The different congruency method

Again, we consider the system

$$\sum_{i=1}^{s} x_i^j = \sum_{i=1}^{s} y_i^j \quad \text{for } 1 \le j \le k \qquad (5)$$

then given $\lambda \neq 0$, u, $x_1, \dots, x_s, y_1, \dots, y_s$ is a solution to (5) if and only if they are solution to

$$\sum_{i=1}^{s} (\lambda x_i + u)^j = \sum_{i=1}^{s} (\lambda y_i + u)^j \quad \text{for } 1 \le j \le k \qquad (6)$$

Note this means that $\underline{z} = (\underline{x}, \underline{1})$ is a solution

$$\iff \lambda \underline{z} + \underline{u} = (\lambda \underline{x} + \underline{u}, \lambda \underline{y} + \underline{u})$$

is a solution

So the system is translation-dilation invariant

Indeed, trivially $(\underline{x}, \underline{y})$ is a solution $\iff (\lambda \underline{x}, \lambda \underline{y})$ is a solution

Moreover

$$\sum_{i=1}^{s} \left((x_i + u)^j - (y_i + u)^j \right) = \sum_{\ell=1}^{j} \binom{j}{\ell} u^{j-\ell} \sum_{i=1}^{s} \left(x_i^\ell - y_i^\ell \right)$$

(and vice-versa $x_i = x_i + k - u$) $\Rightarrow (\underline{x}+u, \underline{y}+u)$ is a solution

This implies the crucial observation: the number of solutions $X_1, \dots, X_s, X_{s+1}, \dots, X_{2s}$ to $\sum_{i=1}^{s} X_i^j = \sum_{i=1}^{s} X_{i+s}^j$, for $1 \le j \le k$

subject to $X_i \equiv u \pmod q \quad \forall\, 1 \le i \le 2s$

is the number of $z_1, z_2, \dots, z_{2s}$; $z_i \le X/q$

s.t. $\sum_{i=1}^{s} z_i^j = \sum_{i=1}^{s} z_{s+i}^j$, for $1 \le j \le k$

which is $J_{k,s}(X/q)$.

Initial set-up and notation

$$f(\underline{\alpha}) = \sum_{1 \le x \le X} e(\alpha_1 x + \alpha_2 x^2 + \dots + \alpha_k x^k)$$

Given $a, \beta \in \mathbb{N}$, $p \in \mathbb{P}$, write

$$S_a(\underline{\alpha}, \beta) = \sum_{\substack{1 \le x \le X \\ x \equiv \beta \pmod{p^a}}} e(\alpha_1 x + \dots + \alpha_k x^k) \qquad (7)$$

We'll fix a prime $p > k$, but will vary β and a.

We'll count solutions to the Vinogradov system

$$x_1^j + \dots + x_s^j = x_{s+1}^j + \dots + x_{2s}^j, \quad 1 \le j \le k \qquad (8)$$

Subject to the congruence conditions, namely

$$x_i \equiv \xi \pmod{p^a} \quad \text{for } 1 \le i \le m \text{ and } s+1 \le i \le 2s-m; \tag{9}$$

$$x_i \equiv \eta \pmod{p^b} \quad \text{for } m+1 \le i \le s \text{ and } 2s-m+1 \le i \le 2s;$$

which we will denote by $I_m(X; \xi, \eta, a, b)$.

Note that

$$I_m(X; \xi, \eta, a, b) = \int_{[0,1]^k} |S_a(\underline{\alpha}, \xi)|^{2m} |S_b(\underline{\alpha}, \eta)|^{2(s-m)} d\underline{\alpha} \tag{10}$$

Indeed, the RHS of (10) is

$$\int_{[0,1]^k} \Big| \sum_{\substack{x \le X \\ x \equiv \xi (p^a)}} e\Big(\sum_{j=1}^{k} \alpha_j x^j\Big) \Big|^{2m} \Big| \sum_{\substack{x \le X \\ x \equiv \eta (p^b)}} e\Big(\sum_{j=1}^{k} \alpha_j x^j\Big) \Big|^{2m-2s} d\underline{\alpha}$$

$$= \int_{[0,1]^k} \sum_{\substack{x_1, \dots, x_m \\ x_{s+1}, \dots, x_{2s-m} \equiv \xi (p^a)}} \sum_{\substack{x_{m+1}, \dots, x_s \\ x_{m+1}, \dots, x_{2s} \equiv \eta (p^b)}} e\Big(\sum_{j=1}^{k} \alpha_j (x_1^j + \dots + x_m^j + x_{m+1}^j + \dots + x_s^j - x_{s+1}^j - \dots - x_{2s}^j)\Big)$$

which is the number of solutions to (8)-(9).

If $m=0$ then the expression in (10) is independent of β & a; and we write

$$I_0(X;\gamma,b) = \int_{[0,1]^k} |S_b(\underline{\alpha},\gamma)|^{2s} d\underline{\alpha} \quad (11)$$

and $I_0(X;b) = \max_{\gamma \pmod p} I_0(X;\gamma,b)$

Similarly for $1 \le m \le s-1$, write

$$I_m(X;a,b) = \max_{\gamma \not\equiv \beta \pmod p} I_m(X;\beta,\gamma;a,b)$$

The classical p-adic method (Linnik, Karatsuba)

Thm (Vinogradov) Let $s > s_k = \frac{1}{2}k(e+1)$. Then one has

$$J_{k,s}(X) \ll_{k,s} X^{2s-s_k+\eta_{s,k}} \text{ ; with } \eta_{s,k} \le \frac{k^2}{2}\left(1-\frac{1}{k}\right)^{\lfloor s/k \rfloor} \quad (12)$$

Note • If $s \ge ck^2\log k$ then $\eta_{s,k} \le \frac{k^2}{2}\left(1-\frac{1}{k}\right)^{-Ck\log k} \le k^{-C}$

and in this range the estimate is almost as good as the main conjecture.

• We'll only sketch the "p-adic" proof of Linnik and Karatsuba.

(13)

Lemma 1. Let $p < X$, $l \geq 1$. Then $J_{k,k+l}(X) \leq p^{2l} I_k(X;p,1)$

Pf Recall that $I_k(X;1) = \sup_{\beta \pmod p} \int_{[0,1]^k} |S_1(\underline{\alpha},\beta)|^{2l} \cdot |S(\underline{\alpha})|^{2k} d\underline{\alpha}$

Also, $|S(\underline{\alpha})|^{2l} = \left|\sum_{\beta \pmod p} S_1(\underline{\alpha},\beta)\right|^{2l} \leq p^{2l-1} \sum_{\beta \pmod p} |S_1(\underline{\alpha},\beta)|^{2l}$

$$\Rightarrow J_{k,k+l}(X) \leq p^{2l-1} \sum_{\beta \pmod p} \int_{[0,1]^k} |S(\underline{\alpha})|^{2k} |S_1(\underline{\alpha},\beta)|^{2l} d\underline{\alpha}$$

$$\leq p^{2l} \sup_{\beta \pmod p} \int_{[0,1]^k} S(\underline{\alpha})^{2k} |S_1(\underline{\alpha},\beta)|^{2l} d\underline{\alpha}$$

Note We have only used Hölder's ineq. □

i.e. $\frac{1}{p} S(\underline{\alpha}) = \frac{1}{p} \sum_{1 \leq x \leq X} e(\alpha_1 x + \cdots + \alpha_k x^k) = \frac{1}{p} \sum_{\beta \pmod p} \sum_{\substack{1 \leq x \leq X \\ x \equiv \beta \pmod p}} e(\alpha_1 x + \cdots + \alpha_k x^k)$

$$\Rightarrow \left(\frac{1}{p}|S(\underline{\alpha})|\right)^{2l} \leq \frac{1}{p} \sum_{\beta \pmod p} |S_1(\underline{\alpha},\beta)|^{2l} = \frac{1}{p} \sum_{\beta} S_1(\underline{\alpha},\beta)$$

- We've embedded a congruence relation into the count $J_{s,k,a}(X)$.

We use translation/dilation invariance to compare $I_k(X;0,1)$ to $J_{s,k}(X/p)$ to obtain a recursive inequality.

Lemma 2. (Linnik's lemma) Let $p \in \mathbb{P}$ s.t. $p^k > X$, $n_1, \dots, n_k \in \mathbb{Z}$. Then $(x_1, \dots, x_k)$ such that $1 \le x_i \le p^k$ satisfying

$$S_j(x) := \sum_{i=1}^{k} x_i^j \equiv n_j \pmod{p^j}, \text{ for } \forall\, 1 \le j \le k$$

is at most $k!\, p^{\frac{1}{2}k(k-1)}$

Pf: Given $1 \le j \le k$ there are p^{k-j} values of $1 \le m_j \le p^k$ s.t. $m_j \equiv n_j \pmod{p^j}$. Given $1 \le m_1, \dots, m_k \le p^k$ s.t.

$$\sum_{i=1}^{k} x_i^j \equiv m_j \pmod{p^j} \quad \text{and} \quad \sum_{i=1}^{k} y_i^j \equiv m_j \pmod{p^j} \quad \Big\} \; 1 \le j \le k$$

$(1 \le y_i \le p^k)$

then $\prod_{i=1}^{k} (z - x_i) \equiv P(z) \equiv \prod_{i=1}^{k} (z - y_i) \Rightarrow P(y_i) \equiv 0 \pmod{p}$

$\Rightarrow y_1, \dots, y_k$ is a permutation of $x_1, \dots, x_k$. $\square$

Lemma 3. We have $I_{k,2;\ell}(X;p,j) \le k!\, p^{\frac{1}{2}k(k-1)} X^k J_{k,\ell}(X/p)$ (7)

Pf By definition $I_{k,2;\ell}(X;p,1)$ is the max of the number solutions $(x_1,\dots,x_k,y_1,\dots,y_k,u_1,\dots,u_\ell,v_1,\dots,v_\ell)$, $\mathfrak{z}$

$$(15)\quad \sum_{i=1}^{k}\left(x_i^j - y_i^j\right) = \sum_{m=1}^{\ell}\left((pu_m+\mathfrak{z})^j - (pv_m+\mathfrak{z})^j\right)\ ;\ 1\le j\le k$$

as it is the max (over $\mathfrak{z} \pmod p$) of the number of solutions to the Vinogradov system

$$(16)\quad \sum_{i=1}^{k} x_i^j + \sum_{m=1}^{\ell} u_m^j = \sum_{i=1}^{k} y_i^j + \sum_{m=1}^{\ell} v_m^j\ ;\ 1\le j\le k$$

under the congruence restrictions $u_m \equiv v_m \equiv \mathfrak{z} \pmod p$ for $1\le m\le \ell$.

By translation invariance (15) is equivalent to:

$$\sum_{i=1}^{k}\left((x_i-\mathfrak{z})^k - (y_i-\mathfrak{z})^k\right) = p^j \sum_{m=1}^{\ell}\left(u_m^j - v_m^j\right) \qquad (17)$$

We solve this in 2 steps, first count the no. of sol'n's to:

$$\sum_{i=1}^{k}(x_i-\mathfrak{z})^j \equiv \sum_{i=1}^{k}(y_i-\mathfrak{z})^j \pmod{p^j} \qquad (18)$$

One may choose $x_1, \dots, y_k$ via X^k arrays, and once $x_1, \dots, y_k$ fixed, by Hua's Lemma using $X \le p^k$ there are at most $e! p^{\frac{1}{2}k(k-1)}$ choices for $y_1, \dots, y_k$.

Writing $p^{k!} w_j = \sum_{i=1}^{k} ((x_i - \xi)^k - (y_i - \xi)^k)$, there are at most $J_{k,\ell}(X/p)$ choices for $1 \le u_m, v_m \le X/p$

solving $\sum_{m=1}^{\ell} u_m^j - v_m^j = w_j \quad , 1 \le j \le k$

uniformly in w_j. Indeed, the # of solutions may be written as:

$$\int_{[0,1]^k} \left| \sum_{1 \le u \le X/p} e(\alpha_1 u + \alpha_2 u^2 + \dots + \alpha_k u^k) \right|^{2\ell} e(-\alpha_1 w_1 - \dots - \alpha_k w_k)\, d\underline{\alpha}$$

$$\le \int_{[0,1]^k} |S_k(\underline{\alpha}, X/p)|^{2\ell} = J_{k,\ell}(X/p)$$

□