Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató
2009. november 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. A G k-szorosan pontösszefüggő irányítatlan gráfban kijelöltünk két csúcshalmazt, X-et és Y-t, úgy, hogy $X \cap Y = \emptyset$, $|X| \geq k$ és $|Y| \geq k$. Bizonyítsuk be, hogy biztosan van k darab különböző $x_1, \ldots, x_k$ csúcs X-ben és k darab különböző $y_1, \ldots, y_k$ csúcs Y-ban, úgy hogy G-ben van út x_i-ből y_i-be és ez a k darab út páronként pontdiszjunkt!

* * * * *

Vegyünk hozzá a G gráfhoz két új csúcsot, s-et és t-t és kössük össze s-et minden X-beli, t-t pedig minden Y-beli csúccsal. (1 pont)
Belátjuk, hogy az így kapott G' gráf szintén k-szorosan összefüggő lesz. (1 pont)
Azt kell megmutatni, hogy akárhogyan hagyok el k-nál kevesebb csúcsot G'-ből, a gráf nem esik szét. (1 pont)
Ha G'-ből elhagyok legfeljebb $k-1$ csúcsot, akkor az eredeti G gráf csúcsai közül is max. ennyit hagytam el. Mivel azonban G k-szorosan összefüggő volt, ezért marad út tetszőleges két G-beli pont között, vagyis a G-ben megmaradt csúcsok egy komponensbe tartoznak. (2 pont)
Azt kell még látni, hogy az esetlegesen megmaradt s és t csúcsok is ehhez a komponenshez tartoznak, ez azonban azért igaz, mert ($|X| \geq k$ és $|Y| \geq k$ miatt) biztosan maradt legalább egy X-beli és legalább egy Y-beli csúcs, amihez így s és t hozzákötődnek. (1 pont)
Mivel G' k-szorosan összefüggő, tetszőleges 2 csúcsa között létezik k darab (végpontjaitól eltekintve) páronként pontdiszjunkt út. Ez igaz az s és t választásra is. (2 pont)
Tekintsük ezt a k darab utat: ezek mindegyike csak úgy indulhat, hogy s-ből elmegyünk valamelyik $x \in X$ csúcsba, onnan valahogyan eljutunk egy $y \in Y$ csúcsba, majd onnan t-be. (1 pont)
Ezen utak belső csúcsai diszjunkt ponthalmazokat alkotnak, vagyis ha a fenti k darab útból elhagyjuk a kiindulási s és érkezési t csúcsokat, akkor éppen kapunk a kívánt tulajdonsággal rendelkező k darab utat. (1 pont)

2. Bizonyítsa be, hogy a $2 \cdot d(n^2) = 3 \cdot d(n)$ egyenlőség akkor és csak akkor igaz egy $n \geq 2$ egész számra, ha n prím.

* * * * *

Ha $n = p$ prímszám, akkor $d(n^2) = d(p^2) = 3$, $d(n) = d(p)$ pedig 2, vagyis az egyenlőség fennáll. (2 pont)
A másik irány bizonyításához tekintsük n prímtényezős felbontását: $n = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}$, ekkor $n^2 = {p_1}^{2\alpha_1} \cdots {p_k}^{2\alpha_k}$. (1 pont)
A tanult képlet szerint $d(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$, $d(n^2) = (2\alpha_1 + 1) \cdots (2\alpha_k + 1)$ (2 pont)
Tehát azt tudjuk, hogy $2(2\alpha_1 + 1) \cdots (2\alpha_k + 1) = 3(\alpha_1 + 1) \cdots (\alpha_k + 1)$. Mindkét oldal első tagját beszorozva a konstanssal kapjuk, hogy $(4\alpha_1 + 2)(2\alpha_2 + 1) \cdots (2\alpha_k + 1) = (3\alpha_1 + 3)(\alpha_2 + 1) \cdots (\alpha_k + 1)$. (1 pont)
Tagonként megvizsgálva a két szorzatot azt kapjuk, hogy $4\alpha_1 + 2 \geq 3\alpha_1 + 3$, mert $\alpha_1 \geq 1$, hiszen $n > 2$, egy prímosztója biztosan van, továbbá látszik, hogy egyenlőség csak az $\alpha_1 = 1$ esetben van. (2 pont)
A második tagtól kezdve pedig $(2\alpha_i + 1) \geq \alpha_i + 1$ és csak akkor van egyenlőség, ha $\alpha_i = 0$. (1 pont)
Mivel a baloldali kifejezés minden tagja legalább akkora, mint a jobboldali szorzat megfelelő tagja, egyenlőség csak akkor állhat fenn, ha minden tagban egyenlőség van, azaz amikor $\alpha_1 = 1$, $\alpha_i = 0$ ha $i \geq 2$, azaz amikor n prím. (1 pont)

3. Egy n egész szám 76-szorosa 24 maradékot ad 50-nel osztva. Mi lehet az n szám utolsó két számjegye? (Ha több lehetőség van, akkor az összeset adja meg.)

* * * * *

A szövegesen megfogalmazott feltételnek pontosan azon n számok tesznek eleget, melyekre $76n \equiv 24 \pmod{50}$ fennáll. (2 pont)
Ez pontosan akkor igaz, ha $26n \equiv 24 \pmod{50}$. (1 pont)
Ez pontosan akkor igaz, ha $13n \equiv 12 \pmod{25}$ (osztottunk 2-vel, a modulust is). (1 pont)
Ez pontosan akkor igaz, ha $-12n \equiv 12 \pmod{25}$ (13 helyére a vele azonos maradékosztályban levő -12-t írva). (1 pont)
Ez pedig pontosan a $n \equiv -1 \pmod{25}$ esetben igaz. (1 pont)
Vagyis pontosan azon n-ek lesznek jók, amik 25-tel osztva 24 maradékot adnak. (1 pont)
Ha az utolsó két számjegyre vagyunk kíváncsiak, akkor azt kérdezzük, hogy az ilyen számok 100-zal osztva mennyi maradékot adhatnak. (1 pont)
Mivel $100 = 4 \cdot 25$, ezért a modulo 25 egy maradékosztályba eső számok közül pontosan 4 fog modulo 100 más maradékot adni, vagyis 4-féle maradék lehetséges 100-zal osztva: 24, 49, 74 és 99. (2 pont)

4. Hány 1111-nél nem nagyobb pozitív egész x szám van, melyre igaz, hogy $x^{1111} \equiv 1 \pmod{11}$?

* * * * *

Ha x osztható 11-gyel, akkor x^{1111} is osztható, vagyis ilyen x-re $x^{1111} \equiv 0 \pmod{11}$, tehát ilyen x sose lesz megoldás. (2 pont)
Feltehetjük tehát, hogy x és 11 relatív prímek, (1 pont)
ekkor az Euler-Fermat-tétel miatt $x^{10} \equiv 1 \pmod{11}$ (3 pont)
vagyis $x^{1110} = x^{10 \cdot 111} \equiv 1 \pmod{11}$. (1 pont)
Ezek szerint $x^{1111} = x \cdot x^{10 \cdot 111} \equiv x$, tehát $x^{1111} \equiv 1 \pmod{11}$ ekvivalens azzal, hogy $x \equiv 1 \pmod{11}$.

(1 pont)
Vagyis pontosan a 11-gyel 1 maradékot adó x-ek lesznek jók, ezekből minden 11 szám között egy darab van, az első 1111 szám között $1111 : 11 = 101$, vagyis összesen 101 megoldás van a kívánt tartományban. (2 pont)

A megoldás elejét a kis-Fermat tétel alkalmazásával is helyettesíthetjük:
Mivel a 11 prímszám, (1 pont)
alkalmazhatjuk a kis-Fermat tételt: $x^{11} \equiv x \pmod{11}$. (4 pont)
Ezek szerint $x^{1111} = x^{11 \cdot 101} \equiv x^{101} = x^{11 \cdot 9} \cdot x^2 \equiv x^9 \cdot x^2 = x^{11} \equiv x \pmod{11}$, tehát $x^{1111} \equiv 1 \pmod{11}$
ekvivalens azzal, hogy $x \equiv 1 \pmod{11}$. (3 pont)

5. Tekintsük a $H = \{3 \cdot k \mid k \in \mathbb{Z}\}$ halmazon az alábbi függvényt: $(3 \cdot k) * (3 \cdot l) = 3 \cdot k \cdot l$. (Tehát például $6 \cdot 12 = (3 \cdot 2) * (3 \cdot 4) = (3 \cdot 2 \cdot 4) = 24$.)

a) Igaz-e, hogy H félcsoportot alkot $*$-ra nézve?

b) Igaz-e, hogy H csoportot alkot $*$-ra nézve ?

* * * * *

a) A $*$ függvény művelet H-n, mert az eredmény mindig 3-mal osztható egész. (2 pont)
A $*$ művelet asszociatív, mert $((3 \cdot k) * (3 \cdot l)) * (3 \cdot m) = (3 \cdot k \cdot l) * (3 \cdot m) = 3 \cdot k \cdot l \cdot m$, míg $(3 \cdot k) * ((3 \cdot l) * (3 \cdot m)) = (3 \cdot k) * (3 \cdot l \cdot m) = 3 \cdot k \cdot l \cdot m$. (2 pont)
Tehát ez egy félcsoport, mert ahhoz ez a 2 dolog kell. (1 pont)

b) Van egységelem is, a $3 = 3 \cdot 1$, mert $(3 \cdot k) * (3 \cdot 1) = 3 \cdot k \cdot 1 = 3 \cdot k$ és $(3 \cdot 1) * (3 \cdot k) = 3 \cdot 1 \cdot k = 3 \cdot k$. (2 pont)
A csoportsághoz kéne, hogy legyen minden elemnek inverze, (1 pont)
de ez nem teljesül, (1 pont)
mert például a $6 = 3 \cdot 2$-nek sincsen, nem lehet 6-ot megszorozni egy (hárommal osztható) egész számmal úgy, hogy 3 legyen az eredmény. (1 pont)

6. Legyen G csoport a $*$ műveletre nézve és legyenek $a, b, c \in G$ tetszőleges (nem feltétlenül különböző) csoportelemek. Igaz-e, hogy a

a) $c * a * c = c * b * c$ egyenlőségből következik $a = b$?

b) $a * c = c * b$ egyenlőségből következik $a = b$?

Ha azt gondolja, hogy az állítás igaz, akkor bizonyítsa be, ellenkező esetben pedig adjon ellenpéldát!

* * * * *

a) Mivel G csoport, ezért létezik a c-nek inverze. (1 pont)
Ezzel beszorozva balról a $c * a * c = c * b * c$ egyenlőséget kapjuk, hogy $c^{-1} * c * a * c = c^{-1} * c * b * c$, tehát $a * c = b * c$. Ezt beszorozva c inverzével jobbról, hasonlóan kapjuk, hogy $a * c * c^{-1} = b * c * c^{-1}$, azaz $a = b$, vagyis az (a) állítás igaz. (3 pont)
b) Nem igaz, mutatunk ellenpéldát. Ellenpéldának jó a D_3 diédercsoport (2 pont)
és ebben az $a = t_1$, $c = f_{120}$, $b = t_2$ választás. (2 pont)
Ekkor ugyanis $t_1 \cdot f_{120} = t_3$ és $f_{120} \cdot t_2 = t_3$, de $t_1 \neq t_2$. (2 pont)

A b) résznél jó ellenpéldát lehet találni a $n \times n$-es invertálható mátrixok csoportjában is, ekkor 2 pont a jó csoport megnevezése, 2 pont a jó elemválasztás és 2 pont annak megmutatása, hogy $a * c = c * b$, de $a \neq b$.
A puszta (nulla indoklással felírt) tippelés nem ér pontot egyik résznél sem, de ha bármi magyarázat van mellé, amiből látszik, hogy volt valami gondolat a tippelés mögött, akkor a jó tipp darabja 1 pontot ér.