Bevezetés a számításelméletbe II.
Zárthelyi feladatok megoldása
2007. április 26.

Ez a példamegoldás minden feladatra csak egy lehetséges megoldást ad, természetesen bármely más jó megoldást is elfogadunk. Ha hibát találtok valahol, azt kérlek jelezzétek nekem emailben! Köszönöm!

Schlotter Ildi

1. Egy 30 fős társaságban mindenki legalább 20 embert ismer a többiek közül (az ismeretségek kölcsönösek). Tudjuk, hogy bárhogyan választunk ki a társaság tagjai közül 4 embert, közülük kiválasztható 2 olyan, akik nem ismerik egymást. A társaság három tagja Bakács úr, Szakács úr és Takács úr. Bakács úr nem ismeri sem Szakács urat, sem Takács urat. Ismeri-e egymást Szakács úr és Takács úr?

Megoldás.

A feladatot modellezzük egy G gráffal, melynek csúcsai a társaság tagjainak felelnek meg, két csúcs pedig akkor van összekötve, ha a nekik megfelelő emberek ismerik egymást. A feladat szövege szerint G-nek 30 pontja van, és minden pontjának a foka legalább 20. Emiatt $|E(G)| \geq \frac{30 \cdot 20}{2} = 300$.

Ugyanakkor mivel tetszőleges 4 pontot kiválasztva biztos van köztük kettő, melyek nem szomszédosak, a gráfban nincs 4 méretű klikk, vagyis $\omega(G) \leq 3$. Ezért a Turán-tétel alapján $|E(G)| \leq |E(T_{30,3})|$, ahol $T_{30,3}$ a 30 pontú, 3 osztályú Turán-gráf. Ennek minden osztályában 10 pont van, így két tetszőleges pontosztály között 10^2 él fut. Innen rögtön adódik, hogy $|E(G)| \leq |E(T_{30,3})| = \binom{3}{2}10^2 = 300$. Ezt összevetve az előző becsléssel azt kapjuk, hogy $|E(G)| = 300$, ami a Turán-tétel szerint csak úgy lehetséges, ha G izomorf a megfelelő Turán-gráffal, azaz a $T_{30,3}$ gráffal.

Az, hogy Bakács nem ismeri sem Szakácsot, sem Takácsot, emiatt azt jelenti, hogy Bakács egy osztályban van Szakács és Takács urakkal is. Ekkor persze Szakács és Takács is egy osztályban vannak, tehát nem ismerik egymást.

2. Határozzuk meg az összes olyan pozitív egészt, amelyekre teljesül, hogy a (pozitív) osztóik száma 8 és a (pozitív) osztóik összege páratlan szám!

Megoldás.

Ha n prímtényezős felbontása $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, akkor n osztóinak száma $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$. Mivel jelen esetben ez a szorzat $8 = 4 \cdot 2 = 2 \cdot 2 \cdot 2$, ezért egy, a feladat szövegének megfelelő n szám prímtényezős felbontásának alakja csak háromféle lehet: p_1^7 vagy $p_1^3p_2$ vagy $p_1p_2p_3$.

Vizsgáljuk meg, hogy a három esetben hogy alakul az osztók száma.

a) $n = p_1^7$ esetén az osztók száma $(1 + p_1 + p_1^2 + p_1^3 + \dots + p_1^7)$. Ha p_1 páratlan, akkor ez 8 darab páratlan szám összege, ami páros. Emiatt p_1 nem lehet páratlan. Mivel az egyetlen páros prímszám a 2, ezért $n = 2^7$. Ekkor az osztók száma valóban páratlan, így ez a szám megfelelő.

b) $n = p_1^3p_2$ esetén az osztók száma $(1 + p_1 + p_1^2 + p_1^3))(1 + p_2)$. Ha p_2 páratlan, akkor ez persze páros. Ugyanakkor ha p_1 páratlan, akkor is páros lesz a szorzat, hiszen 4 páratlan szám összege páros. Ezért az osztók összege csak akkor lehetne páratlan, ha p_1 és p_2 két különböző páros prím lenne, ami nem lehetséges.

c) $n = p_1p_2p_2$ esetén az osztók száma $(1+p_1)(1+p_2)(1+p_3)$. Ennek a szorzatnak a tényezői akkor páratlanok, ha p_1, p_2 és p_3 is páros. Mivel azonban nincs 3 különböző páros prímszám, ezért ez az eset sem hoz be újabb megoldásokat.

Összefoglalva tehát az egyetlen megoldás a 2^7.

3. Valamely n egészre teljesül, hogy $18n$ és $n+1$ ugyanazt a maradékot adják 202-vel osztva. Mi lehet ez a közös maradék?

Megoldás.

A feladatot átfogalmazva azt kapjuk, hogy $18n \equiv n+1 \pmod{202}$. Ezt átrendezve kapjuk a következő kongruenciát:

$$\begin{aligned} 17n &\equiv 1 \pmod{202} && \text{Ezt 12-vel beszorozva:} \\ 204n &\equiv 12 \pmod{202} && \\ 2n &\equiv 12 \pmod{202} && \text{Ezt 2-vel elosztva:} \\ n &\equiv 6 \pmod{101 = 202/(202,2)} && \text{hiszen } (202,2) = 2. \end{aligned}$$

Innen $n \equiv 6$ vagy $n \equiv 107 \pmod{202}$. Vegyük észre, hogy a 12-vel való szorzás nem volt ekvivalens átalakítás, hiszen $(12, 202) \neq 1$. Emiatt bejöhettek hamis gyökök is a megoldás során, így a kapott ereményeket ellenőrizni kell.

$$\begin{aligned} 17 \cdot 6 = 102 \quad &\not\equiv 1 \pmod{202} && \text{tehát a 6 nem megoldás,} \\ 17 \cdot 107 = 1819 \quad &\equiv 1 \pmod{202} && \text{tehát a 107 megoldás.} \end{aligned}$$

A feladat kérdése $18n$ és $n+1$ közös maradéka volt modulo 202, ami a ezek szerint 108.

4. Legyen $n = 200704261601$. Határozzuk meg n^n utolsó három számjegyét!

Megoldás.

Egy szám utolsó három számjegye nem más, mint az 1000-rel vett osztási maradéka, így a feladat az $n^n \equiv x \pmod{1000}$ kongruencia megoldása.

Vegyük észre, hogy n utolsó számjegye 1, így sem 2-vel, sem 5-el nem osztható, emiatt $(n, 1000) = 1$. Ezért alkalmazhatjuk az Euler-Fermat-tételt úgy, hogy n az alap és 1000 a modulus. Ekkor persze szükségünk lesz $\phi(1000)$-re. Felhasználva, hogy $(2^3, 5^3) = 1$:

$$\phi(1000) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 \cdot 100 = 400.$$

Emiatt tehát az Euler-Fermat-tétel a következőt adja: $n^{\phi(1000)} = n^{400} \equiv 1 \pmod{1000}$. Ahhoz, hogy ezt fel tudjuk használni, szükségünk van a kitevő, azaz n maradékára modulo 400. Mivel $400 \mid 10000$, ezért $400 \mid 200704260000 = n - 1601$. Innen adódik, hogy $n = 200704260000 + 1600 + 1$ miatt $n \equiv 1 \pmod{400}$, vagyis n felírható $400k+1$ alakban valamely k egész számra.

Innen a kérdéses maradék meghatározása:

$$n^n = n^{400k+1} = n \cdot n^{400k} = n \cdot (n^{400})^k \equiv n \cdot 1^k = n \equiv 601 \pmod{1000}.$$

Vagyis n^n három utolsó számjegye 601.

5. Milyen maradékot ad a 36 legkisebb 23-mal osztható pozitív egész szám szorzata 37-tel oszva?

Megoldás.

A 36 legkisebb 23-mal oszható pozitív egész szám a következő: $23, 2 \cdot 23, 3 \cdot 23, \ldots, 36 \cdot 23$. Ezek szorzata apró átrendezés után $n = 36! \cdot 23^{36}$.

Mivel $(23, 37) = 1$ valamint a 37 prímszám, ezért az Euler-Fermat-tétel alapján $23^{\phi(37)} = 23^{36} \equiv 1 \pmod{37}$. Ismét kihasználva, hogy a 37 prím, a Wilson-tétel alapján meghatározhatjuk 36! maradékát is: $36! = (37-1)! \equiv -1 \pmod{37}$. Innen tehát a kérdéses maradék $36! \cdot 23^{36} \equiv (-1) \cdot 1 \equiv 36 \pmod{37}$.

6. Legyen $H = \mathbb{R} \setminus \{0\}$ a nullától különböző valós számok halmaza. Értelmezzük H-n a $*$ műveletet a következőképpen:

$$a * b = \begin{cases} a \cdot b, & \text{ha } a > 0, \\ a : b, & \text{ha } a < 0. \end{cases}$$

(Itt $\cdot$ és : a valós számok hagyományos szorzását és osztását jelölik. Így például $2 * 3 = 6$ és $(-4) * 5 = -\frac{4}{5}$.) Csoportot alkot-e H a $*$ műveletre nézve?

Megoldás.

Először ellenőrizzük, hogy a megadott $*$ művelet valóban művelet-e. Mivel két nemnulla valós számok kiindulva mind az osztás, mind a szorzás eredménye is nemnulla valós szám lesz, ezért a műveleti zártság teljesül.

Az asszociativitás nem triviális, hiszen az $(a * b) * c$ és $a * (b * c)$ eredménye függ a és b előjelétől. A négy lehetséges eset a következő:

a) Ha $a > 0$ és $b > 0$, akkor
$(a * b) * c = (a \cdot b) * c = (a \cdot b) \cdot c = abc$ és
$a * (b * c) = a * (b \cdot c) = a \cdot (b \cdot c) = abc.$

b) Ha $a > 0$ és $b < 0$, akkor
$(a * b) * c = (a \cdot b) * c = (a \cdot b) : c = \frac{ab}{c}$ és
$a * (b * c) = a * (b : c) = a \cdot (b : c) = \frac{ab}{c}.$

c) Ha $a < 0$ és $b > 0$, akkor
$(a * b) * c = (a : b) * c = (a : b) : c = \frac{a}{bc}$ és
$a * (b * c) = a * (b \cdot c) = a : (b \cdot c) = \frac{a}{bc}.$

d) Ha $a < 0$ és $b < 0$, akkor
$(a * b) * c = (a : b) * c = (a : b) \cdot c = \frac{ac}{b}$ és
$a * (b * c) = a * (b : c) = a : (b : c) = \frac{ac}{b}.$

Az asszociativitás tehát minden esetben teljesül.

Egységelemnek megfelel az 1 valós szám. Ehhez a következőket kell belátni: $a*1 = 1*a = a$ tetszőleges a elemre teljesül. Mivel $a \cdot 1 = a : 1 = a$, ezért $a * 1 = a$ igaz. Emellet $1 > 0$ miatt $1 * a = 1 \cdot a = a$ szintén teljesül.

Az inverz meghatározásánál külön kell kezelni a pozitív és a negatív számokat. Legyen $a^{-1} = a$, ha $a < 0$, ekkor valóban $a * a^{-1} = a^{-1} * a = a * a = a : a = 1$. Ha pedig $a > 0$, akkor legyen $a^{-1} = \frac{1}{a}$. Ekkor teljesül $a * a^{-1} = a \cdot \frac{1}{a} = a$, és hasonlóan mivel ekkor $\frac{1}{a} > 0$, ezért $a^{-1} * a = \frac{1}{a} \cdot a = a$ szintén igaz.

A megadott struktúra tehát csoport.

7. Legyen $(G, \cdot)$ egy tetszőleges csoport. Tegyük fel, hogy a csoport valamely három $a, b, c \in G$ elemére $a \cdot b = c$, $b \cdot c = a$ és $c \cdot a = b$ teljesül. Határozzuk meg az $a \cdot c \cdot b$ szorzat értékét!

Megoldás.

Keressük tehát azt az x elemét a csoportnak, melyre $x = a \cdot c \cdot b$. Ezt az egyenletet jobbról szorozva a következőt kapjuk: $x \cdot c = a \cdot c \cdot b \cdot c$. Felhasználva, hogy a csoportbeli művelet asszociatív, a megadott egyenlőségek alapján $x \cdot c = a \cdot c \cdot b \cdot c = a \cdot c \cdot a = a \cdot b = c$. A kapott $x \cdot c = c$ egyenletet jobbról c inverzével szorozva (erről tudjuk, hogy létezik) kapjuk, hogy $x = c \cdot c^{-1} = e$, ahol e a csoport egységeleme.

Megjegyzés: nagyon fontos, hogy itt csak olyan tulajdonságokat használtunk (asszociativitás, inverz létezése), melyek minden csoportban teljesülnek. Azt viszont nem tételezhetjük fel, hogy a csoport kommutatív is, így a szorzatokat átrendezni nem lehet!

8. Van-e a D_{15} diédercsoportnak
a) 8 elemű részcsoportja;
b) 10 elemű részcsoportja?

Megoldás.

A D_{15} csoport rendje 30, hiszen 15 tükrözést, és az identitáson kívül még 14 forgatást tartalmaz. A Lagrange-tétel alapján D_{15} tetszőleges részcsoportjának rendje osztója $|D_{15}| = 30$-nak, így persze nem lehet 8 elemű részcsoportja D_{15}-nek.

Vegyük észre, hogy 10 elemű részcsoport létét nem tiltja, de nem is igazolja a Lagrange-tétel. Meg tudjuk viszont adni egy lehetséges 10 elemű részcsoportját D_{15}-nek. Ehhez rögzítsük a 15 csúcsú szabályos sokszögünknek minden harmadik csúcsát, ezek egy szabályos ötszöget alkotnak. Könnyű látni, hogy azon D_{15}-beli transzformációk halmaza, melyek ezt a szabályos ötszöget helyben hagyják, épp egy 10 elemű részcsoportja lesz D_{15}-nek. Ennek oka, hogy ez a halmaz (a kompozícióra nézve) valójában izomorf a D_5 diédercsoporttal.