

$$M_1 = \frac{M}{m_1} = m_2 \dots m_{s-1}, \quad M_s = \frac{M}{m_s} = m_1 \dots m_{s-1}$$

Képezzük olyan $b_1 \dots b_s$ számokat amik $M_1 b_1 \equiv 1 \pmod{m_1}, \dots, M_s b_s \equiv 1 \pmod{m_s}$

vagy a kongruenciák
létezését megmutatjuk

$$\text{L.H.C. } (m_i, M_i) = 1$$

és az előző
lehet $b_1 \dots b_s$ létezik.

$$x_0 \equiv a_1 b_1 M_1 + \dots + a_s b_s M_s$$

Állítás: x_0 a kongruenciák minden egy megfogalmazása

Bar helyettesítve x_0 -t a kongruenciákba

$$x_0 \stackrel{1}{\equiv} a_1 \pmod{m_1}$$

$$x_0 \stackrel{2}{\equiv} a_s \pmod{m_s}$$

$$x_0 = a_1 b_1 M_1 + \underbrace{a_2 b_2 M_2 + \dots + a_s b_s M_s}_{\substack{\equiv 0 \\ \pmod{m_1} \\ m_1 | M_2}} \quad \underbrace{\quad}_{\substack{\equiv 0 \\ \pmod{m_s} \\ m_s | M_1}}$$

$$x_0 \equiv a_1 \underbrace{b_1 M_1}_{\equiv 1} \pmod{m_1}$$

$$x_0 \equiv a_1 \pmod{m_1}$$

többi lozenedem

Állítás: Ha x_0, x_1 megoldások a rendszerre akkor
 $x_0 \equiv x_1 \pmod{M}$

Biz.: tudjuk hogy

$$x_0 \equiv a_1 \pmod{m_1} \quad x_1 \equiv a_1 \pmod{m_1}$$

$$x_0 \equiv a_s \pmod{m_s} \quad x_1 \equiv a_s \pmod{m_s}$$

$$\left. \begin{array}{l} x_1 - x_0 \equiv 0 \pmod{m_1} \\ x_1 - x_0 \equiv 0 \pmod{m_s} \end{array} \right\} \begin{array}{l} m_1 \mid (x_1 - x_0) \dots m_s \mid (x_1 - x_0) \\ \Rightarrow m_1 \dots m_s \mid (x_1 - x_0) \end{array}$$

$$M \mid (x_1 - x_0) \Rightarrow x_0 \equiv x_1 \pmod{M}$$

I Példa

$$s=4$$

$$m_1=4 \quad m_2=3 \quad m_3=5 \quad m_4=7$$

$$a_1=-1 \quad a_2=1 \quad a_3=5 \quad a_4=2$$

$$\left. \begin{array}{l} x \equiv -1 \pmod{4} \\ x \equiv 1 \pmod{3} \\ x \equiv 5 \pmod{5} \\ x \equiv 2 \pmod{7} \end{array} \right\}$$

m_1, m_2, m_3, m_4 páronként relatív prímek.

$$\binom{4}{2} = 6 \text{ ellendöntést jelent}$$

$$M = 4 \cdot 3 \cdot 5 \cdot 7 = 420$$

i	a_i	m_i	M_i	b_i	$a_i b_i m_i$	$M_i b_i \equiv 1 \pmod{m_i}$
1	-1	4	105	1	-105	$M_1 b_1 \equiv 1 \pmod{m_1}$
2	1	3	140	-1	-140	$105 b_1 \equiv 1 \pmod{4}$
3	5	5	84	-1	-420	$b_1 \equiv 1 \pmod{4}$
4	2	7	60	2	120	$M_2 b_2 \equiv 1 \pmod{m_2}$
					± 240	$140 \cdot b_2 \equiv 1 \pmod{3}$
					-425	$2 \cdot b_2 \equiv 1 \pmod{3}$
						$-b_2 \equiv 1 \pmod{3}$
						$b_2 \equiv -1 \pmod{3}$
						$b_2 \equiv 2$

$$x_0 = -425 \text{ nem teljesít a negatív szám}$$

$$x_0 = 415 \text{ és } 0 \text{ és } 419 \text{ zéró zéró}$$

$415 + 420 \cdot 2$ a többi megoldás

$$\begin{aligned} 11 b_1 &\equiv 1 \pmod{m_1} \\ 60 b_1 &\equiv 1 \pmod{7} \\ 4 b_1 &\equiv 1 \pmod{7} \\ b_1 &\equiv 2 \pmod{7} \end{aligned}$$

$$\begin{aligned} M_3 b_3 &\equiv 1 \pmod{m_3} \\ 84 b_3 &\equiv 1 \pmod{5} \\ 4 b_3 &\equiv 1 \pmod{5} \\ -b_3 &\equiv 1 \pmod{5} \\ b_3 &\equiv -1 \end{aligned}$$

ELL:

$$\begin{aligned} 415 &\equiv -1 \pmod{4} \\ 415 &\equiv 1 \pmod{3} \\ 415 &\equiv 5 \pmod{5} \\ 415 &\equiv 2 \pmod{7} \end{aligned}$$

$$\begin{aligned} 4 | 415 &\checkmark \\ 3 | 414 &\checkmark \\ 5 | 410 &\checkmark \\ 7 | 413 &\checkmark \end{aligned}$$

II. Problem

$$S = 4$$

$$\begin{aligned} m_1 &= 100 & m_2 &= 343 & m_3 &= 121 & m_4 &= 299 \\ a_1 &= 50 & a_2 &= -15 & a_3 &= 26 & a_4 &= 102 \end{aligned}$$

$$M = 100 \cdot 343 \cdot 121 \cdot 299 = 1240938700$$

i	a_i	m_i	M_i	b_i
1	50	100	12409387	93
2	-15	343	3617900	-134
3	26	121	10255700	47
4	102	299	4150300	

$$12409387 \cdot b_1 \equiv 1 \pmod{100}$$

$$97 \cdot b_1 \equiv 1 \pmod{100}$$

$$97 \cdot b_1 + 100y = 1$$

100	97	1	-32	33
97	3	32	1	-32
3	1	3	0	1
1	0	1	1	0

$$(97)(33) + (100)(-32) = 1$$

$$3617900 \cdot b_2 \equiv 1 \pmod{343}$$

$$279 \cdot b_2 \equiv 1 \pmod{343}$$

$$(279)(-134) + (343)(109) = 1$$

$$\begin{aligned} &37386 \\ &-37386 \\ &37387 \end{aligned}$$

$$279 \cdot b_2 + 343y = 1$$

343	279	1	109	-134
279	64	4	-25	109
64	23	2	3	-25
23	18	1	-7	9
18	5	3	-1	-7
5	3	1	1	-1
3	2	1	1	0
2	1	1	1	0

$$10255700 \cdot b_3 \equiv 1 \pmod{121}$$

$$103 \cdot b_3 \equiv 1 \pmod{121}$$

$$103 b_3 + 121 y = 1$$

121	103	1	-6	77
103	18	5	12	-15
18	13	1	-5	42
13	5	2	2	-5
5	3	1	-1	2
3	2	1	1	-1
2	1	2	0	1
1	0	-	1	0

-40	47
7	+40
-5	7

$$(103) \begin{pmatrix} 4 \\ 7 \end{pmatrix} + (121) \begin{pmatrix} 40 \\ -65 \end{pmatrix} = 1$$

$$\begin{matrix} 7431 \\ 4841 \end{matrix}$$

$$\begin{matrix} 7865 \\ 4840 \end{matrix}$$

WILSON TETEL

$p \in \mathbb{N}$ és prímszám

$$(p-1)! \equiv -1 \pmod{p}$$

(Biz): indukcióról!

$$p=2 \quad 1 \stackrel{?}{\equiv} -1 \pmod{2} \quad \checkmark$$

$$p=3 \quad 1 \cdot 2 \equiv -1 \pmod{3} \quad \checkmark$$

$$p=5 \quad 1 \cdot 2 \cdot 3 \cdot 4 \equiv -1 \pmod{5} \quad \checkmark$$

$$5-1$$

$$1 \cdot 2 \cdot 3 \cdot 4 \equiv -1 \pmod{5}$$

$$\equiv 1$$

$$p=7 \quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv -1 \pmod{7}$$

$$p=11 \quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv -1 \pmod{11}$$

$$p=13 \quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \equiv -1 \pmod{13}$$

Fü: nézzük a négyzetet

$$2, 3, \dots, p-2$$

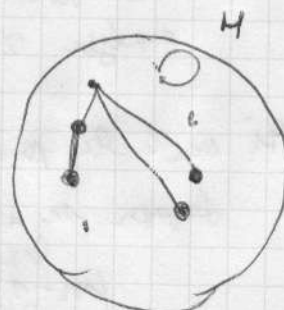
degen. M ren elemek között

kéntük egy gráfot. ($G \rightarrow$)

Grafon M elemek

$a, b \in M$ -t összekötjük

$$a \cdot b \equiv 1 \pmod{p}$$



lehet-e hurok és 0-ban?

$$a \cdot a \equiv 1 \pmod{p} \Leftrightarrow \text{hurok van az } a\text{-n}$$

$$a^2 \equiv 1 \pmod{p}$$

$$p \mid a^2 - 1 \Leftrightarrow p \mid (a-1)(a+1) \Rightarrow p \mid a-1 \text{ vagy } p \mid a+1$$

$$a \in H \text{ azt jelenti } 2 \leq a \leq p-2 \Rightarrow 1 \leq a-1 \leq p-3$$

$$p \nmid a-1 \text{ és hurok}$$

$$a \in H \Rightarrow 2 \leq a \leq p-2 \Rightarrow 3 \leq a+1 \leq p-1$$

$$p \nmid a+1$$

Nem lehet hurok az a -ban

Kérdés: lehet-e olyan 0-ban egy adott pontból nem indul ki 2 él

Ha $a \in H$ akkor létezik $b \in H$ amire a és b össze van kötve

$$a \cdot b \equiv 1 \pmod{p} \text{ áll minden } a \in H\text{-ra}$$

$$a \cdot x \equiv 1 \pmod{p} \text{ mindig megoldható}$$

az egy lineáris kongruencia

Számláljuk ki a és p relatív prímek száma a és p

$$d \mid a, d \mid p \Rightarrow d = 1 \text{ vagy } d = p$$

$$d \mid a \Leftrightarrow p \mid a$$

Von megadom!!!

A lineáris kongruencia

megvan egy a -t kérek

a -ból szeretném egy éllel nem köthető a -ban

a -val van egy közös b

a, b -t kiválasztom.

és az eddigiek ismeretében

Az eddigiek alapján fogom csinálni

$$A \text{ képlet } 2 \cdot 3 \cdot p-2 \text{ szorzat } \equiv 1 \pmod{p}$$

Mi van ha p nem prím?

Legyen m a modulus

$$(m-1)! \equiv -1 \pmod{m}$$

Kérdés: mennyi $\phi(m)$?

Kisérlet!

$$m=1 \quad 0! \equiv 1 \pmod{1} \quad \delta_1 = 1$$

$m=2, 3$ prím

$$m=4 \quad 1 \cdot 2 \cdot 3 \equiv 2 \pmod{4} \quad \delta_4 = 2$$

$m=5$ prím

$$m=6 \quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \equiv 0 \pmod{6} \quad \delta_6 = 0$$

$m=7$ prím

$$m=8 \quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \equiv 0 \pmod{8} \quad \delta_8 = 0$$

$$m=9 \quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \equiv 0 \pmod{9} \quad \delta_9 = 0$$

$$m=10 \quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \equiv 0 \pmod{10} \quad \delta_{10} = 0$$

Szüks. $\delta_m =$ ~~1 ha m~~

$$\text{Szüks. } \delta_m = \begin{cases} -1 & \text{ha } m \text{ prím} \\ 2 & \text{ha } m=4 \\ 0 & \text{ha } m \neq 4 \end{cases} \quad \begin{matrix} \text{ért. tőle} \\ \text{és } m \text{ összetett} \end{matrix}$$

mivel $m \geq 2$ -re

állítás $m \geq 6$ és m nem prím

$$\text{vagy } (m-1)! \equiv 0 \pmod{m}$$

Bizonyítás: mivel m nem prím $m = a \cdot b$ $a \geq 2, b \geq 2$

$$2 \leq a \leq \frac{m}{b} \leq \frac{m}{2} \leq m-1$$

$$\frac{m}{2} \leq m-1 \Leftrightarrow m \leq 2m-2 \Leftrightarrow 0 \leq m-2$$

ha $m \geq 2$ akkor 2 áll. De az ok. mert $m \geq 6$

$$2 \leq b \leq \frac{m}{a} \leq \frac{m}{2} \leq m-1$$

Amikor visszamegyünk $1 \cdot 2 \cdot \dots \cdot (m-1)$ -t akkor

a, b benne van a szorzatban

$$\Rightarrow (m-1)! \equiv 0 \pmod{m} \quad \text{és minden } m \geq 6 \text{ esetén}$$

Görvénnyel $m = a \cdot a$ az állítás is bebizonyosítható.

vagy $m = p^2$ p egy prím.

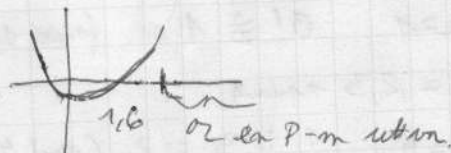
$$m = 9, 25, 49, \dots$$

Kellene hogy $p, 2p$ benne legyen $1, \dots, m-1$ között

$$2 \leq p \leq m-1 = p^2-1$$

$$\text{Ha } p > p^2 - 1 \Rightarrow 0 > p^2 - p - 1$$

$$\frac{1 + \sqrt{1+4}}{2} = \frac{1 + \sqrt{5}}{2}$$



$$1 \leq 2p \leq m-1 = p^2-1$$

$$2p > p^2 - 1$$

$$0 > p^2 - 2p - 1 = (p-1)^2 + 2$$

$$2 > (p-1)^2$$

$$\sqrt{2} > p-1$$

$$1,4 \geq p-1$$

$$2,4 \geq p \text{ mert } p=2 \Rightarrow m=4 \text{ d } m \geq 6$$

FERMA TÉTEL

$p \in \mathbb{N}$, p prím

$a \in \mathbb{Z}$ a relatív ~~prím~~ prím a p -hez $(p \nmid a)$

$$\text{vagy } a^{p-1} \equiv 1 \pmod{p}$$

$$\text{Példa: } p=7, a=4$$

$$4^6 \equiv 1 \pmod{7}$$

$$2^{12}$$

$$\frac{4096 - 1}{7} = 585$$

Bőveítés:

$$G = \{1, 2, \dots, p-1\}$$

$$B = \{1 \cdot a, 2 \cdot a, \dots, (p-1) \cdot a\}$$

Definiálunk egy gráfot G -t

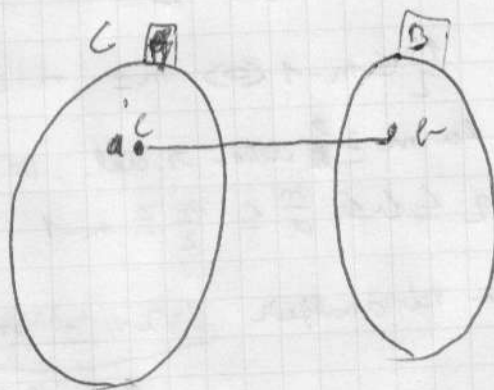
G csúcsai G és B elemei

$ca \in G$ $b \in B$ öre van köztük ha az azaz egy $a \equiv b \pmod{p}$

Értékelés: minden $(b \in B)$ $a \in G$ -hez illik hozzá a

$a \equiv 1 \pmod{p}$ az egy lineáris kongruencia

a relatív prím a modulus-hoz \Rightarrow van megoldás



Emellett legyen $b \in B$ -hez sem illő szám, azaz

$$\left. \begin{aligned} C &\equiv b \pmod{p} \\ C' &\equiv b \pmod{p} \end{aligned} \right\} \text{ Jelenti hogy } b \text{ az } p \text{ rest} \\ \text{el is illő szám.}$$

$$\Rightarrow C \equiv C' \pmod{p} \Rightarrow p \mid (C' - C)$$

$$1 \leq C' \leq p-1 \quad 1 \leq C \leq p-1$$

$$0 \leq C' - C \leq p-2 \quad \text{feltétele hogy } C' \geq C$$

$$0 \leq C' - C \leq p-2$$

$$\Rightarrow C' - C = 0 \Leftrightarrow C' = C$$

Van egy 1-1 megfeleltetés C és B között

B elemei a C elemeinek 1 permutációját adják modulo p

$$1 \cdot 2 \cdot \dots \cdot (p-1) \equiv [1 \cdot a] [2 \cdot a] \dots [(p-1) \cdot a] \pmod{p}$$

Egyenlőség 1, 2, $(p-1)$ -el (mod p -al)

$$1 \equiv a^{p-1} \pmod{p}$$

~~Euler~~

EULER TÉTEL

Fermat tétel általánosítása

$$m \in \mathbb{N}$$

$a \in \mathbb{Z}$, a relatív prím m -hez

$$\Rightarrow a^{f(m)} \equiv 1 \pmod{m}$$

$$(a^{p-1}) \equiv 1 \pmod{p}$$

↑
szorzatosságot m -el

szorzatosságot kell az m egy függvényével.

For Euler felle f függvény

Hogy néz f -t vizsgáljunk!

Ismer fel a szorzat f -től $(m-1)$ -ig

Hisszük szorzat analízis en relatív prímek m -hez.

A megmaradó szám $f(m)$

$$Pl \quad m=6$$

$$1 \cancel{2} \cancel{3} \cancel{4} \cancel{5}$$

$$f(6)=2$$

$$m=9$$

$$1 \cancel{2} \cancel{3} \cancel{4} \cancel{5} \cancel{6} \cancel{7} \cancel{8} \quad f(9)=6$$

mivel azért m -re $f(m)$ -t is tudjuk számolni hogy m -re mindig van.

Problema nr. 1
Pag. 1

$$f(p) = p^{-1} \quad \text{a years}$$

~~1.1~~

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

$$f(p^2) = (p^2 - 1) - (p - 1) = p^2 - p = p(p - 1)$$

$$f(p^3) = p^3 - p^2 = p^2(p - 1)$$

$$f(p^4) = p^4 - p^3 = p^3(p - 1)$$

$$f(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$$

$$f(m) = f(p_1^{d_1} \dots p_s^{d_s})$$

$$f(p_1^{d_1}) \dots f(p_s^{d_s}) \text{ - se vede din expresia de$$

$$= (p_1^{d_1} - p_1^{d_1-1}) \dots (p_s^{d_s} - p_s^{d_s-1})$$

$$= p_1^{d_1} \left(1 - \frac{1}{p_1}\right) \dots p_s^{d_s} \left(1 - \frac{1}{p_s}\right)$$

$$p_1^{d_1} p_s^{d_s} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

$$m = 20000 = 2^5 \cdot 5^4$$

$$f(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

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

$$2^5 \cdot 5^4 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) = 2^4 \cdot 5^3$$

$$\underbrace{2^3 \cdot 5^3}_{1000} \cdot 2 = 8000$$

Rezultatul este a FERMATETELN

LÁNE TÖRTEK

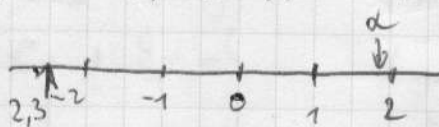
α egy adott valós szám

α -t felváltva két rész összege

$$\alpha = \underbrace{[\alpha]}_{\text{egészrész}} + \underbrace{\{\alpha\}}_{\text{törtész}}$$

Rapideur egy számegyenes

Felváltva az egész számmal mint utóval



$$\alpha = -2,3$$

$$\alpha = 1,9 \quad [\alpha] = 1 \quad \{\alpha\} = 0,9$$

$$\alpha = -2,3 \quad [\alpha] = -3$$

$$\{\alpha\} = 0,7$$

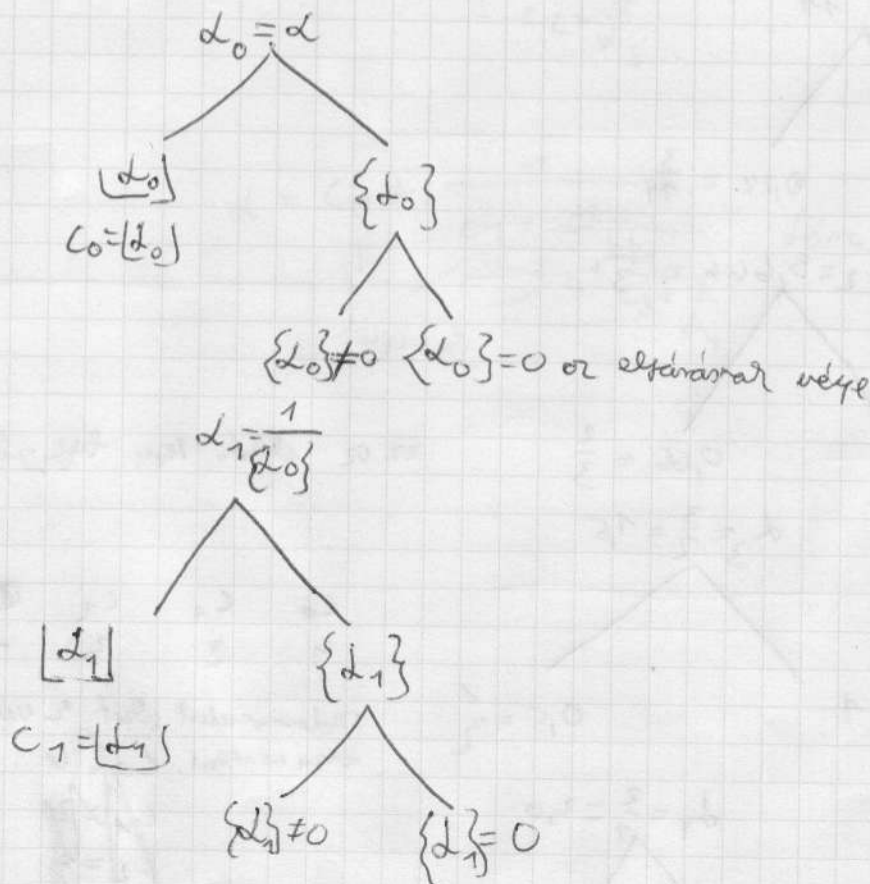
1, $[\alpha]$, $\{\alpha\}$ mindig létezik

2, egyértelmű

3, $[\alpha]$ egy egész szám

$0 \leq \{\alpha\} < 1$ azaz mindig +ív

Egy kis algoritmus



Fonnyalás

1, szűkített lépés

$$d_0 = L$$

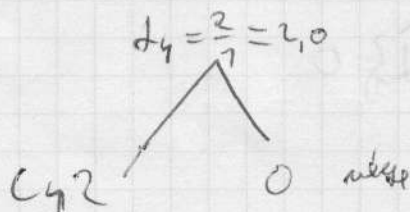
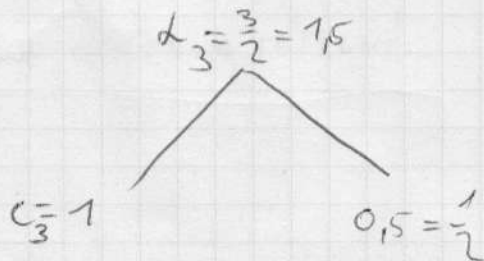
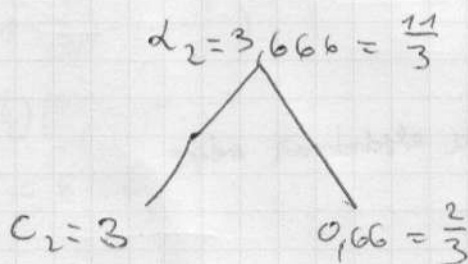
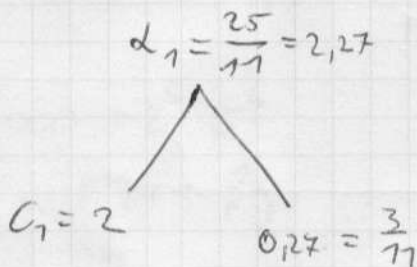
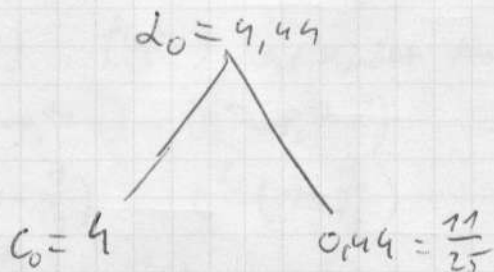
2, számított lépés

~~$d_i = L_i$~~ Ha $\{L_i\} = 0$ akkor vége

Ha $\{L_i\} \neq 0$ akkor

$$C_i = \lfloor L_i \rfloor \quad L_{i+1} = \{L_i\}$$

Például $L = \frac{111}{25} = 4,44$



~~C_0, C_1, C_2, C_3, C_4~~

az az eljárás nagy légszámú lépés

C_0	C_1	C_2	C_3	C_4
4	2	3	1	2

Indukciós lépés az a nagy lépés
nagy lépés. $C_0 = 4$

~~$C_1 = 2$~~
 ~~$C_2 = 3$~~
 ~~$C_3 = 1$~~
 ~~$C_4 = 2$~~

Lernfortschritt.

$$d_0 = c_0 + \{d_0\}$$

$$d_0 = c_0 + \{d_0\}$$

$$d_1 = c_1 + \{d_1\}$$

$$d_1 = c_1 + \{d_1\}$$

$$d_1 = c_1 + \{d_1\}$$

$$d_0 = c_0 + \{d_0\}$$

$$d_0 = c_0 + \frac{1}{d_1}$$

$$d_1 = c_1 + \frac{1}{d_2}$$

$$d_2 = c_2 + \frac{1}{d_3}$$

$$d_3 = c_3 + \frac{1}{d_4}$$

$$d_i = c_i + \frac{1}{d_{i+1}}$$

$$d = c_0 + \frac{1}{c_1 + \frac{1}{d_2}}$$

$$d = c_0 + \frac{1}{c_1 + \frac{1}{c_2 + \frac{1}{d_3}}}$$

$$d = c_0 + \frac{1}{c_1 + \frac{1}{c_2 + \frac{1}{c_3 + \frac{1}{d_4}}}}$$

↓
fortgesetzt

Leere Zeit

l

Adattól a leíródat függ. c_0, c_1, c_2, \dots

Számszerűen a valószínűségi értéket.

$$(c_0) \rightarrow c_0$$

$$(c_0, c_1) \rightarrow c_0 + \frac{1}{c_1}$$

$$(c_0, c_1, c_2) \rightarrow c_0 + \frac{1}{1 + c_1 + \frac{1}{c_2}}$$

$$\text{stb.} \quad (c_0, c_1, c_2, c_3) \rightarrow c_0 + \frac{1}{\frac{c_1 + \frac{1}{c_2 + \frac{1}{c_3}}}{c_2 + \frac{1}{c_3}}}$$

Infinit sorozat visszafelé tört alakban

$$(c_0) = \frac{c_0}{1} = \frac{r_0}{s_0}$$

$$(c_0, c_1) = \frac{c_0 \cdot c_1 + 1}{c_1} = \frac{r_1}{s_1}$$

$$(c_0, c_1, c_2) = c_0 + \frac{1}{c_1 + \frac{1}{c_2}} = \frac{c_0(c_1 + c_2) + 1}{c_1 + c_2}$$

$$c_0 + \frac{1}{\frac{c_1 + \frac{1}{c_2}}{c_1 + c_2}} = c_0 + \frac{1}{\frac{c_1 c_2 + 1}{c_1 + c_2}} = c_0 + \frac{c_1 + c_2}{c_1 c_2 + 1} = \frac{c_0 c_1 c_2 + c_0 + c_1 + c_2}{c_1 c_2 + 1}$$

$$(c_0, c_1, c_2) = \frac{c_0 c_1 c_2 + c_0 + c_1 + c_2}{c_1 c_2 + 1}$$

$$(c_0, c_1, c_2) = \frac{c_0 c_1 c_2 + c_0 + c_1 + c_2}{c_1 c_2 + 1} = \frac{r_2}{s_2}$$

$$c_0 + \frac{1}{\frac{c_1 + \frac{1}{\frac{c_2 + \frac{1}{c_3}}{c_2 + c_3 + 1}}}{c_1 + c_2 + c_3 + 1}} = c_0 + \frac{1}{\frac{c_1 c_2 c_3 + c_1 + c_2 + c_3}{c_2 + c_3 + 1}} = \frac{c_0(c_1 c_2 c_3 + c_1 + c_2 + c_3) + 1}{c_1 c_2 c_3 + c_1 + c_2 + c_3 + 1}$$

$$= c_0 + \frac{c_2 c_3 + 1}{c_1 c_2 c_3 + c_1 + c_2 + c_3 + 1} = \frac{c_0 c_1 c_2 c_3 + c_2 c_3 + c_0 c_1 + c_0 c_2 + c_0 c_3 + 1}{c_1 c_2 c_3 + c_1 + c_2 + c_3 + 1}$$

$$= \frac{c_0 c_1 c_2 c_3 + c_2 c_3 + c_0 c_1 + c_0 c_2 + c_0 c_3 + 1}{c_1 c_2 c_3 + c_1 + c_2 + c_3 + 1}$$

i	r_i	s_i
0	c_0	1
1	$c_0 c_1 + 1$	c_1
2	$c_0 c_1 c_2 + c_0 + c_1 + c_2$	$c_1 c_2 + 1$
3	$c_0 c_1 c_2 c_3 + c_0 c_1 + c_0 c_2 + c_0 c_3 + c_1 c_2 + c_1 + c_2 + c_3 + 1$	$c_1 c_2 c_3 + c_1 + c_2 + c_3 + 1$
4	$c_0 c_1 c_2 c_3 c_4 + c_0 c_1 c_2 c_3 + c_0 c_1 c_2 + c_0 c_1 c_3 + c_0 c_1 c_4 + c_0 c_2 c_3 + c_0 c_2 c_4 + c_0 c_3 c_4 + c_1 c_2 c_3 + c_1 c_2 c_4 + c_1 c_3 c_4 + c_2 c_3 c_4 + c_1 c_2 + c_1 c_3 + c_1 c_4 + c_2 c_3 + c_2 c_4 + c_3 c_4 + c_1 + c_2 + c_3 + c_4 + 1$	$c_1 c_2 c_3 c_4 + c_1 c_2 c_3 + c_1 c_2 c_4 + c_1 c_3 c_4 + c_1 c_4 + c_2 c_3 c_4 + c_2 c_3 + c_2 c_4 + c_3 c_4 + c_1 c_2 + c_1 c_3 + c_1 c_4 + c_2 c_3 + c_2 c_4 + c_3 c_4 + c_1 + c_2 + c_3 + c_4 + 1$

Itt valószínűleg nem érdekel a valószínűség

(1) Készen - visszafelé

inverz le $c_0 c_1 c_2 c_3 \rightarrow c_2$ rell

$$c_0 c_1 (c_2 c_3) \rightarrow c_0 c_1$$

$$c_0 (c_1 c_2) c_3 \rightarrow c_0 c_1$$

$$(c_0 c_1) c_2 c_3 \rightarrow c_2 c_3$$

szimuláció

$$(c_0 c_1)(c_2 c_3) \rightarrow 1$$

Neues: $c_1 c_2 c_3 \rightarrow 2 \text{ Teil}$

$$c_1(c_2 c_3) \rightarrow c_1$$

$$(c_1 c_2) c_3 \rightarrow c_3$$

$$c_0 c_1 c_2 c_3 c_4 \rightarrow 2 \text{ Teil}$$

$$c_0 c_1 c_2 (c_3 c_4) \rightarrow c_0 c_1 c_2$$

$$c_0 c_1 (c_2 c_3) c_4 \rightarrow c_0 c_1 c_4$$

$$c_0 (c_1 c_2) c_3 c_4 \rightarrow c_0 c_3 c_4$$

$$(c_0 c_1) c_2 c_3 c_4 \rightarrow c_2 c_3 c_4$$

$$c_0 (c_1 c_2) (c_3 c_4) \rightarrow c_0$$

$$(c_0 c_1) c_2 (c_3 c_4) \rightarrow c_2$$

$$(c_0 c_1) (c_2 c_3) c_4 \rightarrow c_4$$

Neues: $c_1 c_2 c_3 c_4 \rightarrow 2 \text{ Teil}$

$$c_1 c_2 (c_3 c_4) \rightarrow c_1 c_2$$

$$c_1 (c_2 c_3) c_4 \rightarrow (c_1 c_4)$$

$$(c_1 c_2) c_3 c_4 \rightarrow (c_3 c_4)$$

$$(c_1 c_2) (c_3 c_4) \rightarrow 1$$

2. Rekursion

$$\pi_2 = c_2 \pi_1 + \pi_0$$

$$\pi_3 = c_3 \pi_2 + \pi_1$$

$$\pi_4 = c_4 \pi_3 + \pi_2$$

$$s_2 = c_2 s_1 + s_0$$

$$s_3 = c_3 s_2 + s_1$$

$$s_4 = c_4 s_3 + s_2$$

Rekursion

$$\pi_i = c_i \pi_{i-1} + \pi_{i-2}$$

$$s_i = c_i s_{i-1} + s_{i-2}$$

A rekursiv hierarch $i \geq 2$ -nd

notwendige Anfangswerte

i	π_i	s_i	c_i
-2	0	1	-
-1	1	0	-
0	c_0	1	c_0
1	$c_0 c_1 + 1$	c_1	c_1
2			c_2

Pälder

$$\lambda = \frac{111}{25} = \text{sdmrtst fegyri } (4, 2, 3, 12)$$

$$\begin{array}{r} 4 + \frac{1}{2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}} \end{array}$$

szélesség értéke

i	n_i	s_i	c_i	n_i/s_i
-2	0	1	1	
-1	1	0	1	
0	4	1	4	$4/1 = 4,00$
1	5	2	2	$5/2 = 2,50$
2	3	7	3	$3/7 = 0,4285$
3	4	9	1	$4/9 = 0,4444$
4	11	25	2	$11/25 = 0,44$

Itt egy látszik

$$\lambda \approx 2,71 \text{ sdmrtst fegyri } (2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12)$$

i	n_i	s_i	c_i	n_i/s_i
-2	0	1	1	
-1	1	0	1	
0	2	1	2	$2/1 = 2,000000$
1	3	1	1	$3/1 = 3,000000$
2	8	3	2	$8/3 = 2,66666666$
3	11	4	1	$11/4 = 2,750000$
4	19	7	1	$19/7 = 2,714285714$
5	87	32	4	$87/32 = 2,71875000$
6	106	38	1	$106/38 = 2,78947368$
7	133	71	1	$133/71 = 1,88732394$
8	1264	465	6	$1264/465 = 2,71827957$
9			1	
10			1	
11			8	

SZÁMELMÉLETI FÜGGVÉNYEK

$$f: \mathbb{N} \rightarrow \mathbb{C}$$

↓
térhalmaz

↓
sampler

Egy N belé a be kérdő függvény ~~száma~~ számelméleti függvényre utal.
Közelebben az sampler számelméleti függvény

Használatos függvények

$d(n)$ az n osztói az arány (pozitív egészek és 0)
Nézzük néhány értéket

n	$d(n)$
1	1
2	2
3	2
4	3
5	2
6	4
7	2
8	4
9	3
10	4

$$d(n)=1 \Rightarrow n=1$$

$$d(n)=2 \Rightarrow n = \text{prím}$$

Tétel: Ha $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_s^{a_s}$ az n prím tényezői
akkor $d(n) = (a_1+1) \cdot (a_2+1) \cdot \dots \cdot (a_s+1)$

Működik a tétel $n=1$ -re
1-et nem lehet prímszámra bontani
akkor ellátunk $1=2^0 \cdot 3^0$
Az i -re semleges határozzuk az a_i -t
1-et kapunk
Ez lehet egyszerűen

Bizonyítás $n=1$ (Ez van elengedő)

$$n \geq 2 \quad n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_s^{a_s}$$

Vegyük n -et egy osztót d -t

Ha $d \neq 1$ akkor $d = q_1^{b_1} \cdot q_2^{b_2} \cdot \dots \cdot q_r^{b_r}$ prímtényezői felbontás

Tudjuk hogy p_1, p_s különbözők
 q_1, q_r —

Van-e q_i ami nem egyezik egyik p_j -vel sem.

$$q_i | d \quad d | n \Rightarrow q_i | n \quad n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_s^{a_s}$$

$$\Rightarrow q_i | p_j \Rightarrow q_i = p_j \Rightarrow q_i = 1 \text{ vagy } q_i = p_j$$

$$d = p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_s^{b_s}$$

Ha $d | n$ akkor d van $p_1 \dots p_s$ egyike $d = p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_s^{b_s}$ $0 \leq b_i \leq a_i$
 $\dots, 0 \leq b_s \leq a_s$

Ha $d=1$ akkor valamely $b_i=0 \dots b_s=0$

Ha $d \neq 1$ akkor van q mely osztója

Ha $q | d$; $d | n \Rightarrow q = p_j$

$\sqrt{c} = n$ akkor p_f -nel
 ~~$(\sqrt{p_f}) \rightarrow \dots$~~

$(d/p_f) \cdot c = (n/p_f)$

$\sqrt{c} = p_1^{B_1} \dots p_s^{B_s}$

$0 \leq B_1 \leq L_1, \dots, 0 \leq B_s \leq L_s$

\Downarrow
 $L_1 + 1$
 választási
 lehetőségek

\downarrow
 $L_s + 1$
~~választási~~
 lehetőségek

$\Rightarrow (L_1 + 1) \dots (L_s + 1)$ választási lehetőségek
 ami választási lehetőségek nem

Kiszámol

$d(n) = (L_1 + 1) \dots (L_s + 1)$ ha $n = p_1^{L_1} \dots p_s^{L_s}$

vegyünk $n = 20\,000 = 2^5 \cdot 5^4$

$d(n) = (5+1)(4+1) = 30$

Maximálisan a 20 000-nél 30 db pozitív osztója van

Számoljuk fel az osztókat

$0 \leq B_1 \leq 5$	$0 \leq B_2 \leq 4$	$d = 2^{B_1} \cdot 5^{B_2}$
0	0	1
0	1	2
0	2	4
0	3	8
0	4	16
1	0	2
1	1	10
1	2	20
1	3	40
1	4	80
2	0	4
2	1	20
2	2	40
2	3	80

$\mu(n)$ -t már ismert

van egy új számelméleti függvényről Mőbius féle μ

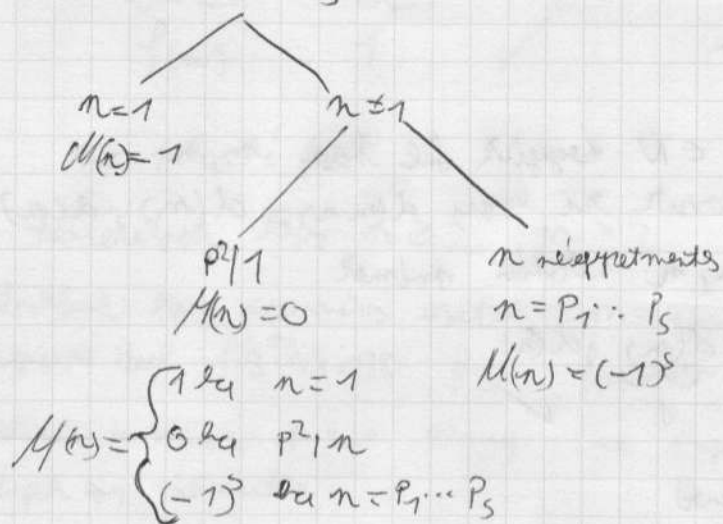
definiáljuk $\mu(n)$ -t

$\mu(1)$ legyen 1

Ha $n \geq 2$ akkor $n = p_1^{a_1} \dots p_s^{a_s}$ prímtényezői felbontás

Ha van $a_i \geq 2$, akkor $\mu(n) = 0$

Ha $a_1 = \dots = a_s = 1$ akkor $\mu(n) = (-1)^s$



Nézzünk néhány értéket.

n	$\mu(n)$
1	1
2	-1
3	-1
4	0
5	-1
6	1
7	-1
8	0
9	0
10	1
11	-1
12	0
13	-1
14	1

MULTIPLIKATÍV SZÁMELMÉLETI FÜGGVÉNYEK

φ számelméleti függvény

Az eddig láttuk φ multiplikatív az $\varphi(mn) = \varphi(m) \varphi(n)$ minden m, n -re ahol m, n relatív prímek

(Ha nem tesszük fel hogy m, n relatív prímek akkor φ -t általában multiplikatív nem hívjuk).

Itétel d multiplikatív

Bizonyítás

vesszünk $m, n \in \mathbb{N}$ tetszőleges fel hogy m, n relatív prím. Mivel φ hogy $d(mn) = d(m) \cdot d(n)$

Ha $m=1$ akkor m, n relatív prímek

$$\underbrace{d(1 \cdot n)}_{d(n)} = \underbrace{d(1)}_1 \cdot \underbrace{d(n)}_{\checkmark}$$

Az $n=1$ eset az hasonló

tetszőleges fel hogy $m \geq 2, n \geq 2$

$m = p_1^{\alpha_1} \dots p_s^{\alpha_s}, n = q_1^{\beta_1} \dots q_r^{\beta_r}$ prímtényező felbontása

deret-e $p_i = q_j$? Nem mert m, n relatív prímek

m, n prímtényező felbontása $p_1^{\alpha_1} \dots p_s^{\alpha_s} q_1^{\beta_1} \dots q_r^{\beta_r}$

$$\underbrace{d(mn)}_{(1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_s)(1+\beta_1)\dots(1+\beta_r)} = \underbrace{d(m)}_{(1+\alpha_1)\dots(1+\alpha_s)} \cdot \underbrace{d(n)}_{(1+\beta_1)\dots(1+\beta_r)}$$

$$(1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_s)(1+\beta_1)\dots(1+\beta_r)$$

Kérdés d valóban multiplikatív

$$m = \underbrace{2^2}_4, n = \underbrace{2^3}_8, mn = 2^5$$

$$\underbrace{d(mn)}_{5+1} = \underbrace{d(m)}_3 \cdot \underbrace{d(n)}_4$$

$$6 \neq 12$$

2, Tétel

mutualizáció

Bor. legyen $m, n \in \mathbb{N}$ relatív prímek
 Mutasd meg hogy $f(mn) = f(m) f(n)$

$m=1$ most m, n relatív prímek

$$\underline{f(mn)} = \underline{f(m)} \quad f(n)$$

$$f(n) = 1 \quad \checkmark$$

$n=1$ hasonlóan

Feltétel: legyen $n \geq 2, m \geq 2$,

nézzünk egy numerus esetet. $m=9 \quad n=10$

Figyessz fel $f(9 \cdot 10) = 480 \quad f(9) \quad f(10) \neq$

nézzük a számok 1-től 90-ig az input a relatív prímek
 input egy táblázatba

		9		10					
1	2	3	4	5	6	7	8	9	
10	11	12	13	14	15	16	17	18	
19	20	21	22	23	24	25	26	27	
28	29	30	31	32	33	34	35	36	
37	38	39	40	41	42	43	44	45	
46	47	48	49	50	51	52	53	54	
55	56	57	58	59	60	61	62	63	
64	65	66	67	68	69	70	71	72	
73	74	75	76	77	78	79	80	81	
82	83	84	85	86	87	88	89	90	

Ha egy elemet

3-al osztva a teljes alakot vizsgáljuk

$$0 \cdot 9 + 3 \quad 1 \cdot 9 + 3 \quad 2 \cdot 9 + 3 \quad \dots \quad 9 \cdot 9 + 3$$

$$0 \cdot m + a \quad 1 \cdot m + a \quad (n-1) \cdot m + a$$

a szám relatív prím az m -szal akkor $i \cdot m + a$ szám egy a
 teljes alakot képviseli

$f(m)$ azaz $\frac{m}{a}$ értéke

Függvények egy modulusz relatív

$$a, b+m, \dots, b+(n-1)m$$

$$\text{mod } n \equiv 1, \dots, n \text{ (mod } n)$$

$$a + i \cdot m \equiv b + j \cdot m \pmod{n}$$

$$i \cdot m \equiv j \cdot m \pmod{n}$$

$$i \equiv j \pmod{n}$$

$$0 \leq i, j < n-1 \Rightarrow i = j$$

+ vizsgáljuk után $f(n)$ szám relatív az osztóhoz

A teljes feladatunk összege $f(m) f(n)$ szám relatív

d multiplikatív

$$f \quad \text{---} \text{---}$$

$$\mu \quad \text{---} \text{---}$$

Tétel: μ multiplikatív (Móbius - féle μ)

(Baz): Válasszunk $m, n \in \mathbb{N}$ m, n relatív prímek

$$\text{Mutassuk meg hogy } \mu(mn) = \mu(m) \mu(n)$$

$$m=1 \text{ eset}$$

$$\frac{\mu(m \cdot n)}{\mu(n)}$$

$$\frac{\mu(m)}{1} \mu(n) \quad \checkmark$$

$$n=1 \text{ eset hasonló}$$

$$m \geq 2 \quad n \geq 2$$

Most van primitív felbontás

$$m = p_1^{d_1} \dots p_s^{d_s} \quad n = q_1^{B_1} \dots q_r^{B_r}$$

Tudjuk hogy $p_i \neq q_j$ (mivel m, n relatív prímek)

$$\Rightarrow mn = p_1^{d_1} p_s^{d_s} q_1^{B_1} \dots q_r^{B_r}$$

Primitív felbontás

$$\text{Számunk } \mu(mn) = \mu(m) \mu(n)$$

Esetek számbavételére meg

$$1, \text{ Valamelyik } d_i \geq 2$$

$$\frac{\mu(mn)}{0} = \frac{\mu(m)}{0} \frac{\mu(n)}{?}$$

$$2, \text{ Valamelyik } B_j \geq 2 \text{ ez teljes esete}$$

$$3. \text{ set } L_1 = L_2 = P_1 = P_2 = 1$$

$$\frac{\mu(m(n))}{(-1)^{s+r}} = \frac{\mu(m)}{(-1)^s} \frac{\mu(n)}{(-1)^r}$$

ÖSSZEKÉPZÉSI FÜGGVÉNY

f, g számelméleti függvények

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

f a g összegzési függvény

g az f megfordítási függvény

$$f(1) = \sum_{d|1} g(d) = g(1)$$

$$f(2) = \sum_{d|2} g(d) = g(1) + g(2)$$

$$f(3) = \sum_{d|3} g(d) = g(1) + g(3)$$

$$f(4) = \sum_{d|4} g(d) = g(1) + g(2) + g(4)$$

A d maga egy összegzési függvény

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

de az összesen 1 függvény összegzési függvény

A f összegzési függvény az $n \rightarrow n$ függvény

$$\text{tétel: } \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{ha } n=1 \\ 0 & \text{ha } n \neq 1 \end{cases}$$

Bemutató: legyen

$$J(n) = \begin{cases} 1 & \text{ha } n=1 \\ 0 & \text{ha } n \neq 1 \end{cases}$$

$$K(n) = \sum_{d|n} \mu(d)$$

Kellne látni $K(n) = J(n)$ minden $n \in \mathbb{N}$

$$n=1$$

$$K(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$$

$$J(1) = 1$$

Felkehetsgáz legyen $n \geq 2$

$$J(n) = 0$$

Kellene legyen $K(n) = 0$

Számok p_i

$$\sum_{d|n} \mu(d) = \sum_{\substack{0 \leq \beta_1 \leq \beta_1 \\ 0 \leq \beta_2 \leq \beta_2 \\ \vdots \\ 0 \leq \beta_s \leq \beta_s}} \mu(p_1^{\beta_1} \dots p_s^{\beta_s}) = \sum_{\substack{0 \leq \beta_1 \leq 1 \\ 0 \leq \beta_2 \leq 1 \\ \vdots \\ 0 \leq \beta_s \leq 1}} \mu(p_1^{\beta_1} \dots p_s^{\beta_s})$$

Az n -nek van prímtényező felbontása

$$n = p_1^{\beta_1} \dots p_s^{\beta_s}$$

Megy, néz p_i n egy d osztója

$$d = p_1^{\beta_1} \dots p_s^{\beta_s} \quad 0 \leq \beta_1 \leq \beta_1, \dots, 0 \leq \beta_s \leq \beta_s$$

2^s tag van

$\beta_1 \dots \beta_s$
↑ ↑
zavaró zavaró

β_1	β_2	\dots	β_s	$\mu(p_1^{\beta_1} \dots p_s^{\beta_s})$
0	0		0	$(-1)^0$
1	0		0	$(-1)^1$
0	1		0	$(-1)^1$
1	1		1	$(-1)^s$

Így az nem nulla van a β -re nézve.

Legyen n a nem nulla néha a $p_1 \dots p_s$ nézve

nevezet 0 és s között

$$n = 0 \text{ egy } \beta_1 \dots \beta_s$$

$$n = 1$$

$$n = 2$$

$$n = k$$

$$n = s$$

$\binom{s}{0}$
1 db van

$\binom{s}{1}$
s db van

$\binom{s}{2}$ db van

$\binom{s}{s}$

$\binom{s}{s}$

$$\sum_{\substack{0 \leq \beta_1 \leq 1 \\ \vdots \\ 0 \leq \beta_s \leq 1}} \mathcal{U}(p_1^{\beta_1} \dots p_s^{\beta_s}) =$$

$$\binom{s}{0} (-1)^0 + \binom{s}{1} (-1)^1 + \dots + \binom{s}{s} (-1)^s$$

$$\sum_{r=0}^s \binom{s}{r} (-1)^r = (1-1)^s = 0$$

$$\sum_{r=0}^s \binom{s}{r} (1)^{s-r} (-1)^r$$

Tétel $\sum_{d|n} \varphi(d) = n$

Boz Nézve az egymásba eső

$$n=10$$

Leírni a számokat 1-től 10-ig

10 és 1-nél nagyobb 1, 2, 5, 10, és

	1	2	3	4	5	6	7	8	9	10
A_1	+		+				+		+	
A_2		+		+		+		+		
A_5					+					
A_{10}										+

$$d=1 \quad \varphi\left(\frac{10}{d}\right) = \varphi(10)$$

$$d=2 \quad \varphi\left(\frac{10}{d}\right) = \varphi(5)$$

$$d=5 \quad \varphi\left(\frac{10}{d}\right) = \varphi(2)$$

$$d=10 \quad \varphi\left(\frac{10}{d}\right) = \varphi(1)$$

$$A_d = \{x: 1 \leq x \leq n \text{ és } \text{eng}(x, n) = d\}$$

Először az egymásba eső d|n

$$(1) A_d \cap A_{d'} = \emptyset \text{ ha } d \neq d'$$

$$\text{válassz } x \in A_d \cap A_{d'}$$

$$0 \leq x \leq n$$

$$\text{eng}(x, n) = d$$

$$d|x \text{ d|n}$$

$$d'|x \text{ d'|n} \Rightarrow d'|d$$

$$\text{eng}(x, n) = d'$$

$$d'|x \text{ d'|n}$$

$$d'|x \text{ d'|n} \Rightarrow d'|d$$

$$(2) \bigcup_{d|n} Ad = \{1, \dots, n\}$$

Válasszunk $x \in \{1, \dots, n\}$

Mondjuk így legyen $x \in Ad$ valamilyen d -re

$$\text{Számunk} \text{ } x \text{ } d = \text{ord}(x_{n/d}) - 1$$

Megyen d van

$$\text{Mond} \ d \in Ad$$

$$(3) |Ad| = \varphi\left(\frac{n}{d}\right)$$

$$\text{Legyen } \frac{n}{d} = \sqrt[n]{\sigma} \Rightarrow d = \frac{n}{\sigma}$$

$$\left| A_{\frac{n}{\sigma}} \right| = \varphi(\sigma)$$

$$\text{ord}\left(x, \frac{n}{\sigma}\right) = \frac{n}{\sigma}$$

$$\text{ord}\left(\frac{x}{\sigma}, \frac{n}{\sigma}\right) = 1$$

$$\text{ord}\left(\frac{x}{\sigma}, \sigma\right) = 1$$

azaz σ osztója $\varphi(\sigma)$ -nak

$$\text{Biz} \ \{1, \dots, n\} = \bigcup_{d|n} Ad$$

\downarrow
 n

$$\sum_{d|n} |Ad| = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{\sigma|n} \varphi(\sigma)$$