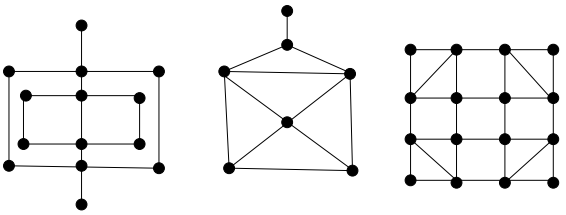
Bevezetés a számításelméletbe II.

2007. FEBRUÁR 14.

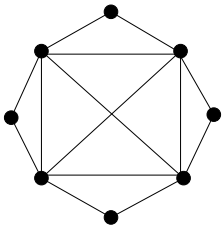
1. gyakorlat: Euler- és Hamilton bejárások

Információk: http://www.cs.bme.hu/∼tothagi

1. Elkészíthetők-e a ceruza felemelése nélkül az alábbi ábrák úgy, hogy minden vonalon pontosan egyszer haladunk végig?



2. Hányszor kell minimálisan felemelni a ceruzát az alábbi gráf lerajzolása során?



3. Igazoljuk, hogy ha egy gráf minden pontjának a foka 4, akkor élei színezhetők piros és kék színekkel úgy, hogy minden ponthoz két piros és két kék él illeszkedjék!

4. Mutassuk meg, hogy ha G-ben van Euler-kör, akkor minden vágásában páros sok él van! Igaz-e ez visszafelé, ha tudjuk, hogy a gráf összefüggő?

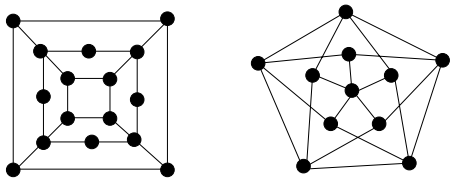
5. Van-e abban a gráfban Euler-út, melynek fokszámai a következők: 4,4,4,4,4,3,3,2,2,2?

6. Egy egyszerű G gráf csúcsait az $1, 2, \ldots, 100$ számok jelölik. Az i és j csúcsok között pontosan akkor vezet él G-ben, ha $|i - j| \leq 2$.

   (a) Tartalmaz-e G Euler-kört, illetve utat?

   (b) Hamilton-kört, illetve utat?

7. Van-e a következő gráfokban Hamilton-kör, illetve út?



8. Be lehet-e járni lóval egy 4×4-es sakktáblát?

9. Legalább hány éle van egy olyan hat pontú gráfnak, melynek van Hamilton-köre?

10. Legfeljebb hány éle van egy olyan hat pontú gráfnak, melynek nincs Hamilton-köre?

11. Bizonyítsuk be, hogy ha egy egyszerű gráfnak n csúcsa és $\binom{n-1}{2} + 1$ éle van, akkor még nem biztos, hogy tartalmaz Hamilton-kört, de ha ennél 1 éllel több, akkor már biztosan lesz benne.

12. Mutassuk meg, hogy $n \geq 5$-re igaz az alábbi két állítás!

    (a) Létezik olyan n csúcsú G gráf, hogy G is és $\overline{G}$ is tartalmaz Hamilton-kört.

    (b) Létezik olyan n csúcsú gráf, hogy sem G, sem $\overline{G}$ nem tartalmaz Hamilton-kört.

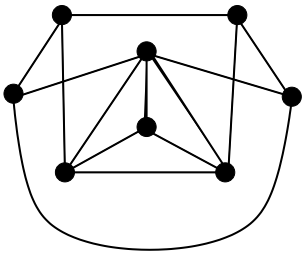
13. Lássuk be, hogy egy $2n - 1$ pontú gráfban, ahol minden csúcs foka legalább $n - 1$ létezik Hamilton-út!

14. Egy hotelba egy 100 fős társaság érkezik, akik közül kezdetben bármely két ember jóban van egymással. Esténként egyetlen nagy kerek asztal körül ül le mindenki. Sajnos egy vacsora alkalmával az egymás mellé került emberek örökre összevesznek egymással. A társaság minden vacsora előtt úgy ül le, hogy mindenki a szomszédjaival jóban legyen. Ha ez lehetetlen, akkor az összes résztvevő még aznap este haza megy. Bizonyítsuk be, hogy legalább 25 éjszakát a hotelban tölt a társaság!

Bevezetés a számításelméletbe II.
2007. FEBRUÁR 21.
2. gyakorlat: Színezések

Információk: http://www.cs.bme.hu/∼tothagi

15. Hány szín szükséges az alábbi gráf pontjainak kiszínezéséhez?



16. Legyen $V(G) = \{v_1, \ldots, v_{100}\}$, ahol v_i és v_j között akkor és csak akkor megy él, ha $7 \geq |i - j|$. Mennyi G kromatikus száma?

17. A sakktábla mezői alkossák most a gráfunk pontjait. Köztük él pontosan akkor menjen, ha az egyik mezőről a másikra bástyával el tudunk lépni. Hány színnel színezhető ez a gráf?

18. G csúcsai legyenek az természetes számok, és legyen az n és m csúcs összekötve pontosan akkor, ha $n + m$ páratlan. Határozzuk meg $\chi(G)$-t!

19. Mutassunk egy olyan gráfot, melyben nincs teljes 4 pontú részgráf, de nem színezhető ki 3 színnel.

20. Legyen G és H két különböző gráf (diszjunkt ponthalmazokkal). Készítsünk belőlük egyetlen F gráfot úgy, hogy G minden pontját összekötjük H minden pontjával. Bizonyítsuk be, hogy $\chi(F) = \chi(G) + \chi(H)$.

21. Bizonyítsuk be, hogy minden gráfnak sorbarendezhetők úgy a csúcsai, hogy ha ebben a sorrendben színezzük a gráfot mohó algoritmussal, akkor $\chi(G)$ színt használunk.

22. Bizonyítsuk be, hogy $\alpha(G) \cdot \chi(G) \geq |V(G)|$!

23. Bizonyítsuk be, hogy $\chi(G) \cdot \chi(\overline{G}) \geq |V(G)|$!

24. Ha tudjuk, hogy két színnel színezhető az n csúcsú G gráf, akkor mennyi lehet legfeljebb az élek száma?

25. Tegyük fel, hogy a G gráfot megszíneztük $\chi(G)$ színnel; legyen ezek közül a színek közül kettő a piros és a kék. Bizonyítsd be, hogy ekkor található a gráfban két szomszédos csúcs, amelyek közül az egyik piros, a másik kék.

26. Lássuk be, hogy $|E(G)| \geq \binom{\chi(G)}{2}$!

27. A G egyszerű gráfban 2006 darab kivételes ponttól eltekintve minden pont foka legföljebb 2005. Bizonyítsd be, hogy $\chi(G) \leq 2006$.

28. Határozzuk meg az összes olyan 10 csúcsú egyszerű G gráfot, amelyre $\chi(G) = 2$, de bárhogy húzunk be G-be egy új élet (két nemszomszédos csúcsa közé), a kapott G' gráfra $\chi(G') > 2$!

29. Egy G gráf csúcshalmaza legyen a $V(G) = \{1, 2, 3, \ldots, 100\}$ halmaz. Egy $x \in V(G)$ csúcs akkor legyen szomszédos az $y \in V(G)$ csúccsal, ha $x \neq y$ és $100 \leq x \cdot y \leq 400$. Határozzuk meg $\chi(G)$ értékét!

30. Legyen G olyan gráf, melyre $\chi(G) = k$. Bizonyítsuk be, hogy G élei irányíthatók úgy, hogy a leghosszabb irányított út legfeljebb k pontot tartalmazzon! (Az élek irányítása azt jelenti, hogy minden él egyik végére egy nyilat teszünk. Irányított út azt jelenti, hogy úgy teszünk meg egy utat a gráfban, hogy a nyilakkal szemben nem haladhatunk.)

31. Legyen G egy olyan egyszerű gráf, amelynek pontjai számozhatóak úgy, hogy minden pont legfeljebb kettő nála nagyobb sorszámúval szomszédos. Igazoljuk, hogy $\chi(G) \leq 3$.

32. Adott a síkban néhány egyenes úgy, hogy semelyik három nem megy át egy ponton. Legyen G az ezek által meghatározott gráf: G csúcsai az egyenesek metszéspontjai, két csúcs pedig akkor szomszédos, ha ez egyik egyenesen szomszédos metszéspontok. Mutassuk meg, hogy $\chi(G) \leq 3$!

Bevezetés a számításelméletbe II.

2007. FEBRUÁR 28.

3. gyakorlat: Élszínezés, perfekt gráfok, PERT-módszer

33. Mennyi a Petersen-gráf élkromatikus száma (χ_e)?

34. A G páros, egyszerű gráfban minden pont foka r ($r \geq 2$). Osszuk fel G egy tetszőleges élét egy ponttal. Mennyi a keletkezett G' gráf $\chi_e(G')$ élkromatikus száma?

35. Egy körmérkőzéses bajnokságot hány forduló alatt tudunk lejátszani, ha

    (a) páros számú játékos

    (b) páratlan számú játékos van a bajnokságban?

36. Mennyi $\chi_e(K_{2n} - \{n \text{ darab független él}\})$?

37. Mely n-ekre lesz $L(K_n)$, az n-szögpontú teljes gráf élgráfja perfekt?

38. Lássuk be, hogy egy páratlan kör komplementere nem perfekt!

39. Bizonyítsuk be, hogy egy páros gráf komplementere perfekt!

40. A G gráf csúcsai legyenek a 8×8-as sakktábla mezői, és két mező akkor legyen szomszédos G-ben, ha egy lóugrásnyira vannak egymástól.

    (a) Határozzuk meg G kromatikus számát, $\chi(G)$-t!

    (b) Bizonyítsuk be, hogy G perfekt!

41. Legyen G összehasonlítási gráf (két csúcs pontosan akkor van összekötve benne, ha egy rendezés szerint az egyik nagyobb, mint a másik), és legyenek az élei úgy irányítva, hogy a rendezés szerint mindig a nagyobb felé mutassanak. Minden csúcs mellé írjuk oda a belőle induló leghosszabb irányított út csúcsainak számát.

    (a) Bizonyítsuk be, hogy szomszédos csúcsok mellé nem írtuk ugyanazt a számot!

    (b) Bizonyítsuk be, hogy G perfekt!

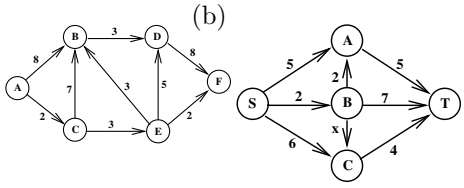
42. Bizonyítsuk be, hogy egy intervallum gráf komplementere összehasonlítási gráf!

43. Jelölje D_9 azt a 18 élű gráfot, amit úgy kaphatunk egy 9 hosszúságú körből, hogy a körben másodszomszédos pontokat is összekötjük. Állapítsuk meg, hogy D_9 perfekt gráf-e!

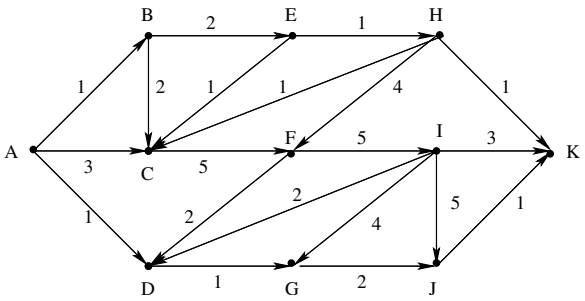
44. Legyenek egy G gráf csúcsai azok a 10^{100}-nál nem nagyobb pozitív egész számok, amelyeknek van 20-nál kisebb prímosztója. G két csúcsa pontosan akkor alkot élet, ha a megfelelő pozitív egészek relatív prímek. Állapítsuk meg G kromatikus számának értékét! Igaz-e hogy perfekt-e?

45. Határozzuk meg a mellékelt PERT-diagrammokhoz tartozó össz-időt és kritikus tevékenységeket. (A második példában az x változó függvényében.)

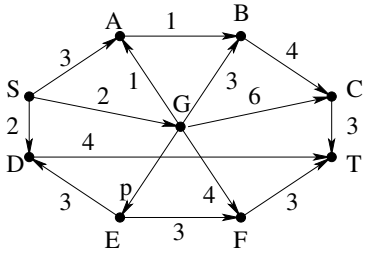
(a) (b)



46. Állapítsuk meg a feladat elvégzéséhez minimálisan szükséges idő hosszát az alábbi PERT diagramon:



47. Állapítsuk meg, hogy a p paraméter függvényében mennyi a feladat elvégzéséhez minimálisan szükséges idő az alábbi PERT diagram által leírt munkafolyamatnál! Melyek a kritikus tevékenységek?



48. A G irányított gráf csúcsai legyenek egy n elemű halmaz összes részhalmazai. Az A részhalmazból akkor vezessen egy irányított él a B részhalmazba, ha $A \subseteq B$, de $A \neq B$. Az A-ból B-be vezető élhez rendeljük hozzá az $|A| + |B|$ értéket. Határozzuk meg az így kapott PERT feladatban a szükséges időt és kritikus tevékenységeket!

49. Mutassuk meg, hogy egy hurokmentes irányított gráf élhalmaza felbontható két diszjunkt részhalmazra úgy, hogy egyik sem tartalmaz irányított kört!

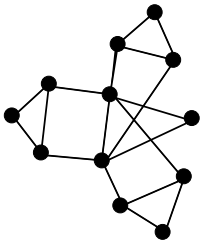
50. A G irányított gráfból legföljebb k él kitörlésével elérhető, hogy a maradék gráfban ne legyen irányított kör. Bizonyítsuk be, hogy ekkor G-ben legföljebb k él irányításának megfordításával is elérhető, hogy a kapott grában ne legyen irányított kör.

Bevezetés a számításelméletbe II.

2007. MÁRCIUS 7.

4. gyakorlat: Párosítások, König és Gallai tételei

51. Van-e teljes párosítás az alábbi gráfban?



52. Bizonyítsd be, hogy egy reguláris páros gráfban mindig létezik teljes párosítás!

53. Lássuk be, hogy egy reguláris páros gráf élhalmaza partícionálható teljes párosításokra! (Tehát az élek kiszínezhetőek r db színnel úgy, hogy mindegyik egyszínű élhalmaz egy teljes párosítást adjon.)

54. Valaki véletlenszerűen szétosztott egy pakli francia kártyát 13 darab 4 lapból álló csomagba. Bizonyítsuk be, hogy ekkor mindegyik csomagból kiválasztható egy lap úgy, hogy a kiválasztott lapok között mindegyik fajta figurából éppen egy legyen (vagyis egy darab 2-es, egy darab 3-as, stb., egy darab A). (A francia kártyában 13 fajta figura van: 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A. Minden figurából 4 darab van egy pakliban.)

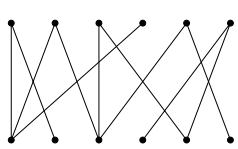
55. Adott egy $n \times n$ -es mátrix, amelynek minden sorában, és oszlopában pontosan k darab egyes van. Bizonyítsd be, hogy ekkor kiválasztható n darab egyes úgy, hogy minden sorból és oszlopból pontosan egy darab egyest választottunk ki!

56. Egy táncmulatságon 25 lány és 25 fiú van jelen. E társaságban minden lány ismeretségben van legalább 13 fiúval és minden fiú legalább 13 lánnyal. Bizonyítsuk be, hogy páros táncra perdülhetnek egyszerre mind az 50-en úgy, hogy az egymással táncolók ismerik egymást!

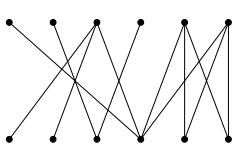
57. Egy ünnep alkalmával török szultán udvarában a férfiak két-két háremhölgyet választanak. Minden férfinek legalább 2 háremhölgy tetszik. Mi a feltétele annak, hogy minden férfi neki tetsző két háremhölggyel tölthesse az éjszakát?

58. Határozzuk meg az alábbi gráfokban a $\tau(G), \nu(G), \rho(G)$ és $\alpha(G)$ értékeket!

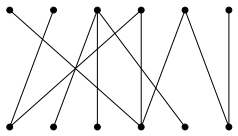
(a)



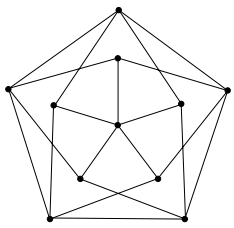
(b)



(c)



(d)



59. Határozzuk meg az alábbi gráfokra $\alpha(G)$, $\nu(G)$, $\rho(G)$ és $\tau(G)$ értékeit?

   (a) $K_{3,3}$,

   (b) K_5

   (c) $V(G) = \{v_1, v_2, \ldots, v_{2004}\}$ és $(v_i, v_j) \in E(G)$, ha $i + j$ hárommal osztva 1 maradékot ad.

   (d) Petersen-gráf

60. Legyen $V(H) = \{v_1, v_2, \ldots v_{74}\}$. A v_i és v_j ($i \neq j$) csúcsok között akkor menjen él, ha $i + j$ és 74 relatív prímek. Határozzuk meg az $\alpha(H)$ – független pontok maximális, $\nu(H)$ – független élek maximális, $\rho(H)$ – a lefogó élek minimális, $\tau(H)$ – lefogó pontok minimális számát!

61. Legyen G egy $2n$ pontú gráf, mely egy $2n-1$ pontú L útból és egy c pontból áll, ami L minden pontjával össze van kötve. Mennyi $\tau(G)$?

62. Lássuk be, hogy egy n pontú egyszerű G gráfban $\tau(G) = n - 1$ akkor és csak akkor, ha $G = K_n$

63. Igazoljuk, hogy minden egyszerű G gráfban $\tau(G) \leq 2\nu(G)$ és létezik olyan gráf is, melyre az egyenlőség teljesül.

64. Jelölje $\Delta(G)$ a G gráf maximális fokszámát, $\tau(G)$ pedig a lefogó pontok minimális számát. Bizonyítsuk be, hogy $\Delta(G) \cdot \tau(G) \geq |E(G)|$.

65. Jelölje $\omega(G)$ a G gráf egyik maximális klikkjének méretét. Mutassuk meg, hogy: $\alpha(G) + \omega(G) \leq |V(G)| + 1$

66. Igazoljuk, hogy tetszőleges n csúcsú G egyszerű gráfra fennáll, hogy $\alpha(G) \geq n - 2\nu(G)$.

Bevezetés a számításelméletbe II.

2007. MÁRCIUS 14.

5. gyakorlat: Folyamok

67. Egy vállalatnál hét pályázó jelentkezett hat üres munkahelyre (számozzuk ezeket 1-től 6-ig), egy ember több helyre is: Aladár az 1-es; Béla az 1, 3-as; Csaba a 2, 4, 6-os; Dani a 2, 5-ös; Erzsi a 3, 4, 5, 6-os; Feri az 1, 3-as; Géza a 3-as munkahelyre.

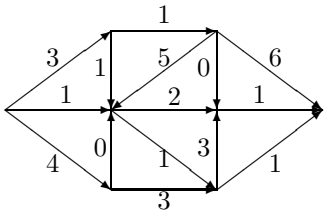
    (a) Döntsd el, hogy betölthető-e mind a hat munkahely (egy ember csak egy helyre kerülhet)! Ha nem, akkor hány tölthető be?

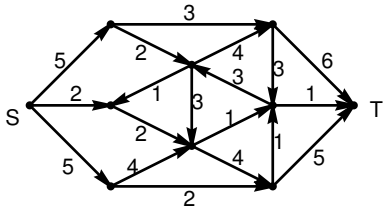
    (b) Változtat-e valamin, ha Feri meggondolja magát és a 2-es munkahelyet is hajlandó elfogadni?

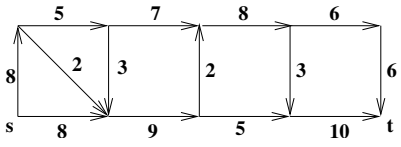
68. Egy $2n$ pontú egyszerű gráfban minden pont foka legalább n. Bizonyítsuk be, hogy ekkor van benne teljes párosítás!

69. Egy kiránduláson n házaspár vesz részt. El kellene osztani közöttük $2n$ különböző fajta csokit úgy, hogy mindenki egyet-egyet kapjon. Tudjuk, hogy mindenki legalább n fajtát szeret a csokik közül. Továbbá minden emberre teljesül, hogy ha ő valamelyik fajta csokit nem szereti, akkor a házastársa ezt a fajtát biztosan szeretni fogja. Bizonyítsd be, hogy a csokik szétoszthatók úgy, hogy mindenki olyat kapjon, amit szeret!

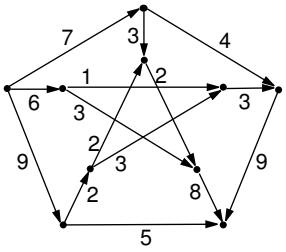
70. Számítsuk ki a maximális folyam értékét és bizonyítsuk be, hogy az tényleg maximális!



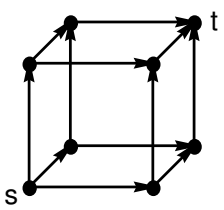




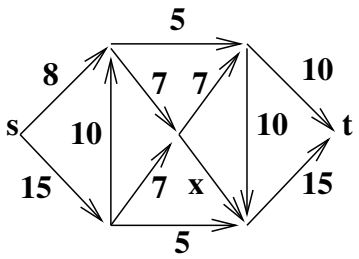
71. Határozzuk meg a maximális folyam értékét az alábbi gráfokban és bizonyítsuk is be, hogy ez maximális.



72. Az alábbi gráf élei közül írjunk hatra 1 és hatra 2 kapacitást úgy, hogy a maximális folyam a lehető legnagyobb illetve a lehető legkisebb legyen.



73. Keressünk maximális folyamot x függvényében!



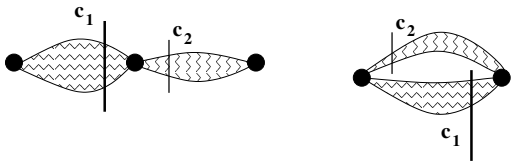
74. Igazak-e az alábbi állítások? Nemleges válasz esetén mutassunk ellenpéldát, igenlő válasz esetén pedig igazoljuk az állítást!

    (a) Egy folyam élein a kapacitások *egész* számok. Létezik-e olyan maximális folyam, aminek minden élén *egész* a folyam értéke?

    (b) ugyanaz a feladat, csak most nem *egész*, hanem *páros*

    (c) ugyanaz a feladat *páratlan* esetre

75. Adott két hálózati folyam, melyekben a minimális vágás értéke c_1 illetve c_2. Mekkora lesz a maximális folyam értéke abban a hálózatban, amit a két folyam soros illetve párhuzamos egymáshoz kapcsolásával kapunk?



76. A G irányított gráf csúcsai legyenek az $1, 2, \ldots, 2k$ egész számok. Az a számból b-be vezessen irányított él, ha $b > a$. Az a-ból b-be vezető él kapacitása legyen 1, ha a páratlan és legyen 2, ha a páros. Mennyi az így kapott hálózatban az 1-ből $2k$-ba vezető maximális folyam értéke?

77. Egy irányított gráfban nincs (irányított) kör $\Longrightarrow$ van forrás és nyelő a gráfban. Igaz-e az állítás? És a megfordítása?

Bevezetés a számításelméletbe II.

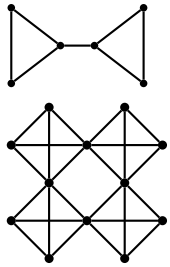
2007. MÁRCIUS 21.

6. gyakorlat: Összefüggőség, Menger-tételek

78. Hányszorosan pont- illetve élösszefüggőek az alábbi gráfok:

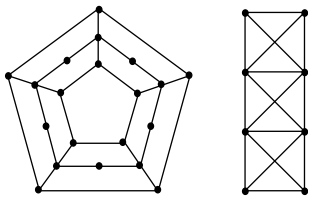
(a)

(b)



(c) Petersen-gráf
(d) végtelen négyzetrács
(e) n hosszú kör
(f) $K_{n,n}$

79. Hányszorosan összefüggőek az alábbi gráfok?



80. Mutassuk meg, hogy a k-szoros pontösszefüggésből következik a k-szoros élösszefüggés, de ugyanez visszafelé már nem teljesül!

81. Bizonyítsuk be, hogy minden háromszorosan összefüggő gráfban van páros hosszúságú kör!

82. Bizonyítsuk be, hogy egy 2-reguláris gráf pont- és élösszefüggőségi száma megegyezik! Mi van, ha a gráf 3- vagy 4-reguláris?

83. Bizonyítsuk be, hogy ha egy $2n$ pontú G gráf n-szeresen élösszefüggő, akkor kétszeresen pontösszefüggő is!

84. Legyen A és B a G gráf csúcsai halmazának két diszjunkt, egyenként legalább k elemű részhalmaza. Tegyük fel, hogy bárhogyan hagyunk el G-ből k-nál kevesebb pontot, a maradék gráfban van olyan út, amely A és B-beli pontokat köt össze. Bizonyítsd be, hogy ekkor létezik G-ben k darab (teljes egészében) pontdiszjunkt út úgy, hogy mindegyik A és B-beli pontokat köt össze!

85. Egy $n \times n$-es négyzetrács n^2 darab csúcsából m-et pirosra festettünk. Szeretnénk minden piros csúcsot vonallal összekötni a rács szélének valamelyik pontjával úgy, hogy a vonalak csak a rács élein haladjanak és semelyik kettő ne messe egymást. Adj (hatékony) algoritmust, amely eldönti, hogy ez lehetséges-e!

86. A $G(V, E)$ összefüggő gráfban minden $v \in V$ ponthoz és $e \in E$ élhez van olyan kör, amely v-n is és e-n is átmegy. Mutassuk meg, hogy a G gráf kétszeresen összefüggő!

87. Legyenek A, B és C diszjunkt, r elemű halmazok. Készítsünk egy G gráfot úgy, hogy a csúcsainak halmaza legyen $A \cup B \cup C$ és két csúcsot akkor kössünk össze éllel, ha nem ugyanabba a halmazba esnek. Határozzuk meg azt a maximális k számot, amelyre a G gráf k-szorosan összefüggő.

88. Legyen $k \leq n - 1$. Bizonyítsd be, hogy ha egy n pontú egyszerű gráfban minden pont foka legalább $\frac{n+k-2}{2}$, akkor a gráf k-szorosan összefüggő!

89. Legyen G reguláris páros gráf, amelyről tudjuk, hogy összefüggő és legalább három csúcsa van. Mutassuk meg, hogy ekkor G 2-szeresen is összefüggő.

90. Bizonyítsuk be, hogy ha G egy egyszerű síkgráf, akkor nem lehet hatszorosan pontösszefüggő!

Bevezetés a számításelméletbe II.

2007. MÁRCIUS 28.

7. gyakorlat: Turán tételek, Számelmélet I.

91. Legyen G a 3 osztályú, 12 pontú Turán-gráf. Állapítsuk meg $\tau(G)$ értékét!

92. Egy 30 fős társaságban bármely 4 ember között van kettő, akik kezet fogtak egymással. Bizonyítsuk be, hogy ekkor a társaság tagjai között legalább 135 kézfogás történt!

93. Egy 49 csúcsú gráfnak 1030 éle van. Mutassuk meg, hogy ekkor a kromatikus száma legalább 8, és hogy pontosan 8 is lehet.

94. Minimálisan hány éle kell legyen egy 2000 csúcsú G gráfnak, ha $\alpha(G) = 5$ teljesül?

95. Legyen adott a térben 100 tetszőleges pont. Bizonyítsd be, hogy ezek közül kiválasztható, éppen egységnyi távolságra lévő pontpárok száma legfeljebb 3750!

96. Legyen $a = 50700$ és $b = 111384$. Végezzük el a két szám prímtényezős felbontását, majd ezen kanonikus alakok segítségével számítsuk ki a legnagyobb közös osztót, a legkisebb közös többszöröst, és mondjuk meg azt is, hogy hány olyan szám van, amely osztója a és b közül legalább az egyiknek!

97. Egy perzsa sahnak 100 felesége van, a börtönében is épp 100 rab sínylődik, 1-től 100-ig számozott cellákban. A börtöncellák zárjai "kétállásúak": ha egyet fordítanak rajtuk, a bezárt ajtó kinyílik, a nyitott ajtó bezáródik. A sah születésnapján a 100 feleség végigvonul a börtönön és a zárakkal játszanak. Az első feleség minden záron egyet fordít, a második feleség minden második ajtó zárján egyet fordít, stb., a k-adik feleség minden k-adik ajtó zárján egyet fordít, egészen a 100. feleségig. Végül azok a rabok, akiknek az ajtaja nyitva van, kiszabadulnak. Milyen sorszámú cellákban laknak a szerencsések?

98. A sah következő születésnapján a feleségek megint rosszalkodnak. Most az első feleség minden záron egyet fordít, a második feleség minden második ajtó zárján kettőt fordít, stb., a k-adik feleség minden k-adik ajtó zárján k-t fordít, egészen a 100. feleségig. Most milyen sorszámú cellák lakói szabadulnak?

99. Legyen a és b két páratlan szám. Mennyi $(a^2 + b^2, 4)$?

100. Bizonyítsuk be, hogy a páratlan négyzetszámok nem csak néggyel, de nyolccal osztva is 1 maradékot adnak!

101. Melyek azok a p prímszámok, melyre

    (a) $p + 10$ és $p + 14$ is prím,

    (b) $p^2 + 2$ is prím,

    (c) $p^2 + 4$ és $p^2 + 6$ is prím?

102. Bizonyítsd be, hogy a szomszédos *Fibonacci-számok* relatív prímek! De vajon mennyi a másodszomszédos Fibonacci-számok legnagyobb közös osztója?

103. Péter a XX. század második felében született, éppen nagyapja 53. születésnapján. Kettejük születési évszámai nem relatív prímek. Hány éves Péter?

104. Lássuk be, hogy öt egymás után következő természetes szám szorzata mindig osztható 120-szal!

105. Bizonyítsuk be, hogy minden n természetes szám egyértelműen felírható $n = k^2q$ alakban, ahol k természetes, q pedig négyzetmentes szám.

106. Bizonyítsd be, hogy ha $2^n - 1$ prím, akkor n is prím!

107. Melyik az a legkisebb 3-mal nem osztható szám, melynek 15 osztója van?

108. Hány olyan háromjegyű szám van, melynek osztóinak száma osztható 11-gyel?

109. Melyek az $n^4 + 4$ alakú prímszámok?

110. Relatív prím-e a következő két szám: $2^{100} - 1$ és $3^{100} - 1$?

Bevezetés a számításelméletbe II.

2007. április 4.

8. gyakorlat: Számelmélet I., Kongruencia

97. Egy perzsa sahnak 100 felesége van, a börtönében is épp 100 rab sínylődik, 1-től 100-ig számozott cellákban. A börtöncellák zárjai "kétállásúak": ha egyet fordítanak rajtuk, a bezárt ajtó kinyílik, a nyitott ajtó bezáródik. A sah születésnapján a 100 feleség végigvonul a börtönön és a zárakkal játszanak. Az első feleség minden záron egyet fordít, a második feleség minden második ajtó zárján egyet fordít, stb., a k-adik feleség minden k-adik ajtó zárján egyet fordít, egészen a 100. feleségig. Végül azok a rabok, akiknek az ajtaja nyitva van, kiszabadulnak. Milyen sorszámú cellákban laknak a szerencsések?

98. A sah következő születésnapján a feleségek megint rosszalkodnak. Most az első feleség minden záron egyet fordít, a második feleség minden második ajtó zárján kettőt fordít, stb., a k-adik feleség minden k-adik ajtó zárján k-t fordít, egészen a 100. feleségig. Most milyen sorszámú cellák lakói szabadulnak?

99. Legyen a és b két páratlan szám. Mennyi $(a^2+b^2, 4)$?

100. Bizonyítsuk be, hogy a páratlan négyzetszámok nem csak néggyel, de nyolccal osztva is 1 maradékot adnak!

101. Melyek azok a p prímszámok, melyre

    (a) $p+10$ és $p+14$ is prím,

    (b) p^2+2 is prím,

    (c) p^2+4 és p^2+6 is prím?

102. Bizonyítsd be, hogy a szomszédos *Fibonacci-számok* relatív prímek! De vajon mennyi a másodszomszédos Fibonacci-számok legnagyobb közös osztója?

103. Péter a XX. század második felében született, éppen nagyapja 53. születésnapján. Kettejük születési évszámai nem relatív prímek. Hány éves Péter?

104. Lássuk be, hogy öt egymás után következő természetes szám szorzata mindig osztható 120-szal!

105. Bizonyítsuk be, hogy minden n természetes szám egyértelműen felírható $n = k^2q$ alakban, ahol k természetes, q pedig négyzetmentes szám.

106. Bizonyítsd be, hogy ha 2^n-1 prím, akkor n is prím!

107. Melyik az a legkisebb 3-mal nem osztható szám, melynek 15 osztója van?

108. Hány olyan háromjegyű szám van, melynek osztóinak száma osztható 11-gyel?

109. Melyek az n^4+4 alakú prímszámok?

110. Relatív prím-e a következő két szám: $2^{100}-1$ és $3^{100}-1$?

111. Bizonyítsuk be, hogy a páratlan négyzetszámok nem csak néggyel, de nyolccal osztva is 1 maradékot adnak!

112. Melyek azok a p prímszámok, melyre

    (a) $p+10$ és $p+14$ is prím,

    (b) p^2+2 is prím,

    (c) p^2+4 és p^2+6 is prím?

113. Bizonyítsd be, hogy ha 2^n-1 prím, akkor n is prím!

114. Határozzuk meg a $3, 8, 17, -17, 120, 54, -40, 236, 227$ számok

    (a) legkisebb nem negatív maradékait,

    (b) abszulutértékben legkisebb maradékait,

    (c) közül melyek kongruensek egymással

    modulo 11!

115. Oldjuk meg az alábbi kongruenciákat:

    (a) $11x \equiv 12 \pmod{18}$,

    (b) $5x \equiv 5 \pmod{35}$,

    (c) $6x \equiv 5 \pmod{35}$,

    (d) $7x \equiv 5 \pmod{35}$,

    (e) $6x+1 \equiv 10 \pmod{15}$,

    (f) $14x-4 \equiv 80 \pmod{21}$.

116. Oldjuk meg minél egyszerűbben az alábbi kongruenciákat:

    (a) $202x \equiv 157 \pmod{203}$,

    (b) $309x \equiv 451 \pmod{617}$,

    (c) $5x \equiv 561 \pmod{1968}$,

    (d) $105x \equiv 761 \pmod{809}$,

117. Milyen maradékot adhat egy egész szám 92-vel osztva, ha az 54-szerese 24 maradékot ad 92-vel osztva?

118. Egy x egész szám ugyanannyi maradékot ad 98-cal osztva, mint $68-23x$. Mi lehet ez a maradék?

119. Melyek megoldhatóak az alábbi szimultán kongruenciák közül? Oldjuk is meg őket!

    (a) $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{7}$

    (b) $x \equiv 3 \pmod{6}$, $x \equiv 6 \pmod{8}$

    (c) $3x \equiv 2 \pmod{4}$, $2x \equiv 3 \pmod{5}$

    (d) $5x \equiv 3 \pmod{7}$, $4x \equiv 5 \pmod{10}$

Bevezetés a számításelméletbe II.

2007. ÁPRILIS 11.

9. gyakorlat: Számelmélet, folytatás

97. Egy perzsa sahnak 100 felesége van, a börtönében is épp 100 rab sínylődik, 1-től 100-ig számozott cellákban. A börtöncellák zárjai "kétállásúak": ha egyet fordítanak rajtuk, a bezárt ajtó kinyílik, a nyitott ajtó bezáródik. A sah születésnapján a 100 feleség végigvonul a börtönön és a zárakkal játszanak. Az első feleség minden záron egyet fordít, a második feleség minden második ajtó zárján egyet fordít, stb., a k-adik feleség minden k-adik ajtó zárján egyet fordít, egészen a 100. feleségig. Végül azok a rabok, akiknek az ajtaja nyitva van, kiszabadulnak. Milyen sorszámú cellákban laknak a szerencsések?

98. A sah következő születésnapján a feleségek megint rosszalkodnak. Most az első feleség minden záron egyet fordít, a második feleség minden második ajtó zárján kettőt fordít, stb., a k-adik feleség minden k-adik ajtó zárján k-t fordít, egészen a 100. feleségig. Most milyen sorszámú cellák lakói szabadulnak?

101. Melyek azok a p prímszámok, melyre

   (a) $p+10$ és $p+14$ is prím,

   (b) p^2+2 is prím,

   (c) p^2+4 és p^2+6 is prím?

102. Bizonyítsd be, hogy a szomszédos *Fibonacci-számok* relatív prímek! De vajon mennyi a másodszomszédos Fibonacci-számok legnagyobb közös osztója?

106. Bizonyítsd be, hogy ha 2^n-1 prím, akkor n is prím!

107. Melyik az a legkisebb 3-mal nem osztható szám, melynek 15 osztója van?

108. Hány olyan háromjegyű szám van, melynek osztóinak száma osztható 11-gyel?

116. Oldjuk meg minél egyszerűbben az alábbi kongruenciákat:

   (a) $202x \equiv 157 \pmod{203}$,

   (b) $309x \equiv 451 \pmod{617}$,

   (c) $5x \equiv 561 \pmod{1968}$,

   (d) $105x \equiv 761 \pmod{809}$,

119. Melyek megoldhatóak az alábbi szimultán kongruenciák közül? Oldjuk is meg őket!

   (a) $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$

   (b) $x \equiv 3 \pmod 6$, $x \equiv 6 \pmod 8$

   (c) $3x \equiv 2 \pmod 4$, $2x \equiv 3 \pmod 5$

   (d) $5x \equiv 3 \pmod 7$, $4x \equiv 5 \pmod{10}$

120. (a) Egy százlábú meg akarja számolni a lábait. Azt tudja biológiából, hogy minden százlábúnak legföljebb 344 lába van. Ha 13-asával számolja a lábait, akkor 3 marad ki, ha 17-esével számolja, akkor viszont 10 marad ki. Hánylábú a százlábú?

   (b) Egy másik százlábú is megirigyli ezt a módszert. Neki 16-osával számolva 5 marad ki, 20-asával számolva pedig 15 marad ki. Bizonyítsd be, hogy elszámolta magát!

   (c) A százlábúak királyához is eljut a módszer. Neki 6-osával számolva 5 marad ki, 7-esével számolva 6, 8-asával számolva pedig 7. Neki hány lába van?

121. Egy háromjegyű számról tudjuk, hogy 23-mal osztva 4 maradékot ad, továbbá hogy a szám 16-szorosának utolsó két számjegye 28. Mi ez a szám?

122. Oldjuk meg a megoldhatóakat az alábbi lineáris diofantikus egyenletek közül!

   (a) $15x+13y=19$

   (b) $17x+11y=22$

   (c) $12x+30y=26$

   (d) $18x+28y=10$

123. (a) Milyen számok állíthatók elő $20x+51y$ alakban, ahol x és y egész számok?

   (b) Milyen számok állíthatók elő $170x+51y$ alakban, ahol x és y egész számok?

   (c) Milyen számok állíthatók elő $21x+33y+77z$ alakban, ahol x, y és z egész számok?

124. Bizonyítsuk be, hogy $1 \cdot 19 \cdot 37 \cdot 55 \cdot 73 \cdot \ldots \cdot 271 + 1$ osztható 17-tel!

125. Pataki Ferenc fejszámolóművész egyszer a tévében a következő trükköt mutatta be: felkért a közönségből valakit, hogy gondoljon egy háromjegyű számra, szorozza meg 6561-gyel, majd az eredmény utolsó három jegyét közölje. Ebből ő pillanatok alatt kitalálta a gondolt számot. Hogyan csinálta? Utána tudnád-e csinálni, ha használhatsz számológépet, de csak nagyon rövid ideig?

126. Legyenek k és n olyan pozitív egészek, amelyekre $k < n$. Mi a legnagyobb közös osztója az $n! + k$ és az $(n+1)! + k$ számoknak?

Bevezetés a számításelméletbe II.

2007. április 18.

10. gyakorlat: Számelmélet, csoportelmélet

128. Számítsuk ki az alábbi értékeket:

   (a) $d(12)$, $\phi(12)$, $\sigma(12)$,

   (b) $d(2004)$, $\phi(2004)$, $\sigma(2004)$.

129. Mennyi $\phi(9)$, $\phi(133)$, $\phi(540)$, $\phi(7!)$?

130. Milyen n értékekre igaz, hogy $\phi(n)$ páratlan? (és milyen n-ekre lesz $d(n)$ páratlan?)

131. Az Euler-féle ϕ függvény tulajdonságait felhasználva,

   (a) bizonyítsuk be, hogy $11 \mid n^{11} + 10n$,

   (b) igazoljuk, hogy ha n nem osztható 17-tel, akkor $n^8 + 1$ vagy $n^8 - 1$ biztosan osztható 17-tel,

   (c) számítsuk ki 108^{182} ill. 5^{17} maradékát 19-cel osztva,

   (d) bizonyítsuk be, hogy $42 \mid n^7 - n$.

132. Bizonyítsuk be, hogy

   (a) $39^{14} - 1$ osztható 5-tel,

   (b) $333^{444} + 444^{333}$ osztható 7-tel,

   (c) $4^{90} + 1$ osztható 17-tel!

133. Kiszámítandó $(((43)^{43})^{43})^{43}$ modulo 49.

134. Oldjuk meg az alábbi kongruenciákat:

   (a) $49^{49} \equiv x \pmod{15}$,

   (b) $3^{80}x \equiv 23 \pmod{100}$.

135. Határozzuk meg az utolsó

   (a) három jegyét számjegyét 403^{402}-nek,

   (b) két számjegyét $29^{39^{49}}$-nek,

   (c) számjegyét $7^{6^{5^{4^{3^2}}}}$ -nek!

136. Mi az utolsó két számjegye az alábbi számoknak?

   (a) 2001^{2005}

   (b) $99^{77^{55}}$

   (c) $99! + 1$

   (d) 51^{151}

   (e) $17^{17^{17}} - 17^{17} + 17$

137. Bizonyítsuk be, hogy a $\frac{21n+4}{14n+3}$ tört semmilyen nemnegatív egész n-re sem egyszerűsíthető!

138. Legyen n páratlan egész szám, amely nem osztható egyetlen prímszám négyzetével sem. Bizonyítsuk be, hogy n pozitív osztóinak átlaga egész szám!

139. Legyen n pozitív egész szám, melynek ismerjük $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ prímtényezős felbontását. Mennyi a

$$\sum_{d_i \mid n} \frac{1}{d_i}$$

   érték, vagyis hogyan számítható ki az n szám osztói reciprokának az összege?

140. Csoportot alkotnak-e az alábbi halmazon definiált műveletek? Ha igen, akkor vizsgáljuk meg, hogy a csoport kommutatív-e?

(a) {egész számok, összeadás},

(b) {páratlan számok, összeadás},

(c) {páros számok, összeadás},

(d) {2×2-es mátrixok, mátrixszorzás},

(e) {n-edik komplex egységgyökök, szorzás},

(f) a síkvektorok halmaza; a síkvektorok összeadása.

(g) egy tetszőleges X halmaz összes részhalmazainak halmaza; a halmazok uniója.

(h) egy tetszőleges X halmaz összes részhalmazainak halmaza; a halmazok szimmetrikus differenciája. (Az A és B halmazok szimmetrikus differenciája alatt definíció szerint az $A \Delta B = (A \setminus B) \cup (B \setminus A)$ halmazt értjük.)

141. Csoportot illetve félcsoportot alkot-e az alábbi H halmaz a $*$ művelettel?

(a) H az egész számok halmaza és az a, $b \in H$ számokra $a * b = a + b + 1$, ahol a szokásos összeadás szerepel;

(b) Legyen m egy rögzített szám és $H = \{1, 2, \ldots, m-1\}$. Továbbá $a * b = ab \pmod{m}$;

(c) H azon f függvények halmaza, melyek $f(x) = cx + d$ alakúak, ahol $c \neq 0$. A $*$ művelet pedig a függvények egymás után való alkalmazása (kompozíció, jelölése analízisben $f \circ g$);

(d) H a valós számok halmaza és $a * b = a + b + ab$;

(e) H a 2002 pozitív osztóinak halmaza és az $a, b \in H$ számokra $a * b = (a, b)$, azaz a és b legnagyobb közös osztója.

142. Bizonyítsd be $a^2 = 1 \quad \forall a \in G$-re $\Longrightarrow G$ – Abel-csoport!

143. A G véges Abel-csoport összes elemét összeszorozzuk valamilyen sorrendben. Bizonyítsd be, hogy eredményül G-nek olyan elemét kapjuk, amelynek az inverze önmaga!

144. Az n-ed rendű ciklikus csoport összes elemét négyzetre emeljük, majd az így kapott elemeket összeszorozzuk. Mivel egyenlő ez a szorzat?

145. Tekintsünk egy páratlan rendű Abel-csoportot (G), ahol a művelet az összeadás. Bizonyítsuk be, hogy $\sum_{a \in G} a = 0$.

146. Legyen $n \geq 4$. Az n hosszú 0-1 sorozatok H_1 halmazán jelölje $\oplus$ a bitenkénti modulo 2 összeadást. Álljon H_2 azokból a sorozatokból, melyekben az egyesek száma kettővel osztható. H_3 pedig azokból, melyekben az egyesek száma osztható hárommal. Az előbb definiált művelettel csoportot alkot-e H_2? Csoport-e H_3?

147. Írjuk fel az alábbi csoportok Cayley-táblázatát! Melyek izomorfak egymással?

(a) {mod 4 maradékosztályok, összeadás}

(b) {mod 8 redukált maradékosztályok, szorzás}

(c) A téglalap szimmetriacsoportja:
(szimmetriacsoport = a rajzot önmagába vivő egybevágósági transzformációk halmaza a kompozícióra, mint műveletre nézve!)

(d) A "füles négyzet" szimmetriacsoportja:

Bevezetés a számításelméletbe II.

2007. ÁPRILIS 25.

11. gyakorlat: Csoportelmélet

142. Bizonyítsd be $a^2 = 1 \quad \forall a \in G$-re $\Longrightarrow G$ Abel-csoport!

143. A G véges Abel-csoport összes elemét összeszorozzuk valamilyen sorrendben. Bizonyítsd be, hogy eredményül G-nek olyan elemét kapjuk, amelynek az inverze önmaga!

144. Az n-ed rendű ciklikus csoport összes elemét négyzetre emeljük, majd az így kapott elemeket összeszorozzuk. Mivel egyenlő ez a szorzat?

145. Tekintsünk egy páratlan rendű Abel-csoportot (G), ahol a művelet az összeadás. Bizonyítsuk be, hogy $\sum_{a \in G} a = 0$.

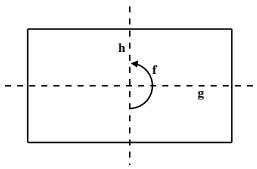
146. Legyen $n \geq 4$. Az n hosszú 0-1 sorozatok H_1 halmazán jelölje $\oplus$ a bitenkénti modulo 2 összeadást. Álljon H_2 azokból a sorozatokból, melyekben az egyesek száma kettővel osztható. H_3 pedig azokból, melyekben az egyesek száma osztható hárommal. Az előbb definiált művelettel csoportot alkot-e H_2? Csoport-e H_3?

147. Írjuk fel az alábbi csoportok Cayley-táblázatát! Melyek izomorfak egymással?

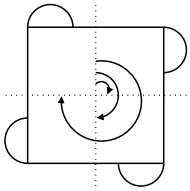
   (a) {mod 4 maradékosztályok, összeadás}

   (b) {mod 8 redukált maradékosztályok, szorzás}

   (c) A téglalap szimmetriacsoportja:
   (szimmetriacsoport = a rajzot önmagába vivő egybevágósági transzformációk halmaza a kompozícióra, mint műveletre nézve!)



   (d) A "füles négyzet" szimmetriacsoportja:



148. Mi az egyes elemek rendje C_{12}-ben (a 12 rendű ciklikus csoportban)?

149. Legyen a G csoport elemeinek halmaza $\{1, 2, 3, 4, 5, 6\}$, a művelet a mod 7 szorzás. Igazoljuk, hogy a G csoport ciklikus!

150. $|G| = 81$ és $\exists a \in G: \ a^{27} \neq 1 \Longrightarrow$ a csoport kommutatív.

151. Jelölje a és b egy csoport két tetszőleges elemét. Bizonyítsuk be, hogy b rendje megegyezik $a^{-1}ba$ rendjével!

152. Mely csoportokra igaz, hogy $(ab)^{-1} = a^{-1}b^{-1}$?

153. Bizonyítsuk be, hogy egy csoport nem állhat elő két valódi részcsoportjának úniójaként.

154. Bizonyítsuk be, hogy ha egy csoportban minden egységelemtől különböző elem rendje ugyanaz, akkor ez a rend prímszám!

155. Bizonyítsuk be, hogy ha a G csoport rendje 55, akkor minden $a \in G$ elemére teljesül, hogy az a és az a^8 elemek rendje azonos.

156. Van-e olyan 20 rendű csoport, melyben van 5 rendű elem, de nincs 20 rendű elem?
   És van-e olyan 20 rendű csoport, melyben van 20 rendű elem, de nincs 5 rendű elem?

157. A D_n diédercsoport elemei közül legyen t az egyik tükrözés és f az egyik forgatás. Igaz-e, hogy $t \cdot f = f^{-1} \cdot t$?

Bevezetés a számításelméletbe II.

2007. MÁJUS 2.

12. gyakorlat: Szimmetrikus csoport, normálosztó

158. Írjuk fel a következő permutációkat diszjunkt ciklusok szorzataként!

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 8 & 1 & 6 & 2 & 4 \end{pmatrix}, b = (456)(567)(671)(123)(234)(345)$$

159. Írjuk át a következő két permutációt ciklikus alakra, majd számítsuk ki a szorzatukat! Mi a kapott permutáció fixpontja?

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

160. Határozzuk meg a következő két elem rendjét az S_8 szimmetrikus csoportban!

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 5 & 6 & 8 & 7 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 8 & 7 & 4 & 3 & 1 & 2 \end{pmatrix}$$

161. Írjuk fel a szabályos háromszög és a szabályos nyolcszög szimmetriacsoportját! (D_3, D_8 diédercsoport)
Milyen egybevágósági transzformációt jelent az (123) illetve az (18)(27)(36)(45) permutáció? (Mindkét sokszögben a csúcsok 1-től n-ig számozottak.)

162. Vegyük a $\{0, 1, 2, 3, \ldots, 11\}$ számokat a $\pmod{12}$ összeadásra nézve.
Normálosztója-e ennek a csoportnak a 4-gyel osztható számok halmaza?
Ha igen, akkor mik a velük képzett faktorcsoportok?

163. Mik lehetnek a C_{12} ciklikus csoport további normálosztói? Mik a velük képzett faktorcsoportok?

164. Tekintsük az egész számokat az összeadás művelettel, és rendezzük a számokat a paritásuk szerint! A páratlan vagy a páros számok osztálya lehet-e normálosztó a csoportban? Mi a hozzá tartozó faktorcsoport?

165. Tekintsük a nemnulla komplex számokat a szorzás müvelettel, és rendezzük a számokat mellékosztályokba a hosszúságuk szerint! Melyik osztály lehet közülük a normálosztó? Mi a faktorcsoport?

166. Tekintsük a 2×2-es invertálható mátrixokat a mátrix-szorzás művelettel, és tegyük egy osztályba azokat a mátrixokat, melyeknek egyenlő a determinánsuk! Melyik osztály lehet közülük normálosztó a csoportban? Mi az ezzel képzett faktorcsoport?

Bevezetés a számításelméletbe II.

2007. MÁJUS 9.

13. gyakorlat: Csoportelmélet

167. Végezd el az alábbi műveleteket az S_n szimmetrikus csoportban. Add meg az eredmény ciklusfelbontását és határozd meg a rendjét!

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 1 & 4 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}$

(b) $(35)(1432)(35)(1234)$

(c) $[(134)(342)]^{-1}$

(d) $[(34)(23)(12)]^{2005}$

168. Határozd meg a megadott G csoportok H részcsoportja szerinti baloldali és jobboldali mellékosztályait, majd döntsd el, hogy H normálosztó-e? Ha igen, határozd meg a G/H faktorcsoportot!

(a) G az ötdimenziós valós vektorok az összeadással, H azokból a vektorokból áll, amelyeknek az utolsó két koordinátája 0;

(b) G a nemnulla valós számok a szorzással, $H = \{-1, 1\}$;

(c) $G = S_3$, $H = \{I, (12)\}$;

(d) G a nemnulla determinánsú $n \times n$-es mátrixok a mátrixszorzással; H az 1 determinánsú mátrixok.

(e) G az egész számok az összeadással, H a 2005-tel osztható egészek;

(f) G az $\{1, 2, \ldots, 10\}$ halmaz összes részhalmazainak halmaza a szimmetrikus differencia műveletével; H azokból a részhalmazokból áll, amelyek a 9-et és a 10-et nem tartalmazzák.

169. Legyen G véges csoport és $N \triangleleft G$ normálosztó. Mutasd meg, hogy a G/N faktorcsoport gN elemének rendje a legkisebb olyan k pozitív egész, melyre $g^k \in N$.

170. Döntsd el, hogy a megadott csoportokban baloldali mellékosztályt alkotnak-e (valamilyen részcsoport szerint) a megadott részhalmazok.

(a) az egész számok csoportja az összeadással; a $8k + 5$ ($k \in \mathbb{Z}$) alakú egészek.

(b) az egész számok csoportja az összeadással; a prímszámok.

(c) D_{15}; $\{t_1 f_{24}, t_1 f_{144}, t_1 f_{264}\}$.

(d) S_n; azok a permutációk, amik 1-hez 2-t rendelnek.

171. Döntsd el, hogy az alábbi G csoportok megadott H részcsoportjai normálosztók-e? Ha igen, határozd meg a G/H faktorcsoportot!

(a) G a nemnulla komplex számok a szorzással, H az 1 abszolútértékű komplex számok;

(b) G a nemnulla determinánsú $n \times n$-es mátrixok a mátrixszorzással, H a ± 1 determinánsú mátrixok;

(c) $G = D_n$, $H = \{I, t_1\}$;

(d) $G = D_n$, H a forgatásokból és az identitásból áll;

(e) $G = D_8$, $H = \{I, f_{90}, f_{180}, f_{270}\}$.

172. Mutasd meg, hogy ha egy G csoport azon elemei, melyek önmaguk inverzei, részcsoportot alkotnak, akkor ez egyben normálosztó is. Igaz-e mindig, hogy ez a részhalmaz részcsoport?

173. Legyen H a G csoport tetszőleges, N pedig a G csoport normális részcsoportja. Bizonyítsuk be, hogy ekkor $H \cap N$ normális részcsoportja H-nak.

174. Melyik az a legkisebb pozitív egész n szám, amire az S_n szimmetrikus csoportnak van D_4-gyel, vagyis a negyedfokú diédercsoporttal izomorf részcsoportja?

175. Bizonyítsd be, hogy egy csoport elemeinek nemüres részhalmaza akkor és csak akkor baloldali mellékosztály (valamely részcsoport szerint), ha jobb oldali mellékosztály (egy – esetleg – másik részcsoport szerint).

Bevezetés a számításelméletbe II.

2007. MÁJUS 16.

14. gyakorlat: Gyűrűk, testek; primtesztelés, gyorshatványozás; titkosítás

176. Gyűrűt, testet vagy ferdetestet alkotnak-e az alábbi halmazok (a szokásos összeadással és szorzással)?

   (a) $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$,

   (b) $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$,

   (c) egész együtthatós polinomok,

   (d) $\{0, 1\}$ a modulo 2 összeadással és szorzással,

   (e) a 4×4-es mátrixok,

   (f) a 4×4-es mátrixok, melyek determinánsa nem nulla, valamint a 4×4-es nulla mátrix

   (g) $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ alakú mátrixok, ahol $a, b \in \mathbb{R}$,

   (h) a kvaterniók.

177. Egy $x \neq 0$ gyűrűelem baloldali nullosztó, ha $\exists y \neq 0$, hogy $xy = 0$. Legyen x_1 és x_2 baloldali nullosztó. Bizonyítsuk be, hogy x_1x_2 is baloldali nullosztó, de $x_1 + x_2$ nem feltétlenül az!

178. A mod 12 maradékosztályok gyűrűjében mely elemeknek van multiplikatív inverzük? Melyek a nullosztók?

179. Adjunk példát az $n \times n$-es mátrixok gyűrűjében nullosztókra!

180. Legyen R egy nullosztómentes gyűrű. Bizonyítsuk be, hogy ha egy a elemre $a^2 = a$, akkor $a = 0$ vagy $a = 1$. Mutassuk meg, hogy egy nem nullosztómentes gyűrűben a fentiek nem igazak!

181. Lássuk be, hogy minden ferdetest nullosztómentes!

182. Igazoljuk, hogy ha egy testben $a + a = 0$ teljesül valamely $a \neq 0$ elemre, akkor minden elemre teljesül!

183. Oldjuk meg az $x^2 + 2x + 3 = 0$ egyenletet $GF(11)$-ben!

184. Számítsuk ki, hogy 15-el osztva mennyi maradékot ad 3^{2005}.
(Kettes számrendszerben $2005 = 11111010101$.)

185. A prímtesztelő algoritmusnak inputként a 15-öt adtuk be. Teszteléskor először az $a_1 = 4$, majd az $a_2 = 7$ számokat választotta ki véletlenszerűen a gép. Melyik szám lett árulója, és melyik lett cinkosa a 15-nek? Ezek után számolás nélkül mondjuk meg, hogy a 13 vajon áruló-e?

186. Lássuk be, hogy $3 \cdot 11 \cdot 17 = 561$ egy Carmichael szám!

187. Sikerült elfognunk Szeszlér tanár úr e-mailjét, amit Recski tanár úrnak küldött, és leírja benne, hogy mi lesz a kérdés a vizsgán. Sajnálatos módon a levél az RSA algoritmussal titkosítva van, de az ismeretes, hogy Recski tanár úr nyilvános kulcsa (85,43). Az eredeti üzenetben a számok jelentése:

A=2	D=6	G=11	J=21	M=26	P=31	S=36	V=41	Y=46
B=3	E=7	H=12	K=22	N=27	Q=32	T=37	W=42	Z=47
C=4	F=8	I=13	L=23	O=28	R=33	U=38	X=43	=48

A titkosított üzenetben a következő számok szerepelnek: 8, 27, 58, 48, 22, 81, 48, 76, 27, 8, 3, 6, 8, 46. Próbáljuk meg dekódolni a levelet!