Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2022. október 18.

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 legföljebb 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. Hány olyan egész szám van 1 és 10 000 között, aminek az utolsó két számjegye (a tízes számrendszerben) 34 és a hexadecimális alakjának az utolsó jegye `E`? (A hexadecimális számrendszerben az `E` a 14-es számjegyet jelöli.)

* * * * *

Egy, a feladat feltételeinek megfelelő n egészre $n \equiv 34 \pmod{100}$ és $n \equiv 14 \pmod{16}$ adódik. (1 pont)
A kapott kongruenciarendszert a tanult módszerrel oldjuk meg. Az első kongruenciából $n = 100k + 34$ valamilyen k egészre. (1 pont)
Ezt a másodikba helyettesítve: $100k + 34 \equiv 14 \pmod{16}$. Mindkét oldalból 34-et levonva a $100k \equiv -20 \pmod{16}$ lineáris kongruenciát kapjuk. (1 pont)
Ez a lineáris kongruencia $(100, 16) = 4 \mid -20$ miatt megoldható. (0 pont)
$100 \equiv 4 \pmod{16}$ és $-20 \equiv 12 \pmod{16}$ miatt a lineáris kongruencia $4k \equiv 12 \pmod{16}$ alakba is írható. (1 pont)
Mindkét oldalt 4-gyel osztva: $k \equiv 3 \pmod{4}$, ahol a modulust $(4, 16) = 4$ miatt osztottuk 4-gyel. (1 pont)
Mivel az osztás ekvivalens átalakítás volt, ezért $k \equiv 3 \pmod{4}$ valóban a lineáris kongruencia megoldáshalmazát adja meg. (2 pont)
Ebből tehát $k = 4\ell + 3$ valamely ℓ egészre. Ezt visszahelyettesítve: $n = 100k + 34 = 100(4\ell + 3) + 34 = 400\ell + 334$. (2 pont)
Mivel ez az $\ell = 0, 1, \ldots, 24$ értékekre esik 1 és 10000 közé, ezért 25 darab, a feladat feltételeinek megfelelő egész szám létezik. (1 pont)
A megoldás közben előállt lineáris kongruencia természetesen más tanult módszerekkel, így akár az Euklideszi algoritmussal is megoldható. Aki a fent leírthoz hasonló utat választ, az a lépések ekvivalenciájára való hivatkozást kiválthatja ellenőrzéssel vagy arra való hivatkozással, hogy a tanultak szerint a megoldások száma modulo 16 $(100, 16) = 4$, ami megfelel a kapott $k \equiv 3 \pmod{4}$ eredménynek (hiszen az $k \equiv 3, 7, 11$ vagy $15 \pmod{16}$ alakba is írható).

2. Egész szám-e az alábbi?

$$\frac{5 \cdot 279^{961} + 5}{1400}$$

* * * * *

A kérdés az, hogy $5 \cdot 279^{961} + 5$ osztható-e 1400-zal. (1 pont)
$\varphi(1400) = \varphi(2^3 \cdot 5^2 \cdot 7) = (2^3 - 2^2)(5^2 - 5)(7 - 1) = 480$ a tanult képlet szerint. (1 pont)
$(279, 1400) = 1$, mert 279 se 2-vel, se 5-tel, se 7-tel nem osztható. (1+1 pont)
Így az Euler-Fermat tételből $279^{480} \equiv 1 \pmod{1400}$ következik. (1 pont)
Ezt négyzetre emelve: $279^{960} \equiv 1^2 = 1 \pmod{1400}$ adódik. (1 pont)
Mindkét oldalt 279-cel szorozva: $279^{961} \equiv 279 \pmod{1400}$. (1 pont)
Most mindkét oldalt 5-tel szorozva: $5 \cdot 279^{961} \equiv 5 \cdot 279 = 1395 \equiv -5 \pmod{1400}$. (1 pont)
Így (a kongruencia definíciója szerint) $1400 \mid 5 \cdot 279^{961} + 5$, (2 pont)
vagyis a feladatban szereplő szám egész szám.
Megjegyezzük, hogy a feladat valójában egyszerűbben, az Euler-Fermat tétel alkalmazása nélkül is megoldható. Ugyanis 5-tel való egyszerűsítés után a feladatbeli tört alakja: $\frac{279^{961}+1}{280}$. Ennek az egész volta pedig könnyen következik a $279 \equiv -1 \pmod{280}$ kongruencia 961-edik hatványra emeléséből: $279^{961} \equiv (-1)^{961} = -1 \pmod{280}$. Ebből tehát $280 \mid 279^{961} + 1$ valóban adódik.

3. A tanult Euklideszi algoritmus segítségével határozzuk meg az összes olyan egészt 0 és 301 között, aminek a 222-szerese 34 maradékot ad 302-vel osztva. (A feladat tehát nem csupán a keresett számok meghatározása, hanem a tanult algoritmus futtatása és a működése közben végzett számítások dokumentálása is.)

* * * * *

A feladat a $222x \equiv 34 \pmod{302}$ lineáris kongruencia megoldása (az Euklideszi algoritmussal). (1 pont)
Az algoritmus először meghatározza $(222, 302)$ értékét: (1 pont)

$$\begin{aligned} 302 &= 1 \cdot 222 + 80 \\ 222 &= 2 \cdot 80 + 62 \\ 80 &= 1 \cdot 62 + 18 \\ 62 &= 3 \cdot 18 + 8 \\ 18 &= 2 \cdot 8 + 2 \\ 8 &= 4 \cdot 2 + 0 \end{aligned}$$

(2 pont)

Így $(222, 302) = 2$. (1 pont)
Mivel ez 1-nél nagyobb, ezért a lineáris kongruenciát leosztjuk vele: $111x \equiv 17 \pmod{151}$. (1 pont)
Az így kapott alakkal folytatjuk az algoritmus végrehajtását:

$$\begin{array}{rll} (*)\ 151x \equiv 0 & & \pmod{151} \\ (B)\ 111x \equiv 17 & & \pmod{151} \\ (*) - 1 \cdot (B) : (1) & 40x \equiv -17 & \pmod{151} \\ (B) - 2 \cdot (1) : (2) & 31x \equiv 51 & \pmod{151} \\ (1) - 1 \cdot (2) : (3) & 9x \equiv -68 & \pmod{151} \\ (2) - 3 \cdot (3) : (4) & 4x \equiv 255 \equiv 104 & \pmod{151} \\ (3) - 2 \cdot (4) : (5) & x \equiv -276 \equiv 26 & \pmod{151} \end{array}$$

(2 pont)

Így a lineáris kongruenciát kielégítő egészek 0 és 301 között: 26 és 177. (2 pont)
Ha egy megoldó $(222, 302)$ meghatározását nem az algoritmussal végzi (hanem például a prímtényezős felbontás alapján), az a fenti pontozás szerint a legnagyobb közös osztó számításáért járó 2 pontot veszítse el. Ha egy megoldó egyáltalán nem foglalkozik a legnagyobb közös osztó számításával, hanem a kongruenciák kivonásán alapuló lépéssort a $222x \equiv 34 \pmod{302}$ kongruenciával kezdi, az a tanult algoritmus ismeretének az alapvető hiányát mutatja, így a lineáris kongruencia felírásáért járó 1 ponton kívül a számolásért legföljebb további 1 pontot kaphat; ha azonban a számolás végén (a $2x \equiv 52 \pmod{302}$ kongruencia 2-vel való osztása után) kapott eredményről helyesen megmutatja, hogy ezzel valóban a lineáris kongruencia megoldásait kapja, akkor ezért további 2 pont adható. (Így tehát egy ilyen, nem a legnagyobb közös osztóval való leosztással induló – és így nem a tanult algoritmust követő – megoldás összesen legföljebb 4 pontot érhet.)

4. Írjuk fel annak a síknak az egyenletét, ami tartalmazza az e egyenest és nincs közös pontja az f egyenessel, ahol e és f egyenletrendszerei az alábbiak:

$$e: \quad \frac{x-1}{2} = 5-y,\ z=2 \qquad\qquad f: \quad \frac{x}{7} = \frac{1-2y}{12} = 8-z$$

* * * * *

Az e egyenes egyenletrendszerét $\frac{x-1}{2} = \frac{y-5}{-1},\ z=2$ alakba írva kiolvasható, hogy e átmegy a $P(1;5;2)$ ponton és irányvektora a $\underline{v}_e = (2;-1;0)$ vektor. (2 pont)
Hasonlóan, f egyenletrendszerét $\frac{x-0}{7} = \frac{y-1/2}{-6} = \frac{z-8}{-1}$ alakba írva kiolvasható, hogy f (átmegy a $Q(0;1/2;8)$ ponton és) irányvektora a $\underline{v}_f = (7;-6;-1)$ vektor. (2 pont)
Mivel S tartalmazza e-t és nincs közös pontja f-fel, ezért mindkettővel párhuzamos. Így az $\underline{n}$ vektor akkor lesz normálvektora S-nek, ha merőleges $\underline{v}_e$-re és $\underline{v}_f$-re is (és $\underline{n} \neq \underline{0}$). (1 pont)
Ebből $\underline{v}_e \cdot \underline{n} = 0$ és $\underline{v}_f \cdot \underline{n} = 0$ következik (a skaláris szorzat definíciója szerint). (1 pont)
Ha $\underline{n} = (a,b,c)$, akkor ebből (a skaláris szorzat kiszámítására tanultak miatt) $2a-b=0$ és $7a-6b-c=0$ adódik. (1 pont)
Az első egyenletből $b=2a$, ezt a másodikba helyettesítve $c=-5a$. Így például $\underline{n} = (1;2;-5)$ normálvektora S-nek. (1 pont)
S átmegy a P-n (mert tartalmazza e-t). Így ebből és $\underline{n}$-ből felírható S egyenlete: $x+2y-5z=1$. (2 pont)

5. Álljon a $V \subseteq \mathbb{R}^5$ halmaz azokból az $\mathbb{R}^5$-beli vektorokból, amelyek első három koordinátájának az összege legalább annyi, mint az utolsó két koordinátájuk összege. Alteret alkot-e $\mathbb{R}^5$-ben a V halmaz?

* * * * *

A $\underline{v} = (1,0,0,0,0)^T$ vektor V-beli (mert $1+0+0 \geq 0+0$). Azonban a $(-1)\cdot\underline{v} = (-1,0,0,0,0)^T$ vektor nem V-beli (mert $-1+0+0 < 0+0$). (6 pont)
Mivel $\underline{v} \in V$, de $(-1)\cdot\underline{v} \notin V$, ezért az altér definíciója sérül, vagyis V nem altér. (4 pont)
Bár ez közvetlenül nem járul hozzá egy helyes megoldáshoz, de ha egy megoldó (hiánytalanul) megmutatja, hogy $\underline{u},\underline{v} \in V$ esetén $\underline{u}+\underline{v} \in V$ is teljesül, akkor ezért 4 pontot kaphat; ha pedig a megoldásban nyoma van annak, hogy a skalárral való szorzásra való zártságot is elkezdi vizsgálni (és nem csak felírja), akkor ezért további 1 pont adható.

6*. Az $\mathbb{R}^n$-beli $\underline{a},\underline{b},\underline{c},\underline{d}$ vektorokról tudjuk, hogy az $\underline{a},\underline{b},\underline{c}$ vektorok lineárisan függetlenek, de az $\underline{a}+\underline{b}+\underline{c}$, $\underline{a}-\underline{b}-3\underline{d}$, $\underline{a}+\underline{c}+5\underline{d}$ vektorok lineárisan összefüggők. Következik-e ebből, hogy $\underline{d} \in \langle \underline{a},\underline{b},\underline{c}\rangle$?

* * * * *

Az $\underline{a}+\underline{b}+\underline{c}$, $\underline{a}-\underline{b}-3\underline{d}$, $\underline{a}+\underline{c}+5\underline{d}$ vektorok lineáris összefüggősége azt jelenti, hogy léteznek olyan α,β,γ skalárok, amik között van 0-tól különböző és $\alpha(\underline{a}+\underline{b}+\underline{c})+\beta(\underline{a}-\underline{b}-3\underline{d})+\gamma(\underline{a}+\underline{c}+5\underline{d}) = \underline{0}$. (2 pont)
Átrendezve: $(\alpha+\beta+\gamma)\underline{a}+(\alpha-\beta)\underline{b}+(\alpha+\gamma)\underline{c}+(5\gamma-3\beta)\underline{d} = \underline{0}$. (1 pont)
Megmutatjuk, hogy $5\gamma-3\beta \neq 0$. Tegyük fel ugyanis, hogy ez nem igaz: $5\gamma-3\beta=0$. Ekkor az előző egyenletből $(\alpha+\beta+\gamma)\underline{a}+(\alpha-\beta)\underline{b}+(\alpha+\gamma)\underline{c} = \underline{0}$ adódik, amiből az $\underline{a},\underline{b},\underline{c}$ vektorok lineáris függetlensége miatt $\alpha+\beta+\gamma=0$, $\alpha-\beta=0$ és $\alpha+\gamma=0$. (1 pont)
Itt a második, illetve harmadik egyenletből $\beta=\alpha$, illetve $\gamma=-\alpha$. Ezeket az elsőbe visszahelyettesítve $\alpha=0$, amiből $\beta=0$ és $\gamma=0$ is következik. (1 pont)
Ez viszont ellentmond annak, hogy α, β és γ között van 0-tól különböző és így valóban igazolja az $5\gamma-3\beta\neq 0$ állítást. (1 pont)
Így a fenti, átrendezés után kapott egyenletből a következőt nyerhetjük:

$$\underline{d} = \frac{\alpha+\beta+\gamma}{3\beta-5\gamma}\underline{a} + \frac{\alpha-\beta}{3\beta-5\gamma}\underline{b} + \frac{\alpha+\gamma}{3\beta-5\gamma}\underline{c}. \qquad \text{(2 pont)}$$

Ebből pedig következik a $\underline{d} \in \langle \underline{a},\underline{b},\underline{c}\rangle$ állítás (hiszen $\underline{d}$ kifejezhető lineáris kombinációval az $\underline{a},\underline{b},\underline{c}$ vektorokból). (2 pont)
A feladat kérdésére tehát a válasz: igen, következik.