Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató
2011. április 21.

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. Az alábbi A mátrix egy G irányítatlan gráf szomszédossági mátrixa, a B mátrix pedig egy H hurokélmentes, irányított gráf illeszkedési mátrixa. Adjuk meg mindkét mátrixban a hiányzó (□-val jelölt) elemeket és rajzoljuk le a G és a H gráfot!

$$A = \begin{pmatrix} 0 & 1 & \square & 0 \\ \square & 0 & 1 & \square \\ 2 & \square & 0 & \square \\ 0 & 3 & 0 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & \square & 1 & 0 \\ \square & 0 & \square & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & \square & \square \end{pmatrix}$$

* * * * *

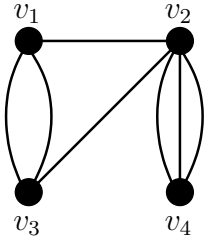
Minden irányítatlan gráf szomszédossági mátrixa (a főátlójára) szimmetrikus, hiszen az $a_{i,j}$ és az $a_{j,i}$ elem is a v_i és a v_j csúcsok közti élek száma. (2 pont)

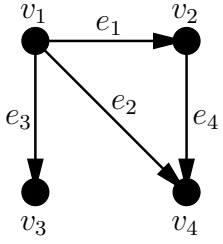
Ez alapján A hiányzó elemei kitölthetők: $A = \begin{pmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 3 \\ 2 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{pmatrix}$. (1 pont)

Minden hurokélmentes, irányított gráf illeszkedési mátrixában minden oszlop 1 darab 1-est és 1 darab (-1)-est tartalmaz, a többi elem 0 (hiszen az oszlopnak megfelelő él egy csúcsból kilép, egy másikba belép, a többire nem illeszkedik). (2 pont)

Ez alapján B hiányzó elemei kitölthetők: $B = \begin{pmatrix} 1 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \end{pmatrix}$. (1 pont)

A mátrixokból G és H már definíció szerint rekonstruálhatók:

$G =$ 

$H =$ 

(2+2 pont)

2. A G egyszerű, n csúcsú gráfban bármely két, nemszomszédos csúcsra teljesül, hogy a fokszámaik összege legalább $n+k-2$ (ahol $k \geq 1$ egész). Bizonyítsuk be, hogy G k-szorosan összefüggő!

* * * * *

Indirekt tegyük fel, hogy G nem k-szorosan összefüggő. Ekkor a $t \leq k-1$ elemű X ponthalmaz elhagyása után kapott gráf már nem összefüggő, vagyis a csúcsai az A és a B (nemüres) halmazokra bonthatók úgy, hogy A és B között nem fut él. (3 pont)
Jelölje A és B elemszámát a, illetve b.
Legyen $u \in A$ és $v \in B$ tetszőleges. Ekkor a fentiek szerint u és v nem szomszédosak. (1 pont)
Mivel u csak (sajátmagától különböző) A-beli, valamint X-beli csúcsokkal lehet szomszédos G-ben, ezért $d(u) \leq a-1+t$. Hasonlóan, $d(v) \leq b-1+t$. (3 pont)
Ezeket összeadva és felhasználva, hogy $a+b+t=n$ kapjuk: $d(u)+d(v) \leq n+t-2$. (2 pont)
Mivel $t \leq k-1$, ebből $d(u)+d(v) \leq n+k-3$, ami ellentmondás (mert u és v nem szomszédos).(1 pont)

3. Milyen maradékot adhat egy egész szám 142-vel osztva, ha a 83-szorosa 1 maradékot ad 142-vel osztva?

* * * * *

A feladat a $83n \equiv 1 \pmod{142}$ lineáris kongruencia. (1 pont)
2-vel szorozva: $166n \equiv 2 \pmod{142}$, vagyis $24n \equiv 2 \pmod{142}$. (1 pont)
2-vel osztva: $12n \equiv 1 \pmod{71}$. (2 pont)
6-tal szorozva: $72n \equiv 6 \pmod{71}$, vagyis $n \equiv 6 \pmod{71}$. (2 pont)
Ebből $n \equiv 6, 77 \pmod{142}$. (1 pont)
Ellenőrzéssel kiderül, hogy a 6 hamis gyök (ami a 2-vel szorzásnál jött be), így a megoldás $n \equiv 77 \pmod{142}$ (vagyis a kérdéses szám 77 maradékot adhat 142-vel osztva). (3 pont)
A lineáris kongruencia nagyon sokféleképp megoldható jól (akár hamis gyököt behozó lépés nélkül is). Aki a fenti megoldást, vagy más, hamis gyököt behozó megoldást ad, de nem foglalkozik a hamis gyök kiszűrésével, az értelemszerűen 3 pontot veszítsen. Ha valaki csak azt ellenőrzi, hogy $(83, 142)|1$, így a kongruenciának van megoldása, de a megoldást kiszámolni nem tudja, az összesen 2 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.

4. Mennyi maradékot ad 3^{2011}-nel osztva $100^{3^{2011}}$?

* * * * *

$\varphi(3^{2011}) = 3^{2011} - 3^{2010} = 2 \cdot 3^{2010}$ (a tanult képlet szerint). (1 pont)
Mivel $(10, 3^{2011}) = 1$ (hiszen a két szám prímtényezős felbontásában nyilván nincs közös prím),(1 pont)
ezért alkalmazható rájuk az Euler-Fermat tétel: $10^{\varphi(3^{2011})} = 10^{2 \cdot 3^{2010}} \equiv 1 \pmod{3^{2011}}$. (2 pont)
Ebből $100 = 10^2$ helyettesítéssel: $100^{3^{2010}} \equiv 1 \pmod{3^{2011}}$. (3 pont)
Ezt köbre emelve: $100^{3 \cdot 3^{2010}} = 100^{3^{2011}} \equiv 1^3 = 1 \pmod{3^{2011}}$ (vagyis a keresett maradék: 1).(3 pont)
Aki nem jön rá, hogy az Euler-Fermat tételt 10-re (és 3^{2011}-re) érdemes alkalmazni, de 100-ra (és 3^{2011}-re) alkalmazza (helyesen), az a fenti pontozásbeli első 4 pontot megkaphatja. (A pontozás utolsó két 3-as pontszáma épp azért ilyen magas, mert itt értékeljük a megoldás lényeges ötletét, a 10-re való alkalmazást.) A feladat megoldása egyébként helyesen, de komplikáltabban befejezhető a 100-ra felírt Euler-Fermat tételből is.

5. Értelmezzük a térvektorok $\mathbb{R}^3$ halmazán a $*$ műveletet a következőképpen:

$$(a,b,c)*(d,e,f)=(a+d,b+e,ae+c+f)$$

Döntsük el, hogy $\mathbb{R}^3$ csoportot alkot-e $*$-ra nézve!

* * * * *

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

$$\Big((a,b,c)*(d,e,f)\Big)*(g,h,i)=$$
$$(a+d,b+e,ae+c+f)*(g,h,i)=(a+d+g,b+e+h,(a+d)h+ae+c+f+i) \quad \text{(1 pont)}$$

és

$$(a,b,c)*\Big((d,e,f)*(g,h,i)\Big)=$$
$$(a,b,c)*(d+g,e+h,dh+f+i)=(a+d+g,b+e+h,a(e+h)+c+dh+f+i), \quad \text{(1 pont)}$$

ami $(a+d)h+ae+c+f+i=a(e+h)+c+dh+f+i$ miatt az asszociativitást igazolja. (1 pont)
Van egységelem a $*$-ra nézve, mégpedig a $(0,0,0)$, (1 pont)
ugyanis $(a,b,c)*(0,0,0)=(a+0,b+0,a\cdot 0+c+0)=(a,b,c)$ (1 pont)
és $(0,0,0)*(a,b,c)=(0+a,0+b,0\cdot b+0+c)=(a,b,c)$. (1 pont)
A tetszőleges (a,b,c) elemnek $(-a,-b,ab-c)$ inverze lesz, (1 pont)
mert $(a,b,c)*(-a,-b,ab-c)=(a-a,b-b,a(-b)+c+ab-c)=(0,0,0)$ (1 pont)
és $(-a,-b,ab-c)*(a,b,c)=(-a+a,-b+b,(-a)b+ab-c+c)=(0,0,0)$. (1 pont)
Mivel a definíció minden feltétele teljesül, ezért $\mathbb{R}^3$ $*$-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 nem csoport).

6. Legyen G véges csoport és g és h két tetszőleges elem G-ben. Mutassuk meg, hogy $o(g\cdot h)=o(h\cdot g)$!
(A G-beli műveletet $\cdot$-tal jelöltük, o pedig az elem rendjét jelöli.)

* * * * *

Vezessük be az $o(g\cdot h)=k$ és az $o(h\cdot g)=l$ jelöléseket, a csoport egységelemét jelölje e.
Mivel $o(g\cdot h)=k$, ezért $e=(g\cdot h)^k$, vagyis $e=g\cdot h\cdot g\cdot h\cdot\ldots\cdot g\cdot h$ (ahol a szorzatban k darab $g\cdot h$ tag szerepel). (1 pont)
Szorozzuk ezt az egyenletet balról g^{-1}-zel; ekkor a bal oldalon $g^{-1}\cdot e=g^{-1}$, a jobb oldalon pedig (a szorzat első tagjánál) keletkező $g^{-1}\cdot g$ szorzat e-t ad, így elhagyható: $g^{-1}=h\cdot g\cdot h\cdot\ldots\cdot g\cdot h$.(2 pont)
Most szorozzuk a kapott egyenletet jobbról g-vel és a bal oldalon keletkező $g^{-1}\cdot g$ szorzatot helyettesítsük e-vel: $e=g^{-1}\cdot g=h\cdot g\cdot h\cdot\ldots\cdot g\cdot h\cdot g$. (2 pont)
Most a jobb oldalon k darab $h\cdot g$ tag keletkezett, vagyis $e=(h\cdot g)^k$. (1 pont)
Így a $(h\cdot g)$ rendjének definíciója miatt $l\le k$. (2 pont)
Mivel g és h szerepe a feladatban szimmetrikus, teljesen hasonlóan $k\le l$ is belátható, amiből a feladat állítása következik. (2 pont)