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: ennek feltétele az is, hogy a megoldáshoz vezető gondolatmenet megfelelő részének végiggondolása is kiderüljön a dolgozatból.
Természetesen az alább ismertetettektől eltérő, ám helyes megoldásokért teljes pontszámok, részmegoldásokért pedig az útmutatóbeli pontozás intelligens közelítésével meghatározott részpontszámok járnak.
Szolgálati közlemény: A zh-k megbeszélése utáni végleges eredményeket legyetek szívesek a kartonokra bejegyezni. Akinek még nincs kartonja, tessék annak keresni. Ha nem lesz, akkor gyártani. Mihamarabb legyetek szívesek egy listát adni Katának azokról a hallgatókról, akik megszerezték az aláírást.

1. Hány 0-ra végződik a $\binom{100}{42}$ binomiális együttható meghatározta szám tizes számrendszerbeli alakja?

   Azt kell meghatározni, hogy melyik az a legmagasabb hatványa a 10-nek, ami osztója az $n = \binom{100}{42} = \frac{100!}{42!\cdot 58!}$ számnak. (1 pont)
   Ehhez kiszámítjuk n kanonikus alakjában az 5 és a 2 prímtényezők kitevőit, és ezek közül a kisebb lesz az általunk keresett szám. (1 pont)
   100! kiszámításakor 20 db 5-tel osztható és 4 db 25-tel osztható számot szorzunk össze, ezért 100!-ban az 5 prímtényező kitevője $20 + 4 = 24$. (1 pont)
   Ugyanez a kitevő 42! esetén 8 db 5-tel és 1 db 25-tel osztható szám miatt $8 + 1 = 9$, míg 58! esetén $11 + 2 = 13$. (1 pont)
   Az n kanonikus alakjában tehát az 5 prímtényező kitevője $24 - (9 + 13) = 2$. (1 pont)
   A 100!-ban a 2 kitevője $50 + 25 + 12 + 6 + 3 + 1 = 97$, hisz ennyi 2-vel, 4-gyel, ..., 64-gyel osztható számot szorzunk össze. (1 pont)
   A 2 kitevője 42!-ban hasonló okokból $21 + 10 + 5 + 2 + 1 = 39$, (1 pont)
   míg 58!-ban $29 + 14 + 7 + 3 + 1 = 54$, (1 pont)
   tehát n osztható $2^{97-(54+39)} = 2^4$-nel. (1 pont)
   A fent elmondottak szerint tehát n kanonikus alakja $n = 2^4 \cdot 5^2 \cdot \ldots$, azaz $100 \mid n$ de $1000 \nmid n$, tehát a $\binom{100}{42}$ binomiális együttható pontosan két nullára végződik. (1 pont)

2. Legfeljebb hány pozitív osztója lehet egy olyan n pozitív egésznek, ami három, nem feltétlenül különböző prím szorzata?

   Ha az n pozitív egész kanonikus alakja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots p_k^{\alpha_k}$, akkor n pozitív osztóinak száma $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$ az órán tanultak szerint. (3 pont)
   Azt kell tehát megvizsgálnunk, hogy legfeljebb mekkora lehet az utóbbi mennyiség, ha $\alpha_1 + \alpha_2 + \ldots + \alpha_k = 3$. (2 pont)
   A kanonikus alakban szereplő kitevők az alábbiak lehetnek: $1, 1, 1$ vagy $2, 1$, vagy 3. (2 pont)
   A pozitív osztók száma rendre $2 \cdot 2 \cdot 2 = 8$, $3 \cdot 2 = 6$, ill. 4 lesz. (2 pont)
   Azt kaptuk, hogy n-nek legfeljebb 8 osztója lehet, (1 pont)
   és ennyi pontosan akkor van, ha n három különböző prímszám szorzata. (0 pont)

3. Oldjuk meg a $42x \equiv 132 \pmod{57}$ kongruenciát!

   A megoldhatóság szükséges feltétele, hogy $(57, 42) \mid 132$ teljesüljön. (3 pont)
   Az euklideszi algoritmus alapján $(57, 42) = (42, 15) = (15, 12) = (12, 3) = (3, 0) = 3 \mid 132$ teljesül, (1 pont)
   a megoldások száma tehát 3 lesz modulo 132. (0 pont)
   A 3-mal való osztás ekvivalens átalakítás, ha a modulust is leosztjuk 3-mal: $14x \equiv 44 \pmod{19}$. (3 pont)
   Modulo 19 redukálva pedig $-5x \equiv 25 \pmod{19}$ adódik. (1 pont)
   Az 5 és a 19 relatív prímek, ezért bátran oszthatunk 5-tel, ekvivalens átalakítást végzünk: $-x \equiv 5 \pmod{19}$. (1 pont)
   Innen pedig $x \equiv -5 \pmod{19}$ a megoldás. (1 pont)
   Ezt átírhatjuk éppenséggel $x \equiv 14 \pmod{19}$ alakba is, de akár meghatározhatjuk a megoldásokat modulo 57 is: $x \equiv 14 \pmod{57}$ vagy $x \equiv 33 \pmod{57}$ vagy $x \equiv 52 \pmod{57}$. (0 pont)

4. Határozzuk meg mindazon x pozitív egész számokat, amelyekre $5x \equiv 2006 \pmod{2x}$ teljesül!

   A kongruencia definíciója szerint azon x pozitív egészeket kell megalálnunk, amelyekre $2x \mid 2006 - 5x$ teljesül. (2 pont)
   Figyeljük meg, hogy $2 \mid 2x$, ezért $2 \mid 2006 - 5x$, tehát $2 \mid 5x$, ahonnan $2 \mid x$-t kapjuk. (2 pont)
   Másrészt $x \mid 2x$, ezért $x \mid 2006 - 5x$, ahonnan $x \mid 2006$ adódik. (2 pont)
   Tehát a keresett x-k mindegyike 2006 páros (pozitív) osztója. (1 pont)
   A 2006 kanonikus alakja $2006 = 2 \cdot 17 \cdot 59$, ezért x kizárólag 2, $2 \cdot 17$, $2 \cdot 59$ vagy $2 \cdot 17 \cdot 59$ lehet. (1 pont)
   Ellenőrizzük mind a négy esetet: $10 \equiv 2 \equiv 2006 \pmod{4}$, tehát $x = 2$ megoldás, $170 \equiv 34 \equiv 2006 \pmod{68}$, tehát $x = 34$ is megoldás, $590 \equiv 59 \equiv 2006 \pmod{236}$, tehát $x = 118$ is megoldás, végül $10030 \equiv 2006 \pmod{4012}$, tehát $x = 2006$ is megoldás. (2 pont)
   Az utolsó rész helyett jó ez is: Ha x páros, és 2006 osztója, akkor $2006 = k \cdot x$ valamilyen páratlan k számra. Ekkor $2006 - 5x = (k - 5)x$, ami $k - 5$ páros lévén a $2x$ többszöröse. Tehát 2006 iménti említett négy páros osztójának mindegyike megoldás. (2 pont)

5. Legyen G egy véges csoport, és legyenek k_1 és k_2 a G csoport olyan elemei, melyek bármely csoportelemmel felcserélhetőek, azaz $k_1 g = g k_1$ és $k_2 g = g k_2$ teljesül tetszőleges $g \in G$-re. Bizonyítsuk be, hogy ekkor G bármely g elemére $(k_1 k_2) g = g (k_1 k_2)$ áll!

   Legyen tehát $g \in G$ tetszőleges. Ekkor $(k_1 \cdot k_2) \cdot g = k_1 \cdot (k_2 \cdot g) =$ a szorzás asszociativitása miatt (2 pont)
   $= k_1 \cdot (g \cdot k_2) =$ a k_2 felcserélhetősége miatt (2 pont)
   $= (k_1 \cdot g) \cdot k_2 =$ a szorzás asszociativitása miatt (2 pont)
   $= (g \cdot k_1) \cdot k_2 =$ a k_1 felcserélhetősége miatt (2 pont)
   $= g \cdot (k_1 \cdot k_2)$ a szorzás asszociativitása miatt. (2 pont)

6. Bizonyítsuk be, hogy $n \geq 2$ esetén az S_n szimmetrikus csoportnak létezik n-edrendű eleme!

   Az S_n elemei az $1, 2, \ldots, n$ elemek permutációi, a művelet pedig a permutációk egymásutánja. Egy $\sigma \in S_n$ rendje az a legkisebb k szám, amire a σ permutációt k-szor elvégezve S_n egységelemét, azaz a minden elemet fixen hagyó identikus permutációt kapjuk. (2 pont)
   Ha pl σ az a permutáció, amire $\sigma(i) := i + 1 \pmod{n}$ minden $1 \leq i \leq n$-re, (5 pont)
   akkor $\sigma^k(i) = i + k \pmod{n}$, (1 pont)
   tehát a legkisebb olyan k, amire $\sigma^k(i) = i$ lesz, az a $k = n$. (1 pont)
   Mivel $\sigma^n(i) = i$ minden $i = 1, 2, \ldots, n$-re, ezért σ rendje csakugyan n, vagyis σ egy kívánt tulajdonságú elem. (1 pont)
   Ha valaki szemléletesen elmondja, hogy egy n méretű ciklikus permutáció hatványai körbeforgatják az elemeket, és éppen n-edikre ér körbe minden elem, az is megkaphatja a 10 pontot, ha egyébként helyes az érvelése.

7. Határozzuk meg a D_5 diédercsoport részcsoportjainak számát!

   Az órán tanultuk, hogy a D_5 diédercsoport elemszáma 10 és van 5 eleme, ami tükrözés, ill. 5 eleme, ami forgatás (utóbbiak között van a a helybenhagyás is). (2 pont)
   A Lagrange tétel miatt D_5 részcsoportjainak elemszáma $1, 2, 5$ vagy 10 lehet. (2 pont)
   Világos, hogy egyelemű részcsoport csak egyetlen egy van, mégpedig az, amelyik csak az egységelemet tartalmazza. Ha viszont egy részcsoport 10 elemű, akkor az bizonyosan az egész D_5 csoport. Ezek tehát a triviális részcsoportok, amikből összesen kettő van. (2 pont)
   A valódi részcsoportok rendje 2 vagy 5 lehet. Mivel minden tükrözés rendje 2, és $2 \nmid 5$, ezért a Lagrange tétel szerint 5 elemű részcsoportban nem lehet tükrözés. Az egyetlen 5 elemű részcsoport jelölt tehát az 5 forgatás halmaza. (1 pont)
   A forgatások azonban egy 5-elemű ciklikus csoportot alkotnak, ami csakugyan D_5 részcsoportja. Így D_5-nek pontosan egy 5-ödrendű részcsoportja van. (1 pont)
   A 2 elemű részcsoportok mindegyike az egységelemen kívül egy 2 rendű elemet tartalmaz, így az 5 tükrözés mindegyike az egységelemmel együtt egy-egy ilyen részcsoportot alkot, azaz pontosan öt másodrendű részcsoport van D_5-ben. (1 pont)
   A fentiek szerint D_5 összes részcsoportjainak száma $2 + 1 + 5 = 8$. (1 pont)

8. Bizonyítsuk be, hogy ha G egy 35 elemű csoport, és a H halmaz a G csoport 8 különböző elemét tartalmazza, akkor a H által generált részcsoport maga a G csoport.

   Azt kell igazolnunk, hogy a G csoport semelyik 8 eleme sem generálhatja G-nek valódi részcsoportját, azaz, hogy G bármelyik valódi részcsoportja legfeljebb 7 elemű. (3 pont)
   A Lagrange tétel miatt G tetszőleges részcsoportjának elemszáma osztója a 35-nek, (5 pont)
   tehát $1, 5, 7$ vagy 35 lehet. (1 pont)
   Innen az következik, hogy ha egy részcsoport legalább 8 elemű, akkor az 35 elemű, azaz maga a G csoport, és éppen ezt kellett igazolunk. (1 pont)