Define $\eta_{s,k} \geq 0$ to be the smallest number such that $\forall \varepsilon > 0 \ \exists \ C_{k,s,\varepsilon} > 0$

$$J_{k,s}(X) \leq C_{k,s,\varepsilon} X^{2s - \frac{1}{2}k(k+1) + \eta_{k,s} + \varepsilon}, \text{ for } X \geq 1$$

Note One can think of $J_{k,s}(X) \approx X^{2s - s_k + \eta_{k,s}}$ as $X \to \infty$.

$X^{\eta_{k,s}}$ measures, hour for $J_{k,s}(X)$ from $X^{2s-s_k}$.

From Lemma 1 & Lemma 3, we have (with $l = s$)

$$J_{k,k+s}(X) \leq p^{2s} I_{k,k+s}(X; 0, 1) \quad \text{and} \quad \left( s_k = \tfrac{1}{2}k(k+1) \right)$$

$$I_{k,k+s}(X; 0, 1) \leq C_k X^k p^{\frac{1}{2}k(k-1)} J_{k,s}(X/p) \quad \left( p \geq X^{\frac{1}{k}} \right)$$

$$\leq C_{k,s} X^{2s+k-s_k+\eta_{s,k}} p^{-2s+\frac{k^2}{2}-\eta_{s,k}}, \text{ as } \tfrac{1}{2}k(k-1) + s_k = k^2$$

Thus choosing $X^{\frac{1}{k}} \leq p \leq 2X^{\frac{1}{k}}$, we have

$$X^{2(s+k)-s_k+\eta_{k,k+s}} \leq C_{k,s} X^{2s+2k-s_k+\eta_{k,s}} p^{2s-2s-\eta_{s,k}}$$

$$\Rightarrow \quad X^{\eta_{k,k+s}} \leq C_{k,s} X^{\eta_{k,s}} X^{-\frac{1}{k}\eta_{k,s}}$$

$$\Rightarrow \quad \eta_{k,k+s} \leq \left(1 - \frac{1}{k}\right) \eta_{k,s}$$

Trivially, $J_{k,0}(X) = \int_{[0,1]^k} |S(\xi;X)|^0 \, d\xi = 1 = X^0 = X^{0-s_k+s_k}$ (2)

thus $\gamma_{k,0} = s_k = \frac{1}{2}k(k+1)$, $\gamma_{k,s_k} \le \frac{1}{2}k(k+1)\left(1-\frac{1}{k}\right)^2$

$\Rightarrow \gamma_{k,s} \le \frac{k(k+1)}{2}\left(1-\frac{1}{k}\right)^{s-s_k}$

$\Rightarrow \gamma_{k,s} \le k^{-c}$ if $s \ge (c+2)k^2\log k$.

This proves the original Mean Value Thm of Vinogradov.

## Efficient congruencing for degree $k=2$

We have $k=2$, $s_k = \frac{3\cdot 2}{2} = 3$; want to prove

$J_{2,3}(X) \ll_\varepsilon X^{3+\varepsilon}$ i.e. the Hardy-Littlewood Conjecture

Note: • We've proved this by elementary means before.

• We use the same basic ideas as in the classical method, but iteratively considering solutions (mod $p^b$) for higher and higher powers $b$.

The basic Lemmas.

Lemma 1. If $p \le X$, then

$$J(X) \ll p\, J(2X/p) + p^6\, I_1(X;1,1). \quad (14.1)$$

Note $J(X) = \#\{1 \le X_1, \dots, X_6 \le X : X_1+X_2+X_3 = X_4+X_5+X_6,$
$X_1^2+X_2^2+X_3^2 = X_4^2+X_5^2+X_6^2\}$ (V)

$I_1(X;1,1) = \#\{1 \le X_1, \dots, X_6 \le X$ ; solutions to (V)
subject to $X_1 \equiv X_4 \equiv 3 \pmod p$
$X_2 \equiv X_3 \equiv X_5 \equiv X_6 \equiv \eta \pmod p$

Lemma 2. If $1 \le a \le 2b$, then $I_1(X;a,b) \le p^{2b-a}\, I_1(X;2a,b)$ (14.2)

Note • $I_1(X;a,b) =$ # solutions to (V) satisfying
$X_1 \equiv X_4 \equiv 3 \pmod{p^a}$
$X_2 \equiv X_3 \equiv X_5 \equiv X_6 \equiv \eta \pmod{p^b}$

• This is a key new step moving from congr. conditions $\pmod{p^b}$ to $\pmod{p^{2b}}$ possibly.

Lemma 3. If $1 \le a \le 2b$ and $p^b \le X$, then

$$I_1(X;a,b) \le p^{2b-a}\, I_1(X;b,2b)^{1/2}\, J(2X/p^b)^{1/2} \quad (14.3)$$

## The iteration scheme (for $k=2$).

We know $X^3 \ll J(X) \ll X^6$; so let

$\delta^* = \inf\{\delta \geq 0 ;\ J(X) \leq C_\delta X^{3+\delta}$, for all $X \geq 1\}$

Then we have that $J(X) \leq C_\varepsilon X^{3+\delta^*+\varepsilon}$ $(\forall \varepsilon > 0\ \exists C_\varepsilon > 0)$

we'll write $J(X) \ll_\varepsilon X^{3+\delta^*+\varepsilon}$

Assuming Lemma 1 – Lemma 3, first we prove

**Prop 1.** For all $b \geq 1$, $n \geq 0$, one has

$$I_1(X; b, 2b) \ll_{n,b,\varepsilon} X^{3+\delta^*+\varepsilon} p^{-nb\delta^*} \qquad (14.4)$$

**Proof** (induction on $n$)

$n=0$: $I_1(X; b, 2b) \leq J(X) \ll_\varepsilon X^{3+\delta^*+\varepsilon}$ ✓

$n \mapsto n+1$:

$$I_1(X; b, 2b) \overset{L.3}{\leq} p^{4b-b} I_1(X; 2b, 4b)^{1/2} J(2X/p^{2b})^{1/2}$$

$$\ll_{b,n,\varepsilon} p^{3b} \left(X^{3+\delta^*+\varepsilon} p^{-2nb\delta^*}\right)^{1/2} (2X/p^{2b})^{\frac{3+\delta^*+\varepsilon}{2}}$$

$$\ll_{b,n,\varepsilon} X^{3+\delta^*+\varepsilon} p^{-(n+1)b\delta^*}$$

□

Note. One may think, in terms of the $p$-adic metric $\|\cdot\|_p$, that $I_1(X;b,2b)$ counts those solutions which fall into a rectangle (a small neighborhood) of size $p^{-b} \times p^{-b} \times p^{-2b} \times \cdots \times p^{-2b}$ and would expect to have $\sim J(X) p^{-10b}$ such solutions. But if one chooses $n$ large then we have much less $\approx J(X) p^{-nb\delta^*}$ solutions as long as $\delta^* > 0$.

Prop 2. Suppose $p^{2n} \leq X$. Then,

$$J(X) \ll_\varepsilon X^{3+\delta^*+\varepsilon}\left(p^{-2-\delta^*} + p^{\frac{11}{2} - \frac{(n+1)\delta^*}{2}}\right) \tag{14.5}$$

Pf $J(X) \ll p\, J(2X/p) + p^6 I_1(X;1,1)$

$$\leq p\, J(2X/p) + p^7 I_1(X;1,2)^{\frac{1}{2}} J(2X/p)^{\frac{1}{2}}$$

$$\ll_{n,\varepsilon} p\, J(2X/p) + p^7\left(X^{3+\delta^*+\varepsilon} p^{-n\delta^*}\right)^{\frac{1}{2}} (2X/p)^{\frac{3+\delta^*+\varepsilon}{2}}$$

$$\ll_{n,\varepsilon} X^{3+\delta^*+\varepsilon}\left(p^{-2-\delta^*} + p^{\frac{11}{2} - \frac{(n+1)\delta^*}{2}}\right)$$

□

**Thm** $J(X) \ll_\varepsilon X^{3+\varepsilon}$

**Pf** Assume indirectly that $\delta^* > 0$. WLOG $X \geq 10^{2^n}$

and choose $p$ s.t. $\frac{1}{2} X^{1/2^n} \leq p \leq X^{1/2^n}$.

Choose $n$ s.t. $(n+1)\delta^* \geq 12$, then Prop 2 $\Rightarrow$

$$J(X) \leq C_{n,\varepsilon} X^{3+\delta^*+\varepsilon} p^{-\frac{1}{2}} \leq C_{n,\varepsilon} X^{3+\delta^* - \frac{1}{2^{n+1}} + \varepsilon}$$

but this contradicts the definition of $\delta^*$,

i.e. to the fact that $\delta^* = \inf\{\delta \geq 0, J(X) \leq C_\varepsilon X^{3+\delta+\varepsilon}$ for all $\varepsilon > 0\}$

□