

$$2 = (1+i)(1-i) = 1 - i^2$$

AD(3) : IRREDUCIBILNÍ PRVEK, KTERÝ NENÍ PRVOČINITEL

~~$$4 = 2 \cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3}) \text{ V OBORU } \mathbb{Z}[i\sqrt{3}]$$~~

→ DVA RŮZNÉ IRREDUCIBILNÍ ROZKLADY PRVKA 4

ALGEBRA I (NMAG 201) – TEST, 8. ÚNORA 2016

~~$$\text{PRVEK } 1 - i\sqrt{3} = 2 | (1+i\sqrt{3})(1-i\sqrt{3}) \text{ ALE } 2 \neq (1+i\sqrt{3}) \text{ ANI } 2 \neq (1-i\sqrt{3})$$~~

Tvrzení a definice pečlivě formulujte včetně všech předpokladů.

Odpovědi na otázky zdůvodněte. Pokud používáte nějaké netrieviální tvrzení z přednášky, uveďte explicitně odkaz (často budete vyzváni, abyste všechna použitá tvrzení zformulovali). Časový limit je 150 minut.

~~$$\mathbb{Z}[\sqrt{5}]: 4 = 2 \cdot 2 = (1+\sqrt{5})(1-\sqrt{5}) \quad 2|4 \text{ ALE } 2 \neq (\sqrt{5} \pm 1)$$~~

(1) Definujte charakteristiku okruhu.

3 NECHť R JE OKRUH.

CHARAKTERISTIKOU OKRUHU ROZUMÍME NEJMENTĚ TAKOVÉ NEN,

~~$$\checkmark \text{ ŽE } \underbrace{1+1+1+\dots}_{n\text{-KRÁT}} = 0; \text{ POKUD EXISTUJE;}$$~~

(3 body) ~~n-KRÁT~~ VINKA JE CHARAKTERISTIKA 0.

(2) Formulujte Čínskou větu o zbytcích.

2 NECHť m_1, m_2, \dots, m_n JSOU PODVOU NEPOUDĚLNÁ PŘIROZENÁ ČÍPRA; m_1, \dots, m_n LIBOVOLNÁ CELÁ ČÍPRA

~~$$M := m_1 \cdot m_2 \cdot \dots \cdot m_n; \text{ PAK } \exists! x \in \{1, \dots, M-1\}$$~~

(3 body) ~~TAKOVÉ, ŽE JE VPLNĚNA SOUPĀVA KONGRUENCÍ.~~

2 (3) Definujte v obecném oboru integrity pojmy irreducibilního prvku a prvočinitele. Uveďte příklad irreducibilního prvku v nějakém oboru integrity, který není prvočinitelem.

$$\begin{aligned} X &\equiv m_1 \pmod{m_1} \\ X &\equiv m_2 \pmod{m_2} \\ &\vdots \\ X &\equiv m_n \pmod{m_n} \end{aligned}$$

Příklad? NECHť R JE OBOR INTEGRITY.

- řekneme, že $a \in R$ je IRREDUCIBILNÍ PRVEK, pokud je nenulový, NEINVERTIBILNÍ A NEMÁ VLÁTNÍ DĚLITELE V R.
- PRVOČINITEL $a \in R$ je TAKOVÝ PRVEK, PRO KTERÝ PLATÍ: $\forall a \neq 0$

R - OBOR INTEGRITY (4) Definujte eukleidovskou normu a uveďte dva příklady.

EUKLEIDOVSKÁ NORMA $\nu: R \rightarrow \mathbb{N}^{(1)}$ JE TAKOVÉ ZOBRAZENÍ,

PRO KTERÉ (1) $\nu(0) = 0$

(2) Kdykoliv $a|b$; $a, b \in R$, $b \neq 0$

(4 body) $\nu(a) \leq \nu(b)$

1 KOMPATABILITY A DĚLITELNOSTI

(3) KONTRAKTní DĚLENÍ

$b \neq 0$

PRO KARŽDOLU DVOJICI PRVKŮ $a, b \in R$ $\exists m, \nu$,

ŽE: $a = m \cdot b + \nu$, PRÍČEMŽ $\nu(0) < \nu(b)$

PŘÍKLADY:

$R = \mathbb{Z}$ EUKLEIDOVSKÁ
a $\in R$ NORMA: $\nu(a) = |a|$

4b. (5) Najděte v $\mathbb{R}[x]$ polynom co nejmenšího stupně, aby
 $f(-1) = 2, f(1) = 0, f(2) = 2 \quad a \quad f(4) = 12.$

1) POLYNOM STUPNĚ 1

$$f(x) = ax + b$$

$$2 = -a + b$$

$$0 = a + b$$

$$2 = 2a + b$$

$$12 = 4a + b$$

NEEXISTUJE
(4 body)

2) POLYNOM STUPNĚ 2

$$f(x) = ax^2 + bx + c$$

$$2 = a - b + c$$

$$0 = a + b + c$$

$$2 = 4a + 2b + c$$

$$12 = 16a + 4b + c$$

(*) POKRAČOVÁNÍ

$$\begin{array}{r} 2 \\ 0 \\ 2 \\ \hline 2 \end{array}$$

$$2 = 2a + 2c$$

$$2 = 2a + 2c$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 4 & 2 & 1 & 2 \\ 16 & 4 & 1 & 12 \end{array} \right)$$

4b. (6) Platí $3x^2 - 1 \parallel x^2 + 2$ v oboru a) $\mathbb{Q}[x]$, b) $\mathbb{Z}_5[x]$, c) $\mathbb{Z}_7[x]$?

• $\mathbb{Q}[x]$ PLATÍ $3x^2 - 1 \parallel x^2 + 2$; NEBOŽ $3x^2 - 1 \neq$ LITI

CD POLYNOMU $x^2 + 2$ POUZE PŘENÁJOZENÍM 5 -

A TO JE INVERTIBILNÍ PRVEK; Tl. $\exists \cdot \tilde{x} \cdot (\tilde{x} \cdot (3x^2 - 1)) = x^2 + 2$

(4 body) PRVEK \tilde{x} JE INVERTIBILNÍ V \mathbb{Q} , NEBOŽ \tilde{x} JE TELENKO

(7) Pro která z následujících těles T existuje irreducibilní polynom stupně

2b. 3 v $T[x]$: a) \mathbb{Z}_3 , b) \mathbb{Q} , c) \mathbb{C} ? V každém ze tří případů odpověď zdůvodněte. Kde irreducibilní polynom existuje, uveďte příklad.

• V $\mathbb{C}[x]$ KŽDNÝ IRREDUCIBILNÝ POLYNOM STUPNĚ 3 NEEXISTUJE,
 NEBOŽ KOMPLEXNÍ ČÍLA VRCU ALGEBRAICKY UZAVŘENÉ TELENKO,
 PROTO JE KŽDÝ POLYNOM ROZKLÁDÁ NA VONČIN POLYNOMŮ
 STUPNĚ 1 - (VIZ. KOMPLEXNÍ ANALÝZA)

(5 bodů)

(*) POKRAČOVÁNÍ

2b. (8) Kolik prvků řádu 4 obsahují grupy $(\mathbb{Z}_{17}, +, -, 0)$ a $(\mathbb{Z}_{17}^*, \cdot, ^{-1}, 1)$?
NEHENYI Které konkrétně prvky to jsou?

KĀD PRVKU NEYTAKOVÉ ČÍLO, KOLIKRÁT MUSÍME PRVEK SLOŽIT NEBOU
 JAMÝM, ABYCHOM DOPALI VEDNOTKU.

$$\forall (\mathbb{Z}_{17}^*, \cdot, ^{-1}, 1) : 2 \cdot 2 \cdot 2 \cdot 2 = 16 \neq 1$$

$$(5 \text{ bodů}) \quad 3 \cdot 3 \cdot 3 \cdot 3 = 81 \neq 1$$

$$4 \cdot 4 \cdot 4 \cdot 4 = 256 \Rightarrow 4 \text{ NE PRVEK ŘÁDU } 4 \quad \checkmark$$

$$5 \cdot 5 \cdot 5 \cdot 5 = 625 \Rightarrow 5 \cdot 5 = 25 \cdot 25 = 625 \neq 1$$

$$6 \cdot 6 \cdot 6 \cdot 6 = 1296 \neq 1$$

$$7 \cdot 7 \cdot 7 \cdot 7 = 2401 \Rightarrow 7 \text{ NE PRVEK ŘÁDU } 4 \quad \checkmark$$

$$8 \cdot 8 \cdot 8 \cdot 8 = 4096 \Rightarrow 8 \text{ NE PRVEK ŘÁDU } 4 \quad \checkmark$$

$$9 \cdot 9 \cdot 9 \cdot 9 = 6561 \neq 1$$

$$10 \cdot 10 \cdot 10 \cdot 10 = 10000 \neq 1$$

$$11 \cdot 11 \cdot 11 \cdot 11 = 14641 \neq 1$$

$$12 \cdot 12 \cdot 12 \cdot 12 = 17280 \neq 1$$

$$13 \cdot 13 \cdot 13 \cdot 13 = 2197 \neq 1$$

$$14 \cdot 14 \cdot 14 \cdot 14 = 2744 \neq 1$$

$$15 \cdot 15 \cdot 15 \cdot 15 = 3375 \neq 1$$

$$16 \cdot 16 \cdot 16 \cdot 16 = 4096 \neq 1$$

$$17 \cdot 17 \cdot 17 \cdot 17 = 4913 \neq 1$$

$$18 \cdot 18 \cdot 18 \cdot 18 = 5832 \neq 1$$

$$19 \cdot 19 \cdot 19 \cdot 19 = 6859 \neq 1$$

$$20 \cdot 20 \cdot 20 \cdot 20 = 8000 \neq 1$$

$$21 \cdot 21 \cdot 21 \cdot 21 = 9261 \neq 1$$

$$22 \cdot 22 \cdot 22 \cdot 22 = 10648 \neq 1$$

$$23 \cdot 23 \cdot 23 \cdot 23 = 12167 \neq 1$$

$$24 \cdot 24 \cdot 24 \cdot 24 = 13824 \neq 1$$

$$25 \cdot 25 \cdot 25 \cdot 25 = 15625 \neq 1$$

$$26 \cdot 26 \cdot 26 \cdot 26 = 17576 \neq 1$$

$$27 \cdot 27 \cdot 27 \cdot 27 = 19683 \neq 1$$

$$28 \cdot 28 \cdot 28 \cdot 28 = 21952 \neq 1$$

$$29 \cdot 29 \cdot 29 \cdot 29 = 24337 \neq 1$$

$$30 \cdot 30 \cdot 30 \cdot 30 = 26244 \neq 1$$

$$31 \cdot 31 \cdot 31 \cdot 31 = 28147 \neq 1$$

$$32 \cdot 32 \cdot 32 \cdot 32 = 30072 \neq 1$$

$$33 \cdot 33 \cdot 33 \cdot 33 = 32000 \neq 1$$

$$34 \cdot 34 \cdot 34 \cdot 34 = 33936 \neq 1$$

$$35 \cdot 35 \cdot 35 \cdot 35 = 35875 \neq 1$$

$$36 \cdot 36 \cdot 36 \cdot 36 = 37824 \neq 1$$

$$37 \cdot 37 \cdot 37 \cdot 37 = 39791 \neq 1$$

$$38 \cdot 38 \cdot 38 \cdot 38 = 41760 \neq 1$$

$$39 \cdot 39 \cdot 39 \cdot 39 = 43736 \neq 1$$

$$40 \cdot 40 \cdot 40 \cdot 40 = 45712 \neq 1$$

$$41 \cdot 41 \cdot 41 \cdot 41 = 47691 \neq 1$$

$$42 \cdot 42 \cdot 42 \cdot 42 = 49672 \neq 1$$

$$43 \cdot 43 \cdot 43 \cdot 43 = 51653 \neq 1$$

$$44 \cdot 44 \cdot 44 \cdot 44 = 53636 \neq 1$$

$$45 \cdot 45 \cdot 45 \cdot 45 = 55617 \neq 1$$

$$46 \cdot 46 \cdot 46 \cdot 46 = 57600 \neq 1$$

$$47 \cdot 47 \cdot 47 \cdot 47 = 59583 \neq 1$$

$$48 \cdot 48 \cdot 48 \cdot 48 = 61568 \neq 1$$

$$49 \cdot 49 \cdot 49 \cdot 49 = 63551 \neq 1$$

$$50 \cdot 50 \cdot 50 \cdot 50 = 65536 \neq 1$$

$$51 \cdot 51 \cdot 51 \cdot 51 = 67521 \neq 1$$

$$52 \cdot 52 \cdot 52 \cdot 52 = 69508 \neq 1$$

$$53 \cdot 53 \cdot 53 \cdot 53 = 71496 \neq 1$$

$$54 \cdot 54 \cdot 54 \cdot 54 = 73484 \neq 1$$

$$55 \cdot 55 \cdot 55 \cdot 55 = 75472 \neq 1$$

$$56 \cdot 56 \cdot 56 \cdot 56 = 77461 \neq 1$$

$$57 \cdot 57 \cdot 57 \cdot 57 = 79451 \neq 1$$

$$58 \cdot 58 \cdot 58 \cdot 58 = 81440 \neq 1$$

$$59 \cdot 59 \cdot 59 \cdot 59 = 83431 \neq 1$$

$$60 \cdot 60 \cdot 60 \cdot 60 = 85424 \neq 1$$

$$61 \cdot 61 \cdot 61 \cdot 61 = 87417 \neq 1$$

$$62 \cdot 62 \cdot 62 \cdot 62 = 89411 \neq 1$$

$$63 \cdot 63 \cdot 63 \cdot 63 = 91406 \neq 1$$

$$64 \cdot 64 \cdot 64 \cdot 64 = 93401 \neq 1$$

$$65 \cdot 65 \cdot 65 \cdot 65 = 95397 \neq 1$$

$$66 \cdot 66 \cdot 66 \cdot 66 = 97394 \neq 1$$

$$67 \cdot 67 \cdot 67 \cdot 67 = 99392 \neq 1$$

$$68 \cdot 68 \cdot 68 \cdot 68 = 101391 \neq 1$$

$$69 \cdot 69 \cdot 69 \cdot 69 = 103391 \neq 1$$

$$70 \cdot 70 \cdot 70 \cdot 70 = 105392 \neq 1$$

$$71 \cdot 71 \cdot 71 \cdot 71 = 107394 \neq 1$$

$$72 \cdot 72 \cdot 72 \cdot 72 = 109397 \neq 1$$

$$73 \cdot 73 \cdot 73 \cdot 73 = 111401 \neq 1$$

$$74 \cdot 74 \cdot 74 \cdot 74 = 113406 \neq 1$$

$$75 \cdot 75 \cdot 75 \cdot 75 = 115411 \neq 1$$

$$76 \cdot 76 \cdot 76 \cdot 76 = 117417 \neq 1$$

$$77 \cdot 77 \cdot 77 \cdot 77 = 119424 \neq 1$$

$$78 \cdot 78 \cdot 78 \cdot 78 = 121431 \neq 1$$

$$79 \cdot 79 \cdot 79 \cdot 79 = 123440 \neq 1$$

$$80 \cdot 80 \cdot 80 \cdot 80 = 125450 \neq 1$$

$$81 \cdot 81 \cdot 81 \cdot 81 = 127461 \neq 1$$

$$82 \cdot 82 \cdot 82 \cdot 82 = 129474 \neq 1$$

$$83 \cdot 83 \cdot 83 \cdot 83 = 131488 \neq 1$$

$$84 \cdot 84 \cdot 84 \cdot 84 = 133503 \neq 1$$

$$85 \cdot 85 \cdot 85 \cdot 85 = 135520 \neq 1$$

$$86 \cdot 86 \cdot 86 \cdot 86 = 137538 \neq 1$$

$$87 \cdot 87 \cdot 87 \cdot 87 = 139557 \neq 1$$

$$88 \cdot 88 \cdot 88 \cdot 88 = 141577 \neq 1$$

$$89 \cdot 89 \cdot 89 \cdot 89 = 143598 \neq 1$$

$$90 \cdot 90 \cdot 90 \cdot 90 = 145621 \neq 1$$

$$91 \cdot 91 \cdot 91 \cdot 91 = 147645 \neq 1$$

$$92 \cdot 92 \cdot 92 \cdot 92 = 149670 \neq 1$$

$$93 \cdot 93 \cdot 93 \cdot 93 = 151700 \neq 1$$

$$94 \cdot 94 \cdot 94 \cdot 94 = 153731 \neq 1$$

$$95 \cdot 95 \cdot 95 \cdot 95 = 155764 \neq 1$$

$$96 \cdot 96 \cdot 96 \cdot 96 = 157800 \neq 1$$

$$97 \cdot 97 \cdot 97 \cdot 97 = 159837 \neq 1$$

$$98 \cdot 98 \cdot 98 \cdot 98 = 161876 \neq 1$$

$$99 \cdot 99 \cdot 99 \cdot 99 = 163917 \neq 1$$

$$100 \cdot 100 \cdot 100 \cdot 100 = 166000 \neq 1$$

$$101 \cdot 101 \cdot 101 \cdot 101 = 168081 \neq 1$$

$$102 \cdot 102 \cdot 102 \cdot 102 = 170164 \neq 1$$

$$103 \cdot 103 \cdot 103 \cdot 103 = 172249 \neq 1$$

$$104 \cdot 104 \cdot 104 \cdot 104 = 174336 \neq 1$$

$$105 \cdot 105 \cdot 105 \cdot 105 = 176424 \neq 1$$

$$106 \cdot 106 \cdot 106 \cdot 106 = 178513 \neq 1$$

$$107 \cdot 107 \cdot 107 \cdot 107 = 180603 \neq 1$$

$$108 \cdot 108 \cdot 108 \cdot 108 = 182694 \neq 1$$

$$109 \cdot 109 \cdot 109 \cdot 109 = 184787 \neq 1$$

$$110 \cdot 110 \cdot 110 \cdot 110 = 186881 \neq 1$$

$$111 \cdot 111 \cdot 111 \cdot 111 = 188976 \neq 1$$

$$112 \cdot 112 \cdot 112 \cdot 112 = 191072 \neq 1$$

$$113 \cdot 113 \cdot 113 \cdot 113 = 193170 \neq 1$$

$$114 \cdot 114 \cdot 114 \cdot 114 = 195269 \neq 1$$

$$115 \cdot 115 \cdot 115 \cdot 115 = 197369 \neq 1$$

$$116 \cdot 116 \cdot 116 \cdot 116 = 199470 \neq 1$$

$$117 \cdot 117 \cdot 117 \cdot 117 = 201573 \neq 1$$

$$118 \cdot 118 \cdot 118 \cdot 118 = 203677 \neq 1$$

$$119 \cdot 119 \cdot 119 \cdot 119 = 205782 \neq 1$$

$$120 \cdot 120 \cdot 120 \cdot 120 = 207888 \neq 1$$

$$121 \cdot 121 \cdot 121 \cdot 121 = 209996 \neq 1$$

<math display

- (9) Vezměte množinu T všech polynomů nad \mathbb{Z}_3 stupně nejvýše 3 spolu s operacemi sčítání a násobení modulo

$$f = x^4 - x - 1$$

(tento polynom je ireducibilní v $\mathbb{Z}_3[x]$, čili T je těleso o 81 prvcích). Najděte v T multiplikativní inverzi prvku $x^2 + 1$.

(7 bodů)

- (10) Formulujte kritérium pro určení násobnosti kořenu polynomu $f \in R[x]$ pomocí formálních derivací f' pro obecný obor integrity R .

Najděte všechny prvky $a \in \mathbb{Z}_{103}$, pro které má $x^3 + 9x + a$ v \mathbb{Z}_{103} násobný kořen. Svůj výsledek zdůvodněte.

(10 bodů)

- (11) Najděte všechna kladná celočíselná řešení soustavy kongruencí

$$\begin{aligned} x^2 &\equiv -1 \pmod{17}, \\ 2^x &\equiv -1 \pmod{17}. \end{aligned}$$

(10 bodů)

- (12) Definujte pojmy levé rozkladové třídy grupy podle podgrupy a transverzálu levého rozkladu grupy podle podgrupy.

Uvažujte permutační grupu $(S_4, \circ, -1, \text{id})$ a podmnožinu H všech permutací π takových, že $\pi(1) = 1$. Ukažte, že H je podgrupa S_4 a najděte transverzálu levého rozkladu S_4 podle H .

(12 bodů)

- (13) Přesně formulujte a dokažte charakterizaci Gaussových oborů pomocí existence NSD a podmínky na řetězce dělitelů.

(14 bodů)

OBOR INTEGRITÉ R JE GAUSSŮV PRÁVĚ TEHDY, KDYŽ:

• PRO KAŽDOU DVOJICI PRVKŮ EXISTUJE NWD

(TJ. $\forall a, b \in R \exists NWD(a, b)$)

• NEEXISTUJE ŽÁDNÁ KLEJAHÍCÍ POROUPNOST a_1, a_2, a_3, \dots ;

$a_i \in R$ až i TAKOVÁ, že $a_{i+1} \mid a_i$; přičemž $a_i \neq a_{i+1}$

K důkazu potřebujeme: 1) Lemma: $NWD(c a, c b) = c \cdot NWD(a, b)$

2) Existuje-li v oboru integrity R NWD všech dvojic prvků, pak platí, že kazdý ireducibilní prvek v R je prvočísel.