

Еще раз: (1)  $|A| < q^{1-\delta_1} \cdot |\pi_{q_1}(A)| > q^{\delta_2}$  где  $\forall q_1 |q, q_1 > q^{\delta_3} \Rightarrow |A+A| \leq |A+A| \leq K|A|$  и  
 потому  $q - \text{то } \exists q' | q, q' > q^{1-\delta_1} \in B \subseteq A, |B| > |A| q^{\delta_2}$  (тогда  $K \geq q^{\delta_3} = q^{\delta_1 \delta_2}$ )  
 $\pi_{q'}(B) \subseteq \mathbb{Z}_q^2$  (т.е. мы сводим все к  $\mathbb{Z}_q^2$ ) тогда (1) и (2) ред. с  $\delta_2 \rightarrow \delta_1/2, \delta_2 \rightarrow \delta_2$  и  
 что  $\forall h \in \mathbb{Z}_q \setminus \{0\} \pi_{q'}(B) \subseteq \pi_{q'}(B)$  (конечно, мы будем иметь л. БКТ)

Примером инт.  $\exists A_0 = A, q_0 = 1, q_0' = 2$  (диффуз  $(A_i, q_i, q_i')$ )  
 $A_i' = \{x \in A_0 \mid \pi_{q_i}(x) \neq 0\}$ . Если  $|A_i'| \geq \frac{q_i}{q_i'} |A_0|$ , то  $A_i = A_i'$  (переходим к новому)  
 и  $q_i' = q_0' p_i, q_i'' = q_0''$  (т.е. год.  $p_i \in \mathbb{Z}_q^2$ )  
 Если  $|A_i'| < \frac{q_i}{q_i'} |A_0|$ , то  $\exists A_i = A_0$  (т.е. не мен.  $A$ ),  $q_i' = q_0', q_i'' = q_0' p_i$  (т.е. год.  $p_i \in \mathbb{Z}_q^2$ )  
 $A_i' \cap A_i = \{x \in A_i \mid \pi_{q_i p_i}(x) \neq 0\}$  и (а)  $A_{i+1} = A_i', q_{i+1}' = q_i' p_i, q_{i+1}'' = q_i''$   
 (б)  $A_{i+1} = A_i, q_{i+1}' = q_i', q_{i+1}'' = q_i'' p_i$

Тогда, что такое  $\exists$  малое  $\exists A' \in A \subseteq \mathbb{Z}_q^2, \pi_{q'}(A') \subseteq \mathbb{Z}_q^2, \pi_{q'}(A') \neq \emptyset$  и  $|\pi_{q'}(A')| \geq |A'|$   
 $\Rightarrow$  с помощью все ОК. Имеем  $q'' < q^{\delta_2}$  ( $\Rightarrow q' \geq q/q'' > q^{1-\delta_2}$ ) тогда  $\exists \delta_2 \geq \delta_1/2$   
 в пред. случае (2) есть  $|\pi_{q''}(A)| \geq (q'')^{\delta_2} > q^{\delta_2 \delta_2}$  и  
 $|A+A| \geq |A+A'| \geq |A|$  (по лемме)  $B = A' \cup A \subseteq A$   $|B| \geq |A'| |\pi_{q'}(A)| \gg |A| q^{\delta_2}$  и все  $q - \text{то}$ .  
 (иногда, что  $A$  не имеет  $\Rightarrow A'$ )  $q' \geq q''$   $\pi_{q'}(A') \neq \emptyset$  (1) - ред

По л. БКТ  $\exists \tilde{A} \in A, |\tilde{A}| \gg |A|$  и  $|e \tilde{A}^e| \leq |A|$ . Останется убедиться (2)  
 $\exists \exists q_1 > (q')^{2\delta_2} > (q^{1-\delta_1})^{2\delta_2} > q^{2\delta_1 \delta_2}$   $q_1 | q' \in \pi_{q'}(A) \subseteq \mathbb{Z}_q^2 \Rightarrow$  по ин. Диффуз  
 $\exists x_0 \in \mathbb{Z}_{q_1}$  и  $A_0 \subseteq A$  т.е.  $\pi_{q_1}(A_0) = \{x_0\}$  и  $|A_0| > q_1^{-\delta_1/2} |A|$ . Как и раньше  
 $|A+A| \geq |A+A_0| \geq |\pi_{q_1}(A)| |A_0| \geq |A| q_1^{\delta_2} q_1^{-\delta_1/2} |A| \gg |A|$  все  $q - \text{то}$ .

Л. (Kneser)  $A \subseteq G, |A+A| \leq \frac{3}{2} |A| \Rightarrow \exists A \subseteq \times H$  ( $H = A+A$ ),  $|H| \leq \frac{3}{2} |A|, H \subseteq G$   
 П.  $A = \{0, 1\}, |A+A| = \frac{3}{2} |A|$  и нигде в  $\mathbb{Z}$  нет (кроме  $H = \{0, 1\}$ )

Т. (BSZG)  $A \subseteq \Gamma$ -ад.  $E(A) \geq |A|^3/K \Rightarrow \exists A' \subseteq A, |A'| \gg |A|^3/K, |A'+A'| \leq K^c |A'|$   
 $A+A = \{a+b \mid (a,b) \in G \subseteq A \times A\} \Rightarrow$  из  $E(A) \geq |A|^3/K$  можно построить

$G = \{a, b \in A \mid a-b \in P\}, P$  - минимальное разность  $P = \{s : \sum_{A \times A}(s) \geq \frac{|A|^3}{K}\}$   
 $E = \sum \sum \sum_A(s) \leq 2 \sum \sum_A(s) \leq 2 |A| |G| \Rightarrow |G| \geq \frac{|A|^3}{2K}$  т.е.  $\sum_{A \times A}(s) \geq \frac{|A|^3}{K}$

Т. (BSZG)  $G \subseteq A \times A, (A \subseteq \Gamma), |G| \geq |A|^3/K$  и  $|A+A| \leq K |A| \Rightarrow \exists A' \in A,$   
 $|A'| \gg |A|^3/K, |A'+A'| \leq K^c |A'|$   $\leftarrow$  форма изв. по BSZG

Т. (BSZG) где  $\text{матрица графа}$   $G \subseteq A \times A$  ( $A \subseteq \Gamma$ ),  $|G| > (1-\delta) |A|^2, \delta \leq \frac{1}{4}$   
 $\Rightarrow \exists |A'| > (1-\delta^2) |A|$  и  $|A'+A'| \leq |A+A|^4 / ((1-\delta^2) (1-2\sqrt{\delta})^2 |A|^3)$

Лемма  $|A+B| \geq |\pi_{q'}(A)| \cdot |B|$ , если  $\pi_{q'}(B) \neq \emptyset, q' | q, A, B \subseteq \mathbb{Z}_q^2$   
 $(a+b = a'+b' \Rightarrow \pi_{q'}(a) = \pi_{q'}(a') \Rightarrow$  будем разг. при  $\pi_{q'}(A)$  и  $B$ ).

Предп. (о связи группировок)  $\exists q_1 | q, q_2 | q/q_1, S \subseteq \mathbb{Z}_q$  и  $\pi_{q_1}(S) = \mathbb{Z}_{q_1},$   
 $\pi_{q_2}(S) = \mathbb{Z}_{q_2} \Rightarrow \exists Q | q_1 q_2$  т.е.  $Q > q_1 q_2^{\frac{1}{10^4}}$  и  $\pi_Q(\mathbb{Z}_{q_1 q_2}) = \mathbb{Z}_Q$

Т.к.  $\pi_{q_1}(S) = \mathbb{Z}_{q_1}$ , то  $\forall p \in \mathbb{Z}_q$   $p | q/q_1$  определит  $\psi(p) \in \mathbb{Z}_p$  т.е.  $(x, \psi_p(x)) \in \pi_{q_1}(S)$   
 и  $\text{деген. } \bullet \text{ по mod } p.$

Уб. 1. Для  $\forall p | q_1$   $\text{бон: } \#\{x, y \in \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_1} : \psi_p(x+y) \neq \psi_p(x) + \psi_p(y)\} \leq$   
 либо не  $\exists B \subseteq \mathbb{Z}_{q_1}$  т.е.  $|B| > \frac{q_1}{200}$  и  $|\psi_p(B)| = 1$ .  $\Rightarrow 10^{-4} q_1^2$

Дво.  $\exists G_+$  -  $\text{кожа} = \emptyset(1) \Rightarrow |G_+| > (1-10^{-4}) q_1^2$   $\text{и все } q - \text{то}$ .  
 $\exists A = \{(x, \psi_p(x)) : x \in \mathbb{Z}_{q_1}\}, |A| = q_1, A \subseteq \mathbb{Z}_{q_1} \times \mathbb{Z}_p \cong \mathbb{Z}_{q_1 p}$   
 $G = \{(x, \psi_p(x)), (y, \psi_p(y)) : (x, y) \in G_+\} \subseteq A \times A \Rightarrow |G| > (1-10^{-4}) |A|^2$