42. Описание алгоритма AKS (6 шагов). Лемма об оценке r (б/д). Оценка сложности алгоритма. Тождество $(X + a)^p = X^p + a (\bmod p)$.

Алгоритм проверки n на простоту: Agarwal, Kayal, Saxena (AKS)

1. $n = a^b, b \geq 2 \Rightarrow n$ составное
2. Ищем наименьшее r, такое что $\operatorname{ord}_r n > \log_2^2 n$
3. Если хотя бы для одного числа a из диапазона $1 \dots r$ выполнено $1 < (a, n) < n \Rightarrow n$ составное ($(a, n) :=$ НОД(a, n))
4. Если $n \leq r$, то n простое
5. Если хотя бы для одного числа a в диапазоне $1 \dots l = \sqrt{\varphi(r)} \cdot \log_2 n$ выполнено $(x+a)^n \neq x^n + a \pmod{x^r - 1, n} \Rightarrow n$ составное
6. n простое

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

1. $n = a^b \Rightarrow b \leq \log_2 n \Rightarrow$ можно перебрать бинпоиском за $\operatorname{poly}(\log_2 n)$
2. Из леммы следует, что шаг 2 можно сделать перебором за $\operatorname{poly}(\log_2 n)$
3. Перебираем числа меньше r и ищем НОД (за логарифм) $\Rightarrow$ этот шаг выполняется за $\operatorname{poly}(\log_2 n)$
4. $O(1)$
5. Всего $\operatorname{poly}(\log_2 n)$ итераций. На каждой делаем бинарное возведение в степень ($\operatorname{poly}(\log_2 n)$), как только превышаем r делим на многочлен $x^r - 1$ ($\operatorname{poly}(\log n)$, так как степень делимого $\leq 2r$, то есть у него $\operatorname{poly}(\log_2 n)$ коэффициентов)

Утверждение: $(x + a)^p = x^p + a \pmod p$
▲

$$(x+a)^p = x^p + a^p + \sum_{i=1}^{p-1} C_p^i x^{p-i} a^i$$

$a^p = a (\bmod p)$ (малая теорема Ферма), $C_p^i = 0 \pmod p$ (доказывалось в прошлом семестре) $\Rightarrow (x+a)^p = x^p + a \pmod p$ ■