HCM Summer School: The Circle Method

An Introduction to the Circle Method Part II

Yu-Ru Liu

University of Waterloo

Tuesday, May 11, 2021

Part II: Vinogradov's Mean Value Theorem

Talk Plan

- Introduction to Vinogradov's mean value theorem
- Lower Bounds for $J_{s,k}(X)$
- Upper Bounds for $J_{s,k}(X)$
- Applications to Waring's problem

1. Introduction to Vinogradov's Mean Value Theorem

Fix $s, k \in \mathbb{N}$ with $k \geq 2$. For $\alpha \in \mathbb{R}$, let $e(\alpha) = e^{2\pi i \alpha}$ and

$$f(\alpha) = \sum_{1 \leq x \leq X} e(\alpha x^k).$$

We recall that to get Hua's Lemma, we consider

$$\int_0^1 |f(\alpha)|^{2s} d\alpha,$$

which counts the number of $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ satisfying

$$x_1^k + \cdots + x_s^k = y_1^k + \cdots + y_s^k$$

with $x_i, y_i \leq X$.

For $\boldsymbol{\alpha} = (\alpha_k, \alpha_{k-1}, \cdots, \alpha_1) \in \mathbb{R}^k$, consider

$$f(\boldsymbol{\alpha}, X) = \sum_{1 \le x \le X} e(\alpha_k x^k + \alpha_{k-1} x^{k-1} + \cdots + \alpha_1 x).$$

Define

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

Vinogradov's Mean Value Theorem is about estimates for $J_{s,k}(X)$, which counts the number of $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ satisfying

$$\begin{aligned} x_1^k + \cdots + x_s^k &= y_1^k + \cdots + y_s^k \\ x_1^{k-1} + \cdots + x_s^{k-1} &= y_1^{k-1} + \cdots + y_s^{k-1} \\ &\vdots \\ x_1 + \cdots + x_s &= y_1 + \cdots + y_s \end{aligned}$$

with $x_i, y_i \le X$.

We recall $J_{s,k}(X)$ counts the number of $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ satisfying

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

with $x_i, y_i \le X$. Since

$$s - sX^j \le (x_1^j + \cdots + x_s^j) - (y_1^j + \cdots + y_s^j) \le sX^j - s,$$

the "probability" that the difference equals to 0 is $O(X^{-j})$. So we expect that $J_{s,k}(X)$ is of size

$$X^{2s} \cdot X^{-k} \cdots X^{-1} = X^{2s-k(k+1)/2}.$$

2. Lower Bounds for $J_{s,k}(X)$

Define $T_s(X)$ to be the number of $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ with

$$\{x_1, \cdots, x_s\} = \{y_1, \cdots, y_s\}$$

and $x_i, y_i \leq X$. Then $\mathbf{x}, \mathbf{y}$ satisfy

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

It follows that

$$J_{s,k}(X) \geq T_s(X) \sim s! X^s.$$

For $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ with $x_i, y_i \le X$, write

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

Let $\mathbf{h} = (h_k, \cdots, h_1)$ and $\boldsymbol{\alpha} \cdot \boldsymbol{h} = \alpha_k h_k + \cdots + \alpha_1 h_1$. By running through all possible $\mathbf{x}, \mathbf{y}$, we have

$$\begin{aligned} X^{2s} &= \sum_{\mathbf{h}} \int_{[0,1)^k} |f(\boldsymbol{\alpha}, X)|^{2s} e(-\boldsymbol{\alpha} \cdot \mathbf{h}) d\boldsymbol{\alpha} \\ &\le \sum_{\mathbf{h}} \int_{[0,1)^k} |f(\boldsymbol{\alpha}, X)|^{2s} d\boldsymbol{\alpha} = \sum_{\mathbf{h}} J_{s,k}(X). \end{aligned}$$

Note that $|h_j| < sX^j$. Since

$$\#\left\{\mathbf{h} : \ |h_j| < sX^j \ (1 \le j \le k)\right\} \ll X^{k(k+1)/2},$$

we have

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

Combining the above two lower bounds for $J_{s,k}(X)$, we have

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

Conjecture For any $\epsilon > 0$, we have

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

Theorem (Wooley, Bourgain-Demeter-Guth)

The conjecture is true.

3. Upper Bounds for $J_{s,k}(X)$

Theorem (Vinogradov's Mean Value Theorem) For $k \geq 3$, let $s = rk$ for some $r \in \mathbb{N}$. We have

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

where

$$\Delta_{s,k} = k^2(1-1/k)^r/2.$$

- Note that

$$k^2(1-1/k)^r \leq k^2(e^{-1/k})^r = k^2 e^{-r/k} \to 0 \quad \text{as} \quad r \to \infty.$$

Thus we have $\Delta_{s,k} \to 0$ as $s \to \infty$.

- Apply Hölder's inequality to bound $J_{s,k}(X)$ for general s.

We will prove Vinogradov's Mean Value Theorem using induction on $r \in \mathbb{N}$. The proof will be divided into the following steps:

- The Base Case
- A Key Lemma
- The General cases

The Base Case

For the base case $r = 1$, i.e., $s = k$, we have

$$x_1^j + \cdots + x_k^j = y_1^j + \cdots + y_k^j \quad (1 \le j \le k).$$

Consider the polynomial with the variable t

$$\prod_{i=1}^{k}(t - x_i),$$

whose coefficients are elementary symmetric polynomials

$$\sum_{\{i_1,\cdots,i_j\}\subseteq\{1,\cdots,k\}} x_{i_1} \cdots x_{i_j} \quad (1 \le j \le k).$$

Since they are linear combinations of

$$x_1^j + \cdots + x_k^j \quad (1 \le j \le k),$$

as a polynomial in t, we have

$$\prod_{i=1}^{k}(t - x_i) = \prod_{i=1}^{k}(t - y_i).$$

Assigning $t = y_1$, we get

$$\prod_{i=1}^{k}(y_1 - x_i) = \prod_{i=1}^{k}(y_1 - y_i) = 0.$$

This implies that $y_1 = x_t$ for some t with $1 \le t \le k$. Repeat the same argument for other y_i $(2 \le i \le k)$. We see that

$$\{x_1, \cdots, x_k\} = \{y_1, \cdots, y_k\}.$$

It follows that

$$J_{k,k}(X) = T_k(X) \sim k!\, X^k.$$

In particular, we have

$$J_{k,k}(X) \ll X^{2k-k(k+1)/2+\Delta_{k,k}} \quad \text{with} \quad \Delta_{k,k} = k^2(1-1/k)/2.$$

So the theorem holds if $r = 1$.

A Key Lemma

Key Lemma Given a prime p with $p > k$ and $\mathbf{h} = (h_k, \ldots, h_1)$, let $S(\mathbf{h}, X)$ be the number of $\mathbf{x} \in \mathbb{N}^k$ satisfying

$$\sum_{i=1}^{k} x_i^j \equiv h_j \pmod{p^j} \quad (1 \leq j \leq k)$$

with $x_i \leq X$ and $\{x_1, \cdots, x_k\}$ distinct (mod p). If $p^k > X$, then

$$S(\mathbf{h}, X) \leq k!\, p^{k(k-1)/2}.$$

Proof. Let $B(\mathbf{g})$ be the number of $\mathbf{x} \in \mathbb{N}^k$ satisfying

$$\sum_{i=1}^{k} x_i^j \equiv g_j \pmod{p^k} \quad (1 \le j \le k)$$

with $x_i \le p^k$ and $\{x_1, \cdots, x_k\}$ distinct (mod p). Using a similar argument to the Base Case, we have $B(\mathbf{g}) \le k!$. Since $p^k > X$,

$$S(\mathbf{h}, X) \le \sum_{\mathbf{g}} B(\mathbf{g}),$$

where the sum is over $\mathbf{g} = (g_k, \ldots, g_1)$ with $1 \le g_j \le p^k$ and $g_j \equiv h_j \pmod{p^j}$ $(1 \le j \le k)$. Note that for a fixed h_j, the number of choices for g_j is p^{k-j}. Thus the number of choices for $\mathbf{g}$ is

$$p^{k-1} \cdot p^{k-2} \cdots p \cdot 1 = p^{k(k-1)/2}.$$

It follows that

$$S(\mathbf{h}, X) \le k!\, p^{k(k-1)/2}.$$

The General Cases

We will prove Vinogradov's Mean Value Theorem by induction on $r \in \mathbb{N}$. We have seen that the theorem holds if $r = 1$. Suppose that the inductive hypothesis holds for all $r' < r$. For $s = rk$, we consider $J_{s,k}(X)$, which counts the number of $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ satisfying

$$\sum_{i=1}^{s} x_i^j = \sum_{i=1}^{s} y_i^j \quad (1 \leq j \leq k)$$

with $x_i, y_i \leq X$.

To bound $J_{s,k}(X)$,

- Show the contribution of singular solutions is small.
- Use the Key Lemma to estimate non-singular solutions.

Singular Solutions and Non-singular Solutions

Note that the Jacobian of the above system with respect to $x_1, \cdots, x_k$ is

$$\begin{pmatrix} kx_1^{k-1} & \cdots & kx_k^{k-1} \\ & \vdots & \\ \cdots & jx_i^{j-1} & \cdots \\ & \vdots & \\ 1 & \cdots & 1 \end{pmatrix}.$$

The singular solutions occur when the determinant is 0, which only happens when $x_i = x_h$ for some $1 \leq i < h \leq k$. A solution is non-singular if $x_i \neq x_h$ for all $1 \leq i < h \leq k$.

Let I_1 denote the number of solutions counted by $J_{s,k}(X)$ with $x_i = x_h$ for some $1 \leq i < h \leq k$.

Let I_2 denote the corresponding number of solutions with $x_i \neq x_h$ for all $1 \leq i < h \leq k$.

Then

$$J_{s,k}(X) = I_1 + I_2$$

and we have

$$J_{s,k}(X) \leq 2I_1 \quad \text{or} \quad J_{s,k}(X) \leq 2I_2.$$

(1) Suppose that $I_1 \geq I_2$ so that $J_{s,k}(X) \ll I_1$. Since $x_i = x_h$ for some $1 \leq i < h \leq k$, by relabelling variables, the $\mathbf{x}, \mathbf{y}$ counted by I_1 satisfy

$$2x_1^j + \sum_{i=3}^{s} x_i^j = \sum_{i=1}^{s} y_i^j \quad (1 \leq j \leq k).$$

Thus

$$J_{s,k}(X) \ll \int_{[0,1)^k} f(2\boldsymbol{\alpha}, X) f(\boldsymbol{\alpha}, X)^{s-2} f(-\boldsymbol{\alpha}, X)^s d\boldsymbol{\alpha}.$$

Apply Hölder's inequality to relate the integral to $J_{s,k}(X)$. We get

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

which implies that $J_{s,k}(X) \ll 1$, a contradiction to $J_{s,k}(X) \gg X^s$.

(2) From (1), we see that $J_{s,k}(X) \ll I_2$. For $\mathbf{x}, \mathbf{y}$ counted by I_2, we have $x_i \neq x_h$ for all $1 \leq i < h \leq k$. Let

$$\Xi(\mathbf{x}) = \prod_{1 \leq i < h \leq k} (x_i - x_h) \neq 0.$$

Note that for a fixed i, there are $(k-i)$ choices for h. Since $|x_i - x_h| \leq X$, we have

$$1 \leq |\Xi(\mathbf{x})| \leq X^{k-1} X^{k-2} \cdots X \cdot 1 = X^{k(k-1)/2}.$$

Let $N(\mathbf{x})$ be the number of primes p with $p | \Xi(\mathbf{x})$ and $X^{1/k} < p \leq 2X^{1/k}$. Then

$$(X^{1/k})^{N(\mathbf{x})} \leq \prod_{\substack{p | \Xi(\mathbf{x}) \\ X^{1/k} < p \leq 2X^{1/k}}} p \leq |\Xi(\mathbf{x})|.$$

Thus

$$N(\mathbf{x}) \leq \frac{\log |\Xi(\mathbf{x})|}{\log(X^{1/k})} \leq \frac{k(k-1)/2}{1/k} < k^3.$$

Let $\mathcal{P}$ be the set of the smallest k^3 primes p with $p > X^{1/k}$. By the prime number theorem, the number of primes between $X^{1/k}$ and $2X^{1/k}$ is of size $(X^{1/k}/\log X)$, which is $> k^3$. Hence if $p \in \mathcal{P}$, then $p \leq 2X^{1/k}$.

We recall that $N(\mathbf{x})$ is the number of primes p with $p|\Xi(\mathbf{x})$ and $X^{1/k} < p \leq 2X^{1/k}$. Since $N(\mathbf{x}) < k^3 = |\mathcal{P}|$, given any $\mathbf{x}, \mathbf{y}$ counted by I_2, there exists at least one prime $p \in \mathcal{P}$ for which $p \nmid \Xi(\mathbf{x})$. It follows that $\{x_1, \cdots, x_k\}$ distinct (mod p).

Define $J_{s,k}(X;p)$ be the number of $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ satisfying

$$\sum_{i=1}^{s} x_i^j = \sum_{i=1}^{s} y_i^j \quad (1 \le j \le k)$$

with $x_i, y_i \le X$ and $\{x_1, \cdots, x_k\}$ distinct (mod p). It follows that

$$J_{s,k}(X) \ll I_2 \le \sum_{p \in \mathcal{P}} J_{s,k}(X;p) \ll \max_{p \in \mathcal{P}} J_{s,k}(X;p).$$

The last inequality holds since $|\mathcal{P}| = k^3$.

We recall that $J_{s,k}(X;p)$ counts the number of $\mathbf{x},\mathbf{y}\in\mathbb{N}^s$ satisfying

$$\sum_{i=1}^{s} x_i^j = \sum_{i=1}^{s} y_i^j \quad (1\le j\le k)$$

with $x_i, y_i \le X$ and $\{x_1,\cdots,x_k\}$ distinct (mod p). By Hölder's inequality, one can show that

$$J_{s,k}(X;p) \ll p^{2s-2k} \max_{0<\eta\le p} I_3(X;p,\eta),$$

where I_3 counts the number of $\mathbf{m},\mathbf{n}\in\mathbb{N}^k$, $\mathbf{u},\mathbf{v}\in\mathbb{N}^{s-k}$ satisfying

$$\sum_{i=1}^{k}(m_i^j - n_i^j) = \sum_{h=1}^{s-k}\left((pu_h+\eta)^j - (pv_h+\eta)^j\right) \quad (1\le j\le k)$$

with $m_i, n_i, pu_h+\eta, pv_h+\eta \le X$, $\{m_1,\cdots,m_k\}$ distinct (mod p) and $\{n_1,\cdots,n_k\}$ distinct (mod p).

Using the binomial theorem, the above equations equal to

$$\sum_{i=1}^{k}\left((m_i-\eta)^j-(n_i-\eta)^j\right)=p^j\sum_{h=1}^{s-k}(u_h^j-v_h^j)\quad(1\le j\le k)$$

with $m_i, n_i, pu_h+\eta, pv_h+\eta \le X$, $\{m_1,\cdots,m_k\}$ distinct (mod p) and $\{n_1,\cdots,n_k\}$ distinct (mod p). Fix one of the $O(X^k)$ possible choices for $\{n_1,\cdots,n_k\}$. Since $m_i \le X < p^k$, by the Key Lemma, the congruence

$$\sum_{i=1}^{k}(m_i-\eta)^j\equiv\sum_{i=1}^{k}(n_i-\eta)^j\pmod{p^j}$$

has $O(p^{k(k-1)/2})$ possible choices for $\{m_1,\cdots,m_k\}$.

For fixed $\mathbf{m}, \mathbf{n}$, write

$$\sum_{i=1}^{k} \big((m_i - \eta)^j - (n_i - \eta)^j\big) = c_j p^j \quad (1 \le j \le k).$$

Then $\mathbf{u}, \mathbf{v}$ satisfy the system of equations

$$(u_1^j + \cdots + u_{s-k}^j) - (v_1^j + \cdots + v_{s-k}^j) = c_j \quad (1 \le j \le k)$$

with $(1 - \eta)/p < u_h, v_h \le (X - \eta)/p$. So the number of $\mathbf{u}, \mathbf{v}$ is bounded by

$$1 + J_{s-k,k}(X/p).$$

It follows that

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

Since $X^{1/k} < p \le 2X^{1/k}$, it follows that

$$J_{s,k}(X) \ll J_{s,k}(X;p) \ll X^{2s-k(k+1)/2+\Delta_{s,k}}$$

with

$$\Delta_{s,k} = \Delta_{s-k,k}(1-1/k).$$

We recall that

$$\Delta_{k,k} = k^2(1-1/k)/2.$$

Thus for $s = rk$, we have

$$\Delta_{s,k} = k^2(1-1/k)^r/2.$$

4. Applications to Waring's Problem

Fix $s, k \in \mathbb{N}$ with $k \geq 3$. Let $X = \lfloor n^{1/k} \rfloor$ and

$$f(\alpha) = \sum_{1 \leq x \leq X} e(\alpha x^k).$$

We recall that for $n \in \mathbb{N}$,

$$\begin{aligned} R(n) &= \#\{\mathbf{x} \in \mathbb{N}^s : n = x_1^k + \cdots + x_s^k\} \\ &= \int_0^1 f(\alpha)^s e(-\alpha n) d\alpha \\ &= \int_{\mathfrak{M}_\delta} f(\alpha)^s e(-\alpha n) d\alpha + \int_{\mathfrak{m}_\delta} f(\alpha)^s e(-\alpha n) d\alpha, \end{aligned}$$

where

$$\mathfrak{M}_\delta = \bigcup_{\substack{0 \leq a < q \leq X^\delta \\ \gcd(a,q)=1}} \mathfrak{M}_\delta(q,a) \quad \text{and} \quad \mathfrak{m}_\delta = [0,1) \setminus \mathfrak{M}$$

with

$$\mathfrak{M}_\delta(q,a) = \{\alpha \in [0,1) : |\alpha - a/q| \leq X^{\delta - k}\}.$$

To get

$$\int_{\mathfrak{m}_\delta} f(\alpha)^s e(-\alpha n) d\alpha = o(X^{s-k}),$$

by Weyl's Inequality,

$$\sup_{\mathfrak{m}_\delta} |f(\alpha)| \ll X^{1-\delta 2^{1-k}+\epsilon}.$$

By Hua's Lemma,

$$\int_0^1 |f(\alpha)|^{2^k} d\alpha \ll X^{2^k-k+\epsilon}.$$

• Both estimates make use of Weyl's differencing $(k-1)$ times, which requires $s \geq 2^k + 1$.

An Analogue of Hua's Lemma

Proposition 1 For $k \geq 3$, let $s = rk$ for some $r \in \mathbb{N}$. We have

$$\int_0^1 |f(\alpha)|^{2s} d\alpha \ll X^{2s-k+\Delta_{s,k}}.$$

Proof. We recall $\int_0^1 |f(\alpha)|^{2s} d\alpha$ counts the number of $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ satisfying

$$(x_1^k + \cdots + x_s^k) - (y_1^k + \cdots + y_s^k) = 0$$

with $x_i, y_i \leq X$. This is equal to the number of $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ satisfying

$$(x_1^j + \cdots + x_s^j) - (y_1^j + \cdots + y_s^j) = h_j \quad (1 \leq j \leq k)$$

with $x_i, y_i \leq X$, $h_k = 0$ and $|h_j| < sX^j$ $(1 \leq j \leq k-1)$. This links $\int_0^1 |f(\alpha)|^{2s} d\alpha$ to $J_{s,k}(X)$.

An Analogue of Weyl's Inequality

By the large sieve inequality and Weyl's shift,

Proposition 2 We have

$$\sup_{\alpha\in\mathfrak{m}_\delta} |f(\alpha)| \ll X^{1-\sigma+\epsilon},$$

where

$$\sigma = \sigma_{s,k}(\delta) = \frac{\delta - (1-\delta)\Delta_{s,k}}{2s} \quad \text{with} \quad s = rk.$$

By taking

$$\delta = 1/8 \quad \text{and} \quad s = k\lceil 2k(\log k + \log\log k)\rceil,$$

we have

$$\sup_{\alpha\in\mathfrak{m}_{1/8}} |f(\alpha)| \ll X^{1-\frac{1}{32k^2(\log k + O(\log\log k))}+\epsilon}.$$

Theorem If $s \geq 4k^2(\log k + O(\log\log k))$, then

$$\int_{\mathfrak{m}_{1/8}} f(\alpha)^s e(-n\alpha)d\alpha = o(X^{s-k}).$$

Proof. Write $s = t + 2rk$. By the above two propositions, we have

$$\begin{aligned}\Big|\int_{\mathfrak{m}_{1/8}} f(\alpha)^{t+2rk} e(-n\alpha)d\alpha\Big| &\leq \sup_{\mathfrak{m}_{1/8}} |f(\alpha)|^t \int_0^1 |f(\alpha)|^{2rk} d\alpha \\ &\ll \left(X^{1-\frac{1}{32k^2(\log k+O(\log\log k))}+\epsilon}\right)^t \cdot X^{2rk-k+\Delta_{rk,k}}.\end{aligned}$$

The above integral is $o(X^{s-k})$ provided that

$$\frac{t}{32k^2(\log k + O(\log\log k))} > \frac{1}{2}k^2(1-1/k)^r.$$

It suffices to take $r = \lceil 2k(\log k + \log\log k)\rceil$ and $t \sim 16k^2/\log k$.

By a refined major arcs analysis, one can show that if $s \geq \max\{5, k+1\}$,

$$\int_{\mathfrak{M}_{1/8}} f(\alpha)^s e(-n\alpha) d\alpha = \mathfrak{S}(n) \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1} + o(n^{s/k-1}).$$

Also, if $s \geq 4k^2(\log k + O(\log\log k))$, then

$$\int_{\mathfrak{m}_{1/8}} f(\alpha)^s e(-n\alpha) d\alpha = o(n^{s/k-1}).$$

It follows that if $s \geq 4k^2(\log k + O(\log\log k))$,

$$R(n) = \mathfrak{S}(n) \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1} + o(n^{s/k-1}).$$

We recall that $G(k)$ denotes the least integer $s = s(k)$ such that for all $n \in \mathbb{N}$ sufficiently large, there exist $\mathbf{x} = (x_1, \cdots, x_s) \in \mathbb{N}^s$ such that

$$n = x_1^k + x_2^k + \cdots + x_s^k.$$

Corollary We have

$$G(k) \leq 4k^2(\log k + O(\log\log k)).$$

• Use the smooth numbers approach to improve the above bound to $G(k) \leq k(\log k + O(\log\log k))$.