Мы φ — М: (1) $|A| < q^{1-\delta_1}$ (2) $\forall q_1 \mid q$, $q_1 > q^{\delta_1/3} = q^{\tau}$ имеет $|\pi_{q_1}(A)| > q_1^{\delta_2}$
$A \subseteq \mathbb{Z}_q$ $\Rightarrow$ для $K(A) := |A+A| + |AA|$ имеем $K > q^{\delta_3} = q^{\delta_3(\delta_1,\delta_2)}$, $\delta_3 > 0$ $\boxed{\delta_1 \le \delta_2}$
В прошлый раз мы для л. (не л'): $\exists q_1 \mid q$, $q_1 > q^{\delta_1/2}$ т. что $\pi_{q_1}(r_1 A^{r_1}) = \mathbb{Z}_{q_1}$
где $r_1 = r_1(\delta_1)$. Кроме того, мы д-ли, что можно сч., что $A \in \mathbb{Z}_{q_1}$ при
этом $\delta_2 \to \delta_2/2$ и $r \to 2r$ $\Rightarrow$ по л. ВКТ мы выведем, что у л' $\exists B \subset A'$
т. что $|B| \gg_K |A|$ и $|eBe| \ll_{K,\varepsilon} |B|$ Отсюда $\boxed{\text{л и л' — повторить}}$
$q_1 = |r_1 A^{r_1}| \ll_{K,\varepsilon} |A| \ll_{K,\varepsilon} q^{1-\delta_1}$ $\Rightarrow$ q_1 мало и, стало, для $q = q_1 q_1'$ имеем $q_1' > q^{\delta_1/2}$,
иначе $K \gg_{q^\varepsilon} \varepsilon$. По л' (не л.) $\exists q_1'' \mid q_1'$, $q_1'' > (q_1')^{\delta_2/2}$ и $\pi_{q_1''}(r_1 A^{r_1}) = \mathbb{Z}_{q_1''}$
Здесь мы пользуемся тем, что $\delta_1/r > \delta_1/3$. Имеем $(q_1'', q_1) = 1$
Была л. о 2-х проекциях: $q_1 \mid q$, $q_2 \mid q/q_1$, $S \subseteq \mathbb{Z}_q$ и $\pi_{q_1}(S) = \mathbb{Z}_{q_1}$,
$\pi_{q_2}(S) = \mathbb{Z}_{q_2}$ $\Rightarrow$ $\exists Q \mid q_1 q_2$ т. что $Q > q_1 q_2^{r_2 \cdot 10^{-4}}$ и $\pi_Q(4000 S^2) = \mathbb{Z}_Q$
Т.о. у нас $q_1 = q_1$ и $q_2 = q_1''$, $S = r_1 A^{r_1}$ $\Rightarrow$ $\exists Q = Q_1 > q_1 \left(\frac{q_1}{q_1''}\right)^{r_1 \cdot 10^{-4}} >$
$> q_1 \left(\frac{q_1}{q_1}\right)^{\frac{\delta_1\delta_2}{80000}}$ т.к. $q_1'' > (q_1')^{\delta_2/2} > (q^{\delta_1/2})^{\delta_2/2} = q^{\frac{\delta_1\delta_2}{4}}$ (можно чуть лучше)
и $\pi_{Q_1}(4000 S^2) = \mathbb{Z}_{Q_1}$. Имеем $4000 S^2 = 4000 (r_1 A^{r_1})^2 \le 4000 r_1^2 A^{2r_1} = r_2 A^{r_2}$, $r_2 = 4000 r_1^2$
Т.о. мы начали с (q_1, q_1'') и перешли к $(Q_1, \tilde{q}_1'')$, где $Q_1 > q_1 \left(\frac{q_1}{q_1}\right)^{\frac{\delta_1\delta_2}{10000}}$
Дем итеративно (Q_i, q_i'') и $Q_i > Q_i \left(\frac{q}{Q_{i-1}}\right)^{\frac{\delta_1\delta_2}{10000}}$ до тех пор пока
$Q_i > q^{1-\delta_1/2}$ $\Rightarrow$ $\pi_{Q_i}(r_{i+1} A^{r_{i+1}}) = \mathbb{Z}_{Q_i}$ $\Rightarrow$ $|Q_i| = |r_{i+1} A^{r_{i+1}}| \ll_{K, r_i} |A| \ll_{K, r_i} q^{1-\delta_1}$ $\Rightarrow$ все. ■
$\boxed{\text{Т. в } SL_2(\mathbb{Z}/q\mathbb{Z}) \text{ — повторить}}$

Л. $\exists p \in \mathbb{Z}$, $g, h \in SL_2(\mathbb{F}_p)$ без общ. собств. векторов под π_p. Тогда отобр.
$x \to (\operatorname{tr} x, \operatorname{tr} gx, \operatorname{tr} hx)$ им. кратность ≤ 2 $(x \in SL_2(\mathbb{F}_p))$ т.е. нет с.в.:
◀ 1) $\exists$ g-рег. $\Rightarrow$ он диаг. $g = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ и $h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ ($\lambda \ne \pm 1$ и $\beta, \gamma \not\equiv 0 (p)$)
Для $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ им. $\operatorname{tr} x = a + d$, $\operatorname{tr} gx = \lambda a + \lambda^{-1} d$ и
$\operatorname{tr} hx = \alpha a + \beta c + \gamma b + \delta d$ $\Rightarrow$ из первых двух ур-й выраж. a, d и т.к.
$ad - bc = 1$, то из 3-го ур. имеем (если $b = 0$, то из 3-го ур. (+ пох.))
$(\operatorname{tr} hx - \alpha a - \delta d) b = b(\beta c + \gamma b) = \beta(ad - 1) + \gamma b^2$ $\Rightarrow$ b удов. кв. ур-ю
2) $\exists$ $\operatorname{tr} g = \pm 2$ $\Rightarrow$ в нек. базисе $g = \begin{pmatrix} \pm 1 & B \\ 0 & \pm 1 \end{pmatrix}$, $h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ и $B \ne 0$, $\gamma \ne 0$ т.к. нет с.в.
Имеем $\operatorname{tr}(gx) = \pm(a + d) + Bc = \pm \operatorname{tr} x + Bc$ $\Rightarrow$ c находим одн.
$(\operatorname{tr} hx - \beta c - \alpha a - \delta(\operatorname{tr} x - a))c = \gamma c^2 = \gamma(ad - 1) = \gamma(a(\operatorname{tr} x - a) - 1)$
$\Rightarrow$ a удов. кв. ур-ю $\Rightarrow$ все. ■

Сл. $\exists g, h \in SL_2(\mathbb{Z}/q\mathbb{Z})$ и $\exists \forall p \mid q$, $p \in [J]$ матр. $\pi_p(g)$, $\pi_p(h)$ не им. общих с.в. Тогда отобр. $SL_2(\mathbb{Z}/q\mathbb{Z}) \to (\mathbb{Z}/q\mathbb{Z})^3$ $x \mapsto (\operatorname{tr} x, \operatorname{tr} gx, \operatorname{tr} hx)$
им. кратность $\le 2^{|J|}$.
В частности, $|\operatorname{tr} A| + |\operatorname{tr}(gA)| + |\operatorname{tr}(hA)| \gg_{|J|} |A|^{1/3}$ — такое слабое сл. в духе Larsen-Pink

Сл. $\exists g, h \in SL_2(\mathbb{Z}/q\mathbb{Z})$ и для нек. τ вып.
$\gcd(q, \operatorname{tr}(g h g^{-1} h^{-1}) - 2) < q^{\tau}$. Тогда $\forall A \subseteq SL_2(\mathbb{Z}/q\mathbb{Z})$ имеем
$|\operatorname{tr}(A)| + |\operatorname{tr}(gA)| + |\operatorname{tr}(hA)| \gg_{|J|} q^{-\tau} |A|^{1/3}$
◀ $\exists q_1 := \gcd(q, \operatorname{tr}[g, h] - 2) < q^{\tau}$ — по усл. и $q' = q/q_1$. Т.о. $\forall p \mid q'$
вектора $\pi_p(g), \pi_p(h) \in SL_2(\mathbb{F}_p)$ не им. общих с. векторов
Д-но, иначе $gv = \lambda v$, $hv = \mu v$ $\Rightarrow$ $\lambda^{-1} v = g^{-1} v$, $\mu^{-1} v = h^{-1} v$ ($\lambda \ne 0$ т.к.
$g, h \in SL_2(\mathbb{F}_p)$ не д. они невырожд.). Здесь $g = \pi_p(g)$, $h = \pi_p(h)$. Тогда
для $g^{-1} h^{-1} v = v$ $\Rightarrow$ $\operatorname{tr}[g, h] \equiv 2 (p)$, но у q' и $\operatorname{tr}[g, h] - 2$ нет общих
дел. по опр. q_1 $\Rightarrow$ все. Т.о. по предыд. сл-ю, получ.
$|\operatorname{tr} A| + |\operatorname{tr}(gA)| + |\operatorname{tr}(hA)| \ge \operatorname{tr} |\pi_{q'}(A)| + \ldots \gg_{|J|} |\pi_{q'}(A)|^{1/3} \gg_{|J|} q^{-\tau} |A|^{1/3}$ ■