Teste de Primalidade

Lucas Gomes dos Santos – 20.1.4108

a) Faça a divisão de 44 por 5 usando o algoritmo Divide(x,y) do slide 5 da aula sobre Teste de primalidade.

R:
Divide(44,5) = (8,4)
Divide(22,5) = (4,2)
Divide(11,5) = (2,1)
Divide(5,5) = (1,0)
Divide(2,5) = (0,2)
Divide(1,5) = (0,1)
Divide(0,5) = (0,0)

b) Faça a análise de complexidade da função modexp(x, y, N) do slide 7 no pior caso.

R:
Linha 1 – if y = 0 → O(n)
Linha 2 – modexp(x,[y/2], N) → O(n) na chamada recursiva para o pior caso
Linha 3 – if y is even → O(1)
Linha 4 – z^2 mod N → $O(n^2)$
Linha 6 – x * z^2 mod N → $O(n^2)$

Complexidade local = $O(n^2)$, no pior caso em que a função é chamada n vezes.
Ou seja $O(n^2)$ x n = $O(n^3)$.

c) Faça a análise de complexidade da função primality2(N) no pior caso (slide 15).

R:

(a i)^n-1 → Exponenciação → $O(n^3)$ k*$O(n^3)$
(mod N) → $O(n^2)$ $O(n^3)$
if (a i)^n-1 ≡ 1 (mod N) → O(n)
for all i = 1,… k: → O(k)