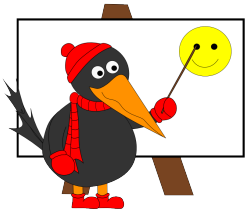
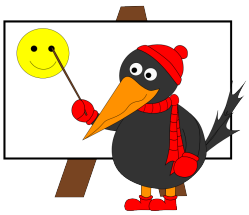


Pomocný text

Počítání v celých číslech



Milí řešitelé,
po poněkud abstraktnější sérii se podíváme na téma, které Vám jistě přijde důvěrně známé, vždyť s celými čísly jste počítali již na základní škole. V tomto pomocném textu si ukážeme některé postupy, které Vám při řešení takovýchto úloh mohou pomoci. Zejména se podíváme, jak řešit některé rovnice v celých číslech. Neexistuje však žádná univerzální metoda, jak tyto problémy řešit, proto neočekávejte, že si s tímto aparátem vystačíte vždy. Avšak v některých případech tyto úvahy povedou přímo k řešení, či Vám snad ukážou cestu, kudy se můžete vydat s jiným nástrojem.

Na začátek přece jenom zaveďme nějaké pojmy, ať víme přesně, o čem se celou dobu budeme bavit. Celými čísly rozumíme množinu přirozených čísel $1, 2, 3, \ldots$, nulu značenou standardně 0 a záporná celá čísla $-1, -2, -3, \ldots$. Pro množinu celých čísel budeme používat označení $\mathbb{Z}$, pro množinu přirozených čísel potom $\mathbb{N}$. Je dobré si uvědomit, že součtem i součinem dvou celých čísel je opět celé číslo, avšak podílem dvou celých čísel nemusí vždy být celé číslo, vždyť například $\frac{1}{4}$ není celé číslo.

Pokud tedy chceme v řešení využít dělení, např. při podělení výrazu jiným výrazem, a tvrdit, že výsledek je stále celé číslo, musíme napřed ukázat, že jeden výraz dělí druhý výraz (beze zbytku!). Tedy pokud například řešíme rovnici $5a = b$ a chceme tvrdit, že $a = \frac{b}{5}$, musíme vědět, že b je dělitelné pěti, aby $\frac{b}{5}$, a tedy i a stále bylo celé číslo. K tomu potřebujeme zformalizovat pojem dělitelnost: řekneme, že číslo b dělí číslo a (píšeme $b|a$), pokud existuje celé číslo $c \in \mathbb{Z}$ tak, že $a = bc$. Všimněte si, že z toho plyne, že i c dělí a. Tedy například $3|6$, protože $6 = 3 \cdot 2$, a také $2|6$. Důležitým pojmem, který je spojen s dělitelností, je pojem *prvočísla*. Prvočíslem nazveme kladné celé číslo, které má právě dva přirozené dělitele. Protože každé číslo je jistě dělitelné 1 a samo sebou, znamená to, že prvočíslo už nesmí mít žádné jiné přirozené dělitele. Povšimněte si, že 1 není prvočíslo, neboť má jediného přirozeného dělitele. Čísla různá od jedné, která nejsou prvočísla, nazýváme *složená*. Prvních několik prvočísel je $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$, aktuálně největším známým prvočíslem je $2^{57885161} - 1$, které má 17425169 cifer.

Důležitou vlastností přirozených čísel (a tedy i celých, až na znaménka) je jednoznačnost rozkladu na součin prvočísel. Každé přirozené číslo totiž můžeme zapsat jako součin několika prvočísel – například $15 = 3 \cdot 5$, $37 = 37$, a tento rozklad je vždy jediný možný (až na pořadí činitelů). Jednou z nejdůležitějších vlastností prvočísel je, že pokud prvočíslo p dělí součin ab, pak nutně dělí některého z činitelů, tedy $p|a$ nebo $p|b$. Toto je důsledkem jednoznačnosti rokladu na součin prvočísel (promyslete si!). Je zajímavé, že v současnosti neexistuje dostatečně rychlý algoritmus na rozkládání přirozených čísel na prvočísla, čehož se využívá v například v kryptografii (zejména u rozšířeného algoritmu RSA).

Dále by se Vám mohla hodit věta o dělení se zbytkem. Pro jednoduchost si ji uveďme

pro přirozená čísla: pro každé $a, b \in \mathbb{N}$ existují jednoznačně daná $c, d \in \mathbb{N} \cup \{0\}$ tak, že $a = bc + d$ a $0 \leq d < b$. Tedy například $15 = 7 \cdot 2 + 1$, kde $0 \leq 1 < 2$. Nejčastěji používaná forma ovšem je, že pro libovolná dvě čísla a, b platí, že a dává po dělení b zbytek c, kde $0 \leq c < b$.

Protože matematika se těžko učí bez počítání, pojďme si ukázat příklady, u kterých můžeme využít nově získaný aparát.

Příklad 4.1. Nechť $a, b \in \mathbb{Z}$. Pokud $5|a + 2b$, je $\frac{2a-b}{5}$ celé číslo.

Řešení. Jistě platí: $5|a+2b \Rightarrow 5|(a+2b)+5a-5b = 6a-3b = 3(2a-b)$. Protože 5 nedělí 3 a 5 je prvočíslo, nutně musí $5|2a - b$. A tedy $\frac{2a-b}{5}$ je celé číslo.

Ukážeme si nyní tři jednoduché triky, které Vám mohou pomoci při řešení rovnic v celých čísel, a to *rozklad na součin*, *redukce modulo přirozené číslo* a *nerovnosti a odhady*.

Příklad 4.2. V celých číslech řešte rovnici $a^2 = b^2 + 15$.

Řešení. Upravme rovnici na tvar

$$a^2 - b^2 = 15$$

a posléze

$$(a - b)(a + b) = 15.$$

Jistě tedy $a - b$, $a + b$ jsou nějací celočíselní dělitelé 15. Protože v celých číslech má 15 pouze konečně mnoho dělitelů, můžeme vyzkoušet všechny možnosti:
$(a + b) = 1$, $(a - b) = 15$: potom $2a = 16$, a tedy $a = 8$ a dále $b = -7$,
$(a + b) = 3$, $(a - b) = 5$: potom $2a = 8$, a tedy $a = 4$ a dále $b = -1$,
$(a + b) = 5$, $(a - b) = 3$: potom $2a = 8$, a tedy $a = 4$ a dále $b = 1$,
$(a + b) = 15$, $(a - b) = 1$: potom $2a = 16$, a tedy $a = 8$ a dále $b = 7$,
$(a + b) = -1$, $(a - b) = -15$: potom $2a = -16$, a tedy $a = -8$ a dále $b = 7$,
$(a + b) = -3$, $(a - b) = -5$: potom $2a = -8$, a tedy $a = -4$ a dále $b = 1$,
$(a + b) = -5$, $(a - b) = -3$: potom $2a = -8$, a tedy $a = -4$ a dále $b = -1$,
$(a + b) = -15$, $(a - b) = -1$: potom $2a = -16$, a tedy $a = -8$ a dále $b = -7$.
Tímto způsobem jsme našli všechny vyhovující dvojice:

$$(8, -7), (4, -1), (4, 1), (8, 7), (-8, 7), (-4, 1), (-4, -1), (-8, -7).$$

V tomto příkladu jsme přitom použili rozklad $a^2 - b^2 = (a + b)(a - b)$. Další rozklady jsou například

$$\begin{aligned} ab - a - b + 1 &= \Upsilon, \\ a^3 - b^3 &= \Upsilon, \\ a^3 + b^3 + c^3 - 3abc &= \Upsilon; \end{aligned}$$

obecněji se dá hezky rozložit $a^n - b^n$, $a^{2n+1} + b^{2n+1}$ a spousta jiných. Υ v tomto případě znamená, že se máte zkusit zamyslet nad vhodným rozkladem sami. Pokud na takovýto rozklad nepřijdete, můžete si o tom popovídat s ostatními řešiteli na našem diskuzním fóru.

Dalším trikem je uvážit celou rovnici *modulo* nějaké přirozené číslo. Vůbec se toho výrazu nebojte, znamená v podstatě jen nahrazení obou stran rovnice jejich zbytkem po

dělení daným modulem. Tedy například $31+25=46$ *modulo* 5 znamená $1+0=1$. Někdy je výhodnější uvažovat zdánlivě nesmyslné rovnice typu $1=6$ *modulo* 5. Nejjednoduším případem je dobře známé uvažování modulo 2, což není nic jiného, než rozhodnout, kdy kdy je některé číslo (popř. výraz) liché nebo sudé.

Příklad 4.3. Ukažte, že rovnice $5y+x^2=2$ nemá řešení pro celá čísla x, y.

Řešení. Ukažme to právě redukcí *modulo* 5. Protože z věty o dělení se zbytkem dává číslo x po dělení 5 zbytek $0, 1, 2, 3$, nebo 4, musí *modulo* 5 platit, že x^2 dává jeden ze zbytků

$$0^2=0, 1^2=1, 2^2=4, 3^2=4, 4^2=1$$

modulo 5. Avšak ze zadání máme podmínku $x^2=2$ *modulo* 5 a vidíme tedy, že tato rovnice nemůže mít řešení.

Možná jste si povšimli, že jsme Vám v tomto řešení zamlčeli jeden důležitý fakt. Skutečnost, že pro $m, n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$ dává číslo $(a+bm)^n$ zbytek $\mathbf{a^n}$ *modulo* m, plyne celkem snadno z binomické věty a v této sérii ji můžete používat bez důkazu. Důsledkem je, že pro zjištění možných zbytků libovolných polynomiálních výrazů stačí zkoumat jen ty možnosti, kdy proměnná nepřevyšuje modul, jako jsme to udělali výše.

Všechny tyto úvahy se dají zformalizovat pomocí takzvaných kongruencí – to je výhodný prostředek, jak usnadnit úvahy o dělitelnosti a zpřehlednit je. O kongruencích si můžete přečíst například v povídání ke 3. sérii 15. ročníku našeho semináře. Většinou však stačí intuitivní úvaha o tom, jakých zbytků můžou po dělení nějakým vhodně zvoleným číslem naše neznámé nabývat. Je výhodné tuto úvahu použít zejména tehdy, když si myslíte, že daná rovnice nemá řešení, protože po dělení nějakým číslem levá strana nabývá jiných zbytků než pravá.

Dalším často využívaným prostředkem jsou nerovnosti. Jedna z naprosto základních a často používaných úvah zní: *čtverec je vždy nezáporný* (čtvercem rozumíme druhou mocninu celého čísla).

Příklad 4.4. Ukažte, že $x^2+y^2+5 \geq 2x-6y-9$ pro libovolná celá čísla x, y.

Řešení. Po převedení na levou stranu si všimneme, že vlastně máme dokázat

$$x^2-2x+y^2+6y+14 \geq 0,$$

po úpravě *na čtverec* ovšem dostáváme na levé straně

$$x^2-2x+y^2+6y+14=(x^2-2x+1)+(y^2+6y+9)+4=(x-1)^2+(y+3)^2+4,$$

což je součet dvou nezáporných a jednoho kladného čísla (čtverec je vždy nezáporný!), což je kladné číslo. Levá strana je tudíž dokonce ostře větší než 0.

Ukažme si nyní, jak lze právě takovouto nerovnost využít k řešení rovnic v celých číslech.

Příklad 4.5. V celých číslech řešte rovnici $(x+1)^2+(y-3)^2=2x(4-y)$.

Řešení. Rovnici nejprve roznásobme:

$$x^2+2x+1+y^2-6y+9=8x-2xy.$$

Dále ji upravme na tvar

$$(x+y-3)^2 = x^2+y^2+9-6x-6y+2xy$$

a poté

$$(x+y-3)^2 = -1.$$

Protože je však čtverec vždy nezáporný, tato rovnice zřejmě nemá v celých číslech řešení.

Vidíme, že i jednoduché nerovnosti můžou být často velmi užitečný nástroj. Více si o nich můžete přečíst například ve třetí sérii 16. ročníku našeho semináře.

Co dál? Nyní se již můžete vrhnout do řešení našich příkladů. Pokud by Vás zajímalo více teorie, vězte, že část matematiky, která se zabývá různými vlastnostmi celých čísel (ale nejenom tím), se nazývá teorie čísel. V češtině existuje spousta vynikajících textů na toto téma, určitě je nutno zmínit třetí kapitolu báječné knihy *Metody řešení matematických úloh* od pánů *Herman, Kučera, Šimša*. Rovnicím, jejichž řešení požadujeme v celých číslech, se většinou říká *Diofantické rovnice*, podle řeckého matematika *Diofanta*, který se jimi zabýval. Řešit rovnice v celých číslech není vůbec jednoduché. Jednou z nejdéle odolávajících diofantických rovnic byla *Velká Fermatova věta*, jednoduše formulovatelné tvrzení z roku 1637, že rovnice $x^n + y^n = z^n$ nemá v celých číslech řešení pro $n > 2$. Tato věta však byla dokázaná až v roce 1995. Spousta jednoduše formulovatelných problémů je však stále otevřených, například slavná Goldbachova hypotéza: Každé sudé přirozené číslo větší než 2 lze zapsat jako součet dvou prvočísel. Kdo ví, třeba její důkaz čeká právě na Vás! :)