Lista 3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
✓	✓		✓	✓						✓		✓		

Zadanie 1

Cz I

Pokazać, że $f(n) = \sum_{k=1}^{n} \lceil log_2 k \rceil$ spełnia zależność rekurencyjną:

$$f(n) = n - 1 + f(\lceil \frac{n}{2} \rceil) + f(\lfloor \frac{n}{2} \rfloor) \; dla \; n \geq 1$$

Dowód:

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

$$\sum_{k=1}^{\lceil \frac{n}{2} \rceil} (log_2 2 + \lceil log_2 (k - \frac{1}{2}) \rceil) + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (log_2 2 + \lceil log_2 (k) \rceil) =$$

$$\left\lceil \frac{n}{2} \right\rceil + \left\lfloor \frac{n}{2} \right\rfloor + \sum_{k=1}^{\lceil \frac{n}{2} \rceil} \lceil log_2 (k - \frac{1}{2}) \rceil + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil log_2 (k) \rceil =$$

$$n + f(\lfloor \frac{n}{2} \rfloor) + \lceil log_2 \frac{1}{2} \rceil + \sum_{k=2}^{\lceil \frac{n}{2} \rceil} \lceil log_2 (k - \frac{1}{2}) \rceil \stackrel{(1)}{=}$$

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

$$n - 1 + f(\lfloor \frac{n}{2} \rfloor) + f(\lceil \frac{n}{2} \rceil)$$

Uzasadnienie przejścia (1):

Wiemy, że $\lceil log_2 (k - \frac{1}{2}) \rceil \leq \lceil log_2 k \rceil$.

Załóżmy nie wprost, że istnieje $k \in \mathbb{N}, k \geq 2$, takie że $\lceil log_2(k - \frac{1}{2}) \rceil \neq \lceil log_2 k \rceil$, czyli że $\lceil log_2(k - \frac{1}{2}) \rceil < \lceil log_2 k \rceil$.

Wtedy $k - \frac{1}{2} = 2^l \iff k = 2^l + \frac{1}{2}, l \in \mathbb{Z}$

Dostajemy sprzeczność z założeniem, iż $k \geq 2$ (dla $l \leq 0$) oraz $k \in \mathbb{N}$ (dla $l > 0$).

Otrzymujemy zatem $\lceil log_2(k - \frac{1}{2}) \rceil = \lceil log_2 k \rceil$ dla $k \geq 2$.

Czyli

$$\sum_{k=2}^{\lceil \frac{n}{2} \rceil} \lceil log_2(k - \frac{1}{2}) \rceil = \sum_{k=2}^{\lceil \frac{n}{2} \rceil} \lceil log_2 k \rceil \overset{(2)}{=} \sum_{k=1}^{\lceil \frac{n}{2} \rceil} \lceil log_2 k \rceil$$

(2) $log_2 1 = 0$

Cz II

Załóżmy nie wprost, że istnieje funkcja g, taka że:

$$\begin{cases} g(1) = 0 \\ g(n) = n - 1 + g(\lfloor \frac{n}{2} \rfloor) + g(\lceil \frac{n}{2} \rceil) \end{cases}$$

Oraz $g \neq f$.

1° $f(1) = 0 = g(1)$

2° Skoro $f \neq g$ to istnieje takie n_0, że $f(n_0) \neq g(n_0)$ oraz $f(k) = g(k)$ dla każdego $k < n_0$.

$$g(n_0) = n_0 - 1 + g(\lfloor \frac{n_0}{2} \rfloor) + g(\lceil \frac{n_0}{2} \rceil) \overset{z\ zał.}{=} n_0 - 1 + f(\lfloor \frac{n_0}{2} \rfloor) + f(\lceil \frac{n_0}{2} \rceil) = f(n_0)$$

Sprzeczność.

Zadanie 2

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

Dowód:
$1^\circ n = 1$

$f(1) = 0 = 1 \cdot 0 - 2^0 + 1$

2° Załóżmy, że zachodzi $\sum_{k=1}^{n_0} \lceil log_2 k \rceil = n_0 \lceil log_2 n_0 \rceil - 2^{\lceil log_2 n_0 \rceil} + 1$ dla każdego $1 \leq n_0 < n$.

$$f(n) = \sum_{k=1}^{n} \lceil log_2 k \rceil \stackrel{zad1}{=} n - 1 + \sum_{k=1}^{\lceil \frac{n}{2} \rceil} \lceil log_2 k \rceil + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil log_2 k \rceil \stackrel{zał.ind.}{=}$$

$$n - 1 + \lceil \frac{n}{2} \rceil \cdot \lceil log_2 \lceil \frac{n}{2} \rceil \rceil - 2^{\lceil log_2 \lceil \frac{n}{2} \rceil \rceil} + 1 + \lfloor \frac{n}{2} \rfloor \cdot \lceil log_2 \lfloor \frac{n}{2} \rfloor \rceil - 2^{\lceil log_2 \lfloor \frac{n}{2} \rfloor \rceil} + 1 =$$

Rozpatrzmy przypadki:

2.1° dla n parzystego

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

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

$$n - 1 + n \cdot \lceil log_2 n \rceil - n - 2^{\lceil log_2 n \rceil} + 2 =$$

$$n \cdot \lceil log_2 n \rceil - 2^{\lceil log_2 n \rceil} + 1$$

2.2° dla n nieparzystego

$$n - 1 + \frac{n+1}{2} \cdot \left\lceil log_2 \frac{n+1}{2} \right\rceil - 2^{\lceil log_2 \frac{n+1}{2} \rceil} + 1 + \frac{n-1}{2} \cdot \left\lceil log_2 \frac{n-1}{2} \right\rceil - 2^{\lceil log_2 \frac{n-1}{2} \rceil} + 1 =$$

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

Rozpatrzmy przypadki:

$2.2.1^\circ$ Gdy $\lceil log_2 (n-1) \rceil = \lceil log_2 (n+1) \rceil = \lceil log_2 n \rceil$

$$\lceil log_2 n \rceil \cdot \frac{n+1+n-1}{2} - 2 \cdot 2^{\lceil log_2 n \rceil - 1} + 1 = n \cdot \lceil log_2 n \rceil - 2^{\lceil log_2 n \rceil} + 1$$

$2.2.2^\circ$ Gdy $\lceil log_2 (n-1) \rceil = \lceil log_2 n \rceil - 1 = \lceil log_2 (n+1) \rceil - 1$, czyli $n - 1 = 2^l$

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

$$\lceil log_2 n \rceil \cdot \frac{n+1+n-1}{2} + \frac{1-n}{2} - \frac{3}{2} \cdot 2^{\lceil log_2 (n-1) \rceil} + 1 =$$

$$n \cdot \lceil log_2 n \rceil + \frac{1 - n - 3(n-1)}{2} + 1 =$$

$$n \cdot \lceil log_2 n \rceil + \frac{-4n+4}{2} + 1 =$$

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

$$n \cdot \lceil log_2 n \rceil - 2^{\lceil log_2 n \rceil} + 1$$

Zadanie 4

Algorytm:

```
foo(x,k,n):
    If k = 1
        Return x mod n

    x2 := foo(x,floor(k/2),n)

    If k mod 2 = 0
        Return (x2 * x2) mod n
    Else
        Return (x * x2 * x2) mod n
```

$M(k)$ – liczba mnożeń wykonywanych przez algorytm.
$M_{max}(k)$ – liczba mnożeń wykonywana przez algorytm w najgorszym przypadku.

W najgorszym wypadku (gdy z każdym wywołaniem zachodzi k mod 2 = 1) wykonujemy dwa mnożenia na wywołanie (poza $M_{max}(1) = 0$), zatem:

$M_{max}(k) = 2 + M_{max}(\frac{k}{2}) = 2 + 2 + M_{max}(\frac{k}{4}) = ... = 2 + 2 + ... + 2 + M_{max}(1) = 2 \cdot log_2 k$.

Zatem $M(k) = O(log_2 k)$.

Zadanie 5

$$M^n = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \; dla \; n \geq 1$$

Dowód

1° $n = 1$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^1 = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix}$$

2° Załóżmy, że zachodzi $M^n = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$.

$$M^{n+1} = M \cdot M^n \overset{zał.ind.}{=} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} =$$

$$\begin{bmatrix} F_{n+1} + F_n & F_n + F_{n-1} \\ F_{n+1} & F_n \end{bmatrix} = \begin{bmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{bmatrix}$$

Algorytm:

```
FibFromMatrix(n):
    Mn[2][2] := MatrixPow(n)
    ret Mn[0][1]

MatrixPow(n)
    M[2][2] := {{1,1}, {1,0}}

    If n = 1
        ret M

    M2 := MatrixPow(n/2)

    If n mod 2 = 0
        *(M2,M2)
    Else
        *(M, *(M2, M2))

*(M1,M2): //For Fib matrix
    Mres[0][0] := M1[0][0] * M2[0][0] + M1[0][1] * M2[1][0]
    Mres[0][1] := M1[0][0] * M2[0][1] + M1[0][1] * M2[1][1]
    Mres[1][0] := M1[1][0] * M2[0][0] + M1[1][1] * M2[1][0]
    Mres[1][1] := M1[1][0] * M2[0][1] + M1[1][1] * M2[1][1]
    ret Mres
```

Lemat: N-ta liczba Fibonacciego jest co najwyżej n-cyfrowa.

$$F_n \leq 2^n$$

Dowód:

1° $n = 0 : F_0 = 0 \leq 1$
$n = 1 : F_1 = 1 \leq 2$

2° Załóżmy, że $F_k \leq 2^k$ dla każdego $k < n$.
$F_n = F_{n-2} + F_{n-1} \overset{zał.ind.}{\leq} 2^{n-2} + 2^{n-1} = 2^{n-2} \cdot 3 < 2^n$

Aby pomnożyć 2 macierze o elementach k-cyfrowych musimy wykonać 8 mnożeń, czyli $8 \cdot M(k)$.

Złożoność funkcji `MatrixPow(n)` w najgorszym przypadku (gdy n nieparzyste przy każdym wywołaniu `MatrixPow(n)` musimy wykonać mnożenie dwóch macierzy o elementach (co najwyżej) k-cyfrowych oraz wykonać dodatkowe 8 mnożeń elementów (co najwyżej) k-cyfrowych przez elementy jednocyfrowe):

$T(n) = 8 \cdot M(n) + 8 \cdot n + T(\frac{n}{2}) =$

$8 \cdot M(n) + 8 \cdot n + 8 \cdot M(\frac{n}{2}) + 8 \cdot \frac{n}{2} + T(\frac{n}{4}) = ... =$

$\sum_{i=1}^{log_2 n}(8 \cdot M(2^i) + 8 \cdot 2^i) = 8\sum_{i=1}^{log_2 n}(M(2^i) + 2^i) =$

$8\frac{2^{log_2 n}-1}{2-1} + 8\sum_{i=1}^{log_2 n} M(2^i) = 8(n-1) + 8\sum_{i=1}^{log_2 n} M(2^i) \leq$

$8(n-1) + 8\sum_{i=1}^{log_2 n}(\frac{1}{2^i}M(n)) = 8(n-1) + 8M(n)\sum_{i=1}^{log_2 n} \frac{1}{2^i} =$

$8(n-1) + 16M(n) \cdot \frac{n-1}{n} < 8n + 16M(n)$

Zadanie 11

a) Przedstaw $gcd(448, 721)$ 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*21 = 14
14	21 - 14 = 7
7	14 - 2*7 = 0

$$7 = 21 - 14 = 21 - 77 + 3 \cdot 21 = 4 \cdot 21 - 77 = 4 \cdot (98 - 77) - 77 =$$

$$4 \cdot 98 - 5 \cdot (175 - 98) = 9 \cdot (273 - 175) - 5 \cdot 175 =$$

$$9 \cdot 273 - 14 \cdot (448 - 273) = 23 \cdot (721 - 448) - 14 \cdot 448 =$$

$$23 \cdot 721 - 37 \cdot 448$$

b) Oblicz takie całkowite x, y, że $333x + 1234y = 1$. Ile równa się 333^{-1} w pierścieniu $\mathbb{Z}_{1234}$?

1234	333
333	1234 - 3*333 = 235
235	333-235 = 98
98	235 - 2*98 = 39
39	98 - 2*39 = 20
20	39 - 20 = 19
19	20 - 19 = 1
1	19 - 19*1 = 0

$$1 = 20 - 19 = 2 \cdot 20 - 39 = 2 \cdot (98 - 2 \cdot 39) - 39 = 2 \cdot 98 - 5 \cdot 39 =$$

$$2 \cdot 98 - 5 \cdot (235 - 2 \cdot 98) = 12 \cdot 98 - 5 \cdot 235 =$$

$$12 \cdot (333 - 235) - 5 \cdot 235 = 12 \cdot 333 - 17 \cdot 235 =$$

$$12 \cdot 333 - 17 \cdot (1234 - 3 \cdot 333) = 63 \cdot 333 - 17 \cdot 1234$$

Zatem $x = 63, y = -17$.

Ile równa się 333^{-1} w pierścieniu $\mathbb{Z}_{1234}$?

$333 \cdot x \ mod \ 1234 = 1$

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

To $x = 63$

Czyli $333^{-1} \equiv 63 \ (mod \ 1234)$

c) Obliczyć $-69^{-1} \ mod \ 1313$

$69 \cdot x \ mod \ 1313 = 1$

1313	69
69	1313 - 19*69 = 2
2	69 - 34*2 = 1
1	2 - 2*1 = 0

$$1 = 69 - 34 \cdot 2 = 69 - 34 \cdot (1313 - 19 \cdot 69) = 647 \cdot 69 - 34 \cdot 1313$$

$x = 647$

Zatem $69^{-1} \equiv 647\ (mod\ 1313)$

$-69^{-1}\ mod\ 1313 = -647\ mod\ 1313 = -647 + 1313 = 666$

Zadanie 13

Pokaż, że 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:

$1^\circ n = 0 \iff gcd(a^m - b^m, 0) = a^m - b^m = a^{gcd(m,0)} - b^{gcd(m,0)}$

2° Załóżmy, że zachodzi $gcd(a^m - b^m, a^{n_0} - b^{n_0}) = a^{gcd(m,n_0)} - b^{gcd(m,n_0)}$ dla każdego $0 \leq m < n_0 < n$

Niech $n = m + d$.

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

$$gcd(a^m - b^m, a^{m+d} - a^m b^d + a^m b^d - b^{m+d}) =$$

$$gcd(a^m - b^m, a^m(a^d - b^d) + b^d(a^m - b^m)) \stackrel{(1)}{=}$$

$$gcd(a^m - b^m, a^m(a^d - b^d)) \stackrel{(2)}{=} gcd(a^m - b^m, a^d - b^d) \stackrel{zał.ind.}{=}$$

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

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

(1) Korzystamy z własności $gcd(x, y) = gcd(x, kx + y)$.

(2) Jeśli $gcd(x, y) = 1$ to $gcd(kx, y) = gcd(k, y)$
Ponieważ $a \perp b$ to $(a^m - b^m) \perp a^m$.
Uzasadnienie:

$$gcd(a^m - b^m, a^m) \stackrel{(1)}{=} gcd(-b^m, a^m) = gcd(b^m, a^m) = 1$$

tags: `mdm`