Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2023. november 3.

Általános alapelvek.

A pontozási útmutató célja, hogy a javítók a dolgozatokat egységesen értékeljék. 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, gondolatért, amely egy megoldásban érdemi szerephez juthat és 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 legfeljebb 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. Adjuk meg az összes olyan n egész számot 1 és 2023 között, amire az $\dfrac{n-2}{21}$ tört és az $\dfrac{n-5}{166}$ tört értéke is egész szám.

* * * * *

A két tört értéke azokra az n-ekre ad egész számot, amikre $n \equiv 2 \pmod{21}$ és $n \equiv 5 \pmod{166}$.(1 pont)
A kapott kongruenciarendszert a tanult módszerrel oldjuk meg. Az első kongruenciából $n = 21k + 2$ valamilyen k egészre. Ezt a másodikba helyettesítve: $21k + 2 \equiv 5 \pmod{166}$. Mindkét oldalból 2-t levonva a $21k \equiv 3 \pmod{166}$ lineáris kongruenciát kapjuk. (1 pont)
Mivel $(21, 166) = 1$ (mert nincs közös prímosztójuk) és $1 \mid 3$, ezért a tanult tételt szerint a lineáris kongruencia megoldható és egyetlen megoldása van modulo 166. (1 pont)
A kongruencia mindkét oldalát 8-cal szorozva $168k \equiv 24 \pmod{166}$, vagyis $2k \equiv 24 \pmod{166}$ következik. (1 pont)
(Ez az átalakítás nem volt ekvivalens lépés, mert $(166, 2) = 2$ és így a $168k \equiv 24 \pmod{166}$ kongruenciát 8-cal osztva nem az eredeti alakot kapnánk vissza.) (0 pont)
Mindkét oldalt 2-vel osztva: $k \equiv 12 \pmod{83}$, ahol a modulust $(2, 166) = 2$ miatt osztottuk 2-vel.(1 pont)
Ebből tehát $k \equiv 12 \pmod{166}$ vagy $k \equiv 95 \pmod{166}$. (1 pont)
Ezek közül $k \equiv 12 \pmod{83}$ nem megoldása a lineáris kongruenciának, mert $21 \cdot 12 = 252 \not\equiv 3 \pmod{166}$. (Ez a hamis gyök a nem ekvivalens lépés miatt keletkezett.) Mivel a fentiek szerint a lineáris kongruenciának egyetlen megoldása van modulo 166, ezért ez a $k \equiv 95 \pmod{166}$. (1 pont)
Ebből tehát $k = 166\ell + 95$ valamely ℓ egészre. Ezt visszahelyettesítve: $n = 21k + 2 = 21(166\ell + 95) + 2 = 3486\ell + 1997$. (2 pont)
Mivel ez csak az $\ell = 0$ értékre esik 1 és 2023 közé, ezért $n = 1997$ az egyetlen, a feladat feltételeinek megfelelő egész szám. (1 pont)

A megoldhatóságra és a megoldások számára vonatkozó tétel alkalmazása kiváltható a $k \equiv 95 \pmod{166}$ megoldás ellenőrzésével is. A megoldás közben előállt lineáris kongruencia természetesen más tanult módszerekkel, így akár az Euklideszi algoritmussal is megoldható; ezzel dolgozva sorra a $166k \equiv 0 \pmod{166}$, $21k \equiv 3 \pmod{166}$, $19k \equiv -21 \pmod{166}$, $2k \equiv 24 \pmod{166}$, végül a $k \equiv -237 \equiv 95 \pmod{166}$ kongruenciák keletkeznek. Ekkor a lineáris kongruencia megoldásáért járó 5 pontból 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 1 pontot ér annak az ellenőrzése, hogy az eljárás a tanultak szerint leosztás nélkül (vagyis az első fázis kihagyásával) alkalmazható, mert $(21, 166) = 1$; végül 3 pontot ér maga a számolás.

2. Mennyi maradékot ad $6 \cdot 10^{23}$ 9998-cal osztva?

* * * * *

Első megoldás. A ismételt négyzetre emelések módszerével kiszámítjuk 10^{23} 9998-as maradékát.(1 pont)
Ehhez meghatározzuk a $10^1, 10^2, 10^4, 10^8, 10^{16}$ hatványok 9998-as maradékát (mindig az előző négyzetre emelésével és a kapott eredmény 9998-as maradékát véve). Ezek sorra: 10, 100, 2, 4, 16. (3 pont)
Mivel $23 = 1 + 2 + 4 + 16$, (1 pont)
ezért kiszámítjuk először a $10^3 = 10^1 \cdot 10^2$, majd a $10^7 = 10^3 \cdot 10^4$, végül a $10^{23} = 10^7 \cdot 10^{16}$ hatványok 9998-as maradékait (a korábban kiszámolt megfelelő maradékokkal való szorzással és a kapott eredmények 9998-as maradékát véve). Ezek sorra: 1000, 2000 és 2006. (3 pont)
A $10^{23} \equiv 2006 \pmod{9998}$ kongruenciát 6-tal szorozva: $6 \cdot 10^{23} \equiv 6 \cdot 2006 = 12036 \equiv 2038 \pmod{9998}$.
Így a keresett maradék a 2038. (2 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 1 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 magyarázat nélkül közöl, az nem érhet maximális pontszámot; az ilyen megoldásokra az algoritmus alkalmazásáért járó első 8 pontból legföljebb 5 pont adható.

Második megoldás. Figyeljük meg, hogy $10^4 = 10000 \equiv 2 \pmod{9998}$. (2 pont)
Ezt 5-ödik hatványra emelve: $10^{20} \equiv 2^5 = 32 \pmod{9998}$. (3 pont)
Mindkét oldalt $10^3 = 1000$-rel szorozva: $10^{23} \equiv 32000 \equiv 2006 \pmod{9998}$. (3 pont)
Ezt 6-tal szorozva: $6 \cdot 10^{23} \equiv 6 \cdot 2006 = 12036 \equiv 2038 \pmod{9998}$. Így a keresett maradék a 2038.(2 pont)

3. Egy szabályos téglatest alakú láda sík felületű, lejtős talajon áll. A láda $A(1; 4; 2)$ csúcsa a talajon van, az ezzel szomszédos $B(4; 2; 1)$ csúcsa viszont nincs a talajon. Metszi-e a talaj síkja a z-tengelyt? Ha igen, hol?

* * * * *

A talaj S síkjának normálvektora $\underline{n} = \overrightarrow{AB}$, (1 pont)
hiszen ez merőleges az S síkra (mert a téglatest oldaléle merőleges az alap síkjára). (1 pont)
Az A-ba, illetve B-be mutató helyvektorokat $\underline{a}$-val, illetve $\underline{b}$-vel jelölve $\underline{n} = \overrightarrow{AB} = \underline{b} - \underline{a} = (4; 2; 1) - (1; 4; 2) = (3; -2; -1)$. (2 pont)
Így S egyenletét $\underline{n}$ és A alapján felírva: $3x - 2y - z = -7$. (3 pont)
A z-tengely pontjai azok, amikre $x = y = 0$ teljesül. Ezt S egyenletébe helyettesítve $-z = -7$, vagyis $z = 7$ adódik. Így S a $(0; 0; 7)$ pontban metszi a z-tengelyt. (3 pont)

4. A p valós paraméter milyen értékeire lineárisan függetlenek az alábbi $\mathbb{R}^4$-beli $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ vektorok?

$$\underline{a} = \begin{pmatrix} 1 \\ 1 \\ 17 \\ 23 \end{pmatrix}, \ \underline{b} = \begin{pmatrix} 4 \\ 5 \\ 19 \\ 29 \end{pmatrix}, \ \underline{c} = \begin{pmatrix} 0 \\ 0 \\ 2 \\ 5 \end{pmatrix}, \ \underline{d} = \begin{pmatrix} 0 \\ 0 \\ 4 \\ p \end{pmatrix}.$$

* * * * *

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 az $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ vektorokat és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} \alpha + 4\beta &= 0 \\ \alpha + 5\beta &= 0 \\ 17\alpha + 19\beta + 2\gamma + 4\delta &= 0 \\ 23\alpha + 29\beta + 5\gamma + p \cdot \delta &= 0 \end{aligned} \qquad \text{(1 pont)}$$

A második egyenletből az elsőt kivonva $\beta = 0$. Ezt az első két egyenlet bármelyikébe visszahelyettesítve $\alpha = 0$ adódik. (1 pont)
Így a harmadik és negyedik egyenletből álló rendszer erre egyszerűsödik: $2\gamma + 4\delta = 0$, $5\gamma + p \cdot \delta = 0$. (0 pont)
Itt az utóbbi egyenletből az előbbi $\frac{5}{2}$-szeresét kivonva: $(p - 10) \cdot \delta = 0$. (1 pont)
Ha $p \neq 10$, akkor ebből az egyenletből $\delta = 0$ adódik. Ezt pedig a $2\gamma + 4\delta = 0$ egyenletbe visszahelyettesítve $\gamma = 0$ is következik. (1 pont)
Így a tanultak szerint minden $p \neq 10$ értékre $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ lineárisan függetlenek (mert $\alpha\underline{a} + \beta\underline{b} + \gamma\underline{c} + \delta\underline{d} = \underline{0}$ csak az $\alpha = \beta = \gamma = \delta = 0$ esetben lehet lehetséges). (2 pont)
Ha viszont $p = 10$, akkor a $(p - 10) \cdot \delta = 0$ egyenlet semmitmondó. Ekkor például a $\gamma = 2$, $\delta = -1$, $\alpha = \beta = 0$ megoldása a fenti lineáris egyenletrendszernek (vagyis $2\underline{c} - \underline{d} = \underline{0}$). (1 pont)
Így a tanultak szerint a $p = 10$ esetben $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ lineárisan összefüggőek. (2 pont)
Ha egy megoldó csak annyit figyel meg, hogy a $p = 10$ esetben $\underline{d} = 2\underline{c}$, akkor ezért megkaphatja a pontozás szerinti utolsó előtti 1 pontot; ha pedig ebből helyesen levonja és megindokolja azt a következtetést, hogy a $p = 10$ esetben $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ lineárisan összefüggők (mert $\underline{d} = 0\underline{a} + 0\underline{b} + 2\underline{c}$), akkor a pontozás szerinti utolsó 2 pontot is. Ha egy megoldó csak azt vizsgálja, hogy $\underline{d} \in \langle \underline{a}, \underline{b}, \underline{c} \rangle$ milyen p értékekre teljesül és tévesen azt gondolja, hogy ez elegendő a lineáris függetlenség vizsgálatához, az alapvető elvi hibának minősül és így (helyes számolást és eredményt feltételezve is) legföljebb csak 3 pont járhat érte (úgy értve, hogy ez nem adódhat hozzá az imént írt 1+2 ponthoz, hanem a kettő közül legföljebb az egyiket adjuk meg). (Ez természetesen nem vonatkozik egy olyan megoldásra, ami először megmutatja $\underline{a}, \underline{b}, \underline{c}$ lineáris függetlenségét, majd az újonnan érkező vektor lemmájára hivatkozva állítja, hogy a négy vektor lineáris függetlensége ekvivalens $\underline{d} \notin \langle \underline{a}, \underline{b}, \underline{c} \rangle$-vel; egy ilyen megoldás elvileg hibátlan lehet és nyilván maximális pontot érhet.)
A megoldás során adódó 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 és negyediknek írt 1+1 pont jár, a többi (az egyenletrendszer egyértelmű megoldhatóságára, illetve a vektorok lineáris függetlenségére) vonatkozó következtetés pontozása megfelel a fentieknek.

5. A $V \leq \mathbb{R}^5$ altér azokból az $\mathbb{R}^5$-beli vektorokból áll, amiknek az első három koordinátája (fölülről lefelé) számtani sorozatot alkot, az utolsó három koordinátája pedig (szintén fölülről lefelé) 2 kvóciensű mértani sorozatot alkot. (Így például a jobbra látható vektor V-beli.) Határozzuk meg $\dim V$-t, a V altér dimenzióját. (Azt nem szükséges bebizonyítani egy teljes értékű megoldáshoz, hogy V valóban altér.)

$$\begin{pmatrix} 1 \\ 6 \\ 11 \\ 22 \\ 44 \end{pmatrix}$$

* * * * *

Első megoldás. Ha egy $\underline{v} \in V$ vektor első három koordinátája alkotta számtani sorozat első tagja α, a differenciája pedig δ, akkor a feladat szövegéből $\underline{v} = (\alpha, \alpha+\delta, \alpha+2\delta, 2\alpha+4\delta, 4\alpha+8\delta)^T$. (0 pont)
Ezért minden $\underline{v} \in V$ felírható így: $\underline{v} = \alpha \cdot (1,1,1,2,4)^T + \delta \cdot (0,1,2,4,8)^T$. (2 pont)
Ez tehát azt jelenti, hogy a $\underline{b}_1 = (1,1,1,2,4)^T$ és $\underline{b}_2 = (0,1,2,4,8)^T$ vektorok generátorrendszert alkotnak V-ben. (2 pont)
Másrészt $\underline{b}_1, \underline{b}_2$ lineárisan független rendszer, mert egyik vektor sem skalárszorosa a másiknak. (2 pont)
Így $\underline{b}_1, \underline{b}_2$ bázis V-ben, (2 pont)
vagyis $\dim V = 2$. (2 pont)
(A $\underline{v}^T$ jelölés a $\underline{v}$ sorvektorból oszlopvektort készít, illetve fordítva; itt a T a *transzponálás* rövidítése, ezt a tárgyban később általánosabban is definiáljuk, itt csak helytakarékosság céljából használtuk.)

Második megoldás. A tanult eljárást használjuk V egy bázisának az elkészítésére. (0 pont)
Ehhez először választunk egy tetszőleges $\underline{b}_1 \in V$, $\underline{b}_1 \neq \underline{0}$ vektort: például $\underline{b}_1 = (1,0,-1,-2,-4)^T$. (1 pont)
Ekkor $\underline{b}_1$ nem generátorrendszer V-ben például azért, mert $\langle \underline{b}_1 \rangle$ minden elemének második koordinátája 0, így könnyen választhatunk egy $\underline{b}_2 \in V$, $\underline{b}_2 \notin \langle \underline{b}_1 \rangle$ vektort: legyen például $\underline{b}_2 = (0,1,2,4,8)^T$. (2 pont)
Most azt kell megvizsgálnunk, hogy $V = \langle \underline{b}_1, \underline{b}_2 \rangle$ már igaz-e. Ehhez vegyünk egy tetszőleges $\underline{v} \in \langle \underline{b}_1, \underline{b}_2 \rangle$ vektort. Ekkor $\underline{v} = \alpha \underline{b}_1 + \beta \underline{b}_2$ valamilyen α, β skalárokra, (1 pont)
vagyis $\underline{v} = (\alpha, \beta, -\alpha+2\beta, -2\alpha+4\beta, -4\alpha+8\beta)^T$. (1 pont)
Megmutatjuk, hogy minden $\underline{v} \in V$ vektor felírható ilyen alakban. Valóban, ha egy $\underline{v} \in V$ első két koordinátája α, illetve β, akkor az első három koordináta alkotta számtani sorozat differenciája $\beta - \alpha$, így $\underline{v}$ harmadik koordinátája $\beta + (\beta - \alpha) = -\alpha + 2\beta$. Innen pedig $\underline{v}$ negyedik és ötödik koordinátája valóban $-2\alpha+4\beta$, illetve $-4\alpha+8\beta$, mert az utolsó három koordináta 2 kvóciensű mértani sorozatot alkot. (1 pont)
Így $\underline{b}_1, \underline{b}_2$ már generátorrendszert alkot V-ben. (2 pont)
A tanult eljárást követve tehát a $\underline{b}_1, \underline{b}_2$ bázist kaptuk V-ben, amiből $\dim V = 2$. (2 pont)
(Az olyan „megoldások”, amik mindössze arra hivatkoznak, hogy egy $\underline{v} \in V$ vektor első két koordinátáját lerögzítve a többi már egyértelműen adódik, így „V elemeinek két szabad paramétere van”, ezért $\dim V = 2$, alapvető elvi hibán alapulnak és így nem érnek pontot.)

6*. Adjuk meg 1024 összes cinkosát (vagyis az összes olyan 1024-nél kisebb, pozitív egészt, amik a Fermat-teszt végrehajtásakor nem tanúsítják 1024 összetett voltát).

* * * * *

Legyen a az 1024 egy tetszőleges cinkosa. Ekkor tehát $1 \leq a \leq 1023$, $(a, 1024) = 1$ és $a^{1023} \equiv 1 \pmod{1024}$ (a cinkos definíciója szerint). (1 pont)
Mivel $1024 = 2^{10}$, ezért a tanult tétel szerint $\varphi(1024) = 2^{10} - 2^9 = 512$. (1 pont)
Mivel $(a, 1024) = 1$, ezért alkalmazható az Euler-Fermat tétel: (1 pont)
$a^{512} \equiv 1 \pmod{1024}$. (1 pont)
Ezt négyzetre emelve: $a^{1024} \equiv 1^2 = 1 \pmod{1024}$. (1 pont)
Ezekből $1 \equiv a^{1024} = a^{1023} \cdot a \equiv 1 \cdot a = a \pmod{1024}$, vagyis $a \equiv 1 \pmod{1024}$. (3 pont)
Ebből pedig $1 \leq a \leq 1023$ miatt $a = 1$ adódik. (1 pont)
Mivel 1 nyilván cinkosa 1024-nek, hiszen $(1, 1024) = 1$ és $1^{1023} = 1 \equiv 1 \pmod{1024}$, (1 pont)
ezért 1024 egyetlen cinkosa az 1. (0 pont)
(A fenti pontozás szerinti 3 pont megszerzéséhez meggyőzően kell indokolni, hogy az $a^{1023} \equiv 1 \pmod{1024}$ és $a^{1024} \equiv 1 \pmod{1024}$ kongruenciákból $a \equiv 1 \pmod{1024}$ valóban következik.)