Čísla

0.1 Obory

Bůh stvořil celá čísla, vše ostatní je dílem člověka.

Leopold Kronecker

Jsou-li podstatou a univerzálním jazykem matematiky čísla, pak je pro další vyjadřování rozumné si některé často užívané soubory (množiny) čísel pojmenovat a přiřadit jim speciální symboly:

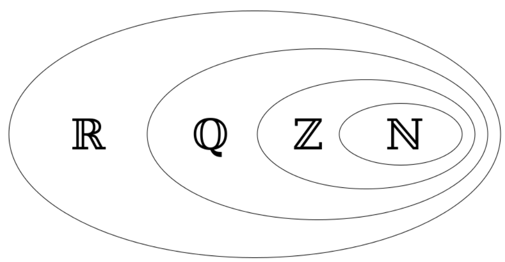
- **přirozená čísla**, $\mathbb{N} = \{1, 2, 3, \ldots\}$ jsou nejstarším nástrojem matematické abstrakce: vznikly jako praktická pomůcka pro zaznamenávání jevů běžného života (počty zvěře, kalendáře, finanční záznamy). S tím souvisí jednoduchost manipulace s přirozenými čísly, avšak na druhou stranu je nebývale složité vymezit, co přirozená čísla *opravdu* jsou.

- **celá čísla**, $\mathbb{Z} = \{\ldots - 3, -2, -1, 0, 1, 2, 3, \ldots\}$ vznikla jako rozšíření přirozených čísel, aby bylo možné vyjadřovat nedostatek (např. pro vyjádření dluhů, tedy již zcela abstraktní myšlenku); z matematického hlediska je tato idea vyjádřena tak, že $\mathbb{Z}$ jsou na rozdíl od $\mathbb{N}$ uzavřená na odčítání, tj. rozdíl libovolných dvou celých čísel je opět celé číslo

- **racionální čísla**, $\mathbb{Q} = \left\{ \frac{a}{b} \,|\, \text{pro celá čísla}\, a, b \in \mathbb{Z}, b \neq 0 \right\}$ vyjadřují části a podíly (přirozených nebo celých čísel a objektů, které reprezentují); každé racionální číslo lze vyjádřit pomocí desetinného čísla s konečným nebo periodickým rozvojem; zajímavým a nečekaným faktem je, že racionálních čísel je stejně jako přirozených

- **reálná čísla**, $\mathbb{R}$ jsou racionální čísla doplněná na úplnou přímku, čímž v mnoha ohledech dostačují popisu fyzického světa matematickými nástroji
- **iracionální čísla**, $\mathbb{I} = \{\pi, e, \sqrt{p} \text{ pro prvočíslo } p\}$ jsou ta reálná čísla, která nejsou racionální; jejich název napovídá, že byla původně „nesmyslná, nepochopitelná“, což souviselo s Pythagorejským pojetím světa a tzv. První krizí matematiky

V tomto pojetí skoro každý nový obor rozšiřuje předcházející, tudíž prvky původního souboru zároveň náležejí do souborů nově vzniklých. Schematicky lze situaci vystihnout například následujícím diagramem:



zdroj: commons.wikimedia.org

Uvedené rozdělení není ani zdaleka úplné a lze na základě zkoumaných vlastností uvažovat i další významné soubory čísel, např. prvočísla, desetinná čísla, algebraická čísla, transcendentní čísla, p-adická čísla atd.

Otázky:

1. *Co* je číslo 2? Jak byste jej popsali návštěvníkovi z amazonského kmene Munduruku (jazyk tohoto kmene nezná čísla, natož přesné pojmy množství, má pouze slova pro „málo“, „několik“ ap.)?

2. Značky $\mathbb{N}, \mathbb{Q}$ a $\mathbb{R}$ odpovídají latinským slovům *naturalis*, *quotiens* a *res*, z nichž vycházejí jejich anglické, resp. francouzské názvy. Kde se vzalo písmeno $\mathbb{Z}$ označující celá čísla?

3. Pro který obor neplatí, že rozšiřuje původní obory, tudíž neobsahuje prvky dříve definovaných oborů?

4. Základní operací na přirozených číslech je sčítání $(+)$, při jejím provádění se nemůže stát, že bychom se dostali mimo přirozená čísla. Jaké další operace lze takto v $\mathbb{N}$ provádět? Jaké operace lze provádět na jiných oborech?

5. Je 0 přirozené číslo? Proč?

Polynomy

Polynom je jakýkoli výraz tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$

Prvkům a_i říkáme **koeficienty** a obvykle jde o reálná čísla, ale možné jsou i jiné případy. Číslu n říkáme **stupeň polynomu** a v případě polynomu 0 definujeme jeho stupeň jako -1 (někdy $-\infty$). Prvku $a_n x^n$ říkáme **vedoucí člen**, prvku a_0 **absolutní člen**.

Příklady polynomů jsou třeba $-2x^{12} + 5x^4 - 3$, $\frac{7}{5}x^5 - \sqrt{3}x^3 + \pi$, $-12x$ nebo 7 a jejich stupně jsou postupně 12, 5, 1, a 0, jejich vedoucí členy $-2x^{12}$, $\frac{7}{5}x^5$, $-12x$ a 7 a jejich absolutní členy -3, π, 0 a 7.

0.2 Dělení polynomů

Dva polynomy mezi sebou umíme dobře sečíst, odečíst a vynásobit a jako výsledek dostaneme vždy nějaké další polynomy. Obecně ale neumíme mezi sebou dva polynomy vydělit tak, abychom opět dostali polynom, za příklad může sloužit podíl polynomů 1 a $x - 3$: zlomek $\frac{1}{x-3}$ totiž nemá tvar, jak jsme definovali v úvodu, a není tedy polynomem. Jediné, co nám zbývá, je polynomy dělit se zbytkem[1].

Jak tedy polynomy dělíme? Vysvětlíme si na příkladu dělení polynomu $P(x) = 2x^3 + 7x^2 - x - 25$ polynomem $Q(x) = 2x - 3$. Počítáme tedy

$$\left(2x^3 + 7x^2 - x - 25\right) : (2x - 3)$$

[1] Rozmyslete si, jak je v tomto chování polynomů podobné chování celých čísel.

krok 1 vydělíme vedoucí člen polynomu $P(x)$ vedoucím členem polynomu $Q(x)$, tedy $\frac{2x^3}{2x} = x^2$

$$\left(2x^3 + 7x^2 - x - 25\right) : (2x - 3) = x^2$$

krok 2 získaným podílem x^2 vynásobíme zpět polynom $Q(x)$ a výsledek odečteme od $P(x)$

$$\begin{array}{l}
(2x^3 + 7x^2 - x - 25) : (2x - 3) = x^2 \\
\underline{-(2x^3 - 3x^2)} \\
\qquad 10x^2 - x - 25
\end{array}$$

krok 3 opakujeme krok 1, ale teď s dvojicí polynomů $10x^2 - x - 25$ a $2x - 3$ (dělíme tedy jejich vedoucí členy, $\frac{10x^2}{2x} = 5x$)

$$\begin{array}{l}
(2x^3 + 7x^2 - x - 25) : (2x - 3) = x^2 + 5x \\
\underline{-(2x^3 - 3x^2)} \\
\qquad 10x^2 - x - 25
\end{array}$$

krok 4 opakujeme krok 2 s novým podílem $5x$

$$\begin{array}{l}
(2x^3 + 7x^2 - x - 25) : (2x - 3) = x^2 + 5x \\
\underline{-(2x^3 - 3x^2)} \\
\qquad 10x^2 - x - 25 \\
\quad \underline{-\left(10x^2 - 15x\right)} \\
\qquad\qquad 14x - 25
\end{array}$$

krok 5 opakujeme krok 1, teď s dvojicí $14x - 25$ a $2x - 3$ (dělíme opět jejich vedoucí členy, $\frac{14x}{2x} = +7$)

$$\begin{array}{l}
(2x^3 + 7x^2 - x - 25) : (2x - 3) = x^2 + 5x + 7 \\
\underline{-(2x^3 - 3x^2)} \\
\qquad 10x^2 - x - 25 \\
\quad \underline{-\left(10x^2 - 15x\right)} \\
\qquad\qquad 14x - 25
\end{array}$$

krok 6 opakujeme krok 2 s novým podílem 7

$$\begin{array}{l}(2x^3+7x^2-x-25):(2x-3)=x^2+5x+7\\ \underline{-(2x^3-3x^2)}\\ \quad 10x^2-x-25\\ \quad \underline{-\left(10x^2-15x\right)}\\ \qquad 14x-25\\ \qquad \underline{-(14x-21)}\\ \qquad\quad -4\end{array}$$

Protože polynom -4 již nelze polynomem $2x-3$ dělit, je postup u konce a zjistili jsme, že platí rovnost

$$2x^3+7x^2-x-25=\left(x^2+5x+7\right)\cdot(2x-3)-4.$$

Polynomu x^2+5x+7 v tomto případě říkáme **kvocient** a polynomu -4 **zbytek**. Důležitým faktem je, že zbytek má stupeň nižší než je stupeň dělitele, v tomto případě má dělitel stupeň 1, kdežto zbytek má stupeň 0.

Obecně lze algoritmus dělení polynomů zapsat takto:

`Vstup: polynomy` $P(x), Q(x)$, `stupeň` $P(x) \geq$ `stupeň` $Q(x)$

$R(x)=P(x); K(x)=0; A(x)=0$

`WHILE stupeň` $R(x) \geq$ `stupeň` $Q(x)$ `DO` :

$$A(x)=\frac{\texttt{vedoucí člen } R(x)}{\texttt{vedoucí člen } Q(x)}$$

$K(x)=K(x)+A(x)$

$R(x)=R(x)-A(x)\cdot Q(x)$

`Výstup: polynomy` $K(x), R(x)$ `takové, že platí: stupeň` $R(x) \leq$ `stupeň` $Q(x)$ `a`

$P(x)=K(x)\cdot Q(x)+R(x)$

0.2.1 Otázky:

1. Vydělte se zbytkem polynomy:

(a) $\left(x^3 - 4x^2 + 2x + 5\right) : (x - 2)$
(b) $\left(12x^3 - 11x + 9x + 18\right) : (4x + 3)$
(c) $\left(2x^5 + x^4 - 6x + 9\right) : \left(x^2 - 3x + 1\right)$

0.3 Hledání kořenů polynomů

Kořen polynomu $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ je takové číslo t, pro které platí $P(t) = 0$, tedy po jeho dosazení za x dostáváme nulu.

Důležitým faktem je, že pokud je číslo t kořenem polynomu $P(x)$, pak lze psát $P(x) = (x - t) \cdot P'(x)$, kde P' je nějaký polynom stupně o 1 menšího než je stupeň $P(x)$. Z toho ihned plyne, že polynom stupně n může mít nanejvýš n kořenů.

V případě reálného polynomu stupně dva, tj. polynomu tvaru $ax^2 + bx + c$ se hledání kořenů x_1 a x_2 redukuje na použití vzorce

$$x_{1,2} = \frac{-b \pm \sqrt{b^{-}4ac}}{2a},$$

resp. na využití Viètových vzorců

$$x_1 + x_2 = -\frac{b}{a} \qquad\qquad x_1 \cdot x_2 = \frac{c}{a}.$$

Dle předchozího odstavce pak platí, že polynom $ax^2 + bx + c$ můžeme napsat jako $a(x - x_1)(x - x_2)$.

V každém případě máme pro polynomy stupně 2 máme jasný postup, jak jejich kořeny najít, nebo se přesvědčit, že neexistují. S polynomy vyšších stupňů je situace složitější: pro stupně 3 a 4 existují analogie k výše uvedeným vzorcům, ale jejich užití je technicky velice složité. Pro stupně 5 a vyšší je dokonce dokázáno, že žádné obecné vzorce využívající běžné operace existovat nemohou[2]!

Pokud tedy máme polynom vyššího stupně, jak nalézt jeho kořen(y)? V případě polynomu s celočíselnými koeficienty lze využít následující věty:

Pro racionální číslo $\frac{p}{q}$, které je kořenem polynomu
$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$

[2] Jde o tzv. Abelovu-Ruffiniho větu, resp. Galoisovu teorii

s celočíselnými koeficienty, platí, že $p|a_0$ a $q|a_n$.

Například pro polynom $4x^7 + 5x^5 - 12x^4 + 6$ tedy p může být jedině $\pm1, \pm2, \pm3, \pm6$ a q jedině $\pm1, \pm2, \pm4$ a příslušné racionální kořeny mohou být jedině jejich kombinace; těch je sice 24, ale v principu je možné všechny vyzkoušet např. dosazením.

Uvedené tvrzení je možné použít i pro polynomy s racionálními koeficienty: označíme d nejmenší společný násobek čitatelů koeficientů polynomu $R(x)$; pak je $R' = d \cdot R(x)$ polynom s celočíselnými koeficienty a jeho kořeny jsou stejné jako u polynomu $R(x)$. Tedy v místo polynomu $R(x) = \frac{2}{3}x^5 + \frac{1}{7}x^3 - 3x + \frac{3}{2}$ je $d = 42$, a můžeme tedy pracovat s polynomem $R'(x) = 42 \cdot R(x) = 28x^5 + 6x^3 - 116x + 63$.

0.3.1 Otázky:

1. Zkuste dokázat fakt, že pokud je t kořenem polynomu $P(x)$, pak lze psát $P(x) = (x - t) \cdot P'(x)$, kde P' je nějaký polynom.
2. Zkuste s využitím předchozího bodu dokázat, že polynom stupně n může mít nanejvýš n kořenů.
3. Které polynomy stupně jedna mají kořen? Jak jej najdeme?
4. Existuje polynom stupně nula, který má kořen?
5. Jaké racionální kořeny může mít polynom $3x^3 + 16x^2 - 33x + 14$?

0.4 Hornerovo schéma

Běžným problémem, například (ale nejen) při testování, zda je číslo c kořenem polynomu $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, je nutné zjistit hodnotu $P(c)$. To je samozřejmě možné provést přímým dosazením, aneb spočtením výrazu $a_n c^n + a_{n-1}c^{n-1} + \ldots + a_1 c + a_0$.

Existuje však rychlejší metoda, která má některé další užitečné vlastnosti, tzv. *Hornerovo schéma*, které funguje na základě myšlenky, že polynom

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

je možné zapsat i ve tvaru

$$x\left(\cdots\left(x\left(x\left(a_n x + a_{n-1}\right) + a_{n-2}\right) + \cdots\right) + a_1\right) + a_0.$$

Při výpočtu pomocí Hornerova schématu pak postupně vyhodnocujeme jednotlivé závorky, což nám (jak uvidíme) ušetří mnoho výpočtů. Jeho princip si ukážeme na příkladu výpočtu hodnoty $P(-1)$ pro polynom $6x^6 + 5x^5 + 4x^4 + 3x^3 + 2x^2 + x - 3$:

krok 1 Připravíme si schéma: v jejím prvním řádku jsou koeficienty polynomu $P(x)$ v pořadí $a_n, a_{n-1}, a_{n-2} \ldots a_1, a_0$ a do prvního pole druhého řádku zapíšeme číslo, ve kterém polynom vyhodnocujeme:

	6	5	4	3	2	1	-3
-1							

krok 2 do druhého pole druhého řádku opíšeme číslo nad ním

	6	5	4	3	2	1	-3
-1	6						

krok 3 do třetího pole druhého řádku napíšeme číslo, které je součtem součinu vedlejších dvou polí a čísla nad ním, tj. $(-1) \cdot 6 + 5 = -1$

	6	5	4	3	2	1	-3
-1	6	-1					

krok 4 stejně jako v kroku 3 pokračujeme až do konce řádku:

- $(-1) \cdot (-1) + 4 = 5$

	6	5	4	3	2	1	-3
-1	6	-1	5				

- $(-1) \cdot (5) + 3 = -2$

	6	5	4	3	2	1	-3
-1	6	-1	5	-2			

- $(-1) \cdot (-2) + 2 = 4$

	6	5	4	3	2	1	-3
-1	6	-1	5	-2	4		

- $(-1) \cdot (4) + 1 = -3$

	6	5	4	3	2	1	-3
-1	6	-1	5	-2	4	-3	

- $(-1) \cdot (-3) - 3 = 0$

	6	5	4	3	2	1	-3
-1	6	-1	5	-2	4	-3	0

krok 5 V posledním poli druhého řádku je hodnota $P(-1)$.

	6	5	4	3	2	1	-3
-1	6	-1	5	-2	4	-3	0

Zjistili jsme tedy, že číslo -1 je kořenem tohoto polynomu. Pro hledání dalších kořenů by bylo nejvýhodnější vydělit $P(x)$ polynomem $x+1$ a pracovat s polynomem $Q(x)$ stupně o jedna nižším. Hornerovo schéma však tuto informaci dává okamžitě: čísla v druhém řádku jsou totiž koeficienty tohoto polynomu, platí tedy

$$P(x) = (x+1) \cdot \left(6x^5 - 1x^4 + 5x^3 - 2x^2 + 4x - 3\right).$$

Tento fakt platí obecně i pro čísla, která nejsou kořenem polynomu, a je tedy možné Hornerovo schéma využívat pro dělení lineárním polynomem, např. takto: chceme-li vydělit náš polynom $P(x)$ polynomem $x+2$, vypočítáme tabulku pro číslo -2:

	6	5	4	3	2	1	-3
-2	6	-7	18	-33	68	-135	267

Dostáváme tedy, že platí rovnost

$$P(x) = (x+2) \cdot \left(6x^5 - 7x^4 + 18x^3 - 33x^2 + 68x - 135\right) + 267.$$

Efektivita Hornerova schématu V případě zjišťování hodnoty $P(c)$ přímým dosazením, tedy spočtením výrazu

$$a_n c^n + a_{n-1} c^{n-1} + \ldots + a_1 c + a_0$$

je obecně potřeba $\frac{n(n+1)}{2}$ násobení a n sčítání (rozmyslete si proč). Pokud použijeme Hornerovo schéma, je potřeba pouze n násobení a n sčítání, tedy tento algoritmus šetří čas. Je dokonce možné ukázat, že pro reálné polynomy neexistuje rychlejší algoritmus na vyhodnocování, a Hornerovo schéma je tedy optimální metodou.

0.4.1 Otázky:

1. Zapište polynom $6x^6 + 5x^5 + 4x^4 + 3x^3 + 2x^2 + x - 3$ ve tvaru $x(\cdots(x(x(a_n x + a_{n-1}) + a_{n-2}) + \cdots) + a_1) + a_0$.
2. Určete hodnoty $P(c)$ pro $c \in \{1, \pm 3\}$, kde $P(x)$ je polynom z předchozího cvičení. Je některé z těchto čísel kořenem?
3. Vydělte pomocí Hornerova schématu polynom $6x^5 - 7x^4 + 18x^3 - 33x^2 + 68x - 135$ polynomem $x - 1$.

Odpovědi

Oddíl 0.1

2. $\mathbb{Z}$ pochází z německého *zahlen*; více na `http://jeff560.tripod.com/nth.html`
3. iracionální čísla, jsou totiž definována jako množinový doplněk (platí $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$)
4. na $\mathbb{N}$: z klasických násobení, mocnění ap. (což jsou jen iterace sčítání, resp. násobení), nelze provádět odčítání, dělení atd.

Oddíl 0.2.1

1. (a) $x^2 - 2x - 2$, zbytek 1
   (b) $3x^2 - 5x + 6$, zbytek 0
   (c) $2x^3 + 7x^2 + 19x + 50$, zbytek $125x - 41$

Oddíl 0.3.1

3. všechny, polynom $x + c$ má kořen $-c$
4. žádný; jediným kandidátem by byl polynom 0, ale ten má stupeň -1
5. $\frac{p}{q}$, kde $p \in \{\pm 1, \pm 2, \pm 7, \pm 14\}$ a $q \in [\pm 1, \pm 3\}$

Oddíl 0.4.1

1. $x\,(x\,(x\,(x\,(x\,(6x + 5) + 4) + 3) + 2) + 1) - 3$
2. $P\,(1) = 18$, $P\,(3) = 6012$, $P\,(-3) = 3114$
3. $6x^4 - x3 + 17x^2 - 16x + 52$, zbytek -83