Bevezetés a számításelméletbe II.
Pótzárthelyi feladatok — pontozási útmutató
2020. december 14.

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.

1. Mennyi maradékot ad 2020^{2021} 1011-gyel osztva?

* * * * *

1011 és 2020 legnagyobb közös osztója osztja 2022-t és így $2022 - 2020 = 2$-t is és 1011 páratlan, (1 pont)
ezért 1011 és 2020 relatív prímek, így használhatjuk az Euler-Fermat tételt: (1 pont)
$2020^{\varphi(1011)} \equiv 1 \pmod{1011}$. (1 pont)
Mivel 1011 prímtényezős felbontása $3 \cdot 337$, a tanult képlet szerint $\varphi(1011) = 2 \cdot 336 = 672$. (1 pont)
Ezek alapján $2020^{2021} = 2020^{3 \cdot 672 + 5} \equiv 2020^5 \pmod{1011}$. (3 pont)
$2020^5 \equiv (-2)^5 = -32 \pmod{1011}$, (2 pont)
a keresett maradék tehát $1011 - 32 = 979$. (1 pont)

2. Egy szám 17-szerese 23 maradékot ad 65-tel osztva. Mennyi maradékot adhat a szám 130-cal osztva?

* * * * *

Először azt döntjük el, hogy milyen maradékot adhat a szám 65-tel osztva. Ehhez a $17x \equiv 23 \pmod{65}$ lineáris kongruenciát kell megoldanunk. (1 pont)
17 és 65 legnagyobb közös osztója 1, így használhatjuk az Euklideszi algoritmust a megoldáshoz. (1 pont)
Az algoritmus végrehajtása során kapott kongruenciák rendre a következők: $65x \equiv 0 \pmod{65}$, $17x \equiv 23 \pmod{65}$, $14x \equiv -69 \equiv -4 \pmod{65}$, $3x \equiv 27 \pmod{65}$, $2x \equiv -112 \equiv 18 \pmod{65}$, $x \equiv 9 \pmod{65}$. (5 pont)
Pontosan azok az x számok jók tehát, melyek 9 maradékot adnak 65-tel osztva, (1 pont)
a kérdéses 130-as osztási maradék tehát 9 vagy 74 lehet. (2 pont)

Számolási hibákért 1 pontot vonjunk le darabonként, de a hiba utáni pontok csak akkor járnak a megoldónak maradéktalanul, ha a megoldás nem lett könnyebb vagy rövidebb. Elírás esetén is hasonlóan

járjunk el (hiszen a végeredményt könnyű visszahelyettesíteni és meggyőződni a helyességéről). Nem hiba, ha valaki a kongruenciák jobb oldalain nem 0 és 64 közti (abszolút értékű) számokat szerepeltet, de a végeredménynek természetesen két 0 és 129 közti számnak kell lennie. Ha valaki más módon oldja meg a lineáris kongruenciát, akkor meg kell indokolnia, hogy a kapott számok miért jók és miért nincs másik megoldás. Ez tipikusan úgy történhet, hogy az átalakításokról belátja, hogy ekivalens átalakítások. Ennek hiányáért darabonként 2 pontot vonjunk le.
Ha valaki Euklideszi algoritmust szeretne használni, de nem követi pontosan annak lépéseit, akkor az átalakításai ugyanúgy magyarázatra szorulnak, mint az előzőként tárgyalt esetben. Pl. ha valaki az utolsó kongruenciát az utolsó előttiből 2-vel osztás útján nyeri, de nem tér ki rá, hogy ez ekvivalens átalakítás, akkor 2 pontot vonjunk le tőle ezért.
Ha valaki csak annyit állapít meg (helyesen), hogy a (mod 65) lineáris kongruenciának van megoldása/egy megoldása van, akkor a vonatkozó 7 pontból 1-et kapjon.

3. Határozzuk meg az $x + 3y + 2z = 7$ és a $4x + 6y + 5z = 10$ egyenletű síkok metszetegyenesének paraméteres egyenletrendszerét.

* * * * *

Az egyenletekből kiolvasható a két sík egy-egy normálvektora: $\underline{n_1} = (1, 3, 2)$, illetve $\underline{n_2} = (4, 6, 5)$. (1 pont)
A keresett egyenes irányvektora (jelöljük (a, b, c)-vel) merőleges $\underline{n_1}$-re és $\underline{n_2}$-re is, (1 pont)
így a skaláris szorzata mindkettővel 0. Ez alapján olyan a, b, c számokat keresünk, melyekre $a+3b+2c = 0$ és $4a + 6b + 5c = 0$. (1 pont)
A második egyenletből az első kétszeresét levonva a $2a + c = 0$ egyenlet adódik, melynek megoldása például $a = 1$, $c = -2$. (1 pont)
Ezeket az értékeket az első és a második egyenletbe helyettesítve is $b = 1$ adódik, az $a = 1$, $b = 1$, $c = -2$ értékek mellett tehát mindkét kívánt egyenlőség teljesül. Az egyenes irányvektorának így alkalmas az $(1, 1, -2)$ vektor. (1 pont)
Az irányvektort természetesen vektoriális szorzás segítségével is meg lehet határozni.
A paraméteres egyenletrendszer megadásához szükségünk van még az egyenes egy pontjára, keresünk tehát egy olyan pontot, mely mindkét síkon rajta van. (1 pont)
Az (x, y, z) pont akkor és csak akkor van rajta mindkét síkon, ha az x, y, z értékekre mindkét sík egyenlete teljesül. Válasszuk (mondjuk) a z koordináta értékét (mondjuk) 0-nak. Ekkor az $x + 3y = 7$ és a $4x + 6y = 10$ egyenleteket kapjuk. (1 pont)
A másodikból az első kétszeresét kivonva $2x = -4$ adódik, ahonnan $x = -2$ és innen $y = 3$, a $(-2, 3, 0)$ pont tehát rajta van a metszetegyenesen. (1 pont)
A fentiek alapján $x = t-2, y = t+3, z = -2t$ a metszetegyenes (egyik) paraméteres egyenletrendszere. (2 pont)

4. Alteret alkotnak-e $\mathbb{R}^4$-ben azok a vektorok, melyek koordinátái (felülről lefelé) számtani sorozatot alkotnak?

* * * * *

Egy (nem üres) vektorhalmaz pontosan akkor alkot alteret, ha zárt az összeadásra és a skalárral szorzásra, (0 pont)
vagyis bármely két, a feltételt kielégítő vektor összege is kielégíti a feltételt és bármely, a feltételt kielégítő vektor minden valós számszorosa is kielégíti a feltételt. (2 pont)
Legyenek ezért $\underline{u}$ és $\underline{v}$ a feltételnek megfelelő, tetszőleges vektorok, λ pedig tetszőleges valós szám. Ekkor $\underline{u}$ felírható $(a, a+d, a+2d, a+3d)^T$, $\underline{v}$ pedig $(b, b+e, b+2e, b+3e)^T$ alakban (ahol a, illetve b a vonatkozó számtani sorozatok első elemei, d, illetve e pedig a számtani sorozatok differenciái. (1 pont)
$\underline{u} + \underline{v} = (a + b, a + b + d + e, a + b + 2d + 2e, a + b + 3d + 3e)^T$, (1 pont)
ahonnan látható, hogy $\underline{u} + \underline{v}$ koordinátái is számtani sorozatot alkotnak, melynek első eleme $a + b$, differenciája pedig $d + e$. (2 pont)
$\lambda\underline{u} = (\lambda a, \lambda(a + d), \lambda(a + 2d), \lambda(a + 3d))^T = (\lambda a, \lambda a + \lambda d, \lambda a + 2\lambda d, \lambda a + 3\lambda d)^T$, (1 pont)
ahonnan látható, hogy $\lambda\underline{u}$ koordinátái is számtani sorozatot alkotnak, melynek első eleme λa,

differenciája pedig λd. (2 pont)
A fentiek szerint a kérdéses halmaz az összeadásra és a skalárral szorzásra is zárt (és nem üres – ennek hiányáért ne vonjunk le pontot), vagyis altér. (1 pont)

5. Tudjuk, hogy az $\underline{a}, \underline{b}, \underline{c}$ vektorrendszer lineárisan független $\mathbb{R}^n$-ben. Következik-e ebből, hogy a $2\underline{a}, \underline{a}+\underline{b}, \underline{a}+\underline{c}$ rendszer is lineárisan független?

* * * * *

Írjuk fel az $2\underline{a},\ \underline{a}+\underline{b},\ \underline{a}+\underline{c}$ vektorok egy lineáris kombinációját az α, β, γ együtthatókkal és vizsgáljuk meg, hogy ez mikor lehet $\underline{0}$. (1 pont)
Az

$$\alpha(2\underline{a}) + \beta(\underline{a}+\underline{b}) + \gamma(\underline{a}+\underline{c}) = \underline{0}$$

egyenlőségben a zárójeleket felbontva, majd átrendezve

$$(2\alpha+\beta+\gamma)\underline{a} + \beta\underline{b} + \gamma\underline{c} = \underline{0}$$

adódik. (3 pont)
Mivel az $\underline{a}, \underline{b}, \underline{c}$ vektorok lineárisan függetlenek, ez csak akkor lehetséges, ha $2\alpha+\beta+\gamma = 0$, $\beta = 0$, $\gamma = 0$. (3 pont)
Ebből azonnal adódik, hogy $\alpha = 0$ is teljesül, (1 pont)
így a $2\underline{a},\ \underline{a}+\underline{b},\ \underline{a}+\underline{c}$ vektorok egy lineáris kombinációja csak akkor lehet a nullvektor, ha mindhárom együttható 0, így az előadáson tanult tétel szerint a vektorok függetlenek. (2 pont)

6*. Határozzuk meg az összes olyan 1 és 100 közti a egész számot, melyre

$$a^{21} \equiv 1 \pmod{100}.$$

* * * * *

Az előadáson tanultak szerint az egymással modulo m kongruens számok m-mel vett legnagyobb közös osztói azonosak. Így a^{21} és 1 100-zal vett legnagyobb közös osztói is azonosak, vagyis a^{21} és 100 relatív prímek. Ebből azonnal következik, hogy a és 100 is relatív prímek, (2 pont)
vagyis használhatjuk az Euler-Fermat tételt: $a^{\varphi(100)} \equiv 1 \pmod{100}$. $100 = 2^2 \cdot 5^2$, tehát a tanult képlet szerint $\varphi(100) = (2^2-2)(5^2-5) = 40$, tehát $a^{40} \equiv 1 \pmod{100}$. (1 pont)
A feladat feltétele szerint $a^{21} \equiv 1 \pmod{100}$, így (mindkét oldalt négyzetre emelve)
$a^{42} \equiv 1 \pmod{100}$ adódik, (1 pont)
vagyis $a^{42} \equiv a^{40} \pmod{100}$. (1 pont)
Mivel a^{40} és 100 (is) relatív prímek, ez utóbbi kongruenciát a^{40}-nel osztva az $a^2 \equiv 1 \pmod{100}$ kongruenciát kapjuk. (1 pont)
Mindkét oldalt a tizedikre emelve $a^{20} \equiv 1 \pmod{100}$. (1 pont)
Ezek szerint $a^{20} \equiv a^{21} \pmod{100}$, (1 pont)
ahonnan a^{20}-nal osztva (és ismét felhasználva, hogy a és 100 relatív prímek) $a \equiv 1 \pmod{100}$. (1 pont)
Az 1 és 100 közti egészek közül tehát csak az 1 felel meg a feladat feltételének (és az persze tényleg meg is felel). (1 pont)