Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2018. december 10.

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.

Zárthelyi feladatok — az **ELSŐ** zárthelyi pótlására

1. A pozitív egész n szám 513-szorosának utolsó három számjegye 001. Mi az n utolsó 3 számjegye?

* * * * *

Első megoldás. A feladat szövege szerint $513n \equiv 1 \pmod{1000}$. (1 pont)
Ebből következik, hogy $513n \equiv 1 \pmod{500}$, vagyis $13n \equiv 1 \pmod{500}$ is teljesül. (Ugyanide jutunk, ha a kongruenciát először 2-vel szorozzuk, majd 2-vel osztjuk.) (2 pont)
Mindkét oldalt 39-cel szorozva: $507n \equiv 39 \pmod{500}$, vagyis $7n \equiv 39 \pmod{500}$. (2 pont)
Ez ekvivalens a $7n \equiv 539 \pmod{500}$ kongruenciával, amelynek mindkét oldalát 7-tel osztva: $n \equiv 77 \pmod{500}$, ahol a modulus $(7, 500) = 1$ miatt nem változott. (1 pont)
Ebből tehát $n \equiv 77 \pmod{1000}$ vagy $n \equiv 500 + 77 = 577 \pmod{1000}$. (1 pont)
Ellenőrzéssel látható, hogy $513 \cdot 77 \not\equiv 1 \pmod{1000}$, de $513 \cdot 577 \equiv 1 \pmod{1000}$. (2 pont)
Ezek szerint a lineáris kongruencia egyetlen megoldása $n \equiv 577 \pmod{1000}$, vagyis n utolsó három számjegye 577. (1 pont)
A két ellenőrzés közül az egyik kiváltható azzal, hogy $(513, 1000) = 1 \mid 1$ miatt a lineáris kongruenciának egyetlen megoldása kell legyen modulo 1000. Ha valaki csak ennyit állapít meg, de a lineáris kongruenciát megoldani nem tudja, az ezért (a lineáris kongruencia felírásáért járó 1 ponton kívül további) 1 pontot kaphat. Számolási hibákért 1-1 pont vonandó le, de a maradék pontszám csak akkor jár, ha a hiba miatt a feladat nem lett lényegesen könnyebb.

Második megoldás. A feladat szövege szerint $513n \equiv 1 \pmod{1000}$. (1 pont)
Ezt az előadáson tanult (euklideszi) algoritmussal oldjuk meg.
Ehhez először 513 és 1000 legnagyobb közös osztóját kell meghatározni: mivel $(513, 1000) = 1 \big| 1$, ezért egyetlen megoldás lesz modulo 1000 és az algoritmust osztás nélkül indíthatjuk a bemenetként kapott kongruenciától. (2 pont)
Az algoritmus végrehajtása során kapott kongruenciák sorra a következők: $1000n \equiv 0 \pmod{1000}$, $513n \equiv 1 \pmod{1000}$, $487n \equiv -1 \pmod{1000}$, $26n \equiv 2 \pmod{1000}$, $19n \equiv -37 \pmod{1000}$, $7n \equiv 39 \pmod{1000}$, $5n \equiv -115 \pmod{1000}$, $2n \equiv 154 \pmod{1000}$, $n \equiv -423 \equiv 577 \pmod{1000}$. (6 pont)
Így n utolsó három számjegye 577. (1 pont)
Számolási hibákért 1-1 pont vonandó le, de a teljes maradék pontszám csak akkor jár, ha a hiba miatt a megoldás nem lett könnyebb vagy rövidebb.

2. Milyen maradékot ad 392-vel osztva $169^{181^{194}}$?

* * * * *

Mivel $\varphi(392) = \varphi(2^3 \cdot 7^2) = (2^3 - 2^2)(7^2 - 7^1) = 168$ (1 pont)
és $(169, 392) = 1$, (1 pont)
ezért az Euler-Fermat tétel miatt $169^{168} \equiv 1 \pmod{392}$. (1 pont)
Ezt tetszőleges $k \geq 1$ egészre k-adik hatványra emelhetjük: $169^{168k} \equiv 1^k = 1 \pmod{392}$. (2 pont)
Mivel $181 \equiv 13 \pmod{168}$, ezt négyzetre emelve $181^2 \equiv 13^2 = 169 \equiv 1 \pmod{168}$. Ezt tovább a 97-edikre emelve: $181^{194} \equiv 1^{97} = 1 \pmod{168}$. (2 pont)
Ezért $181^{194} = 168k + 1$ valamely $k \geq 1$ egészre, amiből $169^{181^{194}} = 169^{168k+1}$. (1 pont)
A fentebb látott $169^{168k} \equiv 1 \pmod{392}$ kongruencia mindkét oldalát 169-cel szorozva: $169^{168k+1} \equiv 169 \pmod{392}$. Ezért $169^{181^{194}} \equiv 169 \pmod{392}$, vagyis a válasz: 169. (2 pont)
A $181^{194} \equiv 1 \pmod{168}$ kongruenciát beláthatjuk az Euler-Fermat tétel egy újabb alkalmazásával is (de ettől még az ezért járó pontszám változatlanul 2.)

3. Legyen $n = 20181210$. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg $45n + 12$ és $35n + 9$ legnagyobb közös osztóját.

* * * * *

Az euklideszi algoritmust alkalmazzuk.
$(45n + 12)$-t $(35n + 9)$-cel maradékosan osztva: $45n + 9 = 1 \cdot (35n + 9) + 10n + 3$. (2 pont)
$(35n + 9)$-et $(10n + 3)$-mal maradékosan osztva: $35n + 9 = 3 \cdot (10n + 3) + 5n$. (2 pont)
$(10n + 3)$-at $5n$-nel maradékosan osztva: $10n + 3 = 2 \cdot (5n) + 3$. (1 pont)
Mivel n számjegyeinek összege 15, vagyis 3-mal osztható, ezért n is, valamint $5n$ is 3-mal osztható.
Így $5n$-et 3-mal osztva a maradék 0. (3 pont)
Így a legnagyobb közös osztó (az utolsó nemnulla maradék, vagyis) 3. (2 pont)

4. Álljon a V halmaz azokból az $\mathbb{R}^4$-beli vektorokból, amelyekben a négy koordináta szorzata nagyobb vagy egyenlő 0-nál. Döntsük el, hogy V alteret alkot-e $\mathbb{R}^4$-ben.

* * * * *

Az $\underline{u} = (1, 0, 0, 0)^T$ és $\underline{v} = (0, -1, 1, 1)^T$ vektorok V-beliek, mert $\underline{u}$ és $\underline{v}$ koordinátáinak szorzata is 0.
Azonban az $\underline{u} + \underline{v} = (1, -1, 1, 1)$ vektor nem V-beli, mert a koordináták szorzata (-1). (6 pont)
Mivel $\underline{u}, \underline{v} \in V$, de $\underline{u} + \underline{v} \notin V$, ezért az altér definíciója sérül, vagyis V nem altér. (4 pont)
Noha ez közvetlenül nem járul hozzá egy helyes megoldáshoz, ha valaki (hiánytalanul) megmutatja, hogy $\underline{v} \in V$ és $\lambda \in \mathbb{R}$ esetén $\lambda \cdot \underline{v} \in V$ is teljesül, akkor ezért 3 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.

5. A $W \leq \mathbb{R}^6$ altér álljon azokból az $\mathbb{R}^6$-beli vektorokból, amelyeknek a páratlan sorszámú koordinátái fölülről lefelé haladva 2 kvóciensű, a páros sorszámú koordinátái pedig fölülről lefelé haladva 3 kvóciensű mértani sorozatot alkotnak. (Így például a jobbra látható vektor W-beli.) Határozzuk meg a W altér dimenzióját. (Azt nem szükséges bebizonyítani egy teljes értékű megoldáshoz, hogy W valóban altér.)

$$\begin{pmatrix} 3 \\ 5 \\ 6 \\ 15 \\ 12 \\ 45 \end{pmatrix}$$

* * * * *

Ha egy $\underline{w} \in W$ első két koordinátája α és β, akkor a feladat szövegéből $\underline{w} = (\alpha, \beta, 2\alpha, 3\beta, 4\alpha, 9\beta)^T$. Ezért minden $\underline{w} \in W$ felírható így: $\underline{w} = \alpha \cdot (1,0,2,0,4,0)^T + \beta \cdot (0,1,0,3,0,9)^T$. (2 pont)
Ez tehát azt jelenti, hogy a $\underline{b}_1 = (1,0,2,0,4,0)^T$ és $\underline{b}_2 = (0,1,0,3,0,9)^T$ vektorok generátorrendszert alkotnak W-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 W-ben, (2 pont)
vagyis $\dim W = 2$. (2 pont)

6*. Határozzuk meg az $A(1;5;2)$, $B(2;7;4)$ és $C(2;9;10)$ pontok által meghatározott háromszög A csúcsán átmenő (belső) szögfelezőjének az egyenletrendszerét.

* * * * *

A megoldásban az egyes pontokba mutató helyvektorokat mindig a megfelelő kisbetűvel jelöljük.
$\overrightarrow{AB} = \underline{b} - \underline{a} = (1,2,2)$ és $\overrightarrow{AC} = \underline{c} - \underline{a} = (1,4,8)$, (1 pont)
amiből a Pitagorasz-tétel miatt $|\overrightarrow{AB}| = \sqrt{1^2+2^2+2^2} = 3$ és $|\overrightarrow{AC}| = \sqrt{1^2+4^2+8^2} = 9$. (1 pont)
Jelöje a háromszög AC oldalának A-hoz közelebbi harmadolópontját H. Ekkor az ABH háromszög egyenlő szárú, mert $|\overrightarrow{AB}| = 3$ és $|\overrightarrow{AH}| = \frac{1}{3} \cdot 9 = 3$. Így az ABC háromszög A csúcsán átmenő belső szögfelezője átmegy a B és H pontok F felezőpontján is. (4 pont)
$\overrightarrow{AH} = \frac{1}{3}\overrightarrow{AC} = (\frac{1}{3}, \frac{4}{3}, \frac{8}{3})$ és így $\underline{h} = \underline{a} + \overrightarrow{AH} = (\frac{4}{3}, \frac{19}{3}, \frac{14}{3})$. (1 pont)
$\underline{f} = \frac{1}{2}(\underline{b} + \underline{h}) = (\frac{5}{3}, \frac{20}{3}, \frac{13}{3})$, (1 pont)
így az $\overrightarrow{AF} = \underline{f} - \underline{a} = (\frac{2}{3}, \frac{5}{3}, \frac{7}{3})$, illetve ennek a 3-szorosa, a $\underline{v} = (2,5,7)$ vektor irányvektora a keresett szögfelezőnek. (1 pont)
Ennek az egyenletrendszere tehát A-ból és $\underline{v}$-ből felírható: $\frac{x-1}{2} = \frac{y-5}{5} = \frac{z-2}{7}$. (1 pont)
A szögfelező egyenletrendszere megadható paraméteres alakban is. A feladat megoldható a szögfelezőtétel használatával is: mivel az A-n átmenő belső szögfelező a BC oldalt a szomszédos oldalak arányában osztja, ezért átmegy a BC oldal B-hez közelebbi negyedelőpontján (az $N(2, \frac{15}{2}, \frac{11}{2})$ ponton).

Zárthelyi feladatok — a **MÁSODIK** zárthelyi pótlására

1. Döntsük el, hogy a p valós paraméter milyen értékeire van megoldása az alábbi egyenletrendszernek. Ha van megoldás, adjuk is meg az összeset.

$$\begin{aligned} x_1 + 4x_2 - 3x_3 &= 1 \\ 3x_1 + 17x_2 - 19x_3 &= 28 \\ 2x_1 + 11x_2 - 12x_3 &= p + 34 \\ 7x_1 + 26x_2 + p \cdot x_3 &= p + 15 \end{aligned}$$

* * * * *

A Gauss-eliminációt alkalmazva a következőket kapjuk:

$$\left(\begin{array}{ccc|c} 1 & 4 & -3 & 1 \\ 3 & 17 & -19 & 28 \\ 2 & 11 & -12 & p+34 \\ 7 & 26 & p & p+15 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 4 & -3 & 1 \\ 0 & 5 & -10 & 25 \\ 0 & 3 & -6 & p+32 \\ 0 & -2 & p+21 & p+8 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 4 & -3 & 1 \\ 0 & 1 & -2 & 5 \\ 0 & 0 & 0 & p+17 \\ 0 & 0 & p+17 & p+18 \end{array}\right) \quad \text{(3 pont)}$$

Ha $p \neq -17$, akkor a harmadik sor „tilos sor”, így az egyenletrendszernek nincs megoldása. (2 pont)
Ha viszont $p = -17$, akkor a negyedik sor „tilos sor”, így ekkor sincs megoldás. (3 pont)
Így az egyenletrendszernek semmilyen p esetén sincs megoldása. (2 pont)
A számolási hibák darabonként 1 pont levonást jelentenek. Ha egy elszámolás után a megoldó helyes következtetéseket von le a hibás alakból, akkor a fenti pontszámok közül az első 2 pont akkor adható meg, ha a hibás alakban is keletkezik „tilos sor” és ebből a megoldó a helyes következtetést vonja le; az utána következő 3 pont pedig megadható az elszámolt alakból fakadó (egyértelmű) megoldás helyes meghatározásáért.

2. Az 6×6-os A mátrix főátlójában és alatta minden elem 1-es, a jobb felső sarkában álló elem 2018, a mátrix összes többi (14 darab) eleme pedig 0. Határozzuk meg A determinánsát.

* * * * *

Vonjuk ki a hatodik sorból az ötödiket. Ekkor a hatodik sor (0 0 0 0 0 1)-re változik. (2 pont)
Most vonjuk ki az első sorból a (megváltozott) hatodik sor 2018-szorosát. Ekkor az első sor (1 0 0 0 0 0)-ra változik. (3 pont)
A keletkezett mátrix alsóháromszög-mátrix, amelynek a főátlójában minden elem 1-es, így a determinánsa 1. (2 pont)
Mivel a megtett lépések a determináns értékét nem változtatták, ezért $\det A = 1$. (3 pont)
A feladat megoldható a Gauss-elimináció pontos követésével is (több lépésben), valamint a kifejtési tételt használva is (az első sor vagy az utolsó oszlop szerint), illetve számos más úton is. Minden, a megoldást érdemben nem befolyásoló számolási hiba 1 pont levonást jelent. A determinánsra vonatkozó egyes alapismeretek teljes vagy részleges hiányából fakadó elvi hibák viszont darabonként 5 pont levonást jelentenek. Ilyen például, ha a megoldó egy sor konstanssal szorzása, vagy sorok cseréje után nem, vagy hibásan követi a determináns megváltozását, vagy ha a kifejtési tételben nem (jól) veszi figyelembe az előjeleket. Kétes esetekben elvi hibának tekintendő minden olyan hiba, amikor nincs nyoma annak, hogy a megoldó a szóban forgó ismeretet helyesen próbálta alkalmazni. Arányos részpontszám jár minden, a determináns kiszámításának irányába mutató, hasznos lépésért.

3. Számítsuk ki az A^{2018} mátrixot az alábbi A mátrixra. (A^{2018} azt a 2018 tényezős szorzatot jelöli, amelynek minden tényezője A.)

$$A = \begin{pmatrix} -5 & -4 & -8 \\ 1 & 0 & 2 \\ 2 & 2 & 3 \end{pmatrix}$$

* * * * *

A mátrixszorzás definíciója szerint A^2-et kiszámítva: $A^2 = \begin{pmatrix} 5 & 4 & 8 \\ -1 & 0 & -2 \\ -2 & -2 & -3 \end{pmatrix}$. (2 pont)
Látható, hogy $A^2 = -A$. (1 pont)
Ebből $A^3 = A^2 \cdot A = (-A) \cdot A = -A^2 = -(-A) = A$. (1 pont)
Innen már sejthető, hogy A-nak a páros kitevőjű hatványai $(-A)$-val, a páratlan kitevőjű hatványai pedig A-val egyenlők. (1 pont)
Így $A^{2018} = -A$. (1 pont)
Az A hatványaira vonatkozó fenti állítást precízen teljes indukcióval láthatjuk be. $n = 1$-re az állítás nyilván igaz. Ha pedig valamely n-re már teljesül, hogy $A^n = (-1)^{n+1} \cdot A$, akkor A-val szorzás után az $A^{n+1} = A^n \cdot A = ((-1)^{n+1} \cdot A) \cdot A = (-1)^{n+1} \cdot A^2 = (-1)^{n+1} \cdot (-A) = (-1)^{n+2} \cdot A$, vagyis az állítás $(n+1)$-re is teljesül. (4 pont)
A pontozás úgy értendő, hogy ha a megoldó A^2 és A^3 kiszámítása után minden magyarázat nélkül közli A^{2018} értékét, arra 5 pontot kaphat. Ha megfogalmazza az A^n-re vonatkozó általános állítást, arra további 1-et. Ha pedig a megoldás legalább részben meggyőzően indokolja, hogy az A^n-re vonatkozó állítás igaz, akkor ezért már további 2 pont adható (a precíz indoklásért járó 4-ből).

4. Határozzuk meg az alábbi A és B mátrixok hiányzó, betűkkel jelölt elemeit, ha tudjuk, hogy $B = A^{-1}$.

$$A = \begin{pmatrix} 5 & 2 & 0 \\ -1 & x & 1 \\ y & z & 1 \end{pmatrix} \qquad\qquad B = \begin{pmatrix} 1 & -2 & p \\ q & 5 & r \\ s & -26 & 27 \end{pmatrix}$$

* * * * *

Az $A \cdot B$ szorzatmátrix i-edik sorának és j-edik oszlopának kereszteződésében álló elemet jelölje $c_{i,j}$.
$B = A^{-1}$ miatt $A \cdot B = E$, (2 pont)
ezért $c_{1,1} = 1$, amiből $5 \cdot 1 + 2q = 1$, így $q = -2$. (1 pont)
Hasonlóan: $c_{2,2} = 1$, amiből $(-1) \cdot (-2) + 5x - 26 = 1$, így $x = 5$. (1 pont)
$c_{2,1} = 0$, amiből $(-1)1 + x \cdot q + s = 0$. Felhasználva x és q értékét: $s = 1 - xq = 11$. (2 pont)
$c_{3,1} = c_{3,2} = 0$, amiből $y - 2z + 11 = 0$ és $-2y + 5z - 26 = 0$. Megoldva az egyenletrendszert: $y = -3$ és $z = 4$. (2 pont)
Végül $c_{1,3} = c_{2,3} = 0$ miatt $5p + 2r = 0$ és $-p + 5r + 27 = 0$, amiből $p = 2$ és $r = -5$. (2 pont)

5. Az 5×10-es A mátrixról tudjuk, hogy elhagyható belőle egy alkalmasan választott sor és oszlop úgy, hogy a kapott 4×9-es mátrix rangja azonos legyen A rangjával. Azt is tudjuk továbbá, hogy bárhogyan hagyunk el A-ból két sort és két oszlopot, a kapott 3×8-as mátrix rangja már különbözik A rangjától. Határozzuk meg A rangját.

* * * * *

Mivel $r(A)$ egyenlő egy 4×9-es mátrix rangjával, ezért (a sorrang definíciója miatt) $r(A) \leq 4$.(3 pont)
Legyen M (a determinánsrang definíciója szerint) egy $r(A) \times r(A)$ méretű, nemnulla determinánsú részmátrix A-ban. (2 pont)
Ha $r(A) \leq 3$ volna, akkor az M-be nem tartozó sorok és oszlopok közül elhagyhatnánk kettőt-kettőt. Az így kapott A' mátrixnak M továbbra is részmátrixa volna, így $r(A') = r(A)$ volna. Mivel ez ellentmondana a feladat szövegének, ezért $r(A) \geq 4$. (4 pont)
Megmutattuk, hogy $r(A) \leq 4$ és $r(A) \geq 4$, így $r(A) = 4$. (1 pont)

6*. Az $n \times n$-es A és B mátrixokra teljesül, hogy $B \neq 0$ és $A \cdot B = B$. Mutassuk meg, hogy ekkor létezik olyan $n \times n$-es C mátrix, amelyre $C \neq 0$ és $A^T \cdot C = C$.

* * * * *

$AB = B$ miatt $AB - B = 0$, amiből (a mátrixszorzás tulajdonságai miatt) $(A - E)B = 0$. (1 pont)
Ha $\det(A - E) \neq 0$ volna, akkor $(A - E)$-nek volna inverze. Ekkor mindkét oldalt balról $(A - E)^{-1}$-zel szorozva: $(A - E)^{-1}(A - E)B = (A - E)^{-1} \cdot 0$, amiből $B = EB = 0$ következne, szemben a feladat állításával. Így tehát $\det(A - E) = 0$. (2 pont)
Ebből a transzponált determinánsára vonatkozó, tanult tétel miatt $\det(A - E)^T = 0$. (2 pont)
A transzponált és az egységmátrix definíciójából azonnal adódik, hogy $(A - E)^T = A^T - E$.(1 pont)
$\det(A^T - E) = 0$-ból a tanult tétel szerint következik, hogy $A^T - E$ oszlopai lineárisan összefüggők, vagyis létezik olyan $\underline{x} \neq \underline{0}$, $\underline{x} \in \mathbb{R}^n$ vektor, amelyre $(A^T - E) \cdot \underline{x} = \underline{0}$. (1 pont)
Legyen most C az az $n \times n$-es mátrix, amelynek minden oszlopa $\underline{x}$. Ekkor $\underline{x} \neq \underline{0}$ miatt $C \neq 0$ és $(A^T - E) \cdot \underline{x} = \underline{0}$ miatt $(A^T - E) \cdot C = 0$. (2 pont)
Ebből $A^T \cdot C - C = 0$, vagyis $A^T \cdot C = C$ valóban teljesül. (1 pont)