

Teorie nejen čísel 2

2. SERIÁLOVÁ SÉRIE

TERMÍN ODESLÁNÍ: 8. ÚNORA 2021

ÚLOHA 1. (5 BODŮ)
Najděte všechna kladná prvočísla p , pro něž existuje přirozené číslo n splňující $p - 1 \mid 2n + 2$ a zároveň $p \mid 2^{n-1} + 3$.

ÚLOHA 2. (5 BODŮ)
Přirozená čísla a, x, y splňují $x^2 - (a^2 + 1)y^2 = 1$. Dokažte, že $a^2 \mid x - 1$.

ÚLOHA 3. (5 BODŮ)
Je dáno přirozené číslo k takové, že $p = 4k - 1$ je prvočíslo. Dále po dvou nesoudělná přirozená čísla x, y, z splňují $x^2 + y^2 = z^k$. Dokažte, že $p \mid xy(x^2 - y^2)$.

Teorie nejen čísel 2

2. SERIÁLOVÁ SÉRIE

VZOROVÉ ŘEŠENÍ

Úloha 1.

Najděte všechna kladná prvočísla p , pro něž existuje přirozené číslo n splňující $p - 1 \mid 2n + 2$ a zároveň $p \mid 2^{n-1} + 3$. (Matěj Doležálek)

ŘEŠENÍ:

Ukážeme, že všechna řešení jsou 2, 11 a 13.

Jako první rozeberme případ $p = 2$, kde funguje $n = 1$, protože pro splnění podmínek stačí, aby $2^{n-1} + 3$ bylo sudé.

Dále předpokládejme $p > 2$. Zde můžeme použít malou Fermatovu větu společně s dělitelností ze zadání na to, abychom pro n vyhovující zadání vyjádřili dvojím způsobem 2^{2n+2} . Z první dělitelnosti máme $2n + 2 = k(p - 1)$, takže dostaneme

$$2^{2n+2} \equiv 2^{k(p-1)} \equiv (2^{p-1})^k \equiv 1^k \equiv 1 \pmod{p}.$$

Pokud naopak použijeme druhou dělitelnost, vyjde

$$2^{2n+2} \equiv 16 \cdot 2^{2(n-1)} \equiv 16 \cdot (2^{n-1})^2 \equiv 16 \cdot (-3)^2 \equiv 144 \pmod{p}.$$

Z toho už plyne $144 \equiv 1 \pmod{p}$. Po převedení na jednu stranu dostáváme $143 \equiv 0 \pmod{p}$, tedy $p \mid 143 = 11 \cdot 13$.

Prvočísla 11 a 13 naopak zadání skutečně splňují. Snadno ověříme, že pro $p = 11$ můžeme vzít třeba $n = 4$ a pro $p = 13$ kupříkladu $n = 11$.

POZNÁMKY:

Úloha se nás ptá na nějakou dělitelnost, kde se vyskytuje 2 umocněná na výraz v proměnné n . Už to by nás mělo navést na malou Fermatovu větu (popřípadě Eulerovu, ale máme zde prvočíslo, takže stačí Fermat).

Řešení, která byla ohodnocena čtyřmi a více body, šla cestou totožnou či velmi podobnou se vzorákem. Jeden bod byl většinou stržen za případ okolo $p = 2$, kde malá Fermatova věta pro základ 2 dělá trochu nepořádek. Dále jsem také strhával za používání pouze důsledkových úprav a následného neprovedení zkoušky, na to příště pozor! (Filip Čermák)

Úloha 2.

Přirozená čísla a, x, y splňují $x^2 - (a^2 + 1)y^2 = 1$. Dokažte, že $a^2 \mid x - 1$. (Matěj Doležálek)

ŘEŠENÍ:

Označme $d = a^2 + 1$, potom je zadaná rovnost obyčejná Pellova rovnice. Podívejme se tedy na jednotky v $\mathbb{Z}[\sqrt{d}]$. Pro $\omega = a + \sqrt{d}$ máme $N(\omega) = a^2 - (a^2 + 1) = -1$, takže existují jednotky s normou -1 , a proto i fundamentální jednotka má normu -1 . Zároveň $\omega = a + 1 + \sqrt{d}$ má nejmenší možnou složku u \sqrt{d} , takže už to určitě musí být fundamentální jednotka. Přesněji, je-li $u + v\sqrt{d}$

jednotka a $u, v > 0$, pak $v \geq 1$ a z $N(u + v\sqrt{d}) = \pm 1$ plyne $u^2 \geq -1 + dv^2 \geq -1 + d = a^2$, tedy $u \geq a$. Dohromady $u + v\sqrt{d} \geq a + \sqrt{d} = \omega$, což je tedy skutečně fundamentální jednotka.

Jelikož má tato fundamentální jednotka normu -1 , jsou řešení Pellovy rovnice vyjádřena přesně jako mocniny ω se sudými exponenty. Ze zadání máme, že $x + y\sqrt{d}$ je řešení Pellovy rovnice a zároveň jsou x i y kladná. To tedy znamená $x + y\sqrt{d} = \omega^{2n}$ pro nějaké přirozené n . Binomickou větou roznásobíme

$$(a + \sqrt{d})^{2n} = a^{2n} + \binom{2n}{1} a^{2n-1} \sqrt{d} + \binom{2n}{2} a^{2n-2} (\sqrt{d})^2 + \dots + \binom{2n}{2n-1} a (\sqrt{d})^{2n-1} + (\sqrt{d})^{2n}.$$

Když tedy v $x + y\sqrt{d} = (a + \sqrt{d})^{2n}$ posbíráme racionální členy, dostaneme

$$x = a^{2n} + \binom{2n}{2} a^{2n-2} d + \dots + \binom{2n}{2n-2} a^2 d^{n-1} + d^n.$$

Všechny sčítance kromě posledního obsahují a v alespoň druhé mocnině (a kombinační čísla jsou celá čísla), takže modulo a^2 zbudě

$$x \equiv d^n \equiv (a^2 + 1)^n \equiv (0 + 1)^n \equiv 1 \pmod{a^2},$$

tedy $a^2 \mid x - 1$.

POZNÁMKY:

Všechna správná řešení postupovala zhruba stejnou cestou jako vzorák. Drobnou odchylností mohlo být, že se z fundamentální jednotky $\omega = a + \sqrt{d}$ odvodí fundamentální řešení Pellovy rovnice $\omega_1 = \omega^2 = 2a^2 + 1 + 2a\sqrt{d}$, které se teprve mocní na n . Namísto binomické věty šlo také postupovat indukci podle n , což je v principu jen jiná formulace téhož. (Matěj Doležálek)

Úloha 3.

Je dáno přirozené číslo k takové, že $p = 4k - 1$ je prvočíslo. Dále po dvou nesoudělná přirozená čísla x, y, z splňují $x^2 + y^2 = z^k$. Dokažte, že $p \mid xy(x^2 - y^2)$. (Matěj Doležálek)

ŘEŠENÍ:

Nejprve si rozmyslíme, že $x + yi$ musí být v okruhu $\mathbb{Z}[i]$ součinem nějaké jednotky a k -té mocniny nějakého prvku, poté si dělitelnost $p \mid xy(x^2 - y^2)$ interpretujeme jako nějakou multiplikativní množinu S v konečném tělese $\mathbb{Z}[i]/(p)$ a následně tyto dva pohledy spojíme dohromady.

Ukažme $x + yi = u \cdot \alpha^k$ pro nějaké $\alpha \in \mathbb{Z}[i]$ a jednotku u . Pokud $k = 1$, pak je to triviální: prostě vezmeme $u = 1$ a $\alpha = x + yi$. Nadále předpokládejme $k \geq 2$. Rozložme rovnost $x^2 + y^2 = z^k$ v okruhu $\mathbb{Z}[i]$ na

$$(x + yi)(x - yi) = z^k.$$

Nahlédneme, že $x + yi$ a $x - yi$ jsou nesoudělná. Pro spor nechť mají společného dělitele $d \in \mathbb{Z}[i]$, který není jednotkou. Potom d dělí i

$$(x + yi) + (x - yi) = 2x \quad \text{a} \quad i(x - yi) - i(x + yi) = 2y,$$

takže norma $N(d)$ je společným dělitelem celých čísel $N(2x) = 4x^2$ a $N(2y) = 4y^2$. Jenže x, y jsou nesoudělná, takže $N(d) \mid 4$. Zároveň by ale $N(d) = 1$ znamenalo, že d je jednotka, takže už určitě $2 \mid N(d)$. To značí

$$2 \mid N(d) \mid N(x + yi) = x^2 + y^2 = z^k,$$

takže z je sudé. Ze vzájemné nesoudělnosti už pak musí x i y být lichá. Vzhledem ke kvadratickým zbytkům mod 4 to díky $k \geq 2$ znamená $0 \equiv z^k = x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod{4}$, což je spor. Určitě

jsou tedy $x + yi$ a $x - yi$ nesoudělná, takže podle tvrzení o nesoudělných mocninách z prvního dílu musí pro nějaké $\alpha \in \mathbb{Z}[i]$ a jednotku u platit $x + yi = u\alpha^k$, jak jsme chtěli.

Nyní tento rozklad na chvíli odložíme a podívejme se na $\mathbb{Z}[i]/(p)$. Jelikož p dává zbytek 3 modulo 4, víme z prvního dílu, že je to prvočinitel v $\mathbb{Z}[i]$. Příslušný okruh $\mathbb{Z}[i]/(p)$ je tak obor integrity a zároveň má jen konečně mnoho (p^2) prvků, takže je to těleso. Jeho prvky můžeme zapisovat jako $x + yi$, kde x a y jsou prvky \mathbb{Z}_p .

Podívejme se na množinu

$$S = \{x + yi \in \mathbb{Z}[i]/(p) : \text{platí } p \mid xy(x^2 - y^2) \text{ a zároveň } x + yi \neq 0\}$$

a ukažme, že je multiplikativní. Jelikož je p prvočíslo, dělitelnost $p \mid x \cdot y \cdot (x - y) \cdot (x + y)$ je ekvivalentní tomu, že jedno z x , y , $x + y$ nebo $x - y$ je nula v \mathbb{Z}_p . Když $x \equiv 0$, znamená to $x + yi \equiv a \cdot i$ pro $a \equiv y \in \mathbb{Z}_p$ a obdobně $y \equiv 0$ odpovídá násobkům 1. Stejně tak $x + y \equiv 0$ odpovídá násobkům $1 - i$ a $x - y \equiv 0$ značí násobek $1 + i$. Dohromady jsou prvky S přesně tvaru $a \cdot \lambda$ pro $a \in \{1, 2, \dots, p-1\}$ a $\lambda \in \{1, i, 1+i, 1-i\}$. Nyní je snadné ověřit, že součin každých dvou $\lambda_1, \lambda_2 \in \{1, i, 1+i, 1-i\}$ opět leží v S , z čehož plyne, že $a_1 \lambda_1 \cdot a_2 \cdot \lambda_2$ také leží v S . Tím jsme nahlédli, že S je multiplikativní množina.

Nechť je g primitivní prvek v $\mathbb{Z}[i]/(p)$. Ze seriálu víme, že každá multiplikativní množina se dá popsat jako

$$S = \{g^m, g^{2m}, \dots, g^{(n-1)m}\}$$

pro vhodné m , přičemž n je počet prvků uvažovaného tělesa, takže pro nás $n = p^2$. Následně má S přesně $\frac{n-1}{m}$ prvků. My ale dovedeme spočítat, kolik má naše S prvků: pro prvek $a \cdot \lambda$ máme 4 možnosti, jak vybrat $\lambda \in \{1, i, 1+i, 1-i\}$, a $p-1$ možností, jak vybrat $a \in \{1, 2, \dots, p-1\}$. Tento zápis $a \cdot \lambda$ je navíc jednoznačný, takže S má $4(p-1)$ prvků, z čehož

$$m = \frac{p^2 - 1}{4(p-1)} = \frac{p+1}{4} = \frac{4k-1+1}{4} = k.$$

Jinými slovy v S leží právě všechny k -té mocniny nenulových prvků $\mathbb{Z}[i]/(p)$.

S tím se můžeme vrátit k $x + yi = u\alpha^k$. Víme, že $x + yi \not\equiv 0 \pmod{p}$, protože x, y jsou nesoudělná, takže i $\alpha \not\equiv 0$, a tudíž modulo p máme $\alpha^k \in S$. Jednotka u je $1, i, -1$ nebo $-i$, což jsou také všechno prvky S . Z multiplikativnosti už tedy $x + yi = u \cdot \alpha^k \in S$, což značí $p \mid xy(x^2 - y^2)$, jak jsme chtěli.

POZNÁMKY:

Úloha se ukázala být těžká a přišla nám jen hrstka řešení. Žádnému jsem neudělil plný počet bodů, nicméně řešení *Matouše Šafránka* bylo správné až na pár (nezanedbatelných) detailů – na rozdíl od vzorového řešení nahlédl, že $(x + yi)^4$ má imaginární složku $4xy(x^2 - y^2)$, což mu umožnilo se namísto $4(p-1)$ -prvkové multiplikativní množiny S dívat na ty prvky $\mathbb{Z}[i]/(p)$, které umocněním na $p-1$ vyrobí 1, což jsou přesně ty s imaginární složkou 0 mod p . (Matěj Doležálek)