# 84. Алгоритм AKS. Верхняя оценка на $r$ (б/д). Обоснование неравенства $p > r > \log_2^2 n$ для подходящего делителя $p$ числа $n$. Вывод тождества $(X+a)^{n/p} = X^{n/p} + a \pmod{X^r - 1, p}$. Определение перестановочности многочлена и числа. Утверждения о свойствах перестановочности.

**Обоснование неравенства:** Рассматриваем корректность последнего шага. Мы знаем, что $(r, n) = 1 \Rightarrow (r, p) = 1$ ($p$ - делитель $n$, который мы выбрали в билете 83). Также $p > r$, в противном случае мы бы останавились на 3 или 4 шаге алгоритма. Тогда $p > r > \varphi(r) \geq \mathrm{ord}_r\, n > \log_2^2 n$ (последнее неравенство следует из построения $r$).

**Тождество:** $(x+a)^{n/p} = x^{n/p} + a \pmod{x^r - 1, p}$

▲

$$(x+a)^p = x^p + a \pmod{x^r - 1, p} \text{ при } a = 0 \dots l \text{ (см. билет 42)}$$

$$(x+a)^n = x^n + a \pmod{x^r - 1, n} \text{ при } a = 0 \dots l \text{ (следствие того, что мы прошли шаг 5)}$$

Второе выражение так же выполняется, если мы заменим $\bmod n$ на $\bmod p$, так как $p$ - делитель $n$ (в дальнейшем будем часто переходить к делителям таким образом). Дальше все тождества рассматриваем для $a = 0 \dots l$.

Предположим, что $(x+a)^{n/p} \neq x^{n/p} + a \pmod{x^r - 1, p}$. Возведем обе части в степень $p$. Получаем $(x+a)^n \neq (x^{n/p} + a)^p \pmod{x^r - 1, p}$. По первому тождеству правая часть распишется как $x^n + a$. Получили, что $(x+a)^n \neq x^n + a \pmod{x^r - 1, p}$ - противоречие со вторым тождеством $\Rightarrow$ тождество верно ■

**Определение:** Пусть $f(x)$ - многочлен, $m$ - число. Считаем, что $f(x)$ и $m$ перестановочны, если $(f(x))^m = f(x^m) \pmod{x^r - 1, p}$

**Утверждение 1:** Если $f$ перестановочно с $m$ и $g$ перестановочно с $m$, то $f \cdot g$ перестановочно с $m$

$$\blacktriangle\ (fg(x))^m = (f(x)g(x))^m = (f(x))^m (g(x))^m = f(x^m)g(x^m) = fg(x^m)\ \blacksquare$$

**Замечание:** $x^{mr} - 1 \vdots x^r - 1$

▲

$$x^r - 1 = (x-1)(1 + x + \ldots + x^{r-1})$$

$$x^{mr} - 1 = (x-1)(1 + x + \ldots + x^{r-1} + x^{r+1} + \ldots + x^{mr-1}) =$$

$$= (x-1)(1 \cdot (1 + \ldots + x^{r-1}) + x^r(1 + \ldots + x^{r-1}) + \ldots x^{(m-1)r}(1 + \ldots + x^{r-1})) =$$

$$= (x-1)(1 + \ldots + x^{r-1})(1 + \ldots + x^{(m-1)r}) \vdots x^r - 1\ \blacksquare$$

**Утверждение 2:** Если $f$ перестановочно с $m$ и $m'$, то $f$ перестановочно с $mm'$

▲

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

Пусть $y = x^m$. Тогда

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

$y^r - 1 = x^{mr} - 1 \Rightarrow y^r - 1 \vdots x^r - 1$ (по замечанию) $\Rightarrow$ тождество верно и по модулю $x^r - 1$ (перешли к делителю). Получаем

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