5. OBORY INTEGRITY A DĚLITELNOST

Polynomy

$$p(x) = \sum_{i=0}^{k} a_i \cdot x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k$$
$$= a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x^1 + a_0 x^0$$

- k – stupeň polynomu, když platí $a_k \neq 0$
  $st(p(x)) = k$
- nulový polynom $p(x) = 0$ – má stupeň -1
  $0 \in R[x]$ kde $R[x]$ je okruh polynomů
- lineární polynom $p(x) = a_1 x^1 + a_0$ – má stupeň 1
  $= a_1 x + a_0$
- konstantní polynom $p(x) = a_0 x^0$ – má stupeň 0
  $= a_0$
- normovaný polynom $p(x) = a_0 + a_1 x + \ldots + a_k x^k$ kde $a_k = 1$
  - $x^2 + 2x + 1$ ✓
  - $3x^3 + 1$ ✗
- kořen polynomu – řešíme $p(x) = 0$
  - a je kořen polynomu $\Longleftrightarrow (x-a) \mid p(x)$
  - polynom s kořenem je tedy dělitelný a dělitelný polynom má kořen nebo kořeny (dělitelný beze zbytku)
  - a a b jsou kořeny $\Longleftrightarrow (x-a)\cdot(x-b) \mid p(x)$
- ireducibilní polynom – $p(x)$ který nelze rozložit na součin polynomů nižšího stupně
  - ireducibilní polynom lze dělit jen konstantou, sám sebou, nebo asociovaným polynomem
  - asociované polynomy $2x^2 + 3x + 1 \cong x^2 + 1{,}5x + 0{,}5$
    $x_1 = -1$, $x_2 = -\frac{1}{2}$; $x_1 = -1$, $x_2 = -\frac{1}{2}$
  - asociované polynomy jsou buď stejné, nebo se liší násobkem konstantou
    $p(x) \cong c \cdot p(x)$ kde $c \in Q$

relace asociace $\sim$

- x^2+2x+1 není ireducibilní nad $\mathbb{Q}$
  $x_1=-1$ - má kořen
  $(x+1) \mid (x^2+2x+1)$
- $x+6$ je ireducibilní
- v $\mathbb{Q}$ a $\mathbb{R}$ jsou ireducibilní jen lineární polynomy (stupeň 1)

Obor integrity

$(A, +, 0, -, \cdot, 1)$ - komutativní okruh s jednotkovým prvkem (neutrální prvek vzhledem k $\cdot$)

$(A, +, 0, -)$ Abelovská grupa

$(A, \cdot, 1)$ komutativní monoid

- $+$ i $\cdot$ jsou uzavřené na A a jsou komutativní i asociativní a $\cdot$ je distributivní vzhledem k $+$
- 0 je neutrální prvek vzhledem k $+$
- nejsou dělitele nuly

$$\forall a, b \in A \setminus \{0\} : a \cdot b \neq 0$$
$$\forall a, b \in A : (a \cdot b = 0) \rightarrow (a = 0 \vee b = 0)$$
$$0 \neq 1$$
$$A \setminus \{0\} \neq \emptyset$$

- $(R_8, +, \cdot)$ není obor integrity
  $4 \in R_8 \wedge 2 \in R_8$
  $4 \neq 0 \wedge 2 \neq 0 \quad 4 \cdot 2 = 0$ v R_8
- $(R_3, +, \cdot)$ je obor integrity
- $(\mathbb{Z}_3, +, \cdot)$ také
- $(\mathbb{R}, +, \cdot)$ také

Dělitelnost v oboru integrity

- b dělí a, tedy a je dělitelné b, píšeme $b \mid a$
  $\iff \exists c \in I : a = b \cdot c$
- asociované prvky a, b $(a \sim b)$ jsou takové, že se navzájem dělí
  $\iff a \mid b \wedge b \mid a$ (viz předchozí strana a polynomy)

$\mathbb{Z} \setminus R = \{[0]_R, [1]_R, [2]_R, [3]_R \ldots\}$

R je $\sim$ $\quad [2]_R = \{-2, 2\}$ $\implies$ relace asociace

- triviální dělitelé prvku a – jsou prvky b pro které platí, že jsou asociované s a ($a \sim b$) a nebo b je jednotkový prvek oboru integrity

$2 \to 2, -2, 1$

$4 \to 2, -2, 4, -4, 1$

- vlastní dělitelé prvku a – jsou všechny netriviální dělitelé
  - $\forall b : a \not\sim b \wedge b$ není jednotka oboru integrity $\wedge\ b | a$

$4 \to 2, -2, 4, -4, 1$

- prvočinitelé – jsou všechny ireducibilní prvky p
  - každý neprvočinitel (neireducibilní prvek) je rozložitelný na součin prvočinitelů

$138 : 2 = 69$ $\quad 138 = 2 \cdot 3 \cdot 23$

$69 : 2 =$ nelze

$69 : 3 = 23$

$23 : 23 = 1$

$72 : 2 = 36$ $\quad 72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$

$36 : 2 = 18$

$18 : 2 = 9$

$9 : 3 = 3$

$3 : 3 = 1$

$$(a | (b \cdot c)) \to ((a | b) \vee (a | c))$$

a je prvočinitel

- jednotka – jednotka oboru integrity / okruhu dělí všechny jeho prvky
  - obor integrity I, $E(I)$ je množina jeho jednotek

Okruh polynomů

- $(R, +, \cdot)$ je okruh – $(R[x], +, \cdot)$ je pak okruh polynomů neznámé x nad okruhem $(R, +, \cdot)$
  - $R[x]$ je nosná množina obsahující všechny polynomy nad R
  - Z_3 je zbytková třída po dělení číslem 3
  - $Z_3 = \{0, 1, 2\}$
  - $Z_3[x]$ je množina všech polynomů nad zbytkovou třídou Z_3 takových, že koeficienty polynomů $a \in Z_3$ (tj násobky – a)
  - $Z_3[x] = \{\sum_{i=0}^{m} a_i x^i \mid a_i \in Z_3, i \in N\}$

- je-li R komutativní, je i $R[x]$ komutativní
- — " — obor integrity, i $R[x]$
- — " — Gaussův obor integrity, i $R[x]$
- — " — těleso, je $R[x]$ Eukleidovský obor

Gaussovy okruhy

- v Gaussově okruhu platí, že každý jeho prvek lze rozložit na součin prvočinitelů
- v $\mathbb{R}$ jsou ti prvočinitelé prvočísla (tedy ireducibilní prvky)
- v $R[x]$ jsou ti prvočinitelé ireducibilní polynomy
- Gaussův okruh je vždy oborem integrity
- existuje pro každé dva prvky největší společný dělitel (NSD) a nejmenší společný násobek (NSN)
- e je jednotka a $p_1, p_2, \dots, p_m$, $m \geq 0$ jsou ireducibilní prvky Gaussova okruhu (třeba prvočísla):

$$\forall a \in G : a = e \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_m$$

G tem G. okruh

$\Rightarrow$ každý prvek Gaussova okruhu je dán součinem jednotky a 0 nebo více ireducibilních prvků tohoto Gaussova okruhu

Největší společný dělitel (NSD)

- je dán rozkladem prvků na prvočinitele
- všechny společné prvky rozkladů čísel ve svých nejmenších mocninách v rámci jednoho rozkladu

NSD (144, 32)

$144 : 2 = 72$	$32 : 2 = 16$
$72 : 2 = 36$	$16 : 2 = 8$
$36 : 2 = 18$	$8 : 2 = 4$
$18 : 2 = 9$	$4 : 2 = 2$
$9 : 3 = 3$	$2 : 2 = 1$
$3 : 3 = 1$	

$144 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^4 \cdot 3^2$

$32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$

$$NSD(144, 32) = 2^4 = \underline{\underline{16}}$$

$2^4 < 2^5$

proto 2^4 a 3 nemá společné

Nejmenší společný násobek (NSN)

- je dán rozkladem prvků na prvočinitele
- ~~...~~ všechny prvky rozkladů čísel (všechny prvky všech rozkladů) ve svých největších mocninách v rámci jednoho rozkladu

$NSN(144, 32) \qquad 144 = 2^4 \cdot 3^2 \qquad 32 = 2^5$

$NSN(144, 32) = 3^2 \cdot 2^5 = \underline{\underline{288}}$

Euklidův okruh

- každý Euklidův okruh je i Gaussův okruh, takže zde také platí, že prvek z tohoto okruhu lze rozložit na součin jednotky okruhu a 0 nebo více prvočinitelů (ireducibilních prvků)
- navíc zde existuje Euklidovská funkce pro nalezení největšího společného dělitele prvků (NSD)
- pro všechny $a, b \in I$, $a \neq 0$ existují prvky $q, r \in I$ kde platí $\quad b = a \cdot q + r \quad , r \geq 0 \wedge r < a$

  kde I je Euklidův okruh

Euklidův algoritmus pro NSD (Euklidovská funkce)

$NSD(a, b) \qquad a < b$ – když není tak prostě prohodíme

$$b = a \cdot q_1 + r_1 \qquad 0 \leq r_1 < a$$
$$a = r_1 \cdot q_2 + r_2 \qquad 0 \leq r_2 < r_1$$
$$r_1 = r_2 \cdot q_3 + r_3 \qquad 0 \leq r_3 < r_2$$
$$\vdots$$
$$r_{n-2} = r_{n-1} \cdot q_n + \boxed{r_n} \qquad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = r_n \cdot q_{n+1} + 0 \longrightarrow NSD(a, b) = r_n$$

poslední prvek jako zbytek před 0

když zde vyšlo někdy 1 tak ta čísla jsou nesoudělná a $NSD(a, b) = 1$

Př.: NSD(123, 456) pomocí Euklidova algoritmu

$456 = 123 \cdot 3 + 87 \qquad 0 \leq 87 < 123$ ✓

$123 = 87 \cdot 1 + 36 \qquad 0 \leq 36 < 87$ ✓

$87 = 36 \cdot 2 + 15 \qquad 0 \leq 15 < 36$ ✓

$36 = 15 \cdot 2 + 6 \qquad 0 \leq 6 < 15$ ✓

$15 = 6 \cdot 2 + \boxed{3} \qquad 0 \leq 3 < 6$ ✓

$6 = 3 \cdot 2 + \underline{\underline{0}}$

$NSD(123, 456) = \underline{\underline{3}}$

největší společný dělitel

Důležité:

Euklidovský obor je Gaussův obor a Gaussův obor je obor integrity

- opačně to platit nemusí
- v Gaussově oboru platí že $a | b$ jestliže a se skládá ze stejného nebo menšího počtu stejných jednoduchých prvočinitelů
- Gaussův obor je třeba $\mathbb{Z}$
- v Euklidově oboru ke $b = a \cdot q + r$ kde $0 \leq r < a$ může platit i pro polynomy a dělalo by se to stejně
- každý polynom $p(x)$ který má tyto kořeny a_1 a a_2 je rozložitelný na součin polynomů $p(x) = (x - a_1) \cdot (x - a_2)$ a je těmi dvěma polynomy tedy dělitelný $(x - a_1) | p(x)$ a $(x - a_2) | p(x)$
- ireducibilní polynom není rozložitelný na součin polynomů nižšího stupně a je dělitelný jen sám sebou nebo konstantou nebo asociovanými prvky – nemá jiné dělitele jen triviální
- asociované prvky jsou takové a, b kde $a | b \wedge b | a$ a u těch polynomů je jeden polynom asociovaný s druhým (je tam relace asociace $\sim$) jestliže je to ten samý pouze vynásobený konstantou

Operace s dělením

Binární operace o se nazývá operace s dělením na množině A právě, když:

$$\forall (a,b) \in A^2 \ \exists (x,y) \in A^2 : \underbrace{a \circ x = b}_{\text{levý zákon o dělení}} \wedge \underbrace{y \circ a = b}_{\text{pravý zákon o dělení}}$$

- jestliže o je binární operace, která je asociativní a $A \neq \emptyset$, pak platí:
  - a) o je operace s dělením
  - b) existuje neutrální prvek e vzhledem k o a každý prvek $a \in A$ je invertibilní $\forall a \in A \ \exists e \in A : a \circ e = e \circ a = a$

$$\exists x \in A : a \circ x = x \circ a = e$$

(ne každá operace s dělením musí být asociativní ale pro každou bin. operaci která je asociativní a $A \neq \emptyset$ platí, že je to operace s dělením)

- je-li o asociativní operace s dělením na neprázdné množině, pak mají rovnice $a \circ x = b$ a $y \circ a = b$ právě jedno řešení a to x, y

Operace s krácením

Binární operace se nazývá operace s krácením na množině A právě, když:

$$\forall x_1, x_2, y_1, y_2, a \in A : \underbrace{(x_1 \circ a = x_2 \circ a \Rightarrow x_1 = x_2)}_{\text{levý zákon o krácení}} \wedge \underbrace{(a \circ y_1 = a \circ y_2 \Rightarrow y_1 = y_2)}_{\text{pravý zákon o krácení}}$$

prostě se to a nezkrátí (nevyskytují se)

- rovnice $a \circ x = b$ a $y \circ a = b$ (y s dělením) mají při operaci o s krácením nejvýše jedno řešení a při asociativní operaci s dělením právě jedno řešení
- pokud je o operace s krácením tak to nemusí být operace s dělením ale pokud o je asociativní operace s dělením, tak je to i operace s krácením
- na konečné množině A : operace o je s dělením $\Longleftrightarrow$ operace o je s krácením

~~(N, +)~~

~~Př.: operace + na N není s dělením ale je s krácením~~

~~$\forall x_1 x_2 y_1 y_2 a \in A : (a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2) \wedge (y_1 \circ a = y_2 \circ a \Rightarrow y_1 = y_2)$~~ $\Longrightarrow$

~~$3 + x_1 = 3 + x_2 \Longrightarrow x_1 = x_2$~~

~~– proč není s dělením? jelikož a a b jsou stejné a x a y by museli být 0 a to tam nepatří?~~

Př.: operace $\cdot$ na N je operace s krácením ale není operace s dělením

$$(5 \cdot x_1 = 5 \cdot x_2 \rightarrow x_1 = x_2) \wedge (y_1 \cdot 5 = y_2 \cdot 5 \rightarrow y_1 = y_2)$$

OK je s krácením $\quad 5 \in N$

$$5 \cdot x = 3 \wedge y \cdot 5 = 3 \qquad 5,3 \in N$$

$$\underbrace{x = \frac{3}{5} \qquad y = \frac{3}{5}}_{\text{nejsou z } N}$$

NENÍ s dělením

Př.: operace $+$ na N je operace s krácením ale není operace s dělením

$$(3 + x_1 = 3 + x_2 \rightarrow x_1 = x_2) \wedge (y_1 + 3 = y_2 + 3 \rightarrow y_1 = y_2)$$

OK je s krácením $\quad 3 \in N$

$$5 + x = 3 \wedge y + 5 = 3 \qquad 5,3 \in N$$

$$\underbrace{x = -2 \qquad y = -2}_{\text{nejsou z } N}$$

5. OBORY INTEGRITY A DĚLITELNOST

Obory integrity

– jedná se o okruh, který je navíc komutativní a obsahuje jednotkový prvek (neutrální prvek vzhledem k operaci $\cdot$) a nejsou zde dělitelé nuly

$(M,+,0,-a,\cdot,1)$ – kde platí že $(M,+,0,-a)$ je Abelovská grupa (+ je uzavřené na M a je komutativní a asociativní a obsahuje neutrální prvek 0 a každý prvek $a\in M$ je invertibilní)

$(2,0,1,2,0)$

a $(M,\cdot,1)$ je komutativní monoid

a také $\cdot$ je distributivní vzhledem k +

tedy $a\cdot(b+c) = a\cdot b + a\cdot c \wedge (b+c)\cdot a = b a + c\cdot a$

a nejsou zde dělitelé nuly, tedy:

$M\setminus\{0\}\neq\emptyset$ a tedy $0\neq 1$

$$\forall a,b\in M\setminus\{0\}: a\cdot b\neq 0 \wedge \underbrace{b\cdot a\neq 0}_{\text{toto se značit nemusí protože víme, že} \cdot \text{ je komutativní}}$$

Okruhy polynomů

– okruh polynomů neurčité x nad R je $\overbrace{(R[x],+,0,-a,\cdot,1)}^{\text{komutativní okruh s jednotkovým prvkem}}$, který je podokruhem okruhu $[R[x]]$

$[R[x]]$ – je okruh formálních mocninných řad neurčité x nad R

$R[x]$ – je následující množina $R[x] = \{a_0 + a_1x^1 + \dots + a_n x^n \mid a_i\in R, n\in N_0\}$

– je to množina polynomů neurčité x nad R (neurčitá/neznámá/proměnná)

– prvky této množiny jsou tedy polynomy

Polynom neurčité x nad R – je možné také zapsat jako $p(x)=\sum_{k=0}^{n} a_k x^k$

– pokud $a^n\neq 0$ tak to se značí stupeň polynomu a tedy polynom $p(x)=x^4+2x^2$ je 4. stupně a píše se $grad(p(x))=4$

– kořeny polynomu získáme jestliže $p(x)=0$

– některé pol. nemusí mít kořeny, třeba x^2+1 v reálných číslech (v komplexních ano)

– polynom $p(x)=0$ má stupeň $grad(p(x))=-1$

– polynom $p(x)=10$ má stupeň $grad(p(x))=0$

– polynom $p(x)=2x$ má stupeň $grad(p(x))=1$

– pokud máme daný polynom $p(x)=\sum_{k}^{n} a_k x^k$ kde $a_k\in R$ a $n\in N_0$ pak hodnota $p(6)$ kde $6\in R$ se nazývá hodnota polynomu v 6 a tato hodnota $p(6)\in R$

– $p(x)=0$ je nulový polynom a má stupeň -1

– $p(x)=5$ je konstantní polynom a má stupeň 0

– $p(x)=2x+1$ je lineární polynom a má stupeň 1

– $p(x)=x^4+2x^3+1$ je normovaný polynom protože $a_n=1$ – $2x^3+x^2+x+2$ není protože $a_n=2$

- okruh polynomů je tedy komutativní okruh s jednotkovým prvkem jehož nosnou množinou tvoří množina $R[x]$ - tedy množina polynomů neurčité x nad R
- nad těmi polynomy z $R[x]$ jsou definovány operace $+$ a $\cdot$ a platí pravidla komutativního okruhu s jednotkovým prvkem

Dělitelnost

- to že prvek a je dělitelný prvkem b, respektive prvek b dělí prvek a značíme $\boxed{b \mid a}$ přičemž musí platit, že $\exists c \in I : a = b.c$ za předpokladu, že $\cdot$ je komutativní (jinak musíme udělat $\exists c \in I : a = b.c \wedge a = c.b$)
- základní pravidla dělitelnosti:
  - $a \mid 0$ – 0 je dělitelná čímkoliv ~~[illegible]~~
  - $1 \mid a$ – cokoliv je dělitelné 1
  - $a \mid a$ – vše je dělitelné samo sebou
  - $a \mid b \wedge b \mid c \rightarrow a \mid c$ – a dělí b a to b dělí c tak a dělí c
    - $2 \mid 10 \wedge 10 \mid 100 \rightarrow 2 \mid 100$
  - $a \mid b \wedge a \mid c \rightarrow a \mid b + c$ – a dělí b a a dělí c tak a dělí i součet
    - součet je dělitelný společným dělitelem sčítanců
    - $2 \mid 8 \wedge 2 \mid 6 \rightarrow 2 \mid 14$
  - $a \mid b \rightarrow a \mid b \cdot c$ – můj dělitel je i dělitel mého násobku
  - $c \neq 0$ a $a \mid b \rightarrow a \cdot c \mid b \cdot c$ – vynásobením dělitele i dělence stejným nenulovým číslem je zachována dělitelnost
  - $a \mid b \wedge c \mid d \rightarrow a \cdot c \mid b \cdot d$ – pokud máme dvě dvojice kde platí že jeden prvek dělí druhý tak součin dělitelů těchto dvojic dělí součin dělenců těchto dvojic
  - $a \mid b \rightarrow a^n \mid b^n$ – pokud a dělí b tak ~~[illegible]~~ je dělitelnost zachována i při umocnění obou prvků na stejnou mocninu
- Jednotka – dělí cokoliv ($1 \mid a$)
  - je to třeba 1 a −1
  - v oboru integrity I je množina jednotek značena $E(I)$
- Asociované prvky $[a \sim b]$ – liší se jen tím, že jeden je ten druhej vynásobenej jednotkou
  - prvek 7 má asociovaný prvek −7
- Triviální dělitelé prvku a – takoví, jednička (jednotkami v tomto případě) a samo sebou jen jak se říká
  - jsou jednotky a asociované prvky prvku a a on sám
  - 7: 1, −1, 7, −7
- Vlastní dělitelé – jsou všechny netriviální dělitelé
- Ireducibilní prvek – nemá vlastní dělitele, má jen triviální dělitele tedy třeba to 7 kterou nic nedělí kromě 7, −7, 1 a −1

Třídy ekvivalence vzhledem k ~

– třídy ekvivalence vzhledem k relaci asociace ~

– pro $\mathbb{Z} = \{0\}, \{-1,1\}, \{2,2\}, \dots \{-n, n\}; n \in \mathbb{N}$

Prvočinitel

$a|(b \cdot c) \rightarrow a|b \vee a|c$ pak a je prvočinitel

– prvočinitel je prvočíslo které dělí nějaké číslo
– každé číslo (složené) lze zapsat jako součin prvočísel → rozklad na prvočinitele
– číslo je buď prvočíslo a nebo je složené a lze provést rozklad na prvočinitele

72 : 2 = 36
36 : 2 = 18
18 : 2 = 9
9 : 3 = 3
3 : 3 = 1

– rozklad čísla 72 je tedy 2,2,2,3

33 : 3 = 11 – rozklad 33 je 3 a 11
11 nejde

Největší společný dělitel (NSD)

– vezmu $\boxed{\text{společná}}$ čísla rozkladu obou hodnot a u každého čísla vezmu $\boxed{\text{nejmenší}}$ mocninu ve které se v rámci jednoho operandu operace NSD vyskytuje

NSD(136, 204)

136 : 2 = 68
68 : 2 = 34
34 : 2 = 17
17 nejde

136 má rozklad $2 \cdot 2 \cdot 2 \cdot 17$

204 : 2 = 102
102 : 2 = 51
51 : 3 = 17
17 nejde

204 má rozklad $2 \cdot 2 \cdot 3 \cdot 17$

společná čísla jsou 2 a 17 – min mocnina 17 je 1 a min. mocnina 2 je 2

$\Rightarrow$ tedy $NSD(136, 204) = 2^2 \cdot 17 = 68$

Nejmenší společný násobek (NSN)

– stejné jako u dělitele ale hledáme ~~společná~~ $\boxed{\text{všechna čísla}}$ čísla rozkladu a jejich $\boxed{\text{největší}}$ mocninu ve které se v rámci jednoho operandu operace NSN vyskytuje

– u předchozího bude NSN(204, 136) →

204 : 2 = 102
102 : 2 = 51
51 : 3 = 17
17 nejde

$204 = 2 \cdot 2 \cdot 3 \cdot 17$

136 : 2 = 68
68 : 2 = 34
34 : 2 = 17
17 nejde

$136 = 2 \cdot 2 \cdot 2 \cdot 17$

$\Rightarrow$ tedy $NSN(204, 136) = 2^3 \cdot 17 \cdot 3 = 408$

Gaussovy okruhy

– obor integrity je Gaussův okruh jestliže platí že ten okruh je I a $\forall a \in I \setminus E(I)$ (množina bez jednotek) $\wedge\ a \neq 0$ existují prvočinitelé $p_1, p_2, \dots, p_r$ takové že $a = p_1 \cdot p_2 \cdot \dots \cdot p_r$

– rozklad každého prvku a na prvočinitele je jednoznačný – pokud jsou dva rozklady jednoho prvku a tak mezi nimi existuje permutace že odpovídající prvočinitelé jsou asociovaní (~)
→ tzn. jeden je pouze permutace toho druhého a tedy třeba 2,2,3,17 a 17,2,3,2

– každý ireducibilní prvek v Gaussově okruhu je prvočíslo

- ireducibilní prvek je tedy v Gaussově okruhu prvočinitelem
- každý neprvočinitel je tvořen součinem mocnin různých prvočinitelů a jednotky
- v Gaussově okruhu platí $a|b \Leftrightarrow$ a se skládá ze stejného nebo menšího počtu stejných jednotlivých prvočinitelů
- Gaussův okruh jsou třeba celá čísla $\mathbb{Z}$

/ rozkladová faktorová množina množiny I tedy $I\backslash\sim$

Normované prvky – množina I se rozdělí na třídy podle ~~rel~~ relace asociace $\sim$ a z každé třídy se vybere jeden zástupce / reprezentant
- na $\mathbb{Z}$ to jsou třídy $\{0\}, \{\pm 1\}, \{\pm 2\}, \dots \{\pm n\}, n \in \mathbb{N}$
- normované prvky jsou jen kladné prvky

Normovaní prvočinitelé – jsou reprezentanti tříd, které obsahují jen prvočinitele

Svaz dělitelnosti – je svaz nad faktorovou množinou množiny I dle relace asociace a tedy $I\backslash\sim$, kde platí uspořádání $[a]_\sim \leq [b]_\sim \Rightarrow a|b$
(faktorová množina asociovaných prvků)

Euklidovy okruhy

Euklidův okruh je obor integrity I když existuje zobrazení $H: I\backslash\{0\} \to \mathbb{N}_0$ a platí že ~~p~~ $\forall a \in I\backslash\{0\}, \forall b \in I, \exists q, r \in I$ takové, že $b = aq + r$
$r = 0 \vee H(r) < H(a)$ ← jedná se o dělení se zbytkem
- H je euklidovské ohodnocení
- $\mathbb{Z}$ je třeba euklidův okruh kde $H(a) = |a|$
- pole je euklidův okruh a každý euklidův okruh je gaussův okruh

↳ okruh na kterém je definováno dělení se zbytkem

$$b = a \cdot q + r$$

– r je ten zbytek který je buď 0 nebo je logicky menší než a

$h(r) < h(a)$

a je tam zobrazení do ~~celý~~ přirozených čísel

$$H: I\backslash\{0\} \to \mathbb{N}_0$$

— dobré pro nalezení NSD