Teorie nejen čísel 3

3. seriálová série — Vzorové řešení

Úloha 1.

Je dáno přirozené číslo n. Nechť je A množina těch čísel $a \in \{1, 2, \ldots, n\}$, která splňují

$$a^2 \equiv a \pmod{n}.$$

Dokažte, že počet prvků A je mocnina dvojky. *(Matěj Doležálek)*

Řešení:
Kongruenci ze zadání si můžeme přepsat do tvaru $a(a-1) \equiv 0 \pmod{n}$. Nechť $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, pak se na tuto kongruenci můžeme podívat modulo $p_\ell^{\alpha_\ell}$, což nám dává kongruenci

$$a(a-1) \equiv 0 \pmod{{p_\ell}^{\alpha_\ell}}.$$

Z Eukleidova algoritmu víme, že čísla a a $a-1$ jsou nesoudělná. Vidíme také, že prvočíslo p_ℓ dělí alespoň jedno z čísel a a $a-1$. Rozeberme tedy dva případy. Za prvé prvočíslo $p_\ell \mid a$, pak z kongruence $a(a-1) \equiv 0 \pmod{p_\ell^{\alpha_\ell}}$ a nesoudělnosti a a $a-1$ platí také $a \equiv 0 \pmod{p_\ell^{\alpha_\ell}}$. Analogicky by dopadl případ, kdy $p_\ell \mid a-1$. Pak platí, že $a \equiv 1 \pmod{p_\ell^{\alpha_\ell}}$.

Nyní už vidíme, že každé a má po dělení $p_\ell^{\alpha_\ell}$ zbytek 0, nebo 1 pro všechna $1 \leq \ell \leq k$. Z toho plyne, že stačí ukázat, že pro každou sadu takovýchto zbytků umíme zkonstruovat právě jedno $a \in \{1, 2, \ldots, n\}$. Potom už bude mít množina A, která obsahuje všechna vyhovující a, velikost mocniny dvojky. Konkrétněji bude její velikost rovna 2^k.

Z Čínské zbytkové věty plyne, že pro každou sadu zbytků a nesoudělné moduly (což mocniny různých prvočísel rozhodně jsou) umíme nalézt právě jedno $a \in \{1, 2, \ldots, n\}$ modulo $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Také je jasně vidět, že se žádné dva prvky množiny A nerovnají, protože po dělení alespoň jedním prvočíslem mají jiný zbytek.

Poznámky:
Většina řešení byla jednoho ze dvou druhů. Buď jako vzorové řešení, nebo ta, která zkoušela odvodit obecný vzorec z malých případů, ale tato řešení nevedla ke zdárnému konci. *(Filip Čermák)*

Úloha 2.

Nekonečnou posloupnost $a_0, a_1, a_2, \ldots$ přirozených čísel nazvěme krutopřísnou, pokud je pro každé $n \in \mathbb{N}$ polynom

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

ireducibilní nad $\mathbb{Z}$. Najděte krutopřísnou posloupnost, v níž se vyskytují jen dva navzájem různé prvky. *(Matěj Doležálek)*

Řešení:
Zvolme libovolné prvočíslo p. Ukážeme, že vyhovuje posloupnost $1, p, p, p, \ldots$, tedy $a_0 = 1$ a následně $a_i = p$ pro každé přirozené i. Uvažme tedy přirozené číslo n a dokažme, že polynom

$$f = px^n + \cdots + px + 1$$

je ireducibilní. Ukážeme si dva způsoby.

Řešení modulením:
Předpokládejme pro spor, že f není ireducibilní, takže $f = gh$ pro nějaké polynomy g, h, které nejsou jednotky. Vidíme, že f je primitivní, tedy i g a h jsou primitivní, takže aby to nebyly jednotky, musí být nekonstantní.

Podívejme se na rovnost $f = gh$ modulo p. V polynomu f se zmodulením všechny koeficienty kromě absolutního členu vynulují, takže $\hat{f} = 1 \in \mathbb{Z}_p[x]$. Máme tak $1 = \hat{g} \cdot \hat{h}$ pro $\hat{g}, \hat{h} \in \mathbb{Z}_p[x]$. Pracujeme s polynomy nad tělesem, takže pro stupně platí

$$0 = \deg 1 = \deg \hat{g} + \deg \hat{h},$$

z čehož už nutně musí být $\deg \hat{g} = \deg \hat{h} = 0$. Oba $\hat{g}$, $\hat{h}$ jsou tedy konstantní. To znamená, že v polynomech g, h byly všechny koeficienty kromě absolutních členů násobky p. Dohromady tak máme polynomy

$$g = b_k x^k + \cdots + b_1 x + b_0,$$
$$h = c_\ell x^\ell + \cdots + c_1 x + c_0,$$

kde stupně k, ℓ jsou větší než 0 a všechny koeficienty b_i, c_i jsou pro $i \geq 1$ násobky p. Roznásobením bude zjevně v polynomu gh koeficient u x^n roven $b_k \cdot c_\ell$, takže $p = b_k \cdot c_\ell$. Jenže na pravé straně jsou obě b_k, c_ℓ násobky p, takže $p^2 \mid p$, což je spor. Polynom f tak určitě je ireducibilní.

Řešení Eisensteinovým kritériem:
Nahlédneme, že když v polynomu obrátíme pořadí koeficientů, jeho (i)reducibilita se nezmění. Namísto polynomu

$$f = a_n x^n + \cdots + a_1 x + a_0$$

tak můžeme uvažovat

$$\tilde{f} = a_0 x^n + \cdots + a_{n-1} x + a_n.$$

Všimněme si, že platí[1] $\tilde{f} = x^n \cdot f\left(\frac{1}{x}\right)$. S tím snadno nahlédneme, že obrácení pořadí koeficientů se chová hezky k násobení. Pokud $f = gh$ a máme $k = \deg g$, $\ell = \deg h$ (tedy $k + \ell = n$), pak i

$$\tilde{f} = x^n f\left(\frac{1}{x}\right) = x^n \cdot g\left(\frac{1}{x}\right) \cdot h\left(\frac{1}{x}\right) = x^k g\left(\frac{1}{x}\right) \cdot x^\ell h\left(\frac{1}{x}\right) = \tilde{g} \cdot \tilde{h}.$$

Navíc zjevně platí, že g nebo h je jednotka, právě když $\tilde{g}$ nebo $\tilde{h}$ je jednotka. Z toho už plyne, že f je ireducibilní, právě když je ireducibilní $\tilde{f}$.

K vyřešení úlohy nám tedy stačí ukázat, že polynom

$$\tilde{f} = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n. = x^n + p x^{n-1} + \cdots + px + p$$

je ireducibilní. To však platí přímočarým použitím Eisensteinova kritéria.

[1] Tady se dopouštíme trochu neformální úpravy: $\frac{1}{x}$ není polynom, takže striktně podle seriálové definice tento výraz nemůžeme dosadit. Když si však řekneme, že x je (nenulové) reálné číslo, bude vše v pořádku. V dalších úpravách zjistíme, že $\tilde{f}$ a $\tilde{g} \cdot \tilde{h}$ se shodují v nekonečně mnoha bodech (všech nenulových reálných x), takže už se rovnají jako polynomy.

Poznámky:
Jak na takovou posloupnost přijít? Kdybychom chtěli pomocí Eisensteinova kritéria vyrábět ireducibilní polynomy, které mají jako koeficienty jen dvě různá čísla, přijdeme na přímočarou volbu $x^n+px^{n-1}+\cdots+px+p$. Potom už stačí obrátit pořadí koeficientů. Z Eisensteinova kritéria lze taky vidět, že kromě $(1, p, p, \dots)$ uspějí i o něco obecnější konstrukce posloupností, např. $(a, b, b, \dots)$ pro a nesoudělné s bezčtvercovým b.

Poznamenejme také, že řešení modulením i řešení Eisensteinovým kritériem dělají ve skutečnosti skoro totéž, neboť Eisensteinovo kritérium jsme v seriálu dokázali dost podobným modulícím argumentem. *(Matěj Doležálek)*

Úloha 3.

Uvažujme zobrazení $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}$, která splňují:

(i) *Pro libovolný polynom $f \in \mathbb{Z}[x]$ platí $\varphi(f+1) = \varphi(f)+1$.*
(ii) *Pokud pro polynomy $f, g \in \mathbb{Z}[x]$ platí $f \mid g$ a zároveň $\varphi(f) \neq 0$, pak už $\varphi(f) \mid \varphi(g)$.*

Dokažte, že pro každé φ splňující tyto podmínky musí existovat celé číslo $z \in \mathbb{Z}$ takové, že pro každé $f \in \mathbb{Z}[x]$ platí $\varphi(f) = f(z)$. *(Matěj Doležálek)*

Řešení:
Za z zvolme obraz polynomu x v zobrazení φ a ukažme, že pak už platí $\varphi(f) = f(z)$ pro všechna f. Pro přirozené číslo n můžeme opakovaným použitím podmínky (i) dostat

$$\varphi(f+n) = \varphi(f+n-1)+1 = \cdots = \varphi(f)+n.$$

Dále když místo f uvážíme $f-1$, dostaneme vztah $\varphi(f-1) = \varphi(f-1+1)-1 = \varphi(f)-1$, takže opět indukcí dostaneme $\varphi(f-n) = \varphi(f)-n$. Dohromady tedy platí $\varphi(f+n) = \varphi(f)+n$ pro libovolné $n \in \mathbb{Z}$.

Vezměme nyní libovolný celočíselný polynom h a k němu libovolné přirozené číslo a. Ukážeme, že celé číslo $\varphi(h)-h(z)$ je násobek a. To už bude znamenat $\varphi(h)-h(z) = 0$, neboť každé nenulové celé číslo má jen konečně mnoho dělitelů. Podmínka (ii) nám garantuje dělitelnost, zvolme v ní proto nejprve f tak, aby $\varphi(f) = a$. To určitě nastane, když vezmeme $f(x) = x+a-z$, neboť $\varphi(f) = \varphi(x)+a-z = z+a-z = a$. Dále využijeme toho, že rozdíl argumentů dělí rozdíl hodnot, takže $f(x) = x-(z-a) \mid h(x)-h(z-a)$. Když tedy v (ii) vezmeme $g(x) = h(x)-h(z-a)$, obdržíme

$$a = \varphi(f) \mid \varphi(g) = \varphi\Big(h(x)-h(z-a)\Big) = \varphi(h)-h(z-a),$$

kde využíváme, že $h(z-a)$ je prostě nějaké celé číslo. Na závěr použijeme

$$a = z-(z-a) \mid h(z)-h(z-a),$$

takže i $\varphi(h)-h(z) \equiv \Big(\varphi(h)-h(z-a)\Big)-\Big(h(z)-h(z-a)\Big) \equiv 0 \pmod a$, jak jsme chtěli.

Celé číslo $\varphi(h)-h(z)$ tak má nekonečně mnoho dělitelů, a tudíž $\varphi(h) = h(z)$.

Poznámky:
Řešení úlohy mělo v zásadě dva důležité kroky: uvědomit si, že za z chceme zvolit $z = \varphi(x)$, a následně z podmínek (i) a (ii) vyrobit nekonečně mnoho dělitelností (resp. kongruencí), které dohromady dokáží rovnost $\varphi(h) = h(z)$. Všechna řešení, která obdržela nějaké body, se ubírala nějakým podobným směrem. *(Matěj Doležálek)*