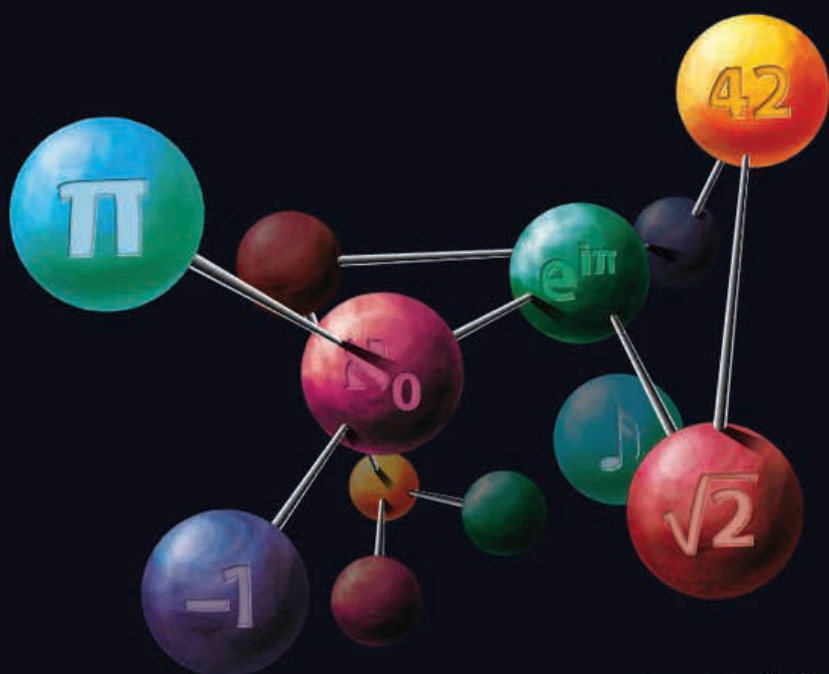


Ian Stewart

NEUVĚŘITELNÁ ČÍSLA

profesora Stewarta



argo / dokořán

Ian Stewart

NEUVĚŘITELNÁ ČÍSLA

profesora Stewarta

DOKOŘÁN

Ian Stewart

Neuvěřitelná čísla profesora Stewarta

Copyright © Joat Enterprises 2015

Translation © Jan Klíma, 2019

Všechna práva vyhrazena. Žádná část této publikace nesmí být rozmnožována a rozšiřována jakýmkoli způsobem bez předchozího písemného svolení nakladatele.

Druhé vydání v českém jazyce (první elektronické).

Z anglického originálu *Professor Stewart's Incredible Numbers* přeložil Jan Klíma.

Odpovědný redaktor Zdeněk Kárník.

Grafická úprava Vladimír Fára, sazba Karel Horák.

Obálka Michal Puhač podle návrhu Pavla Růta.

Redakce Marie Černá.

Vydalo v roce 2021 nakladatelství Dokořán, s. r. o.,

Holečkova 9, Praha 5,

dokoran@dokoran.cz, www.dokoran.cz,

jako svou 1094. publikaci (348. elektronická).

ISBN 978-80-7675-001-2

OBSAH

Předmluva	7
Číslo	10
I. Malá čísla	23
1 Nedělitelná jednička	24
2 Sudá a lichá	28
3 Kubická rovnice	46
4 Čtverec	54
5 Pythagorejská přepona	68
6 Kissing Number	78
7 Čtvrté prvočíslo	83
8 Fibonacciho třetí mocnina	92
9 Magický čtverec	98
10 Desítková soustava	104
II. Nula a záporná čísla	117
0 Je nula číslo?	118
-1 Méně než nic	127
III. Komplexní čísla	133
i Imaginární číslo	134
IV. Racionální čísla	141
$\frac{1}{2}$ Jak rozdělit nedělitelné	142
$\frac{22}{7}$ Aproximace π	147
$\frac{466}{885}$ Hanojská věž	149

V. Iracionální čísla	157
$\sqrt{2}$ První známé iracionální číslo	158
π Měření kruhu	164
φ Zlaté číslo	176
e Přirozené logaritmy	183
$\frac{\log 3}{\log 2}$ Fraktály	194
$\frac{\pi}{\sqrt{18}}$ Uspořádání koulí	202
$\sqrt[12]{2}$ Hudební stupnice	208
$\zeta(3)$ Apéryho konstanta	219
γ Eulerova konstanta	222
VI. Speciální malá čísla	225
11 Teorie strun	226
12 Pentomina	233
17 Mnohouhelníky a vzory	239
23 Narozeninový paradox	250
26 Šifry	256
56 Salámová domněnka	266
168 Konečná geometrie	269
VII. Velká čísla	281
26! Faktoriály	282
43 252 003 274 489 856 000 Rubikova kostka	286
6 670 903 752 021 072 936 960 Sudoku	290
$2^{57\,885\,161} - 1$ Největší známé prvočíslo	293
VIII. Nekonečná čísla	297
$\aleph_0$ Alef nula nejmenší nekonečno:	298
$\mathfrak{c}$ Kardinál kontinua	305
IX. Život, vesmír a ...	309
42 Vůbec to není nudné číslo	310
Doporučená literatura	315
Poděkování za ilustrace	317

PŘEDMLUVA

Čísla mě fascinovala odjakživa. Maminka mě naučila číst a počítat dávno předtím, než jsem šel do školy. Když jsem pak prvního dne ze školy přišel, prý jsem si stěžoval, že jsme „se vůbec nic nenaučili“. Rodiče mě zřejmě připravovali na ten obtížný den v mém životě sliby, že se ve škole dozvím spoustu zajímavých věcí, a já tu propagandu vzal příliš vážně. Ale zakrátko jsem se už učil o planetách a dinosaurech a jak si udělat sádrové zvířátko. A také další věci o číslech.

Čísla mě okouzlují i dnes a stále se o nich dozvídám nové věci. Dnes ale hned zdůrazňuji, že matematika je o mnoha různých věcech, nejen o číslech; kupříkladu studuje tvary, symetrie a pravděpodobnosti – ale čísla jsou v pozadí všeho. A každé číslo je jedinečný originál. Několik z nich vyčnívá z řady a hraje ústřední roli v mnoha různých oblastech matematiky. Nejznámější z nich je π , s nímž se nejdříve setkáváme v souvislosti s kružnicí, ale překvapivě se objevuje i v problémech, které s kružnicí nemají nic společného.

Většina čísel nemůže aspirovat na takovou univerzální důležitost, ale obvykle lze nalézt něco zajímavého i na těch nejnenápadnějších. Ve *Stopařově průvodci po galaxii* je to číslo 42, jež je odpovědí „na základní otázku života, vesmíru a vůbec“. Douglas Adams řekl, že zvolil toto číslo, protože krátký průzkum mezi přáteli ukázal, že to je absolutně nezajímavé číslo. Ve skutečnosti to ale není pravda, jak si ukážeme v poslední kapitole.

Kniha je uspořádána pomocí čísel samých, i když ne vždy v pořadí podle jejich velikosti. Kromě kapitol 1, 2, 3 atd. jsou tu také kapitoly 0, 42 a -1 , kapitola $\frac{22}{7}$, kapitola π , kapitola 43 252 003 274 489 856 000 a kapitola $\sqrt{2}$. Mnoho čísel, která by potenciálně vedla k zajímavým kapitolám, zůstalo pochopitelně jen na číselné ose. Každá kapitola začíná krátkým shrnutím hlavních témat, která budou následovat. Nevadí, když vám tato shrnutí budou připadat záhadná nebo když budou obsahovat tvrzení bez jakéhokoli důkazu: to všechno se vyjasní, až budete číst dál.

Stavba kapitol je jednoduchá: každá kapitola se soustřeďuje na jedno číslo a vysvětluje, čím je zajímavé. Například číslo 2 je zajímavé, protože vede k pojmu sudý/lichý, který se vyskytuje v celé matematice a vědě obecně; číslo 43 252 003 274 489 856 000 je zajímavé, protože odpovídá počtu možných uspořádání Rubikovy kostky.

Jelikož jsem zařadil do knihy i kapitolu 42, musí to být také zajímavé číslo; tedy aspoň trochu.

Na tomto místě musím zmínit recitovanou píseň Arla Guthrieho *Masakr v Alicině restauraci*, která podrobně a opakovaně popisuje likvidaci odpadu. Když píseň trvá deset minut, Guthrie se zarazí a řekne: „Ale to vlastně není to, o čem jsem chtěl s vámi mluvit.“ Nakonec zjistíte, že vlastně o tom chtěl mluvit, ale odpadky tvoří jenom část obsáhlejšího příběhu. Takže tak jako Arlo Guthrie teď říkám: tahle kniha vlastně *není* o číslech.

Čísla jsou jenom úvodem, cestou, která nás vede k úžasné matematice, jež se od nich odvíjí. *Každé číslo je pozoruhodné*. Když k nim budete přistupovat jako ke svébytným osobnostem, stanou se vašimi přáteli. Každé vypráví svůj vlastní příběh, který je často propojen s příběhy řady dalších čísel, ale to, co je důležité, je matematika, jež je spojuje. Čísla jsou postavy v dramatu a to nejdůležitější je právě toto drama. Na druhé straně, bez herců se žádné drama neobejde.

Pro snazší orientaci je kniha rozdělena do částí podle druhu pojednávaných čísel: malá přirozená čísla, zlomky, reálná čísla, komplexní čísla, nekonečno... Až na pár výjimek, kterým se nedalo zabránit, probíráme látku tak, že první kapitoly obsahují základy, na nichž staví pokročilejší kapitoly o zcela nových věcech. Tento požadavek ovlivnil, v jakém pořadí čísla vykládáme, a vyžádal si několik kompromisů. Tím nejzávažnějším je poměrně brzké zavedení komplexních čísel, protože je potřebujeme pro analýzu jistých vlastností běžnějších čísel. Podobně se občas předčasně objeví pokročilejší partie, protože to je jediná příležitost, jak se o nich zmínit. Když budete mít s takovými pasážemi problémy, vynechejte je a pokračujte dál. Později se k nim můžete vrátit.

Tato kniha je partnerem mé stejnojmenné iPadové aplikace *Incredible Numbers*. Ke čtení této knihy aplikaci nepotřebujete a naopak nepotřebujete znát knihu pro sledování aplikace. Dokonce se dá říct, že aplikace a kniha toho mají dost málo společného. Spíše se vzájemně doplňují, protože každé z uvedených médií má jiné možnosti.

Čísla jsou skutečně neuvěřitelná – ne v doslovném slova smyslu, že snad nelze věřit tomu, co se o nich říká, ale naopak, ve smyslu pozitivním. A můžete se z nich těšit bez jakýchkoli výpočtů. Můžete sledovat, jak se postupně vyvíjela v čase, a kochat se z krásy jejich zákonitostí, poučit se, jak se používají, a obdivovat, jak nás dokážou překvapit: „Netušil jsem, jak fascinující je číslo 56!“ Ale fascinující je. Opravdu.

Stejně tak jako ta ostatní. Včetně čísla 42.

ČÍSLA

1, 2, 3, 4, 5, 6, 7, ... Může být něco jednoduššího? A přitom to byla právě čísla spíše než co jiného, co umožnilo lidstvu vyhrabat se z bídy a lopotného života a zamířit ke hvězdám.

Jednotlivá čísla mají různé vlastnosti, což vedlo ke vzniku různých oblastí matematiky. Ale než se těmto vlastnostem budeme postupně věnovat, bude dobré, když v rychlosti zodpovíme tři základní otázky: Jak čísla vznikla? Jak se pojem čísel vyvíjel? A co čísla vlastně jsou?

VZNIK ČÍSEL

Asi před 35 000 lety, v době pozdního paleolitu, udělal nějaký člověk 29 zářezů na lýtkovou kost paviána. Byla nalezena v jeskyni v pohoří Lebombo ve Svazijsku a nazývá se lebombská kost. Předpokládáme, že šlo o *vrubovku*, předmět sloužící k zaznamenání nějakého čísla počtem vrubů: |, ||, |||, atd. Lunární měsíc trvá 29,5 dní, takže to mohl být primitivní lunární kalendář – nebo záznam menstruačních cyklů. Anebo může jít jenom o náhodný počet zářezů, někdo si prostě s tou kostí hrál.



Obr. 1: Pohled na přední a zadní stranu kosti z Ishanga. Přírodovědné muzeum, Brusel.

Jinou vrubovku - vlčí kost s 55 zářezy - našel v roce 1937 Karel Absolon v Československu. Ta je stará asi 30 000 let.

Holenní kost z paviána se zářezy našel v roce 1960 v pozůstatcích po drobné rybářské komunitě, kterou pohřbila erupce sopky, i belgický geolog Jean de Heinzelin de Braucourt. Místo nálezů se dnes jmenuje Ishango a leží na hranici Ugandy s Demokratickou republikou Kongo. Stáří kosti bylo odhadnuto na 20 000 let.

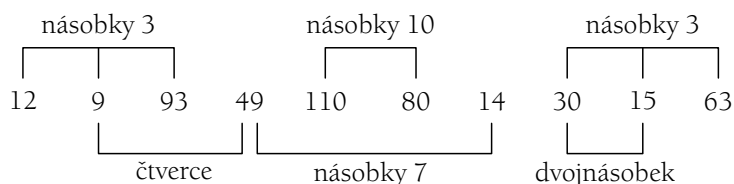
Nejjednodušší vysvětlení je, že jde opět o vrubovku. Někteří antropologové jdou ale dál: vidí v zářezech nějakou aritmetickou strukturu, jako je násobení, dělení či prvočísla; někteří soudí, že jde o šestiměsíční lunární kalendář; jiní jsou přesvědčeni, že zářezy sloužily jen k tomu, aby se kost lépe držela v ruce, a že žádný hlubší význam nemají.

Zářezy jsou rozhodně zvláštní a vyskytují se ve třech skupinách. V prostřední jsou čísla 3, 6, 4, 8, 10, 5, 7. Dvakrát 3 je 6, dvakrát 4 je osm, a dvakrát 5 je 10. Ovšem pořadí poslední dvojice je obrácené a 7 do této interpretace nezapadá vůbec. Nalevo je skupina s čísly 11, 13, 17, 19 - což jsou prvočísla mezi 10 a 20. Skupina napravo obsahuje lichá čísla 11, 21, 19, 9. Součet čísel v levé a pravé skupině je 60.

Problém s objevováním podobných zákonitostí spočívá v tom, že je obtížné nalézt posloupnost malých čísel, která by nějaké takové zákonitosti *nevykazovala*. Tak například v tabulce 1 je uvedena plocha deseti bahamských ostrůvků, což jsou čísla od 11 do 20. Abych čísla uspořádal, seřadil jsem ostrůvky podle abecedy

Jméno	Plocha ve čtverečních mílech
Berry	12
Bimini	9
Crooked Island	93
Little Inagua	49
Mayaguana	110
New Providence	80
Ragged Island	14
Rum Cay	30
Samana Cay	15
San Salvador Island	63

Tabulka 1: Druhá desítka největších ostrůvků Bahamského společenství a jejich velikosti.



Obr. 2: Některé zdánlivé symetrie v rozlohách bahamských ostrovů.

V první řadě má celý seznam rozloh nádhernou symetrii. Na obou koncích jsou tři násobky čísla 3. Uprostřed jsou násobky 10, které oddělují dva násobky 7. A co víc, vlevo jsou dva čtverce, $9 = 3^2$ a $49 = 7^2$, které jsou oba čtverce prvočísel. Dvojici sousedních čísel na druhé straně tvoří čísla 15 a 30, z nichž druhé je dvojnásobkem prvního. V posloupnosti 9-93-49 mají všechna čísla v sobě 9. Všechna po sobě jdoucí čísla jsou alternativně menší a větší, až na čísla 110-80-14. A ještě, všimli jste si, že žádné z čísel není prvočíslo?

Ale pojďme dál. Další problém s kostí z Ishanga spočívá v tom, že je prakticky nemožné nalézt nějaký důkaz, který by podporoval tu nebo onu interpretaci. Nicméně zářezy na kosti jsou jistě zajímavé. Tak jako všechny číselné hádanky. A teď něco méně problematického.

Před deseti tisíci lety používali lidé na Blízkém východě k záznamu čísel hliněné útvary, *tokens*, možná pro účely daní nebo jako důkaz vlastnictví. Nejstarší pocházejí z Tepe Asiab a Ganj-i Dareh Tepe, dvou míst v pohoří Zagros v Íránu. Hliněné tokeny měly různý tvar. Kulička se symbolem + znamenala ovci; sedm kuliček bylo sedm ovcí. Aby kuliček nebylo příliš mnoho, měli hliněný token pro deset ovcí, jenž měl jiný tvar. Podobně existoval hliněný útvar pro deset koz atd. Archeoložka Denise Schmandtová-Besseratová došla k závěru, že hliněné útvary reprezentovaly základní životní potřeby té doby: obilí, zvířata, džbány s olejem.

Kolem roku 4000 př. n. l. se tyto tokeny navlékaly na provázek jako náhrdelník. Jelikož bylo snadné změnit jejich počet tím, že by se tam nějaký přidal nebo odňal, bylo třeba zavést nějaké bezpečnostní opatření: tokeny byly opatřeny hliněným krytem, který pak byl vypálen. Hádku ohledně správného počtu tokenů uvnitř bylo možné rozhodnout rozbitím hliněného pouzdra.

Aby se pouzdra nemusela rozbíjet, začali úředníci staré Mezopotámie přibližně od roku 3500 př. n. l. zaznamenávat počet žetonů obsažených uvnitř na hliněné pouzdro.



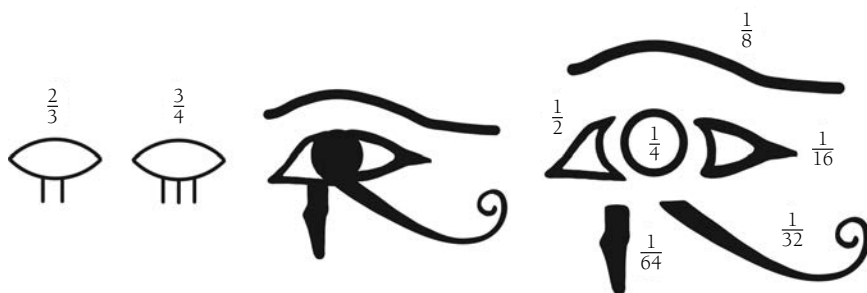
Obr. 3: Hliněné pouzdro a tokeny, urucké období, naleziště Súsy.

Pak si jeden bystrý byrokrat uvědomil, že se symboly na pouzdru už jsou tokeny uvnitř zbytečné. Důsledkem byl vznik symbolů reprezentujících počet, což vedlo ke vzniku všech početních systémů a možná i ke vzniku písma jako takového.

Tato kniha ovšem není primárně historická, takže se zmíníme o pozdějších systémech notace v kontextu konkrétních čísel. Například o starodávne a moderní desetinné soustavě pojednáme v kapitole 10. Nicméně, jak jednou poznamenal slavný matematik Carl Friedrich Gauss, důležité nejsou symboly, ale pojmy. Následující kapitoly budou srozumitelnější, když je pojednáme v kontextu měnící se koncepce čísel. Takže teď rychle probereme hlavní číselné soustavy a s tím spojenou terminologii.

STÁLE SE ROZRŮSTAJÍCÍ ČÍSELNÝ SYSTÉM

Máme sklon považovat čísla za cosi daného a neměnného, za cosi, co je součástí přírody. Ve skutečnosti jsou to ale lidské vynálezy – a navíc velice užitečné, protože reprezentují důležité aspekty světa kolem nás. Třeba kolik vlastního ovčí nebo jak je starý vesmír. Příroda nás stále znova překvapuje tím, že nám klade nové otázky; odpovědi na ně mohou občas vyžadovat nové matematické koncepty. Někdy zase potenciálně užitečné struktury vznikají z vnitřní potřeby matematiky. Matematici proto musí čas od času rozšířit početní systém vytvořením nového typu čísel.



Obr. 4: Vlevo: Egyptské hieroglyfy pro $\frac{2}{3}$ a $\frac{3}{4}$. Uprostřed: Vadžetino oko. Vpravo: Zlomky, které jsou z obrázku oka odvozeny.

Už jsme viděli, jak čísla vznikla z potřeby počítat věci. Ve starém Řecku vypadal seznam čísel následovně: 2, 3, 4, ... Číslo 1 mělo výhradní postavení, nebylo „opravdovým“ číslem. Později začalo být zřejmé, že tato konvence je hloupá, a 1 se stala plnoprávným číslem.

Dalším velkým krokem rozšiřujícím početní systém bylo zavedení zlomků. Jsou užitečné, když potřebujete nějakou komoditu rozdělit mezi několik lidí. Když mají tři lidé dostat stejný díl ze dvou bušlů zrna, každý dostane $\frac{2}{3}$ bušlu.

Staří Egypťané zobrazovali zlomky třemi různými způsoby. Pro zlomky $\frac{2}{3}$ a $\frac{3}{4}$ měli zvláštní hieroglyfy. Pro zlomky tvaru 1 děleno prvními šesti mocninami 2 užívali různé části Horova nebo Vadžetina oka. A konečně měli zvláštní hieroglyfy pro zlomky typu „jedna děleno čímkoli“: $1/2$, $1/3$, $1/4$, $1/5$ atd. Všechny ostatní zlomky vyjadřovali jako součet těchto zlomků s čitatelem 1. Například

$$\frac{2}{3} = \frac{1}{2} + \frac{1}{6}.$$

Nevíme, proč nepsali $\frac{2}{3} = \frac{1}{3} + \frac{1}{3}$, ale nepsali to tak.

Symbol pro nulu se objevil mnohem později, nejspíš pro něj nebylo mnoho uplatnění. Když nemáte žádné ovce, nepotřebujete je ani počítat, ani si psát jejich seznam. Nula byla zavedena jako symbol a nepovažovala se za číslo. Ale když čínští a indiští matematici zavedli záporná čísla (*kapi-tola* -1), začala být 0 považována za číslo. Kupříkladu $1 + (-1) = 0$ a součet dvou čísel musí samozřejmě být zase číslo.

Čísla

0, 1, 2, 3, 4, 5, 6, 7, ...

nazývají matematici *přirozená čísla*, a když se k nim připojí záporná čísla, dostáváme *čísla celá*

$$\dots, -3, -2, -1, 0, 1, 2, 3, \dots$$

Zlomky, nula a záporné zlomky tvoří *racionální čísla*.

Číslo je *kladné*, když je větší než nula, a *záporné*, když je menší než nula. Takže každé číslo (celé nebo racionální) leží v právě jedné kategorii: čísla kladná, záporná nebo nula. Když nějaké objekty počítáme, používáme k tomu kladná celá čísla

$$1, 2, 3, 4, 5, 6, 7, \dots$$

To vede k poněkud neobratné terminologii: přirozená čísla nebo celá čísla

$$0, 1, 2, 3, 4, 5, 6, 7, \dots$$

jsou často nazývána *nezáporná celá čísla*. Pardon.

Rozšíření celých čísel o zlomky bylo na dlouhou dobu poslední. Ale už staří Řekové dokázali, že čtverec racionálního čísla se nikdy nemůže rovnat 2. Později to bylo vyjádřeno tvrzením, že „číslo $\sqrt{2}$ je iracionální“, tedy že není racionální. Řekové to vyjadřovali poněkud komplikovaněji, ale věděli, že $\sqrt{2}$ musí existovat: Podle Pythagorovy věty je to délka úhlopříčky ve čtverci, jehož strana je 1. Takže potřebujeme víc čísel: racionální to sama nezládnou. Řekové objevili složitou geometrickou metodu, jak pracovat s iracionálními čísly, ale nebyla zcela uspokojivá.

Dalším krokem, který umožnil moderní pojetí čísel, bylo zavedení desetinné čárky a desetinného značení. Umožnilo to vyjádřit iracionální čísla s velkou přesností. Například

$$\sqrt{2} \approx 1,414\,213\,5623$$

s přesností na 10 desetinných míst (symbol $\approx$ znamená „je přibližně rovno“). Tento výraz pro odmocninu není přesný: čtverec pravé strany je

$$1,999\,999\,999\,793\,255\,981\,29.$$

Lepší aproximace, správná na 20 desetinných míst, je

$$\sqrt{2} \approx 1,414\,213\,562\,373\,095\,048\,80,$$

ale ani to není přesné. Nicméně, bude-li posloupnost desetinných čísel nekonečně dlouhá, lze bez porušení logiky tvrdit, že takové vyjádření už přesné je.

Samozřejmě že takové rozvoje nelze vypsat celé, ale lze zavést formalismus, v němž mají smysl.

Nekonečně dlouhá desetinná čísla (což zahrnuje i čísla, která mají konečný počet míst – ta můžeme doplnit nekonečným počtem nul) se nazývají *reálná čísla*, částečně i proto, že přímo odpovídají měřením v reálném světě, jakými jsou stanovení délky či váhy. Čím přesnější měření je, tím více desetinných míst potřebujeme; kdybychom měřili absolutně přesně, potřebovali bychom jich nekonečně mnoho. Je trochu ironie, že „reálné“ je definováno nekonečným výrazem, který ani nemůžeme napsat. Záporná reálná čísla jsou také možná.

Až do 18. století se žádné jiné matematické pojmy za skutečná čísla nepovažovaly, nicméně už v 15. století několik matematiků napadlo, jestli by neměl existovat nový typ čísla, a sice odmocnina z -1 . Bylo by to číslo, které násobeno samo sebou by dalo -1 . Na první pohled to vypadá nesmyslně, protože druhá odmocnina z libovolného reálného čísla je buď kladná, nebo rovna nule. Ale ukázalo se, že doplnit čísla o odmocninu z -1 byl dobrý nápad, a Leonhard Euler pro ni zavedl symbol „ i “ – podle slova „imaginární“. Toto pojmenování mělo odlišit $\sqrt{-1}$ od starých dobrých reálných čísel. Bohužel to také vedlo ke zbytečnému mysticismu – Gottfried Leibniz se o tomto čísle jednou zmínil jako o čísle, které „kombinuje bytí a nebytí“ – což zatemnilo důležitý fakt, že reálná i imaginární čísla jsou, pokud jde o jejich logické postavení, zcela rovnocenná. Jsou to lidmi vytvořené pojmy, které modelují realitu, i když samy o sobě „fyzicky reálné“ nejsou.

Existence čísla i má za následek, že je třeba zavést mnoho dalších čísel, abychom mohli provádět aritmetické operace – výsledná čísla se zapisují třeba $2 + 3i$. Říkáme jim komplexní čísla a posledních pár století bychom se bez nich neobešli. Tahle překvapující skutečnost bude pro většinu lidí novinkou, protože ve školní matematice se s komplexními čísly často nesetkali. Ne proto, že by komplexní čísla nebyla dost důležitá, ale protože jde o abstraktní pojem a jejich použití v praxi je příliš složité.

Matematici pro různé typy čísel rádi používají zvláštní symboly. My je dál používat nebudeme, ale asi byste je měli aspoň jednou vidět:

$\mathbb{N}$ = množina všech přirozených čísel 0, 1, 2, 3, ...

$\mathbb{Z}$ = množina všech celých čísel ..., -3, -2, -1, 0, 1, 2, 3, ...

$\mathbb{Q}$ = množina všech racionálních čísel

$\mathbb{R}$ = množina všech reálných čísel

$\mathbb{C}$ = množina všech komplexních čísel

Jednotlivé množiny do sebe zapadají jako ruské matryošky:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

kde symbol $\subset$ znamená „je obsaženo v“. Všimněme si, že například celé číslo 3 je také zlomek $\frac{3}{1}$. My takhle trojku většinou nepíšeme, ale oba zápisy představují stejné číslo. Podobně je každé racionální číslo také reálné a každé reálné číslo je také komplexní. Staré číselné systémy nejsou novými nahrazeny, ale jsou v nich obsaženy.

Ani komplexními čísly nekončí rozšiřování číselného systému, které matematici po staletí podnikají. Existují např. kvaterniony $\mathbb{H}$ a oktoniony $\mathbb{O}$ (kapitola 4). Ale ty je lépe zavádět algebraicky než v rámci aritmetiky.* Takže skončíme výkladem o jednom rozporuplném čísle – nekonečnu. Filozoficky vzato se nekonečno liší od běžných čísel a nepatří do žádného ze standardních číselných množin počínaje čísly přirozenými a komplexními čísly konče, nicméně se vždy vznášelo na obzoru, podobné číslu a přitom mezi čísla nepatřící. Tak tomu bylo, dokud se Georg Cantor nevrátil na začátek, k počítání objektů, a neukázal, že nejenom nekonečno je číslo ve smyslu počítání věcí, ale že existují nekonečna *různých velikostí*. Mezi nimi jsou např. $\aleph_0$, udávající počet přirozených čísel, a $\mathfrak{c}$, počet reálných čísel, který je větší než $\aleph_0$. Jak moc je větší, je sporné: záleží to na systému axiomů, na nichž matematiku budujeme.

Ale zatím to nechme tak, dokud nezískáme dost intuice studiem obyčejných čísel. Což nás přivádí k třetí otázce.

CO JE TO ČÍSLO?

Vypadá to jako jednoduchá otázka, ale odpověď na ni jednoduchá není.

Všichni víme, jak s čísly zacházet. Všichni víme, jak vypadá sedm ovcí nebo sedm krav či sedm židlí. Všichni umíme počítat do sedmi. Ale co to je *sedm*?

Není to ten symbol „7“. To je jen určitá volba a v jiných kulturách je i jiná: Arabové užívají **V**, Číňané 七 nebo formálněji 柒.

* *Aritmetika* se zabývá popisem základních operací s čísly. *Algebra* se zabývá abstrakcí pojmů a objektů (jako jsou čísla, polynomy, matice apod.) a pravidly manipulace s těmito symboly. Pozn. překl.

Není to ani slovo „sedm“ – ve francouzštině to je *sept*, v angličtině *seven* a v němčině *sieben*.

Zhruba v polovině 19. století si několik matematických logiků uvědomilo, že ačkoli všichni spokojeně po tisíce let čísla používáme, nikdo vlastně pořádně neví, co to je. Proto přišli s otázkou, která neměla být nikdy vyslovena: *co je číslo?*

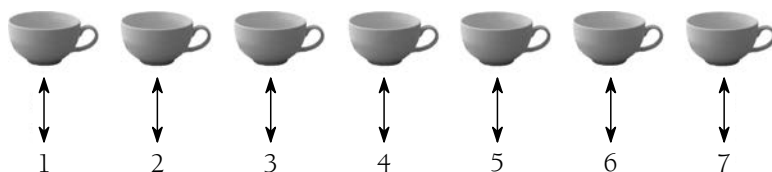
Je to záluďnější, než se zdá. Číslo není nic, na co by se dalo ve světě kolem nás prostě ukázat. Je to abstrakce, lidský výmysl – je odvozen z reality, ale není skutečně *reálný*.

Možná to zní překvapivě, ale čísla v tomto smyslu nejsou ojedinělý koncept. Podobně je na tom všeobecně známý pojem *peníze*. Všichni víme, jak máme za něco zaplatit a kolik dostaneme zpátky – a namlouváme si, že jde o výměnu bankovek a mincí. Ztotožňujeme peníze s mincemi a bankovkami v naší peněžence či kapse. Ale tak jednoduché to není. Když používáme bankovní kartu, nedojde k žádné výměně bankovek a mincí. Místo toho je odeslán signál do karetní společnosti a nakonec do naší banky a změní se čísla na několika účtech – našem, našeho dodavatele a karetní společnosti. Na britské pětilibrové bankovce bývalo napsáno: „Na požádání slibuji zaplatit držiteli této bankovky pět liber.“ Taková bankovka tedy nebyla žádné peníze, jen slib peníze zaplatit. Jednou za čas ji člověk mohl vzít do banky a vyměnit ji za zlato, které bylo považováno za *ty pravé* peníze. Dnes vám jediné vymění starou bankovku za novou. Ale ani zlato nebylo pravými penězi – bylo to jen jednou z fyzických manifestací peněz, jak plyne z toho, že jeho cena není stálá.

Jsou tedy peníze nějakými čísly? Ano, ale pouze v jistém právním smyslu. Když si napíšete na kus papíru 1 000 000 \$, nestanete se milionářem. To, co dělá peníze penězi, je souhrn lidských konvencí o tom, jak reprezentujeme čísla na bankovkách a jak je směňujeme za zboží nebo jiná čísla. Důležité je, co se s nimi dá dělat, ne jejich fyzická podstata. Peníze jsou abstrakcí.

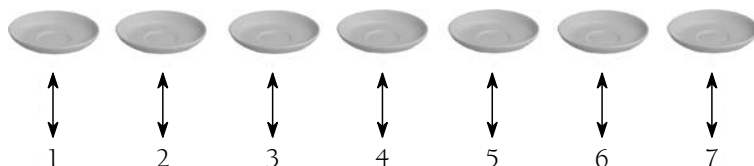
A čísla také. To ale žádné velké objasnění nepředstavuje, protože celá matematika je abstrakcí. Takže několik matematiků si dál lámalo hlavu, co to je za abstrakci, která definuje „číslo“. V roce 1884 napsal německý matematik Gottlob Frege knihu *Die Grundlagen der Arithmetik* (Základy aritmetiky), v níž stanovil základní principy, na nichž spočívá používání čísel. O deset let později zašel ještě dál a pokusil se tyto principy odvodit z ještě fundamentálnějších zákonů logiky. Jeho *Die Grundsetze der Arithmetik* (Základní zákony aritmetiky) vyšly ve dvou dílech, první v roce 1893 a druhý v roce 1903.

Frege se soustředil na počítání objektů a zaměřil se nikoli na *čísla*, která používáme, ale na *objekty*, které počítáme. Když položíme na stůl sedm hrnečků a počítáme je „1, 2, 3, 4, 5, 6, 7“, vypadá to, že důležitými objekty jsou tato čísla. S tím Frege nesouhlasil: jde o hrnky. Počítání umožnila skupinka hrnků, které jsme chtěli spočítat. S jinou skupinou bychom mohli dospět k jinému číslu. Frege nazval tyto skupiny *třídami*. Když počítáme, kolik hrnků tato konkrétní třída obsahuje, vytváříme *korespondenci* mezi třídami hrnků a symboly čísel 1, 2, 3, 4, 5, 6, 7.



Obr. 5: Korespondence mezi počtem hrnků a číslicemi.

Podobně, máme-li třídu talířů, můžeme takovou korespondenci také vytvořit:



Obr. 6: Korespondence mezi počtem talířů a číslicemi.

Když to učiníme, můžeme dojít k závěru, že třída talířů obsahuje stejný počet talířů, jako třída hrnků obsahuje hrnků. Víme, i kolik to je: sedm.

Může nám to připadat jako samozřejmé, až banální. Ale Frege si uvědomil, že ve skutečnosti jde o velice hluboké tvrzení. Můžeme totiž dokázat, že třída talířů i třída hrnků mají stejný počet objektů, aniž bychom používali symboly 1, 2, 3, 4, 5, 6, 7 a aniž bychom věděli, kolik těch hrnků nebo talířů je – stačí vytvořit korespondenci mezi třídou hrnků a třídou talířů.

Technicky je tento typ korespondence nazýván *prosté zobrazení*, každý hrnek odpovídá přesně jednomu talíři. Počítání by nefungovalo, kdybychom nějaký hrnek vynechali nebo ho započítali víckrát. Ale nazývejme to prostě korespondencí a tento technický detail mějme na mysli.

Mimochodem, pokud jste se někdy podívovali, proč děti ve škole tráví čas tím, že „přiřazují“ krávy v jedné množině kuřatům ve druhé množině nebo něco podobného a spojují zvířata na obrázcích čarami, může za to Frege. Někteří teoretici vzdělávání doufali (a možná pořád doufají), že tento postup zlepši dětskou intuici při chápání čísel. Mně se spíš zdá, že jde o přeceňování logiky, ignorování psychologie a nepochopení toho, co „fundamentální“ doopravdy je – ale nechci tady znovu rozpoutat válku mezi matematiky.*

Frege došel k závěru, že podstatou významu slova „číslo“ je právě korespondence mezi třídami. Když počítáme, kolik objektů je v nějaké třídě, srovnáváme tuto třídu se standardní třídou, jejíž prvky jsou označeny konvenčními symboly 1, 2, 3, 4, 5, 6, 7, ... (nebo jinými, v závislosti na kultuře, k níž se hlásíme). Frege si ale nemyslel, že by pojem čísla měl být závislý na naší kultuře, takže přišel s metodou, jak se symbolů a libovolně v nich zbavit úplně. Přesněji řečeno, vynalezl univerzální „supersymbol“, který by byl stejný v každé kultuře. Ale není to něco, co můžete napsat na papír: je to čistě konceptuální záležitost.

Frege v první řadě zdůraznil, že objekty nějaké třídy mohou samy tvořit třídu. Nemusí, ale není důvod, aby ji tvořit nemohly. Bedýnka s plechovkami vařených fazolí může sloužit za příklad z běžného života: objekty bedýnky jsou plechovky a objekty plechovek jsou fazole. Takže klidně můžeme mít třídy, které jsou objekty jiných tříd.

Číslo „sedm“ je prostřednictvím korespondence přidruženo k libovolné třídě, která odpovídá naší třídě hrnků nebo talířů nebo třídě s čísly 1, 2, 3, 4, 5, 6, 7. Když zvolíme jednu z těchto tříd a prohlásíme, že *právě ta* je číslem, je to náhodné rozhodnutí, které postrádá eleganci a není uspokojivé. Takže proč to neudělat pořádně a nepoužít ty třídy všechny? Pak lze číslo „sedm“ definovat jako *třidu všech tříd*, které jsou v korespondenci s libovolnou z dříve zmíněných tříd (čili jsou v korespondenci všechny navzájem). Když číslo sedm definujeme takto, můžeme zjistit, zda určitá třída má sedm objektů,



Obr. 7: Korespondence mezi počtem hrnků a talířů nevyžaduje žádné číslovky.

* *Math war* je spor mezi tradičními a reformními matematiky ohledně filozofie a náplně výuky matematiky na školách v USA, viz např. https://en.wikipedia.org/wiki/Math_wars. Pozn. překl.

když si ověříme, že je ve třídě těchto tříd. Pro pohodlí označíme tuto třídu tříd slovem „sedm“, ale třída s tímto jménem má smysl, i kdybychom to neudělali. Tímto způsobem Frege odlišil nějaké číslo (počet objektů) od libovolně vybraného pojmenování (či symbolu) pro toto číslo.

Teď mohl Frege definovat, co je číslo: je to třída všech tříd, které jsou v korespondenci s danou třídou (a tedy mezi sebou navzájem). Tento typ třídy je tím, co jsme nazvali „supersymbolem“. Pokud se nad tím zamyslíme, je to brilantní řešení. Výsledkem je, že místo abychom vymysleli jméno pro určitý počet objektů, spojíme všechna možná jména dohromady v jeden objekt a ten pak používáme.

Fungovalo to? O tom si povíme později, v kapitole $\aleph_0$.

I. MALÁ ČÍSLA

Nejznámější čísla ze všech jsou přirozená čísla od 1 do 10.

Každé z nich má své ojedinělé
vlastnosti, díky kterým je jedinečné.

Když dokážete ocenit tyto jedinečné vlastnosti,
začnou vám tato čísla sama o sobě připadat
důvěrně známá, přátelská a zajímavá.

Brzy z vás bude matematik.

1

NEDĚLITELNÁ JEDNIČKA

Nejmenší kladné celé číslo je 1. Je to nedělitelná jednotka aritmetiky: jediné kladné celé číslo, které nemůžeme získat sečtením dvou menších kladných čísel.

ZÁKLADY KONCEPCE ČÍSEL

Číslo 1 stojí na počátku všeho počítání. Z každého čísla uděláme to následující přičtením 1:

$$\begin{aligned}2 &= 1 + 1, \\3 &= (1 + 1) + 1, \\4 &= ((1 + 1) + 1) + 1, \\&\vdots\end{aligned}$$

Závorky nám ukazují, které sčítání máme udělat nejdříve. Obvykle je nepíšeme, protože se ukazuje, že při sčítání na pořadí nezáleží, ale je dobré naučit se opatrnosti.

Z těchto definic a základních zákonů algebry, které při formálně správném logickém budování teorie musí být explicitně vysloveny, můžeme teď dokázat i slavnou větu „ $2 + 2 = 4$ “. Důkaz se vejde na jednu řádku:

$$2 + 2 = (1 + 1) + (1 + 1) = ((1 + 1) + 1) + 1 = 4.$$

Když se ve 20. století někteří matematici pokoušeli dát matematice pevné logické základy, používali stejný postup, ale vycházeli z 0 (*kapitola 0*).

Číslo 1 je ztělesněním důležitého matematického pojmu: *jedinečnosti*. Matematický objekt s určitými vlastnostmi je jedinečný, pokud tuto vlastnost nemá žádný jiný objekt. Kupříkladu 2 je jedinečné sudé prvočíslo. Jedinečnost je důležitá, protože s její pomocí můžeme dokázat, že nějaký mírně záhadný objekt je ve skutečnosti týž objekt, který už známe. Když kupříkladu dokážeme, že nějaké neznámé kladné číslo n je jednak sudé, jednak je to prvočíslo, pak n musí být 2. Trochu složitější příklad je následující:

dvanáctistěn je jediné pravidelné těleso s pětiúhelníkovými stěnami (*kapitola 5*). Takže když se někde v nějakém výpočtu objeví pravidelné těleso s pětiúhelníkovými stěnami, víme okamžitě, aniž bychom museli dále bádát, že jde o dvanáctistěn. Všechno další, co o dvanáctistěnu víme, dostaneme přídatkem zadarmo.

NÁSOBENÍ JEDNIČKOU

Ještě nikdo si nikdy nestěžoval, že se musí učit násobilku jedné. „Jednou jedna je jedna, jednou dvě jsou dvě, jednou tři jsou tři...“ Dělíme-li nebo násobíme-li libovolné číslo jedničkou, nezmění se.

$$n \times 1 = n, \quad n : 1 = n.$$

A 1 je i jediné číslo, pro něž to platí.

Důsledkem toho je, že 1 je také rovna své druhé, třetí a všem vyšším mocninám.

$$\begin{aligned} 1^2 &= 1 \times 1 = 1, \\ 1^3 &= 1 \times 1 \times 1 = 1, \\ 1^4 &= 1 \times 1 \times 1 \times 1 = 1, \\ &\vdots \end{aligned}$$

Jediné další číslo s touto vlastností je 0.

Z těchto důvodů bývá jednička zpravidla vynechávána ve vzorcích. Místo abychom psali $1x^2 + 3x + 4$, píšeme jednodušeji $x^2 + 3x + 4$. Jediné další číslo, s nímž zacházíme podobně, je 0, kdy je změna ještě drastičtější: místo $0x^2 + 3x + 4$ píšeme jen $3x + 4$.

JE 1 PRVOČÍSLO?

Bývala jím, ale už není. Číslo 1 se nezměnilo, změnila se definice prvočísla.

Některá čísla můžeme obdržet násobením jiných dvou čísel, kupříkladu $6 = 2 \times 3$ nebo $25 = 5 \times 5$. Takovým číslům říkáme *složená*. Jiná čísla takto získat nelze a těm říkáme *prvočísla*.

Podle této definice je 1 prvočíslo a ještě před 150 lety tomu tak bylo. Pak se ale ukázalo, že je příhodnější považovat 1 za výjimku. Dnes říkáme, že 1 není ani složené číslo, ani prvočíslo, je to *jednotka*. Hned si vysvětlíme proč, ale nejdřív pár dalších faktů.

I. MALÁ ČÍSLA

Posloupnost prvočísel začíná následovně

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

a vypadá značně chaoticky, až na dvě jednoduché zákonitosti. Všechna prvočísla kromě 2 jsou lichá, protože každé další sudé číslo je dělitelné 2. Na pětku může končit jenom 5 a žádné číslo nesmí končit 0, protože by bylo dělitelné 5.

Každé celé číslo větší než 1 může být vyjádřeno jako součin prvočísel. Tomuto procesu říkáme *faktorizace* či *prvočíselný rozklad* a prvočislům, která se v tomto rozkladu vyskytují, říkáme prvočíselné faktory. A co víc, takový rozklad je možný pouze jediným způsobem, až na možná různá pořadí faktorů v rozkladu. Například

$$60 = 2 \times 2 \times 3 \times 5 = 2 \times 3 \times 2 \times 5 = 5 \times 3 \times 2 \times 2 = \dots,$$

ale jediná možnost, jak získat násobením 60, je měnit pořadí v prvním z uvedených výrazů. Kupříkladu neexistuje žádný rozklad tvaru $60 = 7 \times \text{něco}$.

Této vlastnosti říkáme „jednoznačnost prvočíselné faktorizace“. Možná to vypadá samozřejmě, ale pokud jste nestudovali matematiku, asi nebudete vědět, jak to dokázat. Eukleides důkaz uvedl ve svých *Základech* a určitě si uvědomoval, že toto tvrzení není ani samozřejmé, ani snadno dokazatelné, protože si s ním dal velkou práci. Pro některé obecnější číselné systémy dokonce ani neplatí, ale v běžné aritmetice platí a je to velice efektivní nástroj matematické výzbroje.

Prvočíselný rozklad čísel od 2 do 31 vypadá následovně:

2 (prvočíslo)	3 (prvočíslo)	$4 = 2^2$	5 (prvočíslo)	$6 = 2 \times 3$
7 (prvočíslo)	$8 = 2^3$	$9 = 3^2$	$10 = 2 \times 5$	11 (prvočíslo)
$12 = 2^2 \times 3$	13 (prvočíslo)	$14 = 2 \times 7$	$15 = 3 \times 5$	$16 = 2^4$
17 (prvočíslo)	$18 = 2 \times 3^2$	19 (prvočíslo)	$20 = 2^2 \times 5$	$21 = 3 \times 7$
$22 = 2 \times 11$	23 (prvočíslo)	$24 = 2^3 \times 3$	$25 = 5^2$	$26 = 2 \times 13$
$27 = 3^3$	$28 = 2^2 \times 7$	29 (prvočíslo)	$30 = 2 \times 3 \times 5$	31 (prvočíslo)

Hlavní důvod, proč se 1 stala výjimkou, je následující: kdyby byla prvočíslem, rozklad by nebyl jednoznačný. Kupříkladu

$$6 = 2 \times 3 = 1 \times 2 \times 3 = 1 \times 1 \times 2 \times 3 = \dots$$

Zjevným nedostatkem tohoto rozhodnutí je, že 1 nemá prvočíselný rozklad.

1. NEDEĚLITELNÁ JEDNIČKA

Přesto 1 součinem prvočísel je, i když poněkud zvláštním způsobem: 1 je součinem „prázdné množiny“ prvočísel. Jinými slovy, když spolu *žádná prvočísla* nenásobíte, dostanete 1. Asi to zní šíleně, ale pro tuto konvenci existují dobré důvody.

2

SUDÁ A LICHÁ

Sudá čísla jsou dělitelná 2, lichá nikoli. Takže 2 je jediné sudé prvočíslo. Je součtem dvou čtverců: $2 = 1^2 + 1^2$. Jiná prvočísla s touto vlastností jsou právě ta, která dělena 4 dávají zbytek 1. Čísla, která jsou součtem dvou čtverců, mohou být charakterizována svými prvočíselnými faktory.

Binární aritmetika, kterou používají počítače, není založena na mocninách 10, ale na mocninách 2. Kvadratické rovnice obsahující čtverec neznámého čísla mohou být řešeny pomocí druhých odmocnin.

Rozdíl mezi sudým a lichým se vztahuje dokonce i na permutace – způsob, jakým měníme pořadí objektů. Polovina permutací je sudá, druhá polovina lichá. Ukážeme si hezkou aplikaci: jednoduchý důkaz, že jedna známá hádanka nemá řešení.

PARITA (SUDÁ/LICHÁ)

Rozdíl mezi sudými a lichými čísly patří k nejdůležitějším pojmům v celé matematice.

Začněme s přirozenými čísly 0, 1, 2, 3, ... Mezi nimi jsou následující sudá čísla

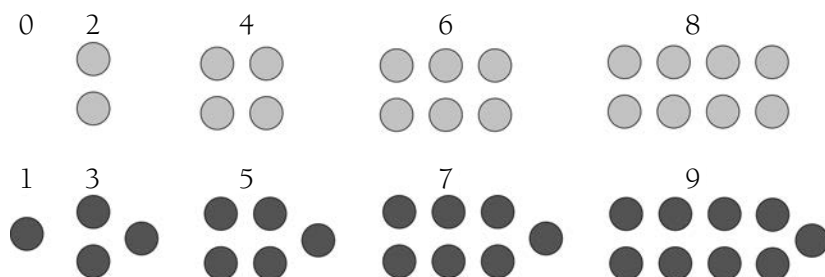
$$0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, \dots,$$

kdežto lichá čísla jsou

$$1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, \dots$$

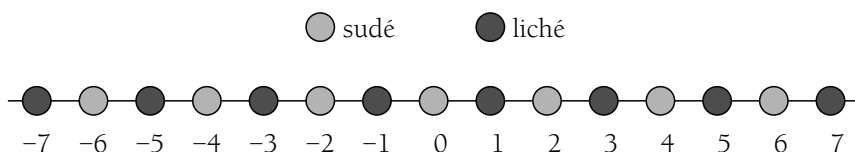
Obecně platí, že každé sudé přirozené číslo je násobkem 2 a každé přirozené číslo, které není násobkem 2, je liché. V rozporu s tím, co si myslí většina učitelů, je 0 číslo sudé, protože je to násobek 2, neboť $0 \times 2 = 0$.

Lichá čísla dělena 2 dávají zbytek 1. (Zbytek je nenulový a menší než 2, takže musí být 1.) Algebraicky mají sudá přirozená čísla tvar $2n$, kde n je celé číslo, a lichá čísla mají tvar $2n + 1$. (Když položíme $n = 0$, vidíme opět, že 0 je sudá.) Chceme-li rozšířit pojem sudé/liché číslo i na čísla záporná, necháme



Obr. 8: Sudá a lichá čísla.

n probíhat i záporná celá čísla. Takže $-2, -4, -6$ atd. jsou čísla sudá a $-1, -3, -5$ atd. jsou čísla lichá. Na číselné ose se sudá a lichá čísla střídají.



Obr. 9: Sudá a lichá čísla se na číselné ose střídají.

Aritmetické operace se sudými a lichými čísly se řídí snadno zapamatovatelnými pravidly:

sudé + sudé = sudé	sudé $\times$ sudé = sudé
liché + liché = sudé	liché $\times$ liché = liché
sudé + liché = liché	sudé $\times$ liché = sudé
liché + sudé = liché	liché $\times$ sudé = sudé

nezávisle na tom, jak velká čísla jsou. Takže když někdo bude tvrdit, že $13 \times 17 = 222$, víte, že to není pravda, aniž byste museli něco počítat. Liché $\times$ liché = liché, kdežto 222 je sudé.

NEJMENŠÍ A JEDINÉ SUDÉ PRVOČÍSLO

Seznam prvočísel začíná číslem 2, takže 2 je nejmenší prvočíslo. Je to také jediné sudé prvočíslo, protože podle definice jsou sudá čísla dělitelná 2. Když je sudé číslo 4 nebo větší, je násobkem dvou menších čísel, a tudíž je to číslo složené. Jakkoli jsou tyto vlastnosti 2 očividné, propůjčují číslu 2 jedinečné postavení.

I. MALÁ ČÍSLA

TEORÉM DVOU ČTVERCŮ

Na Boží hod vánoční roku 1640 napsal vynikající matematik Pierre de Fermat mnichu Mersennovi dopis, v němž mu položil záladnou otázku. Která čísla mohou být napsána jako součet dvou čtverců?

Čtverec (čili dvojmoc) čísla je číslo, které dostaneme, když ho vynásobíme se sebou samým. Takže čtverec 1 je $1 \times 1 = 1$, čtverec 2 je $2 \times 2 = 4$, čtverec 3 je $3 \times 3 = 9$ atd. Symbol pro čtverec čísla n je n^2 . Takže

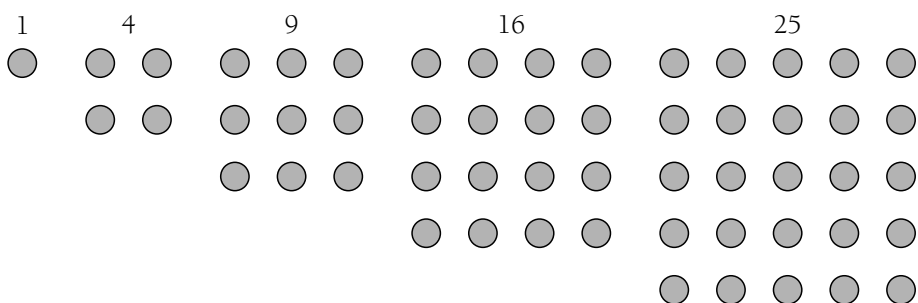
$$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9 \text{ atd.}$$

Čtverce čísel od 0 do 10 jsou:

$$0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100.$$

Číslo 4 je tudíž první „opravdový“ čtverec po méně zajímavých čtvercích čísel 0 a 1.

Výraz „čtverec“ je používán, protože tato čísla vzniknou, když uspořádáme „terčičky“ do podoby čtverce:



Obr. 10: Čtverce čísel 1 až 5.

Sečteme-li dva čtverce, můžeme dostat také původní čtverec: to když tím druhým čtvercem je 0. V ostatních případech dostaneme nová čísla, např.:

$$\begin{array}{lll} 1 + 1 = 2, & 4 + 1 = 5, & 4 + 4 = 8, \\ 9 + 1 = 10, & 9 + 4 = 13, & 16 + 1 = 17. \end{array}$$

Níže je tabulka všech čísel od 0 do 100, která obdržíme jako součet dvou čtverců.

	0	1	4	9	16	25	36	49	64	81	100
0	0	1	4	9	16	25	36	49	64	81	100
1	1	2	5	10	17	26	37	50	65	82	
4	4	5	8	13	20	29	40	53	68	85	
9	9	10	13	18	25	34	45	58	73	90	
16	16	17	20	25	32	41	52	65	80	97	
25	25	26	29	34	41	50	61	74	89		
36	36	37	40	45	52	61	72	83			
49	49	50	53	58	65	74	98				
64	64	65	68	73	80	89					
81	81	82	85	90	97						
100	100										

Tabulka 2: Čísla uvnitř tabulky získáte sečtením tučně vytištěného čísla nahoře v daném sloupci s tučně vytištěným číslem v příslušném řádku nalevo. Například $25 + 4 = 29$. Čísla větší než 100 jsou vynechána.

Na první pohled tu není vidět žádná zákonitost, ale zákonitost tam je a Fermat si jí povšiml. Vtip spočívá v tom, vypsát *prvočíselné faktory* čísel v této tabulce. Vynecháme-li 0 a 1, které jsou výjimkami, dostaneme:

<u>2 = 2</u>	<u>4 = 2²</u>	<u>5 = 5</u>	<u>8 = 2³</u>
9 = 3 ²	10 = 2 × 5	<u>13 = 13</u>	16 = 2 ⁴
<u>17 = 17</u>	18 = 2 × 3 ²	20 = 2 ² × 5	25 = 5 ²
26 = 2 × 13	<u>29 = 29</u>	34 = 2 × 17	36 = 2 ² × 3 ²
<u>37 = 37</u>	40 = 2 ³ × 5	<u>41 = 41</u>	45 = 3 ² × 5
49 = 7 ²	50 = 2 × 5 ²	<u>53 = 53</u>	58 = 2 × 29
<u>61 = 61</u>	64 = 2 ⁶	65 = 5 × 13	68 = 2 ² × 17
72 = 2 ³ × 3 ²	<u>73 = 73</u>	74 = 2 × 37	80 = 2 ⁴ × 5
81 = 3 ⁴	82 = 2 × 41	85 = 5 × 17	<u>89 = 89</u>
90 = 2 × 3 ² × 5	<u>97 = 97</u>	100 = 2 ² × 5 ²	

Podtržena jsou ta čísla, která jsou prvočísla, protože jsou klíčem k naší úloze.

Některá prvočísla tam chybějí, konkrétně: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79 a 83. Dokážete – tak jako Fermat – rozpoznat jejich společnou vlastnost?

Všechna tato prvočísla jsou o 1 menší než násobek 4. Například $23 = 24 - 1 = 6 \times 4 - 1$. V seznamu nahoře se vyskytuje 2, ale to je opět svým způsobem zvláštní případ. Všechna lichá čísla v tabulce jsou o 1 větší

I. MALÁ ČÍSLA

než nějaký násobek 4. Třeba $29 = 28 + 1$ a $28 = 7 \times 4$. A co víc, když začneme zapisovat čísla tohoto formátu, všechna najdeme v naší tabulce, a i kdybychom ji rozšiřovali, nevypadá to, že by některé chybělo.

Každé kladné liché číslo je buď o 1 větší, nebo o 1 menší než násobek 4; jinými slovy jsou tvaru $4k - 1$ nebo $4k + 1$, kde k je *přirozené číslo*. Jediné sudé prvočíslo je 2. Takže pro každé prvočíslo platí jedna z následujících možností:

- je rovno 2,
- je tvaru $4k + 1$,
- je tvaru $4k - 1$.

Prvočísla, která chybějí v naší tabulce součtu dvou čtverců, jsou přesně ta prvočísla, jež mají tvar $4k - 1$.

Tato prvočísla se mohou vyskytovat jako *faktory* v rozkladu čísel v tabulce. Vezmeme třeba číslo 3, které se vyskytuje v rozkladu 9, 18, 36, 45, 72, 81 a 90. Ale všechna tato čísla jsou dokonce násobky $9 = 3^2$.

Když probíráme delší seznam z tohoto pohledu, objevuje se jednoduchá zákonitost. Ve zmiňovaném dopisu Fermat tvrdí, že dokázal, že nenulová čísla, která jsou součtem dvou čtverců, *jsou právě ta*, jejichž prvočíselný faktor $4k - 1$ vystupuje v rozkladu v sudé mocnině. Nejobtížnější bylo dokázat, že každé prvočíslo tvaru $4k + 1$ je součtem dvou čtverců. Albert Girard tuto domněnku v roce 1632 vyslovil, ale důkaz neuvedl.

V naší tabulce je pár příkladů, ale podrobme Fermatovo tvrzení náročnějšímu testu. Číslo 4001 je zjevně tvaru $4k + 1$, stačí položit $k = 1000$. Je to rovněž prvočíslo. Podle Fermatovy věty musí být součtem dvou čtverců. Kterých?

Jelikož nemáme žádnou lepší metodu, musíme zkusit postupně odečítat čtverce $1^2, 2^2, 3^2$ atd. a sledovat, jestli výsledek je čtvercem nějakého čísla. Dostáváme tak

$$\begin{aligned}4001 - 1^2 &= 4000, & \text{což není čtverec,} \\4001 - 2^2 &= 3997, & \text{což není čtverec,} \\4001 - 3^2 &= 3992, & \text{což není čtverec,} \\&\vdots\end{aligned}$$

až to nakonec vyjde:

$$4001 - 40^2 = 2401,$$