Povídání ke druhé sérii

Druhá série je věnována diofantickým rovnicím. To jsou rovnice, u nichž hledáme řešení jen mezi celými (případně přirozenými) čísly[1]. Na jejich řešení neexistuje nějaká obecná metoda, avšak při „louskání" těchto problémů můžeš s úspěchem aplikovat různé zajímavé vlastnosti celých čísel.

Je dobré si uvědomit například skutečnost, že druhá mocnina přirozeného čísla dává při dělení číslem 8 jeden z těchto tří zbytků: 0, 1, 4. Pomocí této vlastnosti můžeme ukázat, že neexistují celá čísla x, y, pro která platí $x^2 + y^2 = 8^{1000} + 3$. Jak si totiž sám snadno rozmyslíš, dává pravá strana při dělení číslem 8 zbytek 3 a levá takový zbytek nemůže při dělení číslem 8 nikdy dosáhnout. Podobně můžeš uvažovat i u některých dalších úloh druhé série.

Užitečné bývá také rozepsat si číslo na součin prvočinitelů (tj. součin prvočísel). Pro přirozená čísla tento zápis vždy existuje a je jednoznačný (až na pořadí prvočísel)[2].

Pro práci s celými čísly lze někdy využít kongruencí. Řekneme, že číslo a je *kongruentní* s číslem b při modulu m (a píšeme $a \equiv b \pmod{m}$), pokud čísla a a b dávají stejný zbytek při dělení m.

Pro kongruence platí několik užitečných faktů. Předně, pokud je $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, pak také $a + c \equiv b + d \pmod{m}$ a $ac \equiv bd \pmod{m}$. Tedy kongruence stejného modulu lze mezi sebou sčítat a násobit podobně jako obyčejné rovnosti. Pro odčítání to platí také, avšak dělení je poněkud zákeřnější a nemusí fungovat.

O kongruencích platí i silnější tvrzení, uveďme zde jen to nejznámější.

Věta. (Malá Fermatova) Nechť p je prvočíslo a a je přirozené číslo nedělitelné p. Potom

$$a^{p-1} \equiv 1 \pmod{p}.$$

2. série

Téma:	Diofantické rovnice
Datum odeslání:	6. listopadu 2006

1. úloha (3 body)

Najděte všechna řešení rovnice $\frac{a+1}{2} = \frac{3}{b+1}$ v oboru přirozených čísel (nulu za přirozené číslo nepovažujeme).

2. úloha (3 body)

Najděte všechny dvojice prvočísel p, q takové, že $p^2 = 2q^2 + 1$.

3. úloha (3 body)

Na louce se pase stádo tří druhů zvířat. Flegmatičtí brundibáři s 5 rohy a 52 očima, kterým nikdo neřekne jinak než „B52", lehkomyslné dalekohledky se 2 rohy a 10 očima, a do třetice devítirožci s 9 rohy a 18 očima se smutným pohledem. Dohromady mají všichni „B52" a devítirožci stejně

---

[1] Pod označením diofantická rovnice se může skrýt i rovnice, u které nás zajímají i racionální řešení, ale to není případ příkladů této série.

[2] U nenulových celých čísel existuje a je jednoznačný „až na pořadí a znaménka": Například $-6 = -2 \cdot 3 = 2 \cdot (-3)$.

rohů jako dalekohledky. A kdybychom k počtu očí všech „B52“ přidali ještě 270, bude to stejně, jako mají dalekohledky s devítirožci dohromady. Kolik se minimálně na louce pase dalekohledek?

4. ÚLOHA (5 BODŮ)

Najděte všechna přirozená čísla n taková, že součin všech jejich vlastních dělitelů je roven n. Přesněji: Najděte všechna $n \in \mathbb{N}$ s následující vlastností: Označíme-li $d_0 = 1, d_1, \dots, d_k = n$ všechny různé dělitele čísla n, platí $d_1 d_2 \cdots d_{k-1} = n$.

5. ÚLOHA (5 BODŮ)

Najděte všechna přirozená čísla a, b, která řeší rovnici $a^2 = 1! + 2! + 3! + \cdots + b!$

6. ÚLOHA (5 BODŮ)

Která čísla lze vyjádřit jako součet několika (aspoň dvou) po sobě jdoucích přirozených čísel?

7. ÚLOHA (5 BODŮ)

Buď n přirozené číslo a p prvočíslo. Najděte všechna řešení rovnice $x(x+1) = p^{2n} y(y+1)$.

8. ÚLOHA (5 BODŮ)

Vyřešte rovnici $x^4 - x^2y^2 + y^4 = z^2$ v oboru přirozených čísel.

Řešení 2. série

1. úloha

Najděte všechna řešení rovnice $\frac{a+1}{2} = \frac{3}{b+1}$ v oboru přirozených čísel (nulu za přirozené číslo nepovažujeme).

Upravme si rovnici do příjemnějšího tvaru (protože $b > 0$, je jistě $b + 1 > 0$, takže můžeme obě strany tímto výrazem pronásobit):

$$\frac{a+1}{2} \cdot (b+1) = 3$$
$$(a+1)(b+1) = 6$$

Má-li tato rovnost platit, musí $a + 1$ dělit 6. Dělitelů šestky není mezi přirozenými čísly mnoho: Snadno zjistíme, že kandidáty na řešení jsou pouze hodnoty $a = 1, 2, 5$. Vydělením obou stran rovnice výrazem $a + 1$ zjistíme, že $b + 1 = \frac{6}{a+1}$, tedy $b = \frac{6}{a+1} - 1$ a odpovídající hodnoty b proto jsou $2, 1, 0$. Nula není přirozené číslo, takže rovnici mohou řešit v přirozených číslech pouze dvojice $a = 1, b = 2$ a $a = 2, b = 1$.

Dosazením snadno ověříme, že tyto dvě dvojice jsou skutečně řešeními původní rovnice a jsme hotovi.

2. úloha

Najděte všechny dvojice prvočísel p, q takové, že $p^2 = 2q^2 + 1$.

Nejprve předpokládejme, že q není 3. Jak si snadno ověříš, q^2 potom dává zbytek 1 po dělení 3 (toto je *velmi důležitý trik*[3], se kterým se při řešení diofantických rovnic často potkáš!), a tedy

[3] Obecně jde o to, že čísla n^2 dávají po dělení libovolným prvočíslem jen polovinu všech možných zbytků.

pravá strana rovnice $2q^2+1$ je dělitelná 3. Číslo p^2 je dělitelné 3, což je možné jen pokud $p=3$. Odtud snadno dopočteme, že $q=2$.

Pokud je $q=3$, mělo by být $p^2=19$, což není možné.

Úloha má tedy jediné řešení $p=3$, $q=2$.

3. úloha

Na louce se pase stádo tří druhů zvířat. Flegmatičtí brundibáři s 5 rohy a 52 očima, kterým nikdo neřekne jinak než „B52", lehkomyslné dalekohledky se 2 rohy a 10 očima, a do třetice devítirožci s 9 rohy a 18 očima se smutným pohledem. Dohromady mají všichni „B52" a devítirožci stejně rohů jako dalekohledky. A kdybychom k počtu očí všech „B52" přidali ještě 270, bude to stejně, jako mají dalekohledky s devítirožci dohromady. Kolik se minimálně na louce pase dalekohledek?

Označme b počet brundibárů, h dalekohledek a d devítirožců. Vidíme, že počet zvířat na louce splňuje soustavu rovnic pro rohy a oči:

$$5b+9d=2h$$
$$52b+270=10h+18d$$

K úplnému vyřešení soustavy nám jedna rovnice chybí, ale můžeme si zkusit soustavu aspoň zjednodušit: Přičtěme dvojnásobek první rovnice ke druhé. Dostáváme podmínku $62b+270+18d=14h+18d$, kterou můžeme zjednodušit na $62b+270=14h$. Vyjádřením b zjišťujeme, že platí:

$$b=\frac{7h-135}{31}.$$

Protože počet brundibárů je celé číslo, musí platit $31|7h-135$ (ta svislá čára se čte „dělí"). Tato podmínka je přitom ekvivalentní s podmínkou $h=6+31\cdot l$ pro nějaké l celé.

Proč? Je $7\cdot 6-135=-93=(-3)\cdot 31$ a v kongruencích můžeme dělit čísly nesoudělnými s modulem: Pokud p,m jsou nesoudělná, tak existuje r, že $nm\equiv k \pmod p$ právě když $n\equiv r \pmod p$.

Důkaz: Nejprve ukážeme jednoznačnost (modulo p) řešení rovnice $nm\equiv r \pmod p$. Pokud je $nm\equiv n'm \pmod p$, tak $p|m(n-n')$ a z nesoudělnosti p,m dostáváme, že musí být $p|n-n'$. Všechna řešení tedy dávají stejný zbytek po dělení p.

Zbývá ukázat, že řešení existuje. Zkoušejme postupně $n=1,2,\dots,p$. Pokaždé bude nm dávat jiný zbytek po dělení p, protože jinak $n\equiv n' \pmod p$, což v našem případě $1\le n,n'\le p$ znamená $n=n'$. Máme celkem p hodnot zbytku nm a p možných zbytků po dělení p, takže každého zbytku bude dosaženo nějakým n. Tedy existuje r, že $nr=k$.

Víme tedy už, že $h=6+31l$ nám zaručí celočíselný počet brundibárů $b=\frac{7\cdot(6+31\cdot l)-135}{31}=7l-3$ (nutně tedy $l\ge 1$, aby brundibárů nebylo záporně). Zvolme $l=1$, které nám dává $h=37, b=4$ a zkusme si z první rovnice soustavy vyjádřit počet devítirožců $d=\frac{2h-5b}{9}=\frac{74-20}{9}=6$. Dosazením do původní soustavy se snadno přesvědčíme, že počty $h=37, b=4, d=6$ vyhovují.

Nejmenší možný počet dalekohledek je 37.

4. úloha

Najděte všechna přirozená čísla n taková, že součin všech jejich vlastních dělitelů je roven n. Přesněji: Najděte všechna $n\in\mathbb{N}$ s následující vlastností: Označíme-li $d_0=1,d_1,\dots,d_k=n$ všechny různé dělitele čísla n, platí $d_1d_2\cdots d_{k-1}=n$.

Předpokládejme, že číslo n má požadovanou vlastnost a že jeho dělitelé jsou uspořádaní podle velikosti, tedy že $d_0 = 1 < d_1 < \cdots < d_k = n$. Nechť $n = {p_1}^{a_1} \cdots {p_l}^{a_l}$ je rozklad n na součin prvočísel a ať $p_1 < p_2 < \cdots < p_l$.

Pak zřejmě je $d_{k-1} = {p_1}^{a_1-1} \cdots {p_l}^{a_l}$, a tedy $d_1 d_2 \cdots d_{k-2} = p_1$. Součin několika přirozených čísel je roven prvočíslu p_1, což je možné jen pokud jde o „součin“ jediného čísla tomuto prvočíslu rovnému. Je tedy $k = 3$ a $d_1 = p_1$. n má jediného jiného vlastního dělitele, a sice d_2. d_2 tedy může nabývat jen dvou možných hodnot:

(i) $d_2 = p_1^2$. Pak $n = p_1^3$; jak snadno ověříš, každá třetí mocnina prvočísla má požadovanou vlastnost.

(ii) $d_2 = p_2$. Pak $n = p_1 p_2$; takovéto číslo zadání také vyhovuje.

5. úloha

Najděte všechna přirozená čísla a, b, která řeší rovnici $a^2 = 1! + 2! + 3! + \cdots + b!$

Vyzkoušejme nejprve několik malých hodnot b, až potom vyřešíme obecný případ:

(i) Pro $b = 1$ je zjevně $a = 1$; pro $b = 3$ je $a = 3$.

(ii) Pro $b = 2$ nebo $b = 4$ rovnice nemá řešení.

(iii) Mějme dále $b \geq 5$ a podívejme se na to, jaký zbytek dává pravá strana rovnice po dělení 5. Čísla 5!, 6!, ... , b! jsou dělitelná 5, zbytek tedy neovlivní. Ten je tedy stejný jako zbytek čísla 1!+2!+3!+4!=33, tedy 3. Jak ale snadno ověříš, druhá mocnina žádného přirozeného čísla po dělení 5 zbytek 3 nedává, rovnice tedy namůže mít žádné řešení.

Rovnice má tedy jen dvě řešení $a = 1$, $b = 1$ a $a = 3$, $b = 3$.

6. úloha

Která čísla lze vyjádřit jako součet několika (aspoň dvou) po sobě jdoucích přirozených čísel?

Dokážeme, že v požadovaném tvaru jdou napsat všechna čísla, která nejsou tvaru 2^m pro nějaké celé číslo $m \geq 0$.

To, že je nějaké číslo n napsané jako součet několika po sobě jdoucích čísel, znamená, že $n = (k+1)+(k+2)+\cdots+l$ pro nějaká čísla $0 \leq k < l-1$. Toto vyjádření můžeme pomocí známého vzorce upravit do tvaru $n = (1+2+\cdots+l) - (1+2+\cdots+k) = \frac{l(l+1)}{2} - \frac{k(k+1)}{2} = \frac{(l-k)(l+k+1)}{2}$. Napišme si n ve tvaru $n = 2^m a$, kde a je liché číslo. Pak $2^{m+1}a = (l-k)(l+k+1)$.

Jak $l - k$, tak $l + k + 1$ jsou čísla větší než 1; jejich součet je lichý, takže jedno z nich je liché, a tedy a je větší než 1. Čísla tvaru 2^m proto nejdou vyjádřit jako součet několika po sobě jdoucích čísel.

Předpokládejme, že je naopak $a > 1$. Uvědom si, že pak je vždy jedno z čísel $a - 2^{m+1} - 1$ a $2^{m+1} - 1 - a$ nezáporné. V prvním případě můžeme volit $l = \frac{a+2^{m+1}-1}{2}$, $k = \frac{a-2^{m+1}-1}{2}$ a v druhém případě zase $l = \frac{a+2^{m+1}-1}{2}$ a $k = \frac{2^{m+1}-a-1}{2}$. Tato čísla podmínky zadání splňují, dostali jsme tedy vyjádření n jako součtu několika po sobě jdoucích čísel.

7. úloha

Buď n přirozené číslo a p prvočíslo. Najděte všechna řešení rovnice $x(x+1) = p^{2n} y(y+1)$.

Dokážeme, že zadaná rovnice žádné řešení nemá. Pro spor předpokládejme, že daná rovnice má nějaké řešení. Pak p^{2n} dělí levou stranu; čísla x a $x+1$ jsou nesoudělná, p^{2n} tedy dělí jedno z nich. Vyřešíme případ, kdy p^{2n} dělí x, druhý případ se vyřeší obdobně. Označme tedy $x = p^{2n} z$.

Po dosazení a úpravě dostaneme, že $z(p^{2n}z+1) = y(y+1)$, neboli $4z^2p^{2n}+4z+1 = (2y+1)^2$. Zřejmě ale platí

$$(2zp^n)^2 < 4z^2p^{2n} + 4z + 1 = (2y + 1)^2 < (2zp^n + 1),$$

což nemůže platit pro žádná přirozená čísla. Rovnice tedy nemá žádné řešení.

8. úloha
Vyřešte rovnici $x^4 - x^2y^2 + y^4 = z^2$ v oboru přirozených čísel.

V řešení dokážeme, že rovnice má pouze triviální řešení tvaru $x = y, z = x^2$. Důkaz je poměrně zdlouhavý, takže abychom nespotřebovali zbytečně mnoho papíru a nemuseli Slovákům vykácet Tatry, napíšu ho stručně. Laskavá čtenářka si ale jistě všechny podrobnosti snadno rozmyslí.

Pro spor předpokládejme, že rovnice má nějaké řešení takové, že $x \neq y$. BÚNO můžeme předpokládat, že čísla x a y jsou nesoudělná; ze všech takovýchto řešení vyberme řešení s nejmenším součinem xy.

Na chvíli si představme, co by se stalo, kdyby nějaké z čísel x, y bylo sudé. Pro určitost ať je to y; označme $y = 2y_0$. x je pak zjevně sudé. Zadání přepíšeme do tvaru $(x^2 - y^2)^2 + (xy)^2 = z^2$; čísla $x^2 - y^2$ a xy jsou nesoudělná a podle známého obecného tvaru řešení pythagorejské rovnice $a^2 + b^2 = c^2$ víme,[4] že existují nesoudělná přirozená čísla m, n, z nichž jedno je sudé, a platí $x^2 - y^2 = m^2 - n^2$ a $xy = 2mn$, tedy $xy_0 = mn$. Jak si můžeš snadno rozmyslet, všechna řešení této rovnice jdou psát ve tvaru $x = ac$, $y_0 = bd$, $m = ad$, $n = bc$, přičemž c a d jsou nesoudělná. Dvojice čísel x, y_0 a m, n jsou nesoudělné, takže čísla a, b, c, d jsou po dvou nesoudělná.

Číslo y je sudé a x liché, takže $x^2 - y^2 = m^2 - n^2$ dává zbytek 1 po dělení 4, takže m je liché a n sudé. To znamená, že čísla a, c, d jsou lichá a b sudé. Dosazením do rovnice $x^2 - y^2 = m^2 - n^2$ dostaneme, že $(a^2 + b^2)c^2 = (a^2 + 4b^2)d^2$. Označme δ největší společný dělitel čísel $a^2 + b^2$ a $a^2 + 4b^2$. Jejich odečtením zjistíme, že δ dělí $3b^2$; δ také dělí $4(a^2 + b^2) - (a^2 + 4b^2) = 3a^2$. a a b jsou nesoudělná, takže δ dělí 3. A protože 3 nedělí $a^2 + b^2$, musí být $\delta = 1$.

Čísla $a^2 + b^2$ a $a^2 + 4b^2$ jsou nesoudělná, takže $(a^2 + b^2)|d^2$ a $c^2|(a^2 + 4b^2)$. Na druhou stranu, z nesoudělnosti čísel c a d vyplývá, že $d^2|(a^2 + b^2)$ a $c^2|(a^2 + 4b^2)$, je tedy $d^2 = a^2 + b^2$ a $c^2 = a^2 + (2b)^2$. Toto je další pythagorejská rovnice, takže existují nesoudělná čísla x_1, y_1, z nichž jedno je sudé, a platí $a = x_1^2 - y_1^2$, $b = x_1y_1$. Dosazením do $d^2 = a^2 + b^2$ dostaneme, že platí $x_1^4 - x_1^2y_1^2 + y_1^4 = d^2$, přičemž $x_1y_1 = b < 2bd = y \leq xy$, což je ve sporu s volbou minimálního možného součinu xy.

Obě čísla x a y tedy musí být lichá; BÚNO předpokládejme, že $x > y$. Číslo $x^2 - y^2$ je sudé a platí $(x^2 - y^2)^2 + (xy)^2 = z^2$, takže existují nesoudělná čísla m, n taková, že $2|mn$, $x^2 - y^2 = 2mn$ a $xy = m^2 - n^2$. Pak

$$m^4 - m^2n^2 + n^4 = (m^2 - n^2)^2 + (mn)^2 = (xy)^2 + \left(\frac{x^2 - y^2}{2}\right)^2 = \left(\frac{x^2 + y^2}{2}\right)^2,$$

přičemž m, n jsou nesoudělná a jedno z nich je sudé. Jak už jsme ale dokázali, toto není možné.

A tím je řešení hotové. Pokud ses pročetl až sem a všechno si cestou důkladně rozmyslel, máš můj obdiv. (:

[4] Známé tvrzení říká, že všechna přirozená řešení rovnice $a^2 + b^2 = c^2$ taková, že b je sudé, jsou tvaru $a = (m^2 - n^2)l$, $b = 2mnl$, $c = (m^2 + n^2)l$, kde m, $n < m$ a l jsou přirozená čísla taková, že m a n jsou nesoudělná a jedno z nich je sudé.