, let $\mathcal{E}$ be a $(p,t)^*$-ellipsephic set. Then $\lambda(tk(k+1)/2, k) = 0$.*

As a corollary, we obtain

**Corollary 2.2.** *For natural numbers $k$ and $t$ with $t \geq 2$, and for $p > k$ an odd prime, let $\mathcal{E}$ be a $(p,t)^*$-ellipsephic set. Let $\tau > 0$ and $\epsilon > 0$, and let $B$ be sufficiently large in terms of $k, \tau$ and $\epsilon$. Set $s = tk(k+1)/2$ and $H = \lceil B/k \rceil$. Then for all $\boldsymbol{\phi} \in \Phi_\tau(B)$ and $\mathfrak{a} \in \mathbb{D}$, we have*

$$U^B_{s,k}(\mathfrak{a}) \ll q^{H\epsilon} U^{B,H}_{s,k}(\mathfrak{a}).$$

*Proof.* By the definition of $\lambda^*(s,k;\tau)$, we have, for sufficiently large $B$, the bound

$$U^B_{s,k}(\mathfrak{a}) \ll (q^H)^{\lambda^*(s,k;\tau)+\epsilon} U^{B,H}_{s,k}(\mathfrak{a}).$$

Allowing $\tau$ to tend to zero and applying Theorem 2.1 gives the result. □

We introduce some final definitions. For $a, b, c, \nu \in \mathbb{N}$, and for $0 \leq r \leq k$ and $R = tr(r+1)/2$, we let

$$K^{r,\boldsymbol{\phi}}_{a,b,c}(\mathfrak{a}; \xi, \eta) = \oint_{p^B} \left| f_a(\boldsymbol{\alpha}, \xi)^{2R} f_b(\boldsymbol{\alpha}, \eta) \right|^{2s-2R} d\boldsymbol{\alpha}$$

and

$$K^{r,\boldsymbol{\phi},\nu}_{a,b,c}(\mathfrak{a}) = \rho_0^{-4} \sum_{\xi \in \mathcal{E}(p^a)} \sum_{\substack{\eta \in \mathcal{E}(p^b) \\ \xi \not\equiv \eta \pmod{p^\nu}}} \rho_a(\xi)^2 \rho_b(\eta)^2 K^{r,\boldsymbol{\phi}}_{a,b,c}(\mathfrak{a}; \xi, \eta).$$

Note that $K^{r,\phi}_{a,b,c}(\mathfrak{a};\xi,\eta)$ counts solutions $(\boldsymbol{x},\boldsymbol{y},\boldsymbol{u},\boldsymbol{v})\in\mathcal{E}^{2s}$ to the congruences

$$\sum_{i=1}^{R}\big(\phi_j(x_i)-\phi_j(y_i)\big)\equiv\sum_{l=1}^{s-R}\big(\phi_j(u_l)-\phi_j(v_l)\big)\ (\mathrm{mod}\ p^B),\quad (1\le j\le k),$$

with $\boldsymbol{x}\equiv\boldsymbol{y}\equiv\xi\ (\mathrm{mod}\ p^a)$ and $\boldsymbol{u}\equiv\boldsymbol{v}\equiv\eta\ (\mathrm{mod}\ p^b)$, where each solution is counted with weight $\rho_a(\xi)^{-2R}\rho_b(\eta)^{2R-2s}\mathfrak{a}_{\boldsymbol{x}}\mathfrak{a}_{\boldsymbol{y}}\mathfrak{a}_{\boldsymbol{u}}\mathfrak{a}_{\boldsymbol{v}}$.

We are also interested in normalised versions of these mean values, so for $\Delta\ge 0$ we define

$$\widetilde{K}^{r,\phi,\nu}_{a,b,c}(\mathfrak{a})_\Delta=\left(\frac{K^{r,\phi,\nu}_{a,b,c}(\mathfrak{a})}{q^{\Delta H}U^{B,H}_{s,k}(\mathfrak{a})}\right)^{\frac{k-1}{r(k-r)}}.\qquad(2.5)$$

We now prove some auxiliary results giving bounds on the above-defined mean values.

**Lemma 2.3.** *For $s,k\in\mathbb{N}$ and $p>k$ an odd prime, let $\mathcal{E}$ be a $(p,t)^*$-ellipsephic set. Let $0<\epsilon<\tau<\delta<1$, and let $B$ be sufficiently large in terms of $s,k$ and $\epsilon$. Set $H=\lceil B/k\rceil$. Then for all $\boldsymbol{\phi}\in\Phi_\tau(B)$, for all $\mathfrak{a}\in\mathbb{D}$, and for all $h\in\mathbb{N}_0$ with $h\le(1-\delta)H$, we have*

$$U^{B,h}_{s,k}(\mathfrak{a})\ll(q^{H-h})^{\lambda(s,k)+\epsilon}U^{B,H}_{s,k}(\mathfrak{a}).$$

*Proof.* The integral within the definition of $U^{B,h}_{s,k}(\mathfrak{a})$ counts solutions to the system of congruences (2.2) with $\boldsymbol{x},\boldsymbol{y}\in\mathcal{E}^s$ and $\boldsymbol{x}\equiv\boldsymbol{y}\equiv\xi\ (\mathrm{mod}\ p^h)$, with weights $\rho_h(\xi)^{-2s}\mathfrak{a}_{\boldsymbol{x}}\mathfrak{a}_{\boldsymbol{y}}$. As in [13, Lemma 4.1], we make use of some linear algebra to transform this situation into one in which we have a set of $p^{c+h}$-spaced polynomials

$$\Phi_j(z)=z^j+p^{c+h}z^{k+1}\Upsilon_j(z),\quad (1\le j\le k),$$

for some $\Upsilon_j\in\mathbb{Z}[z]$, satisfying

$$\sum_{i=1}^{s}\Phi_j(x_i)\equiv\sum_{i=1}^{s}\Phi_j(y_i)\ (\mathrm{mod}\ p^{B-kh}),\quad (1\le j\le k)$$

whenever $\boldsymbol{x},\boldsymbol{y}$ forms a solution to the original system of congruences counted by $U^{B,h}_{s,k}(\mathfrak{a})$.

The fact that $h\le(1-\delta)H$ allows us to assume that $B-kh$ is sufficiently large with respect to $s,k$ and $\epsilon$, and consequently the definition (2.4) yields

$$U^{B-kh}_{s,k}(\mathfrak{c})\ll(q^{H-h})^{\lambda(s,k)+\epsilon}U^{B-kh,H-h}_{s,k}(\mathfrak{c}),$$

where $\mathfrak{c}$ is an auxiliary set of weights defined by $\mathfrak{c}_u=\mathfrak{a}_{p^hu+\xi}\,e\big(\psi(p^hu+\xi;\boldsymbol{\alpha})\big)$. Rearranging, and using orthogonality, we obtain the conclusion. □

**Lemma 2.4.** *For $s,k\in\mathbb{N}$ and $p>k$ an odd prime, let $\mathcal{E}$ be a $(p,t)^*$-ellipsephic set. Let $0<\epsilon<\tau<\delta<1$, and let $B$ be sufficiently large in terms of $s,k$ and $\epsilon$. Set $H=\lceil B/k\rceil$ and let $\nu\in\mathbb{N}_0$ and $r\in\mathbb{N}$ with $1\le r\le k-1$. Suppose that*

$0 < \Lambda \leq \lambda(s,k)$. *Then for all* $\boldsymbol{\phi} \in \Phi_\tau(B)$*, for all* $\mathfrak{a} \in \mathbb{D}$*, and for all* $a, b \in \mathbb{N}_0$ *with* $\max\{a,b\} \leq (1-\delta)H$*, we have*

$$\widetilde{K}^{\tau,\boldsymbol{\phi},\nu}_{a,b,c}(\mathfrak{a})_\Lambda \ll (q^H)^{\lambda(s,k)-\Lambda+\epsilon}.$$

*Proof.* As in [13, Lemma 4.2], this follows from Hölder's inequality, Lemma 2.3 and the various definitions. □

## 3. The base case $k = 1$

In this section, we use the properties of our $(p,t)^*$-ellipsephic sets to prove that Theorem 2.1 holds in the base case $k = 1$. The arguments resemble those used in the author's paper [4], in which we proved that a similar theorem holds when $k = 2$. The following proposition takes the place of [13, Lemma 5.1] in the work of Wooley.

**Proposition 3.1.** *For* $t \geq 2$ *an integer, and* $p$ *an odd prime, let* $\mathcal{E}$ *be a* $(p,t)^*$*-ellipsephic set. Then* $\lambda(t,1) = 0$.

*Proof.* Let $0 < \tau < 1$, and let $B \in \mathbb{N}$ be sufficiently large in terms of $\tau$. Fix any $\mathfrak{a} \in \mathbb{D}$ and any $\phi \in \Phi_\tau(B)$, so that by definition we have $\phi(z) = z + p^c\psi(z)$ for some $c \geq \tau B$ and some $\psi \in \mathbb{Z}[z]$. Then $U^B_{t,1}(\mathfrak{a})$ counts solutions to the congruence

$$\sum_{i=1}^{t} \big(\phi(x_i) - \phi(y_i)\big) \equiv 0 \pmod{p^B} \tag{3.1}$$

with $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}^t$, and where each solution is counted with weight $\rho_0^{-2t}\mathfrak{a}_{\boldsymbol{x}}\mathfrak{a}_{\boldsymbol{y}}$. We may rewrite (3.1) in the form

$$\sum_{i=1}^{t} \big(x_i + p^c\psi(x_i)\big) \equiv \sum_{i=1}^{t} \big(y_i + p^c\psi(y_i)\big) \pmod{p^B}, \tag{3.2}$$

allowing us to deduce that

$$\sum_{i=1}^{t} x_i \equiv \sum_{i=1}^{t} y_i \pmod{p^{c_1}}, \tag{3.3}$$

where we write $c_1 = \min\{B, c\}$. This is effectively a "free" condition which was already contained in our original congruence (3.1).

We now recall a slightly simplified form of a definition which appeared in [4]. For $d \in \mathbb{N}$, and for weights $\mathfrak{b}$ with $|\mathfrak{b}_x| \leq 1$ for all $x \in \mathcal{E}$ and $0 < \sum_{x\in\mathcal{E}} |\mathfrak{b}_x| < \infty$, we define

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

which counts solutions to the congruence

$$\sum_{i=1}^{t} x_i \equiv \sum_{i=1}^{t} y_i \pmod{p^d}, \tag{3.4}$$

with weights $\mathfrak{b}_{\boldsymbol{x}}\overline{\mathfrak{b}_{\boldsymbol{y}}}$. (In the notation of [4], this is essentially $G_{0,d}(\mathbf{0},\mathfrak{b})$.) The following lemma is effectively a special case of [4, Lemma 2.2], which provides the key "lifting" step of the process, in which we make use of the $E_t^*$ property of our digit set to raise the power of $p$ used in our congruences. We present an outline of the proof here for completeness, and note that further details are available in [4].

**Lemma 3.2.** *We have*

$$G_d(\mathfrak{b}) \ll p^{\epsilon} \sum_{\boldsymbol{u}\in\mathcal{E}(p^d)^t} \Bigg| \sum_{\substack{\boldsymbol{x}\in\mathcal{E}^t \\ \boldsymbol{x}\equiv\boldsymbol{u} \ (mod\ p^d)}} \mathfrak{b}_{\boldsymbol{x}} \Bigg|^2 .$$

*Proof.* As in [4, Lemma 2.2], we write

$$x_i = \sum_{r\geq 0} x_i^{(r)} p^r \text{ and } y_i = \sum_{r\geq 0} y_i^{(r)} p^r,$$

with $x_i^{(r)}, y_i^{(r)} \in A_p$ for $1 \leq i \leq t$, and bound the number of solutions to (3.4) by considering each base $p$ digit in turn. For $h \in \mathbb{Z}$, 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 digits of our variables from lowest to highest, we see that a solution of (3.4) satisfies

$$(\boldsymbol{x}^{(r)}, \boldsymbol{y}^{(r)}) \in \widetilde{\mathcal{A}}_t(\lambda_r p - \lambda_{r-1}), \quad (0 \leq r \leq d-1)$$

for some $1-t \leq \lambda_0, \dots, \lambda_{d-1} \leq t-1$ reflecting the potential carry-over in our addition, and where we have written $\lambda_{-1} = 0$ for convenience. For such a tuple $\boldsymbol{\lambda} = (\lambda_0, \dots, \lambda_{d-1})$, we write

$$\boldsymbol{\lambda'} = (\lambda_0 p - \lambda_{-1}, \dots, \lambda_{d-1}p - \lambda_{d-2}).$$

For brevity, we use the notation $\underline{\boldsymbol{u}}$ to denote the tuple $(\boldsymbol{u}^{(0)}, \dots, \boldsymbol{u}^{(d-1)})$, and we write

$$\mathcal{A}_t(\boldsymbol{h}) = \left\{ \underline{\boldsymbol{u}} \in A_p^{td} \,\middle|\, \boldsymbol{u}^{(r)} \in \mathcal{A}_t(h_r) \text{ for } 0 \leq r \leq d-1 \right\}$$

and

$$\widetilde{\mathcal{A}}_t(\boldsymbol{h}) = \left\{ (\underline{\boldsymbol{u}}, \underline{\boldsymbol{v}}) \in A_p^{2td} \,\middle|\, (\boldsymbol{u}^{(r)}, \boldsymbol{v}^{(r)}) \in \widetilde{\mathcal{A}}_t(h_r) \text{ for } 0 \leq r \leq d-1 \right\}.$$

We observe that these are the sets of all possible variables with given digit sums, and that any solution of (3.4) lies in $\widetilde{\mathcal{A}}_t(\boldsymbol{\lambda'})$. Using this notation, we may write

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

Rearranging and applying the triangle inequality and Cauchy's inequality, we remove the dependence on $\boldsymbol{\lambda}$ to deduce that

$$\begin{aligned} G_d(\mathfrak{b}) &\ll \sum_{(\underline{\boldsymbol{u}},\underline{\boldsymbol{v}})\in\widetilde{\mathcal{A}}_t(\boldsymbol{0})} \sum_{\substack{\boldsymbol{x},\boldsymbol{y}\in\mathcal{E}^t\\ (\boldsymbol{x},\boldsymbol{y})\equiv(\boldsymbol{u},\boldsymbol{v}) \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}}\overline{\mathfrak{b}_{\boldsymbol{y}}} \\ &\ll \sum_{0\le\boldsymbol{n}\le t(p-1)} \Bigg( \sum_{\underline{\boldsymbol{u}}\in\mathcal{A}_t(\boldsymbol{n})} \Bigg| \sum_{\substack{\boldsymbol{x}\in\mathcal{E}^t\\ \boldsymbol{x}\equiv\boldsymbol{u} \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}} \Bigg|^2 \Bigg) \Bigg( \sum_{\underline{\boldsymbol{u}}\in\mathcal{A}_t(\boldsymbol{n})} 1 \Bigg). \end{aligned}$$

From our initial assumption that $\mathcal{E}$ is a $(p,t)^*$-ellipsephic set, we know that for $\boldsymbol{n} = (n_0,\dots,n_{d-1})$ with $0 \le \boldsymbol{n} \le t(p-1)$, we have

$$\#\mathcal{A}_t(\boldsymbol{n}) = \#\Bigg\{ \underline{\boldsymbol{u}} \in A_p^{td} \;\Bigg|\; \sum_{i=1}^t u_i^{(r)} = n_r \text{ for } 0 \le r \le d-1 \Bigg\} \ll \prod_{r=0}^{d-1} n_r^\epsilon \ll p^\epsilon,$$

and consequently

$$G_d(\mathfrak{b}) \ll p^\epsilon \sum_{\boldsymbol{u}\in\mathcal{E}(p^d)^t} \Bigg| \sum_{\substack{\boldsymbol{x}\in\mathcal{E}^t\\ \boldsymbol{x}\equiv\boldsymbol{u} \pmod{p^d}}} \mathfrak{b}_{\boldsymbol{x}} \Bigg|^2,$$

as claimed. □

*Proof of Proposition 3.1 (continued).* We now fix the weights $\mathfrak{b}$ appearing in Lemma 3.2 to be

$$\mathfrak{b}_x = \rho_0^{-1}\mathfrak{a}_x e(\alpha\phi(x)).$$

Then $G_{c_1}(\mathfrak{b})$ encodes the number of solutions to (3.3), counted with weights $\rho_0^{-2t}\mathfrak{a}_{\boldsymbol{x}}\mathfrak{a}_{\boldsymbol{y}} e\Big(\alpha\sum_{i=1}^t \big(\phi(x_i)-\phi(y_i)\big)\Big)$, and consequently we may insert the condition (3.3) into our original congruence in the form

$$\begin{aligned} U_{t,1}^B(\mathfrak{a}) &= \oint_{p^B} \Bigg| \rho_0^{-1} \sum_{x\in\mathcal{E}} \mathfrak{a}_x e(\alpha\phi(x)) \Bigg|^{2t} d\alpha \\ &= \oint_{p^B} G_{c_1}(\mathfrak{b})\, d\alpha. \end{aligned}$$

By Lemma 3.2, we have

$$U_{t,1}^B(\mathfrak{a}) \ll p^\epsilon \sum_{\boldsymbol{u}\in\mathcal{E}(p^{c_1})^t} \oint_{p^B} \Bigg| \sum_{\substack{\boldsymbol{x}\in\mathcal{E}^t\\ \boldsymbol{x}\equiv\boldsymbol{u} \pmod{p^{c_1}}}} \mathfrak{b}_{\boldsymbol{x}} \Bigg|^2 d\alpha,$$

where the integrand on the right-hand side now imposes the condition $\boldsymbol{x} \equiv \boldsymbol{y} \equiv \boldsymbol{u} \pmod{p^{c_1}}$. The fact that $p^{c_1}$ divides $x_i - y_i$ implies that $p^{c_1}$ divides

$\psi(x_i)-\psi(y_i)$ for $1 \leq i \leq t$, and substituting this into (3.2) gives the congruence

$$\sum_{i=1}^{t} x_i \equiv \sum_{i=1}^{t} y_i \pmod{p^{c_2}},$$

where $c_2 = \min\{2c, B\}$. Repeating this process, we eventually reach the point at which our congruence holds modulo $p^{c_j}$ with $c_j = \min\{jc, B\} = B$, and since $c \geq \tau B$, this happens after at most $\lceil \tau^{-1} \rceil$ steps. Now

$$U_{t,1}^{B}(\mathfrak{a}) \ll p^{\epsilon} \sum_{\boldsymbol{u} \in \mathcal{E}(p^B)^t} \oint_{p^B} \Big| \sum_{\substack{\boldsymbol{x} \in \mathcal{E}^t \\ \boldsymbol{x} \equiv \boldsymbol{u} \ (\mathrm{mod}\ p^B)}} \mathfrak{b}_{\boldsymbol{x}} \Big|^2 \, d\alpha,$$

so returning to the definition of the weights $\mathfrak{b}$, we obtain

$$\begin{aligned} U_{t,1}^{B}(\mathfrak{a}) &\ll p^{\epsilon} \rho_0^{-2t} \sum_{\boldsymbol{u} \in \mathcal{E}(p^B)^t} \oint_{p^B} \Big| \sum_{\substack{\boldsymbol{x} \in \mathcal{E}^t \\ \boldsymbol{x} \equiv \boldsymbol{u} \ (\mathrm{mod}\ p^B)}} \mathfrak{a}_{\boldsymbol{x}} e\Big(\alpha \sum_{i=1}^{t} \phi(x_i)\Big) \Big|^2 \, d\alpha \\ &= p^{\epsilon} \rho_0^{-2t} \sum_{\boldsymbol{u} \in \mathcal{E}(p^B)^t} \oint_{p^B} \Big| \prod_{i=1}^{t} \rho_B(u_i) f_B(\alpha, u_i) \Big|^2 \, d\alpha. \end{aligned}$$

Using Hölder's inequality twice, we see that

$$\begin{aligned} U_{t,1}^{B}(\mathfrak{a}) &\ll p^{\epsilon} \rho_0^{-2t} \sum_{\boldsymbol{u} \in \mathcal{E}(p^B)^t} \prod_{i=1}^{t} \rho_B(u_i)^2 \Big( \oint_{p^B} |f_B(\alpha, u_i)|^{2t} \, d\alpha \Big)^{1/t} \\ &= p^{\epsilon} \rho_0^{-2t} \Bigg( \sum_{u \in \mathcal{E}(p^B)} \rho_B(u)^2 \Big( \oint_{p^B} |f_B(\alpha, u)|^{2t} \, d\alpha \Big)^{1/t} \Bigg)^t \\ &\ll p^{\epsilon} \rho_0^{-2} \sum_{u \in \mathcal{E}(p^B)} \rho_B(u)^2 \oint_{p^B} |f_B(\alpha, u)|^{2t} \, d\alpha = p^{\epsilon} U_{t,1}^{B,B}(\mathfrak{a}). \end{aligned}$$

We may assume that $B$ is sufficiently large to give $p^{\epsilon} \ll q^{B\epsilon}$, and consequently we deduce that

$$\frac{\log(U_{t,1}^{B}(\mathfrak{a}) / U_{t,1}^{B,B}(\mathfrak{a}))}{\log q^B} \ll \epsilon$$

for any $\epsilon > 0$, and hence, using the definition (2.4), we find that $\lambda(t, 1) = 0$ as claimed. □

## 4. The hierarchy

In order to prove Theorem 1.2, we assume that $\Lambda = \lambda(tk(k+1)/2, k) > 0$, and work towards a contradiction. We introduce small positive numbers

$$0 < \epsilon < \tau < \delta < \mu < 1, \tag{4.1}$$

which form a hierarchy in the sense that each element is assumed to be small enough in terms of $k, \Lambda$ and the larger parameters in the inequality (4.1). We may then choose $B$ large enough, in terms of all of the above, to ensure that, writing $H = \lceil B/k \rceil$, we have

$$U_{s,k}^{B}(\mathfrak{a}) \geq (q^H)^{\Lambda-\epsilon} U_{s,k}^{B,H}(\mathfrak{a}). \tag{4.2}$$

By Lemma 2.3, we may assume that for all $h \in \mathbb{N}_0$ with $h \leq (1-\delta)H$, and for all $\mathfrak{a}' \in \mathbb{D}$, we have

$$U_{s,k}^{B,h}(\mathfrak{a}') \leq (q^{H-h})^{\Lambda+\epsilon} U_{s,k}^{B,H}(\mathfrak{a}').$$

We also fix parameters

$$\nu = \lceil 4\epsilon H \Lambda^{-1} \rceil \quad \text{and} \quad \theta = \lceil \mu H \rceil \tag{4.3}$$

for use in the remainder of the paper, and observe that the existence of $\nu$ is dependent on our assumption that $\Lambda > 0$. The following lemmata provide bounds for $U_{s,k}^{B}(\mathfrak{a})$ which allow us to initiate our iterative process in Section 6.

**Lemma 4.1.** *We have $U_{s,k}^{B}(\mathfrak{a}) \ll q^{s\nu} K_{\nu,\nu,c}^{1,\phi,\nu}(\mathfrak{a})$.*

*Proof.* As in [13, Lemma 6.1], we use the definitions and Hölder's inequality to obtain

$$U_{s,k}^{B}(\mathfrak{a}) \ll U_{s,k}^{B,\nu}(\mathfrak{a}) + q^{s\nu} K_{\nu,\nu,c}^{1,\phi,\nu}(\mathfrak{a}).$$

By Lemma 2.3, and using (4.3), we have

$$\begin{aligned} U_{s,k}^{B,\nu}(\mathfrak{a}) &\ll (q^{H-\nu})^{\Lambda+\epsilon} U_{s,k}^{B,H}(\mathfrak{a}) \\ &\ll q^{-2\epsilon H} (q^H)^{\Lambda-\epsilon} U_{s,k}^{B,H}(\mathfrak{a}), \end{aligned}$$

and by (4.2), this implies

$$U_{s,k}^{B,\nu}(\mathfrak{a}) \ll q^{-2\epsilon H} U_{s,k}^{B}(\mathfrak{a}),$$

so that

$$U_{s,k}^{B}(\mathfrak{a}) \ll q^{s\nu} K_{\nu,\nu,c}^{1,\phi,\nu}(\mathfrak{a})$$

as claimed. □

**Lemma 4.2.** *For $a, b \in \mathbb{N}_0$ with $a \leq b$, and for $w > 0$ and $\xi \in \mathcal{E}$, we have*

$$\rho_a(\xi)^2 \left| f_a(\boldsymbol{\alpha}; \xi) \right|^{2w} \leq q^{w(b-a)} \sum_{\substack{\zeta \in \mathcal{E}(p^b) \\ \zeta \equiv \xi \ (mod\ p^a)}} \rho_b(\zeta)^2 \left| f_b(\boldsymbol{\alpha}; \zeta) \right|^{2w}.$$

*Proof.* Apply Hölder's inequality exactly as in [13, Lemma 6.2]. □

**Lemma 4.3.** *We have $U_{s,k}^{B}(\mathfrak{a}) \ll q^{s\theta} K_{\theta,\theta,c}^{1,\phi,\nu}(\mathfrak{a})$.*

*Proof.* Apply Lemma 4.2 twice, as in [13, Lemma 6.3], to obtain

$$K_{\nu,\nu,c}^{1,\phi,\nu}(\mathfrak{a}) \ll q^{s(\theta-\nu)} K_{\theta,\theta,c}^{1,\phi,\nu}(\mathfrak{a}),$$

and substitute this into Lemma 4.1 to see that

$$U_{s,k}^{B}(\mathfrak{a}) \ll q^{s\nu} q^{s(\theta-\nu)} K_{\theta,\theta,c}^{1,\phi,\nu}(\mathfrak{a}) = q^{s\theta} K_{\theta,\theta,c}^{1,\phi,\nu}(\mathfrak{a})$$

as required. □

## 5. The iterative process

Let $k \geq 2$, and suppose that Theorem 2.1 holds for exponents smaller than $k$. In this section, we make use of the inductive hypothesis and provide the key lemmata underlying our iterative process, before completing the proof of the theorem in Section 6. We begin with a lemma which raises the power of $p$ involved in one of our congruences, at a small cost.

**Lemma 5.1.** *Let $a, b, r \in \mathbb{N}$ with $1 \leq r \leq k-1$ and $\min\{a,b\} \geq \delta\theta$. Suppose that*

$$ra \leq (k-r+1)b \leq B,$$

*and set*

$$b' = \lceil (k-r+1)b/r \rceil.$$

*Then $K^{r,\phi,\nu}_{a,b,c}(\mathfrak{a}) \ll q^{tk^2\nu} K^{r,\phi,\nu}_{b',b,c}(\mathfrak{a})$.*

*Proof.* We focus on $K^{r,\phi,\nu}_{a,b,c}(\mathfrak{a};\xi,\eta)$, in which we may assume that $p^\gamma \| (\xi-\eta)$ for some $\gamma < \nu$, and write $\xi - \eta = \omega p^\gamma$ with $(\omega, p) = 1$. We introduce

$$B' = (k-r+1)b - ra - (k-r)\gamma,$$

and in the case $B' \leq \nu$, we apply Lemma 4.2 as in [13, Lemma 7.1] to obtain $K^{r,\phi,\nu}_{a,b,c}(\mathfrak{a}) \ll q^{tk^2\nu} K^{r,\phi,\nu}_{b',b,c}(\mathfrak{a})$.

When $B' > \nu$, we consider the solutions counted by $K^{r,\phi,\nu}_{a,b,c}(\mathfrak{a};\xi,\eta)$ and, via the same argument used in [13, Lemma 7.1], deduce that any such solution satisfies

$$(\omega p^\gamma)^{k-r} \sum_{i=1}^{R} (p^a)^l \big(\Psi_l(u_i) - \Psi_l(v_i)\big) \equiv 0 \pmod{p^{(k-r+1)b}} \quad (1 \leq l \leq r),$$

where $\Psi_l(z) = z^l + p^{a-(k-r)\gamma}\Xi_l(z)$ for some $\Xi_l \in \mathbb{Z}[z]$. Our hierarchy (4.1) allows us to ensure that

$$k\gamma < k\nu \leq \delta a,$$

and therefore we have

$$a - (k-r)\gamma > (1-\delta)a > \tau B,$$

so the system of polynomials $\boldsymbol{\Psi}$ is $p^c$-spaced for some $c > \tau(k-r+1)b$, and satisfies

$$\sum_{i=1}^{R} \Psi_l(u_i) \equiv \sum_{i=1}^{R} \Psi_l(v_i) \pmod{p^{B'}} \quad (1 \leq l \leq r).$$

Further manipulations, as in [13, Lemma 7.1], lead to the conclusion that

$$K^{r,\phi,\nu}_{a,b,c}(\mathfrak{a}) = \oint_{p^B} U^{B'}_{R,r}(\mathfrak{c})\, |f_b(\boldsymbol{\alpha},\eta)|^{2s-2R}\, d\boldsymbol{\alpha},$$

where $\mathfrak{c}_u = \mathfrak{a}_{p^a u+\xi}\, e\big(\psi(p^a u + \xi; \boldsymbol{\alpha})\big)$. At this point, we apply the inductive hypothesis, in the form of Corollary 2.2, to deduce that

$$U^{B'}_{R,r}(\mathfrak{c}) \ll q^{B'\epsilon^2} U^{B',H'}_{R,r}(\mathfrak{c}).$$

Applying Lemma 4.2 and carrying out a series of substitutions, as in [13, Lemma 7.1], we obtain

$$K_{a,b,c}^{r,\boldsymbol{\phi},\nu}(\mathfrak{a}) \ll q^{B'\epsilon^2+R(b'-a-H')}K_{b',b,c}^{r,\boldsymbol{\phi},\nu}(\mathfrak{a}).$$

Finally, we have

$$R(b'-a-H') = tr(r+1)(b'-a-H')/2 < tk^2\nu/2,$$

and so, using the hierarchy (4.1), we see that

$$K_{a,b,c}^{r,\boldsymbol{\phi},\nu}(\mathfrak{a}) \ll q^{tk^2\nu}K_{b',b,c}^{r,\boldsymbol{\phi},\nu}(\mathfrak{a}),$$

as required. □

From now on we drop any reference to $\boldsymbol{\phi}, \nu$ and $c$ in our notation, since they are assumed to remain fixed. Let $a, b, r \in \mathbb{N}$ satisfy the hypotheses of Lemma 5.1, and let $b' = \lceil (k-r+1)b/r \rceil$. We wish to swap the congruences modulo $p^{b'}$ and modulo $p^b$, which will ultimately permit us to iterate our lifting process.

**Lemma 5.2.** *For $r \geq 2$, we have*

$$K_{a,b}^{r}(\mathfrak{a}) \ll q^{tk^2\nu}K_{b,b'}^{k-r}(\mathfrak{a})^{1/(k-r+1)}K_{b',b}^{r-1}(\mathfrak{a})^{(k-r)/(k-r+1)}.$$

*When $r = 1$, we have*

$$K_{a,b}^{1}(\mathfrak{a}) \ll q^{tk^2\nu}K_{b,kb}^{k-1}(\mathfrak{a})^{1/k}U_{s,k}^{B,b}(\mathfrak{a})^{1-1/k}.$$

*Proof.* As in [13, Lemma 8.1], we apply Hölder's inequality to obtain

$$K_{b',b}^{r}(\mathfrak{a}) \ll K_{b,b'}^{k-r}(\mathfrak{a})^{1/(k-r+1)}K_{b',b}^{r-1}(\mathfrak{a})^{(k-r)/(k-r+1)},$$

so when $r \geq 2$ we are done by Lemma 5.1. When $r = 1$, we observe that $K_{b',b}^{0}(\mathfrak{a}) = U_{s,k}^{B,b}(\mathfrak{a})$, which gives the claimed result. □

We now bound the normalised version of our mean values, and we write $\widetilde{K}_{a,b}^{r}(\mathfrak{a})$ as shorthand for $\widetilde{K}_{a,b}^{r}(\mathfrak{a})_\Lambda$.

**Lemma 5.3.** *For $r \geq 2$, we have*

$$\widetilde{K}_{a,b}^{r}(\mathfrak{a}) \ll q^{tk^2\nu}\widetilde{K}_{b,b'}^{k-r}(\mathfrak{a})^{1/(k-r+1)}\widetilde{K}_{b',b}^{r-1}(\mathfrak{a})^{1-1/r}.$$

*When $r = 1$, we have*

$$\widetilde{K}_{a,b}^{1}(\mathfrak{a}) \ll q^{2tk^2\nu}\widetilde{K}_{b,kb}^{k-1}(\mathfrak{a})^{1/k}(q^{-b})^{\Lambda(1-1/k)}.$$

*Proof.* As in [13, Lemma 8.2], when $r \geq 2$ we use Lemma 5.2 and (2.5) to conclude that

$$\widetilde{K}_{a,b}^{r}(\mathfrak{a}) \ll (q^{tk^2\nu})^{(k-1)/r(k-r)}\widetilde{K}_{b,b'}^{k-r}(\mathfrak{a})^{1/(k-r+1)}\widetilde{K}_{b',b}^{r-1}(\mathfrak{a})^{1-1/r},$$

which leads directly to the desired conclusion since $(k-1)/r(k-r) \leq 1$ for $1 \leq r \leq k-1$. When $r = 1$, we have

$$\widetilde{K}_{a,b}^{1}(\mathfrak{a}) \ll q^{tk^2\nu}\widetilde{K}_{b,kb}^{k-1}(\mathfrak{a})^{1/k}V^{1-1/k},$$

where

$$V = \frac{U_{s,k}^{B,b}(\mathfrak{a})}{q^{\Lambda H}U_{s,k}^{B,H}(\mathfrak{a})}.$$

We also have

$$U_{s,k}^{B,b}(\mathfrak{a}) \ll (q^{H-b})^{\Lambda+\epsilon} U_{s,k}^{B,H}(\mathfrak{a}),$$

by Lemma 2.3, and consequently

$$V \ll q^{\epsilon H - b(\Lambda+\epsilon)} \ll q^{s\nu - \Lambda b}.$$

We therefore see that

$$\begin{aligned}\widetilde{K}_{a,b}^{1}(\mathfrak{a}) &\ll q^{tk^2\nu} \widetilde{K}_{b,kb}^{k-1}(\mathfrak{a})^{1/k} (q^{s\nu-\Lambda b})^{1-1/k} \\ &\ll q^{2tk^2\nu} \widetilde{K}_{b,kb}^{k-1}(\mathfrak{a})^{1/k} (q^{-\Lambda b})^{1-1/k}\end{aligned}$$

since $s = tk(k+1)/2 \leq tk^2$. □

For $1 \leq j \leq k-1$, we write $\rho_j = j/(k-j+1)$ and $b_j = \lceil b/\rho_j \rceil$. In the next lemma, we make use of the inductive hypothesis to improve our bound on $\widetilde{K}_{a,b}^{r}(\mathfrak{a})$.

**Lemma 5.4.** *Let $1 \leq r \leq k-1$, and let $a \geq \delta\theta$ and $b \geq k\delta\theta$ with $ra \leq (k-r+1)b$. Then for $kb \leq B$, we have*

$$\widetilde{K}_{a,b}^{r}(\mathfrak{a}) \ll q^{(r+1)tk^2\nu} (q^{-b})^{\Lambda(1-1/k)/r} \prod_{j=1}^{r} \widetilde{K}_{b,b_j}^{k-j}(\mathfrak{a})^{\rho_j/r}.$$

*Proof.* When $r = 1$, this follows immediately from Lemma 5.3. For $r \geq 2$, we proceed inductively, as in [13, Lemma 9.1]. Suppose that the conclusion is known for all $r < r_0$ for some $2 \leq r_0 \leq k-1$. By Lemma 5.3, we have

$$\widetilde{K}_{a,b}^{r_0}(\mathfrak{a}) \ll q^{tk^2\nu} \widetilde{K}_{b,b_0}^{k-r_0}(\mathfrak{a})^{1/(k-r_0+1)} \widetilde{K}_{b_0,b}^{r_0-1}(\mathfrak{a})^{1-1/r_0}, \tag{5.1}$$

with $b_0 = b_{r_0} = \lceil (k-r_0+1)b/r_0 \rceil \geq 2b/k > \delta\theta$. We also have

$$(r_0-1)b_0 \leq (r_0-1)\big((k-r_0+1)b/r_0 + 1\big) < (k-r_0+2)b,$$

where the second inequality follows from (4.3) and the fact that we may choose $B$ sufficiently large. We therefore use the inductive hypothesis to bound $\widetilde{K}_{b_0,b}^{r_0-1}(\mathfrak{a})$, obtaining

$$\widetilde{K}_{b_0,b}^{r_0-1}(\mathfrak{a}) \ll q^{r_0tk^2\nu} (q^{-b})^{\Lambda(1-1/k)/(r_0-1)} \prod_{j=1}^{r_0-1} \widetilde{K}_{b,b_j}^{k-j}(\mathfrak{a})^{\rho_j/(r_0-1)}.$$

Substituting this into (5.1), and writing $\rho_0 = \rho_{r_0} = r_0/(k-r_0+1)$, we see that

$$\begin{aligned}\widetilde{K}_{a,b}^{r_0}(\mathfrak{a}) &\ll q^{tk^2\nu+(r_0-1)tk^2\nu} (q^{-b})^{\Lambda(1-1/k)/r_0} \widetilde{K}_{b,b_0}^{k-r_0}(\mathfrak{a})^{\rho_0/r_0} \prod_{j=1}^{r_0-1} \widetilde{K}_{b,b_j}^{k-j}(\mathfrak{a})^{\rho_j/r_0} \\ &\ll q^{r_0tk^2\nu} (q^{-b})^{\Lambda(1-1/k)/r_0} \prod_{j=1}^{r_0} \widetilde{K}_{b,b_j}^{k-j}(\mathfrak{a})^{\rho_j/r_0},\end{aligned}$$

and so the lemma follows by induction. □

**Lemma 5.5.** *Suppose that all of the hypotheses of Lemma 5.4 hold. Then there exists an integer $r'$ with $1 \le r' \le r$ such that*

$$\widetilde{K}^r_{a,b}(\mathfrak{a}) \ll \widetilde{K}^{k-r'}_{b,b_{r'}}(\mathfrak{a})^{\rho_{r'}}(q^{-b})^{\Lambda/(2k)}.$$

*Proof.* As in [13, Lemma 9.2], we combine the inequality

$$|z_1 \dots z_n| \le |z_1|^n + \dots + |z_n|^n$$

with Lemma 5.4 to obtain

$$\widetilde{K}^r_{a,b}(\mathfrak{a}) \ll q^{(r+1)tk^2\nu}(q^{-b})^{\Lambda(1-1/k)/r}\sum_{j=1}^{r}\widetilde{K}^{k-j}_{b,b_j}(\mathfrak{a})^{\rho_j}.$$

In particular, for some $1 \le r' \le r$, we have

$$\widetilde{K}^r_{a,b}(\mathfrak{a}) \ll q^{(r+1)tk^2\nu}(q^{-b})^{\Lambda(1-1/k)/r}\widetilde{K}^{k-r'}_{b,b_{r'}}(\mathfrak{a})^{\rho_{r'}},$$

so it remains to prove that

$$q^{(r+1)tk^2\nu}(q^{-b})^{\Lambda(1-1/k)/r} \le (q^{-b})^{\Lambda/(2k)}. \tag{5.2}$$

We have $(1-1/k)/r \ge 1/k$ for $1 \le r \le k-1$, so

$$q^{(r+1)tk^2\nu}(q^{-b})^{\Lambda(1-1/k)/r} \le q^{(r+1)tk^2\nu}(q^{-b})^{\Lambda/k}.$$

By our assumptions on $b$ and $r$, and using (4.3), we see that

$$b\Lambda/k \ge \delta\theta\Lambda \ge \delta\mu H\Lambda \text{ and } 2tk^3\nu \ge 2(r+1)tk^2\nu,$$

and by (4.1) and (4.3), we may choose our parameters to ensure that

$$\delta\mu H\Lambda > 2tk^3\lceil 4\epsilon H\Lambda^{-1}\rceil = 2tk^3\nu,$$

so

$$q^{(r+1)tk^2\nu} \le q^{b\Lambda/(2k)}$$

and (5.2) is proved. □

Finally, we use Lemma 5.5 to deduce an iterative bound of the necessary shape, which will be used in Section 6 to prove Theorem 2.1.

**Lemma 5.6.** *Let $1 \le r \le k-1$, and suppose $a \ge \delta\theta$ and $b \ge k^2\delta\theta$ with $ra \le (k-r+1)b$. Then whenever $k^2b \le B$, there exist integers $r'$ with $1 \le r' \le k-1$, as well as $a' \ge \delta\theta$ and $b' \ge k^2\delta\theta$ with $r'a' \le (k-r'+1)b'$, and there exists a real number $0 < \rho \le (1-1/k)^2$ satisfying*

$$(1+2/k)b \le b' \le k^2b, \qquad b' = \left\lceil \frac{(r'+1)a'}{k-r'} \right\rceil, \qquad \rho b' \ge b,$$

*and such that*

$$\widetilde{K}^r_{a,b}(\mathfrak{a}) \ll \widetilde{K}^{r'}_{a',b'}(\mathfrak{a})^{\rho}(q^{-b})^{\Lambda/(2k)}.$$

*Proof.* Exactly as in [13, Lemma 9.3], we apply Lemma 5.5 twice, and then verify that the conditions hold. □

## 6. Proof of Theorem 2.1

Throughout this section, we consider $k \in \mathbb{N}$ and let $s = tk(k+1)/2$. The case $k = 1$ has been handled in Proposition 3.1, so we may assume that $k \geq 2$, and that Theorem 2.1 is known for exponents smaller than $k$. If $\lambda(s,k) \leq 0$, we are done, so we assume that $\lambda(s,k) = \Lambda > 0$ and work towards a contradiction. As in [13, Section 10], we use Lemma 4.3 and our hierarchy (4.1) to see that

$$\widetilde{K}^1_{\theta,\theta}(\mathfrak{a}) \gg q^{-2s\theta}. \tag{6.1}$$

We now set $N = \lceil 16sk/\Lambda \rceil$, again noting that the existence of $N$ depends on the assumption that $\Lambda > 0$, and repeatedly apply Lemma 5.6 to obtain sequences $(a_n), (b_n), (r_n)$ and $(\rho_n)$ for $0 \leq n \leq N$, satisfying

$$1 \leq r_n \leq k-1, \quad k^2\delta\theta \leq b_n \leq k^{2n+2}\theta, \quad \delta\theta \leq a_n \leq (k - r_n + 1)b_n/r_n,$$

and, for $n \geq 1$,

$$0 < \rho_n \leq (1 - 1/k)^2, \quad \rho_n b_n \geq b_{n-1},$$

and such that

$$\widetilde{K}^1_{\theta,\theta}(\mathfrak{a}) \ll \widetilde{K}^{r_n}_{a_n,b_n}(\mathfrak{a})^{\rho_1 \ldots \rho_n}(q^{-\Lambda/(2k)})^{nb_0}, \tag{6.2}$$

where the empty product $\rho_1 \ldots \rho_n$ for $n = 0$ is interpreted as 1. The initial choice $a_0 = b_0 = \theta$ and $r_0 = \rho_0 = 1$ therefore trivially satisfies (6.2). We prove the existence of such sequences by induction, following the same argument used in [13, Section 10].

Using (6.2) in the case $n = N$ in conjunction with (6.1), and writing $\rho = \rho_1 \ldots \rho_N$, gives the bound

$$q^{-2s\theta} \ll \widetilde{K}^{r_N}_{a_N,b_N}(\mathfrak{a})^{\rho}(q^{-\Lambda/(2k)})^{N\theta}, \tag{6.3}$$

and applying Lemma 2.4 in the case where $\lambda(s,k) = \Lambda$ gives

$$\widetilde{K}^{r_N}_{a_N,b_N}(\mathfrak{a}) \ll q^{H\epsilon}. \tag{6.4}$$

By our hierarchy (4.1), in combination with (6.3) and (6.4), we may assume that $H\epsilon \leq \theta$, so that

$$q^{-2s\theta} \ll (q^{\rho - N\Lambda/(2k)})^{\theta}. \tag{6.5}$$

We now observe that (4.3) implies that $q^\theta$ is sufficiently large with respect to $s$, $k$ and $\Lambda$, so (6.5) can only hold if $4s \geq N\Lambda/(2k)$. The definition of N leads ultimately to the relation

$$\Lambda \leq 8sk/N \leq \Lambda/2,$$

a contradiction to the assumption that $\lambda(s,k) = \Lambda > 0$, and so Theorem 2.1 is proved. □

## 7. Proof of Theorem 1.2

As in [4], it suffices to prove Theorem 1.2 for $X$ a suitably large power of $p$; a convenient choice here turns out to be $X = p^H$, for $H = \lceil B/k \rceil$ as defined in Section 4. We may also assume that we work with a choice of weights satisfying $\mathfrak{a}_x = 0$ for $x \notin \mathcal{E}(X)$.

By Corollary 2.2, we find that

$$\oint_{p^B} |f(\boldsymbol{\alpha})|^{2s} \, d\boldsymbol{\alpha} \ll q^{H\epsilon} \rho_0^{-2} \sum_{\xi \in \mathcal{E}(p^H)} \rho_H(\xi)^2 \oint_{p^B} |f_H(\boldsymbol{\alpha}, \xi)|^{2s} \, d\boldsymbol{\alpha}.$$

By (2.1) and Cauchy's inequality, we see that

$$\begin{aligned} \rho_H(\xi)^2 \, |f_H(\boldsymbol{\alpha}, \xi)|^2 &= \Bigg| \sum_{\substack{x \in \mathcal{E}(X) \\ x \equiv \xi \pmod{p^H}}} \mathfrak{a}_x e(\psi(x; \boldsymbol{\alpha})) \Bigg|^2 \\ &\le \Bigg( \sum_{\substack{x \in \mathcal{E}(X) \\ x \equiv \xi \pmod{p^H}}} \mathfrak{a}_x^2 \Bigg) \Bigg( \sum_{\substack{x \in \mathcal{E}(X) \\ x \equiv \xi \pmod{p^H}}} 1 \Bigg) = \mathfrak{a}_\xi^2, \end{aligned}$$

and consequently that

$$\oint_{p^B} |f(\boldsymbol{\alpha})|^{2s} \, d\boldsymbol{\alpha} \ll q^{H\epsilon} \rho_0^{-2} \sum_{\xi \in \mathcal{E}(p^H)} \mathfrak{a}_\xi^2 \ll q^{H\epsilon} \ll p^{H\epsilon}.$$

We therefore have

$$\oint |f(\boldsymbol{\alpha})|^{2s} \, d\boldsymbol{\alpha} \le \oint_{p^B} |f(\boldsymbol{\alpha})|^{2s} \, d\boldsymbol{\alpha} \ll X^\epsilon,$$

and Theorem 1.2 is proved. □

## 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 quadratic case, arXiv:1912.04338.

[5] 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.

[6] 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.

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

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

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

[10] 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.

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

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

[13] 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