Bevezetés a számításelméletbe II.

Zárthelyi feladatok — az MÁSODIK zárthelyi pótlására

Pontozási útmutató

2012. május 7.

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 100 csúcsú G egyszerű gráfban minden pont foka legalább 2. A G gráffal gondolatban a következő kísérletet végezzük: az összes lehetséges módon kiválasztunk G csúcsai közül két különbözőt és a kiválasztott csúcsokat elhagyjuk G-ből. Azt kapjuk, hogy a kísérletek közül 98 esetben a maradék gráf nem összefüggő, de az összes többi esetben igen. Határozzuk meg a legnagyobb k számot, amelyre G k-szorosan összefüggő.

* * * * *

Mivel létezik két olyan csúcs, melyet elhagyva a gráf már nem összefüggő, G nem háromszorosan összefüggő, azaz k legfeljebb 2 lehet. (2 pont)

Megmutatjuk, hogy $k = 2$. Tegyük fel indirekten, hogy ez nem így van, azaz létezik olyan a csúcs, melyet elhagyva a gráf nem összefüggő. (Mivel a gráfnak kettőnél több csúcsa van, tényleg léteznie kell ilyen a-nak, de ezen megállapítás hiányáért ne vonjunk le pontot.) (1 pont)

Legyenek a gráf többi csúcsai $v_1, v_2, \dots, v_{99}$. Ha a gráf a-t elhagyva szétesik, akkor mindegyik komponensében legalább két pont lesz, ellenkező esetben lenne olyan csúcs, ami csak a-val volt összekötve, ami ellentmond a feltételeknek (minden fok legalább 2, G egyszerű). (2 pont)

Így $G - a$ bármely csúcsát elhagyva olyan gráfot kapunk, ami nem összefüggő, (1 pont)

azaz G-ből az (a, v_i) (minden $1 \le i \le 99$ esetén) párok bármelyikét elhagyva nem összefüggő gráfot kapunk, (3 pont)

ami ellentmondás, hiszen csak 98 ilyen pár létezik a gráfban. (1 pont)

Érdemes megjegyezni, hogy a feltételnek megfelelő gráf csakugyan létezik, például ilyen lesz az a gráf, amit egy 99 csúcsú útból úgy kapunk, hogy az egyik nem szélső csúcs kivételével minden csúcsot összekötünk egy új csúccsal.

2. Egy G egyszerű gráf minden csúcsában lakik egy bogárka. Egy adott pillanatban minden bogárka felkerekedik és átköltözik a gráf egy, a jelenlegi lakhelyével szomszédos csúcsába. A bogárkák ezt úgy szeretnék megtenni, hogy végül ismét minden csúcsban egyetlen bogárka lakjon. Bizonyítsd be, hogy ha G szomszédossági mátrixának a determinánsa nem nulla, akkor a bogárkák terve megvalósítható!

* * * * *

Címkézzük a G csúcsait az $1, 2, \ldots, n$ számokkal és jelölje G szomszédossági mátrixát A (amelynek az i-edik sora és oszlopa az i-vel címkézett csúcsnak felel meg minden $1 \leq i \leq n$ esetén).
A $\det A \neq 0$ feltételből a determináns definíciója szerint következik, hogy létezik az $1, 2, \ldots, n$ számoknak egy olyan $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ permutációja, amelyre az A mátrix i-edik sorának és π_i-edik oszlopának kereszteződésében álló elem 1-es minden $1 \leq i \leq n$ esetén. Ellenkező esetben ugyanis a $\det A$ definíció szerinti kiszámításakor keletkező mind az $n!$ darab tag 0 volna, így $\det A$ is 0 lenne. (Mivel G egyszerű, ezért A minden eleme 0 vagy 1.) (3 pont)
A π permutációt felhasználva a bogárkák megvalósíthatják a tervüket: minden $1 \leq i \leq n$ esetén költözzön az i csúcsban lakó bogárka a π_i csúcsba. (4 pont)
Valóban: minden bogárka szomszédos csúcsba költözik (hiszen a mátrix megfelelő elemei 1-esek) és a költözések után is minden csúcsban egyetlen bogárka lakik (hiszen a $\pi_1, \pi_2, \ldots, \pi_n$ értékek között minden 1 és n közötti szám pontosan egyszer fordul elő, mert π permutáció). (3 pont)
Megjegyezzük, hogy a bogárkák tervének megvalósíthatósága megfogalmazható úgy is, hogy G-ben megadható néhány él és néhány kör úgy, hogy G minden csúcsa pontosan egyre illeszkedik a megadott élek és körök közül. (Valóban: minden bogárka vagy „lakást cserél” valamelyik szomszédjával, vagy részt vesz egy legalább három bogárka által alkotott körbeköltözési láncban.) Bár ez a felismerés a feladat megoldásához közvetlenül nem visz közelebb, de tekinthető a helyes megoldás irányába tett érdemi lépésnek, így a leírásáért legföljebb 3 pont adható.

3. Milyen maradékot ad 5^{73}-nal osztva $16^{5^{73}}$?

* * * * *

$\varphi(5^{73}) = 5^{73} - 5^{72}$ (a tanult képlet szerint). (1 pont)
Mivel 2 és 5^{73} relatív prímek (hiszen a prímtényezős felbontásukban nincs közös prím), (1 pont)
ezért alkalmazható rájuk az Euler-Fermat tétel: $2^{\varphi(5^{73})} = 2^{5^{73} - 5^{72}} \equiv 1 \pmod{5^{73}}$. (2 pont)
Ebből $5^{73} - 5^{72} = 4 \cdot 5^{72}$ figyelembevételével: $2^{4 \cdot 5^{72}} \equiv 1 \pmod{5^{73}}$, (2 pont)
amiből $16 = 2^4$ miatt $16^{5^{72}} \equiv 1 \pmod{5^{73}}$. (1 pont)
Ötödik hatványra emelve: $16^{5 \cdot 5^{72}} = 16^{5^{73}} \equiv 1 \pmod{5^{73}}$ (vagyis a keresett maradék: 1).(3 pont)
Aki nem jön rá, hogy az Euler-Fermat tételt 2-re (és 5^{73}-ra) érdemes alkalmazni, de 16-ra (és 5^{73}-ra) alkalmazza (helyesen), az a fenti pontozásbeli első 4 pontot megkaphatja.

4. Egy egész szám 199-cel vett osztási maradéka 1-gyel nagyobb, mint a szám 43-szorosának a 199-cel vett osztási maradéka. Milyen maradékot adhat ez a szám 199-cel osztva?

* * * * *

A feladat az $n - 1 \equiv 43n \pmod{199}$ kongruencia megoldása. (1 pont)
Rendezve: $42n \equiv -1 \pmod{199}$, (1 pont)
5-tel szorozva: $210n \equiv -5 \pmod{199}$, vagyis $11n \equiv -5 \pmod{199}$. (2 pont)
18-cal szorozva: $198n \equiv -90 \pmod{199}$, (3 pont)
vagyis $-n \equiv -90 \pmod{199}$, azaz $n \equiv 90 \pmod{199}$. (1 pont)
Mivel $(5, 199) = 1$ és $(18, 199) = 1$, a két szorzás ekvivalens lépés, ezért a megoldás $n \equiv 90 \pmod{199}$, vagyis a keresett maradék csak 90 lehet. (2 pont)
Ha valaki csak azt ellenőrzi, hogy $(42, 199) = 1|1$, így a kongruenciának van megoldása, de a megoldást kiszámolni nem tudja, az összesen 2 pontot kapjon. A megtett lépések ekvivalens voltára való hivatkozás helyett ellenőrzéssel is meg lehet győződni a kapott megoldás helyességéről vagy lehet hivatkozni arra is, hogy $(42, 199) = 1$ miatt egyetlen helyes megoldás létezik $\pmod{199}$, így a kapott megoldás helyes. Számolási hibákért 1-1 pontot vonjunk le, de a maradék pontszám csak akkor jár, ha a hiba miatt a feladat nem lett lényegesen könnyebb.

5. Hány olyan n egész szám van 1 és 1000 között, amelyhez található olyan m egész szám, hogy a $37n + 218m = 10$ egyenlet fennálljon?

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

Egy n egészhez akkor és csak akkor létezik a $37n + 218m = 10$ egyenletet kielégítő m egész, ha $10 - 37n$ osztható 218-cal, vagyis ha $37n \equiv 10 \pmod{218}$. A kérdés tehát az, hogy ennek a lineáris kongruenciának hány megoldása van 1 és 1000 között. (3 pont)
A kongruenciát 6-tal szorozva $222n \equiv 60 \pmod{218}$, vagyis $4n \equiv 60 \pmod{218}$. (1 pont)
Ezt 4-gyel osztva $n \equiv 15 \pmod{109}$, hiszen 218 és 4 legnagyobb közös osztója 2, amivel a modulust el kell osztani. (1 pont)
Modulo 218 tehát két megoldást kapunk, melyek 15 és $15 + 109 = 124$. (1 pont)
Mivel a 6-tal való szorzás nem ekvivalens átalakítás, az eredményeket vissza kell helyettesíteni az eredeti kongruenciába, hogy kiszűrjük a hamis gyököt: $37 \cdot 15 = 555$, ami nem kongruens 10-zel modulo 218, $37 \cdot 124 = 37 \cdot 4 \cdot 31 = 148 \cdot 31$, ami $-70 \cdot 31$-gyel, azaz -2170-nel kongruens modulo 218, erről pedig (2180-at hozzáadva) látható, hogy csakugyan kongruens 10-zel modulo 218, a megoldás tehát a 124 (mod 218). A két ellenőrzés közül az egyik kiváltható azzal a megállapítással, hogy mivel 37 és 218 relatív prímek, a kongruenciának pontosan egy megoldása lesz modulo 218. (2 pont)
Az n számnak tehát $218k + 124$ alakúnak kell lennie, ahol k egész. (1 pont)
Ahhoz, hogy n 1 és 1000 között legyen, k-nak 0 és $\frac{1000-124}{218}$ közé kell esnie, azaz 5 ilyen egész n lesz. (1 pont)

6. Értelmezzük a síkvektorok $\mathbb{R}^2$ halmazán a $*$ és a $\diamond$ műveleteket a következőképpen:

$$(a, b) * (c, d) = (a + d, bc) \qquad\qquad (a, b) \diamond (c, d) = (a + c, bd)$$

a) Döntsük el, hogy $\mathbb{R}^2$ csoportot alkot-e $*$-ra nézve!
b) Döntsük el, hogy $\mathbb{R}^2$ csoportot alkot-e $\diamond$-ra nézve!

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

Vizsgáljuk először $*$ asszociativitását. $((a, b) * (c, d)) * (e, f) = (a + d, bc) * (e, f) = (a + d + f, bce)$, míg $(a, b) * ((c, d) * (e, f)) = (a, b) * (c + f, de) = (a + de, bc + bf)$. (1 pont)
Mivel a két kapott eredmény nem feltétlenül egyenlő (pl. $a = 0, d = 0, f = 1$ esetén), a művelet nem asszociatív, (1 pont)
így a kérdéses struktúra nem csoport. (1 pont)
A b) feladatbeli struktúrának a $(0, 1)$ vektor egységeleme lesz, hiszen $(0, 1) \diamond (a, b) = (a, b)$ (2 pont)
és könnyen látható, hogy a $\diamond$ művelet kommutatív (e megállapítás helyett természetesen lehet a másik irányból is megvizsgálni a feltétel teljesülését). (1 pont)
Mivel $(0, 0) \diamond (a, b) = (a, 0)$, (1 pont)
a (0,0) elemnek nincs inverze, (2 pont)
a kérdéses struktúra tehát nem csoport. (1 pont)
Az utolsó 1 pontok annak járnak, aki a korábbi számolásaiból helyes következtetést von le. Az a) feladatban természetesen annak is járnak a megfelelő pontok, aki másképp mutatja meg, hogy a struktúra nem csoport, pl. mert nem létezik egységelem. A b) feladatban nem szükséges az asszociativitást vizsgálni, hiszen anélkül is látható, hogy nem csoportról van szó. Ha valaki ezt mégis megteszi, akkor kaphat 2 pontot a (helyes) vizsgálatért, azzal a megkötéssel, hogy ha nem mutatta meg, hogy nem létezik minden elemnek inverze, akkor (a b) feladatra) legfeljebb 4 pontot kaphat. Nem kell pontot levonni attól, aki nem ellenőrzi, hogy az egységelem csakugyan a halmazban van-e, mivel ez esetünkben magától értetődő. Végül megjegyezzük, hogy $*$ és $\diamond$ csakugyan művelet $\mathbb{R}^2$-en, ennek ellenőrzéséért azonban nem jár külön pont (hiszen ezt a feladat szövege is kimondja).