MIN401 Matematika IV - příklady počítané na cvičení (jarní semestr 2021)

1 1. týden – středoškolská dělitelnost

Cvičení konané 14. 2. 2021.

Příklad 1.1: Jak poznáme, že je celé číslo dělitelné 2, 3, 4, 5, 6, 8, 9, 10, 11? Svá tvrzení zdůvodněte.

Příklad 1.2: Ukažte, že součin pěti po sobě jdoucích čísel je dělitelný 120.

Příklad 1.3: Nejdříve pro $n = 2, 3$ a potom pro další $n \in \mathbb{N}$ si připomeňte

a) vzorec pro rozdíl n-tých mocnin dvou čísel,

b) vzorec pro součet n-tých mocnin dvou čísel,

c) vzorec pro n-tou mocninu součtu, tzv. binomický vzorec.

Příklad 1.4: [10.2] Dokažte, že pro libovolné $a \in \mathbb{Z}$ platí:

(i) a^2 dává po dělení čtyřmi zbytek 0 nebo 1,

(ii) a^2 dává po dělení osmi zbytek 0, 1 nebo 4,

(iii) a^4 dává po dělení šestnácti zbytek 0 nebo 1.

Příklad 1.5:

(i) Ukažte, že pro každé $n \in \mathbb{N}$ platí $3|4^n - 1$.

(ii) Ukažte, že pro každé $n \in \mathbb{N}$ platí $5|n^5 - n$.

(iii) Ukažte, že pro každé $n \in \mathbb{N}$ platí $5|3^{3n+1} + 2^{n+1}$.

Příklad 1.6: [10.1] Určete, pro která přirozená čísla $n \in \mathbb{N}$ je číslo $n^3 + 1$ dělitelné číslem $n - 1$.

Příklad 1.7: Dokažte, že pro přirozená čísla a, k a n platí: jestliže $k \mid n$, pak $a^k - 1 \mid a^n - 1$. Pomocí toho dokažte: Je-li $2^n - 1$ prvočíslo, pak n musí být také prvočíslo. Proto se “největší” prvočísla hledají ve tvaru $2^p - 1$, kde p je prvočíslo.

Příklad 1.8: Dokažte, že $25 \mid 4^{2n+1} - 10n - 4$.

Příklad 1.9:

(i) Nechť $a, b \in \mathbb{N}$, $a \neq b$. Ukažte, že existuje nekonečně mnoho přirozených čísel n takových, že čísla $a + n$ a $b + n$ jsou nesoudělná.

(ii) Nechť má číslo $n \in \mathbb{N}$, $n > 1$ následující vlastnost: pro každou dvojici dělitelů $a > 1$, $b > 1$ čísla n platí, že $(a, b) > 1$. Co můžeme říci o čísle n?

Příklad 1.10: [10.10]

(i) Dokažte, že jsou-li čísla $m, n \in \mathbb{N}$ nesoudělná, jsou nesoudělná i čísla

$$m^2 + mn + n^2 \quad \text{a} \quad m^2 - mn + n^2.$$

(ii) Dokažte, že jsou-li lichá čísla $m, n \in \mathbb{N}$ nesoudělná, jsou nesoudělná i čísla

$$m + 2n \quad \text{a} \quad m^2 + 4n^2.$$

2 2. týden – kongruence, Eulerova funkce

Cvičení konané 10. 3. 2021.

Příklad 2.1: [10.4 a 10.5] Určete největší společný dělitel čísel $a, b \in \mathbb{Z}$ a určete příslušné koeficienty v Bezoutově rovnosti:

(i) $a = 10175$ a $b = 2277$,

(ii) $a = 2^{49} - 1$ a $b = 2^{35} - 1$.

Příklad 2.2: [10.11])

(i) Nalezněte zbytek po dělení čísla 7^{30} číslem 50.

(ii) Určete poslední dvě cifry dekadického zápisu čísla 7^{30}.

Příklad 2.3: [10.15 a 10.16]

(i) Nechť $m, n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$ splňují $a \equiv b \pmod{m^n}$. Ukažte, že pak $a^m \equiv b^m \pmod{m^{n+1}}$

(ii) Ukažte, že lichá čísla a splňují $a^4 \equiv 1 \pmod{16}$.

(iii) Ukažte, že čísla a nedělitelná třemi splňují $a^3 \equiv \pm 1 \pmod{9}$.

Příklad 2.4: [10.17] Pro číslo $n \in \mathbb{N}$ označuje $S(n)$ ciferný součet čísla n.

(i) Zopakujte si pravidla po dělitelnost 2, 3, 4, 5, 6, 8, 9.

(ii) Ukažte, že $n \equiv S(n) \pmod 9$.

(iii) Pravidlo pro dělitelnost 11.

(iv) Ukažte, že pro $n = 1000a + b$ platí $n \equiv -a + b \pmod m$, kde $m \in \{7, 11, 13\}$.

Příklad 2.5: [10.19, 10.20, 10.21]

(i) Určete $\varphi(72)$.

(ii) Dokažte, že pro každé $n \in \mathbb{N}$ platí $\varphi(4n + 2) = \varphi(2n + 1)$.

(iii) Určete všechna $n \in \mathbb{N}$ taková, že $\varphi(n)$ je liché.

(iv) Určete všechna $n \in \mathbb{N}$ taková, že $\varphi(n) = 30$.

(v) Určete všechna $n \in \mathbb{N}$ taková, že $\varphi(n) = \frac{n}{3}$.

Příklad 2.6: [10.24, 10.26, 10.28, 10.29]

(i) Určete poslední dvojčíslí čísla 7^{2013}.

(ii) Určete zbytek po dělení čísla $2^{50} + 3^{50} + 4^{50}$ číslem 17.

(iii) Určete poslední číslici čísla $7^{9^{7^{5^3}}}$.

(iv) Určete poslední číslici čísla $14^{14^{14}}$.

3 3. týden – RSA šifry, primitivní kořeny

Cvičení konané 18. 3. 2021.

Příklad 3.1: Veřejný klíč Honzy pro RSA šifru je $(91, 23)$. Zachytili jste jemu určenou zprávu 3. Dekódujte ji.

Příklad 3.2: [10.32, 10.33, slidy] Najděte primitivní kořeny modulo 8, 11, 41 a 41^2.

4 4. týden – řešení kongruencí

Cvičení konané 25. 3. 2021.

Příklad 4.1: Vyřešte následující kongruence:

(i) $5x \equiv 12 \pmod{23}$.

(ii) $33x \equiv 7 \pmod{143}$.

(iii) $210x \equiv 40 \pmod{212}$.

Příklad 4.2: Vyřešte následující soustavy kongruenci:

(i) $2x \equiv 3 \pmod{7}$, $x \equiv 8 \pmod{15}$.

(ii) $x \equiv 3 \pmod{10}$, $x \equiv 8 \pmod{15}$, $x \equiv 5 \pmod{84}$.

Příklad 4.3: [10.48, 10.57, 10.58] Vyřešte následující kongruence:

(i) $7x^{17} \equiv 11 \pmod{41}$.

(ii) $x^3 \equiv 3 \pmod{18}$,

(iii) $x^2 \equiv 18 \pmod{63}$.

5 5. týden – kongruence, šifrování

Cvičení konané 31. 3. 2021.

Příklad 5.1: Vyřešte následující kongruence:

(i) $x^2 \equiv 1 \pmod{30}$,

(ii) $x^3 + x + 3 \equiv 0 \pmod{25}$,

(iii) $5x^2 + x + 8 \equiv 0 \pmod{11}$,

Příklad 5.2: Spočtěte následující Legendreův nebo Jacobiho symbol

$$\left(\frac{101}{1987}\right), \qquad \left(\frac{-35}{97}\right), \qquad \left(\frac{-23}{85}\right).$$

Příklad 5.3: [Odjinud, 10.67, 10.68] Rozhodněte, zda následující kongruence mají řešení:

(i) $x^2 \equiv 5 \pmod{227}$,

(ii) $x^2 \equiv 5 \pmod{229}$,

(iii) $x^2 \equiv 38 \pmod{65}$,

(iv) $x^2 - 23 \equiv 0 \pmod{77}$.

Příklad 5.4: [10.93] Šifrování:

(i) Ukažte, jak pomocí Rabinova kryptosystému s veřejným klíčem $n = 437$ zašifrovat a pak dešifrovat zprávu $M = 321$.

(ii) Martin a Honza chtějí komunikovat šifrou ElGamal. Martin si zvolil prvočíslo 41 s primitivním kořenem 11 a tajný klíč 10, tj. zveřejnil $(41, 11, A)$, kde $A \equiv 11^{10} \pmod{41}$. Honza mu poslal veřejným kanálem dvojici $(22, 6)$. Jakou zprávu Honza poslal?

(iii) Veřejný klíč Honzy pro RSA šifrování je $(33, 3)$. Někdo mu poslal zprávu 7, kterou jste zachytili. Dekódujte ji.

6 6. týden – Booleovské algebry, uspořádané množiny

Cvičení konané 7. 4. 2021.

Příklad 6.1: Budeme pracovat s výrazy ve výrokové logice.

(i) Zjednodušte výraz $(A \wedge B \wedge C) \vee (A' \wedge B) \vee (A \wedge B \wedge C')$.

(ii) [11.116] Nalezněte úplnou disjunktní formu výrazu $(B' \Rightarrow C) \wedge [(A \vee C) \wedge B]'$.

Příklad 6.2: [11.124] Určete všechny relací uspořádání na čtyřprvkové množině. Pro každý z neizomorfních typů určete, zda se jedná o svaz. Vyskytuje se mezi uspořádáními Booleova algebra?

Příklad 6.3: [11.126, 11.127] Nakreslete Hasseho diagram svazu dělitelů čísla 36. Je tento svaz distributivní? Jedná se o Booleovu algebru? Pak určete totéž pro dělitele čísla 30.

Příklad 6.4: [11.131] Rozhodněte, zda každý řetězec, který má největší a nejmenší prvek, je úplný svaz.

Příklad 6.5: [11.133] Rozhodněte, zda je množina konvexních podmnožin v $\mathbb{R}^3$ svazem pro vhodné operace suprema a infima. Pokud ano, je tento svaz úplný či distributivní?

7 7. týden – Polynomy

Cvičení konané 14. 4. 2021.

Příklad 7.1: [11.76] Rozložte nad $\mathbb{R}$ a $\mathbb{C}$ polynom

$$f(x) = x^4 + 2x^3 + 3x^2 + 2x + 1.$$

Příklad 7.2: [11.77.] Rozložte polynom $f(x) = x^5 + 3x^3 + 3$ nad $\mathbb{Q}$ and $\mathbb{Z}_7$.

Příklad 7.3: [11.80] Najděte všechny ireducibilní polynomy stupně ≤ 2 nad $\mathbb{Z}_3$.

Příklad 7.4: [11.81] Rozhodněte, zda je polynom $x^4 + x^3 + x + 2$ ireducibilní nad $\mathbb{Z}_3$.

8 8. týden – polynomy II.

Cvičení konané 22. 4. 2021.

Příklad 8.1: [11.79]

(i) Eisensteinovo kritérium ireducibility nad $\mathbb{Z}$ (tedy i nad $\mathbb{Q}$).

(ii) Určete polynom s racionálními koeficienty co nejmenšího stupně, jehož kořenem je číslo $\sqrt[2007]{2}$.

Příklad 8.2: [11.82, 11.83]

(i) Pro liché prvočíslo p určete všechny kořeny polynomu

$$f(x) = x^{p-2} + x^{p-3} + \ldots + x + 2.$$

(ii) Rozložte polynom $g(x) = x^2 + x + 1$ v $\mathbb{Z}_5[x]$ and $\mathbb{Z}_7[x]$.

Příklad 8.3: [11.84, 11.84]

(i) Rozložte polynom $f(x) = x^6 - x^4 - 5x^2 - 3$ v $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}_5[x]$ a $\mathbb{Z}_7[x]$ víte-li o něm, že má vícenásobný kořen.

(ii) Rozložte polynom $p(x) = x^6 + x^5 + 4x^4 + 2x^3 + 5x^2 + x + 2$ v $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_2[x]$, $\mathbb{Z}_5[x]$ a $\mathbb{Z}_7[x]$ víte-li o něm, že má vícenásobný kořen i.

(iii) Řešte soustavu $p(x) = q(x) = 0$ nad $\mathbb{C}$, kde $q(x) = x^2y^2 + y^2 + xy + x^2y + 2y + 1$.

9 9. týden – okruhy

Cvičení konané 28. 4. 2021.

Příklad 9.1: [11.65] Rozhodněte, zda množina R s operacemi $\oplus$ a $\odot$ tvoří okruh, komutativní okruh, obor integrity nebo těleso.

(i) $R = \mathbb{Z}$, $a \oplus b = a + b + 3$, $a \odot b = -3$. [Není okruh.]

(ii) $R = \mathbb{Z}$, $a \oplus b = a + b - 3$, $a \odot b = a \cdot b - 1$. [Není okruh.]

(iii) $R = \mathbb{Z}$, $a \oplus b = a + b - 1$, $a \odot b = a + b - a \cdot b$. [Je obor integrity.]

(iv) $R = \mathbb{Q}$, $a \oplus b = a + b$, $a \odot b = b$. [Není okruh.]

(v) $R = \mathbb{Q}$, $a \oplus b = a + b + 1$, $a \odot b = a + b + ab$. [Je těleso.]

(vi) $R = \mathbb{Q}$, $a \oplus b = a + b - 1$, $a \odot b = a + b + ab$. [Není okruh.]

Příklad 9.2: [11.66] Dokažte, že podmožina komplexních čísel $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ tvoří obor integrity. Jedná se o těleso?

Příklad 9.3: [11.67] V okruhu matic $Mat_{2,2}(\mathbb{R})$ uvažme podokruh matic tvaru

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

$a, b \in \mathbb{R}$. Dokažte, že tento podokruh je izomorfní s tělesem $\mathbb{C}$.

Příklad 9.4: [11.68] Ukažte, že identita je jediný automorfismu tělesa reálných čísel.

10 10. týden – grupy I.

Cvičení konané 5. 5. 2021.

Příklad 10.1: [11.1] Rozhodněte o následujících množinách a operacích, jakou algebraickou strukturu tvoří (grupoid, monoid, pologrupa, grupa):

(i) podmnožiny množiny přirozených čísel s operací sjednocení [monoid],

(ii) množina $\mathbb{N}$ spolu s binární operací největší společný dělitel [polorupa],

(iii) množina $\mathbb{N}$ spolu s binární operací nejmenší společný násobek [monoid],

(iv) množina reálných invertibilních matic 2x2 spolu s operací sčítání matic [není ani grupoid],

(v) množina reálných matic 2x2 spolu s operací násobení matic [monoid],

(vi) množina reálných matic 2x2 spolu s operací odčítán ímatic [grupoid],

(vii) množina invertibilních matic 2x2 nad $\mathbb{Z}_2$ spolu s operací násobení matic [grupa],

(viii) množina $\mathbb{Z}_6$ spolu s operací násobení (modulo 6) [monoid],

(ix) množina $\mathbb{Z}_7$ spolu s operací násobení (modulo 7) [grupa].

Příklad 10.2: 11.8 Na množině $(\mathbb{R} \setminus \{0\}) \times \mathbb{R}$ definujeme operaci $\odot$ jako

$$(x, y) \odot (u, v) = (xu, xv + y).$$

Popište, o jakou algebraickou strukturu se jedná.

Příklad 10.3: [2.19] Rozložte následující permutaci v $\mathbb{S}_9$ na součin transpozic:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 6 & 7 & 8 & 9 & 5 & 4 & 2 \end{pmatrix}.$$

Příklad 10.4: [11.10] Určete znaménko následujících permutací v $\mathbb{S}_{3n}$ a $\mathbb{S}_{2n}$:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 3n-2 & 3n-1 & 3n \\ 2 & 3 & 1 & 5 & 6 & 4 & \dots & 3n-1 & 3n & 3n-2 \end{pmatrix},$$
$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & n+2 & \dots & 2n \\ 2 & 4 & 6 & \dots & 2n & 1 & 3 & \dots & 2n-1 \end{pmatrix}.$$

Příklad 10.5: [11.13] Mějme permutaci $\sigma \in \mathbb{S}_7$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 2 & 4 \end{pmatrix}.$$

V grupě $(\mathbb{S}_7, \circ)$ určete řád σ, inverzi k σ, σ^{2013} a ukažte, že σ nekomutuje s transpozicí $\tau = (2, 3)$.

Příklad 10.6: [11.16,11.17] Dokažte, že neexistuje čtyřprvková ani pětiprvková nekomutativní grupa.

11 11. týden – grupy II.

Cvičení konané 12. 5. 2021.

Příklad 11.1: [11.19] Určete (až na izomorfismus) vsechny komutativní grupy řádu 8. Potom určete, ketrým z těchto grup jsou izomorfní grupy

(i) $\mathbb{Z}_{15}^{\times}$,

(ii) $\mathbb{Z}_{16}^{\times}$,

(iii) $\mathbb{Z}_{17}^{\times}/\{\pm 1\}$,

(iv) komplexní kořeny polynomu $z^8 - 1 = 0$ s násobením.

Příklad 11.2: [11.25] Nechť G je grupa dolních trojúhelníkových matic 3×3 s jedničkami na diagonále a operací násobení.

(i) Ukažte, že $G \subseteq GL(3, \mathbb{R})$ je podgrupa a rozhodněte, zda je normální.

(ii) Určete centrum $Z(G) = \{z \in G | \forall g \in G : zg = gz\}$.

Příklad 11.3: [11.38, 11.41, 11.42] Podgrupy v symetrických grupách.

12 12. týden – homomosfismy grup, kódy

Cvičení konané 19. 5. 2021.

Příklad 12.1: [11.48] Rozhodněte, zda předpis φ zadává zobrazení, případně zda jde o homomorfismus grup (se sčítáním) – pak popište jádro/obraz a rozhodněte, zda je to surjekce či injekce:

(i) $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi([[a]_4, [b]_3) = [a - b]_{12}$,

(ii) $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi([[a]_4, [b]_3) = [6a + 4b]_{12}$,

(iii) $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi([[a]_4, [b]_3) = [0]_{12}$.

Příklad 12.2: [11.49] Rozhodněte, zda předpis φ zadává zobrazení, případně zda jde o homomorfismus grup ($\mathbb{Z}_k$ se sčítáním a $\mathbb{C}^*$ s násobením) – pak popište jádro/obraz a rozhodněte, zda je to surjekce či injekce:

(i) $\varphi : \mathbb{Z}_4 \to \mathbb{C}^*$, $\varphi([[a]_4) = i^a$,

(ii) $\varphi : \mathbb{Z}_5 \to \mathbb{C}^*$, $\varphi([[a]_5) = i^a$,

(iii) $\varphi : \mathbb{Z}_4 \to \mathbb{C}^*$, $\varphi([[a]_4) = (-i)^a$,

(iv) $\varphi : \mathbb{Z} \to \mathbb{C}^*$, $\varphi(a) = i^a$

Příklad 12.3: [11.136] Uvažme $(5, 3)$-kód nad $\mathbb{Z}_2$ generovaný polynomem $x^2 + x + 1$. Vypište všechna kódová slova, najděte generující matici a matici kontroly parity.

13 13. týden – kódování

Cvičení konané 26. 5. 2021.

Příklad 13.1: [11.138] Sedmibitové zprávu $a_0 \dots a_6$ chápanou jako $a_0 + a_1x + \dots + a_6x^6$ kódujeme polynomiálním kódem generivaným polynomem $p(x) = x^4 + x + 1$.

(i) Zakódujte zprávu 1100011.

(ii) Obdrželi jste kód 10111010001. Jaká byla posílaná zpráva za předpokladu, že k chybě došlo maximálně v jednom bitu?

(iii) Jaká byla zpráva v (ii) za předpokladu, že k chybě došlo právě na dvou bitech?

Příklad 13.2: [11.141] Určete generující matici a matici kontroly parity $(7, 2)$-kódu generovaného polynomem $x^5 + x^4 + x^2 + 1$. Dekódujte přijaté slovo 0010111 (tj. určete poslanou dvoubitovou zprávu) za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Příklad 13.3: V lineárním $(7,4)$-kódu (tj. dálka zprávy před zakódováním je 4) nad $\mathbb{Z}_2$ zadaném maticí

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

byla přijata zpráva 1010001. Dekódujte ji za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.