105. Алгоритм AKS. Определение и неравенства, связывающие $p, r, \log_2 n, t$, группы G, $\mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $|\mathcal{G}| \le n^{\sqrt{t}}$ при $n \ne p^k$.

Неравенства: $p > r > \log_2^2 n$, $\varphi(r) \ge |G| = t > \log_2^2 n$, $\deg h(x) > \operatorname{ord}_r p > 1$

Лемма 2: $|\mathcal{G}| \le n^{\sqrt{t}}$ при $n \ne p^k$

▲ Рассмотрим в множестве I все элементы с $0 \le i, j \le [\sqrt{t}]$. Всего таких чисел $([\sqrt{t}] + 1)^2 > t$ чисел $\Rightarrow$ среди них $\exists m_1, m_2$ $(m_1 > m_2)$, такие что $m_1 \equiv m_2 \pmod r$ (так как в группе G всего t различных элементов). Тогда

$$x^{m_1} = x^{m_2} \pmod{x^r - 1, p}, \text{ так как } (x^{m_1 - m_2} - 1)x^{m_2} \,\vdots\, x^r - 1 \text{ (см. замечание в билете 84)}$$

Рассмотрим произвольное $f \in \mathcal{G}$. По построению $\mathcal{G}$ он перестановочен с m_1 и m_2. Следовательно, так как $h(x) \mid x^r - 1$

$$(f(x))^{m_1} = f(x^{m_1}) = f(x^{m_2}) = (f(x))^{m_2} \pmod{h(x), p}$$

Уравнение $(f(x))^{m_1} = (f(x))^{m_2}$ имеет $\le \max\{m_1, m_2\} = m_1$ корней (уравнение относительно $f(x)$). Так как это выполнено для любого $f \in \mathcal{G}$, то $|\mathcal{G}| \le m_1$.

По построению $m_1 = \left(\frac{n}{p}\right)^i \cdot p^j$, $0 \le i, j \le [\sqrt{t}] \Rightarrow |\mathcal{G}| \le m_1 \le n^{\sqrt{t}}$ ■