

Arvuteooria (1. osa), 3EAP

Kordamisküsimused

Kevad 2024

Tööga kontrollitavaks **materjaliks** on loengus (loengukonspekti 1.-6. peatükis) käsitletud **teooria** ja esimestes 9 praktikumis vaadeldud ülesannete **lahendusmeetodid** (aine kodulehel olevate materjalide numeratsioonis).

Kontrolltöös peab oskama **defineerida** ja kasutada mõisteid, **sõnastada** ja **tõestada** tulemusi ja **anda ülevaadet** teemadest samas mahus, kui neid käsitleti loengus (seda on kokku üldiselt vähem, aga rohkemate detailidega, kui vastav loengukonspektis sisalduv materjal).

Samuti tuleb osata **lahendada** selliseid ülesandeid, mis kas esinesid mõnes praktikumis mittetärnüleannetena või on lahendatavad samade meetoditega. Mittetärnüleannete alla käivad ka **lisandunud tärnidega** ülesanded, nende lahendusmeetodeid tuleb ikkagi teada **juhul, kui neid praktikumis käsitleti**. NB! Ülesannete hulka kuuluvad ka **tõestusülesanded**.

Loengukonspekt on mõnes kohas küllaltki lakooniline ja seal kirjas olevate **tõestuste** üks-ühele **reprodutseerimine** ei pruugi alati anda täispunkte. Te peate olema valmis tervet oma arutluskäiku **põhjendada** ja ei saa lihtsalt öelda, et “ilmselt” või “on lihtne näidata” või väita midagi ilma mingi tõestuseta. Loengu ajal täideti need lüngad üldiselt ära, vrdl. näiteks loengukonspekti lauseid 1.21 või teoreemi 5.21 ning nende käsitlust loengus.

Keerulisema tõestusega tulemused (tõenäoliselt küsitakse ühte neist):

1. Võrrandi $ax + by = c$ lahendite kuju (teoreem 1.16).
2. SÜT ja VÜK omadused, mis on seotud algteguriteks lahutusega (lause 1.22).
3. Funktsioonide τ ja σ arvutusvalemid (teoreem 5.21).
4. Lineaarkongruentsi lahenduvus ja lahendite kuju (lause 6.2).

Lihtsama tõestusega tulemused (tõenäoliselt küsitakse neist ühte-kahte):

5. Jaguvuse lihtsamad omadused (lause 1.2).
6. SÜT ja VÜK lihtsamad omadused (lause 1.5 ja selle VÜK analoogid).
7. Teoreem jäägiga jagamisest (lause 1.6).
8. Võrrandi $ax + by = c$ lahenduvus (teoreem 1.9).
9. Suurima ühisteguri väljajagamine (järelkus 1.10).
10. Eukleidese lemma (järelkus 1.11).
11. Eukleidese lemma järelkus algarvude jaoks (järelkus 1.12).
12. Eukleidese lemma järelkus algarvu ja korrutise jaoks (järelkus 1.13).
13. Eukleidese lemma järelkus algarvu ja algarvude korrutise jaoks (järelkus 1.14).
14. Aritmeetika põhiteoreem (teoreem 1.19).
15. Naturaalarvu kanoonilise/standardkuju olemasolu (järelkus 1.20).
16. SÜT ja VÜK vaheline seos (lause 1.23).
17. Eukleidese teoreem (teoreem 2.2).
18. Algarvud aritmeetilises jadas $4k + 3$ (teoreem 2.4).
19. Kordarvud aritmeetilises jadas (lause 2.6).
20. Seos kongruentsuse ja jäägiga jagamise vahel (lause 3.3).
21. Seos kongruentsuse ja jäägiklasside vahel (lause 3.5).
22. Jäägiklasside modulo n kirjeldus (lause 3.6).
23. Kongruentsi tehete seotud omadused (lause 3.7).
24. Kongruentsi polünoomväärtustega seotud omadus (järelkus 3.8).

25. Kongruentsi arvuga korrutamine ja jagamine (lause 3.10).
26. Kongruentsi taandamine (lause 3.11).
27. Kongruentsi taandamise erijuht (pöördelemendiga korrutamine) (järelalus 3.12).
28. Kongruentsidel põhinevad jaguvustunnused arvude 3,7,9,11 jaoks (lause 3.14 ja sarnane tunnus arvu 7 jaoks).
29. Ühistegur omavahel ühistegurita arvude korrutisega (lemma 4.1).
30. Jaguvus omavahel ühistegurita arvude korrutisega (lemma 4.2).
31. Jaguvus standardkujul antud arvuga (järelalus 4.3).
32. Teoreem jäägiklassiringide isomorfisusest (teoreem 4.5).
33. Ringi pööratavate elementide hulga struktuur (lause 4.7).
34. Ringide isomorfismi ahend pööratavate elementide rühmadele (lause 4.8).
35. Jäägiklassiringide korrutise pööratavate elementide rühma struktuur (järelalus 4.9).
36. Jäägiklassiringi pööratavate elementide rühma kirjeldus (teoreem 4.10).
37. Jäägiklassikorpuseks oleku kriteerium (lause 4.13).
38. Jäägiklassiringi elementide klassifikatsioon (lause 4.15).
39. Euleri φ -funktsiooni väärtus algarvudel (lause 5.3).
40. Euleri φ -funktsiooni väärtus algarvu astmetel (lause 5.4).
41. Korrutisringi pööratavate elementide rühma struktuur (lause 5.6).
42. Euleri φ -funktsiooni nõrk multiplikatiivsus (teoreem 5.7).
43. Euleri φ -funktsiooni arvutusvalem (teoreem 5.8).

44. Ühisteguriga ja väiksemate arvude loendamine (lause 5.10).
45. Gaussi teoreem teoreem Euleri φ -funktsioonist (teoreem 5.11).
46. Euleri teoreem (teoreem 5.12).
47. Fermat' väike teoreem (teoreem 5.13).
48. Fermat' väikese teoreemi järeldus (järeldus 5.14).
49. Möbiuse funktsiooni väärtuste summa (teoreem 5.17).
50. Möbiuse inversioonivalem (teoreem 5.18).
51. Lineaarkongruentsi ühene lahenduvus (järeldus 6.4).
52. Hiina jäägiteoreem (teoreem 6.6).
53. Polünoomkongruentside lahendamine juhul, kui moodul on algarvu aste (mõttekäik alapeatükist 6.4).
54. Polünoomkongruentsi lahendamine kongruentside süsteemina (lause 6.10).

Tulemused, mida tuleb osata vaid sõnastada, **mitte tõestada**:

55. Bezout' lemma (järeldus 1.7).
56. Dirichlet' teoreem (teoreem 2.5).
57. Bertrand'i postulaat (teoreem 2.7).
58. Algarvude jaotuse teoreem ($\pi(n) \sim \frac{n}{\ln n}$, alapeatükk 2.3).
59. Polünoomi astme ja juurte arvu vaheline seos (lause 2.9).
60. Goldbachi hüpotees (hüpotees 2.11) ja nõrk Goldbachi hüpotees.
61. Fermat' suur teoreem (teoreem 2.12).
62. Lagrange'i teoreem (lisa 1).

Mõisted:

63. Jaguvus (definitsioon 1.1).
64. Suurim ühistegur (definitsioon 1.3).
65. Vähim ühiskordne (definitsioon 1.4).
66. Diofantiline võrrand (alapeatükk 1.3).
67. Algarv, kordarv (alapeatükk 1.3).
68. Algtegur, algteguriteks lahutus (alapeatükk 1.3).
69. Kanooniline/standardkuju (järeldus 1.20).
70. Algarvukaksik (definitsioon 1.1).
71. Funktsioonid p_n ja $\pi(n)$. (alapeatükk 2.3).
72. Kongruents (definitsioon 3.1).
73. Jäägiklass (alapeatükk 3.2).
74. Rühm (alapeatükk 4.1, lisa 1).
75. Ring (alapeatükk 4.1, lisa 1).
76. Korrutisring (alapeatükk 4.1).
77. Rühmade isomorfism (lause 4.8 tõestus, lisa 1).
78. Ringide isomorfism (teoreemi 4.5 tõestus, lisa 1).
79. Jäägiklassiring ja jäägiklassikorpus. (alapeatükid 4.1 ja 4.2).
80. Ringi pööratavad elemendid $U(R)$ (alapeatükk 4.2).
81. Nullitegur (definitsioon 4.14).
82. Euleri φ -funktsioon (definitsioon 5.1).

- 83. Möbiuse funktsioon (definiitsioon 5.16).
- 84. τ - ja σ -funktsioonid (definiitsioon 5.19).
- 85. Täiuslik arv (alapeatükk 5.4).
- 86. Mersenne'i (alg)arv (alapeatükk 5.4).
- 87. Kongruents (kui võrrandi analoog), selle lahend ja lahendamine (alapeatükk 6.1).
- 88. Lineaarkongruents (alapeatükk 6.2).

Oskused ja teadmised, mida kontrollitakse **ülesannete lahendamisel**:

- 89. Arvutamine, sealhulgas efektiivne kongruentside ja jäägiklassidega arvutamine, peast ja paberil 1000 piires.
- 90. Binoomvalemi kasutamine, sh kongruentside analüüsimisel.
- 91. Aritmeetilise ja geomeetrilise jada summa valemid, sh kongruentsidega seotud või jäägiklassidest koosnevate jadade korral.
- 92. Täisarvude põhiomadused.
- 93. Jaguvus ja selle omadused.
- 94. SÜT, VÜK ja nende omadused.
- 95. (Laiendatud) Eukleidese algoritm.
- 96. Diofantilise võrrandi $ax + by = c$ lahendivalemi kasutamine.
- 97. Diofantiliste võrrandite $ax + by = c$ ja $ax + by + cz = d$ lahendamine ja erikujuliste lahendite leidmine.
- 98. Algarvu mõiste kasutamine.
- 99. Algarvuks oleku kontroll.

100. Algteguriteks lahutuse kasutamine.
101. Eratosthenese sõel.
102. Eukleidese algarvude lõpmatuse tõestuse meetodile sarnased tõestused.
103. Dirichlet' teoreemi kasutamine.
104. Bertrand'i postulaadi kasutamine.
105. Algarvude jaotuse valemi $\pi(n) \sim \frac{n}{\ln n}$ kasutamine.
106. Legendre'i valem (2. praktikum).
107. Kongruentsi mõiste kasutamine.
108. Diofantilise võrrandi lahendamatus näitamine.
109. Jaguvustunnused arvude 3, 7, 9, 11 ja 13 jaoks.
110. Jäägiklassiringide elementide klassifikatsiooni kasutamine.
111. Jäägiklassiringide isomorfismiteoreemi kasutamine.
112. Euleri φ -funktsiooni definitsiooni ja arvutusvalemi kasutamine.
113. Euleri ja Fermat' väikese teoreemi ning viimase järelduse kasutamine.
114. Möbiuse funktsiooni definitsiooni kasutamine.
115. Gaussi teoreemi ja Möbiuse funktsiooniga seotud valemite kasutamine.
116. τ - ja σ -funktsioonide arvutusvalemite kasutamine.
117. Horneri skeem.
118. Hiina jäägiteoreemi kasutamine erinevate ülesannete lahendamiseks.
119. Lineaarkongruentside lahendamine.
120. Lineaarkongruentside süsteemide lahendamine.

121. Kõrgema astme kongruentside lahendamine (peatükis 6 kirjeldatud viisidel; ja erimeetodiga valitud polünoomide jaoks juhul $n = p^k$).
122. Kongruentside süsteemide lahendamine.