BRněnský KOrespondenční Seminář

XXXI. ročník
2024/2025

řešení 2. série

Zbytky

úloha 2.1 - Nalezněte všechna $k \in \mathbb{N}$, pro která je rovnice

$$4n^3 + 3n^2 - n \equiv 0 \mod k$$

splněna pro všechna $n \in \mathbb{N}$.

řešení: Označme levou stranu rovnice jako $L(n)$. Jelikož má být rovnice splněna pro všechna n, musí také platit pro $n = 1$. Jednoduchým výpočtem zjišťujeme, že $L(1) = 6$. Nyní tedy požadujeme $6 \equiv 0 \mod k$. Jedinými vyhovujícími k tedy mohou být čísla $1, 2, 3, 6$.

Nyní jsou dva způsoby jak úlohu dokončit:

1: Podíváme se na levou stranu modulo 2 a 3. $1|L(n)$ platí triviálně a dělitelnost 6 plyne z dělitelnosti 2 a 3.

Dělitelnost 2: Platí $L(n) \equiv n^2 - n \equiv (n-1)n \mod 2$. Tedy $L(n)$ dá po dělení 2 stejný zbytek jako výraz $(n-1)n$, který je ale součinem dvou po sobě jdoucích čísel, tedy je vždy dělitelný 2. Pak také platí $2|L(n)$.

Dělitelnost 3: Platí $L(n) \equiv n^3 - n \equiv (n-1)n(n+1) \mod 3$. Obdobný argument, jde o součin tří po sobě jdoucích čísel, tedy je dělitelný třemi. Pak také $3|L(n)$.

Díky tomu zjišťujeme, že řešením úlohy jsou všechna z čísel $k = 1, 2, 3, 6$.

2: Matematická indukce: pokud by číslo 6 bylo řešením našeho příkladu, byli by řešením i všichni jeho dělitelé, tedy bychom vyřešili všechny případy najednou. Dokažme tedy indukcí, že $L(n) \equiv 0 \mod 6$.

Bázový krok: Pro $n = 1$ platí $L(1) = 6 \equiv 0 \mod 6$.

Indukční krok: Nechť $L(n) \equiv 0 \mod 6$, upravujme

$$L(n+1) = 4(n+1)^3 + 3(n+1)^2 - (n+1) = 4n^3 + 12n^2 + 12n + 4 + 3n^2 + 6n + 3 - n - 1 = 4n^3 + 15n^2 + 17n + 6$$

Označme $4n^3 + 15n^2 + 17n + 6 \equiv x \mod 6$. Využijeme indukční předpoklad a odečteme jej od obou stran rovnice:

$$(4n^3 + 15n^2 + 17n + 6) - (4n^3 + 3n^2 - n) \equiv x - 0 \mod 6$$

$$18n^2 + 18n + 6 \equiv x \mod 6$$

Odtud je již jasně vidět, že číslo 6 dělí levou stranu, tedy $x = 0$, což jsme chtěli dokázat.

úloha 2.2 - Určete poslední dvojčíslí čísla $15^{15^{15}}$. Uveďte postup bez kalkulačky.

řešení: Nejprve si uvědomíme, že poslední dvojčíslí sexy patnáctky je její zbytek po dělení číslem 100. Označíme toto číslo n a můžeme psát:

$15^{15^{15}} \equiv n \pmod{100}$

K dalšímu postupu využijeme Čínskou zbytkovou větu, která nám říká, že si náš problém můžeme rozdělit na následující dvě kongruence:

$15^{15^{15}} \equiv n \pmod{4}$

$15^{15^{15}} \equiv n \pmod{25}$

Jelikož 4 a 25 jsou čísla nesoudělná, můžeme podle výše zmíněné věty říci, že $\exists! n < 4 \cdot 25$ takové, že splňuje obě kongruence. Tedy jestliže najdeme n splňující tyto podmínky, máme jistotu, že se jedná skutečně o poslední dvojčíslí sexy patnáctky.

Podívejme se na první kongruenci. Přímo z definice a vlastností kongruencí plyne:

$15 \equiv -1 \pmod 4 \Rightarrow 15^{15^{15}} \equiv (-1)^{15^{15}} \equiv -1 \equiv 3 \pmod 4 \Rightarrow n \equiv 3 \pmod 4$

Poznamejme ještě, že jsme využili faktu, že $15^{15} = 225$ je liché číslo. Dále upravme sexy patnáctku na vhodnější tvar.

$15^{15^{15}} = 15^2 \cdot 15^{15^{15}-2} = 25 \cdot 9 \cdot 15^{15^{15}-2}$,

z čehož jednoznačně plyne $25 | 15^{15^{15}} \Rightarrow 25 | n \Rightarrow n \equiv 0 \pmod{25}$.

Nyní již víme, že hledáme $n < 100$ takové, že $25 | n \wedge n \equiv 3 \pmod 4$. Snadno zjistíme, že tyto podmínky splňuje číslo 75.

Poslední dvojčíslí sexy patnáctky je 75.

Úloha 2.3 - Dokažte, že existuje nekonečně mnoho přirozených čísel, která nelze zapsat ve tvaru $n^{2a} + m^{2b} + 4^c$, kde a, b, c, m, n jsou nezáporná celá čísla a $c \neq 0$.

Řešení: Nejdůležitější myšlenkou řešení bylo podívat se na výraz $n^{2a} + m^{2b} + 4^c$ modulo čtyřmi. Máme

$$n^{2a} + m^{2b} + 4^c = (n^a)^2 + (m^b)^2 + 4^c \equiv (n^a)^2 + (m^b)^2 \bmod 4.$$

Využili jsme toho, že $c \geq 0$, a tak výraz 4^c dává po dělení 4 zbytek 0.

Podívejme se, jaké zbytky mohou dát ostatní dva členy. Oba jsou druhými mocninami nějakého přirozeného čísla a ty nám mohou dát následující zbytky:

$$\begin{aligned} 0^2 &= 0, \\ 1^2 &= 1, \\ 2^2 &= 4 \equiv 0, \\ 3^2 &= 9 \equiv 1. \end{aligned}$$

Dostáváme tedy pouze 3 možnosti:

$$\begin{aligned} (n^a)^2 \equiv (m^b)^2 \equiv 0 \bmod 4 &\Rightarrow n^{2a} + m^{2b} + 4^c \equiv 0 \bmod 4, \\ (n^a)^2 \not\equiv (m^b)^2 \bmod 4 &\Rightarrow n^{2a} + m^{2b} + 4^c \equiv 1 \bmod 4, \\ (n^a)^2 \equiv (m^b)^2 \equiv 1 \bmod 4 &\Rightarrow n^{2a} + m^{2b} + 4^c \equiv 2 \bmod 4. \end{aligned}$$

Ukázali jsme, že ani v jednom případě nemůže nastat $n^{2a} + m^{2b} + 4^c \equiv 3 \bmod 4$. Tedy žádné číslo dávající zbytek 3 po dělení čtyřmi nemůžeme zapsat tímto způsobem. To jsou všechna čísla tvaru $4k+3$ pro nějaké nezáporné celé k, kterých je nekonečně mnoho, proto je důkaz tímto hotov.

Poznámka: Úlohu lze řešit i v případě, že povolíme $c = 0$. Zkuste se na výraz analogicky podívat modulo osmi.

Úloha 2.4 - Zbytek $a \mod b$ nazvěme teseraktovým zbytkem modulo b, pokud existuje nějaké přirozené číslo x takové, že $a \equiv x^4 \mod b$. V závislosti na prvočíslu p určete počet teseraktových zbytků modulo p.

BRKOS Team

Řešení: Rozdělíme si řešení na tři případy $p = 2$, $p \equiv 1$ modulo 4 a $p \equiv 3$ modulo 4.

Nejprve si uvědomíme, že teseraktový zbytek x je ve skutečnosti pouze též kvadratický zbytek. Akorát pro něj musí existovat nějaký kvadratický zbytek y tak, že $x \equiv y^2$ modulo p. Dále víme, že pro libovolné zbytky k a $-k$ je jejich druhá mocnina stejný kvadratický zbytek. Z toho, že nenulových kvadratických zbytků modulo p je $\frac{p-1}{2}$, tedy přesně půlka nenulových zbytků, plyne, že pro každý nenulový kvadratický zbytek existují pouze 2 zbytky k a $-k$, jejichž druhou mocninou je tento zbytek. Pro nulu samozřejmě platí, že je teseraktovým zbytkem vždy.

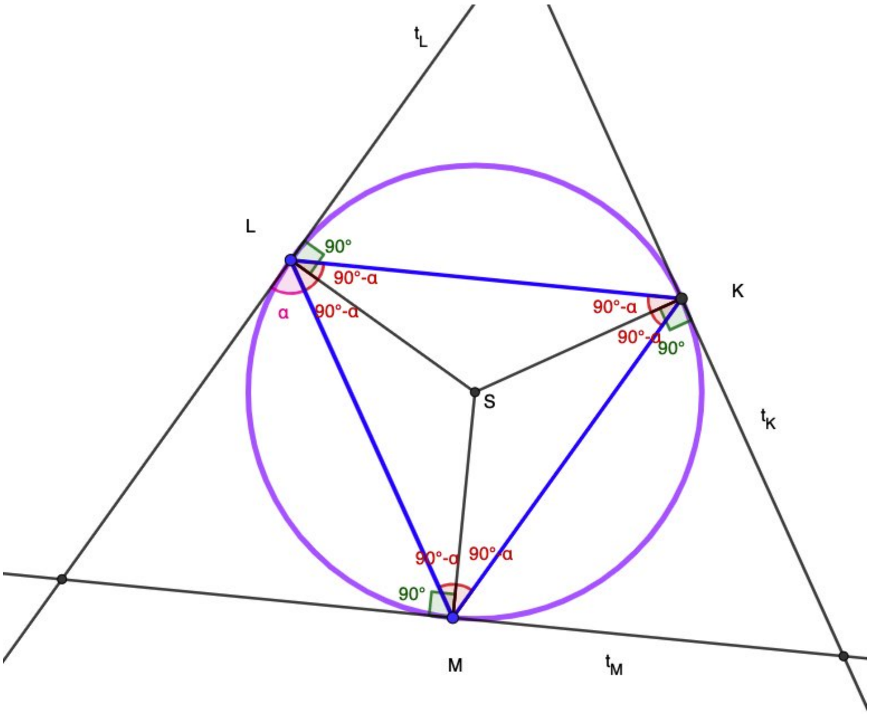
1) $p = 2$: V tomto případě jsou teseraktovými zbytky 0 i 1.

2) $p \equiv 3$ modulo p: v tomto případě ze studijního textu víme, že pokud k je kvadratický zbytek, tak $-k$ je kvadratický nezbytek. Tedy v každé dvojici k a $-k$ bude právě jeden kvadratický zbytek. Tudíž pro každý nenulový kvadratický zbytek x existuje kvadratický zbytek k tak, že $k^2 \equiv x$ modulo p. Proto každý kvadratický zbytek je i teseraktovým zbytkem a v tomto případě dostaneme $\frac{p+1}{2}$ teseraktových zbytků.

3) $p \equiv 1$ modulo p: v tomto případě víme, že pokud je k kvadratický zbytek, tak je i $-k$ kvadratický zbytek. Tedy vždy dva kvadratické zbytky se pošlou na stejný teseraktový zbytek. Proto pouze půlka z nenulových kvadratických zbytků bude i teseraktovým zbytkem. Tedy po přičtení jedničky za nulový teseraktový zbytek dostaneme, že jich bude $\frac{p+3}{4}$.

Úloha 2.a - Ňouma se má jít střelit. Stojí v bodu L na kružnici k a střílí. Pod jakými úhly od tečny t ke kružnici k v bodě L musí vystřelit, aby se kulka dvakrát odrazila a opět jej zasáhla? Kulka se v kružnici odráží jako světlo od tečny v daném bodě.

Řešení: Začněme pořádným obrázkem. Pokud se má kulka dvakrát odrazit a pak Ňoumu střelit, bude muset trajektorie kulky vytvořit trojúhelník vepsaný nebo degenerovaný trojúhelník, ze kterého bude jen úsečka (to by se ale odrazil jen jednou a Ňoumu by už trefil, což nesplňuje zadání. Počítejme tedy s tím, že dráha kulky opisuje trojúhelník.



Nechť tedy Ňouma vystřelí pod úhlem α (prozatím berme jako ostrý, aby odpovídal nákresek), a odrazí se v bodě M a v bodě K. t_L bude tečna v bodě L. Spojnice středu a tečny musí dávat pravý úhel (jinak by to nebyla tečna) a proto $|\sphericalangle SLM| = 90° - \alpha$. Pak ale i $|\sphericalangle SML| = 90° - \alpha$, protože MSL je rovnoramenný trojúhelník. Ze zákona odrazu pak i $|\sphericalangle SMK| = 90° - \alpha$. Protože je SMK rovnoramenný tak získáme stejnými úvahami, že $|\sphericalangle MKS| = 90° - \alpha$ a $|\sphericalangle SKL| = 90° - \alpha$ a pak z rovnoramennosti SKL ještě, že $|\sphericalangle KLS| = 90° - \alpha$. Všechny vnitřní úhly v trojúhelníku jsou nyní stejné a to $180° - 2\alpha$. Zjevně tedy KLM musí být rovnostranný a $\alpha = 60°$.

Bereme-li, že dvě úsečky/přímky mohou svírat jen ostré úhly, pak $\alpha = 60°$ je skutečně jediné řešení. Pokud úhlem výstřelu od tečny myslíme třeba orientovaný úhel, musíme za řešení považovat i $\alpha = 120°$.

Úloha 2.b - Mějme tabulku 1×7. Na této tabulce hrají hru dva hráči. Jeden má červené kamínky a druhý modré. Hráči střídavě hrají tahy se svými kamínky podle následujících pravidel:

1) Na každém poli může být maximálně jeden kamínek.

2) Hráči se střídají po tazích, při každém tahu musí dojít k nějaké změně v tabulce.

2) Hráč může pohnout doprava svým již umístěným kamínkem v tabulce, jestliže při přesunu přeskočí alespoň jeden kamínek libovolné barvy a žádné prázdné pole.

3) V případě, že hráč nemůže či nechce udělat výše uvedený tah, musí umístit nový kámen své barvy na první neobsazené pole tabulky zleva .

4) Hráč prohrává, jestliže umístí kamínek na poslední pole v řadě (nejvíce vpravo).

Jako první hraje hráč s červenými kamínky. Určete, zda existuje výherní strategie pro některého z hráčů, formulujte ji a dokažte, že je výherní.

Řešení: Mějme tabulku 1×7. Na této tabulce hrají hru dva hráči. Jeden má červené kamínky a druhý modré. Hráči střídavě hrají tahy se svými kamínky podle následujících pravidel: 1) Na každém poli může být maximálně jeden kamínek. 2) Hráči se střídají po tazích, při každém tahu musí dojít k nějaké změně v tabulce. 2) Hráč může pohnout doprava svým již umístěným kamínkem v tabulce, jestliže při přesunu přeskočí alespoň jeden kamínek libovolné barvy a žádné prázdné pole. 3) V případě, že hráč nemůže či nechce udělat výše uvedený tah, musí umístit nový kámen své barvy na první neobsazené pole tabulky zleva . 4) Hráč prohrává, jestliže umístí kamínek na poslední pole v řadě (nejvíce vpravo). Jako první hraje hráč s červenými kamínky. Určete, zda existuje výherní strategie pro některého z hráčů, formulujte ji a dokažte, že je výherní.

Úloha 2.c - Dokažte, že omezená neprázdná množina v rovině nemůže být středově souměrná podle dvou a více různých středů. Množina se nazývá omezená, jestliže existuje kružnice s konečným poloměrem taková, že celá množina je uvnitř této kružnice.

Řešení: Předpokládejme pro spor, že existují alespoň dva různé středy S_1 a S_2, podle kterých je množina M souměrná. Bez újmy na obecnosti je můžeme umístit do roviny jako body o souřadnicích $S_1 = [0,0], S_2 = [1,0]$. Označme f_1 středovou souměrnost podle S_1 a f_2 středovou souměrnost podle S_2 Protože je M neprázdná, obsahuje nějaký bod X, označme si jeho souřadnice $[x,y]$. Podívejme se, jak se chovají f_1 a f_2. Dosadíme-li bod X do f_1, dostaneme bod $[-x,-y]$. Nyní druhé zobrazení. Vektor XS_2 je vektor $(1-x,-y)$. Tedy obraz $f_2(X)$ můžeme vyjádřit přičtením tohoto vektoru k bodu $[1,0]$ a dostaneme bod $X_1 = [-x+2,-y]$. Protože bod X patří do množiny M, patří do ní i jeho obraz X_1. Tento bod však musí mít obraz podle středu S_1, který bude $[x-2,y]$. Označme f toto složení $f_1 \circ f_2$. V souřadnicích je tedy $f([x,y]) = [x-2,y]$. Pokud budeme opakovat k-krát za sebou zobrazení f, dostaneme z bodu $[x,y]$ bod $[x-2k,y]$.

Množina M je omezená, proto musí existovat nějaká kružnice s celočíselným poloměrem a středem v X, která obsahuje všechny body M. Označme r poloměr kružnice s touto vlastností. Pokud budeme iterovat třeba r krát (stačí méně) zobrazení f na bod X, dostaneme $f^r([x,y]) = [x-2r,y] = L$. Bod L má x-souřadnici $x-2r$, což je megaspor s tím, že leží uvnitř kružnice se středem v X a poloměrem r.

Tedy taková množina neexistuje.

Úloha 2.d - Mějme trojúhelník ABC a ke každé straně rovnostranný trojúhelník připsaný (AXB, BYC, CZA). Dokažte, že se úsečky AY, BZ, CX protínají v jednom bodě.

Řešení: Označme si průsečík AY a BZ jako P a průsečík AY a CX jako R. Chceme tedy dokázat, že $P = R$.

Všimněme si, že trojůhelníky ABY a XBC jsou shodné podle věty *sus* a stejně tak i YCA a BCZ:

$|AB| = |XB|$; $|\measuredangle ABY| = |\measuredangle XBC| = \beta + 60°$; $|BY| = |BC|$

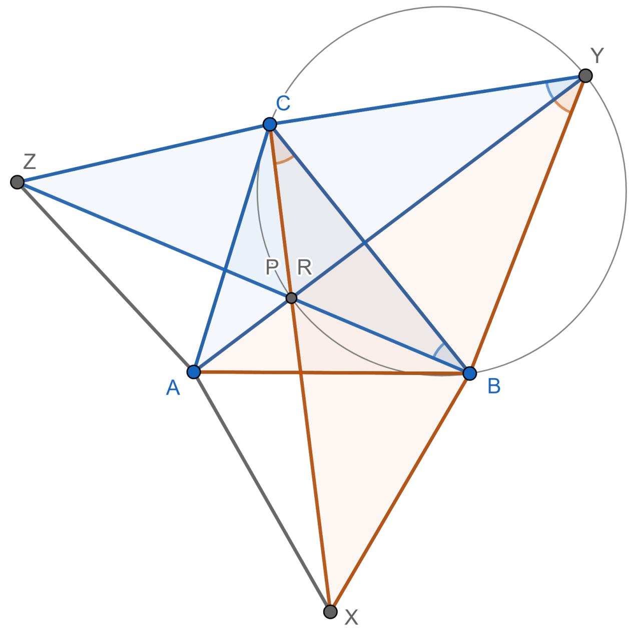
$|YC| = |BC|$; $|\measuredangle ACY| = |\measuredangle BCZ| = \gamma + 60°$; $|AC| = |ZC|$

Proto tedy $|\measuredangle PCB| = |\measuredangle PYB|$ => jsou to obvodové úhly nad PB => body P, B, Y, C leží na jedné kružnici.

Stejně tak $|\measuredangle RBC| = |\measuredangle RYC|$ => body R, B, Y, C leží na jedné kružnici.

Kružnice je jednoznačně určena třemi body (v tomto případě B, Y, C) => všech 5 bodů P, R, B, Y, C leží na jedné kružnici k.

Úsečka má s kružnicí maximálně dva průsečíky. Pokud se zaměříme na průsečíky AY s k: jeden průsečík je Y a druhý musí být $P = R$, protože oba tyto body leží jak na úsečce AY, tak i na kružnici k.



BRKOS Team