

Efficient congruencing: Model Case  $k=2$ .

Want to prove:  $J(X) = I_{3,2}(X) \ll_{\epsilon} X^{3+\epsilon}$ .

We have reduced this to proving the lemmas

Lemma 0. If  $a, b \geq 1$ ,  $p^b \leq X$ , then  $I_0(X; a, b) \leq J(2X/p^b)$ . (5.0)

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

$$J(X) \ll_p J(2X/p) + p^6 I_1(X; 1, 1) \quad (5.1)$$

Lemma 2. If  $1 \leq a \leq 2b$ , then

$$I_1(X; a, b) \leq p^{2b-a} I_1(X; 2b, b) \quad (5.2)$$

Lemma 3. If  $1 \leq a \leq 2b$ , then

$$I_1(X; a, b) \leq p^{2b-a} I_1(X; b, 2b)^{\frac{1}{2}} J(2X/p^b)^{\frac{1}{2}} \quad (5.3)$$

Idea: Apply Lemma 2 - Lemma 3 recursively, to compare  $J(X)$  to  $I(X; b, 2b)$  for large  $b$ .

Pf. Lemma 20. (Works for general  $k$  and  $s$ ).

$$I_0(X_{i_0, b}) = I_0(X_i, b) = \max_{\gamma \pmod{p^b}} = \{1 \leq X_1, \dots, X_s; \text{ sol. to } \textcircled{V}\} \text{ s.t. } X_i \equiv \gamma \pmod{p^b} \forall \{1 \leq i \leq s\}$$

Writing  $X_i = p^b y_i + \gamma$ ;  $1 \leq y_i \leq 2X/p^b$ , we get  $y_1, \dots, y_s$  is a sol. of  $\textcircled{V} \Rightarrow I_0(X_{i_0, b}) \leq J(2X/p^b)$

Pf. Lemma 21 Consider a solution to  $\textcircled{V}$  for  $k=2, s=3$

$$\text{i.e. to } X_1 + X_2 + X_3 = X_4 + X_5 + X_6 \quad (1)$$

$$X_1^2 + X_2^2 + X_3^2 = X_4^2 + X_5^2 + X_6^2$$

such that;

$$\text{I } X_1 \equiv \dots \equiv X_6 \equiv \gamma \pmod{p}.$$

By Lemma 0, the # of such solutions  $\leq p J(2X/p)$

$$\text{II. } \exists i, j: X_i \equiv 3 \pmod{p}, X_j \equiv \gamma \pmod{p}; 3 \not\equiv \gamma \pmod{p}.$$

$$\text{Recall } S_1(\alpha, \beta) = \sum_{\substack{1 \leq x \leq X \\ x \equiv 3 \pmod{p}}} e(\alpha_1 x + \alpha_2 x^2)$$

$$S_1(\alpha, \beta) \sim \frac{1}{p} (4 + \gamma)^2$$

Thus the number of such solutions are odd by.

$$\binom{6}{2} \sum_{\substack{3 \neq \eta \\ (\text{mod } 6)}} \int_{[0,1]^2} |S_1(x,3)| |S_1(x,\eta)| |S(x)|^4 dx \quad (15.5)$$

$\mathcal{J}_2(3,\eta)$

For fixed  $3, \eta$  apply Hölder's ineq. to get:  $\frac{1}{6} + \frac{1}{6} + \frac{2}{3} = 1$

$$|\mathcal{J}_2(3,\eta)| \leq \left( \int |S_1(x,3)|^2 |S_1(x,\eta)|^4 dx \right)^{\frac{1}{6}} \left( \int |S_1(x,3)|^4 |S_1(x,\eta)|^{\frac{6}{5}} dx \right)^{\frac{1}{6}} \times \left( \int |S(x)|^6 dx \right)^{\frac{2}{3}}$$

Using  $\int fgh \leq \left( \int |f|^6 \right)^{\frac{1}{6}} \left( \int |g|^6 \right)^{\frac{1}{6}} \left( \int |h|^{\frac{3}{2}} \right)^{\frac{2}{3}}$  as  $\frac{1}{6} + \frac{1}{6} + \frac{2}{3} = 1$

with  $f = |S_1(x,3)|^{\frac{1}{3}} |S_1(x,\eta)|^{\frac{2}{3}}$ ,  $g = |S_1(x,3)|^{\frac{2}{3}} |S_1(x,\eta)|^{\frac{1}{3}}$   
 $h = |S(x)|^4$

Thus

$$|\mathcal{J}_2(3,\eta)| \leq I_1(x;1,1)^{\frac{1}{3}} J(x)^{\frac{2}{3}}$$

$$\Rightarrow J(x) = \mathcal{J}_1(x) + \mathcal{J}_2(x)$$

$$\ll p^{-\left(\frac{2X}{p}\right)} + p^2 I_1(x,1,1)^{\frac{1}{3}} J(x)^{\frac{2}{3}} \quad (15.6)$$

If  $pJ(2X/p)$  dominates the R.H.S, then (15.1) holds. (4)  
 otherwise

$$\therefore J(X) \ll p I_1(X, 1, 1)^{1/3} J(X)^{2/3}$$

$$\Rightarrow J(X) \ll p^6 I_1(X, 1, 1)$$

Pf. Lemma 2.

Recall that  $I_1(X, \beta, \gamma, a, b)$  is the # of solutions  $X_1, \dots, X_6$  to  $V$ , satisfying

$$\begin{aligned} X_1 &= \beta + p^a y_1, & X_4 &= \beta - p^a y_2 \\ X_i &= \gamma + p^b y_i & \text{for } i &= 2, 3, 5, 6. \end{aligned} \tag{15.7}$$

by translation invariance, writing  $\nu = \beta - \gamma (\not\equiv 0 \pmod{p})$  (15.7) is equiv. to:

$$\begin{aligned} Z_i &= \nu + p^a y_i & (i=1, 4) \\ Z_i &= p^b y_i & (i=2, 3, 5, 6) \end{aligned} \tag{15.8}$$

but then

$$Z_1 \equiv Z_4 \pmod{p^a} \quad \& \quad Z_1^2 \equiv Z_4^2 \pmod{p^{2a}}$$

$$\Rightarrow (\nu + p^a y_1)^2 \equiv (\nu + p^a y_4)^2 \pmod{p^{2a}}$$

$$\text{as } p^{2a} \Rightarrow \nu + p^a y_1 \equiv \nu + p^a y_4 \pmod{p^{2a}}$$

$$\Rightarrow y_1 \equiv y_4 \pmod{p^{2a-a}}$$

Suppose  $y_4$  is fixed  $(\text{mod } p^{2b-a}) \Rightarrow y_1$  is fixed  $(\text{mod } p^{2b-a})$  (5)

$\Rightarrow X_1, X_4$  fixed  $(\text{mod } p^{2b})$  i.e.  $X_1 \equiv X_4 \equiv \bar{3} \pmod{p^{2b}}$

$$\Rightarrow I_1(X_i, \bar{3}, \gamma, a, b) \leq p^{2b-a} I_1(X_i, 2b, b)$$

(as there are  $p^{2b-a}$  choices for  $y_1 \pmod{p^{2b-a}}$ .)

Pf. Lemma 3. We have

$$I_1(X_i, \gamma, 2b, b) = \int_{[0,1]^2} |S_{2b}(\pm, \gamma)|^2 |S_b(\pm, \gamma)|^4 d\alpha$$

$$\leq \left( \int_{[0,1]^2} |S_{2b}(\pm, \gamma)|^4 |S_b(\pm, \gamma)|^2 d\alpha \right)^{\frac{1}{2}} \left( \int |S_b(\pm, \gamma)|^6 \right)^{\frac{1}{2}}$$

$$= I_1(X_i, \gamma, 3, b, 2b)^{\frac{1}{2}} I_0(X_i, \gamma, \frac{b}{2})^{\frac{1}{2}}$$

$$\leq I_1(X_i, b, 2b)^{\frac{1}{2}} J(2X/p^b)^{\frac{1}{2}}$$

Thus by Lemma 2,

$$I_1(X_i, a, b) \leq p^{2b-a} I_1(X_i, 2b, b) \leq p^{2b-a} I_1(X_i, b, 2b)^{\frac{1}{2}} J(2X/p^b)^{\frac{1}{2}}$$

Efficient congruencing for  $k=3$ 

Thm  $J_{6,3}(X) \ll_\epsilon X^{6+\epsilon}$ , for all  $X \geq 1$ ,  $\epsilon > 0$ .

Note. This is a highly non-triv. result, eventually proved by Wooley in 2014?

- Write  $J(X)$  for  $J_{6,3}(X)$
- We follow Heath-Brown's approach, [HB] which simplifies Wooley's proof.

Lemma 3.0. For any  $a, b \geq 1$  if  $p^b \leq X$ , then

$$I_0(X; a, b) \leq J(2X/p^b) \quad (16.0)$$

Note This lemma shows that counting with congruence conditions can be reduced to counting without congr. cond on a smaller range.

Proof (this is Lemma

(7)

Lemma 3.10 If  $p \leq X$ , then  $J(X) \ll_p J(2X/p) + p^{12} I_2(X; 1, 1)$  (16.1)

Note This is used to introduce congruence conditions

Proof Is essentially the same as the proof of Lemma 2.1.

We have, for some  $3 \neq q$

$$J(X) \ll_p J(2X/p) + \binom{12}{2} p(p-1) \int_{[0,1]^3} |S_1(\underline{x}, 3) S_1(\underline{x}, q) S(\underline{x})|^{10} d\underline{x}$$

Using Hölder with  $\frac{1}{12} + \frac{1}{12} + \frac{5}{6} = 1$ , we get

$$J(X) \ll_p J(2X/p) + p^2 I_2(X; 1, 1)^{\frac{1}{12}} \cdot I_2(X; 1, 1)^{\frac{1}{12}} J(X)^{\frac{5}{6}} \quad (16.2)$$

as  $I_2(X; 1, 1) = \max_{3 \neq q \pmod{p}} \int_{[0,1]^3} |S_1(\underline{x}, 3)|^4 |S_1(\underline{x}, q)|^2 d\underline{x}$

As before, this implies

$$J(X) \ll_p J(2X/p) + p^{12} I_2(X; 1, 1)$$

□

We'll get recursive estimates by comparing



$I_1(X; a, b)$  and  $I_2(X; a, b)$  different ways.

Lemma 3.2

$$I_2(X; a, b) \leq I_2(X; b, a)^{1/3} I_1(X; a, b)^{2/3} \quad (16.3)$$

Lemma 3.3

$$I_1(X; a, b) \leq \rho^{3b-a} I_2(X; b, a)^{1/4} J(2X/\rho)^{3/4}$$

Pf of Lemma 3.2.

$\exists 3 \neq 4$  s.t.

$$I_2(X; a, b) = \int |S_a(\pm, 3)|^4 |S_b(\pm, 4)|^8 d\pm$$

Using Holder with  $\frac{1}{3} + \frac{2}{3}$  with  $f = |S_a(\cdot)|^{2/3} \cdot |S_b(\cdot)|^{4/3}$

$$g = |S_a(\cdot)|^{4/3} \cdot |S_b(\cdot)|^{20/3}$$

$$\Rightarrow |I_2(X; a, b)| \leq \left( \int |S_a(\pm, 3)|^8 |S_b(\pm, 4)|^4 d\pm \right)^{1/3} \times$$

$$\times \left( \int |S_a(\pm, 3)|^2 |S_b(\pm, 4)|^{10} d\pm \right)^{2/3}$$

$$= I_2(X; b, a)^{1/3} I_1(X; a, b)^{2/3}$$

□