Trisekce úhlu, kvadratura kruhu a podobné ”nemožné úlohy”

doc. RNDr. Mirko Rokyta, CSc.

Kurz vznikl v rámci projektu ”Rozvoj systému vzdělávacích příležitostí pro nadané žáky a studenty v přírodních vědách a matematice s využitím online prostředí”, Operační program Praha – Adaptabilita, registrační číslo CZ.2.17/3.1.00/31165.

Projekt A-NET je financován Evropským sociálním fondem, rozpočtem ČR a MHMP.

"Praha & EU: Investujeme do vaší budoucnosti.

TRISEKCE ÚHLU, KVADRATURA KRUHU A PODOBNÉ „NEMOŽNÉ“ ÚLOHY

MIRKO ROKYTA

1. Úvod - trocha historie a základní pravidla

V roce 430 před naším letopočtem sužoval starořecké Athény mor. Athéňané se vydali na ostrov Délos v Egejském moři (na tomto ostrově se podle pověstí narodil bůh Apollón, do jehož resortu všechny problémy s morem spadaly), aby od místních věštců získali informaci, jak se s morem vypořádat. Bylo jim řečeno, že mají ve svém domovském chrámu postavit nový oltář, jehož objem bude dvojnásobkem objemu současného oltáře. Protože tento oltář měl přesně krychlový tvar, byli Athéňané (z matematického pohledu) postaveni před úkol zkonstruovat krychli o dvojnásobném objemu než je zadaná krychle. Provést v oné době nějakou geometrickou konstrukci navíc znamenalo provést ji pouze s pomocí pravítka a kružítka.

Taková je (velmi stručná) historie jednoho ze tří slavných starověkých geometrických problémů, tzv. Delského problému. Ony tři starověké úlohy, které nás v tomto textu budou prioritně zajímat, jsou tyto:

- *Zdvojnásobení krychle (Délský problém)*, to jest nalezení hrany krychle o dvojnásobném objemu než je zadaná krychle.
- *Trisekce úhlu*, to jest rozdělení daného úhlu na třetiny.
- *Kvadratura kruhu*, to jest nalezení strany čtverce, jehož obsah je roven zadanému kruhu.

Ve všech případech se přitom vyžaduje, aby se dané konstrukce daly provést pouze pomocí pravítka a kružítka.

Možná nebude na škodu vyjasnit si už nyní, co se vlastně pod obratem „pouze pomocí pravítka a kružítka“ myslí.

Pravidla konstrukcí pomocí pravítka a kružítka:[1]

- Pravítko slouží pouze k narýsování přímky (úsečky), která prochází dvěma již zkonstruovanými body. Pravítko nesmí mít na sobě žádné značky, „jednotky délky“, měřítka, atd. Není ani dovoleno žádné značky na pravítku v průběhu konstrukce vytvářet.
- Kružítko slouží pouze k tomu, aby byl jeho hrot zabodnut do nějakého již zkonstruovaného bodu a aby byl opsán oblouk kružnice (či celá kružnice) o poloměru, který odpovídá vzdálenosti dvou nějakých již zkonstruovaných bodů. Lze tedy pouze tzv. „vzít do kružítka“ nějakou již zkonstruovanou vzdálenost, nelze ale „vzít do kružítka“ žádnou vzdálenost, která by byla nějakým

[1] Takovýmto konstrukcím se také někdy říká eukleidovské konstrukce.

způsobem „vyznačena na pravítku“ (což je ostatně v souladu s předchozím bodem).

- Konstrukce musí sestávat pouze z *konečného počtu kroků*. Nekonečné konstrukce (pomocí kterých se přiblížíme požadovanému výsledku s tzv. „libovolnou přesností“) nepovažujeme za řešení úlohy.
- Konstrukce musí být *přesná*. Přibližná řešení, byť by se hledanému výsledku např. „přiblížila více než je tloušťka běžné tuhy“ opět nejsou považována za řešení úlohy. Nedílnou součástí řešení je tedy *důkaz* toho, že uvedená konstrukce skutečně dává přesně to, co jsme od ní požadovali.

Možná je některým z čtenářů známo, že v průběhu staletí matematici ukázali, že *žádnou* z výše uvedených tří starověkých konstrukcí pouze pravítkem a kružítkem provést *nelze* (usuzujeme tedy, že mor v Athénách se tehdy povedlo zažehnat nějakou jinou, přímočařejší metodou). To je výsledek poněkud překvapující, proto se nelze divit, že se dodnes mezi laickou veřejností tu a tam vyskytnou pokusy ukázat, že to přece jenom lze, a že ti, kdo nemožnost těchto konstrukcí ukázali, se musí mýlit. Často jsou tyto pokusy vyprovokovány špatným pochopením slova *nelze*, které si někteří vykládají jako vyjádření skutečnosti, že to „zatím“ neumíme, či že jsme na to ještě nepřišli, a že přece musí existovat nějaký rafinovaný postup, o kterém se dříve nebo později ukáže, že se s jeho pomocí přece jenom podaří některou ze starověkých konstrukcí provést.

Tak tomu však není. Opravdu to nejde. Tedy: nejde provést žádnou ze tří zmíněných konstrukcí tak, abychom dodrželi naše konstrukční (eukleidovská) pravidla. A navíc existuje přesvědčivý argument, který toto tvrzení dokazuje. Pokusíme se je v tomto článečku předvést. Než se však do toho pustíme, zkusíme čtenáři na jednom jednoduchém příkladu ukázat, jak se v matematice výrok typu „něco nejde“ dokazuje.

2. Rozumíme dobře tvrzení „Nejde to“?

I když by se z výše naznačeného mohlo zdát, že hlavními zbraněmi, kterými se budeme ohánět, bude kružítko, pravítko a dobře ořezaná tužka, není tomu tak. Naší hlavní zbraní bude mozek a hlavní činností budou abstraktní úvahy. Nebudeme tedy posouvat tužku podél hrany pravítka ani zabodávat hrot a rotovat ramenem kružítka, nebudeme vztyčovat kolmice ani se co chvíli shánět po ořezávátku. Budeme si to všecko jenom představovat a přemýšlet o tom, čeho všeho bychom byli schopni pravítkem a kružítkem dosáhnout, kdybychom se do toho pustili.

A čeho bychom za žádnou cenu schopni *nebyli*.

Zásadním heslem tohoto spisku totiž je věta „Co nejde udělat a jak ukázat, že to opravdu *nejde*“. V běžné češtině se s výrazem „nejde to“ setkáváme poměrně často a ve většine případů se ukáže, že ten, kdo tuto větu pronesl, měl spíše na mysli „já to neumím“. V matematickém smyslu má však obrat (věta, tvrzení), začínající slovem „nelze“ mnohem zásadnější a zodpovědnější význam: myslí se tím, že autor takového tvrzení je skutečně mimo jakoukoli pochybnost schopen *dokázat*, že danou věc nelze udělat. Tedy nejenom, že to v dané chvíli neumíme a že se třeba za nějakou dlouhou dobu může najít někdo rafinovaný nebo nadobyčej chytrý, kdo přijde na to, jak to udělat. Ne, myslíme tím toto: předvedeme vám logickou úvahu, jejíž správnost můžete krok za krokem zkontrolovat, která vás přesvědčí, že tu a tu věc skutečně nelze v rámci pravidel, která jsme si domluvili, provést.

Možná bude v této chvíli vhodné ukázat nějaký příklad. I když je následující tvrzení poměrně dobře známé (a omlouvám se tedy těm, kteří ho znají), neuvádím ho zde ani tak pro jeho faktický obsah, jako spíše pro ilustraci úvahy, která předvede, že „něco nelze“.

Tvrzení 2.1. *Číslo $\sqrt{2}$ nelze vyjádřit jako podíl dvou celých čísel.*[2]

Důkaz. Každé tvrzení nebo větu je v matematice potřeba dokázat. My tvrzení 2.1 o iracionalitě $\sqrt{2}$ dokážeme důkazovou technikou zvanou „důkaz sporem“: budeme předpokládat, že dokazované tvrzení neplatí, načež řetězcem logických úvah dojdeme buď k nesmyslu, či k protimluvu, k evidentní nepravdě nebo jinému druhu tzv. *sporu.* Z toho lze učinit jediný závěr: náš předpoklad, že tvrzení neplatí, nebyl správně a dokazované tvrzení tedy platí.

Předveďme si to konkrétně: předpokládejme tedy (matematici říkají: přepokládejme „pro spor“), že číslo $\sqrt{2}$ *lze* napsat jako podíl dvou celých čísel. Existují tedy čísla p, $q \in \mathbb{Z}$ taková, že

$$\sqrt{2} = \frac{p}{q}\,. \tag{2.1}$$

O podílu $\frac{p}{q}$ víme dokonce více, než že jeho čitatel i jmenovatel jsou celá čísla. Protože $\sqrt{2} \approx 1,414\ldots \in (1,2)$, můžeme dokonce bez uzardění přepokládat, že p i q jsou čísla kladná a že q není rovno jedné. Můžeme však přepokládat ještě více, a sice že ve zlomku napravo v (2.1) jsme už provedli všechna možná krácení čitatele a jmenovatele, takže zlomek $\frac{p}{q}$ již nelze dále krátit. Jinak řečeno, *čísla p, q již nemají žádného společného dělitele.* Když už jsme tedy tohle všechno s výrazem (2.1) provedli, budeme pokračovat.

Vynásobíme (2.1) číslem q a umocníme na druhou, dostaneme:

$$2q^2 = p^2\,. \tag{2.2}$$

Tato rovnost nám říká, že číslo p^2 je dvojnásobkem jakéhosi přirozeného čísla (konkrétně čísla q^2), jinak řečeno: číslo p^2 je dělitelné dvěma. Nebo ještě jinak řečeno: číslo 2 se vyskytuje v prvočíselném rozkladu čísla p^2. Odsud ovšem plyne, že číslo 2 se musí vyskytovat už v prvočíselném rozkladu čísla p, tedy i číslo p samotné je dělitelné dvěma. Lze proto psát $p = 2k$ pro nějaké přirozené číslo k. Dosadíme toto vyjádření čísla p do (2.2):

$$2q^2 = 4k^2\,,$$

a po vydělení dvěma dostaneme:

$$q^2 = 2k^2\,.$$

Výsledná rovnice nám něco připomíná: stejně jako před chvíli ve (2.2) vidíme i nyní, že číslo q^2 je dělitelné dvěma, odkud stejnou úvahou dostaneme, že i číslo q samotné je dělitelné dvěma.

[2]Ekvivalentní formulací tohoto tvrzení je výrok „Číslo $\sqrt{2}$ je iracionální“, neboť iracionální čísla, jak čtenář jistě ví, jsou právě ta reálná čísla, která nejsou racionální, tedy je nelze vyjádřit jako podíl dvou celých čísel.

To je ovšem podivné: čísla p a q nemají žádného společného dělitele a my jsme právě ukázali, že ho mají: dvojku. V této chvíli matematik s radostí vykřikne: „spor!“, a ví, že to znamená, že důkaz je hotov. Ví totiž, že jeho (pro spor učiněný) předpoklad, a sice že $\sqrt{2}$ lze napsat jako podíl dvou celých čísel, jej dovedl k logickému sporu. Tento předpoklad byl tedy špatně, a platí jeho negace: tedy, že $\sqrt{2}$ *nelze napsat jako podíl dvou celých čísel.* □

Snad tedy čtenář v této chvíli již chápe, jakou sílu má matematikovo tvrzení, že něco *nelze*. Pokud ano, můžeme se pustit do řešení našich tří problémů.

3. Tři starověké úlohy a novodobý pohled na ně

3.1. Zdvojnásobení krychle. Kdybychom dostali dnes za úkol nalézt krychli, jejíž objem by byl dvojnásobkem objemu zadané krychle, asi bychom na problém nešli pravítkem a kružítkem, ale následující úvahou: má-li původní krychle hranu délky x, má objem roven číslu x^3. Krychle o dvojnásobném objemu má proto objem $2x^3$ a hranu rovnou $\sqrt[3]{2x^3} = x\sqrt[3]{2}$. Vlastně tedy nejde o nic jiného, než o to, jak se ze *zadané délky* x dopracovat k délce $x\sqrt[3]{2}$.

Zkusme tento poznatek interpretovat „v řeči pravítka a kružítka“: nějakým způsobem je nám sdělena délka x a my máme vytvořit (zkonstruovat) délku $x\sqrt[3]{2}$. Protože však nemáme k dispozici žádné měřítko (viz konstrukční pravidla na straně 1) je tato délka x jediný délkový údaj, který máme k dispozici; můžeme ji tedy bez obav považovat za jakousi *jednotku délky*, přidělenou konstrukci, kterou máme provést.

V této chvíli jsme dospěli k důležitému momentu — podařilo se nám naši geometrickou úlohu vyjádřit pomocí algebraických pojmů. Tato algebraická formulace zní: lze z čísla 1 zkonstruovat číslo $\sqrt[3]{2}$? Chtělo by to ovšem ještě nějakou algebraickou interpretaci slova „zkonstruovat“, abychom mohli popsat algebraicky i postup, kterým by se z čísla 1 mělo nějak „odvodit“ číslo $\sqrt[3]{2}$.

I na to dojde. V této chvíli však bude lepší dokončit započatou práci tohoto paragrafu a vyjádřit i zbývající dva konstrukční starověké problémy algebraicky.

3.2. Trisekce úhlu. Už když jsme problém trisekce (roztřetění) úhlu formulovali, mohlo některé z vás napadnout, že přece existují úhly, které lze roztřetit jen pomocí pravítka a kružítka velmi snadno: úhel 180°, například (doufám, že byste to všichni dokázali). O co tedy jde v problému trisekce úhlu? Jde o to, že se hledá *univerzální* konstrukce, která by byla schopna roztřetit *libovolný* úhel. A že pokud chceme ukázat, že taková konstrukce neexistuje, bude stačit nalézt *jeden úhel*, který roztřetit nebudeme schopni.

V tomto povídání nakonec ukážeme, že neexistuje konstrukce pravítkem a kružítkem, která by roztřetila úhel 60°.

Zkusme najít algebraickou formulaci tohoto tvrzení. Vedeni předchozí zkušeností, budeme předpokládat, že je nám dána délka 1. Jistě budeme umět narýsovat kružnici o tomto poloměru (jednotkovou kružnici) a v ní úhel 60°, který máme za úkol roztřetit. Označíme-li si $\alpha = 60°$, je tedy před námi úkol zkonstruovat úhel $\frac{\alpha}{3} = 20°$. Tvrdím, že tento úhel budeme umět zkonstruovat, pokud budeme umět nalézt úsečku délky

$\cos\frac{\alpha}{3} = \cos 20°$. Skutečně (dívejte se na obrázek 1 na str. 5), tuto délku pak bude stačit vynést ze středu kružnice na osu x a vztyčit kolmici v takto získaném bodě.

K převedení tohoto problému do algebraické řeči využijeme goniometrický vztah (najdete ho například v oblíbené „vzorečkové“ publikaci [1])

$$\cos\alpha = 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}\,. \tag{3.1}$$

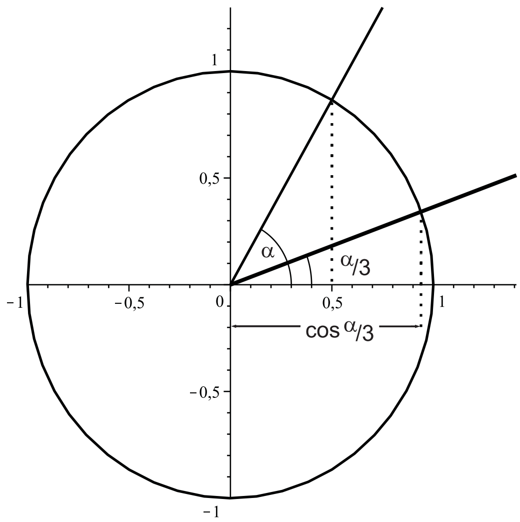
Hodnotu $\cos\alpha = \cos 60° = \frac{1}{2}$ v předchozí rovnici známe (přesněji: umíme z hodnoty „1“ zkonstruovat), a hodnotu $\cos\frac{\alpha}{3}$ hledáme. Označme si proto $x = \cos\frac{\alpha}{3}$. Rovnice (3.1) pak bude mít tvar

$$\frac{1}{2} = 4x^3 - 3x$$

neboli

$$8x^3 - 6x - 1 = 0\,.$$

Algebraická formulace problému konstrukce třetiny úhlu 60° tedy zní takto: je dáno číslo 1, zkonstruujte číslo x, které je řešením rovnice $8x^3 - 6x - 1 = 0$, ležícím v intervalu $(0, 1)$ — to aby mohlo být kosinem úhlu, ležícího v prvním kvadrantu.[3]



Obrázek 1. Ke konstrukci třetiny úhlu 60°.

3.3. **Kvadratura kruhu.** Zde, jak se ukáže, je „algebraizace“ problému poměrně snadná: máme za úkol nalézt délku strany čtverce, který má stejný obsah jako zadaný kruh. Známe tedy poloměr kruhu, a stejně jako výše můžeme předpokládat, že má délku 1. Obsah tohoto kruhu je pak roven $\pi \cdot 1^2 = \pi$ a délka strany čtverce o stejném obsahu je proto $\sqrt{\pi}$. Algebraická formulace našeho problému tedy zní: je dána číslo 1, zkonstruujte číslo $\sqrt{\pi}$.

[3] Možná vás napadne, zda zmíněná rovnice vůbec nějaké řešení v intervalu $(0, 1)$ má, případně jestli jich není víc. Odpověď je uspokojivá: lze ukázat (například pomocí tzv. Cardanových vzorců [1]), že rovnice $8x^3 - 6x - 1 = 0$ má tři reálná řešení, dvě záporná a jedno kladné, jejich přibližné hodnoty jsou $-0,766\,044$, $-0,173\,648$ a $0,939\,692$. Existuje tedy právě jedno $x \in (0, 1)$, řešící rovnici $8x^3 - 6x - 1 = 0$.

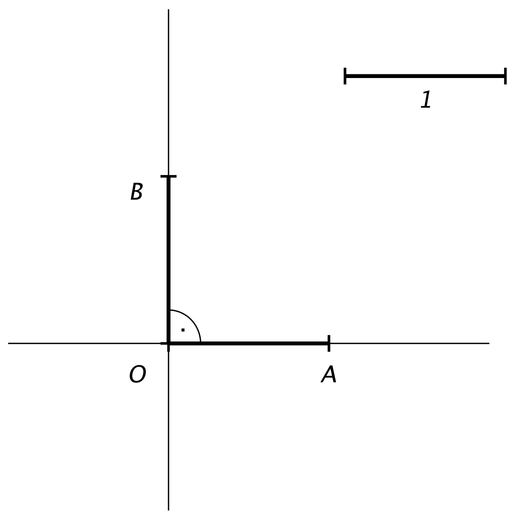
Udělejme si malou rekapitulaci. Všechny tři starověké konstrukční úlohy mají podobné algebraické formulace: je dáno číslo 1; lze pak zkonstruovat čísla $\sqrt[3]{2}$, $\sqrt{\pi}$ a číslo $x \in (0,1)$, které je řešením rovnice $8x^3 - 6x - 1 = 0$?

Jeden důležitý krok na cestě k algebraizaci našich konstrukčních problémů však zůstává dosud nedořešen: jak převést do řeči algebry pojmy „konstruovat“ resp. „konstruovatelný“.

4. Na cestě k pojmu „konstruovatelnost“

Před nějakým časem jsem slíbil, že nebudeme rýsovat a konstruovat, ale že si budeme rýsování a konstruování představovat (pokud si však někdo při tom představování bude chtít pomoci náčrtkem, nebude mu samozřejmě nikdo v takové činnosti bránit).

Představujme si tedy, jak pomocí pravítka a kružítka řešíme některou z výše zmíněných tří úloh. A představujme si dokonce víc: zkusme přijít na to, jaké všechny možné konstrukce bychom uměli pomocí konstrukčních pravidel ze strany 1 učinit. Máme tedy před sebou čistý list papíru, pravítko, kružítko, dobře ořezanou tužku a vědomí toho, že při konstruování máme taky trochu myslet na to, jak to celé převádět do řeči algebry. Jak ale začít? Zdá se, že naše konstrukční pravidla postrádají informaci o tom, jaký je vlastně startovní bod všech eukleidovských konstrukcí. Když o tom budeme chvíli přemýšlet, tak přijdeme na to, že výrok „je zadána úsečka délky 1“, je pro celé naše konstruování naprosto nezbytný. Jinak bychom nemohli žádné body daných vzdáleností na čistém listu papíru vytvořit. Předpokládejme tedy, že „známe úsečku délky jedna“. V myšlenkách se nám tedy někde (pravděpodobně na okraji papíru) objevila úsečka — její délku neumíme změřit, naše pravítko nemá měřítko, je u ní však napsáno, že má délku 1, tedy to vezmeme jako daný fakt.



Obrázek 2. Výchozí situace eukleidovských konstrukcí.

Co dál? Naše konstrukce budou rovinné, proto se zdá vhodné (i s ohledem na možnou algebraizaci problému) vytvořit v rovině listu papíru kartézskou soustavu souřadnic. To není obtížné: vyznačíme si libovolný bod O jako počátek této soustavy, vedeme jím libovolnou přímku („osu x“)[4] a na ni vyneseme nám danou vzdálenost „1“; dostaneme bod A na „ose x“ (sledujte obrázek 2 na str. 6). Jistě umíme pomocí pravítka a kružítka vztyčit také kolmici k „ose x“ a na ni přenést jednotkovou vzdálenost; dostaneme bod B na „ose y“. Dohodněme se, že tuto situaci budeme považovat za startovní bod (výchozí situaci) všech eukleidovských konstrukcí.

Jaký bude další postup? Pravidla eukleidovských konstrukcí říkají, které všechny objekty můžeme z tohoto výchozího stavu vytvořit: další přímky, další kružnice (či jejich oblouky), další body jako jejich průsečíky, a také nové vzdálenosti (délky), jakožto vzdálenosti mezi dvěma dříve zkonstruovanými body. Následující terminologie (mající charakter definic) bude čtenáři jistě srozumitelná:

- *Konstruovatelná přímka* je přímka, procházející dvěma zkonstrurovatelnými body v rovině.
- *Konstruovatelná délka (konstruovatelné číslo)* je vzdálenost mezi dvěma konstruovatelnými body.
- *Konstruovatelná kružnice* je kružnice, jejíž střed leží v konstruovatelném bodě a jejíž poloměr má konstruovatelnou délku.

Dále je jasné, že nový konstruovatelný bod můžeme získat pouze jedním z následujících tří způsobů:

- jako průsečík dvou konstruovatelných přímek;
- jako průsečík konstruovatelné přímky a konstruovatelné kružnice;
- jako průsečík dvou konstruovatelných kružnic.

Nemusíme jistě nijak zvlášť zdůrazňovat (ale nebude to na škodu), že vše, co prohlásíme za „konstruovatelné“, musí vzniknout pouze *konečným počtem* opakování těchto procesů.

A stejně tak nemusíme zdůrazňovat, že ve středu našeho zájmu bude množina všech konstruovatelných čísel, jinak řečeno vzdáleností mezi konstruovatelnými body, které lze těmito procesy dostat. Označme si množinu všech konstruovatelných čísel písmenem $\mathbb{K}$ (od slova „konstruovat“). Jistě by bylo velmi dobré si ujasnit, jaké vlastnosti množina $\mathbb{K}$ má, a poté, pochopitelně, jaká všechna čísla do ní patří.

K tomu všemu ale budeme muset nejprve projít jednu malou matematickou odbočku.

5. Malý výlet do moderní algebry

Jedním ze základních pojmů moderní algebry je pojem *tělesa.* Abychom si rozuměli: slovem „těleso“ zde neoznačujeme třírozměrný geometrický objekt[5], ale, jak se ukáže, množinu čísel[6] s jistými vlastnostmi — přesněji nám to řekne následující definice.

[4] To je poprvé a naposledy v eukleidovských konstrukcích, kdy není přímka určena *dvěma* již dříve zkonstruovanými body.

[5] Mezi pojmem algebraické těleso a geometrické těleso není žádná souvislost, jde jen o terminologickou shodu.

[6] Algebraické těleso může sestávat i z mnohem obecnějších prvků, pro naše potřeby však úplně postačí omezit se na tělesa reálných čísel.

Definice 5.1. Neprázdnou podmnožinu $\mathbb{T}$ reálných čísel nazveme *tělesem*, pokud pro všechna $a \in \mathbb{T}$, $b \in \mathbb{T}$ platí $a+b \in \mathbb{T}$, $a-b \in \mathbb{T}$, $ab \in \mathbb{T}$, a pokud $b \neq 0$, pak i $a/b \in \mathbb{T}$.

Jinými slovy lze říci, že těleso je jistá podmnožina reálných čísel, která je uzavřená na operaci sčítání, odčítání, násobení a dělení nenulovým prvkem. Příkladem tělesa je množina racionálních čísel $\mathbb{Q}$. K tomu stačí ověřit, že každý součet, rozdíl, součin a podíl (dělíme-li nenulovým číslem) racionálních čísel je zase racionální číslo. To je ale jistě pravda.

Dalším příkladem tělesa je množina všech reálných čísel $\mathbb{R}$, jak byste si jistě byli sami schopni uvědomit. Zajímavá a přirozená je v této souvislosti otázka, jestli existují ještě nějaká jiná tělesa reálných čísel, než tato dvě. A odpověď zní: ano, existuje jich dokonce nekonečně mnoho, a jsou z našeho pohledu velmi zajímavá. Můžeme dokonce velmi jednoduše taková nová tělesa vytvářet.

Tvrzení 2.1 na straně 3 nás poučilo, že $\sqrt{2}$ není racionální číslo. Co když ale vytvoříme novou množinu čísel tak, že sjednotíme racionální čísla a číslo $\sqrt{2}$, a pak ještě do této nové množiny „přidáme“ výsledky všech možných sčítání, odčítání, násobení a dělení nenulovými čísly? Pak již těleso vznikne (protože bude uzavřené na výsledky zmíněných operací) a jistě bude větší než těleso racionálních čísel. Uvědomte si také, že způsob, jakým toto těleso vzniklo, zaručuje, že je to nejmenší možné těleso, obsahující jak racionální čísla, tak číslo $\sqrt{2}$. Tento postup leží v pozadí následující obecné definice.

Definice 5.2. Buď $\mathbb{T} \subset \mathbb{R}$ těleso a $r \in \mathbb{R}$ číslo, které neleží v $\mathbb{T}$. Potom symbolem $\mathbb{T}(r)$ značíme nejmenší těleso, které obsahuje všechny prvky $\mathbb{T}$ i číslo r. Říkáme, že těleso $\mathbb{T}(r)$ vzniklo *adjunkcí* prvku $r \in \mathbb{R} \setminus \mathbb{T}$ k tělesu $\mathbb{T}$.

Jak vidíme, před definicí 5.2 jsme nepopsali nic jiného, než způsob, jakým vzniká těleso $\mathbb{Q}(\sqrt{2})$. Není těžké si rozmyslet, jak vypadají prvky $\mathbb{Q}(\sqrt{2})$. Platí, že

$$\mathbb{Q}(\sqrt{2}) = \{p + q\sqrt{2},\ p, q \in \mathbb{Q}\}\,. \tag{5.1}$$

(Zkuste také ověřit, že množina vpravo v (5.1) je skutečně těleso, tj. že součet, rozdíl, součin i podíl čísel tvaru $p+q\sqrt{2}$, $p, q \in \mathbb{Q}$ je opět číslo tohoto tvaru. Malá nápověda: při zkoumání podílu $\frac{p_1+q_1\sqrt{2}}{p_2+q_2\sqrt{2}}$ rozšiřte zlomek výrazem $p_2 - q_2\sqrt{2}$.)

Proč je pojem tělesa v našem případě tak důležitý? Protože i konstruovatelná čísla oplývají vlastnostmi tělesa: jakmile umíme zkonstruovat nějaká dvě čísla, umíme také (kružítkem a pravítkem) zkonstruovat jejich součet, rozdíl, součin a podíl (jsou-li nenulová),[7] jinými slovy platí následující tvrzení.

Tvrzení 5.3. *Množina $\mathbb{K}$ všech konstruovatelných čísel je těleso.*

Jak už jsme řekli, jakmile umíme zkonstruovat nějaká dvě čísla, umíme také (kružítkem a pravítkem) zkonstruovat jejich součet, rozdíl, součin a podíl. To ovšem znamená, že (vycházejíce z délky 1) umíme zkonstruovat všechna racionální čísla, jinými slovy, že $\mathbb{Q} \subset \mathbb{K}$. Umíme však zkonstruovat i některá iracionální čísla, například právě $\sqrt{2}$, jakožto přeponu pravoúhlého trojúhelníka o odvěsnách 1 a 1. S každým

[7] Příslušné konstrukce, zejména konstrukci součinu a podílu dvou nenulových délek, jste jistě na střední škole probírali.

takovým „novým“ konstruovatelným číslem ale umíme ihned zkonstruovat i všechna čísla z tělesa, které vznikne adjunkcí tohoto čísla k tělesu čísel, které jsme doposud byli schopni zkonstruovat. Tedy, například, zapsáno matematicky,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{K}\,.$$

Pokračujme však dále: my jsme schopni zkonstruovat i $\sqrt{3}$, jakožto přeponu pravoúhlého trojúhelníka o odvěsnách 1 a $\sqrt{2}$, obecně dokonce každé číslo tvaru $\sqrt{n}$, $n \in \mathbb{N}$, jakožto přeponu pravoúhlého trojúhelníka o odvěsnách 1 a $\sqrt{n-1}$, a s nimi vždy i všechna čísla, která patří do jim přináležejícího tělesa. Chcete-li,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3}) \subset \cdots \subset \mathbb{K}\,,$$

přičemž každé další těleso v řetězci výše uvedených inkluzí v sobě zahrnuje více a více prvků z $\mathbb{K}$.

V této chvíli jsme, podle názoru autora, připraveni na hlavní větu tohoto článečku.

6. Konstruovatelná čísla

Věta 6.1. *Buď $x \in \mathbb{R}$. Potom číslo x je konstruovatelné (tedy $x \in \mathbb{K}$) právě tehdy, když existuje konečná posloupnost těles*

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n \subset \mathbb{R} \tag{6.1}$$

taková, že platí

- *$x \in \mathbb{K}_n$;*
- *pro všechna $j = 0, \ldots, n-1$ je $\mathbb{K}_{j+1} = \mathbb{K}_j(\sqrt{r_j})$, kde $r_j > 0$, $r_j \in \mathbb{K}_j$, a navíc $\sqrt{r_j} \notin \mathbb{K}_j$.*

Tato věta ukazuje, že způsob, jakým jsme si v předchozím paragrafu začali rozmýšlet „co všechno lze zkonstruovat“, byl podstatný. Věta 6.1 totiž říká, že konstruovatelná čísla vznikají přesně takto, tedy že číslo x je zkonstruovatelné právě tehdy, když se k němu můžeme dopracovat pomocí konečné „cestičky“ navzájem do sebe zařazených těles, přičemž každé další vzniká adjunkcí druhé odmocniny nějakého čísla z tělesa jemu předcházejícího.

Větu 6.1 zde nebudeme rigorózně (tj. matematicky zcela přesně) dokazovat. Autor si však dovolí poznamenat, že velkou část cesty k tomu, abychom porozuměli, proč je znění věty 6.1 právě takové, již máme za sebou: Jestliže umíme zkonstruovat odmocninu z čísla, které jsme byli schopni zkonstruovat dříve, a s ním i všechna čísla z „jím adjungovaného“ tělesa, je jasné, že umíme zkonstruovat postupně čísla z těles $\mathbb{K}_1$, $\mathbb{K}_2$, $\ldots \mathbb{K}_n$ z (6.1). Tím jsme ukázali, že pokud $x \in \mathbb{K}_n$, pak již i $x \in \mathbb{K}$.

Těžší je ukázat opačnou implikaci, tedy že každé konstruovatelné číslo už musí ležet v nějakém tělese tvaru $\mathbb{K}_n$ z (6.1). Ale ani to není nepřekonatelně obtížné: stačí si uvědomit, jak probíhá postupný proces konstruování nových čísel (vzdáleností) a nových bodů. Při výpočtu souřadnic nových bodů vždy hraje roli řešení buď lineární nebo nejvýše kvadratické rovnice, a tedy druhá odmocnina. Ať již počítáme vzdálenost dvou známých bodů pomocí Pythagorovy věty, souřadnice průsečíku dvou přímek, přímky a kružnice nebo dvou kružnic. Odtud už je téměř jasné, že každým takovým krokem přibudou k dosud konstruovatelným číslům čísla vyjádřitelná z nich pomocí čtyř tělesových operací a nejvýše druhé odmocniny známých čísel. Proto probíhá vytváření „cestičky“ těles $\mathbb{K}_1, \mathbb{K}_2, \ldots \mathbb{K}_n$ z (6.1) právě takto.[8]

V této chvíli máme tedy větu, která říká, jak obecně vypadají konstruovatelná čísla. To ovšem ještě neznamená, že pro dané konkrétní číslo je nějak jednoduché řetězec těles (6.1) nalézt nebo naopak ukázat, že žádná taková posloupnost těles neexistuje.

Abychom danou otázku byli schopni uspokojivě odpovědět alespoň pro dvě z našich tří starověkých úloh, budeme potřebovat ještě jednu malou odbočku.

7. Intermezzo: polynomiální rovnice

Autor se domnívá, že výsledky tohoto intermezza jsou nejen potřebné pro další osud našeho pátrání, ale i zajímavé a potřebné samy o sobě. Tedy, chutě do díla.

7.1. **Racionální kořeny polynomu s racionálními koeficienty.** Nejprve zformulujeme (a dokážeme) jedno zajímavé tvrzení a poté ukážeme, jak s jeho pomocí lze vždy nalézt všechny racionální kořeny polynomu s racionálními koeficienty.

Tvrzení 7.1. *Mějme algebraickou rovnici n-tého stupně*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0\,, \qquad a_n \neq 0\,,\ a_0 \neq 0\,, \tag{7.1}$$

s celočíselnými koeficienty, tj. $a_j \in \mathbb{Z}$ pro všechna $j = 0, \ldots, n$. Buď $\frac{p}{q}$ racionální kořen rovnice (7.1) takový, že čísla p, q nemají žádného společného dělitele (jsou nesoudělná). Potom číslo p je dělitelem čísla a_0 a číslo q je dělitelem čísla a_n.

Důkaz. Protože $\frac{p}{q}$ je kořenem rovnice (7.1), platí

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \cdots + a_1 \frac{p}{q} + a_0 = 0\,,$$

nebo, po vynásobení této rovnice číslem q^n,

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0\,. \tag{7.2}$$

Pokud z této rovnice vyjádříme $a_n p^n$, lze ze zbylých členů vytknout q a dostat

$$a_n p^n = -q \left(a_{n-1} p^{n-1} + \cdots + a_1 p q^{n-2} + a_0 q^{n-1}\right)\,.$$

Pravá strana této rovnosti je evidentně dělitelná číslem q. Musí být tedy dělitelný číslem q i výraz $a_n p^n$ na levé straně. Čísla p, q jsou však nesoudělná, proto q musí dělit a_n.

Z (7.2) však můžeme také vyjádřit $a_0 q^n$, a ze zbylých členů vytknout p. Dostaneme

$$a_0 q^n = -p \left(a_n p^{n-1} + a_{n-1} p^{n-2} q + \cdots + a_1 q^{n-1}\right)\,.$$

Podobně jako výše pak dostaneme, že číslo p musí dělit a_0. Důkaz je hotov. □

[8]Při důkazu této časti věty je ještě potřeba si uvědomit některá pomocná tvrzení, a sice že přímka, která spojuje dva konstruovatelné body, je vyjádřitelná rovnicí s konstruovatelnými koeficienty, a podobně v případě kružnice. Tyto (technické) důvody jsou právě tím, co vedlo autora k tomu, aby zde neprezentoval úplný důkaz věty 6.1, ale jen hlavní jeho myšlenku, která, podle jeho mínění, názorně ukazuje podstatu celé věci.

Výše uvedené tvrzení nám pomůže nalézt všechny racionální kořeny algebraické rovnice s racionálními koeficienty libovolného stupně. Jistě jste zaznamenali, že tvrzení 7.1 hovoří o algebraických rovnicích s celočíselnými koeficienty. Není však problém algebraickou rovnici s racionálními koeficienty vynásobit nejmenším společným násobkem jmenovatelů všech koeficientů rovnice, a tím z ní vyrobit rovnici, vyhovující předpokladům tvrzení, aniž se změní hodnoty jejich kořenů. Ukážeme si použití tvrzení 7.1 na příkladech.

Příklad 7.2. (1) Mějme rovnici

$$x^4 - \frac{1}{3}x^3 - \frac{20}{9}x^2 + \frac{2}{3}x + \frac{4}{9} = 0\,. \tag{7.3}$$

Rovnici nejprve vynásobíme devíti, abychom dostali rovnici s celočíselnými koeficienty, jak požaduje tvrzení 7.1:

$$9x^4 - 3x^3 - 20x^2 + 6x + 4 = 0\,.$$

Má-li tato rovnice nějaké racionální kořeny tvaru $\frac{p}{q}$, musí být podle tvrzení 7.1 číslo p dělitelem čísla 4, a číslo q dělitelem čísla 9. Máme tedy konečný seznam „kandidátů na čitatele“ racionálního kořene - jsou to všichni (celočíselní) dělitelé čísla 4, tedy ± 1, ± 2, ± 4. Podobně jmenovatelé případného racionálního kořene mohou být pouze čísla ± 1, ± 3, ± 9. Uvážením všech možností přicházíme tedy k závěru, že pokud má rovnice (7.3) racionální kořeny, musí se tyto nacházet v následujícím „seznamu kandidátů na racionální kořeny“:

$$\pm 1\,,\ \pm 2\,,\ \pm 4\,,\ \pm\frac{1}{3}\,,\ \pm\frac{2}{3}\,,\ \pm\frac{4}{3}\,,\ \pm\frac{1}{9}\,,\ \pm\frac{2}{9}\,,\ \pm\frac{4}{9}\,.$$

I když je tento výčet relativně dlouhý (obsahuje 18 prvků), je z principu věci vždy konečný. Lze tedy v konečném čase dosazováním jednoho kandidáta po druhém zjistit, zda je daný kandidát skutečně kořenem rovnice (7.3) či ne. Touto metodou snadno zjistíte, že $-\frac{1}{3}$ a $\frac{2}{3}$ jsou kořeny rovnice (7.3). Můžeme však říci dokonce víc: žádné další racionální kořeny tato rovnice již nemá. Kdyby je totiž měla, museli bychom na ně naší metodou přijít. Zbývající dva kořeny rovnice (7.3) tedy musí být iracionální nebo komplexní. Mimochodem, není těžké je odhalit: Protože známe dva kořeny rovnice (7.3), a sice $-\frac{1}{3}$ a $\frac{2}{3}$, musí být polynom $9x^4-3x^3-20x^2+6x+4$ dělitelný polynomem $(x+\frac{1}{3})(x-\frac{2}{3}) = x^2 - \frac{x}{3} - \frac{2}{9}$. Vydělením dostaneme

$$(9x^4 - 3x^3 - 20x^2 + 6x + 4)\ :\ \left(x^2 - \frac{x}{3} - \frac{2}{9}\right)\ =\ 9x^2 - 18 = 9\,(x^2 - 2)\,,$$

a kořeny rovnice $x^2 - 2 = 0$ snadno spočteme: $x_{1,2} = \pm\sqrt{2}$. Naše metoda tedy nakonec pomohla najít všechny kořeny rovnice (7.3). Jsou to $-\frac{1}{3}$, $\frac{2}{3}$, $\sqrt{2}$ a $-\sqrt{2}$.

(2) Ne vždy jsme takto úspěšní. Uvažujme například rovnici

$$x^4 + 2x^3 - 6x - 9 = 0\,. \tag{7.4}$$

Podobnými úvahami jako v předchozím příkladu zjistíme, že jedinými kandidáty na racionální kořeny této rovnice jsou čísla

$$\pm 1\,,\ \pm 3\,,\ \pm 9\,.$$

Dosazením však zjistíme, že žádné z nich rovnici nevyhovuje. Nepodařilo se nám tedy najít žádný kořen rovnice (7.4), přesto jsme se však o této rovnici něco dozvěděli, a sice to, že nemá žádné racionální kořeny. Kdyby totiž měla nějaké racionální kořeny, naší metodou bychom je našli.[9]

Naše intermezzo pokračuje ještě jednou malou odbočkou:

7.2. **Dvě zajímavé vlastnosti kořenů kubické rovnice.** Uvažujme algebraickou rovnici 3. stupně (neboli kubickou rovnici) tvaru

$$ax^3 + bx^2 + cx + d = 0\,, \qquad a, b, c, d \in \mathbb{R}\,, \quad a \neq 0\,. \tag{7.5}$$

Podle základní věty algebry má tato rovnice tři (obecně komplexní a nikoli nutně různé) kořeny z_1, z_2, z_3. Lze proto psát

$$ax^3 + bx^2 + cx + d = a(x - z_1)(x - z_2)(x - z_3)\,.$$

Vydělme tuto rovnici nenulovým číslem a a vpravo proveďme roznásobení. Dostaneme:

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = x^3 - x^2(z_1 + z_2 + z_3) + x(z_1z_2 + z_2z_3 + z_1z_3) - (z_1z_2z_3)\,.$$

Porovnáním koeficientů u stejných mocnin proměnné x vlevo a vpravo získáváme rovnosti[10]:

$$z_1 + z_2 + z_3 = -\frac{b}{a}\,, \tag{7.6}$$

$$z_1z_2 + z_2z_3 + z_1z_3 = \frac{c}{a}\,, \tag{7.7}$$

$$z_1z_2z_3 = -\frac{d}{a}\,. \tag{7.8}$$

Kromě matematické krásy, plynoucí ze symetrie získaných vztahů, hodí se (7.6)–(7.8) například v situaci, kdy známe dva kořeny rovnice (7.5). Třetí z nich pak snadno spočteme ze vztahu (7.6). Přesně to za chvíli použijeme. Předtím však zformulujeme druhou zajímavou vlastnost.

Tvrzení 7.3. *Buď $\mathbb{K}_j$, $j \in \{0, \dots, n-1\}$ jedno z těles definovaných ve větě 6.1. Uvažujme kubickou rovnici*

$$ax^3 + bx^2 + cx + d = 0\,, \qquad a \neq 0\,, \tag{7.9}$$

s koeficienty a, b, c, $d \in \mathbb{K}_j$. Nechť rovnice (7.9) *má kořen tvaru $p + q\sqrt{r}$, kde $p, q, r \in \mathbb{K}_j$, $r > 0$, přičemž $\sqrt{r} \notin \mathbb{K}_j$. Pak $p - q\sqrt{r}$ je také kořenem rovnice* (7.9).

[9] Pokud vás to zajímá, kořeny rovnice (7.4) jsou $\pm\sqrt{3}$, $-1 \pm i\sqrt{2}$.

[10] Tyto rovnosti jsou známy jako Viètovy vzorce. Uměli byste podobné vztahy odvodit i pro algebraické rovnice čtvrtého, pátého, případně n-tého stupně?

Důkaz. Definujme nejprve číslo „s pruhem“, přesněji tzv. číslo „přidružené k číslu“ $p + q\sqrt{r}$ předpisem[11]

$$\overline{p + q\sqrt{r}} := p - q\sqrt{r}\,.$$

Pro $z = p + q\sqrt{r}$ pak dostáváme

$$\overline{z^2} = \overline{(p + q\sqrt{r})^2} = \overline{p^2 + 2pq\sqrt{r} + q^2 r} = p^2 - 2pq\sqrt{r} + q^2 r = (p - q\sqrt{r})^2 = \overline{z}^2$$

a podobně dostaneme i

$$\overline{z^3} = \overline{(p + q\sqrt{r})^3} = \cdots = \overline{(p + q\sqrt{r})}^3 = \overline{z}^3\,.$$

Je-li tedy $z = p + q\sqrt{r}$ kořenem rovnice (7.9), platí

$$\begin{aligned} 0 = \overline{0} = \overline{az^3 + bz^2 + cz + d} &= \overline{az^3} + \overline{bz^2} + \overline{cz} + \overline{d} \\ &= \overline{a}\overline{z}^3 + \overline{b}\overline{z}^2 + \overline{c}\overline{z} + \overline{d} \\ &= a\overline{z}^3 + b\overline{z}^2 + c\overline{z} + d\,, \end{aligned}$$

a proto i $\overline{z} = p - q\sqrt{r}$ je kořenem rovnice (7.9), což jsme měli dokázat. □

Blížíme se k finále.

8. Dořešení starořeckých problémů

Už nám chybí jenom malý krůček, sestávající z několika ještě menších krůčků. Učiňme je.

Následující věta je prvním z nich a je většinou označována slovy „docela překvapující“.

Věta 8.1. *Buď*

$$ax^3 + bx^2 + cx + d = 0\,, \qquad a \neq 0\,, \tag{8.1}$$

kubická rovnice s racionálními koeficienty, tj. a, b, c, $d \in \mathbb{Q}$. Pokud rovnice (8.1) *nemá žádné racionální kořeny, pak nemá ani žádné konstruovatelné kořeny.*

Důkaz. Předpokládejme pro spor, že rovnice (8.1) má konstruovatelný kořen $x \in \mathbb{R}$. Potom podle věty 6.1 existuje konečná posloupnost těles

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n \subset \mathbb{R} \tag{8.2}$$

taková, že

- $x \in \mathbb{K}_n$;
- pro všechna $j = 0, \ldots, n-1$ je $\mathbb{K}_{j+1} = \mathbb{K}_j(\sqrt{r_j})$, kde $r_j > 0$, $r_j \in \mathbb{K}_j$, a navíc $\sqrt{r_j} \notin \mathbb{K}_j$.

Kýženého sporu dosáhneme v několika krocích.

Krok 1: Ukážeme nejprve, že pokud rovnice (8.1) nemá žádné racionální kořeny, pak nemá ani žádné kořeny z tělesa $\mathbb{K}_1$. Prvky tělesa $\mathbb{K}_1$ jsou tvaru $p + q\sqrt{r}$, kde $p, q, r \in \mathbb{Q}$, $r > 0$, a $\sqrt{r} \notin \mathbb{Q}$. Pokud by rovnice (8.1) měla kořen uvedeného tvaru, pak by podle tvrzení 7.3 (pro $j = 0$) bylo i číslo $p - q\sqrt{r}$ kořenem rovnice (8.1).

[11]Čtenář, znalý komplexních čísel, speciálně pojmu „komplexně sdružené číslo“, možná vidí jakousi paralelu.

Tyto dva kořeny by pak spolu se (zatím neznámým) třetím kořenem z podle (7.6) splňovaly vztah

$$z + (p + q\sqrt{r}) + (p - q\sqrt{r}) = -\frac{b}{a} \qquad \text{odkud dostaneme} \qquad z = -\frac{b}{a} - 2p \in \mathbb{Q}\,.$$

Třetí kořen z rovnice (8.1), by tedy byl racionální. To je ovšem spor s tím, že rovnice (8.1) nemá podle předpokladů žádné racionální kořeny.

Krok 2: Buď nyní $j \in \mathbb{N}$. Ukážeme, pokud rovnice (8.1) nemá žádné kořeny v tělese $\mathbb{K}_j$, pak nemá ani žádné kořeny z tělesa $\mathbb{K}_{j+1}$. Postupujeme stejně jako v předchozím kroku: prvky tělesa $\mathbb{K}_{j+1}$ jsou tvaru $p+q\sqrt{r}$, kde $p, q, r \in \mathbb{K}_j$, $r > 0$, a $\sqrt{r} \notin \mathbb{K}_j$. Pokud by rovnice (8.1) měla kořen uvedeného tvaru, pak by podle tvrzení 7.3 bylo i číslo $p - q\sqrt{r}$ kořenem rovnice (8.1). Tyto dva kořeny by pak spolu se (zatím neznámým) třetím kořenem z podle (7.6) splňovaly vztah

$$z + (p + q\sqrt{r}) + (p - q\sqrt{r}) = -\frac{b}{a} \qquad \text{odkud dostaneme} \qquad z = -\frac{b}{a} - 2p \in \mathbb{K}_j\,.$$

Třetí kořen z rovnice (8.1), by tedy byl prvkem $\mathbb{K}_j$, to je ovšem spor.

Krok 3: Zbývá vlastně shrnout to, co jsme doposud ukázali. Předpokládali jsme, že rovnice (8.1) má konstruovatelný kořen $x \in \mathbb{R}$, což implikovalo, že takový kořen musí ležet v tělese $\mathbb{K}_n$ zkonstruovaném v (8.2). Z kroku 1 však plyne, že těleso $\mathbb{K}_1$ neobsahuje žádný konstruovatelný kořen rovnice (8.1). Postupnou aplikací kroku 2 odtud dostaneme, že takový kořen nemůže ležet ani v tělesech $\mathbb{K}_2$, $\mathbb{K}_3$, $\dots \mathbb{K}_n$, tedy $x \notin \mathbb{K}_n$. Tento spor ukazuje, že rovnice (8.1) nemá žádný konstruovatelný kořen. $\square$

A už jsme ve finále. Podívejme se znovu, naposledy, na tři starověké problémy.

8.1. **Zdvojnásobení krychle.** Máme odpovědět na otázku, je-li číslo $\sqrt[3]{2}$ konstruovatelné. Číslo $\sqrt[3]{2}$ je ovšem řešením rovnice $x^3 - 2 = 0$, což je kubická rovnice s celočíselnými koeficienty. Pokud by tato rovnice měla nějaký racionální kořen, muselo by to podle postupu z paragrafu 7.1 být jedno z čísel ± 1, ± 2. Žádné z těchto čtyř čísel však (jak zjistíme dosazením) rovnici $x^3 - 2 = 0$ nevyhovuje, proto v souladu s úvahami z paragrafu 7.1 docházíme k závěru, že rovnice $x^3 - 2 = 0$ nemá žádné racionální kořeny. To však podle věty 8.1 znamená, že nemá ani žádné konstruovatelné kořeny, a že tedy její kořen $\sqrt[3]{2}$ není konstruovatelné číslo. Proto *zdvojnásobení krychle není možno provést eukleidovskou konstrukcí, s použitím pouze pravítka a kružítka.*

8.2. **Trisekce úhlu.** Postupujeme zcela obdobně. Máme odpovědět na otázku, je-li řešení rovnice $8x^3 - 6x - 1 = 0$ konstruovatelné. Jedinými kandidáty na případný racionální kořen této rovnice jsou podle paragrafu 7.1 čísla ± 1, $\pm\frac{1}{2}$, $\pm\frac{1}{4}$, $\pm\frac{1}{8}$. Žádné z těchto čísel však (jak zjistíme dosazením) rovnici $8x^3 - 6x - 1 = 0$ nevyhovuje, proto tato rovnice nemá žádné racionální kořeny. To však podle věty 8.1 znamená, že nemá ani žádné konstruovatelné kořeny. Proto *trisekci obecného úhlu (speciálně úhlu 60°) není možno provést eukleidovskou konstrukcí, s použitím pouze pravítka a kružítka.*

8.3. **Kvadratura kruhu.** Čtenáře v této chvíli možná trochu zklameme, protože otázku kvadratury kruhu nebudeme schopni vyřešit bez jedné další dodatečné znalosti, kterou čtenáři předložíme bez důkazu. Jde o jednu důležitou vlastnost čísla π, kterou dokázal v roce 1882 německý matematik Ferdinand von Lindemann (viz [2]). Lindemann dokázal, že číslo π není řešením žádné algebraické rovnice s racionálními koeficienty. Této vlastnosti se říká *transcendence*, o čísle π tedy již téměř 130 let víme, že je transcendentní. Vyzbrojeni touto znalostí, uvažujme. Kdyby číslo π bylo konstruovatelné, leželo by podle věty 6.1 v některém z těles $\mathbb{K}_n$. Jak však vypadají čísla z tohoto tělesa? Tato čísla jsou sestavena z racionálních čísel pomocí čtyř základních aritmetických operací a dále z konečného počtu druhých odmocnin, postupně adjungovaných k racionálním číslům, které odpovídají počtu těles na „cestičce“ od $\mathbb{Q}$ ke $\mathbb{K}_n$. Taková čísla jsou však vždy kořeny nějaké algebraické rovnice s racionálními koeficienty: rozmyslete si to na příkladu čísla $a = 2 + \sqrt{\frac{1}{2} + \sqrt{3}}$. Není těžké vypozorovat, jakým způsobem následující konstrukce z vyjádření čísla a „odstraní odmocniny“: $((a-2)^2 - \frac{1}{2})^2 = 3$. To, co jsme však dostali, není nic jiného než výrok, že číslo a řeší algebraickou rovnici s racionálními koeficienty. Kdyby tedy číslo π bylo konstruovatelné, leželo by v některém z těles $\mathbb{K}_n$ a bylo by tedy kořenem nějaké algebraické rovnice s racionálními koeficienty. Lindenmann však ukázal, že to není možné. Proto číslo π není konstruovatelné a není tedy konstruovatelné ani číslo $\sqrt{\pi}$ (kdyby bylo, byl by konstruovatelný i jeho součin se sebou samým, tedy číslo π).

A to jsme chtěli vědět. Proto ani *kvadraturu kruhu není možno provést eukleidovskou konstrukcí, s použitím pouze pravítka a kružítka.*

Jsme tedy hotovi. Ale možná přece jenom ještě něco, jen tak pro úplnost, o konstruovatelných objektech prozradíme.

9. A co pravidelný n-úhelník?

Možná vás v průběhu čtení o tom, co všechno lze zkonstruovat pomocí pravítka a kružítka, napadlo: a které pravidelné n-úhelníky v rovině lze sestrojit pomocí zmíněných dvou nástrojů, ví se to? Ano, ví se to, odpověď na tuto otázku však vyžaduje překvapivě hlubší znalosti z teorie čísel, zejména znalosti o tzv. Fermatových číslech.

Fermatova čísla dostala své jméno po Pierru de Fermat, francouzském matematikovi 17. století, který se jim jako první soustavně věnoval. Fermatova čísla jsou čísla tvaru

$$F_n = 2^{2^n} + 1\,, \qquad n = 0, 1, 2, \ldots \tag{9.1}$$

Fermat vyslovil domněnku, že všechna čísla uvedeného tvaru jsou prvočísla. Připustil však, že neumí tuto domněnku dokázat, předvedl pouze to, že $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ a $F_4 = 65\,537$ skutečně prvočísla jsou. Domněnce se všeobecně věřilo. Proto bylo překvapením, když Leonhard Euler téměř o sto let později ukázal, že číslo F_5 je číslo složené. Platí totiž:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417\,.$$

Od té doby došlo ve zkoumání Fermatových čísel k zajímavému vývoji. Ukázalo se totiž, že navzdory Fermatově domněnce jsou čísla F_0, F_1, F_2, F_3 a F_4 naopak jediná k dnešnímu dni známá prvočísla mezi čísly tvaru (9.1). Pomocí (mimo jiné i) výpočetní techniky bylo ukázáno,[12] že čísla F_5 až F_{32} jsou čísla složená. A co číslo F_{33}? Věřte nebo nevěřte, ani dnešní pokročilá technika nestačí na to, aby ukázala, jestli číslo F_{33} (které má přes dvě a půl miliardy cifer) je číslo složené nebo prvočíslo. Neví se ani to, je-li mezi Fermatovými čísly konečně nebo nekonečně mnoho prvočísel, ani to, je-li konečně nebo nekonečně mnoho z nich číslo složené.

Jak to celé souvisí s konstruovatelností pravidelného n-úhelníku pomocí pravítka a kružítka? Německý matematik Carl Friedrich Gauss ukázal v roce 1796, že pokud je přirozené číslo $n \geq 3$ buď přirozenou mocninou dvojky nebo číslem tvaru $2^k p_1 p_2 \dots p_m$, kde k je nezáporné celé číslo a $p_1, p_2, \dots, p_m$ jsou navzájem různá Fermatova prvočísla, lze pravidelný n-úhelník sestrojit pomocí pravítka a kružítka. Gauss se navíc správně domníval, že jiné pravidelné mnohoúhelníky pomocí pravítka a kružítka sestrojit nelze, dokázat se to však podařilo až Pierru Wantzelovi v roce 1837, viz [3].

Kdybychom si tedy chtěli udělat jasno v konstrukcích pravidelných n-úhelníků pro (například) $n \leq 20$, zjistili bychom tot: 4, 8 a 16 jsou mocninami dvojky a 3, 5, $3 \cdot 5 = 15$ a 17 jsou Fermatovými prvočísly nebo součiny Fermatových prvočísel, menších než 20. Konečně, do seznamu zkonstruovatelných n-úhelníků patří ještě 6, 10, 12 a 20 – dvojnásobky a čtyřnásobky Fermatových prvočísel a jejich součinů.

A to je vše, všechny ostatní pravidelné mnohoúhelníky (pro $n \leq 20$) už sestrojit nelze: jsou to (pro $n \leq 20$) pravidelné n-úhelníky s počtem stran $n = 7, 9, 11, 13, 14, 18$ a 19.

10. Závěrečné poznámky a pár úloh

Tento text je záznamem přednášky, kterou měl autor dne 27.4.2011 v rámci tzv. „Kurzů pro nadané žáky“, které pro středoškoláky s matematickými zájmy pořádá Matematicko-fyzkální fakulta Univerzity Karlovy v Praze, viz [6]. V rámci této přednášky bylo účastníkům předloženo několik úloh, na kterých si mohli procvičit probíranou látku. Pro úplnost a taky jako odpověď na sugestivní otázku „Proč ne?“ jsou zmíněné úlohy i součástí tohoto textu.

Cvičení 10.1.
(1) Využitím metody popsané v paragrafu 7.1 na straně 10 nalezněte všechna řešení rovnice
$$4\,x^4 - 3\,x^3 - 4\,x^2 + 27\,x - 18 = 0\,.$$
(2) Ukažte použitím téže metody, že rovnice
$$x^4 + x^2 + 2\,x + 6 = 0$$
nemá žádná racionální řešení.
(3) V důkazu tvrzení 2.1 na straně 3 jsme ukázali, že číslo $\sqrt{2}$ není racionální (tj. nelze zapsat jako podíl dvou celých čísel).
- Ukažte stejnou metodou, že ani číslo $\sqrt{5}$ není racionální.

[12] Všechna tvrzení o Fermatových číslech odpovídají stavu znalostí o nich k 20.6.2011, viz [5].

- (*) Ukažte, že pokud p_1, p_2, …, p_k jsou různá (tedy nesoudělná) prvočísla, že pak ani číslo $\sqrt{p_1 \cdot p_2 \cdots p_k}$ není racionální. (*Návod*: napište opět $\sqrt{p_1 \cdot p_2 \cdots p_k}$ jako podíl dvou celých čísel a zkoumejte dělitelnost jedním konkrétním vybraným prvočíslem p_j.)
- Ukažte, že pro všechna n přirozená platí: $\sqrt{n}$ je buď přirozené nebo už iracionální. (*Návod*: napište prvočíselný rozklad čísla n, odmocněte vše, co odmocnit lze — tedy sudé mocniny všech prvočísel obsažených v rozkladu n — a využijte výsledek z předchozího bodu.)
- (*) Využijte tento postup ke studiu iracionality vyšších odmocnin přirozených čísel, tedy výrazů tvaru $\sqrt[k]{n}$, kde $k, n \in \mathbb{N}$.

(4) Odvoďte Viètovy vzorce (viz (7.6)–(7.8)) pro obecnou algegraickou rovnici n-tého stupně.

(5) Napište, které všechny n-úhelníky pro $n \leq 100$ lze sestrojit pomocí pravítka a kružítka.

(6) (*) Zkuste nalézt konstrukci, kterou se pomocí pravítka a kružítka sestrojí pravidelný pětiúhelník.

Reference

[1] H.-J. Bartsch, *Matematické vzorce*, Academia, Praha, 2009.
[2] F. Lindemann, Über die Zahl π, *Mathematische Annalen* 20 (1882), pp. 213-225.
[3] P. L. Wantzel, Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas, *Journal de Mathématiques Pures et Appliquées* 1 (2) (1837), pp. 366-372.
[4] D. Wells, *The Penguin Dictionary of Curious and Interesting Geometry*, Penguin Books, 1991.
[5] http://www.prothsearch.net/fermat.html
[6] http://www.karlin.mff.cuni.cz/olympiada/?page=courses

doc. RNDr. Mirko Rokyta, CSc.
katedra matematické analýzy MFF UK Praha
Sokolovská 83
186 00 Praha 8 – Karlín
rokyta@karlin.mff.cuni.cz