Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató
2013. november 29.

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 lenne 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. Tegyük fel, hogy a 100 csúcsú G (egyszerű) gráf szomszédossági mátrixának 2013-adik hatványának legalább 9900 pozitív eleme van.

a) Lehet-e G-nek izolált csúcsa?

b) Lehet-e G összefüggő?

* * * * *

A tanult tétel szerint a szomszédossági mátrix 2013-adik hatványában az i-edik sor j-edik eleme egyenlő a G-ben i-ből j-be vezető 2013 hosszú élsorozatok számával. (3 pont)

a) Így, ha lenne G-nek izolált csúcsa, akkor a szomszédossági mátrix összes hatványában (speciálisan a 2013-adikban is) az ő sorában és az ő oszlopában minden elemnek 0-nak kellene lennie. (2 pont)

Tehát lenne a mátrixban legalább 199 db 0, viszont a feltétel szerint $100^2 - 9900 = 100$ elem kivételével mindegyik pozitív, és így G-nek nem lehet izolált csúcsa. (2 pont)

b) Ha pl. a $G = K_{100}$ gráfból indulunk ki, akkor bármely két (esetleg egyező) csúcs között van 2013 hosszú élsorozat, így a szomszédossági mátrix 100-adik hatványának mind a 10000 eleme pozitív lesz. Tehát elképzelhető, hogy G összefüggő. (3 pont)

Megjegyzés. Nem nehéz azt sem belátni, hogy G biztosan összefüggő, hiszen, ha szét lehetne osztani a csúcsait 2 részre úgy, hogy az egyikben k, a másikban $100 - k$ csúcs van, és a két rész között nem fut él, akkor az egyik részből a másikba semmilyen élsorozat nem vezetne, és így legalább $2k(n-k) \geq 2 \cdot 99 > 100$ db 0 szerepelne a szomszédossági mátrix összes hatványában.

2. Hány olyan szám van $1, 2, \ldots, 1000$ között, ami 8-cal osztva 7, 12-vel osztva pedig 11 maradékot ad?

* * * * *

I. megoldás. Az a szám pontosan akkor ad 8-cal osztva 7, 12-vel osztva 11 maradékot, ha az $a+1$ szám osztható 8-cal és 12-vel is. (4 pont)

Egy szám pontosan akkor osztható 8-cal és 12-vel is, ha a legkisebb közös többszörösükkel, azaz 24-gyel is osztható. (3 pont)

Tehát az a kérdés, hogy a $2, 3, \ldots, 1001$ számok között hány 24-gyel osztható van, vagyis, hogy hány olyan k egész szám van, amelyre $2 \leq 24k \leq 1001$. Ez pontosan akkor teljesül, ha a k egész számra

$1 \le k \le 41 = \lfloor 1001/24 \rfloor$. Tehát 41 ilyen szám van. (3 pont)

II. megoldás. Az a egész szám pontosan akkor ad 8-cal osztva 7 maradékot, ha felírható $a = 8b + 7$ alakban, ahol b egész szám. Ehhez hasonlóan, pontosan akkor ad 11 maradékot 12-vel osztva, ha felírható $12c + 11$ alakban, ahol c egész szám. (2 pont)
Tehát $8b + 7 = 12c + 11$ egyenletnek is teljesülnie kell a b, c egész számokra. (1 pont)
Ezt az egyenletet modulo 12 nézve azt kapjuk, hogy $8b + 7 \equiv 11\ (12)$. (1 pont)
Mindkét oldalhoz 1-et adva a $8b + 8 \equiv 0\ (12)$ kongruenciát kapjuk, amit 8-cal leosztva $b + 1 \equiv 0\ (12/(12, 8))$, vagyis $b \equiv -1\ (3)$ adódik. Ez azt jelenti, hogy valamely B egész számra $b = 3B - 1$ teljesül, amiből c értékére $c = (8b - 4)/12 = 2B - 1$ adódik. (4 pont)
Tehát a feltételek pontosan akkor teljesülnek, ha $a = 8b + 7 = 12c + 11 = 24B - 1$ valamely B egész számra. (1 pont)
Az $1 \le a \le 1000$ feltételből $1 \le B \le 41$ adódik, tehát 41 ilyen szám van. (1 pont)

3. Milyen maradékot ad 38-cal osztva $383^{18^{38}}$?

* * * * *

Mivel $(38, 383) = 1$, ezért alkalmazható az Euler-Fermat tétel a feladatban szereplő hatványra. (2 pont)
Ehhez először számoljuk ki $\varphi(38)$ értékét: $\varphi(38) = \varphi(2 \cdot 19) = (2 - 1)(19 - 1) = 18$. (2 pont)
Így az Euler-Fermat tétel szerint

$$383^{18} \equiv 1\ (38),$$

(1 pont)

és ezt felhasználva

$$383^{18^{38}} = 383^{18 \cdot 18^{37}} = (383^{18})^{18^{37}} \equiv 1^{18^{37}} \equiv 1\ (38)$$

adódik. (4 pont)
Tehát a $383^{18^{38}}$ szám 38-cal osztva 1 maradékot ad. (1 pont)

4. Hány olyan szám van 1-től 1000-ig, amelynek pontosan 14 pozitív osztója van?

* * * * *

Tegyük fel, hogy $d(n) = 14$ és az n szám prímtényezős felbontása $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Ekkor $14 = (\alpha_1 + 1) \dots (\alpha_r + 1)$, itt a 14-et 1-nél nagyobb pozitív egész számok szorzataként írtuk fel. (2 pont)
Erre csak 2 lehetőség van: 14 (egy tényezős szorzat), illetve $2 \cdot 7$. (1 pont)
Az előbbi esetben $n = p^{13}$ alakú, ahol p prímszám, viszont a legkisebb prímszám 13-adik hatványa is nagyobb 1000-nél: $1000 < 2^{13} \le p^{13}$, így ebben az esetben nem kapunk megoldást. (2 pont)
Tehát csak a másik eset állhat fenn, és $n = p^6 q$ alakú, ahol p és q egymástól különböző (pozitív) prímszámok. Ha $p \ge 3$, akkor $n = p^6 q \ge 3^6 \cdot 2 > 1000$, azaz ekkor sem kapunk megoldást. Így csak $p = 2$ lehet, ekkor az $n = 2^6 \cdot q = 64q \le 1000$ feltételből $q < 16$-ot kapjuk, tehát q olyan prímszám lehet, ami 2-nél nagyobb, de 16-nál kisebb, azaz $q \in \{3, 5, 7, 11, 13\}$. (4 pont)
Tehát 5 ilyen szám van. (Ezek a számok: $2^6 \cdot 3$, $2^6 \cdot 5$, $2^6 \cdot 7$, $2^6 \cdot 11$, $2^6 \cdot 13$.) (1 pont)

5. Igazoljuk, hogy bármely a, b egész számra $a^{100}b^{20} - a^{20}b^{100}$ osztható 41-gyel.

* * * * *

I. megoldás Azt kell belátnunk, hogy $a^{100}b^{20} - a^{20}b^{100} = a^{20}b^{20}(a^{80} - b^{80})$ osztható 41-gyel. Ha a vagy b osztható 41-gyel, akkor ez nyilván teljesül. (2 pont)
Ha sem a, sem b nem osztható 41-gyel, akkor a kis Fermat-tétel szerint $a^{40} \equiv 1\ (41)$ és $b^{40} \equiv 1\ (41)$ is teljesül. (3 pont)

Ezeket a kongruenciákat négyzetre emelve és egymásból kivonva azt kapjuk, hogy $a^{80}-b^{80}\equiv 1^2-1^2\equiv 0\ (41)$, tehát $41|a^{80}-b^{80}$, és így $41|a^{100}b^{20}-a^{20}b^{100}$ ekkor is teljesül. (5 pont)
Megjegyzés. A kis Fermat-tétel másik alakját használva az esetszétválasztás is elkerülhető: $a^{41}\equiv a\ (41)$ és $b^{41}\equiv b\ (41)$ összefüggéseket használva:

$$a^{100}b^{20}-a^{20}b^{100}\equiv (a^{41})^2a^{18}b^{20}-a^{20}(b^{41})^2b^{18}\equiv a^2a^{18}b^{20}-a^{20}b^2b^{18}\equiv a^{20}b^{20}-a^{20}b^{20}\equiv 0\ (41)$$

II. megoldás (csak kicsit másképpen). Azt kell igazolni, hogy $a^{100}b^{20}\equiv a^{20}b^{100}\ (41)$. Osszuk le mindkét oldalt $a^{20}b^{20}$-nal, ez ekvivalens átalakítás, ha $(a^{20}b^{20},41)=1$, azaz, ha sem a, sem b nem osztható 41-gyel (hiszen a 41 prímszám). A kapott kongruencia: $a^{80}\equiv b^{80}\ (41)$. (3 pont)
Mivel $(a,41)=(b,41)=1$, ezért az Euler-Fermat tétel szerint $a^{40}\equiv b^{40}\equiv 1\ (41)$. Ezt a kongruenciát négyzetre emelve éppen az igazolni kívánt $a^{80}\equiv b^{80}\ (41)$ kongruenciát kapjuk. (5 pont)
Meg kell még vizsgálnunk azt az esetet, ha a vagy b osztható 41-gyel, de ekkor $a^{100}b^{20}\equiv a^{20}b^{100}\ (41)$ kongruencia mindkét oldala 0-val kongruens, így ekkor is teljesül. Ezzel igazoltuk az állítást. (2 pont)

6. A valós számok halmazán a $\circ$ műveletet a következőképpen definiáljuk:

$$a\circ b=ab+2a+2b+2.$$

Igaz-e, hogy $(\mathbb{R},\circ)$ félcsoport? Igaz-e, hogy $(\mathbb{R},\circ)$ csoport?

* * * * *

Mivel

$$(a\circ b)\circ c=(ab+2a+2b+2)\circ c=(ab+2a+2b+2)c+2(ab+2a+2b+2)+2c+2=\\ abc+2(ab+bc+ca)+4(a+b+c)+6$$

és

$$a\circ(b\circ c)=a\circ(bc+2b+2c+2)=a(bc+2b+2c+2)+2a+2(bc+2b+2c+2)+2=\\ abc+2(ab+bc+ca)+4(a+b+c)+6,$$

ezért látható, hogy $\circ$ asszociatív, így $(\mathbb{R},\circ)$ félcsoport. (4 pont)
Ha létezik e egységelem, akkor minden a-ra teljesülnie kell, hogy $a=a\circ e=ae+2a+2e+2$ és $a=e\circ a=ea+2e+2a+2$. Mindkét egyenlet átrendezésből $a(e+1)+2(e+1)=0$ adódik. Látható, hogy ez pontosan $e=-1$ esetén teljesül tetszőleges a mellett, így az egységelem a -1. (3 pont)
Az a egész számnak pontosan akkor lesz b az inverze, ha $e=a\circ b=ab+2a+2b+2$ és $e=b\circ a=ba+2b+2a+2$ teljesül. Mindkét egyenlet $b(a+2)=-2a-3$ alakban is írható $e=-1$ behelyettesítése után. Ha $a\neq -2$, akkor a-nak ezek szerint $b=-(2a+3)/(a+2)$ az inverze, viszont $a=-2$ esetén ellentmondást kapunk, tehát a -2-nek nincs inverze. Így $(\mathbb{R},\circ)$ nem csoport. (Itt a 3 pont természetesen akkor is jár, ha valaki nem ír arról, hogy $a\neq -2$-nak van-e inverze, csak bebizonyítja, hogy a -2-nek nincs inverze.) (3 pont)
Arra is jár a 3+3=6 pont, ha valaki az egységelem meghatározása nélkül igazolja, hogy nem csoport. Pl.: $a\circ -2=-2$ teljesül minden a-ra, ezért a Cayley-táblázatban a -2 oszlopában mindenhol -2 áll, ami ellentmond annak, hogy csoport esetén minden oszlopban (és minden sorban) minden elem pontosan egyszer szerepel, vagyis $(\mathbb{R},\circ)$ nem csoport.
Ha valaki azt is ellenőrzi, hogy $\circ$ valóban művelet, vagyis azt, hogy nem vezet ki $\mathbb{R}$-ből, akkor erre a korábbiakon felül +1 pontot kaphat, ha máshol vesztett részpontszámot.
Megjegyzés. Láttuk, hogy csak a -2-nek nincs inverze, és nem nehéz megmutatni, hogy $(\mathbb{R}\setminus\{-2\},\circ)$ Abel-csoport.