A2b

№1

Мы представляем степень в двоичном виде
=> нам только надо будет совершить
$\lceil \log_2(N) \rceil$ – операций $p = p \cdot p$
далее надо совершить k умножений $r = r \cdot p$,
где k – кол-во бит $= 1$ в степени числа.
в худшем случае это тоже $\lceil \log_2(N) \rceil$ =>
=> в худшем случае $2\lceil \log_2(N) \rceil$, в лучшем $\lceil \log_2(N) \rceil + 1$.
Этот алгоритм всегда лучше наивного, т.к в наивном мы совершим $n-1$ умножений

№2

$r \cdot p^e = x^n$ – будет являться инвариантом

INIT: $r = 1$ $p = x$ $e = n$ => $1 \cdot x^n = x^n$

MNT: если e чётное, то $p = p^2$, а $e = \frac{e}{2}$, то есть p^e не изменилось т.к мы просто вынесли 2 из степени (было: p^e, стало: $(p^2)^{\frac{e}{2}}$ $(p^2)^{\frac{e}{2}} = p^{2 \cdot \frac{e}{2}} = p^e$)
Если e нечётное, то $r = r \cdot p$
Это тоже не меняет инвариант
т.к мы компенсируем потерю при целочислен. делении, умножением $\left(p^{\frac{2n+1}{2}} = p^n\right)$

TRM: $r \cdot p^e = x^n$, $e = 0$ $r = x^n$ => $x^n \cdot 1 = x^n$