83. Алгоритм AKS. Определение и неравенства, связывающие числа $p, r, \log_2 n$ (б/д). Определение множеств I, P. Определение группы G, неравенство $|G| > \log_2^2 n$. Утверждения о делителе $h(X)$ многочлена $X^r - 1$ (б/д). Группа $\mathcal{G}$.

Замечание: Среди простых делителей числа n точно найдется число p с $\operatorname{ord}_r p > 1$ (так как $\operatorname{ord}_r n > \log_2^2 n > 1$).

Неравенство: $p > r > \log_2^2 n$

Определение:

$$I = \{\left(\frac{n}{p}\right)^i p^j;\ i, j \geq 0\}$$

$$P = \{\prod_{a=0}^{l} (x+a)^{e_a};\ e_a \geq 0\}$$

Рассмотрим в I вычеты по модулю r. Получаем группу G. Обозначим $t := |G|$.

Неравенство: $t \geq \operatorname{ord}_r n$ (так как в I есть элементы вида n^i, когда $i = j$) $> \log_2^2 n$ (по построению r) $\Rightarrow |G| > \log_2^2 n$

Утверждение: Пусть $h(x)$ - неприводимый над $\mathbb{Z}_p$ делитель $x^r - 1$. Тогда $\deg h(x) = \operatorname{ord}_r p > 1$

Утверждение: Рассмотрим классы многочленов равные по модулю $(h(x), p)$. Множество таких классов эквивалентности образует поле F, а в пересечении с P дает мультипликативную группу $\mathcal{G} \subset F^*$