Bevezetés a számításelméletbe II.

2. ZH 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. Határozzuk meg 2700 és 1620 közös (pozitív) osztóinak számát!

   Az órán tanultak szerint bármely a és b egész számok közös osztóinak halmaza megegyezik (a,b) osztóinak halmazával. (2 pont)
   Meghatározzuk tehát a $(2700,1620)$ legnagyobb közös osztót az Euklideszi algoritmus segítségével: $(2700,1620) = (1620,1080) = (1080,540) = (540,0) = 540$. (A prímtényezőkre bontással való meghatározás is elfogadható.) (3 pont)
   A közös osztók száma tehát 540 osztóinak számával azonos, ezért meghatározzuk 540 kanonikus alakját, ami $540 = 2^2 \cdot 3^3 \cdot 5$. (2 pont)
   Az órán tanultak szerint a kanonikus alakból kiszámítható az osztók száma, (1 pont)
   amely jelen esetben $(2+1)\cdot(3+1)\cdot(1+1) = 3\cdot 4\cdot 2 = 24$-nek adódik. (1 pont)
   A feladatra tehát 24 a helyes válasz.

2. Hány olyan (a,b) számpár van a pozitív egész számok között, amelyre $(a,b) = 2006$ és a és b legkisebb közös többszöröse pedig 2006^2?

   Az órán láttuk, hogy az (a,b) kanonikus alakjában pontosan a és b közös prímtényezői szerepelnek, mégpedig az a és b felbontásában szereplő kisebb kitevővel. A legkisebb közös többszöröshöz minden, a vagy b kanonikus alakjában szereplő prímet a nagyobbik kitevőre emelve kell összeszorozni. (3 pont)
   A 2006 kanonikus alakja $2006 = 2\cdot 17\cdot 59$, (1 pont)
   a 2006^2-é pedig $2006^2 = 2^2\cdot 17^2\cdot 59^2$. (1 pont)
   Eszerint a és b kanonikus alakjaiban a 2 prímtényező 1 ill. 2 kitevővel, a 17 prímtényező ugyancsak 1 ill. 2 kitevővel, végül az 59 prímtényező is 1 ill. 2 kitevővel szerepel. (2 pont)
   Van tehát 3 független választásunk az egyes prímtényezők szerint, (2 pont)
   ezért az összes keresett (a,b) számpárok száma $2^3 = 8$. (1 pont)

   Ha valaki nem rendezett számpárokra gondol (és ezért a válasza 4), akkor az is elfogadható.

3. Hány megoldása van modulo 2006 a $136x \equiv 680 \pmod{2006}$ ill. a $136x \equiv 700 \pmod{2006}$ kongruenciáknak?

   Az $ax \equiv b \pmod m$ kongruencia megoldhatóságának feltétele, hogy $(a,m) \mid b$ teljesüljön. (2 pont)
   Ha ez teljesül, akkor a megoldások száma (a,m) modulo m. (2 pont)
   Konkrétan (pl. az Euklideszi algoritmus segítségével) $(136,2006) = (2006,136) = (136,102) = (102,34) = (34,0) = 34$. (2 pont)
   Mivel $34\cdot 20 = 68\cdot 10 = 680$, ezért $(136,2006) \mid 680$, tehát az első kongruenciának 34 megoldása van modulo 2006. (2 pont)
   Azonban $34 \nmid 20 = 700 - 680$, ezért $34 \nmid 700$, tehát a második kongruenciának egyáltalán nincs megoldása. (2 pont)

   Ha vki az euklideszi algoritmus helyett a kanonikus alakokból számolja ki a legnagyobb közös osztót, az is ugyanolyan jó. (Itt legalábbis.)

4. Bizonyítsuk be, hogy ha $(a,m) = 1$, $(b,m) = 1$ és $ax \equiv b \pmod m$ valamint $by \equiv a \pmod m$ teljesülnek az x,y egész számokra, akkor $xy \equiv 1 \pmod m$ is igaz!

   Azonos modulusú kongruenciákat összeszorozhatunk, ezért $abxy \equiv ab \pmod m$ áll. (3 pont)
   Mivel $(a,m) = 1$, ezért a-val itt leoszthatunk a modulus változtatása nélkül: $bxy \equiv b \pmod m$. (4 pont)
   Innen $(b,m) = 1$ miatt a b-vel való osztás eredménye $xy \equiv 1 \pmod m$ lesz, és éppen ezt kellett igazolnunk. (3 pont)

5. Határozzuk meg mindazon $n \geq 2$ egészeket, melyekre a D_n diédercsoportban minden elem rendje n-nek osztója!

   A D_n diédercsoport elemei a sík olyan egybevágóságai, melyek a szabályos n oldalú sokszöget fixen hagyják, a művelet pedig az egybevágóságok egymás utáni elvégzése. (2 pont)
   Egy szabályos n oldalú sokszöget kétféleképpen hagyhat fixen egy egybevágóság: vagy megőrzi a körüljárást (és ekkor szükségképpen egy, a sokszög középpontja körüli forgatásról van szó), vagy megfordul a körüljárás, ám ekkor biztosan a sokszög valamelyik szimmetriatengelyére tükröztünk. (2 pont)
   A D_n csoportnak tehát $2n$ eleme van: n db forgatás, és n db tükrözés. (Mindezt egyébként az órán is tanultuk. Ha vki erre hivatkozik, kapjon meg minden eddigi pontot.) (1 pont)
   Minden tükrözés rendje 2, hisz ugyanarra a tengelyre kétszer tükrözve a minden pontot helybenhagyó, identikus egybevágóságot kapjuk, ami D_n egységeleme. (2 pont)
   A szabályos n oldalú sokszög tetszőleges forgásszimmetriája egy $\frac{2k\pi}{n}$ szögű forgatás, amit n-szer egymás után elvégezve a $2k\pi$ forgatást, azaz az identitást kapjuk. (1 pont)
   Ezért D_n minden forgatás-elemének a rendje osztója n-nek. (1 pont)
   Azt kaptuk, hogy pontosan akkor lesz minden elemrend n osztója, ha a tükrözések rendje (2) is osztója n-nek, azaz, ha n páros. (1 pont)

6. Csoportot alkotnak-e a szokásos szorzásra a valós és tiszta képzetes számok a 0 nélkül, azaz csoport-e $(X,\cdot)$, ahol $X = \{a \in \mathbb{R} : a \neq 0\} \cup \{ai : 0 \neq a \in \mathbb{R}\}$, ill. $\cdot$ a komplex számokon értelmezett szokásos szorzást jelöli?

   Négy dolgot kell ellenőriznünk: azt, hogy a szorzás valóban művelet, hogy asszociatív, hogy létezik egységelem, és hogy létezik inverz. (1 pont)
   A szorzás művelet $\mathbb{C}$-n, ezért itt akkor lesz művelet, ha nem vezet ki az X halmazból. Két X-beli elem szorzásakor nem kaphatunk 0-t, hisz egy szorzat pontosan akkor 0, ha legalább az egyik tényezője 0. Valósak szorzata valós, tiszta képzetesek szorzata valós, és valóst tiszta képzetessel szorozva tiszta képzetest kapunk. A szorzás tehát zárt X-en, csakugyan művelet. (2 pont)
   A szorzásról láttuk, hogy asszociatív $\mathbb{C}$-n, ezért annak X részhalmazán is az. (2 pont)
   Tudjuk, hogy $1\cdot z = z\cdot 1 = 1$, ezért az 1 valós szám a komplex szorzásnak egységeleme, tehát $1 \in X$ a mi struktúránknak egységeleme. (2 pont)
   Az $x \in X$ szorzásra vonatkozó inverze az az y szám, amire $xy = yx = 1$ teljesül, azaz az inverz nem más, mint $\frac{1}{x}$.
   Ha $x \in \mathbb{R}\setminus\{0\}$, akkor $x^{-1} = \frac{1}{x} \in \mathbb{R}\setminus\{0\}$, illetve $(ix)^{-1} = \frac{1}{ix} = -\frac{i}{x} = -i\cdot\frac{1}{x}$, tehát X valóban tartalmazza minden elem inverzét is. (2 pont)
   Azt kaptuk, hogy a kérdéses struktúra csakugyan csoport. (1 pont)
   A szorzás egyébként kommutatív, ezért Abel csoportról van szó. (0 pont)

7. Tegyük fel, hogy G egy 49-elemű csoport, és H_1 ill. H_2 a G valódi részcsoportjai. Bizonyítsuk be, hogy $|H_1| = |H_2|$ teljesül! (Egy G csoport valódi részcsoportja egy olyan $H \leq G$ részcsoport, ami az egységelem mellett még legalább egy másik elemet is tartalmaz és $H \neq G$.)

   A G csoport valódi részcsoportjai pontosan azok a részcsoportok lesznek, melyeknek rendje nem 1 és nem 49. (2 pont)
   A Lagrange tétel miatt G bármely részcsoportjának rendje osztója a 49-nek. (4 pont)
   A $49 = 7^2$ kanonikus alak miatt G tetszőleges részcsoportjának rendje csak 1, 7, vagy 49 lehet. (2 pont)
   A valódi részcsoportok rendje tehát egyaránt 7, és ez bizonyítja a feladatbeli állítást. (2 pont)

8. Tegyük fel, hogy H a G csoport egy 2 indexű részcsoportja, azaz $H \leq G$ és $|G : H| = 2$. Bizonyítsuk be, hogy G tetszőleges g elemére $gH = Hg$ teljesül!

   Az órán láttuk, hogy ha $g \in H$, akkor $gH = H = Hg$ teljesül. (2 pont)
   A feladat állítását tehát csak $g \notin H$ esetén kell ellenőrizni. (1 pont)
   Az órán azt is tanították, hogy ha $g \notin H$, akkor $|gH| = |H| = |Hg|$ mellett $gH \cap H = \emptyset = Hg \cap H$ áll. (2 pont)
   Mivel H egy 2 indexű részcsoport, ezért $|G| = 2\cdot|H|$, (1 pont)
   tehát $|H| = |G\setminus H|$. (1 pont)
   Ezért a gH mellékosztály, ami H-tól diszjunkt csakis $gH = G\setminus H$ lehet, (1 pont)
   és ugyanez igaz a Hg mellékosztályra is. (1 pont)
   Ezzel a feladat állítását beláttuk. (1 pont)