Pomocný text k 6. sérii

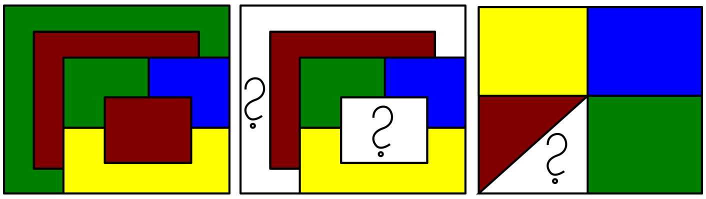
Velké věty

autor: *BRKOS Team*

Podobně jako tento odstavec je celý jedna velká věta, je i tato série věnována velkým větám, které, ačkoli jsou velice težké na dokázání a mnohdy si nevystačíte ani s několika léty na vysoké škole, mají znění, které je krásně pochopitelné se základními znalostmi, a proto vám je předkládáme zde v pomocném textu i s drobným komentářem a umožňujeme vám je použít v řešení úloh této série.

Věta o čtyřech barvách

Jedním z velkých matematických problémů, který dlouhou dobu odolával důkazu, je tzv. Problém čtyř barev. V nejjednodušší variantě se jedná o tvrzení, že každou politickou mapu lze obarvit pomocí čtyř barev tak, aby žádné dva sousedící státy neměly stejnou barvu. Tato formulace je ovšem poněkud vágní, jelikož z ní například není jasné, jestli spolu sousedí státy, jejichž území se dotýkají jen rohem (bodem), nebo jestli území jednoho státu může být nesouvislé (např. USA a Aljaška). Pro oba tyto příklady lze ovšem snadno najít mapu takovou, která čtyřmi barvami obarvit nelze.

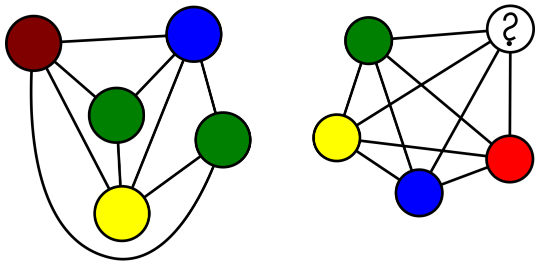


Obrázek 1: Příklady obarvení map

Na obrázku 1 se nachází tři mapy. Map nalevo jen ukazuje, že i složitější mapy lze skutečně dobře obarvit. Pokud ovšem požadujeme, aby dvě území měla stejnou barvu (respektive jeden stát měl více území), mapa uprostřed je protipříkladem, který čtyřmi barvami obarvit nelze. Konečně třetí mapa nezle obarvit v případě, že nechceme, aby státy stejné barvy sdílely roh.

I když se původní motivace tohoto problému ukrývá právě v obarvování map, dnes je Problém čtyř barev většinou formulován jako problém teorie grafů. Teorie grafů je odvětví matematiky, které zkoumá tzv. grafy, což jsou v podstatě pouze kolekce bodů (vrcholů) a hran, které spojují některé dvojice těchto bodů. O grafu řeknem, že je rovinný, pokud lze nakreslit na papír tak, aby se nekřížily žádné nakreslené hrany. Na obrázku můžete vidět příklad rovinného a nerovinného grafu.

V teorii grafů lze Větu o čtyřech barvách formulovat následovně:



Obrázek 2: Příklady rovinného a nerovinného grafu

Věta. (O čtyřech barvách) Vrcholy každého rovinného grafu lze obravit čtyřmi barvami tak, že neexistuje dvojice vrcholů stejné barvy, které by sdílely hranu.

Za zmínku stojí také příběh důkazu této věty. Slabší varianta věty hovořící o pěti barvách byla dokázána již v roce 1890 Percym Heawoodem. Důkaz věty o čtyřech barvách však odolával mnoho dalších let. Dokonce ani dnes někteří matematici jejímu důkazu nevěří. Všechny dosud předložené důkazy totiž využívají počítačový program. Důkaz redukují problém na pouze konečné množství (několik tisíc) „elementárních“ grafů, jejichž obarvitelnost zaručí obarvitelnost libovolného grafu. Obarvitelnost těchto „elementárních“ grafů vždy ověřuje počítač. Právě část zahrnující výpočet počítače není mnoha matematiky uznávána, a to ze dvou důvodů. Samotný program může obsahovat chybu a i pokud je napsán správně, je jistá šance, že došlo k hardwarové chybě výpočtu. Asi nejdůvěryhodnější důkaz byl napsán v roce 2005. Jednalo se o program v dokazovacím systému Coq. Coq je plnohodnotný programovací jazyk doplněný o důkazový systém. Lze v něm proto napsat program a rovnou ho vybavit formálním důkazem korektnosti, který je počítačově ověřen. Můžeme si pro být jistí, že program použitý pro důkaz byl korektní, za předpokladu, že je korektní jádro samotného Coqu.

Velká Fermatova věta

První věc, kterou můžeme s jistotou říci, je, že Velká Fermatova věta patří k celkově nejznámějším matematickým problémům, a to nejen mezi matematiky: na české wiki si můžete přečíst, v kolika různých seriálech, povídkách, divadelních hrách atd. se Velká Fermatova věta objevila. Důvod, proč je toto tvrzení tak známé mezi širší veřejností, je pravděpodobně stejný, jako proč je věta zajímavá pro matematiky: jedná se o tvrzení velmi jednodnoduché co do formulace, ale extrémně náročné co do důkazu. Pierre de Fermat toto tvrzení načmáral na okraj jedné knihy v roce 1637 a až v roce 1995 zvládl Andrew Wiles (a to až na druhý pokus) podat kompletní důkaz.

Připomeňme tedy znění: Velká Fermatova věta nám říká, že pro žádné přirozené $n > 2$ rovnice

$$x^n + y^n = z^n$$

nemá v oboru přirozených čísel řešení. Tedy formulovat toto tvrzení opravdu zvládné každý, kdo ví, co je sčítání a umocňování. Co se týče jeho důkazu: povšimněme si, že nám stačí toto tvrzení dokázat pro $n = 4$ a n liché prvočíslo: ostatní případy pak již hned vyplynou (jednoduše protože $x^{pq} = (x^p)^q$). Důkaz pro $n = 4$ zvládl sám Fermat (sice tvrdil, že i pro ostatní n, ale dnes už mu to nikdo nevěří) a případ $n = 3$ byl vyřešen jen o málo později. Tím ale úspěchy na delší dobu končí. Až v 19. století přišel další průlom, především díky práci Kummera a Dedekinda, kteří položili základy algebraické teorie čísel. Díky novým metodám (motivovaným právě Fermatovým tvrzením) se z domněnky stala věta pro třídu tzv. regulárních prvočísel. Důvod k bujarým oslavám to ale tak úplně nebyl, jelikož prvočísel, která regulární nejsou, je nekonečně mnoho (fun fact: dodnes nevíme, jestli těch regulárních je konečně či nekonečně mnoho, nicméně patří mezi ně všechna prvočísla menší než 23).

Na další pokrok si musíme počkat až do roku 1955, kdy byla poprvé vyslovena Taniyama-Shimurova domněnka, o níž bylo záhy dokázáno, že pouze její částečný důkaz implikuje Velkou Fermatovu větu. Jednalo se však o natolik fascinující a hluboké tvrzení, že mnoho matematiků v té době ani nevěřili, že ji v následujích staletích někdo zvládne dokázat (leckdo si dnes myslí totéž např. o Riemannově hypotéze). Tato domněnka zhruba říká, že každé eliptické křivce nad racionalními čísly (cca se jedná o množinu řešení rovnice $y^2 = x^3 + ax^2 + bx + c$, kde a, b, c jsou racionální koeficienty) lze přiřadit jedinou modulární formu (cca funkce komplexní proměnné, která něco splňuje).

Příběh končí v letech 1994-5, kdy Andrew Wiles před značně šokovaným sálem matematiků předvedl důkaz Taniyama-Shimurovy domněnky pro třídu tzv. Freyových křivek a následně po dalším roce tvrdé práce zládl opravit chybu, která byla v důkaze nalezena. Z toho pak vyplynula Velká Fermatova věta. Důkaz je zhruba následující: předpokládejme, že rovnice $x^n + y^n = z^n$ má pro nějaké $n > 2$ řešení (a, b, c). Potom můžeme sestrojit eliptickou křivku

$$y^2 = (x - a)(x - b)(x - c).$$

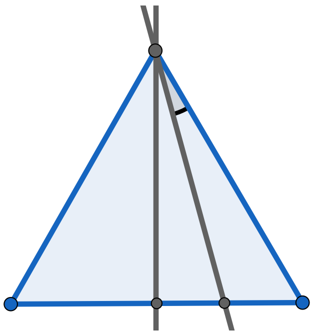
Ta patří mezi Freyovy křivky, tedy podle Wilesova dlůkazu jí přísluší modulární forma jistých parametrů. Ale jak už bylo řečeno, modulárních forem je dost málo, speciálně pro dané parametry neexistuje žádná a máme spor. Tím tedy skončil příběh Velké Fermatovy věty, ale začala se psát historie tzv. Langlandsova programu – série velmi odvážných a hlubokých domněnek, z níž Taniyama-Shimurova byla jen první krůček.

Trisekce úhlu

Narozdíl od spousty vět a metod pro řešení planimetrických úloh se zde setkáváme s problémem, jehož krása je, že žádnými metodami řešit nelze. Jde o problém třetění (tedy *trisekce*) libovolného úhlu, a to pouze pomocí pravítka a kružítka. Z úhlu θ chceme jednoduše získat úhel $\frac{\theta}{3}$ (na kalkulačce by se tento problém jistě vyřešil snadno)

Samozřejmě existuje hromada úhlů, které roztřetit umíme ($90°$, $360°, \dots$). Pěkným příkladem je i úhel 3θ pro nějaký zkonstruovatelný úhel θ (úhel, který lze pomocí pravítka a kružítka zkonstruovat, např. $45°, 108°, \dots$). Jednoduše na počáteční úhel zapomeneme a úhel θ zkonstruujeme přímo.

Příklad. Sestrojte třetinu úhlu $\alpha = 45°$.

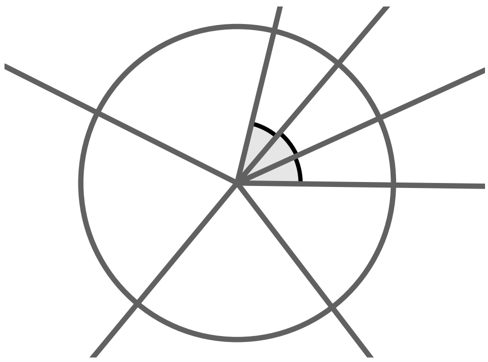


Dá-li nám někdo úhel 45° na papíře, můžeme jej okamžitě zahodit a spokojeně sestrojit 15° jakožto polovinu poloviny vnitřního úhlu rovnostranného trojúhelníku. Všechny tyto operace lze pomocí pravítka a kružítka provést.

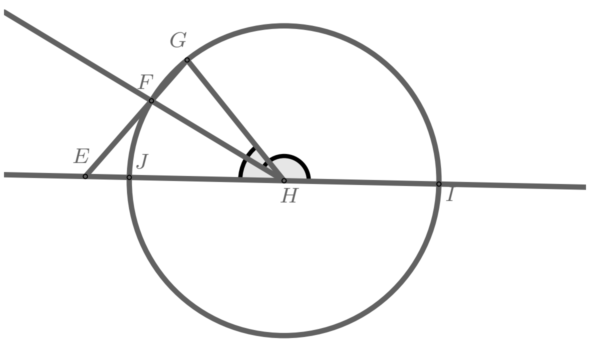
Všechny roztřetitelné úhly však nemusí být nutně zkonstruovatelné, potom však není zkonstruovstelná ani jeho třetina:

Příklad. Sestrojte třetinu úhlu $\beta = \frac{3\pi}{7}$

Tentokrát daný úhel použijeme. Když jej totiž zpětinásobíme, což je možné, dostaneme úhel $\frac{15\pi}{7}$, což po odečtení plného úhlu dělá $\frac{\pi}{7}$, což je opravdu třetina původního. (Na obrázku jsou uvedeny tři třetiny dávající dohromady původní úhel)



Existují však úhly (jako třeba i 60°), které pravítkem a kružítkem roztřetit nelze. Důkaz však používá složitějších algebraických struktur a proto jej zde uvádět nebudeme. Existují však geometrie, ve kterých toto učinit lze. Jedním příkladem je tzv. *neusis* konstrukce:



Kde máme zadaný úhel $\sphericalangle IHF$ a roztřetíme jej tak, že pravítko, které je stejně dlouhé jako poloměr kružnice (čili $|GH|$), budeme přikládat k bodu F, dokud jeden konec E nebude ležet na přímce HJ a druhý konec G na kružnici k. Potom nám vznikne úhel $\sphericalangle GHE$, jehož trojnásobek je právě $\sphericalangle IHF$.

Dalším příkladem rozšířené geometrie, kde je možné roztřetit úhel, je *origami geometrie*. Její přesný postup však necháme čtenáři.

Catalanova věta

Catalanova věta (někdy také Catalanova domněnka nebo Mihăilescova věta) patří mezi ta nádherná tvrzení v matematice, která jsou ve své podstatě velice komplikovaná, ale jejichž formulace je přitom velice jednoduchá. Posuďte sami:

Věta. Nechť x, y, a, b jsou přirozená čísla taková, že a i b jsou větší než 1. Pak rovnice

$$x^a - y^b = 1$$

má jediné řešení a to $3^2 - 2^3 = 1$.

Zdá se vám tvrzení jednoduché? Tak se pokuste o důkaz. Celé matematické komunitě trvalo přes 150 let, než se jí podařilo ho najít. Tvrzení postuloval belgicko-francouzský matematik Eugène Charles Catalan už v roce 1844 (mimochodem je to ten stejný, po kterém jsou pojmenována Catalanova čísla) a dokázáno bylo poměrně nedávno – v roce 2002. Dokázal ho rumunský matematik Preda Mihăilescu. Zajímavostí je, že trvzení dokazoval nadvakrát – ne že by první důkaz snad byl nekorektní, ale potřeboval vyzkoušet mnoho možností, a tak bylo zapotřebí pomoci počítače. Na druhý pokus pak našel dostatečně elegantní argument, aby tohoto nebylo třeba.

Řekněme si přeci jen něco málo k důkazu. První jednoduché pozorování (a jediná věc, kterou si zvládneme odůvodnit my tady) je, že nám stačí uvažovat, že a a b jsou prvočísla. Proč? Tak pokud víme, že neexistuje žádné řešení (kromě $3^2 - 2^3$), když a, b jsou libovolná, tak určitě neexistuje, když podmínky zpřísníme, aby a, b byla prvočísla. Ukažme si, že to funguje i naopak. Předpokládejme tedy, že rovnice má jediné řešení pro a, b prvočísla, ale existuje řešení x_1, a_1, y_1, b_1, kde a_1, b_1 jsou složená (případ, kdy je jenom jedno z čísel složené by se vyřešil úplně stejně). Pak ale $a = pk$ a $b = ql$ pro vhodná přirozená čísla k, l a prvočísla p, q. Potom máme následující rovnost:

$$1 = x_1^{a_1} - y_1^{b_1} = x_1^{pk} - y_1^{ql} = \left(x_1^k\right)^p - \left(y_1^l\right)^q.$$

Ale jelikož předpokládáme platnost Catalanovy věty pro prvočísla v exponentu, tak to znamená, že $3 = x_1^k$, což se nemůže stát, když k není 1 (což není, jelikož kp musí být složené číslo).

Bohužel si toho více nejsme schopni ukázat, vězte však, že důkaz by dále bylo nutno rozvést do několika částí. Nejprve by bylo třeba vyřešit zvláště případy, kdy alespoň jeden z exponentů je sudý (mimochodem jedná se o poměrně častý jev v teorii čísel, když chcete dokázat, že něco platí pro všechna prvočísla, tak je často potřeba vzít dvojku zvlášť). Tyto případy jsou jednodušší a alespoň některé z nich se dají udělat elementárně, ale jsou i tak technické a náročné. Mimochodem jeden z případů, kde je exponent sudý ($y^2 - x^3 = 1$) vyřešil už Leonhard Euler a ač o tom tehdy nevěděl, tak k důkazu použil eliptické křivky, které byly zmíněny v části o Velké Fermatově větě. Zbytek důkazu (tak jak ho vedl Mihăilescu) využívá pokročilých matematických oblastí jako je Galoisova teorie a kruhová tělesa. Jediné, co o těchto oblastech zvládnu říci je, že kruhová tělesa jsou matematické objekty, které se chovají podobně jako racionální čísla, ale navíc obsahují speciální prvek (komplexní číslo), který splňuje, že jeho několikátá mocnina je rovna jedné, ale žádná menší přirozená mocnina jedné rovna není. Pro ty, kdo znají komplexní čísla, tak můžu říct, že například množina $\{a + bi \mid a, b \in \mathbb{Q}\}$ je kruhové těleso – význačným prvkem je imaginární jednotka, jejíž čtvrtá mocnina je rovna jedné, ale žádná dřívější mocnina ne. Pro ty z vás, kdo by si chtěli procvičit použití Catalanovy věty na nějakých příkladech ze středoškoleské matematiky ještě jinde než v Brkosu, tak jí lze použít například při řešení následujícího příkladu (MO67-A-II-4): Rozhodněte, zda existují kladná celá čísla n a k taková, že

$$\frac{n}{11^k - n}$$

je druhou mocninou přirozeného čísla.

Zdroj: `https://www.mimuw.edu.pl/~zbimar/Catalan.pdf`