Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató
2013. április 25.

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 hurokélmentes, irányított gráf illeszkedési mátrixa. Adjuk meg a hiányzó (□-val jelölt) elemeket és rajzoljuk le a gráfot!

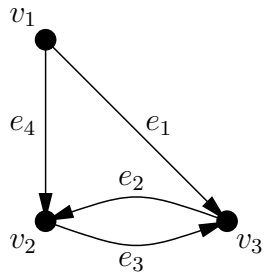
$$\begin{pmatrix} 1 & \square & 0 & 1 \\ 0 & -1 & \square & \square \\ \square & 1 & -1 & 0 \end{pmatrix}$$

* * * * *

Az illeszkedési mátrix definíciójából következik, hogy annak minden oszlopában 1 darab 1-es és 1 darab (-1)-es található, az összes többi elem 0. Ez alapján már a mátrix minden hiányzó eleme megállapítható:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & -1 \\ -1 & 1 & -1 & 0 \end{pmatrix} \qquad \text{(5 pont)}$$

A mátrix ismeretében pedig a gráf már (definíció szerint) rekonstruálható: ha v_1, v_2, illetve v_3 jelöli sorban lefelé haladva a mátrix sorainak megfelelő csúcsokat és hasonlóan $e_1, \ldots, e_4$ az oszlopoknak megfelelő éleket, akkor az alábbi gráfot kapjuk:



(5 pont)

Ha egy megoldó felcseréli a mátrixbeli 1-esek és (-1)-esek szerepét (és így a fenti ábrához képest minden élt fordítva rajzol), az ezért 1 pontot veszítsen.

2. A legalább négy pontú G gráf bármely két, nemszomszédos pontja között található G-ben három, páronként éldiszjunkt út. Mutassuk meg, hogy G-nek bármely két szomszédos pontja között is található három, páronként éldiszjunkt út!

* * * * *

Legyenek s és t szomszédos pontjai G-nek és tegyük fel indirekt, hogy ezek között nem létezik három, páronként éldiszjunkt út G-ben. Ekkor Menger megfelelő (irányítatlan gráfbeli éldiszjunkt utakra vonatkozó) tétele szerint kell legyen G-ben két olyan él – jelölje ezeket e_1 és e_2 – amelyek az összes, s és t közötti utat lefogják. (Megjegyezzük, hogy e_1 és e_2 egyike nyilván az s és t közötti él kell legyen – de ez a megoldás szempontjából közömbös.) (2 pont)
Ekkor az e_1 és e_2 elhagyásával kapott G' gráf már nem összefüggő, így a csúcsai szétoszthatók a V_1 és V_2 nemüres halmazokra úgy, hogy G'-nek nincs V_1-beli csúcsot V_2-belivel összekötő éle.(2 pont)
Ha most $v_1 \in V_1$ és $v_2 \in V_2$ tetszőlegesek, akkor nyilván nem lehet v_1 és v_2 között három, páronként éldiszjunkt út G-ben, mert e_1 és e_2 a v_1 és v_2 közötti utakat is lefogják. (2 pont)
Ezért (a feladat feltétele szerint) v_1-nek és v_2-nek szomszédosaknak kell lenniük G-ben. (2 pont)
Mivel ez bármely $v_1 \in V_1$ és $v_2 \in V_2$ csúcspárról elmondható, ezért G-ben legalább $|V_1| \cdot |V_2|$ olyan élnek kell lenni, ami V_1-beli csúcsot köt össze V_2-belivel. Ez azonban ellentmondás: egyrészt $|V_1| + |V_2| \geq 4$ miatt $|V_1| \cdot |V_2| \geq 3$, másrészt V_1 és V_2 között G-ben csak az e_1 és e_2 élek mehetnek. Ez az ellentmondás bizonyítja a feladat állítását. (2 pont)

3. Egy egész szám 222-vel vett osztási maradéka 4-gyel kisebb, mint a szám 60-szorosának a 222-vel vett osztási maradéka. Milyen maradékot adhat ez a szám 222-vel osztva?

* * * * *

A keresett számot n-nel jelölve a feladat szövege szerint $n \equiv 60n - 4 \pmod{222}$. (1 pont)
Átrendezve az $59n \equiv 4 \pmod{222}$ lineáris kongruenciát kapjuk. (1 pont)
4-gyel szorozva: $236n \equiv 16 \pmod{222}$, vagyis $14n \equiv 16 \pmod{222}$. (1 pont)
2-vel osztva: $7n \equiv 8 \pmod{111}$, ahol $(2, 222) = 2$ miatt kellett a modulust 2-vel osztani.(1 pont)
16-tal szorozva: $112n \equiv 128 \pmod{111}$, vagyis $n \equiv 17 \pmod{111}$. (2 pont)
Ebből $n \equiv 17 \pmod{222}$ vagy $n \equiv 17 + 111 = 128 \pmod{222}$. (1 pont)
Ellenőrzéssel kiderül, hogy a 17 hamis gyök (ami a 4-gyel szorzás miatt jött be, ami nem ekvivalens lépés, mert $(222, 4) > 1$). Így a megoldás $n \equiv 128 \pmod{222}$ (vagyis a kérdéses szám 128 maradékot adhat 222-vel osztva). (3 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 $(59, 222)|4$, így a kongruenciának van megoldása, de a megoldást kiszámolni nem tudja, az (az átrendezéssel együtt) összesen 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. Egy n egész szám 3 maradékot ad 82-vel osztva. Milyen maradékot adhat az n szám 182-vel osztva?

* * * * *

A feladat azt kérdezi, hogy az $n \equiv 3 \pmod{82}$, $n \equiv a \pmod{182}$ kongruenciarendszernek milyen $a \in \{0, 1, \ldots, 181\}$ értékekre van megoldása. (2 pont)
Az első kongruenciából $n = 82k + 3$ valamilyen $k \in \mathbb{Z}$ esetén. (1 pont)
Ezt a másodikba helyettesítve: $82k + 3 \equiv a \pmod{182}$. (1 pont)
Átrendezés után a $82k \equiv a - 3 \pmod{182}$ lineáris kongruenciára jutunk. (1 pont)
A tanult tétel szerint ez pontosan akkor megoldható, ha $(82, 182)|a - 3$. (2 pont)
Mivel $(82, 182) = 2$, ezért ez azzal ekvivalens, hogy $2|a - 3$, vagyis hogy a páratlan szám.(1 pont)
Tehát n bármilyen páratlan maradékot $(1, 3, 5, \ldots, 181)$ adhat maradékul 182-vel osztva.(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. Hány olyan n egész szám van 1 és 100 között, amelyre $(n+51!)^{52}-1$ osztható 53-mal?

* * * * *

Mivel 53 prím, ezért Wilson tétele szerint $52! \equiv -1 \pmod{53}$, (1 pont)
vagyis $52! \equiv 52 \pmod{53}$. (1 pont)
Ezt 52-vel osztva: $51! \equiv 1 \pmod{53}$, ahol a modulus $(52, 53) = 1$ miatt nem változott. (1 pont)
Mindkét oldalhoz n-et adva, majd 52-edik hatványra emelve:

$$(n+51!)^{52} \equiv (n+1)^{52} \pmod{53}.$$ (1 pont)

Mivel 53 prím, ezért $\varphi(53) = 52$, (1 pont)
így az Euler-Fermat tétel miatt $a^{52} \equiv 1 \pmod{53}$ teljesül minden 53-hoz relatív prím, vagyis 53-mal nem osztható a-ra. (1 pont)
Összevetve az eddigieket: ha $n+1$ nem osztható 53-mal, akkor

$$(n+51!)^{52} \equiv (n+1)^{52} \equiv 1 \pmod{53},$$

vagyis $(n+51!)^{52}-1$ osztható 53-mal. (2 pont)
Ha viszont $n+1$ osztható 53-mal, akkor nyilván $(n+1)^{52}$ is osztható 53-mal, így a fentiek szerint $(n+51!)^{52}$ is. Ezért ilyenkor $(n+51!)^{52}-1$ nem osztható 53-mal. (1 pont)
Következésképp 1 és 100 között 99 darab olyan n van, amelyre $(n+51!)^{52}-1$ osztható 53-mal: az 52 kivételével mindegyik. (1 pont)
Ha egy megoldó elfelejtkezik az Euler-Fermat tétel feltételéről (miszerint $(a, 53) = 1$) és ezért arra jut, hogy az állítás minden n-re teljesül, az (ha egyébként a megoldás hibátlan) ezért 2 pontot veszítsen (a fenti pontozás szerinti 6. és 8. részpontokat).

6. Legyen $H = \{a, b, c, d, p, q, r, s\}$ és értelmezzük a H halmazon a $*$ műveletet az alábbi műveleti tábla szerint:

$*$	a	b	c	d	p	q	r	s
a	b	q	d	r	a	p	s	c
b	q	p	r	s	b	a	c	d
c	s	r	b	a	c	d	p	q
d	c	s	q	b	d	r	a	p
p	a	b	c	d	p	q	r	s
q	p	a	s	c	q	b	d	r
r	d	c	p	q	r	s	b	a
s	r	d	a	p	s	c	q	b

(A műveleti tábla használata magától értetődő: az $x * y$ művelet eredménye az x-nek megfelelő sor és az y-nak megfelelő oszlop kereszteződésében található. Így például $q * c = s$ és $b * q = a$.)
Döntsük el, hogy a H halmaz csoportot, illetve Abel-csoportot alkot-e a $*$ műveletre nézve, ha azt már tudjuk, hogy $*$ asszociatív! (Az asszociativitást tehát nem kell ellenőrizni.)

* * * * *

A műveleti táblából látszik, hogy $*$-ra nézve p egységelem, mert $x * p = p * x = x$ minden $x \in H$ elemre igaz. (2 pont)
Ezért a inverze q (és viszont), mert $a * q = q * a = p$. Hasonlóan látszik, hogy c és r egymás inverzei, d és s is egymás inverzei és b és p sajátmaguk inverzei. (3 pont)
Mivel a művelet asszociatív, van egységelem és minden elemnek van inverze, ezért $(H, *)$ csoport. (2 pont)
Viszont $*$ nem kommutatív: például $a * c = d$, de $c * a = s$. Így $(H, *)$ nem Abel-csoport. (3 pont)