Bevezetés a számításelméletbe II.

Zárthelyi feladatok — az **MÁSODIK** zárthelyi pótlására

Pontozási útmutató

2011. május 9.

Általános alapelvek.

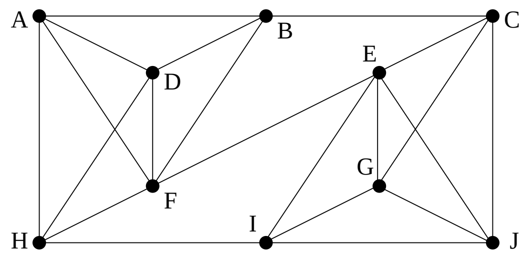
A pontozási útmutató célja, hogy a javítók a dolgozatokat egységesen értékeljék. Ezért az útmutató minden feladat (legalább egy lehetséges) megoldásának főbb gondolatait és az ezekhez rendelt részpontszámokat közli. Az útmutatónak *nem célja* a feladatok teljes értékű megoldásának részletes leírása; 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. Igaz-e, hogy az alábbi gráf
a) 4-szeresen élösszefüggő;
b) 4-szeresen pontösszefüggő?



* * * * *

a) A $\{B, C\}$, $\{E, F\}$ és $\{H, I\}$ élek elhagyásával kapott gráf nem összefüggő,(2 pont) így a gráf nem 4-szeresen élösszefüggő. (4 pont)

b) Mivel a gráf 4-szeres pontösszefüggőségéből a 4-szeresen élösszefüggőség is következne, ezért a gráf 4-szeresen pontösszefüggő sem lehet. (4 pont)
(A b) feladat persze a definíciót használva is megoldható: például a B, F és H pontok elhagyásával kapott gráf nem összefüggő.)

2. A 100 csúcsú, hurokélmentes G gráf szomszédossági mátrixát jelölje A. Mutassuk meg, hogy ha az A^{14} mátrix főátlójában álló elemek összege 10^9-nél kisebb, akkor G-nek van olyan csúcsa, amelynek a foka legföljebb 9.

* * * * *

Legyen $V(G)=\{v_1,v_2,\ldots,v_{100}\}$. Az A^{14} főátlójában álló i-edik elem a v_i-ből sajátmagába vezető, pontosan 14 élű élsorozatok száma. (1 pont)
Bármely v_i-ből indulva 14 élű, v_i-be vezető élsorozatot kapunk, ha tetszőlegesen megválasztva a v_i-re illeszkedő $e_1,e_2,\ldots,e_7$ (nem feltétlen különböző) éleket, először e_1-en, majd e_2-n, stb., végül e_7-en „oda-vissza" haladunk. (4 pont)
Ha $d(v_i)=d$, akkor ezzel d^7 különböző, v_i-ből v_i-be vezető élsorozatot kapunk. (3 pont)
Ha tehát indirekt feltesszük, hogy minden pont foka legalább 10, akkor ezzel minden v_i-re legalább 10^7, összesen pedig legalább $100\cdot 10^7=10^9$ különböző élsorozatot kapnánk. Ez ellentmond annak, hogy az A^{14} főátlójában álló elemek összege 10^9-nél kisebb. (2 pont)
(Megjegyezzük, hogy a fenti megoldásban d^7 természetesen nem az *összes* v_i-ből v_i-be vezető, 14 hosszúságú élsorozat száma; a megoldásban csupán annyit állítunk, hogy d^7 darab ilyen élsorozatot még a leírt, nagyon speciális módon is találhatunk.)

3. Egy n egész számra teljesül, hogy $50n$ és $n+1$ azonos maradékot ad 178-cal osztva. Mi lehet ez a közös maradék?

* * * * *

A feladat az $50n\equiv n+1 \pmod{178}$ lineáris kongruencia. (1 pont)
n-et levonva: $49n\equiv 1 \pmod{178}$. (1 pont)
4-gyel szorozva: $196n\equiv 4 \pmod{178}$, vagyis $18n\equiv 4 \pmod{178}$. (1 pont)
2-vel osztva: $9n\equiv 2 \pmod{89}$. (1 pont)
10-zel szorozva: $90n\equiv 20 \pmod{89}$, vagyis $n\equiv 20 \pmod{89}$. (1 pont)
Ebből $n\equiv 20, 109 \pmod{178}$. (1 pont)
Ellenőrzés mutatja, hogy a 20 hamis gyök (ami a 4-gyel szorzásnál jött be), így $n\equiv 109 \pmod{178}$. (3 pont)
Ebből $n+1\equiv 110 \pmod{178}$, így a keresett közös maradék a 110. (1 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 $(49,178)|1$, így a kongruenciának van megoldása, de azt kiszámolni nem tudja, az összesen (az első átrendezéssel együtt) 3 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. Mutassuk meg, hogy végtelen sok olyan pozitív egész n szám létezik, amelyre 2011^n-1 osztható n-nel!

* * * * *

Olyan n egészeket keresünk, amelyekre $2011^n\equiv 1 \pmod{n}$. (1 pont)
Legyen n 2-hatvány, vagyis $n=2^k$ valamely $k\geq 1$-re. (2 pont)
Ekkor $\varphi(n)=2^k-2^{k-1}=2^{k-1}$. (1 pont)
Mivel 2011 páratlan, $(n,2011)=1$, (1 pont)
ezért az Euler-Fermat tétel miatt $2011^{2^{k-1}}\equiv 1 \pmod{n}$. (2 pont)
Ezt négyzetre emelve: $2011^{2^k}=2011^n\equiv 1 \pmod{n}$. (2 pont)
Tehát mutattunk végtelen sok olyan pozitív egészt (a 2-hatványokat), amelyekre az állítás igaz. (1 pont)
Megjegyezzük, hogy a fenti megoldás azon múlik, hogy n-et 2-hatványnak választjuk. Azonban erre rájönni nem nehéz: ha az Euler-Fermat tételből nyert kongruenciát hatványozva akarunk eljutni a feladatbeli $2011^n\equiv 1 \pmod{n}$ állításhoz, akkor ebből a $\varphi(n)\big|n$ feltételhez jutunk. A $\varphi(n)$ képletéből pedig nem nehéz észrevenni, hogy ez a 2-hatványokra teljesül. (Egyébként $\varphi(n)\big|n$ a $2^k\cdot 3^l$, $k\geq 1$, $l\geq 0$ alakú számokra igaz, így a 2-hatványokon kívül is vannak megoldásai a feladatnak.)

5. Legyen $H = \{(a,b) : a,b \in \mathbb{R}, a \neq 0\}$ a nem az y-tengelyre eső síkvektorok halmaza. Értelmezzük H-n a $*$ műveletet a következőképpen:

$$(a,b) * (c,d) = (ac, ad + b)$$

Döntsük el, hogy H csoportot alkot-e $*$-ra nézve!

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

Az asszociativitás ellenőrzéséhez vegyünk három H-beli elemet: (a,b), (c,d), (e,f).
Ekkor $\big((a,b)*(c,d)\big)*(e,f) = (ac, ad+b)*(e,f) = (ace, acf + ad + b)$ és (1 pont)
$(a,b)*\big((c,d)*(e,f)\big) = (a,b)*(ce, cf+d) = (ace, a(cf+d)+b)$, (1 pont)
ami $acf + ad + b = a(cf+d)+b$ miatt az asszociativitást igazolja. (1 pont)
Van egységelem a $*$-ra nézve, mégpedig az $(1,0)$, (1 pont)
ugyanis $(a,b)*(1,0) = (a\cdot 1, a\cdot 0 + b) = (a,b)$ (1 pont)
és $(1,0)*(a,b) = (1\cdot a, 1\cdot b + 0) = (a,b)$. (1 pont)
A tetszőleges (a,b) elemnek $(\frac{1}{a}, -\frac{b}{a}) \in H$ inverze lesz, (1 pont)
mert $(a,b)*(\frac{1}{a}, -\frac{b}{a}) = (1, -b+b) = (1,0)$ (1 pont)
és $(\frac{1}{a}, -\frac{b}{a})*(a,b) = (1, \frac{b}{a} - \frac{b}{a}) = (1,0)$. (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 nem csoport). Megjegyezzük, hogy a feladatbeli H zárt $*$-ra, hiszen $(a,b) \in H$ és $(c,d) \in H$ esetén $a \neq 0$, $c \neq 0$, így $ac \neq 0$, vagyis $(ac, ad+b) \in H$. Azonban H zártságát a feladat szövege is állítja, amikor $*$-ot műveletnek nevezi. Ezért ennek ellenőrzéséért nem jár külön pont.

6. Bizonyítsuk be, hogy 50 elemű Abel-csoportban nem létezhet két olyan, egymástól és az egységelemtől különböző elem, amelyeknek a négyzete egyaránt az egységelem!

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

Tegyük fel indirekt, hogy $a^2 = e$ és $b^2 = e$ egy 50 elemű G Abel-csoport két különböző elemére, ahol e az egységelem és $a \neq e \neq b$ (és G műveletét szorzással jelöltük).
Legyen $c = a \cdot b$. Ekkor $c \neq a$, mert $a = a \cdot b$-ből balról a^{-1}-zel szorzással $e = b$ következne.
Hasonlóan, $c \neq b$. (1 pont)
Legyen $H = \{a, b, c, e\}$. Állítjuk, hogy H részcsoportja G-nek; ez viszont a Lagrange-tétel miatt ellentmondás (hiszen $4 \nmid 50$), amiből a feladat állítása következik. (3 pont)
H zárt az inverzképzésre: $c^2 = (ab)^2 = a^2 b^2 = e \cdot e = e$ miatt $c^{-1} = c$ és hasonlóan $a^{-1} = a$ és $b^{-1} = b$ (és $e^{-1} = e$). (2 pont)
H zárt a szorzásra is. Ez e-vel szorzásra nyilván igaz, $x^2 = e \in H$ minden $x \in H$-ra fennáll, $ab = c$ definíció szerint, így (felhasználva a művelet kommutativitását is) elég az ac és bc szorzatokat ellenőrizni. Ebből $ac = a(ab) = a^2 b = eb = b$ és $bc = b(ab) = ab^2 = ae = a$, ami a zártságot valóban mutatja. (3 pont)
Mivel pedig H zárt a műveletre és az inverzképzésre, ezért valóban részcsoport. (1 pont)