Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2020. október 30.

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. Ha egy megoldó egy feladatra több, egymástól lényegesen különböző megoldást is elkezd, akkor legfőljebb az egyikre adható pontszám. Ha mindegyik leírt megoldás vagy megoldásrészlet helyes vagy helyessé kiegészíthető, akkor a legtöbb részpontot érő megoldáskezdeményt értékeljük. Ha azonban több megoldási kísérlet között van helyes és (lényeges) hibát tartalmazó is, továbbá a dolgozatból nem derül ki, hogy a megoldó melyiket tartotta helyesnek, akkor a kevesebb pontot érő megoldáskezdeményt értékeljük (akkor is, ha ez a pontszám 0).

Az útmutatóban szereplő részpontszámok szükség esetén tovább is oszthatók. Az útmutatóban leírttól eltérő jó megoldás természetesen maximális pontot ér, de bizonyítás nélkül csak az előadáson szereplő tételekre és állításokra lehet hivatkozni.

1. Mely 1 és 111 közötti egész számok 1111-szerese ad 11 maradékot 2020-szal osztva?

* * * * *

Ha n ilyen egész, akkor rá $1111n \equiv 11 \pmod{2020}$ teljesül. (2 pont)
$2020 = 2^2 \cdot 5 \cdot 101$ és $1111 = 11 \cdot 101$, ezért $(1111, 2020) = 101$. (3 pont)
Mivel $101 \nmid 11$, ezért a lineáris kongruenciák megoldhatóságára tanult tétel értelmében (miszerint $ax \equiv b \pmod{m}$ pontosan akkor megoldható, ha $(a, m) \mid b$) nem létezik ilyen n egész. (5 pont)
2020 és 1111 legnagyobb közös osztója a prímtényezős felbontásuk helyett természetesen az Euklideszi algoritmussal is meghatározható. Ha viszont egy megoldó az Euklideszi algoritmussal próbálja megoldani a lineáris kongruenciát, az (önmagában) nem ér pontot, hiszen az algoritmus (előadáson tanult) változata csak az $(a, m) = 1$ feltétel ellenőrzése után alkalmazható az $ax \equiv b \pmod{m}$ lineáris kongruencia megoldására. Ha egy ilyen számolás végén (a $101n \equiv -99 \pmod{2020}$, majd a $0n \equiv 220 \pmod{2020}$ sorok után) a megoldó felismeri, hogy ebből $(1111, 2020) = 101$ következik (hiszen n együtthatói sorra az Euklideszi algoritmus legnagyobb közös osztó meghatározására szolgáló változatának során keletkező maradékok) és ebből következtet a lineáris kongruencia megoldhatatlanságára, az természetesen jó megoldás. Ugyancsak helyes indoklás, ha a megoldó arra hivatkozik, hogy a számolás során keletkező kongruenciák a kongruenciákkal végzett műveletekkel kapcsolatban tanultak miatt mind következményei az eredetinek, így a $0n \equiv 220 \pmod{2020}$ ellentmondásból a lineáris kongruencia megoldhatatlansága következik. Ha azonban a számolás után mindenféle indoklás nélkül csak a „nincs megoldás” állítás szerepel, az nem ér pontot, mert egy ilyen megoldás se tanult algoritmust nem alkalmaz, se helyes gondolatmenetet nem közöl, így a következtetése indoklás nélküli eredményközlésnek minősül. Ha egy megoldó a lineáris kongruencia felírása után azt 11-gyel (helyesen) elosztja (hivatkozva arra is, hogy a modulus $(2020, 11) = 1$ miatt nem változik), akkor ezért a lépésért (bár az érdemben nem visz közelebb a megoldáshoz) 1 pontot kaphat – feltéve, hogy a megoldás további része nem tartalmaz értékelhető részt.

2. Milyen maradékot ad 4^{74} 70-nel osztva?

* * * * *

Első megoldás. A ismételt négyzetre emelések módszerével oldjuk meg a feladatot. (2 pont)
Kiszámítjuk a $4^1, 4^2, 4^4, \ldots, 4^{64}$ hatványok 70-es maradékát (mindig az előző négyzetre emelésével és a kapott eredmény 70-es maradékának kiszámításával). Ezek sorra: 4, 16, 46, 16, 46, 16, 46. (3 pont)
Mivel $74 = 2 + 8 + 64$, (2 pont)
ezért meghatározzuk először a $4^{10} = 4^2 \cdot 4^8$, majd a $4^{74} = 4^{10} \cdot 4^{64}$ hatványok 70-es maradékait (a korábban kiszámolt megfelelő maradékokkal való szorzással és a kapott eredmények 70-es maradékának meghatározásával). Ezek sorra: 46 és 16. Így a keresett maradék: 16. (3 pont)
A teljes értékű megoldáshoz nem szükséges a fenti részletességgel leírni az elvégzett műveletek mögötti szándékot, elegendő a helyes számítások közlése. A fenti pontozás szerinti első 2 pont annak jár, aki felismeri, hogy a feladat az ismételt négyzetre emelések módszerével megoldható (és ezt legalább azzal jelzi, hogy az algoritmus alkalmazását megkezdi). Mivel azonban a feladat nem kéri a tanult algoritmus alkalmazását, ezért bármilyen, helyes eredményre vezető és elvileg helyes számolás maximális pontszámot ér – akkor is, ha az fölöslegesen komplikált vagy nem felel meg az algoritmus pontos alkalmazásának. Ha azonban egy megoldás nem (pontosan) követi az algoritmust, akkor a számítások helyessége és az azokból levont következtetések indoklásra szorulnak. Így ha egy megoldó pusztán egy, az algoritmus pontos alkalmazásának nem megfelelő számítást közöl, az nem érhet maximális pontszámot; az ilyen megoldások (helyes számításokat és eredményt feltételezve) 6 pontot érjenek.

Második megoldás. 35 prímtényezős felbontása $35 = 5 \cdot 7$, ezért $\varphi(35) = (5-1) \cdot (7-1) = 24$ a tanult képlet szerint. (1 pont)
Mivel $(4, 35) = 1$, (1 pont)
ezért az Euler-Fermat tételből $4^{24} \equiv 1 \pmod{35}$ következik. (2 pont)
Ezt köbre emelve, majd 4^2-nel szorozva: $4^{72} \equiv 1 \pmod{35}$, illetve $4^{74} \equiv 16 \pmod{35}$. (2 pont)
Azt kaptuk tehát, hogy $35 \mid 4^{74} - 16$. Másrészt nyilván $2 \mid 4^{74} - 16$ is igaz, hiszen 4^{74} és 16 is páros. Ebből viszont $(2, 35) = 1$ miatt $70 \mid 4^{74} - 16$ is következik (hiszen $4^{74} - 16$ prímtényezős felbontásában a 2, 5 és 7 prímek is szerepelnek). Ebből tehát $4^{74} \equiv 16 \pmod{70}$ következik, így a keresett maradék a 16. (4 pont)
Ha egy megoldó az Euler-Fermat tételt hibásan 4-re és 70-re próbálja alkalmazni, majd az így kapott (hamis) kongruenciából kiindulva jut el a helyes végeredményre, akkor ez nem ér pontot. (Még a fenti pontozás szerinti köbre emelésért és beszorzásért, illetve $\varphi(70)$ kiszámításáért járó részpontszám sem adható meg az útmutató elején írt általános alapelvek második bekezdésében írtak szerint.) A fenti pontozás utolsó 4 pontjának megfelelő gondolat helyettesíthető a következővel is:
Mivel egy 35-tel osztva 16 maradékot adó szám 70-nel osztva nyilván 16 vagy 51 maradékot adhat, ezért $4^{74} \equiv 16 \pmod{70}$ vagy $4^{74} \equiv 51 \pmod{70}$. (1 pont)
Az utóbbi eset azonban lehetetlen, mert 4^{74} páros és így nem adhat 70-nel osztva 51 maradékot. Ezért $4^{74} \equiv 16 \pmod{70}$. (3 pont)

3. Az origón áthaladó S sík tartalmazza az $\frac{x-4}{9} = \frac{3-y}{2} = \frac{z-1}{6}$ egyenletrendszerű e egyenest. Rajta van-e a $P(9;5;3)$ pont az S síkon?

* * * * *

Az e egyenletrendszeréből (a középső tört $\frac{y-3}{-2}$ alakba való átírása után) kiolvasható, hogy e átmegy a $Q(4;3;1)$ ponton és egy irányvektora $\underline{v} = (9;-2;6)$. (2 pont)
Mivel az origó S-en van, ezért S-sel párhuzamos az origóból a Q-ba mutató $\underline{q} = (4;3;1)$ vektor. (1 pont)
S-nek normálvektora lesz az $\underline{n} \neq \underline{0}$ vektor, ha az merőleges $\underline{q}$-ra és $\underline{v}$-re is. (1 pont)
Az $\underline{n} = (a,b,c) \neq \underline{0}$ pontosan akkor ilyen, ha az $\underline{n} \cdot \underline{q}$ és az $\underline{n} \cdot \underline{v}$ skaláris szorzatok értéke 0. (1 pont)
A skaláris szorzat képletéből: $4a + 3b + c = 0$ és $9a - 2b + 6c = 0$. (1 pont)
Az első egyenlet 6-szorosából a másodikat kivonva $15a + 20b = 0$, vagyis $3a + 4b = 0$ következik. Így például az $a = 4$, $b = -3$ választással mindkét egyenletből $c = -7$ adódik, vagyis $\underline{n} = (4;-3;-7)$ normálvektora S-nek. (1 pont)
Ebből (például) az origót használva felírható S egyenlete: $4x - 3y - 7z = 0$. (2 pont)
Ebbe a $P(9;5;3)$ pont koordinátáit behelyettesítve az egyenlet teljesül, ezért P rajta van S-en. (1 pont)

A hiánytalan megoldáshoz valójában hozzátartozna annak ellenőrzése is, hogy az O origó nincs rajta e-n (és így $\underline{v} \nparallel \underline{q}$). Mivel azonban a feladat szövege implicite állítja S egyértelműségét és ezáltal az $O \notin e$ állítást, ezért ennek a hiányáért nem vonunk le pontot. A feladat megoldható azt a gondolatot használva is, hogy P akkor és csak akkor van S-en, ha a $\underline{p} = \overrightarrow{OP} = (9; 5; 3)$ helyvektor előáll a $\underline{v}$ és $\underline{q}$ vektorok lineáris kombinációjaként (mert S origón átmenő sík); így a $\underline{p} = \frac{1}{5}\underline{v} + \frac{9}{5}\underline{q}$ állítás mutatja, hogy $P \in S$.

4. Álljon a $V \subseteq \mathbb{R}^4$ halmaz azokból az $\mathbb{R}^4$-beli vektorokból, amelyeknek az első két koordinátája egyenlő. A $W \subseteq \mathbb{R}^4$ halmaz pedig azokból az $\mathbb{R}^4$-beli vektorokból álljon, amiknek az utolsó két koordinátája egyenlő.

a) Alteret alkot-e $\mathbb{R}^4$-ben a $V \cap W$ halmaz?

b) Alteret alkot-e $\mathbb{R}^4$-ben a $V \cup W$ halmaz?

* * * * *

a) $(V \cap W)$-ben azok az $(x_1, x_2, x_3, x_4)^T \in \mathbb{R}^4$ vektorok vannak, amelyekre $x_1 = x_2$ és $x_3 = x_4$.(1 pont)
Ezért ha $\underline{v} = (x_1, x_2, x_3, x_4)^T \in V \cap W$ és $\underline{w} = (y_1, y_2, y_3, y_4)^T \in V \cap W$, akkor $\underline{v} + \underline{w} = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4)^T \in V \cap W$ szintén teljesül, mert az $x_1 = x_2$ és $y_1 = y_2$ egyenlőségekből $x_1 + y_1 = x_2 + y_2$ következik és ezzel analóg módon adódik $x_3 + y_3 = x_4 + y_4$ is. (1 pont)
Hasonlóan, ha $\underline{v} = (x_1, x_2, x_3, x_4)^T \in V \cap W$ és $\lambda \in \mathbb{R}$, akkor $\lambda \cdot \underline{v} = (\lambda \cdot x_1, \lambda \cdot x_2, \lambda \cdot x_3, \lambda \cdot x_4)^T \in V \cap W$ is teljesül, mert az $x_1 = x_2$, illetve $x_3 = x_4$ egyenlőségekből $\lambda \cdot x_1 = \lambda \cdot x_2$, illetve $\lambda \cdot x_3 = \lambda \cdot x_4$ adódik.(1 pont)
Mindezekből következik, hogy $V \cap W$ altér $\mathbb{R}^4$-ben. (2 pont)
A teljes értékű indokláshoz hozzátartozna az is, hogy $V \cap W \neq \emptyset$; ennek hiányáért nem vonunk le pontot, de ha egy megoldó ezt leírja, akkor kaphat érte 1 pontot abban az esetben, ha ezzel az a) feladatra járó összpontszáma nem haladja meg az 5-öt.

b) $\underline{v} = (0, 0, 1, 2)^T \in V$ és $\underline{w} = (1, 2, 0, 0)^T \in W$ a V és a W definíciója szerint, így $\underline{v}$ és $\underline{w}$ is $(V \cup W)$-beli. Azonban a $\underline{v} + \underline{w} = (1, 2, 1, 2)$ vektor nem $(V \cup W)$-beli, mert ez a vektor sem V-be, sem W-be nem tartozik. (3 pont)
Mivel $\underline{v}, \underline{w} \in V \cup W$, de $\underline{v} + \underline{w} \notin V \cup W$, ezért az altér definíciója sérül, vagyis $V \cup W$ nem altér.(2 pont)
Ha egy megoldó az összegre való zártság sérülésére nem tud példát mutatni, de megmutatja, hogy $\underline{v} \in V \cup W$ és $\lambda \in \mathbb{R}$ esetén $\lambda \cdot \underline{v} \in V \cup W$ is teljesül, akkor – noha ez közvetlenül nem járul hozzá egy helyes megoldáshoz – ezért 1 pontot kaphat; ha pedig a megoldásban nyoma van annak, hogy az összegre való zártságot is elkezdi vizsgálni (és nem csak felírja), akkor ezért további 1 pont adható. (Ez az 1 vagy $1 + 1$ pont tehát csak akkor adható meg, ha a fenti pontozás szerint a b) feladatra egyébként nem járna pont.)

5. A p valós paraméter milyen értékeire lineárisan függetlenek az alábbi, $\mathbb{R}^4$-beli $\underline{u}$, $\underline{v}$, $\underline{w}$ vektorok?

$$\underline{u} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ p \end{pmatrix}, \ \underline{v} = \begin{pmatrix} 1 \\ -1 \\ p \\ 8 \end{pmatrix}, \ \underline{w} = \begin{pmatrix} -2 \\ -1 \\ 1 \\ p \end{pmatrix}$$

* * * * *

Tegyük fel, hogy $\alpha \cdot \underline{u} + \beta \cdot \underline{v} + \gamma \cdot \underline{w} = \underline{0}$ teljesül valamilyen $\alpha, \beta, \gamma \in \mathbb{R}$ skalárokra. (1 pont)
Behelyettesítve $\underline{u}, \underline{v}, \underline{w}$ konkrét értékét és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} \alpha + \beta - 2\gamma &= 0 \\ 2\alpha - \beta - \gamma &= 0 \\ 3\alpha + p \cdot \beta + \gamma &= 0 \\ p \cdot \alpha + 8\beta + p \cdot \gamma &= 0 \end{aligned} \qquad \text{(2 pont)}$$

Az első két egyenlet összegéből $3\alpha - 3\gamma = 0$, vagyis $\alpha = \gamma$. Ezt az első két egyenlet közül bármelyikbe visszahelyettesítve $\alpha = \beta = \gamma$ adódik. (1 pont)
Ezt az utolsó két egyenletbe helyettesítve $(4 + p) \cdot \alpha = 0$, illetve $(8 + 2p) \cdot \alpha = 0$ adódik. (1 pont)
Ha $p = -4$, akkor ez a két egyenlet minden α-ra teljesül. Így ebben az esetben például $\alpha = \beta = \gamma = 1$ megoldása a fenti egyenletrendszernek, ezért a tanultak szerint $\underline{u}$, $\underline{v}$ és $\underline{w}$ lineárisan összefüggők. (2 pont)
Ha viszont $p \neq -4$, akkor a $(4 + p) \cdot \alpha = 0$ egyenletből $\alpha = 0$, amiből $\beta = \gamma = 0$ is adódik. Így ebben az esetben $\underline{u}$, $\underline{v}$ és $\underline{w}$ lineárisan függetlenek. (3 pont)
Így a feladat kérdésére a válasz: $\underline{u}$, $\underline{v}$ és $\underline{w}$ a $p \neq -4$ értékekre lineárisan függetlenek.

A fenti lineáris egyenletrendszer Gauss-eliminációval is megoldható (annak ellenére is, hogy ez nem az első zárthelyi anyagában szerepel). Ha valaki így dolgozik, akkor az eliminációért 2 pont jár, majd annak az eredményéből a $p = -4$, illetve a $p \neq -4$ esetben a helyes következtetés (világosan megindokolt) levonásáért 2, illetve 3 pont jár. Ebből a $2+3$ pontból pedig $1+1$ pont jár az egyenletrendszerre vonatkozó következtetésért (végtelen sok megoldása van, illetve egyértelműen megoldható) és $1+2$ pont a vektorok lineáris függetlenségére vonatkozó helyes következtetésért.

6*. Legyen $f(n) = n^{n+1}$ és $g(n) = (n+2)^{n+3}$ minden $n \geq 1$ esetén. Mutassuk meg, hogy végtelen sok olyan n egész létezik, amire fennáll az $f(n)^{g(n)} \equiv 1 \pmod{g(n)}$ kongruencia.

* * * * *

Megmutatjuk, hogy ha $n > 0$ és $n+2$ prímszám, akkor a feladatbeli kongruencia fennáll. Mivel a tanultak szerint a prímek száma végtelen, ezért ebből a feladat állítása következik. (2 pont)
Tegyük fel tehát, hogy $n+2 > 2$ prím. Ekkor a tanult képlet szerint $\varphi(g(n)) = (n+2)^{n+3} - (n+2)^{n+2} = (n+2)^{n+2} \cdot (n+2-1) = (n+1) \cdot (n+2)^{n+2}$. (2 pont)
Mivel $g(n)$ egyedüli prímosztója $n+2$, ez nyilván nem szerepelhet n prímtényezős felbontásában. Így $(n, g(n)) = 1$. (1 pont)
Alkalmazva az Euler-Fermat tételt n-re és $g(n)$-re: $n^{(n+1)\cdot(n+2)^{n+2}} \equiv 1 \pmod{g(n)}$. (2 pont)
Ezt a kongruenciát az $(n+2)$-edik hatványra emelve: $n^{(n+1)\cdot(n+2)^{n+3}} \equiv 1 \pmod{g(n)}$. (2 pont)
Ez pedig $f(n)$ és $g(n)$ definíciói szerint épp a bizonyítandó állítás. (1 pont)