8. (**Z** 2pkt) [1]

Ułóż algorytm dla następującego problemu:

PROBLEM.[2]

*dane*: $n, m \in \mathcal{N}$

*wynik*: wartość współczynnika przy $x^2$ (wzięta modulo $m$) wielomianu $\underbrace{(...((x-2)^2-2)^2...-2)^2}_{n \text{ razy}}$

Czy widzisz zastosowanie metody użytej w szybkim algorytmie obliczania $n$-tej liczby Fibonacciego do rozwiązania tego problemu?

Rozważmy ciąg wielomianów

$W_0(x) = x$

$W_n(x) = (W_{n-1}(x) - 2)^2$

Wtedy $W_n(x) = \underbrace{(...((x-2)^2-2)^2...-2)^2}_{n \text{ razy}}$.

Obliczamy współczynnik przy $x^2$, więc możemy obliczać wyrażenia mod $x^2$. Otrzymamy wtedy wyrażenie $a_n x^2 + b_n x + c_n$.

Zauważ, że $W_0(x) = x = a_0 x^2 + b_0 x + c_0$

$a_0 = 0, \; b_0 = 1 \quad c_0 = 0$

$W_n(x) = (a_n x^2 + b_n x + c_n - 2)^2 =$

$= a_n^2 x^4 + 2(b_n x + c_n - 2)(a_n x^2) + (b_n x + c_n - 2)^2 =$

$= a_n^2 x^4 + 2x^3 a_n b_n + 2 a_n c_n x^2 - 4 a_n x^2 + b_n^2 x^2 + 2 b_n x (c_n - 2) + (c_n - 2)^2$

$= a_n^2 x^4 + 2x^3 a_n b_n + 2 a_n c_n x^2 - 4 a_n x^2 + b_n^2 x^2 + 2 b_n x c_n - 4 b_n c_n x + (c_n - 2)^2 =$

$= a_n^2 x^4 + 2 a_n b_n x^3 + x^2(2 a_n c_n - 4 a_n + b_n^2) + x(2 b_n c_n - 4 b_n) + (c_n - 2)^2$

Stąd

$c_{n+1} = (c_n - 2)^2, \quad c_0 = 0 \quad c_1 = (0-2)^2 = 4 \Rightarrow c_2 = (4-2)^2 = 4 \Rightarrow \ldots \Rightarrow c_n = 4$

$b_{n+1} = 2 b_n c_n - 4 b_n \qquad b_0 = 1 \Rightarrow b_1 = 2 \cdot 1 \cdot 0 - 4 \cdot 1 = -4$

$b_2 = 2(-4) \cdot 4 - 4 \cdot (-4) = -32 + 16 = -16 = -4^2$

$b_n = 2 \cdot 4 b_n - 4 b_n = 8 b_n - 4 b_n = 4 b_n \Rightarrow b_{k+1} = -4^k$

$$a_{k+1} = 2a_kc_k - 4a_k + 4^{k^2}$$

$$a_{k+1} = 8a_k - 4a_k + (-4^k)^2$$

$$a_{k+1} = 4a_k + 16^k$$

Korzystając z zadania 1.5 możemy pokazać, że

$$\begin{bmatrix} 4 & 1 \\ 0 & 16 \end{bmatrix} \begin{bmatrix} a_k \\ 16^k \end{bmatrix} = \begin{bmatrix} a_{k+1} \\ 16^{k+1} \end{bmatrix}.$$

Chcę obliczyć n-ty wyraz muszę podnieść macierz do n-tej potęgi

$$\begin{bmatrix} 4 & 1 \\ 0 & 16 \end{bmatrix}^n \cdot \begin{bmatrix} a_0 \\ 16^0 \end{bmatrix} = \begin{bmatrix} a_n \\ 16^n \end{bmatrix} \iff \begin{bmatrix} 4 & 1 \\ 0 & 16 \end{bmatrix}^n \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a_n \\ 16^n \end{bmatrix}.$$

Jak możemy to szybko policzyć? Weźmy

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 0 & 16 \end{bmatrix}^n, \text{ wtedy}$$

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} a_0 \\ 16^0 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a_n \\ 16^n \end{bmatrix}$$

$$||$$

$$\boxed{a_n = a_{12}}$$

$$13_{10} = 1101_2$$

$$A \times A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} a_{11}^2 + \cancel{a_{21}^2} & a_{11}a_{12} + a_{12}a_{22} \\ \cancel{a_{21}a_{11}} + a_{22}a_{21} & \cancel{a_{21}a_{12}} + a_{22}^2 \end{bmatrix}$$

$$a_{21} = 0$$

Możemy użyć algorytmu szybkiego potęgowania macierzy, tzn. obliczać

$$A^k = \begin{cases} A(A^2)^{\frac{k-1}{2}} & \text{, jeśli } k \text{ jest nieparzyste} \\ (A^2)^{\frac{k}{2}} & \text{, jeśli } k \text{ jest parzyste} \end{cases}$$

Np. $A^{13} = A(A^2)^6 = A((A^2)^2)^3 = A(A^4)^2 A^4 = A A^4 A^8$