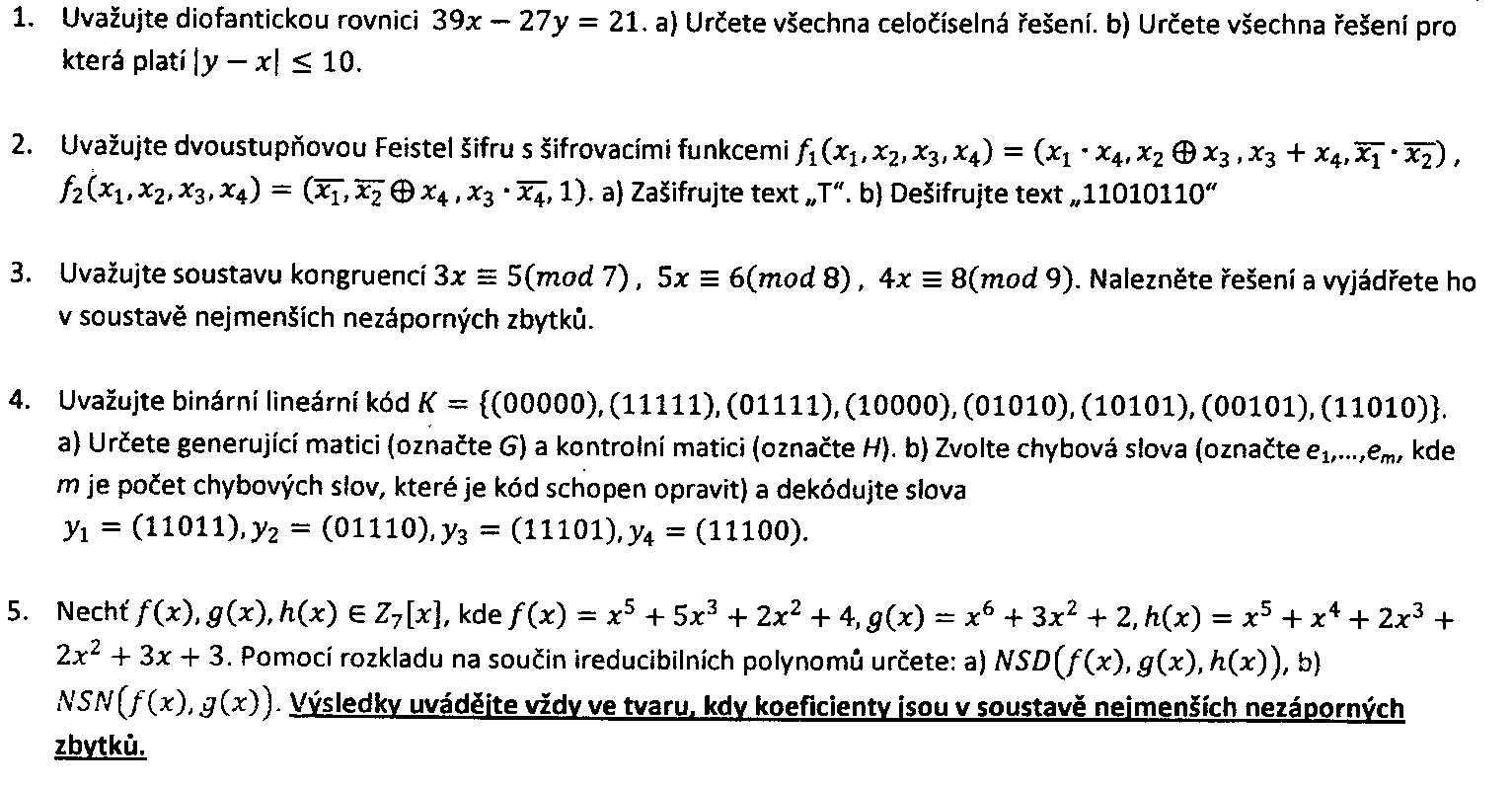
2012.01.09



2011.01.10

1. Dešifrujte text „RBI“ zašifrovaný Hillovým šifrováním s maticí .

, ,

2. Nalezněte všechna celočíselná řešení rovnice .

řešení existuje

3. Nalezněte všechna řešení kongruence . Výsledek uveďte v soustavě nejmenších nezáporných zbytků odpovídajícího modulu!

3 řešení

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | -1 | 0 | 1 | 2 | 3 | 4 | 5 |
|  | - | 0 | 3 | 3 | 2 | 3 | 2 |
|  | 1 | 0 | 1 | 3 | 7 | **24** | 55 |
|  | 0 | 1 | 3 | 10 | 23 | 79 | 181 |

4. Uvažujte dvoustupňové Feistel šifrování s šifrovacími funkcemi a . Zašifrujte text „kz“. Znaky šifrujte osmibitovým ASCII kódem, tj. ; .

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ↘ ↙ |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ↘ ↙ |  |
|  |  |  |

5. Uvažujte binární lineární kód . Určete: a) kontrolní matici; b) generující matici; c) minimální vzdálenost kódu a kolikanásobné chyby objevuje. Obě matice řádně označte!

b) Generující matici tvoří lineárně nezávislé vektory (báze).

a) Kontrolní matice se vytvoří z generující matice.

c) Minimální vzdálenost kódu , kód objevuje chyby.

2010.03.25

1. Uvažujte binární lineární kód zadaný soustavou . a) Vypište všechna kódová slova, b) určete minimální vzdálenost daného kódu počet kontrolních znaků, c) sestavte generující a kontrolní matici (matice řádně označte, aby bylo jasné, která je generující a která kontrolní), d) zvolte chybová slova (s nejmenší Hammingovou váhou) a dekódujte , , , .

c) Z 1. a 2. rovnice plyne 3. rovnice.

a) počet všech kódových slov

b)  kód detekuje 1 chybu a neopravuje žádnou chybu

d) ,

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 10000 | 00001 | 01000 | 00010 | 00100 | 00011 |
|  | 11 | 11 | 10 | 10 | 10 | 01 |

2. Dešifrujte text „ZEOA" zašifrovaný pomocí Hillova šifrování s maticí 2×2, jestliže víte, že slovo „text" bylo zašifrováno na „DMOT".

,

ověření správnosti matice :

3. V symetrické grupě vypočtěte , kde , . Výsledek zapište ve tvaru součinu disjunktních cyklů.

4. Nalezněte největší celé záporné číslo s následujícími vlastnostmi: při dělení číslem 7 dává zbytek 1, při dělení číslem 8 dává zbytek 1 a při dělení číslem 9 dává zbytek 3.

( jsou zbytky ze zadání)

5. Nalezněte všechna celočíselná řešení diofantické rovnice . Dále nalezněte řešení, kde je nejmenší celé číslo větší než 214.

, → řešení existuje

2010.02.15

1. Uvažujte polynomy , kde , . Určete .

Polynom vydělím , protože jím nejde zkrátit druhý polynom.

Eukleidův algoritmus:

2. Uvažujte binární lineární kód zadaný soustavou . a) Vypište všechna kódová slova. b) Určete minimální vzdálenost daného kódu. c) Vypište všechna možná chybová slova (s nejmenší Hammingovou vahou) a jejich syndromy a následně dekódujte slova (01100), (11111).

c) Z 1. a 2. rovnice plyne 3. rovnice.

a) počet všech kódových slov

b)  kód detekuje 1 chybu a neopravuje žádnou chybu

3. Uvažujte dvoustupňové Feistel šifrování s šifrovacími funkcemi a . Zašifrujte text „co“. Znaky šifrujte osmibitovým ASCII kódem. Symbol označuje xor, označuje negaci, označuje konjunkci (and), + označuje disjunkci (or).

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ↘ ↙ |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ↘ ↙ |  |
|  |  |  |

4. Nalezněte všechna řešení soustavy kongruencí , , . Výsledek uveďte v soustavě absolutně nejmenších zbytků.

delší řešení převodu jednotlivých kongruencí

a) 1 řešení

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | -1 | 0 | 1 | 2 |
|  | - | 0 | 1 | 2 |
|  | 1 | 1 | **2** | 5 |
|  | 0 | 1 | 1 | 3 |

b) 1 řešení

|  |  |  |  |
| --- | --- | --- | --- |
|  | -1 | 0 | 1 |
|  | - | 1 | 6 |
|  | 1 | **1** | 7 |
|  | 0 | 1 | 6 |

c) 1 řešení

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | -1 | 0 | 1 | 2 | 3 | 4 |
|  | - | 0 | 1 | 1 | 1 | 4 |
|  | 1 | 0 | 1 | 1 | **2** | 9 |
|  | 0 | 1 | 1 | 2 | 3 | 14 |

Dále řešíme tuto soustavu kongruencí

( jsou zbytky ze zadání)

5. Rozhodněte, které z následujících algebraických struktur tvoří grupu: a) , b) , c) , kde , , je soustava zbytků modulo , + je operace sčítání, je operace sčítání modulo a je operace násobení modulo . Svá tvrzení řádně zdůvodněte, tj. ověřte všechny vlastnosti grupy!

2010.02.09

1. Nalezněte všechna celočíselná řešení rovnice . Dále nalezněte řešení s vlastností, že je největší celé číslo menší než -100.

řešení existuje

2. Uvažujte racionální číslo . a) Sestavte tabulku přibližných zlomků. b) Nalezněte přibližný zlomek s vlastností .

a)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | -1 | 0 | 1 | 2 | 3 | 4 | 5 |
|  | - | 0 | 2 | 2 | 3 | 12 | 2 |
|  | 1 | 0 | 1 | 2 | 7 | 86 | 179 |
|  | 0 | 1 | 2 | 5 | 17 | 209 | 435 |

b)

3. Uvažujte polynomy , kde , . a) Pomocí Hornerova schématu určete , , b) Polynomy rozložte na součin kořenových činitelů (kořeny jsou celá čísla v absolutní hodnotě nepřevyšující 3) a určete a .

a)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| -2 | 1 | -4 | 1 | 10 | -4 | -8 |
|  |  | -2 | 12 | -26 | 32 | -56 |
|  | 1 | -6 | 13 | -16 | 28 | **-64** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 | 1 | 0 | -5 | 0 | 4 |
|  |  | 3 | 9 | 12 | 36 |
|  | 1 | 3 | 4 | 12 | **40** |

b)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 | 1 | -4 | 1 | 10 | -4 | -8 |
|  |  | 2 | -4 | -6 | 8 | 8 |
|  | 1 | -2 | -3 | 4 | 4 | 0 |
|  |  | -1 | 3 | 0 | -4 |  |
|  | 1 | -3 | 0 | 4 | 0 |  |
|  |  | 2 | -2 | -4 |  |  |
|  | 1 | -1 | -2 | 0 |  |  |
|  |  | 2 | 2 |  |  |  |
|  | 1 | 1 | 0 |  |  |  |
|  |  | -1 |  |  |  |  |
|  | 1 | 0 |  |  |  |  |

c)

4. Uvažujte množinu čísel . Rozhodněte, zda daná množina tvoří: a) grupu vzhledem k násobení, b) grupu vzhledem ke sčítání, c) těleso. Svá tvrzení řádně zdůvodněte.

5. Popište Huffmanovu konstrukci nejkratšího kódu, jestliže kódujeme pomocí 4 znaků (nezapomeňte vysvětlit, jak určíme počet znaků redukovaných v prvním kroku). Dále nalezněte nejkratší binární kód abecedy , kde pravděpodobnost výskytu samohlásky je dvakrát větší než výskyt souhlásky a spočtěte střední délku kódového slova.

Postup Huffmanova kódování: Abecedu seřadíme podle pravděpodobnosti výskytu nerostoucím způsobem. V prvním kroku redukujeme znaků s nejmenší pravděpodobností výskytu. V dalších krocích redukujeme znaků s nejmenší pravděpodobností výskytu. Algoritmus končí, když pravděpodobnost výskytu redukovaných znaků je 1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | 1 |
|  |  |  |  | 0,4 | 0 |  |
| a | 1 | 0,2 |  | 0,2 | 1 |  |
| e | 2 | 0,2 |  | 0,2 | 2 |  |
| i | 3 | 0,2 |  | 0,2 | 3 |  |
| b | 00 | 0,1 | 0 |  |  |  |
| c | 01 | 0,1 | 1 |  |  |  |
| d | 02 | 0,1 | 2 |  |  |  |
| f | 03 | 0,1 | 3 |  |  |  |

střední délka kódového slova:

2010.02.02

1. V krabici je neznámý počet předmětů, přičemž je známo, že jich je alespoň 1000. Pokud bychom uvedené předměty rozdělili rovným dílem mezi 7 osob, zbylo by 6 předmětů. Pokud bychom je rozdělili rovným dílem mezi 8 osob, zbyly by 3 předměty. Pokud bychom uvedené předměty rozdělili rovným dílem mezi 13 osob, zbylo by 5 předmětů. Určete počet předmětů.

( jsou zbytky ze zadání)

2. Uvažujte binární lineární kód definovaný kontrolní maticí . a) Vypište všechna kódová slova. b) Vypište chybová slova (a jejich syndromy), která je daný kód schopen opravit.

3. Rozhodněte, zda polynom je ireducibilní v . Následně v  spočtěte , kde , . Koeficienty výsledku zapište v soustavě nejmenších nezáporných zbytků. Svá tvrzení řádně zdůvodněte.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 3 | 4 | 0 | 1 | 3 |
|  |  | 6 | 0 | 0 | 2 |
|  | 3 | 0 | 0 | 1 | 0 |

není v ireducibilní.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | ← výsledek |  |

4. Dešifrujte text „DOJP“ zašifrovaný pomocí Hillova šifrování s maticí 2×2, jestliže víte, že text „help“ byl zašifrován na „DQVR“.

, ,

5. Uvažujte jednoduché transpoziční šifrování s klíčem . a) Zašifrujte text „diminution“, b) dešifrujte text „AGLMIATELN“.

a) IMDNIOIUNO

b) ligamental

2010.02.01

1. Nalezněte všechna řešení kongruence . Výsledek zapište v soustavě nejmenších nezáporných zbytků odpovídajícího modulu!

3 řešení

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  | - | 0 | 1 | 1 | 1 | 2 | 1 | 7 | 2 |
|  | 1 | 0 | 1 | 1 | 2 | 5 | 7 | **54** | 115 |
|  | 0 | 1 | 1 | 2 | 3 | 8 | 11 | 85 | 181 |

2. Uvažujte dvoustupňové Feistel šifrování s šifrovacími funkcemi a . Zašifrujte text „se“. Znaky šifrujte osmibitovým ASCII kódem, tj. ; .

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ↘ ↙ |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ⊕← | ←↙ |
|  | ↘ ↙ |  |
|  |  |  |
|  | ↘ ↙ |  |
|  |  |  |

3. Uvažujte binární lineární kód definovaný generující maticí . Určete: a) kontrolní matici, b) počet kódových slov, c) dekódujte slova , , , , , kde , , jsou opravovaná chybová slova.

a)

, permutace

zpětná permutace

(Kód není systematický, protože bylo potřeba promést permutaci.)

b) počet všech kódových slov

4. V  nalezněte nejmenši spol. násobek a největšího spol. dělitele polynomů kde , . Koeficienty výsledků zapište v soustavě nejmenších nezáporných zbytků příslušného modulu.

Hornerova schémata:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 5 | 2 | 1 | 1 |
|  |  | 20 | 4 | 20 |
|  | 5 | 1 | 5 | 0 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 3 | 4 | 2 | 0 | 3 | 6 |
|  |  | 12 | 8 | 12 | 20 | 8 |
|  | 3 | 2 | 3 | 5 | 2 | 0 |
|  |  | 12 | 0 | 12 | 12 | 0 |
| /3 | 3 | 0 | 3 | 3 | 0 | 0 |
|  | 1 | 0 | 1 | 1 |  |  |

5. nalezněte , která vyhovují soustavě ; , kde , . Výsledek zapište ve tvaru součinu disjunktních cyklů (!) a rozhodněte o sudosti .

|  |  |
| --- | --- |
|  |  |

Sudá permutace obsahuje sudý počet cyklů sudé délky. Permutace je sudá.

2010.01.20

1. Uvažujte následující binární kódy:

;

;

;

;

.

a) Rozhodněte, které z nich jsou lineární. b) Určete kolika násobné chyby dané kódy objevují a kolikanásobné opravují. c) U alespoň jednoho lineárního kódu určete kontrolní a generující matici. Své závěry řádně zdůvodněte.

a) Pro binární lineární kódy platí, že součet dvou kódových slov je kódové slovo.

; je lineární

; není lineární

; je lineární

; není lineární

; je lineární

b) Minimální vzdálenost kódu je , kód objevuje chyb, kód opravuje chyb.

;

;

;

;

;

c)

Kontrolní matice se vytvoří z generující matice.

2. Dešifruje text „CZE" zašifrovaný pomocí Hillova šifrování s šifrovací maticí .

3. Uvažujte permutace , kde , . a) Vypočtěte , , b) výraz nejprve maximálně zjednodušte a následně ho vypočtěte, c) vypište všechny prvky podgrupy grupy , která je generovaná permutací . Výsledky uvádějte vždy ve tvaru součinu disjunktních cyklů!

4. Vysvětlete/definujte pojem nejkratší kód a nalezněte nejkratší kód následující abecedy.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Znak | x | u | t | a | m | e |
| Pst. | 0,17 | 0,05 | 0,50 | 0,05 | 0,13 | 0,06 |

5. Uvažujte diofantickou rovnici . a) Nalezněte všechna řešení v oboru celých čísel, b) nalezněte řešení, kde je nejmenší kladné přirozené číslo.

a)  řešení existuje

b)

2010.01.19

1. Uvažujte lineární kód nad Z5 definovaný soustavou . Určete: a) generující matici, b) zda kód je systematický, c) Rozhodněte, která z následujících slov jsou kódová: (1111310), (0131310), (1230021), (0220124).

2. Dešifrujte text „ERL“, který byl zašifrovaný pomocí afinního šifrování, jestliže víte, že znak „g“ byl zašifrován na „p“ a znak „p“ na znak „g“.

,

Dešifrování

, ,

3. Uvažujte permutace π, ρ, σ ϵ S7, kde π = (246)(13)(57), ρ=(125)(36)(74), σ=(426)(512). Spočtěte: a) π-1, b) π∙ρ∙σ, c) σ∙ρ∙π. Výsledky vždy zapište ve tvaru disjunktních cyklů!

4. Uvažujte binární kódování abecedy s devíti znaky. Rozhodněte, zda existuje binární prefixový kód této abecedy s následujícími délkami kódových slov: a) , b) .

5. Nechť . a) Pomocí dvojkového NSD algoritmu vypočtěte , a b) dále určete . Jednotlivé kroky výpočtu řádně zapište.

a)

b)

2009.04.16

1. Určete nejmenší možný počet objektů, který vyhovuje následujícím podmínkám. Jestliže všechny objekty rozdělíte do 7 stejně velkých skupin, zůstanou 2 objekty nerozděleny. Pokud je rozdělíte do 10 stejně velkých skupin, zůstanou 3 nerozděleny. Konečně, pokud je rozdělíte do 9 stejně velkých skupin, zůstane 6 objektů nerozdělených.

( jsou zbytky ze zadání)

2. Dešifrujte text „TREK" zašifrovaný pomocí Hillova šifrování s maticí .

3. Uvažujte , kde , . Nalezněte: a), b) pomocí Hornerova schématu určete kořeny polynomu .

a)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 5 | 6 | 3 | 1 | 5 |
|  |  | 1 | 0 | 2 | 2 |
|  | 5 | 0 | 3 | 3 | 0 |
|  |  | 1 | -4 | 4 | 5 |
|  | 5 | 1 | 6 | 0 | 0 |
|  |  | 3 | 8 |  |  |
|  | 5 | 4 | 0 |  |  |
|  |  | -25 |  |  |  |
|  | 5 | 0 |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 6 | 6 | 3 | 0 | 5 | 4 |
|  |  | -5 | -2 | -2 | 4 | -4 |
|  | 6 | 1 | 1 | -2 | 2 | 0 |
|  |  | 4 | 1 | 6 | 5 |  |
|  | 6 | 5 | 2 | 4 | 0 |  |
|  |  | 4 | 6 | 3 |  |  |
|  | 6 | 2 | 1 | 0 |  |  |
|  |  | 3 | 6 |  |  |  |
|  | 6 | 5 | 0 |  |  |  |
|  |  | 30 |  |  |  |  |
|  | 6 | 0 |  |  |  |  |

b) Kořeny polynomu jsou .

4. Nalezněte všechna celočíselná řešení rovnice .

řešení existuje

5. Uvažujte binární kód s generující maticí , který opravuje chybová slova uvedená v následující tabulce. Pomocí syndromů dekódujte slova (110110), (111110), (110101), (111111).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| (100000) | (010000) | (001000) | (000010) | (000001) | (011000) | (010010) |

2009.01.26

1. Uvažujte binární lineární kód, o kterém víte, že obsahuje následující slova (101101), (011010), (110111), (000111), (110000). a) Sestavte jeho kontrolní a generující matici. b) Určete minimální vzdálenost tohoto kódu a rozhodněte, kolikanásobné chyby objevuje.

a)

Kontrolní matice se vytvoří z upravené generující matice.

permutace (2,3)

permutace (3,2)

b) Minimální vzdálenost kódu je , kód objevuje  chyb, kód opravuje  chyb.

2. Uvažujte kongruenci . Nalezněte řešení této kongruence. Výsledek zapište v soustavě nejmenších nezáporných zbytků modulo!

4 řešení

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | -1 | 0 | 1 | 2 | 3 | 4 | 5 |
|  | - | 1 | 5 | 1 | 3 | 2 | 2 |
|  | 1 | 1 | 6 | 7 | 27 | **61** | 149 |
|  | 0 | 1 | 5 | 6 | 23 | 52 | 127 |

3. Nalezněte nejkratší kódování abecedy uvedené v následující tabulce pomocí čtyř znaků . Spočtěte střední délku kódového slova.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i |
| 0,3 | 0,14 | 0,14 | 0,14 | 0,08 | 0,07 | 0,05 | 0,04 | 0,04 |

Huffmanovo kódování

V prvním kroku redukujeme znaků.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | 1 |
|  |  |  |  |  |  | 0,42 | 0 |  |
| a | 1 | 0,3 |  |  |  | 0,3 | 1 |  |
| b | 2 | 0,14 |  |  |  | 0,14 | 2 |  |
| c | 3 | 0,14 |  |  |  | 0,14 | 3 |  |
| d | 00 | 0,14 |  | 0,14 | 0 |  |  |  |
|  |  |  |  | 0,13 | 1 |  |  |  |
| e | 02 | 0,08 |  | 0,08 | 2 |  |  |  |
| f | 03 | 0,07 |  | 0,07 | 3 |  |  |  |
| g | 010 | 0,05 | 0 |  |  |  |  |  |
| h | 011 | 0,04 | 1 |  |  |  |  |  |
| i | 012 | 0,04 | 2 |  |  |  |  |  |

střední délka kódového slova:

4. Použijte Vernamovo šifrování s klíčovým slovem „RCS“. a) Zašifrujte „KOPEC“. b) Dešifrujte . V úloze a) nechte výsledek v podobě binárního řetězce. V obou případech použijte 7bitový ASCII kód.

a)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| K | 1001011 | O | 1001111 | P | 1010000 | E | 1000101 | C | 1000011 |
| R | 1010010 | C | 1000011 | S | 1010011 | R | 1010010 | C | 1000011 |
|  | 0011001 |  | 0001100 |  | 0000011 |  | 0010111 |  | 0000000 |

b)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ? | 0010011 | ? | 0011011 | ? | 0010110 | ? | 0000001 |
| R | 1010010 | C | 1000011 | S | 1010011 | R | 1010010 |
| **A** | 1000001 | **X** | 1011000 | **E** | 1000101 | **S** | 1010011 |

5. Uvažujte polynomy , nad . a) Určete kořeny polynomu ; b) vypočtěte ; c) podíl a zbytek při dělení polynomu polynomem . Výsledky uvádějte v soustavě nejmenších nezáporných zbytků.

a)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 4 | 2 | 1 | 3 |
|  |  | 4 | 1 | 2 |
|  | 4 | 1 | 2 | 0 |
|  |  | 8 | 8 |  |
|  | 4 | 4 | 0 |  |
|  |  | 16 |  |  |
|  | 4 | 0 |  |  |

Kořeny polynomu jsou .

b)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  | ← výsledek |  |

c)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

2009.01.24

1. Uvažujte permutace , kde , . a) Spočtěte π-1, b) z rovnice vyjádřete . Výsledky uvádějte vždy ve tvaru součinu disjunktních cyklů!

b)

2. Nechť , , . a) Určete počet společných dělitelů čísel a, b a všechny je vypište v pořadí od nejmenšího k největšímu. b) Určete součet všech dělitelů čísla c.

a) Postupně vytýkám z obou čísel prvočíslo nebo vydělím jedno číslo prvočíslem.

počet všech dělitelů (součin exponentů zvětšených o jedna)

seznam dělitelů:

b)

součet všech dělitelů

3. Nechť , kde , . a) Vypočtěte . Určete kořeny polynomů . Výpočty provádíte v , koeficienty uvádějte v soustavě nejmenších nezáporných zbytků.

4. Nalezněte všechna řešení soustavy kongruencí , , . Výsledek uveďte v soustavě absolutně nejmenších zbytků!

5. Uvažujte ternární Hammingův kód řádu 2. a) Sestavte generující matici. b) Vypište všechna kódová slova. c) Dekódujte slova: (1111), (1001), (2121), (0220)

2009.01.19

1. Uvažujte binární lineární kód, o kterém víte, že obsahuje kódová slova (10101), (01010), (11111), (00011), (10110). a) Vypište všechna kódová slova. b) Určete generující i kontrolní matici. c) Určete počet chybových slov, která je schopen daný kód při standardním dekódování opravit a vypište je (uvažujte chybová slova nejmenší Hammingovy váhy).

2. Použijte Vernamovo šifrování s klíčovým slovem „ALE“. a) Zašifrujte text „LIVRES“. b) Dešifrujte (0000100), (0011010), (0000100). (Použijte 7 bitů pro každý znak.)

3. Nalezněte všechna celočíselná řešení rovnice .

4. Pomocí kanonických rozkladů nalezněte , kde ; ; . Dále číslo rozviňte v řetězový zlomek, sestavte tabulku přibližných zlomků a spočtěte vzdálenost přibližných zlomků .

5. Dešifrujte text „ZFJUTF“ zašifrovaný pomocí Hillova šifrování s maticí .

2009.01.17

1. Uvažujte ternární lineární kód s generující maticí . a) Nalezněte kontrolní matici. b) Určete, která z následujících slov jsou kódová - (11111), (22122), (01210), (12202), (22102).

2. Pomocí Eukleidova algoritmu nalezněte pro daná čísla ; ; : a) ; b) .

a)

:

:

b)

:

:

3. Uvažujte polynomy , kde a . a) Nalezněte podíl a zbytek při dělení polynomu polynomem . b) Pomocí Hornerova schématu určete kořeny polynomu . c) Nalezněte . Vždy používejte soustavu nejmenších nezáporných zbytků .

4. Nalezněte všechna řešení soustavy kongruencí , , . Výsledek uveďte v soustavě absolutně nejmenších zbytků.

5. Nalezněte [nejkratší ternární kód](http://nejkrats.ternarn.kod) abecedy

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Znak | A | B | C | D | E | F | G | H | I |
| Pst. | 0,3 | 0,17 | 0,13 | 0,10 | 0,075 | 0,075 | 0,06 | 0,05 | 0,04 |

a spočtěte střední délku kódového slova.

2009.01.14

1. Uvažujte kongruenci . a) Nalezněte její řešení (výsledek vyjádřete v soustavě nejmenších nezáporných zbytků modulo 1060). b) Nalezněte třetí největší záporné celé číslo vyhovující dané kongruenci.

2. Uvažujte binární kód s kontrolní maticí . a) Vypište všechna kódová slova. b) Určete počet chybových slov, které je schopen tento kód při standardním dekódování opravit a vypište je (volte chybová slova s nejmenší Hammingovou váhou). c) Dekódujte slova .

3. V , uvažujte polynomy , . a) Vypočtěte , . Dále pomocí Hornerova schématu určete podíl a zbytek při dělení polynomu polynomem . Koeficienty polynomů uvádějte vždy v soustavě nejmenších nezáporných zbytků!

4. Dešifrujte: a) text „RSNUESZY” zašifrovaný pomocí Vigenérova šifrování s klíčovým slovem „houba“. b) text „ARINFSIGIL“ zašifrovaný pomocí jednoduché transpozice klíčem .

a)

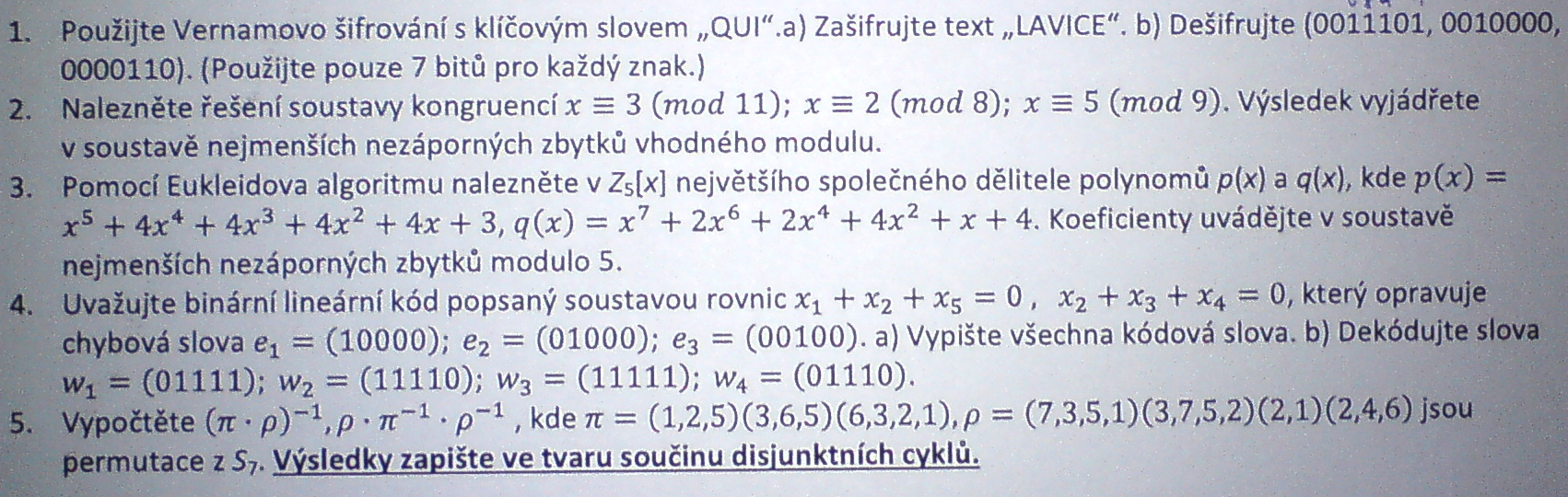
b)

anfirsilgi

5. Nalezněte nejkratší ternární kódování následující abecedy. Dále uvažujte nezakódovanou zprávu obsahující 27 znaků a odhadněte její délku po zakódování.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Znak | A | B | C | D | E | F | G | H | I | J |
| Pst. | 0,15 | 0,15 | 0,1 | 0,1 | 0,1 | 0,1 | 0,08 | 0,08 | 0,08 | 0,06 |

2009.01.12



2009.01.05

