Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2017. október 19.

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.

1. Mennyi maradékot ad 176-tal osztva 799^{801}?

* * * * *

176 prímtényezős felbontása: $176 = 2^4 \cdot 11$. (1 pont)
Ezért a tanult képlet szerint $\varphi(176) = (2^4 - 2^3)(11 - 1) = 80$. (2 pont)
Mivel $(799, 176) = 1$ (hiszen 799 sem 2-vel, sem 11-gyel nem osztható), (1 pont)
ezért az Euler-Fermat tételből $799^{80} \equiv 1 \pmod{176}$ következik. (2 pont)
Mindkét oldalt a 10-edik hatványra emelve: $799^{800} \equiv 1^{10} = 1 \pmod{176}$. (2 pont)
Mindkét oldalt 799-cel szorozva: $799^{801} \equiv 799 \equiv 95 \pmod{176}$. (2 pont)
Így 799^{801} 95 maradékot ad 176-tal osztva.
Ha valaki az utolsó lépésben 799-nek a 176-os maradékát már nem számítja ki (és ezért 799-et ad végeredménynek), az ezért 1 pontot veszítsen. 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 legfőljebb 2 pontot kaphat annak felismeréséért, hogy ez az algoritmus elvileg alkalmas a kérdés megválaszolására. További 8 pontot kaphat a helyes számításokért: a 799^{2^k} hatványok 176-os maradékai a $k = 0, \ldots, 9$ értékekre (ezek sorra : 95, 49, 113, 97, 81, 49, 113, 97, 81, 49) darabonként fél-fél pontot érjenek, a 801 felírása 2-es számrendszerben ($801 = 2^0 + 2^5 + 2^8 + 2^9$) 1 pontot, majd a 799^1, 799^{33}, 799^{289}, 799^{801} hatványok maradékai (ezek sorra: 95, 79, 63, 95) ismét darabonként fél-fél pontot érjenek.

2. Egy n egész szám 115-szöröse 110-zel nagyobb maradékot ad 344-gyel osztva, mint maga az n szám. Milyen maradékot adhat n 344-gyel osztva?

* * * * *

Első megoldás. A feladat szövege szerint $115n \equiv n + 110 \pmod{344}$. Mindkét oldalból n-et levonva a $114n \equiv 110 \pmod{344}$ lineáris kongruenciát kapjuk. (1 pont)
Mindkét oldalt 2-vel osztva: $57n \equiv 55 \pmod{172}$, ahol a modulust $(2, 344) = 2$ miatt kellett 2-vel elosztani. (1 pont)
Mindkét oldalt 3-mal szorozva: $171n \equiv 165 \pmod{172}$, vagyis $-n \equiv -7 \pmod{172}$. (2 pont)
Mindkét oldalt (-1)-vel szorozva: $n \equiv 7 \pmod{172}$. (1 pont)
Minden megtett lépés ekvivalens lépés volt – beleértve a 3-mal való szorzást is, $(3, 172) = 1$ miatt. Ezért az $n \equiv 7 \pmod{172}$ feltételt kielégítő n-ek valóban megoldásai a lineáris kongruenciának. (3 pont)
Ebből $n \equiv 7 \pmod{344}$ vagy $n \equiv 7 + 172 = 179 \pmod{344}$, vagyis az n egész 7 vagy 179 maradékot adhat 344-gyel osztva. (2 pont)
A lépések ekvivalenciája helyett hivatkozhatunk arra is, hogy $(114, 344) = 2$ miatt két megoldás kell legyen modulo 344, vagy akár ellenőrizhetjük is a kapott eredményeket. (Viszont a három érv közül valamelyikre szükség van annak annak kizárásához, hogy a kapott eredmények között hamis gyök lehessen.) Ha egy megoldó csak azt ellenőrzi, hogy $(114, 344) = 2 \big| 110$, így a lineáris kongruenciának két megoldása van modulo 344, de ezeket kiszámolni nem tudja, az (az átrendezéssel együtt) összesen 3 pontot kapjon. Számolási hibákért 1-1 pont vonandó le, de a maradék pontszám csak akkor jár, ha a hiba miatt a feladat nem lett lényegesen könnyebb. Ha valaki a szöveget félreértelmezi és a $115n + 110 \equiv n \pmod{344}$ feladatot oldja meg, az ezért 1 pontot veszítsen.

Második megoldás. A feladat szövege szerint $115n \equiv n + 110 \pmod{344}$. Mindkét oldalból n-et levonva a $114n \equiv 110 \pmod{344}$ lineáris kongruenciát kapjuk. (1 pont)
Ezt az előadáson tanult (euklideszi) algoritmussal oldjuk meg.
Ehhez először 114 és 344 legnagyobb közös osztóját kell meghatározni; mivel $(114, 344) = 2 \big| 110$, ezért lesz megoldás (mégpedig 2 darab modulo 344) és az algoritmust 2-vel való osztással kell kezdenünk hogy az n együtthatója és a modulus relatív prímek legyenek. (2 pont)
2-vel osztva: $57n \equiv 55 \pmod{172}$, ahol a modulust $(2, 344) = 2$ miatt kellett 2-vel elosztani. (2 pont)
Most a $172n \equiv 0 \pmod{172}$ kongruenciából ki kell vonnunk a $57n \equiv 55 \pmod{172}$ kongruencia 3-szorosát: $n \equiv -165 \equiv 7 \pmod{172}$. Ezzel az algoritmus futása máris véget ért. (3 pont)
Ebből $n \equiv 7 \pmod{344}$ vagy $n \equiv 7 + 172 = 179 \pmod{344}$, vagyis az n egész 7 vagy 179 maradékot adhat 344-gyel osztva. (2 pont)
Ha egy megoldó $(114, 344)$ meghatározása és 2-vel osztás helyett rögtön a $114n \equiv 110 \pmod{344}$ lineáris kongruenciára kezdi futtatni az algoritmust és így (annak a 3-szorosát a $344n \equiv 0 \pmod{344}$ kongruenciából kivonva) egy lépésben a $2n \equiv 14 \pmod{344}$ kongruenciához jut, majd ebből 2-vel osztás után jut a végeredményhez, akkor a teljes értékű megoldáshoz indokolnia kell, hogy a kapott eredmények tényleg helyesek. (Ugyanis az a megoldó, aki így jár el, nem az előadáson tanult módszert követi, ezért nem is hagyatkozhat annak az előadáson bizonyított helyességére.) Ez az indoklás történhet az eredmények ellenőrzésével vagy arra hivatkozva, hogy $(114, 344) = 2$ miatt két megoldásnak kell lennie modulo 344, ezért a kapott eredmények között nem lehet hamis gyök. Ha egy megoldó ezt az indoklást elmulasztja, ezért 3 pontot veszítsen.

3. Tartalmazza-e az $R(1; 3; 4)$ pontot az a sík, amelyet a $P(1; 7; -1)$ és a $Q(11; 9; -5)$ pontokat összekötő egyenes a P-ben merőlegesen döf?

* * * * *

A keresett síkra merőleges a P-t és Q-t összekötő egyenes, ezért $\overrightarrow{PQ}$ normálvektora a síknak. (3 pont)
$\overrightarrow{PQ} = \underline{q} - \underline{p} = (11; 9; -5) - (1; 7; -1) = (10; 2; -4)$, ahol $\underline{p}$ és $\underline{q}$ a megfelelő pontokba mutató helyvektorokat jelöli. (2 pont)
$\overrightarrow{PQ}$ helyett használhatjuk annak a felét, az $\underline{n} = (5; 1; -2)$ vektort is normálvektornak.
A síkra illeszkedő P pont és $\underline{n}$ ismeretében már felírható a sík egyenlete:
$5x + y - 2z = 5 \cdot 1 + 1 \cdot 7 + (-2) \cdot (-1) = 14$. (3 pont)
Behelyettesítve az R pont koordinátáit az egyenlet nem teljesül, így a sík nem tartalmazza R-et.(2 pont)

4. Tegyük fel, hogy az ($\mathbb{R}^n$-beli) $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{10}$ vektorok lineárisan összefüggők, de közülük bármely 9-et kiválasztva lineárisan független vektorrendszert kapunk. Mutassuk meg, hogy a $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{10}$ vektorok bármely $\underline{0}$-t adó lineáris kombinációjában vagy mindegyik együttható 0 vagy egyik együttható sem 0. (Azaz: mutassuk meg, hogy $\lambda_1 \cdot \underline{v}_1 + \lambda_2 \cdot \underline{v}_2 + \ldots + \lambda_{10} \cdot \underline{v}_{10} = \underline{0}$ esetén $\lambda_1 = \lambda_2 = \ldots = \lambda_{10} = 0$ vagy $\lambda_1 \cdot \lambda_2 \cdot \ldots \cdot \lambda_{10} \neq 0$ teljesül.)

* * * * *

Tegyük fel indirekt, hogy a feladat állítása hamis: léteznek a $\lambda_1, \lambda_2, \ldots, \lambda_{10}$ együtthatók úgy, hogy ezek nem mindegyike 0, de van köztük 0 és $\lambda_1 \cdot \underline{v}_1 + \lambda_2 \cdot \underline{v}_2 + \ldots + \lambda_{10} \cdot \underline{v}_{10} = \underline{0}$. (2 pont)
Mivel a $\underline{v}_i$-k (és ezekkel együtt a λ_i-k) számozása érdektelen, feltehetjük, hogy például $\lambda_{10} = 0$. Ekkor a $\lambda_1 \cdot \underline{v}_1 + \lambda_2 \cdot \underline{v}_2 + \ldots + \lambda_9 \cdot \underline{v}_9 = \underline{0}$ összefüggést kapjuk, ahol a $\lambda_1, \lambda_2, \ldots, \lambda_9$ együtthatók nem mindegyike 0 (hiszen $\lambda_1, \lambda_2, \ldots, \lambda_{10}$ között volt 0-tól különböző). (2 pont)
Ebből a tanultak szerint következik, hogy a $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_9$ vektorok lineárisan összefüggők. (4 pont)
Ez pedig ellentmond a feladat állításának (miszerint $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{10}$ közül bármelyik 9 lineárisan független), amivel tehát az állítást beláttuk. (2 pont)

5. Határozzuk meg az alábbi, $\mathbb{R}^3$-beli vektorok generált alterét. Amennyiben ez az altér egyenes vagy sík, adjuk meg az egyenletét vagy egyenletrendszerét.

$$\underline{a} = \begin{pmatrix} 4 \\ 3 \\ 0 \end{pmatrix}, \underline{b} = \begin{pmatrix} 5 \\ 2 \\ 1 \end{pmatrix}, \underline{c} = \begin{pmatrix} 13 \\ 1 \\ 5 \end{pmatrix}$$

* * * * *

Első megoldás. Mivel $\underline{a}$ és $\underline{b}$ nem párhuzamosak (mert nem skalárszorosai egymásnak), (1 pont)
ezért az $\langle \underline{a}, \underline{b} \rangle$ generált altér (vagyis az $\underline{a}$-ból és $\underline{b}$-ből lineáris kombinációval kifejezhető vektorok halmaza) az $\underline{a}$ és $\underline{b}$ (origóba tolt, vagyis helyvektor példányai) által kifeszített, origón átmenő S sík vektoraiból áll. (1 pont)
S-nek normálvektora bármilyen $\underline{n} \neq \underline{0}$ vektor, ami $\underline{a}$-ra és $\underline{b}$-re is merőleges. (1 pont)
Az $\underline{n} = (a, b, c)$ vektor pontosan akkor ilyen, ha az $\underline{n} \cdot \underline{a}$ és az $\underline{n} \cdot \underline{b}$ skaláris szorzatok értéke 0. (1 pont)
A skaláris szorzat képletéből: $4a + 3b = 0$ és $5a + 2b + c = 0$. (1 pont)
Például a $b = -4$ választással $a = 3$ és $c = -7$ adódik, vagyis $\underline{n} = (3; -4; -7)$ jó normálvektor. (1 pont)
Ebből tehát S egyenlete: $3x - 4y - 7z = 0$. (1 pont)
A $\underline{c}$ koordinátái kielégítik ezt az egyenletet, így $\underline{c}$ (origóba tolt példánya) is S-ben fekszik (hiszen a $C(13; 1; 5)$ pont S-en van és $\underline{c}$ az origóból C-be mutat). (1 pont)
Ezért az $\langle \underline{a}, \underline{b}, \underline{c} \rangle$ generált altér is csak az S vektoraiból áll (hiszen S-beli vektorok lineáris kombinációja is S-beli kell legyen). (2 pont)
Így tehát $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : 3x - 4y - 7z = 0 \right\}$.

A fenti megoldásban az utolsó 3 pontnak megfelelő rész helyett az alábbi is jó:
Mivel $\underline{c} = -3\underline{a} + 5\underline{b}$, (1 pont)
ezért minden $\underline{a}$-ból, $\underline{b}$-ből és $\underline{c}$-ből lineáris kombinációval kifejezhető vektor már $\underline{a}$-ból és $\underline{b}$-ből is kifejezhető; vagyis $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \langle \underline{a}, \underline{b} \rangle$. (2 pont)

Második megoldás. A $\underline{v} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ vektor pontosan akkor van az $\langle \underline{a}, \underline{b}, \underline{c} \rangle$ generált altérben, ha $\underline{v}$ kifejezhető $\underline{a}$-ból, $\underline{b}$-ből és $\underline{c}$-ből lineáris kombinációval; vagyis ha léteznek olyan α, β, γ együtthatók, hogy $\alpha \cdot \underline{a} + \beta \cdot \underline{b} + \gamma \cdot \underline{c} = \underline{v}$. (1 pont)
Behelyettesítve $\underline{a}, \underline{b}, \underline{c}$ konkrét értékét és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} 4\alpha + 5\beta + 13\gamma &= x \\ 3\alpha + 2\beta + \gamma &= y \\ \beta + 5\gamma &= z \end{aligned}$$ (2 pont)

Az utolsó egyenletből $\beta = z - 5\gamma$. Ezt az első két egyenletbe helyettesítve: $4\alpha - 12\gamma = x - 5z$, $3\alpha - 9\gamma = y - 2z$. Vagyis átrendezés után: $\alpha - 3\gamma = \frac{x-5z}{4}$, illetve $\alpha - 3\gamma = \frac{y-2z}{3}$. (1 pont)

Ebből már látszik, hogy az egyenletrendszer akkor és csak akkor megoldható, ha $\frac{x-5z}{4} = \frac{y-2z}{3}$. Valóban: ez a feltétel egyrészt nyilván szükséges a megoldhatósághoz (az utóbbi két egyenlet miatt). (1 pont)

Másrészt elégséges is: ha $\frac{x-5z}{4}$ és $\frac{y-2z}{3}$ közös értékét t jelöli, akkor például $\alpha = t$, $\beta = z$, $\gamma = 0$ nyilván megoldása az egyenletrendszernek. (2 pont)

A kapott feltételt átrendezve: $3x - 4y - 7z = 0$. Így $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : 3x - 4y - 7z = 0 \right\}$. (1 pont)

Ez pedig a tanultak szerint egy sík egyenlete (mégpedig az origón átmenő, $\underline{n} = (3; -4; -7)$ normálvektorú síké). (2 pont)

A teljes értékű megoldáshoz nem szükséges megadni a sík normálvektorát, sem azt, hogy az origón megy át. Ha valaki az első megoldás után írtak szerint először belátja, hogy $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \langle \underline{a}, \underline{b} \rangle$ és ezután a fentihez hasonló módon az $\langle \underline{a}, \underline{b} \rangle$ generált alteret határozza meg, akkor $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \langle \underline{a}, \underline{b} \rangle$ megmutatásáért 2 pontot kapjon, viszont az (ebben az esetben csak két változós) lineáris egyenletrendszer megoldhatóságának feltétele a fentiek szerinti $4(= 1 + 1 + 2)$ pont helyett csak 2 pontot érjen.

6*. Létezik-e páros Carmichael-szám?

* * * * *

Legyen $n > 2$ tetszőleges páros egész. Megmutatjuk, hogy n nem Carmichael-szám – vagyis a kérdésre a válasz nemleges. (Az $n = 2$ esettel nem kell foglalkoznunk, mert a Carmichael-számok definíció szerint nem lehetnek prímek.)

Ehhez a Carmichael-szám definíciója szerint be kell látnunk, hogy létezik olyan a egész, amelyre az $1 \leq a \leq n-1$, $(a, n) = 1$ és $a^{n-1} \not\equiv 1 \pmod{n}$ feltételek teljesülnek (vagyis a árulója n-nek).(4 pont)

Állítjuk, hogy az $a = n - 1$ választás megfelel ezeknek a feltételeknek.

Valóban, egyrészt $(a, n) = (n - 1, n) = 1$, mert ha egy d egészre $d|n$ és $d|n-1$, akkor $d|n-(n-1) = 1$ is fennáll, így n és $n - 1$ közös osztói csak a ± 1. (2 pont)

Másrészt $a = n - 1 \equiv -1 \pmod{n}$ miatt $a^{n-1} \equiv (-1)^{n-1} = -1 \not\equiv 1 \pmod{n}$, ahol $(-1)^{n-1} = -1$ azért igaz, mert $n - 1$ páratlan (4 pont)

(és $-1 \not\equiv 1 \pmod{n}$ pedig azért, mert $n > 2$).

Így $a = n - 1$ valóban árulója n-nek, amivel az állítást beláttuk.