Bevezetés a számításelméletbe I.
Pótzárthelyi feladatok — pontozási útmutató
2024. november 15.

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. Hány olyan szám van 1 és 10000 között, mely osztható 7-tel és 8-cal is, a 22-vel vett osztási maradéka pedig 10?

* * * * *

Mivel $(7, 8) = 1$, ezért egy szám akkor és csak akkor osztható 7-tel és 8-cal is, ha osztható 56-tal. (1 pont)
Vagyis a feladat feltételeiből $n \equiv 0 \pmod{56}$ és $n \equiv 10 \pmod{22}$ adódik. (1 pont)
A kapott kongruenciarendszert a tanult módszerrel oldjuk meg. Az első kongruenciából $n = 56k$ következik valamilyen k egészre. Ezt a másodikba helyettesítve: $56k \equiv 10 \pmod{22}$, vagyis $12k \equiv 10 \pmod{22}$. (2 pont)
Mivel $(12, 22) = 2 \mid 10$, ezért a kongruencia a tanult tétel szerint megoldható (és két megoldása lesz modulo 10). (1 pont)
Mindkét oldalt 2-vel osztva: $6k \equiv 5 \pmod{11}$, ahol a modulust le kellett osztani $(22, 2) = 2$-vel. Mindkét oldalt 2-vel szorozva: $12k \equiv 10 \pmod{11}$, vagyis $k \equiv 10 \pmod{11}$. A 2-vel való szorzás $(2, 11) = 1$ miatt ekvivalens lépés volt (vagyis a megoldáshalmaz nem változott). Tehát $k = 11\ell + 10$ valamilyen ℓ egészre. (3 pont)
Ezt visszahelyettesítve: $n = 56(11\ell + 10) = 616\ell + 560$. (1 pont)
Mivel ez a szám pontosan akkor esik 0 és 10000 közé, ha $\ell \in \{0, 1, \ldots, 15\}$, ezért 16 darab olyan szám van, ami megfelel a feladat feltételeinek. (1 pont)

A lineáris kongruencia megoldásakor a lépések ekvivalenciája helyett hivatkozhatunk arra is, hogy két megoldást kaptunk modulo 22, nevezetesen a 10-et és a 21-et, és mivel a megoldások száma kettő modulo 22, ezért csak ezek lehetnek a megoldások; illetve természetesen ellenőrzéssel is meggyőződhetünk a kapott megoldások helyességéről. 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 első 1 pont az ilyen (egyébként teljes értékű) megoldásokra is jár.

A lineáris kongruenciát természetesen a tanult euklideszi algoritmussal is megoldhatjuk. Ezzel a 2-vel való leosztás után sorra a $11k \equiv 0 \pmod{11}$, $6k \equiv 5 \pmod{11}$, $5k \equiv -5 \pmod{11}$, $k \equiv 10 \pmod{11}$ kongruenciák keletkeznek. Ekkor a 3 pontot érő blokkból 1 pontot ér, hogy az eljárás az első fázisban 2-vel leoszt, és 2 pontot ér maga a számolás. Ha egy megoldó az euklideszi algoritmus elején nem oszt le, akkor az algoritmus végrehajtásáért legfeljebb 2 pontot kaphat.

2. Legyen $n = 1122334455667788$. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg $48n + 12$ és $33n + 8$ legnagyobb közös osztóját.

* * * * *

Az euklideszi algoritmust alkalmazzuk. (Ez a pontszám tehát annak jár, aki felismeri, hogy ezt az algoritmust kell alkalmazni – akkor is, ha ezt külön nem írja le.) (2 pont)
A $(48n + 12)$-t $(33n + 8)$-cal maradékosan osztva: $48n + 12 = 1 \cdot (33n + 8) + 15n + 4$.
A $(33n + 8)$-at $(15n + 4)$-gyel maradékosan osztva: $33n + 8 = 2 \cdot (15n + 4) + 3n$.
A $(15n + 4)$-et $3n$-nel maradékosan osztva: $15n + 4 = 5 \cdot 3n + 4$. (4 pont)
Mivel az n utolsó két számjegyéből képzett szám 88, ami osztható 4-gyel, ezért n is, valamint $3n$ is osztható 4-gyel. Így $3n$-et 4-gyel osztva a maradék 0. (2 pont)
Így a legnagyobb közös osztó (az utolsó nemnulla maradék, vagyis) 4. (2 pont)

3. A p valós paraméter minden lehetséges értékére döntsük el, hogy az alábbi egyenletrendszerű e és f egyenesek

a) párhuzamosak-e; b) merőlegesek-e.

$$e: \ \frac{2-x}{4} = \frac{y-7}{p} = \frac{z-6}{3} \qquad f: \ \frac{x+9}{2} = 2y = \frac{5-2z}{3}$$

* * * * *

a) Az e egyenletrendszerét átalakítva $\frac{x-2}{-4} = \frac{y-7}{p} = \frac{z-6}{3}$ adódik, amiből már kiolvasható e irányvektora: $\underline{v}_e = (-4; p; 3)$. (1 pont)
Hasonlóan az f egyenletrendszerét átalakítva $\frac{x+9}{2} = \frac{y}{1/2} = \frac{z-5/2}{-3/2}$ adódik, amiből kiolvasható f irányvektora: $\underline{v}_f = (2; 1/2; -3/2)$. (2 pont)
Két egyenes pontosan akkor párhuzamos, ha irányvektoraik párhuzamosak, vagyis ha $\underline{v}_e$ és $\underline{v}_f$ egymás (nemnulla) konstansszorosai, azaz ha létezik olyan $\lambda \in \mathbb{R}$ szám, hogy $\underline{v}_e = \lambda \cdot \underline{v}_f$. (1 pont)
Vagyis $-4 = 2\lambda$, $p = 1/2 \cdot \lambda$, $3 = -3/2 \cdot \lambda$, amiből $\lambda = -2$ adódik, és innen $p = -1$. (1 pont)
Tehát a két egyenes akkor és csak akkor párhuzamos, ha $p = -1$. (1 pont)

b) Két egyenes pontosan akkor merőleges, ha irányvektoraik merőlegesek, (1 pont)
vagyis ha $\underline{v}_e \cdot \underline{v}_f = 0$. (1 pont)
Tehát $0 = -4 \cdot 2 + p \cdot \frac{1}{2} + 3 \cdot \left(-\frac{3}{2}\right) = -\frac{25}{2} + \frac{p}{2}$, amiből $p = 25$. (1 pont)
Tehát a két egyenes akkor és csak akkor merőleges, ha $p = 25$. (1 pont)

Ha egy megoldó helytelenül írja fel az irányvektorokat, akkor az irányvektorok meghatározásáért járó 1+2 pont elvesztése után a további részpontszámokat még megkaphatja. Ha azonban a hiba következtében a megoldás könnyebbé válik, akkor csak a fentieknek lényegében megfeleltethető részekért adható pont.

4. Legyenek $\underline{u}$ és $\underline{v}$ az alábbi $\mathbb{R}^4$-beli vektorok. Határozzuk meg az $\langle \underline{u}, \underline{v} \rangle$ generált altér összes olyan elemét, aminek az első és a harmadik koordinátája azonos, a negyedik koordinátája pedig 5-tel nagyobb a másodiknál.

$$\underline{u} = \begin{pmatrix} 2 \\ 1 \\ 0 \\ -1 \end{pmatrix}, \quad \underline{v} = \begin{pmatrix} -1 \\ 0 \\ 1 \\ 3 \end{pmatrix}$$

* * * * *

Legyen $\underline{z}$ egy ilyen vektor. Ekkor $\underline{z} \in \langle \underline{u}, \underline{v} \rangle$ azt jelenti, hogy $\underline{z}$ kifejezhető $\underline{u}$-ból és $\underline{v}$-ből lineáris kombinációval, vagyis léteznek olyan α, β skalárok, hogy $\alpha \cdot \underline{u} + \beta \cdot \underline{v} = \underline{z}$. (3 pont)
Ekkor a műveleteket elvégezve a következőt kapjuk:

$$\underline{z} = \begin{pmatrix} 2\alpha - \beta \\ \alpha \\ \beta \\ -\alpha + 3\beta \end{pmatrix}.$$

(2 pont)
Vagyis a feladat feltételei szerint a következő egyenletrendszert kapjuk.

$$2\alpha - \beta = \beta$$
$$-\alpha + 3\beta = \alpha + 5$$

(2 pont)
Az első egyenletből $\alpha = \beta$ adódik. Ezt a másodikba behelyettesítve $\alpha = \beta = 5$. (1 pont)
Így az $\langle \underline{u}, \underline{v} \rangle$ generált altérnek az egyetlen, a feltételeknek megfelelő eleme a $\underline{z} = (5; 5; 5; 10)^\top$ vektor. (2 pont)

5. Legyenek $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ olyan $\mathbb{R}^n$-beli vektorok, melyekre az $\underline{a}, \underline{b}, \underline{c}$ rendszer lineárisan független, de az $\underline{a}, \underline{b}, \underline{d}$ lineárisan összefüggő. Döntsük el, hogy az alábbi három állítás közül melyik teljesül.

- Az $\underline{a}$, $\underline{b}$, $\underline{c} + \underline{d}$ rendszer biztosan lineárisan független.
- Az $\underline{a}$, $\underline{b}$, $\underline{c} + \underline{d}$ rendszer biztosan lineárisan összefüggő.
- Az $\underline{a}$, $\underline{b}$, $\underline{c} + \underline{d}$ rendszer lehet lineárisan független és lehet lineárisan összefüggő is az $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ vektorok választásától függően.

* * * * *

Megmutatjuk, hogy az $\underline{a}$, $\underline{b}$, $\underline{c} + \underline{d}$ rendszer biztosan lineárisan független.

1. megoldás.
Mivel az $\underline{a}, \underline{b}, \underline{c}$ rendszer lineárisan független, ezért az $\underline{a}, \underline{b}$ rendszer is az. (1 pont)
Mivel azonban az $\underline{a}, \underline{b}, \underline{d}$ rendszer már lineárisan összefüggő, ezért az újonnan érkező vektor lemmája szerint $\underline{d} \in \langle \underline{a}, \underline{b} \rangle$, azaz léteznek olyan α, β skalárok, hogy $\alpha \cdot \underline{a} + \beta \cdot \underline{b} = \underline{d}$. (2 pont)
Tegyük fel, hogy $\lambda_1 \cdot \underline{a} + \lambda_2 \cdot \underline{b} + \lambda_3 \cdot (\underline{c} + \underline{d}) = \underline{0}$ teljesül valamilyen $\lambda_1, \lambda_2, \lambda_3$ skalárokra. (1 pont)
Behelyettesítve ebbe a $\underline{d} = \alpha \cdot \underline{a} + \beta \cdot \underline{b}$ összefüggést, majd átrendezve az egyenletet

$$(\lambda_1 + \lambda_3 \cdot \alpha) \cdot \underline{a} + (\lambda_2 + \lambda_3 \cdot \beta) \cdot \underline{b} + \lambda_3 \cdot \underline{c} = \underline{0}$$

adódik. (2 pont)
Mivel az $\underline{a}, \underline{b}, \underline{c}$ vektorok lineárisan függetlenek, ezért ez csak úgy lehetséges, ha $(\lambda_1 + \lambda_3 \cdot \alpha) = 0$ és $\lambda_2 + \lambda_3 \cdot \beta = 0$ és $\lambda_3 = 0$. (2 pont)
Ebből azonnal adódik, hogy $\lambda_1 = 0$ és $\lambda_2 = 0$ is teljesül. (1 pont)
Így az $\underline{a}$, $\underline{b}$, $\underline{c} + \underline{d}$ vektorok egy lineáris kombinációja akkor és csak akkor lehet a nullvektor, ha mindhárom együttható 0, így az előadáson tanult tétel szerint a vektorok lineárisan függetlenek. (1 pont)

2. megoldás.
Indirekt tegyük fel, hogy az $\underline{a}$, $\underline{b}$, $\underline{c} + \underline{d}$ rendszer összefüggő.

Mivel az $\underline{a}, \underline{b}, \underline{c}$ rendszer lineárisan független, ezért az $\underline{a}, \underline{b}$ rendszer is az. (1 pont)
Mivel azonban az $\underline{a}$, $\underline{b}$, $\underline{c}+\underline{d}$ rendszer már lineárisan összefüggő, ezért az újonnan érkező vektor lemmája szerint $\underline{c}+\underline{d} \in \langle \underline{a}, \underline{b} \rangle$. (2 pont)
Hasonlóan, mivel az $\underline{a}, \underline{b}, \underline{d}$ rendszer is lineárisan összefüggő, ezért az újonnan érkező vektor lemmája szerint $\underline{d} \in \langle \underline{a}, \underline{b} \rangle$. (2 pont)
Mivel minden altér zárt az összeadásra és a skalárral való szorzásra, ezért ekkor $-\underline{d} \in \langle \underline{a}, \underline{b} \rangle$, és így $\underline{c} = (\underline{c}+\underline{d}) + (-1) \cdot \underline{d} \in \langle \underline{a}, \underline{b} \rangle$, (3 pont)
ami ellentmond annak, hogy az $\underline{a}, \underline{b}, \underline{c}$ vektorok lineárisan függetlenek. (2 pont)
Tehát az $\underline{a}$, $\underline{b}$, $\underline{c}+\underline{d}$ rendszer valóban lineárisan független.

6*. Legyenek a és b egymáshoz relatív prím, pozitív egész számok. Mennyi maradékot ad az $a^{\varphi(b)} + b^{\varphi(a)}$ szám ab-vel osztva?

* * * * *

Tekintsük az $a^{\varphi(b)} + b^{\varphi(a)}$ szám a-val, illetve b-vel vett osztási maradékát.
Nyilván $a^{\varphi(b)} \equiv 0 \pmod{a}$ és $b^{\varphi(a)} \equiv 0 \pmod{b}$. (1 pont)
Mivel $(a, b) = 1$, ezért az Euler–Fermat-tétel szerint $a^{\varphi(b)} \equiv 1 \pmod{b}$ és $b^{\varphi(a)} \equiv 1 \pmod{a}$. (1 pont)
Vagyis $a^{\varphi(b)} + b^{\varphi(a)} \equiv 0 + 1 \equiv 1 \pmod{a}$ és $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 + 0 \equiv 1 \pmod{b}$. (2 pont)
Így a kongruencia ekvivalens definíciója szerint $a^{\varphi(b)} + b^{\varphi(a)} - 1$ osztható a-val és b-vel is, (3 pont)
tehát $(a, b) = 1$ miatt $a^{\varphi(b)} + b^{\varphi(a)} - 1$ osztható ab-vel is. (2 pont)
Vagyis a $a^{\varphi(b)} + b^{\varphi(a)}$ szám 1 maradékot ad ab-vel osztva. (1 pont)