Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2024. október 25.

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 500 között, aminek a 48-szorosa 1-gyel nagyobb maradékot ad 277-tel osztva, mint maga az n szám.

* * * * *

A feladat feltételeiből $48n \equiv n+1 \pmod{277}$. Átrendezve: $47n \equiv 1 \pmod{277}$. (1 pont)
Mivel $(47, 277) = 1$ (mert 47 prím és $47 \nmid 277$), ezért a kapott lineáris kongruencia a tanult tétel szerint megoldható és 1 megoldása van modulo 277. (1 pont)
Mindkét oldalt 6-tal szorozva: $282n \equiv 6 \pmod{277}$, vagyis $5n \equiv 6 \pmod{277}$. (1 pont)
A 6-tal való szorzás $(6, 277)$ miatt ekvivalens lépés volt (vagyis a megoldáshalmaz nem változott). (1 pont)
Ez $6 \equiv 560 \pmod{277}$ miatt ekvivalens ezzel: $5n \equiv 560 \pmod{277}$. (1 pont)
Mindkét oldalt 5-tel osztva: $n \equiv 112 \pmod{277}$, (1 pont)
ahol a modulus $(277, 5) = 1$ miatt nem változott. (1 pont)
Mivel minden megtett lépés ekvivalens volt, így a kapott $n \equiv 112 \pmod{277}$ valóban megoldása a lineáris kongruenciának. (Itt a lépések ekvivalenciája helyett hivatkozhatunk arra is, hogy mivel a megoldások száma 1 modulo 277, ezért ez csak a 112 lehet, így az valóban megoldás; illetve természetesen ellenőrzéssel is meggyőződhetünk a 112 helyességéről.) (2 pont)
Így az 1 és 500 közötti számok közül $n = 112$ és $n = 389$ felel meg a feladat feltételeinek. (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 $277n \equiv 0 \pmod{277}$, $47n \equiv 1 \pmod{277}$, $42n \equiv -5 \pmod{277}$, $5n \equiv 6 \pmod{277}$, $2n \equiv -53 \pmod{277}$, $n \equiv 112 \pmod{277}$ 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 közvetlenül, az első fázisbeli leosztás nélkül alkalmazható, mert $(47, 277) = 1$; végül 5 pontot ér maga a számolás. A hiányzó 2 pont a fenti pontozás szerinti első, illetve utolsó $1 + 1$ pont.

2. Adjuk meg az összes olyan n egész számot 1 és 2024 között, aminek az utolsó két számjegye a 6-os és a 8-as számrendszerben is 11.

* * * * *

A feladat feltételeiből $n \equiv 7 \pmod{36}$ és $n \equiv 9 \pmod{64}$ adódik. (3 pont)
A kapott kongruenciarendszert a tanult módszerrel oldjuk meg. Az első kongruenciából $n = 36k + 7$ valamilyen k egészre. Ezt a másodikba helyettesítve: $36k + 7 \equiv 9 \pmod{64}$. (2 pont)
Mindkét oldalból 7-et levonva a $36k \equiv 2 \pmod{64}$ lineáris kongruenciát kapjuk. (1 pont)
Mivel azonban $(36, 64) = 4 \nmid 2$, ezért ennek a tanult tétel szerint nincs megoldása. (3 pont)
Így nincs megoldása a kongruenciarendszernek sem, vagyis nem létezik a feltételeknek megfelelő n egész (1 és 2024 között sem). (1 pont)
Ha egy megoldó a feladat szövegéből adódó kongruenciarendszert nem tudja helyesen felírni és ezért egy másik kongruenciarendszert old meg, akkor az első 3 pont elvesztése után maradó 7 pontból is csak annyit kaphat meg, amennyi a fenti megoldásnak megfeleltethető. Így a hibás kongruenciarendszerből adódó helyes számolásért megadható a pontozás szerint következő $2 + 1$ pont. Ha azonban az így kapott lineáris kongruencia megoldható, akkor annak az (akár hibátlan) megoldásért már nem adható meg a pontozás szerinti utolsó $3 + 1$ pont.

3. Az S sík tartalmazza a $P(8; 1; 6)$ pontot és az $x-3 = \frac{y-4}{5} = 3-z$ egyenletrendszerű e egyenest. Metszi-e az S sík az y-tengelyt? Ha igen, hol?

* * * * *

Az e egyenes egyenletrendszerét $\frac{x-3}{1} = \frac{y-4}{5} = \frac{z-3}{-1}$ alakba írva kiolvasható, hogy e átmegy a $Q(3; 4; 3)$ ponton és irányvektora a $\underline{v} = (1; 5; -1)$ vektor. (2 pont)
Mivel S tartalmazza e-t, ezért $\underline{v}$ párhuzamos S-sel. (1 pont)
Ugyancsak párhuzamos S-sel a $\overrightarrow{QP}$ vektor is, vagyis a $\underline{p} - \underline{q} = (5; -3; 3)$ vektor (ahol $\underline{p}$ és $\underline{q}$ a megfelelő pontokba mutató helyvektorokat jelöli). (1 pont)
Így az $\underline{n}$ vektor akkor lesz normálvektora S-nek, ha merőleges $\underline{v}$-re és $\overrightarrow{QP}$-re is (és $\underline{n} \neq \underline{0}$). Ebből $\underline{v} \cdot \underline{n} = 0$ és $\underline{v} \cdot \overrightarrow{QP} = 0$ következik (a skaláris szorzat definíciója szerint). (1 pont)
Ha $\underline{n} = (a, b, c)$, akkor ebből (a skaláris szorzat kiszámítására tanultak miatt) $a + 5b - c = 0$ és $5a - 3b + 3c = 0$ adódik. (1 pont)
Ebből például a $c = 1$ választással az $a + 5b = 1$, $5a - 3b = -3$ egyenletrendszert kapjuk. Az első 5-szöröséből a másodikat levonva $28b = 8$, vagyis $b = \frac{2}{7}$; amiből pedig $a = -\frac{3}{7}$. A kapott $(-\frac{3}{7}; \frac{2}{7}; 1)$ vektor helyett annak a (-7)-szeresét választva normálvektornak: $\underline{n} = (3; -2; -7)$. (1 pont)
Ebből és (például) P-ből már felírhatjuk S egyenletét: $3x - 2y - 7z = -20$. (1 pont)
Az y-tengelyen azok a pontok vannak, amiknek az x és z koordinátája 0. Ebből S és az y-tengely metszéspontjára a $-2y = -20$ egyenletet kapjuk. Így S metszi az y-tengelyt, mégpedig a $(0; 10; 0)$ pontban. (2 pont)

4. Az $\mathbb{R}^n$-beli $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ vektorokról tudjuk, hogy $\underline{d} \in \langle \underline{a}, \underline{b}, \underline{c} \rangle$ és $\underline{a} \notin \langle \underline{b}, \underline{c}, \underline{d} \rangle$. Döntsük el, hogy az alábbi állításokra melyik áll fenn a következő lehetőségek közül:

(i) az állítás biztosan igaz;
(ii) az állítás biztosan hamis;
(iii) az állítás lehet igaz és hamis is ($\underline{a}, \underline{b}, \underline{c}$ és $\underline{d}$ választásától függően).

a) $\underline{d} \in \langle \underline{b}, \underline{c} \rangle$ b) $\underline{b} \in \langle \underline{c}, \underline{d} \rangle$

(Döntéseinket természetesen indokoljuk is.)

* * * * *

a) Az állítás (biztosan) igaz. (0 pont)
Ugyanis $\underline{d} \in \langle \underline{a}, \underline{b}, \underline{c} \rangle$ miatt léteznek olyan α, β, γ skalárok, amikre $\underline{d} = \alpha\underline{a} + \beta\underline{b} + \gamma\underline{c}$. (1 pont)
Megmutatjuk, hogy itt $\alpha = 0$. Ha ugyanis $\alpha \neq 0$ volna, akkor átrendezéssel az $\underline{a} = -\frac{\beta}{\alpha}\underline{b} - \frac{\gamma}{\alpha}\underline{c} + \frac{1}{\alpha}\underline{d}$ egyenletet kapnánk. (1 pont)
Ebből viszont $\underline{a} \in \langle \underline{b}, \underline{c}, \underline{d} \rangle$ következne, szemben a feladat állításával. Így $\alpha = 0$ valóban következik. (2 pont)
Ebből és a fenti egyenletből tehát $\underline{d} = \beta\underline{b} + \gamma\underline{c}$, ami valóban bizonyítja a $\underline{d} \in \langle \underline{b}, \underline{c} \rangle$ állítást. (1 pont)
b) Az állítás lehet igaz és hamis is. (0 pont)
Ennek megmutatásához először olyan példát mutatunk, amikor az állítás igaz. Legyen például $\underline{a}$ és $\underline{b}$ két, egymással nem párhuzamos síkvektor (vagyis $\mathbb{R}^2$-beli vektor) és legyen $\underline{b} = \underline{c} = \underline{d}$. (Például lehet $\underline{a} = (1; 0)$ és $\underline{b} = \underline{c} = \underline{d} = (0; 1)$.) (0 pont)
Ekkor $\underline{a} \notin \langle \underline{b}, \underline{c}, \underline{d} \rangle$ igaz, hiszen a $\underline{b} = \underline{c} = \underline{d}$ vektorokból csak a velük párhuzamos síkvektorok fejezhetők ki lineáris kombinációval és $\underline{a}$ nem ilyen. (1 pont)
Másrészt a $\underline{d} \in \langle \underline{a}, \underline{b}, \underline{c} \rangle$ és $\underline{b} \in \langle \underline{c}, \underline{d} \rangle$ állítások is igazak, mert $\underline{d} = 0 \cdot \underline{a} + 1 \cdot \underline{b} + 0 \cdot \underline{c}$ és $\underline{b} = 1 \cdot \underline{c} + 0 \cdot \underline{d}$. (1 pont)
Most olyan példát mutatunk, amikor az állítás hamis. Legyen például $\underline{a}$, $\underline{b}$ és $\underline{c}$ három olyan térvektor (vagyis $\mathbb{R}^3$-beli vektor), amik nem esnek egy síkba és legyen $\underline{d} = \underline{c}$. (Például lehet $\underline{a} = (1; 0; 0)$, $\underline{b} = (0; 1; 0)$ és $\underline{c} = \underline{d} = (0; 0; 1)$.) (0 pont)
Ekkor $\underline{d} \in \langle \underline{a}, \underline{b}, \underline{c} \rangle$ igaz, mert $\underline{d} = 0 \cdot \underline{a} + 0 \cdot \underline{b} + 1 \cdot \underline{c}$. (1 pont)
Igaz továbbá $\underline{a} \notin \langle \underline{b}, \underline{c}, \underline{d} \rangle$ is, mert a $\underline{b}$ és $\underline{c} = \underline{d}$ vektorokból csak az általuk meghatározott (origón átmenő) sík vektorai fejezhetők ki lineáris kombinációval és $\underline{a}$ nem ilyen. (1 pont)
Viszont most nem igaz a $\underline{b} \in \langle \underline{c}, \underline{d} \rangle$ állítás, mert a $\underline{c} = \underline{d}$ vektorból csak a vele párhuzamos vektorok fejezhetők ki lineáris kombinációval és $\underline{b}$ nem ilyen (különben $\underline{a}$, $\underline{b}$ és $\underline{c}$ egy síkba esnének). (1 pont)
Természetesen számtalan más jó példa mutatható arra is, hogy $\underline{b} \in \langle \underline{c}, \underline{d} \rangle$ igaz és arra is, hogy nem az. Ezeknek a pontozása minden esetben úgy alakul, hogy a konkrét példák megadása önmagában nem ér pontot, a helyességüknek az indoklása pedig 2, illetve 3 pontot ér az igaz, illetve a hamis esetben. Részpontszám mindkét esetben csak akkor adható, ha a megoldó világossá tette a célkitűzését – vagyis hogy az állítás igaz vagy hamis voltára kíván példát mutatni – és a példája ennek a célkitűzésnek valóban megfelel. Így tehát nem adható részpontszám arra, ha a megoldó négy, általa megadott vektorra ötletszerűen ellenőrzi bizonyosak teljesülését a $\underline{d} \in \langle \underline{a}, \underline{b}, \underline{c} \rangle$, $\underline{a} \notin \langle \underline{b}, \underline{c}, \underline{d} \rangle$ és $\underline{b} \in \langle \underline{c}, \underline{d} \rangle$ állítások közül. (Ha viszont ilyen ellenőrzésekből csak utólag veszi észre, hogy sikerült példát mutatnia valamelyik esetre, az természetesen nem baj, a megfelelő részpontszám jár.)

5. Lineárisan függetlenek-e az alábbi, $\mathbb{R}^4$-beli vektorok?

$$\underline{u} = \begin{pmatrix} 1 \\ -3 \\ 1 \\ 1 \end{pmatrix}, \ \underline{v} = \begin{pmatrix} -2 \\ 6 \\ 1 \\ 4 \end{pmatrix}, \ \underline{w} = \begin{pmatrix} 0 \\ 0 \\ 4 \\ 9 \end{pmatrix}$$

* * * * *

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. (2 pont)
Behelyettesítve az $\underline{u}, \underline{v}, \underline{w}$ vektorokat és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} \alpha - 2\beta &= 0 \\ -3\alpha + 6\beta &= 0 \\ \alpha + \beta + 4\gamma &= 0 \\ \alpha + 4\beta + 9\gamma &= 0 \end{aligned} \qquad \text{(2 pont)}$$

Az első egyenletből $\alpha = 2\beta$. Ezt a harmadikba és a negyedikbe beírva: $3\beta + 4\gamma = 0$ és $6\beta + 9\gamma = 0$. (1 pont)
Az utóbbi egyenletből az előbbi dupláját kivonva: $\gamma = 0$. Ezt (például) a $3\beta + 4\gamma = 0$ egyenletbe visszahelyettesítve $\beta = 0$ is adódik, amiből $\alpha = 2\beta$ miatt $\alpha = 0$. (2 pont)
Így a tanultak szerint $\underline{u}, \underline{v}, \underline{w}$ lineárisan függetlenek (mert $\alpha\underline{u} + \beta\underline{v} + \gamma\underline{w} = \underline{0}$ csak az $\alpha = \beta = \gamma = 0$ esetben lehetséges). (3 pont)

A feladat természetesen megoldható a lineáris függetlenség eredeti definíciójára alapozva is (vagyis annak megmutatásával, hogy $\underline{u}, \underline{v}$ és $\underline{w}$ közül egyik sem kifejezhető a másik kettő lineáris kombinációjaként). Ekkor az $\underline{u} \notin \langle \underline{v}, \underline{w} \rangle$ és $\underline{v} \notin \langle \underline{u}, \underline{w} \rangle$ állítások indoklásáért 2–2 pont, a $\underline{w} \notin \langle \underline{u}, \underline{v} \rangle$ állítás indoklásáért pedig 3 pont jár; a hiányzó 3 pont pedig a definíció helyes alkalmazásáért jár (beleértve tehát ebbe annak az ismeretét is, hogy ezt az utat járva mindhárom állítás igazolása szükséges a lineáris függetlenség megmutatásához). 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+2 pont jár, a többi rész pontozása megfelel a fentieknek.

6*. Hány olyan n egész szám van 1 és 275 között, amire teljesül az $n^{201} \equiv n \pmod{275}$ kongruencia?

* * * * *

$n^{201} \equiv n \pmod{275}$ pontosan akkor teljesül, ha igazak az $n^{201} \equiv n \pmod{11}$ és az $n^{201} \equiv n \pmod{25}$ kongruenciák. Valóban: $n^{201} \equiv n \pmod{275}$ a kongruencia (második, ekvivalens) definíciója szerint azt jelenti, hogy $275 \mid n^{201} - n$; márpedig egy szám pontosan akkor osztható 275-tel, ha 11-gyel és 25-tel is osztható ($5^2 \cdot 11 = 275$, $(25, 11) = 1$, valamint a számelmélet alaptétele miatt). (1 pont)
Így külön-külön fogjuk megvizsgálni, hogy ez a két kongruencia milyen n-ekre teljesül. Először megmutatjuk, hogy $n^{201} \equiv n \pmod{11}$ minden n egészre igaz. (0 pont)
Ha $11 \mid n$, akkor $11 \mid n^{201}$ is nyilván igaz, így az $n^{201} \equiv n \pmod{11}$ kongruencia fennáll (mert mindkét oldala 0 maradékot ad 11-gyel osztva). (1 pont)
Ha viszont $11 \nmid n$, akkor $(n, 11) = 1$ (mert 11 prím). Így $n^{\varphi(11)} \equiv 1 \pmod{11}$ adódik az Euler-Fermat tételből. Itt $\varphi(11) = 10$, ismét mert 11 prím. (1 pont)
A kapott kongruenciát 20-adik hatványra emelve, majd mindkét oldalt n-nel szorozva $n^{200} \equiv 1 \pmod{11}$, majd $n^{201} \equiv n \pmod{11}$ valóban következik a $11 \nmid n$ esetben is. (1 pont)
Az $n^{201} \equiv n \pmod{25}$ kongruencia viszont már nem minden n-re teljesül. Valóban, ha $5 \mid n$, akkor n^{201} nyilván osztható 25-tel (sőt, még 5^{201}-nel is). Így ha $5 \mid n$, de $25 \nmid n$, akkor $n^{201} \not\equiv n \pmod{25}$. (1 pont)
Megmutatjuk, hogy $n^{201} \equiv n \pmod{25}$ minden más n egészre teljesül; vagyis igaz az 5-tel nem osztható és a 25-tel osztható n-ekre is. (0 pont)
Ha $25 \mid n$, akkor a fentihez hasonlóan $25 \mid n^{201}$ is igaz, így $n^{201} \equiv n \pmod{25}$ fennáll. (0 pont)
Ha viszont $5 \nmid n$, akkor $(25, n) = 1$, mert 25-nek és n-nek nincs közös prímosztója. (1 pont)
$\varphi(25) = \varphi(5^2) = 5^2 - 5^1 = 20$ a tanultak szerint. (1 pont)
Így az Euler-Fermat tételt n-re és 25-re alkalmazva: $n^{20} \equiv 1 \pmod{25}$. (1 pont)
A kapott kongruenciát 10-edik hatványra emelve, majd mindkét oldalt n-nel szorozva $n^{200} \equiv 1 \pmod{25}$, majd $n^{201} \equiv n \pmod{25}$ valóban következik minden $5 \nmid n$ esetben. (1 pont)
A fentieket összegezve tehát azt kaptuk, hogy $n^{201} \equiv n \pmod{275}$ pontosan azokra az n egészekre nem teljesül, amikre $5 \mid n$ és $25 \nmid n$. Ezeknek a száma 1 és 275 között $55 - 11 = 44$ (mert az 5-tel osztható n-ek száma 55, a 25-tel oszthatóké pedig 11). Így azon n-ek száma 1 és 275 között, amikre a $n^{201} \equiv n \pmod{275}$ fennáll: $275 - 44 = 231$. (1 pont)
Ha egy megoldó csak addig jut el, hogy az Euler-Fermat tétel közvetlen alkalmazásával (és a kapott kongruencia n-nel való beszorzásával) kideríti, hogy $n^{201} \equiv n \pmod{275}$ teljesül minden olyan n-re, amire $(n, 275) = 1$, akkor ezért a részeredményért 2 pontot kaphat (annak ellenére is, hogy ez a gondolat önmagában nem tekinthető egy teljes értékű megoldás első érdemi lépésének). Természetesen ez a 2 pont sem jár akkor, ha a megoldó elfelejtkezik az $(n, 275) = 1$ feltételről és így azt hiszi, hogy a kongruencia minden n-re igaz. Ha pedig egy megoldó abban az értelemben használja rosszul az Euler-Fermat tételt, hogy tévesen azt hiszi, hogy $(n, 275) = 1$ szükséges és elégséges feltétele a feladatbeli kongruencia teljesülésének (és így például $\varphi(275)$-öt gondolja a megfelelő n-ek számának), az ebből a 2 pontból csak 1-et kaphat meg.