An Introduction to Vinogradov's Mean Value Theorem

Andrew Luo

University of Waterloo

Canadian Undergraduate Mathematics Conference 2021

Review

Recall we are concerned with the number of solutions to the system

$$\begin{aligned} x_1 + x_2 + \ldots + x_s &= y_1 + y_2 + \ldots + y_s \\ x_1^2 + x_2^2 + \ldots + x_s^2 &= y_1^2 + y_2^2 + \cdots + y_s^2 \\ &\vdots \\ x_1^k + x_2^k + \ldots + x_s^k &= y_1^k + y_2^k + \ldots + y_s^k, \end{aligned}$$

where $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{N}^s$ with $1 \leq \boldsymbol{x}, \boldsymbol{y} \leq X$.

Review

Let $J_{s,k}(X)$ count the solutions to the system above. Our goal is to prove

Theorem (The Main Conjecture in Vinogradov's MVT)

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

By orthogonality, this is equivalent to proving

Theorem (The Main Conjecture in Vinogradov's MVT)

$$\int_{[0,1)^k} |f_k(\alpha; X)|^{2s} d\alpha \ll X^{s+\varepsilon} + X^{2s-k(k+1)/2}$$

where

$$f_k(\alpha; X) = \sum_{1 \le x \le X} e(\alpha_1 x + \ldots + \alpha_k x^k).$$

Let $J_{s,k}(X)$ count the solutions to the system above. Our goal is to prove

Theorem (The Main Conjecture in Vinogradov's MVT)

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

By orthogonality, this is equivalent to proving

Theorem (The Main Conjecture in Vinogradov's MVT)

$$\int_{[0,1)^k} |f_k(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^{s+\varepsilon} + X^{2s-k(k+1)/2}$$

where

$$f_k(\boldsymbol{\alpha}; X) = \sum_{1 \le x \le X} e(\alpha_1 x + \ldots + \alpha_k x^k).$$

Review

We temporarily restrict our attention to the mean value $U_{s,k}^{B}$ which is the number of solutions of the simultaneous congruences

$$\sum_{j=1}^{s}(x_j^i - y_j^i) \equiv 0 \pmod{p^B}$$

where $1 \leq i \leq k$, $1 \leq \boldsymbol{x}, \boldsymbol{y} \leq X$ and each solution counted with weight ρ_0^{-2s}.

We may further impose that $\boldsymbol{x} \equiv \boldsymbol{y} \pmod{p^h}$. We will denote this quantity of this new restricted system $U_{s,k}^{B,h}$.

Review

We temporarily restrict our attention to the mean value $U_{s,k}^B$ which is the number of solutions of the simultaneous congruences

$$\sum_{j=1}^{s}(x_j^i - y_j^i) \equiv 0 \pmod{p^B}$$

where $1 \leq i \leq k$, $1 \leq \boldsymbol{x}, \boldsymbol{y} \leq X$ and each solution counted with weight ρ_0^{-2s}.

We may further impose that $\boldsymbol{x} \equiv \boldsymbol{y} \pmod{p^h}$. We will denote this quantity of this new restricted system $U_{s,k}^{B,h}$.

For $0 \leq r \leq k$ and a, b, ν non-negative integers, we define $K_{a,b}^{r,\nu}$ to count solutions to the system of congruences

$$\sum_{j=1}^{R}(x_j^i - y_j^i) \equiv \sum_{\ell=1}^{s-R}(v_\ell^i - w_\ell^i) \pmod{p^B}$$

with $R = r(r+1)/2$, $\boldsymbol{x} \equiv \boldsymbol{y} \equiv \xi \pmod{p^a}$ and $\boldsymbol{v} \equiv \boldsymbol{w} \equiv \eta \pmod{p^b}$, counted with weight $\rho_a(\xi)^{-2R}\rho_b(\eta)^{2R-2s}$.

We define

$$K_{a,b}^{r} = \rho^{-4} \sum_{\xi \bmod p^a} \sum_{\substack{\eta \bmod p^b \\ \xi \not\equiv \eta \pmod{p^\nu}}} \rho_a(\xi)^2 \rho_b(\eta)^2 K_{a,b}^{r,\nu}(\xi, \eta).$$

Review

For $0 \leq r \leq k$ and a, b, ν non-negative integers, we define $K_{a,b}^{r,\nu}$ to count solutions to the system of congruences

$$\sum_{j=1}^{R}(x_j^i - y_j^i) \equiv \sum_{\ell=1}^{s-R}(v_\ell^i - w_\ell^i) \pmod{p^B}$$

with $R = r(r+1)/2$, $\boldsymbol{x} \equiv \boldsymbol{y} \equiv \xi \pmod{p^a}$ and $\boldsymbol{v} \equiv \boldsymbol{w} \equiv \eta \pmod{p^b}$, counted with weight $\rho_a(\xi)^{-2R}\rho_b(\eta)^{2R-2s}$.

We define

$$K_{a,b}^{r} = \rho^{-4} \sum_{\xi \bmod p^a} \sum_{\substack{\eta \bmod p^b \\ \xi \not\equiv \eta \pmod{p^\nu}}} \rho_a(\xi)^2 \rho_b(\eta)^2 K_{a,b}^{r,\nu}(\xi, \eta).$$

Recall the orthgonality relation

Lemma (Orthogonality)

Letting $e(x) = e^{2\pi i x}$, *one has*

$$\int_{[0,1)} e(\alpha n)\, d\alpha = \begin{cases} 1, & \text{if } n = 0 \\ 0, & \text{otherwise.} \end{cases}$$

The modular equivalent relation is

Lemma (Orthogonality)

Letting $e(x) = e^{2\pi i x}$, *one has*

$$q^{-1} \sum_{r=1}^{q} e(hr/q) = \begin{cases} 1, & \text{if } q | h, \\ 0, & \text{otherwise.} \end{cases}$$

Recall the orthgonality relation

Lemma (Orthogonality)

Letting $e(x) = e^{2\pi i x}$, *one has*

$$\int_{[0,1)} e(\alpha n)\, d\alpha = \begin{cases} 1, & \text{if } n = 0 \\ 0, & \text{otherwise.} \end{cases}$$

The modular equivalent relation is

Lemma (Orthogonality)

Letting $e(x) = e^{2\pi i x}$, *one has*

$$q^{-1} \sum_{r=1}^{q} e(hr/q) = \begin{cases} 1, & \text{if } q|h, \\ 0, & \text{otherwise.} \end{cases}$$

An application of Holder's Inequality tells us that

$$U_{s,k}^{B} \leq p^{sH} U_{s,k}^{B,H}.$$

We let Λ be the least non-negative value such that, when B is sufficiently large and $H = \lceil B/k \rceil$,

$$U_{s,k}^{B} \ll (p^{B})^{\Lambda+\varepsilon} U_{s,k}^{B,H}$$

for any $\varepsilon > 0$. Our first goal is to prove $\Lambda = 0$.

An application of Holder's Inequality tells us that

$$U_{s,k}^{B} \leq p^{sH} U_{s,k}^{B,H}.$$

We let Λ be the least non-negative value such that, when B is sufficiently large and $H = \lceil B/k \rceil$,

$$U_{s,k}^{B} \ll (p^{B})^{\Lambda+\varepsilon} U_{s,k}^{B,H}$$

for any $\varepsilon > 0$. Our first goal is to prove $\Lambda = 0$.

An application of Holder's Inequality tells us that

$$U_{s,k}^{B} \leq p^{sH} U_{s,k}^{B,H}.$$

We let Λ be the least non-negative value such that, when B is sufficiently large and $H = \lceil B/k \rceil$,

$$U_{s,k}^{B} \ll (p^{B})^{\Lambda+\varepsilon} U_{s,k}^{B,H}$$

for any $\varepsilon > 0$. Our first goal is to prove $\Lambda = 0$.

We define the normalized value of $K_{a,b}^r$ by

$$\tilde{K}_{a,b}^r = \left(\frac{K_{a,b}^r}{p^{\Lambda H} U_{s,k}^{B,H}} \right)^{\frac{k-1}{r(k-r)}}.$$

It can be shown using a congruencing argument that

$$\tilde{K}_{a,b}^r \ll p^{H\varepsilon}.$$

We define the normalized value of $K_{a,b}^r$ by

$$\tilde{K}_{a,b}^r = \left(\frac{K_{a,b}^r}{p^{\Lambda H} U_{s,k}^{B,H}} \right)^{\frac{k-1}{r(k-r)}}.$$

It can be shown using a congruencing argument that

$$\tilde{K}_{a,b}^r \ll p^{H\varepsilon}.$$

We want to find an iterative bound on the value $\tilde{K}^r_{a,b}$. To do so, we will establish a hierarchy of small values $\varepsilon < \tau < \delta < \mu < 1$ and set $\theta = \lfloor \mu H \rfloor$.

Lemma

Suppose

$$1 \leq r \leq k-1, \quad a \geq \delta\theta, \quad b \geq k^2\delta\theta, \quad ra \leq (k-r+1)b.$$

Whenever $k^2 b \leq (1-\delta)B$, there exist a', b', r' and ρ with $0 < \rho < (1-1/k)^2$ and $\rho b' \geq b$ such that

$$\tilde{K}^r_{a,b} \ll (\tilde{K}^{r'}_{a',b'})^\rho p^{-b\Lambda/(2k)}$$

with a', b', r' satisfying the conditions of the lemma.

We want to find an iterative bound on the value $\tilde{K}^r_{a,b}$. To do so, we will establish a hierarchy of small values $\varepsilon < \tau < \delta < \mu < 1$ and set $\theta = \lfloor \mu H \rfloor$.

Lemma

Suppose

$$1 \leq r \leq k-1, \quad a \geq \delta\theta, \quad b \geq k^2\delta\theta, \quad ra \leq (k-r+1)b.$$

Whenever $k^2 b \leq (1-\delta)B$, there exist a', b', r' and ρ with $0 < \rho < (1-1/k)^2$ and $\rho b' \geq b$ such that

$$\tilde{K}^r_{a,b} \ll (\tilde{K}^{r'}_{a',b'})^{\rho} p^{-b\Lambda/(2k)}$$

with a', b', r' satisfying the conditions of the lemma.

Proof that $\Lambda = 0$.

Let $N = \lceil 16sk/\Lambda \rceil$. Note that $8sk/N \leq \Lambda/2$. We start with

$$U_{s,k}^{B} \ll p^{s\theta} K_{\theta,\theta}^{1}.$$

By applying the iterative lemma N times we obtain the bound

$$p^{-2s\theta} \ll (\tilde{K}_{a,b}^{r})(p^{-\Lambda/(2k)})^{N\theta}.$$

Recalling the bound

$$\tilde{K}_{a,b}^{r} \ll p^{H\varepsilon},$$

we obtain $(p^{\theta})^{4s} \gg (p^{\theta})^{N\Lambda/(2k)}$. This implies $\Lambda \leq 8sk/N$. So $\Lambda = 0$.

∎

Proof that $\Lambda = 0$.

Let $N = \lceil 16sk/\Lambda \rceil$. Note that $8sk/N \le \Lambda/2$. We start with

$$U^B_{s,k} \ll p^{s\theta} K^1_{\theta,\theta}.$$

By applying the iterative lemma N times we obtain the bound

$$p^{-2s\theta} \ll (\tilde{K}^r_{a,b})(p^{-\Lambda/(2k)})^{N\theta}.$$

Recalling the bound

$$\tilde{K}^r_{a,b} \ll p^{H\varepsilon},$$

we obtain $(p^\theta)^{4s} \gg (p^\theta)^{N\Lambda/(2k)}$. This implies $\Lambda \le 8sk/N$. So $\Lambda = 0$.

Proof that $\Lambda = 0$.

Let $N = \lceil 16sk/\Lambda \rceil$. Note that $8sk/N \leq \Lambda/2$. We start with

$$U_{s,k}^{B} \ll p^{s\theta} K_{\theta,\theta}^{1}.$$

By applying the iterative lemma N times we obtain the bound

$$p^{-2s\theta} \ll (\tilde{K}_{a,b}^{r})(p^{-\Lambda/(2k)})^{N\theta}.$$

Recalling the bound

$$\tilde{K}_{a,b}^{r} \ll p^{H\varepsilon},$$

we obtain $(p^{\theta})^{4s} \gg (p^{\theta})^{N\Lambda/(2k)}$. This implies $\Lambda \leq 8sk/N$. So $\Lambda = 0$.

∎

Theorem (1)

Let s be a positive number with $s \leq \frac{k(k+1)}{2}$. Then for each $\varepsilon > 0$, one has

$$\int_{[0,1)^k} \left| \sum_{1 \leq x \leq X} e(\alpha_1 x + \ldots + \alpha_k x^k) \right|^{2s} d\boldsymbol{\alpha} \ll X^{s+\varepsilon}.$$

Outline of Proof. We assume $s = k(k+1)/2$ and the general case follows from Holder's Inequality. Consider solutions to the system

$$\sum_{j=1}^{s} x_j^i \equiv \sum_{j=1}^{s} y_j^i \pmod{p^B} \quad (1 \leq i \leq k)$$

Theorem (1)

Let s be a positive number with $s \leq \frac{k(k+1)}{2}$. Then for each $\varepsilon > 0$, one has

$$\int_{[0,1)^k} \left| \sum_{1 \leq x \leq X} e(\alpha_1 x + \ldots + \alpha_k x^k) \right|^{2s} d\boldsymbol{\alpha} \ll X^{s+\varepsilon}.$$

Outline of Proof. We assume $s = k(k+1)/2$ and the general case follows from Holder's Inequality. Consider solutions to the system

$$\sum_{j=1}^{s} x_j^i \equiv \sum_{j=1}^{s} y_j^i \pmod{p^B} \quad (1 \leq i \leq k)$$

By restricting the variables $\boldsymbol{x}, \boldsymbol{y}$ to lie in congruence classes modulo p^c for some small c, we can show the number of solutions of the above system is bounded from above by

$$p^{sc}\rho_0^{-2} \sum_{\xi \bmod p^c} \rho_c(\xi)^2 I_p(\xi),$$

where $I_p(\xi)$ counts the solutions $\boldsymbol{y}, \boldsymbol{z}$ of the system

$$\sum_{j=1}^{s}(p^c y_j + \xi)^i \equiv \sum_{j=1}^{s}(p^c z_j + \xi)^i \pmod{p^B} \quad (1 \le i \le k).$$

This can be rearranged to the system

$$\sum_{j=1}^{s}(p^c)^i y_j^i \equiv \sum_{j=1}^{s}(p^c)^i z_j^i \pmod{p^B} \quad (1 \le i \le k),$$

from which we obtain the additional set of constraints

$$\sum_{j=1}^{s} y_j^i \equiv \sum_{j=1}^{s} z_j^i \pmod{p^{B-kc}} \quad (1 \le i \le k).$$

The last system is just $U_{s,k}^{B-kc}$.

This can be rearranged to the system

$$\sum_{j=1}^{s}(p^c)^i y_j^i \equiv \sum_{j=1}^{s}(p^c)^i z_j^i \pmod{p^B} \quad (1 \leq i \leq k),$$

from which we obtain the additional set of constraints

$$\sum_{j=1}^{s} y_j^i \equiv \sum_{j=1}^{s} z_j^i \pmod{p^{B-kc}} \quad (1 \leq i \leq k).$$

The last system is just $U_{s,k}^{B-kc}$.

This can be rearranged to the system

$$\sum_{j=1}^{s}(p^c)^i y_j^i \equiv \sum_{j=1}^{s}(p^c)^i z_j^i \pmod{p^B} \quad (1 \leq i \leq k),$$

from which we obtain the additional set of constraints

$$\sum_{j=1}^{s} y_j^i \equiv \sum_{j=1}^{s} z_j^i \pmod{p^{B-kc}} \quad (1 \leq i \leq k).$$

The last system is just $U_{s,k}^{B-kc}$.

A consequence of the main iterative lemma tells us

$$I_p(\xi) \ll p^{B\varepsilon} U_{s,k}^{B-kc,H} \ll p^{B\varepsilon}(1 + X/p^{c+H})^s.$$

We conclude that the solutions to our original system is bounded by

$$p^{sc+B\varepsilon}(1 + X/p^{c+H})^s \ll p^{B\varepsilon/(4k)}(1 + X/p^{c+H})^s \ll X^{s+\varepsilon}$$

A consequence of the main iterative lemma tells us

$$I_p(\xi) \ll p^{B\varepsilon} U_{s,k}^{B-kc,H} \ll p^{B\varepsilon}(1 + X/p^{c+H})^s.$$

We conclude that the solutions to our original system is bounded by

$$p^{sc+B\varepsilon}(1 + X/p^{c+H})^s \ll p^{B\varepsilon/(4k)}(1 + X/p^{c+H})^s \ll X^{s+\varepsilon}$$

■

Theorem (The Main Conjecture in Vinogradov's MVT)

$$\int_{[0,1)^k} |f_k(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^{s+\varepsilon} + X^{2s-k(k+1)/2}$$

where

$$f_k(\boldsymbol{\alpha}; X) = \sum_{1 \le x \le X} e(\alpha_1 x + ... + \alpha_k x^k)$$

Recall that this mean value counts the number of solutions to

$$\sum_{j=1}^{s} x_j^i = \sum_{j=1}^{s} y_j^i$$

for $1 \le i \le k$ and $1 \le \boldsymbol{x}, \boldsymbol{y} \le X$.

Theorem (The Main Conjecture in Vinogradov's MVT)

$$\int_{[0,1)^k} |f_k(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^{s+\varepsilon} + X^{2s-k(k+1)/2}$$

where

$$f_k(\boldsymbol{\alpha}; X) = \sum_{1\leq x\leq X} e(\alpha_1 x + ... + \alpha_k x^k)$$

Recall that this mean value counts the number of solutions to

$$\sum_{j=1}^{s} x_j^i = \sum_{j=1}^{s} y_j^i$$

for $1 \leq i \leq k$ and $1 \leq \boldsymbol{x}, \boldsymbol{y} \leq X$.

Proof. When $s \leq k(k+1)/2$ the result follows directly from Theorem 1.

When $s > k(k+1)/2$ we have

$$\begin{aligned}\int_{[0,1)^k} |f_k(\alpha; X)|^{2s} d\alpha &\ll \int_{[0,1)^k} |f_k(\alpha; X)|^{2s-k(k+1)} |f_k(\alpha; X)|^{k(k+1)} d\alpha \\ &\ll X^{2s-k(k+1)} \int_{[0,1)^k} |f_k(\alpha; X)|^{k(k+1)} d\alpha \\ &\ll X^{2s-k(k+1)/2+\varepsilon}.\end{aligned}$$

∎

Proof. When $s \leq k(k+1)/2$ the result follows directly from Theorem 1.

When $s > k(k+1)/2$ we have

$$\begin{aligned}\int_{[0,1)^k} |f_k(\boldsymbol{\alpha};X)|^{2s} d\boldsymbol{\alpha} &\ll \int_{[0,1)^k} |f_k(\boldsymbol{\alpha};X)|^{2s-k(k+1)} |f_k(\boldsymbol{\alpha};X)|^{k(k+1)} d\boldsymbol{\alpha} \\ &\ll X^{2s-k(k+1)} \int_{[0,1)^k} |f_k(\boldsymbol{\alpha};X)|^{k(k+1)} d\boldsymbol{\alpha} \\ &\ll X^{2s-k(k+1)/2+\varepsilon}.\end{aligned}$$

■

Thank You!

Andrew Luo

University of Waterloo

Canadian Undergraduate Mathematics Conference 2021