Mean Value theorems

Let $p \in \mathbb{P}$, $k \geq 2$ s.t. $(p, k) = 1$.

For given $a_1, \dots, a_k \in \mathbb{Z}$ consider

$$S_p(\underline{a}) = \frac{1}{p} \sum_{x=1}^{p} e\left(\frac{a_k x^k + \cdots + a_1 x}{p}\right) \qquad (1)$$

Thm 1. (Mordell) If $a_k \not\equiv 0 \pmod p$, then

$$|S_p(\underline{a})| \leq C_k \, p^{-\frac{1}{k}} \qquad (2)$$

Let $J_p(2k) = \sum_{a_1, \dots, a_k = 1}^{p} |S_p(\underline{a})|^{2k}$.

Lemma 1. $J_p(2k) = k!$

Pf $J_p(2k) = p^{-2k} \sum_{x_1, \dots, x_k = 1}^{p} \sum_{y_1, \dots, y_k = 1}^{p} \sum_{a_1, \dots, a_k = 1}^{p} \times$

$$\times \, e\left(\frac{a_k(x_1^k + \cdots + x_k^k - y_1^k - \cdots - y_k^k) + \cdots + a_1(x_1 + \cdots + x_k - y_1 - \cdots - y_k)}{p}\right)$$

The inner sum $= \begin{cases} p^k, & \text{if } x_1^j + \cdots + x_k^j \equiv y_1^j + \cdots + y_k^j, \text{ for } 1 \leq j \leq k \\ 0, & \text{otherwise} \end{cases}$

Thus,

$$J_p(2k) = p^{-k} \# \{(x_1,\dots,x_k,y_1,\dots,y_k) \in [1,p]^{2k} : x_1^j + \dots + x_k^j \equiv y_1^j + \dots + y_k^j \pmod p \text{ for all } 1 \le j \le k\}$$

Note that $J_p(2k) \ge k!$ as one may choose

$y_1 = x_{\pi(1)}, \dots, y_k = x_{\pi(k)}$ for some permutation $\pi : \{1,\dots,k\} \to \{1,\dots,k\}$

in this case we say $(x_1,\dots,x_k,y_1,\dots,y_k)$ is a "diagonal solution"

Write $P_j(x_1,\dots,x_k) \equiv x_1^j + \dots + x_k^j \pmod p$, for $1 \le j \le k$

and $\sigma_j(x_1,\dots,x_k) = \sum_{1 \le i_1 < i_2 < \dots < i_j} x_{i_1} x_{i_2} \dots x_{i_j}$ for the elementary symmetric polynomials

Then $\sigma_1,\dots,\sigma_k$ are polynomials of $P_1,\dots,P_k$ thus

$$P_j(x_1,\dots,x_k) \equiv P_j(y_1,\dots,y_k) \pmod p, \text{ for } 1 \le j \le k$$

implies that

$$\sigma_j(x_1,\dots,x_k) \equiv \sigma_j(y_1,\dots,y_k) \pmod p, \text{ for } 1 \le j \le k$$

thus $(z-x_1)\cdots(z-x_k) = (z-y_1)\cdots(z-y_k) \in \mathbb{F}_p[z]$

with $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ finite field $\Rightarrow y_i = x_{\pi(i)}$ $1 \le i \le k$

$\Rightarrow J_p(2k) = k!$

Pf of Thm 1.

Write $f(x;\underline{a}) = a_k x^k + \cdots + a_1 x$, where $\underline{a} = (a_k, a_{k-1}, \ldots, a_1)$

and also for $r \in (\mathbb{Z}/p\mathbb{Z})^\times$, $u \in (\mathbb{Z}/p\mathbb{Z})$ let

$$f(x;\underline{a}(r,u)) = f(rx+u;\underline{a}) - f(u)$$

Then

$$|S_p(\underline{a}(r,u))| = \frac{1}{p}\left|\sum_{x \pmod p} e\left(\frac{f(rx+u;\underline{a})}{p}\right)\right| = \frac{1}{p}\left|\sum_{y \pmod p} e\left(\frac{f(y;\underline{a})}{p}\right)\right| =$$

$$= |S_p(\underline{a})|, \text{ as } x \longmapsto y = rx+u : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \text{ bijection}$$

We have, assuming $a_k \not\equiv 0 \pmod p$,

$$f(x;\underline{a}(r,u)) = a_k(rx+u)^k + a_{k-1}(rx+u)^{k-1} + \cdots + a_1(rx+u) =$$

$$= r^k a_k x^k + r^{k-1}(k a_k u + a_{k-1}) x^{k-1} + \cdots$$

Thus given r_1, u_1, we have that $\underline{a}(r,u) = \underline{a}(r_1,u_1)$

if $r^k = r_1^k$ and $r^{k-1}(k a_k u + a_{k-1}) = r_1^{k-1}(k a_k u_1 + a_{k-1})$

thus the number of such pairs is $\le k$.

$$\Rightarrow k! = \sum_{\underline{a}} |S_p(\underline{a})|^{2k} \ge \frac{p(p-1)}{k} |S_p(\underline{a})|^{2k} \text{ for any given } \underline{a} = (a_k, \ldots, a_1), \text{ with } a_k \not\equiv 0 \ (p).$$

$$\Rightarrow |S_p(\underline{a})| \le c_k p^{-\frac{1}{k}}$$

□

Vinogradov's mean value theorem

Given $s, k \geq 1$, let $f_k(\underline{\alpha}, X) = \sum_{1 \leq x \leq X} e(\alpha_1 x + \cdots + \alpha_k x^k)$ (3)

where $\underline{\alpha} = (\alpha_1, \ldots, \alpha_k)$.

We'd like to study the expression

$$J_{s,k}(X) = \int_{[0,1]^k} |f_k(\underline{\alpha}, X)|^{2s} \, d\underline{\alpha} \qquad (4)$$

Note. $J_{s,k}(X)$ is a weighted mean value of the exponential sum $S_k(\alpha, X)$,

- Trivially $J_{s,k}(X) \leq X^{2s}$

As before one can expand (4), to obtain

$$J_{s,k}(X) = \sum_{X_1 = 1, \ldots, X_{2s} = 1}^{X} \int_0^1 \cdots \int_0^1 e\left(\alpha_1 (X_1 + \cdots + X_s - X_{s+1} - \cdots - X_{2s}) + \cdots + \alpha_k (X_1^k + \cdots + X_s^k - X_{s+1}^k - \cdots - X_{2s}^k)\right) d\alpha_1 \cdots d\alpha_k$$

$$= \#\left\{ 1 \leq X_1, \ldots, X_{2s} \leq X ; \; X_1^j + \cdots + X_s^j = X_{s+1}^j + \cdots + X_{2s}^j, \; \forall 1 \leq j \leq k \right\}$$

Note. $J_{s,k}(X) \geq X^s$ setting $X_{i+s} := X_i$ for $1 \leq i \leq s$.

• If $0 \leq \alpha_j \leq \frac{1}{10sX^j}$ for all $1 \leq j \leq k$

then $\sum_{j=1}^{k} \alpha_j x^j \leq \sum_{j=1}^{k} \alpha_j X^j \leq \frac{1}{10}$

$2\pi\alpha \leq \frac{\pi}{3}$, $\cos(\frac{\pi}{3})$, $\alpha \leq \frac{\pi}{6}$

$\Rightarrow$ $\mathrm{Re}\, e(\alpha_1 x + \cdots + \alpha_k x^k) = \cos[2\pi(\alpha_1 x + \cdots + \alpha_k x^k)] \geq \cos\left(\frac{\pi}{3}\right) \geq \frac{1}{2}$

for $1 \leq x \leq X$

$\Rightarrow |S_k(\alpha, X)| \geq \mathrm{Re}\, S_k(\alpha, X) \geq \frac{1}{2} X$

$\Rightarrow |J_{s,k}(X)| \geq c_{s,k} X^{2s - \frac{k(k+1)}{2}}$ as $1 + \cdots + k = \frac{k(k+1)}{2}$.

Thus $J_{s,k} \geq c_{s,k}\left(X^s + X^{2s - \frac{k(k+1)}{2}}\right)$

Thm (Vinogradov's Main Conjecture) For all $s, k \geq 1$, $X \geq 1$ one has that

$$|J_{s,k}(X)| \leq C_{s,k,\varepsilon}\left(X^s + X^{2s - \frac{k(k+1)}{2}}\right) \cdot X^{\varepsilon} \quad (*)$$

Note When $s = s_k = \frac{k(k+1)}{2}$ then both terms are the same.

It is enough to verify (*) when $s = s_k$;

indeed: for $s \geq s_k$, one has

$$J_{s,k}(X) \leq X^{2s-2s_k} J_{s_k,k}(X) \leq X^{2s-2s_k} X^{s_k} X^{\varepsilon}$$
$$= X^{2s-s_k} X^{\varepsilon}$$

and for $s \leq s_k$ $\quad J_{s,k}(X) \leq J_{s_k,k}(X) \leq X^{s_k+\varepsilon} \leq \left(X^{s} + X^{2s-s_k}\right) X^{\varepsilon}$

History

- Vinogradov: (*) holds for $s \geq Ck^2 \log k$
- Linnik–Karatsuba: (*) holds for $s \geq 3k^2(\log k + O(\log\log k))$

  more importantly they introduced the "p-adic approach"
- Wooley (2011): $s \geq k(k+1)$ "efficient congruencing"

  (2014): $s \geq k(k-1)$
- Bourgain–Demeter–Guth (2015): $s \geq \frac{1}{2}k(k+1)$ full-solution

  "decoupling Euclidean harmonic analysis"
- Wooley (2017) $s \geq \frac{1}{2}k(k+1)$ "nested efficient congruencing"