1. domácí úloha z MIN401, jaro 2023

Zadáno: 28. 2. 2023 Odevzdejte do: 28. 3. 2023

Definice. *Výškou Euclidova algoritmu* $h(a)$ čísla $a \in \mathbb{N}, a \geq 2$ označme největší potřebný počet kroků Euclidova algoritmu pro výpočet $\mathrm{NSD}(a, b)$ ze všech čísel $b \in N$, $b < a$.

Poznámka. Např. $h(4) = h(3) = 2$. Pouze pro $a = 2$ platí $h(a) = 1$.

Definice. Fibonacciho posloupnosti $\{f_k\}_{k=0}^{\infty} = \{0, 1, 1, 2, 3, 5, 8, 13, 21, \dots\}$ je posloupnost zadaná rekurentně:

$$f_0 \coloneqq 0, \quad f_1 \coloneqq 1, \quad f_n \coloneqq f_{n-1} + f_{n-2} \quad \text{pro } n \geq 2.$$

Zadání. *Dokažte, že pro libovolné číslo $f_n, n \geq 3$ z Fibonacciho posloupnosti platí:*

$$h(f_n) = n - 2.$$

Hint: *Začněte důkazem, že Euclidův algoritmus pro* $\mathrm{NSD}(f_n, f_{n-1})$ *má* $n - 2$ *kroků. (A taky si uvědomte, že tento samotný fakt ještě nestačí. ☺)*

Další hint: *Důkaz z předešlého* hintu *nám dokazuje, že* $h(f_n) \geq n - 2$*, takže je potřeba ještě ukázat* $h(f_n) \leq n - 2$*. Toho lze určitě dosáhnout vícero způsoby. Já bych rovnou dokázal, že pro všechna* $a, b \in \mathbb{N}$ *taková, že* $f_n \geq a > b$*, má Euclidův algoritmus pro* $NSD(a, b)$ *nanejvýš* $n - 2$ *kroků. (Využije se silná indukce.)*

Poznámka. Pro ilustraci problému ukážeme průběh Euklidova algoritmu pro $\mathrm{NSD}(f_6, f_5)$.

$$\begin{array}{lllll} \text{1. krok} & 8 = 1 \cdot 5 + 3 & (f_6 = f_5 + f_4) & & \\ \text{2. krok} & 5 = 1 \cdot 3 + 2 & (f_5 = f_4 + f_3) & & \\ \text{3. krok} & 3 = 1 \cdot 2 + 1 & (f_4 = f_3 + f_2) & & \\ \text{4. krok} & 2 = 2 \cdot 1 + 0 & (f_3 = 2 \cdot f_2) & \to & \text{Konec algoritmu} \end{array}$$

Řešení. Nejprve dokážeme $h(f_n) \geq n - 2$, k tomu nám stačí ukázat, že Euklidův algoritmus pro $\mathrm{NSD}(f_n, f_{n-1})$ má $n - 2$ kroků. To nám totiž říká, že existuje nějaké $b \in \mathbb{N}$, $b < f_n$ takové, že Euclidův algoritmus pro $\mathrm{NSD}(f_n, b)$ má $n - 2$ kroků.

- Pro $n = 3$ počítáme $\mathrm{NSD}(2, 1)$ a Euclidův algoritmus (EA) má tento průběh:

  $$\text{1. krok} \quad 2 = 2 \cdot 1 + 0 \quad \to \quad \text{Konec algoritmu}$$

- Předpokládejme, že máme tvrzení dokázané pro nějaké $k \in \mathbb{N}$, $k > 3$ (tzv. *indukční předpoklad*). Ukážeme, že z toho plyne platnost tvrzení i pro $k + 1$. Protože $f_{k+1} - f_k = f_{k-1} < f_k$, pro dělení se zbytkem

  $$f_{k+1} = q \cdot f_k + r$$

  očividně máme $q = 1$ a $r = f_{k-1}$. To je 1. krok EA pro $\mathrm{NSD}(f_{k+1}, f_k)$.

  Do dalšího kroku EA tedy máme jako vstupní hodnoty f_k a f_{k-1}, tedy následující kroky jsou stejné, jako při výpočtu $\mathrm{NSD}(f_k, f_{k-1})$. Z indukčního předpokladu víme, že pro k tvrzení platí, tedy $\mathrm{NSD}(f_k, f_{k-1})$ spočítáme v $k - 2$ krocích.

  Dohromady tedy $\mathrm{NSD}(f_{k+1}, f_k)$ spočítáme v $1 + (k - 2) = (k + 1) - 2$ krocích. Tvrzení tedy platí i pro $k + 1$. Protože $k \in \mathbb{N}$ bylo libovolné, dokázali jsme tvrzení pro všechna $k \in \mathbb{N}$.

Nyní dokážeme, že pro všechna $2 \leq a \leq f_n$ je $h(a) \leq n-2$. Tím dostaneme jako speciální případ $h(f_n) \leq n-2$. Pro jednoduchost označme $\mathrm{pk}\,(a,b)$ *počet kroků EA* pro $\mathrm{NSD}(a,b)$. Podle definice platí $h(a) = \max_{2 \leq b < a}(\mathrm{pk}\,(a,b))$.

- Pro $n = 3$ je jediné $a = f_3 = 2$ a $h(2) = 1$.
- Pro[1] $n = 4$ máme možnosti $a = 2$ a $a = 3$. Pro oboje se snadno ukáže $h(a) \leq 2$.
- Předpokládejme, že máme tvrzení dokázané pro všechna k menší než nějaké $n \in \mathbb{N}$. Ukážeme, že z toho plyne tvrzení i pro n. Vezměme libovolné $a, b \in \mathbb{N}$ splňující $2 \leq a \leq f_n$, $b < a$. Chceme tedy ukázat, že $\mathrm{pk}\,(a,b) \leq n-2$. Mohou nastat dvě možnosti:

  1. $b \leq f_{n-1}$: Označme r zbytek po dělení a číslem b, tedy $\mathrm{pk}\,(a,b) = 1 + \mathrm{pk}\,(b,r)$. Protože $r < b < f_{n-1}$ (z def. dělení se zbytkem), dostáváme z indukční předpokladu

  $$\mathrm{pk}\,(a,b) = 1 + \mathrm{pk}\,(b,r) \leq 1 + (n-3) = n-2.$$

  2. $f_{n-1} < b$: Označme dělení se zbytkem $a = q \cdot b + r$. Protože

  $$a - b \leq f_n - b < f_n - f_{n-1} = f_{n-2},$$

  máme $q = 1$ a $r = a - b < f_{n-2}$. Nyní označme r' zbytek po dělení b číslem r. S využitím indukčního předpokladu dohromady dostáváme

  $$\mathrm{pk}\,(a,b) = 1 + \mathrm{pk}\,(b,r) = 2 + \mathrm{pk}\,(r,r') \leq 2 + (n-4) = n-2. \qquad \square$$

[1] Tento případ potřebujeme dokázat zvlášť kvůli druhé možnosti indukční části důkazu.