Bevezetés a számításelméletbe I.
Zárthelyi feladatok az ELSŐ zárthelyi pótlására — pontozási útmutató
2017. december 11.

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.

1. Adjuk meg az összes olyan négyjegyű pozitív egész számot, amelyre teljesül, hogy 51-gyel osztva 3 maradékot ad, továbbá a szám 17-szeresének utolsó két számjegye 15.

* * * * *

A keresett számot n-nel jelölve a feladat feltételei: $n \equiv 3 \pmod{51}$ és $17n \equiv 15 \pmod{100}$. (1 pont)
Az utóbbi feltétel egy lineáris kongruencia, ezt a tanult módszerekkel oldjuk meg.
Mindkét oldalt 6-tal szorozva: $102n \equiv 90 \pmod{100}$, vagyis $2n \equiv 90 \pmod{100}$. (1 pont)
Mindkét oldalt 2-vel osztva: $n \equiv 45 \pmod{50}$, ahol a modulust $(2, 100) = 2$ miatt osztottuk 2-vel. (1 pont)
Ebből $n \equiv 45 \pmod{100}$ vagy $n \equiv 95 \pmod{100}$. Ellenőrzéssel azt kapjuk, hogy a két megoldás közül az első hamis gyök (ami a 6-tal szorzás miatt jött be, hiszen $(6, 100) \neq 1$), a második viszont helyes. (1 pont)
Azokat az n-eket keressük tehát, amik kielégítik az $n \equiv 95 \pmod{100}$ és az $n \equiv 3 \pmod{51}$ feltételeket.
Ez egy kongruenciarendszer, amit a tanult módszerrel oldunk meg. (1 pont)
Az első feltételből: $n = 100k + 95$ valamely k egészre. Ezt a másodikba helyettesítve: $100k + 95 \equiv 3 \pmod{51}$. Mindkét oldalból 95-öt levonva a $100k \equiv -92 \pmod{51}$ lineáris kongruenciát kapjuk. (1 pont)
$100 \equiv -2 \pmod{51}$ miatt ez a $-2k \equiv -92 \pmod{51}$ alakba írható. (1 pont)
(-2)-vel osztva: $k \equiv 46 \pmod{51}$, ahol a modulus $(-2, 51) = 1$ miatt nem változott. Mivel mindkét megtett lépésünk ekvivalens átalakítás volt, ezzel valóban a lineáris kongruencia megoldását kaptuk. (1 pont)
Ebből tehát $k = 51\ell + 46$ valamely ℓ egészre. Ezt visszahelyettesítve: $n = 100k + 95 = 100(51\ell + 46) + 95 = 5100\ell + 4695$. (1 pont)
Így a feladat feltételeit az $n \equiv 4695 \pmod{5100}$ feltételt kielégítő n egészek teljesítik. Ezek közül a 4695 és a 9795 négyjegyű pozitív egészek, így a feladatnak ez a két megoldása van. (1 pont)
A feladat rövidebben is megoldható, ha az $n \equiv 3 \pmod{51}$ feltételből kapott $n = 51k + 3$ alakot helyettesítjük az n helyére a $17n \equiv 15 \pmod{100}$ kongruenciában. A megoldás során előkerülő lineáris kongruenciák az Euklideszi algoritmussal is megoldhatók. (Ez mindegyik esetben közvetlenül alkalmazható, mert az ismeretlen együtthatója a modulushoz relatív prím.) Aki a fent leírthoz hasonló utat választ, annak az első esetben a két ellenőrzés közül az egyik, a második esetben a lépések ekvivalenciájára való hivatkozás kiváltható azzal, hogy a megoldások száma mindkét esetben előre tudhatóan 1 lesz, mert az ismeretlen együtthatója a modulushoz relatív prím.

2. Milyen maradékot ad 108-cal osztva $73^{37} + 37^{73}$?

$* \quad * \quad * \quad * \quad *$

108 prímtényezős felbontása: $108 = 2^2 \cdot 3^3$. (1 pont)
Ezért a tanult képlet szerint $\varphi(108) = (2^2 - 2^1)(3^3 - 3^2) = 36$. (1 pont)
Mivel $(73, 108) = 1$, (1 pont)
ezért az Euler-Fermat tételből $73^{36} \equiv 1 \pmod{108}$ következik. (1 pont)
Mindkét oldalt 73-mal szorozva: $73^{37} \equiv 73 \pmod{108}$. (1 pont)
Mivel $(37, 108) = 1$ is igaz, (1 pont)
ezért ismét az Euler-Fermat tételből $37^{36} \equiv 1 \pmod{108}$ következik. (1 pont)
Mindkét oldalt négyzetre emelve: $37^{72} \equiv 1^2 = 1 \pmod{108}$. (1 pont)
Mindkét oldalt 37-tel szorozva: $37^{73} \equiv 37 \pmod{108}$. (1 pont)
A kapott $73^{37} \equiv 73 \pmod{108}$ és $37^{73} \equiv 37 \pmod{108}$ kongruenciákat a tanult szabály szerint összeadva: $73^{37} + 37^{73} \equiv 73 + 37 = 110 \equiv 2 \pmod{108}$, (1 pont)
vagyis a keresett maradék a 2.
A feladat elvileg megoldható az ismételt négyzetre emelések módszerével is, de az (számológép nélkül) sokkal kellemetlenebb és hosszabb megoldásra vezet; ha egy hallgató ilyen megoldással próbálkozik (és az ahhoz szükséges számításokat legalább elkezdi), akkor legföljebb 2 pontot kaphat pusztán annak felismeréséért, hogy ez az algoritmus elvileg alkalmas a két hatvány 108-as maradékának meghatározására.

3. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg 5^{85}-nek a 155-tel vett osztási maradékát.

$* \quad * \quad * \quad * \quad *$

A tanultak szerint ismételt négyzetre emelésekkel és a kapott eredmények 155-ös maradékának meghatározásával kiszámítjuk az $5^1, 5^2, 5^4, \ldots, 5^{64}$ hatványok 155-ös maradékát. Ezek sorra: 5, 25, 5 (mert $625 \equiv 5 \pmod{155}$), 25, 5, 25 és 5. (4 pont)
Mivel $85 = 1 + 4 + 16 + 64$, (2 pont)
ezért sorra meghatározzuk az $5^5 = 5^1 \cdot 5^4$, $5^{21} = 5^5 \cdot 5^{16}$, végül az $5^{85} = 5^{21} \cdot 5^{64}$ hatványok 155-ös maradékait a korábban kiszámolt megfelelő maradékokkal való szorzással és a kapott eredmények 155-ös maradékának meghatározásával. Ezek sorra: 25, 125 és 5. (4 pont)
Így a keresett maradék: 5.
A teljes értékű megoldáshoz nem szükséges a fenti részletességgel leírni az elvégzett műveletek mögötti szándékot, elegendő a helyes számítások közlése. Nem jelent pontlevonást, ha egy megoldó a végeredményhez először $5^{80} = 5^{64} \cdot 5^{16}$, majd sorban 5^{84} és végül 5^{85} maradékait határozza meg a fentihez hasonló módon. Ha viszont egy megoldó a kapott részeredményeit nem helyettesíti azok 155-ös maradékaival és például 5^8 maradékához a 625 négyzetre emelésével próbál eljutni, az lényeges elvi hibának számít, ami az algoritmus ismeretének alapvető hiányát mutatja; egy ilyen megoldó legföljebb 5 pontot kaphat (azt is csak akkor, ha a további számolásai hasznosak és a helyes végeredményt megkapja).

4. Van-e az $A(-1;-2;1)$, $B(3;1;3)$ és $C(7;6;3)$ pontokat tartalmazó síknak olyan pontja, amely az y-tengelyre esik? Ha igen, melyik?

$* \quad * \quad * \quad * \quad *$

$\overrightarrow{AB} = \underline{b} - \underline{a} = (3;1;3) - (-1,-2;1) = (4;3;2)$ és $\overrightarrow{AC} = \underline{c} - \underline{a} = (7;6;3) - (-1,-2;1) = (8;8;2)$, ahol $\underline{a}$, $\underline{b}$ és $\underline{c}$ a megfelelő pontokba mutató helyvektorokat jelöli. (1 pont)
Az A, B és C pontokat tartalmazó S síknak normálvektora lesz az $\underline{n} \neq \underline{0}$ vektor, ha az merőleges $\overrightarrow{AB}$-re és $\overrightarrow{AC}$-re is. (1 pont)
Így az $\underline{n} = (p,q,r) \neq \underline{0}$ pontosan akkor ilyen, ha az $\underline{n} \cdot \overrightarrow{AB}$ és az $\underline{n} \cdot \overrightarrow{AC}$ skaláris szorzatok értéke 0.(1 pont)
A skaláris szorzat képletéből: $4p + 3q + 2r = 0$ és $8p + 8q + 2r = 0$. (1 pont)
A második egyenlet feléből az elsőt kivonva: $q - r = 0$, vagyis $q = r$. Ezt bármelyik egyenletbe helyettesítve a $4p + 5r = 0$ egyenletet kapjuk. Így például $r = -4$ választással $p = 5$ és $q = -4$ adódik, vagyis $\underline{n} = (5;-4;-4)$ normálvektora S-nek. (2 pont)
Ebből A, B és C közül bármelyiket használva felírható S egyenlete: $5x - 4y - 4z = -1$. (1 pont)

A $P(x, y, z)$ pont akkor és csak akkor van az y tengelyen, ha $x = z = 0$. (1 pont)
Ezt S egyenletébe helyettesítve: $-4y = -1$, vagyis $y = \frac{1}{4}$. Így az S-en az y-tengelynek egyetlen pontja van: a $(0; \frac{1}{4}; 0)$. (2 pont)
A fenti megoldásban a normálvektor kiszámítására vonatkozó rész helyettesíthető az $\overrightarrow{AB} \times \overrightarrow{AC}$ vektoriális szorzat meghatározásával is. (Ebből közvetlenül a $(-10; 8; 8)$ vektor adódik, ami a fent kiszámítottnak a (-2)-szerese, így természetesen szintén normálvektora S-nek.)

5. Legyen $\mathbb{R}^4$-ben

$$\underline{u} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix}, \ \underline{v} = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 5 \end{pmatrix} \text{ és } \underline{w} = \begin{pmatrix} 1 \\ 2 \\ 4 \\ 11 \end{pmatrix}.$$

Határozzuk meg az $\langle \underline{u}, \underline{v}, \underline{w} \rangle$ generált alteret. (A generált altér meghatározása alatt azt értjük, hogy készítünk egy olyan „gyorstesztet", amellyel egy tetszőleges $\mathbb{R}^4$-beli vektorról egyszerűen megmondható, hogy a generált altérhez tartozik-e.)

* * * * *

Az $\underline{x} = (p, q, r, s)^T$ vektor definíció szerint pontosan akkor tartozik az $\langle \underline{u}, \underline{v}, \underline{w} \rangle$ generált altérbe, ha léteznek olyan α, β, γ skalárok, amelyekre $\alpha\underline{u} + \beta\underline{v} + \gamma\underline{w} = \underline{x}$. (2 pont)
Elvégezve a műveleteket: $\alpha\underline{u} + \beta\underline{v} + \gamma\underline{w} = (\gamma, \beta + 2\gamma, \alpha + 2\beta + 4\gamma, 2\alpha + 5\beta + 11\gamma)^T$. (2 pont)
Így $\underline{x}$ pontosan akkor van a generált altérben, ha léteznek olyan α, β, γ skalárok, amelyekre $\gamma = p$, $\beta + 2\gamma = q$, $\alpha + 2\beta + 4\gamma = r$ és $2\alpha + 5\beta + 11\gamma = s$. (3 pont)
Ezekből az egyenletekből sorban: $\gamma = p$, $\beta = q - 2\gamma = q - 2p$, $\alpha = r - 2\beta - 4\gamma = r - 2(q - 2p) - 4p = r - 2q$.
Ezt a negyedik egyenletbe helyettesítve: $2(r - 2q) + 5(q - 2p) + 11p = s$, vagyis $p + q + 2r - s = 0$.(2 pont)
Azt kaptuk tehát, hogy $\underline{x} = (p, q, r, s)^T \in \langle \underline{u}, \underline{v}, \underline{w} \rangle$ pontosan akkor igaz, ha $p + q + 2r - s = 0$. (1 pont)

6*. Tegyük fel, hogy a $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{10}, \underline{w} \in \mathbb{R}^n$ vektorokra teljesül, hogy a $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{10}$ rendszer lineárisan független, a $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{10}, \underline{w}$ rendszer viszont lineárisan összefüggő és $\underline{w} \neq \underline{0}$. Mutassuk meg, hogy létezik olyan $1 \leq i \leq 10$ és olyan $\alpha \neq 0$ skalár, hogy a $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{i-1}, \underline{v}_i + \alpha \cdot \underline{w}, \underline{v}_{i+1}, \ldots, \underline{v}_{10}$ rendszer lineárisan összefüggő.

* * * * *

A feladat feltételeiből az újonnan érkező vektor lemmája szerint azonnal következik, hogy $\underline{w} \in \langle \underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{10} \rangle$, (1 pont)
vagyis léteznek a $\lambda_1, \lambda_2, \ldots, \lambda_{10}$ skalárok úgy, hogy $\lambda_1\underline{v}_1 + \lambda_2\underline{v}_2 + \ldots + \lambda_{10}\underline{v}_{10} = \underline{w}$. (1 pont)
Mivel $\underline{w} \neq 0$, ezért a $\lambda_1, \ldots, \lambda_{10}$ együtthatók között van nullától különböző. Legyen például $\lambda_k \neq 0$.(2 pont)
Ekkor a fentiből átrendezéssel:

$$\lambda_1\underline{v}_1 + \ldots + \lambda_{k-1}\underline{v}_{k-1} + \lambda_k\left(\underline{v}_k - \frac{1}{\lambda_k}\underline{w}\right) + \lambda_{k+1}\underline{v}_{k+1} + \ldots + \lambda_{10}\underline{v}_{10} = \underline{0}. \qquad \text{(3 pont)}$$

Mivel $\lambda_k \neq 0$, ez a tanultak szerint azt jelenti, hogy a $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{k-1}, \underline{v}_k - \frac{1}{\lambda_k}\underline{w}, \underline{v}_{k+1}, \ldots, \underline{v}_{10}$ rendszer lineárisan összefüggő. Vagyis a feladat állítása az $i = k$ és $\alpha = -\frac{1}{\lambda_k}$ választással valóban teljesül. (3 pont)