Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2021. október 28.

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. Milyen maradékot ad az n egész szám 106-szorosa 271-gyel osztva, ha tudjuk, hogy ez a maradék 1-gyel több, mint magának az n-nek a 271-es osztási maradéka?

* * * * *

A feladat feltételeiből $106n \equiv n+1 \pmod{271}$. Átrendezve: $105n \equiv 1 \pmod{271}$. (1+1 pont)
Mivel $(105, 271) = 1$ (mert nincs közös prímosztójuk), ezért a kapott lineáris kongruencia a tanult tétel szerint megoldható és 1 megoldása van modulo 271. (1 pont)
Mindkét oldalt 3-mal szorozva: $315n \equiv 3 \pmod{271}$, vagyis $44n \equiv 3 \pmod{271}$. (1 pont)
Most mindkét oldalt 6-tal szorozva: $264n \equiv 18 \pmod{271}$, vagyis $-7n \equiv 18 \pmod{271}$. (1 pont)
Itt mindkét oldalt 39-cel szorozva: $-273n \equiv 702 \pmod{271}$, vagyis $-2n \equiv 160 \pmod{271}$. (1 pont)
Végül mindkét oldalt (-2)-vel osztva: $n \equiv -80 \equiv 191 \pmod{271}$. (1 pont)
Mivel $(3, 271) = 1$, $(6, 271) = 1$ és $(39, 271) = 1$, ezért minden megtett lépés ekvivalens volt, így a kapott $n \equiv 191 \pmod{271}$ valóban megoldása a lineáris kongruenciának. (Itt a lépések ekvivalenciája helyett hivatkozhatunk arra is, hogy mivel a megoldások száma 1 modulo 271, ezért ez csak a 191 lehet, így az valóban megoldás; illetve természetesen ellenőrzéssel is meggyőződhetünk a 191 helyességéről.) (2 pont)
Ebből $n + 1 \equiv 192 \pmod{271}$, így n 106-szorosa is 192 maradékot ad 271-gyel osztva. (1 pont)
Ha a fenti megoldásban a kapott eredmény helyességéről a lépések ekvivalenciájával vagy ellenőrzéssel győződünk meg, akkor a megoldhatóság tényének, illetve a megoldások számának az előzetes megállapítására nincs feltétlen szükség; így a fenti pontozás szerinti második 1 pont az ilyen (egyébként teljes értékű) megoldásokra is jár. A lineáris kongruenciát természetesen a tanult Euklideszi algoritmussal is megoldhatjuk. Ezzel sorra a $271n \equiv 0 \pmod{271}$, $105n \equiv 1 \pmod{271}$, $61n \equiv -2 \pmod{271}$, $44n \equiv 3 \pmod{271}$, $17n \equiv -5 \pmod{271}$, $10n \equiv 13 \pmod{271}$, $7n \equiv -18 \pmod{271}$, $3n \equiv 31 \pmod{271}$, $n \equiv -80 \equiv 191 \pmod{271}$ kongruenciák keletkeznek. Ekkor 1 pontot ér az a tény, hogy a megoldó az algoritmust alkalmazza (amit nem kell feltétlen megneveznie, elég, ha az alkalmazása révén ezt egyértelműen demonstrálja); további 2 pontot ér annak az ellenőrzése, hogy az eljárás a tanultak szerint alkalmazható, mert $(105, 271) = 1$; végül 4 pontot ér maga a számolás. A hiányzó 3 pont a fenti pontozás szerinti első $1 + 1$, illetve utolsó 1 pont.

2. Milyen maradékot ad 600-zal osztva $2021^{2021} - 2021^{101}$?

* * * * *

$\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = (2^3 - 2^2)(3-1)(5^2-5) = 160$ a tanult képlet szerint. (1 pont)
$(2021, 600) = 1$, mert 2021 se 2-vel, se 3-mal, se 5-tel nem osztható. (2 pont)
Így az Euler-Fermat tételből $2021^{160} \equiv 1 \pmod{600}$ következik. (1 pont)
Ezt a 12-edik hatványra emelve: $2021^{1920} \equiv 1^{12} = 1 \pmod{600}$ adódik. (2 pont)
Mindkét oldalt 2021^{101}-nel szorozva: $2021^{2021} \equiv 2021^{101} \pmod{600}$. (2 pont)
Így (a kongruencia definíciója szerint) $600 \mid 2021^{2021} - 2021^{101}$, vagyis a keresett maradék a 0. (2 pont)

3. Határozzuk meg a p paraméter értékét és írjuk fel az S sík egyenletét, ha tudjuk, hogy S tartalmazza az $A(1;2;2)$ és $B(3;4;1)$ pontokat és merőleges arra az e egyenesre, aminek az egyenletrendszere:

$$\frac{2x-7}{12} = \frac{8-y}{5} = \frac{z}{p}.$$

* * * * *

Első megoldás. e egyenletrendszerét átalakítva: $\frac{x-7/2}{6} = \frac{y-8}{-5} = \frac{z}{p}$. Ebből az alakból már kiolvasható e egy irányvektora: $v = (6;-5;p)$ (mert a tanultak szerint e a $(\frac{7}{2};8;0)$ ponton átmenő, $\underline{v}$ irányvektorú egyenes). (3 pont)
Mivel e merőleges S-re, ezért $\underline{v}$ merőleges az $\overrightarrow{AB}$ vektorra, (1 pont)
így $\underline{v} \cdot \overrightarrow{AB} = 0$. (1 pont)
$\overrightarrow{AB} = \underline{b} - \underline{a} = (2;2;-1)$ (ahol $\underline{b}$ és $\underline{a}$ a megfelelő pontokba mutató helyvektorokat jelöli), (1 pont)
amiből $0 = \underline{v} \cdot \overrightarrow{AB} = 6 \cdot 2 - 5 \cdot 2 - p$, vagyis $p = 2$ adódik. (1 pont)
$\underline{v} = (6;-5;2)$ normálvektora S-nek, mert e merőleges S-re. (2 pont)
Ebből és (például) A-ból a tanultak szerint felírható S egyenlete: $6x - 5y + 2z = 0$. (1 pont)

Második megoldás. e egyenletrendszerét átalakítva: $\frac{x-7/2}{6} = \frac{y-8}{-5} = \frac{z}{p}$. Ebből az alakból már kiolvasható e egy irányvektora: $v = (6;-5;p)$ (mert a tanultak szerint e a $(\frac{7}{2};8;0)$ ponton átmenő, $\underline{v}$ irányvektorú egyenes). (3 pont)
$\underline{v}$ normálvektora S-nek, mert e merőleges S-re. (2 pont)
Ezzel és az A ponttal felírva S egyenletét: $6x - 5y + p \cdot z = 6 \cdot 1 - 5 \cdot 2 + p \cdot 2 = 2p - 4$. (1 pont)
Mivel S-en B is rajta van, ezért szintén kielégíti ezt az egyenletet: $6 \cdot 3 - 5 \cdot 4 + p \cdot 1 = 2p - 4$. (2 pont)
Ebből $p - 2 = 2p - 4$, vagyis $p = 2$. (1 pont)
Ezt a fentibe visszahelyettesítve S egyenlete: $6x - 5y + 2z = 0$. (1 pont)

4. Legyenek $\underline{u}$ és $\underline{v}$ az alábbi $\mathbb{R}^3$-beli vektorok. Adjuk meg az $\langle \underline{u}, \underline{v} \rangle$ generált altér összes olyan elemét, aminek a második koordinátája 2-vel, a harmadik 3-mal nagyobb az elsőnél.

$$\underline{u} = \begin{pmatrix} 3 \\ 10 \\ 1 \end{pmatrix}, \ \underline{v} = \begin{pmatrix} 1 \\ -6 \\ -2 \end{pmatrix}.$$

* * * * *

Első megoldás. Legyen $\underline{z}$ egy ilyen vektor. Ekkor $\underline{z} \in \langle \underline{u}, \underline{v} \rangle$ azt jelenti, hogy $\underline{z}$ kifejezhető $\underline{u}$-ból és $\underline{v}$-ből lineáris kombinációval, vagyis léteznek olyan α, β skalárok, hogy $\alpha \cdot \underline{u} + \beta \cdot \underline{v} = \underline{z}$. (2 pont)
$\underline{z}$ első koordinátáját p-vel jelölve és elvégezve a műveleteket a következő egyenletrendszerre jutunk:

$$\begin{aligned} 3\alpha + \beta &= p \\ 10\alpha - 6\beta &= p + 2 \\ \alpha - 2\beta &= p + 3 \end{aligned}$$ (3 pont)

Az első egyenletből p-t a másik kettőbe helyettesítve és rendezve a $7\alpha - 7\beta = 2$, $2\alpha + 3\beta = -3$ egyenletrendszerre jutunk. Ebből $\alpha = -\frac{3}{7}$ és $\beta = -\frac{5}{7}$. Ezt visszahelyettesítve az első egyenletbe: $p = -2$. (3 pont)
Így az $\langle \underline{u}, \underline{v} \rangle$ generált altérnek az egyetlen, a feltételeknek megfelelő eleme a $\underline{z} = (-2;0;1)^T$ vektor .(2 pont)

Második megoldás. $\underline{u}$ és $\underline{v}$ nem párhuzamosak, mert nem skalárszorosai egymásnak, (1 pont)
ezért a tanultak szerint az $\langle \underline{u}, \underline{v} \rangle$ generált altér egy origón átmenő S sík vektoraiból áll. (1 pont)
S-nek normálvektora lesz az $\underline{n} \neq \underline{0}$ vektor, ha az merőleges $\underline{u}$-ra és $\underline{v}$-re is. (1 pont)
Az $\underline{n} = (a, b, c) \neq \underline{0}$ pontosan akkor ilyen, ha az $\underline{n} \cdot \underline{u}$ és az $\underline{n} \cdot \underline{v}$ skaláris szorzatok értéke 0. (1 pont)
A skaláris szorzat képletéből: $3a + 10b + c = 0$ és $a - 6b - 2c = 0$. (1 pont)
Az első egyenlet kétszereséhez a másodikat adva $7a + 14b = 0$, vagyis $a + 2b = 0$ adódik. Így például az $a = 2$, $b = -1$ választással mindkét egyenletből $c = 4$, vagyis $\underline{n} = (2; -1; 4)$ normálvektora S-nek.(1 pont)
Ebből (például) az origót használva felírható S egyenlete: $2x - y + 4z = 0$. (1 pont)
A keresett vektor koordinátáit jelölje sorra $x = p$, $y = p + 2$ és $z = p + 3$. (1 pont)
Ezeket S egyenletébe helyettesítve: $2p - (p + 2) + 4(p + 3) = 0$, amiből $p = -2$ adódik. (1 pont)
Így az $\langle \underline{u}, \underline{v} \rangle$ generált altérnek az egyetlen, a feltételeknek megfelelő eleme a $(-2; 0; 1)^T$ vektor . (1 pont)
A fenti megoldáshoz nem szükséges megfigyelni, hogy a $(p; p + 2; p + 3)$ koordinátájú vektorok a $(0; 2; 3)$ ponton átmenő, $(1, 1, 1)$ irányvektorú egyenes vektorai, így a feladat valójában egy sík és egy egyenes döféspontjának a meghatározását kérte. Ennek ellenére, ezért a megfigyelésért (legföljebb) 2 pont „visszaadható" a pusztán figyelmetlenségekért, számolási hibákért elvesztett esetleges pontok közül (de az érdemi, tartalmi hibákért elvesztettek közül nem - és a feladatért adott összpontszám természetesen semmiképp nem haladja meg a 10-et).

5. A p valós paraméter milyen értékeire alkotnak bázist $\mathbb{R}^4$-ben az alábbi $\underline{a}$, $\underline{b}$, $\underline{c}$, $\underline{d}$ vektorok?

$$\underline{a} = \begin{pmatrix} 2 \\ 2 \\ 2 \\ 2 \end{pmatrix}, \ \underline{b} = \begin{pmatrix} 1 \\ 2 \\ 1 \\ 1 \end{pmatrix}, \ \underline{c} = \begin{pmatrix} 1 \\ 1 \\ 3 \\ 1 \end{pmatrix}, \ \underline{d} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ p \end{pmatrix}$$

* * * * *

Megvizsgáljuk, hogy $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ lineárisan függetlenek-e. Ehhez tegyük fel, hogy $\alpha \cdot \underline{a} + \beta \cdot \underline{b} + \gamma \cdot \underline{c} + \delta \cdot \underline{d} = \underline{0}$ teljesül valamilyen $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ skalárokra. (1 pont)
Behelyettesítve $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ konkrét értékét és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} 2\alpha + \beta + \gamma + \delta &= 0 \\ 2\alpha + 2\beta + \gamma + \delta &= 0 \\ 2\alpha + \beta + 3\gamma + \delta &= 0 \\ 2\alpha + \beta + \gamma + p \cdot \delta &= 0 \end{aligned} \qquad \text{(1 pont)}$$

A második, illetve a harmadik egyenletből az elsőt kivonva $\beta = 0$ és $\gamma = 0$ adódik. Hasonlóan, a negyedik egyenletből az elsőt kivonva: $(p - 1) \cdot \delta = 0$. (1 pont)
Ha $p = 1$, akkor $\alpha = 1$, $\beta = \gamma = 0$, $\delta = -2$ megoldása a lineáris egyenletrendszernek (más szóval: $\underline{a} = 2\underline{d}$), így ebben az esetben $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ lineárisan összefüggők, (1 pont)
így bázist sem alkotnak. (1 pont)
Ha viszont $p \neq 1$, akkor a fenti egyenletből $\delta = 0$ adódik. Ezt (és a $\beta = \gamma = 0$ értékeket) bármelyik egyenletbe helyettesítve $\alpha = 0$ is következik, így a $p \neq 1$ esetben $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ lineárisan függetlenek. (1 pont)
Az előadáson tanultak szerint $\dim \mathbb{R}^4 = 4$, (1 pont)
így a tanult tétel szerint $\mathbb{R}^4$-ben minden 4 elemű, lineárisan független rendszer bázis. Ezért a $p \neq 1$ esetben $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ bázis $\mathbb{R}^4$-ben. (3 pont)
Így a feladat kérdésére a válasz: $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ a $p \neq 1$ értékekre alkot bázist $\mathbb{R}^4$-ben.
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 (a fenti pontozás szerinti harmadiknak írt) 1 pont jár, majd annak az eredményéből a $p = 1$, illetve a $p \neq 1$ esetben a helyes következtetés (világosan megindokolt) levonásáért (a negyediknek, illetve hatodiknak írt) 1-1 pont.

A fenti megoldásban az utolsó $1 + 3$ pont megszerezhető az alábbi, sokkal több számolást igénylő módon is (tételek helyett közvetlenül a definíciók alkalmazásával):

Most megvizsgáljuk, hogy a $p \neq 1$ esetben $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ generátorrendszert alkot-e $\mathbb{R}^4$-ben. Ehhez legyen $\underline{v} = (x, y, z, u)^T \in \mathbb{R}^4$ tetszőleges vektor és keressük az $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ skalárokat úgy, hogy $\alpha \cdot \underline{a} + \beta \cdot \underline{b} + \gamma \cdot \underline{c} + \delta \cdot \underline{d} = \underline{v}$ teljesüljön. Megint behelyettesítve $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ konkrét értékét a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} 2\alpha + \beta + \gamma + \delta &= x \\ 2\alpha + 2\beta + \gamma + \delta &= y \\ 2\alpha + \beta + 3\gamma + \delta &= z \\ 2\alpha + \beta + \gamma + p \cdot \delta &= u \end{aligned} \qquad \text{(1 pont)}$$

A fentihez hasonló számolással: $\beta = y - x$, $\gamma = \frac{1}{2}(z - x)$, $\delta = \frac{1}{p-1}(u - x)$, végül $\alpha = \left(\frac{1}{2(p-1)} + \frac{5}{4}\right) x - \frac{1}{2} y - \frac{1}{4} z - \frac{1}{2(p-1)} u$. (1 pont)
Azt kaptuk tehát, hogy ha $p \neq 1$, akkor az egyenletrendszer minden x, y, z, u esetén megoldható, így $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ generátorrendszert alkot $\mathbb{R}^4$-ben. (1 pont)
Így a $p \neq 1$ esetben $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ bázist alkot $\mathbb{R}^4$-ben. (1 pont)

6*. Határozzuk meg az összes olyan p pozitív prímszámot, amire minden x egész és p-től különböző q pozitív prím esetén az $x^2 \equiv 1 \pmod{p \cdot q}$ kongruenciából $x \equiv 1 \pmod{p \cdot q}$ vagy $x \equiv -1 \pmod{p \cdot q}$ következik.

* * * * *

Először megmutatjuk, hogy $p = 2$ megfelel a feladat feltételének. Legyen ezért $q > 2$ prím és tegyük fel, hogy $x^2 \equiv 1 \pmod{2q}$ teljesül valamely x egészre. Ebből a kongruencia definíciója szerint $2q \mid x^2 - 1 = (x-1)(x+1)$ adódik. (0 pont)
Mivel q prím és $q \mid (x-1)(x+1)$ ezért $x-1$ vagy $x+1$ prímtényezős felbontásában q-nak szerepelnie kell, vagyis $q \mid x-1$ vagy $q \mid x+1$. (1 pont)
$x-1$ és $x+1$ paritása nyilván azonos. Mivel a szorzatuk páros, ezért mindkettőnek párosnak kell lennie, vagyis $2 \mid x-1$ és $2 \mid x+1$. (1 pont)
Így $x-1$ és $x+1$ közül az egyik prímtényezős felbontásában 2 és q is szerepel, vagyis $2q \mid x-1$ vagy $2q \mid x+1$. Az első esetben $x \equiv 1 \pmod{2q}$, a másodikban $x \equiv -1 \pmod{2q}$, így $p = 2$ valóban teljesíti a kívánt feltételt. (1 pont)
Most azt látjuk be, hogy semmilyen $p > 2$ prím nem teljesíti a feladat feltételeit. Legyenek ezért $p, q > 2$, $p \neq q$ tetszőleges prímek. (0 pont)
Tekintsük az $x \equiv 1 \pmod{p}$, $x \equiv -1 \pmod{q}$ kongruenciarendszert; azt állítjuk, hogy ez megoldható. (1 pont)
A kongruenciarendszerek megoldására tanult módszer szerint az első kongruenciából $x = p \cdot k + 1$ valamilyen $k \in \mathbb{Z}$ egészre. Ezt a második kongruenciába helyettesítve: $p \cdot k + 1 \equiv -1 \pmod{q}$. Átrendezve: $p \cdot k \equiv -2 \pmod{q}$. (1 pont)
Mivel $p \neq q$ prímek, ezért nyilván $(p, q) = 1$. Így a tanult tétel szerint (mivel $1 \mid -2$) a $p \cdot k \equiv -2 \pmod{q}$ lineáris kongruencia megoldható. Egy tetszőleges k_0 megoldásra pedig $x_0 = p \cdot k_0 + 1$ valóban megoldása a kongruenciarendszernek. (2 pont)
Ekkor x_0-ra $p \mid x_0 - 1$ és $q \mid x_0 + 1$, így $p \cdot q \mid (x_0 - 1)(x_0 + 1) = x_0^2 - 1$, vagyis $x_0^2 \equiv 1 \pmod{pq}$.(1 pont)
Másrészt sem $x_0 \equiv 1 \pmod{pq}$, sem $x_0 \equiv -1 \pmod{pq}$ nem igaz. Valóban, például az első esetben $pq \mid x_0 - 1$ és így $q \mid x_0 - 1$ adódna. Ez azonban lehetetlen, mert $q \mid x_0 + 1$ (hiszen x_0 teljesíti az $x \equiv -1 \pmod{q}$ kongruenciát) és $q > 2$ miatt q nem lehet $(x_0 - 1)$-nek és $(x_0 + 1)$-nek is osztója. Hasonlóan, a $x_0 \equiv -1 \pmod{pq}$ esetben a $p \mid x_0 + 1$ és $p \mid x_0 - 1$ ellentmondásra jutnánk. (2 pont)
Összefoglalva tehát: a feladat feltételét egyedül a $p = 2$ prím teljesíti. (0 pont)
(Megjegyezzük, hogy a megoldás második felében többet láttunk be annál, mint amit a feladat kíván: ha $p > 2$ prím, akkor egyetlen $q > 2$, $q \neq p$ prím esetén sem következik az $x^2 \equiv 1 \pmod{p \cdot q}$ kongruenciából $x \equiv 1 \pmod{p \cdot q}$ vagy $x \equiv -1 \pmod{p \cdot q}$.)