

Když do vzorce, který má pro funkci  $f : \mathbb{P} \rightarrow \mathbb{P}$  platit, dosadíme dvě stejná prvočísla  $p$ , dostaneme:

$$\text{NSD}(p, p) = p = \text{NSD}(f^p(p), f^p(p)) = f^p(p)$$

Tedy pro každé prvočíslu  $p$  musí platit, že  $f^p(p) = p$ .

Teď předpokládejme, že  $f(p) = x$ . Protože nutně platí, že  $f^x(x) = x$ , platí pak:

$$\begin{aligned} f^{p-1}(f(p)) &= f^{p-1}(x) = p \\ x = f(p) &= f(f^{p-1}(x)) = f^p(x) = f^x(x) \end{aligned}$$

Pokud  $p = x$ , pak podmínka zjevně platí a získáme z toho předpis funkce  $f(p) = p$ . Teď dokážu, že jenom tato funkce umí splnit tyto podmínky.

Předpokládejme, že  $p \neq x$ . Pak víme, že platí  $\text{NSD}(p, x) = 1$  a proto když do rovnice  $f^p(x) = f^x(x)$  budeme postupně dosazovat z jedné strany do druhé na principu Euklidova algoritmu, dostaneme  $f(x) = x$ . To je však ve sporu s tím, že  $f^p(p) = p$ , protože by z toho vyplývalo  $f^p(p) = f^{p-1}(f(p)) = f^{p-1}(x) = x$ .

Tím jsme tedy dokázali, že jediná platná funkce je  $f(p) = p$ . Q. E. D.