Bevezetés a számításelméletbe II.
Pótzárthelyi feladatok
2007. december 3.

1. A hurokélmentes G gráfra teljesül, hogy G nem 4-szeresen élösszefüggő, de bárhogyan húzunk be G-be egy új élet két különböző csúcs közé, a kapott gráf már 4-szeresen élösszefüggő lesz. Hány csúcsa és hány éle van G-nek? (Itt az új él behúzása azt jelenti, hogy G két meglévő, esetleg már eleve is szomszédos csúcsa közé veszünk fel egy új élet.)

2. Legyen G egy 2007 csúcsú gráf és jelöljük G szomszédossági mátrixát A-val. Tegyük fel, hogy az $A + A^3 + A^5 + \ldots + A^{2007}$ mátrix főátlójában álló számok összege 0. Bizonyítsuk be, hogy G páros gráf.

3. Oldjuk meg az alábbi egyenletet (vagyis adjuk meg az összes olyan n pozitív egész számot, amelyre az egyenlet fennáll)!

$$\varphi(n^2) = 20071203 \cdot \varphi(n)$$

4. Valamely n egészre teljesül, hogy $120n + 12$ és $27n + 40$ ugyanazt a maradékot adják 379-cel osztva. Milyen maradékot ad a $93n + 72$ szám 379-cel osztva?

5. Egy számtani sorozat első tagja 1, differenciája 72. (A sorozat tagjai tehát: 1, 73, 145, ...) Milyen maradékot ad a sorozat első 70 tagjának szorzata 71-gyel osztva?

6. Egy mértani sorozat első tagja 13, kvóciense 11. (A sorozat tagjai tehát: 13, 143, 1573, ...). Képzeletben szorozzuk össze a sorozat első 800 tagját. Mi a kapott szám utolsó 3 számjegye?

7. Legyen H a 4-gyel osztva 1 maradékot adó egész számok halmaza. Értelmezzük H-n a $*$ műveletet a következőképpen:

$$a * b = a + b - 5$$

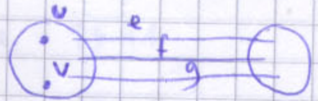
(Itt $+$ és $-$ az egész számok körében jól megszokott összeadást, illetve kivonást jelöli. Így például $9 * 17 = 21$.) Csoportot alkot-e H a $*$ műveletre nézve?

8. Legyen G egy véges csoport. Tegyük fel, hogy az e egységelemen kívül G-nek nincs olyan a eleme, amelyre $a*a = e$ teljesülne. Bizonyítsuk be, hogy G elemszáma páratlan. (Itt a G csoport műveletét $*$-gal jelöltük.)

A dolgozatra kérjük jól olvashatóan felírni a következő adatokat: név, Neptun-kód, Neptun szerinti gyakorlatvezető neve.

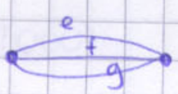
A feladatok megoldását indokolni kell, puszta eredményközlésért nem jár pont. A dolgozat megírása közben számológép (vagy más segédeszköz) nem használható.

1.) G nem 4-élösszefüggő, $\exists$ 3 db él, melyeket elhagyva G szétesik. T. f. h.



valamely komponens 2 pontú. (u, v)

Ha behúzok +1. élt (u-v között) 4 élösszefüggő lesz.
e, f, g elhagyásával továbbra is szétesik a gráf. ↯
$\Rightarrow \forall$ komponens 1 pontú



2 db csúcs 3 db él

Mivel csak ez felel meg.

2.)

A szomsz. mátrixa G-nek

$\Sigma = A + A^3 + A^5 + \ldots A^{2007}$ főátlójában lévő elemek összege 0.

$|V(G)| = 2007$

$\overset{\text{állítás}}{\Longrightarrow}$ G páros

Tudjuk, hogy A^k mátrixban az $a_{i,j}$ elem az i-j közötti séták száma. (k hosszú)

$\Sigma_{i,i} = A^1_{i,i} + A^3_{i,i} + \ldots + A^{2007}_{i,i} = 0$

↑

pl. 3 hosszú, i-n átmenő körséták száma ≥ 0

$\Rightarrow A^k_{i,i} = 0 \quad \forall$ ptln k-ra, ($k \leq 2007$)

Bármely csúcsra igaz, hogy a rajta átmenő páratlan hosszú körséták száma $= 0$ $\Rightarrow$ spec. nincs rajta átmenő páratlan kör $\Rightarrow \forall$ kör ps hosszú $\Rightarrow$ G páros gráf.

3.) $\varphi(n^2) = 2007\,1203 \cdot \varphi(n)$

Tudjuk, ha $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} \Rightarrow \varphi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)^k = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$

$\varphi(n^2) = 2007\,1203 \underbrace{\prod \left(1 - \frac{1}{p}\right) n}_{\varphi(n)}$

$\boxed{\begin{array}{c} \varphi(n^2) \neq \varphi(n) \cdot \varphi(n) \\ \text{miért?} \Downarrow \\ (n, n) \neq 1 \end{array}}$

$$n^2 \cdot \cancel{\prod}\left(1-\frac{1}{p}\right) = 20071203\, \cancel{n} \cancel{\prod}\left(1-\frac{1}{p}\right)$$

$$n = \underline{\underline{20071203}}$$

4.)

$120n + 12 \equiv 27n + 40 \quad (379)$ $\qquad$ $93n + 72 \equiv x \quad (379)$

$x = ?$

rendezve

$93n - 28 \equiv 0 \quad (379) \quad / +100$

$93n + 72 \equiv 100 \quad (379)$

5.)

$a_1 \quad 1$

$a_2 \quad 1 + 72$

a_3

$a_4 \quad 1 + 3 \cdot 72$

$\vdots$

$a_{70} = 1 + 69 \cdot 72$

$\vdots$

$\equiv 70 \quad (71)$

$\equiv 70! \quad (71)$

Wilson

ha p prim

$(p-1)! \equiv -1 \quad (p)$

$(71-1)! \equiv -1 \quad (71)$ mivel 71 prim

6.)

$a_1 = 13$

$a_2 = 13 \cdot 11$

$a_3 = 13 \cdot 11^2$

$a_{800} = 13 \cdot \cancel{11^{...}} 11^{799}$

$$\prod_{i=1}^{800} a_i = 13^{800} \cdot 11^0 \cdot 11^1 \cdot \ldots \cdot 11^{799} = 13^{800} \cdot 11^{\overset{400 \cdot 799 \text{ Gauss}}{0+1+\ldots 799}} = 13^{800} \cdot 11^{799 \cdot 400} \overset{?}{\equiv} x$$

(1000)

Euler – Fermat : ha $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1$ (m)

m: 1000

Tudjuk : $a^{\varphi(1000)} \equiv 1 \ (1000)$

$$\varphi(1000) = \varphi(2^3 \cdot 5^3) \underset{\uparrow \text{ multiplikatív}}{=} \varphi(2^3) \cdot \varphi(5^3) = (2^3 - 2^2) \cdot (5^3 - 5^2) = 400$$

$$\underbrace{(13^2)^{400}}_{\substack{\equiv \ (13^2, 1000) = 1 \\ 1}} \cdot \underbrace{(11^{799})^{400}}_{\substack{\equiv \ (11^{799}, 1000) = 1 \\ 1}} \equiv 1 \quad (1000)$$

$\Rightarrow$ az utolsó 3 számjegy <u>001</u>

7.)

$H = \{ x : x \equiv 1 \ (4) \}$ $(H, \times)$ csoport – e ? észrevétel: $\times$ komm

$a \times b := a + b - 5$

$\times$ nem vezet ki H- ból

$$\underbrace{\underbrace{a+b}_{\equiv\, 2(4)} \underbrace{-5}_{\equiv\, -1(4)}}_{\equiv\, 1\,(4)}$$

$\times$ asszoc. – e?

$(a \times b) \times c \overset{?}{=} a \times (b \times c)$

$(a + b - 5) + c - 5 = a + (b + c - 5) - 5$

$\exists$ egységelem azaz $e + a - 5 = a$

$e = 5 \in H$!

$\exists$ inverz

Kell $\forall\, a \in H$-ra $\exists\, a^{-1}$

$a \times a^{-1} = e$ és $a^{-1} \times a = e$

$a^{-1} + a - 5 = 5 \qquad a^{-1} = 10 - a \in H$

Tehát csoport.

8.) G véges csoport ha $a \neq e$, akkor $a \times a \neq e$

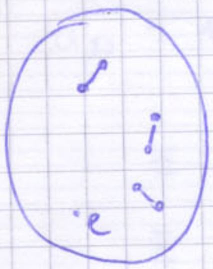
<u>Áll</u>: $|G|$ ptln (páratlan)

Feltétel: az egységen kívül nincs olyan elem, aminek önmaga az inverze.

Mivel G csoport, $\forall$ elemnek $\exists$ inverze. (pontosan 1 db) Ld. EA

Minden elemet párba állítunk a saját inverzével.

pl: $a \underset{inverz}{\overset{inverz}{\rightleftarrows}} b$



G

e-nek nincs párja, ld. feltétel $\Rightarrow$ páratlan sok.