

## Zadanie 10

$$a, b \in \mathbb{N} \quad ; \quad x, y \in \mathbb{Z} \setminus \{0\} \quad ; \quad ax + by = 1$$

( $a', b' \in \mathbb{N}$ )

- Zał. nie uprost.  $\text{NWD}(a, b) \neq 1 = k \iff k \mid a \wedge k \mid b \iff a = a'k, b = b'k$   
 $\iff k(a'x + b'y) = 1 \quad \nabla \quad \text{bo } a'x + b'y \in \mathbb{Z} \quad \text{czyli } \text{NWD}(a, b) = 1$
- Zał. nie wprost  $\text{NWD}(a, y) \neq 1 = k \iff k \mid a \wedge k \mid y \iff a = a'k, y = y'k$   
 $\iff k(a'x + y'b) = 1 \quad \nabla \quad \text{bo } a'x + y'b \in \mathbb{Z}$

( $a', y' \in \mathbb{Z}$ )

• (dla kolejnych dwóch przykładeów postępujemy analogicznie)

• mamy więc  $\text{NWD}(a, b) = \text{NWD}(a, y) = \dots = 1$  ■

• jeśli  $x > 0 \wedge y > 0$ :

$$1 = ax + by \geq a + b \geq 2 \quad \nabla$$

wobec tego  $x < 0 \vee y < 0$  ■

• jeśli  $x < 0 \wedge y < 0$ :

$$1 = ax + by \leq -(a + b) \leq -2 \quad \nabla$$

## Zadanie 1

$$f(n) = \sum_{k=1}^n \lceil \log_2 k \rceil \quad \text{teza: } f(n) = f(\lceil n/2 \rceil) + f(\lfloor n/2 \rfloor) + n - 1 \quad \text{dla } n \geq 1$$

$$\sum_{k=1}^n \lceil \log_2 k \rceil = \sum_{k=1}^{\lceil n/2 \rceil} \lceil \log_2 k \rceil + \sum_{k=\lceil n/2 \rceil+1}^n \lceil \log_2 k \rceil$$

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

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

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

zauważmy, że  $f(1) = 0$  jednoznacznie określa kolejne wartości:

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

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

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

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

## Zadanie 2

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

Fakt:  
 ~~$x$~~   $2^m \leq x < 2^{m+1}$   
 $m \leq \log_2 x < m+1$   
 t.e. zależność spełnia  
 $2^m$  liczb (naturalnych)

$$\begin{aligned} f(n) &= 1 \cdot \lceil \log_2 2 \rceil + 2 \cdot \lceil \log_2 4 \rceil + 4 \cdot \lceil \log_2 8 \rceil + \dots + 2^{\lfloor \log_2 n \rfloor - 1} \cdot \lceil \log_2 2^{\lfloor \log_2 n \rfloor} \rceil + \\ &+ \sum_{i=2^{\lfloor \log_2 n \rfloor} + 1}^n \lceil \log_2 i \rceil = \sum_{k=1}^{\lfloor \log_2 n \rfloor} 2^{i-1} \cdot i + \sum_{k=\lfloor \log_2 n \rfloor + 1}^n \lceil \log_2 k \rceil = \\ &= \sum_{k=1}^{\lfloor \log_2 n \rfloor} 2^{i-1} i + (n - (2^{\lfloor \log_2 n \rfloor} + 1) + 1) \lceil \log_2 n \rceil = \sum_{k=1}^{\lfloor \log_2 n \rfloor} 2^{i-1} i + \\ &\quad + (n - 2^{\lfloor \log_2 n \rfloor}) \lceil \log_2 n \rceil \end{aligned}$$

Lemat:

$$\begin{aligned} S &= \sum_{i=1}^m i \cdot 2^i = ? \quad S = 2S - S = \sum_{i=1}^m i 2^{i+1} - \sum_{i=1}^m i \cdot 2^i = \\ &= \sum_{i=2}^{n+1} (i-1)2^i - \sum_{i=1}^n i \cdot 2^i = m2^{n+1} - 2 + \sum_{i=2}^n (i-1)2^i - \sum_{i=2}^n i2^i = \\ &= m2^{n+1} - 2 + \sum_{i=2}^n 2^i = m2^{n+1} - 2 - \frac{2^2(2^{n-1}-1)}{2-1} = \\ &= m2^{n+1} - 2 - 2^{n+2} + 4 = (m-1)2^{n+1} + 2 \end{aligned}$$

Wobec tego  $\sum_{k=1}^{\lfloor \log_2 n \rfloor} 2^{i-1} i = \frac{1}{2}((\lfloor \log_2 n \rfloor - 1)2^{\lfloor \log_2 n \rfloor + 1} + 2) =$

$$= (\lfloor \log_2 n \rfloor - 1)2^{\lfloor \log_2 n \rfloor} + 1 \quad \text{Można więc teraz obliczyć } f(n):$$

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

Lemat: (do zad. 3)

$$S(n) = \sum_{i=2}^n a_i F_i < F_{n+1} \quad , \quad a_i \in \{0,1\} , \quad \forall j \quad a_j + a_{j+1} \leq 1$$

+ indukcyjnie:

$$\bullet n=2 \quad F_2 < F_3 \quad \checkmark$$

$$\bullet \exists a_i . \exists e \quad \forall m < n$$

$$\cancel{\sum_{i=2}^n} S(m) < F_{m+1}$$

rozważmy  $S(m)$ :  $a_m$  niech będzie równa 1 (jeśli  $a_m=0$ , to  $S(m) \leq S(m-1) < F_m$ )

wtedy  $a_{m-1}=0$ .

Zauważmy, że  $S(m) - F_m \leq S(m-2) < F_{m-1}$ , więc

$$S(m) < F_{m-2} + F_m = F_{m+1} \quad \blacksquare$$

✓

### Zadanie 3

VII Kazda liczba  $n$  ma reprezentację w ukl. liczb Fibonacciego

- jeśli  $n$  jest liczbą Fib., to oczywiście ma reprezentację
- zauważmy więc, że  $n$  nie jest liczbą Fib. i przeprowadźmy indukcję:

① Baza:  $n=4$ .  $4 = 3 + 1 = 1 \cdot F_2 + 0 \cdot F_3 + 1 \cdot F_4$  ✓

② Zał. że  $\forall m < n$  m ma przedstawienie.

Zauważmy, że  $n$  znajduje się między pewnymi dwiema liczbami Fib:

$$F_i < n < F_{i+1}$$

~~Istnieje reprezentacja~~

(\*)  $n - F_i$  ma reprezentację (z zał. ind.)

(\*\*)  $n - F_i < F_{i-1}$ , bo  $n < F_{i+1}$

Jeli więc istnieje reprezentacja  $n$ , to musi się koniecznie skończyć:  $\dots + 0 \cdot F_{i-1} + 1 \cdot F_i$  (\*\*), a skoro (\*) to  $n$  ma reprezentację w tym układzie. ✓

Dowód jednoznaczności:

A, B - różne reprezentacje  $n$  i  $A \neq B$  (chcemy wykazać spójność)

$$\sum A = \sum B = n \quad \text{więc } A' = A \setminus B, B' = B \setminus A$$

mamy więc  $\sum A' = \sum B'$ . Ponieważ  $A \neq B$ , to  $A', B'$  są niepuste.

Wówczas  ~~$F_A = \max(A')$~~   $F_A = \max(A')$ , analogicznie  $F_B$ .

$F_A \neq F_B$  z definicji  $A' \cap B' = \emptyset$ . Zauważmy, że  $F_A < F_B$  (bez straty ogólności)

Z lematu mamy  $\sum A' < F_{A+1}$ .

Jednak  $\sum B' \geq F_{A+1}$ , bo  $F_A < F_B$  więc spójność ✓

Tak więc ta liczba l. naturalna ma reprezentację w takim układzie i ta reprezentacja jest jednoznaczna.

## Zadanie 12.

poznamy, że  $\text{NWD}(F_{m-1}, F_m) = 1$

① Baza: dla  $n=1$  mówiąc mniej oznacza:  $\text{NWD}(0, 1) = 1$

② zał. że  $\forall_{m \in \mathbb{N}} \text{NWD}(F_{m-1}, F_m) = 1$

$$\text{NWD}(F_n, F_{n-1}) = \text{NWD}(F_{n-1}, F_{n-2}) = 1$$

poznamy, że  $\text{NWD}(F_m, F_n) = F_{\text{NWD}(m, n)}$

gdzie  $m=n$ :  $\text{NWD}(F_n, F_n) = F_n$ , więc mniej

niech więc  $m > n$  i zał. bez straty ogólności  $m > n$

Demat 1  $m \mid n \Rightarrow F_m \mid F_n$

$m \mid n$  czyli  $\exists a \in \mathbb{N}$ :  $m = a \cdot n$

wiemy (z wykładowca):  $F_{n+m+1} = F_{n+1}F_{m+1} + F_nF_m$  (1)

Przeprowadźmy indukcję po  $a$ :

①  $a=1$ , czyli  $m=n$   $F_n \mid F_n$  ✓

② niech  $\forall a' < a \quad m = a'm \Rightarrow F_m \mid F_{a'm}$

z (1) mamy:  $F_{a'm} = F_n = F_m F_{(a-1)m+1} + F_{(a-1)m} F_{m+1}$

aby dowieść tego należy pokazać, że  $F_m \mid F_{(a-1)m} F_{m+1}$   
ponieważ oznacza  $F_m \mid F_{m} \cdot F_{(a-1)m+1}$ .

jednak z założenia ind. wiemy, że  $F_m \mid F_{(a-1)m}$ , więc

$\bullet F_m \mid F_n$  ✓

Demat 2,  $\text{NWD}(F_m, F_{qm+r}) = \text{NWD}(F_m, F_r)$

$$\text{NWD}(F_m, F_{qm+r}) = \text{NWD}(F_m, F_{qm+2}F_r + F_{qm}F_{r-1}) \stackrel{\text{L1}}{=}$$

$$= \text{NWD}(F_m, F_{qm+2}F_r) \stackrel{\text{bo}}{=} \text{NWD}(F_m, F_r)$$

Indukcja po  $n$ : ① dla  $n=0$ :  $\text{NWD}(F_m, F_0) = F_m$  ✓

② zał. że  $\forall_{m < n} \text{NWD}(F_m, F_n) = F_{\text{NWD}(m, n)}$  ( $m < n$ )

niech  $n = qm+r$

$$\text{NWD}(F_n, F_m) = \text{NWD}(F_{qm+r}, F_m) \stackrel{\text{L2}}{=} \text{NWD}(F_r, F_m) \stackrel{\text{zał. ind.}}{=}$$

$$= F_{\text{NWD}(m, r)} = F_{\text{NWD}(m, n)}$$

zadanie 4  $x, k, n \in \mathbb{Z}$   $x^k \bmod n = ?$

$f(x, k, n)$ :

if ( $k == 0$ ) return  $1 \bmod n$

if ( $k == 1$ ) return  $x \bmod n$

tmp :=  $f(x, \lfloor \frac{k}{2} \rfloor, n)$

$\rightarrow$  if ( $k \bmod 2 == 0$ ) return  $(\text{tmp} * \text{tmp}) \bmod n$  (1)

$\rightarrow$  else return  $(x * \text{tmp} * \text{tmp}) \bmod n$  (2)

w najgorszym przypadku (dla  $x$  postaci  $2^l - 1$ ) wchodzimy do (2)  
w każdym wywołaniu wchodzimy do (2)

w najlepszym przypadku (dla  $x$  postaci  $2^l$ ) w każdym wywołaniu wchodzimy do (1)

~~~~~

$$T(k) \leq c(T(\lfloor \frac{k}{2} \rfloor) + 2) = c(T(\lfloor \frac{k}{4} \rfloor) + 2 + 2) = \dots = \\ = \underset{T(1)=0}{\cancel{c}} (T(\frac{k}{2^{l-1}}) + \lfloor \log_2 k \rfloor + 2) = \underset{T(1)=0}{\cancel{c}} 2 \cdot \lfloor \log_2 k \rfloor$$

$$T(k) \geq c'(T(\frac{k}{2}) + 1) = c' (T(\frac{k}{4}) + 1 + 1) = \dots \\ = c' (T(\frac{k}{2^l}) + \log_2 k) = c' \cdot \log_2 k$$

maranny więc

$$c' \cdot \log_2 k \leq T(k) \leq c \cdot 2 \cdot \lfloor \log_2 k \rfloor$$

z czego łatwo wywnioskować, że  $T(k) = \Theta(\log_2 k)$

FAKTY:

$$x^{2L} = x^L \cdot x^L$$

$$x^{2L+1} = x \cdot x^{2L}$$

$$xy \bmod n = (x \bmod n \cdot y \bmod n) \bmod n$$

zadanie 11

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

$$\text{czyli } \text{NWD}(721, 448) = 7$$

tak więc  $x=23, y=-37$

| 1234 | 333 |                                                       |
|------|-----|-------------------------------------------------------|
| 333  | 235 | $1234 - 3 \cdot 333$                                  |
| 235  | 98  | <del><math>809 - 2 \cdot 235</math></del> $333 - 235$ |
| 98   | 39  | $235 - 2 \cdot 98$                                    |
| 39   | 20  | $98 - 2 \cdot 39$                                     |
| 20   | 19  | $39 - 20$                                             |
| 19   | 1   | $20 - 19$                                             |
| 1    | 0   |                                                       |

$$333^{-1} = x = ?$$

$$333 \cdot x \pmod{1234} = 1$$

$$\text{skoro jednak } 63 \cdot 333 - 17 \cdot 1234 = 1,$$

$$\text{to } 333 \cdot 63 \pmod{1234} = 1$$

$$\text{więc } 333^{-1} \equiv 63 \pmod{1234}$$

$$\begin{aligned}
 7 &= 21 - 14 = 21 - (77 - 3 \cdot 21) = \\
 &= 4 \cdot 21 - 77 = 4 \cdot (98 - 77) - 77 = \\
 &= 4 \cdot 98 - 5 \cdot 77 = 4 \cdot 98 - 5(175 - 98) = \\
 &= 9 \cdot 98 - 5 \cdot 175 = 9 \cdot (273 - 175) - 5 \cdot 175 = \\
 &= 9 \cdot 273 - 14 \cdot 175 = 9 \cdot 273 - 14 \cdot (448 - 273) = \\
 &= 23 \cdot 273 - 14 \cdot 448 = 23 \cdot (721 - 448) - 14 \cdot 448 = \\
 &= \boxed{23 \cdot 721 - 37 \cdot 448}
 \end{aligned}$$

$$\begin{aligned}
 1 &= 20 - 19 = 20 - (33 - 20) = \\
 &= 2 \cdot 20 - 33 = 2 \cdot (33 - 2 \cdot 17) - 33 = \\
 &= 2 \cdot 33 - 5 \cdot 17 = 2 \cdot 33 - 5 \cdot (333 - 2 \cdot 98) = \\
 &= 12 \cdot 98 - 5 \cdot 235 = \\
 &= 12 \cdot (333 - 235) - 5 \cdot 235 = \\
 &= -17 \cdot 235 + 12 \cdot 333 = \\
 &= -17 \cdot (1234 - 3 \cdot 333) + 12 \cdot 333 = \\
 &= 63 \cdot 333 - 17 \cdot 1234
 \end{aligned}$$

$$\text{czyli } \boxed{y = -17, x = 63}$$

| 1313 | 69 |                      |
|------|----|----------------------|
| 69   | 2  | $1313 - 19 \cdot 69$ |
| 2    | 1  | $69 - 34 \cdot 2$    |
| 1    | 0  |                      |

$$\text{NWD}(1313, 69) = 1 \quad \checkmark$$

$$\begin{aligned}
 1 &= 69 - 34 \cdot 2 = 69 - 34 \cdot (1313 - 19 \cdot 69) = \\
 &= -34 \cdot 1313 + \boxed{647} \cdot 69
 \end{aligned}$$

$$69^{-1} \equiv 647 \pmod{1313}$$

$$-647 \equiv \boxed{666} \pmod{1313}$$