Bevezetés a számításelméletbe II.
2. Pótzárthelyi — pontozási útmutató
2012. december 3.

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. Létezik-e olyan összefüggő, egyszerű gráf, melyben minden csúcs foka 4 és a gráf nem háromszorosan élösszefüggő?

* * * * *

Jó példa legfeljebb 4 pont, a maradék 6 pont a jó indoklásért jár. Ha valaki csak leírást ad egy jó példáról, de nem tudja megadni, akkor a leírás pontosságától függően kaphat (jó indoklással együtt) legfeljebb 8 pontot. Rossz definícióból induló próbálkozások tipikusan 0 pontot kapjanak.

2. Jelöljük $\lambda(u,v)$-vel a G gráfban az u és v csúcsok közt található éldiszjunkt utak maximális számát. Tudjuk, hogy a gráf a és b csúcsaira teljesül, hogy $\lambda(a,b) \geq 4$. Igaz-e, hogy ha ezen kívül minden c csúcsra $\lambda(a,c) + \lambda(b,c) \geq 4$, akkor a gráf négyszeresen élösszefüggő?

* * * * *

Az állítás nem lesz igaz, itt egy ellenpélda megtalálásáért akár 5 pontot is adhatunk, a maradék 5 jár az indoklásért. Ha valaki megpróbálja igazolni az állítást, akkor minőségtől függően 0-2 pontot adjunk.

3. Oldjuk meg a $93x \equiv 9 \pmod{129}$ kongruenciát.

* * * * *

93 és 129 lnko-ja 3, ez osztja 9-et, tehát lesz megoldás (ha valaki csak eddig jut el, arra adhatunk 1 pontot), éspedig 3 darab modulo 129 (erre is adhatunk 1 pontot, ha valaki nem oldja meg a lineáris kongruenciát). A kongruenciát 3-mal osztva az eredetivel ekvivalens

$$31x \equiv 3 \pmod{43}$$

kongruenciát kapjuk. (1 pont)
A bal oldalról $43x$-et elvéve

$$-12x \equiv 3 \pmod{43}.$$

(1 pont)
Mivel -3 és 43 relatív prímek, (1 pont)
(-3)-mal osztva az eredetivel ekvivalens

$$4x \equiv -1 \pmod{43}$$

kongruenciát kapjuk. (2 pont)
A jobb oldalról 43-at elvéve

$$4x \equiv -44 \pmod{43}.$$

(1 pont)
Mivel 4 és 43 relatív prímek, (1 pont)
4-gyel osztva az eredetivel ekvivalens

$$x \equiv -11 \pmod{43}$$

kongruencia adódik, (2 pont)
ami már a megoldás, hiszen nem volt követelmény az eredmények mod 129 megadása. (1 pont)
(Ha valaki mégis megadja a megoldásokat mod 129, az természetesen nem baj, de ha hiba van benne, akkor nem jár a pont.)

4. Határozzuk meg az összes olyan n számot, melyre $\varphi(n)$ prím.

* * * * *

Legyen n prímtényezős felbontása $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Használjuk az előadáson tanult $\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \dots (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$ képletet. (Idáig még nem jár pont.) A szorzat tényezői mind pozitív egészek, így a szorzatuk csak akkor lehet a p prím, ha egyikük éppen p, a többi pedig 1. (2 pont)
$p_i^{\alpha_i} - p_i^{\alpha_i - 1} \geq p_i - 1$, (1 pont)
így $p_i^{\alpha_i} - p_i^{\alpha_i - 1} = 1$ csak akkor lehetséges, ha $p_i = 2$ és $\alpha_i = 1$. (2 pont)
Ha $p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p$, akkor $\alpha_i \geq 2$ esetén $i = 2$, $p_i = p$ és $p_i - 1 = 1$, és n-nek más prímosztója (a korábbiak szerint) nem lehet, azaz $n = 4$. (2 pont)
$\alpha_i = 1$ esetén $p_i - 1 = p$, ami csak $p = 2$, $p_i = 3$ esetén lehetséges. (1 pont)
Így tehát megoldás még a 3 és a 6, más megoldás pedig (a korábban látottakat is felhasználva) nincs. (2 pont)

5. Legyen p tetszőleges prímszám. Mutassuk meg, hogy ha $n^2 \equiv 1 \pmod{p}$, akkor $n \equiv 1 \pmod{p}$ vagy $n \equiv -1 \pmod{p}$.

* * * * *

$n^2 \equiv 1 \pmod{p}$ a kongruencia definíciója szerint ekvivalens azzal, hogy $p \mid n^2 - 1$, (2 pont)
azaz $p \mid (n-1)(n+1)$. (2 pont)
Mivel p prím, ebből következik, hogy $p \mid n-1$ vagy $p \mid n+1$ teljesül, (5 pont)
ahonnan a kongruencia definícióját használva a feladat állítása adódik. (1 pont)

6. Mutassuk meg, hogy végtelen sok olyan n szám van, melyre $52 \mid 5^n - 21$.

* * * * *

Egy ilyen n számot könnyű találni: $5^3 - 21 = 125 - 21 = 104 = 2 \cdot 52$, tehát a 3 jó lesz. (1 pont)
Mivel 52 és 5 relatív prímek, (1 pont)
az Euler-Fermat tétel szerint $5^{\varphi(52)} \equiv 1 \pmod{52}$. (2 pont)

Így tetszőleges k pozitív egészre $5^{k\varphi(52)} \equiv 1 \pmod{52}$. (1 pont)
Mivel $5^3 \equiv 21 \pmod{52}$, (1 pont)
$5^{k\varphi(52)+3} \equiv 21 \pmod{52}$, (2 pont)
azaz $52 \mid 5^{k\varphi(52)+3} - 21$, (1 pont)
amiből az állítás következik. (1 pont)

Ha valaki kiszámolja $\varphi(52)$ értékét, az nem baj, de pont nem jár érte, hiszen a megoldásban szerepe nincs (csak annyi, hogy nem 0, de ez triviális). Természetesen ha valaki hibázik $\varphi(52)$ értékének kiszámításakor, akkor ezért pontot sem kell levonni tőle.