Bevezetés a számításelméletbe I.
Első pótzárthelyi — pontozási útmutató
2023. november 17.

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. A Nagy Piréz Rendszer harmadik bolygóján ősidők óta minden hónap 29 napos, az év végén visszamaradó 22 napot pedig a messzeföldön híres piréz kumisz mértéktelen fogyasztásával töltik a lakosok. A Piréz Nemzeti Bank mélyreható elemzése azonban nemrég kimutatta, hogy a gazdaság teljesítményére az év végi 22 napos szünet kedvezőtlen hatással van, ezért bevezetik a 32 napos hónapot, így a hónapokból kimaradó napok száma 5-re csökken. Hány napból áll az év a harmadik bolygón, ha tudjuk, hogy a negyedik bolygó éve (ami persze hosszabb a harmadikénál) 1000 napos?

* * * * *

Az év napjainak számát a harmadik bolygón n-nel jelölve a feladat szövegéből az $n \equiv 22 \pmod{29}$ és $n \equiv 5 \pmod{32}$ kongruenciákat kapjuk. (2 pont)
A kongruenciarendszert a tanult módszerrel oldjuk meg. Az első kongruenciából $n = 29k + 22$ valamilyen k egészre. Ezt a második kongruenciába helyettesítve: $29k + 22 \equiv 5 \pmod{32}$. Mindkét oldalból 22-t levonva a $29k \equiv -17 \pmod{32}$ lineáris kongruenciát kapjuk. (1 pont)
Mivel $(29, 32) = 1$ (pl. mert 29 prím és 32 nem a többszöröse) és $1|5$, ezért a tanult tételt szerint a lineáris kongruencia megoldható és egy megoldása van modulo 32. (1 pont)
A bal oldalból $32k$-t levonva és a jobb oldalhoz 32-t adva (az eredetivel ekvivalens) $-3k \equiv 15 \pmod{32}$ kongruencia adódik. (1 pont)
Ezt (-3)-mal osztva, majd a jobb oldalhoz 32-t adva (ez utóbbi igazából el is maradhat) $k \equiv 27 \pmod{32}$, ahol a modulus azért nem változott, mert 32 és -3 relatív prímek. (1 pont)
Mivel a kongruenciának más megoldása nem lehet, de tudjuk, hogy egy megoldásnak lennie kell modulo 32, a kapott 27 érték valóban a megoldás. (1 pont)
Így $k = 32m + 27$ valamilyen m egészre, ezt behelyettesítve $n = 29(32m + 27) + 22 = 928m + 805$. (2 pont)
Az ilyen n-ek közt egy olyan van, ami pozitív és 1000-nél kisebb, nevezetesen 805, ez a keresett szám. (1 pont)

Azt, hogy a kongruenciának valóban az egyetlen megoldása a 27 persze máshogy is be lehet látni, pl. úgy, hogy ellenőrizzük, hogy minden átalakításunk ekvivalens átalakítás volt, erre is jár az 1+1 pont.
A megoldás közben előállt lineáris kongruencia természetesen más módszerekkel, így akár az Euklideszi algoritmussal is megoldható; ezzel dolgozva sorra a $32k \equiv 0 \pmod{32}$, $29k \equiv -17 \pmod{32}$, $3k \equiv 17 \pmod{32}$, $2k \equiv -10 \pmod{32}$, $k \equiv 27 \pmod{32}$ kongruenciák keletkeznek. Ekkor a lineáris kongruencia megoldásáért járó 4 pontból 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 1 pontot ér annak az ellenőrzése, hogy az eljárás a tanultak szerint leosztás nélkül (vagyis az első fázis kihagyásával) alkalmazható, mert $(29, 32) = 1$; végül 2 pontot ér maga a számolás.

2. Mennyi maradékot ad 499^{4201} 539-cel osztva?

* * * * *

499 és 539 relatív prímek, mert $539 = 7^2 \cdot 11$, 499 pedig sem 7-tel, sem 11-gyel nem osztható (persze rengeteg más indoklás is adható). (1 pont)
Az Euler-Fermat tétel szerint $499^{\varphi(539)} \equiv 1 \pmod{539}$. (2 pont)
A tételt azért tudtuk használni, mert 499 és 539 relatív prímek, mint azt már korábban láttuk. (2 pont)
A tanultak szerint $\varphi(539) = (7^2 - 7)(11 - 1) = 420$. (2 pont)
Az eddigiek alapján tehát $499^{420} \equiv 1 \pmod{539}$, (1 pont)
ezt a tizedik hatványra emelve $499^{4200} \equiv 1 \pmod{539}$, (1 pont)
mindkét oldalt 499-cel szorozva pedig $499^{4201} \equiv 499 \pmod{539}$ adódik, (1 pont)
a keresett maradék tehát 499. (0 pont)

3. Legyen $\underline{i} = (3; 0; -1)$ irányvektora az e és az f egyenesnek is. Az e egyenes tartalmazza a $(3; 1; 2)$ pontot, f pedig az $(5; -1; 1)$ pontot. Adjuk meg annak a síknak az egyenletét, mely e-t és f-et is tartalmazza.

* * * * *

A keresett sík $\underline{n} = (a, b, c)$ normálvektora merőleges $\underline{i}$-re (1 pont)
és a két megadott pont egyikéből a másikba mutató vektorra is. (1 pont)
Ilyen vektor az $(5; -1; 1) - (3; 1; 2) = (2; -2; -1)$. (1 pont)
Így $\underline{n}$ skalárszorzata $\underline{i}$-vel és a $(2; -2; -1)$ vektorral is 0, (2 pont)
vagyis $3a - c = 0$ és $2a - 2b - c = 0$. (1 pont)
Ennek az egyenletrendszernek megoldása (pl.) $a = 2, b = -1, c = 6$. (2 pont)
A sík egyenlete a normálvektor és az egyik megadott pont alapján így $2x - y + 6z = 17$. (2 pont)

Teljes megoldáshoz meg kéne indokolni, hogy az így kapott sík valóban tartalmazza mindkét egyenest, ennek hiányáért azonban ne vonjunk le pontot. Aki helyes indoklást ad és ebben a feladatban pontot vesztene, az kapjon egy extra pontot. A normálvektort most már vektoriális szorzattal is ki lehet számolni, hiszen szerepelt az előadáson, természetesen erre is jár a vonatkozó 5 pont ha a felírás és a számolás helyes – elvi hibáért (pl. a sakktábla szabály használatának elmulasztása) 4, számolási hibáért 1 pontot vonjunk le.

4. A $V \subseteq \mathbb{R}^5$ halmaz azon vektorokból áll, melyeknek az első 4 koordinátája számtani sorozatot alkot, az utolsó koordináta pedig az első 4 koordináta összege. Így például a jobbra látható $\underline{v}$ vektor V-beli. Altér-e V $\mathbb{R}^5$-ben?

$$\underline{v} = \begin{pmatrix} 1 \\ 3 \\ 5 \\ 7 \\ 16 \end{pmatrix}$$

* * * * *

Legyenek $\underline{x}$ és $\underline{y}$ tetszőleges V-beli vektorok, λ pedig tetszőleges valós szám. (0 pont)
V leírása alapján $\underline{x} = (a, a + d, a + 2d, a + 3d, 4a + 6d)^T$ és $\underline{y} = (b, b + c, b + 2c, b + 3c, 4b + 6c)^T$ valamely a, b, c, d számokra. (1 pont)

Ekkor $\underline{x}+\underline{y}=(a+b, a+b+d+c, a+b+2d+2c, a+b+3d+3c, 4a+4b+6d+6c)^T$, (1 pont)
ami V-ben van, hiszen a számtani sorozat első elemét $(a+b)$-nek, a differenciáját pedig $(c+d)$-nek választva épp ezt a vektort kapjuk. (2 pont)
$\lambda\underline{x}=(\lambda a, \lambda(a+d), \lambda(a+2d), \lambda(a+3d), \lambda(4a+6d))^T$, (1 pont)
ami szintén V-ben van, hiszen a számtani sorozat első elemét λa-nak, a differenciáját pedig λd-nek választva épp ezt a vektort kapjuk. (2 pont)
Mivel V akkor és csak akkor alkot alteret, ha nem üres (ha ez kimarad, azért ne vonjunk le pontot, ha viszont valaki megemlíti és ebben a feladatban pontot veszítene, akkor adjunk egyet) és bármely két V-beli vektor összege is V-beli, továbbá bármely V-beli vektor bármely skalárszorosa is V-beli, a fentiek szerint V altér. (3 pont)

Az utolsó 3 pont természetesen csak akkor jár a megoldónak, ha úgy teszi a vonatkozó megállapítást, hogy korábban valóban foglalkozott V-beli vektorok összegének és skalárszorosának vizsgálatával.

5. Mely p valós számok esetén teljesül, hogy a jobbra látható vektorrendszert $\mathbb{R}^4$ bázisává lehet kiegészíteni?

$$\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\\p\end{pmatrix}, \begin{pmatrix}1\\1\\p\\p\end{pmatrix}$$

* * * * *

A tanultak szerint a lineárisan független vektorrendszerek kiegészíthetők bázissá. (2 pont)
Ha egy rendszer nem lineárisan független, akkor viszont nem egészíthető ki bázissá, mert bármely vektort hozzávéve továbbra sem lesz független, a bázisoknak viszont függetleneknek kell lenniük. (E megjegyzés hiányáért ne vonjunk le pontot, aki viszont leírja és ebben a feladatban pontot vesztene, annak adjunk egy extra pontot.) (0 pont)

A függetlenség vizsgálatához tekintsük az $\alpha\begin{pmatrix}1\\1\\1\\1\end{pmatrix}+\beta\begin{pmatrix}1\\1\\1\\p\end{pmatrix}+\gamma\begin{pmatrix}1\\1\\p\\p\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\end{pmatrix}$ egyenlőséget. (1 pont)

Innen az

$$\begin{aligned}\alpha+\beta+\gamma &= 0\\ \alpha+\beta+\gamma &= 0\\ \alpha+\beta+\gamma p &= 0\\ \alpha+\beta p+\gamma p &= 0\end{aligned}$$

egyenletrendszert kapjuk. (1 pont)
Az első egyenletet a harmadikból levonva $(p-1)\gamma=0$, így ha $p\neq 1$, akkor $\gamma=0$. (1 pont)
A harmadik egyenletet a negyedikből levonva $(p-1)\beta=0$, így ha $p\neq 1$, akkor $\beta=0$. (1 pont)
Mindezek alapján ha $p\neq 1$, akkor β és γ mellett az első egyenlet miatt α is 0 kell legyen, (1 pont)
vagyis a kérdéses vektoroknak ekkor csak a triviális lineáris kombinációja adja a nullvektort, tehát ekkor a vektorok lineárisan függetlenek. (2 pont)
Ha azonban $p=1$, akkor a vektorrendszer nem lineárisan független, hiszen (pl.) az $\alpha=1, \beta=-1, \gamma=0$ skalárokkal vett lineáris kombináció is a nullvektort adja (de persze hivatkozhatunk arra is, hogy ugyanaz a vektor egynél többször szerepel a rendszerben). (1 pont)
A rendszer tehát pontosan $p\neq 1$ esetén egészíthető ki bázissá. (0 pont)

6*. Adjuk meg az összes olyan x egész számot, melyre $x^6\equiv 2 \pmod{201}$.

* * * * *

Legyen x olyan szám, melyre a fenti kongruencia teljesül. Mivel 2 és 201 relatív prímek, a tanultak szerint x^6 és 201 is relatív prímek kell legyenek, (1 pont)
amiből következik, hogy x és 201 is relatív prímek. (1 pont)
Az Euler-Fermat tétel szerint így $x^{\varphi(201)}\equiv 1 \pmod{201}$. (2 pont)

Mivel $\varphi(201) = (3-1)(67-1) = 132$, $x^{132} \equiv 1 \pmod{201}$. (1 pont)
Az $x^6 \equiv 2 \pmod{201}$ kongruenciát a 22. hatványra emelve $x^{6\cdot 22} = x^{132} \equiv 2^{22} \pmod{201}$.
(2 pont)
$2^{22} \equiv 37 \pmod{201}$ (ez kideríthető ismételt négyzetre emelések segítségével (az adódó maradékok sorban 2,4,16,55,10) vagy pl. az alapján, hogy $2^{11} = 2048$ 38 maradékot ad 201-gyel osztva, $38^2 = 1444$ pedig 37 maradékot ad 201-gyel osztva). (2 pont)
Ezek alapján tehát $x^{132} \equiv 37 \pmod{201}$, ami ellentmond a korábban látottaknak, így a fenti tulajdonságú x szám nem létezik. (1 pont)

Az Euler-Fermat tétel felírásáért természetesen csak akkor jár pont, ha az valóban haszonnal jár a feladat megoldása szempontjából, tehát pl. x-et és nem x^6-t vagy 2-t emeljük a 132. hatványra. Hasonlóképpen nem ér pontot $\varphi(201)$ meghatározása, ha ez a feladat megoldását nem viszi előre.