Bevezetés a számításelméletbe II.
2. pótzárthelyi feladatok — pontozási útmutató
2014. december 12.

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. Az útmutatóban szereplő részpontszámok szükség esetén tovább is oszthatók. Az útmutatóban leírttól eltérő jó megoldás természetesen maximális pontot ér.

Minden feladat 10 pontot ér. Az elégséges határa 24 pont. A vizsgajegybe a dolgozat pontszáma számít bele, így a dolgozatokra osztályzatot nem adunk.

1. A G gráfot egy 10 csúcsú teljes gráfból két csatlakozó él elhagyásával kapjuk. Határozzuk meg $\lambda(G)$-t, azaz a legnagyobb olyan k számot, melyre G k-szorosan élösszefüggő.

* * * * *

Mivel G-nek van olyan csúcsa, melynek foka 7, $\lambda(G) \leq 7$, (1 pont)
hiszen a csúcsra illeszkedő éleket elhagyva a gráf szétesik. (1 pont)
Megmutatjuk másrészt, hogy $\lambda(G) \geq 7$ is, ehhez azt kell belátni, hogy G 7-szeresen élösszefüggő.
Ehhez az előadáson tanultak szerint elég azt megmutatni, hogy G 7-szeresen összefüggő, (2 pont)
azaz bármely legfeljebb 6 csúcsát elhagyva összefüggő marad (és van legalább 8 csúcsa – e megjegyzés hiányáért ne vonjunk le pontot). (1 pont)
Legfeljebb 6 tetszőleges csúcsot elhagyva olyan gráfot kapunk, melynek legalább 4 csúcsa van és a komplementere legfeljebb két élet tartalmaz (ha pontosan kettőt, akkor azok csatlakozó élek). (3 pont)
Az elhagyás utáni gráfnak tehát lesz olyan csúcsa, mely minden másikkal össze van kötve, így a gráf nyilván összefüggő. (2 pont)

Ha valaki nem legfeljebb, hanem pontosan 6 csúcs törlését vizsgálja, akkor önmagában ezért nem kell pontot levonnunk.

2. Határozzuk meg minden pozitív egész n-re az $n^3 + 3n^2 + 2n$ és $n - 1$ számok legnagyobb közös osztóját.

* * * * *

n és $n - 1$ relatív prímek, (1 pont)
hiszen a különbségük 1, azaz minden közös osztójuk osztja az 1-et is. (1 pont)
Így $n^3 + 3n^2 + 2n$ és $n - 1$ közös osztói mind osztják $(n^2 + 3n + 2)$-t is a számelmélet alaptétele miatt (hiszen $n^3 + 3n^2 + 2n = n(n^2 + 3n + 2)$). (2 pont)
$n^2 + 3n + 2$ és $n - 1$ lnko.-ja osztja $(n^2 + 3n + 2) - n(n - 1) = (4n + 2)$-t is, (1 pont)

így $(4n+2)-4(n-1)=6$-ot is. (1 pont)
A legnagyobb közös osztó tehát az 1,2,3,6 számok közül kerül ki. (1 pont)
Ha $n \equiv 1 \pmod 6$, akkor $n-1$ és n^2+3n+2 is osztható 6-tal, a keresett lnko. tehát 6. (1 pont)
Ha $n \equiv 3 \pmod 6$ vagy $n \equiv 5 \pmod 6$, akkor az lnko. 2. (1 pont)
Ha $n \equiv 4 \pmod 6$, akkor az lnko. 3, (1 pont)
végül $n \equiv 0 \pmod 6$ vagy $n \equiv 2 \pmod 6$ esetén az lnko. nyilván 1. (1 pont)

3. Egy n egész szám 14-szerese 3 maradékot ad 51-gyel osztva. Milyen maradékokat adhat n 34-gyel osztva?

* * * * *

A $14n \equiv 3 \pmod{51}$ lineáris kongruencia megoldásaira vagyunk kíváncsiak. (1 pont)
14 és 51 lnko.-ja 1, ez osztja a 3-at, így lesz megoldás (mégpedig 1 darab modulo 51, de ezt nem muszáj megállapítani és persze nem baj, ha az, hogy létezik megoldás csak később derül ki). (1 pont)
Mindkét oldalt 4-gyel szorozva az eredetivel ekvivalens $56n \equiv 12 \pmod{51}$ kongruenciát kapjuk, (1 pont)
hiszen 4 és 51 relatív prímek. (1 pont)
Innen $5n \equiv 12 \pmod{51}$. A jobboldalból 102-t elvéve $5n \equiv -90 \pmod{51}$. (1 pont)
Ezt oszthatjuk 5-tel, miközben a modulus nem változik: $n \equiv -18 \pmod{51}$, (1 pont)
hiszen 5 és 51 relatív prímek. (1 pont)
Innen $51 \mid n+18$, tehát $17 \mid n+18$, (1 pont)
azaz $n \equiv -18 \equiv 16 \pmod{17}$. (1 pont)
Mivel n lehet páros és páratlan is, n lehetséges maradékai modulo 34: 16 és 33. (1 pont)

Ha az utolsó lépésben negatív maradék is felbukkan, azért (noha szigorúan véve nem helyes) ne vonjunk le pontot.
Fontos, hogy (mint az a bevezetőben is szerepel) a fenti részpontok az egyes gondolatokra akkor járnak, ha azok egy megoldás irányába mutató próbálkozás lépéseiként szerepelnek. Összevissza végzett, megoldás felé nem mutató osztásokért, szorzásokért, stb. akkor is legfeljebb 1-2 pont adható, ha egyébként helyesek és (jól) meg vannak indokolva. Ha valaki Euklideszi algoritmussal oldja meg a lineáris kongruenciát, akkor nem kell minden egyes lépést megindokolnia (hiszen a módszer szerepelt az előadáson), de ez esetben vagy le kell írnia, hogy az Euklideszi algoritmust használja, vagy meg kell indokolnia, hogy a kapott megoldás miért jó és miért nincs más megoldás. Ezek hiányáért 1-1 pontot vonjunk le.

4. Oldjuk meg a

$$76x \equiv 3 \pmod{111}$$

lineáris kongruenciát.

* * * * *

111 és 76 lnko.-ja 1, ez osztja a 3-at, így lesz megoldás (mégpedig 1 darab modulo 111, de ezt itt sem muszáj rögtön megállapítani és most sem baj, ha az, hogy létezik megoldás csak később derül ki). (1 pont)
A kongruenciát Euklideszi algoritmussal oldjuk meg. Tudjuk, hogy $111x \equiv 0 \pmod{111}$. (1 pont)
Innen $35x = 111x - 76x \equiv 0 - 3 \pmod{111}$. (2 pont)
Így $6x = 76x - 2 \cdot 35x \equiv 3 - 2 \cdot (-3) = 9 \pmod{111}$, (2 pont)
ahonnan $5x = 35x - 5 \cdot 6x \equiv -3 - 5 \cdot 9 = -48 \pmod{111}$, (2 pont)
végül $x = 6x - 5x \equiv 9 - (-48) = 57 \pmod{111}$. (2 pont)

Ha (ebben a megoldásban) nem esik szó arról, hogy Euklideszi algoritmussal dolgozunk, akkor itt is meg kell indokolni, hogy a kapott megoldás miért jó és miért nincs más megoldás. Ezek hiányáért 1-1 pontot vonjunk le.
Olyan számolásokért, amik nem mutatnak semmilyen megoldás irányába, akkor is legfeljebb 1-2 pontot adjunk, ha egyébként alátámasztottak (vagyis az átalakított és a kiinduló kongruenciák ekvivalenciáját a hallgató belátja).

5. Az n szám hármas számrendszerbeli alakja 200102100202. Határozzuk meg n^n hármas számrendszerbeli alakjának utolsó három számjegyét.

* * * * *

Egy szám hármas számrendszerbeli alakjának utolsó három számjegyét a szám 27-tel vett osztási maradéka határozza meg, így először ezt számoljuk ki. Mivel 202 a 20 hármas számrendszerbeli alakja, $n^n \equiv 20^n \pmod{27}$, hiszen n utolsó három számjegye 202. (1 pont)
Mivel 20 és 27 relatív prímek, (1 pont)
az Euler-Fermat tétel szerint $20^{\varphi(27)} \equiv 1 \pmod{27}$. (1 pont)
$\varphi(27) = 3^3 - 3^2 = 18$, (1 pont)
így most n 18-cal vett osztási maradékát kéne meghatároznunk. (1 pont)
Ez a hármas számrendszerbeli alakból könnyen leolvasható: az utolsó két jegy 02, így a 9-cel vett osztási maradék 2, a 18-cal vett maradék tehát 2 vagy 11. (1 pont)
Hogy a kettő közül melyik, azt az n paritása dönti el: ha n páros, akkor 2, ha páratlan, akkor 11. (1 pont)
Az n hármas számrendszerbeli alakjában páros sok páratlan szám (1-es) fordul elő, így n páros, tehát $n = 18k + 2$ valamely k egészre. (1 pont)
Innen $20^n = 20^{18k+2} = (20^{18})^k 20^2 \equiv 20^2 \equiv (-7)^2 \equiv 22 \pmod{27}$. (1 pont)
A keresett utolsó három számjegy tehát 211. (1 pont)

6. Mely $n \geq 2$ egészekre teljesül, hogy

$$\varphi(n) + \frac{\mathrm{d}(n)}{2} = n?$$

(Ahol φ az Euler-féle φ-függvény, $\mathrm{d}(n)$ pedig az n szám pozitív osztóinak száma.)

* * * * *

Az n szám pozitív osztói 1 és n közé esnek, de ezek közül azok, amik relatív prímek n-nel, az 1 kivételével nem lehetnek n osztói, (3 pont)
így $\mathrm{d}(n) \leq n - \varphi(n) + 1$, (1 pont)
azaz $\mathrm{d}(n) + \varphi(n) \leq n + 1$. (1 pont)
Mivel $\mathrm{d}(n) \geq 2$,

$$\frac{\mathrm{d}(n)}{2} + \varphi(n) \leq \mathrm{d}(n) + \varphi(n) - 1 \leq n$$

(1 pont)
és egyenlőség csak akkor állhat fenn, ha $\mathrm{d}(n) = 2$, (1 pont)
azaz ha n prím. (1 pont)
Ha n prím, akkor $\varphi(n) = n - 1$, így az egyenlőség ilyenkor valóban teljesül, (1 pont)
a keresett n egészek tehát a pozitív prímek. (1 pont)