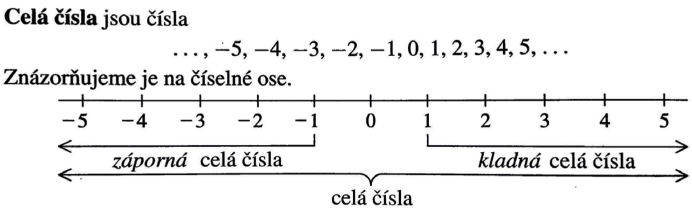
5 Celá čísla

Pozn. 14. Pokud bychom se drželi historického vývoje číselných oborů, následovala by nyní čísla, která by byla racionální a zároveň nezáporná. My ovšem budeme postupovat podle schématu 1. Pokud bychom totiž nyní definovali čísla racionální, museli bychom po zavedení celých čísel zvlášť dodatečně zavést záporná racionální čísla.

Na základní škole jsou zavedena celá čísla jako čísla kladná, nula a čísla záporná. Záporná jsou taková čísla, která jsou opačná k číslům kladným vzhledem k operaci sčítání. Dále jsou znázorněna na číselné ose, jak ukazuje obrázek 4 z učebnice *MATEMATIKA [1] pro 7. ročník základní školy* (Odvárko, Kadleček, 1998).



Obrázek 4: Celá čísla na číselné ose (Odvárko, Kadleček, 1998, s. 39)

Ve středoškolské učebnici *Matematika pro gymnázia, Základní poznatky z matematiky* (Bušek, Calda, 1992) se o celých číslech hovoří pouze jako o druhu čísel, který umožňuje vyjádřit změnu/nárůst/úbytek. Dále je zavedeno značení $\mathbb{Z}$ (z německého *Zahlen*, což jsou v překladu *čísla*). Nakonec učebnice uvádí věty o operacích sčítání a násobení. Konkrétně jsou uvedeny věty o jejich uzavřenosti, asociativitě, komutativitě, existenci neutrálního prvku, opačných prvků a distributivitě.

Zavedení celých čísel na základní i střední škole předpokládá jisté intuitivní chápání toho, jak budou čísla na ose uspořádána (o tom blíže kapitola 5.4), fungování aritmetických operací na oboru, i toho, že vůbec nějaká záporná čísla mohou existovat. K objevu záporných čísel však vedla dlouhá cesta, jak je popsáno dále.

5.1 Historie záporných a celých čísel

Fine (1907) o záporných číslech říká, že na rozdíl od čísel komplexních a iracionálních, která byla objevena skrze problémy geometrie, záporná čísla vycházejí z řešení algebraických rovnic. Proto je existence celých čísel těsně spjata právě s historií řešení rovnic.

Definice 12. Nechť V, W jsou dva výrazy, z nichž alespoň jeden obsahuje proměnnou. Jsou-li $x_1, x_2, \ldots, x_n$ všechny proměnné, které jsou obsaženy buď ve V, nebo W, nazýváme zápis $V = W$ rovnicí o n neznámých $x_1, x_2, \ldots, x_n$. Výraz V je levá strana, výraz W pravá strana rovnice. Speciálně zápis tvaru $V = 0$, kde V obsahuje alespoň jednu proměnnou, je rovnice v základním tvaru.

(Novotná, Trch, 1993)

O rovnicích se poprvé dočteme ve staroegyptském spisu písaře Ahmese (2000 př. n. l.), který řeší rovnice s jednou neznámou, kterou označuje slovem *hau* znamenajícím *kupa*. Crilly (2007) uvádí jako první Babyloňany, kteří pracovali dokonce s kvadratickými rovnicemi, a to až dva tisíce let před naším letopočtem. (Fine, 1907)

5.1.1 Záporná čísla v Řecku?

V raném Řecku byly hlavním tématem matematiky problémy z oblasti geometrie. Přístup k nim byl čistě syntetický. Algebraizace se objevuje teprve u Eukleida ve třetím století před naším letopočtem a to stále ve spojitosti s geometrickými problémy. Dánský matematik Zeuthen ve svém díle *Die Lehre von den Kegelschnitten im Altertum* (1886) zkoumá práci *Conics* (2. století př. n. l.) matematika Apollónia z Pergy žijícího ve druhém století před naším letopočtem a dochází k závěru, že autor musel využívat algebraického aparátu k popisu geometrických zákonitostí, o kterých hovoří. (Fine, 1907)

Rovnice se poté objevuje až ve spisech Hera z Alexandrie okolo roku 120 před naším letopočtem. Hero měl za cíl složité geometrické pravdy učinit použitelnými a srozumitelnými pro práci zeměměřičů. Geometrii formuloval do vět a problémy řešil pomocí rovnic, ze kterých se tak stal plnohodnotný nástroj geometrů. Hero řešil i rovnice kvadratické. (Fine, 1907)

Poslední z významných řeckých matematiků Diofantos z Alexandrie žijící ve třetím století našeho letopočtu zásadně přispěl k rozvoji teorie týkající se algebraických rovnic a jejich symbolismu. Diofantos využíval označení pro rovnost, neznámou nebo mocninu neznámé. Dále používal speciální znak pro odčítání, zatímco pro sčítání nikoliv. Dvě čísla se sčítala, pokud stála za sebou. Dále se zde také neobjevovaly obecné znaky pro známé hodnoty. Společně se značením přišla i nová pravidla pro algebraické operace. Dále pak Diofantos popsal pravidla pro sčítání, odečítání a násobení polynomů. (Fine, 1907)

Rovnice, které řešil, jsou následujícího tvaru:

1. $ax^m = bx^n$,
2. $ax^2 + bx = c$,
3. $ax^2 + c = bx$,
4. $ax^2 = bx + c$,
5. $y^2 = ax^2 + bx + c$,

kde koeficienty jsou nezáporná čísla. (Proto rozlišujeme případy 2, 3 a 4.)

Dále se v díle *Aritmetika* (Diofantos, 3. st. n. l.) objevuje i jedna rovnice kubická.

Řešením rovnice typu 5 nazýval Diofantos libovolnou dvojici $[x, y]$, pro kterou byla rovnice po dosazení pravdivá. Diofantos ve svém díle nediskutoval počet řešení a za uspokojivé považoval nalezení jednoho řešení, a to i v případě, kdy jich má daná rovnice nekonečně mnoho.

V *Aritmetice* (3. st. n. l.) také nenajdeme popsané obecné postupy výpočtů daných typů rovnic, nýbrž řešení konkrétních příkladů. (Fine, 1907)

Přesto lze vysledovat, jakým způsobem Diofantos a před ním také Hero řešili rovnici typu 3:

$$\begin{aligned} ax^2 + c &= bx, \\ a^2x^2 + ac &= abx, \\ a^2x^2 - abx + \left(\frac{b}{2}\right)^2 &= \left(\frac{b}{2}\right)^2 - ac, \\ ax - \frac{b}{2} &= \sqrt{\left(\frac{b}{2}\right)^2 - ac}, \\ x &= \frac{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 - ac}}{a}. \end{aligned}$$

Za řešení Diofantos považoval pouze takové případy, kdy číslo pod odmocninou bylo nezáporné a zároveň druhou mocninou přirozeného čísla. Zatímco dnes bychom za řešení $x^2 = a$, kde $a \in \mathbb{N}$, považovali $\pm\sqrt{a}$, Difantos bral v potaz pouze řešení s kladným znaménkem. Z toho a z faktu, že Diofantos byl posledním z velkých řeckých matematiků, Fine usuzuje, že řecká matematika o záporných (natož komplexních) číslech nikdy neuvažovala.

Pozn. 15. Fine upozorňuje, že rovnice, které dnes známe pod názvem Diofantické, se v žádném z Diofantových děl nevyskytují. Nazvány po řeckém matematikovi byly zřejmě pro jeho zásluhy v oblasti řešení rovnic jako takových.

5.1.2 Al-Chorezmí

Další pokrok, co se řešení rovnic týče, pak přichází z východu s prací matematika Al-Chorezmího (z jehož jména pochází slovo *algoritmus*). Ve své knize *Hisáb* *al-džabr wa-l-muqábala* (Al-Chorezmí, 825) se zabývá řešitelností lineárních a kvadratických rovnic. V knize se také objevuje slovo *al-džabr* znamenající *skládat dohromady*, které později dalo jméno tomu, co dnes známe jako *algebra*. (Crilly, 2007)

„U Diofanta algebra nebyla ničím více než uměním, jež řeší numerické problémy, mezi kterými neníž souvislosti; v Indii je povýšena na důstojnost vědy se svými vlastními obecnými metodami a koncepty.“

(Fine, 1907, s. 70)

5.1.3 Indie a objev záporných čísel

Na poznání Řeků navázali indičtí astronomové a matematici Árjabhata, Brahmagupta a Bháskara. Geometrii přijali od Hera a neučinili v ní další významné pokroky. Zato algebra přejatá od Diofanta v rukou indických matematiků byla rozvíjena a obohacena o velké množství poznatků. Indové začali více pracovat s obecnými symboly a zaváděli universální značení. Sčítání a odčítání byly značeny obdobně jako u Diofanta, jen nad odčítaným byla napsána tečka. Dále měli symboly pro násobení, dělení nebo odmocninu. (Fine, 1907)

Největším přínosem symbolismu indických matematiků je jejich přístup k odčítání. Na rozdíl od Diofanta, který mezi menšenec a menšitel vložil symbol značící odečítání, v Indii byl symbol odčítání přímo součástí menšitele. To znamená, že problém odčítání byl převeden na problém přičítání záporného čísla. Dalším důsledkem této formy zápisu je fakt, že číslo odečítané nyní mohlo stát samo jako plnohodnotný koeficient v rovnici. (Fine, 1907)

Bháskara dále objevil další vlastnosti odmocnin, uvědomil si, že znaménko po odmocnění může být jak kladné, tak záporné. Díky tomu již byl schopen nacházet oba kořeny kvadratických rovnic. Také zmínil, že odmocnit záporné číslo není možné. Fine tuto poznámku považuje za první výrok týkající se čísel komplexních v historii matematiky. (Fine,1907)

O kladných číslech se zprvu hovořilo jako o *means* znamenajícím *prostředky* a záporných jako o *debt*, tedy *dluh*. (Fine, 1907)

5.1.4 Cardano a Viète

Pro úplnost ještě uvádíme další dva významné matematiky, kteří se zasloužili o rozvoj algebry a řešení rovnic. Prvním byl Cardano, který dokázal, že algebraické rovnice stupně menšího nebo rovného čtyřem je možno řešit algebraicky, tj. vyjádřit kořeny pomocí koeficientů a operací sčítání, odčítání, násobení, dělení, umocnění a odmocnění. Také byl prvním, kdo uspokojivě odůvodnil existenci záporných řešení lineárních rovnic a přijal existenci záporných kořenů odmocniny. (Crilly, 2007; Heffeer, 2011)

Druhým byl Viète, který výrazy začal zapisovat pomocí písmen a přinesl nové metody řešení rovnic. (Crilly, 2007; Heffeer, 2011)

5.2 Descartova Geometrie

Na významu záporná čísla však nabyla až s vydáním dvojice Descarteových knih *Géométrie* (1637). Knihy byly počátkem analytické geometrie. Descartes se snažil veškeré problémy matematiky převést na rovnice a začal právě u geometrie.

Fine (1907) popisuje, jak Descartes v knize *Géométrie, Livre II.* (1637) převáděl křivky na rovnice. Postupoval tak, že známé označil pro nás konvenčním způsobem $a, b, c \ldots$ a neznámé x, y. Obecně poté popisoval každý bod křivky ve vztahu ke zvolené *line of reference* (budeme překládat jako *vztažná přímka*) způsobem, kde nejprve spustil kolmici z bodu křivky ke vztažné přímce a vzdálenost křivky od paty označil y. Vzdálenost paty kolmice od pevně zvoleného bodu na vztažné přímce označil x. Rovnicí křivky rozuměl takovou rovnici, která je platná pro každou dvojici x a y, kterou dostaneme v každém bodě křivky.

Před Descartem ležel problém, jak rozlišit případy, kdy křivka je na jedné, nebo druhé „straně“ vztažné přímky. Jelikož y označovalo pouze vzdálenost od přímky, ztrácela se z rovnice tato informace a například dvě rovnoběžné přímky s přímkou vztažnou, kde jedna by ležela „nad ní“ a druhá „pod ní“ ve stejné vzdálenosti, by měly stejnou rovnici. Descartes proto zavedl, že před délkou kolmic ležících na opačné „strany“ od přímky vztažné budou stát opačná znaménka. (Fine, 1907)

Tento konstrukt čísla záporná postavil na roveň číslům kladným. Nyní byla nepostradatelnými a přestala být něčím nepředstavitelným, jelikož měla reálnou aplikaci, kterou bylo možné graficky znázornit. (Fine, 1907)

Pozn. 16. V předchozím textu jsme mluvili o tzv. vztažné přímce. Z dnešního pohledu by se jednalo o osu x, pevně zvolený bod by byl počátek soustavy souřadnic a délky x, y bychom nazvali souřadnicemi. Fine (1907) píše, že Descartes sám nepoužíval pevně zvolenou soustavu os, kterou dnes známe pod jeho jménem jako kartézskou.

5.3 Konstrukce celých čísel

V konstrukci budeme postupovat podle následujících kroků tak, jak je uvedeno ve skriptech *Posloupnosti a řady* (Kubínová, Novotná, 1997, s. 146):

1. Konstrukce množiny $\mathbb{Z}$
   a) Na $\mathbb{N} \times \mathbb{N}$ zadefinujeme vhodnou relaci. Označíme ji $\sim$.
   b) Ověříme, že $\sim$ je ekvivalencí na $\mathbb{N}$.
   c) Rozklad množiny $\mathbb{N} \times \mathbb{N}$ podle ekvivalence $\sim$ nazveme množinou $\mathbb{Z}$.
2. Vytvoření Abelovy grupy $(\mathbb{Z}, +)$
   a) Definujeme operaci sčítání na $\mathbb{Z}$.

b) Ověříme, že struktura $(\mathbb{Z}, +)$ je skutečně Abelova grupa.

c) Najdeme souvislost mezi $(\mathbb{N}, +)$ a $(\mathbb{Z}, +)$.

d) Izomorfně vnoříme $(\mathbb{N}, +)$ do $(\mathbb{Z}, +)$.

1.a) Relaci na $\mathbb{N} \times \mathbb{N}$ definujeme takto:

$$(a, b) \sim (c, d) \Leftrightarrow (a + d = c + b).$$

(Kubínová, Novotná, 1997)

Pozn. 17. V relaci jsou tedy například dvojice $(1, 2)$ a $(4, 5)$ protože:

$$1 + 5 = 4 + 2.$$

1.b)

Věta 15. *Relace* $\sim$ *na* $\mathbb{N} \times \mathbb{N}$ *je ekvivalence.*

Důkaz. Chceme ukázat, že $\sim$ je reflexivní, symetrická a tranzitivní.

i) $\sim$ je reflexivní $\Leftrightarrow \forall (a, b) \in (\mathbb{N} \times \mathbb{N}) : (a, b) \sim (a, b)$.

Pro $\forall a, b \in \mathbb{N}$ platí, že $a + b = a + b$. Z toho podle definice $\sim$ plyne $(a, b) \sim (a, b)$.

Relace $\sim$ je reflexivní.

ii) $\sim$ je symetrická $\Leftrightarrow (\forall (a, b), (c, d) \in (\mathbb{N} \times \mathbb{N}) : (a, b) \sim (c, d) \Rightarrow (c, d) \sim$ $\sim (a, b))$.

Platí $(a, b) \sim (c, d)$. Z toho vyplývá $a + d = c + b$. To lze díky symetrii relace $=$ zapsat jako $c + b = a + d$, což z definice relace $\sim$ platí právě tehdy, když $(c, d) \sim (a, b)$.

Relace $\sim$ je symetrická.

iii) $\sim$ je tranzitivní $\Leftrightarrow (\forall (a,b),(c,d),(e,f) \in (\mathbb{N} \times \mathbb{N}))$:

$((a,b) \sim (c,d) \wedge (c,d) \sim (e,f)) \Rightarrow ((a,b) \sim (e,f))$.

Vyjdeme z předpokladů, které přepíšeme pomocí definice, tedy:

$$a + d = c + b,$$
$$c + f = e + d.$$

K první rovnosti přičteme f, ke druhé b. Získáváme tedy:

$$a + d + f = c + b + f,$$
$$c + f + b = e + d + b.$$

Pravá strana první rovnosti se rovná levé straně druhé (využijeme komutativitu přirozených čísel). Proto tedy platí:

$$a + d + f = e + d + b.$$

Můžeme využít pravidlo pro krácení z věty 5. Tím získáme rovnost $a + f = e + b$, což je ale z definice relace $\sim$ právě $(a,b) \sim (e,f)$. Relace $\sim$ je tedy tranzitivní relací.

Ukázali jsme, že relace je reflexivní, symetrická i tranzitivní, a je tedy ekvivalencí na $\mathbb{N} \times \mathbb{N}$. $\square$

1.c)

Definice 13. Množinou celých čísel $\mathbb{Z}$ nazveme rozklad na $\mathbb{N} \times \mathbb{N}$ podle ekvivalence $\sim$. Třídy tohoto rozkladu jsou prvky množiny $\mathbb{Z}$. Tedy platí:

$$\mathbb{Z} = \{T_{(a,b)}; (a,b) \in \mathbb{N} \times \mathbb{N}\}, T_{(a,b)} = \{(x,y) \in \mathbb{N} \times \mathbb{N}; (x,y) \sim (a,b)\}.$$

(Kubínová, Novotná, 1997)

2.a) Nyní na množině $\mathbb{Z}$, kterou jsme sestrojili, definujeme operaci $+$ takto:

Definice 14. $\forall T_{(a,b)}, T_{(c,d)} \in \mathbb{Z} : T_{(a,b)} + T_{(c,d)} = T_{(a+c,b+d)}$.

Aby byla definice 14 korektní, musí splňovat následující dvě podmínky:

i) $T_{(a+c,b+d)} \in \mathbb{Z}$,

ii) $\forall (x,y) \in T_{(a,b)}, \forall (u,v) \in T_{(c,d)} : (x+u, y+v) \in T_{(a+c,b+d)}$.

i) platí, jelikož každý prvek $T_{(x,y)}$, kde $x, y \in \mathbb{N}$, je z množiny $\mathbb{Z}$, tedy i $T_{(a+c,b+d)}$. (Součet dvou přirozených čísel je znovu přirozené číslo podle definice 4.)

ii) je nutné ověřit:

$$\forall (x,y) \sim (a,b), \forall (u,v) \sim (c,d) : (x+u, y+v) \sim (a+c, b+d).$$

Opět přepíšeme předpoklady podle definice relace $\sim$: $(x+b = a+y) \wedge (u+d = c+v)$. Rovnosti sečteme a dostáváme $x+b+u+d = a+y+c+v$. Využijeme komutativitu sčítání přirozených čísel (viz věta 5) a poslední rovnost přepíšeme jako $x+u+b+d = a+c+y+v$, což ale je právě $(x+u, y+v) \sim (a+c, b+d)$. Tedy i druhá podmínka pro korektnost definice sčítání je splněna.

(Kubínová, Novotná, 1997)

2.b) Ptáme se, zda množina $\mathbb{Z}$ s operací $+$ tvoří Abelovu grupu.

Věta 16. *Struktura* $(\mathbb{Z}, +)$ *je Abelovou grupou.*

(Kubínová, Novotná, 1997)

Důkaz. Aby struktura byla Abelovou grupou, musí platit:

i. $T_{(a,b)}, T_{(c,d)} \in \mathbb{Z} \Rightarrow T_{(a,b)} + T_{(c,d)} \in \mathbb{Z}$,

ii. $\forall T_{(a,b)}, T_{(c,d)} \in \mathbb{Z} : T_{(a,b)} + T_{(c,d)} = T_{(c,d)} + T_{(a,b)}$,

iii. $\forall T_{(a,b)}, T_{(c,d)}, T_{(e,f)} \in \mathbb{Z} : (T_{(a,b)} + T_{(c,d)}) + T_{(e,f)} = T_{(a,b)} + (T_{(c,d)} + T_{(e,f)})$,

iv. $\exists T_{(x,y)} \in \mathbb{Z} \quad \forall T_{(a,b)} \in \mathbb{Z} : T_{(a,b)} + T_{(x,y)} = T_{(x,y)} + T_{(a,b)} = T_{(a,b)}$,

v. $\forall T_{(a,b)} \in \mathbb{Z} \quad \exists T_{(x,y)} \in \mathbb{Z} : T_{(a,b)} + T_{(x,y)} = T_{(0,0)}$.

i. Uzavřenost operace + byla jednou z ověřovaných podmínek po zavedení definice 14. Sčítání celých čísel je tedy vnitřní operace na množině $\mathbb{Z}$.

ii. Pro důkaz komutativity přepíšeme zvlášť levou a zvlášť pravou stranu rovnosti:

$$\left.\begin{aligned} L &= T_{(a,b)} + T_{(c,d)} = T_{(a+c,b+d)} \\ P &= T_{(c,d)} + T_{(a,b)} = T_{(c+a,d+b)} \overset{def.\,5}{=} T_{(a+c,b+d)} \end{aligned}\right\} L = P.$$

Sčítání celých čísel je komutativní.

iii. Dokážeme asociativitu sčítání celých čísel. Chceme ukázat, že pro všechna $T_{(a,b)}, T_{(c,d)}, T_{(e,f)} \in \mathbb{Z}$ platí $\Big(T_{(a,b)} + T_{(c,d)}\Big) + T_{(e,f)} = T_{(a,b)} + \Big(T_{(c,d)} + T_{(e,f)}\Big)$. Pro sčítání použijeme definici 14. Upravíme zvlášť levou a pravou stranu rovnosti a ukážeme, že se strany rovnají:

$$\left.\begin{aligned} L &= \Big(T_{(a,b)} + T_{(c,d)}\Big) + T_{(e,f)} = \Big(T_{(a+c,b+d)}\Big) + T_{(e,f)} = T_{(a+c+e,b+d+f)} \\ P &= T_{(a,b)} + \Big(T_{(c,d)} + T_{(e,f)}\Big) = T_{(a,b)} + \Big(T_{(c+e,d+f)}\Big) = T_{(a+c+e,b+d+f)} \end{aligned}\right\} L = P.$$

Sčítání celých čísel je asociativní.

iv. Dokážeme existenci neutrálního prvku. Zvolme za hledanou třídy $T_{(n,n)}$, kde $n \in \mathbb{N}$. Ověříme, že platí $T_{(a,b)} + T_{(n,n)} = T_{(a,b)}$. Vyjdeme z rovnosti $a+b+n = a+b+n$, kde $a, b, n \in \mathbb{N}$. Využijeme komutativitu a asociativitu sčítání přirozených čísel podle věty 5 a dostáváme rovnost $a + (b + n) = = (a + n) + b$. Pak ovšem z definice relace $\sim$ platí $(a, b) \sim (a + n, b + n)$.

Podle definice 13 platí, že pokud $(a, b) \sim (a + n, b + n)$, pak se rovnají i třídy $T_{(a,b)}$ a $T_{(a+n,b+n)}$. Platí:

$$T_{(a,b)} = T_{(a+n,b+n)}.$$

Pravá strana rovnosti lze podle definice 14 přepsat jako $T_{(a,b)} + T_{(n,n)}$. Tudíž víme, že platí:

$$T_{(a,b)} + T_{(n,n)} = T_{(a,b)}.$$

Že $T_{(a,b)} + T_{(n,n)} = T_{(n,n)} + T_{(a,b)}$, už víme z dokázané komutativity sčítání celých čísel. $T_{(n,n)}$ je tedy neutrálním prvkem vzhledem ke sčítání celých čísel.

Pozn. 18. Podle definice 13 platí, že třída $T_{(n,n)} = T_{(0,0)}$.

v. Dokážeme existenci opačných prvků. Nechť $T_{(a,b)} \in \mathbb{Z}$. Dokážeme, že pro $T_{(b,a)} \in \mathbb{Z}$ platí $T_{(a,b)} + T_{(b,a)} = T_{(0,0)}$. Vyjdeme z rovnosti $a + b = a + b$, kde $a, b \in \mathbb{N}$. Využijeme komutativitu a neutrálnost prvku 0 vzhledem ke sčítání přirozených čísel podle věty 5 a dostáváme rovnost $a + b + 0 =$ $= 0 + b + a$. Pak z definice relace $\sim$ platí $(a + b, b + a) \sim (0, 0)$. Podle definice relace $\sim$ platí, že pokud $(a + b, b + a) \sim (0, 0)$, pak se rovnají i třídy $T_{(a+b,b+a)}$ a $T_{(0,0)}$. Tudíž platí:

$$T_{(a+b,b+a)} = T_{(0,0)}.$$

Levá strana rovnosti lze rozepsat podle definice 14 jako $T_{(a,b)} + T_{(b,a)}$. Tudíž platí:

$$T_{(a,b)} + T_{(b,a)} = T_{(0,0)}.$$

Opačným prvkem pro každý prvek $T_{(a,b)} \in \mathbb{Z}$ je prvek ve tvaru $T_{(b,a)} \in \mathbb{Z}$.

Množina celých čísel s operací + je tedy Abelovou grupou. □

2.c) Přirozená čísla nejsou podmnožinou čísel celých. Ovšem můžeme zkonstruovat podstrukturu $(\mathbb{Z}', +)$, která bude se stukrurou $(\mathbb{N}, +)$ izomorfní. (Kubínová, Novotná, 1997)

Věta 17. *Ve struktuře* $(\mathbb{Z}, +)$ *existuje podstruktura* $(\mathbb{Z}', +)$*, která je s* $(\mathbb{N}, +)$ *izomorfní.*

Důkaz. Zkonstruujeme $(\mathbb{Z}', +)$:

$$\mathbb{Z}' = \{T_{(z,0)}; z \in \mathbb{N}\}, + \text{ je zúžením operace sčítání ze } \mathbb{Z} \text{ na } \mathbb{Z}'.$$

Aby platilo, že $(\mathbb{N}, +)$ je izomorfní s $(\mathbb{Z}', +)$, musí existovat bijektivní zobrazení $\varphi : \mathbb{N} \to \mathbb{Z}$, pro které navíc platí: $\forall x, y \in \mathbb{N} : \varphi(x + y) = \varphi(x) + \varphi(y)$.

Zobrazení definujeme takto:

$$\forall x \in \mathbb{N} : \varphi(x) = T_{(x,0)}.$$

(Kubínová, Novotná, 1997, s. 147)

Je bijektivní?

- Nejprve ukážeme, že zobrazení φ je injektivní. Ukážeme, že platí:

  $$\forall x_1, x_2 \in \mathbb{N} : x_1 \neq x_2 \Rightarrow \varphi(x_1) \neq \varphi(x_2).$$

  Tvrzení dokážeme sporem. Předpokládejme, že $\exists x_1, x_2 \in \mathbb{N}(x_1 \neq x_2) \wedge \wedge(\varphi(x_1) = \varphi(x_2))$. Pak se ovšem $T_{(x_1,0)} = T_{(x_2,0)}$, což nastává právě tehdy, když $(x_1, 0) \sim (x_2, 0)$. Pak platí $x_1 + 0 = x_2 + 0$, což podle věty 5 přepíšeme jako $x_1 = x_2$. To je spor s předpokladem, že x_1 a x_2 jsou různá.

  Zobrazení φ je injektivní.

- Ukážeme, že zobrazení φ je surjektivní. Tedy že platí:

$$\forall T_{(x,0)} \in \mathbb{Z} \quad \exists x \in \mathbb{N} : \varphi(x) = T_{(x,0)}.$$

  Z definice celých čísel platí, že pro každý prvek $T_{(a,b)}$ jsou $a, b \in \mathbb{N}$. Tedy i x z celého čísla $T_{(x,0)}$ je přirozené číslo. Pro x platí $\varphi(x) = T_{(x,0)}$.

  Zobrazení φ je surjektivní.

Zobrazení φ je injektivní i surjektivní. Je tedy bijekce.

Ověříme, zda platí:

$$\varphi(x + y) = \varphi(x) + \varphi(y).$$

Obě strany rovnosti přepíšeme podle definice zobrazení φ:

$$\left.\begin{array}{l} L = \varphi(x + y) = T_{(x+y,0)} = T_{(x,0)} + T_{(y,0)} \\ P = \varphi(x) + \varphi(y) = T_{(x,0)} + T_{(y,0)} \end{array}\right\} L = P.$$

Platí tedy $\varphi(x+y) = \varphi(x)+\varphi(y)$. Struktura $(\mathbb{Z}', +)$ je izomorfní se strukturou $(\mathbb{N}, +)$. □

2.d) Jestliže položíme $\forall x \in \mathbb{N} : x \equiv T_{(x,0)}$, je $\mathbb{N} \subset \mathbb{Z}$. (Kubínová, Novotná, 1997, s. 148)

Věta 18. $\forall T_{a,b} \quad \exists! c \in \mathbb{N} : \left(T_{(a,b)} = T_{(c,0)}\right) \vee \left(T_{(a,b)} = T_{(0,c)}\right).$

Důkaz. Podle věty 7 platí pro přirozená čísla a, b právě jedna z následujících možností:

- $a < b : \exists! c \in \mathbb{N} - \{0\} : a + c = b$, pak

$$T_{(a,b)} = T_{(a,a+c)} = T_{(a+0,a+c)} = T_{(a,a)} + T_{(0,c)} = T_{(0,0)} + T_{(0,c)} = T_{(0,c)}$$

- $a = b : T_{(a,b)} = T_{(a,a)} = T_{(0,0)}$, c položíme rovno nule a platí.

- $a > b : \exists! c \in \mathbb{N} - \{0\} : b + c = a$ pak,

$$T_{(a,b)} = T_{(b+c,b)} = T_{(b+c,b+O)} = T_{(b,b)} + T_{(c,0)} = T_{(0,0)} + T_{(c,0)} = T_{(c,0)}.$$

Jednoznačnost plyne z krácení přirozených čísel (viz věta 5). □

(Kubínová, Novotná, 1997, s. 148)

Pozn. 19. Typy tříd z věty 18 budeme nazývat a značit takto:

- Množinu $\{T_{(c,0)} \in \mathbb{Z}; c \neq 0\}$ nazveme množinou kladných celých čísel a její prvky kladnými čísly. Budeme ji značit $\mathbb{Z}^+$. Třídu $T_{(c,0)}$ budeme značit zkráceně c.

- Množinu $\{T_{(0,c)} \in \mathbb{Z}; c \neq 0\}$ nazveme množinou záporných celých čísel a její prvky zápornými čísly. Budeme ji značit $\mathbb{Z}^-$. Třídu $T_{(0,c)} = -T_{(c,0)}$ budeme značit zkráceně $-c$.

- Nulu nebudeme zahrnovat ani do jedné z množin $\mathbb{Z}^+, \mathbb{Z}^-$. Budeme ji považovat za číslo, které není ani kladné, ani záporné. Třídu $T_{(0,0)}$ budeme značit 0.

  Platí tedy, že $\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$.

(Kubínová, Novotná, 1997)

Definice 15. Operaci násobení $\odot$ na celých číslech definujeme jako:

$$\begin{aligned} a \odot b &= a \cdot b \quad \forall a, b \in \mathbb{N}; \\ &= (-a) \cdot (-b) \quad \forall a, b \in \mathbb{Z}^-; \\ &= -((-a) \cdot b)) \quad \forall a \in \mathbb{Z}^-, b \in \mathbb{N}; \\ &= -(a \cdot (-b)) \quad \forall a \in \mathbb{N}, b \in \mathbb{Z}^-. \end{aligned}$$

(Kubínová, Novotná, 1997)

Pozn. 20. Násobení celých čísel lze zavést také pomocí tříd:

$$\forall T_{(a,b)}, T_{(c,d)} \in \mathbb{Z} : T_{(a,b)} \cdot T_{(c,d)} = T_{(a\cdot c+b\cdot d, a\cdot d+b\cdot c)}.$$

Aby byla definice násobení korektní, musí splňovat následující dvě podmínky:

i) $T_{(a\cdot c+b\cdot d, a\cdot d+b\cdot c)} \in \mathbb{Z}$,

ii) $\forall (x,y) \in T_{(a,b)}, \forall (u,v) \in T_{(c,d)} : (x\cdot u + y\cdot v, x\cdot v + y\cdot u) \in T_{(a\cdot c+b\cdot d, a\cdot d+b\cdot c)}$.

Pozn. 21. Násobení celých čísel jsme definovali pomocí násobení čísel přirozených ($\cdot$), proto se přenáší vlastnost komutativity, asociativity, distributivity násobení vzhledem ke sčítání, existence neutrálního prvku a pravidla krácení pro násobení z $\mathbb{N}$ na $\mathbb{Z}$.

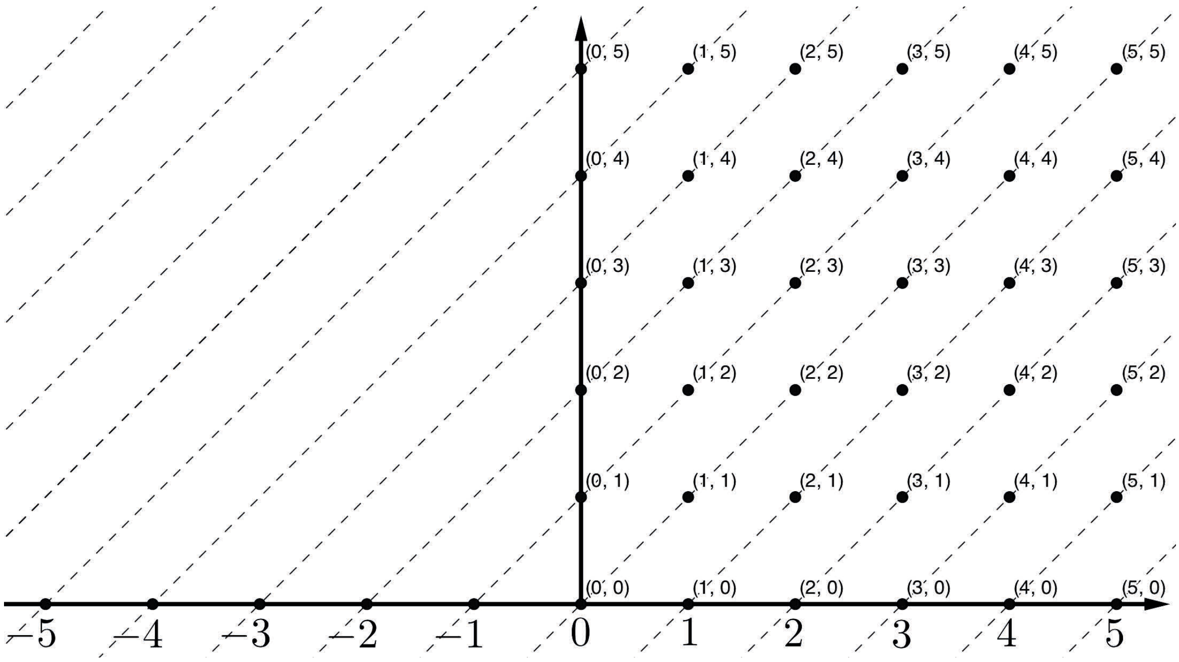
Pozn. 22. Definice 15 využívá podobné logiky jako Euler při argumentaci, proč mínus krát mínus dává plus (viz 5.4.2), a sice té, že popíše všechny případy, které mohou nastat pro pravou stranu.

Třídy ekvivalence po zavedení značení z poznámky 19 můžeme znázornit obrázkem 5. Souřadnice bodů odpovídají uspořádaným dvojicím přirozených čísel, šrafovaná čára znázorňuje třídu ekvivalence. Číslo na konci této čáry odpovídá označení této třídy, tedy označení prvku množiny celých čísel.

Pozn. 23. Věty, důkazy a definice v kapitole 5.3 jsou převzaty ze skript (Kubínová, Novotná, 1997). Důkazy vět 15 a první dva body důkazu 16 jsou vlastní, třetí bod vychází také ze skript (Kubínová, Novotná, 1997).

5.4 Celá čísla a číselná osa

V úvodu kapitoly 5 jsme zmínili číselnou osu jako způsob grafické interpretace celých čísel na základní škole. S chápáním číselné osy v souvislosti se zápornými čísly



Obrázek 5: Rozklad podle ekvivalence (vlastní obrázek)

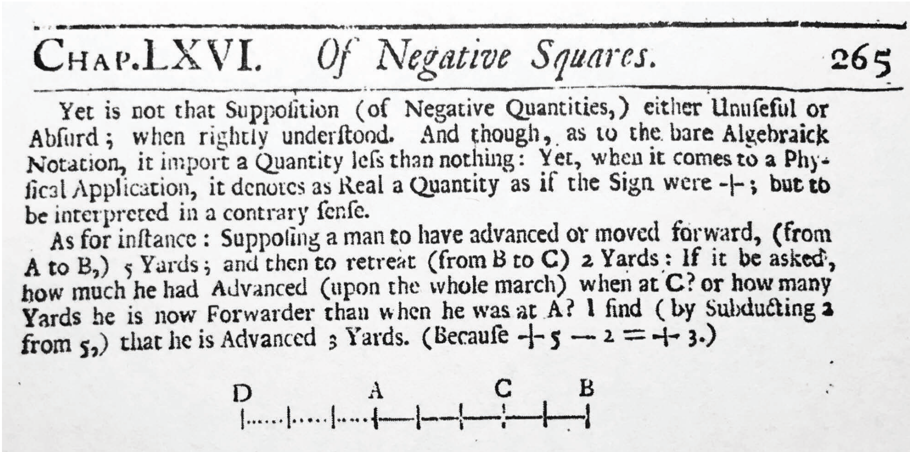
ovšem vznikla v historii celá řada problémů, jimiž se v sedmnáctém a osmnáctém století zabývali matematici jako Euler, Leibnitz nebo d'Alembert. (Heeffer, 2011)

Jak v článku *Historical objections against the number line* (2011) říká Heeffer, je důležité rozumět těmto problémům, které v chápání koncept záporných čísel na ose způsobil v historii, zejména pro učitele, kteří tak snáze dokáží porozumět obtížím žáků s uchopením záporných čísel.

Definice 16. Číselnou osou rozumíme reprezentaci čísel na přímce, na níž jsou body představující celá/reálná čísla. Vzdálenost mezi body číselně odpovídá rozdílu mezi příslušnými čísly. V západní kultuře obvykle znázorňujeme vodorovně, tak, že kladná čísla jsou směrem vpravo, záporná vlevo od nuly. (Heeffer, 2011)

Jako první číselnou osu představil Wallis ve své knize *Algebra* (1685) v souvislosti se slovní úlohou o vzdálenosti (viz obrázek 6). (Heeffer, 2011)

Heeffer (2011) se zamýšlí nad přínosy a nedostatky tohoto modelu. Model od-



CHAP. LXVI. *Of Negative Squares.* 265

Yet is not that Suppoſition (of Negative Quantities,) either Unuſeful or Abſurd; when rightly underſtood. And though, as to the bare Algebraick Notation, it import a Quantity leſs than nothing: Yet, when it comes to a Phyſical Application, it denotes as Real a Quantity as if the Sign were $+$; but to be interpreted in a contrary ſenſe.

As for inſtance: Suppoſing a man to have advanced or moved forward, (from A to B,) 5 Yards; and then to retreat (from B to C) 2 Yards: If it be asked, how much he had Advanced (upon the whole march) when at C? or how many Yards he is now Forwarder than when he was at A? I find (by Subducting 2 from 5,) that he is Advanced 3 Yards. (Becauſe $+5 - 2 = +3$.)

Obrázek 6: První výskyt číselné osy v knize Wallise *Algebra* (1685)

Obrázek převzat od Heeffera (2011, s. 14).

povídá množině $\mathbb{Z}$ v tom, že pro každé číslo existuje číslo větší i menší, a stejně tak osa, tedy přímka, lze „protáhnout“ do nekonečna na obou jejích stranách. Osa také dobře znázorňuje rozdíly mezi čísly a v případě racionálních čísel je vhodným nástrojem pro představu, mezi která dvě celá čísla zlomek patří. Jako nedostatky osy Heeffer (2011) spatřuje znázornění aritmetických operací jako násobení, dělení nebo poměry v kombinaci se záporným číslem. Dále si klade otázku, zda je umístění nuly jako předělu mezi kladnými a zápornými čísly zejména pro žáky intuitivní a zda je představení celých čísel osou vůbec vhodné. Z tohoto důvodu zmiňuje problémy, se kterými se v historii matematici potýkali a o nichž budou následující kapitoly.

5.4.1 Poměr

Jako první na problémy s osou a intuitivním chápáním celých čísel upozornil Arnauld. V knize *Geometry* (1667) zmínil vlastnost, že pokud zvolíme přirozené číslo

n větší než jedna, poměr čísel $n+1$ ku $n-1$ bude vždy větší než poměr převrácený:

$$\frac{n+1}{n-1} > \frac{n-1}{n+1},$$

jakmile však k přirozeným číslům na ose přidáme opačná čísla (stále za podmínky, že nedělíme nulou), přestává vlastnost, že větší číslo ku menšímu je větší než menší číslo ku většímu, platit. Uvádí to na následujícím případu:

$$\frac{1}{-1} > \frac{-1}{1},$$

to evidentně neplatí. (Heeffer, 2011)

5.4.2 Mínus krát mínus

Dále Heeffer (2011) uvádí součin dvou záporných čísel. Vlastnost, kterou dnes známe (viz definice 15), není, jak říká, z osy patrná.

Čemu je roven takový součin, se zabýval v pojednání *Aliabraa argibra* (1344) Dardi. Vysvětlil na konkrétním příkladě za využití distributivity, proč se součin dvou záporných čísel musí rovnat číslu kladnému:

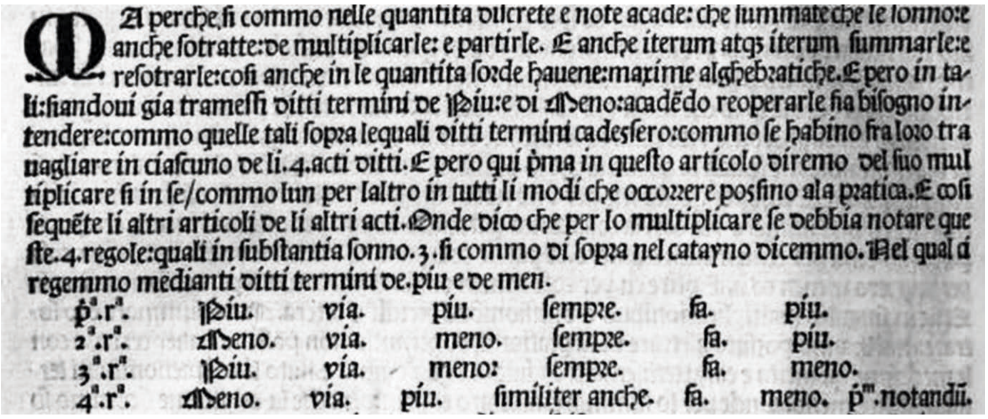
$$64 = 8 \cdot 8 = (10-2)(10-2) = 100 - 20 - 20 + ((-2)(-2)),$$

aby rovnost platila, musí se součin $(-2)(-2)$ rovnat 4.

Obecněji vztahy mezi znaménky stanovil na konci patnáctého století Paciolli v díle *Summa* (1494). Viz obrázek 7 a 8. (Heeffer, 2011)

Ve volném překladu z italštiny tabulka na obrázku 7 stanoví:
„Součin kladného s kladným je kladný."
„Součin záporného se záporným je kladný."
„Součin kladného se záporným je záporný."
„Součin záporného s kladným je záporný."

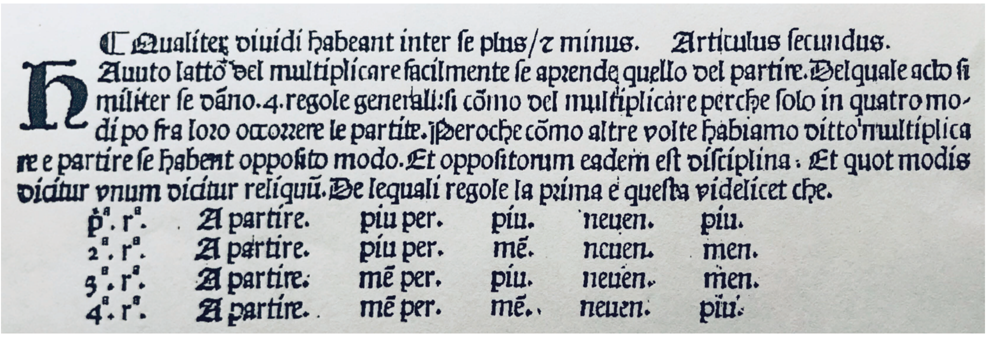
Obdobně tabulka v překladu na obrázku 8 popisuje:
„Podíl kladného s kladným je kladný."



M A perche, si commo nelle quantita discrete e note acade: che summate che le sonno: e anche sotratte: de multiplicarle: e partirle. E anche iterum atqз iterum summarle: e resotrarle: cosi anche in le quantita sorde hauene: maxime alghebratiche. E pero in tali: siandoui gia tramessi ditti termini de Piu: e di Meno: acadẽdo reoperarle sia bisogno intendere: commo quelle tali sopra lequali ditti termini cadessero: commo se habino fra loro tra uagliare in ciascuno de li.4.acti ditti. E pero qui pma in questo articolo diremo del suo multiplicare si in se/commo lun per laltro in tutti li modi che occorere posino ala pratica. E cosi sequẽte li altri articoli de li altri acti. Onde dico che per lo multiplicare se debbia notare queste.4.regole: quali in substantia sonno.3. si commo di sopra nel catayno dicemmo. Nel qual diregemmo medianti ditti termini de.piu e de men.

pª.rª.	Piu.	via.	piu.	sempre.	fa.	piu.	
2ª.rª.	Meno.	via.	meno.	sempre.	fa.	piu.	
3ª.rª.	Piu.	via.	meno:	sempre.	fa.	meno.	
4ª.rª.	Meno.	via.	piu.	similiter anche.	fa.	meno.	pᵐ.notandū.

Obrázek 7: Pravidla pro znaménka při násobení (Paciolli, 1494, s. 112)



Qualiter diuidi habeant inter se plus/et minus. Articulus secundus.

H Auuto latto del multiplicare facilmente se aprende quello del partire. Delquale acto similiter se dãno.4.regole generali: si cõmo del multiplicare perche solo in quatro modi po fra loro occorere le partite. Peroche cõmo altre volte habiamo ditto multiplicare e partire se habent opposito modo. Et oppositorum eadem est disciplina: Et quot modis dicitur vnum dicitur reliquũ. De lequali regole la prima e questa videlicet che.

pª. rª.	A partire.	piu per.	piu.	neuen.	piu.
2ª. rª.	A partire.	piu per.	mẽ.	neuen.	men.
3ª. rª.	A partire.	mẽ per.	piu.	neuen.	men.
4ª. rª.	A partire.	mẽ per.	mẽ.	neuen.	piu.

Obrázek 8: Pravidla pro znaménka při dělení (Paciolli, 1494, s. 113)

„Podíl kladného se záporným je záporný.“

„Podíl záporného s kladným je záporný.“

„Podíl záporného se záporným je kladný.“

Důležitým pozorováním na tabulkách je, že zcela upustily od hodnot a pravidla jsou stanovena zcela obecně. (Paciolli, 1494; Heeffer, 2011)

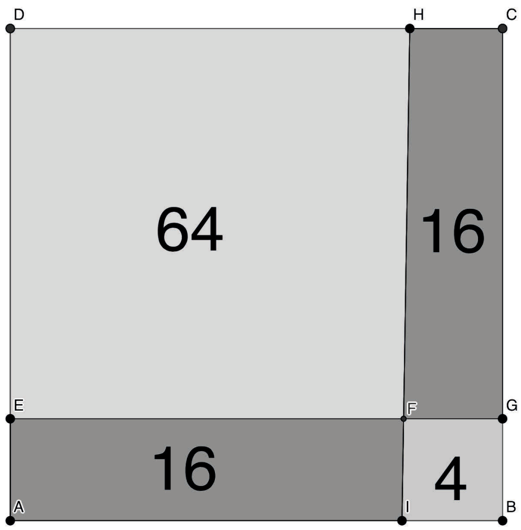
Dardiho argumentaci zpochybnil Cardano v dílech *De Aliza Regulae* (1570) a *Sermo de plus and minus* (1663). Vyšel ze stejného příkladu jako Dardi a tvrdil, že stejně, jako z něj můžeme usuzovat, že mínus krát mínus dává plus, můžeme také říct, že plus krát plus dává mínus. Cardano argumentoval takto:

1. Mějme čtverec $ABCD$ o délce strany 10 (viz obrázek 9).
2. Obsah čterce $IBGF$ je roven 4 a obsahy shodných obdélníků $AIFE$ a $FGCH$ jsou rovny 16.
3. Obsah čtverce $EFHD$ je tedy 64.
4. Abychom ze 100 dostali 64, musíme odebrat obdélník $ABGE$ a $IBCH$.
5. Tím jsme ovšem odebrali čtverec $IBGF$ dvakrát, musíme ho tedy jednou přičíst.

Neboli:

$$100 - (10 \cdot 2) - (10 \cdot 2) + (2 \cdot 2) = 64.$$

To je rovno $(10 - 2) \cdot (10 - 2)$ stejně, jako tomu bylo v případě Dardiho, ovšem podle Cardana je přičtená čtyřka důsledek dvojnásobného odečtení čtverce, nikoliv součinu $(-2) \cdot (-2)$. (Heeffer, 2011)



Obrázek 9: Dardi vs. Cardano (vlastní obrázek)

Cardano uzavřel svůj argument slovy, že stejně jako můžeme tvrdit, že mínus krát mínus dává plus, můžeme říct, že mínus krát mínus dává mínus (Heeffer, 2011). Heeffer soudí, že Cardano chtěl touto demonstrací poukázat, že je třeba i zákonitosti, které jsou obecně příjmány nebo se jeví jako samozřejmé, zakotvit v definicích a blíže prozkoumat. Odůvodnění matematiků tehdejší doby včetně Dardiho pro Cardana nebylo uspokojivé, a tak ukázal, jak jednoduše lze Dardiho argumentaci napadnout.

5.4.3 Podíl větší než nekonečno

Wallis v *Arithmetica Infinitorium* (1656) představuje v souvislosti s problematikou kvadratury křivek, kterou se zabýval, myšlenku, že dělíme-li kladné číslo záporným, dostáváme číslo větší než nekonečno. Úvahu stavěl na tom, že čím menším číslem dělíme, tím větší číslo dostáváme. Dělíme-li nulou, dostáváme podle Wallise nekonečno (původně Bháskarova myšlenka, viz 2.2), a překročíme-li tuto mez a dělíme stále menšími čísly, dostaneme čísla větší než samotné nekonečno. (Heeffer, 2011)

Ke stejnému závěru dospěl v textu *De seriebus divergentibus* (1746) Euler (Heeffer, 2011). Euler zavedl rozdělení na dvě záporna:

1. Záporno prvního druhu je takové, které dostaneme, odečteme-li od čísla a jeho následníka $\sigma(a)$.

2. Jako záporno druhého druhu Euler chápal výsledek dělení kladného čísla záporným, tedy například $\frac{1}{-1}$, nebo případy, kdy se sčítaly divergentní řady a výsledky byly záporné.

(Heeffer, 2011)

První druh jsou záporná čísla menší než nula. Druhý druh jsou záporná čísla větší než nekonečno. To Euler demonstroval na obdobném příkladu jako Wallis:

$$\frac{1}{3}, \frac{1}{2}, \frac{1}{1}, \frac{1}{0}, \frac{1}{-1}, \frac{1}{-2}, \dots,$$

směrem zleva do prava čísla rostou, až dosáhnou nekonečna, a tak budou podle Eulera růst i nadále až přes nekonečno. (Heeffer, 2011)

Heeffer zmiňuje miskoncepce mnohých historiků (Kline, Dunham, Sandifer, ...), kteří tato pozorování interpretovali tak, že Euler s Wallisem tvrdili, že záporná čísla na ose nemají místo vlevo od nuly, nýbrž za nekonečnem. Euler sám ve své knize elementární algebry (1822) napsal, že záporná čísla jsou méně než ničím. To také demonstroval na ose tím, že od nuly odečítal opakovaně -1 (obdoba následníka v přirozených číslech). Dále přišel s argumentem, proč součin dvou záporných čísel je kladný. Řekl, že víme-li, že mínus krát plus je mínus, musí mínus krát mínus mít jiný výsledek, tedy plus. (Heeffer, 2011)

D'Alembert v *Encyclopédie* (1761-1790) o záporných číslech zmiňuje: „Záporné kvantity jsou ty, které jsou ovlivněny znaménkem mínus a které jsou několika matematiky považovány za menší než nula. Poslední myšlenka je chybná, jak bude za moment vidno." (d'Alembert, 1785, s. 445) Argumentoval poté tím, že nemůžeme tvrdit, že záporná čísla jsou menší než nula, protože ne vždy musí přejít z kladných do záporných právě přes nulu. To ukázal na příkladu $y = x - a$, který přes nulu z kladných do záporných vždy přejde, a poté na příkladu $y = \frac{1}{x-a}$, kdy z kladných do záporných nepřecházíme přes nulu, nýbrž nekonečno (pro hodnotu $x = a$). Proto není podle d'Alemberta možné říkat, že záporná čísla jsou vždy menší než nula. (Heeffer, 2011)

5.5 Spočetnost

Věta 19. *Množina celých čísel je spočetná.*

Důkaz. Celá čísla přerovnáme do následující posloupnosti:

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

Podle definice 9 je množina spočetná, právě když existuje bijektivní zobrazení f na přirozená čísla. To zajisté existuje, můžeme ho definovat například následujícím způsobem:

$$
\begin{aligned}
f(0) &= 1, \\
f(1) &= 2, \\
f(-1) &= 3, \\
f(2) &= 4, \\
f(-2) &= 5, \\
&\dots
\end{aligned}
$$

□

Věta 20. *Množina celých čísel je nekonečná množina.*

Důkaz. Celá čísla jsou nadoborem přirozených čísel (definice 2). Dále platí věta 11. Z toho plyne, že i množina celých čísel je nekonečná. □

5.6 Uspořádání celých čísel

Definice 17. Relace $<$, kterou nazveme uspořádáním na $\mathbb{Z}$, je definována takto:

$$\forall a, b \in \mathbb{Z} : a < b \Leftrightarrow b + (-a) \in \mathbb{Z}^+.$$

(Kubínová, Novotná, 1997)

Věta 21. *Relace $<$ je na $\mathbb{Z}$ tranzitivní a trichotomická.*

Důkaz. i. Nejprve dokážeme tranzitivitu relace $<$. Chceme ukázat, že pro všechna $a, b, c \in \mathbb{Z}$ platí $[(a < b) \wedge (b < c)] \Rightarrow (a < c)$. Víme, že $b + (-a) = u$, kde $u \in \mathbb{Z}^+$. Také víme, že $c + (-b) = v$, kde $v \in \mathbb{Z}^+$. K oběma stranám rovnosti $b + (-a) = u$ přičteme číslo $a \in \mathbb{Z}$. Dostaneme $b = u + a$. Do druhé rovnosti dosadíme za b a dostaneme rovnost $c + (-u - a) = v$. K oběma stranám přičteme u. Dostaneme $c - a = v + u$, $v, u \in \mathbb{Z}^+$, proto i součet u a v, který označíme w, je ze $\mathbb{Z}^+$. $c - a = w, w \in \mathbb{Z}^+$, přepíšeme podle definice relace $<$ jako $a < c$.

Relace je tedy tranzitivní.

ii. Nyní ukážeme, že relace $<$ je trichotomická. Chceme ukázat, že pro všechna $a, b \in \mathbb{Z}$ platí právě jedna z možností $a < b, a = b, a > b$. Zajisté platí právě jedna z možností, buď $b+(-a) \in \mathbb{Z}^+$, nebo $a+(-b) \in \mathbb{Z}^+$, a nebo $a+(-b) = 0$.

Relace $<$ je trichotomická

Relace $<$ je uspořádáním na $\mathbb{Z}$. □

Množina $(\mathbb{Z}, <)$ není dobře uspořádaná množina, jelikož nemá nejmenší prvek.

5.7 Celá čísla jako algebraická struktura

Definice 18. Strukturu $(O, +, \cdot)$ nazveme oborem integrity, pokud platí:

- $(O, +)$ je Abelova grupa.
- Násobení je asociativní, komutativní a má neutrální prvek. Násobení je distributivní vzhledem ke sčítání.
- Ve struktuře neexistují dělitelé nuly, tedy platí:

$$\forall a, b \in O : a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0).$$

Věta 22. *Celá čísla spolu s operacemi + a · tvoří obor integrity.*

Důkaz. Podle věty 16 víme, že struktura $(\mathbb{Z}, +)$ tvoří Abelovu grupu. Z definice 15 víme, že pro násobení celých čísel platí stejné vlastnosti jako pro násobení přirozených čísel, tedy asociativita, komutativita, existence neutrálního prvku i distributivita. Stačí ukázat, že v $\mathbb{Z}$ neexistují dělitelé nuly. Chceme ukázat, že pro všechna

$T_{(a,b)}, T_{(c,d)} \in \mathbb{Z}$ platí:

$$\left(T_{(a,b)} \cdot T_{(c,d)} = 0\right) \Rightarrow \left(T_{(a,b)} = 0 \vee T_{(c,d)} = 0\right).$$

Předpokládejme, že $T_{(a,b)} \cdot T_{(c,d)} = 0$ a bez újmy na obecnosti předpokládejme, že $T_{(a,b)} \neq 0$. Chceme ukázat, že pak platí $T_{(c,d)} = 0$. Podle poznámky 20 pro součin celých čísel platí:

$$T_{(a,b)} \cdot T_{(c,d)} = T_{(a\cdot c+b\cdot d, a\cdot d+b\cdot c)}.$$

Z předpokladu víme, že se součin čísel $T_{(a,b)}, T_{(c,d)}$ rovná nule. Proto:

$$T_{(a\cdot c+b\cdot d, a\cdot d+b\cdot c)} = 0.$$

Podle poznámky 18 a věty 19 platí:

$$\left(T_{(a\cdot c+b\cdot d, a\cdot d+b\cdot c)} = 0\right) \Leftrightarrow (a \cdot c + b \cdot d = a \cdot d + b \cdot c).$$

Protože $a \neq b$, je podle věty 7 buď $a > b$, nebo $b > a$.

i) Předpokládejme nejprve, že $a > b$. Pak existuje $k \in \mathbb{N} - \{0\} : a = b + k$. Do rovnosti $a \cdot c + b \cdot d = a \cdot d + b \cdot c$ dosadíme za a:

$$(b + k) \cdot c + b \cdot d = (b + k) \cdot d + b \cdot c.$$

Využijeme distributivitu násobení vzhledem ke sčítání přirozených čísel podle věty 9:

$$b \cdot c + k \cdot c + b \cdot d = b \cdot d + k \cdot d + b \cdot c.$$

Zkrátíme podle věty 5 a dostaneme:

$$k \cdot c = k \cdot d.$$

Protože $k \neq 0$, můžeme použít vlastnost krácení podle věty 9 a dostaneme:

$$c = d.$$

Potom platí $T_{(c,d)} = T_{(c,c)} = 0$, což jsme právě chtěli ukázat.

ii) Nyní předpokládejme, že $b > a$. Pak existuje $k \in \mathbb{N} - \{0\} : b = a + k$. Do rovnosti $a \cdot c + b \cdot d = a \cdot d + b \cdot c$ dosadíme za b:

$$a \cdot c + (a + k) \cdot d = a \cdot d + (a + k) \cdot c.$$

Využijeme distributivitu násobení vzhledem ke sčítání přirozených čísel podle věty 9:

$$a \cdot c + a \cdot d + k \cdot d = a \cdot d + a \cdot c + k \cdot c.$$

Zkrátíme podle věty 5 a dostaneme:

$$k \cdot d = k \cdot c.$$

Protože $k \neq 0$, můžeme použít vlastnost krácení podle věty 9 a dostaneme:

$$d = c.$$

Potom platí $T_{(c,d)} = T_{(c,c)} = 0$, což jsme právě chtěli ukázat.

Na $\mathbb{Z}$ neexistují dělitelé nuly a struktura $(\mathbb{Z}, +, \cdot)$ je obor integrity. $\square$