Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató az **Második** pótzhhoz
2009. december 3.

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. Legyen G k-szorosan élösszefüggő egyszerű, legalább két csúcsú irányítatlan gráf. Készítsük el a G_1 gráfot úgy, hogy lerajzoljuk G-t két példányban, felveszünk egy új csúcsot és ezt összekötjük mindkét G gráf-példány minden csúcsával. (Tehát így egy n csúcsú, e élű G gráfból kaptunk egy $2n+1$ csúcsú, $2e+2n$ élű G_1 gráfot.) Bizonyítsuk be, hogy G_1 $(k+1)$-szeresen élösszefüggő!

* * * * *

Vegyük észre, hogy ha G k-szorosan élösszefüggő volt, akkor G-ben van legalább $k+1$ csúcs, (1 pont)
mert $k=1$ esetben ez a feltételben benne van, $k \geq 2$ esetben pedig ha G-nek legfeljebb k csúcsa lenne, akkor egy csúcsának fokszáma maximum $k-1$ lehetne, de akkor ezen csúcs összes (az egyszerű gráfság miatt legfeljebb $k-1$) élét elhagyva a csúcs izoláltá válna, azaz G szétesne, tehát G nem lenne k-szorosan élösszefüggő. (2 pont)
A feladat megoldásához azt kell megmutatnunk, hogy akárhogyan hagyok el $k+1$-nél kevesebb élet G_1-ből, a gráf nem esik szét. (1 pont)
Hagyjunk el legfeljebb k élet G_1-ból és nézzük meg, hogy mi történik. Ha az összes elhagyott él egy G példányon belül volt, akkor a másik G-példányból és a új csúcsból álló rész biztosan összefüggő marad (hiszen onnan nem hagytam el semmit). (1 pont)
Ehhez a komponenshez kapcsolódik a megritkított G-példány minden csúcsa is, az új csúcshoz vezető éleken át, ezért ebben az esetben G_1 összefüggő marad. (2 pont)
Ha nem igaz, hogy az elhagyott élek mindegyike benne volt az egyik G-példányban, akkor mindkét G-példány összefüggő marad, (1 pont)
mert ekkor mindegyik G-ből legfeljebb $k-1$ élet hagytam le és G k-szorosan élösszefüggő volt.(1 pont)
Maradt továbbá legalább egy-egy él mindkét G-ből az új csúcsba, hiszen eredetileg az új csúcsból mindkét példányba legalább $k+1$ él futott. Így az új csúcs és a két maradék G-példány egy komponensben lesz az élelhagyás után. (1 pont)

2. a) Hány 71-nél kisebb, pozitív egész x szám van, melyre

$$30x \equiv 20 \pmod{35}?$$

b) Adja meg a fenti kongruencia legnagyobb kétjegyű megoldását!

* * * * *

(a) A tanult tétel szerint a lineáris kongruenciának $(30, 35) = 5 \mid 20$ miatt 5 megoldása van modulo 35, (1 pont)
azaz az $1, 2, \ldots, 70$ számok között pontosan 10. (2 pont)
(b) Oldjuk meg a kongruenciát! A feladatbeli lineáris kongruencia pontosan akkor áll fenn, ha $6x \equiv 4 \pmod{7}$ (osztottunk 5-tel, a modulust is). (2 pont)
Ez pontosan akkor igaz, ha $3x \equiv 2 \pmod{7}$ (osztottunk 2-vel). (1 pont)
Ez pontosan akkor igaz, ha $3x \equiv 9 \pmod{7}$ (2 helyére a vele azonos maradékosztályban levő 9-t írva). (1 pont)
Ez pedig pontosan az $x \equiv 3 \pmod{7}$ esetben igaz (osztottunk 3-mal). (1 pont)
A legnagyobb $7k + 3$ alakú kétjegyű szám pedig a 94. (2 pont)

3. A Télapó narancsot csomagol, 100 darab kerül mindegyik zsákba, kivéve az utolsóba, azt már nem tudja teljesen megtölteni. Mennyi jut ebbe az utolsó zsákba, ha összesen $41^{39^{38}}$ darab narancsa volt?

* * * * *

A feladat megoldásához azt kell meghatároznunk, hogy milyen maradékot ad $41^{39^{38}}$ 100-zal osztva, (1 pont)
Mivel 41 és 100 relatív prímek, (1 pont)
ezért az Euler-Fermat tétel értelmében $41^{\varphi(100)} \equiv 1 \pmod{100}$. (1 pont)
$\varphi(100) = \varphi(2^2 \cdot 5^2) = (4-2)(25-5) = 40$, tehát $41^{40} \equiv 1 \pmod{100}$. (1 pont)
Az a kérdés tehát, hogy 39^{38} mennyi maradékot ad 40-nel osztva. (2 pont)
$39^{38} \equiv (-1)^{38} \pmod{40}$ (39 helyére a vele kongruens -1-et írva). (1 pont)
Így kapjuk, hogy $39^{38} \equiv 1 \pmod{40}$, (1 pont)
vagyis $41^{39^{38}} = 41^{40 \cdot k + 1} = (41^{40})^k \cdot 41$ miatt (felhasználva, hogy $41^{40} \equiv 1 \pmod{100}$)
$41^{39^{38}} \equiv 41 \pmod{100}$. (2 pont)

4. Legyen b tetszőleges pozitív egész szám. Bizonyítsa be, hogy az $1 + kb$ ($k \geq 1$ egész szám) alakú számokból álló végtelen számtani sorozatban nem lehet minden szám prím.

* * * * *

Tegyük fel, hogy $1 + b$ és $1 + 2b$ is prím, $1 + b = p_1$ és $1 + 2b = p_2$. (3 pont)
Tekintsük a $p_1 \cdot p_2 = (1 + b)(1 + 2b)$ számot, ez összetett. (3 pont)
De $(1 + b)(1 + 2b) = 1 + 3b + 2b^2 = 1 + (3 + 2b)b$ szintén egy tag a számtani sorozatban $k = 3 + 2b$ esetén, (3 pont)
vagyis a számtani sorozat tartalmaz összetett számot. (1 pont)

5. Tudjuk, hogy G csoport a $*$ műveletre nézve. Tekintsük az alábbi H halmazt:
$H = \{(g, 0), (g, 1) \mid g \in G\}$ (vagyis H elemei olyan párok, melyek első tagja egy G-beli elem, második tagja pedig 0 vagy 1) és értelmezzük H-n az alábbi függvényt:
$(g_1, i) \diamond (g_2, j) = (g_1 * g_2, i + j \mod 2)$. (Itt $i + j \mod 2$ az i és j összegének 2-vel vett osztási maradékát

jelöli.)
Bizonyítsa be, hogy H csoport a $\diamond$ függvénnyel.

* * * * *

A $\diamond$ függvény művelet H-n, mert az eredmény első komponense (G $*$-ra való zártsága miatt) G-beli, a második komponens pedig 0 vagy 1 lesz mindig. (2 pont)
A $\diamond$ művelet asszociatív, mert $((g_1,i)\diamond(g_2,j))\diamond(g_3,k) = (g_1 * g_2, i+j \mod 2)\diamond(g_3,k) = ((g_1*g_2)*g_3, i+j+k \mod 2)$, (1 pont)
míg $(g_1,i)\diamond((g_2,j)\diamond(g_3,k)) = (g_1,i)\diamond(g_2*g_3, j+k \mod 2) = (g_1*(g_2*g_3), i+j+k \mod 2)$ (1 pont)
és a fenti két dolog megegyezik, mert a $*$ asszociatív művelet G-n. (1 pont)
Van egységelem is, az $(e,0)$ pár, ahol e G egységelemét jelöli: $(e,0)\diamond(g,i) = (e*g, 0+i \mod 2) = (g,i)$, mert e G-beli egységelem $*$-ra nézve. (2 pont)
Hasonlóan $(g,i)\diamond(e,0) = (g*e, i+0 \mod 2) = (g,i)$ (1 pont)
Van inverz is: (g,i) inverze (g^{-1},i), ahol g^{-1} a g G-beli inverze (1 pont)
mert ekkor $(g,i)\diamond(g^{-1},i) = (g*g^{-1},0) = (e,0)$ és $(g^{-1},i)\diamond(g^{-1},i) = (g^{-1}*g,0) = (e,0)$. (1 pont)

6. Az S halmazon értelmezett $*$ művelet olyan, hogy
(i) S-ben van egységelem $*$-ra nézve és
(ii) tetszőleges (nem feltétlenül különböző) $a,b,c \in S$ elemekre fennáll hogy $a*(b*c) = b*(a*c)$.
Bizonyítsa be, hogy ekkor
(a) $*$ kommutatív, (b) $*$ asszociatív.

* * * * *

a) c helyébe az egységelemet, e-t, írva kapjuk, hogy $a*(b*e) = b*(a*e)$. (2 pont)
Másrészt $a*(b*e) = a*b$ és $b*(a*e) = b*a$ az e tulajdonságai miatt, vagyis $a*b = b*a$. (2 pont)
(b) Be kéne látni, hogy $x*(y*z) = (x*y)*z$ tetszőleges $x,y,z \in S$ elemekre fennáll. (2 pont)
De $x*(y*z) = x*(z*y)$ a $*$ művelet most belátott kommutativitása miatt, (1 pont)
$x*(z*y) = z*(x*y)$ igaz a feladatbeli (ii) tulajdonság miatt $x=a, z=b, y=c$ szereposztással (2 pont)
és $z*(x*y) = (x*y)*z$ is igaz (ismét $*$ kommutativitása miatt). (1 pont)