Analytic Number Theory
Lecture 10

Mariusz Mirek
Rutgers University

Padova, April 9, 2025.

Supported by the NSF grant DMS-2154712,
and the CAREER grant DMS-2236493.

Vinogradov's system of diophantine equations

- Let $k, n \geqslant 1$ be integers, and $P \in \mathbb{Z}_+$ be a large integer. Let $J_{k,n}(P)$ be the number of integer solutions of the system of diophantine equations

$$\begin{aligned} x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{2k} &= 0 \\ x_1^2 + \cdots + x_k^2 - x_{k+1}^2 - \cdots - x_{2k}^2 &= 0 \\ \vdots \qquad\qquad\qquad & \ \ \vdots \\ x_1^n + \cdots + x_k^n - x_{k+1}^n - \cdots - x_{2k}^n &= 0, \end{aligned} \tag{HE}$$

  where $1 \leqslant x_1, \ldots, x_{2k} \leqslant P$.

- More generally, for given integers $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$, let us define $J_{k,n}(P; \lambda_1, \ldots, \lambda_n)$ as the number of solutions of the system

$$\begin{aligned} x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{2k} &= \lambda_1 \\ x_1^2 + \cdots + x_k^2 - x_{k+1}^2 - \cdots - x_{2k}^2 &= \lambda_2 \\ \vdots \qquad\qquad\qquad & \ \ \vdots \\ x_1^n + \cdots + x_k^n - x_{k+1}^n - \cdots - x_{2k}^n &= \lambda_n, \end{aligned} \tag{IE}$$

  where $1 \leqslant x_1, \ldots, x_{2k} \leqslant P$. Then $J_{k,n}(P) = J_{k,n}(P; 0, \ldots, 0)$.

Integral representation of $J_{k,n}(P; \lambda_1, \ldots, \lambda_n)$

- The basis of this method is the elementary orthogonality identity

$$\int_0^1 e(kx)dx = \int_0^1 e^{2\pi ikx}dx = \begin{cases} 1 & \text{if } k = 0, \\ 0 & \text{if } k \neq 0. \end{cases}$$

- Using this identity we note that

$$J_{k,n}(P; \lambda_1, \ldots, \lambda_n) = \sum_{1 \leqslant x_1, \ldots, x_{2k} \leqslant P} \prod_{m=1}^{n} \delta_{\lambda_m}\left(\sum_{j=1}^{k} x_j^m - \sum_{j=k+1}^{2k} x_j^m\right)$$

$$= \sum_{1 \leqslant x_1, \ldots, x_{2k} \leqslant P} \prod_{m=1}^{n} \int_0^1 e\left(\left(\sum_{j=1}^{k} x_j^m - \sum_{j=k+1}^{2k} x_j^m - \lambda_m\right)\alpha_m\right) d\alpha_m$$

$$\int_0^1 \cdots \int_0^1 \left| \sum_{x \in [P]} e(\alpha_1 x + \cdots + \alpha_n x^n) \right|^{2k} e(-\alpha_1\lambda_1 - \cdots - \alpha_n\lambda_n)\, d\alpha_1 \cdots d\alpha_n.$$

- We then immediately see that

$$J_{k,n}(P; \lambda_1, \ldots, \lambda_n) \leq J_{k,n}(P),$$

by taking $\lambda_1 = \ldots = \lambda_n = 0$.

Simple properties of $J_{k,n}(P; \lambda_1, \ldots, \lambda_n)$

- When $x_1, \ldots, x_{2k}$ run over all possible P^{2k} values, then the left-hand side of the system (IE) assumes all possible values $\lambda_1, \ldots, \lambda_n$, which satisfy
$$|\lambda_1| < kP, |\lambda_2| < kP^2, \ldots, |\lambda_n| < kP^n.$$
- By the Fourier inverse transform we have
$$\Big| \sum_{x \leqslant P} e\left(\alpha_1 x + \cdots + \alpha_n x^n\right) \Big|^{2k} = \sum_{|\lambda_1| < kP, \ldots, |\lambda_n| < kP^n} J_{k,n}\left(\lambda_1, \ldots, \lambda_n\right) e\left(-\alpha_1 \lambda_1 - \cdots - \alpha_n \lambda_n\right).$$
- Now taking $\alpha_1 = \ldots = \alpha_n = 0$ in the above equation we obtain
$$\sum_{|\lambda_1| < kP, \ldots, |\lambda_n| < kP^n} J_{k,n}\left(\lambda_1, \ldots, \lambda_n\right) = P^{2k}.$$
- Further, we have trivially $J_{k,n}(P) \leqslant P^{2k}$, and moreover $J_{k,n}(P)$ is clearly nondecreasing as a function of k or P.

Simple properties of $J_{k,n}(P;\lambda_1,\ldots,\lambda_n)$

- Our interest will be primarily in the upper bounds for $J_{k,n}(P)$, but we may note here that a lower bound may be obtained as follows.

$$\begin{aligned} P^{2k} &= \sum_{|\lambda_1|<kP,\ldots,|\lambda_n|<kP^n} J_{k,n}(\lambda_1,\ldots,\lambda_n) \\ &\leqslant J_{k,n}(P) \sum_{|\lambda_1|<kP,\ldots,|\lambda_n|<kP^n} 1 \leqslant J_{k,n}(P)(2k)P\cdots(2k)P^n \\ &= J_{k,n}(P)(2k)^n P^{n(n+1)/2}, \end{aligned}$$

  which gives

$$J_{k,n}(P) \geqslant (2k)^{-n} P^{2k-n(n+1)/2},$$

  and this is a nontrivial bound if $k > \frac{1}{4}\left(n^2+n\right)$.
- If we consider the diagonal solutions $x_j = x_{j+k}$ for all $j \in [k]$, and $1 \leq x_1,\ldots,x_k \leq P$, then $J_{k,n}(P) \geq P^n$.
- If we consider only the first $n-1$ equations in (IE), then the number of their solutions is $J_{k,n-1}(\lambda_1,\ldots,\lambda_{n-1})$, and if we let $|\lambda_n|$ take all possible values ($< kP^n$) in the last equation in (IE), then we obtain

$$\sum_{|\lambda_n|<kP^n} J_{k,n}(\lambda_1,\ldots,\lambda_n) = J_{k,n-1}(\lambda_1,\ldots,\lambda_{n-1}).$$

Linnik's lemma

Lemma (Linnik)

Let $m, n \in \mathbb{Z}_+$, and also let $A \in \mathbb{Z}$, let $p > n$ be a prime number, and let $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$. Let T denote the number of solutions $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ of the simultaneous congruences

$$
\begin{aligned}
x_1 + \cdots + x_n &\equiv \lambda_1 \pmod{p}, \\
x_1^2 + \cdots + x_n^2 &\equiv \lambda_2 \pmod{p^2}, \\
&\vdots \\
x_1^n + \cdots + x_n^n &\equiv \lambda_n \pmod{p^n},
\end{aligned}
\tag{LE}
$$

where x_j are distinct modulo p and $A \leq x_j < A + mp^n$ for all $j \in [n]$. Then for all integers $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$, we have

$$T \leq n! m^n p^{n(n-1)/2}.$$

Proof.

- We can assume that $A = 0$. If $x_1, \ldots, x_n$ satisfy (LE) with $A = 0$, then we take $l \in \mathbb{Z}$ such that $lp^n - 1 < A \leq lp^n$ and consider $y_j = x_j + lp^n$, then $A \leq y_j \leq A + mp^n$ for $j \in [n]$, and we readily see that $y_1, \ldots, y_n$ satisfy (LE), since $x_j \equiv y_j \pmod{p^n}$ for $j \in [n]$.

Proof

- We can also assume that $m = 1$. If $(x_1, \ldots, x_n)$ is a solution of (LE) such that $0 \le x_j < p^n$ for $j \in [n]$, then $(x_1 + l_1 p^n, \ldots, x_n + l_n p^n)$ with $l_1, \ldots, l_n \in [m]$ is also a solution of (LE), and there are m^n such solutions.
- For each $\lambda \in \mathbb{Z}$ and $j \in [n]$ there is p^{n-j} choices of the residue class $\mu \pmod{p^n}$ such that $\lambda \equiv \mu \pmod{p^j}$.
- Thus for any given tuple of integers $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$, there are $\prod_{j=1}^{n-1} p^{n-j} = p^{n(n-1)/2}$ different vectors $(\mu_1, \ldots, \mu_n) \in \mathbb{Z}/p^n\mathbb{Z}$ so that

$$\mu_j \equiv \lambda_j \pmod{p^j} \quad \text{for all} \quad j \in [n].$$

- It will suffices to prove that for any fixed vector $(\mu_1, \ldots, \mu_n) \in \mathbb{Z}/p^n\mathbb{Z}$ there are at most $n!$ solutions $(x_1, \ldots, x_n) \in \mathbb{Z}/p^n\mathbb{Z}$ that the x_j are distinct $\pmod{p}$ and satisfy

$$\begin{aligned} x_1 + \cdots + x_n &\equiv \mu_1 \pmod{p^n}, \\ x_1^2 + \cdots + x_n^2 &\equiv \mu_2 \pmod{p^n}, \\ &\vdots \\ x_1^n + \cdots + x_n^n &\equiv \mu_n \pmod{p^n}. \end{aligned} \tag{LEM}$$

We have "lifted" all of our congruences to be congruences modulo p^n.

Proof

- Recall the Girard–Newton formulae. For $k \in \mathbb{Z}_+$, let

$$p_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k = x_1^k + \cdots + x_n^k.$$

- For $k \in \mathbb{N}$, let $e_k(x_1, \ldots, x_n)$ be the elementary symmetric polynomial

$$\begin{aligned}
e_0(x_1, \ldots, x_n) &= 1, \\
e_1(x_1, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n, \\
e_2(x_1, \ldots, x_n) &= \sum_{1 \le i < j \le n} x_i x_j, \\
&\vdots \\
e_n(x_1, \ldots, x_n) &= x_1 x_2 \cdots x_n, \\
e_k(x_1, \ldots, x_n) &= 0, \quad \text{for } k > n.
\end{aligned}$$

- Then Newton's identities can be stated as

$$k e_k(x_1, \ldots, x_n) = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i}(x_1, \ldots, x_n) p_i(x_1, \ldots, x_n),$$

valid for all $n \ge k \ge 1$.

Proof

- From (LEM) we see that $p_i(x_1, \ldots, x_n) \equiv \mu_i \pmod{p^n}$ for $i \in [n]$.
- Since $(p, n!) = 1$, then the elementary functions $e_j = e_j(x_1, \ldots, x_n)$ given as solutions $\pmod{p^n}$ of the following linear equations

$$e_1 = p_1, 2e_2 = (e_1 p_1 - p_2), 3e_3 = (e_2 p_1 - e_1 p_2 + p_3),$$
$$4e_4 = (e_3 p_1 - e_2 p_2 + e_1 p_3 - p_4), \ldots, ne_n = \sum_{i=1}^{n} (-1)^{i-1} e_{n-i} p_i,$$

  are uniquely determined by $\mu_i \pmod{p^n}$ for $i \in [n]$.
- We also know that the polynomial with roots $x_1, \ldots, x_n$ may be expressed as

$$\prod_{i \in [n]} (x - x_i) = \sum_{k=0}^{n} (-1)^k e_k(x_1, \ldots, x_n) x^{n-k}.$$

- Therefore, the polynomial $\prod_{i \in [n]} (x - x_i)$ in also uniquely determined by $\mu_i \pmod{p^n}$ for $i \in [n]$.

Proof

- Now suppose that there are two solutions $(x_1, \ldots, x_n) \in \mathbb{Z}/p^n\mathbb{Z}$ and $(y_1, \ldots, y_n) \in \mathbb{Z}/p^n\mathbb{Z}$ with distinct entries $\pmod p$ such that

$$\sum_{j \in [n]} x_j^k \equiv \sum_{j \in [n]} y_j^k \equiv \mu_k \pmod{p^n} \quad \text{for all} \quad k \in [n],$$

  then we show that $(y_1, \ldots, y_n)$ is a permutation of $(x_1, \ldots, x_n)$.
- By the previous discussion the polynomials

$$P(z) = \prod_{i \in [n]} (z - x_i) \quad \text{and} \quad Q(z) = \prod_{i \in [n]} (z - y_i)$$

  are identically congruent $\pmod{p^n}$.
- But we have $P(x_j) \equiv 0 \pmod{p^n}$ for all $j \in [n]$, and so we must have

$$Q(x_j) = \prod_{i=1}^{n} (x_j - y_i) \equiv 0 \pmod{p^n} \quad \text{for all} \quad j \in [n].$$

- If the y_i are distinct modulo p this implies that x_j is congruent to one of the $y_i \pmod{p^n}$, and so (since the x_j are also distinct modulo p) the x_j are forced to be a permutation of the $y_j \pmod{p}^n$. This implies that there are at most $n!$ possible solution vectors $(x_1, \ldots, x_n)$. $\square$

Recursive estimate

We now formulate a recursive estimate for $J_{k,n}(P)$, which will enable us to bound it explicitly. This is the crucial part of the Vinogradov–Korobov method.

Proposition

Let $n \geqslant 2, P \geqslant (2n)^{3n}$, and $k \geqslant n^2 + n$. Then

$$J_{k,n}(P) \leqslant 4^{2k} P^{2k/n+(3n-5)/2} J_{k-n,n}\left(P_1\right), \tag{RE}$$

where P_1 is a number which satisfies $P^{(n-1)/n} \leqslant P_1 \leqslant 4P^{(n-1)/n}$.

Proof.

- Let $p \in \mathbb{P}$ be a prime from $\left[\frac{1}{2}P^{1/n}, P^{1/n}\right]$ (such a prime exists by Bertrand's postulate or the prime number theorem).
- Thus $p > n$, and if we set $P_1 = \lfloor Pp^{-1} \rfloor + 1$, then

$$P^{(n-1)/n} \leqslant P_1 \leqslant 4P^{(n-1)/n}, \quad \text{and} \quad P < pP_1.$$

- This gives $J_{k,n}(P) \leqslant J_{k,n}\left(pP_1\right)$. It will suffices to prove

$$J_{k,n}\left(pP_1\right) \leq 4^{2k} Z^{2k/n+(3n-5)/2} J_{k-n,n}\left(P_1\right).$$

Proof

- Let us also note that $p > n$, because of our hypothesis that $P \geq (2n)^{3n}$. We will be able to apply Linnik's lemma to n of our variables.
- We choose $p \simeq P^{1/n}$ so that the ranges mp^n of the variables in Linnik's lemma will approximately match the ranges P of our variables.
- Next, let J_1 denote the number of solution vectors $(x_1, \ldots, x_{2k})$, counted by $J_{k,n}(pP_1)$, in which $(x_1, \ldots, x_k)$ and $(x_{k+1}, \ldots, x_{2k})$ each contain n numbers that are distinct modulo p, and let J_2 denote the number of solution vectors not counted by J_1.
- Then it suffices to estimate J_1 and J_2 separately, since

$$J_{k,n}(pP_1) = J_1 + J_2.$$

- Also let J_1' denote the number of solution vectors $(x_1, \ldots, x_{2k})$, counted by $J_{k,n}(pP_1)$, for which the first n elements $(x_1, \ldots, x_n)$ and $(x_{k+1}, \ldots, x_{k+n})$ are distinct modulo p. Then we have

$$J_{k,n}(pP_1) = J_1 + J_2 \leq k^{2n} J_1' + J_2,$$

  since each vector counted by J_1' corresponds to at most k^{2n} vectors counted by J_1. This is by noting that the first n entries of a vector from J_1' may be placed in $k(k-1)\cdots(k-n+1)$ ways in k places without changing the order of the remaining $k-n$ entries of the vector.

Proof

- We now prove that
$$J_1' \leq \max_{x\in[p]} J_1'(x),$$
where $J_1'(x)$ denotes the number of solution vectors $(x_1,\ldots,x_{2k})$, counted by J_1', for which all of the $2k-2n$ components $(x_{n+1},\ldots,x_k)$ and $(x_{k+n+1},\ldots,x_{2k})$ are congruent to $x \pmod p$.
- Indeed, for $\alpha=(\alpha_1,\ldots,\alpha_n)\in[0,1)^n$, let
$$S_x(\alpha) = \sum_{\substack{z=1 \\ z\equiv x (\bmod p)}}^{P_1} e(\alpha_1 z+\ldots+\alpha_n z^n),$$
and observe that
$$J_1' = \int_{[0,1)^n} \Big| \sum_{\substack{x_1,\ldots,x_n\in[p] \\ \text{distinct}}} S_{x_1}(\alpha)\cdots S_{x_n}(\alpha)\Big|^2 \Big|\sum_{x\in[p]} S_x(\alpha)\Big|^{2k-2n} d\alpha.$$
- Using Hölder's inequality, pulling out the inner sum $\sum_{x\in[p]}$ and taking $\max_{x\in[p]}$ we obtain
$$J_1' \leq p^{2k-2n} \max_{x\in[p]} \int_{[0,1)^n} \Big| \sum_{\substack{x_1,\ldots,x_n\in[p] \\ \text{distinct}}} S_{x_1}(\alpha)\cdots S_{x_n}(\alpha)\Big|^2 |S_x(\alpha)|^{2k-2n} d\alpha.$$
- For every $x\in[p]$, the last integral is precisely equal to $J_1'(x)$ as desired.

Proof

- If $(x_1, \ldots, x_{2k})$ is a solution counted by $J_1'(x)$, then it has the form

  $$\begin{aligned}&(x_1, \ldots, x_n, x_{n+1}, \ldots, x_k, x_{k+1}, \ldots, x_{k+n}, x_{k+n+1}, \ldots, x_{2k})\\ &= (x_1, \ldots, x_n, py_{n+1} + x, \ldots, py_k + x, x_{k+1}, \ldots, x_{k+n}, py_{k+n+1} + x, \ldots, py_{2k} + x),\end{aligned}$$

  where $(x_1, \ldots, x_n)$ and $(x_{k+1}, \ldots, x_{k+n})$ are distinct modulo p, and $y_{n+1}, y_{k+n+1}, \ldots, y_k, y_{2k} \in [P_1]$.
- Observe that the system (HE) is translation invariant, which means that if $(x_1, \ldots, x_{2k})$ satisfies (HE), then $(x_1 - x, \ldots, x_{2k} - x)$ also does.
- Hence, by the translation invariance, we have

  $$\begin{aligned}&\sum_{i=1}^{n} x_i^j - x_{k+i}^j + \sum_{i=n+1}^{k} (py_i + x)^j - (py_{k+i} + x)^j = 0 \quad \text{for all} \quad j \in [n],\\ \iff &\sum_{i=1}^{n} z_i^j - z_{k+i}^j + p^j \sum_{i=n+1}^{k} y_i^j - y_{k+i}^j = 0 \quad \text{for all} \quad j \in [n],\end{aligned}$$

  where $z_i = x_i - x$ and $z_{k+i} = x_{k+i} - x$ for all $i \in [n]$. Moreover, we have $1 - x \leq z_i, z_{k+i} \leq pP_1 - x$ for $i \in [n]$, and $1 \leq y_i, y_{k+i} \leq P_1$ for $i \in [k] \setminus [n]$, and $(z_1, \ldots, z_n)$ and $(z_{k+1}, \ldots, z_{k+n})$ are distinct modulo p.

Proof

- The last system of equations can be rewritten as

$$\sum_{i=1}^{n} z_i^j = \sum_{i=1}^{n} z_{k+i}^j - p^j \sum_{i=n+1}^{k} y_i^j - y_{k+i}^j \quad \text{for all} \quad j \in [n].$$

- Fixing $z_{k+1}, \ldots, z_{k+n}$, each vector $(z_1, \ldots, z_n)$ satisfies the conditions of Linnik's lemma, with $A = 1 - x$ and $m \geq pP_1p^{-n} > Pp^{-n}$, so that we may take $m = \lfloor Pp^{-n} \rfloor + 1$. Thus by Linnik's lemma

$$T \leq n! m^n p^{n(n-1)/2}.$$

- For any fixed $z_1, \ldots, z_n$ and $z_{k+1}, \ldots, z_{k+n}$, the number of vectors $(y_{n+1}, \ldots, y_k, y_{k+n+1}, \ldots, y_{2k})$ that are counted in $J_1'(x)$ is at most $J_{k-n,n}(P_1)$.
- So in total, using the trivial bound $(pP_1)^n$ for the number of choices of $z_{k+1}, \ldots, z_{k+n}$, we may write

$$J_1 \leq k^{2n} J_1'(x) \leq k^{2n} p^{2k-2n} n! m^n p^{n(n-1)/2} (pP_1)^n J_{k-n,n}(P_1).$$

Proof

- Since $p \geqslant \frac{1}{2}P^{1/n}$ we have $Pp^{-n} \leqslant 2^n$, implying $m^n \leqslant 2^{n^2+n} \leqslant 2^k$.
- Using further $p \leqslant P^{1/n}$, and $P_1 \leqslant 4P^{(n-1)/n}$, we obtain

$$J_1 \leqslant n!2^k k^{2n} P^{2k/n+(3n-5)/2} 4^n J_{k-n,n}(P_1) \leqslant \frac{1}{2} 4^{2k} P^{2k/n+(3n-5)/2} J_{k-n,n}(P_1),$$

  because $k \geqslant n^2 + n$, and $n \geqslant 2$.
- Recall that J_2 counts all those vectors $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_{2k})$, counted by $J_{k,n}(pP_1)$, in which either $(x_1, \ldots, x_k)$ or $(x_{k+1}, \ldots, x_{2k})$ contains at most $n-1$ numbers that are distinct $\pmod p$.
- In the first case there are at most $p^{n-1}(n-1)^k$ possibilities for $(x_1 \pmod p), \ldots, x_k \pmod p)$. Indeed, there are at most p^{n-1} ways of choosing $\{u_1, \ldots, u_k\} \subseteq \mathbb{Z}/p\mathbb{Z}$, and then there are at most $(n-1)^k$ possibilities of fixing $(x_1 \pmod p), \ldots, x_k \pmod p)$ with coordinates from $\{u_1, \ldots, u_k\}$. Hence, there are at most $p^{n-1+k}n^k$ possibilities for $(x_1 \pmod p), \ldots, x_k \pmod p), x_{k+1} \pmod p), \ldots, x_{2k} \pmod p)$.
- We proceed similarly in the second case.
- Therefore, if $\mathcal{A}$ denote the set of all possible vectors of the form $(x_1 \pmod p), \ldots, x_k \pmod p), x_{k+1} \pmod p), \ldots, x_{2k} \pmod p)$ that are counted in J_2, then $\#\mathcal{A} \leq 2p^{n-1+k}n^k$.

Proof

- Observe that

$$\left|\sum_{(x_1,\ldots,x_{2k})\in\mathcal{A}} S_{x_1}(\alpha)\cdots S_{x_k}(\alpha)\overline{S_{x_{k+1}}(\alpha)\cdots S_{x_{2k}}(\alpha)}\right|$$
$$\leqslant \left(\sum_{(x_1,\ldots,x_{2k})\in\mathcal{A}} |S_{x_1}(\alpha)|^{2k}\right)^{1/2k}\cdots\left(\sum_{(x_1,\ldots,x_{2k})\in\mathcal{A}} |S_{x_{2k}}(\alpha)|^{2k}\right)^{1/2k}$$
$$\leqslant \sum_{x\in[p]} |S_x(\alpha)|^{2k} \sum_{(x_1,\ldots,x_{2k})\in\mathcal{A}} 1 \leqslant 2p^{k+n-1}n^k \sum_{x\in[p]} |S_x(\alpha)|^{2k}$$
$$\leqslant 2p^{k+n-1}n^k P_1^{2n} \sum_{x\in[p]} |S_x(\alpha)|^{2(k-n)}.$$

since trivially $|S_x(\alpha)| \leqslant P_1$. Therefore

$$J_2 = \int_{[0,1)^n} \sum_{(x_1,\ldots,x_{2k})\in\mathcal{A}} S_{x_1}(\alpha)\cdots S_{x_k}(\alpha)\overline{S_{x_{k+1}}(\alpha)\cdots S_{x_{2k}}(\alpha)}d\alpha$$
$$\leqslant p^{k+n-1}n^k P_1^{2n}\int_{[0,1)^n} \sum_{x\in[P_1]} |S_x(\alpha)|^{2(k-n)}d\alpha$$
$$= p^{k+n-1}n^k P_1^{2n} J_{k-n,n}(P_1) \leqslant \frac{1}{2}4^{2k}P^{2k/n+(3n-5)/2}J_{k-n,n}(P_1).$$

- This completes the proof. □

Vinogradov's mean value theorem

Theorem (Vinogradov's mean value theorem)

Let $r \in \mathbb{N}$, $n \geq 2$, $k \geqslant n^2 + nr$, *and* $P \geqslant P_0$ *and define*

$$c_r = \frac{1}{2}\left(n^2+n\right)\left(1-\frac{1}{n}\right)^r .$$

Then

$$J_{k,n}(P) \leqslant (4n)^{4kr} P^{2k-(n^2+n)/2+c_r}. \qquad (*)$$

Proof.

- We use induction on $r \in \mathbb{N}$. For $r = 0$ inequality (*) is true, since trivially $J_{k,n}(P) \leqslant P^{2k}$.
- Suppose now that (*) is true for $r = m \geqslant 0$ and consider $r = m+1$. If

$$P \geqslant (2n)^{3n(1+1/(n-1))^r}$$

  then $k \geqslant n^2 + n(m+1)$, and $P \geqslant (2n)^{3n(1+1/(n-1))^{m+1}}$.
- An application of the previous proposition gives

$$J_{k,n}(P) \leqslant 4^{2k} P^{2k/n+(3n-5)/2} J_{k-n,n}\left(P_1\right). \qquad \text{(A)}$$

Proof

- To bound $J_{k-n,n}(P_1)$ we may use the the induction hypothesis, since

$$k-n \geqslant n^2+nm, \quad \text{and} \quad P_1 \geqslant P^{1-1/n} \geqslant (2n)^{3n(1+1/(n-1))^m}.$$

- It follows that

$$\begin{aligned} J_{k-n,n}(P_1) &\leqslant (4n)^{4(k-n)m} P_1^{2(k-n)-(n^2+n)/2+c_m} \\ &\leqslant (4n)^{4(k-n)m} 4^{2(k-n)} P^{(1-1/n)(2k-2n-(n^2+n)/2+c_m)}, \end{aligned}$$

which combined with (A) gives (*).

- Let now

$$P < (2n)^{3n(1+1/(n-1))^r},$$

and use induction again, supposing

$$P < (2n)^{3n(1+1/(n-1))^{m+1}}, \quad \text{and} \quad k \geqslant n^2+n(m+1).$$

- Then we have trivially

$$J_{k,n}(P) \leqslant P^{2n} J_{k-n,n}(P), \tag{B}$$

and if $P \geqslant (2n)^{3n(1+1/(n-1))^m}$ then by the first part of the proof $J_{k-n,n}(P)$ may be estimated by (*) as before.

Proof

- Otherwise, we use the induction hypothesis to estimate $J_{k-n,n}(P)$, so that we obtain in any case

$$J_{k-n,n}(P) \leqslant (4n)^{4km} P^{2(k-n)-(n^2+n)/2+c_m},$$

and (B) gives

$$J_{k,n}(P) \leqslant (4n)^{4k(m+1)} P^{2k-(n^2+n)/2+c_{m+1}},$$

since

$$P < (2n)^{3n(1+1/(n-1))^{m+1}}, \quad \text{and} \quad k \geqslant n^2 + n(m+1),$$

implies

$$P^{c_m - c_{m+1}} \leqslant (4n)^{4k}.$$

- This completes the proof of the Vinogradov mean value theorem. □