1. série

Téma: Diofantické rovnice

Termín odeslání: 14. října 2002

1. Úloha (3 body)

Nalezněte všechna řešení rovnice $x^2 + 2002y^2 = 7777xy - 2003$ v přirozených číslech.

2. Úloha (3 body)

V celých číslech řešte rovnici $a^2b + ab^2 = 2(a^3 + b^3)$.

3. Úloha (3 body)

Dokažte, že pro každé $\varepsilon > 0$ existuje číslo x z intervalu $\left(\frac{1}{4}, \frac{1}{4} + \varepsilon\right)$ takové, že rovnice

$$xabc = ab + bc + ca$$

má řešení v přirozených číslech a platí $a > b > c \geq 5$.

4. Úloha (5 bodů)

Ukažte, že rovnice $2^{2^n} + 1 = kp$ má pro pevné prvočíslo p maximálně jedno celočíselné řešení.

5. Úloha (5 bodů)

Ukažte, že rovnice $a^2 + b^2 + c^2 = d^3 + e^3$ má nekonečně mnoho celočíselných řešení takových, že čísla a, b, c, d a e jsou po dvou různá.

6. Úloha (5 bodů)

Řešte rovnici

$$1(1 + 2)(1 + 2 + 3) \cdots (1 + 2 + \cdots + (p - 2)) = pk + 2002,$$

kde p je prvočíslo a k je celé číslo.

7. Úloha (5 bodů)

Dokažte, že pro každé n přirozené existují x, y a z přirozená taková, že platí $x^2 + y^2 = z^n$.

8. Úloha (5 bodů)

Mějme přirozené číslo k. Vytvořme nyní posloupnost nul a jedniček tak, že n-tý člen je jedna právě tehdy, když má rovnice $1 + 2^2 + 3^3 + \cdots + n^n = kl$ řešení pro l přirozené. Zjistěte, pro která k je tato posloupnost periodická.

Řešení 1. série

1. úloha (56, 41, 2.00, 3.0)

Nalezněte všechna řešení rovnice $x^2 + 2002y^2 = 7777xy - 2003$ v přirozených číslech.

Podívejme se, jaký zbytek dávají obě strany rovnosti při dělení sedmi. Protože $2002 = 7 \cdot 286$, dává levá strana stejný zbytek jako výraz x^2, což je číslo z množiny $\{0, 1, 2, 4\}$ (tuto množinu dostaneme tak, že se podíváme, jaké zbytky po dělení sedmi dávají čísla 0^2, 1^2, ... , 6^2). Číslo 7777 jistě sedmi dělitelné je, $-2003 = 7 \cdot (-287) + 6$, pravá strana tedy při dělení sedmi dává zbytek 6. Pokud by se obě strany rovnaly, musely by se rovnat i jejich zbytky po dělení sedmi, což ale, jak vidíme, v našem případě nastat nemůže, rovnice proto v přirozených číslech žádné řešení nemá.

Poznámky k došlým řešením: Většina řešitelů postupovala shodně tak, že řešila rovnici modulo 7 (případně 11). V těchto případech se nevyskytly větší problémy a všichni řešitelé dostali za více či méně pěkné zápisy tohoto řešení po 3 bodech. Zbytek řešitelů postupoval nejčastěji řešením kvadratických rovnic pro x resp. y s parametrem y resp. x, či zkoumali paritu neznámých x a y. Buď však své řešení nedokončili, nebo se dopustili závažných chyb, takže tato řešení jsem většinou ohodnotil 0 body.

2. úloha (100, 80, 2.00, 2.0)

V celých číslech řešte rovnici $a^2b + ab^2 = 2(a^3 + b^3)$.

Nejprve si rovnici trochu poupravme na tvar

$$\frac{1}{2}ab(a+b) = (a+b)(a^2 - ab + b^2),$$

z něhož lze nahlédnout, že řešením jsou dvojice čísel $a, b \in \mathbb{Z}$, kde $a + b = 0$.

Hledáme-li jiná řešení, předpokládejme, že $a + b \neq 0$. Zkraťme rovnici nenulovým výrazem $a + b$ a k oběma stranám přičtěme $3ab$ (respektive odečtěme ab), dostáváme vztahy:

$$-\frac{1}{2}ab = (a-b)^2,$$

$$\frac{7}{2}ab = (a+b)^2.$$

Z první rovnice lze usoudit, že výraz ab je nekladný, z druhé, že je nezáporný. Celkově vychází ab nulový, ale pak z druhé rovnice $a + b = 0$. Jelikož jsme tuto možnost vyloučili, další řešení v celých číslech již neexistují.

3. úloha (54, 41, 2.00, 3.0)

Dokažte, že pro každé $\varepsilon > 0$ existuje číslo x z intervalu $\left(\frac{1}{4}, \frac{1}{4} + \varepsilon\right)$ takové, že rovnice

$$xabc = ab + bc + ca$$

má řešení v přirozených číslech a platí $a > b > c \geq 5$.

Protože a, b, c jsou kladná, je vydělení rovnice výrazem abc ekvivalentní úpravou a dostáváme:

$$x = \frac{1}{c} + \frac{1}{a} + \frac{1}{b}.$$

Volíme-li $b = 20$ a $c = 5$, dostáváme:

$$x = \frac{1}{4} + \frac{1}{a}.$$

Nyní už stačí volit $a > \frac{1}{\epsilon}$ a zároveň $a > b$ (takové a existuje), potom je splněna podmínka $a > b > c \geq 5$ a také $a > \frac{1}{\varepsilon} \Rightarrow \varepsilon > \frac{1}{a}$, čili $x = \frac{1}{4} + \frac{1}{a}$ leží v požadovaném intervalu. Tím je úloha vyřešena.

Poznámky k došlým řešením: Poměrně často se v řešeních vyskytovalo následující nedorozumění: interval $(\frac{1}{4}, \frac{1}{4} + \varepsilon)$ je **otevřený** interval, tedy množina všech bodů x takových, že $\frac{1}{4} < x < \frac{1}{4} + \varepsilon$; uzavřený interval, který obsahuje i svoje krajní body, se obvykle značí $\langle a, b\rangle$ nebo $[a, b]$. Ovšem ani pro uzavřený interval neplatí tvrzení podobná tomuto: „Existují přirozená čísla taková, která splňují danou rovnost pro krajní body daného intervalu. Proto ke každému bodu tohoto intervalu existují přirozená čísla, která splňují zadanou rovnost.“ Je totiž například zřejmé, že pro žádné iracionální číslo taková čísla neexistují. Někteří řešitelé se spokojili s tvrzením, že nějaká posloupnost je klesající pro rostoucí a a žádný její člen není menší než $\frac{1}{4}$. To ale není postačující podmínka pro splnění předpokladů ze zadání (a dokonce ani nutná): například o posloupnosti $2 + \frac{1}{n}$ můžeme říct totéž a přece neexistuje n takové, že $2 + \frac{1}{n} = \frac{1}{2}$, tj. pro $\varepsilon = \frac{1}{4}$ řešení neexistuje. Bylo tedy třeba najít obecné řešení pro libovolně malé ε.

4. úloha (45, 33, 3.00, 5.0)

Ukažte, že rovnice $2^{2^n} + 1 = kp$ má pro pevné prvočíslo p maximálně jedno celočíselné řešení.

Pro spor předpokládejme, že řešení mohou být dvě. Zjevně pomocí n je jednoznačně určeno k (p je pevné), tudíž se tato dvě řešení musí lišit v hodnotě n. Předpokládejme, že tedy máme dvě různe hodnoty l a m pro n, jež jsou řešením. Aby na levé straně rovnosti bylo celé číslo, musí být l i m nezáporné. Odtud $2^{2^l} \equiv -1 \pmod p$, ale i $2^{2^m} \equiv -1 \pmod p$. BÚNO (Bez újmy na obecnosti) můžeme předpokládat $l < m$, potom ale

$$2^{2^m} = 2^{2^{m-l} \cdot 2^l} = \left(2^{2^l}\right)^{2^{m-l}} \equiv (-1)^{2^{m-l}} = 1 \pmod p,$$

což je spor.

Poznámky k došlým řešením: Většina řešitelů si s úlohou poradila dobře. Objevovaly se jen drobné chyby, nejčastěji opomenutí toho, že neznámá n může být i záporná. Tento případ byl sice jednoduchý, nicméně za zmínku stál. Nakonec bylo dohodnuto, že se za to body strhávat nebudou. Všechna správná řešení si byla vesměs podobná.

5. úloha (51, 46, 3.00, 4.0)

Ukažte, že rovnice $a^2 + b^2 + c^2 = d^3 + e^3$ má nekonečně mnoho celočíselných řešení takových, že čísla a, b, c, d a e jsou po dvou různá.

Mějme libovolné přirozené číslo n větší než 2 (těch je jistě nekonečně mnoho) a uvažujme čísla n^2, $4n^2$, $2n^3$, $5n^3$ a $6n^3$. Díky volbě n jsou tato ostře uspořádána vzestupně podle velikosti, jsou tedy po dvou různá. Navíc platí

$$(2n^3)^2 + (5n^3)^2 + (6n^3)^2 = (2^2 + 5^2 + 6^2)n^6 = 65n^6 = (1^3 + 4^3)n^6 = (n^2)^3 + (4n^2)^3,$$

dostali jsme tedy nekonečně mnoho pětic vyhovujících zadání, navíc pro různá n se jedná o různé pětice (např. proto, že nejmenší číslo z nich – n^2 – je pro každé n jiné), úloha je tedy dokázána.

Poznámky k došlým řešením: Většina řešitelů správně pochopila, co znamená, že čísla jsou po dvou různá (tj. žádná dvě nejsou stejná) (to se ale nedá zapsat jako $a \neq b \neq c \neq d \neq e$), a našla nějaké obecné vyjádření $a, \dots, e$, které rovnost splňovalo. Mnozí postupovali způsobem podobným autorskému, časté bylo i rozložení rovnosti na $a = 0$, $b^2 = d^3$ a $c^2 = e^3$. Horší to už bylo s důkazem toho, že nalezená čísla $a, \dots, e$ jsou po dvou různá, případně s nalezením všech případů, kdy různá nejsou, a důkazem, že zbylých případů je nekonečně mnoho. Nemalé množství řešitelů při tom z nerovností, které mají platit, dokazovalo, že musí platit nějaké podmínky (použili implikaci špatným směrem), už ale nedokázali, že tyto podmínky stačí.

Jediný řešitel si uvědomil, že je potřeba napsat, že nalezené pětice čísel jsou navzájem různé, a obdržel $+i$. Dále jsem $+i$ dal dvěma řešitelům za vyřešení těžší úlohy.

6. úloha **(28, 19, 3.00, 5.0)**

Řešte rovnici

$$1(1+2)(1+2+3)\cdots(1+2+\cdots+(p-2)) = pk + 2002,$$

kde p je prvočíslo a k je celé číslo.

Nejprve si uvědomme vzorec $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$, který platí pro každé přirozené n. Ten lze dokázat například matematickou indukcí nebo úvahou, že

$$1 + 2 + 3 + \cdots + n = x$$

$$(1+n) + (2 + (n-1)) + (3 + (n-2)) + \cdots + (n+1) = x + x,$$

tedy $x = \frac{n(n+1)}{2}$.

Pro $p = 2$ úloha nedává smysl. Dále se pro $p \neq 2$ pokusme zjistit, jaký zbytek při dělení p dává výraz na levé straně rovnosti. Označme ho r, tedy

$$1\,(1+2)\,(1+2+3) + \cdots + (1+2+3+\cdots+(p-2)) \equiv r.$$

Užitím našeho vzorce dostáváme:

$$\frac{1\cdot 2}{2}\cdot\frac{2\cdot 3}{2}\cdot\frac{3\cdot 4}{2}\cdots\frac{(p-2)\,(p-1)}{2} \equiv r,$$

p a 2 jsou nesoudělná, tedy

$$(1\cdot 2)\cdot(2\cdot 3)\cdot(3\cdot 4)\cdots((p-2)\,(p-1)) \equiv r\cdot 2^{p-2}.$$

Nadále $-1 \equiv p - 1$ a p jsou nesoudělná, tedy

$$((p-1)!)^2 \equiv (-1)\cdot r\cdot 2^{p-2}.$$

Wilsonova věta říká, že pro p prvočíslo je $(p-1)! \equiv (-1) \pmod p$, užitím a vynásobením -2 získáváme:

$$-2 \equiv r \cdot 2^{p-1}.$$

Použitím Malé Fermatovy věty, která říká, že $a^{p-1} \equiv 1 \pmod p$ pro p prvočíslo a a a p nesoudělná, konečně máme

$$r \equiv -2.$$

Protože pravá strana dává zbytek 2002 při dělení p, musí p nutně dělit $2002-(-2)=2004$. Číslo 2004 má prvočíselný rozklad $2^2 \cdot 3 \cdot 167$, tedy p je rovno 3 nebo 167 (možnost 2 jsme již dříve vyloučili).

Pro $p=3$ dostáváme: $1=3k+2002$, neboli $k=-667$.

Pro $p=167$ dostáváme:

$$1\,(1+2)\,(1+2+3)+\cdots+(1+2+3+\cdots+165)=167k+2002,$$

s užitím součtového vzorce:

$$\frac{1\cdot 2}{2}\cdot\frac{2\cdot 3}{2}\cdot\frac{3\cdot 4}{2}\cdots\frac{165\cdot 166}{2}-2002=167k,$$

neboli

$$k=\frac{(165!)\,(166!)-2002\cdot 2^{165}}{2^{165}\cdot 167},$$

kde podle předchozího určení zbytku máme jistotu, že toto číslo je celé.

Úloha má dvě již zmiňovaná řešení.

Poznámky k došlým řešením: Riešiteľov, ktorý poslali tento príklad by sme mohli rozdeliť do dvoch množín. V jednej by boli tí čo poznali Wilsonovu a Malú Fermatovu vetu a vedeli čo to o kongurenciach a v tej druhej by boli ostatní. Tí z prvej množiny to potom mali vačšinou za 5 bodov a tí z druhej, bohužial, väčšinou 0. Najčastejšie nedostatky v riešení boli, že mnohí násobili (prípadne delili) kongurenciu nejakým výrazom bez toho aby ukázali, že je to ekvivalentná úprava a nakonci potom prehlásili, že pre $p=3$ a $p=167$ víde k isto celé, čo by ale nemuselo.

7. úloha **(66, 58, 4.00, 5.0)**

Dokažte, že pro každé n přirozené existují x, y a z přirozená taková, že platí $x^2+y^2=z^n$.

Následující odstavec přináší trikové řešení, avšak je k němu zapotřebí znalost komplexních čísel. Pokud ses s nimi doposud nesetkal, zkus požádat staršího kamaráda nebo svou učitelku matematiky, aby Ti pomohli se jimi prokousat. Nejprve uvažujme komplexní číslo $w=m+i$ s modulem φ. Volbou velkého přirozeného čísla m můžeme docílit toho, aby velikost modulu[1] byla $0<|\sphericalangle\varphi|<\frac{90^\circ}{n}$. Následně komplexní číslo w^n s modulem $n\varphi$ leží v prvním kvadrantu Gaussovy roviny, a tak $w^n=x+yi$ má souřadnice z přirozených čísel. Nyní zbývá jen označit $z=|w|$ a ověřit, že čísla x, y a z splňují rovnost ze zadání:

$$z^n=|w|^n=|w^n|=|x+yi|=x^2+y^2,$$

což již nečiní žádné obtíže.

[1]Modul je úhel, který svírá vektor určený komplexním číslem s kladnou poloosou x.

K nalezení řešení však nemusíme vůbec použít komplexních čísel. Postačí nalézt kupříkladu následující rovnosti:

$$1^2 + 2^2 = 5^1 \text{ a } 3^2 + 4^2 = 5^2.$$

Řešení je pak nasnadě – pouze rovnice vynásobíme několikrát číslem 5^2. Řešením pro liché $n = 2k + 1$ je $(1 \cdot 5^k)^2 + (2 \cdot 5^k)^2 = 5^{2k+1}$ a pro sudé $n = 2k$ je $(3 \cdot 5^{k-1})^2 + (4 \cdot 5^{k-1})^2 = 5^{2k}$.

Poznámky k došlým řešením: V zadaní úlohy vypadol predpoklad, že x, y, z majú byť po dvoch nesúdeliteľné, čím sa úloha podstatne zjednodušila. Väčšine riešiteľov teda nerobila problémy, *Víťa Kala* a *Honza Moláček* si vyslúžili $+2i$ vyriešením úlohy s pôvodným zadaním. Niektorí riešitelia považovali nulu za prirodzené číslo, potom však bola úloha celkom triviálna a keďže nula sa za prirodzené číslo väčšinou nepovažuje, dostali 0 bodov.

8. úloha (10, 6, 2.00, 4.0)

Mějme přirozené číslo k. Vytvořme nyní posloupnost nul a jedniček tak, že n-tý člen je jedna právě tehdy, když má rovnice $1 + 2^2 + 3^3 + \cdots + n^n = kl$ řešení pro l přirozené. Zjistěte, pro která k je tato posloupnost periodická.

Označme si onu posloupnost $\{A_n\}_{n=1}^{\infty}$, potom označme $\{a_n\}_{n=1}^{\infty}$ posloupnost zbytků při dělení k posloupnosti $\{1 + 2^2 + \cdots + n^n\}_{n=1}^{\infty}$ a $\{b_n\}_{n=1}^{\infty}$ posloupnost zbytků při dělení k posloupnosti $\{n^n\}_{n=1}^{\infty}$.

Nejprve si uvědomme, že posloupnost $\{b_n\}_{n=1}^{\infty}$ je pro každé k od jistého členu periodická. Délka periody (nikoliv nejkratší) je například $k!$. Abychom toto tvrzení dokázali, stačí dokázat, že

$$x^x \equiv (x + k!)^{x+k!} \pmod k$$

pro dostatečně vysoká x. Označme D největšího společného dělitele čísel k a x. Dále uvažujme

$$k = p_1^{q_1} p_2^{q_2} \cdots p_r^{q_r}$$

rozklad čísla k na součin prvočísel a

$$D = p_{\alpha_1}^{\beta_{\alpha_1}} p_{\alpha_2}^{\beta_{\alpha_2}} \cdots p_{\alpha_s}^{\beta_{\alpha_2}}$$

rozklad čísla D (jelikož D dělí k, je $\{\alpha_1, \alpha_2, \cdots, \alpha_s\} \subseteq \{1, 2, \cdots, r\}$ a $\beta_i \leq q_i$). Nyní si určeme D' jako:

$$D' = p_{\alpha_1}^{q_{\alpha_1}} p_{\alpha_2}^{q_{\alpha_2}} \cdots p_{\alpha_s}^{q_{\alpha_2}}.$$

D' je tedy součin prvočísel vyskytujících se v D v nejvyšší mocnině, ve které se vyskytují v k. D' je dělitel k, tedy $\exists l; k = lD'$, navíc l a D' obsahují různá prvočísla, jsou tedy nesoudělná. Nejprve dokažme, že

$$x^x \equiv (x + k!)^{x+k!} \pmod l,$$

totiž:

$$(x + k!)^{x+k!} \equiv x^{x+k!} = x^x x^{k!} \equiv x^x \pmod l.$$

První kongruence plyne z toho, že l dělí k, tedy i $k!$, druhá plyne z Eulerovy věty (počet dělitelů čísla l je menší než k, tedy dělí $k!$, navíc l a x jsou nesoudělná (kdyby byla soudělná, je tento dělitel i dělitelem k, což je spor s tím, že D bylo zvoleno jako největší společný dělitel k a x)).

Dále pro x, která jsou větší nebo rovné mocnině největšího prvočísla v prvočíselném rozkladu k je:

$$(x+k!)^{x+k!} \equiv x^{x+k!} \equiv 0 \equiv x^x \pmod{D'}.$$

První kongruence plyne z toho, že D' dělí k, tedy i $k!$, druhá a třetí plynou z toho, že exponenty jsou větší nebo rovné největším exponentům v prvočíselném rozkladu k, tedy i D', a přitom ta prvočísla, která ve svém rozkladu obsahují D', obsahují i x (D dělí x; D a D' obsahují tatáž prvočísla ve svém rozkladu). x^x a $(x+k!)^{x+k!}$ se rovnají modulo l i modulo D', tedy podle Čínské zbytkové věty (l a D' jsou nesoudělná, $k = lD'$) se rovnají i modulo k. Posloupnost $\{b_n\}_{n=1}^{\infty}$ je tedy od jistého členu (nejvýše nejvyšší exponent prvočísla obsažený v rozkladu k) periodická.

Nyní si uvědomíme, že i $\{a_n\}_{n=1}^{\infty}$ je od jistého členu periodická. Označme c první člen posloupnosti $\{b_n\}_{n=1}^{\infty}$, od kterého je periodická, a d délku periody téže posloupnosti. Uvědomme si, že $\{a_n\}_{n=c}^{\infty}$ (počínaje prvním členem) je periodická s (ne nutně nejmenší) délkou periody kd. Totiž pro $n \geq c$:

$$a_{n+kd} \equiv \sum_{i=1}^{n+kd} i^i = \sum_{i=1}^{n} i^i + \sum_{i=n+1}^{n+kd} i^i \equiv a_n + \sum_{i=n+1}^{n+kd} i^i \pmod{k},$$

kde

$$\sum_{i=n+1}^{n+kd} i^i = \sum_{i=0}^{k-1} \sum_{j=1}^{d} (n+id+j)^{n+id+j},$$

čili:

$$a_{n+kd} \equiv a_n + \sum_{i=0}^{k-1} \sum_{j=1}^{d} (n+id+j)^{n+id+j} \equiv a_n + \sum_{i=0}^{k-1} \sum_{j=1}^{d} (n+j)^{n+j} =$$

$$= a_n + k \sum_{j=1}^{d} (n+j)^{n+j} \equiv a_n \pmod{k}.$$

Druhá kongruence plyne z toho, že d je délka periody $\{b_n\}_{\infty}^{n=c}$ $(n+j > c)$. Tím je periodicita $\{a_n\}_{n=c}^{\infty}$ dokázána.

Jelikož je $\{a_n\}_{n=1}^{\infty}$ od jistého členu periodická, potom je nutně i $\{A_n\}_{n=1}^{\infty}$ od téhož členu periodická, neboť $A_n = 1 \Leftrightarrow a_n = 0$.

Tím je důkaz úlohy ukončen.

Poznámky k došlým řešením: Nesprávných řešení se nevyskytlo mnoho, k nim bych pouze dodal, že má-li se dokázat nějaké tvrzení pro všechna přirozená n, nestačí pouze prozkoumat několik prvních čísel, a to ještě špatně. Správných řešení bylo o něco více (i když také ne mnoho). *Honza Moláček* a *Daniel Petrík* dostali jeden imaginární bod za částečné zkoumání předperiody. Někteří řešitelé psali svá řešení stylem „opravující si po chvilce počítání odvodí, že zmiňovaná tvrzení opravdu plynou z předchozích“, a tak si vysloužili záporné imaginární body.