Talteori, Föreläsning 3

Aritmetiska funktioner, Dirichletfaltning, Multiplikativa funktioner, Möbiusinversion

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Föreläsningsanteckningar på kurshemsidan `http://courses.mai.liu.se/GU/TATA54/`

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

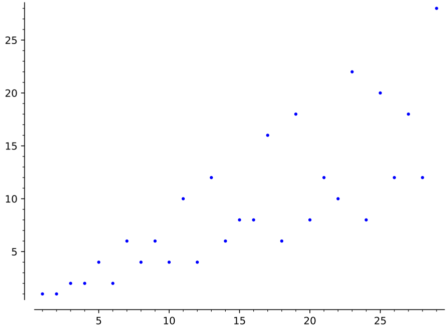
1. **Aritmetiska funktioner**
   - Definition
   - Några vanliga aritmetiska funktioner
   - Dirichletfaltning
   - Algebran av aritmetiska funktioner
   - Matristolkning
   - Summering
   - Multiplikativ invers
   - Ordning, Norm, Oändliga summor
   - Dirichletserier
2. **Multiplikativa funktioner**
   - Definition
   - Euler ϕ
3. **Möbiusinversion**
   - Multiplikativitet bevaras av multiplikation
   - Matrisverifikation
   - Divisorfunktioner
   - Euler ϕ igen
   - μ

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Definition

En *aritmetisk funktion* är en funktion $f : \mathbb{Z}_+ \to \mathbb{C}$.

Oftast, men inte alltid, så kommer f att anta heltalsvärden. Euler-ϕ ett exempel:



Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier

Multiplikativa funktioner

Möbiusinversion

Aritmetiska funktioner definierade genom primtalsfaktorisering

$$n = p_1^{a_1} \cdots p_r^{a_r}, \quad p_i \text{ olika primtal}$$

Liouvilles funktion λ, Möbiusfunktionen μ:

$$\omega(n) = r$$

$$\Omega(n) = a_1 + \cdots + a_r$$

$$\lambda(n) = (-1)^{\Omega(n)}$$

$$\mu(n) = \begin{cases} \lambda(n) & \omega(n) = \Omega(n) \\ 0 & \text{annars} \end{cases}$$

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Aritmetiska funktioner relaterade till divisorer

d antal delare, σ summa av delare, kändisen Euler ϕ.

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

$$\sigma(n) = \sum_{k|n} k$$

$$\phi(n) = \sum_{\substack{1 \le k < n \\ \gcd(k,n)=1}} 1$$

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Ännu fler aritmetiska funktioner

p primtal. Von Mangoldt-funktion Λ, primtalsräknarfunktionen π, Legendre symbol $\left(\frac{n}{p}\right)$, p-valuation v_p.

$$\Lambda(n) = \begin{cases} \log q & n = q^k,\ q \text{ primtal} \\ 0 & \text{annars} \end{cases}$$

$$\pi(n) = \sum_{\substack{1 \le k \le n \\ k \text{ primtal}}} 1$$

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & n \equiv 0 \mod p \\ +1 & n \not\equiv 0 \mod p \text{ och existerar } a \text{ så att } n \equiv a^2 \mod p \\ -1 & n \not\equiv 0 \mod p \text{ och existerar inget } a \text{ så att } n \equiv a^2 \mod p \end{cases}$$

$$v_p(n) = k,\ p^k | n,\ p^{k+1} \not| n$$

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Viktiga aritmetiska funktioner (ej standardnotation)

$$\mathrm{e}(n) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

$$0(n) = 0$$

$$1(n) = 1 \qquad \text{ofta betecknad } \zeta$$

$$\mathrm{I}(n) = n$$

$$\mathrm{e}_i(n) = \begin{cases} 1 & n = i \\ 0 & n \neq i \end{cases}$$

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Definition

Låt f, g vara aritmetiska funktioner. Deras *Dirichletfaltning* är den aritmetiska funktion som ges av

$$(f * g)(n) = \sum_{\substack{1 \le a,b \le n \\ ab=n}} f(a)g(b) = \sum_{\substack{1 \le k \le n \\ k|n}} f(k)g(n/k) = \sum_{\substack{1 \le \ell \le n \\ \ell|n}} f(n/\ell)g(\ell) \quad \text{(DC)}$$

Exempel

$$(f * g)(10) = f(1)g(10) + f(2)g(5) + f(5)g(2) + f(10)g(1)$$

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Algebran av aritmetiska funktioner

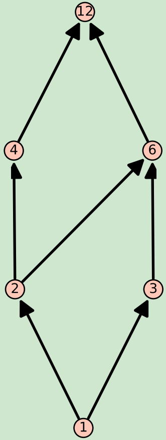
- $f * (g * h) = (f * g) * h$
- $f * g = g * f$
- Multiplikativ enhet, $\mathrm{e}(1) = 1$, $\mathrm{e}(n) = 0$ för $n > 1$
- Inte alla a.f. är inverterbara
- Vi kan addera: $(f + g)(n) = f(n) + g(n)$
- Vi kan skala: $(cf)(n) = cf(n)$
- $0(n) = 0$ nollvektor
- Ett $\mathbb{C}$-vektorrum med multiplikation; en *algebra*. Också en unitär kommutativ ring.

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Matristolkning

- Låt $n \in \mathbb{Z}_+$ och $D(n) = \{ 1 \leq k \leq n \mid k|n \}$ vara dess delare.
- Vi vill förstå a.f. begränsade till $D(n)$, speciellt hur multiplikationen fungerar
- Givet a.f. f, bilda matris A med rader och kolumner indexerade med $D(n)$, och $A_{ij} = f(j/i)$ om $i|j$, 0 annars
- P.s.s. för a.f. g, får matris B
- Då AB matrisen för $f * g$

Exempel

- $n = 12$, $D(n)$ as follows
- 

- $f = 1$
- $A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$
- $A * A = \begin{pmatrix} 1 & 2 & 2 & 3 & 4 & 6 \\ 0 & 1 & 0 & 2 & 2 & 4 \\ 0 & 0 & 1 & 0 & 2 & 3 \\ 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

Summering

- $F(n) = (1 * f)(n) = \sum_{k|n} f(k)$
- Summeringen av f
- Ibland känner vi F men vill återskapa f
- $$\begin{aligned} F(1) &= f(1) \\ F(2) &= f(1) + f(2) \\ F(3) &= f(1) + f(3) \\ F(4) &= f(1) + f(2) + f(4) \\ &\vdots \end{aligned}$$
- Kan lösa ut f unikt:
- $$\begin{aligned} f(1) &= F(1) \\ f(2) &= F(2) - f(1) \\ &= F(2) - F(1) \\ f(3) &= F(3) - f(1) \\ &= F(3) - F(1) \\ f(4) &= F(4) - f(1) - f(2) \\ &= F(4) - F(1) - (F(2) - F(1) \\ &= F(4) - F(2) \\ &\vdots \end{aligned}$$

Inverser

Teorem

f har multiplikativ invers $g = f^{-1}$ omm $f(1) \neq 0$

Bevis.

Vill ha $f * g = e$, så $(f * g)(m) = 1$ om $m = 1$, 0 annars. Får

$$\begin{aligned}
1 &= (f * g)(1) = f(1)g(1) \\
0 &= (f * g)(2) = f(1)g(2) + f(2)g(1) \\
0 &= (f * g)(3) = f(1)g(3) + f(3)g(1) \\
0 &= (f * g)(4) = f(1)g(4) + f(2)g(2) + f(4)g(1) \\
0 &= (f * g)(5) = f(1)g(5) + f(5)g(1) \\
&\vdots \\
0 &= (f * g)(n) = f(1)g(n) + \sum_{\substack{k|n \\ 1<k\leq n}} f(k)g(n/k)
\end{aligned}$$

så vi kan, med induktion, lösa ut $g(n)$. $\square$

Exempel

$$
\begin{aligned}
g(1) &= \frac{1}{f(1)} \\
g(2) &= \frac{-f(2)g(1)}{f(1)} = \frac{-f(2)}{f(1)^2} \\
g(3) &= \frac{-f(3)g(1)}{f(1)} = \frac{-f(3)}{f(1)^2} \\
g(4) &= \frac{-f(2)g(2) - f(4)g(1)}{f(1)} = \frac{-f(2)\frac{-f(2)}{f(1)^2} - \frac{f(4)}{f(1)}}{f(1)}
\end{aligned}
$$

Normerad algebra

Definition

Om $f \neq \mathbf{0}$, så är *ordningen* av f

$$\operatorname{ord}(f) = \min\{\, n \,|\, f(n) \neq 0 \,\}$$

och *normen*

$$\|f\| = 2^{-\operatorname{ord}(f)}$$

Nota bene att detta är ett exemple på en *ultranorm*; $\left\| \frac{1}{1000} f \right\| = \|f\|$

Exempel

Låt

$$f(n) = \begin{cases} p & \text{om } n = p^2 \text{ där } p > 2 \text{ är ett primtal} \\ 0 & \text{annars} \end{cases}$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	4

Då är $\operatorname{ord}(f) = 9$ och $\|f\| = 2^{-9}$.

Lemma

- *Sätt* $f_n = f(n)e_n$, *då gäller att* $f_n * f_m = f_{nm}$
- $f = \sum_n f_n$, *i.e., partialsummorna konvergerar mot* f*:*

$$\left\| f - \sum_{n=1}^{N} f_n \right\| \to 0 \text{ då } N \to \infty$$

- *om* $f(1) = 0$ *så* $e + f$ *inverterbar, med invers given av den konvergenta geometriska serien*

$$\frac{e}{e+f} = e - f + f * f - f * f * f + \cdots$$

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Dirichletserier (utblick)

Definition

Om f är en aritmetisk funktion så definierar vi dess *Dirichletserie* som

$$\mathfrak{D}_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

där s är en komplex variabel. Om f inte växer för fort så konvergerar serien i stora delar av $\mathbb{C}$: tex om $f(n) \in \mathcal{O}(n^k)$ så konvergerar serien för $\mathfrak{Re}(s) > k+1$. Definitionsområdet kan ofta utvidgas vidare via *analytisk fortsättning*.

Dirichletserier (utblick)

Dirichletfaltningen är inspirerad av följande:

Lemma

Låt f, g vara aritmetiska funktioner. Då

$$\mathfrak{D}_f(s)\mathfrak{D}_g(s) = \mathfrak{D}_{f*g}(s)$$

Bevis.

Vi ser att

$$\frac{a}{k^s}\frac{b}{\ell^s} = \frac{ab}{(k\ell)^s}$$

så

$$\sum_{k=1}^{\infty}\frac{f(k)}{k^s}\sum_{\ell=1}^{\infty}\frac{g(\ell)}{\ell^s} = \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{k\ell=n} f(k)g(\ell) = \sum_{n=1}^{\infty}\frac{1}{n^s}(f*g)(n)$$

$\square$

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Dirichletserier (utblick)

Teorem

Om f är en inverterbar a.f. så är $\mathfrak{D}_f$ inverterbar, och

$$\frac{1}{\mathfrak{D}_f(s)} = \mathfrak{D}_{f^{-1}}(s).$$

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Definition

Riemanns zetafunktion definieras som

$$\zeta(s) = \mathfrak{D}_1(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Serien konvergerar för $\mathfrak{Re}(s) > 1$, har en essentiel singularitet i $s = 1$, och kan analytiskt fortsättas till nästan hela $\mathbb{C}$. Den har då nollställen i $-2, -4, -6, -8, \ldots$ och *Riemanns förmodan* säger att de övriga nollställena alla har imaginärdel $\frac{1}{2}$.

Dirichletserier (Riemann zeta, Eulerprodukt)

Teorem

Riemann zeta kan skrivas som en oändlig Eulerporukt:

$$\zeta(s) = \prod_{p \text{ primtal}} \frac{1}{1 - \frac{1}{p^s}}$$

Bevis.

Använder att 1 är *multiplikativ*. $\square$

Aritmetiska funktioner
Definition
Några vanliga aritmetiska funktioner
Dirichletfaltning
Algebran av aritmetiska funktioner
Matristolkning
Summering
Multiplikativ invers
Ordning, Norm, Oändliga summor
Dirichletserier
Multiplikativa funktioner
Möbiusinversion

Dirichletserier (Riemann zeta, Möbius)

Teorem

$$\frac{1}{\zeta(s)} = \mathfrak{D}_{\mu}(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

Bevis.

Använder *Möbiusinversion*. $\square$

Definition

- f är *totalt multiplikativ* om $f(nm) = f(n)f(m)$ för alla m, n
- f är *multiplikativ* om $f(nm) = f(n)f(m)$ närhelst $\gcd(n, m) = 1$

Observera att

$$f_n * f_m = f_{nm}$$

är en likhet för a.f. som alltid gäller, men

$$f(n)f(m) = f(nm)$$

är en likhet förkomplexa tal, som inte behöver gälla.

Teorem

Låt $n = \prod_j p_j^{a_j}$*, primtalsfaktorisering. Då*

- *Om* f *mult. så antingen* $f = 0$ *eller* $f(1) = 1$ *och* $f(n) = \prod_j f(p^j)$*, i.e.,* f *är bestämd av dess värden på primtalspotenser*
- *Om* f *tot. mult. så* $f(n) = \prod_j f(p)^j$*, i.e.,* f *är bestämd av dess värden på primtal*

Bevis.

Uppenbart. $\square$

Teorem

Euler ϕ är multiplikativ.

Bevis

Antag $\gcd(m, n) = 1$. Vill visa $\phi(mn) = \phi(m)\phi(n)$, d.v.s.

$$\left|\mathbb{Z}_{mn}^*\right| = \left|\mathbb{Z}_m^*\right| \left|\mathbb{Z}_n*\right| \tag{1}$$

Hävdar att nedanstående funktion är en bijektion:

$$\mathbb{Z}_{mn}^* \ni [a]_{mn} \mapsto ([a]_m, [a]_n) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^* \tag{2}$$

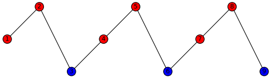
Bevis.

- Väldefinierad, ty $a \equiv a' \mod mn$ medför $a \equiv a' \mod m$ och $a \equiv a' \mod n$. Vidare, $\gcd(a, mn) = 1$ omm $\gcd(a, n) = 1$ och $\gcd(a, m) = 1$.
- Injektiv, ty $a \equiv a' \mod m$ och $a \equiv a' \mod n$ medför $a \equiv a' \mod mn$
- Surjektiv, p.g.a. Kinesiska Restsatsen: välj c, d så att $\gcd(c, m) = 1$, $\gcd(d, n) = 1$. Då finns unikt x mod mn med

$$x \equiv c \mod m$$
$$x \equiv d \mod n$$

så $[x]_{mn} \mapsto ([c]_m, [d]_n)$. Som tidigare, $\gcd(x, mn) = 1$.

$\square$

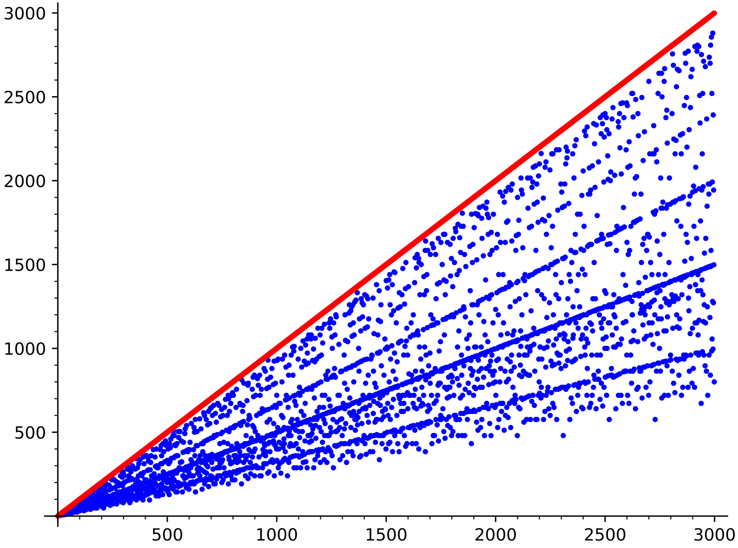
1. Tag p primtal
2. Då alla $1 \leq a < p$ relativt prima till p, så $\phi(p) = p - 1$
3. Nu betraktar vi primpotensen p^r
4. För $1 \leq a < p^r$, $\gcd(a, p^r) > 1$ omm $p|a$
5. Exempel: $p = 3$, $r = 2$: 
6. Så $\phi(p^r) = p^r - \frac{p^r}{p} = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right)$
7. För $n = p_1^{r_1} \cdots p_s^{r_s}$, så ger multiplikativiteten att

$$\begin{aligned}
\phi(p_1^{r_1} \cdots p_s^{r_s}) &= \phi(p_1^{r_1}) \cdots \phi(p_s^{r_s}) \\
&= p_1^{r_1} \cdots p_s^{r_s} (1 - 1/p_1) \cdots (1 - 1/p_s) \\
&= n \prod_j (1 - 1/p_j)
\end{aligned}$$

Exempel

- $\phi(15) = \phi(3)\phi(5) = 2 * 4 = 8$
- $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$
- $\phi(120) = \phi(2^3 * 3 * 5) = 120(1 - 1/2)(1 - 1/3)(1 - 1/5) = 120 * (4/15) = 32.$

$n = p$ ger $\phi(n) = n - 1$. Det kan ses i grafen till $\phi(n)$. Kan du tolka de andra linjerna?



Teorem

f, g (ej konstant noll) multiplikativa aritmetiska funktioner, $h = f * g$

1. *e är multiplikativ*
2. *$f(1) = 1$, så f inverterbar*
3. *h är multiplikativ*
4. *f^{-1} är multiplikativ*

Bevis

(i-ii) Trivial. (iii): Antag $\gcd(m, n) = 1$. Då

$$h(mn) = (f * g)(mn) = \sum_{k|mn} f(k)g(\frac{mn}{k}) = \sum_{\substack{k_1|m \\ k_2|n}} f(k_1k_2)g(\frac{m}{k_1}\frac{n}{k_2})$$

$$= \sum_{\substack{k_1|m \\ k_2|n}} f(k_1)f(k_2)g(\frac{m}{k_1})g(\frac{n}{k_2}) = \sum_{k_1|m} f(k_1)g(\frac{m}{k_1}) \sum_{k_2|n} f(k_2)g(\frac{n}{k_2}) = h(m)h(n)$$

Bevis.

(iv): Formeln för inversen blir nu

$$f^{-1}(n) = -\sum_{\substack{d|n \\ d<n}} f^{-1}(d) f(\frac{n}{d})$$

så om $\gcd(n,m) = 1$ så

$$f^{-1}(nm) = -\sum_{\substack{d|nm \\ d<nm}} f^{-1}(d) f(\frac{nm}{d}) = -\sum_{\substack{d_1|n \\ d_2|m \\ d_1 d_2<nm}} f^{-1}(d_1 d_2) f(\frac{nm}{d_1 d_2})$$

Antag med induktion att f^{-1} är multiplikativ för argument $< nm$. $\square$

Teorem (Möbiusinversion)

1. $1 * \mu = e$
2. $F(n) = \sum_{k|n} f(k)$ *för alla* n *omm* $f(n) = \sum_{k|n} F(k)\mu(n/k)$ *för alla* n

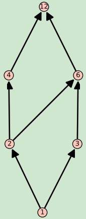
Bevis.

(1): Då de aktuella a.f. är multiplikativa (kontrollera!), räcker det att undersöka värdena på primpotenser p^r. Då $(1 * \mu)(p^0) = 1$, och för $r > 0$

$$(1 * \mu)(p^r) = (\mu * 1)(p^r) = \sum_{k=0}^{r} \mu(p^k) = 1 - 1 + 0 + \cdots + 0 = 0.$$

(2): Om $F = f * 1$ så $f = f * e = f * 1 * \mu = F * \mu$. □

Exempel

- $n = 12,\ D(n)$
- 

- $f = 1$
- $A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$
- $g = \mu$
- $C = \begin{pmatrix} 1 & -1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$
- $AC = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

Kom ihåg:

$$d(n) = \sum_{k|n} 1, \qquad \sigma(n) = \sum_{k|n} k$$

Vi kan skriva detta som

$$d = 1 * 1, \qquad \sigma = 1 * \mathrm{I}$$

och dra slutsatsen att d, σ är multiplikativa, och att

$$\mu * d = 1, \qquad \mu * \sigma = \mathrm{I}$$

eller med andra ord

$$\sum_{k|n} \mu(k) d(n/k) = 1, \qquad \sum_{k|n} \mu(k) \sigma(n/k) = n$$

Definition

$\sigma_k(n) = \sum_{d|n} d^k$. Speciellt, $\sigma_0 = d$, $\sigma_1 = \sigma$.

Lemma

σ_k är multiplikativ

Bevis.

Antag $\gcd(m,n) = 1$. Då

$$\sigma_k(mn) = \sum_{d|mn} d^k = \sum_{\substack{d_1|m \\ d_2|n}} (d_1 d_2)^k = \sum_{\substack{d_1|m \\ d_2|n}} d_1^k d_2^k =$$

$$\sum_{d_1|m} d_1^k \sum_{d_2|n} d_2^k = \sigma_k(m)\sigma_k(n)$$

$\square$

Teorem

1. $\sigma_k(p_1^{a_1} \cdots p_r^{a_r}) = \prod_{j=1}^{r} \frac{1-p_j^{k(a_j+1)}}{1-p_j^k}$
2. $\sum_{d|n} d^k \mu(n/d) = n^k$

Bevis.

Försök på egen hand! $\square$

Lemma

$1 * \phi = \mathrm{I}$

Bevis.

M.a.o., vill bevisa

$$\sum_{k|n} \phi(k) = n.$$

Multiplikativ, så sätt $n = p^r$.

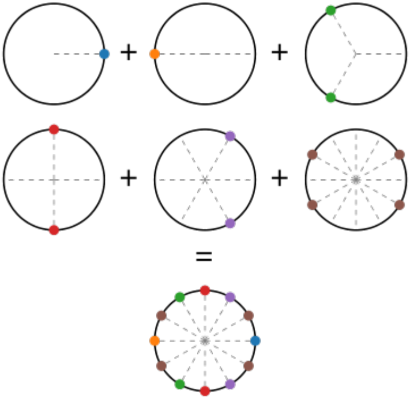
Om $r = 0$: $\mathrm{LHS} = 1$, OK.

Om $r > 0$: $\mathrm{LHS} = \sum_{j=0}^{r} \phi(p^j) = 1 + \sum_{j=1}^{r} (p^j - p^{j-1}) = p^r$, ty teleskopsumma. $\square$

Aritmetiska funktioner
Multiplikativa funktioner
Möbiusinversion
Multiplikativitet bevaras av multiplikation
Matrisverifikation
Divisorfunktioner
Euler ϕ igen
μ

Divisorer till 12

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$$



Teorem

$$\phi(n) = \sum_{k|n} \mu(k)\frac{n}{k} = \sum_{k|n} k\mu(\frac{n}{k})$$

Bevis.

Då

$$1 * \phi = \mathrm{I},$$

har vi att

$$\phi = \mu * \mathrm{I} = \mathrm{I} * \mu$$

$\square$

Definition

En n:e enhetsrot är en komplex rot till ekvationen $z^n = 1$. En primitiv sådan är ej k:e enhetsrot för mindra k.

Lemma

Sätt $\xi_n = \exp(\frac{2\pi}{n} i)$*. Då är de* n*: enhetsrötterna* ξ_n^s, $1 \leq s \leq n$, *och de primitiva är* ξ_n^k, $\gcd(k, n) = 1$.

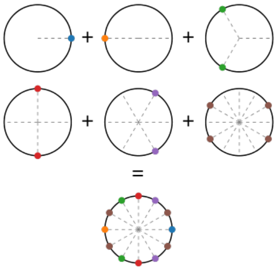
Lemma

För $n > 1$,

$$\sum_{s=1}^{n} \xi_n^s = \frac{\xi_n^n - 1}{\xi_n - 1} = 0.$$

Lemma

$$0 = \sum_{s=1}^{n} \xi_n^s = \sum_{k|n} \sum_{\gcd(\ell,k)=1} \xi_n^\ell$$



Låt $f(d)$ beteckna summan av de primitiva d:e enhetsrötterna. Då $f(1) = 1$, och för $n > 1$, $\sum_{d|n} f(d) = 0$. Så $1 * f = e$, varför $f = \mu$. Så the Möbiusfunktionen är summan av de primitiva enhetsrötterna.