Bevezetés a számításelméletbe II.
2. pótzárthelyi — pontozási útmutató
2011. december 5.

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. Egy gráf négyszeresen élösszefüggő, de van olyan éle, melyet elhagyva már nem lesz az. Mutassuk meg, hogy van még legalább három éle, melyekre ugyanez teljesül.

* * * * *

A feltétel szerint a gráf bármely három élét elhagyva még összefüggő gráfot kapunk, viszont létezik olyan e_1 él, amelyet elhagyva ez már nem teljesül, (2 pont)
vagyis lesznek olyan e_2, e_3, e_4 élek, hogy $G - \{e_1, e_2, e_3, e_4\}$ nem összefüggő. (3 pont)
Mivel három élet elhagyva a gráf még összefüggő, az e_1, e_2, e_3, e_4 éleknek mind különbözőknek kell lenniük. (3 pont)
Világos, hogy az e_2, e_3, e_4 élek bármelyikét elhagyva sem lesz négyszeresen élösszefüggő a gráf, azaz valóban lesz legalább három él, amire ugyanaz teljesül, mint e_1-re. (2 pont)

2. Legyenek a és b tetszőleges pozitív egészek. Mutassuk meg, hogy a és b legkisebb közös többszöröse nem lehet $3a + 5b$.

* * * * *

Tegyük fel indirekten, hogy a kérdéses lkkt. $3a + 5b$. Ekkor $a|3a + 5b$ (és $b|3a + 5b$). (2 pont)
Innen $a|5b$. (2 pont)
Mivel $a|5b$ és $b|5b$, az $5b$ (pozitív) közös többszöröse a-nak és b-nek, (4 pont)
ami ellentmondás, hiszen $5b < 3a + 5b$ (mivel a pozitív). (2 pont)

3. Legyen p tetszőleges prímszám, a pedig olyan egész szám, ami nem osztható p-vel és pontosan p^2 darab pozitív osztója van. Mutassuk meg, hogy ekkor a 1 maradékot ad p-vel osztva.

* * * * *

Legyen a prímtényezős felbontása $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Ekkor a osztóinak száma $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_r+1)$, ennek kell egyenlőnek lennie p^2-tel. (1 pont)

Mivel p prím, p^2 csak $p \cdot p$ és $p^2 \cdot 1$ alakban áll elő két pozitív egész szorzataként, (2 pont)
azaz vagy $r = 1$ és ekkor $\alpha_1 = p^2 - 1$ (1 pont)
vagy $r = 2$ és ekkor $\alpha_1 = \alpha_2 = p - 1$. (1 pont)
Azt kellene tehát belátnunk, hogy $p_1^{p^2-1}$ és $p_1^{p-1}p_2^{p-1}$ is 1 maradékot ad p-vel osztva. Mivel a nem osztható p-vel, sem p_1, sem p_2 nem osztható p-vel, (1 pont)
így mindkét esetben alkalmazhatjuk az Euler-Fermat tételt, (1 pont)
eszerint $p_1^{p^2-1} = (p_1^{p+1})^{p-1} \equiv 1 \pmod{p}$ (2 pont)
és $p_1^{p-1}p_2^{p-1} \equiv 1 \pmod{p}$. (1 pont)

4. Egy szám 36-szorosa 68 maradékot ad 82-vel osztva. Milyen maradékot ad maga a szám 82-vel osztva?

* * * * *

A

$$36x \equiv 68 \pmod{82}$$

kongruencia megoldásait kell megkeresnünk modulo 82. (1 pont)
36 és 82 lnko-ja 2, ez osztja 68-at, tehát lesz megoldás (ha valaki csak eddig jut el, arra adhatunk 1 pontot), éspedig 2 darab modulo 82 (erre is adhatunk 1 pontot, ha valaki nem oldja meg a lineáris kongruenciát). A kongruenciát 4-gyel osztva, az eredetivel ekvivalens

$$9x \equiv 17 \pmod{41}$$

kongruenciát kapjuk. (2 pont)
Mindkét oldalt 5-tel szorozva az eredetivel ekvivalens

$$45x \equiv 85 \pmod{41}$$

kongruenciát kapjuk, (3 pont)
ahonnan

$$4x \equiv 44 \pmod{41}$$

adódik. (1 pont)
Ezt 4-gyel osztva az eredetivel ekvivalens

$$x \equiv 11 \pmod{41}$$

kongruencia adódik. (1 pont)
Innen a megoldások 11 és 11+41=52 modulo 82. (2 pont)

5. Határozzuk meg az összes olyan n számot, melyre

$$\varphi(n) = n - 4.$$

* * * * *

A definíció szerint $\varphi(n)$ az n-nél kisebb, n-hez relatív prím pozitív egészek száma (ezért még nem jár pont), így a feltétel szerint az n-nél kisebb, n-hez nem relatív prím pozitív egészek száma pontosan 3. (1 pont)
Ha n prímhatvány, akkor előáll két egynél nagyobb relatív prím szám, a és b szorzataként (feltehető, hogy $a < b$), (1 pont)

ekkor a és b nem relatív prímek n-hez, sőt $2a$ sem, (1 pont)
így a feltétel csak akkor teljesülhet, ha ezzel felsoroltuk az összes n-nél kisebb, n-hez nem relatív prím pozitív egész számot, hiszen az említett számok csakugyan mind különbözőek és kisebbek n-nél. (1 pont)
Innen $a \leq 2$ és $b \leq 3$, (2 pont)
azaz $n = 6$, mivel a többi 6-nál kisebb számnak nincs két különböző osztója, $\varphi(6)$ pedig valóban 6-4=2. (1 pont)
Ha $n = p^\alpha$, a $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha - 4$ egyenlőségből $p^{\alpha-1} = 4$ következik, (1 pont)
azaz $n = 8$, ami csakugyan megoldás, hiszen $\varphi(8)$ valóban 8-4=4. (1 pont)
A fentiek szerint tehát két számra teljesül az egyenlőség, a 6-ra és a 8-ra. (1 pont)

6. Határozzuk meg 125^{125} utolsó két számjegyét a hetes számrendszerben.

* * * * *

A feladat 125^{125} 49-cel való osztási maradékának meghatározása és az eredmény felírása hetes számrendszerben. Mivel 125 és 49 relatív prímek (persze 125 helyett lehet 27-tel számolni, de ezért még nem jár pont), (1 pont)
az Euler-Fermat tétel szerint

$$125^{\varphi(49)} \equiv 1 \pmod{49}.$$

(1 pont)
$\varphi(49) = 42$, (1 pont)
így 125^{41} 49-cel való osztási maradékát kéne kiszámolnunk. (1 pont)
Legyen

$$x \equiv 125^{41} \pmod{49},$$

ekkor

$$125x \equiv 125^{42} \equiv 1 \pmod{49}.$$

(2 pont)
A jobboldalhoz 49-et adva a

$$125x \equiv 50 \pmod{49}$$

kongruenciát kapjuk, (1 pont)
ahonnan

$$5x \equiv 2 \pmod{49}.$$

(1 pont)
A jobboldalhoz 98-at adva most az

$$5x \equiv 100 \pmod{49}$$

kongruenciát kapjuk, ahonnan

$$x \equiv 20 \pmod{49}.$$

(1 pont)
Az utolsó két számjegy tehát (sorrendben) 2 és 6. (1 pont)