1. seriálová série

Téma: Teorie čísel

Datum odeslání: 1. prosince 2008

1. úloha (5 bodů)
Nalezněte všechna $x \in \mathbb{Z}$, aby platilo

$$x^2 + 1 \equiv x \pmod{21}.$$

2. úloha (5 bodů)
Nechť m a n jsou přirozená čísla. Dokažte, že $2^m - 1$ a $2^n - 1$ jsou nesoudělná, právě když m a n jsou nesoudělná.

3. úloha (5 bodů)
Nechť n je přirozené a a, b jsou celá čísla taková, že dávají stejný zbytek po dělení n. Dokažte, že

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

Řešení 1. seriálové série

1. úloha
Nalezněte všechna $x \in \mathbb{Z}$, aby platilo

$$x^2 + 1 \equiv x \pmod{21}.$$

Nejdříve si kongruenci trochu upravíme:

$$\begin{aligned} x^2 + 1 &\equiv x \pmod{21} \\ x^2 - x + 1 &\equiv 0 \\ x^2 - x - 20 &\equiv 0 \\ (x-5)(x+4) &\equiv 0 \end{aligned}$$

tedy víme, že platí $21 \mid (x-5)(x+4)$. Bohužel 21 není prvočíslo, takže nemůžeme použít stejný postup jako v textu seriálu. Zato pokud rozložíme 21 na prvočinitele, tj. $21 = 3 \cdot 7$, tak budeme vědět, že $3 \mid (x-5)(x+4)$ i $7 \mid (x-5)(x+4)$ a tentokráte 3 i 7 jsou prvočísla, tedy každé z nich musí dělit jednu nebo druhou závorku.

Snadno nahlédneme, že $3 \mid x-5 \iff 3 \mid x+4 \iff x \equiv 2 \pmod{3}$, stačí jen vše zapsat pomocí kongruencí a přičíst nebo odečíst nějaké násobky 3 k jedné straně.

Podobně můžeme postupovat i pro modul 7, tentokráte nám však vyjdou zbytky 5 a 3 modulo 7. Tedy víme, že x je tvaru $7k+5$ nebo $7k+3$ pro nějaké k. Teď najdeme všechna taková k, aby x splňovalo i kongruenci modulo 3. Takže řešíme kongruence

$$\begin{aligned} 7k + 5 &\equiv 2 \pmod{3} & \qquad 7k + 3 &\equiv 2 \pmod{3} \\ k &\equiv 0 & k &\equiv 2 \end{aligned}$$

Tedy víme, že v prvním případě jsou řešením všechny x tvaru $7k+5$ pro k tvaru $3l$, tj. $x = 21l+5$. V druhém případě $x = 7(3l+2)+3 = 21l+17$. Přitom všechna tato čísla jsou řešení, to se ověří snadno dosazením do zadání. (Samozřejmě k, l jsou celá čísla.)

Nebo na konci můžeme postupovat i tak, že si uvědomíme, že 3 dělí každopádně obě závorky, a tedy když si vezmeme tu závorku, kterou dělí 7, tak ji dělí i $7 \cdot 3 = 21$. Tj. platí $21 \mid x-5$ nebo $21 \mid x+4$ a máme řešení $x \equiv 5, 17 \pmod{21}$. Tedy všechna čísla tvaru $21k+5$ nebo $21k+17$, pro nějaké $k \in \mathbb{Z}$.

2. úloha

Nechť m a n jsou přirozená čísla. Dokažte, že $2^m - 1$ a $2^n - 1$ jsou nesoudělná, právě když m a n jsou nesoudělná.

Namísto dělení důkazu na dvě implikace, zkusme nejprve spočíst největší společný dělitel čísel $2^n - 1$ a $2^m - 1$. Tedy číslo $(2^n - 1, 2^m - 1)$.

Použijeme Euklidův algoritmus. Předpokládejme BÚNO, že $m \geq n$.

$$2^m - 1 = 2^{m-n}(2^n - 1) + (2^{m-n} - 1)$$

Máme tedy $(2^m - 1, 2^n - 1) = (2^n - 1, 2^{m-n} - 1)$.

V jednom kroku jsme dvojici exponentů $[m, n]$ nahradili dvojicí $[n, m-n]$. Opakováním tohoto postupu tedy vlastně provádíme Euklidův algoritmus pro čísla m a n! To znamená, že

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1.$$

Nyní již snadno dokončíme důkaz ekvivalence, neboť pro $(m, n) = 1$ je $(2^n - 1, 2^m - 1) = 1$ a pro $(m, n) > 1$ je $(2^n - 1, 2^m - 1) > 2^1 - 1 = 1$. Tedy čísla m, n jsou nesoudělná, právě když jsou nesoudělná čísla $2^n - 1$ a $2^m - 1$.

3. úloha

Nechť n je přirozené a a, b jsou celá čísla taková, že dávají stejný zbytek po dělení n. Dokažte, že

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

Řešení podle šnEka

Podívejme se na výraz $a^n - b^n$, o kterém chceme dokázat, že je dělitelný n^2. Dle známého vzorce platí:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$$

Přitom víme, že $n \mid a - b$. A pokud se nám povede dokázat, že n dělí i druhou závorku, tak budeme mít hotovo. Znovu zopakujeme argument, že $a \equiv b \pmod{n}$, tedy můžeme v kongruenci za b dosadit a dostáváme:

$$a^{n-1} + a^{n-2}b + \cdots + b^{n-1} = a^{n-1} + a^{n-2}a + \cdots + a^{n-1} \equiv na^{n-1} \equiv 0 \pmod{n}$$

A tedy n dělí první i druhou závorku a tedy n^2 dělí jejich součin.

Řešení podle Kennyho
Víme, že $n \mid a-b$. Ekvivalentně existuje $k \in \mathbb{Z}$, pro které platí $a = nk + b$. Podívejme se nyní na rozdíl $a^n - b^n$, dosadíme za a a rozepíšeme podle binomické věty:

$$a^n - b^n = (nk+b)^n - b^n = n^n k^n + \binom{n}{1} n^{n-1} k^{n-1} + \cdots + \binom{n}{n-1} nkb^{n-1} + b^n - b^n$$

Vidíme, že poslední dva členy se nám odečtou. Všechny ostatní jsou však dělitelné n^2, neboť v prvních členech se n vyskytuje přímo v alespoň druhé mocnině a ve členu $\binom{n}{n-1} nkb^n - 1$ můžeme ještě dosadit za kombinační číslo $\binom{n}{n-1} = n$ a máme opět n v druhé mocnině, tudíž n^2 dělí úplně všechny zbývající členy, tedy i rozdíl $a^n - b^n$.

2. seriálová série

Téma: Teorie čísel

Datum odeslání: 16. února 2009

4. úloha (5 bodů)
Nechť p je prvočíslo a b celé číslo. Dokažte, že $b^{p^2-1} \equiv 1 \pmod{p^2}$, právě když $b^{p-1} \equiv 1 \pmod{p^2}$.

5. úloha (5 bodů)
Dokažte, že z posloupnosti $a_n = 2^n - 3$ lze vybrat nekonečně mnoho čísel tak, aby každá dvě z nich byla nesoudělná.

6. úloha (5 bodů)
Kenny a šnEk chystají na Frantu nějakou vylomeninu (teď v zimě ho asi budou chtít spíš zkoulovat, než hodit do Vltavy). Franta o tom dobře ví, dokonce se dozvěděl, že to bude v pátek, ale pořád neví v kolik hodin – na tom se musí Kenny se šnEkem ještě domluvit (ideálně tak, aby se Franta nic nedozvěděl). Jenže Kennymu zrovna přestal fungovat internet a šnEk zase zapomněl mobil ve vlaku, a proto se můžou dorozumívat jen přes nástěnku na Matfyze.

Rozhodnou se, že budou komunikaci šifrovat. Nejdříve si Kenny vymyslí klíče a veřejný klíč pověsí na nástěnku. Franta si klíče na nástěnce všimne, tak si ho rychle opíše: $n = 55, d = 17$. Opíše si ho i šnEk, zakóduje hodinu pomocí tohoto klíče a na nástěnku pak pověsí nic neříkající číslo 24. Franta však nezaváhá a opíše si ho také. Nakonec si Kenny číslo přečte a dešifruje, takže už ví, kdy se na Frantu něco chystá.

Pomožte Frantovi: Kenny se šnEkem používají algoritmus RSA. Zlomte ho (tj. nalezněte soukromý Kennyho klíč) a dešifrujte předanou zprávu.

Řešení 2. seriálové série

4. úloha
Nechť p je prvočíslo a b celé číslo. Dokažte, že $b^{p^2-1} \equiv 1 \pmod{p^2}$, právě když $b^{p-1} \equiv 1 \pmod{p^2}$.

Zadanou ekvivalenci si můžeme rozdělit na dvě implikace.[1] Nejprve se pustíme do té jednodušší:

$$b^{p-1} \equiv 1 \pmod{p^2} \implies b^{p^2-1} \equiv 1 \pmod{p^2}$$

Při důkazu této implikace si vystačíme s tvrzením, že kongruence můžeme násobit. Pak nám stačí už jen $(p+1)$-krát vynásobit kongruenci $b^{p-1} \equiv 1 \pmod{p^2}$ samu sebou (neboli ji umocníme na $(p+1)$-tou) a dostaneme kýženou kongruenci $b^{p^2-1} \equiv 1^{p+1} \equiv 1 \pmod{p^2}$.

Implikaci

$$b^{p^2-1} \equiv 1 \pmod{p^2} \implies b^{p-1} \equiv 1 \pmod{p^2}$$

vyřešíme pomocí Eulerovy věty.

Na začátek si uvědomíme, že pro každé prvočíslo platí $\varphi(p^2) = p(p-1)$. Tento fakt lze jednoduše nahlédnout z definice Eulerovy funkce. S druhou mocninou prvočísla jsou totiž soudělné jen násobky tohoto prvočísla.

Dále potřebujeme vyloučit případ, kdy b a p^2 jsou soudělné. Z prvočíselnosti p vyplývá, že tento případ nastává pouze pro taková b, která jsou násobkem p. Pak ale nemůže platit $b^{p^2-1} \equiv 1 \pmod{p^2}$, protože $b^{p^2-1} \equiv 0 \pmod{p^2}$ (p^2-1 je zřejmě větší než 2, a proto dostáváme na levé straně číslo dělitelné p^2).

Nyní máme splněné podmínky pro Eulerovu větu, do které dosadíme b a p^2. Dostáváme tedy novou platnou kongruenci $b^{p^2-p} \equiv 1 \pmod{p^2}$. Obě strany vynásobíme b^{p-1} a dostáváme $b^{p^2-1} \equiv b^{p-1} \pmod{p^2}$. K dokončení už si stačí jen uvědomit, že výraz na levé straně je kongruentní s 1, a dopracovali jsme se tím k hledané kongruenci $1 \equiv b^{p-1} \pmod{p^2}$.

5. úloha

Dokažte, že z posloupnosti $a_n = 2^n - 3$ lze vybrat nekonečně mnoho čísel tak, aby každá dvě z nich byla nesoudělná.

Vybranou posloupnost budeme konstruovat indukcí, přičemž první člen zvolíme libovolně. Uvažme nyní, že již máme vybrána čísla $x_1, x_2, \ldots, x_{k-1}$. Prvočísla, která dělí alespoň jedno z nich, označme $p_1, p_2 \ldots p_m$. Všechna čísla x_i jsou lichá, takže číslo 2 mezi vybranými prvočísly není. Položme

$$x_k = 2^{(p_1-1)(p_2-1)\ldots(p_m-1)} - 3.$$

Toto číslo je zřejmě vybráno z posloupnosti a_n a navíc jest

$$x_k \equiv -2 \pmod{p_i} \qquad \text{pro } i = 1, 2, \ldots, m$$

jak snadno ověříme z malé Fermatovy věty. No a díky tomu, že čísla p_i jsou lichá, tak $p_i \nmid x_k$ pro žádné i a číslo x_k je nesoudělné s čísly $x_1, \ldots, x_{k-1}$. A to nám již k důkazu stačí.

6. úloha

Kenny a šnEk chystají na Frantu nějakou vylomeninu (teď v zimě ho asi budou chtít spíš zkoulovat, než hodit do Vltavy). Franta o tom dobře ví, dokonce se dozvěděl, že to bude v pátek, ale pořád neví v kolik hodin – na tom se musí Kenny se šnEkem ještě domluvit (ideálně tak, aby se Franta nic nedozvěděl). Jenže Kennymu zrovna přestal fungovat internet a šnEk zase zapomněl mobil ve vlaku, a proto se můžou dorozumívat jen přes nástěnku na Matfyze.

[1] Tedy musíme dokázat, že z první kongruence plyne druhá a naopak.

Rozhodnou se, že budou komunikaci šifrovat. Nejdříve si Kenny vymyslí klíče a veřejný klíč pověsí na nástěnku. Franta si klíče na nástěnce všimne, tak si ho rychle opíše: $n = 55, d = 17$. Opíše si ho i šnEk, zakóduje hodinu pomocí tohoto klíče a na nástěnku pak pověsí nic neříkající číslo 24. Franta však nezaváhá a opíše si ho také. Nakonec si Kenny číslo přečte a dešifruje, takže už ví, kdy se na Frantu něco chystá.

Pomožte Frantovi: Kenny se šnEkem používají algoritmus RSA. Zlomte ho (tj. nalezněte soukromý Kennyho klíč) a dešifrujte předanou zprávu.

Úkolem je rozlousknout RSA, známe veřejný klíč (n, d), potřebujeme zjistit soukromý, označme ho třeba (n, e). Číslo n už známe, to se vyskytuje v obou klíčích. Hledáme tedy jen číslo e, aby pro libovolnou zprávu m platilo $m^{de} \equiv m \pmod{n}$. Přitom víme, že pokud $de \equiv 1 \pmod{\phi(n)}$, tak toto bude platit z Eulerovy věty. Hodilo by se nám tedy spočítat $\phi(n)$.

K tomu potřebujeme rozklad čísla n na prvočinitele – pokud budeme znát $\phi(n)$, tak z něj rozklad n můžeme zpátky spočítat. Vskutku víme, že je-li $n = pq$, tak $\phi(55) = (p-1)(q-1) = pq - (p+q) + 1 = n + 1 - (p+q)$. Znali bychom tedy součet i součin dvou čísel p a q a pak už není problém je spočítat (jsou to právě řešení kvadratické rovnice $x^2 + (\phi(n) - n - 1)x + n$).

Dobře, tak tedy uhodneme rozklad $55 = 5 \cdot 11$ – tím jsme provedli jediný netriviální krok. Teď už stačí jen postupovat podle textu seriálu a dopočítat druhý klíč. Máme $\phi(55) = 4 \cdot 10 = 40$. Hledáme tedy e, že $17e + 40k = 1$ pro nějaké celé číslo k. To umíme z Euklidova algoritmu:

$$\begin{aligned} 40 &= 2 \cdot 17 + 6 \\ 17 &= 2 \cdot 6 + 5 \\ 6 &= 5 + 1 \end{aligned}$$

a zpětným chodem

$$1 = 6 - 5 = 3 \cdot 6 - 17 = 3 \cdot 40 - 7 \cdot 17$$

dostáváme, že $-7 \cdot 17 \equiv 1 \pmod{40}$. Ovšem na -7 se celkem špatně umocňuje, nezbyde nám tedy než přičíst modul 40, tedy $e = 33$. A máme soukromý klíč $(55, 33)$.

Vrhněme se na dešifrování zprávy 24. Chceme spočítat $24^{33} = 24^{32+1} \bmod 55$.

$$24^2 \equiv 26, \quad 24^4 \equiv 26^2 \equiv 16, \quad 24^8 \equiv 16^2 \equiv 36, \quad 24^{16} \equiv 36^2 \equiv 31, \quad 24^{32} \equiv 31^2 \equiv 26 \pmod{55}$$
$$24^{33} \equiv 24^{32+1} \equiv 26 \cdot 24 \equiv 19 \pmod{55}$$

Dešifrovali jsme zprávu 19, nezbývá nám tedy než zavolat Frantovi a říct mu, že v sedm hodin večer se na něj něco chystá (nebo se přidat v tuto dobu ke šnEkovi a Kennymu;-)).

3. seriálová série

Téma: Teorie čísel

Datum odeslání: 14. dubna 2009

7. úloha (5 bodů)

Najdi všechny dvojice celých čísel a, b, která splňují

$$a^3 = b^3 + 4b^2 + 4b + 2.$$

8. ÚLOHA (5 BODŮ)
Najdi všechny trojice x, y, z celých čísel, které řeší rovnici

$$x^2 + y^2 = 11z^2.$$

9. ÚLOHA (5 BODŮ)
Najdi všechna celočíselná řešení a, b, c rovnice

$$a^2 + 2b^2 = 3c^2.$$

Řešení 3. seriálové série

7. úloha
Najdi všechny dvojice celých čísel a, b, která splňují

$$a^3 = b^3 + 4b^2 + 4b + 2.$$

Idea řešení tkví v použití *Tvrzení o po sobě jdoucích mocninách*, o němž jste se dočetli v posledním díle seriálu. Nuže zkoumejme tedy, pro která b platí nerovnosti

$$(b+1)^3 < b^3 + 4b^2 + 4b + 2 < (b+2)^3.$$

Pro taková b nebude výraz b^3+4b^2+4b+2 zcela jistě třetí mocninou celého čísla. První nerovnost je ekvivalentní s nerovností

$$b^2 + b + 1 > 0,$$

která platí pro každé b, jak se snadno sami přesvědčíte. Druhá nerovnost po roznásobení a ekvivalentních úpravách přejde v

$$b^2 + 4b + 3 > 0,$$

která platí pro $b \in (-\infty, -3) \cup (-1, \infty)$.

Ukázali jsme, že jedině pokud $b \in \{-3, -2, -1\}$, může mít daná rovnice řešení. Tyto případy ručně prozkoušíme a získáme dvě řešení $(1, -1)$, $(-1, -3)$.

8. úloha
Najdi všechny trojice x, y, z celých čísel, které řeší rovnici

$$x^2 + y^2 = 11z^2.$$

Je snadné vidět, že $x = y = z = 0$ je řešení. Dále vyloučíme všechna ostatní řešení nekonečným sestupem.

Všimni si, že je-li $z = 0$, tak nutně už jediné takové řešení musí být dříve popsané triviální. Tedy všechna ostatní řešení mají $z \neq 0$. Dále pro spor předpokládejme, že x, y, z je řešení úlohy, že $z \neq 0$. Bez újmy na obecnosti můžeme navíc předpokládat, že x, y a z jsou nezáporná.

Podívejme se na zadanou rovnici modulo 4. Víme, že možné kvadratické zbytky modulo 4 jsou jedině 0 a 1. Tedy pravá strana má hodnotu 0 nebo 3 (modulo 4). V případě $z^2 \equiv 1 \pmod 4$ řešíme rovnici

$$x^2 + y^2 \equiv 3 \pmod 4,$$

která zřejmě nemá řešení, protože z kvadratických zbytků může levá strana nabývat pouze hodnot $0, 1$ nebo 2. Tedy nutně platí $4 \mid z^2$, tj. $2 \mid z$. Řešíme kongruenci

$$x^2 + y^2 \equiv 0 \pmod 4.$$

Ta má z podobného důvodu jako výše jediné řešení modulo 4, a to $x^2 \equiv y^2 \equiv 0 \pmod 4$, tj. $2 \mid x, y$. Nechť tedy $x = 2x_1$, $y = 2y_1$ a $z = 2z_1$, pak podělením původní kongruence čtyřmi:

$$(2x_1)^2 + (2y_1)^2 = 11(2z_1)^2$$
$$x_1^2 + y_1^2 = 11z_1^2$$

dostaneme menší řešení x_1, y_1 a z_1. Takto můžeme postupovat indukcí, čímž dostaneme ostře klesající nekonečnou posloupnost řešení $(x_n, y_n, z_n)_{n=1}^{\infty}$. Avšak třeba $(x_n)_{n=1}^{\infty}$ je nekonečná ostře klesající posloupnost přirozených čísel. Taková nemůže existovat, a tedy dostáváme spor.

Úloha má tedy jediné (triviální) řešení $x = y = z = 0$.

Určitě tě zarazila na první pohled volba modulu. Proč vzít zrovna 4? Důvod není skoro žádný, stejný postup by fungoval třeba i pro 11, jen by se muselo rozebírat více kvadratických zbytků. Naproti tomu 4 je přece jen nejlepší modul pro tuto úlohu[2], protože celé řešení funguje nejen pro rovnici $x^2 + y^2 = 11z^2$, ale i pro libovolnou rovnici tvaru $x^2 + y^2 = (4k + 3)z^2$, kde k je dané celé číslo.

9. úloha

Najdi všechna celočíselná řešení a, b, c rovnice

$$a^2 + 2b^2 = 3c^2.$$

Budeme postupovat podobně jako při řešení vzorové úlohy v poslední sekci seriálu, místy ale budeme postupovat již trochu svižněji než předtím. (: Pokud by ti toto řešení přišlo nesrozumitelné, může ti pomoci, pokud si napřed přečteš řešení zmíněné vzorové úlohy.

Pokud $c = 0$, dostáváme jediné řešení $(0, 0, 0)$; dále předpokládejme, že $c \neq 0$. BÚNO můžeme předpokládat, že čísla a, b, c jsou po dvou nesoudělná – když najdeme všechna nesoudělná řešení, bude každé řešení tvaru (ka, kb, kc) pro nějaké $k \in \mathbb{N}$ a nesoudělné řešení (a, b, c) (rozmysli si, že totiž $\mathrm{NSD}(a, b, c) = \mathrm{NSD}(a, b) = \mathrm{NSD}(b, c)$). Budeme-li uvažovat i $k < 0$, můžeme navíc předpokládat, že $c > 0$. Označme $x = a/c, y = b/c$; vidíme, že (x, y) je racionální bod elipsy $x^2 + 2y^2 = 3$. $A = (1, 1)$ je racionální bod na této elipse, všechny racionální body pak dostaneme jako průsečíky elipsy s racionálními přímkami procházejícími bodem A.

Rovnice přímky je tvaru $x = q, q \in \mathbb{Q}$ nebo $y = kx + l, k, l \in \mathbb{Q}$. V prvním případě máme $q = 1$ (aby bod A ležel na přímce), kromě bodu A je jediný průsečík bod $(1, -1)$.

[2]Souvisí to se součtem dvou druhých mocnin: kdyby ses pokoušel řešit rovnici $x^2 + y^2 = a$ s parametrem $a \in \mathbb{N}$, pak bys brzo přišel na to, že tu významnou roli hraje právě modul 4, který ti ukáže, že pro čísla a tvaru $4k + 3$ daná rovnice nemá žádné celočíselné řešení.

Ve druhém případě musí být $l = 1 - k$. Dosadíme-li hodnotu $y = kx + 1 - k$ do rovnice elipsy, po úpravě dostaneme, že x-ové souřadnice průsečíků splňují rovnici $(2k^2 + 1)x^2 + 4k(1 - -k)x + (2k^2 - 4k - 1) = 0$. Jeden z kořenů odpovídá známému průsečíku A, tedy $x = 1$. Druhý kořen r pak snadno dopočítáme z Viètových vztahů:[3] $xr = \frac{2k^2-4k-1}{2k^2+1}$, čili $r = \frac{2k^2-4k-1}{2k^2+1}$. Druhá souřadnice hledaného průsečíku je pak $s = kr + 1 - k = \frac{-2k^2-2k+1}{2k^2+1}$.

Zjistili jsme tedy, že množina všech racionálních bodů na kružnici k je

$$M = \left\{ \left(\frac{2k^2 - 4k - 1}{2k^2 + 1}, \frac{-2k^2 - 2k + 1}{2k^2 + 1} \right) : k \in \mathbb{Q} \right\} \cup \{(1, \pm 1)\}.$$

Těmto bodům zpětně odpovídají řešení zadané rovnice, pojďme je tedy spočítat! k je racionální číslo, můžeme ho tedy napsat ve tvaru zlomku $k = u/v$, kde $u \in \mathbb{Z}, v \in \mathbb{N}, (u, v) = 1$. Pak $\frac{a}{c} = x = \frac{2k^2-4k-1}{2k^2+1} = \frac{2u^2-4uv-v^2}{2u^2+v^2}$ a $\frac{b}{c} = y = \frac{-2k^2-2k+1}{2k^2+1} = \frac{-2u^2-2uv+v^2}{2u^2+v^2}$. Už už bychom chtěli říct, že $a = 2u^2 - 4uv - v^2, b = -2u^2 - 2uv + v^2$ a $c = 2u^2 + v^2$, to by ale byla chyba – nesmíme totiž zapomenout na to, že nás zatím zajímají jenom nesoudělná řešení.

Zkusme tedy určit největšího společného dělitele D čísel $a_0 = 2u^2 - 4uv - v^2$ a $c_0 = 2u^2 + v^2$. Pokud $D \neq 1$, existuje prvočíslo p, které dělí D, a tedy i a_0 a c_0. p pak musí dělit i součet těchto dvou čísel, což je $4u(u - v)$. Tedy $p \mid 4$ nebo $p \mid u$ nebo $p \mid u - v$.

V prvním případě zjevně $p = 2$.

Pokud $p \mid u$, pak také p dělí v^2 (protože $p \mid c_0 = 2u^2 + v^2$), a tedy p musí dělit v, což je spor s nesoudělností u a v.

Konečně pokud $p \mid u - v$, máme $u \equiv v \pmod p$, a tedy vztah $p \mid c_0$ můžeme přepsat jako $3u^2 \equiv 2u^2 + v^2 \equiv 0 \pmod p$. Tedy $p \mid 3u^2$. Podle předchozího odstavce p nedělí u, tudíž nutně $p \mid 3$ a $p = 3$.

Zjistili jsme, že D mohou dělit pouze prvočísla 2 a 3; nechť $D = 2^m 3^n$ pro $m, n \in \mathbb{N}$. Vidíme, že 2 dělí D, právě když 2 dělí v. Kdyby 4 dělilo D, pak by bylo v sudé a $c_0 \equiv 0 \pmod 4$. Pak ale u musí být liché (u, v jsou totiž nesoudělná) a platí $c_0 = 2u^2 + v^2 \equiv 2 \cdot 1 + 0 = 2 \pmod 4$, což odporuje $c_0 \equiv 0 \pmod 4$. Zjistili jsme, že pokud je v liché, je $m = 0$ a pokud je v sudé, je $m = 1$.

Posviťme si ještě na zoubek trojce z prvočíselného rozkladu čísla D: Při zkoumání obecného p jsme viděli, že $p = 3 \mid D$ se může stát, jen pokud $u \equiv v \pmod 3$. Pokud toto platí, tak naopak opravdu 3 dělí a_0 a c_0. Protože jsou u, v nesoudělná, nemohou být obě dělitelná 3. Zbývá ještě zjistit exponent n v tomto případě. Předpokládejme, že 9 dělí D. Pak 9 dělí $a_0 + c_0 = 4u(u - v)$. Jelikož 3 nedělí $4u$, je 9 nesoudělné s $4u$, takže nutně 9 dělí $u - v$. Vidíme, že dokonce $u \equiv v \pmod 9$. Pak ale máme $0 \equiv c_0 = 2u^2 + v^2 \equiv 3u^2 \pmod 9$, tedy $9 \mid 3u^2$, neboli $3 \mid u^2$, což není možné, protože 3 nedělí u. Můžeme tento odstavec uzavřít zjištěním, že pokud $u \not\equiv v \pmod 3$, je $n = 0$, a pokud $u \equiv v (\not\equiv 0) \pmod 3$, je $n = 1$.

Spočetli jsme tedy hodnotu D v závislosti na u a v:

$D = 1$, pokud je v liché a $u \not\equiv v \pmod 3$;

$D = 2$, pokud je v sudé a $u \not\equiv v \pmod 3$;

$D = 3$, pokud je v liché a $u \equiv v \pmod 3$;

$D = 6$, pokud je v sudé a $u \equiv v \pmod 3$.

Podle poznámky v závorce v druhém odstavci vyjde $\mathrm{NSD}(b_0, c_0)$ úplně stejně. Všechna nesoudělná řešení tedy jsou $a = (2u^2 - 4uv - v^2)/D, b = (-2u^2 - 2uv + v^2)/D$ a $c = (2u^2 + v^2)/D$,

[3] Pro matematické blaho čtenářovo tentokráte používáme druhý ze vztahů namísto toho, jenž jsme použili v seriálu.

kde $u \in \mathbb{Z}, v \in \mathbb{N}, (u,v) = 1$ a D závisí na u, v tak, jak jsme před chvílí spočítali. Neměli bychom samozřejmě zapomenout ani na řešení $a = 1, b = \pm 1, c = 1$ odpovídající bodům $(1, \pm 1)$.

Úplně všechna řešení pak jsou $a = k(2u^2 - 4uv - v^2)/D, b = k(-2u^2 - 2uv + v^2)/D$ a $c = k(2u^2 + v^2)/D$, kde $u \in \mathbb{Z}, v \in \mathbb{N}, (u,v) = 1, k \in \mathbb{Z}$, a $a = k, b = \pm k, c = k$, $k \in \mathbb{Z}$ (pro $k = 0$ dostáváme triviální řešení $(0,0,0)$).

A máme to za sebou. (: Na závěr již jen otázka pro zvídavé čtenářky: Kde jsme v řešení použili počáteční předpoklad, že $c > 0$?