103. Алгоритм AKS. Верхняя оценка на r: вывод из утверждения о нижней оценке $[1, 2, \ldots, n]$.

Лемма: $r \le \max\{3, \lceil \log_2^5 n \rceil\}$

▲ Пусть $n \ge 3 \Rightarrow B = \lceil \log_2^5 n \rceil \ge 10 > 7 \Rightarrow$ можем применять оценку на $[1, \ldots, B]$ из билета 80, то есть $[1, \ldots, B] \ge 2^B$

Рассмотрим

$$S = n^{[\log_2 B]} \prod_{i=1}^{\left[\log_2^2 n\right]} (n^i - 1)$$

Возьмем минимальное r, такое что r не делит $S \Rightarrow n^i \not\equiv 1 \pmod{r}$ $i = 1, \ldots, [\log_2^2 n] \Rightarrow$ если $(r, n) = 1$, то $\operatorname{ord}_r n > \log_2^2 n$.

Осталось доказать, что $(r, n) = 1$ и $r \le B$. Воспользуемся тем, что $n^i - 1 < n^i$ и просуммируем степени по арифметической прогрессии.

$$S < n^{[\log_2 B]} \cdot n^{\frac{\left[\log_2^2 n\right]\left(\left[\log_2^2 n\right]+1\right)}{2}} \le n^{\log_2^4 n} = 2^{\log_2^5 n} \le 2^B$$

Во втором неравенстве мы прибавили $\frac{\log_2^4 n}{2}$ и отняли $[\log_2 B] = [\log_2 \log_2^5 n]$. Очевидно, что второе является двойным логарифмом и оно меньше первого.

Предположим, что $r > B$. Тогда по определению r S делится на все числа меньшие r, то есть $S \ge [1, \ldots, B] \ge 2^B$ - противоречие $\Rightarrow r \le B$

Пусть $r = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s} \Rightarrow k_i \le \log_2 B$, так как $r \le B$. Предположим, что $\forall i\; n \,\vdots\, p_i$. Тогда $\forall i\; n^{[\log_2 B]} \,\vdots\, p_i^{[\log_2 B]} \,\vdots\, p_i^{k_i}$ (так как $k_i \le \log_2 B$) $\Rightarrow n^{[\log_2 B]} \,\vdots\, r$ - противоречие, так как тогда $S \,\vdots\, r$. Следовательно, $\exists p_i \nmid n$. Перенумеруем p так что $p_1, \ldots, p_t$ не делят n, $p_{t+1}, \ldots, p_s$ делят n. Тогда $p_1^{k_1} \cdot \ldots \cdot p_t^{k_t} \nmid \prod_{i=1}^{\left[\log_2^2 n\right]} (n^i - 1)$, так как иначе r делит S.

Рассмотрим

$$\frac{r}{(r, n)} = \underbrace{p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}}_{\text{не делит } S} \cdot \underbrace{p_{t+1}^{k'_{t+1}} \cdot \ldots \cdot p_s^{k'_s}}_{\text{делит } S} \Rightarrow \frac{r}{(r, n)} \nmid S$$

Из того, что r выбиралось минимальным следует, что $(r, n) = 1$. Следовательно $\operatorname{ord}_r n > \log_2^2 n$ и все доказано ■