Bevezetés a számításelméletbe I.
Pótzh, első zárthelyi pótlása — pontozási útmutató
2021. december 13.

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 éro 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 ad $3^{147} + 70^{147}$ 73-mal osztva?

* * * * *

Első megoldás. $70 \equiv -3 \pmod{73}$, (2 pont)
ezért $70^{147} \equiv (-3)^{147} \pmod{73}$, (4 pont)
vagyis $70^{147} \equiv -3^{147} \pmod{73}$, (2 pont)
tehát $3^{147} + 70^{147}$ 0 maradékot ad 73-mal osztva. (2 pont)

Második megoldás. Ismert, hogy $a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} - ba^{2k-1} + b^2a^{2k-2} - \ldots + b^{2k})$. (2 pont)
Ez alapján mivel 147 páratlan, (1 pont)
$3^{147} + 70^{147} = (3+70)(\ldots)$, ahol a második zárójelben lévő kifejezés egész, (6 pont)
tehát $3^{147} + 70^{147}$ 73-mal osztva 0 maradékot ad. (1 pont)

Ha valaki a hatványokra vonatkozó egyenlőség helyett csak annyit ír, hogy $(a^{2k+1} + b^{2k+1})$-ből kiemelhető $a+b$, azt is fogadjuk el.

Harmadik megoldás. 3 és 70 is relatív prím 73-hoz, ezért használhatjuk az Euler-Fermat tételt. (2 pont)
73 prím, így $\varphi(73) = 72$. (1 pont)
A tétel szerint $3^{72} \equiv 1 \pmod{73}$ és $70^{72} \equiv 1 \pmod{73}$. (1 pont)
Így $3^{147} \equiv 3^{2\cdot 72+3} \equiv 3^{2\cdot 72} \cdot 3^3 \equiv 3^3 = 27 \pmod{73}$ (1+1 pont)
és $70^{147} \equiv 70^{2\cdot 72+3} \equiv 70^{2\cdot 72} \cdot 70^3 \equiv 70^3 = 343000 \equiv 46 \pmod{73}$. (1+1+1 pont)
Így a keresett maradék $27 + 46 = 73$ miatt 0. (1 pont)

2. Hány olyan egész szám van 1 és 2021 között, melyre teljesül, hogy 63-mal osztva 18, 91-gyel osztva pedig 34 maradékot ad?

* * * * *

Első megoldás. Ha x ilyen szám, akkor $x \equiv 18 \pmod{63}$ és $x \equiv 34 \pmod{91}$. (1 pont)
Az első kongruencia alapján $x = 63k + 18$ valamely k egészre. (2 pont)
Ezt a második kongruenciába beírva $63k + 18 \equiv 34 \pmod{91}$, vagyis $63k \equiv 16 \pmod{91}$. (2 pont)
A tanultak szerint ez a kongruencia akkor és csak akkor megoldható, ha $(63, 91)|16$ (ahol (a, b) a és b legnagyobb közös osztóját jelöli). (2 pont)
Mivel 63 és 91 is osztható 7-tel, 16 viszont nem, ez nem teljesül, (2 pont)
így 1 és 2021 között (vagy bárhol másutt) ilyen szám nem létezik. (1 pont)

Második megoldás. A keresett számokra teljesül, hogy 7-tel osztva 4 maradékot adnak, (3 pont)
mivel 63 osztható 7-tel és $18 \equiv 4 \pmod{7}$. (1 pont)
Teljesül ugyanakkor az is, hogy 7-tel osztva 6 maradékot adnak, (3 pont)
mivel 91 is osztható 7-tel és $34 \equiv 6 \pmod{7}$. (1 pont)
Nem létezik olyan szám, melynek két különböző maradéka lenne 7-tel osztva, így egyetlen ilyen szám sincs 1 és 2021 között. (2 pont)
Az ennél a megoldásnál adható részpontoknál különösen ügyeljünk arra az általános szabályra, mely szerint „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."

3. Az e egyenes egyenletrendszere $x = y = \frac{z-3}{2}$, az f egyenes egyenletrendszere $\frac{x-3}{2} = y = z$. Döntsük el, hogy e és f egy síkba esnek-e (vagyis létezik-e olyan sík, amely mindkét egyenest tartalmazza).

* * * * *

Első megoldás. Két egyenes akkor és csak akkor esik egy síkba, ha párhuzamosak vagy metszők. (1 pont)
A két egyenes akkor és csak akkor metsző, ha a két egyenletrendszernek van közös (x, y, z) megoldása. (1 pont)
Az első egyenletrendszer alapján $x = y$, a második alapján $y = z$, (2 pont)
ahonnan $z = (z - 3)/2$, vagyis $x = y = z = -3$ következik. (2 pont)
Ez csakugyan megoldása az egyenletrendszereknek, (2 pont)
így a két egyenes metsző és így egy síkba esik. (2 pont)

Ha valaki nem jut helyes megoldásra, de vizsgálja a két egyenes párhuzamosságának kérdését, az az alábbi pontokat kaphatja még meg (azzal a megkötéssel, hogy a maximális 10 pont alatt kell maradnia a feladat pontszámának):

Az egyenletrendszerekből leolvasható, hogy e irányvektora $(1, 1, 2)$, f irányvektora $(2, 1, 1)$, (1 pont)
a két egyenes tehát nem párhuzamos, mivel az irányvektorok egyike sem számszorosa a másiknak. (1 pont)

Második megoldás. 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 e irányvektora $(1, 1, 2)$, f irányvektora $(2, 1, 1)$. (1 pont)
Legyen a kérdéses normálvektor (a, b, c), ekkor a két merőlegességi feltételből (a skaláris szorzat használatával) $a + b + 2c = 0$ és $2a + b + c = 0$. (1 pont)
A második egyenletből az első kivonva $a = c$ adódik, innen pedig $b = -3a$, a normálvektor(ok egyike) tehát $(1, -3, 1)$. (2 pont)

Az $(1,-3,1)$ normálvektorú síkok tehát mindkét egyenessel párhuzamosak, azt kell vizsgálnunk, hogy van-e köztük olyan, ami mindkét egyenest tartalmazza is. (1 pont)
Vegyünk ehhez egy tetszőleges pontot e-ről, legyen ez mondjuk a $(0,0,3)$. (1 pont)
Mivel S tartalmazza ezt a pontot, az egyenlete $x-3y+z=3$. (1 pont)
Vegyünk egy tetszőleges pontot f-ről is, legyen ez a $(3,0,0)$. Az S egyenletébe való behelyettesítéssel meggyőződhetünk róla, hogy ez a pont rajta van S-en, (1 pont)
így S tartalmazza e-t és f-et is, hiszen párhuzamos velük és van mindkettővel közös pontja. (1 pont)

A két irányvektorra merőleges vektort most már a vektoriális szorzatra vonatkozó képlet alkalmazásával is ki lehet számítani, hiszen az már szerepelt az előadáson.

4. Döntsük el, hogy alteret alkotnak-e $\mathbb{R}^4$-ben azok a vektorok, melyeknek van két azonos koordinátája.

* * * * *

Jelöljük a kérdéses vektorok halmazát V-vel. Ha V altér, akkor bármely két V-beli vektor összege is V-beli kell legyen. (2 pont)
Az $(1,2,0,0)^T$ és $(0,0,3,4)^T$ vektorok V-ben vannak, az összegük, az $(1,2,3,4)^T$ vektor azonban nincs, (6 pont)
így V nem altér. (2 pont)

Aki nem jut helyes eredményre, de megmutatja, hogy minden V-beli vektor minden skalárszorosa is V-ben van, az kapjon ezért 2 pontot.

5. Tudjuk, hogy az $\underline{a},\underline{b},\underline{c},\underline{d}$ vektorrendszer lineárisan független $\mathbb{R}^4$-ben. Következik-e ebből, hogy az $\underline{a},\underline{b},\underline{c},\underline{a}+\underline{b}+\underline{c}+\underline{d}$ rendszer bázis $\mathbb{R}^4$-ben?

* * * * *

Megmutatjuk először, hogy a kérdéses rendszer független. Tekintsük ehhez a vektorok egy olyan lineáris kombinációját, mely a nullvektort adja: $\alpha\underline{a}+\beta\underline{b}+\gamma\underline{c}+\delta(\underline{a}+\underline{b}+\underline{c}+\underline{d})=\underline{0}$. (1 pont)
A zárójelet felbontva és rendezve $(\alpha+\delta)\underline{a}+(\beta+\delta)\underline{b}+(\gamma+\delta)\underline{c}+\delta\underline{d}=\underline{0}$ adódik. (1 pont)
Mivel az $\underline{a},\underline{b},\underline{c},\underline{d}$ rendszer lineárisan független, ez csak úgy lehetséges, ha $\alpha+\delta=0,\ \beta+\delta=0,\ \gamma+\delta=0,\ \delta=0$, (2 pont)
ahonnan $\alpha=\beta=\gamma=\delta=0$, vagyis a kérdéses vektoroknak csak a triviális lineáris kombinációja lehet a nullvektor, így valóban függetlenek. (2 pont)
A vonatkozó tanult tétel szerint k dimenziós altérben k független vektor bázist alkot, tehát $\mathbb{R}^4$-ben a kérdéses vektorrendszer bázis, hiszen 4 elemű és független, (3 pont)
$\mathbb{R}^4$ pedig a tanultak szerint 4 dimenziós. (1 pont)

6*. Igaz-e, hogy ha az a és b egész számokra $a^{40}\not\equiv b^{40} \pmod{100}$, akkor $a^{40}b^{40}\not\equiv 1 \pmod{100}$?

* * * * *

Az állítás igaz. Ha a és b is relatív prím lenne 100-hoz, akkor az Euler-Fermat tétel szerint a $\varphi(100)$. hatványuk 1-gyel lenne kongruens modulo 100. (2 pont)
Mivel a tanult képlet szerint $\varphi(100)=(2^2-2^1)(5^2-5^1)=40$, (1 pont)
ez ellentmondana a feladat feltételének. (2 pont)
Így a és b közül legalább az egyik nem relatív prím 100-hoz, így a szorzatuk sem lesz az, (2 pont)
vagyis annak 40. hatványának is lesz 1-nél nagyobb közös osztója 100-zal. (1 pont)
Ebből következik, hogy a szorzat 40. hatványa nem lehet 1-gyel kongruens modulo 100, hiszen az előadáson tanultuk, hogy modulo m kongruens számok m-mel vett legnagyobb közös osztója azonos. (2 pont)