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

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

1. Если $a > b$, то $C_a^k > C_b^k \ \forall k$
2. Если $\frac{n}{2} > a > b$, то $C_n^a > C_n^b$

▲ 1. В переходе с неравенством добавляем $b - a < 0$ к каждому множителю

$$C_a^k = \frac{a!}{k!\,(a-k)!} = \frac{(a-k+1)\cdot \ldots \cdot a}{k!} > \frac{(b-k+1)\cdot \ldots \cdot b}{k!} = \frac{b!}{k!\,(b-k)!} = C_b^k$$

2. В переходе с неравенством добавляем $a - b > 0$ к каждому множителю

$$C_n^a = \frac{n!}{a!\,(n-a)!} = \frac{n!}{a!\,b!\,(b+1)\cdot \ldots \cdot (n-a)} > \frac{n!}{a!\,b!\,(a+1)\cdot \ldots \cdot (n-b)} = \frac{n!}{b!\,(n-b)!}$$

Утверждение 2: $C_{2x+1}^x \geq 2^{x+1}$

▲ 1. База: $x = 2$ (при $x = 1$ неверно, но нам важно на больших) $C_5^2 = 10 \geq 2^3 = 8$

2. Переход: пусть верно для x. Докажем для $x + 1$

$$C_{2x+3}^{x+1} = \frac{(2x+3)!}{(x+1)!\,(x+2)!} = \frac{(2x+1)!\,(2x+2)(2x+3)}{(x+1)!\,x!\,(x+1)(x+2)} = C_{2x+1}^x \cdot \frac{(2x+2)(2x+3)}{(x+1)(x+2)} =$$

$$= 2C_{2x+1}^x \frac{2x+3}{x+2} > 2C_{2x+1}^x \geq 2^{x+2} \blacksquare$$

Лемма 3: $C_{t+l}^{t-1} > n^{\sqrt{t}}$
▲ Так как $t > \log_2^2 n \Rightarrow t > \sqrt{t}\log_2 n \Rightarrow t \geq [\sqrt{t}\log_2 n] + 1$. $l = \sqrt{\varphi(r)}\log_2 n \geq \sqrt{t}\log_2 n$.

$$C_{t+l}^{t-1} \geq C_{[\sqrt{t}\log_2 n]+1+l}^{[\sqrt{t}\log_2 n]} \geq C_{2[\sqrt{t}\log_2 n]+1}^{[\sqrt{t}\log_2 n]} \geq 2^{[\sqrt{t}\log_2 n]+1} > 2^{\sqrt{t}\log_2 n} = n^{\sqrt{t}} \blacksquare$$

Так как верны все леммы 1-3 из билетов 104-106, то $n = p^k$, но если $k > 1$, то мы бы остановились еще на шаге 1 нашего алгоритма $\Rightarrow n = p \Rightarrow$ последний шаг алгоритма корректен