Bevezetés a számításelméletbe II.
2. zárthelyi feladatok — pontozási útmutató
2014. november 28.

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. Legyen G az a gráf, melyet egy 9 csúcsú körből úgy kapunk, hogy a körön másodszomszédos csúcsokat is összekötjük. Határozzuk meg $\lambda(G)$-t, azaz a legnagyobb olyan k számot, melyre G k-szorosan élösszefüggő.

* * * * *

Mivel G-nek van olyan csúcsa, melynek foka 4, $\lambda(G) \leq 4$, (1 pont)
hiszen a csúcsra illeszkedő éleket elhagyva a gráf szétesik. (1 pont)
Megmutatjuk másrészt, hogy $\lambda(G) \geq 4$ is, ehhez azt kell belátni, hogy G 4-szeresen élösszefüggő, azaz bármely legfeljebb három élét elhagyva összefüggő marad. (1 pont)
G élhalmaza két Hamilton-kör uniója, hiszen az eredeti 9 csúcsú kör és az ezen másodszomszédos csúcsokat összekötő élek is Hamilton-kört alkotnak. (1 pont)
Ez utóbbi azért teljesül, mert mindig a másodszomszédra továbblépve 9 lépés után visszajutunk a kezdőpontba, de korábban nem (aminek az oka az, hogy 2 és 9 relatív prímek, de ezt nem muszáj megállapítani). (1 pont)
Ha csak három, vagy kevesebb élet hagyunk el, akkor a két Hamilton-kör közül az egyikből csak legfeljebb egy élet hagytunk el, (3 pont)
azaz a gráfnak marad Hamilton-útja, tehát összefüggő. (2 pont)

Ha valaki nem legfeljebb, hanem pontosan 3 él törlését vizsgálja, akkor önmagában ezért nem kell pontot levonnunk.

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

* * * * *

$n+1$ relatív prím $3n+2$-vel, (1 pont)
hiszen $3(n+1)-(3n+2)=1$, így $n+1$ és $3n+2$ minden közös osztója osztja az 1-et is. (2 pont)
Hasonló gondolatmenettel látható, hogy n és $3n+2$ lnko.-ja legfeljebb 2: (1 pont)
mivel $3n+2-3n=2$, így n és $3n+2$ minden közös osztója osztja a 2-t is. (1 pont)

Mivel $n^2+n=n(n+1)$, a számelmélet alaptétele miatt (1 pont)
n^2+n prímosztói n és $n+1$ prímosztói közül kerülnek ki. (1 pont)
Így $3n+2$ és n^2+n legnagyobb közös osztója legfeljebb 2 lehet. (1 pont)
n^2+n mindig páros, $3n+2$ pedig pontosan akkor, ha n páros, (1 pont)
így a keresett lnko. páratlan n esetén 1, páros n esetén 2. (1 pont)

3. Egy n egész szám 45-szöröse 21 maradékot ad 78-cal osztva. Milyen maradékokat adhat n 130-cal osztva?

* * * * *

A $45n \equiv 21 \pmod{78}$ lineáris kongruencia megoldásaira vagyunk kíváncsiak. (1 pont)
45 és 78 lnko.-ja 3, ez osztja a 21-et, így lesz megoldás (mégpedig 3 darab modulo 78, de ezt nem muszáj megállapítani és persze nem baj, ha az, hogy létezik megoldás csak később derül ki). (1 pont)
A kongruenciát 3-mal osztva az eredetivel ekvivalens $15n \equiv 7 \pmod{26}$ kongruenciát kapjuk, (1 pont)
mivel a modulust osztanunk kell 3 és 78 lnko.-jával, azaz 3-mal. (1 pont)
A jobboldalhoz 26-ot adva $15n \equiv 33 \pmod{26}$. (1 pont)
Ezt oszthatjuk 3-mal, miközben a modulus nem változik, hiszen 3 és 26 relatív prímek: $5n \equiv 11 \pmod{26}$. (1 pont)
A jobboldalból 26-ot elvéve $5n \equiv -15 \pmod{26}$. (1 pont)
Ezt oszthatjuk 5-tel, miközben a modulus nem változik, hiszen 5 és 26 relatív prímek: $n \equiv -3 \pmod{26}$. (1 pont)
Innen n lehetséges maradékai modulo 130: 23, 49, 75, 101, 127. (2 pont)

Ha az utolsó lépésben negatív maradék is felbukkan, azért (noha szigorúan véve nem helyes) ne vonjunk le pontot. Egy hiányzó maradékért vagy más kisebb zavarért 1 pontot vonjunk le, ha ennél nagyobb a gond, az utolsó 2 pont nem jár.
A $15n \equiv 7 \pmod{26}$ lineáris kongruencia persze másképp is megoldható, pl.
A baloldalból $26n$-et elvéve és a jobboldalhoz 26-ot adva $-11n \equiv 33 \pmod{26}$ (3 pont)
Ezt oszthatjuk -11-gyel, miközben a modulus nem változik, hiszen -11 és 26 relatív prímek: (1 pont)
$n \equiv -3 \pmod{26}$. (1 pont)

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

$$113x \equiv 2 \pmod{531}$$

lineáris kongruenciát.

* * * * *

113 és 531 lnko.-ja 1, ez osztja a 2-t, így lesz megoldás (mégpedig 1 darab modulo 531, 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 $531x \equiv 0 \pmod{531}$. (1 pont)
Innen $79x = 531x - 4 \cdot 113x \equiv 0 - 4 \cdot 2 \pmod{531}$. (2 pont)
Így $34x = 113x - 79x \equiv 2 - (-8) = 10 \pmod{531}$, (2 pont)
ahonnan $11x = 79x - 2 \cdot 34x \equiv -8 - 2 \cdot 10 = -28 \pmod{531}$, (2 pont)
végül $x = 34x - 3 \cdot 11x \equiv 10 - 3 \cdot (-28) = 94 \pmod{531}$. (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. Természetesen a lineáris kongruencia másképp is megoldható, pl.
mivel 5 és 531 relatív prímek, a kongruenciát 5-tel szorozva az eredetivel ekvivalens (1 pont)
$565x \equiv 10 \pmod{531}$ kongruenciát kapjuk, ahonnan $34x \equiv 10 \pmod{531}$. (2 pont)
Ezt oszthatjuk 2-vel, miközben a modulus nem változik, hiszen 2 és 531 relatív prímek: (1 pont)
$17x \equiv 5 \pmod{531}$. (1 pont)
Mivel 31 és 531 is relatív prímek, a kongruenciát 31-gyel szorozva az eredetivel ekvivalens (1 pont)
$527x \equiv 165 \pmod{531}$ kongruenciát kapjuk, ahonnan $-4x \equiv 155 \pmod{531}$. (2 pont)
A jobboldalból 531-et elvéve $-4x \equiv -376 \pmod{531}$. (1 pont)
Mivel -4 és 531 relatív prímek, az $x \equiv 94 \pmod{531}$ kongruencia is ekvivalens az eredetivel. (1 pont)

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. Határozzuk meg 43^{98} kettes számrendszerbeli alakjának utolsó öt számjegyét.

* * * * *

Egy szám kettes számrendszerbeli alakjának utolsó öt számjegyét a szám 32-vel vett osztási maradéka határozza meg, így először ezt számoljuk ki. (1 pont)
Mivel $43 \equiv 11 \pmod{32}$, elég 11^{98} 32-vel vett osztási maradékát meghatározni. (1 pont)
Mivel 11 és 32 relatív prímek, (1 pont)
az Euler-Fermat tétel szerint $11^{\varphi(32)} \equiv 1 \pmod{32}$. (2 pont)
$\varphi(32) = 2^5 - 2^4 = 16$, (1 pont)
ahonnan $11^{98} = 11^{96+2} = 11^{96}11^2 = (11^{16})^6 11^2 \equiv 11^2 = 121 \pmod{32}$. (2 pont)
A keresett maradék innen 25, (1 pont)
aminek kettes számrendszerbeli alakja 11001, ez lesz tehát 43^{98} kettes számrendszerbeli alakjának utolsó öt számjegye. (1 pont)

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

$$\varphi(n) + \mathrm{d}(n) = n + 1?$$

(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, (2 pont)
így $\mathrm{d}(n) \leq n - \varphi(n) + 1$ (1 pont)
és egyenlőség akkor és csak akkor áll fenn, ha az n-nél kisebb, n-hez nem relatív prím pozitív számok mind n osztói. (1 pont)
Ez prím n esetén igaz, így a pozitív prímszámokra teljesül a feladatbeli egyenlőség. (1 pont)

Ha n nem prím, akkor legyen p a legkisebb prímosztója, erre nyilván teljesül, hogy $p \leq \sqrt{n}$. (1 pont)
Az n és $n-p$ számok nem relatív prímek, tehát teljesülnie kellene rájuk, hogy $(n-p) \mid n$. (1 pont)
Ha $n - p > n/2$, akkor ez lehetetlen, (1 pont)
így az egyenlőség ebben az esetben csak akkor teljesülhet, ha $n - p \leq n/2$, azaz $n/2 \leq p \leq \sqrt{n}$, ahonnan $n \leq 4$, tehát már csak a 4-et kell megvizsgálnunk, (1 pont)
ez pedig szintén kielégíti az egyenlőséget, (1 pont)
így tehát a megoldások a pozitív prímek és a 4.