Seriál – Teorie čísel

Kongruence

Během celého našeho povídání o teorii čísel se budeme držet obvyklého značení. Pro připomenutí: Množinu přirozených čísel budeme označovat písmenem $\mathbb{N}$ (tj. $\mathbb{N} = \{1, 2, 3, 4, \dots\}$), množinu celých čísel písmenem $\mathbb{Z}$, racionálních $\mathbb{Q}$, reálných $\mathbb{R}$. Největší společný dělitel čísel $a, b \in \mathbb{Z}$ bude značen (a, b). Vlastnost, že a dělí b (resp. b je násobkem a), budeme zapisovat $a|b$ (to znamená, že existuje $q \in \mathbb{Z}$ takové, že $b = aq$).

Dnes se budeme zabývat vlastnostmi kongruencí. Začněme definicí.

Definice: Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Pokud platí $m|(b-a)$, zapisujeme tuto skutečnost symbolem $a \equiv b \pmod{m}$, čteme „a je kongruentní s b při modulu m“. Uvedený výraz se nazývá *kongruencí* a neznamená tedy nic jiného než, že číslo m dělí rozdíl $(b-a)$. Pokud $a \equiv b \pmod{m}$, nazývá se m modul a číslo b zbytek od a při modulu m. Místo zápisu $a \equiv b \pmod{m}$, budu občas používat též $a \equiv b \ (m)$.

Lidsky lze uvedenou definici též přeformulovat takto: dvě čísla a, b jsou spolu kongruentní při modulu m, pokud dávají při celočíselném dělení číslem m stejný zbytek.

Příklad: Přímo z definice vidíme, že $20 \equiv 11 \pmod{9}$, $-12 \equiv 2 \pmod{7}, \dots$

Uvědomme si, že $a \equiv b \pmod{m}$ neznamená rovněž nic jiného, než že existuje $q \in \mathbb{Z}$ takové, že $a = b + q \cdot m$. Na základě tohoto pozorování již snadno nahlédneme, že kongruence splňuje vlastnosti uvedené v následujícím lemmatu:

Lemma 1: (a) Pokud $a \equiv b \ (m)$ a $c \equiv d \ (m)$, pak $a + c \equiv b + d \ (m)$ a $ac \equiv bd \ (m)$;
(b) Pokud $a \equiv b \ (m)$ a $d|m$, pak $a \equiv b \ (d)$;
(c) Pokud $a \equiv b \ (m)$, $a = a_0 d$, $b = b_0 d$ a $(d, m) = 1$, pak $a_0 \equiv b_0 \ (m)$.
Důkaz: (a) Předpoklady $a \equiv b \ (m)$ a $c \equiv d \ (m)$ znamenají dle definice, že $m|(b-a)$, $m|(d-c)$, tedy existují celá čísla k, l taková, že $b - a = km$ a $d - c = lm$. Proto
$(b + d) - (a + c) = (b - a) + (d - c) = (k + l)m$, neboli $m|((b + d) - (a + c))$; obdobně
$bd - ac = bd - bc + bc - ac = b(d - c) + c(b - a) = blm + ckm = (bl + ck)m$, tj. $m|bd - ac$;
proto $a + c \equiv b + d \ (m)$, $ac \equiv bd \ (m)$.
Důkaz částí (b), (c) ponecháváme čtenáři jako cvičení.

Dle *lemmatu 1* tedy vidíme, že kongruence lze mezi sebou sčítat, násobit a za jistých předpokladů dělit číslem. Nechť nyní je $m \in \mathbb{N}$, uvažujme m čísel $0, 1, 2, \dots, (m-1)$. Je-li $a \in \mathbb{Z}$, je a kongruentní s právě jedním z čísel $0, 1, 2, \dots, (m-1)$ při modulu m, všechna celá čísla můžeme tedy rozdělit do m dijsunktních skupin podle toho, se kterým z čísel $0, 1, 2, \dots, (m-1)$ jsou sledovaná čísla kongruentní.[1] Vybereme-li nyní z každé skupiny po jednom číslu, dostáváme systém m čísel, který nazýváme *úplný systém zbytků při modulu m*. Vybereme-li z úplného systému zbytků při modulu m pouze ta čísla, která jsou nesoudělná s m, dostáváme systém, který nazýváme *redukovaný systém zbytků při modulu m*. Počet čísel tvořících redukovaný systém zbytků

[1] Do první skupiny dáme čísla dávající při dělení m zbytek 0, do druhé ta, která dávají zbytek 1, do třetí ta se zbytkem 2, ..., do m-té čísla, která při dělení m dají zbytek $(m-1)$.

při modulu m se označuje jako $\varphi(m)$. Funkce φ, která každému m přiřazuje $\varphi(m)$, se nazývá *Eulerova funkce.*[2]

Příklad: Nechť $m = 12$. Úplným systémem zbytků při modulu m je například systém $0, 1, \ldots, 11$, ale i $-7, -5, -2, 0, 1, 2, 3, 6, 8, 9, 11, 16$. Redukované systémy zbytků jsou např. $1, 5, 7, 11$, nebo $-7, -5, 1, 11$ a tedy $\varphi(12) = 4$ (což nám dává i vztah uvedený v poznámce).

Lemma 2: (a) (*Eulerova věta*) Pokud (a, m)=1, pak $a^{\varphi(m)} \equiv 1 \pmod m$.
(b) (*Fermatova věta*) Je-li p prvočíslo, pak $a^p \equiv a \pmod p$.
Důkaz: (a) Nechť $c_1, c_2, \ldots, c_{\varphi(m)}$ je redukovaný systém zbytků při modulu m, pak také $ac_1, ac_2, \ldots, ac_{\varphi(m)}$ je redukovaný systém zbytků při modulu m (neboť $(ac_i, m) = 1$, protože $(c_i, m) = 1$; a kdyby pro nějaké $i \neq j$ bylo $ac_i \equiv ac_j \ (m)$, pak by muselo dle *lemmatu 1(c)* být též $c_i \equiv c_j \ (m)$, což nelze). Proto pro každé c_i existuje právě jedno ac_j s ním kongruentní. Máme tedy $\varphi(m)$ kongruencí $c_i \equiv ac_j \ (m)$, kde i, j nabývají hodnot 1, 2, ... , $\varphi(m)$, každou právě jednou. Vynásobením těchto kongruencí dle *lemmatu 1(a)* dostaneme $c_1 \cdot c_2 \cdot \ldots \cdot c_{\varphi(m)} \equiv ac_1 \cdot ac_2 \cdot \ldots \cdot ac_{\varphi(m)} \pmod m$, což po zkrácení čísla $c_1 c_2 \ldots c_{\varphi(m)}$ (podle *lemmatu 1(c)*), dává dokazovaný vztah.
(b) Snadný důsledek části (a). Rozebereme případy $p|a$ a $(p, a) = 1$. V druhém si pak uvědomíme, že pro prvočíslo p je $\varphi(p) = p - 1$.

Příklad: Na základě Eulerovy věty spočítáme zbytek čísla 121^{121} při dělení číslem 18. Jde vlastně o to najít takové nezáporné z menší než 18, pro které $121^{121} \equiv z \pmod{18}$. Eulerova funkce $\varphi(18) = 6$ a jelikož číslo 121 je nesoudělné s číslem 18, máme z Eulerovy věty[3] $121^6 \equiv 1 \pmod{18}$, proto po jednoduchých úpravách máme

$$121^{121} = 121^{6 \cdot 20} \cdot 121 \equiv 121 \equiv 13 \pmod{18},$$

proto hledaný zbytek je 13.

Jak vidíme, Eulerova věta je poměrně účinný nástroj pro upravování kongruencí obsahujících mocniny a při řešení úloh, které na takové kongruence vedou (např. hledání posledních číslic mocnin (nejen v desítkové soustavě) atd.). Nyní bude naše povídání směřovat k důkazu tvrzení, které nám usnadní řešení obdobných úloh s faktoriály.

Lemma 3: Nechť f je polynom stupně n proměnné x, p prvočíslo. Pak kongruence $f(x) \equiv 0 \pmod p$ má maximálně n vzájemně nekongruentních řešení[4], nebo jsou všechny koeficienty polynomu f kongruentní s nulou podle modulu p.
Důkaz: Indukcí podle stupně polynomu, přenecháváme čtenáři.

Lemma 3 se v literatuře často nazývá *Lagrangeova věta*. Poznamenejme, že pro neprvočíselný modul již tvrzení neplatí. Například pro polynom druhého stupně $f(x) = x^2 - 1$ má kongruence $f(x) \equiv 0 \pmod 8$ čtyři řešení 1, 3, 5, 7 (to vlastně znamená, že druhá mocnina libovolného lichého čísla je tvaru $8k + 1$). Na základě Lagrangeovy věty nyní dokážeme větu Wilsonovu.

Lemma 4: (*Wilsonova věta*) Pokud p je prvočíslo, pak $(p - 1)! \equiv -1 \pmod p$.

---

[2] Známe-li rozklad čísla m na prvočinitele $m = p_1^{q_1} p_2^{q_2} \ldots p_n^{q_n}$, $(q_i \in \mathbb{N})$, můžeme Eulerovu funkci $\varphi(m)$ vypočíst pomocí vztahu $\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_n})$. Důkaz tohoto přenecháváme laskavému čtenáři jako cvičení. Uvědomte si při tom, že pro dané m vyjadřuje $\varphi(m)$ počet přirozených čísel menších než m a s m nesoudělných.

[3] V Eulerově větě pokládáme $a = 121$, $m = 18$

[4] To znamená, že když vezmeme libovolný úplný systém zbytků při modulu p, nejvýše n čísel z tohoto systému splňuje po dosazení za x uvedenou kongruenci.

Důkaz: Pokud $p = 2$, dostaneme výsledek přímým dosazením. Pokud $p > 2$, pak uvažujme polynom $h(x) = x^{p-1} - 1 - (x-1)(x-2)\dots(x-p+1)$. Podle *Fermatovy věty (Lemma 2(b))* je každé $x, 1 \leq x \leq (p-1)$ řešením kongruence $h(x) \equiv 0 \pmod{p}$, ale polynom h má stupeň menší než $(p-1)$, proto musí být všechny koeficienty polynomu h kongruentní s nulou podle modulu p. Jelikož p je liché, je absolutní člen polynomu h roven $-1-(p-1)!$, proto $-1-(p-1)! \equiv 0(p)$, což jsme v podstatě chtěli.

Wilsonovu větu lze samozřejmě (jako většinu matematických tvrzení) dokázat i jinými postupy. Trochu přirozenější důkaz dostaneme využitím teorie kvadratických zbytků. Lze ho (stejně jako všechny zde uvedené poznatky) nalézt v libovolné učebnici elementární teorie čísel. V loňském ročníku semináře byla v řešení třetí série tato důkazová technika ukázána, a proto jsem zde volil tuto trochu „méně přirozenou“ variantu důkazu.

Diofantické rovnice

Teorie čísel je jednou z nejstarších částí matematiky. Proslulá je především spoustou problémů, které se dají sice tak snadno formulovat, že jejich zadání pochopí bez obtíží i žák základní školy, ale které se mnohdy nedaří rozřešit ani těm nejlepším matematikům. Jednou z nejdůležitějších partií teorie čísel je bezesporu studium diofantických rovnic, tj. rovnic, které chceme řešit v celých číslech. A právě těmi se dnes budeme zabývat. Oproti minulému dílu seriálu bude dnešní část trochu více upovídaná, chtěli bychom však tímto trošku ukázat, v čem tkví kouzlo této matematické disciplíny. Nebudeme se tady tedy snažit budovat žádnou teorii, ale vše si pokusíme vysvětlit na příkladech.

Příklad: Budeme hledat taková přirozená čísla x, y, pro která platí $3x^2 - 7y^2 = -1$.

Máme tedy v přirozených číslech vyřešit jistou rovnici. První otázka, která by nás měla napadnout, je, zda-li vůbec nějaká taková řešení existují. Když však budeme za x, y postupně dosazovat malá čísla, snadno zjistíme, že $x = 3$, $y = 2$ jsou řešení naší rovnice. Takže nějaká řešení jsme našli. Na řadě je hned další otázka: Existují nějaká další řešení a kolik jich dohromady je? Odpověď na tento problém závisí značně na konkrétní diofantické rovnici. Můžeme mít rovnice, které nemají žádné řešení, či jich mají konečně, nebo nekonečně mnoho. Naše zadaná rovnice je příkladem posledně zmíněných. To nahlédneme drobným trikem: Vyjdeme z identity

$$3(55a + 84b)^2 - 7(36a + 55b)^2 = 3a^2 - 7b^2,$$

kterou snadno ověříme úpravou výrazu vlevo. Když tedy přirozená čísla $x = a$ a $x = b$ splňují rovnici $3x^2 - 7y^2 = -1$, pak ji splňují i čísla $x = 55a + 84b$ a $y = 36a + 55b$. Takže z jediného řešení $x = 3$ a $y = 2$ dostaneme postupně nekonečně mnoho řešení naší rovnice. Na mysli nám hned vyvstanou další otázky: Předně, jak nalézt použitou identitu?[5] A též, jestli jsme našli všechna řešení naší rovnice? Ty však ponecháme nezodpovězeny.

Příklad: Ukážeme, že rovnice $x^2 = 3 - 8z + 2y^2$ nemá řešení v celých x, y, z.

Asi nejpřirozenější přístup k řešení této úlohy je sporem. Předpokládáme, že nějaké řešení máme a odvodíme spor. K tomu účelu je dost často dobré počítat obě strany zadané rovnosti

[5] Celé naše řešení bylo založeno na jisté „z nebe spadlé“ identitě, kterou sice roznásobením snadno ověříme, ale objevit ji se může na první pohled zdát značně těžké, či přímo nemožné. Když však víme, v jakém tvaru máme danou identitu očekávat, není to již takový problém, jak se můžeš sám přesvědčit při řešení úlohy 5, která je naší původní úloze docela podobná, a tak u ní lze očekávat i identitu podobného tvaru.

modulo nějaké číslo. V našem případě můžeme postupovat například takto: Dle příkladu uvedeného za *lemmatem 3* v minulé části seriálu vidíme, že $x^2 \equiv 0, 1, 4 \pmod 8$ (tzn. levá strana naší rovnice dává při dělení osmi jeden ze zbytků 0,1, nebo 4). Pokud je y sudé, pak pro pravou stranu $3 - 8z + 2y^2 \equiv 3 \pmod 8$, což nelze. Pokud je y liché, pak $3 - 8z + 2y^2 \equiv 5 \pmod 8$, což opět není možné, neboť levá strana ani zbytek 3, ani zbytek 5 při dělení číslem 8 nemůže nikdy dát.

V předcházejícím příkladě, jsme ukázali jeden ze způsobů, kterak ukázat, že daná rovnice nemá žádné řešení. Dalším způsobem a v teorii čísel poměrně rozšířenou metodou je tzv. (Fermatova) metoda nekonečného klesání, anglicky „method of descent“ (dále (FMD)). Co se pod tím názvem skrývá si asi nejlépe vysvětlíme na příkladech, viz důkaz *lemmatu 5* a dále. Zde si řekneme jen hlavní myšlenku této metody: Máme-li dokázat, že nějaká diofantická rovnice nemá žádné řešení, předpokládáme pro spor, že nějaké řešení má, a vezmeme to, které je v nějakém smyslu nejmenší. Postupně pak z tohoto řešení zkonstruujeme jiné, které je v daném smyslu ještě menší, což bude hledaný spor. Pokud Ti to připadá moc zatemňující, tak snad na dále uvedených příkladech pochopíš, co chtěl básník touto větou říci. Dříve však uvedeme ještě několik motivačních historických poznámek.

Jedním z nejslavnějších problémů matematiky jest tzv. velká Fermatova věta, což je tvrzení, že rovnice $x^n + y^n = z^n$ nemá celočíselná řešení x, y, z, $xyz \neq 0$, pro $n \geq 3$. Tento poznatek si v první polovině sedmnáctého století (1637) poznamenal Pierre de Fermat[6] při studiu Diofantovy Aritmetiky na okraj stránky. Myslel si, že nalezl i jeho důkaz, leč neuvedl ho. Tento problém pak odolával matematikům po několik staletí, během kterých podnítil rozvoj mnoha odvětví „čisté“ matematiky a až teprve před třemi roky ho pokořil Andrew Wiles.

Následující *lemma 5* nám ukazuje, že velká Fermatova věta platí pro $n = 4$. Kdyby totiž neplatila, dostali bychom snadno spor s tímto lemmatem. (*Sám si rozmysli proč.*) Snadno též nahlédneme, že pokud Fermatova věta platí pro nějaké $n = k$, platí i pro jeho libovolný m-násobek, tj. pro $n = mk$. (*Opět sporem.*) Tím vidíme, že stačí Fermatovu větu dokázat pro lichá prvočísla a zbytek snadno vyplývá.

Poznámka (zatemňující): Případ $n = 4$ je asi jediná část velké Fermatovy věty s elementárním důkazem. Nejobvyklejší postup, jak dokazovat tuto větu pro jiná $n = 3, 5, 7, 11, \ldots$, je rozšířit celá čísla na mnohem obecnější množinu, ve které pak už půjde dokázat Fermatovu větu pomocí nějaké standartní metody (například (FMD)). Hlavní problém tohoto postupu pak je, že v té obecnější množině už se nemusí čísla chovat tak slušně jako celá čísla.

Lemma 5: Rovnice $x^4 + y^4 = z^2$ nemá řešení v celých číslech splňující $xyz \neq 0$.

Myšlenka důkazu: Zde si konkrétně ukážeme, co je to (FMD). Budeme předpokládat, že naše rovnice je řešitelná a že (x_1, y_1, z_1) je řešení takové, že $x_1 y_1 \neq 0$ a z_1 je kladné a **nejmenší** možné. Pak zkonstruujeme nové řešení (x_2, y_2, z_2), kde $0 < z_2 < z_1$, a tím ukážeme, že náš předpoklad byl chybný. To je v podstatě základní myšlenka (FMD). Za předpokladu existence řešení vezmeme v nějakém smyslu nejmenší, a pak se z něho snažíme kvůli sporu dostat ještě menší.

Vlastní důkaz: Můžeme předpokládat, že x_1, y_1, z_1 jsou po dvou nesoudělná (jinak bychom mohli celou rovnici krátit), tj. $(x_1, y_1) = (y_1, z_1) = (x_1, z_1) = 1$. Pokud by čísla x_1 a y_1 byla obě lichá, pak by $z_1^2 = x_1^4 + y_1^4 \equiv 2 \pmod 4$, což je nemožné, neboť druhá mocnina nemůže při dělení číslem čtyři dávat zbytek 2. Takže můžeme brát bez újmy na obecnosti x_1 liché a y_1 sudé; z toho plyne, že i číslo z_1 musí být liché. Nyní si stačí rozmyslet, že pokud je číslo t rovno čtyřem, nebo je to liché prvočíslo, nemůže být zároveň $t | z_1 - x_1^2$ a $t | z_1 + x_1^2$, protože to by po sečtení a odečtení

[6] Pierre de Fermat (1601–1665) — slavný francouzský matematik, vlastním povoláním právník

uvedených vztahů postupně dávalo $t|2z_1$ a $t|2x_1^2$, což je spor s předpokladem $(x_1, z_1) = 1$. Tedy $(z_1 - x_1^2, z_1 + x_1^2) = 2$ (♡). Jelikož $y_1^4 = (z_1 - x_1^2)(z_1 + x_1^2)$, vidíme,[7] že jeden z činitelů $(z_1 - x_1^2)$ a $(z_1 + x_1^2)$ je dělitelný číslem 2 (ale ne číslem 4) a druhý je dělitelný číslem 8. Proto můžeme psát $y_1 = 2ab$ a dále buď

$$z_1 - x_1^2 = 2a^4, \quad z_1 + x_1^2 = 8b^4 \qquad (1) \qquad \text{nebo} \qquad z_1 - x_1^2 = 8b^4, \quad z_1 + x_1^2 = 2a^4, \qquad (2)$$

kde v obou případech $a > 0$, a je liché a $(a, b) = 1$. Případ (1) nemůže nastat, protože odečtením rovností bychom dostali $x_1^2 = -a^4 + 4b^4$, z čehož máme $1 \equiv -1 \pmod 4$, neboť obě čísla x_1 a a jsou lichá. Proto musí platit (2). Sečtením a odečtením zde uvedených vztahů máme po drobné úpravě $z_1 = a^4 + 4b^4$, kde $0 < a < z_1$, a $4b^4 = (a^2 - x_1)(a^2 + x_1)$. Jelikož $(a, b) = 1$, máme z posledního vztahu též $(a, x_1) = 1$ a stejně jako při důkazu vlastnosti (♡) nahlédneme, že $(a^2 - x_1, a^2 + x_1) = 2$. Proto můžeme psát $a^2 - x_1 = 2x_2^4$ a $a^2 + x_1 = 2y_2^4$, kde $b = x_2y_2$. Pokud položíme $a = z_2$, pak sečtením rovností $a^2 - x_1 = 2x_2^4$ a $a^2 + x_1 = 2y_2^4$ dostaneme vztah $z_2^2 = x_2^4 + y_2^4$, kde $0 < z_2 < z_1$. Zkonstruovali jsme tedy řešení naší rovnice s kladným $z = z_2$ menším než nejmenší takové z, což je hledaný spor popsaný v myšlence důkazu.

Dříve než si ukážeme ještě jeden příklad na použití (FMD) (viz *lemma 7*), připomeneme si ještě jedno známé tvrzení, které nám v podstatě popisuje všechny pravoúhlé trojúhelníky s celočíselnými délkami stran a které nám též říká, že pro $n = 2$ má diofantická rovnice vyskytující se ve Fermatově větě nekonečně mnoho řešení.

Lemma 6: Všechna řešení diofantické rovnice $x^2 + y^2 = z^2$ splňující podmínky $x > 0$, $y > 0$, $(x, y) = 1$, $2|x$, $z > 0$ jsou tvaru $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$, kde a, b jsou čísla opačné parity (jedno sudé a druhé liché) a $(a, b) = 1$, $a > b > 0$.

Důkaz tohoto lemmatu ponecháváme čtenáři. V loňském ročníku semináře byl rovněž uveden v řešení úlohy číslo 4 první série. Na základě *lemmatu 6* lze pomocí (FMD) dokázat též *lemma 5*, jak se v mnoha knihách běžně činí. Zkus si tento důkaz sám rozmyslet. Důkaz, který jsem uvedl, *lemma 6* trochu obchází. S jeho pomocí si však můžeš sám vyzkoušet (FMD) rovněž na důkazu následujícího *lemmatu 7*.

Lemma 7: Neexistují žádná dvě přirozená čísla taková, že součet i rozdíl jejich druhých mocnin jsou opět druhé mocniny přirozených čísel.

Návod na důkaz: Zkus pro spor předpokládat, že taková x, y existují, tj. $x^2+y^2 = z^2$ a $x^2-y^2 = t^2$ pro nějaká přirozená z, t, a vezmi takovou dvojici x, y, pro kterou je $x^2 + y^2$ nejmenší možné. Sečtením uvedených rovností snadno dostaneš $x^2 = (\frac{z+t}{2})^2+(\frac{z-t}{2})^2$. Nyni si stačí rozmyslet, kdy lze na poslední vztah aplikovat *lemma 6* a vyloučit ostatní případy. Pak již stačí zkonstruovat taková x_0, y_0 přirozená, která jsou rovněž řešením naší úlohy a pro která $x_0^2 + y_0^2 < x^2 + y^2$. To je hlavní myšlenka důkazu založená na (FMD), k jeho provedení je však potřeba ještě trocha počítání jako v důkazu *lemmatu 5*.[8]

[7] Na tomto místě používáme obrat, který je v teorii čísel často používaný. Zjednodušeně řečeno, dojdeme-li při řešení podobných typů diofantických rovnic ke vztahu $ab = c^2$ pro nějaká přirozená čísla a, b, c, stačí si rozmyslet, jestli jsou náhodou čísla a, b nesoudělná. Pokud ano, musí být ve tvaru druhých mocnin přirozených čísel, tj. existují přirozená x, y, že platí $a = x^2, b = y^2$ (*snadno si rozmyslíš, proč*), což se nám leckdy může hodit. Třeba při řešení úlohy 6 Ti mohou být podobné úvahy užitečné. V našem konkrétním případě sice používáme trošku obměněný postup (pro čtvrté mocniny), ale základní myšlenka je stejná.

[8] Vlastní důkaz *lemmatu 7* je ponechán na Tobě. Při řešení úloh seriálu však můžeš toto lemma používat bez důkazu. Například při řešení úlohy 6 se Ti může hodit.
(Pokud by se Ti i s uvedeným návodem *lemma 7* nepodařilo dokázat, nenech se tím odradit (on ten návod je možná trochu stručný), samotné příklady seriálové série jsou mnohem jednodušší.)

Ukázali jsme několik jednoduchých postupů, kterak řešit diofantické rovnice. Možná Ti to připadá trochu chaotické, ale obecnou metodu na řešení takovýchto rovnic nemáme. Pro jisté speciální typy rovnic samozřejmě byly vytvořeny celé teorie, postupy a metody, jak na ně, ale to by přesahovalo rámec tohoto textu.

Řetězové zlomky

Ačkoliv je teorie čísel jednou z nejstarších matematických disciplín, skládala se po dlouhé věky jen ze směsice zdánlivě izolovaných výsledků. Jistý řád jí vdechnul až geniální Carl Friedrich Gauss,[9] který v roce 1801 ve svých *Disquisitiones arithmeticae* shrnul všechna mistrovská díla svých předchůdců v teorii čísel a obohatil ji v takové míře, že tento čin můžeme směle datovat za počátek moderní teorie čísel. Ta je sama o sobě vědou značně rozsáhlou a není v možnostech našeho seriálu se ani zmínit o všech oblastech, které zkoumá. Pro naše poslední povídání jsem se rozhodl něco málo říci o řetězových zlomcích. Zkušenější čtenář možná namítne, že jsme tím opomenuli mnohé snad důležitější partie (prvočísla apod.), ale myslím si, že právě na řetězových zlomcích lze pěkně demonstrovat, jak různé oblasti teorie čísel spolu souvisejí.

Pro úplnost se na tomto místě dohodněme, že pro $\alpha \in \mathbb{R}$ budeme symbolem $\lfloor \alpha \rfloor$ značit (dolní) celou část čísla α, tj. $\lfloor \alpha \rfloor$ je největší celé číslo menší nebo rovno než α; a symbolem $\{\alpha\}$ budeme značit zlomkovou část čísla α, což je číslo z intervalu $\langle 0, 1)$, pro které platí $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$.

Příklad: Celá část čísla 11.56 je 11 a jeho zlomková část je 0.56.

Nechť nyní α je kladné reálné číslo. Položme $q_1 = \lfloor \alpha \rfloor$, pokud $\{\alpha\} \neq 0$, můžeme psát $\alpha = q_1 + \frac{1}{\alpha_1}$, kde $\alpha_1 = \frac{1}{\{\alpha\}}$. Nyní můžeme pro α_1 opakovat postup uvedený pro α. To znamená: položíme $q_2 = \lfloor \alpha_1 \rfloor$ a pokud zlomková část $\{\alpha_1\} \neq 0$, lze psát $\alpha_1 = q_2 + \frac{1}{\alpha_2}$, kde $\alpha_2 = \frac{1}{\{\alpha_1\}}$, tedy dohromady máme $\alpha = q_1 + \frac{1}{q_2 + \frac{1}{\alpha_2}}$. Opakováním uvedeného postupu[10] pro α_2 dostaneme q_3 a α_3, a zase můžeme náš postup aplikovat na $\alpha_3 \ldots$.

Celkem tedy dostaneme po n krocích našeho postupu, pokud se náš postup nezastaví dříve (tedy pokud pro každé $i < n$ je $\{\alpha_i\} \neq 0$), zápis čísla α ve tvaru:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n + \cfrac{1}{\alpha_n}}}}}$$

Pokud se uvedený postup zastaví, tj. pro nějaké n nastává $\{\alpha_n\} = 0$, dostáváme vyjádření čísla α ve tvaru *konečného řetězového zlomku*:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ldots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

[9] Carl Friedrich Gauss (1777 – 1855) — jeden z nejvýznamnějších matematiků v dějinách, zasahoval však s úspěchem i do jiných věd (astronomie, fyzika, geodézie, ...), k matematice však vždycky choval velice vřelý vztah, nazýval ji totiž „královnou všech věd“ a teorii čísel pak „královnou matematiky“

[10] Tedy pokud je $\{\alpha_2\} \neq 0$.

Místo zápisu konečného řetězového zlomku ve tvaru uvedeném vpravo budeme dále pro úsporu místa používat zápis $\alpha = (q_1, q_2, q_3, \dots, q_n)$. Pokud se však náš postup nezastaví dostaneme nekonečnou posloupnost prvků q_n, *nekonečný řetězový zlomek* a píšeme $\alpha = (q_1, q_2, q_3, \dots)$.

Je dobré si uvědomit, že číslo α je vyjádřitelné ve tvaru konečného řetězového zlomku tehdy a jen tehdy, když je uvedené číslo racionální. Iracionálnímu číslu přísluší vždy řetězový zlomek nekonečný.

Příklad: Například pro číslo $\frac{18}{13}$ máme dle výše uvedeného postupu $\frac{18}{13} = (1, 2, 1, 1, 2)$, pro iracionální číslo $\sqrt{2}$ jest $\sqrt{2} = (1, 2, 2, 2, \dots)$. *Sami si přepočítejte!*

Nechť α je kladné iracionální číslo, kterému tedy přísluší nekonečný řetězový zlomek $\alpha = (q_1, q_2, q_3, \dots)$. Vezmeme-li prvních k členů v posloupnosti $q_n, n = 1, 2, \dots$, lze na na tyto členy pohlížet jako na konečný řetězový zlomek $(q_1, q_2, q_3, q_4, \dots, q_k)$, což je racionální číslo, které označíme $\frac{A_k}{B_k}$. Číslo $\frac{A_k}{B_k}$ aproximuje v jistém smyslu velice dobře číslo α, nazýváme ho *sblíženým zlomkem* k číslu α.

Pokud je číslo α kladné racionální tvaru $\alpha = (q_1, q_2, q_3, \dots, q_n)$, definujeme pro $k \leq n$ sblížené zlomky stejným způsobem jako pro iracionální α.

Příklad: Iracionální Ludolfovo číslo $\pi = 3.14159265358979\dots$ má řetězový zlomek tvaru $\pi = (3, 7, 15, 1, 292, 1, 1, \dots)$, jeho několik prvních sblížených zlomků je
$\frac{A_1}{B_1} = 3, \quad \frac{A_2}{B_2} = \frac{22}{7} = 3.\overline{142857}, \quad \frac{A_3}{B_3} = \frac{333}{106} = 3.141509\dots, \quad \frac{A_4}{B_4} = \frac{355}{113} = 3.1415929\dots$.
Opět si sami přepočítejte!

Poznámka: Jak vidíme v předchozím příkladě, postupně získáváme stále lepší přiblížení čísla π pomocí racionálních čísel. Takto můžeme pomocí sblížených zlomků aproximovat samozřejmě libovolné číslo α (nejen π) a platí dokonce tato obecná věta: Hodnota sblíženého zlomku $\frac{A_k}{B_k}$ se méně liší od hodnoty α než hodnota kteréhokoliv jiného zlomku $\frac{p}{q}$, pro jehož jmenovatele platí $q < B_k$, tj. platí nerovnost $\left|\alpha - \frac{A_k}{B_k}\right| < \left|\alpha - \frac{p}{q}\right|$, pokud je $q < B_k$. Tedy přiblížení čísla α pomocí sblížených zlomků jsou v jistém smyslu nejlepší.

Příklad: Zkus si spočítat několik prvních členů v řetězovém zlomku Eulerova čísla
$e = 2,718281828\dots$. Po troše počítání bys měl dojít k tomuto výsledku
$e = (2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, \dots)$. To by nám mohlo napovídat, že řetězový zlomek čísla e má jisté snadno odhadnutelné zákonitosti (po sobě jdoucí sudá čísla, mezi kterými jsou dvě jedničky). Tato skutečnost se dá i dokázat. V tom je třeba rozdíl čísla e od čísla π, u kterého žádná podobná zákonitost nebyla nalezena. Podobnou i když trochu komplikovanější zákonitost lze nalézt a dokázat i u čísla e^2.

Lemma 8. *Pro čitatele A_k a jmenovatele B_k sblíženého zlomku $\frac{A_k}{B_k}$ konečného řetězového zlomku $(q_1, q_2, q_3, \dots, q_n)$, $(k \leq n)$, nebo nekonečného řetězového zlomku $(q_1, q_2, q_3, \dots)$, platí tyto rekurentní vztahy:*

$$A_1 = q_1, \quad B_1 = 1, \qquad A_2 = q_1 q_2 + 1, \quad B_2 = q_2,$$
$$A_k = q_k A_{k-1} + A_{k-2}, \qquad B_k = q_k B_{k-1} + B_{k-2}, \qquad k \geq 3. \qquad (*)$$

Důkaz: Matematickou indukcí. Stačí si povšimnout, jak sblížený zlomek $\frac{A_k}{B_k}$ „vzniká“ z předcházejících sblížených zlomků. Přenecháváme čtenáři.

Na základě *lemmatu 8* můžeme počítat sblížené zlomky z předcházejích. Přímým důsledkem tohoto lemmatu je též následující tvrzení:

Lemma 9. *Při označení z lemmatu 8 a předchozích úvah máme* $(k \geq 2)$
(a) $A_k B_{k-1} - A_{k-1} B_k = (-1)^k$; *(b)* $\frac{A_k}{B_k} - \frac{A_{k-1}}{B_{k-1}} = \frac{(-1)^k}{B_k B_{k-1}}$;

(c) $(A_k, B_k) = 1$; *(d)* $\frac{A_1}{B_1} < \frac{A_3}{B_3} < \frac{A_5}{B_5} < \cdots < \frac{A_6}{B_6} < \frac{A_4}{B_4} < \frac{A_2}{B_2}$.

Důkaz: (a) Vyjděme ze vztahů v lemmatu 8 označených $(*)$. První z nich vynásobme číslem B_{k-1}, druhý číslem A_{k-1} a odečtěme je. Dostaneme vztah
$A_kB_{k-1} - A_{k-1}B_k = A_{k-2}B_{k-1} - A_{k-1}B_{k-2} = -(A_{k-1}B_{k-2} - A_{k-2}B_{k-1})$.
Tedy náš vztah můžeme dokázat matematickou indukcí: Pro $k = 2$ tvrzení plyne přímým dosazením. Předpokládejme nyní, že dokazovaný vztah platí pro $(k-1)$, pak dle výše uvedeného vztahu $A_kB_{k-1} - A_{k-1}B_k = -(A_{k-1}B_{k-2} - A_{k-2}B_{k-1}) = -(-1)^{k-1} = (-1)^k$, tím je hotov druhý indukční krok.
(b) Vztah z (a) je pouze vydělen číslem B_kB_{k-1}.
(c) Plyne přímo ze vztahu (a), číslo (A_k, B_k) musí totiž dle (a) dělit číslo 1.
(d) Plyne z (b) a z úvahy podobné důkazu části (a). Rozmyslete si sami.

Poznámka: Dle *lemmatu 9(b),(d)* může čtenář, který má základní znalosti matematické analýzy, usoudit, že hodnoty sblížených zlomků nekonečného řetězového zlomku $(q_1, q_2, q_3, \dots)$ se „v jistém smyslu“ blíží k jisté hodnotě α. To nám pak už „v jistém smyslu“ ospravedlňuje smysluplnost rovnosti v zápisu $\alpha = (q_1, q_2, \dots)$. Přesnými formulacemi se však na tomto místě nebudeme zabývat.

Poznámka: (**pro náročnějšího čtenáře)** Zde se zmíníme o dvou pěkných vzorečcích, ve kterých budou figurovat řetězové zlomky v trochu jiném pojetí, než v jakém jsme je dosud uvažovali. Platí:

$$\frac{\pi}{4} = \cfrac{1}{1+\cfrac{1^2}{2+\cfrac{3^2}{2+\cfrac{5^2}{2+\cfrac{7^2}{2+\dots}}}}}, \qquad \log 2 = \cfrac{1}{1+\cfrac{1^2}{1+\cfrac{2^2}{1+\cfrac{3^2}{1+\cfrac{4^2}{1+\dots}}}}}.$$

Pokusím se zde naznačit důkaz prvního z těchto vzorečků, který bývá nazýván *Brounckerovou formulí* a byl objeven již v roce 1655. Nejprve si samozřejmě musíme uvědomit, co přesně chceme dokazovat. Tj. chceme ukázat, že limita sblížených zlomků (snad je jasné, co tím zde míníme) je rovna právě číslu $\pi/4$. Snadno však nahlédneme, že sblížený zlomek končící číslem $(2n-3)^2$ se dá zapsat též ve tvaru $\frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots + \frac{(-1)^{n-1}}{2n-1}$. Z toho a ze známé[11] *Leibnizovy formule* $\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \dots$ již snadno dostaneme dokazovaný vztah.

Nyní se ještě vrátíme k řetězovým zlomkům, jak jsme je na počátku našeho povídání zavedli a zmíníme se o jejich použití při řešení lineárních kongruencí.

Definice: Kongruenci $ax \equiv b \pmod m$ $(*)$ nazýváme *lineární kongruencí* s neznámou x; přitom $a, b \in \mathbb{Z}, m \in \mathbb{N}, m \geq 2$. Celá čísla x, která vyhovují této kongruenci, se nazývají její řešení.

Jestliže x je řešení kongruence $(*)$, pak existuje nekonečně mnoho řešení této kongruence ve tvaru $y = x + m \cdot t, t \in \mathbb{Z}$. Budeme tedy hledat pouze taková řešení x_0, pro která $0 \leq x_0 < (m-1)$. Takových řešení je zjevně konečný počet, který nám vyčísluje následující *lemma 10.*

[11] Leibnizovu formuli pro číslo $\pi/4$ lze dokázat mnoha způsoby, většinou pomocí metod matematické analýzy. Je celkem zajímavé, že tento vztah lze též dokázat pomocí prostředků teorie čísel a celkem jednoduše ho dostaneme jako důsledek teorie o počtu řešení diofantické rovnice $x^2 + y^2 = n$ pro pevné přirozené n. Jak je vidět, všechno nakonec souvisí se vším. (Pokud by Tě tento důkaz uvedené poučky zajímal, či cokoliv jiného, co jsme zde moc nerozvedli, klidně nám napiš a může se to objevit v závěrečných komentářích.)

Lemma 10. *Uvažujme kongruenci* $(*)$ *a označme* $d = (a, m)$*, pak platí:*
(a) Je-li $d = 1$*, pak* $(*)$ *má právě jedno řešení* x *ze soustavy zbytků* $\{0, 1, 2, \ldots, (m-1)\}$.
(b) Je-li $d > 1$ *a neplatí* $d|b$ *, pak* $(*)$ *nemá řešení.*
(c) Je-li $d > 1$ *a platí* $d|b$ *, pak* $(*)$ *má právě* d *řešení, z nichž každé je prvkem soustavy zbytků* $\{0, 1, 2, \ldots, (m-1)\}$.

Důkaz: (a) Budiž $d = 1$. Nechť $x_i = (i-1), i = 1, 2, 3, \ldots, m$ je úplná soustava zbytků modulo m, pak také $a \cdot x_i, i = 1, 2, 3, \ldots, m$ je taková soustava,[12] a tedy existuje $j \in \{1, 2, \ldots, m\}$, pro které je $a \cdot x_j$ ve stejné zbytkové třídě jako b, tj. $a \cdot x_j \equiv b(m)$, a x_j je hledaným jediným řešením kongruence $(*)$.
(b) Z předpokladu $d > 1$ máme, že existují a_1, m_1 tak, že je $a = a_1 \cdot d, m = m_1 \cdot d$. Pak nám $(*)$ dává, že existuje $q \in \mathbb{Z}$ takové, že $a_1 dx - b = m_1 dt$. Pokud však neplatí $d|b$, nemůže být tato rovnost splněna pro žádné x, a tedy kongruence $(*)$ nemá řešení.
(c) Přenecháváme čtenáři jako cvičení.

Jak vidíme z *lemmatu 10*, je kongruence $(*)$ řešitelná pouze za předpokladů[13] (a) či (c). Případ (c) však lze jednoduše (zkrácením) převést na případ (a). Proto se dále stačí zabývat jen řešením kongruence $(*)$ za předpokladu, že $(a, m) = 1$. V tomto případě použijeme řetězového zlomku čísla $\frac{m}{a}$. Předpokládejme, že $a, m \in \mathbb{N}$, pokud by tomu tak nebylo stačí přenásobit kongruenci $(*)$ číslem -1. Pak $\frac{m}{a}$ je kladné racionální číslo, jehož sblížené zlomky označíme

$$\frac{A_1}{B_1}, \quad \frac{A_2}{B_2}, \quad \ldots, \quad \frac{A_{n-1}}{B_{n-1}}, \quad \frac{A_n}{B_n} = \frac{m}{a}.$$

Dle vztahu z *lemmatu 9(a)* $A_n B_{n-1} - A_{n-1} B_n = (-1)^n$ máme po drobné úpravě $mB_{n-1} - A_{n-1}a = (-1)^n$, neboli $aA_{n-1} = (-1)^{n-1} + mB_{n-1}$. Jelikož $B_{n-1} \in \mathbb{Z}$, lze poslední rovnost přepsat do tvaru $aA_{n-1} \equiv (-1)^{n-1} \pmod{m}$ a po vynásobení obou stran této kongruence číslem $(-1)^{n-1}b$ vidíme, že $a(-1)^{n-1}A_{n-1}b \equiv b \pmod{m}$, což však znamená, že $(-1)^{n-1}A_{n-1}b$ je řešením kongruence $(*)$. Jestliže takto vypočítané x není prvkem soustavy $\{0, 1, 2, \ldots, (m-1)\}$, pak řešení x_0 z této soustavy dostaneme přičtením mt, kde t je vhodné celé číslo. Tento postup si můžeš vyzkoušet při řešení úlohy 7.
Poznámka: Když se podíváš na řetězové zlomky druhých odmocnin, $\sqrt{2} = (1, 2, 2, 2, 2, \ldots)$, $\sqrt{3} = (1, 1, 2, 1, 2, 1, 2, 1, 2, \ldots)$, $\sqrt{6} = (2, 2, 4, 2, 4, 2, 4, 2, 4, \ldots)$, asi Tě napadne, že jednotlivé členy se v nich periodicky opakují (po případné předperiodě). Stejnou vlastnost má třeba i číslo $\frac{1+\sqrt{5}}{2} = (1, 1, 1, 1, 1, 1, 1, 1, 1, \ldots)$, ale třetí odmocnina ze dvou už periodický rozvoj nemá. Platí dokonce tato obecná věta: Řetězový zlomek čísla α má periodický rozvoj právě tehdy, je-li číslo α tvaru $\frac{a+\sqrt{b}}{c}$, kde a, b, c jsou celá čísla (b není druhou mocninou přirozeného čísla).[14] Tuto vlastnost řetězových zlomků druhých odmocnin, spolu se specielními zákonitostmi tvorby jejich periody, lze též využít při řešení tzv. *Pellovy diofantické rovnice*, což je rovnice tvaru $x^2 - D \cdot y^2 = 1$, kde D je přirozené číslo, ale to by už přesahovalo rámec tohoto textu.

[12] To nahlédneme stejně jako při důkazu *lemmatu 2*.

[13] Uvědomme si, že případy (a), (b), (c) z *lemmatu 10* postihují všechny možné typy lineárních kongruencí.

[14] Pro čísla konkrétního tvaru lze dokonce přesně najít, jak ta perioda vypadá. Není to většinou nic těžkého, jak si můžeš sám vyzkoušet při řešení příkladu 8.

Literatura

V letošním ročníku semináře jsi se v seriálu (a nejen v něm) mohl jemně seznámit s několika partiemi matematiky, kterými se zabývá teorie čísel. V těchto kratičkých textech nešlo samozřejmě jít příliš do hloubky, snažil jsem se pouze ukázat pár kouzel a triků této úžasné teorie. Ona je to samo o sobě věda značně rozsáhlá, a tak se nelze divit, že o mnohých oblastech, které zkoumá, jsem se nestačil ani zmínit. Z tohoto důvodu zde ještě uvádím (na přání několika řešitelů) seznam literatury, kde vědění chtivý student může čerpat další informace.

Všechny z uvedených publikací Ti můžou posloužit k hlubšímu proniknutí do tajů teorie čísel. Uvádím zde jen knihy, které by měly být dostupné i v nespecializovaných knihovnách a jsou psány česky nebo slovensky.

Knížky [1], [2] obsahují vpodstatě všechna základní témata, kterými se zabývá (elementární) teorie čísel. Ostatní publikace vyšly svorně v edici Škola mladých matematiků a pojednávají o specializovaných tématech, které výstižně charakterizují jejich názvy. Knížka [4] mimo jiné obsahuje i soupis základních vět (bez důkazů) ze „středoškolské“ teorie čísel.

[1] *Š. Znám: Teória čísel, Bratislava, Alfa 1977,*

[2] *I. M. Vinogradov: Základy theorie čísel, Praha, NČSAV, 1956*,

[3] *T. Šalát: Dokonalé a spriatelené čísla, Praha, Mladá fronta, 1969*,

[4] *I. Korec: Úlohy o veĺkých číslach, Praha, Mladá fronta, 1988*,

[5] *P. Vít: Řetězové zlomky, Praha, Mladá fronta, 1982*

[6] *J. Sedláček: Co víme o přirozených číslech, Praha, Mladá fronta, 1976*

[7] *F. Veselý: O dělitelnosti čísel celých, Praha, Mladá fronta, 1966*

[8] *A. Apfelbeck: Kongruence, Praha, Mladá fronta, 1968*

Pokud Tě teorie čísel zaujala, snad Ti tento kratičký seznam pomůže v objevování dalších jejích kouzel. Kdybys měl někdy při tom nějaký problém, například nevěděl, kde co nalézt, klidně nám můžeš napsat.