Dělitelnost pro začátečníky

Kuba Krásenský

Během přednášky se budeme zabývat dělitelností, což je jeden z ústředních pojmů teorie čísel. Probereme její známé i méně známé vlastnosti, některé z nich se naučíme i dokázat. Při té příležitosti si procvičíme různé techniky důkazu – přímý, sporem, indukcí. Ukážeme si, proč funguje Eukleidův algoritmus. Zavedeme pojem kongruence a naučíme se s ním pracovat. Zavadíme i o kvadratické zbytky a Malou Fermatovu větu, kterou si také dokážeme. Posléze ji zobecníme na větu Eulerovu a probereme i větu Wilsonovu.

Úvodní pojmy

Úmluva. Pokud nebude výslovně uvedeno jinak, myslí se v tomto příspěvku pod pojmem „číslo“ vždy číslo celé.

Definice. Řekneme, že číslo a je *dělitelné* číslem b právě tehdy, když existuje číslo k takové, že $k \cdot b = a$. Druhé možné vyjádření stejné skutečnosti je, že b *dělí* a. Také lze říci, že b je *dělitelem* čísla a nebo číslo a *násobkem* b. Zapisujeme $b \mid a$.

Poznámka. (Základní vlastnosti) Pro libovolná celá a, b, c platí:

(i) $1 \mid a$,
(ii) $a \mid a$,
(iii) $a \mid 0$,
(iv) $a \mid b \wedge b \mid c \Rightarrow a \mid c$,
(v) $a \mid b \wedge a \mid c \Rightarrow a \mid b + c$,
(vi) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$.

Věta. *Pro každá přirozená m a n existuje právě jedna dvojice nezáporných celých čísel k a r, $r < m$, tak, že platí $n = km + r$. Říkáme, že k je celočíselný podíl m a n a že r je zbytek n po dělení m.*

Příklady

Příklad 1. O přirozeném čísle n řekneme, že je magické, jestliže dělí každé číslo vzniklé tak, že před n napíšeme jednu nebo několik nových číslic. Najdi všechna

magická čísla.

Příklad 2. Dokaž, že $6 \mid n^3 - n$ pro každé přirozené n.

Příklad 3. Dokažte, že pro každá celá x, y platí

$$50 \mid 19x + 3y \Leftrightarrow 50 \mid 23x + y.$$

Příklad 4. Najděte všechna čísla x, pro která platí

$$x - 3 \mid x^3 - 3.$$

Příklad 5. Určete počet deseticiferných čísel, ve kterých je možno škrtnout dvě sousední cifry a dostat tak číslo 99krát menší.

Příklad 6. Dokažte, že pro každé přirozené n platí $133 \mid 11^{n+1} + 12^{2n-1}$.

Eukleidův algoritmus

Definice. Nechť jsou a a b nezáporná celá čísla, alespoň jedno z nich nenulové. Jejich *největším společným dělitelem* – značíme $\mathrm{NSD}(a, b)$ – je největší přirozené číslo d takové, že $d \mid a \wedge d \mid b$. Čísla a, b nazýváme nesoudělná, když $\mathrm{NSD}(a, b) = 1$.

Definice. Podobně nazveme *nejmenším společným násobkem* a a b nejmenší číslo, které je dělitelné jak číslem a, tak i b. Značíme ho $\mathrm{nsn}(a, b)$ pro snadnější odlišení od $\mathrm{NSD}(a, b)$.

Věta. *Pro každou dvojici a, b $(a \geq b)$ platí:* $\mathrm{NSD}(a, b) = \mathrm{NSD}(a - b, b)$.

Díky tomu funguje tzv. Eukleidův algoritmus hledání největšího společného dělitele. Dvojici a, b nahradíme dvojicí $a - b$, b. Tu opět uspořádáme podle velikosti, větší číslo označíme a a menší b. Poté znovu odečítáme. Skončíme ve chvíli, kdy bude jedno z čísel rovno nule. Tehdy je druhé číslo právě rovno hledanému NSD.

Příklady

Příklad 7. Najděte $\mathrm{NSD}(3k + 1, 2k - 1)$.

Příklad 8. Máme množinu čísel $\{1, 2, \ldots, 2n - 1, 2n\}$. Dokažte, že mezi každými $n + 1$ vybranými prvky je nějaká dvojice nesoudělných čísel.

Příklad 9. Ukažte, že dva po sobě jdoucí členy Fibonacciho posloupnosti jsou nesoudělné.

Příklad 10. Dokažte, že pro každá přirozená m, n platí

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

Prvočísla

Definice. *Prvočíslem* nazveme takové přirozené číslo, které má právě dva kladné dělitele. Číslo, které má dělitelů více, je *složené*.

Poznámka. Všimněte si, že jednička není ani prvočíslo, ani číslo složené.

Věta. *Číslo p je prvočíslo právě tehdy, když pro všechna čísla b, c platí*

$$p \mid bc \Rightarrow (p \mid b \vee p \mid c).$$

Věta. (Základní věta aritmetiky) *Každé $n \geq 2$ lze rozložit na součin prvočísel jednoznačně až na pořadí činitelů.*

Věta. *Existuje nekonečně mnoho prvočísel.*

Příklady

Příklad 11. Máme číslo n, které lze zapsat ve tvaru $m^6 - m^2$, kde m je přirozené číslo. Jakým nejvyšším číslem bude n jistě dělitelné?

Příklad 12. Najděte všechny dvojice prvočísel p, q, pro které existuje přirozené číslo n tak, že platí

$$p(p+1) + q(q+1) = n(n+1).$$

Příklad 13. Máme přirozené n vyjádřené jako součin prvočísel. Jak určíme, kolik má dělitelů?

Příklad 14. Známe $\mathrm{NSD}(a, b)$ i $\mathrm{nsn}(a, b)$. Jsou tím a a b jednoznačně dána?

Příklad 15. Čemu se rovná $\mathrm{nsn}(a, b) \cdot \mathrm{NSD}(a, b)$?

Příklad 16. Pro prvočísla p, q platí $p \mid q^3 - 1$ a $q \mid p - 1$. Dokažte, že $p = q^2 + q + 1$.

Příklad 17. Ukažte, že pro každé přirozené n existuje řada alespoň n po sobě jdoucích přirozených čísel, neobsahující žádné prvočíslo.

Kongruence

Definice. Říkáme, že a je *kongruentní* s b modulo n právě tehdy, když $n \mid a - b$. Značíme $a \equiv b \pmod{n}$.

Poznámka. To znamená, že a a b dávají stejný zbytek po dělení n.

Příklady

Příklad 18. Určete poslední cifru čísel $17^{17^{17}}$ a $23^{23^{23^{23}}}$.

Příklad 19. Najděte taková celá čísla x, y, že $x^2 = 4y + 2$.

Těžké věty na závěr

Věta. (Malá Fermatova) *Pro každé prvočíslo p a s ním nesoudělné přirozené číslo a platí*

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

Definice. Zavedeme Eulerovu funkci $\varphi\colon \mathbb{N} \to \mathbb{N}$. Její funkční hodnotou bude počet všech přirozených čísel, která jsou s n nesoudělná a zároveň jsou menší než n.

Věta. (Eulerova) *Pro každou dvojici přirozených nesoudělných čísel a, n platí:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Věta. (Wilsonova) *Přirozené číslo n je prvočíslo právě tehdy, když*

$$(n-1)! \equiv -1 \pmod{n}.$$

Příklady

Příklad 20. Dokažte, že neexistuje žádné přirozené číslo n takové, aby platilo $n \mid 2^n - 1$.

Příklad 21. Dokažte, že pro lichá n platí $n \mid 2^{n!} - 1$.

Poděkování

Chtěl bych poděkovat Pepovi Tkadlecovi za poskytnutí materiálů, ze kterých jsem při přípravě přednášky částečně čerpal. Dále svému cvičícímu z předmětu Diskrétní matematika, inženýru Tomáši Vávrovi, za to, že zadává i na VŠ příklady, které se podobají olympiádní matematice a dají se využít na takovéto přednášce. Také děkuji Jiřímu Růžičkovi, z jehož diplomové práce „Teorie čísel – sbírka příkladů“ jsem přebral několik cvičení.