

$$x \equiv 2 \pmod{3} \rightarrow x - \text{nr. } 3\text{-rul este } \text{atârni } m \text{ modulo } 2.$$

$$x = 3z + 2$$

$$3 \mid (x-2)$$

$$\text{Def } x \equiv a \pmod{m} \quad m \mid (x-a)$$

Teoremă

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_s \pmod{m_s} \quad (s \in \mathbb{Z}_F)$$

Ha m_1, m_2, m_s pairwise relatively prime or $M = m_1 \cdot m_2 \cdot \dots \cdot m_s = \prod_{i=1}^s m_i$

$$M_i = \frac{M}{m_i} = \prod_{j=1, j \neq i}^s m_j$$

$$M_i \cdot b_i \equiv 1 \pmod{m_i}$$

$$\text{soluția este: } x = M_1 \cdot b_1 \cdot a_1 + M_2 \cdot b_2 \cdot a_2 + \dots + M_s \cdot b_s \cdot a_s = \sum_{i=1}^s M_i b_i a_i$$

$$1) x \equiv 4 \pmod{5}$$

$$x \equiv 4 \pmod{7}$$

$$x \equiv 3 \pmod{8}$$

$$M_1 = m_2 \cdot m_3 = 7 \cdot 8 = 56$$

$$56 \cdot b_1 \equiv 1 \pmod{5}$$

$$b_1 \equiv 1 \pmod{5}$$

$$b_1 = 1$$

$$M_2 = 5 \cdot 8 = 40$$

$$40 \cdot b_2 \equiv 1 \pmod{7}$$

$$5b_2 \equiv 1 \pmod{7}$$

$$b_2 = 3$$

$$M_3 = 35$$

$$35 \cdot b_3 \equiv 1 \pmod{8}$$

$$3b_3 \equiv 1 \pmod{8}$$

$$b_3 = 3$$

$$x = (56 \cdot 1 \cdot 4) + (40 \cdot 3 \cdot 4) + (35 \cdot 3 \cdot 3) = 1019$$

$$2 \quad \begin{aligned} x &\equiv 5 \pmod{7} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 1 \pmod{11} \end{aligned}$$

$$M_1 = 4 \cdot 11 = 44$$

$$\begin{aligned} 44b_1 &\equiv 1 \pmod{7} \\ 2b_1 &\equiv 1 \pmod{7} \\ \underline{b_1} &= 4 \end{aligned}$$

$$M_2 = 77$$

$$\begin{aligned} 77b_2 &\equiv 1 \pmod{4} \\ 7b_2 &\equiv 1 \pmod{4} \\ \underline{b_2} &= 1 \end{aligned}$$

$$M_3 = 28$$

$$\begin{aligned} 28b_3 &\equiv 1 \pmod{11} \\ 6b_3 &\equiv 1 \pmod{11} \\ \underline{b_3} &= 2 \end{aligned}$$

$$44 \cdot 4 \cdot 5 + 77 \cdot 1 \cdot 3 + 28 \cdot 2 \cdot 1 = 839$$

$$\begin{aligned} 2x &\equiv 3 \pmod{5} \\ 3x &\equiv 5 \pmod{7} \\ 5x &\equiv 7 \pmod{8} \end{aligned}$$

$$\begin{aligned} 2x &\equiv 3 \pmod{5} & /3 \\ 6x &\equiv 9 \pmod{5} \\ 5x+x & \\ x &\equiv 4 \pmod{5} \end{aligned}$$

$$\begin{aligned} 3x &\equiv 5 \pmod{7} & /5 \\ 15x &\equiv 25 \pmod{7} \\ x &\equiv 4 \pmod{7} \end{aligned}$$

MEGO

$$\begin{aligned} 5x &\equiv 7 \pmod{8} \\ 25x &\equiv 35 \\ x &\equiv 3 \end{aligned}$$

$$\begin{aligned} 1, 2x &\equiv 4 \pmod{5} \\ 2x &\equiv 1 \pmod{3} \\ 3x &\equiv 4 \pmod{7} \end{aligned}$$

Állítás Legyen $n \in \mathbb{N}$ $a, b \in \mathbb{Z}$

Az $ax \equiv b \pmod{n}$ lineáris kongruencia akkor és csak akkor megoldható ha $d = (a, n)$ osztója $d | b$
 és $a \cdot d^{-1} \pmod{n}$

1, Van-e megoldása az alábbi kongruenciáknak?

a, $3x \equiv 5 \pmod{7}$

d, $14x \equiv 84 \pmod{21}$

b, $104x \equiv 74 \pmod{60}$

e, $26x \equiv 16 \pmod{34}$

c, $30x \equiv 48 \pmod{58}$

f, $40x \equiv 28 \pmod{62}$

a, $3x \equiv 5 \pmod{7}$

$d = ?$

$d = 3 \cdot 7 \text{ és } 0 \cdot 7 = 1$

$1/5 \checkmark \Rightarrow$ megoldható

b, $104x \equiv 74 \pmod{60}$

$d(104, 60)$

$$\begin{array}{r|l} 104 & 2 \\ 52 & 2 \\ 26 & 2 \\ 13 & 13 \\ 1 & \end{array}$$

$$\begin{array}{r|l} 74 & 2 \\ 37 & \end{array}$$

$$\begin{array}{r|l} 60 & 2 \\ 30 & 2 \\ 15 & 5 \\ 3 & 3 \\ 1 & \end{array}$$

$\left. \begin{array}{l} 2^3 \cdot 13 \\ 2^2 \cdot 5 \cdot 3 \end{array} \right\} \text{ és } a^2 = 4$

$4 | 74 \Rightarrow$ nincs megoldás

c, $30x \equiv 48 \pmod{58}$

$d(30, 58) = 2$

$$\begin{array}{r|l} 30 & 2 \cdot 3 \cdot 5 \\ 58 & 2 \cdot 29 \end{array}$$

$2 | 48$ megoldható

Def Legyen $n \in \mathbb{N}$ Legyen $f(n)$ -et a $0, 1, 2, \dots, n-2$ számok közül
az n -hoz relatív prímsámságú számok

$$(n_1 \text{ és } n_2 \text{ relatív prímsámságú ha } \text{lcm}(n_1, n_2) = 1)$$

A f függvénynek Euler tétele f függvényeinek nevezzük

pl $f(7) = 6$ db $\phi: 1, 2, 3, 4, 5, 6$
 $f(8) = 4$ db $\phi: 1, 3, 5, 7$

1, állítás Ha P prímsám akkor $f(P) = P-1$

2, állítás Ha $n \in \mathbb{N}$ prímszámok felbontása $n = p_1^{z_1} \cdot p_2^{z_2} \cdot \dots \cdot p_k^{z_k}$

$$\text{akkor } f(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$$

pl $f(36) = f(2^2 \cdot 3^2) = 2^2 \cdot 3^2 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 2^2 \cdot 3^2 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12$

$$f(104) = f(2^3 \cdot 13) = 2^3 \cdot 13 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{13}\right) = 2^3 \cdot 13 \cdot \frac{1}{2} \cdot \frac{12}{13} = 48$$

$$f(13) = 12 \text{ db}$$

1, Tétel (Fermat): Legyen $a \in \mathbb{Z}$, P egy adott prímsám, legyen $P \nmid a$ -t

$$\text{Ekkor } a^{P-1} \equiv 1 \pmod{P}$$

3, tétel (Euler tétele) Legyen $a \in \mathbb{Z}$ $n \in \mathbb{N}$ olyan, legyen $(a, n) = 1$
 akkor $a^{f(n)} \equiv 1 \pmod{n}$

pl $39^{17} \equiv ? \pmod{40}$

$$(39, 40) = 1$$

$$f(40) = 40 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 40 \cdot \frac{1}{2} \cdot \frac{4}{5} = 16$$

$$39^{f(40)} \equiv 1 \pmod{40}$$

$$\Downarrow$$

$$39^{16} \equiv 1 \pmod{40}$$

$$39^{17} \equiv 39 \pmod{40}$$

MF

$$39^{41} \pmod{100}$$

$$(39, 100) = 1$$

$$39^8 \pmod{16}$$

$$a) 39^{41} \equiv ? \pmod{100}$$

$$(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1$$

$$b) 39^8 \equiv ? \pmod{16}$$

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right)$$

$$\text{also } n = p_1^{k_1} \cdot p_2^{k_2}$$

$$g(39, 100) = 1$$

$$\left(\varphi(100) = \varphi(2^2 \cdot 5^2) = 2^2 \cdot 5^2 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 2^2 \cdot 5^2 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40 \right)$$

$$39^{40} \equiv 1 \pmod{100} \quad | \cdot 39$$

$$39^{41} \equiv 39 \pmod{100}$$

$$b) (39, 16) = 1 \Rightarrow 39^{\varphi(16)} \equiv 1 \pmod{16}$$

$$\varphi(16) = \varphi(2^4) = 2^4 \cdot \left(1 - \frac{1}{2}\right) = 2^4 \cdot \frac{1}{2} = 8 \quad 39^8 \equiv 1 \pmod{16}$$

$$a) 9^{17} \equiv ? \pmod{40}$$

$$(9, 40) = 1$$

$$\varphi(40) = \varphi(2^3 \cdot 5) = \begin{array}{r} 40 \\ 20 \\ 10 \\ 5 \end{array} \begin{array}{l} 2 \\ 2 \\ 2 \\ 5 \end{array}$$

$$= 2^3 \cdot 5 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 16$$

$$9^{\varphi(40)} \equiv 1 \pmod{40}$$

$$9^{16} \equiv 1 \pmod{40}$$

$$9^{17} \equiv 9 \pmod{40}$$

~~6/3~~

$$a) 5^{13} \equiv ?$$

$$5, 36 = 1$$

$$(\varphi(36) = \varphi(2^2 \cdot 3^2) = 2^2 \cdot 3^2 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12)$$

$$5^{12} \equiv 1$$

$$5^{13} \equiv 5 \pmod{36}$$

$$c) 7^8 \equiv ? \pmod{30}$$

$$7_{30} = 1 \quad 7^{f(30)} \equiv 1 \pmod{30}$$

$$f(30) = f(2 \cdot 3 \cdot 5) = 2 \cdot 3 \cdot 5 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8 \Rightarrow \underline{7^8 \equiv 1 \pmod{30}}$$

$$d) 7^{16} = 7^8 \cdot 7^8 = 1 \cdot 1 \equiv 1 \pmod{30}$$

$$e) 7^{33} \equiv ? \pmod{30}$$

$$7^{33} \equiv 7^{32} \cdot 7 = (7^8)^4 \cdot 7 \equiv 7 \pmod{30}$$

$$\equiv 1$$

$$3) a) 39^{390} \equiv ? \pmod{40}$$

$$b) 39^{39^{390}} \equiv ? \pmod{400}$$

$$a) 39^{390} \equiv ? \pmod{40}$$

$$\left. \begin{array}{l} f(40) = 16 \\ (39, 40) = 1 \end{array} \right\} \Rightarrow 39^{16} \equiv 1 \pmod{40}$$

$$390 : 16 = 24 \text{ remainder } 6$$

$$390 = 16 \cdot 24 + 6$$

$$39^{390} = 39^{16 \cdot 24 + 6} = (39^{16})^{24} \cdot 39^6 \equiv 39^6 \equiv (-1)^6 \equiv 1 \pmod{40}$$

$$b) 39^{39^{390}} \equiv ? \pmod{100}$$

$$\left. \begin{array}{l} (39, 100) = 1 \\ f(100) = 40 \end{array} \right\} \Rightarrow 39^{40} \equiv 1 \pmod{100}$$

$$39^{390} \equiv ? \pmod{40}$$

$$a) \Rightarrow 39^{380} \equiv 1 \pmod{40}$$

$$\Downarrow \\ 39^{380} = 40 \cdot M + 1 \quad (M \in \mathbb{N})$$

$$39^{39^{390}} = 39^{40 \cdot M + 1} = (39^{40})^M \cdot 39 \equiv 39 \pmod{100}$$

$$63^{493} \equiv ? \pmod{100}$$

$$(63, 100) = 1 \quad \left. \begin{array}{l} \\ \end{array} \right\} \rightarrow \text{Et} \quad 63^{40} \equiv 1 \pmod{100}$$

$$493^{640} \equiv ? \pmod{40}$$

$$\frac{493:40=12}{13}$$

$$493 = 40 \cdot 12 + 13$$

$$493^{640} \equiv 13^{640} \pmod{40}$$

$$(13, 40)$$

$$\varphi(40) = 2^3 \cdot 5 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 2^3 \cdot \frac{1}{2} \cdot \frac{4}{5} = 16 \quad \left. \begin{array}{l} \\ \end{array} \right\} \Rightarrow 13^{16} \equiv 1 \pmod{40}$$

$$13^{16} \equiv 1 \pmod{40}$$

$$493^{640} \equiv 13^{640} \quad \frac{640}{16} = 40$$

$$13^{16 \cdot 40} = [13^{16}]^{40} \equiv 1^{40} \pmod{40}$$

$$493^{640} = 40 \cdot M + 1$$

$$63^{493^{640}} \equiv 63^{40M+1} \equiv 63^{40M} \cdot 63 \equiv 63 \pmod{100}$$

LANCTÖRTEK

$$L = L_0 + \frac{1}{c_1 + \frac{1}{c_2 + \frac{1}{\ddots}}}$$

$$L = 0,7 \quad \downarrow \quad \{L\} = \frac{7}{10}$$

$$L_1 = \frac{10}{7}$$

$$L_1 = \frac{10}{7}$$

$$c_1 = \lfloor L_1 \rfloor = 1 \quad \{L_1\} = \frac{3}{7}$$

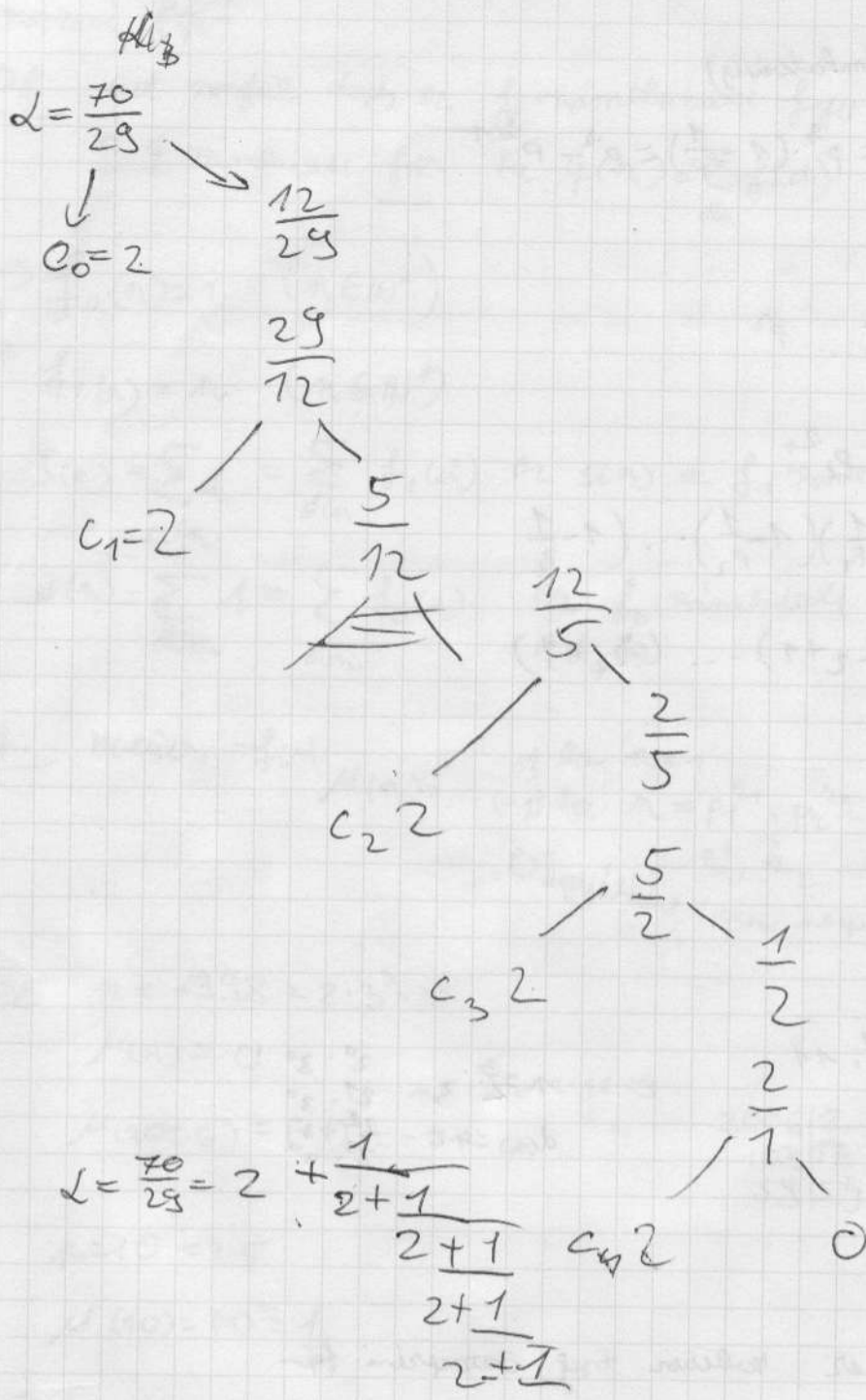
$$L_2 = \frac{7}{3}$$

$$c_2 = \lfloor L_2 \rfloor = 2$$

$$\{L_2\} = \frac{1}{3}$$

$$L_3 = 3 \quad \downarrow \quad c_3 = \lfloor L_3 \rfloor = 3 \quad L_3 = 0 \text{ vége}$$

$$L = 0,7 = \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}}$$



Számelméleti fegyver

Def Az $f: \mathbb{N}^* \rightarrow \mathbb{C}$ függvényeket számelméleti függvényeknek nevezzük

Megf: ett értendő alatt mindegy rendűn egész szárat kaptunk.

Def Legyen jelölje a $0, 1, 2, \dots, n-1$ számok az n -hez relatív prímos számok. Euler-féle ϕ -fgy.

$d(n)$ legyen az n osztóinak száma

$\sigma(n)$, $\phi(n)$ számelméleti fgy.

$$1, n = p^2 \quad (\text{primális})$$

$$\varphi(n) = ? = \varphi(p^2) = p^2 \cdot \left(1 - \frac{1}{p}\right) = p^2 - p^{2-1}$$

$$d(n) = ? = 2+1$$

$$1, p, p^2, p^3, \dots, p^2$$

$$2, n = p_1^{z_1} \cdot p_2^{z_2} \cdot \dots \cdot p_t^{z_t}$$

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_t}\right)$$

$$d(n) = (z_1 + 1) \cdot (z_2 + 1) \cdot \dots \cdot (z_t + 1)$$

$$n = 2^3 \cdot 3$$

$$d(n) = 4 \cdot 2$$

$$1, x = \frac{26}{135}$$

$$2, n = 2^5 \cdot 3^2 \cdot 11$$

$$\varphi(n) =$$

$$d(n) =$$

$$n = 2^3 \cdot 3$$

$$d(n) = 4 \cdot 2$$

$$\begin{array}{l} 2^0 \cdot 3^0 \\ 2^1 \cdot 3^0 \\ 2^2 \cdot 3^0 \\ 2^3 \cdot 3^0 \end{array}$$

Számelméleti függvény - az aritmetikai függvény összege

$S(n)$ - az n értékű összege

$$S(n) = \sum_{d|n} d$$

$$d(n) = \sum_{d|n} 1$$

Összegzési függvény

Def Azt mondjuk hogy az f számelméleti függvény összegzési függvénye a g számelméleti fv. ha $g(n) = \sum_{d|n} f(d)$

$$\rightarrow f_0(n) = 1 \quad (n \in \mathbb{N}^*)$$

$$f_1(n) = n \quad (n \in \mathbb{N}^*)$$

$$s(n) = \sum_{d|n} d = \sum_{d|n} f_1(d) \quad \text{Az } s(n) \text{ az } f_1 \text{ számelméleti függvény összegzési függvénye}$$

$$d(n) = \sum_{d|n} 1 = \sum_{d|n} f_0(d) \quad \text{Az } f_0 \text{ számelméleti függvény összegzési függvénye a } d(n)$$

Def: Möbius-függvény: $\mu(n) = \begin{cases} 1 & \text{ha } n=1 \\ (-1)^k & \text{ha } n = p_1^{z_1} \cdot p_2^{z_2} \cdot \dots \cdot p_k^{z_k} \text{ - en} \\ & z_1, z_2, \dots, z_k \leq 1 \end{cases}$
 0 egyébként (vagy nem prímszám osztója)

pl $n = 1998 = 2 \cdot 3^3 \cdot 37$

$$\mu(n) = 0$$

$$\mu(2006) = (-1)^3 = -1 \quad n = 2006 = 2 \cdot 17 \cdot 59$$

$$\begin{array}{r} 2006 \overline{) 2} \\ 1003 \overline{) 17} \\ 59 \overline{) 59} \end{array}$$

$$n = 10 = 2 \cdot 5$$

$$\mu(10) = (-1)^2 = 1$$

Def: Egy $f(n)$ számelméleti függvény Möbius transzformáció

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$$

Tétel Möbius-féle megfordítási tétel

Ha az $(f(n))$ számelméleti függvény összegzési függvénye a $g(n)$ függvény

$(g(n) := \sum_{d|n} f(d))$ akkor a $g(n)$ függvény Möbius transzformációja

3. Ha f és g számelméleti transzformációk akkor az f függvény

$$(f(n)) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot g(d)$$

$$\text{HF} \quad \begin{array}{cc} 1, n=8 & 2=36 \\ f(n) & f(n) \\ d(n) & d(n) \\ \mu(n) & \mu(n) \end{array}$$

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) \quad \text{or } n = p^2 \text{ esetén}$$

\downarrow
ostói

Def: Azt mondjuk f és g aritmetikai függvények, ha minden $n, m \in \mathbb{N}^+$ helyére $(n, m) = 1$ teljesül: $f(n \cdot m) = f(n) \cdot f(m)$

f multiplikatív

μ - is

d, s - is

Állítás: Ha f multiplikatív aritmetikai függvény, akkor az $af(n) = \sum_{d|n} f(d)$ aritmetikai függvény

$af(n) = \sum_{d|n} f(d)$ aritmetikai függvény

Állítás: Ha f és g multiplikatív aritmetikai függvények, akkor az $h(n) = f(n) \cdot g(n)$ is multiplikatív aritmetikai függvény.

Bizs: $f(n) = f(p_1^{z_1}) \cdot f(p_2^{z_2}) \cdot \dots \cdot f(p_t^{z_t})$

$$f(n) = f(p_1^{z_1} p_2^{z_2} \dots p_t^{z_t}) = f(p_1^{z_1}) \cdot f(p_2^{z_2}) \cdot \dots \cdot f(p_t^{z_t})$$

hiszen $p_1^{z_1}, p_2^{z_2}, \dots, p_t^{z_t}$ párhuzamosak egymással

1. Számítsuk ki az f összegét

$$g(n) = \sum_{d|n} f(d) = ?$$

f multiplikatív

\downarrow Munkamezői függetlenek, így a multiplikatív

$g(n)$ is

\downarrow

g -t eleve nem lehet számítani

$$p^2: g(p^2) = \sum_{d|p^2} f(d)$$

$$p^2 \text{ ostói } d \in \{1, p, p^2\}$$

$$f(1) = 1$$

$$f(p) = p - 1 = p \cdot \left(1 - \frac{1}{p}\right) \quad 1, 2, \dots, p$$

$$f(p^2) = p^2 \left(1 - \frac{1}{p}\right) = p^2 \cdot \frac{p-1}{p} = p^2 \cdot \left(1 - \frac{1}{p}\right)$$

$$f(p^2) = p^2 \cdot \left(1 - \frac{1}{p}\right) = p^2 \cdot \frac{p-1}{p} = p^2 \cdot \left(1 - \frac{1}{p}\right)$$

$$\left[\begin{array}{l} f \xrightarrow{\text{om}} g \xrightarrow{\text{Möbius}} f \\ g \xrightarrow{\text{Möbius}} h \xrightarrow{\text{om}} g \end{array} \right]$$

1/ f_0 özeqürü fqr $\rightarrow f_1(n) = n \quad (n \in \mathbb{N}^*)$

$$1) f \xrightarrow{\text{om}} f_1 \xrightarrow{\text{Möbius}} f$$

ayrur ney or $f_1(n) = n$ fqr Möbius transf. $|f|$

2/ Tuduqa lqy or $S(n) = \sum_{d|n} d = \sum_{d|n} f_1(d)$ fqr or f_1 fqr-ney or özeqürü fqr-e ayrur ney or $S(n)$ Möbius transformalr

$$f_1 \xrightarrow{\text{om}} S(n) \xrightarrow{\text{Möbius}} f_1(n)$$

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) S(d) = n \quad \underline{\underline{f_1(n) = n}}$$

3/ tuduqa lqy or $d(n) = \sum_{d|n} 1 = \sum_{d|n} f_0(d)$ fqr or f_0 fqr-ne özeqürü fqr-e ayrur or $d(n)$ Möbius transf.-r

$$f_0 \xrightarrow{\text{om}} d(n) \xrightarrow{\text{Möbius}} f_0$$

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) d(n) = 1$$

4/ lqy or lqy

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot d = f(n)$$

I nqy or

$$f(n) \xrightarrow{\text{özeqürü}} f_1(n) \xrightarrow{\text{Möbius}} f(n)$$

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot f_1(d) = f(n)$$

II rész 1. lépés

• μ multiplikatív

$$f_1(d) = d \text{ multiplikatív } \left(f_1(n \cdot m) = n \cdot m = f_1(n) \cdot f_1(m) \right) \Rightarrow \mu f_1 \text{ multiplikatív}$$

2. lépés

• Mivel multiplikatív a μ és f_1 multiplikatív, ezért a $h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot f_1(d)$ is multiplikatív

3. lépés

Első lépésben számoljuk ki:

$$h(p^2) = \sum_{d|p^2} \mu\left(\frac{p^2}{d}\right) f_1(d) = 0 + 0 + \dots + 0 + (-1) \cdot p^2 + 1 \cdot p^2 = p^2 - p^2 = 0$$

$$p^2 \text{ osztói: } 1, p, p^2, \dots, p^2$$

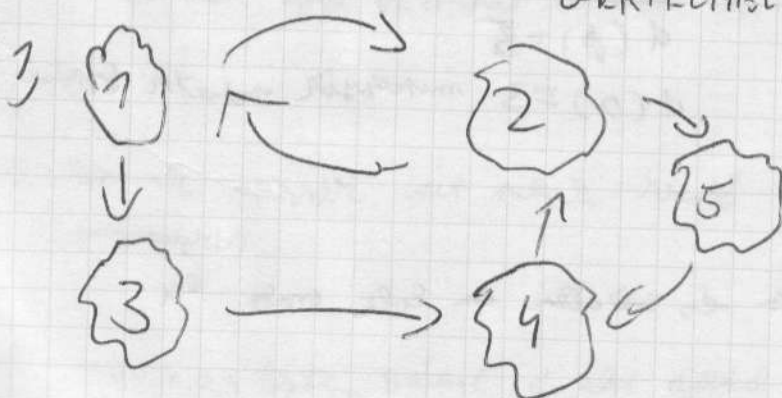
$d=1$	$\frac{p^2}{d} = p^2$	$\mu\left(\frac{p^2}{d}\right) = 0$
$d=p$	$\frac{p^2}{d} = p$	$\mu\left(\frac{p^2}{d}\right) = 0$

$d=p^{2-1}$	$\frac{p^2}{d} = p$	$\mu\left(\frac{p^2}{d}\right) = -1$	$(-1)^s \text{ ahol } s=1$
$d=p^2$	$\frac{p^2}{d} = 1$	$\mu\left(\frac{p^2}{d}\right) = 1$	

$$f(n) = f(p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_t^{a_t}) = f(p_1^{a_1}) \cdot f(p_2^{a_2}) \cdot \dots \cdot f(p_t^{a_t}) =$$

$$= p_1^{a_1} \cdot 1 \cdot \left(-\frac{1}{p_1}\right) \cdot p_2^{a_2} \cdot \left(-\frac{1}{p_2}\right) \cdot \dots \cdot p_t^{a_t} \cdot \left(-\frac{1}{p_t}\right) = f(n)$$

GRÁFELMŐLET



az élekkel leírt állapotok közötti átmeneteket

az állap

a, áll és állat 4

b, áll és állat 1

az áll és állat

az áll és állat

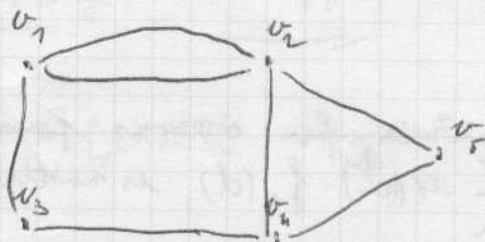
az áll és állat

c, mi a mai állat és állat a mai állat

az áll és állat

Def: Graf alatt n csomópont és m éllel érthetjük

Def Egy (súsz) pont v fokszáma a gráfrészletre G_v alatt $d(v)$



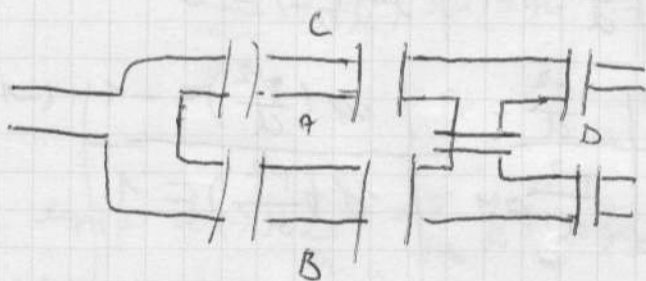
$$d(v_1) = 3$$

$$d(v_2) = 4$$

Def Euler körrel (körút) alatt egy olyan zárt útunk mely a graf minden élét pontosan 1-szer tartalmazza

2. A gráfelméleti kisebb problémák

Összekapcsolható-e két pont a gráfban? Ha igen, akkor a gráfban van-e út a két pont között?



$$d(A) = 3$$

$$d(B) = 3$$

$$d(C) = 5$$

$$d(D) = 3 \text{ miniszor is meglátjuk}$$

III

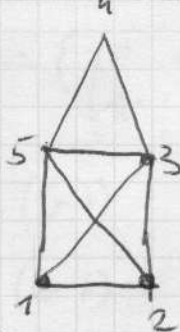
Tétel: Egy gráfban akkor és csak akkor van Euler kör, ha

→ $d(v) = 2$ minden v esetén

és

→ G összefüggő

3

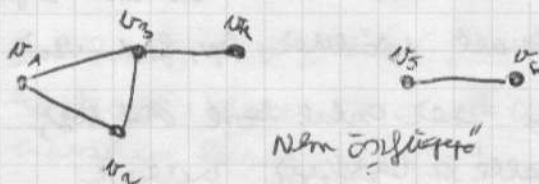


$$1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 3 \rightarrow 1 \rightarrow 5 \rightarrow 2$$

Égér vörlet vörlet: A v_1, v_2 vörletével vörlet sörst fepör
 rör i f p vörlet vörlet v_1, v_2 - t vörlet vörlet

Def Égér f p vörlet vörlet la vörlet sörst f p vörlet
 vörlet vörlet

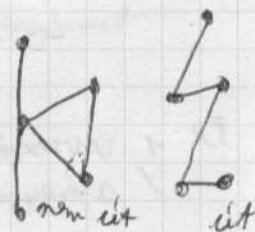
Pl



Hörlet vörlet vörlet

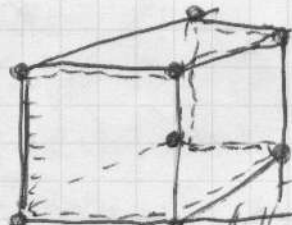
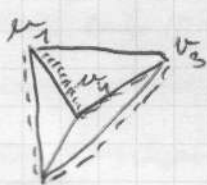
Def Égér f p vörlet vörlet vörlet 1x vörlet vörlet
 vörlet 1 f p vörlet vörlet vörlet 1x vörlet vörlet
 vörlet vörlet

Def vörlet vörlet vörlet vörlet vörlet vörlet
 vörlet vörlet vörlet vörlet vörlet vörlet



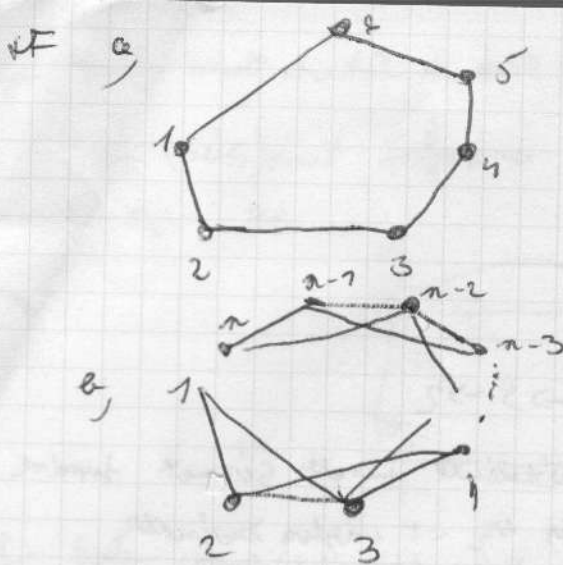
Def vörlet vörlet vörlet vörlet vörlet vörlet
 vörlet vörlet.

1. vörlet vörlet vörlet vörlet vörlet vörlet
 vörlet vörlet vörlet vörlet vörlet vörlet



v_1, v_2 Hörlet $(v_1, v_2) \rightarrow (v_2, v_3) \rightarrow (v_3, v_4) \rightarrow (v_4, v_1)$
 $\rightarrow v_1, v_2$

Hörlet



H -szár }
 H -út ,

c) Isolated tulajdonság minden n-re: minden n-re létezik olyan legfeljebb 2 elemű halmazok egy felszámolható halmazán, le egy, ezek közül kettő az az, egy ~~minden~~ n -es halmaz mellett a tesséké n -es halmaz.

CSOPORTOK

Def: adott a G halmaz és legyen \circ egy minden művelet a G -n az-az a művelet nem vet ki a G -ből

$A(G, \circ)$ egy csoport ha

\rightarrow a művelet asszociatív

$$(a \circ b) \circ c = a \circ (b \circ c)$$

\rightarrow egységelem létezése

$$\exists e \in G \quad a \circ e = e \circ a = a$$

\rightarrow inverzum létezése

$$\forall a \in G \quad \exists a^{-1} \in G \text{ úgy, hogy } a \circ a^{-1} = a^{-1} \circ a = e$$

Pé 1. Vizsgáljuk meg, hogy melyek a csoportok az alábbi halmazok a megadott művelettel?

a) $(\mathbb{R}, +)$

b) $(\mathbb{Z}, +)$

c) (\mathbb{Z}, \cdot)

d) (\mathbb{R}, \cdot)

e) $(\mathbb{R} \setminus \{0\}, \cdot)$

f) $G = \{\pm 1, \pm i\}$

(G, \cdot)

$$g \quad G = \left\{ \begin{pmatrix} p & q \\ r & 1 \end{pmatrix} : p, q, r \in \mathbb{Q} \right\}$$

$$(G, \cdot)$$

$$(G, +)$$

$$h \quad G = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

$$(G, +)$$

$$(G, \cdot)$$

$$1/a) \rightarrow \forall a, b \in \mathbb{R} \quad a+b \in \mathbb{R} \quad \checkmark$$

$$\rightarrow \text{assziativitás} \quad \forall a, b, c \in \mathbb{R} \quad (a+b)+c = a+(b+c) \quad \checkmark$$

$$\rightarrow \text{egységelem: } e=0 \quad a+0=a \quad \forall a \in \mathbb{R} \quad \checkmark$$

$$\rightarrow \text{inverzsem elvise} \quad \forall a \in \mathbb{R} \quad a^{-1} = -a \quad \text{valleplese} \\ a+a^{-1} = a^{-1}+a = 0 \quad \checkmark$$



$(\mathbb{R}, +)$ csoport

$$1/c \quad e=1 \quad \checkmark$$

$$\rightarrow \text{nincs inverzsem az } a \neq 1 \text{ } a \in \mathbb{Z} \text{ -hez } \nexists a^{-1} \in \mathbb{Z} \quad a \cdot a^{-1} = 1$$

∇
nem csoport

$$1/d \rightarrow a, b \in \mathbb{R} \quad a \cdot b \in \mathbb{R} \quad \checkmark$$

$$\rightarrow \text{assziativitás} \quad \checkmark$$

$$\rightarrow \text{egységelem } e=1 \quad \checkmark$$

$$\rightarrow \text{inverzsem elvise}$$

$$a=0 \quad \text{nincs inverzsem}$$

∇
nem csoport

$$1/e \rightarrow a, b \in \mathbb{R} \quad a \cdot b \in \mathbb{R} \quad \checkmark$$

$$\rightarrow \text{assziativitás} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \checkmark$$

$$\rightarrow \text{egységelem } e=1 \quad \exists 1 \in \mathbb{R} \quad \forall a \in \mathbb{R} \quad a \cdot 1 = a \quad 1 \cdot a = a \quad e=1$$

$$\rightarrow \text{inverzsem} \quad a=1 \text{ van inverzsem} \quad \checkmark \quad \exists a^{-1} = \frac{1}{a} \quad a \neq 0 \quad a \cdot a^{-1} = a^{-1} \cdot a = 1$$

$$\begin{aligned} 1/f &\rightarrow \text{nem v\u00e9rt mi? } (+1) \cdot (-1) = -1 \\ &(+1) \cdot i = i \\ &(-1) \cdot (-1) = +1 \in G \dots \end{aligned}$$

$$\rightarrow \text{asszi\u00f3ci\u00e1t\u00edv} \quad \forall a, b, c \in G \quad (a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \checkmark$$

$$\rightarrow \text{egys\u00e9gsem} \quad e = 1 \in G \quad \forall a \in G \quad a \cdot 1 = a$$

\rightarrow inverz

$$\begin{aligned} 1 &\rightarrow 1 \\ -1 &\rightarrow -1 \\ i &\rightarrow -i \\ -i &\rightarrow i \end{aligned}$$



GEOPONT

Def. Azt mondjuk hogy $a(G, \circ)$ csoport akkor ha a nem v\u00e9rt
 \u00e9s a G -b\u00e9l (= egy n\u00e9vel a G -ben van)

$$\rightarrow \circ \text{ asszi\u00f3ci\u00e1t\u00edv} \quad \forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$$

$$\rightarrow \text{egys\u00e9gsem} \quad \text{l\u00e9tezik } \exists e \in G : a \circ e = e \circ a = a$$

$$\rightarrow \text{inverz} \quad \text{l\u00e9tezik } \forall x \in G \quad \exists x^{-1} \in G : x \circ x^{-1} = x^{-1} \circ x = e \quad \forall a \in G$$

Def. $A(G, \circ)$ csoport kommutativ csoport (Abel-f\u00e9le csoport) akkor ha
 \u00e9s n\u00e9vel $\forall a, b \in G \quad a \circ b = b \circ a$

~~R\u00e9szletek:~~

Def: Azt mondjuk hogy (M, ρ) struktur\u00e1l n\u00e9rzem\u00e9nt $a(G, \circ)$

$$\text{csoportnak ha } \rightarrow \emptyset \neq M \subseteq G$$

$$\rightarrow (M, \rho) \text{ csoport akkor}$$

$$\text{PL \u00e9l\u00e9t\u00e1s: } (M, \rho) \text{ n\u00e9rzem\u00e9nt } (G, \circ) \text{-n } \Leftrightarrow \begin{cases} \forall a, b \in M \Rightarrow a \circ b \in M \\ \forall a \in M \Rightarrow a^{-1} \in M \end{cases}$$

$$1, G = \{\pm 1, \pm i\} \quad (G, \circ) \quad i^2 = -1$$

(K\u00e9rd\u00e9s) Cayley-f\u00e9le t\u00e1bl\u00e1zat

\circ	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Sz\u00e9nt.

Van inverz

\overline{I}

$$\rightarrow \text{f\u00e9lt\u00e9len szimmetrikus } \Leftrightarrow a \circ b = b \circ a$$

$$\text{Van egys\u00e9gsem } e = 1$$

$$M = \{+1, -1\}$$

M = Menge der (b, c) -ner

Def $A(G, \circ)$ ist eine Gruppe wenn a, b beliebige Elemente sind für alle $|G|$

A ist eine Gruppe wenn $|G| < +\infty$

~~FEAD~~ BONTOUT FEADATOR

Gruppe?

1, $(\mathbb{N}, *)$ wobei $x * y = x \cdot y - x + y$

2, (\mathbb{N}, \oplus) wobei $x \oplus y = x \cdot y + x + y$

③ (\mathbb{N}, \odot) wobei $x \odot y = x$ \rightarrow non kommutativ, assoziativ, neut. Element

④ (\mathbb{R}, \diamond) wobei $x \diamond y = 3x + 2y$ $\rightarrow \equiv$

5 (\mathbb{R}, \boxplus) wobei $x \boxplus y = x + y - 1$

6 (\mathbb{N}, \ominus) wobei $x \ominus y = x + y - xy$

⑦ $K = \{a + b\sqrt{5}; a, b \in \mathbb{Z}\}$

$(K, +)$ (K, \cdot)

1, $(\mathbb{N}, *)$ wobei $x * y = x \cdot y - x + y$

\rightarrow * ist eine Verknüpfung auf \mathbb{N}

$$\forall x, y \in \mathbb{N} \quad x * y = x \cdot y - x + y \in \mathbb{N}$$

Per $y=0 \quad x=1$

\rightarrow assoziativ

$$\begin{aligned} (a * b) * c &= (a \cdot b - a + b) * c = (a \cdot b - a + b) \cdot c - (a \cdot b - a + b) + c = \\ &= a \cdot b \cdot c - a \cdot c + b \cdot c - a \cdot b + a - b + c = \\ a * (b * c) &= a * (b \cdot c - b + c) = a \cdot (b \cdot c - b + c) - a + b \cdot c - b + c = \\ &= a \cdot b \cdot c - a \cdot b + a \cdot c + b \cdot c - a - b + c \end{aligned}$$

Nun assoziativ.

\rightarrow neutrales Element

$$\exists e \in \mathbb{N} \quad e * a = a * e = a$$

$$\text{I} \quad e \cdot a - e + a = a$$

$$e \cdot (a - 1) = 0$$

$$e = 0$$

$$\text{II} \quad a + e = a$$

$$a \cdot e - a + e = a$$

$$-a = a \quad \text{II}$$

nicht annehmen, \Rightarrow nicht möglich

$$2, (\mathbb{N} \oplus) \quad x \oplus y = x \cdot y + x + y$$

$$\rightarrow \oplus \text{ nem vezet } \exists i \in \mathbb{N} \text{ s\ddot{u}l} \quad x \oplus y = xy + x + y \in \mathbb{N}$$

$$(a \oplus b) \oplus c = (a \cdot b + a + b) \oplus c = (a \cdot b + c + b)c + (a \cdot b + a + b) + c =$$

$$a \oplus (b \oplus c) = a \oplus (bc + b + c) = a \cdot (bc + b + c) + a + bc + b + c =$$

$$\rightarrow e \cdot a + e + a = a$$

$$e \cdot (a+1) = 0$$

$$\boxed{e=0}$$

Vegyesen

\rightarrow inverzen

$$\forall a \in \mathbb{N} \text{ s\ddot{u}l} \exists a^{-1} \in \mathbb{N}$$

$$a \oplus a^{-1} = 0$$

$$a \cdot a^{-1} + a + a^{-1} = 0$$

$$a^{-1} \cdot (a+1) = -a$$

$$a^{-1} = \frac{-a}{a+1} > 0 \} \notin \mathbb{N}$$

\downarrow

nincs inverz

$$\text{ - kommutativ } x \oplus y = y \oplus x$$