Bevezetés a számításelméletbe II.

Zárthelyi feladatok — az **MÁSODIK** zárthelyi pótlására

Pontozási útmutató

2013. május 16.

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.

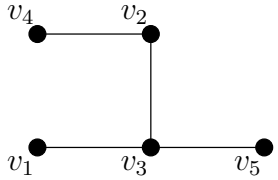
Minden feladat 10 pontot ér. Az elégséges határa 24 pont. A vizsgajegybe a dolgozat pontszáma számít bele, így a dolgozatokra osztályzatot nem adunk.

1. Az alábbi mátrix egy egyszerű, összefüggő gráf szomszédossági mátrixa. Adjuk meg a hiányzó (□-val jelölt) elemeket és rajzoljuk le a gráfot!

$$\begin{pmatrix} \square & 0 & \square & 0 & \square \\ \square & \square & \square & \square & 0 \\ \square & \square & \square & \square & \square \\ \square & 1 & 0 & \square & 0 \\ 0 & \square & \square & \square & \square \end{pmatrix}$$

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

Jelölje a gráf csúcsait az oszlopok és sorok sorrendjének megfelelően $v_1, v_2, \ldots, v_5$, a mátrixot A.
Mivel a gráf egyszerű, ezért nincs benne hurokél, így a főátló minden eleme 0. (1 pont)
A szomszédossági mátrix (irányítatlan gráf esetén) a főátlóra szimmetrikus (hiszen $a_{i,j}$ és $a_{j,i}$ is a v_i és v_j közti élek száma). Ez alapján a megadott 7 elem „tükörképe" kitölthető. (2 pont)
Látszik, hogy v_1 és v_5 sorában és oszlopában minden elem 0, kivéve a harmadikat, ami egyelőre ismeretlen. Mivel azonban a gráf összefüggő, v_1 és v_5 nem lehetnek izolált csúcsok, vagyis mindkettő szomszédos v_3-mal. Ezek alapján $a_{1,3} = a_{3,1} = a_{5,3} = a_{3,5} = 1$. (2 pont)
Már csak $a_{2,3}$ és $a_{3,2}$ (közös) értéke nem ismert. Azonban ha v_2 és v_3 nem volnának szomszédosak, akkor a $\{v_1, v_3, v_5\}$ és a $\{v_2, v_4\}$ csúcshalmazok külön komponenseket feszítenének, a gráf nem volna összefüggő. Így $a_{2,3} = a_{3,2} = 1$. (2 pont)
A szomszédossági mátrix ismeretében pedig a gráf már lerajzolható:



(3 pont)

2. Legyen G egy hurokélmentes, irányítatlan gráf és $s \in V(G)$ egy rögzített csúcs. Jelölje minden $v \in V(G)$, $v \neq s$ esetén $\lambda(v)$ az s-ből a v-be vezető, páronként éldiszjunkt utak maximális számát. Tegyük fel, hogy valamely $t \in V(G)$ csúcsra $\lambda(t) = 10$, de minden $v \in V(G)$, $v \neq s, t$ esetén $\lambda(v) > 10$. Mutassuk meg, hogy ekkor t foka 10.

* * * * *

$\lambda(t) = 10$ miatt s-ből t-be nem létezik 11 darab páronként éldiszjunkt út, ezért Menger megfelelő tétele miatt van G-ben egy 10 elemű Z élhalmaz, amely lefogja az s és t közti utakat. (2 pont)
Z elhagyása után tehát a gráf több komponensre esik és s és t különböző komponensbe kerül. Jelölje a t-t tartalmazó (Z elhagyása utáni) komponens csúcshalmazát T. (1 pont)
Z minden élének egyik végpontja T-ben van, különben az s és t közti utak 10-nél kevesebb éllel is lefoghatók volnának, ami ellentmond $\lambda(t) = 10$-nek. (2 pont)
Ha létezne egy $v \in T$, $v \neq t$ csúcs, akkor Z az s és v közötti utakat is lefogná, amiből $\lambda(v) \leq 10$ következne. Ez ellentmond a feladatban írt feltételnek, így ilyen v nem lehet. (3 pont)
Így Z élei épp a t-re illeszkedő élek, vagyis t foka 10. (2 pont)

3. Egy egész számra teljesül, hogy $37n + 9$ és $n + 10$ azonos maradékot ad 235-tel osztva. Mi lehet ez a közös maradék?

* * * * *

A keresett számot n-nel jelölve a feladat szövege szerint $37n + 9 \equiv n + 10 \pmod{235}$. (1 pont)
Átrendezve a $36n \equiv 1 \pmod{235}$ lineáris kongruenciát kapjuk. (1 pont)
7-tel szorozva: $252n \equiv 7 \pmod{235}$, vagyis $17n \equiv 7 \pmod{235}$. (1 pont)
14-gyel szorozva: $238n \equiv 98 \pmod{235}$, vagyis $3n \equiv 98 \pmod{235}$. (2 pont)
$98 \equiv 333 \pmod{235}$ miatt ugyanez $3n \equiv 333 \pmod{235}$ alakba is írható. (1 pont)
3-mal osztva: $n \equiv 111 \pmod{235}$, ahol a modulus $(3, 235) = 1$ miatt nem változott. (2 pont)
Ebből $n + 10 \equiv 121 \pmod{235}$, így a közös maradék 121. (2 pont)

4. Egy n egész szám 3 maradékot ad 72-vel osztva. Milyen maradékot adhat 102-vel osztva a $2n + 7$ szám?

* * * * *

A feladat azt kérdezi, hogy az $n \equiv 3 \pmod{72}$, $2n+7 \equiv a \pmod{102}$ kongruenciarendszernek milyen $a \in \{0, 1, \ldots, 101\}$ értékekre van megoldása. (2 pont)
Az első kongruenciából $n = 72k + 3$ valamilyen $k \in \mathbb{Z}$ esetén. (1 pont)
Ezt a másodikba helyettesítve: $2(72k + 3) + 7 = 144k + 13 \equiv a \pmod{102}$. (1 pont)
Átrendezés után a $144k \equiv a - 13 \pmod{102}$ lineáris kongruenciára jutunk. (1 pont)
A tanult tétel szerint ez pontosan akkor megoldható, ha $(144, 102)|a - 13$. (2 pont)
Mivel $(144, 102) = 6$, ezért ez azzal ekvivalens, hogy $6|a - 13$, vagyis hogy $a \equiv 13 \pmod{6}$, azaz $a \equiv 1 \pmod{6}$. (1 pont)
Tehát $2n + 7$ lehetséges maradékai 102-vel osztva a 6-tal osztva 1 maradékot adó számok $(1, 7, 13, \ldots, 97)$. (2 pont)
Természetesen nem jár pontlevonás azért, ha valaki a fenti megoldás első mondatát nem írja le, de a megoldásból kiderül, hogy valójában a paraméteres kongruenciarendszert oldja meg.

5. Mi az utolsó két számjegye a 11-es számrendszerben a (10-es számrendszerben felírt) $42^{41^{40}}$ számnak?

* * * * *

A feladat azt kérdezi, hogy $42^{41^{40}}$ milyen maradékot ad 121-gyel osztva. (1 pont)
Mivel $\varphi(121) = \varphi(11^2) = 11^2 - 11 = 110$ (1 pont)
és $(42, 121) = 1$, (1 pont)
ezért az Euler-Fermat tétel miatt $42^{110} \equiv 1 \pmod{121}$. (1 pont)
Ezt tetszőleges $k \geq 1$ egészre k-adik hatványra emelhetjük: $42^{110k} \equiv 1^k = 1 \pmod{121}$. (1 pont)
Mivel $\varphi(110) = \varphi(2 \cdot 5 \cdot 11) = 1 \cdot 4 \cdot 10 = 40$ és $(41, 110) = 1$, (1 pont)
ezért az Euler-Fermat tétel miatt $41^{40} \equiv 1 \pmod{110}$. (1 pont)
Ezért $41^{40} = 110k + 1$ valamely $k \geq 1$ egészre. Ebből $42^{41^{40}} = 42^{110k+1} = 42^{110k} \cdot 42$. (1 pont)
Így a fentebb látott $42^{110k} \equiv 1 \pmod{121}$ kongruencia miatt $42^{41^{40}} \equiv 42 \pmod{121}$. (1 pont)
Ezért ($42 = 3 \cdot 11 + 9$ miatt) $42^{41^{40}}$ utolsó két számjegye a 11-es számrendszerben 39. (1 pont)

6. A G (tetszőleges) csoport a, b, c és d (különböző) elemeire fennállnak az $a * b = a$, $c * d = b$ és $a * c = d$ összefüggések (ahol a G műveletét $*$-gal jelöltük). Döntsük el, hogy az alábbi állításokra melyik áll fenn a következő lehetőségek közül:

(i) az állítás biztosan igaz;

(ii) az állítás biztosan hamis;

(iii) az állítás lehet igaz is és hamis is (G és a, b, c, d választásától függően).

a) $c^{-1} \in \{a, b, c, d\}$

b) $c * a \in \{a, b, c, d\}$

c) $d * a \in \{a, b, c, d\}$

* * * * *

Az $a * b = a$ egyenlet mindkét oldalát balról a^{-1}-zel szorozva: $a^{-1} * (a * b) = a^{-1} * a$. Itt $a^{-1} * (a * b) = (a^{-1} * a) * b = e * b = b$ és $a^{-1} * a = e$, ahol e az egységelemet jelöli. Tehát $b = e$. (1 pont)
Így a $c * d = b$ egyenletből ($b = e$-t használva és balról c^{-1}-zel szorozva) kapjuk, hogy $c^{-1} = d$.(1 pont)
Ezért a $c^{-1} \in \{a, b, c, d\}$ állítás biztosan igaz. (1 pont)
Az $a * c = d$-ből $c^{-1} = d$-t használva $a * c = c^{-1}$ adódik. Ezt balról c-vel szorozva: $c * a * c = c * c^{-1} = e$. Jobbról c^{-1}-zel szorozva: $c * a * c * c^{-1} = e * c^{-1}$, vagyis $c * a = c^{-1}$. Mivel $c^{-1} = d$, ezért a $c * a \in \{a, b, c, d\}$ állítás is biztosan igaz. (3 pont)
A $d * a \in \{a, b, c, d\}$ állítás viszont lehet igaz is és hamis is, aminek igazolására két példát mutatunk.
Legyen például $(G, *) = (\mathbb{Z}, +)$ (vagyis a feladatbeli csoportot válasszuk az egészek összeadással vett csoportjának) és legyen $a = -2$, $b = 0$, $c = 1$ és $d = -1$. Ekkor a feladatban írt három összefüggés valóban teljesül: $a * b = (-2) + 0 = -2 = a$, $c * d = 1 + (-1) = 0 = b$ és $a * c = (-2) + 1 = -1 = d$. Viszont $d * a = (-1) + (-2) = -3 \notin \{a, b, c, d\}$. (2 pont)
Másrészt legyen a $(G, *)$ csoport a $\{0, 1, 2, 3\}$ halmaz a modulo 4 összeadással (amit $\oplus$-szal jelölünk). Előadásról ismert, hogy ez (ciklikus) csoport. Legyen $a = 2$, $b = 0$, $c = 1$ és $d = 3$. Ekkor a feladatban írt három összefüggés megint teljesül: $a * b = 2 \oplus 0 = 2 = a$, $c * d = 1 \oplus 3 = 0 = b$ és $a * c = 2 \oplus 1 = 3 = d$. Most viszont $d * a = 3 \oplus 2 = 1 = c \in \{a, b, c, d\}$. (2 pont)