Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató
2012. április 19.

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. Egy öt csúcsú egyszerű gráf szomszédossági mátrixának harmadik hatványában a főátló elemeinek szorzata 64. Mutassuk meg, hogy a gráf kétszeresen élösszefüggő.

* * * * *

A definíció szerint egy gráf szomszédossági mátrixának harmadik hatványában a főátló i. eleme az i. csúcson átmenő három hosszú zárt élsorozatok számával egyenlő. (1 pont)
Mivel a gráf (nevezzük G-nek) egyszerű (valójában elég a hurokélmentességet használni), a három hosszú zárt élsorozatok épp a három hosszú körök. (2 pont)
A feltétel miatt a főátlóban nem szerepel a 0, ezért minden csúcson átmegy legalább egy három hosszú kör. (2 pont)
Tegyük fel indirekten, hogy G nem kétszeresen élösszefüggő, ekkor lesz olyan éle, amit elhagyva a kapott G' gráf nem lesz összefüggő. (1 pont)
G' legkisebb komponense (nevezzük K-nak) ekkor legfeljebb két pontból állhat, hiszen G'-nek legalább két komponense van és öt csúcsa. (1 pont)
K nem állhat egy csúcsból, mert G-ben minden csúcson megy át kör, azaz minden csúcs foka legalább kettő. (1 pont)
K azonban nem állhat két csúcsból sem, mert a bármelyikükön átmenő három hosszú körnek két éle menne ki K-ból G-ben, ami lehetetlen, ezzel az állítást beláttuk. (2 pont)
Érdemes megjegyezni, hogy a feltételnek megfelelő gráf csakugyan létezik, például ilyen lesz az a gráf, ami két olyan háromszögből áll, melyeknek egy közös csúcsa van. (Sőt, azt sem túl nehéz megmutatni, hogy valójában ez az egyetlen, a feltételeknek megfelelő gráf.)

2. A 15 pontú G gráf egy 4 pontú, egy 5 pontú és egy 6 pontú körből készült úgy, hogy az 5 pontú kör minden csúcsát összekötöttük (egyetlen éllel) a másik két kör minden csúcsával. Legyen s a 4 pontú kör egyik csúcsa, t pedig a 6 pontú kör egyik csúcsa.

a) Maximálisan hány páronként csúcsdiszjunkt út adható meg s és t között G-ben?

b) Maximálisan hány páronként éldiszjunkt út adható meg s és t között G-ben?

* * * * *

a) Jelölje $v_1, v_2, \ldots, v_5$ az 5 pontú kör csúcsait. Ekkor az (s, v_i, t) utak (a szomszédos csúcsok közti éleket beleértve) öt darab, páronként csúcsdiszjunkt utat alkotnak s és t között. (2 pont)
Ennél több ilyen út viszont (Menger irányítatlan gráfokra és s és t közötti csúcsdiszjunkt utakra vonatkozó tétele szerint) nem létezhet, mert a $v_1, v_2, \ldots, v_5$ csúcsok lefogják az s és t közötti összes utat (hiszen ezeket G-ből elhagyva már nincs s-ből t-be út). Vagyis a válasz: 5. (3 pont)

b) Jelölje s két szomszédját a 4 pontú körön s_1 és s_2 és t két szomszédját a 6 pontú körön jelölje t_1 és t_2. Az a) feladatban megadott öt utat kiegészíthetjük két továbbival: (s, s_1, v_1, t_1, t) és (s, s_2, v_1, t_2, t). Az így kapott 7 darab út páronként éldiszjunkt. (3 pont)
Ennél több ilyen út viszont (Menger irányítatlan gráfokra és s és t közötti éldiszjunkt utakra vonatkozó tétele szerint) nem létezhet, mert például az s-re illeszkedő 7 darab él nyilván lefogja az s és t közötti összes utat (hiszen ezek elhagyása után s izolált csúcs lesz, t nem érhető el belőle). Így a válasz: 7. (2 pont)

3. Milyen maradékot adhat egy egész szám 153-mal osztva, ha a 31-szerese 10 maradékot ad 153-mal osztva?

* * * * *

A feladat a $31n \equiv 10 \pmod{153}$ lineáris kongruencia. (1 pont)
5-tel szorozva: $155n \equiv 50 \pmod{153}$, vagyis $2n \equiv 50 \pmod{153}$. (3 pont)
2-vel osztva: $n \equiv 25 \pmod{153}$, (2 pont)
ahol $(2, 153) = 1$ miatt az osztás a kongruencia modulusát nem változtatta meg. (2 pont)
Mivel $(5, 153) = 1$ miatt az először végzett 5-tel való szorzás is ekvivalens lépés, ezért a megoldás $n \equiv 25 \pmod{153}$, vagyis a keresett maradék csak 25 lehet. (2 pont)
Ha valaki csak azt ellenőrzi, hogy $(31, 153) = 1|1$, így a kongruenciának van megoldása, de a megoldást kiszámolni nem tudja, az összesen 2 pontot kapjon. A megtett lépések ekvivalens voltára való hivatkozás helyett ellenőrzéssel is meg lehet győződni a kapott megoldás helyességéről (vagy lehet hivatkozni arra is, hogy $(31, 153) = 1$ miatt egyetlen helyes megoldás létezik $\pmod{153}$, így a kapott megoldás helyes). Számolási hibákért 1-1 pont vonandó le, de a maradék pontszám csak akkor jár, ha a hiba miatt a feladat nem lett lényegesen könnyebb.

4. Hány olyan 2012-nél kisebb pozitív egész szám van, amely 19-cel osztva 10 maradékot ad és 37-tel osztva 15 maradékot ad?

* * * * *

A feladat az $n \equiv 10 \pmod{19}$, $n \equiv 15 \pmod{37}$ kongruenciarendszer 2012-nél kisebb pozitív megoldásai számának meghatározása. (1 pont)
Az első kongruencia szerint $n = 19k + 10$ alakú valamilyen k egészre. (1 pont)
Ezt a második kongruenciába helyettesítve: $19k + 10 \equiv 15 \pmod{37}$. (2 pont)
10-et mindkét oldalból levonva: $19k \equiv 5 \pmod{37}$. (1 pont)
2-vel szorozva: $38k \equiv 10 \pmod{37}$, vagyis $k \equiv 10 \pmod{37}$. (2 pont)
Így $k = 37\ell + 10$ alakú valamely ℓ egészre. Ezt a fentibe helyettesítve:

$$n = 19k + 10 = 19(37\ell + 10) + 10 = 703\ell + 200.$$

A kongruenciarendszer megoldásai tehát az ilyen alakú (vagyis az $n \equiv 200 \pmod{703}$ kongurenciának eleget tevő) n egészek. (2 pont)
Látható, hogy az $\ell = 0, 1, 2$ esetekben kapunk 2012-nél kisebb pozitív megoldásokat (ezek 200, 903 és 1606), így tehát három ilyen szám van. (1 pont)

5. Legyen $p > 2$ olyan prímszám, amelyre $2p+1$ is prím. Bizonyítsuk be, hogy ekkor fennáll az alábbi kongruencia:

$$(p-1)^{(p-2)^{p-1}} \equiv p-1 \pmod{2p+1}$$

* * * * *

Mivel $2p+1$ prím, ezért $(p-1, 2p+1) = 1$, (1 pont)
és $\varphi(2p+1) = 2p$. (1 pont)
Így az Euler-Fermat tételt alkalmazva: $(p-1)^{2p} \equiv 1 \pmod{2p+1}$. (1 pont)
Ezt tetszőleges $k \geq 0$ egészre k-adik hatványra emelve, majd $(p-1)$-gyel szorozva: $(p-1)^{k\cdot 2p+1} \equiv p-1 \pmod{2p+1}$. (2 pont)
Ezért a feladat megoldásához elegendő lesz megmutatni, hogy $(p-2)^{p-1} = k \cdot 2p + 1$ teljesül valamilyen alkalmas k-ra, vagyis hogy $(p-2)^{p-1} \equiv 1 \pmod{2p}$. (2 pont)
Mivel p prím, ezért $2p$ valódi osztói csak 2 és p, ezek pedig $(p-2)$-nek nyilván nem osztói. Így $(p-2, 2p) = 1$. (1 pont)
A φ kiszámítására tanult képletből $\varphi(2p) = (2-1)(p-1) = p-1$ következik, (1 pont)
így az Euler-Fermat tételt $(p-2)$-re és $2p$-re alkalmazva éppen a kívánt $(p-2)^{p-1} \equiv 1 \pmod{2p}$ állítást kapjuk, ezzel a feladat állítását bizonyítva. (1 pont)

6. Legyen $H = \{(a,b,c) : a,b,c \in \mathbb{R}, a \neq 0, b \neq 0\}$, vagyis H a térnek azokból a vektoraiból áll, amelyeknek az első két koordinátája nem 0. Értelmezzük H-n a $*$ műveletet a következőképpen:

$$(a,b,c) * (d,e,f) = (ad, be, af + ce)$$

(Így tehát például $(1,2,3)*(4,5,6) = (4,10,21)$.) Döntsük el, hogy H csoportot alkot-e $*$-ra nézve!

* * * * *

Az asszociativitás ellenőrzéséhez vegyünk három H-beli vektort: (a,b,c), (d,e,f), (g,h,i).
Ekkor

$$\Big((a,b,c) * (d,e,f)\Big) * (g,h,i) = (ad, be, af+ce) * (g,h,i) =$$
$$= (adg, beh, adi + (af+ce)h) = (adg, beh, adi + afh + ceh) \quad \text{(1 pont)}$$

és

$$(a,b,c) * \Big((d,e,f) * (g,h,i)\Big) = (a,b,c) * (dg, eh, di + fh) =$$
$$= (adg, beh, a(di+fh) + ceh) = (adg, beh, adi + afh + ceh), \quad \text{(1 pont)}$$

ami az asszociativitást igazolja. (1 pont)
Van egységelem a $*$-ra nézve, mégpedig az $(1,1,0)$ (amely $1 \neq 0$ miatt H-beli), (1 pont)
ugyanis $(a,b,c) * (1,1,0) = (a\cdot 1, b\cdot 1, a\cdot 0 + c\cdot 1) = (a,b,c)$ (1 pont)
és $(1,1,0) * (a,b,c) = (1\cdot a, 1\cdot b, 1\cdot c + 0\cdot b) = (a,b,c)$. (1 pont)
A tetszőleges (a,b,c) elemnek $(\frac{1}{a}, \frac{1}{b}, \frac{-c}{ab})$ inverze lesz, mert $\frac{1}{a} \neq 0 \neq \frac{1}{b}$ miatt $(\frac{1}{a}, \frac{1}{b}, \frac{-c}{ab}) \in H$ (1 pont)
és $(a,b,c) * (\frac{1}{a}, \frac{1}{b}, \frac{-c}{ab}) = (a\cdot\frac{1}{a}, b\cdot\frac{1}{b}, a\cdot\frac{-c}{ab} + c\frac{1}{b}) = (1,1,0)$ (1 pont)
és $(\frac{1}{a}, \frac{1}{b}, \frac{-c}{ab}) * (a,b,c) = (\frac{1}{a}\cdot a, \frac{1}{b}\cdot b, \frac{1}{a}\cdot c + \frac{-c}{ab}\cdot b) = (1,1,0)$. (1 pont)
Mivel a definíció minden feltétele teljesül, ezért H $*$-ra nézve csoport. (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 $(H,*)$ nem csoport). Megjegyezzük, hogy a feladatbeli H zárt $*$-ra, hiszen $(a,b,c) \in H$ és $(d,e,f) \in H$ esetén $a \neq 0 \neq b$ és $d \neq 0 \neq e$, így $ad \neq 0$ és $be \neq 0$, vagyis $(ad, be, af+ce) \in H$. Azonban H zártságát a feladat szövege is állítja, amikor $*$-ot műveletnek nevezi. Ezért ennek ellenőrzéséért nem jár külön pont.