Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató
2013. december 11.

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 lenne 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 100 csúcsú G (egyszerű) gráf szomszédossági mátrixa A.
a) Mutassuk meg, hogy ha A^{111} főátlójában az elemek összege 0, akkor G páros gráf.
b) Igaz-e, hogy ha G páros gráf, akkor A^{111} főátlójában az elemek összege 0?

* * * * *

a) Egy gráf pontosan akkor páros, ha nincs benne páratlan kör. Ha G-ben lenne páratlan kör, akkor ennek egy pontját kiválasztva lenne onnan induló 111 hosszú körséta: végigmegyünk a körön (amelynek legfeljebb 99 éle lehet), majd a legutolsó élen oda-vissza lépegetünk még addig, amíg 111 hosszú körsétát nem kapunk. (2 pont)
Így felhasználva, hogy az A^{111} mátrix főátlójának i-edik eleme az i-edik csúcsból induló 111 hosszú körséták száma, ebből már következne, hogy a főátlóban olyan nemnegatív számok szerepelnek, amelyek között pozitív is van, vagyis nem lehetne 0 a főátlóbeli elemek összege. Ebből következik, hogy gráfban valójában nem lehet páratlan kör, és így G páros. (3 pont)

b) Ha G páros gráf, akkor csúcsai feloszthatók két halmazra, A-ra és B-re úgy, hogy A-beli csúcsok csak B-beliekkel szomszédosak. Ekkor ha egy 111 hosszú (azaz 111 élből álló) séta kezdőpontja A-beli, akkor a 2. pont B-beli, a 3. ismét A-beli, és így tovább..., végül az utolsó, 111. él végpontja, vagyis a 112. pont ismét B-beli. Ez viszont azt jelenti, hogy ez nem lehet körséta, vagyis 111 hosszú körséta egyáltalán nincs a gráfban. (4 pont)
Így ismét felhasználva a séták számáról szóló tételt azt kapjuk, hogy A^{111} főátlójában minden elem 0, azaz az összegük is 0. Tehát b) igaz. (1 pont)

2. Egy óriási tábla csokit úgy daraboltunk fel, hogy minden egyes lépésben valamelyik kezünk ügyébe eső darabot 4, vagy 7 kisebb részre osztottuk. Kaphattunk-e ilyen módon végül
a) 2013
b) 2014
darabot?

* * * * *

Ha egy darabot 4 részre törünk, akkor a darabok száma 3-mal nő, ha pedig 7 részre, akkor 6-tal. Így, ha összességében x-szer törtünk 4 részre, y-szor 7 részre, akkor a darabok száma $1+3x+6y$ lesz, hiszen kezdetben 1 volt. (3 pont)
Az a kérdés, hogy az $1+3x+6y=2013$, illetve az $1+3x+6y=2014$ egyenleteknek van-e nemnegatív egész számokból álló megoldása. Az elsőből azt kapjuk, hogy $3x+6y=2012$, itt az egyenlet bal oldalán álló kifejezés $3(x+2y)$ alakban is írható, tehát osztható 3-mal, míg a jobb oldalon álló 2012 nem, tehát nincs egész megoldás, vagyis a)-ra nemleges a válasz. (3 pont)
A második egyenletből $3x+6y=2013$ adódik, amelynek pl. $x=2013/3=671, y=0$ nemnegatív egész megoldása, tehát ha pl. 671-szer törünk 4 részre, akkor éppen 2014 darabunk lesz, azaz b)-re igen a válasz. (4 pont)
(A második egyenletnél, ha valaki csak annyit ír, hogy $3x+6y=2013$-nak van egész megoldása, mert $(3,6)|2013$, az még kevés, hiszen nekünk most *nemnegatív* egész megoldás kell.)

3. Milyen maradékot adhat egy egész szám 93-mal osztva, ha a 75-szöröse 51 maradékot ad 93-mal osztva?

* * * * *

A feladat megválaszolásához először megoldjuk a $75x \equiv 51\ (93)$ kongruenciát. (1 pont)
(Ezt sokféleképpen megtehetjük, egy lehetséges megoldás:) Leosztunk 3-mal, és mivel $(3,93)=3$, ezért a modulust is osztanunk kell 3-mal: $25x \equiv 17\ (31)$. A kongruencia jobb oldalán 17 helyett $17+3\cdot 31=110$-et is írhatunk, ahonnan 5-tel való osztás után $5x \equiv 22\ (31)$ kongruenciát kapjuk, hiszen $(5,31)=1$. Most 22 helyett $22-2\cdot 31=-40$-et írva, és ismét 5-tel osztva $x \equiv -8 \equiv 23\ (31)$ kongruenciát kapjuk. (5 pont)
Ez pontosan azt jelenti, hogy valamely k egész számra $x=31k+23$. A $31k+23$ szám 93-as maradéka pedig

- 23, ha $k=3l$ alakú, hiszen ekkor $31k+23=93l+23$,
- 54, ha $k=3l+1$ alakú, hiszen ekkor $31k+23=31(3l+1)+23=93l+54$,
- 85, ha $k=3l+2$ alakú, hiszen ekkor $31k+23=31(3l+2)+23=93l+85$.

Így mod 93 a megoldások: $x \equiv 23, 54, 85\ (93)$. Tehát a lehetséges maradékok: 23, 54, 85. (4 pont)

4. Mely pozitív egész n számokra teljesül, hogy $\varphi(n^2)=n\varphi(n)$?

* * * * *

I. megoldás. A tanult képlet alapján $\varphi(n^2)=n^2\prod_{p|n^2}=n^2\prod_{p|n}=n\cdot n\prod_{p|n}=n\varphi(n)$, hiszen itt a produktumoknál p az n^2, illetve n számok (pozitív) prímosztóin fut végig, de n és n^2 prímosztói ugyanazok. (8 pont)
Tehát minden pozitív egész n-re teljesül, hogy $\varphi(n^2)=n\varphi(n)$. (2 pont)

II. megoldás. Legyen az n szám prímtényezős felbontása $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$. Ekkor $n^2=p_1^{2\alpha_1}p_2^{2\alpha_2}\dots p_r^{2\alpha_r}$. (2 pont)
Így a tanult összefüggés szerint

$$\begin{aligned}\varphi(n^2)&=(p_1^{2\alpha_1}-p_1^{2\alpha_1-1})(p_2^{2\alpha_2}-p_2^{2\alpha_2-1})\dots(p_r^{2\alpha_r}-p_r^{2\alpha_r-1})=\\&=p_1^{\alpha_1}(p_1^{\alpha_1}-p_1^{\alpha_1-1})p_2^{\alpha_2}(p_2^{\alpha_2}-p_2^{\alpha_2-1})\dots p_r^{\alpha_r}(p_r^{\alpha_r}-p_r^{\alpha_r-1})=\\&=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}(p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\dots(p_r^{\alpha_r}-p_r^{\alpha_r-1})=n\varphi(n)\end{aligned}$$

(6 pont)
Tehát minden pozitív egész n-re teljesül, hogy $\varphi(n^2)=n\varphi(n)$. (2 pont)

5. Mely n egész számokra lesz $n^3 - n + 3$ prímszám?

* * * * *

A kis Fermat-tétel szerint $n^3 \equiv n$ (3), vagyis $3|n^3 - n$, és így $3|n^3 - n + 3$. (3 pont)
Tehát $n^3 - n + 3$ egy 3-mal osztható prímszám, így vagy a 3, vagy a -3. (1 pont)
Ha $n^3 - n + 3 = 3$, akkor $n^3 = n$, amiből $n = -1, 0$, vagy 1. (2 pont)
Ha $n^3 - n + 3 = -3$, akkor $n^3 - n + 6 = 0$. Ennek a harmadfokú egyenletnek egyetlen egész megoldása van: $n = -2$. Ez leolvasható pl. az $n^3 - n + 6 = (n + 2)((n - 1)^2 + 2)$ átalakításból, de megkapható a racionális gyökteszt segítségével is, ami itt most azt jelenti, hogy $n^3 - n = -6$ felírásból látható, hogy $n|6$, a 6 osztóit $(-6, -3, -2, -1, 1, 2, 3, 6)$ behelyettesítve pedig kiderül, hogy egyedül $n = -2$ megoldás. Egy harmadik lehetséges indoklás: $n^3 - n = (n-1)n(n+1) = -6$ egyenletet kell megoldani, vagyis -6-ot kell előállítani 3 egymást követő egész szám szorzataként. A 0 nem szerepelhet köztük (mert akkor 0 lenne a szorzat), tehát mindháromnak negatívnak kell lennie (különben pozitív lenne a szorzat), a $(-3)(-2)(-1)$ szorzat éppen -6-ot ad (itt $n = -2$), viszont ha n értékét csökkentjük, akkor a szorzat abszolút értéke már 6-nál nagyobb lesz, így nem kaphatunk újabb megoldást. (3 pont)
Tehát $n^3 - n + 3$ pontosan akkor prímszám, ha $n = -2, -1, 0$, vagy 1. (1 pont)

6. Legyen H a 2×2-es invertálható mátrixok halmaza. A (szokásos) mátrixszorzás segítségével egy $*$ és egy $\circ$ kétváltozós függvényt definiálunk H-n a következő módon:

$$A * B = A^{-1} \cdot B^{-1},$$

$$A \circ B = B \cdot A.$$

a) Igaz-e, hogy $(H, *)$ csoport?
b) Igaz-e, hogy $(H, \circ)$ csoport?

* * * * *

a) *I. megoldás* Könnyen megmutatható, hogy $*$ művelet (de mivel a)-ra végül nemleges lesz a válasz, erre nem jár részpontszám). Az asszociativitás ellenőrzése:

$$(A * B) * C = (A^{-1}B^{-1}) * C = (A^{-1}B^{-1})^{-1}C^{-1} = BAC^{-1}$$

$$A * (B * C) = A * (B^{-1}C^{-1}) = A^{-1}(B^{-1}C^{-1})^{-1} = A^{-1}CB$$

(2 pont)
Ez a két kifejezés nem mindig egyenlő, hiszen pl.: $A = 2E, B = E, C = E$ esetén, ahol E az egységmátrix, az első változat $2E$-t, a második $E/2$-t ad eredményül. (2 pont)
Tehát $*$ nem asszociatív, így $(H, *)$ nem csoport. (1 pont)

II. megoldás. Ha lenne egységelem, mondjuk F, akkor $A = A * F = A^{-1}F^{-1}$-nek teljesülnie kellene minden invertálható 2×2-es A mátrixra, ebből $F = A^{-2}$. (2 pont)
Tehát elég mutatni két olyan invertálható 2×2-es mátrixot, amelyek -2-edik hatványa nem egyenlő. Ilyen pl. E és $2E$, előbbinek a -2-edik hatványa E, utóbbinak pedig $E/4$. (2 pont)
Tehát nincs egységelem, így $(H, *)$ nem csoport. (1 pont)
(Ha valaki belátja azt is, hogy nem teljesül az asszociativitás, és azt is, hogy nincs egységelem, akkor is csak 5 pontot kaphat a)-ra.)
Megjegyzés. Inverzről persze már nincs is értelme beszélni, hiszen egységelem sincsen.
b) Először is, $\circ$ művelet, hiszen 2×2-es invertálható mátrixok szorzata is az. (1 pont)
A $\circ$ művelet asszociatív, hiszen

$$(A \circ B) \circ C = (BA) \circ C = CBA = A \circ (CB) = A \circ (B \circ C).$$

(2 pont)

Van egységelem is: az E egységmátrixra teljesül, hogy $A \circ E = E \circ A = A$. (1 pont)

Végül, minden elemnek van inverze: A-nak az inverze ebben a csoportban éppen a hagyományos inverze, vagyis A^{-1}, hiszen:

$$A \circ A^{-1} = A^{-1}A = E,$$

$$A^{-1} \circ A = AA^{-1} = E.$$

(1 pont)

Tehát $(H, \circ)$ csoport.