Bevezetés a számításelméletbe I.

Zárthelyi feladatok — az **ELSŐ** zárthelyi pótlására

2019. december 16.

1. Hány olyan 504-nél nem nagyobb, pozitív egész szám van, amelynek van 504-gyel osztva 1 maradékot adó többszöröse?

2. Határozzuk meg az összes olyan n egészt 1 és 1000 között, amelyre $n+10$ 36-tal osztva, $n-10$ pedig 38-cal osztva ad 1 maradékot.

3. Van-e az $5x-3y+2z=1$ egyenletű síknak olyan P pontja, amelyre a P, a $Q(5;9;11)$ és az $R(13;7;7)$ pontok egy egyenesbe esnek? Ha igen, akkor határozzuk meg az összes ilyen P-t.

4. Legyenek $\underline{u}$, $\underline{v}$ és $\underline{w}$ az alábbi $\mathbb{R}^4$-beli vektorok. Az $\langle \underline{u}, \underline{v}, \underline{w} \rangle$ generált altér $\underline{a}$ elemének első két koordinátája 1. Határozzuk meg az $\underline{a}$ koordinátáinak az összegét.

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

5. A p valós paraméter milyen értékeire lineárisan függetlenek az alábbi, $\mathbb{R}^4$-beli $\underline{u}$, $\underline{v}$, $\underline{w}$ vektorok?

$$\underline{u} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \ \underline{v} = \begin{pmatrix} 0 \\ 1 \\ -2 \\ 1 \end{pmatrix}, \ \underline{w} = \begin{pmatrix} -1 \\ 0 \\ 1 \\ p \end{pmatrix}.$$

6*. Létezik-e olyan n egész szám, amelyre n^4+1 osztható 101-gyel?

A dolgozatra kérjük jól olvashatóan felírni a következő adatokat: név, Neptun-kód, Neptun szerinti gyakorlatvezető neve.

Minden feladat 10 pontot ér, a munkaidő 90 perc. Az aláírás feltétele: a két zárthelyin átlagosan legalább 24 pont és mindkét zárthelyin külön-külön legalább 18 pont elérése. A 100%-os eredményhez elegendő 50 pontot elérni a 60-ból, az összpontszám 50 pont feletti részét IMSc pontként könyveljük el.

A feladatok megoldását indokolni kell, puszta eredményközlésért nem jár pont. A dolgozat megírása közben számológép (vagy más segédeszköz) nem használható.

Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2019. december 16.

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.

Zárthelyi feladatok — az **ELSŐ** zárthelyi pótlására

1. Hány olyan 504-nél nem nagyobb, pozitív egész szám van, amelynek van 504-gyel osztva 1 maradékot adó többszöröse?

* * * * *

Az $a \in \{1, 2, \ldots, 504\}$ egésznek akkor és csak akkor van 504-gyel osztva 1 maradékot adó többszöröse, ha megoldható az $ax \equiv 1 \pmod{504}$ lineáris kongruencia, (3 pont)
ami a tanult tétel szerint azzal ekvivalens, hogy $(a, 504) \mid 1$, vagyis $(a, 504) = 1$. (3 pont)
Az ilyen a-k száma éppen $\varphi(504) =$ (2 pont)
$= \varphi(2^3 \cdot 3^2 \cdot 7) = (2^3 - 2^2)(3^2 - 3^1)(7^1 - 7^0) = 4 \cdot 6 \cdot 6 = 144$ a tanult tétel szerint. (2 pont)

2. Határozzuk meg az összes olyan n egészt 1 és 1000 között, amelyre $n + 10$ 36-tal osztva, $n - 10$ pedig 38-cal osztva ad 1 maradékot.

* * * * *

A feladat feltételeiből $n + 10 \equiv 1 \pmod{36}$ és $n - 10 \equiv 1 \pmod{38}$ adódik. (1 pont)
Átrendezés után: $n \equiv -9 \pmod{36}$, $n \equiv 11 \pmod{38}$. (1 pont)
A kapott kongruenciarendszert a tanult módszerrel oldjuk meg.
Az első kongruenciából: $n = 36k - 9$ valamely k egészre. (1 pont)
Ezt a második kongruenciába helyettesítve: $36k - 9 \equiv 11 \pmod{38}$. Mindkét oldalhoz 9-et adva a $36k \equiv 20 \pmod{38}$ lineáris kongruenciát kapjuk. (1 pont)
$36 \equiv -2 \pmod{38}$ miatt ez a $-2k \equiv 20 \pmod{38}$ alakba írható. Mindkét oldalt (-2)-vel osztva: $k \equiv -10 \equiv 9 \pmod{19}$, ahol a modulust $(-2, 38) = 2$ miatt kellett 2-vel osztani. (2 pont)

Mivel az osztás ekvivalens átalakítás volt, ezért $k \equiv 9 \pmod{19}$ valóban a lineáris kongruencia megoldáshalmazát adja meg. (1 pont)
Ebből tehát $k = 19\ell + 9$ valamely ℓ egészre. Ezt visszahelyettesítve: $n = 36k - 9 = 36(19\ell + 9) - 9 = 684\ell + 315$. (2 pont)
Az $\ell = 0, 1$ értékekre kapunk 1 és 1000 közötti n-eket: $n = 315$ és $n = 999$, így ez a két megoldása van a feladatnak. (1 pont)
A megoldás során előállt lineáris kongruencia természetesen más tanult módszerekkel, így akár az Euklideszi algoritmussal is megoldható. A megoldáshalmaz a $k \equiv 9 \pmod{19}$ alak helyett megadható így is: $k \equiv 9 \pmod{38}$ vagy $k \equiv 28 \pmod{38}$; aki így jár el, annak a $k = 38\ell + 9$ és a $k = 38\ell + 28$ esetet is vissza kell helyettesíteni az $n = 36k - 9$ egyenletbe. Ebben az esetben a lépések ekvivalenciájára való hivatkozás kiváltható azzal is, hogy $(36, 38) = 2 \mid 2$ miatt a lineáris kongruenciának 2 megoldása van modulo 38, így mindkét kapott megoldásnak jónak kell lennie.

3. Van-e az $5x - 3y + 2z = 1$ egyenletű síknak olyan P pontja, amelyre a P, a $Q(5; 9; 11)$ és az $R(13; 7; 7)$ pontok egy egyenesbe esnek? Ha igen, akkor határozzuk meg az összes ilyen P-t.

* * * * *

A keresett P-nek (ha létezik) az $5x - 3y + 2z = 1$ egyenletű S sík és a QR egyenes döféspontjának kell lennie. (1 pont)
A QR egyenesnek irányvektora a $\overrightarrow{QR}$ vektor, (1 pont)
vagyis a $\overrightarrow{QR} = \underline{r} - \underline{q} = (8; -2; -4)$ (ahol $\underline{r}$, illetve $\underline{q}$ a megfelelő pontokba mutató helyvektorokat jelölik). (1 pont)
$\overrightarrow{QR}$ helyett kényelmi okokból használhatjuk a $\underline{v} = \frac{1}{2}\overrightarrow{QR} = (4; -1; -2)$ vektort is irányvektornak.
$\underline{v}$-ből és (például) Q-ból felírható a QR egyenes paraméteres egyenletrendszere: $x = 5 + 4t$, $y = 9 - t$, $z = 11 - 2t$ $(t \in \mathbb{R})$. (3 pont)
A döféspont meghatározásához ezeket S egyenletébe helyettesítjük: $5(5+4t)-3(9-t)+2(11-2t) = 1$. Ebből $19t = -19$, vagyis $t = -1$ adódik. Így a keresett döféspont koordinátái: $x = 5 + 4 \cdot (-1) = 1$, $y = 9 - (-1) = 10$, $z = 11 - 2 \cdot (-1) = 13$. Tehát egyetlen P pont felel meg a feladat szövegének: $P(1; 10; 13)$. (4 pont)
Természetesen az egyenes nem paraméteres egyenletrendszerét is használhatjuk a feladat megoldásához, majd az ebből, illetve a sík egyenletéből álló egyenletrendszer megoldásaként kaphatjuk a döféspontot. Az egyenletrendszerért, illetve a számításért ebben az esetben is 3+4 pont jár.

4. Legyenek $\underline{u}$, $\underline{v}$ és $\underline{w}$ az alábbi $\mathbb{R}^4$-beli vektorok. Az $\langle \underline{u}, \underline{v}, \underline{w} \rangle$ generált altér $\underline{a}$ elemének első két koordinátája 1. Határozzuk meg az $\underline{a}$ koordinátáinak az összegét.

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

* * * * *

Mivel $\underline{a} \in \langle \underline{u}, \underline{v}, \underline{w} \rangle$, ezért $\underline{a}$ kifejezhető $\underline{u}$-ból, $\underline{v}$-ből és $\underline{w}$-ből lineáris kombinációval; vagyis léteznek olyan α, β, γ skalárok, hogy $\alpha \cdot \underline{u} + \beta \cdot \underline{v} + \gamma \cdot \underline{w} = \underline{a}$. (2 pont)
Jelölje $\underline{a}$ utolsó két koordinátáját p, illetve q. Behelyettesítve $\underline{u}, \underline{v}, \underline{w}$ konkrét értékét és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} \alpha &= 1 \\ -2\alpha + \beta &= 1 \\ -4\beta + 5\gamma &= p \\ -5\gamma &= q \end{aligned}$$ (4 pont)

Az első két egyenletből $\alpha = 1$ és $\beta = 1 + 2\alpha = 3$ adódik. (1 pont)
Így az $\underline{a}$ koordinátáinak összege: $1 + 1 + p + q = 1 + 1 + (-4 \cdot 3 + 5\gamma) + (-5\gamma) = -10$. (3 pont)

5. A p valós paraméter milyen értékeire lineárisan függetlenek az alábbi, $\mathbb{R}^4$-beli $\underline{u}$, $\underline{v}$, $\underline{w}$ vektorok?

$$\underline{u} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \ \underline{v} = \begin{pmatrix} 0 \\ 1 \\ -2 \\ 1 \end{pmatrix}, \ \underline{w} = \begin{pmatrix} -1 \\ 0 \\ 1 \\ p \end{pmatrix}.$$

* * * * *

Tegyük fel, hogy $\alpha \cdot \underline{u} + \beta \cdot \underline{v} + \gamma \cdot \underline{w} = \underline{0}$ teljesül valamilyen $\alpha, \beta, \gamma \in \mathbb{R}$ skalárokra. (1 pont)
Behelyettesítve $\underline{u}, \underline{v}, \underline{w}$ konkrét értékét és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

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

Az első két egyenletből: $\alpha = \beta = \gamma$. Ezt a harmadikba helyettesítve: $\alpha - 2\alpha + \alpha = 0$ adódik, vagyis ez az egyenlet következménye az első kettőnek. (1 pont)
(Valóban: a harmadik egyenlet az első (-1)-szeresének és a második (-2)-szeresének az összege.)
A negyedik egyenlet $\beta = \alpha$ és $\gamma = \alpha$ helyettesítés után $(p+1)\alpha = 0$ alakot ölt. (1 pont)
Ha $p \neq -1$, akkor ebből $\alpha = 0$ és így $\beta = \gamma = 0$ adódik. Így ebben az esetben a tanultak szerint $\underline{u}$, $\underline{v}$ és $\underline{w}$ lineárisan függetlenek. (3 pont)
Ha viszont $p = -1$, akkor a negyedik egyenlet is következménye az első kettőnek (azok összege). Így ebben az esetben a rendszernek megoldása például $\alpha = \beta = \gamma = 1$, ezért $\underline{u}$, $\underline{v}$ és $\underline{w}$ nem lineárisan függetlenek. (2 pont)
Így a feladat kérdésére a válasz: $\underline{u}$, $\underline{v}$ és $\underline{w}$ a $p \neq -1$ értékekre lineárisan függetlenek.
A fenti lineáris egyenletrendszer Gauss-eliminációval is megoldható (annak ellenére is, hogy ez már az első zárthelyi után szerepelt az anyagban). Ha valaki így dolgozik, akkor a (nagyon egyszerű) eliminációért 2 pont jár, majd annak az eredményéből a $p \neq -1$, illetve a $p = -1$ esetben a helyes következtetés (világosan megindokolt) levonásáért 3, illetve 2 pont jár. Ebből a 3+2 pontból pedig 1+1 pont jár az egyenletrendszerre vonatkozó következtetésért (egyértelműen megoldható, illetve végtelen sok megoldása van) és 2+1 pont a vektorok lineáris függetlenségére vonatkozó helyes következtetésért.

6*. Létezik-e olyan n egész szám, amelyre $n^4 + 1$ osztható 101-gyel?

* * * * *

Tegyük fel, hogy $101 \mid n^4 + 1$ valamely n egészre. Ekkor $n^4 \equiv -1 \pmod{101}$. (1 pont)
Ha $101 \mid n$ teljesülne, akkor $101 \mid n^4$, vagyis $n^4 \equiv 0 \pmod{101}$ következne, ami ellentmondás. Így $101 \nmid n$, amiből $(101, n) = 1$ (hiszen 101 prím). (2 pont)
Ezért alkalmazható az Euler-Fermat tétel n-re és 101-re: $n^{\varphi(101)} \equiv 1 \pmod{101}$. (2 pont)
Mivel 101 prím, ezért $\varphi(101) = 100$. Vagyis $n^{100} \equiv 1 \pmod{101}$. (1 pont)
Másrészt az $n^4 \equiv -1 \pmod{101}$ kongruenciát 25-ödik hatványra emelve: $n^{100} \equiv (-1)^{25} \pmod{101}$, vagyis $n^{100} \equiv -1 \pmod{101}$. (2 pont)
Ez az ellentmondás mutatja, hogy ilyen n egész nem létezhet (hiszen $1 \not\equiv -1 \pmod{101}$). (2 pont)