Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató
2009. március 23.

Általános alapelvek.

A pontozási útmutató célja, hogy a javítók a dolgozatokat egységesen értékeljék. Ezért az útmutató minden feladat (legalább egy lehetséges) megoldásának főbb gondolatait és az ezekhez rendelt részpontszámokat közli. Az útmutatónak *nem célja* a feladatok teljes értékű megoldásának részletes leírása; a leírt lépések egy maximális pontszámot érő megoldás vázlatának tekinthetők.

Az útmutatóban feltüntetett részpontszámok csak akkor járnak a megoldónak, ha a kapcsolódó gondolat egy áttekinthető, világosan leírt és megindokolt megoldás egy lépéseként szerepel a dolgozatban. Így például az anyagban szereplő ismeretek, definíciók, tételek puszta leírása azok alkalmazása nélkül nem ér pontot (még akkor sem, ha egyébként valamelyik leírt tény a megoldásban valóban szerephez jut). Annak mérlegelése, hogy az útmutatóban feltüntetett pontszám a fentiek figyelembevételével a megoldónak (részben vagy egészében) jár-e, teljes mértékben a javító hatásköre.

Részpontszám jár minden olyan ötletekért, részmegoldásért, amelyből a dolgozatban leírt gondolatmenet alkalmas kiegészítésével a feladat hibátlan megoldása volna kapható. Az útmutatóban szereplő részpontszámok szükség esetén tovább is oszthatók. Az útmutatóban leírttól eltérő jó megoldás természetesen maximális pontot ér.

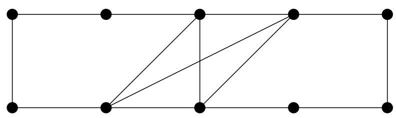
Minden feladat 10 pontot ér. Az elégséges határa 24 pont. A vizsgajegybe a dolgozat pontszáma számít bele, így a dolgozatokra osztályzatot nem adunk.

1. Legyen G egy 101 csúcsú egyszerű gráf, amelyben az egyik pont foka 50, az összes többi pont foka 49. Bizonyítsuk be, hogy G-hez hozzá lehet venni 50 darab élet úgy, hogy a kapott gráf továbbra is egyszerű gráf legyen és tartalmazzon Euler-kört.

* * * * *

G komplementerében, $\overline{G}$-ben 100 darab 51 fokú pont és egyetlen 50 fokú pont van (legyen ez v). (1 pont)
Így az Ore-tételből következik, hogy $\overline{G}$-ben van Hamilton-kör. (2 pont)
A $\overline{G}$-beli Hamilton-kör mentén haladva válasszuk ki minden második élet úgy, hogy v-re ne illeszkedjen kiválasztott él. (2 pont)
Az így kapott 50 darab $\overline{G}$-beli élet G-hez véve a kapott G' gráfban minden pont foka 50. (1 pont)
Állítjuk, hogy G' összefüggő. (1 pont)
Ha ugyanis nem volna az, akkor a legkisebb komponense legföljebb 50 csúcsú lenne; ekkor viszont ebben a komponensben minden pont foka legföljebb csak 49 lehetne. (2 pont)
G' összefüggő és minden pont foka páros, ezért a tanult tétel szerint valóban van Euler-köre. (1 pont)
(A pontozás úgy értendő, hogy aki az összefüggőség vizsgálatáról teljesen megfeledkezik, az 3 pontot veszít; aki megemlíti, hogy ez is szükséges, csak bizonyítania nem sikerül, az 2 pontot veszít.)

2. Legkevesebb hány élet kell törölni az alábbi gráfból ahhoz, hogy páros gráfot kapjunk?



* * * * *

Töröljük a gráfból a rajzon 45°-os szögben álló két élet. Ekkor a maradék gráf páros, mert a rajz keretét adó téglalap által meghatározott kör mentén a csúcsokat felváltva pirosra és kékre színezve a kapott gráf jó 2-színezését kapjuk. (4 pont)
2-nél kevesebb él törlésével nem kaphatunk páros gráfot, mert a gráfban található két diszjunkt, öt pontú kör (a felső sor első három és az alsó sor első két csúcsa alkotja az egyiket, a másik szimmetrikusan helyezkedik el); ezért legföljebb 1 él törlése után biztosan marad még páratlan kör, így a kapott gráf nem lehet páros. (Érvelhetünk úgy is, hogy a gráfban van 4 pontú klikk, ebből egy élet törölve biztosan marad még háromszög.) (6 pont)
Így legkevesebb 2 él törlése szükséges.

3. Legyen G egy 20 csúcsú egyszerű gráf, amelyben minden pont foka 8. Legyen v a G egy tetszőleges csúcsa és jelölje $G-v$ azt a gráfot, amelyet G-ből a v (és az összes v-re illeszkedő él) törlésével kapunk. Bizonyítsuk be, hogy $\chi_e(G-v) = \chi_e(G)$ (ahol χ_e a gráfok élkromatikus számát jelöli).

* * * * *

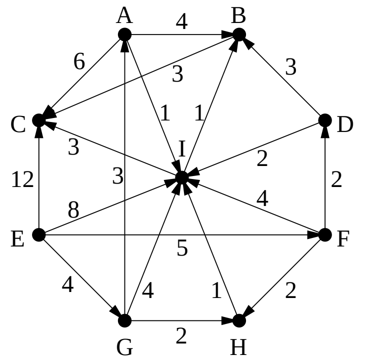
$(G-v)$-nek 19 csúcsa van, ebből 8 darab 7 fokú, a többi 8 fokú. (1 pont)
Így G-ben és $(G-v)$-ben is a maximális fokszám 8, ezért (a Vizing-tételt használva) mindkét gráf élkromatikus száma 8 vagy 9. (1 pont)
Ha $\chi_e(G-v) = 9$, akkor $\chi_e(G) = 9$ is nyilván igaz. Ezért azt kell csak belátni, hogy ha $\chi_e(G-v) = 8$, akkor $\chi_e(G) = 8$. (1 pont)
Tegyük fel, hogy adott $G-v$ egy tetszőleges élszínezése 8 színnel és jelölje $1 \leq i \leq 8$ esetén z_i azt, hogy hány olyan csúcsa van $(G-v)$-nek, amelyre nem illeszkedik i-edik színű él. (1 pont)
Mivel a 8 fokú csúcsokra illeszkedő élek között minden szín előfordul és a 7 fokú csúcsok esetén csak egy-egy hiányzó szín van, ezért $\sum_{i=1}^{8} z_i = 8$. (1 pont)
Másrészt $z_i \geq 1$ minden i-re igaz, hiszen $z_i = 0$ esetén minden csúcsra illeszkedne i-edik színű él; ez lehetetlen, mert $(G-v)$-nek páratlan sok csúcsa van, így az i-edik színű élek nem alkothatnak benne teljes párosítást. (2 pont)
Ezekből következik, hogy $z_i = 1$ teljesül minden i-re, vagyis a 8 darab 7 fokú csúcs mindegyikénél különbözik az egyetlen hiányzó szín. (2 pont)
Így minden v-re illeszkedő élet az él másik végpontjánál hiányzó színnel színezve valóban a G jó élszínezését kapjuk 8 színnel. (1 pont)
(A megoldás lényeges gondolatát helyettesíthetjük a következővel: a 19 csúcsú $G-v$ élszínezésében minden színt legföljebb 9-szer használhatunk; így 8 színt használva legföljebb 72 élt színezhetünk meg. Mivel $(G-v)$-nek éppen 72 éle van, ezért 8 színnel élszínezni csak úgy lehet, ha minden színt pontosan 9-szer használunk, vagyis minden szín csak egyetlen csúcsnál hiányzik.)

4. A G gráf csúcshalmaza legyen $V(G) = \{1, 2, \ldots, 60\}$. Az $x, y \in V(G)$ csúcsok akkor legyenek szomszédosak G-ben, ha $x \neq y$ és $x \cdot y$ osztható 6-tal. Határozzuk meg $\nu(G)$, vagyis a G-beli független élek maximális számának értékét!

* * * * *

G-ben lefogó ponthalmazt alkotnak a 3-mal osztható számok (hiszen két, 3-mal nem oszhtató szám szorzata nemhogy 6-tal, de még 3-mal sem osztható). (2 pont)
Ezért $\tau(G) \leq 20$ (ahol τ a lefogó pontok minimális számát jelöli). (1 pont)
Így $\nu(G) \leq 20$ is igaz a tanult egyszerű összefüggés szerint. (2 pont)
Vegyünk 10 olyan számot, amelyek sem 2-vel, sem 3-mal nem oszhatók (ezekből 20 darab is van) és állítsuk őket párba (tetszőlegesen) a 10 darab 6-tal osztható számmal. Minden ilyen pár éle a gráfnak (hiszen ha az egyik tényező 6-tal osztható, akkor nyilván a szorzat is). (2 pont)
Most vegyük a 10 darab 3-mal osztható, de páratlan számot és állítsuk őket (tetszőlegesen) párba 10 darab páros, de 3-mal nem osztható számmal (ezekből is 20 darab van). Ezek a párok is élei a gráfnak (hiszen a tényezők közül az egyik 3-mal, a másik 2-vel oszható, így a szorzat 6-tal osztható). (2 pont)
Ezzel megadtunk 20 független élet G-ben, amiből $\nu(G) \geq 20$ következik. Így tehát $\nu(G) = 20$.(1 pont)

5. Bontsuk emeletekre a PERT diagram irányított gráfját, majd határozzuk meg a feladat elvégzéséhez szükséges minimális időt és a kritikus részfeladatokat!

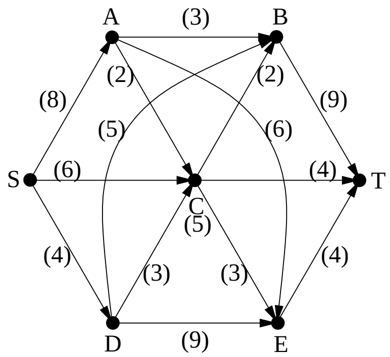


* * * * *

A tanult (a nyelők ismételt levágásából álló) eljárást alkalmazva a következő emeletekre bontást kapjuk:
$$E \;\begin{array}{|c|c|c|c|c}G & H & & & \\ & D & I & B & C \\ F & A & & & \end{array}\ .$$
(4 pont)

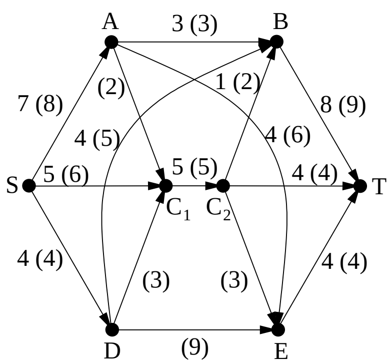
A kezdési idők: $E \to 0$, $G \to 4$, $F \to 5$, $H \to 7$, $D \to 7$, $A \to 7$, $I \to 9$, $B \to 11$, $C \to 14$. (4 pont)
A kritikus részfeladatok az $E \to G \to A \to B \to C$ úton vannak. (2 pont)

6. Az alábbi hálózatban az éleken kívül a C csúcsnak is van kapacitása. Adjunk meg egy maximális folyamot S-ből T-be (és bizonyítsuk be róla, hogy maximális)!



* * * * *

A C csúcsot az ábrán látható módon „széthúzzuk” a $\overrightarrow{C_1C_2}$ éllé, hogy a feladatot visszavezessük az eredeti folyamfeladatra. (2 pont)
A kapott hálózatban van 16 értékű folyam (lásd az ábrát). (3 pont)
Található 16 értékű vágás is: ha az S-sel egy oldalra az A, C_1 és E csúcsokat tesszük, akkor a kapott vágásban az S-et tartalmazó oldalról a T-t tartalmazó oldalra az $\overrightarrow{SD}$, $\overrightarrow{AB}$, $\overrightarrow{C_1C_2}$ és $\overrightarrow{ET}$ élek mennek; ezek összkapacitása pedig éppen 16. (4 pont)
A 16 értékű vágás bizonyítja, hogy 16-nál nagyobb folyam nem lehet, így a megadott 16 értékű folyam maximális. (1 pont)
(Jó megoldás az is, ha a 16 értékű folyamhoz készített segédgráfot lerajzoljuk és megmutatjuk, hogy ebben már nincs javítóút.)



Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató
2009. április 24.

Általános alapelvek.

A pontozási útmutató célja, hogy a javítók a dolgozatokat egységesen értékeljék. Ezért az útmutató minden feladat (legalább egy lehetséges) megoldásának főbb gondolatait és az ezekhez rendelt részpontszámokat közli. Az útmutatónak *nem célja* a feladatok teljes értékű megoldásának részletes leírása; a leírt lépések egy maximális pontszámot érő megoldás vázlatának tekinthetők.

Az útmutatóban feltüntetett részpontszámok csak akkor járnak a megoldónak, ha a kapcsolódó gondolat egy áttekinthető, világosan leírt és megindokolt megoldás egy lépéseként szerepel a dolgozatban. Így például az anyagban szereplő ismeretek, definíciók, tételek puszta leírása azok alkalmazása nélkül nem ér pontot (még akkor sem, ha egyébként valamelyik leírt tény a megoldásban valóban szerephez jut). Annak mérlegelése, hogy az útmutatóban feltüntetett pontszám a fentiek figyelembevételével a megoldónak (részben vagy egészében) jár-e, teljes mértékben a javító hatásköre.

Részpontszám jár minden olyan ötletért, részmegoldásért, amelyből a dolgozatban leírt gondolatmenet alkalmas kiegészítésével a feladat hibátlan megoldása volna kapható. Az útmutatóban szereplő részpontszámok szükség esetén tovább is oszthatók. Az útmutatóban leírttól eltérő jó megoldás természetesen maximális pontot ér.

Minden feladat 10 pontot ér. Az elégséges határa 24 pont. A vizsgajegybe a dolgozat pontszáma számít bele, így a dolgozatokra osztályzatot nem adunk.

1. Hány olyan 600-nál nem nagyobb, pozitív egész a szám van, amelyre az $a \cdot x \equiv 1 \pmod{600}$ lineáris kongruencia megoldható?

* * * * *

A tanult tétel szerint a lineáris kongruencia akkor és csak akkor oldható meg, ha $(a, 600)|1$, (2 pont)
vagyis ha $(a, 600) = 1$. (1 pont)
Így tehát a 600-nál nem nagyobb, 600-hoz relatív prím pozitív egészek számát, vagyis definíció szerint $\varphi(600)$ értékét keressük. (3 pont)
Mivel $600 = 2^3 \cdot 3 \cdot 5^2$, (1 pont)
a tanult képlet szerint $\varphi(600) = (2^3 - 2^2)(3-1)(5^2 - 5) = 160$. Így tehát 160 db ilyen a létezik. (3 pont)

2. Egy mértani sorozat első tagja 41, kvóciense 7. (A sorozat tagjai tehát: 41, 287, 2009, ...). Képzeletben szorozzuk össze a sorozat első 800 tagját. Mi a kapott szám utolsó 3 számjegye?

* * * * *

A sorozat i-edik tagja: $a_i = 41 \cdot 7^{i-1}$. (1 pont)
Így $P = a_1 \cdot a_2 \cdot \ldots \cdot a_{800} = 41^{800} \cdot 7^{1+2+\ldots+799} = 41^{800} \cdot 7^{\frac{800\cdot 799}{2}} = 41^{800} \cdot 7^{400\cdot 799}$. (1 pont)
Mivel $(41, 1000) = 1$ és $(7, 1000) = 1$ (2 pont)
és $\varphi(1000) = \varphi(2^3 \cdot 5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 \cdot 100 = 400$, (1 pont)
ezért az Euler-Fermat tétel értelmében $41^{400} \equiv 1 \pmod{1000}$ és $7^{400} \equiv 1 \pmod{1000}$. (2 pont)
Ebből $P = (41^{400})^2 \cdot (7^{400})^{799} \equiv 1^2 \cdot 1^{799} = 1 \pmod{1000}$. (2 pont)
Így tehát P utolsó három számjegye 001. (1 pont)

3. Bizonyítsuk be, hogy ha a egy 11-gyel nem osztható egész szám, akkor az $x^3 \equiv a \pmod{121}$ kongruencia megoldható (vagyis létezik olyan x egész, amelyre a kongruencia fennáll).

* * * * *

Mivel $121 = 11^2$, ezért ha a 11-gyel nem oszhtató, akkor a-nak és 121-nek nincs közös prímtényezője, így $(a, 121) = 1$. (2 pont)
$\varphi(121) = \varphi(11^2) = 11^2 - 11 = 110$, (1 pont)
így az Euler-Fermat tétel miatt $a^{110} \equiv 1 \pmod{121}$. (1 pont)
Mindkét oldalt a-val szorozva: $a^{111} \equiv a \pmod{121}$. (2 pont)
Mivel $111 = 3 \cdot 37$, ez így is írható: $(a^{37})^3 \equiv a \pmod{121}$. (2 pont)
Ez éppen azt jelenti, hogy $x = a^{37}$ valóban megoldása a feladatbeli kongruenciának. (2 pont)

4. Értelmezzük a valós számok $\mathbb{R}$ halmazán a $*$ műveletet a következőképpen:

$$a * b = \sqrt[3]{a^3 + b^3 - 8}$$

Döntsük el, hogy $\mathbb{R}$ csoportot alkot-e $*$-ra nézve.

* * * * *

Ha $a, b, c \in \mathbb{R}$, akkor $(a * b) * c = \sqrt[3]{a^3 + b^3 - 8} * c = \sqrt[3]{a^3 + b^3 - 8 + c^3 - 8} = \sqrt[3]{a^3 + b^3 + c^3 - 16}$ és hasonlóan $a * (b * c) = \sqrt[3]{a^3 + b^3 + c^3 - 16}$ is igaz. Így a $*$ művelet asszociatív $\mathbb{R}$-en. (3 pont)
Egységelem a 2, mert $a * 2 = 2 * a = \sqrt[3]{a^3 + 8 - 8} = a$ teljesül minden $a \in \mathbb{R}$ esetén. (3 pont)
a-nak akkor lesz inverze x, ha $a * x = x * a = 2$, azaz ha $\sqrt[3]{a^3 + x^3 - 8} = 2$. Ebből $x = a^{-1} = \sqrt[3]{16 - a^3}$, vagyis minden elemnek van inverze. (3 pont)
A fentiek miatt $\mathbb{R}$ csoportot alkot $*$-ra nézve. (1 pont)
Az utolsó 1 pont annak jár, aki a korábbi számolásaiból helyes következtetést von le (akkor is, ha egy hibás számolásból arra következtet, hogy nem csoport).

5. Az alábbiakban a $\{p, q, r, s, t, u\}$ alaphalmazon értelmezett G csoport műveleti táblája látható:

$*$	p	q	r	s	t	u
p	u	t	q	p	r	s
q	t	u	p	q	s	r
r	q	p	s	r	u	t
s	p	q	r	s	t	u
t	r	s	u	t	p	q
u	s	r	t	u	q	p

(A műveleti tábla használata értelemszerű: $a * b$ értékét az a-nak megfelelő sor és a b-nek megfelelő oszlop kereszteződésében találjuk; így például $p * q = t$ és $t * u = q$.)
a) Mennyi az u elem rendje?
b) Ciklikus csoport-e G?
(A megoldáshoz feltételezhetjük, hogy G valóban csoport, ezt bizonyítani nem kell.)

* * * * *

G egységeleme s, mert $a * s = s * a = a$ minden a elemre fennáll. (2 pont)
a) Az u elem hatványai: $u^1 = u$, $u^2 = u * u = p$, $u^3 = p * u = s$. (1 pont)
Mivel u^3 az egységelem és ez u alacsonyabb hatványira nem áll fenn, ezért u rendje 3. (2 pont)
b) A kérdés az, hogy van-e a csoportban 6 rendű elem. (2 pont)
Például a t elem hatványai: $t^1 = t$, $t^2 = p$, $t^3 = r$, $t^4 = u$, $t^5 = q$, $t^6 = s$. Ebből látszik, hogy $o(t) = 6$, így a csoport ciklikus. (3 pont)
(A t elemen kívül még a q-ra teljesül, hogy a rendje 6.)

6. Legyen G véges Abel-csoport és legyen $g, h \in G$ két tetszőleges elem. Mutassuk meg, hogy ha $(o(g), o(h)) = 1$, akkor $o(g * h) = o(g) \cdot o(h)$. (A G-beli műveletet $*$-gal jelöltük. A gömbölyű zárójel a legnagyobb közös osztót, o pedig az elem rendjét jelöli.)

* * * * *

Mivel G Abel-csoport, ezért minden pozitív egész m-re igaz benne a $(g * h)^m = g^m * h^m$ azonosság (hiszen mindegy, hogy m darab g-t és m darab h-t milyen sorrendben szorzunk össze). (1 pont)
Vezessük be az $o(g) = k$ és $o(h) = l$ jelöléseket, G egységelemét jelölje e.
Ekkor $(g * h)^{kl} = g^{kl} * h^{kl} = (g^k)^l * (h^l)^k = e^l * e^k = e$. (2 pont)
Legyen most m olyan kitevő, amelyre $(g * h)^m = e$. Azt kell megmutatni, hogy $m \geq k \cdot l$, hiszen ekkor definíció szerint valóban $k \cdot l = o(g) \cdot o(h)$ a $g * h$ rendje. (1 pont)
Az $e = (g*h)^m$ egyenletet k-adikra emelve: $e = e^k = (g*h)^{mk} = (g^k)^m * h^{mk} = e^m * h^{mk} = h^{mk}$. (1 pont)
Mivel $o(h) = l$, ezért $h^n = e$ akkor és csak akkor teljesül, ha $l|n$ (hiszen h hatványainak sorozata az $(l + 1)$-edik hatványtól kezdve periodikus). (1 pont)
A fentiekből adódik, hogy $l|mk$. (1 pont)
Mivel $(k, l) = 1$, ezért ebből $l|m$ is következik. (1 pont)
A fentiekhez hasonlóan (az $e = (g*h)^m$ egyenletet l-edikre emeléséből) adódik az is, hogy $k|m$. (1 pont)
Mivel $(k, l) = 1$, $l|m$ és $k|m$, ezért $kl|m$ is igaz, amiből valóban következik, hogy $m \geq k \cdot l$. (1 pont)

Bevezetés a számításelméletbe II.

Zárthelyi feladatok — az ELSŐ zárthelyi pótlására

Pontozási útmutató

2009. május 4.

Általános alapelvek.

A pontozási útmutató célja, hogy a javítók a dolgozatokat egységesen értékeljék. Ezért az útmutató minden feladat (legalább egy lehetséges) megoldásának főbb gondolatait és az ezekhez rendelt részpontszámokat közli. Az útmutatónak *nem célja* a feladatok teljes értékű megoldásának részletes leírása; a leírt lépések egy maximális pontszámot érő megoldás vázlatának tekinthetők.

Az útmutatóban feltüntetett részpontszámok csak akkor járnak a megoldónak, ha a kapcsolódó gondolat egy áttekinthető, világosan leírt és megindokolt megoldás egy lépéseként szerepel a dolgozatban. Így például az anyagban szereplő ismeretek, definíciók, tételek puszta leírása azok alkalmazása nélkül nem ér pontot (még akkor sem, ha egyébként valamelyik leírt tény a megoldásban valóban szerephez jut). Annak mérlegelése, hogy az útmutatóban feltüntetett pontszám a fentiek figyelembevételével a megoldónak (részben vagy egészében) jár-e, teljes mértékben a javító hatásköre.

Részpontszám jár minden olyan ötletekért, részmegoldásért, amelyből a dolgozatban leírt gondolatmenet alkalmas kiegészítésével a feladat hibátlan megoldása volna kapható. Az útmutatóban szereplő részpontszámok szükség esetén tovább is oszthatók. Az útmutatóban leírttól eltérő jó megoldás természetesen maximális pontot ér.

Minden feladat 10 pontot ér. Az elégséges határa 24 pont. A vizsgajegybe a dolgozat pontszáma számít bele, így a dolgozatokra osztályzatot nem adunk.

1. A G gráf csúcshalmaza legyen $V(G) = \{1, 2, \dots, 20\}$. Az x és az y különböző csúcsok akkor legyenek szomszédosak G-ben, ha $x + y$ vagy $x \cdot y$ osztható 7-tel.

a) Van-e G-ben Hamilton-út?

b) Van-e G-ben Hamilton-kör?

* * * * *

G-ben az „$x \cdot y$ osztható 7-tel” feltétel miatt a 7 és a 14 az összes többi csúccsal szomszédos; további éleket ez a feltétel nem hoz létre. Az „$x + y$ osztható 7-tel” feltétel miatt ezen kívül szomszédos még az 1, 8, 15 csúcsok mindegyike a 6, 13, 20 csúcsok bármelyikével; a 2, 9, 16 csúcsok mindegyike az 5, 12, 19 csúcsok bármelyikével; végül a 3, 10, 17 csúcsok mindegyike a 4, 11, 18 csúcsok bármelyikével. (2 pont)

Ebből látható, hogy a 7 és a 14 csúcsok törlése után a gráf három komponensre esik szét: ezek épp az „$x + y$ osztható 7-tel” feltétel miatt létrejövő, fentebb leírt $K_{3,3}$ gráfok. (2 pont)

Így a tanult feltétel miatt G-ben nincs Hamilton-kör. (3 pont)

Hamilton-út viszont könnyen található: a három $K_{3,3}$ gráfban vehetünk három Hamilton-utat, ezeket pedig összekapcsolhatjuk a 7 és a 14 pontokon keresztül. (Így például egy lehetséges Hamilton-út: 1, 6, 8, 13, 15, 20, 7, 2, 5, 9, 12, 16, 19, 14, 3, 4, 10, 11, 17, 18.) (3 pont)

2. A G gráf csúcsai legyenek a sakktábla mezői; két különböző csúcs akkor legyen szomszédos G-ben, ha egy huszár az egyik megfelelő mezőről indulva pontosan három lépéssel el tudja érni a másikat. Döntsük el, hogy G páros gráf-e! (A sakkban a huszár egy lépése abból áll, hogy először két mezőt halad függőlegesen vagy vízszintesen, utána még egy mezőt halad az előző mozgásirányára merőlegesen.)

* * * * *

Ha a huszár egyet lép, akkor mindig (a sakktábla szokásos színezése szerint) ellentétes színű mezőre lép. (2 pont)

Ebből következik, hogy három lépés megtételével háromszor vált színt, vagyis végül ellentétes színű mezőre érkezik. (3 pont)

Ezért a sakktábla szokásos színezése a G gráfnak is jó színezése. (2 pont)

Mivel pedig G 2 színnel színezhető, ezért páros gráf. (3 pont)

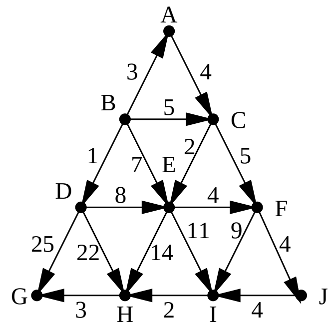
3. Legyen $k \geq 3$ és jelölje G_k azt a Mycielski-konstrukció által készített gráfot, amelyre $\chi(G_k) = k$ és legyen G_k csúcsainak száma n. Mutassuk meg, hogy $\chi(\overline{G_k}) \geq \frac{n+1}{2}$ (ahol $\overline{G_k}$ a G_k gráf komplementerét jelöli).

$* \quad * \quad * \quad * \quad *$

A Mycielski-konstrukció működéséből következik, hogy ha a G_{k-1} gráf t csúcsú, akkor G_k csúcsainak száma $2t+1$. (2 pont)
Mivel G_3 is páratlan (5) csúcsú, ezért tehát feltehetjük, hogy $n = 2t+1$ páratlan szám. (1 pont)
A tanult tétel szerint G_k-ban nincs háromszög, amiből következik, hogy $\overline{G_k}$-ban nincs három elemű független ponthalmaz. (2 pont)
Ezért $\overline{G_k}$ tetszőleges színezésében minden szín csak kétszer használható (hiszen három azonos színű csúcs már egy három elemű független ponthalmazt jelentene). (3 pont)
Így tehát $\overline{G_k}$ kiszínezéséhez valóban legalább $t+1$ szín szükséges (hiszen t színnel csak $2t$ csúcs volna kiszínezhető). Mivel $t+1 = \frac{n+1}{2}$, az állítást beláttuk. (2 pont)

Aki észrevesz annyit, hogy G_k-ban van $\frac{n-1}{2}$ csúcsú független ponthalmaz, így a komplementerében van ugyanekkora klikk és ebből kihozza, hogy $\chi(\overline{G_k}) \geq \frac{n-1}{2}$, az erre a megfigyelésére 2 pontot kaphat (függetlenül attól, hogy ez a gondolat nem visz közelebb a feladat megoldásához).

4. Bontsuk emeletekre a PERT diagram irányított gráfját, majd határozzuk meg a feladat elvégzéséhez szükséges minimális időt és a kritikus részfeladatokat!



$* \quad * \quad * \quad * \quad *$

A tanult (a nyelők ismételt levágásából álló) eljárást alkalmazva a következő emeletekre bontást kapjuk:

$$\begin{array}{c|c|c|c|c|c|c|c|c} B & A & \begin{matrix} D \\ \\ C \end{matrix} & E & F & J & I & H & G \end{array}.$$ (4 pont)

A kezdési idők: $B \to 0$, $A \to 3$, $D \to 1$, $C \to 7$, $E \to 9$, $F \to 13$, $J \to 17$, $I \to 22$, $H \to 24$ $G \to 27$. (4 pont)
A kritikus részfeladatok a $B \to D \to E \to F \to I \to H \to G$ és a $B \to A \to C \to E \to F \to I \to H \to G$ utakon vannak. (2 pont)

5. Határozzuk meg annak a gráfnak az élkromatikus számát, amelyet egy öt élű körből nyerünk úgy, hogy minden élét helyettesítjük három párhuzamos éllel!

$* \quad * \quad * \quad * \quad *$

Tetszőleges élszínezésben minden szín legföljebb 2-szer használható (hiszen három azonos színű él legalább 6 csúcsot jelentene). (3 pont)
Mivel a gráfnak 15 éle van, ezért legalább 8 szín szükséges a színezéshez (mert 7 színnel csak 14 él volna kiszínezhető). (3 pont)
8 színnel viszont könnyen kiszínezhetjük a gráf éleit - ennek igazolásához meg kell adni egy konkrét élszínezést. (3 pont)
Így az élkromatikus szám 8. (1 pont)
(*Megjegyzés.* Mivel a feladatbeli gráf nem egyszerű, ezért rá a Vizing-tétel nem alkalmazható. Így nem meglepő, hogy bár a maximális fokszám csak 6, az élkromatikus szám mégis 8.)

6. Legyen $k \geq 1$ egész és legyen G egy legalább $2k+1$ pontú, k-szorosan összefüggő gráf. Értelmezzük a H gráfot a következőképpen: legyen $V(H) = V(G)$ és két különböző csúcs akkor legyen szomszédos H-ban ha G-ben szomszédosak vagy van közös szomszédjuk. Bizonyítsuk be, hogy a H gráf $2k$-szorosan összefüggő.

* * * * *

Tegyük fel, hogy a H gráfból az X csúcshalmazt elhagyva a maradék gráf már nem összefüggő. Ekkor a $V(H) \setminus X$ csúcshalmaz az A és B halmazokra osztható úgy, hogy köztük nem fut H-beli él.(2 pont)
Legyen $v \in X$ tetszőleges csúcs. Ha v-nek a G gráfban volna egy A-beli a és egy B-beli b szomszédja, akkor H értelmezése miatt a és b szomszédos volna H-ban (mert közös szomszédjuk v), ami nem lehet. Ezért minden X-beli csúcs vagy csak A-beliekkel, vagy csak B-beliekkel szomszédos G-ben. (2 pont)
Legyen X_A, illetve X_B azon X-beli csúcsok halmaza, amik szomszédosak A-beli, illetve B-beli csúccsal G-ben. A fentiek szerint $X_A \cap X_B = \emptyset$. (1 pont)
X_A csúcsait törölve nyilván megszűnik G összefüggősége, hiszen a maradék gráfban A-beli csúcsnak nem lehet már szomszédja sem X-ben, sem B-ben (hiszen ez az él H-ba is bekerülne). Ezért G k-szoros összefüggősége miatt $|X_A| \geq k$. Teljesen hasonlóan $|X_B| \geq k$ is következik. (3 pont)
Mivel X_A és X_B az X halmaz diszjunkt, egyenként legalább k elemű részhalmazai, ezért $|X| \geq 2k$ fennáll. Így H összefüggőségének megszüntetéséhez legalább $2k$ csúcsot kell elhagyni, ami (legalább $2k+1$ csúcsú gráfról lévén szó) valóban azt jelenti, hogy H $2k$-szorosan összefüggő. (2 pont)

Bevezetés a számításelméletbe II.

Zárthelyi feladatok — az MÁSODIK zárthelyi pótlására

Pontozási útmutató

2009. május 4.

Általános alapelvek.

A pontozási útmutató célja, hogy a javítók a dolgozatokat egységesen értékeljék. Ezért az útmutató minden feladat (legalább egy lehetséges) megoldásának főbb gondolatait és az ezekhez rendelt részpontszámokat közli. Az útmutatónak *nem célja* a feladatok teljes értékű megoldásának részletes leírása; a leírt lépések egy maximális pontszámot érő megoldás vázlatának tekinthetők.

Az útmutatóban feltüntetett részpontszámok csak akkor járnak a megoldónak, ha a kapcsolódó gondolat egy áttekinthető, világosan leírt és megindokolt megoldás egy lépéseként szerepel a dolgozatban. Így például az anyagban szereplő ismeretek, definíciók, tételek puszta leírása azok alkalmazása nélkül nem ér pontot (még akkor sem, ha egyébként valamelyik leírt tény a megoldásban valóban szerephez jut). Annak mérlegelése, hogy az útmutatóban feltüntetett pontszám a fentiek figyelembevételével a megoldónak (részben vagy egészében) jár-e, teljes mértékben a javító hatásköre.

Részpontszám jár minden olyan ötletekért, részmegoldásért, amelyből a dolgozatban leírt gondolatmenet alkalmas kiegészítésével a feladat hibátlan megoldása volna kapható. Az útmutatóban szereplő részpontszámok szükség esetén tovább is oszthatók. Az útmutatóban leírttól eltérő jó megoldás természetesen maximális pontot ér.

Minden feladat 10 pontot ér. Az elégséges határa 24 pont. A vizsgajegybe a dolgozat pontszáma számít bele, így a dolgozatokra osztályzatot nem adunk.

1. Hány olyan 540-nél nem nagyobb, pozitív egész a szám van, amelyre az $a \cdot x \equiv 2 \pmod{540}$ lineáris kongruencia megoldható?

* * * * *

A tanult tétel szerint a lineáris kongruencia akkor és csak akkor oldható meg, ha $(a, 540)|2$, vagyis ha $(a, 540) = 1$ vagy $(a, 540) = 2$. (2 pont)
Az első esetben a lehetőségek száma definíció szerint $\varphi(540)$, (1 pont)
vagyis $\varphi(2^2 \cdot 3^3 \cdot 5) = (2^2 - 2)(3^3 - 3^2)(5 - 1) = 144$. (2 pont)
$(a, 540) = 2$ azt jelenti, hogy a és 540 prímtényezős felbontásában a 2 az egyetlen közös prím és az is első hatványon szerepel. Ez pedig pontosan akkor teljesül, ha mindkét számot (a-t és 540-et) kettővel osztva relatív prím számokat kapunk. Vagyis $a = 2b$ akkor és csak akkor felel meg a feltételeknek, ha $1 \le b \le 270$ és $(b, 270) = 1$. (1 pont)
Ezért az $(a, 540) = 2$-t teljesítő a-k száma megegyezik a 270-nél nem nagyobb, 270-hez relatív prím b-k számával, (2 pont)
ami definíció szerint $\varphi(270)$, vagyis $\varphi(2 \cdot 3^3 \cdot 5) = (2 - 1)(3^3 - 3^2)(5 - 1) = 72$. (1 pont)
Így a lehetőségek száma összesen $144 + 72 = 216$. (1 pont)

2. Valamely n egészre teljesül, hogy $24n + 24$ és $n + 25$ ugyanazt a maradékot adják 188-cal osztva. Mi lehet ez a közös maradék?

* * * * *

A feladat a $24n + 24 \equiv n + 25 \pmod{188}$ lineáris kongruencia. (1 pont)
Átrendezve: $23n \equiv 1 \pmod{188}$. (1 pont)
9-cel szorozva: $207n \equiv 9 \pmod{188}$, vagyis $19n \equiv 9 \pmod{188}$. (1 pont)
10-zel szorozva: $190n \equiv 90 \pmod{188}$, azaz $2n \equiv 90 \pmod{188}$. (1 pont)
2-vel osztva: $n \equiv 45 \pmod{94}$, vagyis $n \equiv 45, 139 \pmod{188}$. (1 pont)
Ebből ellenőrzéssel kiderül, hogy 45 hamis gyök (ami a 10-zel szorzásnál jött be), így a megoldás $n \equiv 139 \pmod{188}$. (3 pont)
Ebből $n + 25 \equiv 164 \pmod{188}$, vagyis a keresett közös maradék 164. (2 pont)
A lineáris kongruencia nagyon sokféleképp megoldható jól (például a fentinél rövidebb, hamis gyököt nem behozó megoldást kapunk, ha az első lépésben 7-tel szorzunk). A lineáris kongruencia minden jó megoldása 6 pontot ér (a hibásak arányosan kevesebbet). Aki a fenti megoldást írja, de nem foglalkozik

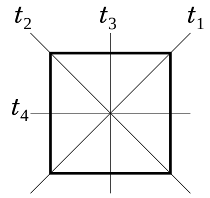
a hamis gyök kiszűrésével, az értelemszerűen a 6 pontból 3-at kapjon. Ha valaki csak azt ellenőrzi, hogy $(23, 188)|1$, így a kongruenciának van megoldása, de a megoldást kiszámolni nem tudja, az (az átrendezéssel együtt összesen) 3 pontot kapjon. Számolási hibákért 1-1 pont vonandó le, de a maradék pontszám csak akkor jár, ha a hiba miatt a feladat nem lett lényegesen könnyebb.

3. Az (a_n) sorozatot értelmezzük a következő rekurziós képlettel: $a_1 = 25$ és $a_{n+1} = 4a_n - 3$ minden $n \geq 1$ egész esetén. (A sorozat tagjai tehát: 25, 97, 385, ...) Milyen maradékot ad a sorozat első 25 tagjának szorzata 72-vel osztva?

* * * * *

Minden n-re $a_n \equiv 25 \pmod{72}$ teljesül. Ugyanis ez $n = 1$-re igaz, ha pedig valamely n-re már fennáll, akkor $a_{n+1} = 4a_n - 3 \equiv 4 \cdot 25 - 3 = 97 \equiv 25 \pmod{72}$ is igaz. (2 pont)
Ezért $a_1 \cdot a_2 \cdot \ldots \cdot a_{25} \equiv 25^{25} \pmod{72}$. (1 pont)
Mivel $(25, 72) = 1$ (1 pont)
és $\varphi(72) = \varphi(2^3 \cdot 3^2) = (2^3 - 2^2)(3^2 - 3) = 24$, (1 pont)
ezért az Euler-Fermat tétel miatt $25^{24} \equiv 1 \pmod{72}$. (2 pont)
Mindkét oldalt 25-tel szorozva: $25^{25} \equiv 25 \pmod{72}$. (1 pont)
Így tehát az első 25 tag szorzata 25 maradékot ad 72-vel osztva. (2 pont)

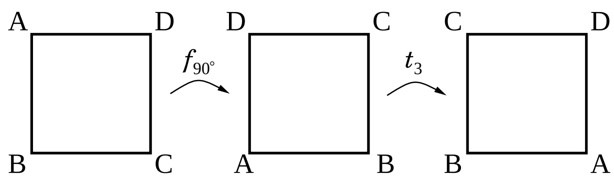
4. Egy négyzetet önmagába vivő tengelyes tükrözéseket jelölje t_1, t_2, t_3 és t_4 az ábra szerint. Jelölje továbbá a négyzet középpontja körüli α szögű (pozitív, vagyis az óramutató járásával ellentétes forgásirány szerinti) elforgatást f_α. Adjuk meg az alábbi műveletek eredményét a D_4 diédercsoportban!



a) $t_3 \cdot f_{90^\circ}$ b) $(t_1 \cdot t_2)^{-1}$

* * * * *

a) A négyzet csúcsainak megjelölésével nyomon követhető, hogy először f_{90°-et, majd t_3-at elvégezve a csúcsok képei hol lesznek (lásd az ábrát). Látható, hogy a t_1-et alkalmazva a csúcsok képei megegyeznek a $(t_3 \cdot f_{90^\circ})$-kal vett képeikkel, így $t_3 \cdot f_{90^\circ} = t_1$. (5 pont)



b) A fentihez hasonlóan megmutatható, hogy $t_1 \cdot t_2 = f_{180^\circ}$. (2 pont)
Mivel pedig $f_{180^\circ} \cdot f_{180^\circ} = I$, ezért $(f_{180^\circ})^{-1} = f_{180^\circ}$. Így $(t_1 \cdot t_2)^{-1} = f_{180^\circ}$. (3 pont)

Aki az a) feladatban a műveletet fordított sorrendben (de jól) végzi (és így t_2-t kap), az 2 pontot veszítsen (és ugyanezért a hibáért a b) feladatban már ne járjon pontlevonás). Aki jó sorrendben végzi a műveletet, de a 90°-os forgatással együtt t_3-at is elforgatja (és így valójában $t_4 \cdot f_{90^\circ}$-ot végzi el), az 3 pontot veszítsen.

5. Legyen adott a valós számok $\mathbb{R}$ halmazán a $*$ művelet. Tegyük fel, hogy $(\mathbb{R}, *)$ csoport, amely izomorf a nullától különböző valós számok szorzással vett csoportjával. Tudjuk továbbá, hogy fennállnak a következő egyenlőségek: $3 * 3 = 7$, $5 * 5 = 7$, $7 * 7 = \sqrt{2}$ és $9 * 9 = \sqrt{2}$. Határozzuk meg $3 * 5$ értékét!

* * * * *

Legyen $f : \mathbb{R} \to \mathbb{R} \setminus \{0\}$ izomorfizmus az $(\mathbb{R}, *)$ és az $(\mathbb{R} \setminus \{0\}, \cdot)$ csoportok között. Legyen $f(3) = a$, $f(5) = b$, $f(7) = c$, $f(9) = d$ és $f(\sqrt{2}) = e$. (2 pont)
Ekkor tehát a feladatban megadott egyenlőségek (és az izomorfia definíciója miatt) $a^2 = c$, $b^2 = c$, $c^2 = e$ és $d^2 = e$. (2 pont)
Az első két egyenletből $b = -a$ (hiszen $3 \neq 5$ miatt $a \neq b$). Innen $ab = -a^2 = -c$. Másrészt a második két egyenletből $c^2 = d^2$, így $-c = d$ (hiszen $c = d$ ismét lehetetlen). Ezekből tehát $ab = d$. (3 pont)
Így az izomorfia definíciója miatt $3 * 5 = 9$. (3 pont)

6. Tegyük fel, hogy a 77 elemű G csoport az egységelemtől különböző a és b elemeire teljesül, hogy van olyan $k \geq 1$ egész, amelyre $a^k = b$, de nincs olyan $l \geq 1$ egész, amelyre $b^l = a$. Bizonyítsuk be, hogy G ciklikus csoport!

* * * * *

Tegyük fel indirekt, hogy G nem ciklikus csoport, vagyis nincs 77 rendű eleme. (1 pont)
Legyen $o(a) = n$. Ekkor Lagrange tétele miatt $n|77$. Mivel $n = 77$ és $n = 1$ kizárt (utóbbi azért, mert $a \neq e$), ezért $n = 7$ vagy $n = 11$. (1 pont)
Az $a^n = e$ egyenletet r-edikre emelve ($r \geq 1$ tetszőleges), majd a-val szorozva: $a^{rn+1} = a$. (1 pont)
Mivel nincs olyan l, amelyre $b^l = a$, ezért ($b = a^k$-t felhasználva) nincs olyan l, amelyre $a^{kl} = a$. (1 pont)
A fentieket összevetve: $kl = rn+1$ nem állhat elő semmilyen l és r értékekre, vagyis a $k \cdot l \equiv 1 \pmod n$ lineáris kongruencia nem megoldható. (2 pont)
Felhasználva a lineáris kongruenciák megoldhatóságára vonatkozó tételt $(k, n) > 1$ következik. (1 pont)
Mivel n prím (7 vagy 11), ezért ebből $n|k$, vagyis $k = n \cdot d$. (1 pont)
Ez azonban ellentmondás: az $a^n = e$ egyenletet d-edikre emelve $b = a^k = a^{nd} = e$ következik, márpedig $b \neq e$ a feladat szövege szerint. (2 pont)

Második megoldás. Vezessük be az $o(a) = n$ és $o(b) = m$ jelöléseket.
Tegyük fel indirekt, hogy G nem ciklikus csoport. Ekkor $n \in \{7, 11\}$ és $m \in \{7, 11\}$ (ugyanúgy, mint az előbb). (2 pont)
Előadásról ismert, hogy $H = \{e, a, a^2, \ldots, a^{n-1}\}$ és $K = \{e, b, \ldots, b^{m-1}\}$ részcsoportok G-ben. (2 pont)
Mivel a feladat szövege szerint $b \in H$, ezért $K \subseteq H$ (hiszen H zárt a műveletre). (2 pont)
Ekkor Lagrange tétele szerint $|K|$ osztója $|H|$-nak (mivel K részcsoport H-ban). (1 pont)
Mivel $|K| = n$ és $|H| = m$ (és $n, m \in \{7, 11\}$), ez csak úgy fordulhat elő, ha $n = m$. (1 pont)
Ekkor azonban $H = K$, vagyis b hatványai között a is szerepel, ellentmondásban a feladat szövegével. (2 pont)