Efficient congruencing for $k=3$

We consider the system:

$$\left.\begin{aligned} X_1 + \cdots + X_6 &= X_7 + \cdots + X_{12} \\ X_1^2 + \cdots + X_6^2 &= X_7^2 + \cdots + X_{12}^2 \\ X_1^3 + \cdots + X_6^3 &= X_7^3 + \cdots + X_{12}^3 \end{aligned}\right\} \quad \text{(V)}$$

$$J(X) = \int_{[0,1]^3} |S(\underline{\alpha})|^{12} d\underline{\alpha} = \#\text{ solutions } 1 \le X_1, \dots, X_{12} \le X \text{ of the system (V).}$$

$$S(\underline{\alpha}) = S(\alpha, X) = \sum_{1 \le x \le X} e(\alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3)$$

For given $p \in \mathbb{P}$, $(p < X)$, $\beta \bmod p^a$, we define

$$S_a(\underline{\alpha}, \beta) = \sum_{\substack{x \le X \\ x \equiv \beta \,(p^a)}} e(\alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3)$$

and

$$I_m(X; a, b; \beta, \gamma) = \int_{[0,1]^3} |S_a(\underline{\alpha}, \beta)|^{2m} |S_b(\underline{\alpha}, \gamma)|^{2(6-m)} d\underline{\alpha}$$

$$= \#\text{ of solutions to (V), subject to}$$

$$X_i \equiv X_{6+i} \equiv \beta \pmod{p^a}, \text{ for } 1 \le i \le m$$

$$X_j \equiv X_{6+j} \equiv \gamma \pmod{p^b}, \text{ for } m+1 \le j \le 6$$

We had the following

Lemma 3.0. For $a, b \ge 1$, s.t. $p^b \le X$ we have

$$I_0(X; a, b) \le J(2X/p^b) \qquad (0)$$

Pf Trans. invariance: $X_j \equiv \gamma \ (p^b) \ \forall 1 \le j \le 12$

$$X_j = p^b y_j + \gamma \Rightarrow 1 \le y_1, \dots, y_{12} \le 2X/p^b$$

Lemma 3.1. If $p \in \mathcal{X}_1$, then $J(X) \ll p J(2X/p) + p^2 I_2(X_1;1,1)$ (2)

(1)

Pf

i) $X_1 = \exists X_{12} \equiv \eta \pmod p \rightarrow \ll p J(2X/p)$

2) $\exists i,j \quad X_i \equiv \xi \pmod p, \quad X_j \equiv \eta \pmod p$

$$\Rightarrow I_2(X) \ll p^2 \int_{[0,1]^3} |S_1(\xi,\beta)|\,|S_1(\xi,\eta)|\,|S(\xi)|^{10}\,d\xi$$

Hölder $\frac{1}{10} + \frac{1}{10} + \frac{8}{10} = 1 \Rightarrow I_2(X) \ll p^2 I_2(X_1;1,1)^{\frac{1}{5}} J(X)^{\frac{4}{5}}$

Lemma 3.2. $I_2(X;a,a) \ll I_2(X;b,a)^{1/3} I_1(X;a,a)^{1/2}$ (16.5)

Pf Hölder with $\frac{1}{3} + \frac{2}{3} = 1$, (→ see prev. notes)

Lemma 3.3. $I_1(X;a,b) \ll p^{3b-a} I_2(X;b,a)^{1/4} J(2X/p^b)^{3/4}$, $b \le \frac{1}{2}$

Pf There is β or η such that

$$I_1(X;a,a) = \int_{[0,1]^3} |S_a(\xi,\beta)|^2\,|S_b(\xi,\eta)|^{10}\,d\xi$$

$$\le \left(\int_{[0,1]^3} |S_b(\xi,\eta)|^4\,|S_a(\xi,\beta)|^2\,d\xi\right)^{1/4} \left(\int_{[0,1]^3} |S_b(\xi,\alpha)|^{12}\,d\xi\right)^{3/4}$$

$$\le I_2(X;b,a)^{1/4}\, I_0(X;b,a)^{3/4} \ll I_2(X;b,a)^{1/4}\, J(2X/p^b)^{3/4}$$

□

Lemma 3.4. If $1 \le a \le 3b$, then

$$I_1(X_i; a, b) \le p^{3b-a} I_1(X_i; 3b, b) \qquad (16.4)$$

Pf $I_1(X_i; a, b)$ counts solutions to I_1 in which

$X_i = \beta + p^a y_i$ for $i = 1, 7$ and $X_i = \gamma + p^b y_i$ for $i \neq 1, 7$

"By translation invariance (with $\nu = \beta - \gamma$)

$Z_i = \nu + p^a y_i$ for $i = 1, 7$ and $Z_i = p^b y_i$ for $i \neq 1, 7$

is also a solution to $\mathrm{I} \Rightarrow (\nu + p^a y_1)^3 \equiv (\nu + p^a y_7)^3 \pmod{p^{3b}}$

Using, crucially that $\beta \not\equiv \gamma \pmod p$ since $(\nu, p) = 1$,

we have that $\nu + p^a y_1 \equiv \nu + p^a y_7 \pmod{p^{3b}}$

$$\Rightarrow y_1 \equiv y_7 \pmod{p^{3b-a}}$$

$\Rightarrow X_1 \equiv X_7 \equiv \beta' \pmod{p^{3b}}$ with p^{3b-a} possible values of β'

$\Rightarrow I_1(X_i; a, b) \le p^{3b-a} I_1(X_i; 3b, b)$ □

Note So far everything is proved also in the $b = 2$ case.

Lemma 3.5. If $1 \le a < b$, then

$$I_2(X; a, b) \le 2b\, p^{4(b-a)}\, I_2(X; 2b-a, b) \qquad (16.5)$$

Pf $I_2(X; a, b)$ counts solutions, in which

$X_i = \beta + p^a y_i$ for $i = 1, 2, 7, 8$ and $X_i = \gamma + p^b y_i$ for $3 \le i \le 6$ and $9 \le i \le 12$

Writing $Z_i = X_i - \gamma$, we have $Z_i = \delta + p^a y_i$ for $i = 1, 2, 7, 8$

and $Z_i = p^a y_i$ for $i \neq 1, 2, 7, 8$

thus $(\delta + p^a y_1)^j + (\delta + p^a y_2)^j - (\delta + p^a y_7)^j - (\delta + p^a y_8)^j \equiv 0 \pmod{p^{bj}}$

for $j = 1, 2, 3$

Write $S_j = y_1^j + y_2^j - y_7^j - y_8^j$, for $j = 1, 2, 3$.

then we have $p^a S_1 \equiv 0 \pmod{p^b} \Leftrightarrow S_1 \equiv 0 \pmod{p^{b-a}}$

$$2\delta p^a S_1 + p^{2a} S_2 \equiv 0 \pmod{p^{2b}}$$

$$2\delta S_1 + p^a S_2 \equiv 0 \pmod{p^{2b-a}} \qquad (16.6)$$

$$3\delta^2 S_1 + 3\delta p^a S_2 + p^{2a} S_3 \equiv 0 \pmod{p^{3b-a}} \qquad (16.7)$$

One can eliminate S_1 to obtain

$$3\delta p^a S_2 + 2p^{2a} S_3 \equiv 0 \pmod{p^{2b-a}}.$$

Then $3\nu S_2 + 2p^a S_3 \equiv 0 \pmod{p^{2b-2a}}$ (16.8)

and $2\nu S_1 + p^a S_2 \equiv 0 \pmod{p^{2b-2a}}$ ⇐ (16.6')

We need the following Claim (proved later)

Given $a \geq 1, c \geq 0$.

Claim Let $N(p;a,c)$ be the number of $(y_1, y_2, y_7, y_8) \pmod{p^c}$ satisfying the congruences

$$2\nu S_1 + p^a S_2 \equiv 0 \pmod{p^c}$$
$$3\nu S_2 + 2p^a S_3 \equiv 0 \pmod{p^c}$$

then $N(p;a,c) \leq (c+1)p^c$.

Assuming Claim, we argue as follows. Suppose we have a solution $(y_1', y_2', y_7', y_8') \pmod{p^{2b-2a}}$ of (16.8) and (16.6').

If $y_i \equiv y_i' \pmod{p^{2b-2a}}$, then $x_i \equiv \xi + p^a y_i' =: \xi_i' \pmod{p^{2b-a}}$ for $i = 1, 2, 7, 8$, (& $x_i \equiv \eta \pmod{p^b}$ if $i \neq 1, 2, 7, 8$)

The number of such solutions to V, is given by

$$I = \int_{[0,1]^2} S_{2b-a}(\alpha; \xi_1) S_{2b-a}(\alpha; \xi_2) \overline{S_{2b-a}(\alpha; \xi_3)} \overline{S_{2b-a}(\alpha; \xi_4)} |S_b(\alpha; \eta)|^8 d\alpha$$

Thus

$$|I| \le \int_{[0,1]^2} \prod_{i=1,2,7,8} |S_{2b-a}(\alpha,\beta,\cdot)| \, |S_b(\alpha,\gamma)|^8 \, d\underline{\alpha}$$

$$\le \prod_{i=1,2,7,8} \left(\int_{[0,1]^2} |S_{2b-a}(\alpha,\beta,\cdot)|^4 \, |S_b(\alpha,\gamma)|^8 \, d\underline{\alpha} \right)^{1/4}$$

$$= \prod_{i=1,2,7,8} I_2(X_i; 2b-a, b, \beta_i, \gamma)^{1/4} \le I_2(X_i; 2b-a, b)$$

Using Claim 1, the number of choices of y_1', y_2', y_7', y_8' modulo p^{2b-2a} is at most

$$(2(b-a)+1)\, p^{4(b-a)} \le 2b\, p^{4(b-a)},$$

thus $I_2(X;a,b) \le 2b\, p^{4(b-a)} I_2(X; 2b-a, b)$ □

Pf of Claim 1. (Induction on c)

$c=0$ ✓ $\quad$ $\underline{c=1}$: We have $S_1 \equiv 0 \pmod p$, $S_2 \equiv 0 \pmod p$

$\Rightarrow y_1 + y_2 - y_7 - y_8 \equiv 0 \pmod p \Rightarrow y_8 \equiv y_1 + y_2 - y_7$

$\Rightarrow y_1^2 + y_2^2 - y_7^2 - (y_1+y_2-y_7)^2 \equiv 0 \pmod p$

$\Rightarrow$ given y_1, y_2 there are at most 2 values of $y_7 \pmod p$

$\Rightarrow N(p;a,1) \leq 2p^2$ ✓.

$C \mapsto C+1$:

We say that a solution (y_1, y_2, y_7, y_8) is singular, if

$$y_1 \equiv y_2 \equiv y_7 \equiv y_8 \pmod{p}$$

and non-singular otherwise.

First, we count non-singular solutions, by using Hensel's lemma for a system of 2 equations as follows.

Given $y_1, y_2, y_7, y_8 \pmod{p^c}$ consider $z_1, \dots, z_8 \pmod{p^{c+1}}$

s.t. $z_i \equiv y_i \pmod{p^c}$, i.e. $z_i = p^c u_i + y_i$; $0 \leq u_i \leq p-1$ $i = 1, 2, 7, 8$

Then for any $1 \leq j \leq 3$ we have that

$$S_j(z_1, z_2, z_7, z_8) \equiv S_j(y_1, y_2, y_7, y_8) + p^c \nabla S_j(y_1, y_2, y_7, y_8) \cdot (u_1, u_2, u_7, u_8) \pmod{p^{c+1}} \quad (16.10)$$

Here $S_j(y_1, y_2, y_7, y_8) = y_1^j + y_2^j - y_7^j + y_8^j$

$$\nabla S_j(y_1, y_2, y_7, y_8) = j(y_1^{j-1}, y_2^{j-1}, -y_7^{j-1}, -y_8^{j-1})$$

Thus the second term in (16.10) is

$$jp^c(y_1^{j-1}u_1 + y_2^{j-1}u_2 - y_7^{j-1}u_7 - y_8^{j-1}u_8)$$

all other terms $\equiv 0 \pmod{p^{2c}}$ and hence $\equiv 0 \pmod{p^{c+1}}$ as $c \geq 1$.

Thus if (y_1, y_2, y_3, y_4) is a non-sing sol. $(\mathrm{mod}\ p^c)$
then (z_1, z_2, z_3, z_4) is a sol $(\mathrm{mod}\ p^{c+1})$ if

$$p^c \nabla(2\gamma S_1 + p^a S_2)\cdot \underline{u} + (2\gamma S_1 + p^a S_2) \equiv 0 \quad (\mathrm{mod}\ p^{c+1})$$
$$p^c \nabla(3\gamma S_2 + 2p^a S_3)\cdot \underline{u} + (3\gamma S_2 + 2p^a S_3) \equiv 0 \quad (\mathrm{mod}\ p^{c+1})$$

where $S_j = S_j(y_1, y_2, y_3, y_4)$.
Since (y_1, y_2, y_3, y_4) is a solution, this is equivalent to solving

$$\nabla(2\gamma S_1 + p^a S_2)\cdot \underline{u} \equiv T_1 \quad (\mathrm{mod}\ p)$$
$$\nabla(3\gamma S_2 + 2p^a S_3)\cdot \underline{u} \equiv T_2 \quad (\mathrm{mod}\ p)$$

$\Longleftrightarrow$

$$\cancel{2\gamma}\ \nabla S_1 \cdot \underline{u} \equiv T_1 \quad (\mathrm{mod}\ p)$$
$$\cancel{3\gamma}\ \nabla S_2 \cdot \underline{u} \equiv T_2 \quad (\mathrm{mod}\ p) \qquad (16.11)$$

Since $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field this is the number of solutions $\underline{u} = (u_1, u_2, u_3, u_4) \in \mathbb{F}_p^4$ satisfying (16.11). Note that $\nabla S_1 = (1, 1, -1, -1)$

$$\nabla S_2 = 2\cdot(y_1, y_2, -y_3, -y_4)$$

thus if (y_1, y_2, y_3, y_4) is non-singular, then ∇S_1 and ∇S_2 are linearly independent in $\mathbb{F}_p^4$

$\Rightarrow$ # solutions to (16.11) $\leq p^2$.

$\Rightarrow$ # non-sing sol's $(\mathrm{mod}\ p^{c+1}) \leq p^2 \cdot$ # solutions $(\mathrm{mod}\ p^c)$ $\Rightarrow$ ↙

$\Rightarrow$ # non-sing sol's $\leq 2p^{2c}$