

**104. Алгоритм АКС. Определение и неравенства, связывающие параметры  $p, r, \log_2 n, t$ , группы  $G, \mathcal{G}$ , многочлена  $h(x)$  (б/д). Неравенство  $|\mathcal{G}| > C_{t+l}^{t-1}$ .**

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

**Утверждение (б/д):** У многочлена степени  $k$  над любым полем  $\leq k$  корней в поле.

**Лемма 1:**  $|\mathcal{G}| \geq C_{t+l}^{t-1}$

▲ Докажем, что если  $f(x), g(x)$  - многочлены из  $P$  (см. билет 83) степени  $\leq t-1$ , то они не совпадают в  $\mathcal{G}$ . Пусть  $m \in G$

$$f(x^m) = (f(x))^m \pmod{x^r - 1, p}$$

$$f(x^m) = (f(x))^m \pmod{h(x), p} \text{ (перешли к делителю)}$$

$$g(x^m) = (g(x))^m \pmod{h(x), p}$$

Предположим  $f = g \pmod{h(x), p}$ . Тогда  $f(x^m) = g(x^m) \pmod{h(x), p}$ . Рассмотрим многочлен  $f - g$ .  $\deg(f - g) \leq t-1$ , а количество корней равно  $|G| = t$  (так как подходят все  $x^m$ ) - противоречие  $\Rightarrow f$  и  $g$  различны в  $\mathcal{G}$

Рассмотрим в множестве  $P$  многочлены  $x, x+1, \dots, x+l$  - не равны по модулю  $h(x)$ , так как  $\deg h(x) > 1$ . Покажем, что они не совпадают и по модулю  $p$ . Так как  $\log_2^2 n \leq r \Rightarrow \log_2 n \leq \sqrt{r}$

$$l = \sqrt{\varphi(r)} \log_2 n < \sqrt{r} \log_2 n \leq r \leq p$$

Найдем количество многочленов из  $P$  степени  $\leq t-1$  (они все точно различные в  $\mathcal{G}$  по доказанному выше). Выбираем из нашего списка многочленов степени  $1 \dots t-1$  штуку с повторениями. Получаем

$$\overline{C}_{l+1}^{t-1} = C_{t+l}^{t-1}$$

Так как все эти многочлены лежат в  $\mathcal{G} \Rightarrow |\mathcal{G}| \geq C_{t+l}^{t-1}$  ■