простую P пуб. эл-т Хелфготта: $\exists$ 0. $H(x_1, x_2, \dots, x_n) \in SL_2(\mathbb{F}_p)$ [illegible]

def $(x_1, \dots, x_n)$ [illegible] $\ge |\,\dots\,| / p^2$ [illegible]

По Безу (Шварцу) $f(x, \dots, x_n)$ или $SL(p^n)$ [illegible], если $f \not\equiv 0$

иначе $f \equiv 0$ на $SL_2(\mathbb{F}_p)^3$ только [illegible] (см. уб.)

T (Rudnev-S) $A \subseteq SL_2(\mathbb{F}_p)$, $A\,A^{-1}$ [illegible] $|A|$ [illegible]

$\Rightarrow A^3 = SL_2(\mathbb{F}_p)$ или же $|A^3| \gg |A|^{1+c}$ (Helfgott [illegible])

Разговор о росте в $Aff(\mathbb{F}_p)$ [illegible]

T. $A = \mathbb{F}_p^2$, $1 < |A| < p$ [illegible] точки [illegible] A [illegible]

$\frac{|A|+3}{2}$ раза. Напоминание. ($|A| < p \Rightarrow$ все [illegible])

Пусть $u = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, $\beta_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ [illegible] $\in SL_2(\mathbb{F}_p)$

и $\forall$ прост. в G [illegible] сопр. к U_0 [illegible]

$\forall$ рег. полупр. эл-т g сопр. в [illegible]

[illegible] $g \in SL_2(\mathbb{F}_p)$ (A группа, SL_2 [illegible] A группа)

T = split, если $T = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ и non-split, если $T = \{\,\dots\,\}$ [illegible]

$|N(T)| = 2|T|$, [illegible], в сл. split добавляется [illegible] $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, а в сл. non-split, доб. [illegible] $x^2 + ay^2 = 1$

$\forall T \le G$ ($T \ne \pm C$) имеем $|\{h T h^{-1} \mid h \in G\}| \gg p^2$

$Conj(g) = \{h g h^{-1} := g^h \mid h \in G\}$ — если g рег. полупр., то это [illegible]

Если $tr\, g = 2$ (или -2), то [illegible] $= \{1\} \cup Con\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) \cup Con\left(\begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix}\right)$ [illegible]

[illegible] прямые в G [illegible] $\ell_\gamma = \left\{\begin{pmatrix} \delta & t \\ 0 & \delta^{-1} \end{pmatrix} \mid t \in A\right\}$ [illegible]

Л.1 $A = A^{-1}$, $|AAA| = K|A| \Rightarrow \forall k \ge 3$ $|A^k| \le K^{k-2}|A|$ [illegible]

◀ $a_1 \dots a_k \to (a_1 a_2 a)(a^{-1} a_3 \dots a_k) \Rightarrow$ [illegible] ■

Л.2 $|A| \gg p^{8/3} \Rightarrow A^2 = G$ и $|AA| \ge \frac{1}{2}\min\{|G|, |A|^2/p^2\}$ [illegible] $|A| \le p^{8/3}$ [illegible]

Л.3 (escape from subvarieties) $\exists\, p \ge 5$ и $|A| > 2 \cdot 2 + 6K|A|^{1/3}$

$\Rightarrow A^2$ сор. рег. полупростой эл-т, т.е. $tr\, g \in O(\dots)$ [illegible]

◀ Нам надо избавиться от тех с $tr \in \{0, \pm 2\}$ [illegible] $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Меняя базис (= ф-я сопр.), счит., что, [illegible]

По Л.4 $|A_1| \le 8K|A|^{2/3} \Rightarrow$ [illegible] $\exists A_1 = A \setminus A_0$ [illegible]

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & at+b \\ c & ct+d \end{pmatrix} \Rightarrow tr(gu) = a + d + tc$ и $tr(gu^2) = a + d + 2tc$ [illegible]

$\Rightarrow$ для $p \ne 2, 3$ имеем $a + d = 0 \Rightarrow tr(A_1) = 0$ [illegible] $t \ne 0$

Сопрягая, счит., что $w \in A_1$ и если $|A_1| > 4$, то $\exists g \in A_1$, $g = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ [illegible]

$\Rightarrow a \ne 0$. Считаем $tr(gw) = c - b + S \Rightarrow (1)\ c - b = \pm 2$ $(2)\ b = c$ [illegible]

$(1)\ -a^2 - bc = -a^2 - b(\pm 2 + b) = 1 \Leftrightarrow (b \pm 1)^2 = -a^2 \Rightarrow$ 1-на [illegible]

$w \to x := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. Снова сопрягая, счит., что $x \in A_2$ и $\exists g = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in A_2$ [illegible]

Имеем $tr(gx) = 2ia + S \Rightarrow a = \pm 1$ [illegible] det $= 1$, то $bc = 0$ [illegible]

матр. [illegible] по $|A_1|$ [illegible] $8K|A|^{2/3}$ [illegible] $\Rightarrow (1)$

Для (2) имеем $\begin{pmatrix} a & b \\ b & -a \end{pmatrix}$, $a \ne 0$, $a^2 + b^2 = -1$ — „окружность" [illegible]

[illegible] $\in \{0, \pm 1\}$ [illegible] $\{\pm(a, b), \pm(-b, a)\}$ — 4 [illegible] ■

Л.4 $\exists A \le G$, $|A^3| = K|A| \Rightarrow |\ell_\gamma \cap A^2| \le 2|A^{8k+2}|^{1/3} \le 2K^4|A|^{1/3}$

◀ $\exists h = (ab|cd)$, $c \ne 0$ — нек. эл-т из A. Расм. отобр.

$\psi: \ell_\gamma \times \ell_\gamma^0 \times \ell_\gamma \to G$; $\psi(g_1, g_2, g_3) = g_1 h g_2 h^{-1} g_3$ и $\ell_\gamma^0 = \ell_\gamma \setminus 1$ [illegible]

Если ψ — инъект. $\Rightarrow$ все, ибо [illegible] $\in A^{8k+2}$ и [illegible]

$h g_2 h^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \delta & t_2 \\ 0 & \delta^{-1} \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} * & * \\ \delta\bar{\delta}cd - c^2 t_2 & * \end{pmatrix}$ [illegible], $\bar{\delta} = 1 - \delta^{-2}$

эл-т $\delta\bar{\delta}cd - c^2 t_2 \ne 0 \Leftrightarrow t_2 \ne \delta\bar{\delta}c^{-1}d$ [illegible] — [illegible] из ℓ_γ.