Bevezetés a számításelméletbe II.
Zárthelyi feladatok — pontozási útmutató
2011. november 24.

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_1 gráf bármely két csúcsa közt létezik három éldiszjunkt út és ugyanez teljesül a G_2 gráfra is. Legyen G az a gráf, amit úgy kapunk, hogy a G_1 és G_2 (diszjunkt) gráfok közé behúzunk három tetszőleges élet. Igaz-e, hogy G bármely két csúcsa közt is létezik három éldiszjunkt út?

* * * * *

A válasz igen. G_1-ből tetszőlegesen elhagyva legfeljebb két élet G_1 összefüggő marad, hiszen bármely két csúcsa között létezik út, azaz G_1 háromszorosan élösszefüggő. Ugyanez vonatkozik természetesen G_2-re is. (Az állítás természetesen a megfelelő Menger-tételből is következik). (3 pont)
Megmutatjuk, hogy G is háromszorosan élösszefüggő, amiből az említett Menger-tétel szerint az állítás következik. (2 pont)
Legfeljebb két élet elhagyva G-ből a G_1 csúcsai által feszített részgráf és a G_2 csúcsai által feszített részgráf is összefüggő marad, (2 pont)
és a két feszített részgráf bármely két csúcsa között is lesz út, hiszen a keresztbe menő élek közül legalább egy megmarad. (3 pont)

Menger-tételek használata nélkül az állítás bizonyítása elég macerás, egy adott pontból különböző pontokba menő éldiszjunkt utakat találni nem olyan egyszerű. Aki ebbe az irányba próbálkozik, de érdemi előrelépés nélkül, az 1-2 pontnál ne kapjon többet.

2. Legyen n tetszőleges páratlan szám. Határozzuk meg az n^2-n+2 és n^3+n^2 számok legnagyobb közös osztóját.

* * * * *

Jelöljük a és b legnagyobb közös osztóját (a,b)-vel. Ismert, hogy $(a,b)=(a,a-b)$, illetve innen $(a,b)=(a,a-kb)$ tetszőleges k egészre. (1 pont)
Így $(n^3+n^2, n^2-n+2) = (n^3+n^2-n(n^2-n+2), n^2-n+2) = (2n^2-2n, n^2-n+2) =$ (2 pont)
$(2n^2-2n-2(n^2-n+2), n^2-n+2) = (-4, n^2-n+2)$. (2 pont)
A kérdéses lnko tehát osztója -4-nek, azaz 1, 2 vagy 4 lehet. (1 pont)
Mivel n^2-n+2 mindig páros, az 1 nem jön szóba, (1 pont)

4 pedig pontosan akkor lesz a lnko, ha $n^2 - n$ maradéka 2 lesz 4-gyel osztva, (1 pont)
vagyis ha sem n, sem $n-1$ nem osztható 4-gyel (lévén ezek relatív prímek), azaz (mivel n páratlan) ha az n szám $4k+3$ alakú. (1 pont)
A keresett lnko tehát 2 a $4k+1$ alakú számokra és 4 a $4k+3$ alakú számokra. (1 pont)

A feladat valamivel egyszerűbben is megoldható, ha észrevesszük, hogy n és n^2-n+2 relatív prímek (mivel n páratlan), ekkor a keresett lnko $n^2 - n + 2$ és $n + 1$ lnko-jával lesz azonos.

3. Oldjuk meg a

$$21x \equiv 51 \pmod{111}$$

lineáris kongruenciát.

* * * * *

111 és 21 lnko-ja 3, ez osztja 51-et, tehát lesz megoldás (ha valaki csak eddig jut el, arra adhatunk 1 pontot), éspedig 3 darab modulo 111 (erre is adhatunk 1 pontot, ha valaki nem oldja meg a lineáris kongruenciát). A kongruenciát 3-mal osztva, az eredetivel ekvivalens

$$7x \equiv 17 \pmod{37}$$

kongruenciát kapjuk. (2 pont)
A jobboldalhoz 74-et adva

$$7x \equiv 91 \pmod{37},$$

(4 pont)

ezt 7-tel osztva az eredetivel ekvivalens

$$x \equiv 13 \pmod{37}$$

kongruencia adódik. (2 pont)
Innen a megoldások 13, 13+37=50 és 13+74=87 modulo 111. (2 pont)

Persze számos más módszerrel is megoldható a feladat, például (a 3-mal való osztás után) 5-tel szorozva vagy Euklideszi algoritmussal (innen hamar kiderül, hogy $16 \cdot 7 = 112$, azaz 16-tal érdemes szorozni a kongruenciát).

4. Határozzuk meg az összes olyan n számot, melyre

$$\varphi(n) = n - 3.$$

* * * * *

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 2. (2 pont)
Ha n-nek lenne két különböző prímosztója, p és q (feltehető, hogy $p < q$), (1 pont)
akkor p és q nem relatív prímek n-hez, sőt $2p$ sem, (2 pont)
így a feltétel nem teljesülhet, hiszen ezek a számok mind különbözőek és kisebbek n-nél. (1 pont)
n tehát prímhatvány, (1 pont)
legyen $n = p^\alpha$. Ekkor $n - 3 = \varphi(n) = p^\alpha - p^{\alpha-1}$, ahonnan $p^{\alpha-1} = 3$. (1 pont)
Innen $p = 3$, $\alpha = 2$, vagyis $n = 9$. (1 pont)
Erre valóban teljesül az egyenlőség és a fentiek szerint más ilyen n szám nincs. (1 pont)

Ha valaki megtalálja a 9-et, mint megoldást, de nem indokolja, hogy nincs más, az 1 pontot kapjon, aki belátja, hogy a prímhatványok között nincs más megoldás, az még 1-et, aki csak annyit mutat meg, hogy a prímek nem jók, annak nem jár pont.

5. Határozzuk meg $2011^{11^{24}}$ utolsó két számjegyét (a tízes számrendszerben).

* * * * *

A feladat $2011^{11^{24}}$ százzal való osztási maradékának meghatározása. Mivel 2011 és 100 relatív prímek (persze 2011 helyett lehet 11-gyel számolni, de ezért nem jár pont), (1 pont)
az Euler-Fermat tétel szerint

$$2011^{\varphi(100)} \equiv 1 \pmod{100}.$$

(1 pont)
$\varphi(100) = 40$, (1 pont)
így 11^{24} 40-nel való osztási maradékát kéne kiszámolnunk. (1 pont)
Mivel 11 és 40 relatív prímek, (1 pont)
az Euler-Fermat tétel szerint

$$11^{\varphi(40)} \equiv 1 \pmod{40}.$$

(1 pont)
$\varphi(40) = 16$, (1 pont)
tehát

$$11^{24} \equiv 11^8 \pmod{40}.$$

$11^2 = 121$, tehát

$$11^2 \equiv 1 \pmod{40},$$

ahonnan

$$11^8 \equiv 1 \pmod{40}.$$

(1 pont)
Így tehát

$$2011^{11^{24}} = 2011^{40k+1} = 2011^{40k} \cdot 2011 \equiv 2011 \equiv 11 \pmod{100},$$

(2 pont)
vagyis az utolsó két számjegy 11.

Természetesen $11^2 = 121$ miatt 11^{24} 40-nel való osztási maradéka Euler-Fermat nélkül is kiszámolható, a vonatkozó pontok persze ilyenkor is járnak.

6. Csoport, illetve félcsoport-e a következő struktúra? Az alaphalmaz az összes kenguruk és koalák halmaza, két kenguru szorzata (sorrendtől függetlenül) az idősebbik kenguru, két koala szorzata (sorrendtől függetlenül) az idősebbik koala, egy kenguru és egy koala szorzata pedig (sorrendtől függetlenül) a kenguru. (Tudjuk, hogy nincs két pontosan egyidős kenguru, sem két pontosan egyidős koala, bármely állat saját magával vett szorzata pedig - ha az eddigiekből nem lenne egyértelmű - saját maga.)

* * * * *

A megadott szorzás művelet, mivel az eredmény is kenguru vagy koala. (1 pont)
Világos, hogy a szorzás kommutatív (ezért a megfigyelésért alapvetően nem jár pont, hiszen közvetlenül egyik kérdés megválaszolásához sincs rá szükség, de a leírást sok helyen egyszerűsíti, így akik érdemben használják és nem kapnának 10 pontot a példára, azoknak adhatunk 1-et érte.)
Az asszociativitás is teljesül, ennek ellenőrzéséhez érdemes észrevenni, hogy ha a kengurukat mind idősebbnek feltételezzük a koaláknál és két állat szorzatát egyszerűen az idősebbikként adjuk meg, akkor pont a feladatbeli struktúrát kapjuk, így pedig az asszociativitás magától értetődő, hiszen

bármely 3 erszényes szorzata a zárójelezéstől függetlenül a legidősebb lesz közülük. (Természetesen az asszociativitás a fenti észrevétel nélkül, részletes esetvizsgálattal is ellenőrizhető.) (4 pont)
Az eddigiekből már következik, hogy a struktúra félcsoport. (1 pont)
Ahhoz, hogy eldöntsük, csoport is-e, elsőként az egységelem létezését kell vizsgálnunk. A definícióból könnyen adódik, hogy lesz egységelem, éspedig a legfiatalabb koala (nevezzük Beninek), (1 pont)
hiszen ezt bármely x erszényessel szorozva x-et kapjuk. (1 pont)
Most már vizsgálhatjuk az inverz létezésének kérdését: meg kéne állapítani, hogy bármely x erszényeshez létezik-e olyan y erszényes, mellyel x-et szorozva Benit kapjuk. (1 pont)
Könnyen látható, hogy ilyen nem létezik (kivéve, ha x épp maga Beni), hiszen a szorzat sosem fiatalabb a tényezőinél, a kérdéses struktúra tehát nem csoport. (1 pont)

Szigorúan véve azt is vizsgálni kellene, hogy a struktúra nem üres-e, hiszen ekkor félcsoport sem lehetne, de ennek hiányáért ne vonjunk le pontot. Ha az alaphalmaz egyelemű lenne, akkor nem csak félcsoport, hanem csoport is lenne a struktúra és érdemes azt is megfigyelni, hogy ha nincs koala, akkor a legfiatalabb kenguru lesz az egységelem.