Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2018. október 18.

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 különböző megoldást is elkezd, akkor legfőljebb 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.

1. Mennyi maradékot ad 363-mal osztva 4^{444}?

* * * * *

363 prímtényezős felbontása: $363 = 3 \cdot 11^2$. (1 pont)
Ezért a tanult képlet szerint $\varphi(363) = (3-1)(11^2-11) = 220$. (2 pont)
Mivel $(4, 363) = 1$ (hiszen 363 páratlan), (1 pont)
ezért az Euler-Fermat tételből $4^{220} \equiv 1 \pmod{363}$ következik. (2 pont)
Mindkét oldalt négyzetre emelve: $4^{440} \equiv 1^2 = 1 \pmod{363}$. (2 pont)
Mindkét oldalt $4^4 = 256$-tal szorozva: $4^{444} \equiv 256 \pmod{363}$. (2 pont)
Így 4^{444} 256 maradékot ad 363-mal osztva.

A feladat elvileg megoldható az ismételt négyzetre emelések módszerével is, de az (különösen számológép nélkül) sokkal kellemetlenebb és hosszabb megoldásra vezet; ha egy hallgató ilyen megoldással próbálkozik (és az ahhoz szükséges számításokat legalább elkezdi), akkor 1 pontot kaphat pusztán annak felismeréséért, hogy ez az algoritmus elvileg alkalmas a kérdés megválaszolására. A további 9 pont a helyes számításokért járhat: a 4^{2^k} hatványok 363-as maradékai a $k = 0, \ldots, 8$ értékekre (ezek sorra: 4, 16, 256, 196, 301, 214, 58, 97, 334) darabonként fél-fél pontot érjenek, a 444 felírása 2-es számrendszerben ($444 = 2^2 + 2^3 + 2^4 + 2^5 + 2^7 + 2^8$) 1 pontot, majd a 4^4, 4^{12}, 4^{28}, 4^{60}, 4^{188}, 4^{444} hatványok maradékai (ezek sorra: 256, 82, 361, 298, 229, 256) ismét darabonként fél-fél pontot érjenek, végül a végeredmény megadása is fél pontot.

2. Az alábbi C kód a bemenetként (10-es számrendszerben) kapott n pozitív egész négyzetét számítja ki. Tegyük fel, hogy a kód végrehajtásakor a gép az alapműveleteket az „írásbeli" összeadás és kivonás segítségével végzi el. Döntsük el, hogy az eljárás polinomiális-e.

```
x = n; y = 0;
while (x > 0) {
   x = x-1;
   y = y+n;
}
printf("Eredmény: %d", y);
```

* * * * *

Jelölje n számjegyeinek számát (a 10-es számrendszerben) k. Ekkor az eljárás bemenetének mérete k (hiszen számjegyenként egy bájt szükséges a bemenet tárolásához). (2 pont)
Ekkor tehát $n \geq 10^{k-1}$ (hiszen a k jegyű számok 10^{k-1} és $10^k - 1$ között vannak). (2 pont)
Az eljárás a ciklusmagot n-szer hajtja végre, hiszen az x változó értéke n-től 1-ig csökken, mielőtt a ciklus megáll. (1 pont)
Ezért az algoritmus lépésszáma legalább 10^{k-1} (hiszen ez még akkor is igaz volna, ha a ciklusmag végrehajtásához mindig egyetlen lépés elég volna). (2 pont)
Mivel az eljárás k méretű inputon legalább 10^{k-1} lépést tesz, ezért exponenciális lépésszámú(2 pont)
és így nem polinomiális futásidejű. (1 pont)
Mivel az előadáson az exponenciális algoritmus definíciója az volt, hogy minden $k \geq 1$ esetén van olyan k méretű input, amelyre az eljárás legalább a^k lépést tesz, ahol $a > 1$ fix konstans, ezért a fenti megoldást valójában még ki kellene egészíteni például azzal, hogy $10^{k-1} \geq 3^k$ igaz, ha $k \geq 2$. Ezért a hiányosságért azonban ne vonjunk le pontot, a 10^{k-1}-es alsó becslés is legyen elegendő egy teljes értékű megoldáshoz. Ha egy megoldó nem tudja ugyan precízen indokolni, hogy az eljárás nem polinomiális, de a megoldásából világosan kiderül, hogy látja, hogy az nem hatékony (például: „egy 100 jegyű input esetén legalább 10^{99} összeadást és kivonást végez, ami egy szuperszámítógépnek is évmilliárdokig tartana"), az ezért legföljebb 4 pontot kaphat. (Ebben az esetben azonban ehhez már nem adhatók a fenti pontozás szerinti további részpontok. Így minden ilyen megoldást úgy kell értékelni, hogy a precíz megoldásból származó részpontszám, illetve a nem precíz megoldásért adható legföljebb 4 pont közül a nagyobbat adjuk.)

3. Átmegy-e az origón az az S sík, amely tartalmazza a $P(2;-1;4)$ pontot és az $\frac{x-1}{4} = \frac{1-y}{5} = \frac{z-3}{6}$ egyenletrendszerű e egyenest?

* * * * *

Az e egyenletrendszeréből (a középső tört $\frac{y-1}{-5}$ alakba való átírása után) kiolvasható, hogy e átmegy a $Q(1;1;3)$ ponton és egy irányvektora $\underline{v} = (4;-5;6)$. (2 pont)
S-sel párhuzamos a $\overrightarrow{QP} = \underline{p} - \underline{q} = (2;-1;4) - (1;1;3) = (1;-2;1)$ vektor, ahol $\underline{p}$ és $\underline{q}$ a megfelelő pontokba mutató helyvektorokat jelöli. (1 pont)
S-nek normálvektora lesz az $\underline{n} \neq \underline{0}$ vektor, ha az merőleges $\overrightarrow{QP}$-re és $\underline{v}$-re is. (1 pont)
Az $\underline{n} = (a,b,c) \neq \underline{0}$ pontosan akkor ilyen, ha az $\underline{n} \cdot \overrightarrow{QP}$ és az $\underline{n} \cdot \underline{v}$ skaláris szorzatok értéke 0.(1 pont)
A skaláris szorzat képletéből: $a - 2b + c = 0$ és $4a - 5b + 6c = 0$. (1 pont)
A második egyenletből az első 4-szeresét kivonva: $3b+2c = 0$. Így például a $b = 2$, $c = -3$ választással mindkét egyenletből $a = 7$ adódik, vagyis $\underline{n} = (7;2;-3)$ normálvektora S-nek. (1 pont)
Ebből (például) P-t használva felírható S egyenlete: $7x + 2y - 3z = 0$. (2 pont)
Mivel a $(0;0;0)$ pont ezt kielégíti, ezért S átmegy az origón. (1 pont)
A hiánytalan megoldáshoz valójában hozzátartozna annak ellenőrzése is, hogy $P \notin e$ (és így $\overrightarrow{QP} \nparallel \underline{v}$). Mivel azonban a feladat szövege implicite állítja S egyértelműségét és ezáltal a $P \notin e$ állítást, ezért ennek a hiányáért ne vonjunk le pontot.

4. Generátorrendszert alkotnak-e $\mathbb{R}^3$-ben az alábbi $\underline{a}$, $\underline{b}$, $\underline{c}$ vektorok?

$$\underline{a} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \ \underline{b} = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix} \text{ és } \ \underline{c} = \begin{pmatrix} 3 \\ 4 \\ 2 \end{pmatrix}.$$

* * * * *

Első megoldás. Az $\underline{a}$ és $\underline{b}$ vektorok nem párhuzamosak, mert nem skalárszorosai egymásnak.(1 pont)
Mivel két nem párhuzamos vektorból (1 pont)
az őket tartalmazó sík minden vektora kifejezhető lineáris kombinációval, (1 pont)
ezért ha a $\underline{c}$ benne volna az $\underline{a}$ és $\underline{b}$ által kifeszített, origón átmenő síkban, akkor léteznének olyan α és β együtthatók, amelyekre $\alpha\underline{a} + \beta\underline{b} = \underline{c}$. (2 pont)
Ebből $\alpha + 2\beta = 3$, $\alpha + 2\beta = 4$ (és $\beta = 2$) adódna. Mivel ezek az egyenletek ellentmondásra vezetnek, ezért ilyen α és β nincs. (2 pont)
Tehát az $\underline{a}$, $\underline{b}$ és $\underline{c}$ vektorok nem esnek egy (origón átmenő) síkba, így az előadáson tanultak szerint generátorrendszert alkotnak $\mathbb{R}^3$-ben (mert $\mathbb{R}^3$ minden vektora kifejezhető belőlük lineáris kombinációval). (3 pont)

Második megoldás. $\underline{a}$ és $\underline{b}$ nem párhuzamosak, mert nem skalárszorosai egymásnak. (1 pont)
Az $\underline{a}$ és $\underline{b}$ által kifeszített, origón átmenő S síknak normálvektora lesz az $\underline{n} \neq \underline{0}$ vektor, ha az merőleges $\underline{a}$-ra és $\underline{b}$-re is. (1 pont)
Az $\underline{n} = (a, b, c) \neq \underline{0}$ pontosan akkor ilyen, ha az $\underline{n} \cdot \underline{a}$ és az $\underline{n} \cdot \underline{b}$ skaláris szorzatok értéke 0. (1 pont)
A skaláris szorzat képletéből: $a + b = 0$ és $2a + 2b + c = 0$. (1 pont)
Ezeknek megfelel például az $\underline{n} = (1; -1; 0)$ vektor, így az normálvektora S-nek. (1 pont)
Ebből (felhasználva, hogy átmegy az origón) felírható S egyenlete: $x - y = 0$. (1 pont)
Mivel $\underline{c}$ ezt nem elégíti ki, ezért nem fekszik S-ben. (1 pont)
Tehát az $\underline{a}$, $\underline{b}$ és $\underline{c}$ vektorok nem esnek egy (origón átmenő) síkba, így az előadáson tanultak szerint generátorrendszert alkotnak $\mathbb{R}^3$-ben (mert $\mathbb{R}^3$ minden vektora kifejezhető belőlük lineáris kombinációval). (3 pont)

Harmadik megoldás. A $\underline{v} = \begin{pmatrix} p \\ q \\ r \end{pmatrix}$ vektor pontosan akkor van az $\langle \underline{a}, \underline{b}, \underline{c} \rangle$ generált altérben, ha $\underline{v}$ kifejezhető $\underline{a}$-ból, $\underline{b}$-ből és $\underline{c}$-ből lineáris kombinációval; vagyis ha léteznek olyan α, β, γ együtthatók, hogy $\alpha \cdot \underline{a} + \beta \cdot \underline{b} + \gamma \cdot \underline{c} = \underline{v}$. (1 pont)
Behelyettesítve $\underline{a}, \underline{b}, \underline{c}$ konkrét értékét és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} \alpha + 2\beta + 3\gamma &= p \\ \alpha + 2\beta + 4\gamma &= q \\ \beta + 2\gamma &= r \end{aligned} \quad \text{(2 pont)}$$

Az első két egyenlet különbségéből: $\gamma = q - p$. Ebből és a harmadik egyenletből: $\beta = r - 2(q - p) = 2p - 2q + r$. Ezeket az első két egyenlet közül bármelyikbe visszahelyettesítve: $\alpha = q - 2r$. (1 pont)
A kapott $\alpha = q - 2r$, $\beta = 2p - 2q + r$, $\gamma = q - p$ valóban megoldása az egyenletrendszernek.(1 pont)
Ebből következik, hogy a fenti egyenletrendszer minden p, q és r esetén megoldható, (1 pont)
vagyis minden $\underline{v} \in \mathbb{R}^3$ benne van az $\langle \underline{a}, \underline{b}, \underline{c} \rangle$ generált altérben. (2 pont)
Ezért $\underline{a}$, $\underline{b}$, $\underline{c}$ generátorrendszert alkot $\mathbb{R}^3$-ben. (2 pont)

5. Lineárisan függetlenek-e az alábbi, $\mathbb{R}^4$-beli vektorok?

$$\underline{u} = \begin{pmatrix} 2 \\ 4 \\ 3 \\ 6 \end{pmatrix}, \ \underline{v} = \begin{pmatrix} 3 \\ 6 \\ 2 \\ 4 \end{pmatrix}, \ \underline{w} = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix}.$$

* * * * *

Tegyük fel, hogy az α, β, γ skalárokra $\alpha \cdot \underline{u} + \beta \cdot \underline{v} + \gamma \cdot \underline{w} = \underline{0}$ teljesül. (1 pont)
Behelyettesítve $\underline{u}, \underline{v}, \underline{w}$ konkrét értékét és elvégezve a műveleteket a következő lineáris egyenletrendszerre jutunk:

$$\begin{aligned} 2\alpha + 3\beta + \gamma &= 0 \\ 4\alpha + 6\beta + 2\gamma &= 0 \\ 3\alpha + 2\beta &= 0 \\ 6\alpha + 4\beta &= 0 \end{aligned}$$ (2 pont)

Látható, hogy a második egyenlet duplája az elsőnek, a negyedik pedig duplája a harmadiknak; ezért a második és negyedik egyenletek elhagyhatók (a megoldáshalmaz változtatása nélkül). (1 pont)
Ekkor például az $\alpha = 2$, $\beta = -3$ választás a harmadik egyenletet kielégíti, amiből az első egyenletből $\gamma = 5$ adódik. (1 pont)
Mindezekből tehát $2\underline{u} - 3\underline{v} + 5\underline{w} = \underline{0}$. (2 pont)
Mivel tehát az $\underline{u}, \underline{v}, \underline{w}$ vektorokból a $\underline{0}$ kifejezhető nem csupa 0 együtthatójú lineáris kombinációval, ezért a tanultak szerint $\underline{u}, \underline{v}, \underline{w}$ lineárisan összefüggő (és így a válasz: nem). (3 pont)
Ha egy megoldó felírja és meggyőzően (ellenőrzéssel) indokolja a $2\underline{u} - 3\underline{v} + 5\underline{w} = \underline{0}$ összefüggést, azért természetesen akkor is jár az ezért adható maximális részpontszám (7 pont), ha az ehhez vezető utat a megoldó nem részletezi. A feladat megoldható a lineáris függetlenség eredeti definíciójával is: például a fentiekhez hasonló számolással kihozható, hogy $\underline{w} = -\frac{2}{5}\underline{u} + \frac{3}{5}\underline{v}$, amiből definíció szerint szintén következik $\underline{u}, \underline{v}, \underline{w}$ lineáris összefüggősége.

6*. Legyen n egy 8-cal osztható, de 3-mal nem osztható pozitív egész szám. Mutassuk meg, hogy a 3 árulója n-nek (vagyis a Fermat-teszt végrehajtásakor a 3 tanúsítja n összetett voltát).

* * * * *

Mivel $3 \nmid n$ (és 3 prím), ezért $(3, n) = 1$. (1 pont)
Így a feladat állítása azt jelenti, hogy $3^{n-1} \not\equiv 1 \pmod{n}$, ezt kell tehát megmutatni. (2 pont)
Tegyük fel ezért indirekt, hogy $3^{n-1} \equiv 1 \pmod{n}$.
Ebből $8|n$ miatt $3^{n-1} \equiv 1 \pmod{8}$ is következik. Valóban: $3^{n-1} \equiv 1 \pmod{n}$ azt jelenti, hogy $n \Big| 3^{n-1} - 1$; ebből $8|n$ miatt $8 \Big| 3^{n-1} - 1$, ami ekvivalens a $3^{n-1} \equiv 1 \pmod{8}$ állítással. (2 pont)
Mivel $3^2 = 9 \equiv 1 \pmod{8}$, ebből ($k$-adik hatványra emeléssel) $3^{2k} \equiv 1 \pmod{8}$, amiből pedig (3-mal szorzással) $3^{2k+1} \equiv 3 \pmod{8}$ minden $k \geq 1$ egészre. (2 pont)
Ebből és a $3^{n-1} \equiv 1 \pmod{8}$ állításból következik, hogy $n - 1$ páros, vagyis n páratlan. (1 pont)
Ez pedig $8|n$ miatt ellentmondás, amivel $3^{n-1} \not\equiv 1 \pmod{n}$ indoklása teljes. (2 pont)