Examen la Fundamentele Algebrice ale Informaticii

Nume şi prenume: •
An: •
Grupa: •
Data: • 30 mai 2016

Anul în care aţi trecut seminarul: •
Cadrul didactic: •

Nota:

1. (a) Descrieţi algoritmul extins al lui Euclid şi demonstraţi corectitudinea acestuia. (5p+5p)
   (b) Determinaţi o soluţie a ecuaţiei $4x + 11y = 17$ folosind algoritmul extins al lui Euclid. (5p)
   (c) Folosind faptul că complexitatea unei împărţiri
   $$x = y \cdot q + r, \quad 0 \leq r < y$$
   este $\mathcal{O}((\log y)(\log q))$, arătaţi că algoritmul extins al lui Euclid, aplicat întregilor $a > b > 0$, are complexitatea $\mathcal{O}((\log a)(\log b))$. (10p)
2. (a) Definiţi conceptul de subgrup generat de o parte a unui grup, şi apoi conceptul de grup ciclic. (5p)
   (b) Definiţi ordinul unui element într-un grup notat aditiv. (5p)
   (c) Fie G un grup finit şi $a \in G$. Arătaţi că a este generator pentru G dacă şi numai dacă $a^{|G|/q} \neq 1_G$, pentru orice factor prim q al lui $|G|$. (12p)
   (d) Arătaţi că pentru orice număr prim $p \geq 3$, $\mathbf{Z}_p^*$ are rădăcini primitive. (18p)
3. (a) Definiţi conceptul de spaţiu vectorial. (5p)
   (b) Definiţi conceptul de detecţie a unei erori de un cod, precum şi cel de cod t-detector de erori. (5p)
   (c) Construiţi un cod C cu cel puţin 5 elemente şi care să aibă distanţa 3. Găsiţi apoi o eroare ce nu poate fi detectată de C. (10p)
4. Un cod bloc binar C cu lungimea n, $C = m$ şi distanţă d va fi numit cod de tip (n, m, d).
   Fie $n \geq 1$ şi $1 \leq d \leq n$ impar. Arătaţi că există coduri de tip (n, m, d) dacă şi numai dacă există coduri de tip $(n + 1, m, d + 1)$. Se păstrează rezultatul dacă d este par? (15p)

Examen la Fundamentele Algebrice ale Informaticii

Nume şi prenume: •
An: •
Grupa: •
Data: • 30 mai 2016

Anul în care aţi trecut seminarul: •
Cadrul didactic: •

Nota:

1. (a) Descrieţi algoritmul sugerat de demostraţia Teoremei Chineze a Resturilor de rezolvare a sistemelor de ecuaţii liniare congruenţiale, şi argumentaţi corectitudinea lui. (5p+5p)

   (b) Determinaţi o soluţie a sistemului

   $$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 7 \bmod 11 \end{cases}$$

   folosind algoritmul descris la (1a). (5p)

   (c) Studiaţi complexitatea algoritmului de la (1a). (10p)

2. (a) Definiţi conceptul de spaţiu vectorial. (5p)

   (b) Definiţi conceptele de vectori liniar independenţi, vectori liniar dependenţi, şi bază a unui spaţiu vectorial. (5p)

   (c) Arătaţi că o submulţime finită B a unui spaţiu vectorial V peste un corp F este bază pentru V dacă şi numai dacă orice vector din V se scrie unic ca o combinaţie liniară a vectorilor din B. (10p)

   (d) Un cod bloc binar C cu lungimea n, $|C| = m$ şi distanţă d va fi numit cod de tip (n, m, d).

   Fie $n \geq 1$ şi $1 \leq d \leq n$ impar. Arătaţi că există coduri de tip (n, m, d) dacă şi numai dacă există coduri de tip $(n+1, m, d+1)$. Se păstrează rezultatul dacă d este par? (15p)

3. (a) Definiţi rata informaţiei unui cod bloc binar, şi explicaţi semnificaţia ei. (5p)

   (b) Definiţi conceptul de corecţie a unei erori de un cod, precum şi cel de cod t-corector de erori. (5p)

   (c) Construiţi un cod C cu cel puţin 5 elemente şi care să aibă distanţa 3. Găsiţi apoi o eroare ce nu poate fi corectată de C. (10p)

4. Fie $p \geq 3$ un număr prim şi $k \geq 1$. Arătaţi că dacă α este rădăcină primitivă impară modulo p^k, atunci α este rădăcină primitivă modulo $2p^k$, iar dacă α este rădăcină primitivă pară modulo p^k, atunci $(\alpha + p^k) \bmod p^k$ este rădăcină primitivă modulo $2p^k$. (20p)

Examen la Fundamentele Algebrice ale Informaticii

Nume şi prenume: •
An: •
Grupa: •
Data: • 30 mai 2016

Anul în care aţi trecut seminarul: •
Cadrul didactic: •

Nota:

1. (a) Descrieţi algoritmul extins al lui Euclid şi demonstraţi corectitudinea acestuia. (5p+5p)
   (b) Determinaţi o soluţie a ecuaţiei $4x + 11y = 17$ folosind algoritmul extins al lui Euclid. (5p)
   (c) Folosind faptul că complexitatea unei împărţiri
   $$x = y \cdot q + r, \quad 0 \leq r < y$$
   este $\mathcal{O}((\log y)(\log q))$, arătaţi că algoritmul extins al lui Euclid, aplicat întregilor $a > b > 0$, are complexitatea $\mathcal{O}((\log a)(\log b))$. (10p)
2. (a) Definiţi conceptul de subgrup generat de o parte a unui grup, şi apoi conceptul de grup ciclic. (5p)
   (b) Definiţi ordinul unui element într-un grup notat aditiv. (5p)
   (c) Fie G un grup finit şi $a \in G$. Arătaţi că a este generator pentru G dacă şi numai dacă $a^{|G|/q} \neq 1_G$, pentru orice factor prim q al lui $|G|$. (10p)
   (d) Arătaţi că pentru orice număr prim $p \geq 3$, $\mathbf{Z}_p^*$ are rădăcini primitive. (15p)
3. (a) Definiţi conceptul de spaţiu vectorial. (5p)
   (b) Definiţi conceptele de vectori liniar independenţi, vectori liniar dependenţi, şi bază a unui spaţiu vectorial. (5p)
   (c) Arătaţi că o submulţime finită B a unui spaţiu vectorial V peste un corp F este bază pentru V dacă şi numai dacă orice vector din V se scrie unic ca o combinaţie liniară a vectorilor din B. (10p)
4. Fie $p \geq 3$ un număr prim şi $k \geq 1$. Arătaţi că dacă α este rădăcină primitivă impară modulo p^k, atunci α este rădăcină primitivă modulo $2p^k$, iar dacă α este rădăcină primitivă pară modulo p^k, atunci $\alpha + p^k$ este rădăcină primitivă modulo $2p^k$. (20p)

Examen la Fundamentele Algebrice ale Informaticii

Nume şi prenume: •
An: •
Grupa: •
Data: • 14 iunie 2017

Anul în care aţi trecut seminarul: •
Cadrul didactic: •

Nota:

1. (a) Descrieţi algoritmul extins al lui Euclid şi demonstraţi corectitudinea acestuia. (5p+5p)
   (b) Determinaţi o soluţie a ecuaţiei $4x + 11y = 17$ folosind algoritmul extins al lui Euclid. (5p)
   (c) Folosind faptul că complexitatea unei împărţiri
   $$x = y \cdot q + r, \quad 0 \leq r < y$$
   este $\mathcal{O}((\log y)(\log q))$, arătaţi că algoritmul extins al lui Euclid, aplicat întregilor $a > b > 0$, are complexitatea $\mathcal{O}((\log a)(\log b))$. (10p)
2. (a) Definiţi conceptul de subgrup generat de o parte a unui grup, şi apoi conceptul de grup ciclic. (5p)
   (b) Definiţi ordinul unui element într-un grup notat aditiv. (5p)
   (c) Fie G un grup finit şi $a \in G$. Arătaţi că a este generator pentru G dacă şi numai dacă $a^{|G|/q} \neq 1_G$, pentru orice factor prim q al lui $|G|$. (12p)
   (d) Arătaţi că pentru orice număr prim $p \geq 3$, $\mathbf{Z}_p^*$ are rădăcini primitive. (18p)
3. Fie p prim impar astfel încât $p - 1 = 2^s \cdot t$ cu $s \geq 1$ şi t impar, fie $a \in \mathbf{Z}_p^*$ un reziduu pătratic modulo p şi $d \in \mathbf{Z}_p^*$ un non-reziduu pătratic modulo p. Demonstraţi că există $k \in \mathbf{N}^*$ astfel încât $a^t \equiv (d^t)^k \ mod \ p$. (15p)
4. Un cod bloc binar C cu lungimea n, $|C| = m$ şi distanţă d va fi numit cod de tip (n, m, d).
   Fie $n \geq 1$ şi $1 \leq d \leq n$ impar. Arătaţi că există coduri de tip (n, m, d) dacă şi numai dacă există coduri de tip $(n + 1, m, d + 1)$. Se păstrează rezultatul dacă d este par? (20p)

Examen la Fundamentele Algebrice ale Informaticii

Nume şi prenume: •
An: •
Grupa: •
Data: • 14 iunie 2017

Anul în care aţi trecut seminarul: •
Cadrul didactic: •

Nota:

1. (a) Enunţaţi Teorema Chineză a Resturilor (TCR) şi descrieţi un algoritm de determinare a unei soluţii a sistemului din enunţul ei. (5p+5p)
   (b) Discutaţi corectitudinea şi complexitatea algorimului de la punctul anterior. 5p
   (c) Determinaţi o soluţie în $\mathbf{Z}_{21}$ a sistemului de mai jos folosind algoritmul de la (a)
   $$\begin{cases} x \equiv 5 \bmod 3 \\ x \equiv 6 \bmod 7 \end{cases}$$
   (5p)
   (d) Folosiţi algoritmul de la (a) pentru a determina o soluţie în $\mathbf{Z}_{42}$ a sistemului de mai jos
   $$\begin{cases} x \equiv 2 \bmod 6 \\ x \equiv 6 \bmod 14 \end{cases}$$
   (5p)
2. (a) Definiţi conceptul de subgrup generat de o parte a unui grup, şi apoi conceptul de grup ciclic. (5p)
   (b) Definiţi ordinul unui element într-un grup notat aditiv. (5p)
   (c) Fie p prim impar şi $a \in \mathbf{Z}_p^*$. Demonstraţi că $ord_p(a) = q$, unde q este un divizor al lui $(p-1)$, dacă şi numai dacă sunt satisfăcute următoarele două condiţii:
   - $a^q \equiv 1 \ mod \ p$
   - $a^{q/r} \not\equiv 1 \ mod \ p$, oricare ar fi r un divizor prim al lui q

   (18p)
   (d) Fie p prim impar astfel încât $p - 1 = 2^s \cdot t$, unde $s \geq 1$, t impar şi $d \in \mathbf{Z}_p^*$ un non-reziduu pătratic modulo p. Demonstraţi că $ord_p(d^t \ mod \ p) = 2^s$ (12p)
3. Fie p prim de forma $p = 2q+1$, unde q este prim impar şi $a \in \mathbf{Z}_p^*$, $a \neq p-1$. Demonstraţi că a este rădăcină primitivă modulo p dacă şi numai dacă a este non-reziduu pătratic modulo p. (15p)
4. (a) Definiţi rata informaţiei unui cod bloc binar, şi explicaţi semnificaţia ei. (5p)
   (b) Definiţi conceptul de corecţie a unei erori de un cod, precum şi cel de cod t-corector de erori. (5p)
   (c) Construiţi un cod C cu cel puţin 5 elemente şi care să aibă distanţa 3. Găsiţi apoi o eroare ce nu poate fi corectată de C. (10p)

Examen la Fundamentele Algebrice ale Informaticii

Nume şi prenume: •
An: •
Grupa: •
Data: • 14 iunie 2017

Anul în care aţi trecut seminarul: •
Cadrul didactic: •

Nota:

1. (a) Definiţi $\Theta(g(n))$, unde $g : \mathbf{N} \to \mathbf{R}_+$. (5p)
   (b) Ce se înţelege prin $f(n) = \Theta(g(n))$? (5p)
   (c) Arătaţi că dacă $f(x) = a_0 + a_1 x + \cdots + a_k x^k$ este un polinom cu coeficienţi reali pentru care $a_k > 0$, atunci $f(n) = \Theta(n^k)$. (10p)
2. (a) Definiţi conceptele de cod de lungime variabilă, cod prefix, sursă de informaţie şi cod Huffman pentru o sursă de informaţie. (3p+2p+3p+2p)
   (b) Descrieţi algoritmul de obţinere a unui cod Huffman. 5p
   (c) Aplicaţi algoritmul Huffman (de la pasul anterior) pentru textul "sunt student la informatică în anul întâi". (5p)
   (d) Justificaţi corectitudinea algoritmului Huffman. (15p)
3. (a) Fie G un grup finit şi $a \in G$. Arătaţi că a este generator pentru G dacă şi numai dacă $a^{|G|/q} \neq 1_G$, pentru orice factor prim q al lui $|G|$. (10p)
   (b) Definiţi conceptul de rădăcină primitivă modulo p, unde p este prim. (5p)
   (c) Determinaţi o rădăcină primitivă modulo 23 (justificaţi răspunsul). (5p)
   (d) Folosind rădăcina primitivă de la (b), determinaţi toate rădăcinile primitive modulo 23. (10p)
   (e) Fie p prim de forma $p = 4q + 1$, unde q este prim impar. Demonstraţi că 2 este rădăcină primitivă modulo p. (15p)

Examen la Fundamentele Algebrice ale Informaticii

Nume şi prenume: •
An: •
Grupa: •
Data: • 14 iunie 2017

Anul în care aţi trecut seminarul: •
Cadrul didactic: •

Nota:

1. Algoritmul Sardinas-Patterson: justificare teoretică, descriere şi proprietatea de terminare pentru cazul finit. 5p+5p+10p
2. Daţi un exemplu de cod infinit de lungime variabilă pentru care algoritmul Sardinas-Patterson se termină. 5p
3. Fie $p > 2$ un număr prim şi $a, b, c \in \mathbf{Z}$ astfel încât $(a, p) = 1$. Arătaţi că, congruenţa

$$ax^2 + bx + c \equiv 0 \ mod \ p$$

are

   (a) 2 rădăcini (distincte) în $\mathbf{Z}_p$ dacă există $y \in \mathbf{Z}$ cu $p \not| y$ şi $\Delta \equiv y^2 \ mod \ p$; (10p)
   (b) o rădăcină în $\mathbf{Z}_p$ dacă $\Delta \equiv 0 \ mod \ p$; (5p)
   (c) nicio rădăcină, altfel, (5p)

unde $\Delta = b^2 - 4ac$.

4. Fie $p > 2$ număr prim.
   (a) Definiţi QR_p şi QNR_p. (5p)
   (b) Arătaţi că dacă $a, b \in QR_p$ atunci $(ab \bmod p) \in QR_p$. (10p)
   (c) Arătaţi că dacă $a \in QR_p$ şi $b \in QNR_p$ atunci $(ab \bmod p) \in QNR_p$. (10p)
   (d) Arătaţi că dacă $a, b \in QNR_p$ atunci $(ab \bmod p) \in QR_p$. (10p)
5. (a) Definiţi conceptul de spaţiu vectorial. (5p)
   (b) Definiţi conceptul de detecţie a unei erori de un cod, precum şi cel de cod t-detector de erori. (5p)
   (c) Construiţi un cod C cu cel puţin 5 elemente şi care să aibă distanţa 3. Găsiţi apoi o eroare ce nu poate fi detectată de C. (10p)

Examen la Fundamente Algebrice ale Informaticii

Nume şi prenume: •
An: •
Grupa: •
Data: • 26 iunie 2017

Anul în care aţi trecut seminarul: •
Cadrul didactic: •

Nota:

1. Fie ρ o relaţie binară pe o mulţime A şi $s(\rho)$ închiderea simetrică a ei. Arătaţi că au loc următoarele proprietăţi:
   - $s(\rho) = \rho \cup \rho^{-1}$
   - $(\rho^n)^{-1} = (\rho^{-1})^n$

   10p

2. Fie $f : \mathbf{N} - \{0\} \to \mathbf{R}_+$ astfel încât $f(1) = c$ şi $f(n) \leq af(\lfloor n/b \rfloor) + cn^k$, unde a, b, c, k sunt constante pozitive. Definiţi ordinul de magnitudine Θ şi arătaţi că

$$f(n) = \begin{cases} \Theta(n^k), & \text{dacă } a < b^k \\ \Theta(n^k \cdot \log n), & \text{dacă } a = b^k \\ \Theta(n^{\log_b a}), & \text{dacă } a > b^k \end{cases}$$

   5p+15p

3. Discutaţi $\mathbf{Z}_m$ după numărul întreg m. 10p

4. Care sunt regulile de evaluare a funcţiei lui Euler folosind descompunerea în factori primi a numerelor naturale ? Justificaţi-le. 10p+15p

5. Fie A un alfabet şi $C \subseteq A^*$. Definim $CA^- = \{u \in A^+ | \exists w \in A^+ : \ uw \in C\}$.

   Arătaţi că un cod prefix C peste A este maximal (nu poate fi estins la un cod care să îl includă strict) dacă şi numai dacă $A^+ = CA^- \cup C \cup CA^+$. 15p

6. Arătaţi că în orice inel comutativ R de caracteristică p număr prim are loc

$$(a+b)^{p^n} = a^{p^n} + b^{p^n},$$

   pentru orice $a, b \in R$ şi $n \in \mathbf{N}$. 10p

7. Coduri corectoare de erori (pondere şi distanţă Hamming, distanţa unui cod, definiţia codurilor corectoare de erori, teorema codurilor corectoare de erori). 10p