Poziční reprezentace okruhu Gaussových celých čísel a tělesa $\mathbb{C}$

Edita Pelantová

katedra matematiky, FJFI, ČVUT v Praze
Tigří seminář

7. 12. 2010

Gaussova celá čísla

Množina $\mathbb{Z}[i] := \{a + ib \mid a, b, \in \mathbb{Z}\}$ - tzv. okruh Gaussových celých čísel.

Věta (Penney, 1964)

Nechť $\beta = i - 1$. Každé $z \in \mathbb{Z}[i]$ lze jednoznačně zapsat ve tvaru

$$z = \sum_{k=0}^{n} a_k \beta^k, \qquad \text{kde} \;\; a_k \in \mathcal{A} = \{0, 1\}\,.$$

Zapisujeme $z = a_n a_{n-1} \ldots a_1 a_0 \bullet$

$$\beta = i - 1, \;\; \beta^2 = -2i, \;\; \beta^3 = 2 + 2i, \;\; \beta^4 = -4, \ldots$$

β je kořen rovnice $x^2 + 2x + 2 = 0$, tedy $N(\beta) = \beta\overline{\beta} = 2$, tedy $|\beta| = \sqrt{2}$.

Důkaz

Jednoznačnost rozvoje:

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k \beta^k = \sum_{k=0}^{n} b_k \beta^k \implies \sum_{k=0}^{n} (a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 $-$ spor

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje:

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

To už implikuje $S = \mathbb{Z}[i]$

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

To už implikuje $S = \mathbb{Z}[i]$
$1 + 1 = 2 = \beta^3 + \beta^2 \implies 2 = 1100\bullet$

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

To už implikuje $S = \mathbb{Z}[i]$
$1 + 1 = 2 = \beta^3 + \beta^2 \implies 2 = 1100\bullet$
To jest: součet $z + \beta^i$ lze upravit pomoci pravidla $2 \to 1100$, bez zvýšení součtu cifer. Toto pravidlo lze aplikovat tak dlouho, až se zastavíme

Příklad:

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

To už implikuje $S = \mathbb{Z}[i]$
$1 + 1 = 2 = \beta^3 + \beta^2 \implies 2 = 1100\bullet$
To jest: součet $z + \beta^i$ lze upravit pomoci pravidla $2 \to 1100$, bez zvýšení součtu cifer. Toto pravidlo lze aplikovat tak dlouho, až se zastavíme

Příklad:
$3 = 1101\bullet$

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 $-$ spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

To už implikuje $S = \mathbb{Z}[i]$
$1 + 1 = 2 = \beta^3 + \beta^2 \implies 2 = 1100\bullet$
To jest: součet $z + \beta^i$ lze upravit pomoci pravidla $2 \to 1100$, bez zvýšení součtu cifer. Toto pravidlo lze aplikovat tak dlouho, až se zastavíme

Příklad:
$3 = 1101\bullet$
$4 = 1101\bullet + 1\bullet = \ldots = 111010000\bullet$

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

To už implikuje $S = \mathbb{Z}[i]$
$1 + 1 = 2 = \beta^3 + \beta^2 \implies 2 = 1100\bullet$
To jest: součet $z + \beta^i$ lze upravit pomoci pravidla $2 \to 1100$, bez zvýšení součtu cifer. Toto pravidlo lze aplikovat tak dlouho, až se zastavíme

Příklad:

$3 = 1101\bullet$

$4 = 1101 \bullet +1\bullet = \ldots = 111010000\bullet$

$\frac{4}{\beta^4} = 11101\bullet$

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 $-$ spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

To už implikuje $S = \mathbb{Z}[i]$
$1 + 1 = 2 = \beta^3 + \beta^2 \implies 2 = 1100\bullet$
To jest: součet $z + \beta^i$ lze upravit pomoci pravidla $2 \to 1100$, bez zvýšení součtu cifer. Toto pravidlo lze aplikovat tak dlouho, až se zastavíme

Příklad:
$3 = 1101\bullet$
$4 = 1101 \bullet + 1\bullet = \ldots = 111010000\bullet$
$\frac{4}{\beta^4} = 11101\bullet = -1$

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 – spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

To už implikuje $S = \mathbb{Z}[i]$
$1 + 1 = 2 = \beta^3 + \beta^2 \implies 2 = 1100\bullet$
To jest: součet $z + \beta^i$ lze upravit pomoci pravidla $2 \to 1100$, bez zvýšení součtu cifer. Toto pravidlo lze aplikovat tak dlouho, až se zastavíme

Příklad:
$3 = 1101\bullet$
$4 = 1101 \bullet +1\bullet = \ldots = 111010000\bullet$
$\frac{4}{\beta^4} = 11101\bullet = -1$
$i = \beta + 1 \implies i = 11\bullet$ a

Důkaz

Jednoznačnost rozvoje:
$\sum_{k=0}^{n} a_k\beta^k = \sum_{k=0}^{n} b_k\beta^k \implies \sum_{k=0}^{n}(a_k - b_k)\beta^k = 0 \implies$
β je kořen polynomu s absolutním členem ± 1 $-$ spor

Existence rozvoje: Označme $S = \left\{\sum_{k=0}^{n} a_k\beta^k \mid a_k \in \{0,1\}\right\}$.

Ukážeme, že A) $1, i, -1, -i \in S$ B) S je uzavřena na operaci $+$.

To už implikuje $S = \mathbb{Z}[i]$
$1 + 1 = 2 = \beta^3 + \beta^2 \implies 2 = 1100\bullet$
To jest: součet $z + \beta^i$ lze upravit pomoci pravidla $2 \to 1100$, bez zvýšení součtu cifer. Toto pravidlo lze aplikovat tak dlouho, až se zastavíme

Příklad:
$3 = 1101\bullet$
$4 = 1101 \bullet + 1\bullet = \ldots = 111010000\bullet$
$\frac{4}{\beta^4} = 11101\bullet = -1$
$i = \beta + 1 \implies i = 11\bullet$ a $-i = \beta^2 + \beta + 1 \implies -i = 111\bullet$

$Fin(\beta)$

$$\frac{1}{\beta}S = \Big\{\sum_{k=0}^{n} a_k\beta^k + \frac{a_{-1}}{\beta} \mid a_k \in \{0,1\}\Big\} = S \cup \left(\frac{1}{\beta} + S\right) \qquad \text{přičemž } \frac{1}{\beta} = \frac{-1-i}{2}$$

$Fin(\beta)$

$$\frac{1}{\beta}S = \Big\{\sum_{k=0}^{n} a_k\beta^k + \frac{a_{-1}}{\beta} \mid a_k \in \{0,1\}\Big\} = S \cup \left(\frac{1}{\beta} + S\right) \qquad \text{přičemž } \frac{1}{\beta} = \frac{-1-i}{2}$$

$$\frac{1}{\beta^2}S = S \cup \left(\frac{1}{\beta} + S\right) \cup \left(\frac{1}{\beta^2} + S\right) \cup \left(\frac{1}{\beta} + \frac{1}{\beta^2} + S\right) \quad \text{kde } \frac{1}{\beta^2} = \frac{i}{2} \text{ a } \frac{1}{\beta} + \frac{1}{\beta^2} = -\frac{1}{2}$$

$Fin(\beta)$

$$\frac{1}{\beta}S = \Big\{ \sum_{k=0}^{n} a_k\beta^k + \frac{a_{-1}}{\beta} \mid a_k \in \{0,1\} \Big\} = S \cup \left(\frac{1}{\beta}+S\right) \qquad \text{přičemž } \frac{1}{\beta} = \frac{-1-i}{2}$$

$$\frac{1}{\beta^2}S = S \cup \left(\frac{1}{\beta}+S\right) \cup \left(\frac{1}{\beta^2}+S\right) \cup \left(\frac{1}{\beta}+\frac{1}{\beta^2}+S\right) \quad \text{kde } \frac{1}{\beta^2} = \frac{i}{2} \text{ a } \frac{1}{\beta}+\frac{1}{\beta^2} = -\frac{1}{2}$$

$$Fin(\beta) = \bigcup_{n\in N} \frac{1}{\beta^n}S \quad \text{je hustá v } \mathbb{C}\,.$$

$Fin(\beta)$

$$\frac{1}{\beta}S = \Big\{\sum_{k=0}^{n} a_k\beta^k + \frac{a_{-1}}{\beta} \mid a_k \in \{0,1\}\Big\} = S \cup \Big(\frac{1}{\beta}+S\Big) \qquad \text{přičemž } \frac{1}{\beta} = \frac{-1-i}{2}$$

$$\frac{1}{\beta^2}S = S \cup \Big(\frac{1}{\beta}+S\Big) \cup \Big(\frac{1}{\beta^2}+S\Big) \cup \Big(\frac{1}{\beta}+\frac{1}{\beta^2}+S\Big) \quad \text{kde } \frac{1}{\beta^2} = \frac{i}{2} \text{ a } \frac{1}{\beta}+\frac{1}{\beta^2} = -\frac{1}{2}$$

$$Fin(\beta) = \bigcup_{n\in N} \frac{1}{\beta^n}S \quad \text{je hustá v } \mathbb{C}\,.$$

Věta

Každé $z \in \mathbb{C}$ lze napsat (ne nutně jednoznačně) ve tvaru

$$z = \sum_{k=-\infty}^{n} a_k\beta^k, \quad \text{kde } a_k \in \{0,1\}\,.$$

$Fin(\beta)$

$$\frac{1}{\beta}S = \Big\{\sum_{k=0}^{n} a_k\beta^k + \frac{a_{-1}}{\beta} \mid a_k \in \{0,1\}\Big\} = S \cup \Big(\frac{1}{\beta}+S\Big) \qquad \text{přičemž } \frac{1}{\beta} = \frac{-1-i}{2}$$

$$\frac{1}{\beta^2}S = S \cup \Big(\frac{1}{\beta}+S\Big) \cup \Big(\frac{1}{\beta^2}+S\Big) \cup \Big(\frac{1}{\beta}+\frac{1}{\beta^2}+S\Big) \;\text{ kde }\; \frac{1}{\beta^2} = \frac{i}{2} \;\text{ a }\; \frac{1}{\beta}+\frac{1}{\beta^2} = -\frac{1}{2}$$

$$Fin(\beta) = \bigcup_{n\in N} \frac{1}{\beta^n}S \quad \text{je hustá v } \mathbb{C}\,.$$

Věta

Každé $z \in \mathbb{C}$ lze napsat (ne nutně jednoznačně) ve tvaru

$$z = \sum_{k=-\infty}^{n} a_k\beta^k, \quad \text{kde } a_k \in \{0,1\}\,.$$

Např. $1 \bullet (1101\,0000)^\omega = 0 \bullet (0000\,1101)^\omega = \frac{1}{5}$

Snadný důkaz?

Věta (Thurston 1989)

Nechť β je komplexní číslo, $|\beta| > 1$ a nechť $\mathcal{A} \subset \mathbb{C}$ je konečná množina. Když existuje omezené okolí V bodu nula takové, že $\beta V \subset V + \mathcal{A}$, pak každé $z \in \mathbb{C}$ lze zapsat ve tvaru

$$z = \sum_{k=-\infty}^{n} a_k \beta^k \,, \quad \text{kde} \;\; a_k \in \mathcal{A} \,.$$

Dk. Stačí ukázat pro každé $z \in V$.

$\beta z = a_1 + r_1$, kde $a_1 \in \mathcal{A}$ a $r_1 \in V \quad \Longrightarrow \quad z = \frac{a_1}{\beta} + \frac{1}{\beta} r_1$

$\beta r_1 = a_2 + r_2$, kde $a_2 \in \mathcal{A}$ a $r_2 \in V \quad \Longrightarrow \quad z = \frac{a_1}{\beta} + \frac{1}{\beta}\left(\frac{a_2}{\beta} + \frac{1}{\beta} r_2\right)$

$$z = \frac{a_1}{\beta} + \frac{a_2}{\beta^2} + \frac{a_3}{\beta^3} + \ldots + \frac{a_k}{\beta^k} + \frac{1}{\beta^k} r_k \,.$$

Omezenost V implikuje konvergenci.

Co vzít za naše okolí V ?

$\beta = i - 1 \quad \mathcal{A} = \{0, 1\}$

$$\beta V \subset V \cup (V + 1)$$

Co vzít za naše okolí V ?

$\beta = i - 1 \quad \mathcal{A} = \{0, 1\}$

$$\beta V \subset V \cup (V + 1)$$

Kdyby V měřitelná, pak $\mu(\beta V) = 2\mu(V)$

Co vzít za naše okolí V ?

$\beta = i - 1 \quad \mathcal{A} = \{0, 1\}$

$$\beta V \subset V \cup (V + 1)$$

Kdyby V měřitelná, pak $\mu(\beta V) = 2\mu(V)$
$\implies \quad \beta V = V \cup (V + 1) \quad$ a $\quad$ vnitřky V a $V + 1$ disjunktní.

Co vzít za naše okolí V ?

$\beta = i - 1 \quad \mathcal{A} = \{0, 1\}$

$$\beta V \subset V \cup (V + 1)$$

Kdyby V měřitelná, pak $\mu(\beta V) = 2\mu(V)$
$\implies \quad \beta V = V \cup (V + 1)$ a vnitřky V a $V + 1$ disjunktní.
Hledáme V pevý bod zobrazení $F(X) = \frac{1}{\beta} X \cup \frac{1}{\beta}(X + 1)$.

Co vzít za naše okolí V ?

$\beta = i - 1 \quad \mathcal{A} = \{0, 1\}$

$$\beta V \subset V \cup (V + 1)$$

Kdyby V měřitelná, pak $\mu(\beta V) = 2\mu(V)$
$\implies \quad \beta V = V \cup (V + 1)$ a vnitřky V a $V + 1$ disjunktní.
Hledáme V pevý bod zobrazení $F(X) = \frac{1}{\beta} X \cup \frac{1}{\beta}(X + 1)$.

Věta (Hutchinson, 1981)

Nechť $f_1, f_2, \ldots, f_\ell$ jsou kontraktivní zobrazení v $\mathbb{R}^d$. Pak existuje jediná neprázdná kompaktní množina $X \subset \mathbb{R}^d$ taková, že

$$X = f_1(X) \cup f_2(X) \cup \ldots \cup f_\ell(X)$$

Naše V

$$V := \Big\{0 \bullet a_{-1}a_{-2}a_{-3}\dots \big| a_{-k} \in \{0,1\}\Big\}.$$

Naše V

$$V := \left\{0 \bullet a_{-1}a_{-2}a_{-3}\dots | a_{-k} \in \{0,1\}\right\}.$$

$$\beta V = \left\{a_{-1} \bullet a_{-2}a_{-3}\dots | a_{-k} \in \{0,1\}\right\} = V \cup (V+1)$$

Naše V

$$V := \left\{ 0 \bullet a_{-1}a_{-2}a_{-3}\ldots | a_{-k} \in \{0,1\} \right\}.$$

$$\beta V = \left\{ a_{-1} \bullet a_{-2}a_{-3}\ldots | a_{-k} \in \{0,1\} \right\} = V \cup (V+1)$$

Ukázat obrázek!!!

Naše V

$$V := \left\{ 0 \bullet a_{-1}a_{-2}a_{-3}\ldots \middle| a_{-k} \in \{0,1\} \right\}.$$

$$\beta V = \left\{ a_{-1} \bullet a_{-2}a_{-3}\ldots \middle| a_{-k} \in \{0,1\} \right\} = V \cup (V+1)$$

Ukázat obrázek!!!

$V + \mathbb{Z}[i]$ je periodické dláždění roviny

Méně naivní postup hledání rozvoje v $\mathbb{Z}[i]$

$R = \mathbb{Z}[i]$ je okruh, $\beta = i - 1 \in R$, množina βR je ideál v R.

Méně naivní postup hledání rozvoje v $\mathbb{Z}[i]$

$R = \mathbb{Z}[i]$ je okruh, $\beta = i - 1 \in R$, množina βR je ideál v R.
Kongruence definovaná

$$x \equiv y \mod \beta \Longleftrightarrow x - y \in \beta R$$

má dvě zbytkové třídy s reprezentanty 0 a 1,
označ množinu reprezentantů $\mathcal{A}$.

Méně naivní postup hledání rozvoje v $\mathbb{Z}[i]$

$R = \mathbb{Z}[i]$ je okruh, $\beta = i - 1 \in R$, množina βR je ideál v R.
Kongruence definovaná

$$x \equiv y \mod \beta \Longleftrightarrow x - y \in \beta R$$

má dvě zbytkové třídy s reprezentanty 0 a 1,
označ množinu reprezentantů $\mathcal{A}$.

Algoritmus pro hledání rozvoje

Méně naivní postup hledání rozvoje v $\mathbb{Z}[i]$

$R = \mathbb{Z}[i]$ je okruh, $\beta = i - 1 \in R$, množina βR je ideál v R.
Kongruence definovaná

$$x \equiv y \mod \beta \Longleftrightarrow x - y \in \beta R$$

má dvě zbytkové třídy s reprezentanty 0 a 1,
označ množinu reprezentantů $\mathcal{A}$.

Algoritmus pro hledání rozvoje

Dané $z \in R$
$z_0 := z$
pokud $z_k \neq 0$ dělej
$a_k := z_k \mod \beta \in \mathcal{A}$
$z_{k+1} := \frac{1}{\beta}(z_k - a_k) \in R$

Které báze β jsou vhodné

Které báze β jsou vhodné

- R - obor integrity s normou N.
- $N : R \rightarrow \mathbb{R}^+$, taková že
  1. $N(a+b) \leq N(a) + N(b)$
  2. $N(a.b) = N(a).N(b)$
  3. $N(a) = 0 \Leftrightarrow a = 0$
- pro každé k je $\{r \in R | N(r) \leq k\}$ je konečná

Které báze β jsou vhodné

- R - obor integrity s normou N.
- $N : R \to \mathbb{R}^+$, taková že
  1. $N(a+b) \leq N(a) + N(b)$
  2. $N(a.b) = N(a).N(b)$
  3. $N(a) = 0 \Leftrightarrow a = 0$
- pro každé k je $\{r \in R | N(r) \leq k\}$ je konečná

Věta (Nielsen a Kornerup, 1999)

Nechť $\mathcal{A} \subset R$ je množina cifer tvořena reprezentanty všech zbytkových tříd mod β. Pak každý prvek okruhu R lze reprezentovat v bázi β s ciframi z $\mathcal{A}$ právě tehdy, když takto lze reprezentovat každé $r \in R$ s normou $N(r) \leq \frac{D_{Max}}{N(\beta)-1}$, kde $D_{Max} = \max\{N(a) | a \in \mathcal{A}\}$.

Které báze β jsou vhodné

Které báze β jsou vhodné

pro abecedu $\mathcal{A} = \{0, 1\}$?

Které báze β jsou vhodné

pro abecedu $\mathcal{A} = \{0, 1\}$?
Nutná podmínka: mod β má dvě zbytkové třídy.

Které báze β jsou vhodné

pro abecedu $\mathcal{A} = \{0, 1\}$?
Nutná podmínka: $\mod \beta$ má dvě zbytkové třídy.

Věta (Gauss)

Nechť $\beta \in \mathbb{Z}[i]$. Počet zbytkových tříd $\mod \beta$ je roven $N(\beta)$.

Které báze β jsou vhodné

pro abecedu $\mathcal{A} = \{0, 1\}$?
Nutná podmínka: $\mod \beta$ má dvě zbytkové třídy.

Věta (Gauss)

Nechť $\beta \in \mathbb{Z}[i]$. Počet zbytkových tříd $\mod \beta$ je roven $N(\beta)$.

$N(\beta) = 2 \quad \Longrightarrow \quad \beta = \pm 1 \pm i \quad \Longrightarrow$

Které báze β jsou vhodné

pro abecedu $\mathcal{A} = \{0, 1\}$?
Nutná podmínka: $\mod \beta$ má dvě zbytkové třídy.

Věta (Gauss)

Nechť $\beta \in \mathbb{Z}[i]$. Počet zbytkových tříd $\mod \beta$ je roven $N(\beta)$.

$N(\beta) = 2 \quad \Longrightarrow \quad \beta = \pm 1 \pm i \quad \Longrightarrow \quad 0, 1$ reprezentanti různých tříd

Které báze β jsou vhodné

pro abecedu $\mathcal{A} = \{0, 1\}$?
Nutná podmínka: $\mod \beta$ má dvě zbytkové třídy.

Věta (Gauss)

Nechť $\beta \in \mathbb{Z}[i]$. Počet zbytkových tříd $\mod \beta$ je roven $N(\beta)$.

$N(\beta) = 2 \implies \beta = \pm 1 \pm i \implies 0, 1$ reprezentanti různých tříd
báze $\beta = -i - 1$ je vhodná

Které báze β jsou vhodné

pro abecedu $\mathcal{A} = \{0, 1\}$?
Nutná podmínka: mod β má dvě zbytkové třídy.

Věta (Gauss)

Nechť $\beta \in \mathbb{Z}[i]$. Počet zbytkových tříd mod β je roven $N(\beta)$.

$N(\beta) = 2 \quad \Longrightarrow \quad \beta = \pm 1 \pm i \quad \Longrightarrow \quad 0, 1$ reprezentanti různých tříd
báze $\beta = -i - 1$ je vhodná
báze $\beta = i + 1$ není vhodná

Které báze β jsou vhodné

pro abecedu $\mathcal{A} = \{0, 1\}$?
Nutná podmínka: $\mod \beta$ má dvě zbytkové třídy.

Věta (Gauss)

Nechť $\beta \in \mathbb{Z}[i]$. Počet zbytkových tříd $\mod \beta$ je roven $N(\beta)$.

$N(\beta) = 2 \quad \Longrightarrow \quad \beta = \pm 1 \pm i \quad \Longrightarrow \quad 0, 1$ reprezentanti různých tříd
báze $\beta = -i - 1$ je vhodná
báze $\beta = i + 1$ není vhodná důvod: $i = (i + 1)i + 1$.

Které báze β jsou vhodné

pro abecedu $\mathcal{A} = \{0, 1\}$?
Nutná podmínka: $\mod \beta$ má dvě zbytkové třídy.

Věta (Gauss)

Nechť $\beta \in \mathbb{Z}[i]$. Počet zbytkových tříd $\mod \beta$ je roven $N(\beta)$.

$N(\beta) = 2 \implies \beta = \pm 1 \pm i \implies 0, 1$ reprezentanti různých tříd
báze $\beta = -i - 1$ je vhodná
báze $\beta = i + 1$ není vhodná důvod: $i = (i + 1)i + 1$.

Věta (Kátai, Szabó, 1975)

Nechť $\beta \in \mathbb{Z}[i]$ a $\mathcal{A} = \{0, 1, \dots, N(\beta) - 1\}$. Každé $z \in \mathbb{Z}[i]$ lze reprezentovat v bázi β s ciframi z abecedy $\mathcal{A}$ právě tehdy, když β je tvaru $-n \pm i$, kde $n \in \mathbb{N}, n \geq 1$.

Nelze zvolit lepší abecedu?

Nelze zvolit lepší abecedu?

Věta (Lagarias, 1996)

Nechť $\beta \in \mathbb{Z}[i]$ a $\mathcal{A} = \{-N(\beta)+1, \dots, -1, 0, 1, \dots, N(\beta)-1\}$. Každé $z \in \mathbb{Z}[i]$ lze reprezentovat v bázi β s ciframi z abecedy $\mathcal{A}$.

Nelze zvolit lepší abecedu?

Věta (Lagarias, 1996)

Nechť $\beta \in \mathbb{Z}[i]$ a $\mathcal{A} = \{-N(\beta)+1, \ldots, -1, 0, 1, \ldots, N(\beta)-1\}$. Každé $z \in \mathbb{Z}[i]$ lze reprezentovat v bázi β s ciframi z abecedy $\mathcal{A}$.

Věta (Milena, 2010)

Nechť $\beta \in \mathbb{Z}[i]$. Pak existuje takové $a \in \mathbb{N}$, že v abecedě $\mathcal{A} = \{-a, -a+1, \ldots, -1, 0, 1, \ldots, a-1\}$ lze sčítání v okruhu $\mathbb{Z}[i]$ provádět paraleně.

Děkuji za pozornost