Bevezetés a számításelméletbe I.
Első pótzárthelyi — pontozási útmutató
2022. november 4.

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 különbözo 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. Mennyi maradékot adhat 273-mal osztva egy olyan szám, melynek 57-szerese 99 maradékot ad 273-mal osztva?

* * * * *

Ha x ilyen szám, akkor $57x \equiv 99 \pmod{273}$. (0 pont)
A tanultak szerint ez a lineáris kongruencia akkor és csak akkor megoldható, ha $(57, 273)|99$ (ahol (a, b) az a és b legnagyobb közös osztóját jelöli). (0 pont)
Mivel $57 = 3 \cdot 19, 273 = 3 \cdot 7 \cdot 13$, a kérdéses lnko 3, amivel 99 osztható, így lesz megoldás, éspedig három darab modulo 273. (0 pont)
A fentiekre persze lehet pontokat kapni (ld. később), de teljes megoldás adható nélkülük is, ezért a hiányuk nem kell, hogy pontlevonással járjon.
A kongruenciát 3-mal osztva az eredetivel ekvivalens $19x \equiv 33 \pmod{91}$ kongruenciát kapjuk. (1+1 pont)
Ezt 5-tel szorozva $95x \equiv 165 \pmod{91}$, ebből pedig $4x \equiv 74 \pmod{91}$ adódik. (1 pont)
Mivel a modulushoz relatív prím számmal történő szorzás ekvivalens átalakítás, ez is ekvivalens az eredeti kongruenciával. (1 pont)
Ezt 2-vel osztva a $2x \equiv 37 \pmod{91}$ kongruenciát kapjuk, ami szintén ekvivalens az eredetivel. (1+1 pont)
Innen $2x \equiv 128 \pmod{91}$, végül 2-vel való újabb osztás után $x \equiv 64 \pmod{91}$. (1 pont)
Ez az osztás is (mint minden helyesen elvégzett osztás) ekvivalens átalakítás, (1 pont)
így a keresett maradékok $64, 64 + 91 = 155$ és $64 + 2 \cdot 91 = 246$. (2 pont)

A kongruenciát természetesen máshogy is meg lehet oldani, pl. Euklideszi algoritmussal. Elvi hibás átalakításért (pl. osztásnál a modulus változásának figyelmen kívül hagyása) darabonként 4 pontot vonjunk le. Aki nem vizsgálja, hogy egy átalakítás ekvivalens-e, attól esetenként 1 pontot

vonjunk le. Ez természetesen kiváltható pl. a kapott megoldások ellenőrzésével vagy a megoldások darabszámára való hivatkozással. A kongruencia két oldalához egymással kongruens számokat adva (vagy olyan átalakítást végezve, ami ennek felel meg) nem szükséges az átalakítás ekvivalenciáját vizsgálni. Ha osztásnál nem világos, hogy a hallgató érti-e, hogy miért nem változik a modulus, ezért darabonként 1 pontot vonjunk le, mint ahogy számolási hibákért is. Aki az Euklideszi algoritmust nem a tanult módon hajtja végre, annak a teljes pontszámért indokolnia kell, hogy a végeredmény miért helyes. Az Euklideszi algoritmust a tanult módon futtató hallgatóknak elég arra hivatkozniuk, hogy az algoritmust használják (ami tudottan helyes eredményt ad). Erre utaló állítás hiányában 1 pontot vonjunk le. Aki csak annyit állapít meg, hogy van megoldás és azt helyesen indokolja, ezért 1 pontot kapjon, aki azt is meg tudja mondani, hogy mod 273 három megoldás lesz, az pedig még 1 pontot.

2. Mennyi maradékot ad 2^{1032} 70-nel osztva?

* * * * *

Első megoldás. Az Euler-Fermat tételt közvetlenül nem tudjuk használni, mert 2 és 70 nem relatív prímek. (0 pont)
Használhatjuk viszont a tételt 2^{1032} 35-ös maradékának meghatározására: $2^{\varphi(35)} \equiv 1 \pmod{35}$, hiszen 2 és 35 relatív prímek. (2 pont)
A tanultak szerint $\varphi(35) = (5-1)(7-1) = 24$, (1 pont)
a $2^{24} \equiv 1 \pmod{35}$ kongruenciát a 43.-ra emelve ($43 \cdot 24 = 1032$ miatt) $2^{1032} \equiv 1 \pmod{35}$ adódik. 2^{1032} 35-ös maradéka tehát 1, (2 pont)
a 70-es maradéka így vagy 1 vagy 36. (3 pont)
Mivel 2^{1032} páros, a keresett maradék 36 kell legyen. (2 pont)

Aki csak annyit állapít meg, hogy az Euler-Fermat tételt közvetlenül nem tudjuk használni, mert 2 és 70 nem relatív prímek és más megoldásra sem kap részpontot, az ezért a megállapításért 1 pontot kapjon.

Második megoldás. A feladatot a modulo m hatványozásról tanultak segítségével oldjuk meg. (0 pont)
$2^1 \equiv 2 \pmod{70}$, $2^2 \equiv 4 \pmod{70}$, $2^4 \equiv 16 \pmod{70}$, $2^8 \equiv 46 \pmod{70}$, mert 46 a $16^2 = 256$ 70-es osztási maradéka. (3 pont)
$2^{16} \equiv 16 \pmod{70}$, mert 16 a $46^2 = 2116$ 70-es osztási maradéka. (2 pont)
A további négyzetre emelések esetén tehát a 16-os és a 46-os maradékok váltogatják egymást, (3 pont)
így $2^{1024} \equiv 16 \pmod{70}$. (1 pont)
A keresett maradék így 2^{1024} és 2^8 maradékai alapján $16 \cdot 46 = 736$ maradéka, vagyis 36 lesz. (1 pont)

3. Mutassuk meg, hogy az $\frac{x-1}{3} = \frac{y-2}{7} = \frac{z-3}{11}$ és $\frac{x+2}{2} = \frac{y+6}{5} = \frac{z-2}{4}$ egyenletrendszerű egyeneseknek van közös pontja és adjuk meg annak a síknak az egyenletét, amely mindkét egyenest tartalmazza.

* * * * *

A közös pont koordinátái a két egyenes egyenletrendszereinek közös megoldásaként adódnak. (0 pont)
Az első egyenletrendszer első egyenletéből $7x - 7 = 3y - 6$, a második egyenletrendszer második egyenletéből pedig $5x + 10 = 2y + 12$. Az utóbbi másfélszereséből az előbbit levonva $\frac{1}{2}x + 22 = 24$, vagyis $x = 4$, majd innen $y = 9$ adódik. (1 pont)
Az első egyenletrendszer második egyenletéből így $z = 14$-et kapjuk. (1 pont)
Az így kapott értékekre persze teljesül az első egyenletrendszer mindkét egyenlete és a második egyenletrendszer első egyenlete, ellenőriznünk kell azonban, hogy a második egyenletrendszer második egyenlete is teljesül-e (igen). (1 pont)

Számolási hibáért (darabonként) 1 pontot vonjunk le. Természetesen aki megadja az $x = 4, y = 9, z = 14$ koordinátákat és ellenőrzi, hogy ezek mindkét egyenletrendszert kielégítik, az is kapjon 3 pontot. A közös pont kiszámítása helyett lehet arra is hivatkozni, hogy létezik a két egyenest tartalmazó sík (amennyiben ezt a hallgató csakugyan megmutatja) és a két egyenes nem párhuzamos (hiszen az irányvektoraik nem számszorosai egymásnak), így kell legyen metszéspontjuk.

Olyan S síkot keresünk, mely tartalmazza mindkét egyenest (vagyis párhuzamos is mindkettővel), a normálvektora tehát merőleges mindkét egyenes irányvektorára. (1 pont)
Az egyenletrendszerekből leolvasható, hogy az első egyenes irányvektora $(3, 7, 11)$, a másodiké $(2, 5, 4)$. (1 pont)
Legyen a keresett normálvektor (a, b, c), ekkor a két merőlegességi feltételből (a skaláris szorzat használatával) $3a + 7b + 11c = 0$ és $2a + 5b + 4c = 0$. (1 pont)
Az első egyenletből a második másfélszeresét kivonva $5c = \frac{b}{2}$, vagyis $b = 10c$ adódik, innen pedig $a = -27c$, a normálvektor(ok egyike) tehát $(-27, 10, 1)$. (2 pont)
A $(-27, 10, 1)$ normálvektorú síkok tehát mindkét egyenessel párhuzamosak, azt keressük közülük, amely tartalmazza is az egyeneseket, ehhez elég pl. ha a sík tartalmazza a már kiszámított metszéspontot, (1 pont)
innen a keresett egyenlet $-27x + 10y + z = -27 \cdot 4 + 10 \cdot 9 + 14 = -4$. (1 pont)
Aki nem számítja ki a metszéspontot, annak persze másképp kell garantálnia, hogy a sík mindkét egyenest tartalmazza: vehet például az egyik egyenesről egy pontot és annak segítségével felírhatja a sík egyenletét, majd a másik egyenes egy pontját ebbe behelyettesítve győződhet meg róla, hogy a sík nem csak párhuzamos mindkét egyenessel, hanem tartalmazza is azokat.

4. A $V \subseteq \mathbb{R}^6$ halmaz azon vektorokból áll, melyeknek ugyanannyi pozitív koordinátájuk van, mint negatív. Így például a jobbra látható $\underline{v}$ vektor V-beli, míg $\underline{w}$ nem V-beli. Altér-e V $\mathbb{R}^6$-ban?

$$\underline{v} = \begin{pmatrix} 2 \\ 0 \\ 5 \\ -1 \\ -3 \\ 0 \end{pmatrix}, \underline{w} = \begin{pmatrix} 3 \\ -2 \\ 6 \\ 0 \\ 2 \\ 7 \end{pmatrix}$$

* * * * *

V akkor és csak akkor altér, ha bármely két V-beli vektor összege is V-beli és bármely V-beli vektor bármely számszorosa is V-beli. (0 pont)
Az $(1, -1, 0, 0, 0, 0)^T$ és $(-1, 2, 0, 0, 0, 0)^T$ vektorok V-ben vannak, az összegük, a $(0, 1, 0, 0, 0, 0)^T$ vektor azonban nincs, (6 pont)
így V a fentiek szerint nem altér. (4 pont)

Természetesen rengeteg másik ellenpélda is adható. Aki ténylegesen nem bizonyítja be (pl. ellenpéldával), hogy az összeadásra nem zárt V, hanem csak annyit állapít meg, hogy *nem feltétlen* zárt, az az ezt alátámasztó érvelése minőségétől függően 0 és 4 közti pontot kapjon az első 6-ból.

Bár ez közvetlenül nem járul hozzá egy helyes megoldáshoz, de ha egy megoldó (hiánytalanul) megmutatja, hogy a skalárral szorzás nem vezet ki V-ből, akkor ezért 4 pontot kaphat; ha pedig a megoldásban nyoma van annak, hogy az összeadásra való zártságot is elkezdi vizsgálni (és nem csak felírja), akkor ezért további 1 pont adható.

5. Az $\underline{a}, \underline{b}, \underline{c}, \underline{d} \in \mathbb{R}^3$ vektorokról annyit tudunk, hogy $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \langle \underline{a}, \underline{b}, \underline{d} \rangle$. Mutassunk példát arra, hogy ekkor a $\underline{b}, \underline{c}, \underline{d}$ vektorok lehetnek lineárisan függetlenek és arra is, hogy lehetnek lineárisan összefüggők is (a példák helyességét természetesen indokolni kell).

* * * * *

Legyen például $\underline{a} = (1, 0, 0), \underline{b} = (0, 1, 0), \underline{c} = (0, 0, 1)$ és legyen először $\underline{d} = (1, 1, 1)$. (0 pont)
Ekkor $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \mathbb{R}^3$, hiszen $\underline{a}, \underline{b}, \underline{c}$ az $\mathbb{R}^3$-beli standard bázis. (1 pont)
$\langle \underline{a}, \underline{b}, \underline{d} \rangle = \mathbb{R}^3$ pedig (például) azért teljesül, mert a három vektor nem esik egy síkba, hiszen $\underline{a}$ és $\underline{b}$ nem párhuzamosak és $\underline{d}$ nincs benne az általuk meghatározott síkban (mivel a harmadik koordinátája nem 0, szemben $\underline{a}$-val és $\underline{b}$-vel). Az előadáson szerepelt, hogy három nem egy síkba eső vektor lineáris kombinációjaként bármely térvektor előállítható, így $\langle \underline{a}, \underline{b}, \underline{d} \rangle = \mathbb{R}^3$, vagyis

$\langle \underline{a}, \underline{b}, \underline{c} \rangle = \langle \underline{a}, \underline{b}, \underline{d} \rangle$ csakugyan teljesül. (2 pont)
A $\underline{b}, \underline{c}, \underline{d}$ vektorok ekkor lineárisan függetlenek, mert $\beta\underline{b} + \gamma\underline{c} + \delta\underline{d} = \underline{0}$ esetén az első koordináta miatt $\delta = 0$, innen pedig a második, illetve a harmadik koordinátát figyelve $\beta = 0$ és $\gamma = 0$ is adódik. (3 pont)
Legyen most továbbra is $\underline{a} = (1,0,0), \underline{b} = (0,1,0), \underline{c} = (0,0,1)$, de $\underline{d} = (0,1,1)$. (0 pont)
Ekkor persze továbbra is teljesül, hogy $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \mathbb{R}^3$, (0 pont)
$\langle \underline{a}, \underline{b}, \underline{d} \rangle = \mathbb{R}^3$ pedig ismét azért teljesül, mert a három vektor nem esik egy síkba, hiszen $\underline{a}$ és $\underline{b}$ nem párhuzamosak és $\underline{d}$ nincs benne az általuk meghatározott síkban (mivel a harmadik koordinátája nem 0, szemben $\underline{a}$-val és $\underline{b}$-vel). A korábban látottak szerint ebből valóban következik, hogy $\langle \underline{a}, \underline{b}, \underline{d} \rangle = \mathbb{R}^3$, vagyis $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \langle \underline{a}, \underline{b}, \underline{d} \rangle$ teljesül. (2 pont)
A $\underline{b}, \underline{c}, \underline{d}$ vektorok ekkor lineárisan összefüggők, mert $\underline{d} = \underline{b} + \underline{c}$. (2 pont)

Mivel a feladat szövege nem kötötte ki, hogy a vektoroknak különbözőknek kell lenniük, választhatjuk úgy $\underline{d}$-t, hogy azonos legyen $\underline{c}$-vel. Ekkor bármely $\underline{a}, \underline{b}, \underline{c} \in \mathbb{R}^3$ esetén teljesül, hogy $\langle \underline{a}, \underline{b}, \underline{c} \rangle = \langle \underline{a}, \underline{b}, \underline{d} \rangle$ és az is, hogy a $\underline{b}, \underline{c}, \underline{d}$ vektorok összefüggők. Aki erre rámutat, természetesen kapja meg az erre a részre vonatkozó maximális pontszámot.

6*. Határozzuk meg a

$$\max_{n \in \mathbb{Z}^+} \text{lnko}(21n + 6, 6n + 4)$$

értéket, ahol $\text{lnko}(a, b)$ az a és b számok legnagyobb közös osztóját, $\mathbb{Z}^+$ pedig a pozitív egészek halmazát jelöli. (Vagyis határozzuk meg a $21n + 6$ és $6n + 4$ számok legnagyobb közös osztójának lehetséges legnagyobb értékét, ahol n végigfut a pozitív egész számokon.)

* * * * *

Első megoldás. Használjuk az Euklideszi algoritmust. (0 pont)
Az első maradékos osztás $n \geq 2$ esetén

$$21n + 6 = 3(6n + 4) + 3n - 6,$$

mert $0 \leq 3n - 6 < 6n + 4$. (2 pont)
Ha $3n - 6 = 0$, vagyis $n = 2$, akkor ezzel az algoritmus véget is ér, az lnko $6n + 4 = 16$. (1 pont)
Az előző megállapítás hiányáért ne vonjunk le pontot, de aki leírja (és nem kapna maximum pontot), annak adjuk meg.
A második maradékos osztás $n \geq 8$ esetén

$$6n + 4 = 2(3n - 6) + 16,$$

mert ekkor $0 \leq 16 < 3n - 6$. (2 pont)
Ha tehát $n \geq 8$, akkor az algoritmusról tanultak szerint 16-nál semmikép sem lehet nagyobb az lnko, (3 pont)
a 16-os érték viszont elérhető (mint azt már láttuk, $n = 2$-re, de az is elég, ha $16 | 3n - 6$, tehát pl. $n = 18$ esetén). (2 pont)
Ha $n \leq 7$, akkor $n = 1$ esetén az lnko 1, $n = 2$ esetén 16, $3 \leq n \leq 7$ esetén pedig az első maradékos osztásnál keletkező maradék $3n - 6 \leq 15$, így a keresett maximum a korábban kapott 16. (1 pont)

Aki csak azt nem vizsgálja meg, hogy $3n - 6$ nemnegatív-e, attól ne vonjunk le pontot, aki viszont azt nem nézi meg, hogy $16 < 3n - 6$ teljesül-e, attól az utolsón kívül a második részpontszámból is vonjunk le 1-et.

Második megoldás. Az előadásról tudjuk, hogy ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$. (1 pont)
A $21n + 6 \equiv 3n - 6 \pmod{6n + 4}$ kongruencia miatt így $(21n + 6, 6n + 4) = (6n + 4, 3n - 6)$, (2 pont)
a $6n + 4 \equiv 16 \pmod{3n - 6}$ kongruencia miatt pedig $(6n + 4, 3n - 6) = (3n - 6, 16)$. (2 pont)
A keresett maximum tehát nem lehet több 16-nál, (3 pont)

a 16-os érték viszont elérhető, pl. $n = 2$ esetén, vagyis a maximum 16. (2 pont)

Aki csak annyit állapít meg, hogy a 16 elérhető, 2 pontot kapjon.

Harmadik megoldás. Legyen $d = \text{lnko}(21n + 6, 6n + 4)$. (0 pont)
Ekkor $d|42n + 12 = 2 \cdot (21n + 6)$ és $d|42n + 28 = 7 \cdot (6n + 4)$, így $d|(42n + 28) - (42n + 12) = 16$. (6 pont)
Így $d \leq 16$, (2 pont)
és mivel $n = 2$ esetén $d = 16$, a keresett maximum 16. (2 pont)