Bevezetés a számításelméletbe II.

1. pótZH javítókulcs

Az útmutató mintamegoldásokat tartalmaz. A pontszámok tájékoztató jelleggel lettek megállapítva az értékelés egységesítése céljából. Egy részpontszám előtt szereplő állítás kimondása, tétel vagy definíció felidézése nem jelenti automatikusan az adott pontszám megszerzését. Az adott részpontszám megítélésenek az a feltétele, hogy a megoldáshoz vezető gondolatmenet megfelelő részének végiggondolása is világosan kiderüljön a dolgozatból. Ha ez utóbbi kiderül, ám a kérdéses állítás, tétel, definíció nincs rendesen kimondva, akkor a részpontszámn legalább részben jár.
Természetesen az ismertetettektől eltérő, ám helyes megoldásokért teljes pontszámok, részmegoldásokért pedig az útmutatóbeli pontozás intelligens közelítésével meghatározott arányos részpontszámok járnak. Számolási hibáért általában 1 pontot vonunk le.

1. Mutassuk meg, hogy ha G egy 16 csúcsú, 6-reguláris, egyszerű, páros gráf, akkor G-nek van Euler-köre. (G 6-reguláris, ha minden csúcsának 6 a foka.)

   Mivel a feladatbeli G gráf 6-reguláris, ezért G minden fokszáma páros. (2 pont)
   Tanultuk, hogy egy véges **összefüggő** G gráfnak pontosan akkor van Euler-köre, ha G-ben minden fokszám páros. Ezért elegendő azt megmutatni, hogy G összefüggő. (2 pont)
   Legyen K a G egy komponense, v pedig K egy pontja, mondjuk az A színosztályban. Mivel v-nek 6 szomszédja van, ezért K legalább 6 csúcsot tartalmaz a B színosztályból. (2 pont)
   Ha tehát u a K egy B színosztálybeli pontja, akkor u-nak 6 szomszédja lévén K az A színosztályból is legalább 6 csúcsot tartalmaz. (2 pont)
   Azt kaptuk, hogy G tetszőleges komponensének legalább $6 + 6 = 12$ pontja van. (1 pont)
   Mivel azonban G összesen 16 csúccsal rendelkezik, G-nek legfeljebb csak egy komponense lehet, tehát G összefüggő. Mi pedig pontosan ezt akartuk igazolni. (1 pont)

2. Igazak-e az alábbi állítások? ($\alpha(G)$ a független csúcsok maximális száma.)

   (a) Ha a G véges gráf páros, akkor G minden G' részgráfjára $\alpha(G') \geq \frac{|V(G')|}{2}$ teljesül.

   (b) Ha G minden részgráfjára $\alpha(G') \geq \frac{|V(G')|}{2}$ teljesül, akkor G páros.

   Az (a) részhez tegyük fel, hogy G páros, és G' a G egy részgráfja. Világos, hogy G' élei is két diszjunkt színosztály között futnak, ezért G' is páros gráf. (2 pont)
   Mivel G' csúcsai két színosztályba sorolhatók, ezért az egyik színosztály a G' olyan független csúcshalmaza, ami G' csúcsainak legalább a felét tartalmazza. (2 pont)
   Ezek szerint $\alpha(G') \geq \frac{|V(G')|}{2}$, tehát az (a) állítás igaz. (1 pont)
   Az (b) részhez tegyük fel, hogy G nem páros. Tanultuk, hogy egy gráf pontosan akkor páros, ha nem tartalmaz részgráfként páratlan kört. (2 pont) Jelen esetben tehát létezik G-nek egy olyan G' részgráfja, ami páratlan (mondjuk $2n + 1$ pontú kör. (3 pont)
   Tudjuk, hogy egy $2n + 1$ pontú körből legfeljebb n független csúcs választható ki, (1 pont)
   ezért $\alpha(G') = n < \frac{2n+1}{2}$, tehát nem páros gráfokra a feltétel nem teljesül. (1 pont)

3. Legyen G egy tetszőleges 99 csúcsú egyszerű gráf, melynek minden csúcsa legalább 80 másik csúccsal szomszédos. Igazoljuk, hogy G csúcsait kiszínezhetjük legfeljebb 20 szín felhasználásával úgy, hogy bármely két összekötetlen pont színe különböző legyen.

   Azt kell igazolnunk, hogy a $\overline{G}$ komplementer gráf kromatikus száma legfeljebb 20. (3 pont)
   Mivel G-ben minden fokszám legalább 80, ezért a $\overline{G}$-ben tetszőleges fokszám legfeljebb 19 lesz, azaz $\Delta(\overline{G}) \leq 19$. (2 pont)
   Tanultuk, hogy tetszőleges G gráfra $\chi(G) \leq \Delta(G) + 1$ teljesül. Ezt a $\overline{G}$-re alkalmazva $\chi(\overline{G}) \leq 19 + 1 = 20$ adódik,(4 pont)
   és nekünk pontosan ezt kellett bizonyítanunk. (1 pont)

4. Tegyük fel, hogy G perfekt gráf, és G csúcsainak X részhalmaza rendelkezik azzal a tulajdonsággal, hogy X bármely pontja szomszédos $V(G) \setminus X$ tetszőleges pontjával. Bizonyítsuk be, hogy az a G' gráf is perfekt, amit úgy kapunk, hogy G-t X-n belül komplementáljuk, azaz u és v közt pontosan akkor fut él G'-ben, ha $u, v \in X$ és u és v G-ben nem szomszédosak, vagy akkor, ha u és v közül legalább az egyik nem X-beli, és u és v G-ben szomszédosak.

   A gyenge perfekt gráf tétel szerint egy G gráf pontosan akkor perfekt, ha $\overline{G}$ komplementere perfekt, ezért tudjuk, hogy a $\overline{G}$ gráf perfekt. (3 pont)
   Az X halmazból a $\overline{G}$ gráfban nem vezet él X-en kívülre, ezért X a $\overline{G}$ néhány komponensének uniója. (2 pont)
   A perfektség definíciójából következik, hogy egy gráf pontosan akkor perfekt, ha minden komponense perfekt. Ezért a gyenge perfekt gráf tétel miatt az a G^* gráf is perfekt, amit úgy kapunk $\overline{G}$-ből, hogy az X-beli komponensek helyett a komplementereiket vesszük. (2 pont)
   A feladatban szereplő G' gráf a perfekt G^* gráf komplementere, (2 pont)
   ezért a gyenge perfekt gráf tétel szerint G' is perfekt. (1 pont)

   Lehet persze az erős perfekt gráf tételt is használni.

Az erős perfekt gráf tétel miatt elegendő azt igazolni, hogy G' nem tartalmaz feszített részgráfként sem legalább 5 hosszú páratlan kört, sem annak komplementerét. (3 pont)

Indirekt bizonyítunk: tegyük fel, hogy van ilyen. Ez a feszített részgráf nem lehet sem X-től diszjunkt, sem pedig nem lehet X részhalmaza, (2 pont)

hiszen ekkor már a perfekt G gráf is feszített volna tiltott részgráfot. (1 pont)

A tiltott részgráf tehát X-t és a komplementerét is metszi. Mivel X minden csúcsa szomszédos a komplementere minden pontjával, ezért a tiltott részgráf X-be eső meteszet is szomszédos a részgráf X-en kívüli minden csúcsával. (1 pont)

Ha a tiltott részgráf egy páratlan kör, akkor ez csak úgy lehetséges, ha C_3-ról van szó, ámde nekünk legalább 5 hosszú a körünk. (1 pont)

Ha pedig páratlan kör komplementere a szóban forgó feszített részgráf, akkor ha annak egy v csúcsa X-ben van, akkor páratlan körön v szomszédainak szintén X-be kell esniük, azok szomszédainak szintúgy, vagyis az egész tiltott részgráf X-be esik, ami ellentmondás. (1 pont)

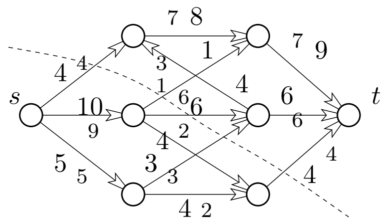
Azt kaptuk, hogy G' nem feszíthet egyetlen tiltott részgráfot sem, így csakugyan perfekt. (1 pont)

5. Határozzunk meg az alábbi hálózatban egy maximális nagyságú folyamot és egy minimális vágást!

   A mellékelt ábrán a növelő algoritmussal kapott 18 nagyságú folyam látható. (Az élre írt kisebb szám az élhez rendelt folyamértéket jelöli.) (6 pont)

   Az ábrán bejelöltünk egy 18 kapacitású st-vágást is. (2 pont)

   Mivel a vágás kapacitása megegyezik a folyam nagyságával, (az MFMC tétel triviális iránya miatt) a kapott folyam maximális nagyságú, és az st-vágás pedig minimális kapacitású. (2 pont)



6. Bizonyítsuk be, hogy ha egy 20 csúcsú, egyszerű, irányítatlan G gráf 12-szeresen élösszefüggő, akkor a komplementere nem lehet 8-szorosan élösszefüggő.

   G 12-élöf, ezért Menger idevágó tétele szerint G bármely két csúcsa között legalább 12 éldiszjunkt út vezet. (3 pont)

   Ez speciálisan azt jelenti, hogy G bármely csúcsának fokszáma legalább 12. (2 pont)

   Ebből azt kapjuk, hogy a $\overline{G}$ gráfban minden csúcs legfeljebb 7 másikkal van összekötve. (2 pont)

   Ezek szerint $\overline{(G)}$-ben nem lehet két különböző csúcs között 8 éldiszjunkt út, (2 pont)

   következésképpen $\overline{G}$ nem lehet 8-szorosan élösszefüggő. (1 pont)

Bevezetés a számításelméletbe II.

2. pótZH javítókulcs

Az útmutató mintamegoldásokat tartalmaz. A pontszámok tájékoztató jelleggel lettek megállapítva az értékelés egységesítése céljából. Egy pontszám előtt szereplő állítás kimondása, tétel felidézése nem jelenti automatikusan az adott pontszám megszerzését. Az adott részpontszám megítélésenek az a feltétele, hogy a megoldáshoz vezető gondolatmenet megfelelő részének végiggondolása is világosan kiderüljön a dolgozatból.
Természetesen az ismertetettektől eltérő, ám helyes megoldásokért teljes pontszámok, részmegoldásokért pedig az útmutatóbeli pontozás intelligens közelítésével meghatározott arányos részpontszámok járnak. Számolási hibáért általában 1 pontot vonunk le.

1. Legyenek a G gráf csúcsai az $\{1, 2, \ldots, 100\}$ számok, és az i és j csúcsok akkor legyenek G-ben szomszédosak, ha $i \neq j$ és i és j legnagyobb közös osztója páros, de 4-gyel nem osztható. Határozzuk meg a $\nu(G)$ és $\alpha(G)$paramétereket. (Emlékeztetőül: a $\nu(G)$ és $\alpha(G)$ mennyiségek a független élek ill. pontok maximális számát jelentik.)

   Az i és j csúcsok pontosan akkor szomszédosak, ha i és j is párosak, és legalább az egyik nem osztható 4-gyel. (1 pont)
   Ez azt jelenti, hogy ha i páratlan, akkor i a G gráf izolált pontja, (1 pont)
   ha i páros, de nem osztható 4-gyel, akkor i minden páros számnak megfelelő csúccsal össze van kötve, végül ha $4 \mid i$, akkor i pontosan a páros, 4-gyel nem osztható számoknak megfelelő csúcsoknak szomszédja. (1 pont)
   Ha tehát rendre P, K és N az 1 és 100 közti páratlan, páros, de 4-gyel nem osztható, ill. a 4-gyel osztható számok halmaza, akkor a P-beli 50 csúcs mindegyike izolált, a K-beli 25 csúcs mindegyike össze van kötve a $K \cup N$ halmaz minden más pontjával, míg N bármely csúcsa kizárólag K csúcsaival van összekötve, de azokból minddel. (2 pont)
   Világos, hogy egy F független csúcshalmaznak legfeljebb egy K-beli pontja lehet, és ha F-nek van ilyen pontja, akkor F diszjunkt N-től, így ekkor $|F| \leq 51$. Mivel G-nek a K-tól különböző 75 pontja egy független ponthalmazt alkot, így $\alpha(G) = 75$. (1 pont)
   Tudjuk, hogy $\nu(G) \geq 25$, ugyanis G-nek van 25 független éle, hiszen minden $i \in K$ szomszédos az $i + 2 \in N$ csúccsal, és ennek a 25 élnek nincs közös csúcsa. (1 pont)
   Másrészt viszont a 25 K-beli pont lefog minden élt, (1 pont)
   ezért $\nu(G) \leq \tau(G) \leq 25$, (1 pont)
   vagyis $\nu(G) = 25$. (1 pont)

2. Oldjuk meg a $18x \equiv 27 (\mathrm{mod}\ 105)$ kongruenciát.

   A modulus és az együttható legnagyobb közös osztója $(105, 18) = 3$ osztója a 27-nek, azaz a tanult feltétel szerint a kongruenciának léteznek megoldásai (és azok 3 maradékosztályt alkotnak modulo 105). (2 pont)
   Leosztunk tehát a legnagyobb közös osztóval, okosan ügyelve, hogy a modulust is osszuk: $6x \equiv 9 (\mathrm{mod}\ 35)$ (2 pont)
   Ügyesen észrevesszük, hogy a 6-tal szorzás ekvivalens átalakítás, hiszen $(6, 35) = 1$. (2 pont)
   Azt kapjuk, hogy $36x \equiv 54 (\mathrm{mod}\ 35)$, (2 pont)
   amit modulo 35 redukálva $x \equiv 19 (\mathrm{mod}\ 35)$ adódik. (1 pont)
   Végig ekvivalens átalakításokat végeztünk, így a kongruencia megoldásainak halmaza pontosan az imént kapott maradékosztály. (1 pont)
   Éppenséggel megkereshetjük a megoldásokat modulo 105 is, bár ezt senki sem kérte. Konkrétan azt kapjuk, hogy $x \equiv 19 (\mathrm{mod}\ 105)$ vagy $x \equiv 54 (\mathrm{mod}\ 105)$ vagy $x \equiv 89 (\mathrm{mod}\ 105)$. (0 pont)

3. Határozzuk meg mindazon n egész számokat, melyekre $3n + 1 \equiv 6 (\mathrm{mod}\ 2n)$ teljesül.

   A kongruencia definíciója szerint $2n \mid 3n + 1 - 6 = 3n - 5$ a feltétel. (2 pont)
   Mivel tetszőleges n egészre $2n \mid 2n$, ezért a fenti feltétel azzal ekvivalens, hogy $2n \mid 3n - 5 - 2n = n - 5$ teljesül. (2 pont)
   Mivel $n - 5$ egy páros szám többszöröse, $n - 5$ is páros, így n páratlan. (2 pont)
   A páros $n - 5$ tehát pontosan akkor lesz $2n$ többszöröse, ha a páratlan n-nek többszöröse, azaz, ha $n \mid n - 5$, (1 pont)
   ez pedig azzal ekvivalens, hogy $n \mid -5$, vagyis $n \mid 5$. (1 pont)
   A keresett n megoldások tehát az 5 páratlan osztói, azaz $n = 1$ és $n = 5$ (1 pont)
   valamint $n = -1$ és $n = -5$. (1 pont)

4. Adjuk meg mindazon n pozitív egészek kanonikus alakját, amikre $d(n)$ prím.

   Tanultuk, hogy ha n kanonikus alakja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, akkor n osztóinak száma $d(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots (\alpha_k + 1)$.
   A feladat szerint ez a szorzat prím. (4 pont)
   Pozitív egészek szorzata csak úgy lehet prím, hogy egy kivételével minden tényező 1-gyel egyenlő, a kivételes tényező pedig prím. (2 pont)
   Ezért n kanonikus alakjában egyetlen prím szerepel, aminek a kitevője egy prímnél 1-gyel kisebb szám, (3 pont)
   azaz n kanonikus alakja $n = p^{q-1}$, ahol p és q prímek. (1 pont)

5. Mi az utolsó két jegye az 5^{5^6} számnak 7-es számrendszerben?

   Azt kell meghatároznunk, hogy az 5^{5^6} szám $7^2 = 49$-cel milyen osztva maradékot ad, (2 pont)
   és ezt a maradékot kell 7-es számrendszerben két jeggyel felírnunk. (1 pont)
   Mivel 5 és 49 relatív prímek, ezért az Euler-Fermat tétel miatt $5^{\varphi(49)} \equiv 1 (\mathrm{mod}\ 49)$. (2 pont)
   A tanult képlet szerint $\varphi(49) = \varphi(7^2) = 7^2 - 7^1 = 42$. (1 pont)

A cél tehát az 5^6 kitevő 42-es maradékának meghatározása. (1 pont)

Mivel $5^3 = 125 = 3 \cdot 42 - 1$, ezért $5^3 \equiv -1 (\mathrm{mod}\ 42)$, így $5^6 = (5^3)^2 \equiv 1 (\mathrm{mod}\ 42)$. (1 pont)

Vagyis $5^{5^6} = 5^{42k+1} = 5^{42k} \cdot 5 = (5^{42})^k \cdot 5 \equiv 1^k \cdot 5 = 5 (\mathrm{mod}\ 49)$ adódik az Euler-Fermat tételből. (2 pont)

Eszerint az 5^{5^6} szám utolsó két jegye 7-es számrendszerben 05. (1 pont)

6. Adjuk meg mindazon n pozitív egészek kanonikus alakját, amikre $\varphi(n) = \frac{n}{2}$.

A $\varphi(n)$ mindig egész, ezért $\frac{n}{2}$ egész, vagyis n páros. (3 pont)

Mivel n páros, ezért a 2 az n prímosztója. (1 pont)

Tanultuk, hogy $\varphi(n) = n \prod_{p|n, p \text{ prím}} (1 - \frac{1}{p})$. Innen $\varphi(n) = \frac{1}{2} n \prod_{2<p|n, p \text{ prím}} (1 - \frac{1}{p})$, hiszen a $p = 2$ prímosztó. (2 pont)

A $\varphi(n)$ képletében tehát $\frac{n}{2}$-t kell még további 1-nél kisebb tényezőkkel szorozni akkor, ha n-nek van a 2-től különböző prímosztója. (1 pont)

Ha van ilyen tényező, akkor a szorzat $\frac{n}{2}$-nél kisebb lesz. Ezért n-nek nem lehet 2-n kívül más prímosztója, (2 pont)
tehát n a 2 pozitív kitevős hatványa, vagyis kanonikus alakja $n = 2^k$. (1 pont)