Д-во т. Helfgott. $K = |A^3|/|A|$, $|A| \le p^{5/2}$ — от. тож и $\exists g$ — рег. $\Leftrightarrow$ $\mathrm{tr}\, g = 0, \pm 2$

По л. 3 $A^{-1}A = A^2$ сод. рег. эл-т, иначе $K \gg |A|^{2/3}$ и все р-но. (involved)

$\exists T_0 \ni g$ — наш тор. Рассмотрим все торы $a T_0 a^{-1}$, $a \in A$, вкл. нед. вклю-(выполненный) центрами или нет. Если выполн., то слова сопр. эл-ми из A. И т.д. По усл. $\langle A \rangle = G$, то либо $\boxed{\text{сущ. нед. т. вкл., если } \exists g \in A^2 \cap T\text{-рег.}}$

1) $\exists$ тор T вкл. в A, но для нек. $h \in A$ $T' = hTh^{-1}$ не вкл. в A

2) $\forall g \in G$ gTg^{-1} включен в A.

Первый случай $\exists g \in A^{-1}A = A^2 \in T \Rightarrow g' = hgh^{-1}$ — регулярный и включен в A^2 (не A) т.к. T' не включен, то $a \to a g' a^{-1}$ — инъекция, ибо иначе $a g' a^{-1} = b g' b^{-1} \Rightarrow b^{-1}a$ комм. с $g' \Rightarrow b^{-1}a \in T'$ (тор, сод. g') $\Rightarrow$ $\Rightarrow \mathrm{tr}(b^{-1}a) = \mathrm{tr}(T') \ne 0, \pm 2$, т.е. $b^{-1}a$ рег. Иными словами, по л. 6.

$|A| \le |A^6 \cap C_{\mathrm{tr}(g)}| \le [\text{л. } 6] \le K^{\frac{20}{3}} |A|^{2/3} + K^6 |A|^{1/3} \Rightarrow K \ge |A|^{1/20}$ — это противоречит тому, что

Второй случай $\forall$ эл-т A^2A прин. какому-то тору hT_0h^{-1}, $h \in G$

Отсюда $K|A| \ge |A^2| \ge \sum |A^2A \cap hT_0h^{-1}| \gg$ [было раньше] $\gg$ $\oplus$ л. 6 сложат эл. л.

$\gg p^2 \frac{|A|}{K^4 \text{ т.к. } A^2 \cap T_0 \text{ сод. рег. эл-т}} \gg p^2 \frac{|A|^2}{K^4 |A|^{2/3}} \to |A^4 \cap C_\tau|$ $h \in G/N(T_0)$ и, значит, $K \gg p^2 |A|^{2/3} \gg [|A| \le p^{5/2}]$

$\gg |A|^{2/3 + 4/5} \Rightarrow K \gg |A|^{\frac{17}{15}} \gg |A|^{1/20}$ ■

Sum-prod. в $\mathbb{F}_p$ ($\Leftrightarrow$ " $\forall A$, $|A| \ge p^{\varepsilon} \Rightarrow \exists n = n(\varepsilon)$ и $A^n = \mathbb{F}_p$ (обратно — нер. проблемы)

Сл-е (Бургейн) $\sum e_p(x_1 \dots x_n) \le \prod_{j=1}^{n} |A_j| \cdot p^{-\delta}$, $\delta = \delta(\varepsilon)$ и $|A_j| > p^{\varepsilon}$ $\prod |A_j| > p^{1+\varepsilon}$

Второе на вып. ответ. если $n \ge 2/\varepsilon$, напр. (ш. д-л, что если вып. не усл., то т.е. не надо)

где $\forall \tau > 0$ $\exists r = r(\tau)$, что для $\forall |A_{s,s'}| > p^{\tau}$, $s, s' \le r$ имеет место

$\sum_{s=1}^{r} \prod_{s'=1}^{r} A_{s,s'} = \mathbb{F}_p$, где $\forall y = \sum_{s=1}^{r} x_{s,1} \dots x_{s,r}$ $\forall y \in \mathbb{F}_p$ $\boxed{\text{Списать форм. sum-prod.}}$

▲ Надо д-ть, что $\frac{1}{p} \sum_{a \in \mathbb{F}_p} \sum_{x_{s,s'} \in A_{s,s'}} e_p\left(a\left(y - \sum_{s=1}^{r} x_{s,1} \dots x_{s,r}\right)\right) - \frac{1}{p} \prod_{s,s'=1}^{r} |A_{s,s'}| +$

$+ \prod_{s,s'=1}^{r} |A_{s,s'}| p^{-\delta(\tau) r} > 0$ для доф. δ. r. ■

Вообще, если $|A+A| + |AA| \le K|A|$, то по Рейнгольде $\forall \ell$ $|\ell A| \le K^{\ell}|A|$, $A^{\ell} \le K^{\ell}|A|$

Более того, (это из ВКТ) $\exists A' \subseteq A$, $|A'| \ge |A|/K^2$ и $|\ell(A')| < K^{C(\ell)}|A'|$

Л. $\exists A \subseteq \mathbb{Z}_q$ и $\forall q_1 | q$, $z \in \mathbb{Z}_{q_1}$ вып. $\#\{x \in A \mid \pi_{q_1}(x) = z\} \le \frac{|A|}{q_1^{1/2}}$ $\Rightarrow$ $\boxed{A \subset \mathbb{Z}_q^n}$

$\Rightarrow \exists n = n(C)$ т, что $\mathbb{Z}_q = nA^2$ (для $q \notin P$, $|A| \gg p^{1/2} \Rightarrow |A^2 + A^2| > p/2 \Rightarrow 4A^2 = \mathbb{F}_p$)

В част. если $|A| / q_1^{1/20} \Rightarrow \mathbb{Z}_q = 100 A^2$.

▲ $\frac{1}{q} \sum_{z \in \mathbb{Z}_q} \left|\sum_{x,y \in A} e_q(zxy)\right|^n e(-z\lambda) = \frac{|A|^m}{q} - \frac{1}{q} \sum_{q_1 | q, q_1 > 1} \sum_{z \in \mathbb{Z}_{q_1}^*} \left|\sum_{x,y \in A} e_{q_1}(zxy)\right|^n > 0$ хотим

Д-во, $\forall z \in [1, q-1]$ имеет вид $z = d z_1$, $(z_1, q) = 1$. Далее, $\forall z \in \mathbb{Z}_m^*$

$\Rightarrow$ сокращаем и для $q_1 = q/d$ имеем эту сумму.

$\sum_{x,y \in \mathbb{Z}_m} f(x) g(y) e_m(xyz) \le \|f\|_{L_2(\mathbb{Z}_m)} \|g\|_{L_2(\mathbb{Z}_m)} \Rightarrow \sigma_{q_1}(z) \le \|\pi\|_2^2 \sqrt{q_1}$ и

т.к. $\|\pi_{q_1}\|_\infty \le \frac{|A|}{q_1^{1/2}cc}$, то $\sigma > \frac{|A|^{2n}}{q} - \frac{1}{q} \sum_{q_1 | q, q_1 > 1} \frac{|A|^{2n}}{q_1^{n c}} e(q_1) \le [nc \gg 1] > 0$ ■ (напр. $nc > 5$)

Л. $\exists q$ — св. от кв. и $A \subseteq \mathbb{Z}_q$, $|A| > q^{1/5} \Rightarrow \exists q' | q$ т, что $q' > q^{\frac{20}{5}} = q^{4/9}$ и

$\pi_{q'}(100 A^2) = \mathbb{Z}_{q'}$ (для самого $\mathbb{Z}_q$ это, конечно, совсем неверно).

▲ Ясно, что $\exists q_1 | q$ и $z_1 \in \mathbb{Z}_{q_1}$ т, что для $A_1 = \{a \in A \mid \pi_{q_1}(a) = z_1\}$ вып.

$|A_1| > |A| / q_1^{1/20} \ge \delta q / q_1^{1/20}$ (напомним, что $\delta = q^{-1/5}$). Всегда $|\pi_{q_1}(A)| \le \frac{q}{q_1}$ $\Rightarrow$

$\frac{q}{q_1} \ge \delta q / q_1^{1/20} \Rightarrow$ [посчитать] $\Rightarrow q_1 < \delta^{-20/9} = q^{4/9}$. Заметим $q \to q/q_1$ и $A \to A' = \pi_{q_1}(A_1)$

Если нельзя прим. предыд. лемму, то $\exists q_2 | q/q_1$ и $z_2 \in \mathbb{Z}_{q_2}$ т, что $|A_2| > q_2^{-1/20} |A_1|$, где

$A_1 = \{x \in A_2 \mid \pi_{q_2}(x) = z_2\}$ $\Rightarrow$ по инд. $\exists q_1, \dots, q_s$ — делители q и мы имеем

$q/(q_1 \cdot \dots \cdot q_s) \ge |A_s| \ge \delta q (q_1 \cdot \dots \cdot q_s)^{-1/20} \Rightarrow$ как раньше $\omega < \delta^{-20/9} = q^{4/9} \Rightarrow$ процесс завершится ■