Zad 4.

środa, 9 listopada 2022 23:32

4. Niech x, k, n będą liczbami całkowitymi. Skonstuuj algorytm obliczający x^k modulo n. Algorytm powinien korzystać z wzorów: $x^{2l} = x^l \cdot x^l$, $x^{2l+1} = x \cdot x^{2l}$. Określ liczbę mnożeń wykonywanych przez ten algorytm.

```
Alg(x,k,n) →
    if k=1
        return x mod n
    else if k parzyste
        a := Alg(x, k/2, n)
        return [a·a] mod n
    else
        a := Alg(x, (k-1)/2, n)
        return [x·a·a] mod n
```

ilość mnożeń:
długość zapisu binarnego n
+
liczba zapalonych bitów w zapisie binarnym n
$\leq 2\lceil \log_2 n \rceil = O(\log_2 n)$