ESSENTIAL NUMBER THEORY

The cubic case of Vinogradov’s mean value theorem

D. R. Heath-Brown

2022

vol. 1 no. 1

msp

Essential Number Theory
Vol. 1, No. 1, 2022
https://doi.org/10.2140/ent.2022.1.1

The cubic case of Vinogradov's mean value theorem

D. R. Heath-Brown

We present a self-contained proof of the cubic case of Vinogradov's mean value theorem, based on Wooley's "efficient congruencing" approach.

1. Introduction

In a remarkable series of papers, Wooley [2012; 2013; 2015; 2016; 2017], and in collaboration with Ford [Ford and Wooley 2014], has made dramatic progress with Vinogradov's mean value theorem. This culminated in the full proof of the main conjecture, by Bourgain, Demeter and Guth [Bourgain et al. 2016], using rather different methods — but see [Wooley 2019] for a subsequent treatment by the original approach. Wooley's survey article [2014] gives an excellent introduction to his results and their applications.

The mean value theorem concerns the integer $J_{s,k}(X)$ defined as the number of solutions $(x_1, \dots, x_{2s}) \in \mathbb{N}^{2s}$ of the simultaneous equations

$$x_1^j + \cdots + x_s^j = x_{s+1}^j + \cdots + x_{2s}^j \quad (1 \le j \le k) \tag{1}$$

with $x_1, \dots, x_{2s} \le X$. Here $X \ge 1$ is an arbitrary real number, and s and k are positive integers, which one treats as being fixed. The key feature of this system is that if $(x_1, \dots, x_{2s})$ is a solution, so is any translate $(x_1 + c, \dots, x_{2s} + c)$.

The various forms of the Vinogradov mean value theorem give upper bounds for $J_{s,k}(X)$. It is not hard to see that

$$J_{s,k}(X) \gg_{s,k} X^s + X^{2s-k(k+1)/2},$$

for $X \ge 1$, and the central conjecture is that

$$J_{s,k}(X) \ll_{s,k,\varepsilon} X^{\varepsilon}(X^s + X^{2s-k(k+1)/2})$$

for any $\varepsilon > 0$. "Classically" this was known for $k = 1$ and 2, for $s \le k + 1$, and for $s \ge s_0(k)$ with a value $s_0(k) \ll k^2 \log k$. However Wooley [2012] showed that one may take $s_0(k) = k^2 + k$. Moreover, in [Wooley 2016], he showed that the full conjecture holds for $k = 3$.

MSC2020: primary 11L15; secondary 11D45, 11L07.
Keywords: exponential sum, mean value, cubic, Vinogradov.

The purpose of this paper is to present a much simplified version of Wooley's methods, sufficient to handle the case $k=3$.

Theorem. *We have*

$$J_{6,3}(X) \ll_{\varepsilon} X^{6+\varepsilon}$$

for any fixed $\varepsilon > 0$.

It is trivial from (2) below that if s and t are any positive integers then we will have $J_{s+t,k}(X) \le X^{2t} J_{s,k}(X)$ and $J_{s,k}(X) \le J_{s+t,k}(X)^{s/(s+t)}$. Thus for $k=3$ we can deduce the general case of the conjecture immediately from the theorem.

It should be stressed that, while the argument of the present paper appears cleaner and shorter than that presented by Wooley [2016], the underlying principles are the same.

2. Outline of the proof

Investigations into the mean value theorem depend crucially on an alternative interpretation of $J_{s,k}(X)$ in terms of exponential sums. If $\boldsymbol{\alpha} \in \mathbb{R}^k$ we write

$$f_k(\boldsymbol{\alpha};\, X) = f(\boldsymbol{\alpha}) = \sum_{x \le X} e(\alpha_1 x + \cdots + \alpha_k x^k),$$

whence

$$J_{s,k}(X) = \int_{(0,1]^k} |f(\boldsymbol{\alpha})|^{2s}\, d\boldsymbol{\alpha}. \tag{2}$$

Our version of the efficient congruencing method will also use the exponential sums

$$f_k(\boldsymbol{\alpha};\, X, \xi, a) = f_a(\boldsymbol{\alpha};\, \xi) = \sum_{\substack{x \le X \\ x \equiv \xi \pmod{p^a}}} e(\alpha_1 x + \cdots + \alpha_k x^k),$$

where p is prime and a is a positive integer exponent. The prime $p \ge 5$ will be chosen to be a small power of X. Since it will not change during the argument we will not include it explicitly among the parameters for $f_a(\boldsymbol{\alpha};\, \xi)$. Taking s and k as fixed we will write

$$I_m(X;\, \xi, \eta;\, a, b) = \int_{(0,1]^k} |f_a(\boldsymbol{\alpha};\, \xi)|^{2m} |f_b(\boldsymbol{\alpha};\, \eta)|^{2(s-m)}\, d\boldsymbol{\alpha}, \quad (0 \le m \le s-1),$$

which counts solutions of (1) in which

$$x_i \equiv \xi \pmod{p^a} \quad (1 \le i \le m \text{ and } s+1 \le i \le s+m),$$

and

$$x_i \equiv \eta \pmod{p^b} \quad (m+1 \le i \le s \text{ and } s+m+1 \le i \le 2s).$$

We will use this notation even when p^a or p^b is larger than X. We observe that when $m = 0$ we have

$$I_0(X; \xi, \eta; a, b) = \int_{(0,1]^k} |f_b(\boldsymbol{\alpha}; \eta)|^{2s}\, d\boldsymbol{\alpha},$$

which is independent of ξ and a.

We will also work with $I_m(X; a, b)$ defined by

$$I_0(X; a, b) = \max_{\eta \pmod{p^b}} I_0(X; \xi, \eta; a, b)$$

and

$$I_m(X; a, b) = \max_{\xi \not\equiv \eta \pmod{p}} I_m(X; \xi, \eta; a, b) \quad (1 \le m \le s-1).$$

The condition $\xi \not\equiv \eta \pmod{p}$ is the last remaining vestige of Wooley's "conditioning" step. Wooley [2016, page 538] uses functions $I^m_{a,b}(X)$ and $K^m_{a,b}(X)$, both of which correspond to our function $I_m(X; a, b)$. We are able to work with a single (simpler) function because we have a simpler version of the conditioning process.

Although many of our results can be proved for general s and k we shall now specialize to the case $s = 6$, $k = 3$, and write $J(X) = J_{6,3}(X)$ for brevity. We proceed to present a series of estimates relating $J(X)$ and $I_m(X; a, b)$ for $m = 0, 1, 2$, with various values of a and b. Iterating these will ultimately establish our theorem. The lemmas below will be proved in the next section. For the time being we content ourselves with stating the results, and showing how they lead to the theorem.

When $m = 0$ we can relate $I_0(X; a, b)$ to $J(X)$ as follows.

Lemma 1. *If $p^b \le X$ we have*

$$I_0(X; a, b) \le J(2X/p^b).$$

Our next result shows how to bound $J(X)$ in terms of $I_2(X; 1, 1)$.

Lemma 2. *If $p \le X$ we have*

$$J(X) \ll pJ(2X/p) + p^{12} I_2(X; 1, 1).$$

One way to compare values of $I_1(X; a, b)$ and $I_2(X; a, b)$ is by applying Hölder's inequality. We give two such estimates.

Lemma 3. *We have*

$$I_2(X; a, b) \le I_2(X; b, a)^{1/3} I_1(X; a, b)^{2/3}$$

irrespective of the size of p.

Lemma 4. *If $p^b \le X$ we have*

$$I_1(X; a, b) \le I_2(X; b, a)^{1/4} J(2X/p^b)^{3/4}.$$

Next we show how successively larger values of a and b arise.

Lemma 5. *For any p we have*

$$I_1(X; a, b) \le p^{3b-a} I_1(X; 3b, b)$$

if $1 \le a \le 3b$.

Lemma 6. *For any prime p we have*

$$I_2(X; a, b) \le 2bp^{4(b-a)} I_2(X; 2b-a, b)$$

whenever $1 \le a \le b$.

We are now ready to assemble all these results to prove the following recursive estimate for I_2.

Lemma 7. *If* $1 \le a \le b$ *and* $p^b \le X$ *we have*

$$I_2(X; a, b) \le 2bp^{-10a/3+14b/3} I_2(X; b, 2b-a)^{1/3} I_2(X; b, 3b)^{1/6} J(2X/p^b)^{1/2}.$$

The reader may note that the above inequality is a neat form of the bound in Lemma 5.2 of [Wooley 2016].

For the proof we successively apply Lemmas 6, 3, 5 and 4, giving

$$\begin{aligned}
&I_2(X; a, b) \\
&\qquad \le 2bp^{4(b-a)} I_2(X; 2b-a, b) \\
&\qquad \le 2bp^{4(b-a)} I_2(X; b, 2b-a)^{1/3} I_1(X; 2b-a, b)^{2/3} \\
&\qquad \le 2bp^{4(b-a)} I_2(X; b, 2b-a)^{1/3} \{p^{3b-(2b-a)} I_1(X; 3b, b)\}^{2/3} \\
&\qquad \le 2bp^{4(b-a)+2(a+b)/3} I_2(X; b, 2b-a)^{1/3} \{I_2(X; b, 3b)^{1/4} J(2X/p^b)^{3/4}\}^{2/3} \\
&\qquad = 2bp^{-10a/3+14b/3} I_2(X; b, 2b-a)^{1/3} I_2(X; b, 3b)^{1/6} J(2X/p^b)^{1/2}.
\end{aligned}$$

Here we should observe that, in applying Lemma 5 to $I_1(X; 2b-a, b)$, the necessary condition "$a \le 3b$" is satisfied, since $2b-a \le 3b$.

Everything is now in place to complete the proof of the theorem. We note the trivial upper bound $J(X) \ll X^{12}$ and the trivial lower bound $J(X) \ge [X]^6 \gg X^6$ (coming from the obvious diagonal solutions $x_i = x_{6+i}$ for $i \le 6$). Thus we may define a real number $\Delta \in [0, 6]$ by setting

$$\Delta = \inf\{\delta \in \mathbb{R} : J(X) \ll X^{6+\delta} \text{ for } X \ge 1\}. \tag{3}$$

It follows that we will have $J(X) \ll_\varepsilon X^{6+\Delta+\varepsilon}$ for any $\varepsilon > 0$. Our goal of course is to show that $\Delta = 0$.

We observe that

$$I_2(X; a, b) \le J(X) \ll_\varepsilon X^{6+\Delta+\varepsilon}$$

for $1 \le a \le b$, and hence that

$$I_2(X;\, a, b) \ll_\varepsilon X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{3(3b-a)}, \tag{4}$$

since $3(3b-a) \ge 2a+4b$ for $a \le b$. We now proceed to use Lemma 7 to prove, by induction on n, that

$$I_2(X;\, a, b) \ll_{\varepsilon,n,a,b} X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{(3-n\Delta/6)(3b-a)} \tag{5}$$

for any integer $n \ge 0$, provided that

$$1 \le a \le b \tag{6}$$

and

$$p^{3^n b} \le X. \tag{7}$$

The base case $n = 0$ is exactly the bound (4). The reader may be puzzled by the choice of the exponent for p in (5). We shall discuss this further in the final section.

Given (5) we have

$$\begin{aligned} I_2(X;\, b, 2b-a) &\ll_{\varepsilon,n,a,b} X^{6+\Delta+\varepsilon} p^{-2b-4(2b-a)} p^{(3-n\Delta/6)(3(2b-a)-b)} \\ &= X^{6+\Delta+\varepsilon} p^{4a-10b} p^{(3-n\Delta/6)(5b-3a)}. \end{aligned}$$

Note that the conditions corresponding to (6) and (7) are satisfied if

$$p^{3^{n+1}b} \le X.$$

since we will have $1 \le b \le 2b-a$ whenever $1 \le a \le b$, and

$$p^{3^n(2b-a)} \le p^{3^{n+1}b} \le X.$$

In a similar way, (5) implies that

$$\begin{aligned} I_2(X;\, b, 3b) &\ll_{\varepsilon,n,b} X^{6+\Delta+\varepsilon} p^{-2b-12b} p^{(3-n\Delta/6)(9b-b)} \\ &= X^{6+\Delta+\varepsilon} p^{-14b} p^{(3-n\Delta/6)(8b)} \end{aligned}$$

the conditions corresponding to (6) and (7) holding whenever $b \ge 1$.

Finally we have

$$J(2X/p^b) \ll_\varepsilon X^{6+\Delta+\varepsilon} p^{-6b-\Delta b}$$

provided that $p^b \le X$. Feeding these estimates into Lemma 7 we deduce that

$$\begin{aligned} I_2(X;\, a, b) &\ll_{\varepsilon,n,a,b} p^{-10a/3+14b/3} \{X^{6+\Delta+\varepsilon} p^{4a-10b} p^{(3-n\Delta/6)(5b-3a)}\}^{1/3} \\ &\qquad \times \{X^{6+\Delta+\varepsilon} p^{-14b} p^{(3-n\Delta/6)(8b)}\}^{1/6} \{X^{6+\Delta+\varepsilon} p^{-6b-\Delta b}\}^{1/2} \\ &= X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{(3-n\Delta/6)(3b-a)} p^{-\Delta b/2} \\ &\le X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{(3-(n+1)\Delta/6)(3b-a)}, \end{aligned}$$

since $b/2 \ge (3b-a)/6$. This provides the required induction step.

Having established (5) we apply it with $a=b=1$, and p chosen to lie in the range

$$\tfrac{1}{2}X^{1/3^n} \le p \le X^{1/3^n}.$$

There will always be a suitable $p \ge 5$ if

$$X \ge 10^{3^n}.$$

We then deduce from Lemma 2 that

$$J(X) \ll pJ(2X/p) + p^{12}I_2(X;1,1) \ll_{\varepsilon,n} p(X/p)^{6+\Delta+\varepsilon} + X^{6+\Delta+\varepsilon}p^{12-n\Delta/3}.$$

If Δ were strictly positive we could choose n sufficiently large that $n\Delta \ge 39$, and would then conclude that

$$J(X) \ll_{\varepsilon,n} X^{6+\Delta+\varepsilon}p^{-1} \ll_{\varepsilon,n} X^{6+\Delta-3^{-n}+\varepsilon},$$

contradicting the definition (3). We must therefore have $\Delta = 0$, as required for the theorem.

The reader will probably feel that the final stages of the argument, from (5) onward, are lacking in motivation. The final section of the paper will offer an explanation for the route chosen.

3. Proof of the lemmas

We begin by examining Lemma 1. We observe that there is an $\eta \in (0, p^b]$ such that $I_0(X;a,b)$ counts solutions to (1) in which each x_i takes the shape $\eta + p^b y_i$, with integer variables y_i. We will have $0 \le y_i \le X/p^b$. Thus if we set $z_i = y_i + 1$ we find that $1 \le z_i \le 1 + X/p^b \le 2X/p^b$, in view of our condition $p^b \le X$. Moreover we know that if the x_i satisfy (1) then so too will the y_i and the z_i. It follows that $I_0(X;a,b) \le J_{s,k}(2X/p^b)$ as claimed.

To prove Lemma 2 we split solutions of (1) into congruence classes for which $x_i \equiv \xi_i \pmod{p}$ for $1 \le i \le 12$. The number of solutions in which

$$x_1 \equiv \cdots \equiv x_{12} \pmod{p}$$

is at most

$$\sum_{\eta \pmod{p}} I_0(X;0,\eta;1,1) \le pI_0(X;1,1) \le pJ(2X/p),$$

by Lemma 1. For the remaining solutions to (1) there is always a pair of variables that are incongruent modulo p, and it follows that there exist $\xi \not\equiv \eta \pmod{p}$ such that

$$J(X) \le pJ(2X/p) + \binom{12}{2}p(p-1)\int_{(0,1]^3} |f_1(\boldsymbol{\alpha};\xi)f_1(\boldsymbol{\alpha};\eta)f(\boldsymbol{\alpha})^{10}|\,d\boldsymbol{\alpha}.$$

By Hölder's inequality we have

$$\begin{aligned}
&\int_{(0,1]^3} |f_1(\boldsymbol{\alpha};\xi) f_1(\boldsymbol{\alpha};\eta) f(\boldsymbol{\alpha})^{10}|\, d\boldsymbol{\alpha}\\
&\quad\le \left\{\int_{(0,1]^3} |f_1(\boldsymbol{\alpha};\xi)|^4 |f_1(\boldsymbol{\alpha};\eta)|^8\, d\boldsymbol{\alpha}\right\}^{1/12} \left\{\int_{(0,1]^3} |f_1(\boldsymbol{\alpha};\xi)|^8 |f_1(\boldsymbol{\alpha};\eta)|^4\, d\boldsymbol{\alpha}\right\}^{1/12}\\
&\qquad\qquad \times \left\{\int_{(0,1]^3} |f(\boldsymbol{\alpha})|^{12}\, d\boldsymbol{\alpha}\right\}^{5/6},
\end{aligned}$$

whence

$$J(X) \ll pJ(2X/p) + p^2 I_2(X;1,1)^{1/12} I_2(X;1,1)^{1/12} J(X)^{5/6}.$$

We deduce that

$$J(X) \ll pJ(2X/p) + p^{12} I_2(X;1,1),$$

as required for the lemma.

Lemma 3 is a trivial application of Hölder's inequality. We have

$$\begin{aligned}
&I_2(X;\xi,\eta;a,b)\\
&\quad= \int_{(0,1]^3} |f_a(\boldsymbol{\alpha};\xi)|^4 |f_b(\boldsymbol{\alpha};\eta)|^8\, d\boldsymbol{\alpha}\\
&\quad\le \left\{\int_{(0,1]^3} |f_a(\boldsymbol{\alpha};\xi)|^8 |f_b(\boldsymbol{\alpha};\eta)|^4\, d\boldsymbol{\alpha}\right\}^{1/3} \left\{\int_{(0,1]^3} |f_a(\boldsymbol{\alpha};\xi)|^2 |f_b(\boldsymbol{\alpha};\eta)|^{10}\, d\boldsymbol{\alpha}\right\}^{2/3}\\
&\quad\le I_2(X;b,a)^{1/3} I_1(X;a,b)^{2/3},
\end{aligned}$$

and the lemma follows.

For Lemma 4 we note that

$$\begin{aligned}
&I_1(X;\xi,\eta;a,b)\\
&\qquad= \int_{(0,1]^3} |f_a(\boldsymbol{\alpha};\xi)|^2 |f_b(\boldsymbol{\alpha};\eta)|^{10}\, d\boldsymbol{\alpha}\\
&\qquad\le \left\{\int_{(0,1]^3} |f_b(\boldsymbol{\alpha};\xi)|^4 |f_a(\boldsymbol{\alpha};\eta)|^8\, d\boldsymbol{\alpha}\right\}^{1/4} \left\{\int_{(0,1]^3} |f_b(\boldsymbol{\alpha};\eta)|^{12}\, d\boldsymbol{\alpha}\right\}^{3/4}\\
&\qquad\le I_2(X;b,a)^{1/4} I_0(X;b,b)^{3/4}\\
&\qquad\le I_2(X;b,a)^{1/4} J(2X/p^b)^{3/4},
\end{aligned}$$

by Hölder's inequality and Lemma 1.

Turning next to Lemma 5 we note that $I_1(X;\xi,\eta;a,b)$ counts solutions of (1) in which $x_i = \xi + p^a y_i$ for $i = 1$ and $i = 7$, and $x_i = \eta + p^b y_i$ for the remaining indices i. If we set $\nu=\xi-\eta$ we deduce that the variables

$$z_i=\begin{cases}\nu+p^a y_i & i=1 \text{ or } 7,\\ p^b y_i & \text{otherwise,}\end{cases}$$

also satisfy (1). In particular, the equation of degree $j=3$ yields

$$(\nu+p^a z_1)^3\equiv(\nu+p^a z_7)^3 \pmod{p^{3b}}.$$

Now, crucially, we use the fact that $\xi\not\equiv\eta \pmod{p}$, whence $p\nmid\nu$. It follows that we must have $\nu+p^a z_1\equiv\nu+p^a z_7 \pmod{p^{3b}}$, and hence $z_1\equiv z_7 \pmod{p^{3b-a}}$. We therefore have $x_1\equiv x_7\equiv\xi' \pmod{p^{3b}}$ for one of p^{3b-a} possible values of ξ', so that

$$I_1(X;\xi,\eta;a,b)\le p^{3b-a}I_1(X;3b,b),$$

which suffices for the lemma.

Finally we must handle Lemma 6. We note that $I_2(X;\xi,\eta;a,b)$ counts solutions of (1) in which $x_i=\xi+p^a y_i$ for $i=1,2,7$ and 8, and $x_i=\eta+p^b y_i$ for the remaining indices i. As in the proof of Lemma 5 we set $\nu=\xi-\eta$ and $z_i=x_i-\eta$, so that the z_i also satisfy (1). We will have $p^b\mid z_i$ for $3\le i\le 6$ and $9\le i\le 12$, whence

$$(\nu+p^a y_1)^j+(\nu+p^a y_2)^j\equiv(\nu+p^a y_7)^j+(\nu+p^a y_8)^j \pmod{p^{bj}} \quad (1\le j\le 3)$$

with $\nu=\xi-\eta\not\equiv 0 \pmod{p}$. We shall use only the congruences for $j=2$ and 3. On expanding these we find that

$$2\nu S_1+p^a S_2\equiv 0 \pmod{p^{2b-a}} \tag{8}$$

and

$$3\nu^2 S_1+3\nu p^a S_2+p^{2a}S_3\equiv 0 \pmod{p^{3b-a}},$$

where

$$S_j=y_1^j+y_2^j-y_7^j-y_8^j \quad (j=1,2,3).$$

Eliminating S_1 from these yields

$$3\nu p^a S_2+2p^{2a}S_3\equiv 0 \pmod{p^{2b-a}},$$

whence

$$3\nu S_2+2p^a S_3\equiv 0 \pmod{p^{2b-2a}}.$$

Moreover (8) trivially implies that

$$2\nu S_1+p^a S_2\equiv 0 \pmod{p^{2b-2a}}.$$

It appears that we have wasted some information here, but the above congruences are sufficient.

We now call on the following result, which we shall prove at the end of this section.

Lemma 8. *With the notations above for S_j, let $N(p; a, c)$ denote the number of solutions (y_1, y_2, y_7, y_8) modulo p^c of the congruences*

$$2\nu S_1 + p^a S_2 \equiv 3\nu S_2 + 2p^a S_3 \equiv 0 \pmod{p^c}.$$

Then if $a \geq 1$ and $c \geq 0$ we will have $N(p; a, c) \leq (c+1)p^{2c}$.

If $y_i \equiv y_{i0} \pmod{p^{2(b-a)}}$ for $i = 1, 2, 7, 8$ then $x_i \equiv \xi_i \pmod{p^{2b-a}}$, with $\xi_i = \xi + p^a y_{i0}$. The number of solutions to (1) counted by $I_2(X; \xi, \eta; a, b)$ for which $y_i \equiv y_{i0} \pmod{p^{2(b-a)}}$ is then given by

$$\int_{(0,1]^3} f_{2b-a}(\boldsymbol{\alpha}; \xi_1) f_{2b-a}(\boldsymbol{\alpha}; \xi_2) \overline{f_{2b-a}(\boldsymbol{\alpha}; \xi_7) f_{2b-a}(\boldsymbol{\alpha}; \xi_8)} |f_b(\boldsymbol{\alpha}; \eta)|^8 \, d\boldsymbol{\alpha}$$
$$\leq \int_{(0,1]^3} \left| \prod_{i=1,2,6,7} f_{2b-a}(\boldsymbol{\alpha}; \xi_i) \right| |f_b(\boldsymbol{\alpha}; \eta)|^8 \, d\boldsymbol{\alpha}$$
$$\leq \prod_{i=1,2,6,7} \left\{ \int_{(0,1]^3} |f_{2b-a}(\boldsymbol{\alpha}; \xi_i)|^4 |f_b(\boldsymbol{\alpha}; \eta)|^8 \, d\boldsymbol{\alpha} \right\}^{1/4}$$
$$\leq \prod_{i=1,2,6,7} I_2(X; \xi_i, \eta; 2b-a, b)^{1/4}$$
$$\leq I_2(X; 2b-a, b),$$

by Holder's inequality. It then follows from Lemma 8 that

$$I_2(X; a, b) \leq N\big(p; a, 2(b-a)\big) I_2(X; 2b-a, b) \leq 2bp^{4(b-a)} I_2(X; 2b-a, b)$$

as required.

It remains to prove Lemma 8, for which we use induction on c. The base case $c = 0$ is trivial. When $c = 1$ we have $p \mid S_1$ and $p \mid S_2$ and the number of solutions is $2p^2 - p$, which is also satisfactory. In general we shall say that a solution (y_1, y_2, y_7, y_8) is singular if

$$y_1 \equiv y_2 \equiv y_7 \equiv y_8 \pmod{p},$$

and nonsingular otherwise. For a nonsingular solution the vectors

$$\nabla(2\nu S_1 + p^a S_2) \quad \text{and} \quad \nabla(3\nu S_2 + 2p^a S_3)$$

are not proportional modulo p, since $a \geq 1$ and $p \nmid 6\nu$. It follows that a nonsingular solution (y_1, y_2, y_7, y_8) of the congruences modulo p^c will lift to exactly p^2 solutions modulo p^{c+1}. Thus if we write $N_0(p; a, c)$ for the number of nonsingular solutions modulo p^c we will have $N_0(p; a, c) \leq 2p^{2c}$, by induction.

For a singular solution we have

$$y_1 \equiv y_2 \equiv y_7 \equiv y_8 \equiv \beta \pmod{p},$$

say. If we write $y_i = \beta + pu_i$ and

$$S'_j = u_1^j + u_2^j - u_7^j - u_8^j$$

we find that

$$2\nu S_1 + p^a S_2 = 2(\nu + \beta p^a) p S'_1 + p^{a+2} S'_2$$

and

$$3\nu S_2 + 2p^a S_3 = 6\beta(\nu + \beta p^a) p S'_1 + 3(\nu + 2\beta p^a) p^2 S'_2 + 2p^{a+3} S'_3.$$

Hence

$$2\nu' p S'_1 + p^{a+2} S'_2 \equiv 6\beta\nu' p S'_1 + 3(\nu' + \beta p^a) p^2 S'_2 + 2p^{a+3} S'_3 \equiv 0 \pmod{p^c}$$

with $\nu' = \nu + \beta p^a \not\equiv 0 \pmod{p}$. Eliminating S'_1 from the second expression yields

$$3\nu' p^2 S'_2 + 2p^{3+a} S'_3 \equiv 0 \pmod{p^c}$$

and we deduce that

$$2\nu' S'_1 + p^{a+1} S'_2 \equiv 0 \pmod{p^{c-1}} \tag{9}$$

and

$$3\nu' S'_2 + 2p^{a+1} S'_3 \equiv 0 \pmod{p^{c-2}}. \tag{10}$$

Since we are counting values of y_i modulo p^c we have to count values of u_i modulo p^{c-1}. However any solution of

$$2\nu' S'_1 + p^{a+1} S'_2 \equiv 3\nu' S'_2 + 2p^{a+1} S'_3 \equiv 0 \pmod{p^{c-2}}$$

modulo p^{c-2} lifts to exactly p^3 solutions of the two congruences (9) and (10) modulo p^{c-1}, since

$$\nabla(2\nu' S'_1 + p^{a+1} S'_2) \equiv 2\nu'(1, 1, -1, -1) \not\equiv 0 \pmod{p}.$$

It follows that (9) and (10) have $p^3 N(p; a+1, c-2)$ solutions for each of the p possible choices of β, provided of course that $c \geq 2$.

We are therefore able to conclude that

$$N(p; a, c) \leq N_0(p; a, c) + p^4 N(p; a+1, c-2) \leq 2p^{2c} + p^4 N(p; a+1, c-2)$$

for $c \geq 2$, and the lemma then follows by induction on c.

We conclude this section by remarking that in this final inductive argument, we have estimates of the same order of magnitude for both the number of singular solutions and the number of nonsingular solutions. When one tries to generalize the argument to systems of more congruences the singular solutions can dominate the count in an unwelcome way. It is for this reason that Wooley's approach requires a "conditioning" step in general, in order to remove singular solutions at the outset. Fortunately we just manage to avoid this in our situation.

4. Remarks on the conclusion to the proof

This final section is intended to shed some light on the argument that leads from Lemma 7 to the theorem. In particular the reader may be curious as to how one is led to formulate the induction hypothesis (5). The issue is that repeated applications of Lemma 7, starting from $I_2(X;\,1,\,1)$ for example, produce values of $I_2(X;\,a,\,b)$ with a large number of different pairs a, b; and one wants an induction hypothesis that will apply successfully to all of them.

Suppose one assumes that $J(X) \ll_\varepsilon X^{\theta+\varepsilon}$ for any $\varepsilon > 0$ and that for any positive integers $a \le b$ one has

$$I_2(X;\,a,\,b) \ll_\varepsilon X^{\theta+\varepsilon} p^{\alpha a+\beta b} \tag{11}$$

for some constants α and β, for a suitable range $p \le X^{\delta(\alpha,\beta)}$, say.

Then Lemma 7 yields

$$I_2(X;\,a,\,b) \ll_b X^{\theta} p^{\alpha' a+\beta' b}$$

for $a \le b$, with new constants

$$\alpha' = -\tfrac{10}{3} - \tfrac{1}{3}\beta, \quad \beta' = \tfrac{14}{3} + \tfrac{1}{2}\alpha + \tfrac{7}{6}\beta - \tfrac{1}{2}\theta.$$

We can express this by writing

$$\begin{pmatrix}\alpha'\\ \beta'\end{pmatrix} = \boldsymbol{c} + M\begin{pmatrix}\alpha\\ \beta\end{pmatrix},$$

with

$$\boldsymbol{c} = \begin{pmatrix} -10/3 \\ 14/3-\theta/2\end{pmatrix}, \quad M = \begin{pmatrix} 0 & -1/3 \\ 1/2 & 7/6\end{pmatrix}.$$

Starting with $\alpha = \beta = 0$, for example, we obtain inductively a succession of bounds of the shape (11), with

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\alpha_n\\ \beta_n\end{pmatrix} = \boldsymbol{c} + M\boldsymbol{c} + \cdots + M^n\boldsymbol{c}.$$

The matrix M has eigenvalues 1 and $\frac{1}{6}$, and can be diagonalized as PDP^{-1} with

$$P = \begin{pmatrix} -1 & -2 \\ 3 & 1\end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{6}\end{pmatrix}.$$

It then follows that

$$\begin{pmatrix}\alpha_n\\ \beta_n\end{pmatrix} = nP\begin{pmatrix} 1 & 0 \\ 0 & 0\end{pmatrix}P^{-1}\boldsymbol{c} + O(1) = \frac{(6-\theta)n}{5}\begin{pmatrix} -1 \\ 3\end{pmatrix} + O(1)$$

as n tends to infinity. For any starting pair a, b we will have $3b - a \ge 2b \ge 2$. Thus if $\theta > 6$ we will eventually have $\alpha_n a + \beta_n b < -1$, say, for suitably large n.

We therefore obtain

$$I_2(X;a,b) \ll_\varepsilon X^{\theta+\varepsilon}p^{-1}$$

for $p \le X^\delta$, for some $\delta = \delta_n$ depending on θ. This leads to a contradiction, as in Section 2.

We therefore see that the crucial feature of Lemma 7 is that it leads to a matrix M having its largest eigenvalue equal to 1. The corresponding eigenvector is $(\alpha, \beta) = (-1, 3)$, and the argument of Section 2 has therefore been expressed in terms of the linear combination $3b - a$.

References

[Bourgain et al. 2016] 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**:2 (2016), 633–682. MR Zbl

[Ford and Wooley 2014] K. Ford and T. D. Wooley, "On Vinogradov's mean value theorem: strongly diagonal behaviour via efficient congruencing", *Acta Math.* **213**:2 (2014), 199–236. MR Zbl

[Wooley 2012] T. D. Wooley, "Vinogradov's mean value theorem via efficient congruencing", *Ann. of Math.* (2) **175**:3 (2012), 1575–1627. MR Zbl

[Wooley 2013] T. D. Wooley, "Vinogradov's mean value theorem via efficient congruencing, II", *Duke Math. J.* **162**:4 (2013), 673–730. MR Zbl

[Wooley 2014] T. D. Wooley, "Translation invariance, exponential sums, and Waring's problem", pp. 505–529 in *Proceedings of the International Congress of Mathematicians* (Seoul, 2014), vol. II, edited by S. Y. Jang et al., Kyung Moon Sa, Seoul, South Korea, 2014. MR Zbl

[Wooley 2015] T. D. Wooley, "Multigrade efficient congruencing and Vinogradov's mean value theorem", *Proc. Lond. Math. Soc.* (3) **111**:3 (2015), 519–560. MR Zbl

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

[Wooley 2017] T. D. Wooley, "Approximating the main conjecture in Vinogradov's mean value theorem", *Mathematika* **63**:1 (2017), 292–350. MR Zbl

[Wooley 2019] T. D. Wooley, "Nested efficient congruencing and relatives of Vinogradov's mean value theorem", *Proc. Lond. Math. Soc.* (3) **118**:4 (2019), 942–1016. MR Zbl

Received 6 Jul 2021. Revised 14 Sep 2021.

D. R. HEATH-BROWN:

rhb@maths.ox.ac.uk
University of Oxford, Mathematical Institute, Oxford, United Kingdom

ESSENTIAL NUMBER THEORY

msp.org/ent

See inside back cover or msp.org/ent for submission instructions.

Essential Number Theory (ISSN 2834-4634 electronic, 2834-4626 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ENT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
https://msp.org/

ESSENTIAL NUMBER THEORY

2022 vol. 1 no. 1