

Zadanie 1. Niech  $f(n) = \sum_{k=1}^n \lceil \log_2 k \rceil$ , wykaz  $f(n) = n - 1 + f(\lceil \frac{n}{2} \rceil) + f(\lfloor \frac{n}{2} \rfloor)$  dla  $n \geq 1$ .

$$\begin{aligned}
 f(n) &= \sum_{k=1}^n \lceil \log_2 k \rceil = \underbrace{\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil \log_2 (2k-1) \rceil}_{\text{nieparzyste}} + \underbrace{\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil \log_2 (2k) \rceil}_{\text{parzyste}} = \\
 &= \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (1 + \lceil \log_2 k \rceil) + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (1 + \lceil \log_2 (k - \frac{1}{2}) \rceil) = \\
 &= \lfloor \frac{n}{2} \rfloor + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil \log_2 k \rceil + \lfloor \frac{n}{2} \rfloor + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil \log_2 (k - \frac{1}{2}) \rceil = \\
 &= n + f(\lfloor \frac{n}{2} \rfloor) + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil \log_2 (k - \frac{1}{2}) \rceil = \\
 &= n + f(\lfloor \frac{n}{2} \rfloor) + \lceil \log_2 \frac{1}{2} \rceil + \sum_{k=2}^{\lfloor \frac{n}{2} \rfloor} \lceil \log_2 (k - \frac{1}{2}) \rceil = \\
 &= n + f(\lfloor \frac{n}{2} \rfloor) + (-1) + \sum_{k=2}^{\lfloor \frac{n}{2} \rfloor} \lceil \log_2 k \rceil = \\
 &= n - 1 + f(\lfloor \frac{n}{2} \rfloor) + f(\lceil \frac{n}{2} \rceil)
 \end{aligned}$$

$$\begin{aligned}
 \log_2(2k) &= \log_2 2 + \log_2 k = \\
 &= 1 + \log_2 k \\
 \lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil &= n
 \end{aligned}$$

Jeśli wymagamy, aby  $f(1)=0$ , to  $f$  jest jedyną funkcją spełniającą tę zależność (tj. funkcja jest jednoznaczna):

$$f(1) = 0$$

$$f(2) = 2 - 1 + f(1) + f(1)$$

$$f(3) = 3 - 1 + f(1) + f(2)$$

$$f(4) = 4 - 1 + f(2) + f(2)$$

$$f(5) = 5 - 1 + f(2) + f(3)$$

dla każdych kolejnych wartości  $n$  funkcja  $f(n)$  rekurencyjnie odwołuje się do  $f(1)=0$ , więc jeśli  $f(1)$  byłoby inne, to funkcja przyjmowałaby inne wartości

Zadanie 3. Przedstawienie  $n \in \mathbb{N}$  w postaci sumy liczb Fibonacciego jako ciąg

### REPREZENTACJA ZECKENDORFA

$a_1, \dots, a_k \in \{0, 1\}$ , takich że  $n = a_1 F_2 + \dots + a_k F_k$  oraz  
 $a_i + a_{i+1} \leq 1$  dla wszystkich  $i$  (tzn. dwie kolejne liczby  
Fibonacciego nie mogą wystąpić w tym zapisie).

Fakt: Każda liczba Fibonacciego ma jednoznaczny reprezentant (sumę siebie).

Dowód: dla  $n = 1, 2, 3$  mamy  $F_2 = 1$ ,  $F_3 = 2$ ,  $F_4 = 3$ , więc liczby te  
mają jednoznaczny reprezentant.

Podstawa indukcji:  $n = 4 = F_4 + F_2 = 3 + 1$

Krok indukcyjny: jeśli każda liczba  $n \leq k$  ma jednoznaczny reprezentant, to  $k+1$  też ma. } założenie  
indukcyjne

1°  $k+1$  jest liczbą Fibonacciego, więc ma jednoznaczny reprezentant (zgodnie z faktem).

2°  $k+1$  nie jest liczbą Fibonacciego:

Istnieje takie  $j \in \mathbb{Z}$ , że  $F_j < k+1 < F_{j+1}$  (cyfry  
 $k+1$  jest pomiędzy kolejnymi liczbami Fibonacciego).

Weźmy  $n = k+1 - F_j$  (z założenia  $n \leq k$ , więc ma  
jednoznaczny reprezentant).

$$\begin{aligned} n = k+1 - F_j &\Rightarrow F_j + n = k+1 < F_{j+1} = F_j + F_{j-1} \\ &\Rightarrow n < F_{j-1}, \end{aligned}$$

Wobec reprezentacja  $n$  nie zawiera  $F_{j-1}$ , stąd wiemy,  
że  $k+1$  ma jednoznaczny reprezentant jako  $n + F_j$ . ■

Dowód (jednoznaczność):

Załóżmy, że  $S$  i  $T$  są innymi reprezentacjami  $n$ . Weźmy  
też sumy bez wspólnych elementów, tzn.  $S' = S \setminus T$ ,  $T' = T \setminus S$ .

Skoro usunęliśmy wspólne elementy, to  $\sum S = \sum T$  implikuje

$\sum S' = \sum T'$ . Gdyby  $S'$  był pusty, to  $T'$  musiałby być  
również pusty, aby suma elementów się zgadzała, lecz  $S \neq T$ ,  
więc zbiory te nie mogą być puste.

Ważny tenar najwyższe elementy obu zbiorów:  $F_S$  dla zbioru  $S'$  oraz  $F_T$  dla zbioru  $T'$ . Załóżmy, że stąd wynika, że  $F_S < F_T$ . Wtedy  $\sum S' < F_{S+1}$  oraz  $\sum S' < F_T$ , jednak wiemy, że  $\sum S' = \sum T'$  dochodząc do sprzeczności, czyli  $S'$  oraz  $T'$  nie mogą być zbiorami niepustymi, a więc  $S=T$ , czyli reprezentacja liczb jest jednoznaczna. ■

Zadanie 4. Niech  $x, k, n \in \mathbb{Z}$ , konstruuj algorytm obliczający  $x^k \bmod n$ . Poinformuj on konstantę ze wzoru  $x^{2^l} = x^l \cdot x^l$ ,  $x^{2^{l+1}} = x \cdot x^{2^l}$ . Określ liczbę mnożeń wykonanych przez algorytm.

ALGORYTM:

$f(x, k, n)$ :

if  $k == 1$ : return  $x \bmod n$

else:  $x\_temp = f(x, \frac{k}{2}, n)$

if  $k \bmod 2 == 0$ : return  $(x\_temp * x\_temp) \bmod n$

if  $k \bmod 2 == 1$ : return  $(x * x\_temp * x\_temp) \bmod n$

Liczba mnożeń algorytmu:

$$T(k) = T\left(\left\lfloor \frac{k}{2} \right\rfloor\right) + c =$$

$$= T\left(\left\lfloor \frac{k}{4} \right\rfloor\right) + c + c =$$

$$= T\left(\left\lfloor \frac{k}{8} \right\rfloor\right) + c + c + c = \dots =$$

$$= T\left(\left\lfloor \frac{k}{2^{\log_2 k}} \right\rfloor\right) + c \cdot \log_2 k =$$

$$= c \cdot \log_2 k =$$

$$= O(\log_2 k)$$

# Zadanie 11.

(a) przedstawić  $\gcd(448, 721)$  w postaci  $721x + 448y$  dla  $x, y \in \mathbb{Z}$

721	448
448	$721 - 448 = 273$
273	$448 - 273 = 175$
175	$273 - 175 = 98$
98	$175 - 98 = 77$
77	$98 - 77 = 21$
21	$77 - 3 \cdot 21 = 14$
14	$21 - 14 = 7$
7	$14 - 2 \cdot 7 = 0$

więc  $\gcd(448, 721) = 7$

$$\begin{aligned}
 7 &= 21 - 14 = 21 - (77 - 3 \cdot 21) = \\
 &= 4 \cdot 21 - 77 = 4 \cdot (98 - 77) - 77 = \\
 &= 4 \cdot 98 - 5 \cdot 77 = 4 \cdot 98 - 5 \cdot (175 - 98) = \\
 &= 9 \cdot 98 - 5 \cdot 175 = 9 \cdot (273 - 175) - 5 \cdot 175 = \\
 &= 9 \cdot 273 - 14 \cdot 175 = \\
 &= 9 \cdot 273 - 14 \cdot (448 - 273) = \\
 &= 23 \cdot 273 - 14 \cdot 448 = \\
 &= 23 \cdot (721 - 448) - 14 \cdot 448 = \\
 &= 23 \cdot 721 - 37 \cdot 448, \\
 \text{a więc } x &= 23, y = -37.
 \end{aligned}$$

(b) oblicz  $x, y$  całkowite, takie że  $333x + 1234y = 1$ , ile można się  $333^{-1}$  w pierścieniu  $\mathbb{Z}_{1234}$ !

1234	333
333	$1234 - 3 \cdot 333 = 235$
235	$333 - 235 = 98$
98	$235 - 98 \cdot 2 = 39$
39	$98 - 2 \cdot 39 = 20$
20	$39 - 20 = 19$
19	$20 - 19 = 1$
1	$1 - 1 = 0$

$$\begin{aligned}
 1 &= 20 - 19 = 20 - (39 - 20) = \\
 &= 2 \cdot 20 - 39 = 2 \cdot (98 - 2 \cdot 39) - 39 = \\
 &= 2 \cdot 98 - 5 \cdot 39 = 2 \cdot 98 - 5 \cdot (235 - 2 \cdot 98) = \\
 &= 12 \cdot 98 - 5 \cdot 235 = \\
 &= 12 \cdot (333 - 235) - 5 \cdot 235 = \\
 &= 12 \cdot 333 - 17 \cdot 235 = \\
 &= 12 \cdot 333 - 17 \cdot (1234 - 3 \cdot 333) = \\
 &= 63 \cdot 333 - 17 \cdot 1234, \\
 \text{więc } x &= 63, y = -17
 \end{aligned}$$

Wartość  $333^{-1}$  w pierścieniu  $\mathbb{Z}_{1234}$ :

$$\begin{aligned}
 333 \cdot x \bmod 1234 &= 1, \text{ ale mamy} \\
 \text{a więc } 333^{-1} &\equiv 63 \pmod{1234}
 \end{aligned}$$

to działa jak modulo

$$63 \cdot 333 - 17 \cdot 1234 = 1,$$

(c) oblicz  $-69^{-1} \bmod 1313 \equiv x$

$$(1313 - 69)x + 1244y = \gcd(1313, 1244)$$

1313	1244
1244	$1313 - 1244 = 69$
69	$1244 - 18 \cdot 69 = 2$
2	$69 - 34 \cdot 2 = 1$
1	$1 - 1 = 0$

$$1 = 69 - 34 \cdot 2 =$$

$$= 69 - 34 \cdot (1244 - 18 \cdot 69) =$$

$$= 613 \cdot 69 - 34 \cdot 1244 =$$

$$= 613(1313 - 1244) - 34 \cdot 1244 =$$

$$= 613 \cdot 1313 - 647 \cdot 1244,$$

$$\text{zatem } x = -647 \equiv 666 \pmod{1313}$$

Zadanie 15. Niech  $ax_0 + by_0 = c^{(*)}$  dla pewnych  $a, b, c, x_0, y_0 \in \mathbb{Z}$ . Oweś zbiór wszystkich rozwiązań  $(x, y)$  równania  $ax + by = c$ .

Niech  $x = x_0 + x'$ ,  $y = y_0 + y'$ , wtedy

$$ax + by = c \Rightarrow ax_0 + ax' + by_0 + by' = c \stackrel{(*)}{\Rightarrow} ax' + by' = 0$$

$$\Rightarrow b \mid ax' \text{ oraz } a \mid by' \quad (\text{z } ax' = -by')$$

Zatem:

$$\frac{b}{\gcd(a, b)} \mid x' \cdot \frac{a}{\gcd(a, b)}, \text{ czyli } \frac{b}{\gcd(a, b)} \mid x' \text{ oraz } \frac{a}{\gcd(a, b)} \mid y' \quad \text{analogicznie}$$

Stąd dla każdego  $k \in \mathbb{Z}$  poniżej parę jest rozwiązaniem:

$$\left( x_0 + \frac{b}{\gcd(a, b)} \cdot k, y_0 - \frac{a}{\gcd(a, b)} \cdot k \right),$$

ponieważ:

$$ax + by = ax_0 + by_0 + \frac{ab}{\gcd(a, b)} k - \frac{ab}{\gcd(a, b)} k = ax_0 + by_0 = c \quad \blacksquare$$



Zadanie 13. Jeśli  $a \perp b, a > b$ , to  $\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$   
dla  $0 \leq m < n$ .

Dowód indukcyjny dla  $n$ :

$$1^\circ n=1 \quad \gcd(a^m - b^m, a^1 - b^1) = a^{\gcd(m,1)} - b^{\gcd(m,1)} = a^1 - b^1 = a - b$$

2° Załóżmy, że dla każdego  $n_0 < n$  zachodzi

$$\gcd(a^m - b^m, a^{n_0} - b^{n_0}) = a^{\gcd(m, n_0)} - b^{\gcd(m, n_0)}, \text{ podczas, że}$$

wtedy zachodzi dla wszystkich  $n$ .

$$\gcd(a^m - b^m, a^n - b^n) = \gcd(a^m - b^m, a^{m+k} - b^{m+k}) =$$

$$= \gcd(a^m - b^m, \cancel{a^m} (a^k - b^k) + (a^m b^k - b^{m+k})) =$$

$$= \gcd(\underbrace{a^m - b^m}_m, \underbrace{a^m(a^k - b^k)}_r + \underbrace{b^k(a^m - b^m)}_{q \cdot m}) \stackrel{(*)1}{=} \underbrace{\phantom{a^m - b^m}}_m$$

$$= \gcd(a^m - b^m, a^m(a^k - b^k)) \stackrel{(*)2}{=} \underbrace{\phantom{a^m - b^m}}_m$$

$$= \gcd(a^m - b^m, a^k - b^k) \stackrel{\text{zał. ind}}{=} \underbrace{\phantom{a^m - b^m}}_m$$

$$= a^{\gcd(m,k)} - b^{\gcd(m,k)} =$$

$$= a^{\gcd(m, n-m)} - b^{\gcd(m, n-m)} =$$

$$= a^{\gcd(m,n)} - b^{\gcd(m,n)} \quad \blacksquare$$

show  $0 \leq m < n$ ,  
to  $\exists k > 0 : m+k = n$

$$*1: \gcd(m, qm+r) =$$

$$= \gcd(m, r)$$

$$*2: b \perp c \Rightarrow$$

$$\Rightarrow \gcd(ab, c) = \gcd(a, c)$$

Zadanie 2. Zwróć uwagę na funkcję  $f(n) = \sum_{k=1}^n \lceil \log_2 k \rceil$ .

Rozważmy dwa przypadki:

$$\begin{aligned}
 1^\circ \quad n = 2^k : \quad f(2^k) &= 2^k - 1 + f(2^{k-1}) + f(2^{k-1}) = \\
 &= (2^k - 1) + 2f(2^{k-1}) = \\
 &= (2^k - 1) + 2((2^{k-1}) + 2f(2^{k-2})) = \\
 &= (2^k - 1) + (2^k - 2) + 4f(2^{k-2}) = \\
 &= (2^k - 1) + (2^k - 2) + 4((2^{k-2} - 2) + 2f(2^{k-3})) = \\
 &= (2^k - 1) + (2^k - 2) + (2^k - 3) + 2^3 \cdot f(2^{k-3}) = \\
 &= \sum_{i=0}^{k-1} ((2^k - 2^i) + 2^i f(2^{k-i})), \text{ gdzie } a \leq k
 \end{aligned}$$

Dla  $a=k$  otrzymamy:

$$\sum_{i=0}^{k-1} (2^k - 2^i) + \underbrace{2^k \cdot f(1)}_{0, \text{ bo } f(1)=0} = k \cdot 2^k - 2^k + 1 = 2^k(k-1) + 1$$

$$2^\circ \quad n \neq 2^k \quad (n = 2^{\lceil \log_2 n \rceil})$$

$$f(n) = f(2^{\lceil \log_2 n \rceil}) - \sum_{k=n+1}^{2^{\lceil \log_2 n \rceil}} 1 = f(2^{\lceil \log_2 n \rceil}) - (2^{\lceil \log_2 n \rceil} - n) \cdot \lceil \log_2 n \rceil$$

$$\sum_{k=1}^n \lceil \log_2 k \rceil = 0$$

$$+ 1$$

$$+ 2 + 2$$

$$+ 3 + 3 + 3 + 3$$

$$+ 8 \cdot 4$$

$$+ 16 \cdot 5$$

$$+ \dots$$

$$\begin{aligned}
 \text{a więc } \sum_{k=1}^n \lceil \log_2 k \rceil &= \sum_{i=1}^{\log_2 n} i \cdot 2^{i-1} = 2^0 \\
 &+ 2^1 + 2^1 \\
 &+ 2^2 + 2^2 + 2^2 \\
 &+ 2^3 + 2^3 + 2^3 + 2^3 \\
 &+ \dots + \dots + \dots \\
 &+ 2^{\log_2 n - 1} + \dots
 \end{aligned}$$

$$\text{dodajmy wyniki z lewej strony otrzymamy } \sum_{i=1}^{\log_2 n} (2^{\log_2 n} - 1 - 2^i)$$

Zadanie 8. Dany jest algorytm typu „dziel i zwyciężaj” wywołujący sam siebie a razy dla podproblemu rozmiaru  $\frac{n}{b}$  i wykonujący pracę  $cn^d$  operacji.  $T(n) = aT(\frac{n}{b}) + cn^d$ , oszacuj  $T(n)$  jako  $O(\cdot)$  w zależności od  $a, b, d$ .

$$T(n) = aT\left(\frac{n}{b}\right) + cn^d, \quad T(1) = c$$

$k$  - poziom drzewa

$$a^k c \left(\frac{n}{b}\right)^d = cn^d \frac{a^k}{b^{dk}}$$

$$= cn^d \left(\frac{a}{b^d}\right)^k$$

$$c \cdot a^{\log_b n}$$

$$T(n) \leq c \cdot a^{\log_b n} + \sum_{k=0}^{\log_b n - 1} cn^d \left(\frac{a}{b^d}\right)^k = c \cdot a^{\log_b n} + cn^d \sum_{k=0}^{\log_b n - 1} \left(\frac{a}{b^d}\right)^k$$

$$1^\circ a = b^d \Rightarrow \log_b a = d$$

$$T(n) \leq cn^d + cn^d \sum_{k=0}^{\log_b n - 1} 1 = cn^d + cn^d \log_b n = O(n^d \log_b n)$$

$$2^\circ a < b^d \Rightarrow \log_b a < d$$

$$T(n) < cn^d + cn^d \sum_{k=0}^{\log_b n - 1} \left(\frac{a}{b^d}\right)^k < cn^d + cn^d \sum_{k=0}^{\infty} \left(\frac{a}{b^d}\right)^k < cn^d \left(1 + \frac{1}{1 - \frac{a}{b^d}}\right) = O(n^d)$$

$$3^\circ a > b^d \Rightarrow \log_b a > d$$

$$T(n) \leq cn^{\log_b a} + cn^d \sum_{k=1}^{\log_b n} \left(\frac{a}{b^d}\right)^{k-1} = cn^{\log_b a} + cn^d \left( \frac{\left(\frac{a}{b^d}\right)^{\log_b n} - 1}{\left(\frac{a}{b^d}\right) - 1} \right) <$$

$$< cn^{\log_b a} + cn^d \left(\frac{a}{b^d}\right)^{\log_b n} \left( \frac{1}{\left(\frac{a}{b^d}\right) - 1} \right) = cn^{\log_b a} + cn^d \left(\frac{a}{b^d}\right)^{\log_b n} \cdot \Theta(1) =$$

$$= cn^{\log_b a} + cn^d \cdot \frac{a^{\log_b n}}{b^{d \log_b n}} \cdot \Theta(1) = cn^{\log_b a} + cn^d \frac{n^{\log_b a}}{n^d} \cdot \Theta(1) =$$

$$= cn^{\log_b a} + cn^{\log_b a} \Theta(1) = O(n^{\log_b a})$$



Zadanie 9.  $T(n) \leq T(\lceil \frac{n}{5} \rceil) + T(\lceil \frac{7n}{10} \rceil) + cn$ , pokazać  $T(n) < c'n$  dla pewnej stałej  $c'$ .

$$n \geq 100 \quad T(n) < kn \quad (k \equiv c', \text{ dla wygodny})$$

$$n < 100, \quad T(n) \leq d$$

Dowód indukcyjny po  $n$ :

$$1^\circ \quad n < 100 \quad k > d, \text{ wtedy } T(n) < kn$$

$$2^\circ \text{ załóżmy } T(n') < kn' \text{ dla pewnego } k, \quad n' < n, \quad n \geq 100$$

$$T(n) \leq T(\lceil \frac{n}{5} \rceil) + T(\lceil \frac{7n}{10} \rceil) + cn \leq$$

$$\leq k \lceil \frac{n}{5} \rceil + k \lceil \frac{7n}{10} \rceil + cn \leq$$

$$\leq k(\frac{n}{5} + 1) + k(\frac{7n}{10} + 1) + cn =$$

$$= \frac{nk}{5} + k + \frac{7nk}{10} + k + cn =$$

$$= \frac{9nk}{10} + 2k + cn =$$

$$= kn - \frac{kn}{10} + 2k + cn =$$

$$= kn + \underbrace{(cn + 2k - \frac{kn}{10})}_0$$

$$2.1^\circ \quad a \leq 0$$

$$2.2^\circ \quad a \geq 0$$

$$cn + 2k - \frac{kn}{10} > 0$$

$$2k - \frac{kn}{10} > -cn$$

$$\frac{kn}{10} - 2k < cn$$

$$\frac{kn - 20k}{10} < cn$$

$$k \left( \frac{n-20}{10} \right) < cn$$

$$k < cn \left( \frac{10}{n-20} \right)$$

$$k < 10c \left( \frac{n}{n-20} \right)$$

$$\text{wybierz } k = 50 \blacksquare$$

Zadanie 12. Pokaż, że  $\gcd(F_{n-1}, F_n) = 1$ .

bazą: 
$$\left. \begin{array}{l} F_1 = 1 \\ F_2 = 1 \\ F_3 = 2 \\ F_4 = 3 \end{array} \right\} \begin{array}{l} \text{liczby} \\ \text{urządzone} \\ \text{pierwsze} \end{array}$$

krok: załóżmy, że  $\forall i \leq n \quad \gcd(F_{i-1}, F_i)$

$$\left. \begin{array}{l} F_{n-2} = a \\ F_{n-1} = b \end{array} \right\} \gcd(F_n, F_{n+1}) = \gcd(a+b, a+2b) = \gcd(a+b, b) = \gcd(a, b) = 1$$

Udowodnij  $\gcd(F_m, F_n) = F_{\gcd(m, n)}$ . Indukcja względem  $m+n$ :

bazą:  $\gcd(F_1, F_1) = 1 = F_1$

krok: załóżmy, że  $m \leq n$ ,  $m \geq 2$ ,  $n-m > 1$

lemat:  $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$

$$F_n = F_{m+(n-m)} = F_m F_{(n-m)+1} + F_{m-1} F_{n-m}$$

$$\gcd(F_m, F_n) = \gcd(F_m, F_m F_{(n-m)+1} + F_{m-1} F_{n-m}) =$$

$$= \gcd(F_m, F_{m-1} F_{n-m}) =$$

$$= \gcd(F_m, F_{n-m}) \stackrel{\text{zał. ind.}}{=} \quad$$

$$m + (n-m) < m+n$$

$$= F_{\gcd(m, n-m)} =$$

$$= F_{\gcd(m, n)} \quad \blacksquare$$

Zadanie 5.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a+b & a \\ c+d & c \end{bmatrix}$$

Po podniesieniu  $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$  do  $n$ -tej potęgi <sup>(dla  $n=2,3,4,5,\dots$ )</sup> można zauważyć, że  $A^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$

Algorytm:

$$\left. \begin{array}{l} n \text{ potęgok: } \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{\frac{n}{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{\frac{n}{2}} \\ n \text{ nieparzyste: } \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{\frac{n}{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{\frac{n}{2}} \end{array} \right\} \begin{array}{l} \text{szybkie} \\ \text{potęgowanie} \end{array}$$

$F_n$  ma co najmniej  $n$  cyfr, więc złożoność dla  $n$ -tej liczby Fibonacciego:

$$\begin{aligned} \sum_{i=1}^{\log_2 n} (8M(2^i) + 4 \cdot 2^i), \quad \sum_{i=1}^{\log_2 n} 8M(2^i) &= 8[M(n) + M(\frac{n}{2}) + M(\frac{n}{4}) + M(\frac{n}{8}) + \dots + M(1)] \leq \\ &\leq 8[M(n) + \frac{1}{2}M(n) + \frac{1}{4}M(n) + \dots + \frac{1}{2^{\log_2 n}}M(n)] = \\ &= 8M(n) \sum_{i=1}^{\log_2 n} \left(\frac{1}{2}\right)^i < 8M(n) \cdot 2 \end{aligned}$$

Zadanie 6.  $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} F_2 \\ F_1 \end{bmatrix} = \begin{bmatrix} F_{n+2} \\ F_{n+1} \end{bmatrix}$



$$\begin{bmatrix} a_{n-1} & a_{n-2} & \dots & a_{n-k} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & 0 \end{bmatrix} \underbrace{\begin{bmatrix} p_1 & 1 & 0 & 0 \\ p_2 & 0 & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ p_k & 0 & 0 & 1 \end{bmatrix}}_M = \begin{bmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_{n-k} \\ 0 & & & & 0 \\ \vdots & & & & \vdots \\ 0 & & & & 0 \end{bmatrix}$$

$$\begin{bmatrix} a_k & a_{k-1} & a_{k-2} & \dots & a_0 \\ 0 & & & & 0 \\ \vdots & & & & \vdots \\ 0 & & & & 0 \end{bmatrix} \cdot M^{n-k} = \begin{bmatrix} a_n & & & & \\ & \ddots & & & \\ & & & & \end{bmatrix}$$