Math 571, Spring 2025, Vinogradov's Mean Value Theorem

Robert C. Vaughan

April 29, 2025

- Let
$$\boldsymbol{\nu}(n) = (n, n^2, \dots, n^k)$$

- Let

$$\boldsymbol{\nu}(n) = (n, n^2, \ldots, n^k)$$

- and let

$$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_k),$$
$$f(\boldsymbol{\alpha}, \mathcal{A}) = \sum_{n\in\mathcal{A}} e\big(\boldsymbol{\alpha}.\boldsymbol{\nu}(n)\big)$$

where $\mathcal{A}$ is a finite set of integers.

- Let

$$\boldsymbol{\nu}(n) = (n, n^2, \ldots, n^k)$$

- and let

$$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_k),$$

$$f(\boldsymbol{\alpha}, \mathcal{A}) = \sum_{n \in \mathcal{A}} e(\boldsymbol{\alpha}.\boldsymbol{\nu}(n))$$

  where $\mathcal{A}$ is a finite set of integers.

- We are interested in the mean value

$$J_k(\mathcal{A}, b) = \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}, \mathcal{A})|^{2b} \, \boldsymbol{d\alpha}.$$

- Now

$$f(\alpha,\mathcal{A})^b = \sum_{\boldsymbol{m}} r\big(\boldsymbol{m},\mathcal{A}^b\big)e(\boldsymbol{\alpha}.\mathbf{m})$$

where $r\big(\boldsymbol{m},\mathcal{A}^b\big)$ denotes the number of solutions of the system

$$\begin{array}{ccccccc} n_1 & + & \cdots & + & n_b & = & m_1 \\ n_1^2 & + & \cdots & + & n_b^2 & = & m_2 \\ \vdots & & & & \vdots & & \vdots \\ n_1^k & + & \cdots & + & n_b^k & = & m_k \end{array} \tag{1}$$

with $n_i \in \mathcal{A}$.

- Now
$$f(\alpha,\mathcal{A})^b = \sum_{\boldsymbol{m}} r\big(\boldsymbol{m},\mathcal{A}^b\big)e(\boldsymbol{\alpha}.\mathbf{m})$$
where $r\big(\boldsymbol{m},\mathcal{A}^b\big)$ denotes the number of solutions of the system
$$\begin{array}{ccccccc} n_1 & + & \cdots & + & n_b & = & m_1 \\ n_1^2 & + & \cdots & + & n_b^2 & = & m_2 \\ \vdots & & & & \vdots & & \vdots \\ n_1^k & + & \cdots & + & n_b^k & = & m_k \end{array} \tag{1}$$
with $n_i \in \mathcal{A}$.
- Thus by Parseval's identity,
$$J_k(\mathcal{A},b) = \sum_{\boldsymbol{m}} r\big(\boldsymbol{m},\mathcal{A}^b\big)^2.$$

- When $\mathcal{B}$ and $\mathcal{C}$ are subsets of $\mathbb{R}^b$ containing only finitely many lattice points, let $N(\mathcal{B}, \mathcal{C}, \boldsymbol{\ell})$ denote the number of solutions of

$$\begin{array}{ccccccccccccc} m_1 & + & \cdots & + & m_b & = & n_1 & + & \cdots & + & n_b & + & \ell_1 \\ m_1^2 & + & \cdots & + & m_b^2 & = & n_1^2 & + & \cdots & + & n_b^2 & + & \ell_2 \\ \vdots & & & & \vdots & & \vdots & & & & \vdots & & \vdots \\ m_1^k & + & \cdots & + & m_b^k & = & n_1^k & + & \cdots & + & n_b^k & + & \ell_k \end{array}$$

with $\boldsymbol{m} \in \mathcal{B}$ and $\boldsymbol{n} \in \mathcal{C}$.

- When $\mathcal{B}$ and $\mathcal{C}$ are subsets of $\mathbb{R}^b$ containing only finitely many lattice points, let $N(\mathcal{B},\mathcal{C},\boldsymbol{\ell})$ denote the number of solutions of

$$\begin{array}{ccccccccccccc} m_1 & + & \cdots & + & m_b & = & n_1 & + & \cdots & + & n_b & + & \ell_1 \\ m_1^2 & + & \cdots & + & m_b^2 & = & n_1^2 & + & \cdots & + & n_b^2 & + & \ell_2 \\ \vdots & & & & \vdots & & \vdots & & & & \vdots & & \vdots \\ m_1^k & + & \cdots & + & m_b^k & = & n_1^k & + & \cdots & + & n_b^k & + & \ell_k \end{array}$$

with $\boldsymbol{m} \in \mathcal{B}$ and $\boldsymbol{n} \in \mathcal{C}$.

- For brevity write $N(\mathcal{B},\boldsymbol{\ell}) = N(\mathcal{B},\mathcal{B},\boldsymbol{\ell})$, $N(\mathcal{B}) = N(\mathcal{B},\mathbf{0})$ and $N(\mathcal{B},\mathcal{C}) = N(\mathcal{B},\mathcal{C},\mathbf{0})$.

- When $\mathcal{B}$ and $\mathcal{C}$ are subsets of $\mathbb{R}^b$ containing only finitely many lattice points, let $N(\mathcal{B},\mathcal{C},\boldsymbol{\ell})$ denote the number of solutions of

$$\begin{array}{ccccccccccccc} m_1 & + & \cdots & + & m_b & = & n_1 & + & \cdots & + & n_b & + & \ell_1 \\ m_1^2 & + & \cdots & + & m_b^2 & = & n_1^2 & + & \cdots & + & n_b^2 & + & \ell_2 \\ \vdots & & & & \vdots & & \vdots & & & & \vdots & & \vdots \\ m_1^k & + & \cdots & + & m_b^k & = & n_1^k & + & \cdots & + & n_b^k & + & \ell_k \end{array}$$

  with $\boldsymbol{m} \in \mathcal{B}$ and $\boldsymbol{n} \in \mathcal{C}$.
- For brevity write $N(\mathcal{B},\boldsymbol{\ell}) = N(\mathcal{B},\mathcal{B},\boldsymbol{\ell})$, $N(\mathcal{B}) = N(\mathcal{B},\mathbf{0})$ and $N(\mathcal{B},\mathcal{C}) = N(\mathcal{B},\mathcal{C},\mathbf{0})$.
- Then we can define the more general mean

$$J_k(\mathcal{A},b,\boldsymbol{\ell}) = N\big(\mathcal{A}^b,\boldsymbol{\ell}\big),$$

  so that

$$J_k(\mathcal{A},b) = N\big(\mathcal{A}^b\big).$$

- The following elementary observations are useful.

Lemma 1

In the above notation,
(a) *If* $\mathcal{B} \subseteq \mathcal{C}$, *then* $N(\mathcal{B}, \ell) \le N(\mathcal{C}, \ell)$,
(b) $N(\mathcal{B}, \ell) \le N(\mathcal{B})$ *for all* ℓ,
(c) *If* $\mathcal{C} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_j$, *then* $N(\mathcal{C}) \le j \sum_{i=1}^{j} N(\mathcal{B}_i)$,
(d) *If* $a \ne 0$ *and* $\mathbf{d} = (d, d, \ldots, d)$, *then*
$N(a\mathcal{B} + \mathbf{d}, a\mathcal{C} + \mathbf{d}) = N(\mathcal{B}, \mathcal{C})$,
(e) $J_k(\mathcal{A}, b, \ell) \le J_k(\mathcal{A}, b)$.

- The following elementary observations are useful.

Lemma 1

In the above notation,
(a) *If* $\mathcal{B} \subseteq \mathcal{C}$*, then* $N(\mathcal{B}, \ell) \le N(\mathcal{C}, \ell)$,
(b) $N(\mathcal{B}, \ell) \le N(\mathcal{B})$ *for all* ℓ,
(c) *If* $\mathcal{C} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_j$*, then* $N(\mathcal{C}) \le j \sum_{i=1}^{j} N(\mathcal{B}_i)$,
(d) *If* $a \ne 0$ *and* $\boldsymbol{d} = (d, d, \ldots, d)$*, then*
$N(a\mathcal{B} + \boldsymbol{d}, a\mathcal{C} + \boldsymbol{d}) = N(\mathcal{B}, \mathcal{C})$,
(e) $J_k(\mathcal{A}, b, \ell) \le J_k(\mathcal{A}, b)$.

- (d) is the fundamental *translation-dilation* property.

- The following elementary observations are useful.

Lemma 1

In the above notation,
(a) *If* $\mathcal{B} \subseteq \mathcal{C}$, *then* $N(\mathcal{B}, \ell) \le N(\mathcal{C}, \ell)$,
(b) $N(\mathcal{B}, \ell) \le N(\mathcal{B})$ *for all* ℓ,
(c) *If* $\mathcal{C} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_j$, *then* $N(\mathcal{C}) \le j \sum_{i=1}^{j} N(\mathcal{B}_i)$,
(d) *If* $a \ne 0$ *and* $\mathbf{d} = (d, d, \ldots, d)$, *then*
$N(a\mathcal{B} + \mathbf{d}, a\mathcal{C} + \mathbf{d}) = N(\mathcal{B}, \mathcal{C})$,
(e) $J_k(\mathcal{A}, b, \ell) \le J_k(\mathcal{A}, b)$.

- (d) is the fundamental *translation-dilation* property.
- **Proof.** (a) is obvious.

- The following elementary observations are useful.

Lemma 1

In the above notation,
(a) *If* $\mathcal{B} \subseteq \mathcal{C}$, *then* $N(\mathcal{B}, \boldsymbol{\ell}) \le N(\mathcal{C}, \boldsymbol{\ell})$,
(b) $N(\mathcal{B}, \boldsymbol{\ell}) \le N(\mathcal{B})$ *for all* $\boldsymbol{\ell}$,
(c) *If* $\mathcal{C} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_j$, *then* $N(\mathcal{C}) \le j \sum_{i=1}^{j} N(\mathcal{B}_i)$,
(d) *If* $a \ne 0$ *and* $\mathbf{d} = (d, d, \ldots, d)$, *then* $N(a\mathcal{B} + \mathbf{d}, a\mathcal{C} + \mathbf{d}) = N(\mathcal{B}, \mathcal{C})$,
(e) $J_k(\mathcal{A}, b, \boldsymbol{\ell}) \le J_k(\mathcal{A}, b)$.

- (d) is the fundamental *translation-dilation* property.
- **Proof.** (a) is obvious.
- (b) We have already seen versions of this.

$$N(\mathcal{B}, \boldsymbol{\ell}) = \int_{\mathbb{T}^k} \Big| \sum_{\boldsymbol{m}} r(\boldsymbol{m}, \mathcal{B}) e(\boldsymbol{m} \cdot \boldsymbol{\alpha}) \Big|^2 e(-\boldsymbol{\ell} \cdot \boldsymbol{\alpha})\, \boldsymbol{d\alpha}$$
$$\le \int_{\mathbb{T}^k} \Big| \sum_{\boldsymbol{m}} r(\boldsymbol{m}, \mathcal{B}) e(\boldsymbol{m} \cdot \boldsymbol{\alpha}) \Big|^2 \boldsymbol{d\alpha} = N(\mathcal{B}),$$

- **Lemma.**
  (c) *If* $\mathcal{C} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_j$, *then* $N(\mathcal{C}) \le j \sum_{i=1}^{j} N(\mathcal{B}_i)$,
  (d) *If* $a \ne 0$ *and* $\boldsymbol{d} = (d, d, \ldots, d)$, *then* $N(a\mathcal{B} + \boldsymbol{d}, a\mathcal{C} + \boldsymbol{d}) = N(\mathcal{B}, \mathcal{C})$,
  (e) $J_k(\mathcal{A}, b, \boldsymbol{\ell}) \le J_k(\mathcal{A}, b)$.

- **Lemma.**
  (c) *If* $\mathcal{C} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_j$, *then* $N(\mathcal{C}) \le j \sum_{i=1}^{j} N(\mathcal{B}_i)$,
  (d) *If* $a \ne 0$ *and* $\boldsymbol{d} = (d, d, \dots, d)$, *then*
  $N(a\mathcal{B} + \boldsymbol{d}, a\mathcal{C} + \boldsymbol{d}) = N(\mathcal{B}, \mathcal{C})$,
  (e) $J_k(\mathcal{A}, b, \boldsymbol{\ell}) \le J_k(\mathcal{A}, b)$.
- (c) In the above notation,

$$r(\boldsymbol{m}, \mathcal{C}) \le \sum_{i=1}^{j} r(\boldsymbol{m}, \mathcal{B}_i)$$

- **Lemma.**
  (c) *If* $\mathcal{C} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_j$, *then* $N(\mathcal{C}) \le j \sum_{i=1}^{j} N(\mathcal{B}_i)$,
  (d) *If* $a \ne 0$ *and* $\boldsymbol{d} = (d, d, \ldots, d)$, *then* $N(a\mathcal{B} + \boldsymbol{d}, a\mathcal{C} + \boldsymbol{d}) = N(\mathcal{B}, \mathcal{C})$,
  (e) $J_k(\mathcal{A}, b, \ell) \le J_k(\mathcal{A}, b)$.
- (c) In the above notation,

$$r(\boldsymbol{m}, \mathcal{C}) \le \sum_{i=1}^{j} r(\boldsymbol{m}, \mathcal{B}_i)$$

- and so by Cauchy's inequality

$$r(\boldsymbol{m}, \mathcal{C})^2 \le j \sum_{i=1}^{j} r(\boldsymbol{m}, \mathcal{B}_i)^2.$$

- **Lemma.**
  (c) *If* $\mathcal{C} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_j$, *then* $N(\mathcal{C}) \le j \sum_{i=1}^{j} N(\mathcal{B}_i)$,
  (d) *If* $a \ne 0$ *and* $\boldsymbol{d} = (d, d, \ldots, d)$, *then* $N(a\mathcal{B} + \boldsymbol{d}, a\mathcal{C} + \boldsymbol{d}) = N(\mathcal{B}, \mathcal{C})$,
  (e) $J_k(\mathcal{A}, b, \ell) \le J_k(\mathcal{A}, b)$.
- (c) In the above notation,

$$r(\boldsymbol{m}, \mathcal{C}) \le \sum_{i=1}^{j} r(\boldsymbol{m}, \mathcal{B}_i)$$

- and so by Cauchy's inequality

$$r(\boldsymbol{m}, \mathcal{C})^2 \le j \sum_{i=1}^{j} r(\boldsymbol{m}, \mathcal{B}_i)^2.$$

- It now suffices to sum this over $\boldsymbol{m}$, since

$$N(\mathcal{C}) = \sum_{\boldsymbol{m}} r(\boldsymbol{m}, \mathcal{C})^2, \quad N(\mathcal{B}_i) = \sum_{\boldsymbol{m}} r(\boldsymbol{m}, \mathcal{B}_i)^2.$$

- **Lemma 1.**
  (d) *If* $a \neq 0$ *and* $\boldsymbol{d} = (d, d, \ldots, d)$*, then* $N(a\mathcal{B} + \boldsymbol{d}, a\mathcal{C} + \boldsymbol{d}) = N(\mathcal{B}, \mathcal{C})$*,*
  (e) $J_k(\mathcal{A}, b, \ell) \leq J_k(\mathcal{A}, b)$.

- **Lemma 1.**
  (d) *If* $a \neq 0$ *and* $\boldsymbol{d} = (d, d, \ldots, d)$, *then* $N(a\mathcal{B} + \boldsymbol{d}, a\mathcal{C} + \boldsymbol{d}) = N(\mathcal{B}, \mathcal{C})$,
  (e) $J_k(\mathcal{A}, b, \ell) \leq J_k(\mathcal{A}, b)$.
- It is useful to introduce the notation

$$s_j(\boldsymbol{\theta}) = s_j(\boldsymbol{\theta}; b) = \sum_{r=1}^{b} \theta_r^j.$$

- **Lemma 1.**
  (d) *If* $a \neq 0$ *and* $\boldsymbol{d} = (d, d, \ldots, d)$, *then* $N(a\mathcal{B} + \boldsymbol{d}, a\mathcal{C} + \boldsymbol{d}) = N(\mathcal{B}, \mathcal{C})$,
  (e) $J_k(\mathcal{A}, b, \ell) \leq J_k(\mathcal{A}, b)$.
- It is useful to introduce the notation
  $$s_j(\boldsymbol{\theta}) = s_j(\boldsymbol{\theta}; b) = \sum_{r=1}^{b} \theta_r^j.$$
- Then $N(\mathcal{B}, \mathcal{C})$ is the number of solutions of $s_j(\mathbf{m}) = s_j(\mathbf{n})$ $(1 \leq j \leq k)$ with $m_j \in \mathcal{B}$ and $\mathbf{n}_j \in \mathcal{C}$.

- **Lemma 1.**
  (d) *If* $a \neq 0$ *and* $\mathbf{d} = (d, d, \ldots, d)$, *then* $N(a\mathcal{B} + \mathbf{d}, a\mathcal{C} + \mathbf{d}) = N(\mathcal{B}, \mathcal{C})$,
  (e) $J_k(\mathcal{A}, b, \boldsymbol{\ell}) \leq J_k(\mathcal{A}, b)$.
- It is useful to introduce the notation
  $$s_j(\boldsymbol{\theta}) = s_j(\boldsymbol{\theta}; b) = \sum_{r=1}^{b} \theta_r^j.$$
- Then $N(\mathcal{B}, \mathcal{C})$ is the number of solutions of $s_j(\mathbf{m}) = s_j(\mathbf{n})$ $(1 \leq j \leq k)$ with $m_j \in \mathcal{B}$ and $\mathbf{n}_j \in \mathcal{C}$.
- Suppose $s_j(\mathbf{m}) = s_j(\mathbf{n})$ $(1 \leq j \leq k)$. By the binomial theorem $s_j(a\mathbf{m} + d) = \sum_{\ell=0}^{j} \binom{j}{\ell} a^\ell d^{j-\ell} s_\ell(\mathbf{m}) = s_j(a\mathbf{n} + d)$.

- **Lemma 1.**
  (d) *If* $a \neq 0$ *and* $\mathbf{d} = (d, d, \ldots, d)$, *then* $N(a\mathcal{B} + \mathbf{d}, a\mathcal{C} + \mathbf{d}) = N(\mathcal{B}, \mathcal{C})$,
  (e) $J_k(\mathcal{A}, b, \boldsymbol{\ell}) \le J_k(\mathcal{A}, b)$.
- It is useful to introduce the notation
$$s_j(\boldsymbol{\theta}) = s_j(\boldsymbol{\theta}; b) = \sum_{r=1}^{b} \theta_r^j.$$
- Then $N(\mathcal{B}, \mathcal{C})$ is the number of solutions of $s_j(\mathbf{m}) = s_j(\mathbf{n})$ $(1 \le j \le k)$ with $m_j \in \mathcal{B}$ and $\mathbf{n}_j \in \mathcal{C}$.
- Suppose $s_j(\mathbf{m}) = s_j(\mathbf{n})$ $(1 \le j \le k)$. By the binomial theorem $s_j(a\mathbf{m} + d) = \sum_{\ell=0}^{j} \binom{j}{\ell} a^\ell d^{j-\ell} s_\ell(\mathbf{m}) = s_j(a\mathbf{n} + d)$.
- If instead $s_j(a\mathbf{m} + d) = s_j(a\mathbf{n} + d)$ $(1 \le j \le k)$, then $a^j s_j(\mathbf{m}) = s_j\big((a\mathbf{m} + d) - d\big) = a^j s_j(\mathbf{n})$ in the same way.

- **Lemma 1.**
  (d) *If* $a \neq 0$ *and* $\mathbf{d} = (d, d, \dots, d)$, *then* $N(a\mathcal{B} + \mathbf{d}, a\mathcal{C} + \mathbf{d}) = N(\mathcal{B}, \mathcal{C})$,
  (e) $J_k(\mathcal{A}, b, \boldsymbol{\ell}) \le J_k(\mathcal{A}, b)$.
- It is useful to introduce the notation
  $$s_j(\boldsymbol{\theta}) = s_j(\boldsymbol{\theta}; b) = \sum_{r=1}^{b} \theta_r^j.$$
- Then $N(\mathcal{B}, \mathcal{C})$ is the number of solutions of $s_j(\mathbf{m}) = s_j(\mathbf{n})$ $(1 \le j \le k)$ with $m_j \in \mathcal{B}$ and $\mathbf{n}_j \in \mathcal{C}$.
- Suppose $s_j(\mathbf{m}) = s_j(\mathbf{n})$ $(1 \le j \le k)$. By the binomial theorem $s_j(a\mathbf{m} + d) = \sum_{\ell=0}^{j} \binom{j}{\ell} a^\ell d^{j-\ell} s_\ell(\mathbf{m}) = s_j(a\mathbf{n} + d)$.
- If instead $s_j(a\mathbf{m} + d) = s_j(a\mathbf{n} + d)$ $(1 \le j \le k)$, then $a^j s_j(\mathbf{m}) = s_j\big((a\mathbf{m} + d) - d\big) = a^j s_j(\mathbf{n})$ in the same way.
- (e) is a special case of (b).

- There is a close connection between the $s_r(\boldsymbol{\theta})$ and the *elementary symmetric functions* of the θ_j, $\sigma_r(\boldsymbol{\theta})$ which can be defined so that $(-1)^r\sigma_r(\boldsymbol{\theta})$ is the coefficient of z^r in the polynomial $P(z) = \prod_{j=1}^{b}(1 - z\theta_j)$.

- There is a close connection between the $s_r(\boldsymbol{\theta})$ and the *elementary symmetric functions* of the θ_j, $\sigma_r(\boldsymbol{\theta})$ which can be defined so that $(-1)^r\sigma_r(\boldsymbol{\theta})$ is the coefficient of z^r in the polynomial $P(z) = \prod_{j=1}^{b}(1 - z\theta_j)$.
- By considering the power series expansion of $zP'(z)/P(z)$ in a small disc centred on 0 one obtains the Newton-Girard formulæ which assert that

$$\sum_{j=0}^{r-1}(-1)^{r-1-j}\sigma_j s_{r-j} = r\sigma_r \tag{2}$$

for $1 \le r \le b$, and that

$$\sum_{j=0}^{b}(-1)^{j}\sigma_j s_{r-j} = 0 \tag{3}$$

for $r \ge b$.

- There is a close connection between the $s_r(\boldsymbol{\theta})$ and the *elementary symmetric functions* of the θ_j, $\sigma_r(\boldsymbol{\theta})$ which can be defined so that $(-1)^r\sigma_r(\boldsymbol{\theta})$ is the coefficient of z^r in the polynomial $P(z) = \prod_{j=1}^{b}(1 - z\theta_j)$.
- By considering the power series expansion of $zP'(z)/P(z)$ in a small disc centred on 0 one obtains the Newton-Girard formulæ which assert that

$$\sum_{j=0}^{r-1}(-1)^{r-1-j}\sigma_j s_{r-j} = r\sigma_r \tag{2}$$

for $1 \le r \le b$, and that

$$\sum_{j=0}^{b}(-1)^{j}\sigma_j s_{r-j} = 0 \tag{3}$$

for $r \ge b$.
- In this second identity, the quantity s_0 arises when $j = r = b$ and it is to be understood that $s_0 = b$ even if one or more of the θ_j vanishes.

- **Lemma 2.**
  (a) *Suppose that* $\theta_1, \ldots, \theta_b, \phi_1, \ldots, \phi_b$ *are such that*

$$s_r(\boldsymbol{\theta}) = s_r(\boldsymbol{\phi}) \qquad (1 \le r \le b).$$

Then the polynomial $Q(z;\boldsymbol{\xi}) = \prod_{r=1}^{b}(z-\xi_r)$ *satisfies* $Q(z;\boldsymbol{\theta}) = Q(z;\boldsymbol{\phi})$ *identically.*
(b) *Suppose that* p *is a prime number with* $p > b$*, that* u *is a positive integer and that* $\theta_1, \ldots, \theta_b, \phi_1, \ldots, \phi_b$ *are integers such that*

$$s_r(\boldsymbol{\theta}) \equiv s_r(\boldsymbol{\phi}) \pmod{p^u} \qquad (1 \le r \le b).$$

Then

$$Q(z;\boldsymbol{\theta}) \equiv Q(z;\boldsymbol{\phi}) \pmod{p^u}$$

for all integers z*.*

- **Lemma 2.**
  (a) *Suppose that* $\theta_1,\ldots,\theta_b,\phi_1,\ldots,\phi_b$ *are such that*

$$s_r(\boldsymbol{\theta}) = s_r(\boldsymbol{\phi}) \qquad (1\le r\le b).$$

  Then the polynomial $Q(z;\boldsymbol{\xi})=\prod_{r=1}^b(z-\xi_r)$ *satisfies* $Q(z;\boldsymbol{\theta})=Q(z;\boldsymbol{\phi})$ *identically.*
  (b) *Suppose that* p *is a prime number with* $p>b$, *that* u *is a positive integer and that* $\theta_1,\ldots,\theta_b,\phi_1,\ldots,\phi_b$ *are integers such that*

$$s_r(\boldsymbol{\theta}) \equiv s_r(\boldsymbol{\phi}) \pmod{p^u} \qquad (1\le r\le b).$$

  Then

$$Q(z;\boldsymbol{\theta}) \equiv Q(z;\boldsymbol{\phi}) \pmod{p^u}$$

  for all integers z.
- Proof. (a). It is a simple induction on the Newton-Girard formulæ that $\sigma_r(\boldsymbol{\theta})=\sigma_r(\boldsymbol{\phi})$ for $1\le r\le b$. (b). Likewise $\pmod{p^u}$ as long as $p>b$.

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (a) $J_k(X,b) \le b!X^b$ *when* $b \le k$,
  (b) $J_k(X,b) \le k!X^{2b-k}$ *when* $b > k$,
  (c) $J_k(X,b) \ge \lfloor X \rfloor^b$,
  (d) $J_k(x,b) \ge (2b+1)^{-k} \lfloor X \rfloor^{2b-k(k+1)/2}$.

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (a) $J_k(X,b) \le b!X^b$ *when* $b \le k$,
  (b) $J_k(X,b) \le k!X^{2b-k}$ *when* $b > k$,
  (c) $J_k(X,b) \ge \lfloor X \rfloor^b$,
  (d) $J_k(x,b) \ge (2b+1)^{-k} \lfloor X \rfloor^{2b-k(k+1)/2}$.
- (a) $J_k(X,b)$ is the number of choices of $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,X]^b$ such that

$$s_r(\boldsymbol{m}) = s_r(\boldsymbol{n}) \quad (1 \le r \le k).$$

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (a) $J_k(X,b) \le b!X^b$ *when* $b \le k$,
  (b) $J_k(X,b) \le k!X^{2b-k}$ *when* $b > k$,
  (c) $J_k(X,b) \ge \lfloor X \rfloor^b$,
  (d) $J_k(x,b) \ge (2b+1)^{-k}\lfloor X \rfloor^{2b-k(k+1)/2}$.
- (a) $J_k(X,b)$ is the number of choices of $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,X]^b$ such that
$$s_r(\boldsymbol{m}) = s_r(\boldsymbol{n}) \quad (1 \le r \le k).$$
- Since $b \le k$
$$Q(z;\boldsymbol{m}) = Q(z;\boldsymbol{n})$$
identically.

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (a) $J_k(X,b) \le b!X^b$ *when* $b \le k$,
  (b) $J_k(X,b) \le k!X^{2b-k}$ *when* $b > k$,
  (c) $J_k(X,b) \ge \lfloor X \rfloor^b$,
  (d) $J_k(x,b) \ge (2b+1)^{-k} \lfloor X \rfloor^{2b-k(k+1)/2}$.
- (a) $J_k(X,b)$ is the number of choices of $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,X]^b$ such that
$$s_r(\boldsymbol{m}) = s_r(\boldsymbol{n}) \quad (1 \le r \le k).$$
- Since $b \le k$
$$Q(z;\boldsymbol{m}) = Q(z;\boldsymbol{n})$$
identically.
- Thus the n_i are permutations of the m_i.

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (a) $J_k(X,b) \le b!X^b$ *when* $b \le k$,
  (b) $J_k(X,b) \le k!X^{2b-k}$ *when* $b > k$,
  (c) $J_k(X,b) \ge \lfloor X \rfloor^b$,
  (d) $J_k(x,b) \ge (2b+1)^{-k} \lfloor X \rfloor^{2b-k(k+1)/2}$.
- (a) $J_k(X,b)$ is the number of choices of $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,X]^b$ such that
$$s_r(\boldsymbol{m}) = s_r(\boldsymbol{n}) \quad (1 \le r \le k).$$
- Since $b \le k$
$$Q(z;\boldsymbol{m}) = Q(z;\boldsymbol{n})$$
identically.
- Thus the n_i are permutations of the m_i.
- (b) When $b \ge k$,
$$J_k(X,b) = \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha})|^2 b d\boldsymbol{\alpha} \le x^{2b-2k} J_k(X,k).$$

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (a) $J_k(X,b) \le b!X^b$ *when* $b \le k$,
  (b) $J_k(X,b) \le k!X^{2b-k}$ *when* $b > k$,
  (c) $J_k(X,b) \ge \lfloor X \rfloor^b$,
  (d) $J_k(x,b) \ge (2b+1)^{-k}\lfloor X \rfloor^{2b-k(k+1)/2}$.
- (a) $J_k(X,b)$ is the number of choices of $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,X]^b$ such that
$$s_r(\boldsymbol{m}) = s_r(\boldsymbol{n}) \quad (1 \le r \le k).$$
- Since $b \le k$
$$Q(z;\boldsymbol{m}) = Q(z;\boldsymbol{n})$$
identically.
- Thus the n_i are permutations of the m_i.
- (b) When $b \ge k$,
$$J_k(X,b) = \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha})|^2 b d\boldsymbol{\alpha} \le x^{2b-2k} J_k(X,k).$$
- (c) Just take the variables on the right to be a permutation of those on the left.

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$*. Then*
(d) $J_k(x,b) \geq (2b+1)^{-k}\lfloor X\rfloor^{2b-k(k+1)/2}$.

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (d) $J_k(x,b) \ge (2b+1)^{-k}\lfloor X\rfloor^{2b-k(k+1)/2}$.
- (d) For brevity put $N = \lfloor X \rfloor$. We have already seen this.

$$\left| \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha})|^{2b} e(\boldsymbol{\alpha}.\boldsymbol{\ell}) d\boldsymbol{\alpha} \right| \le J_k(N,b).$$

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (d) $J_k(x,b) \ge (2b+1)^{-k}\lfloor X\rfloor^{2b-k(k+1)/2}$.
- (d) For brevity put $N = \lfloor X\rfloor$. We have already seen this.

$$\left|\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha})|^{2b} e(\boldsymbol{\alpha}.\boldsymbol{\ell})d\boldsymbol{\alpha}\right| \le J_k(N,b).$$

- The integral on the left is the number of solutions of

$$s_r(\boldsymbol{m}) - s_r(\boldsymbol{n}) = \ell_r \quad (1 \le r \le k)$$

with $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,N]^b$.

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
(d) $J_k(x,b) \ge (2b+1)^{-k}\lfloor X\rfloor^{2b-k(k+1)/2}$.
- (d) For brevity put $N = \lfloor X\rfloor$. We have already seen this.

$$\left|\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha})|^{2b} e(\boldsymbol{\alpha}.\boldsymbol{\ell})d\boldsymbol{\alpha}\right| \le J_k(N,b).$$

- The integral on the left is the number of solutions of

$$s_r(\boldsymbol{m}) - s_r(\boldsymbol{n}) = \ell_r \quad (1 \le r \le k)$$

with $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,N]^b$.
- Since $0 < s_r(\boldsymbol{m}) \le bN^r$ there are no solutions unless $\boldsymbol{\ell}$ satisfies $|\ell_r| \le bN^r$ $(1 \le r \le k)$.

- **Lemma 3.** *Let $J_k(X,b) = J_k((0,X],b)$. Then*
  (d) $J_k(x,b) \ge (2b+1)^{-k}\lfloor X\rfloor^{2b-k(k+1)/2}$.
- (d) For brevity put $N = \lfloor X\rfloor$. We have already seen this.

$$\left|\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha})|^{2b} e(\boldsymbol{\alpha}.\boldsymbol{\ell})d\boldsymbol{\alpha}\right| \le J_k(N,b).$$

- The integral on the left is the number of solutions of

$$s_r(\boldsymbol{m}) - s_r(\boldsymbol{n}) = \ell_r \quad (1 \le r \le k)$$

  with $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,N]^b$.
- Since $0 < s_r(\boldsymbol{m}) \le bN^r$ there are no solutions unless $\boldsymbol{\ell}$ satisfies $|\ell_r| \le bN^r$ $(1 \le r \le k)$.
- Sum both sides over all such $\boldsymbol{\ell}$.

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (d) $J_k(x,b) \ge (2b+1)^{-k}\lfloor X\rfloor^{2b-k(k+1)/2}$.
- (d) For brevity put $N = \lfloor X \rfloor$. We have already seen this.

$$\left| \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha})|^{2b} e(\boldsymbol{\alpha}.\boldsymbol{\ell}) d\boldsymbol{\alpha} \right| \le J_k(N,b).$$

- The integral on the left is the number of solutions of

$$s_r(\boldsymbol{m}) - s_r(\boldsymbol{n}) = \ell_r \quad (1 \le r \le k)$$

  with $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,N]^b$.
- Since $0 < s_r(\boldsymbol{m}) \le bN^r$ there are no solutions unless $\boldsymbol{\ell}$ satisfies $|\ell_r| \le bN^r$ $(1 \le r \le k)$.
- Sum both sides over all such $\boldsymbol{\ell}$.
- On the left we are just counting all possible choices of $\boldsymbol{m}$ and $\boldsymbol{n}$. N^{2b} in total.

- **Lemma 3.** *Let* $J_k(X,b) = J_k((0,X],b)$. *Then*
  (d) $J_k(x,b) \ge (2b+1)^{-k}\lfloor X\rfloor^{2b-k(k+1)/2}$.
- (d) For brevity put $N = \lfloor X\rfloor$. We have already seen this.

$$\left|\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha})|^{2b} e(\boldsymbol{\alpha}.\boldsymbol{\ell})d\boldsymbol{\alpha}\right| \le J_k(N,b).$$

- The integral on the left is the number of solutions of

$$s_r(\boldsymbol{m}) - s_r(\boldsymbol{n}) = \ell_r \quad (1 \le r \le k)$$

  with $\boldsymbol{m}$, $\boldsymbol{n}$ in $(0,N]^b$.
- Since $0 < s_r(\boldsymbol{m}) \le bN^r$ there are no solutions unless $\boldsymbol{\ell}$ satisfies $|\ell_r| \le bN^r$ $(1 \le r \le k)$.
- Sum both sides over all such $\boldsymbol{\ell}$.
- On the left we are just counting all possible choices of $\boldsymbol{m}$ and $\boldsymbol{n}$. N^{2b} in total.
- The number of $\boldsymbol{\ell}$ is $\le (2b+1)^k N^{\frac{1}{2}k(k+1)}$.

- All significant methods to bound $J_k(X, b)$ generally are motivated by some kind of "completion" process. The simplest is a p-adic argument due to Linnik.

- All significant methods to bound $J_k(X,b)$ generally are motivated by some kind of "completion" process. The simplest is a p-adic argument due to Linnik.
- **Lemma 4.** *Suppose that $p > k$. Let $A(p,\boldsymbol{h})$ be the number of $m_r \le p^k$ such that*

$$\sum_{r=1}^{k} m_r^j \equiv h_j \pmod{p^j} \qquad (1 \le j \le k)$$

and the m_r distinct modulo p. Then $A(p,\boldsymbol{h}) \le k!p^{\frac{1}{2}k(k-1)}$.

- All significant methods to bound $J_k(X,b)$ generally are motivated by some kind of "completion" process. The simplest is a p-adic argument due to Linnik.
- **Lemma 4.** *Suppose that $p > k$. Let $A(p,\boldsymbol{h})$ be the number of $m_r \le p^k$ such that*

$$\sum_{r=1}^{k} m_r^j \equiv h_j \pmod{p^j} \qquad (1 \le j \le k)$$

and the m_r distinct modulo p. Then $A(p,\boldsymbol{h}) \le k! p^{\frac{1}{2}k(k-1)}$.
- **Proof.** Let $B(p,\boldsymbol{g})$ denote the number of solutions of

$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k)$$

with $m_r \le p^k$ and the m_r distinct modulo p.

- All significant methods to bound $J_k(X,b)$ generally are motivated by some kind of "completion" process. The simplest is a p-adic argument due to Linnik.
- **Lemma 4.** *Suppose that $p>k$. Let $A(p,\boldsymbol{h})$ be the number of $m_r\le p^k$ such that*

$$\sum_{r=1}^{k} m_r^j \equiv h_j \pmod{p^j} \qquad (1\le j\le k)$$

and the m_r distinct modulo p. Then $A(p,\boldsymbol{h})\le k!p^{\frac12 k(k-1)}$.

- **Proof.** Let $B(p,\boldsymbol{g})$ denote the number of solutions of

$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1\le j\le k)$$

with $m_r\le p^k$ and the m_r distinct modulo p.
- Then for each $\boldsymbol{h}$, $A(p,\boldsymbol{h})$ is the sum of those $B(p,\boldsymbol{g})$ with $g_j\equiv h_j \pmod{p^j}$ and $1\le g_j\le p^k$ for $1\le j\le k$.

- All significant methods to bound $J_k(X,b)$ generally are motivated by some kind of "completion" process. The simplest is a p-adic argument due to Linnik.
- **Lemma 4.** *Suppose that $p > k$. Let $A(p,\boldsymbol{h})$ be the number of $m_r \le p^k$ such that*

$$\sum_{r=1}^{k} m_r^j \equiv h_j \pmod{p^j} \qquad (1 \le j \le k)$$

and the m_r distinct modulo p. Then $A(p,\boldsymbol{h}) \le k! p^{\frac12 k(k-1)}$.
- **Proof.** Let $B(p,\boldsymbol{g})$ denote the number of solutions of

$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k)$$

with $m_r \le p^k$ and the m_r distinct modulo p.
- Then for each $\boldsymbol{h}$, $A(p,\boldsymbol{h})$ is the sum of those $B(p,\boldsymbol{g})$ with $g_j \equiv h_j \pmod{p^j}$ and $1 \le g_j \le p^k$ for $1 \le j \le k$.
- The total number of possible choices for $\boldsymbol{g}$ is $p^{\frac12 k(k-1)}$.

- All significant methods to bound $J_k(X,b)$ generally are motivated by some kind of "completion" process. The simplest is a p-adic argument due to Linnik.
- **Lemma 4.** *Suppose that $p > k$. Let $A(p,\mathbf{h})$ be the number of $m_r \le p^k$ such that*

$$\sum_{r=1}^{k} m_r^j \equiv h_j \pmod{p^j} \qquad (1 \le j \le k)$$

and the m_r distinct modulo p. Then $A(p,\mathbf{h}) \le k!p^{\frac{1}{2}k(k-1)}$.
- **Proof.** Let $B(p,\mathbf{g})$ denote the number of solutions of

$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k)$$

with $m_r \le p^k$ and the m_r distinct modulo p.
- Then for each $\mathbf{h}$, $A(p,\mathbf{h})$ is the sum of those $B(p,\mathbf{g})$ with $g_j \equiv h_j \pmod{p^j}$ and $1 \le g_j \le p^k$ for $1 \le j \le k$.
- The total number of possible choices for $\mathbf{g}$ is $p^{\frac{1}{2}k(k-1)}$.
- Thus it suffices to show that $B(p,\mathbf{g}) \le k!$.

- $B(p, \boldsymbol{g})$ is the number of distinct $m_r \le p^k$ with

$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k).$$

It suffices to show that $B(p, \boldsymbol{g}) \le k!$.

- $B(p,\mathbf{g})$ is the number of distinct $m_r \le p^k$ with
$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k).$$
It suffices to show that $B(p,\mathbf{g}) \le k!$.
- For a given $\mathbf{g}$ let $\mathbf{m}$ be such a solution. modulo p.

- $B(p, \boldsymbol{g})$ is the number of distinct $m_r \le p^k$ with

$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k).$$

It suffices to show that $B(p, \boldsymbol{g}) \le k!$.

- For a given $\boldsymbol{g}$ let $\mathbf{m}$ be such a solution. modulo p.
- Suppose that $n_1, \ldots, n_k$ is another such solution.

- $B(p, \boldsymbol{g})$ is the number of distinct $m_r \le p^k$ with

$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k).$$

It suffices to show that $B(p, \boldsymbol{g}) \le k!$.

- For a given $\boldsymbol{g}$ let $\mathbf{m}$ be such a solution. modulo p.
- Suppose that $n_1, \ldots, n_k$ is another such solution.
- Then,

$$Q(z; \boldsymbol{m}) \equiv Q(z; \boldsymbol{n}) \pmod{p^k}$$

- $B(p,\boldsymbol{g})$ is the number of distinct $m_r \le p^k$ with
$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k).$$
It suffices to show that $B(p,\boldsymbol{g}) \le k!$.
- For a given $\boldsymbol{g}$ let $\mathbf{m}$ be such a solution. modulo p.
- Suppose that $n_1, \ldots, n_k$ is another such solution.
- Then,
$$Q(z;\boldsymbol{m}) \equiv Q(z;\boldsymbol{n}) \pmod{p^k}$$
- so $Q(n_s;\boldsymbol{m}) \equiv Q(n_s;\boldsymbol{n}) \equiv 0 \pmod{p^k}$ $(1 \le s \le k)$.

- $B(p, \boldsymbol{g})$ is the number of distinct $m_r \le p^k$ with
$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k).$$
It suffices to show that $B(p, \boldsymbol{g}) \le k!$.
- For a given $\boldsymbol{g}$ let $\mathbf{m}$ be such a solution. modulo p.
- Suppose that $n_1, \ldots, n_k$ is another such solution.
- Then,
$$Q(z; \boldsymbol{m}) \equiv Q(z; \boldsymbol{n}) \pmod{p^k}$$
- so $Q(n_s; \boldsymbol{m}) \equiv Q(n_s; \boldsymbol{n}) \equiv 0 \pmod{p^k}$ $(1 \le s \le k)$.
- Since $Q(z; \boldsymbol{m}) = \prod_{r=1}^{k}(z - m_r)$, for each s there is an r such that $n_s \equiv m_r \pmod{p}$.

- $B(p, \boldsymbol{g})$ is the number of distinct $m_r \le p^k$ with
$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k).$$
It suffices to show that $B(p, \boldsymbol{g}) \le k!$.
- For a given $\boldsymbol{g}$ let $\mathbf{m}$ be such a solution. modulo p.
- Suppose that $n_1, \ldots, n_k$ is another such solution.
- Then,
$$Q(z; \boldsymbol{m}) \equiv Q(z; \boldsymbol{n}) \pmod{p^k}$$
- so $Q(n_s; \boldsymbol{m}) \equiv Q(n_s; \boldsymbol{n}) \equiv 0 \pmod{p^k}$ $(1 \le s \le k)$.
- Since $Q(z; \boldsymbol{m}) = \displaystyle\prod_{r=1}^{k}(z - m_r)$, for each s there is an r such that $n_s \equiv m_r \pmod{p}$.
- Also, since the m_r are distinct modulo p it follows that m_r is unique, and so $n_s \equiv m_r \pmod{p^k}$.

- $B(p,\boldsymbol{g})$ is the number of distinct $m_r \le p^k$ with
$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k).$$
It suffices to show that $B(p,\boldsymbol{g}) \le k!$.
- For a given $\boldsymbol{g}$ let $\mathbf{m}$ be such a solution. modulo p.
- Suppose that $n_1, \ldots, n_k$ is another such solution.
- Then,
$$Q(z;\boldsymbol{m}) \equiv Q(z;\boldsymbol{n}) \pmod{p^k}$$
- so $Q(n_s;\boldsymbol{m}) \equiv Q(n_s;\boldsymbol{n}) \equiv 0 \pmod{p^k}$ $(1 \le s \le k)$.
- Since $Q(z;\boldsymbol{m}) = \prod_{r=1}^{k}(z - m_r)$, for each s there is an r such that $n_s \equiv m_r \pmod{p}$.
- Also, since the m_r are distinct modulo p it follows that m_r is unique, and so $n_s \equiv m_r \pmod{p^k}$.
- Thus $n_s = m_r$.

- $B(p,\boldsymbol{g})$ is the number of distinct $m_r \le p^k$ with
$$\sum_{r=1}^{k} m_r^j \equiv g_j \pmod{p^k} \qquad (1 \le j \le k).$$
It suffices to show that $B(p,\boldsymbol{g}) \le k!$.
- For a given $\boldsymbol{g}$ let $\mathbf{m}$ be such a solution. modulo p.
- Suppose that $n_1, \ldots, n_k$ is another such solution.
- Then,
$$Q(z;\boldsymbol{m}) \equiv Q(z;\boldsymbol{n}) \pmod{p^k}$$
- so $Q(n_s;\boldsymbol{m}) \equiv Q(n_s;\boldsymbol{n}) \equiv 0 \pmod{p^k}$ $(1 \le s \le k)$.
- Since $Q(z;\boldsymbol{m}) = \displaystyle\prod_{r=1}^{k}(z-m_r)$, for each s there is an r such that $n_s \equiv m_r \pmod{p}$.
- Also, since the m_r are distinct modulo p it follows that m_r is unique, and so $n_s \equiv m_r \pmod{p^k}$.
- Thus $n_s = m_r$.
- Since the n_s are distinct modulo p, and so are distinct, it follows that the $\boldsymbol{n}$ are a permutation of the $\boldsymbol{m}$.

- We now have all the machinery we need to establish the classical version of the Vinogradov Mean Value Theorem.
  Theorem 5. *For each $k, r \in \mathbb{N}$ with $k \ge 2$ There is a positive number $C(k,r)$ such that foe every real number $X \ge 1$ we have*

$$J_k(X, kr) \le C(k,r) X^{2rk - \frac{1}{2}k(k+1) + \eta(k,r)}$$

where

$$\eta(k,r) = \tfrac{1}{2}k^2\left(1 - \frac{1}{k}\right)^r.$$

- We now have all the machinery we need to establish the classical version of the Vinogradov Mean Value Theorem.
  Theorem 5. *For each $k, r \in \mathbb{N}$ with $k \geq 2$ There is a positive number $C(k, r)$ such that foe every real number $X \geq 1$ we have*
  $$J_k(X, kr) \leq C(k, r) X^{2rk - \frac{1}{2}k(k+1) + \eta(k,r)}$$
  where
  $$\eta(k, r) = \tfrac{1}{2}k^2\left(1 - \frac{1}{k}\right)^r.$$
- The proof is inductive on r. More precisely we establish a reduction formula.

- **Theorem 5.** *For each* $k, r \in \mathbb{N}$ *with* $k \geq 2$ *There is a positive number* $C(k,r)$ *such that foe every real number* $X \geq 1$ *we have* $J_k(X, kr) \leq C(k,r) X^{2rk - \frac{1}{2}k(k+1) + \eta(k,r)}$ *where* $\eta(k,r) = \frac{1}{2}k^2\left(1 - \frac{1}{k}\right)^r$.

- **Theorem 5.** *For each* $k, r \in \mathbb{N}$ *with* $k \geq 2$ *There is a positive number* $C(k, r)$ *such that foe every real number* $X \geq 1$ *we have* $J_k(X, kr) \leq C(k, r)X^{2rk-\frac{1}{2}k(k+1)+\eta(k,r)}$ *where* $\eta(k, r) = \frac{1}{2}k^2\left(1 - \frac{1}{k}\right)^r$.
- **Proof.** In the case $r = 1$ we have by Lemma 3(a) that $J_k(X, k) \leq k!X^k$, and we also have $2k - \frac{1}{2}k(k+1) + \eta(k, 1) = k$ and $k! \leq k^k = \exp(k \log k)$.

- **Theorem 5.** *For each $k, r \in \mathbb{N}$ with $k \geq 2$ There is a positive number $C(k,r)$ such that foe every real number $X \geq 1$ we have $J_k(X, kr) \leq C(k,r) X^{2rk - \frac{1}{2}k(k+1) + \eta(k,r)}$ where $\eta(k,r) = \frac{1}{2}k^2\left(1 - \frac{1}{k}\right)^r$.*
- **Proof.** In the case $r = 1$ we have by Lemma 3(a) that $J_k(X,k) \leq k! X^k$, and we also have $2k - \frac{1}{2}k(k+1) + \eta(k,1) = k$ and $k! \leq k^k = \exp(k \log k)$.
- Suppose $r \geq 2$ and result holds with r replaced by $r - 1$.

- **Theorem 5.** *For each $k, r \in \mathbb{N}$ with $k \ge 2$ There is a positive number $C(k,r)$ such that foe every real number $X \ge 1$ we have $J_k(X, kr) \le C(k,r) X^{2rk - \frac{1}{2}k(k+1) + \eta(k,r)}$ where $\eta(k,r) = \frac{1}{2}k^2\left(1 - \frac{1}{k}\right)^r$.*
- **Proof.** In the case $r = 1$ we have by Lemma 3(a) that $J_k(X, k) \le k! X^k$, and we also have $2k - \frac{1}{2}k(k+1) + \eta(k,1) = k$ and $k! \le k^k = \exp(k \log k)$.
- Suppose $r \ge 2$ and result holds with r replaced by $r - 1$.
- Let $R_1(\boldsymbol{h})$ denote the number of solutions to the system

$$\sum_{r=1}^{kr} m_r^j = h_j \qquad (1 \le j \le k)$$

with $m_r \le X$ and $m_1, \ldots, m_k$ distinct, and let $R_2(\boldsymbol{h})$ denote the number with $m_1, \ldots, m_k$ not distinct.

- **Theorem 5.** *For each* $k, r \in \mathbb{N}$ *with* $k \geq 2$ *There is a positive number* $C(k,r)$ *such that foe every real number* $X \geq 1$ *we have* $J_k(X, kr) \leq C(k,r) X^{2rk - \frac{1}{2}k(k+1) + \eta(k,r)}$ *where* $\eta(k,r) = \frac{1}{2}k^2\left(1 - \frac{1}{k}\right)^r$.
- **Proof.** In the case $r = 1$ we have by Lemma 3(a) that $J_k(X, k) \leq k! X^k$, and we also have $2k - \frac{1}{2}k(k+1) + \eta(k,1) = k$ and $k! \leq k^k = \exp(k \log k)$.
- Suppose $r \geq 2$ and result holds with r replaced by $r-1$.
- Let $R_1(\boldsymbol{h})$ denote the number of solutions to the system

$$\sum_{r=1}^{kr} m_r^j = h_j \qquad (1 \leq j \leq k)$$

with $m_r \leq X$ and $m_1, \ldots, m_k$ distinct, and let $R_2(\boldsymbol{h})$ denote the number with $m_1, \ldots, m_k$ not distinct.
- Then $J_k(X, kr) = \sum_{\boldsymbol{h}} \left(R_1(\boldsymbol{h}) + R_2(\boldsymbol{h})\right)^2 \leq 2(S_1 + S_2)$ where $S_i = \sum_{\boldsymbol{h}} R_i(\boldsymbol{h})^2$.

- We can quickly deal with S_2. One each side of the equations there are two variables the same, and $\binom{k}{2}$ choices for the matching pair.

- We can quickly deal with S_2. One each side of the equations there are two variables the same, and $\binom{k}{2}$ choices for the matching pair.
- Thus $S_2 \le \binom{k}{2}^2 \int_{\mathbb{T}^k} |f(2\alpha)|^2 |f(\alpha)|^{2kr-4} d\alpha$.

- We can quickly deal with S_2. One each side of the equations there are two variables the same, and $\binom{k}{2}$ choices for the matching pair.
- Thus $S_2 \le \binom{k}{2}^2 \int_{\mathbb{T}^k} |f(2\boldsymbol{\alpha})|^2 |f(\boldsymbol{\alpha})|^{2kr-4} d\boldsymbol{\alpha}$.
- By Hölder's inequality this is

$$\le \binom{k}{2}^2 \left(\int_{\mathbb{T}^k} |f(2\boldsymbol{\alpha})|^{2kr} d\boldsymbol{\alpha} \right)^{\frac{1}{kr}} \left(\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha})|^{2kr} d\boldsymbol{\alpha} \right)^{\frac{kr-2}{kr}}$$

$$= \binom{k}{2}^2 J_k(X, kr)^{1-1/kr}.$$

- We can quickly deal with S_2. One each side of the equations there are two variables the same, and $\binom{k}{2}$ choices for the matching pair.
- Thus $S_2 \le \binom{k}{2}^2 \int_{\mathbb{T}^k} |f(2\alpha)|^2 |f(\alpha)|^{2kr-4} d\alpha.$
- By Hölder's inequality this is

$$\le \binom{k}{2}^2 \left(\int_{\mathbb{T}^k} |f(2\alpha)|^{2kr} d\alpha\right)^{\frac{1}{kr}} \left(\int_{\mathbb{T}^k} |f(\alpha)|^{2kr} d\alpha\right)^{\frac{kr-2}{kr}}$$

$$= \binom{k}{2}^2 J_k(X, kr)^{1-1/kr}.$$

- Thus

$$J_k(X, kr) \le 2S_1 + 2\binom{k}{2}^2 J_k(X, kr)^{1-1/kr}.$$

- We can quickly deal with S_2. One each side of the equations there are two variables the same, and $\binom{k}{2}$ choices for the matching pair.
- Thus $S_2 \le \binom{k}{2}^2 \int_{\mathbb{T}^k} |f(2\alpha)|^2 |f(\alpha)|^{2kr-4} d\alpha$.
- By Hölder's inequality this is

$$\le \binom{k}{2}^2 \left(\int_{\mathbb{T}^k} |f(2\alpha)|^{2kr} d\alpha\right)^{\frac{1}{kr}} \left(\int_{\mathbb{T}^k} |f(\alpha)|^{2kr} d\alpha\right)^{\frac{kr-2}{kr}}$$

$$= \binom{k}{2}^2 J_k(X, kr)^{1-1/kr}.$$

- Thus

$$J_k(X, kr) \le 2S_1 + 2\binom{k}{2}^2 J_k(X, kr)^{1-1/kr}.$$

- And so

$$J_s(X, kr) \le \left(4\binom{k}{2}^2\right)^{kr} + 4S_1.$$

- It remains to treat S_1. We are concerned with solutions in which $m_1, \dots, m_k$ are distinct and $n_1, \dots, n_k$ are distinct.

- It remains to treat S_1. We are concerned with solutions in which $m_1, \ldots, m_k$ are distinct and $n_1, \ldots, n_k$ are distinct.
- Let $P(\mathbf{m}) = \prod_{q=1}^{k-1} \prod_{r=q+1}^{k} (m_q - m_r)$ where $m_j \le X$.

- It remains to treat S_1. We are concerned with solutions in which $m_1, \dots, m_k$ are distinct and $n_1, \dots, n_k$ are distinct.
- Let $P(\mathbf{m}) = \prod_{q=1}^{k-1} \prod_{r=q+1}^{k} (m_q - m_r)$ where $m_j \le X$.
- The number of possible primes p with $p > X^{1/k}$ and $p|P(\mathbf{m})P(\mathbf{n})$ is at most $\frac{k \log |P(\mathbf{m})P(\mathbf{n})|}{\log X} < k^2(k-1)$.

- It remains to treat S_1. We are concerned with solutions in which $m_1, \ldots, m_k$ are distinct and $n_1, \ldots, n_k$ are distinct.
- Let $P(\mathbf{m}) = \prod_{q=1}^{k-1} \prod_{r=q+1}^{k} (m_q - m_r)$ where $m_j \le X$.
- The number of possible primes p with $p > X^{1/k}$ and $p | P(\mathbf{m})P(\mathbf{n})$ is at most $\frac{k \log |P(\mathbf{m})P(\mathbf{n})|}{\log X} < k^2(k-1)$.
- Thus if $\mathcal{P}$ is a set of $\ge k^2(k-1)$ primes p with $p > X^{1/k}$, then for each set of distinct $m_1, \ldots, m_k$ and $n_1, \ldots, n_k$ there will always be a prime $p \in \mathcal{P}$ such that $p \nmid P(\mathbf{m})P(\mathbf{n})$.

- It remains to treat S_1. We are concerned with solutions in which $m_1, \ldots, m_k$ are distinct and $n_1, \ldots, n_k$ are distinct.
- Let $P(\mathbf{m}) = \prod_{q=1}^{k-1} \prod_{r=q+1}^{k} (m_q - m_r)$ where $m_j \le X$.
- The number of possible primes p with $p > X^{1/k}$ and $p|P(\mathbf{m})P(\mathbf{n})$ is at most $\frac{k \log |P(\mathbf{m})P(\mathbf{n})|}{\log X} < k^2(k-1)$.
- Thus if $\mathcal{P}$ is a set of $\ge k^2(k-1)$ primes p with $p > X^{1/k}$, then for each set of distinct $m_1, \ldots, m_k$ and $n_1, \ldots, n_k$ there will always be a prime $p \in \mathcal{P}$ such that $p \nmid P(\mathbf{m})P(\mathbf{n})$.
- We can also assume that $X > C_1 e^k$, for otherwise trivially $J_k(X; lk) \le X^{2lk} \le C(k, l)$, and $p > k$.

- It remains to treat S_1. We are concerned with solutions in which $m_1, \dots, m_k$ are distinct and $n_1, \dots, n_k$ are distinct.
- Let $P(\mathbf{m}) = \prod_{q=1}^{k-1} \prod_{r=q+1}^{k} (m_q - m_r)$ where $m_j \le X$.
- The number of possible primes p with $p > X^{1/k}$ and $p | P(\mathbf{m})P(\mathbf{n})$ is at most $\frac{k \log |P(\mathbf{m})P(\mathbf{n})|}{\log X} < k^2(k-1)$.
- Thus if $\mathcal{P}$ is a set of $\ge k^2(k-1)$ primes p with $p > X^{1/k}$, then for each set of distinct $m_1, \dots, m_k$ and $n_1, \dots, n_k$ there will always be a prime $p \in \mathcal{P}$ such that $p \nmid P(\mathbf{m})P(\mathbf{n})$.
- We can also assume that $X > C_1 e^k$, for otherwise trivially $J_k(X; lk) \le X^{2lk} \le C(k, l)$, and $p > k$.
- Furthermore we can suppose by a standard form of the prime number theorem that the set $\mathcal{P}$ of primes p can be chosen so that $p \le C_2 k^2 X^{1/k}$ for some absolute constant C_2 (and probably better than that).

- Recall that $S_1 = \sum_{\mathbf{h}} R_1(\mathbf{h})^2$ where $R_1(\boldsymbol{h})$ is the number of solutions to the system $\sum_{r=1}^{kr} m_r^j = h_j \qquad (1 \le j \le k)$ with $m_r \le X$ and $m_1, \ldots, m_k$ distinct.

- Recall that $S_1 = \sum_{\mathbf{h}} R_1(\mathbf{h})^2$ where $R_1(\boldsymbol{h})$ is the number of solutions to the system $\sum_{r=1}^{kr} m_r^j = h_j \qquad (1 \le j \le k)$ with $m_r \le X$ and $m_1, \ldots, m_k$ distinct.
- We have $R_1(\boldsymbol{h}) \le \sum_{p \in \mathcal{P}} R_3(\boldsymbol{h}, p)$ where $R_3(\boldsymbol{h}, p)$ is the no. of solutions with $m_r \le X$ & $m_1, \ldots, m_k$ distinct $\pmod{p}$.

- Recall that $S_1 = \sum_{\mathbf{h}} R_1(\mathbf{h})^2$ where $R_1(\boldsymbol{h})$ is the number of solutions to the system $\sum_{r=1}^{kr} m_r^j = h_j \qquad (1 \le j \le k)$ with $m_r \le X$ and $m_1, \dots, m_k$ distinct.
- We have $R_1(\boldsymbol{h}) \le \sum_{p \in \mathcal{P}} R_3(\boldsymbol{h}, p)$ where $R_3(\boldsymbol{h}, p)$ is the no. of solutions with $m_r \le X$ & $m_1, \dots, m_k$ distinct $\pmod p$.
- Let $I(p) = \sum_{\boldsymbol{h}} R_3(\boldsymbol{h}, p)^2$.

- Recall that $S_1 = \sum_{\mathbf{h}} R_1(\mathbf{h})^2$ where $R_1(\boldsymbol{h})$ is the number of solutions to the system $\sum_{r=1}^{kr} m_r^j = h_j \qquad (1 \le j \le k)$ with $m_r \le X$ and $m_1, \ldots, m_k$ distinct.
- We have $R_1(\boldsymbol{h}) \le \sum_{p \in \mathcal{P}} R_3(\boldsymbol{h}, p)$ where $R_3(\boldsymbol{h}, p)$ is the no. of solutions with $m_r \le X$ & $m_1, \ldots, m_k$ distinct $\pmod p$.
- Let $I(p) = \sum_{\boldsymbol{h}} R_3(\boldsymbol{h}, p)^2$.
- Then $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \ldots, m_b, n_1, \ldots, n_b$ in $(0, x]$, $m_1, \ldots, m_k$ distinct modulo p and likewise $n_1, \ldots, n_k$.

- Recall that $S_1 = \sum_{\mathbf{h}} R_1(\mathbf{h})^2$ where $R_1(\boldsymbol{h})$ is the number of solutions to the system $\sum_{r=1}^{kr} m_r^j = h_j \qquad (1 \le j \le k)$ with $m_r \le X$ and $m_1, \dots, m_k$ distinct.
- We have $R_1(\boldsymbol{h}) \le \sum_{p\in\mathcal{P}} R_3(\boldsymbol{h}, p)$ where $R_3(\boldsymbol{h}, p)$ is the no. of solutions with $m_r \le X$ & $m_1, \dots, m_k$ distinct $\pmod{p}$.
- Let $I(p) = \sum_{\boldsymbol{h}} R_3(\boldsymbol{h}, p)^2$.
- Then $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \dots, m_b, n_1, \dots, n_b$ in $(0, x]$, $m_1, \dots, m_k$ distinct modulo p and likewise $n_1, \dots, n_k$.
- Thus $J_k(X, rk) \le 4 \sum_{\boldsymbol{h}} R_1(\boldsymbol{h}))^2 \le 4 \sum_{\boldsymbol{h}} \Big(\sum_{p\in\mathcal{P}} R_3(\boldsymbol{h}, p) \Big)^2$

$$\le 4 \sum_{\boldsymbol{h}} \frac{1}{2} k^3 \sum_{p\in\mathcal{P}} R_3(\boldsymbol{h}, p)^2 \le 2k^3 \sum_{p\in\mathcal{P}} I(p) \le k^6 \max_{\substack{p \\ p\in\mathcal{P}}} I(p).$$

- $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \dots, m_k, n_1, \dots, n_k$ in $(0, x]$, $m_1, \dots, m_k$ distinct mod p & likewise $n_1, \dots, n_k$ and $J_k(X, rk) \le k^6 \max_{p \in \mathcal{P}} I(p)$

- $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \ldots, m_k, n_1, \ldots, n_k$ in $(0, x]$, $m_1, \ldots, m_k$ distinct mod p & likewise $n_1, \ldots, n_k$ and $J_k(X, rk) \le k^6 \max_{p \in \mathcal{P}} I(p)$
- Let $g(\boldsymbol{\alpha}, a) = \sum_{\substack{n \le X \\ n \equiv a \,(mod p)}} e\big(\boldsymbol{\alpha}.\boldsymbol{\nu}(m)\big)$, and

- $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \ldots, m_k, n_1, \ldots, n_k$ in $(0, x]$, $m_1, \ldots, m_k$ distinct mod p & likewise $n_1, \ldots, n_k$ and $J_k(X, rk) \le k^6 \max_{p \in \mathcal{P}} I(p)$
- Let $g(\alpha, a) = \sum_{\substack{n \le X \\ n \equiv a \,(\mathrm{mod} p)}} e(\boldsymbol{\alpha}.\boldsymbol{\nu}(m))$, and
- $\mathcal{A}$ be the $\boldsymbol{a}$ with $0 \le a_r < p$ and a_r distinct. Then $I(p) =$

$$\int_{\mathbb{T}^k} \Big| \sum_{\boldsymbol{a} \in \mathcal{A}} g(\boldsymbol{\alpha}, a_1) \cdots g(\boldsymbol{\alpha}, a_k) \Big|^2 \Big| \sum_{a=0}^{p-1} g(\boldsymbol{\alpha}, a) \Big|^{2b-2k} \boldsymbol{d\alpha}$$

- $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \ldots, m_k, n_1, \ldots, n_k$ in $(0, x]$, $m_1, \ldots, m_k$ distinct mod p & likewise $n_1, \ldots, n_k$ and $J_k(X, rk) \le k^6 \max_{p \in \mathcal{P}} I(p)$
- Let $g(\alpha, a) = \sum_{\substack{n \le X \\ n \equiv a \,(mod p)}} e(\boldsymbol{\alpha}.\boldsymbol{\nu}(m))$, and
- $\mathcal{A}$ be the $\boldsymbol{a}$ with $0 \le a_r < p$ and a_r distinct. Then $I(p) =$

$$\int_{\mathbb{T}^k} \Big| \sum_{\boldsymbol{a} \in \mathcal{A}} g(\boldsymbol{\alpha}, a_1) \cdots g(\boldsymbol{\alpha}, a_k) \Big|^2 \Big| \sum_{a=0}^{p-1} g(\boldsymbol{\alpha}, a) \Big|^{2b-2k} \boldsymbol{d\alpha}$$

- By Hölder's inequality

$$\Big| \sum_{a=0}^{p-1} g(\boldsymbol{\alpha}, a) \Big|^{2rk-2k} \le p^{2rk-2k-1} \sum_{a=0}^{p-1} |g(\boldsymbol{\alpha}, a)|^{2rk-2k},$$

- $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \ldots, m_k, n_1, \ldots, n_k$ in $(0, x]$, $m_1, \ldots, m_k$ distinct mod p & likewise $n_1, \ldots, n_k$ and $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} I(p)$
- Let $g(\alpha, a) = \sum_{\substack{n\le X \\ n\equiv a\,(\mathrm{mod} p)}} e(\boldsymbol{\alpha}.\boldsymbol{\nu}(m))$, and
- $\mathcal{A}$ be the $\boldsymbol{a}$ with $0 \le a_r < p$ and a_r distinct. Then $I(p) =$

$$\int_{\mathbb{T}^k} \Big|\sum_{\boldsymbol{a}\in\mathcal{A}} g(\boldsymbol{\alpha}, a_1)\cdots g(\boldsymbol{\alpha}, a_k)\Big|^2 \Big|\sum_{a=0}^{p-1} g(\boldsymbol{\alpha}, a)\Big|^{2b-2k} \boldsymbol{d\alpha}$$

- By Hölder's inequality

$$\Big|\sum_{a=0}^{p-1} g(\boldsymbol{\alpha}, a)\Big|^{2rk-2k} \le p^{2rk-2k-1}\sum_{a=0}^{p-1} |g(\boldsymbol{\alpha}, a)|^{2rk-2k},$$

- and so $I(p) \le p^{2b-2k} \max_{0\le a<p} I_1(p, a)$ where $I_1(p, a) =$

$$\int_{\mathbb{T}^k} \Big|\sum_{\boldsymbol{a}\in\mathcal{A}} g(\boldsymbol{\alpha}, a_1)\cdots g(\boldsymbol{\alpha}, a_k)\Big|^2 |g(\boldsymbol{\alpha}, a)|^{2rk-2k} \boldsymbol{d\alpha}.$$

- $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \ldots, m_b, n_1, \ldots, n_{rk}$ in $(0, x]$, $m_1, \ldots, m_k$ distinct mod p & likewise $n_1, \ldots, n_k$ and $J_k(X, rk) \le k^6 \max_{p \in \mathcal{P}} I(p)$, $I(p) \le p^{2rk-2k} \max_{0 \le a < p} I_1(p, a)$ where $I_1(p, a) =$
$$\int_{\mathbb{T}^k} \Big| \sum_{\boldsymbol{a} \in \mathcal{A}} g(\boldsymbol{\alpha}, a_1) \cdots g(\boldsymbol{\alpha}, a_k) \Big|^2 |g(\boldsymbol{\alpha}, a)|^{2rk-2k} \, \boldsymbol{d\alpha},$$
and $g(\boldsymbol{\alpha}, a) = \sum_{n \le X, n \equiv a \,(mod p)} e(\boldsymbol{\alpha}.\boldsymbol{\nu}(m))$.

- $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \ldots, m_b, n_1, \ldots, n_{rk}$ in $(0, x]$, $m_1, \ldots, m_k$ distinct mod p & likewise $n_1, \ldots, n_k$ and $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} I(p)$, $I(p) \le p^{2rk-2k} \max_{0\le a<p} I_1(p, a)$ where $I_1(p, a) =$

$$\int_{\mathbb{T}^k} \Big| \sum_{\boldsymbol{a}\in\mathcal{A}} g(\boldsymbol{\alpha}, a_1) \cdots g(\boldsymbol{\alpha}, a_k) \Big|^2 |g(\boldsymbol{\alpha}, a)|^{2rk-2k} \, \boldsymbol{d\alpha},$$

and $g(\boldsymbol{\alpha}, a) = \displaystyle\sum_{n\le X, n\equiv a \,(mod p)} e(\boldsymbol{\alpha}.\boldsymbol{\nu}(m))$.

- This is the number of solutions of

$$\sum_{i=1}^{k} (m_i^j - n_i^j) = \sum_{r=1}^{rk-k} \big((pu_r + a)^j - (pv_r + a)^j\big) \quad (1 \le j \le k)$$

with $m_i, n_i \le X$, $-a/p < u_r, v_r \le (X - a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.

- $I(p)$ is the no. of solns. of $s_j(\boldsymbol{m}) = s_j(\boldsymbol{n})$ $(1 \le j \le k)$ with $m_1, \ldots, m_b, n_1, \ldots, n_{rk}$ in $(0, x]$, $m_1, \ldots, m_k$ distinct mod p & likewise $n_1, \ldots, n_k$ and $J_k(X, rk) \le k^6 \max_{p \in \mathcal{P}} I(p)$, $I(p) \le p^{2rk-2k} \max_{0 \le a < p} I_1(p, a)$ where $I_1(p, a) =$
$$\int_{\mathbb{T}^k} \Big| \sum_{\boldsymbol{a} \in \mathcal{A}} g(\boldsymbol{\alpha}, a_1) \cdots g(\boldsymbol{\alpha}, a_k) \Big|^2 |g(\boldsymbol{\alpha}, a)|^{2rk-2k} \, \boldsymbol{d\alpha},$$
and $g(\boldsymbol{\alpha}, a) = \displaystyle\sum_{n \le X, n \equiv a \,(mod p)} e(\boldsymbol{\alpha}.\boldsymbol{\nu}(m))$.
- This is the number of solutions of
$$\sum_{i=1}^{k} (m_i^j - n_i^j) = \sum_{r=1}^{rk-k} \left((pu_r + a)^j - (pv_r + a)^j \right) \quad (1 \le j \le k)$$
with $m_i, n_i \le X$, $-a/p < u_r, v_r \le (X-a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.
- This system is TDI so under the same conditions
$$\sum_{i=1}^{k} \left((m_i - a)^j - (n_i - a)^j \right) = \sum_{r=1}^{rk-k} p^j (u_r^j - v_r^j) \qquad (1 \le j \le k)$$

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k}\left((m_i-a)^j-(n_i-a)^j\right) = \sum_{h=1}^{rk-k} p^j\left(u_h^j-v_h^j\right) \qquad (1 \le j \le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1,\ldots,m_k$ distinct mod p and $n_1,\ldots,n_k$ likewise.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k}\left((m_i-a)^j-(n_i-a)^j\right) = \sum_{h=1}^{rk-k} p^j\left(u_h^j-v_h^j\right) \qquad (1\le j\le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1,\ldots,m_k$ distinct mod p and $n_1,\ldots,n_k$ likewise.

- We can sort the solutions as follows.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k}\left((m_i-a)^j-(n_i-a)^j\right) = \sum_{h=1}^{rk-k} p^j\left(u_h^j-v_h^j\right) \qquad (1 \le j \le k)$$

  with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.
- We can sort the solutions as follows.
- Pick $n_1, \ldots, n_k$.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k} \left((m_i - a)^j - (n_i - a)^j\right) = \sum_{h=1}^{rk-k} p^j \left(u_h^j - v_h^j\right) \qquad (1 \le j \le k)$$

  with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.
- We can sort the solutions as follows.
- Pick $n_1, \ldots, n_k$.
- Then choose $m_1, \ldots, m_k$ modulo p^k so that $(m_i - a)^j \equiv (n_i - a)^j \pmod{p^j}$ $(1 \le j \le k)$.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p, a)$ where $I_1(p, a)$ is no. solns.

$$\sum_{i=1}^{k} \left((m_i - a)^j - (n_i - a)^j\right) = \sum_{h=1}^{rk-k} p^j \left(u_h^j - v_h^j\right) \qquad (1 \le j \le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \dots, m_k$ distinct mod p and $n_1, \dots, n_k$ likewise.

- We can sort the solutions as follows.
- Pick $n_1, \dots, n_k$.
- Then choose $m_1, \dots, m_k$ modulo p^k so that $(m_i - a)^j \equiv (n_i - a)^j \pmod{p^j}$ $(1 \le j \le k)$.
- Use Linnik's lemma: There are $\le k! p^{k(k-1)/2}$ choices modulo p^k.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k} \left((m_i-a)^j-(n_i-a)^j\right) = \sum_{h=1}^{rk-k} p^j\left(u_h^j-v_h^j\right) \qquad (1 \le j \le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.

- We can sort the solutions as follows.
- Pick $n_1, \ldots, n_k$.
- Then choose $m_1, \ldots, m_k$ modulo p^k so that $(m_i - a)^j \equiv (n_i - a)^j \pmod{p^j}$ $(1 \le j \le k)$.
- Use Linnik's lemma: There are $\le k! p^{k(k-1)/2}$ choices modulo p^k.
- Since $p > X^{1/k}$ the m_i are uniquely determined modulo p^k, i.e. there are at most $k! p^{k(k-1)/2}$ choices in all.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k} \left((m_i - a)^j - (n_i - a)^j\right) = \sum_{h=1}^{rk-k} p^j \left(u_h^j - v_h^j\right) \qquad (1 \le j \le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.

- We can sort the solutions as follows.
- Pick $n_1, \ldots, n_k$.
- Then choose $m_1, \ldots, m_k$ modulo p^k so that $(m_i - a)^j \equiv (n_i - a)^j \pmod{p^j}$ $(1 \le j \le k)$.
- Use Linnik's lemma: There are $\le k! p^{k(k-1)/2}$ choices modulo p^k.
- Since $p > X^{1/k}$ the m_i are uniquely determined modulo p^k, i.e. there are at most $k! p^{k(k-1)/2}$ choices in all.
- Now given the m_i and n_i the number of choices for u_h, v_h is at most $J_k\big((-a/p, (X-a)/p], rk - k\big)$.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k} \left((m_i - a)^j - (n_i - a)^j\right) = \sum_{h=1}^{rk-k} p^j \left(u_h^j - v_h^j\right) \qquad (1 \le j \le k)$$

  with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.
- We can sort the solutions as follows.
- Pick $n_1, \ldots, n_k$.
- Then choose $m_1, \ldots, m_k$ modulo p^k so that $(m_i - a)^j \equiv (n_i - a)^j \pmod{p^j}$ $(1 \le j \le k)$.
- Use Linnik's lemma: There are $\le k! p^{k(k-1)/2}$ choices modulo p^k.
- Since $p > X^{1/k}$ the m_i are uniquely determined modulo p^k, i.e. there are at most $k! p^{k(k-1)/2}$ choices in all.
- Now given the m_i and n_i the number of choices for u_h, v_h is at most $J_k\big(((-a/p, (X-a)/p], rk-k\big)$.
- Apply the inductive hypothesis.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k}\left((m_i-a)^j-(n_i-a)^j\right) = \sum_{h=1}^{rk-k} p^j\left(u_h^j-v_h^j\right) \qquad (1 \le j \le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \dots, m_k$ distinct mod p and $n_1, \dots, n_k$ likewise.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k} \big((m_i - a)^j - (n_i - a)^j\big) = \sum_{h=1}^{rk-k} p^j \big(u_h^j - v_h^j\big) \qquad (1 \le j \le k)$$

  with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.
- The total number of solutions is at most the maximum over $p \in \mathcal{P}$ of

$$k^6 k! X^k p^{\frac{k(k-1)}{2}+2rk-2k} C(k, r-1)(1+\tfrac{X}{p})^{2rk-2k-\frac{k(k+1)}{2}+\eta_{r-1}}$$

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k} \big((m_i-a)^j-(n_i-a)^j\big) = \sum_{h=1}^{rk-k} p^j\big(u_h^j-v_h^j\big) \qquad (1 \le j \le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.

- The total number of solutions is at most the maximum over $p \in \mathcal{P}$ of

$$k^6 k! X^k p^{\frac{k(k-1)}{2}+2rk-2k} C(k, r-1)(1+\tfrac{X}{p})^{2rk-2k-\frac{k(k+1)}{2}+\eta_{r-1}}$$

- $\le k^6 k! C(k, r-1) p^{k^2-\eta_{r-1}} 2^{2rk} X^{2rk-k-\frac{k(k+1)}{2}+\eta_{r-1}}$.

- $J_k(X,rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k}\left((m_i-a)^j-(n_i-a)^j\right)=\sum_{h=1}^{rk-k}p^j\left(u_h^j-v_h^j\right)\qquad(1\le j\le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1,\dots,m_k$ distinct mod p and $n_1,\dots,n_k$ likewise.

- The total number of solutions is at most the maximum over $p\in\mathcal{P}$ of

$$k^6 k! X^k p^{\frac{k(k-1)}{2}+2rk-2k} C(k,r-1)(1+\tfrac{X}{p})^{2rk-2k-\frac{k(k+1)}{2}+\eta_{r-1}}$$

- $\le k^6 k! C(k,r-1) p^{k^2-\eta_{r-1}} 2^{2rk} X^{2rk-k-\frac{k(k+1)}{2}+\eta_{r-1}}$.
- Recall $\mathcal{P}$ is a set of $k^2(k-1)$ primes p with $X^{1/k} < p \le C_2 k^2 X^{1/k}$.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p,a)$ where $I_1(p,a)$ is no. solns.

$$\sum_{i=1}^{k}\big((m_i-a)^j-(n_i-a)^j\big) = \sum_{h=1}^{rk-k} p^j\big(u_h^j-v_h^j\big) \qquad (1\le j\le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X-a)/p$, $m_1, \dots, m_k$ distinct mod p and $n_1, \dots, n_k$ likewise.

- The total number of solutions is at most the maximum over $p \in \mathcal{P}$ of

$$k^6 k! X^k p^{\frac{k(k-1)}{2}+2rk-2k} C(k, r-1)(1+\tfrac{X}{p})^{2rk-2k-\frac{k(k+1)}{2}+\eta_{r-1}}$$

- $\le k^6 k! C(k, r-1) p^{k^2-\eta_{r-1}} 2^{2rk} X^{2rk-k-\frac{k(k+1)}{2}+\eta_{r-1}}$.
- Recall $\mathcal{P}$ is a set of $k^2(k-1)$ primes p with $X^{1/k} < p \le C_2 k^2 X^{1/k}$.
- Thus the above is $\le C(k,r) X^{k-\eta_{r-1}/k+2rk-k-\frac{k(k+1)}{2}+\eta_{r-1}}$.

- $J_k(X, rk) \le k^6 \max_{p\in\mathcal{P}} p^{2rk-2k} \max_a I_1(p, a)$ where $I_1(p, a)$ is no. solns.

$$\sum_{i=1}^{k} \big((m_i - a)^j - (n_i - a)^j\big) = \sum_{h=1}^{rk-k} p^j \big(u_h^j - v_h^j\big) \qquad (1 \le j \le k)$$

with $m_i, n_i \le X$, $-a/p < u_h, v_h \le (X - a)/p$, $m_1, \ldots, m_k$ distinct mod p and $n_1, \ldots, n_k$ likewise.

- The total number of solutions is at most the maximum over $p \in \mathcal{P}$ of

$$k^6 k! X^k p^{\frac{k(k-1)}{2}+2rk-2k} C(k, r-1)(1 + \tfrac{X}{p})^{2rk-2k-\frac{k(k+1)}{2}+\eta_{r-1}}$$

- $\le k^6 k! C(k, r-1) p^{k^2-\eta_{r-1}} 2^{2rk} X^{2rk-k-\frac{k(k+1)}{2}+\eta_{r-1}}$.
- Recall $\mathcal{P}$ is a set of $k^2(k-1)$ primes p with $X^{1/k} < p \le C_2 k^2 X^{1/k}$.
- Thus the above is $\le C(k, r) X^{k-\eta_{r-1}/k+2rk-k-\frac{k(k+1)}{2}+\eta_{r-1}}$.
- The exponent here is $2rk - \frac{k(k+1)}{2} + \eta_r$