

Něco málo z aritmetiky

Jindřich Bečvář

Praha, 16. září 2025

becvar@karlin.mff.cuni.cz
www.karlin.mff.cuni.cz/~becvar

Aritmetika

- Věda o číslech, o číselných oborech, o operacích s čísly a o jejich vlastnostech.

Aritmetika

- Věda o číslech, o číselných oborech, o operacích s čísly a o jejich vlastnostech.
- V dnešní škole je aritmetika značně opomíjená,

Aritmetika

- Věda o číslech, o číselných oborech, o operacích s čísly a o jejich vlastnostech.
- V dnešní škole je aritmetika značně opomíjená, stejně jako geometrie, zejména stereometrie,

Aritmetika

- Věda o číslech, o číselných oborech, o operacích s čísly a o jejich vlastnostech.
- V dnešní škole je aritmetika značně opomíjená, stejně jako geometrie, zejména stereometrie, stejně jako trigonometrie, algebra,

Aritmetika

- Věda o číslech, o číselných oborech, o operacích s čísly a o jejich vlastnostech.
- V dnešní škole je aritmetika značně opomíjená, stejně jako geometrie, zejména stereometrie, stejně jako trigonometrie, algebra, stejně jako pravděpodobnost, statistika, kombinatorika,

Aritmetika

- Věda o číslech, o číselných oborech, o operacích s čísly a o jejich vlastnostech.
- V dnešní škole je aritmetika značně opomíjená, stejně jako geometrie, zejména stereometrie, stejně jako trigonometrie, algebra, stejně jako pravděpodobnost, statistika, kombinatorika, stejně jako fyzika, chemie, biologie, čeština, dějepis,

Aritmetika

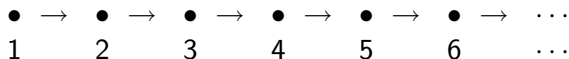
- Věda o číslech, o číselných oborech, o operacích s čísly a o jejich vlastnostech.
- V dnešní škole je aritmetika značně opomíjená, stejně jako geometrie, zejména stereometrie, stejně jako trigonometrie, algebra, stejně jako pravděpodobnost, statistika, kombinatorika, stejně jako fyzika, chemie, biologie, čeština, dějepis, stejně jako tělesná výchova, výtvarná výchova, ...

Aritmetika

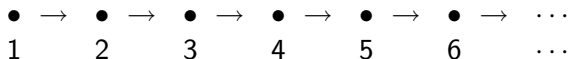
- Věda o číslech, o číselných oborech, o operacích s čísly a o jejich vlastnostech.
- V dnešní škole je aritmetika značně opomíjená, stejně jako geometrie, zejména stereometrie, stejně jako trigonometrie, algebra, stejně jako pravděpodobnost, statistika, kombinatorika, stejně jako fyzika, chemie, biologie, čeština, dějepis, stejně jako tělesná výchova, výtvarná výchova, ... stejně jako výchova morálně volných vlastností.

Přirozená čísla

- Přirozená čísla můžeme vnímat jako
 - nikde nekončící proces,
 - nekonečný průvod,
 - nekonečné stromořadí,
 - posloupnost atd.
- Tato představa je do značné míry ve sporu s naší konečností, přesahuje nás ... [Dítě: *Čísla začínají, ale nekončí!*]



- Přirozená čísla jsou úplně uspořádanou množinou.



Množinu přirozených čísel $\mathbb{N}$ dobře popisují Peanovy axiomy:

- Číslo 1 je přirozené, tj. $1 \in \mathbb{N}$.
- Každé přirozené číslo n má následníka $s(n) \in \mathbb{N}$.
- Neexistuje přirozené číslo, jehož následníkem je 1, tj. $\forall n \in \mathbb{N} \quad s(n) \neq 1$.
- Různá přirozená čísla mají různé následníky, tj. $n \neq m \implies s(n) \neq s(m)$.
- Princip matematické indukce:
jestliže pro $X \subseteq \mathbb{N}$ platí

$$1 \in X,$$

$$n \in X \implies s(n) \in X,$$

potom je $X = \mathbb{N}$.

Dva ekvivalentní principy:

- Princip matematické indukce.
- Princip dobrého uspořádání: *Každá neprázdna podmnožina množiny $\mathbb{N}$ obsahuje nejmenší prvek.*

Další důležitá skutečnost (důsledek):

- *Každá omezená množina přirozených čísel má největší prvek.*

- Giuseppe Peano (1858–1932):

Arithmetices principia, nova methodo exposita,
Torino, 1889, xvi+20

- Richard Julius Wilhelm Dedekind (1831–1916):

Was sind und was sollen die Zahlen?,
Braunschweig, 1888, xix+58 stran

*Die Zahlen sind freie Schöpfungen des menschlichen Geistes,
sie dienen als ein Mittel, um die Verschiedenheit der Dinge
leichter und schärfer aufzufassen.*

- Leopold Kronecker (1823–1891)

Roku 1886 na schůzi berlínských přírodovědců:

*Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist
Menschenwerk.*

■ Dělitelnost v oboru přirozených čísel

- **Definice.** Jestliže je $a = bc$, říkáme, že b dělí a a že a je násobkem b . Píšeme $b|a$.

Uvažujme množinu všech společných dělitelů čísel $a_1, a_2, \dots, a_k$.

Ta je omezená, existuje tedy tzv. *největší společný dělitel* čísel $a_1, a_2, \dots, a_k$.

Uvažujme množinu všech společných násobků čísel $a_1, a_2, \dots, a_k$.

Ta je neprázdná, má tedy nejmenší prvek, tzv. *nejmenší společný násobek* čísel $a_1, a_2, \dots, a_k$.

- **Definice.** *Prvočíslem* rozumíme přirozené číslo p , které má právě dva dělitele, číslo 1 a číslo p .
Čísla, která mají více dělitelů, se nazývají *složená*.
- Prvočísla menší než 100:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.
- Složená čísla jsou:
4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 atd.
- Stranou stojí číslo 1.

Věta. Každé přirozené číslo větší než 1 má prvočíselného dělitele.

Důkaz. Sporem. Necht' M je množina všech přirozených čísel, pro která to neplatí, a m její nejmenší prvek. Protože m není prvočíslo, je $m = m_1 \cdot m_2$, kde $m_1 < m$ a $m_2 < m$. Číslo $m_1 \notin M$ má prvočíselného dělitele, který je rovněž dělitelem čísla m . Spor.

Věta. Každé přirozené číslo je součinem prvočísel (nebo je prvočíslem).

Důkaz. Sporem. Necht' M je množina všech přirozených čísel, pro která to neplatí, a m její nejmenší prvek. Protože m není prvočíslo, je $m = m_1 \cdot m_2$, kde $m_1 < m$ a $m_2 < m$. Čísla $m_1 \notin M$, $m_2 \notin M$ jsou součiny prvočísel, tedy m je rovněž součinem prvočísel. Spor.

Číslo 1 je součinem nulového počtu prvočísel (prázdný součin).

Věta. Prvočísel je nekonečně mnoho.

Důkaz. Sporem. Necht' $p_1, \dots, p_k$ jsou všechna prvočísla.

Přirozené číslo

$$n = p_1 \cdots p_k + 1$$

má podle předchozího prvočíselného dělitele, ale není dělitelné žádným z prvočísel $p_1, \dots, p_k$. To je spor.

Modifikovaný důkaz. Ukážeme, že ke každému prvočíslu p existuje prvočíslu, které je větší.

Uvažujme číslo

$$p! + 1.$$

Podle předchozího má prvočíselného dělitele, který musí být větší než prvočíslu p .

Jiný důkaz. Uvažujme Fermatova čísla

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, \dots$$

Zřejmě je pro $t > 0$

$$F_{n+t} - 1 = (F_n - 1)^{2^t}, \quad \text{je totiž} \quad 2^{2^{n+t}} = \left(2^{2^n}\right)^{2^t}.$$

Tedy $F_{n+t} = a \cdot F_n + 2$. Prvočíslo $p \neq 2$, které dělí F_n , nemůže dělit žádné další F_{n+t} .

Poznámka. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$.

Fermat předpokládal, že jsou $F_0, F_1, F_2, \dots$ prvočísla. Euler ukázal, že F_5 je dělitelné číslem 641:

$$\begin{aligned} 2^{32} &= 2^2(2^{10})^3 = 4(1\,024)^3 = 4(641 + 383)^3 = 4(641a + 383^3) = \\ &= 4(641a + 56\,181\,887) = 4(641a + 641 \cdot 87\,647 + 160) = 641b + 640. \end{aligned}$$

Uvažujme na množině $\mathbb{N}$ uspořádání $a \preccurlyeq b$ definované vztahem $a|b$.

Ke každým dvěma přirozeným číslům a, b existuje jejich největší společný dělitel $a \wedge b = d(a, b)$

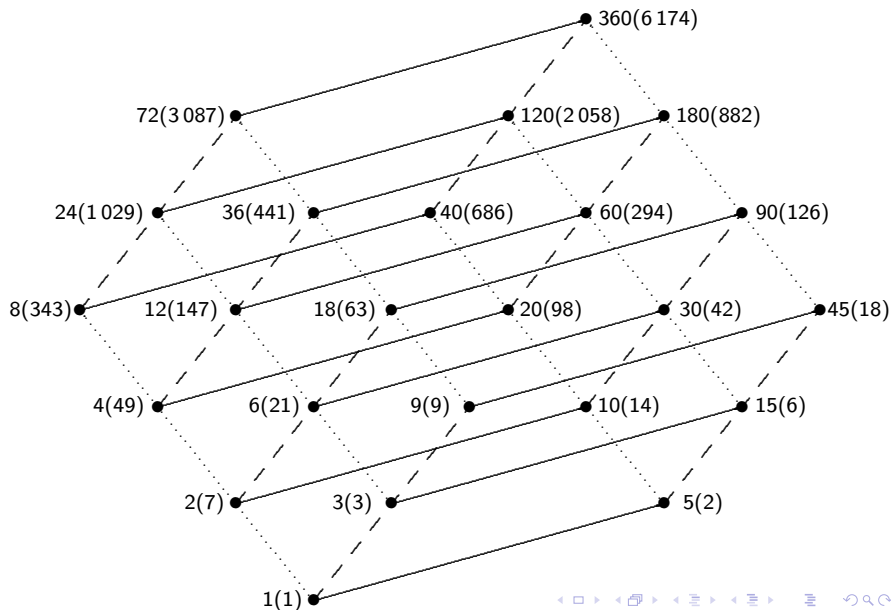
a nejmenší společný násobek $a \vee b = n(a, b)$.

Vzhledem k těmto operacím, které jsou asociativní a komutativní, tvoří přirozená čísla *svaz*, neboť navíc platí *zákon absorbce*:

$$a \wedge (a \vee b) = a \vee (a \wedge b) = a.$$

Každé přirozené číslo definuje jeho podsvaz.

Pro čísla $360 = 2^3 \cdot 3^2 \cdot 5$ (resp. $6174 = 7^3 \cdot 3^2 \cdot 2$) tento podsvaz vypadá takto:



Celá čísla

Řada poznatků se přenesla z oboru přirozených čísel do *oboru integrity* celých čísel. Snadno se rozšíří dělitelnost.

Věta (dělení se zbytkem). Necht' $b \in \mathbb{N}$. Pro každé celé číslo $a \in \mathbb{Z}$ existují jednoznačně určená celá čísla q a r , pro která

$$a = bq + r, \quad \text{kde} \quad 0 \leq r < b.$$

Důkaz. Množina $\mathbb{Z}$ se rozpadne na disjunktní množiny

$$\begin{aligned} \dots, \{-b, \dots, -1\}, \{0, \dots, b-1\}, \{b, \dots, 2b-1\}, \\ \{2b, \dots, 3b-1\}, \dots, \{qb, \dots, (q+1)b-1\}, \dots \end{aligned}$$

Číslo a leží právě v jedné z nich.

Eukleidův algoritmus. Nechť $a > b$ jsou přirozená čísla.

Následující posloupnost celočíselných dělení je konečná:

$$a = bq_0 + r_0, \quad \text{kde} \quad 0 \leq r_0 < b,$$

$$b = r_0q_1 + r_1, \quad \text{kde} \quad 0 \leq r_1 < r_0 \quad (\text{je-li } 0 < r_0),$$

$$r_0 = r_1q_2 + r_2, \quad \text{kde} \quad 0 \leq r_2 < r_1 \quad (\text{je-li } 0 < r_1),$$

$$\dots$$
$$\dots$$

$$r_{k-2} = r_{k-1}q_k + r_k, \quad \text{kde} \quad 0 \leq r_k < r_{k-1} \quad (\text{je-li } 0 < r_{k-1}),$$

$$r_{k-1} = r_kq_{k+1}.$$

Přitom je $r_k = d(a, b)$ a existují celá čísla u, v taková, že

$$d(a, b) = u \cdot a + v \cdot b.$$

Důkaz. Posloupnost přirozených čísel $r_0 > r_1 > \dots > 0$ je klesající, a tedy konečná. Ostatní je zjevné.

Důsledek. Jsou-li čísla a, b nesoudělná, existují celá čísla u, v taková, že

$$1 = au + bv.$$

Eukleidovo lemma. Jestliže prvočíslo p dělí součin ab , pak dělí buď číslo a nebo číslo b .

Důkaz. Jestliže p nedělí a , jsou tato čísla nesoudělná. Existují celá čísla u, v , pro něž

$$1 = au + pv$$

Odtud

$$b = abu + pbv,$$

p dělí pravou stranu, a tedy dělí i levou stranu.

Základní věta aritmetiky. Každé přirozené číslo n lze jediným způsobem vyjádřit ve tvaru

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot \dots \cdot p_s^{k_s},$$

kde $p_1 < p_2 < p_3 < \dots < p_s$ jsou prvočísla a $k_1, k_2, k_3, \dots, k_s$ přirozená čísla.

Důkaz. Existence rozkladu již byla dokázána, jednoznačnost plyne z Eukleidova lemmatu.

Poznámka. Pro celá čísla přibude případně znaménko.

Gaussova celá čísla

$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ – mřížové body v Gaussově rovině
(čtvercová síť)

Norma: $N(a + bi) = a^2 + b^2$

Platí: $N(0) = 0$, $N(\alpha) \in \mathbb{N}$ pro $\alpha \neq 0$

Zákon normy: $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$ (homomorfismus)

Důkaz: Pro $\alpha = a + bi$, $\beta = c + di$ je

$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2) \cdot (c^2 + d^2).$$

Invertibilní prvky: $\alpha \cdot \alpha^{-1} = 1$, tedy $N(\alpha) \cdot N(\alpha^{-1}) = N(1) = 1$,
tedy $N(\alpha) = 1$, tedy $\alpha = \pm 1, \pm i$

Která čísla x mohou být normou nějakého Gaussova celého čísla?

$$a^2 + b^2 = x \quad (\text{symetrické vzhledem k } a \text{ a } b)$$

	$a^2 = 0$	1	4	9	16	25	36	49	64	81	100	...
$b = 0$	$x = 0$	1	4	9	16	25	36	49	64	81	100	...
$b = 1$		2	5	10	17	26	37	50	65	82	101	...
$b = 2$			8	13	20	29	40	53	68	85	104	...
$b = 3$				18	25	34	45	58	73	90	109	...
$b = 4$					32	41	52	65	80	97	116	...
$b = 5$						50	61	74	89	106	125	...
$b = 6$							72	85	100	117	136	...
$b = 7$								98	113	130	149	...
$b = 8$									128	145	164	...
$b = 9$										162	181	...
$b = 10$											200	...

Normy Gaussových čísel tvoří množinu

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

Nerozložitelná Gaussova čísla: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, ...

$N(3) = 9$,	číslo	$9 = 3^2$	nelze rozložit v množině $\mathcal{B}$
$N(7) = 49$,	číslo	$49 = 7^2$	nelze rozložit v množině $\mathcal{B}$
$N(11) = 121$,	číslo	$121 = 11^2$	nelze rozložit v množině $\mathcal{B}$
$N(19) = 361$,	číslo	$361 = 19^2$	nelze rozložit v množině $\mathcal{B}$
$N(23) = 529$,	číslo	$529 = 23^2$	nelze rozložit v množině $\mathcal{B}$
$N(31) = 961$,	číslo	$961 = 31^2$	nelze rozložit v množině $\mathcal{B}$

Další nerozložitelná čísla: $1 \pm i, 2 \pm i, 3 \pm 2i, 4 \pm i, 5 \pm 2i, 5 \pm 4i,$
 $6 \pm i, 6 \pm 5i, 7 \pm 2i, 8 \pm 3i, 8 \pm 5i, 9 \pm 4i, \dots$

$N(1 \pm i) = 2,$	číslo 2	nelze rozložit v množině $\mathcal{B}$
$N(2 \pm i) = 5,$	číslo 5	nelze rozložit v množině $\mathcal{B}$
$N(3 \pm 2i) = 13,$	číslo 13	nelze rozložit v množině $\mathcal{B}$
$N(4 \pm i) = 17,$	číslo 17	nelze rozložit v množině $\mathcal{B}$
$N(5 \pm 2i) = 29,$	číslo 29	nelze rozložit v množině $\mathcal{B}$
$N(6 \pm i) = 37,$	číslo 37	nelze rozložit v množině $\mathcal{B}$
$N(5 \pm 4i) = 41,$	číslo 41	nelze rozložit v množině $\mathcal{B}$
$N(7 \pm 2i) = 53,$	číslo 53	nelze rozložit v množině $\mathcal{B}$
$N(6 \pm 5i) = 61,$	číslo 61	nelze rozložit v množině $\mathcal{B}$
$N(8 \pm 3i) = 73,$	číslo 73	nelze rozložit v množině $\mathcal{B}$
$N(8 \pm 5i) = 89,$	číslo 89	nelze rozložit v množině $\mathcal{B}$
$N(9 \pm 4i) = 97,$	číslo 97	nelze rozložit v množině $\mathcal{B}$

Rozložitelná Gaussova čísla: 2, 5, 13, 17, 29, 37, 41, 53, 61, 73,
89, 97, ...

$$\begin{aligned}
 2 &= (1 + i)(1 - i), & \text{tomu odpovídá rozklad } N(2) &= 4 = 2^2 \\
 5 &= (2 + i)(2 - i), & \text{tomu odpovídá rozklad } N(5) &= 25 = 5^2 \\
 13 &= (3 + 2i)(3 - 2i), & \text{tomu odpovídá rozklad } N(13) &= 169 = 13^2 \\
 17 &= (4 + i)(4 - i), & \text{tomu odpovídá rozklad } N(17) &= 289 = 17^2 \\
 29 &= (5 + 2i)(5 - 2i), & \text{tomu odpovídá rozklad } N(29) &= 841 = 29^2
 \end{aligned}$$

Další rozložitelná čísla: $3 \pm i$, $4 \pm 3i$, $5 \pm i$, $5 \pm 3i$, $7 \pm i$, $7 \pm 3i$,
 $7 \pm 4i$, $7 \pm 5i$, $7 \pm 6i$, $8 \pm i$, ...

$$\begin{aligned}
 3 + i &= (1 + i)(2 - i), & \dots \text{ rozklad } N(3 \pm i) &= 10 = 2 \cdot 5 \\
 4 + 3i &= (2 - i)(1 + 2i), & \dots \text{ rozklad } N(4 \pm 3i) &= 25 = 5^2 \\
 5 + i &= (1 + i)(3 - 2i), & \dots \text{ rozklad } N(5 \pm i) &= 26 = 2 \cdot 13 \\
 5 + 3i &= (1 + i)(4 - i), & \dots \text{ rozklad } N(5 \pm 3i) &= 34 = 2 \cdot 17 \\
 7 + i &= (1 - i)(2 + i)^2, & \dots \text{ rozklad } N(7 \pm i) &= 50 = 2 \cdot 5^2
 \end{aligned}$$

Rekapitulace:

Původní prvočísla $p \in \mathbb{P}$ tvaru $p = 4k + 1$ jsou v $\mathbb{Z}[i]$ **rozložitelná**. Je jich nekonečně mnoho. [Fermat: Každé prvočíslo tvaru $4k + 1$ je součtem dvou čtverců.]

Původní prvočísla $p \in \mathbb{P}$ tvaru $p = 4k + 3$ jsou v $\mathbb{Z}[i]$ **nerozložitelná**. Je jich rovněž nekonečně mnoho.

Navíc jsou v $\mathbb{Z}[i]$ další nerozložitelná čísla (prvočísla).

Jednoznačnost rozkladu (až na asociovanost):

$$5 = (2+i)(2-i) = (1-2i)(1+2i) \quad [\text{jako v } \mathbb{Z} : 6 = 2 \cdot 3 = (-2) \cdot (-3)]$$

$$(2+i) \cdot [(-i) \cdot i] \cdot (2-i) = (1-2i)(1+2i)$$

Nerozložitelná čísla mají vlastnost prvočísla: $p|ab \implies p|a$ nebo $p|b$

Podivný obor integrality

$\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ – mřížové body
(obdélníková síť, jiná měřítka na osách !)

Norma: $N(a + bi\sqrt{5}) = a^2 + 5b^2$

Platí: $N(0) = 0$, $N(\alpha) \in \mathbb{N}$ pro $\alpha \neq 0$

Zákon normy: $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$

Důkaz: Pro $\alpha = a + bi\sqrt{5}$, $\beta = c + di\sqrt{5}$ je
$$(ac - 5bd)^2 + 5(ad + bc)^2 = (a^2 + 5b^2) \cdot (c^2 + 5d^2).$$

Invertibilní prvky: $\alpha \cdot \alpha^{-1} = 1$, tedy $N(\alpha) \cdot N(\alpha^{-1}) = N(1) = 1$,
pro $\alpha = a + bi\sqrt{5}$ má být $N(\alpha) = a^2 + 5b^2 = 1$, tedy $\alpha = \pm 1$

Která čísla x mohou být normou nějakého čísla $a + bi\sqrt{5}$?

$$a^2 + 5b^2 = x \quad (\text{nesymetrické vzhledem k } a \text{ a } b)$$

	$a^2 = 0$	1	4	9	16	25	36	49	64	81	100
$b = 0$	$x = 0$	1	4	9	16	25	36	49	64	81	100
$b = 1$	5	6	9	14	21	30	41	54	69	86	105
$b = 2$	20	21	24	29	36	45	56	69	84	101	120
$b = 3$	45	46	49	54	61	70	81	94	109	126	145
$b = 4$	80	81	84	89	96	105	116	129	144	161	180
$b = 5$	125	126	129	134	141	150	161	174	189	206	225
...	...	...	...	...	...	...	...	...	...	...	...

Normy čísel tvaru $a + bi\sqrt{5}$ tvoří množinu

$$\mathcal{B} = \{0, 1, 4, 5, 6, 9, 14, 16, 20, 21, 24, 25, 29, 30, 36, 41, 45, 46, 49, 54, \\ 56, 61, 64, 69, 70, 80, 81, 84, 86, 89, 94, 96, 100, 101, 105, \dots\}$$

Nerozložitelná čísla: 2, 3, 7, 11, 13, 17, 19, 23, 31, 37, 43, 47, 53, 59, 67, 71, 73, 79, 83, 97, 103, ...

$$N(2) = 4, \text{ číslo } 4 = 2^2 \text{ nelze rozložit v množině } \mathcal{B}$$

$$N(3) = 9, \text{ číslo } 9 = 3^2 \text{ nelze rozložit v množině } \mathcal{B}$$

$$N(7) = 49, \text{ číslo } 49 = 7^2 \text{ nelze rozložit v množině } \mathcal{B}$$

$$N(11) = 121, \text{ číslo } 121 = 11^2 \text{ nelze rozložit v množině } \mathcal{B}$$

$$N(13) = 169, \text{ číslo } 169 = 13^2 \text{ nelze rozložit v množině } \mathcal{B}$$

$$N(17) = 289, \text{ číslo } 289 = 17^2 \text{ nelze rozložit v množině } \mathcal{B}$$

$$N(19) = 361, \text{ číslo } 361 = 19^2 \text{ nelze rozložit v množině } \mathcal{B}$$

$$N(23) = 529, \text{ číslo } 529 = 23^2 \text{ nelze rozložit v množině } \mathcal{B}$$

$$N(31) = 961, \text{ číslo } 961 = 31^2 \text{ nelze rozložit v množině } \mathcal{B}$$

...

...

...



Další nerozložitelná čísla: $1 \pm i\sqrt{5}$, $2 \pm i\sqrt{5}$, $3 \pm i\sqrt{5}$, $1 \pm 2i\sqrt{5}$,
 $4 \pm i\sqrt{5}$, $3 \pm 2i\sqrt{5}$, $6 \pm i\sqrt{5}$,
 $1 \pm 3i\sqrt{5}, \dots$

$N(1 \pm i\sqrt{5}) = 6$,	číslo 6	nelze rozložit v množině $\mathcal{B}$
$N(2 \pm i\sqrt{5}) = 9$,	číslo 9	nelze rozložit v množině $\mathcal{B}$
$N(3 \pm i\sqrt{5}) = 14$,	číslo 14	nelze rozložit v množině $\mathcal{B}$
$N(1 \pm 2i\sqrt{5}) = 21$,	číslo 21	nelze rozložit v množině $\mathcal{B}$
$N(4 \pm i\sqrt{5}) = 21$,	číslo 21	nelze rozložit v množině $\mathcal{B}$
$N(3 \pm 2i\sqrt{5}) = 29$,	číslo 29	nelze rozložit v množině $\mathcal{B}$
$N(6 \pm i\sqrt{5}) = 41$,	číslo 41	nelze rozložit v množině $\mathcal{B}$
$N(1 \pm 3i\sqrt{5}) = 46$,	číslo 46	nelze rozložit v množině $\mathcal{B}$
$N(2 \pm 3i\sqrt{5}) = 49$,	číslo 49	nelze rozložit v množině $\mathcal{B}$
$N(4 \pm 3i\sqrt{5}) = 61$,	číslo 61	nelze rozložit v množině $\mathcal{B}$
$N(8 \pm i\sqrt{5}) = 69$,	číslo 69	nelze rozložit v množině $\mathcal{B}$

Rozložitelná čísla: 5, 29, 41, 61, 89, 101, ...

$$5 = (i\sqrt{5})(-i\sqrt{5}), \quad \text{rozklad } N(5) = 25 = 5^2$$

$$29 = (3 + 2i\sqrt{5})(3 - 2i\sqrt{5}), \quad \text{rozklad } N(29) = 841 = 29^2$$

$$41 = (6 + i\sqrt{5})(6 - i\sqrt{5}), \quad \text{rozklad } N(41) = 1681 = 41^2$$

$$61 = (4 + 3i\sqrt{5})(4 - 3i\sqrt{5}), \quad \text{rozklad } N(61) = 3721 = 61^2$$

$$89 = (3 + 4i\sqrt{5})(3 - 4i\sqrt{5}), \quad \text{rozklad } N(89) = 7921 = 89^2$$

$$101 = (9 + 2i\sqrt{5})(9 - 2i\sqrt{5}), \quad \text{rozklad } N(101) = 10201 = 101^2$$

Nejednoznačnost rozkladů:

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

$$N(6) = 36 = 4 \cdot 9 = 6 \cdot 6$$

$$9 = 3^2 = (2 + i\sqrt{5})(2 - i\sqrt{5})$$

$$N(9) = 81 = 9 \cdot 9$$

číslo 9 je v tabulce $2 \times$: $b = 0, b = 1$

$$21 = 3 \cdot 7 = (1 + 2i\sqrt{5})(1 - 2i\sqrt{5}) = (4 + i\sqrt{5})(4 - i\sqrt{5})$$

$$N(21) = 441 = 9 \cdot 49 = 21 \cdot 21$$

číslo 21 je v tabulce $2 \times$: $b = 1, b = 2$

$$36 = 2^2 \cdot 3^2 = 2^2 \cdot (2 + i\sqrt{5})(2 - i\sqrt{5}) = (1 + i\sqrt{5})^2(1 - i\sqrt{5})^2$$

$$N(36) = 1\,296 = 16 \cdot 81 = 16 \cdot 9 \cdot 9 = 6^4$$

$$45 = 3^2 \cdot 5 = (2 + i\sqrt{5})(2 - i\sqrt{5})(i\sqrt{5})(-i\sqrt{5}) = 3^2 \cdot (i\sqrt{5})(-i\sqrt{5})$$

$$N(45) = 2\,025 = 9 \cdot 9 \cdot 5 \cdot 5$$

$$49 = 7^2 = (2 + 3i\sqrt{5})(2 - 3i\sqrt{5})$$

$$N(49) = 2\,401 = 49 \cdot 49$$

$$\begin{aligned} 54 &= 2 \cdot 3^3 = 3^2 \cdot (1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \cdot 3 \cdot (2 + i\sqrt{5})(2 - i\sqrt{5}) = \\ &= (1 + i\sqrt{5})(1 - i\sqrt{5})(2 + i\sqrt{5})(2 - i\sqrt{5}) \end{aligned}$$

$$69 = 3 \cdot 23 = (8 + i\sqrt{5})(8 - i\sqrt{5}) = (7 + 2i\sqrt{5})(7 - 2i\sqrt{5})$$

$$81 = 3^4 = 3^2 \cdot (2 + i\sqrt{5})(2 - i\sqrt{5}) = (2 + i\sqrt{5})^2(2 - i\sqrt{5})^2$$

$$\begin{aligned} 84 &= 2^2 \cdot 3 \cdot 7 = 2^2 \cdot (1 + 2i\sqrt{5})(1 - 2i\sqrt{5}) = \\ &= 2^2 \cdot (4 + i\sqrt{5})(4 - i\sqrt{5}) = \\ &= (3 + i\sqrt{5})(3 - i\sqrt{5})(1 + i\sqrt{5})(1 - i\sqrt{5}) = \\ &= 2 \cdot 3 \cdot (3 + i\sqrt{5})(3 - i\sqrt{5}) = \\ &= 2 \cdot 7 \cdot (1 + i\sqrt{5})(1 - i\sqrt{5}) \end{aligned}$$

Nerozložitelné prvky nemají vlastnost prvočísel !!!

Pro nerozložitelné prvky totiž obecně neplatí implikace

$$p|ab \implies p|a \text{ nebo } p|b.$$

V teoretické algebře se proto rozlišují *prvočinitelé* a *nerozložitelné* neboli *irreducibilní prvky*.

Věta. Každý prvočinitel je nerozložitelným prvkem.

Důkaz. Sporem. Kdyby byl prvočinitel p rozložitelný, tj. $p = ab$, pak $p|ab$, tedy buď $p|a$ nebo $p|b$.

Proto je p asociované s prvkem a nebo s prvkem b , jedná se o triviální rozklad – spor.

Pozor. Neplatí naopak!

Např. číslo $i\sqrt{5}$ je prvočinitel.

Pokud např. $i\sqrt{5} \mid \alpha\beta$, pak $5 \mid N(\alpha)N(\beta)$,

tedy např. $5 \mid N(\alpha) = a^2 + 5b^2$.

Odtud $a = 5k$, tj.

$$\alpha = 5k + bi\sqrt{5} = i\sqrt{5} \cdot (b - ki\sqrt{5}).$$

Poznámky:

Původní prvočísla $p \in \mathbb{P}$ tvaru $p = 4k + 3$ jsou v $\mathbb{Z}[i\sqrt{5}]$ **nerozložitelná**. Těch je nekonečně mnoho.

Mnohá původní prvočísla $p \in \mathbb{P}$ tvaru $p = 4k + 1$ jsou v $\mathbb{Z}[i\sqrt{5}]$ rovněž **nerozložitelná**.

Prvočísla tvaru $p = a^2 + 5b^2$ jsou rozložitelná (např. 29, 41):

$$p = a^2 + 5b^2 = (a + bi\sqrt{5})(a - bi\sqrt{5})$$

S celou problematikou je možno si pěkně pohrát.

Literatura:

V. Dlab, J. Bečvář: *Od aritmetiky k abstraktní algebře*,
2. vydání, Ústav aplikované matematiky, Fakulta dopravní,
ČVUT, Praha, 2022, 479 stran, ISBN 978-80-01-06978-3

ŠKOLA BADATELSKOU HROU!

ŠKOLA BADATELSKOU HROU!

NE VŠAK SLABOMYSLNOU!

HOWGH!

HOWGH!

ŠMYTEC!

HOWGH !

ŠMYTEC !

Děkuji za pozornost !