

## KAPITULLI 4

### 4.1. FUNKSIONET ARITMETIKE

**Përkufizim 1.** Funkzioni  $f : \mathbb{N} \rightarrow \mathbb{C}$  quhet *funksion aritmetik*.

Për shembull, funksionet:

- a)  $f(n) = e^{in}, \forall n \in \mathbb{N}$
- b)  $g(n) = n!, \forall n \in \mathbb{N}$
- c)  $h(n) = n^k, k \in \mathbb{Z}, \forall n \in \mathbb{N}$

janë funksione aritmetike.

Funksionet vijuese paraqesin funksione aritmetike të rëndësishme në teorinë e numrave.

- 1)  $\pi(n) = \sum_{p \leq n} 1$  numri i numrave të thjeshtë më të vegjël ose baraz me  $n$ .
- 2)  $\omega(n) = \sum_{p|n} 1$  numri i faktorëve të ndryshëm të thjeshtë të numrit  $n$ .
- 3)  $\Omega(n) = \sum_{p^i|n} 1$  numri i faktorëve të thjeshtë fuqi të numrit  $n$ .
- 4)  $\tau(n) = \sum_{d|n} 1$  numri i pjesëtuesve të numrit  $n$ .
- 5)  $\sigma(n) = \sum_{d|n} d$  shuma e pjesëtuesve të numrit  $n$ .
- 6)  $\varphi(n) = \sum_{\substack{(a,n)=1 \\ 1 \leq a \leq n}} 1$  funksioni i Eulerit ( $\varphi(n)$  është numri i numrave natyrorë  $a$  më të vegjël ose baraz me  $n$  të cilët janë relativisht të thjeshtë me numrin  $n$ ).

$$7) \mu(n) = \begin{cases} 1, & n = 1 \\ 0, & \text{nëse ekziston numri i thjeshtë } p \text{ i tillë që } p^2 | n \\ (-1)^s, & n = p_1 \cdot \dots \cdot p_s, \text{ ku } p_1 \cdot \dots \cdot p_s \text{ janë të thjeshtë, } p_i \neq p_j, i \neq j. \end{cases}$$

Funksioni  $\mu$  quhet funksioni i Mobiusit (Möbius). Vërejmë se  $\mu : \mathbb{N} \rightarrow \{0, 1, -1\}$ .

8)  $\gamma(n) = \prod_{d|n} d$  prodhimi i pjesëtuesve natyrorë të numrit natyror  $n$ .

**Shënim.** Funksionet aritmetike me dy variabla janë funksionet e trajtës  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{C}$ .

P.sh. funksionet  $(m, n), [m, n]$  janë funksione të tilla.

Le të ilustrujmë me anë të shembullit vijues funksionet e sipërpërmendura.

Le të jetë  $n = 12$ .

70

1) Meqë 2,3,5,7,11 janë numra të thjeshtë më të vegjël ose baraz me 12

$$\text{atëherë } \pi(12) = \sum_{p \leq 12} 1 = 5.$$

2) Meqë  $12 = 2 \cdot 2 \cdot 3$  dhe meqë 2,3 janë faktorë të ndryshëm të thjeshtë të

$$\text{numrit 12 atëherë } \omega(12) = \sum_{p|12} 1 = \sum_{2|12} 1 + \sum_{3|12} 1 = 1 + 1 = 2.$$

3) Meqë  $12 = 2^2 \cdot 3$  dhe meqë  $2^2$  është faktor i numrit 12 atëherë

$$\Omega(12) = \sum_{2^2|12} 1 = 1.$$

4) Meqë pjesëtuesit e numrit 12 janë 1,2,3,4,6,12 atëherë  $\tau(12) = \sum_{d|12} 1 = 6.$

5)  $\sigma(12) = \sum_{d|12} d = 1 + 2 + 3 + 4 + 6 + 12 = 28.$

6) Meqë 1,5,7,11 janë relativisht të thjeshtë dhe më të vegjël se 12 atëherë

$$\varphi(12) = \sum_{\substack{(a,12)=1 \\ 1 \leq a \leq 12}} 1 = 4.$$

7) Meqë ekziston numri i thjeshtë 2 i tillë që  $2^2 | 12$  atëherë  $\mu(12) = 0.$

8)  $\gamma(12) = \prod_{d|12} d = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 12 = 1728.$

## 4.2. FUNKSIONET MULTIPLIKATIVE (SHUMEZUES)

**Përkufizim 1.** Funkzioni aritmetik jo zero  $f: \mathbb{N} \rightarrow \mathbb{C}$  quhet *funksion multiplikativ (shumëzues)* nëse  $f(m \cdot n) = f(m) \cdot f(n)$ , nëse numrat natyrorë  $m, n \in \mathbb{N}$  janë relativisht të thjeshtë, d.m.th. nëse  $(m, n) = 1, m, n \in \mathbb{N}$ .

Shembuj të funksioneve multiplikative.

**Shembulli 1.** Funkzioni  $f: \mathbb{N} \rightarrow \mathbb{C}$  i dhënë me  $f(n) = 1, \forall n \in \mathbb{N}$  është multiplikativ.

Vërtetë, le të jenë  $m, n \in \mathbb{N} | (m, n) = 1$ . Atëherë  $m \cdot n \in \mathbb{N}$ , prandaj  $f(m \cdot n) = 1$ . Po ashtu  $f(m) \cdot f(n) = 1 \cdot 1 = 1$ . D.m.th.  $f(m \cdot n) = f(m) \cdot f(n)$ .

**Shembulli 2.** Le të jetë  $f$  funksion multiplikativ. Atëherë  $f(1) = 1$ .

Vërtetë, meqë  $f$  është funksion jo zero, ekziston  $n \in \mathbb{N} \mid f(n) \neq 0$ . Meqë  $(n,1) = 1$  dhe  $f$  kemi

$$f(n) = f(n \cdot 1) = f(n) \cdot f(1).$$

Meqë  $f(n) \neq 0$  duke pjesëtuar të dy anët e relacionit të fundit me  $f(n)$  kemi  $f(1) = 1$ .

**Shembulli 3.** Funksioni  $g(n) = n^k, k \in \mathbb{Z}, \forall n \in \mathbb{N}$  është multiplikativ.

Vërtetë, le të jenë  $m, n \in \mathbb{N} \mid (m, n) = 1$ .

$$\text{Atëherë } g(m \cdot n) = (m \cdot n)^k = m^k \cdot n^k = g(m) \cdot g(n).$$

Le të shohim në vijim një shembull të një funksioni që nuk është multiplikativ.

**Shembulli 4.** Funksioni  $s(n) = n!, \forall n \in \mathbb{N}$  nuk është multiplikativ.

Vërtetë,  $(2,3) = 1$  por  $s(2 \cdot 3) = s(6) = 6! = 720$ ,  $s(2) \cdot s(3) = 2! \cdot 3! = 2 \cdot 3 \cdot 2 = 12$ .

**Teorema 1.** Le të jetë  $f: \mathbb{N} \rightarrow \mathbb{C}$  funksion multiplikativ. Funksioni  $g: \mathbb{N} \rightarrow \mathbb{C}$  i dhënë me

$$g(n) = \sum_{m|n} f(m), \forall n \in \mathbb{N}$$

është multiplikativ.

**Vërtetim.** Lë të jenë  $a, b \in \mathbb{N}$  të tillë që  $(a, b) = 1$ .

Nëse  $u$  është pjesëtues pozitiv i numri  $a$  dhe  $v$  pjesëtues pozitiv i numrit  $b$  atëherë është e qartë se  $uv$  është pjesëtues i  $ab$ . Në bazë të teoremës ....., çdo pjesëtues pozitiv  $m$  i  $ab$  mund të shprehet në mënyrë të vetme në trajtën  $m = u \cdot v$ , ku  $u, v$  janë pjesëtues të numrave  $a, b$  përkatësisht.

Poashtu është e qartë se  $(u, v) = 1$ . Kemi:

$$\begin{aligned} g(ab) &= \sum_{m|ab} f(m) = \sum_{uv|ab} f(uv) = \sum_{uv|ab} f(u) \cdot f(v) = \sum_{u|a} \sum_{v|b} f(u) \cdot f(v) \\ &= \left( \sum_{u|a} f(u) \right) \cdot \left( \sum_{v|b} f(v) \right) = g(a) \cdot g(b), \text{ gjë që duhej treguar.} \end{aligned}$$

**Pohimi 1.** Në qoftë se  $f$  është një funksion multiplikativ dhe  $n_1, n_2, \dots, n_s$  janë numra natyrorë dy nga dy të thjeshtë mes vete, atëherë

$$f(n_1 \cdot n_2 \cdot \dots \cdot n_s) = f(n_1) \cdot f(n_2) \cdot \dots \cdot f(n_s).$$

**Vërtetim.** Pohimin do ta vërtetojmë me anë të induksionit matematik.

Le të jenë  $n_1, n_2 \in \mathbb{N}, (n_1, n_2) = 1$ . Atëherë nga përkufizimi i funksionit multiplikativ kemi  $f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2)$ .

Supozojmë se vlen

$$f(n_1 \cdot n_2 \cdot \dots \cdot n_s) = f(n_1) \cdot f(n_2) \cdot \dots \cdot f(n_s) \quad (\text{hipoteza induktive})$$

ku  $n_1, n_2, \dots, n_s$  janë numra natyrorë të tillë që  $(n_i, n_j) = 1, i \neq j, i, j \in \{1, 2, \dots, s\}$ .

Tregojmë se pohimi vlen për numrat  $n_1, n_2, \dots, n_s, n_{s+1}$ , të cilët plotësojnë kushtet  $(n_i, n_j) = 1, i \neq j, i, j \in \{1, 2, \dots, s, s+1\}$ .

Duhet të tregojmë se

$$f(n_1 \cdot n_2 \cdot \dots \cdot n_s \cdot n_{s+1}) = f(n_1) \cdot f(n_2) \cdot \dots \cdot f(n_s) \cdot f(n_{s+1}).$$

Le të jetë  $n = n_1 \cdot n_2 \cdot \dots \cdot n_s$ .

Sikur  $(n, n_{s+1}) = d, d \neq 1$  atëherë  $d | n$  dhe  $d | n_{s+1}$ .

Nga relacioni  $d | n$  rrjedh që ekziston  $i \in \{1, 2, \dots, s\} | d | n_i$ .

Pra  $d | n_i$  dhe  $d | n_{s+1}$ . D.m.th.  $(n_i, n_{s+1}) \neq 1$  gjë që nuk është e mundur sepse  $(n_i, n_j) = 1, i \neq j, i, j \in \{1, 2, \dots, s, s+1\}$ .

D.m.th. mbetet që  $(n, n_{s+1}) = 1$ . Atëherë

$$\begin{aligned} f(n_1 \cdot n_2 \cdot \dots \cdot n_s \cdot n_{s+1}) &= f(n \cdot n_{s+1}) = f(n) \cdot f(n_{s+1}) \\ &= f(n_1 \cdot n_2 \cdot \dots \cdot n_s) \cdot f(n_{s+1}) \\ &= f(n_1) \cdot f(n_2) \cdot \dots \cdot f(n_s) \cdot f(n_{s+1}). \end{aligned}$$

**Rrjedhimi 1.** Nëse  $f$  është funksion multiplikativ dhe  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  numër natyrorë më i madh se 1 i zbërthyer në faktor të thjeshtë atëherë

$$f(n) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdot \dots \cdot f(p_k^{\alpha_k}).$$

**Pohimi 2.** Le të jenë  $f, g$  dy funksione multiplikative. Atëherë:

(i) Funksioni  $fg : \mathbb{N} \rightarrow \mathbb{C}$  i dhënë me

$$(fg)(n) = f(n)g(n), \forall n \in \mathbb{N}$$

është funksion multiplikativ.

(ii) Nëse  $g(n) \neq 0, \forall n \in \mathbb{N}$  funksioni  $\frac{f}{g} : \mathbb{N} \rightarrow \mathbb{C}$  i dhënë me

$$\left(\frac{f}{g}\right)(n) = \frac{f(n)}{g(n)}, \forall n \in \mathbb{N}$$

është funksion multiplikativ.

**Vërtetim.** (i) Meqë  $(fg)(1) = f(1) \cdot g(1) = 1$  funksioni  $fg$  është i ndryshëm nga zero.

Le të jenë  $m, n \in \mathbb{N} \mid (m, n) = 1$ . Atëherë

$$\begin{aligned} (fg)(mn) &= f(mn) \cdot g(mn) = f(m) \cdot f(n) \cdot g(m) \cdot g(n) \\ &= f(m) \cdot g(m) \cdot f(n) \cdot g(n) \\ &= (fg)(m) \cdot (fg)(n). \end{aligned}$$

Pra  $fg$  është funksion multiplikativ.

(ii) Meqë  $\left(\frac{f}{g}\right)(1) = \frac{f(1)}{g(1)} = 1$  funksioni  $\frac{f}{g}$  është i ndryshëm nga zero.

Le të jenë  $m, n \in \mathbb{N} \mid (m, n) = 1$ . Atëherë

$$\begin{aligned} \left(\frac{f}{g}\right)(mn) &= \frac{f(mn)}{g(mn)} = \frac{f(m) \cdot f(n)}{g(m) \cdot g(n)} \\ &= \frac{f(m)}{g(m)} \cdot \frac{f(n)}{g(n)} = \left(\frac{f}{g}\right)(m) \cdot \left(\frac{f}{g}\right)(n). \end{aligned}$$

Pra  $\frac{f}{g}$  është funksion multiplikativ.

## 4.2. FUNKSIONI I MOBIUSIT

**Përkufizim 1.** Funkzioni  $\mu: \mathbb{N} \rightarrow \mathbb{C}$  i dhënë me:

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & \text{nëse } \exists p \in P \text{ i tillë që } p^2 \mid n \\ (-1)^s, & \text{nëse } n = p_1 \cdot \dots \cdot p_s, \text{ ku } p_1, \dots, p_s \in P \mid p_i \neq p_j, i \neq j \end{cases}$$

quhet *Funksioni i Mobiusit*.

**Shënim:**  $P$  - paraqet bashkësinë e numrave të thjeshtë.

**Shembull:**  $\mu(1) = 1$ ,

$\mu(90) = 0$  sepse ekziston  $p = 3$  (numër i thjeshtë) i tillë që  $3^2 \mid 90$ .

$\mu(6) = (-1)^2 = 1$  sepse  $6 = \underset{p_1}{2} \cdot \underset{p_2}{3}$ .

$\mu(30) = (-1)^3 = -1$  sepse  $30 = \underset{p_1}{2} \cdot \underset{p_2}{3} \cdot \underset{p_3}{5}$ .

$\mu(60) = 0$  sepse  $60 = 2^2 \cdot 3 \cdot 5$ .

Në lidhje me funksionin e Mobiusit vlen kjo teoremë:

**Teorema 1.** a) Funkzioni i Mobiusit është multiplikativ

$$b) \sum_{d \mid n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$$

**Vërtetim.** a) Duhet të tregojmë se  $\forall m, n \in \mathbb{N} \mid (m, n) = 1$  vlen

$$\mu(m \cdot n) = \mu(m) \cdot \mu(n) \quad (1)$$

Le të faktorizojmë numrat  $m$  dhe  $n$  si prodhim të fuqive të numrave të thjeshtë. Sikur në ndonjërin prej faktorizimeve të paraqitet ndonjë eksponent më i madh ose i barabartë me 2 atëherë në të dy anët e barazimit (1) do të merret zero. Pse?

Pra, mbetet të shqyrtojmë rastin kur  $m, n$  paraqiten si prodhim të  $s, t$  numrave të thjeshtë të ndryshëm mes vete, përkatësisht.

Pra,  $m = p_1 \cdot p_2 \cdot \dots \cdot p_s$ ;  $n = q_1 \cdot q_2 \cdot \dots \cdot q_t$ .

Atëherë  $m \cdot n = p_1 \cdot p_2 \cdot \dots \cdot p_s \cdot q_1 \cdot q_2 \cdot \dots \cdot q_t$ .

D.m.th.  $m \cdot n$  paraqitet si prodhim i  $s+t$  numrave të thjeshtë të ndryshëm mes vete.

Shënim. Meqë  $(m, n) = 1$  atëherë

$$p_i \neq q_j, \forall i \in \{1, \dots, s\}, j \in \{1, \dots, t\}.$$

D.m.th.  $\mu(m) = (-1)^s$ ;  $\mu(n) = (-1)^t$ ;  $\mu(m \cdot n) = (-1)^{s+t}$ .

Përfundojmë se

$\mu(m \cdot n) = (-1)^{s+t} = (-1)^s \cdot (-1)^t = \mu(m) \cdot \mu(n)$ , gjë që duhej treguar.

b) Le të jetë  $n=1$ . Pjesëtuesi i vetëm i numrit 1 është  $d=1$ , prandaj  $\sum_{d|n} \mu(d) = \sum_{d|1} \mu(d) = \mu(1) = 1$ .

Le të jetë  $n > 1$ .

Nëse  $n$  është numër i thjeshtë, pra nëse  $n = p$ , meqë pjesëtuesit e vetëm të numrit të thjeshtë  $p$  janë 1 dhe  $p$  kemi:

$$\sum_{d|n} \mu(d) = \sum_{d|p} \mu(d) = \mu(1) + \underbrace{\mu(p)}_{-1} = 1 - 1 = 0.$$

Në vijim mjafton të shqyrtojmë rastin  $n = p^\alpha, \alpha > 1$ .

Pjesëtuesit e numrit  $p^\alpha$  janë:  $1, p, p^2, \dots, p^{\alpha-1}, p^\alpha$ , prandaj

$$\sum_{d|n} \mu(d) = \sum_{d|p^\alpha} \mu(d) = \mu(1) + \underbrace{\mu(p)}_{-1} + \underbrace{\mu(p^2) + \dots + \mu(p^\alpha)}_0 = 0,$$

gjë që duhej treguar.

**Shënim.** Sikur  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$  atëherë nga rasti a) meqë  $\mu$  është multiplikativ do të merret:

$$\mu(n) = \mu(p_1^{\alpha_1}) \cdot \mu(p_2^{\alpha_2}) \cdot \dots \cdot \mu(p_r^{\alpha_r})$$

dhe në secilin rast do të merret  $\mu(p_i^{\alpha_i}) = 0$ .

**Detyrë.** Të vërtetohet se  $\sum_{d=1}^x \left[ \frac{x}{d} \right] \mu(d) = 1$ .

### 4.3. SHUMËZIMI SIPAS DIRICHLEUT DHE FORMULA E ANASJELLË E MOBIUSIT

#### (Dirichlet Convolution and Möbius Inversion Formula)

**Përkufizimi 1.** Shumëzim sipas Dirichlet të funksioneve aritmetike  $f, g$  quhet funksioni aritmetik

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

Nëse  $d_1, d_2, \dots, d_{\tau_n}$  janë pjesëtuesit natyrorë të numrit  $n$  atëherë edhe  $\frac{n}{d_1}, \frac{n}{d_2}, \dots, \frac{n}{d_{\tau_n}}$  janë të gjithë pjesëtuesit natyrorë të numrit  $n$ , prandaj

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

Meqë  $d|n \Leftrightarrow \frac{n}{d}|n$ , kur  $d$  përshkon të gjithë pjesëtuesit natyrorë të  $n$ -it, çiftet e renditura  $\left(d, \frac{n}{d}\right)$  përshkojnë të gjitha çiftet e renditura të numrave natyrorë prodhimi i të cilëve është  $n$ .

Prandaj, mund të shënojmë:

$$(f * g)(n) = \sum_{st=n} f(s)g(t)$$

**Teorema 1.** Le të jenë  $f, g, h$  funksione aritmetike. Vlen:

- 1)  $f * g = g * f$
- 2)  $f * (g * h) = (f * g) * h$
- 3) Për çdo funksion aritmetik  $f$  ekziston funksioni aritmetik  $I$  i tillë që  $f * I = I * f = f$ .

**Vërtetim.** 1) Për çdo  $n \in \mathbb{N}$  kemi

$$(f * g)(n) = \sum_{st=n} f(s)g(t) = \sum_{ts=n} g(t)f(s) = (g * f)(n).$$

$$\begin{aligned}
2) \quad (f * (g * h))(n) &= \sum_{st=n} f(s)(g * h)(t) \\
&= \sum_{st=n} f(s) \left( \sum_{rp=t} g(r)h(p) \right) = \sum_{srp=n} f(s)g(r)h(p) \\
&= \sum_{kp=n} \left( \sum_{sr=k} f(s)g(r) \right) h(p) = \sum_{kp=n} ((f * g)(k))h(p) \\
&= ((f * g) * h)(n).
\end{aligned}$$

3) Së pari funksionin aritmetik  $I$  e definojmë si vijon:

$$I(n) = \begin{cases} 1, & n=1 \\ 0, & n > 1 \end{cases}$$

Kemi:

$$\begin{aligned}
(I * f)(n) &= \sum_{d|n} I(d) \cdot f\left(\frac{n}{d}\right) \\
&= I(1) \cdot f(n) + \sum_{\substack{d|n \\ 1 < d \leq n}} I(d) \cdot f\left(\frac{n}{d}\right) \\
&= I(1) \cdot f(n) = f(n).
\end{aligned}$$

Pra  $I * f = f$ .

Ngjashëm tregohet pjesa tjetër.

Në rastet 1), 2), 3) pamë se shumëzimi sipas Dirichlet është komutativ, asociativ dhe se në lidhje me të ekziston funksioni njësi.

Le të shohim në vijim kushtet që duhen plotësuar në mënyrë që funksioni aritmetik të ketë funksion inverz në lidhje me shumëzimin sipas Dirichlet, pra do të shohim kur ekziston funksioni aritmetik  $f^{-1}$  i tillë që

$$f * f^{-1} = I = f^{-1} * f.$$

**Teorema 2.** Le të jetë  $f$  funksion aritmetike. Funksioni inverz i  $f$  – it në lidhje me shumëzimin sipas Dirichlet ekziston dhe është i vetëm atëherë dhe vetëm atëherë kur  $f(1) \neq 0$ .

Funksioni  $f^{-1}$  njehsohet sipas formulave:

$$f^{-1}(n) = \begin{cases} \frac{1}{f(1)}, & n = 1 \\ -\frac{1}{f(1)} \sum_{\substack{d|n \\ 1 < d < n}} f\left(\frac{n}{d}\right) f^{-1}(d), & n > 1 \end{cases}.$$

**Vërtetim.** Supozojmë së pari se ekziston funksioni inverz.

Atëherë  $(f * f^{-1})(1) = I(1)$  prej nga  $f(1) \cdot f^{-1}(1) = 1$ . Pra është e qartë se  $f(1) \neq 0$ .

Anasjelltas, supozojmë se  $f(1) \neq 0$ .

Në bazë të ekuacionit:

$(f * f^{-1})(1) = I(1)$  kemi  $f(1) \cdot f^{-1}(1) = 1$ . Meqë  $f(1) \neq 0$

atëherë  $f^{-1}(1) = \frac{1}{f(1)}$ .

Supozojmë se vlerat  $f^{-1}(2), \dots, f^{-1}(n-1)$  janë të caktuara në mënyrë të vetme.

Atëherë nga relacioni  $(f * f^{-1})(n) = I(n)$  merret:

$$\sum_{d|n} f(d) f^{-1}\left(\frac{n}{d}\right) = 0 \text{ apo}$$

$$f(1) f^{-1}(n) + \sum_{\substack{d|n \\ 1 < d \leq n}} f(d) f^{-1}\left(\frac{n}{d}\right) = 0$$

$$f(1) f^{-1}(n) + \sum_{\substack{d|n \\ 1 < d \leq n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0$$

prej nga meqë  $f(1) \neq 0$  merret:

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ 1 < d < n}} f\left(\frac{n}{d}\right) f^{-1}(d) \text{ gjë që duhej vërtetuar.}$$

**Rrjedhim.** Nëse  $f$  është funksion multiplikativ, atëherë ai ka funksion inverz në lidhje me shumëzimin sipas Dirichlet.

**Vërtetim.** Nëse  $f$  është multiplikativ atëherë  $f(1) = 1 \neq 0$ .

**Shembulli 1.** Funkzioni aritmetik  $\log n$  nuk ka funksion inverz në lidhje me shumëzimin sipas Dirichlet sepse  $\log 1 = 0$ .

**Shembulli 2.** Funkzioni  $\Lambda$  i Mangoldt i përkufizuar si vijon:

$$\Lambda(n) = \begin{cases} \log p, & \text{nëse } n = p^m, p - \text{i thjeshtë}, m \geq 1 \\ 0 & \text{në çdo rast tjetër} \end{cases}$$

nuk ka inverz në lidhje me shumëzimin sipas Dirichlet sepse  $\Lambda(1) = 0$ .

**Shembulli 3.** Funkzioni  $\mu$  i Mobiusit ka të anasjellë në lidhje me shumëzimin sipas Dirichlet sepse  $\mu(1) = 1$ .

## 9. FUNKSIONET $\sigma$ DHE $\tau$

**Përkufizim.** Le të jetë  $n > 0$ . Me  $\tau(n)$  e shënojmë me numrin e pjesëtuesve pozitiv të  $n$ -it, kurse me  $\sigma(n)$  shumën e pjesëtuesve pozitiv.

P.sh. Le të jetë  $n = 24$ . Atëherë pjesëtuesit pozitiv janë:

$$1, 2, 3, 4, 6, 8, 12, 24.$$

$$\text{D.m.th. } \tau(n) = 8$$

$$\sigma(n) = 1 + 2 + 3 + 4 + 6 + 8 + 12 + 24 = 60.$$

Teorema vijuese paraqet një mënyrë të lehtë për të njehsuar  $\sigma(n)$  dhe  $\tau(n)$  nëse dihet faktorizimi i  $n$ -it në numra të thjeshtë.

**Teorema 1.** Le të jetë  $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_r^{e_r}$ ,  $r \geq 1$ , ku  $p_1 < p_2 < \dots < p_r$  janë numra të thjeshtë dhe  $e_i \geq 1$  për çdo  $i \in \{1, 2, \dots, r\}$ . Atëherë

$$1) \tau(n) = (e_1 + 1) \cdot (e_2 + 1) \cdot \dots \cdot (e_r + 1).$$

$$2) \sigma(n) = \left( \frac{p_1^{e_1+1} - 1}{p_1 - 1} \right) \cdot \left( \frac{p_2^{e_2+1} - 1}{p_2 - 1} \right) \cdot \dots \cdot \left( \frac{p_r^{e_r+1} - 1}{p_r - 1} \right).$$

**Vërtetim.** 1) Nëse  $n = p^r$ , ku  $p$  është numër i thjeshtë,  $r > 0$ , atëherë pjesëtuesit pozitiv të numrit  $n$  janë:  $1, p, p^2, \dots, p^r$ , pra gjithsejt janë  $r + 1$  pjesëtues.

Kështu nëse  $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_r^{e_r}$  ( $r \geq 1$ ) kemi

$(e_1 + 1) \cdot (e_2 + 1) \cdot \dots \cdot (e_r + 1)$  pjesëtues të numrit  $n$ . **(Të verifikohet kjo pjesë!)**

Para se të vërtetojmë pjesën e dytë do të vërtetojmë dy lema:

**Lema 1.** Le të jetë  $n = ab$ ,  $a > 0, b > 0$ ,  $(a, b) = 1$ . Atëherë  $\sigma(n) = \sigma(a) \cdot \sigma(b)$ .

**Vërtetim.** Meqë  $a, b$  kanë vetëm numrin 1 faktor të thjeshtë, duke zbatuar *Teoremën Fundamentale të Aritmetikës* është lehtë të shihet se  $d \mid ab \Leftrightarrow d = d_1 \cdot d_2$  ku  $d_1 \mid a$  dhe  $d_2 \mid b$ . D.m.th. se pjesëtuesit e  $a \cdot b$  janë prodhimet e pjesëtuesve të  $a$ -së dhe  $b$ -së.

Le të jenë

$$1, a_1, \dots, a_s$$

pjesëtuesit e  $a$ -së dhe

$$1, b_1, \dots, b_t$$

pjesëtuesit e  $b$ -së. Atëherë

$$\sigma(a) = 1 + a_1 + a_2 + \dots + a_s$$

$$\sigma(b) = 1 + b_1 + b_2 + \dots + b_t.$$

Pjesëtuesit e  $n = a \cdot b$  mund të paraqiten si vijon:

$$1 + b_1 + b_2 + \dots + b_t$$

$$a_1 \cdot 1, a_1 \cdot b_1, a_1 \cdot b_2, \dots, a_1 \cdot b_t$$

$$a_2 \cdot 1, a_2 \cdot b_1, a_2 \cdot b_2, \dots, a_2 \cdot b_t$$

.....

$$a_s \cdot 1, a_s \cdot b_1, a_s \cdot b_2, \dots, a_s \cdot b_t.$$

Është me rëndësi të ceket se meqë  $(a, b) = 1$  atëherë  $a_i b_j = a_k b_l$  implikon që  $a_i = a_k, b_j = b_l$ . D.m.th. se në vargun e mësipërm nuk ka përsëritje të termave.

Atëherë kemi:

$$1 + b_1 + b_2 + \dots + b_t = \sigma(b)$$

$$a_1 \cdot 1 + a_1 \cdot b_1 + \dots + a_1 \cdot b_t = a_1 \cdot \sigma(b)$$

.....

$$a_s \cdot 1 + a_s \cdot b_1 + \dots + a_s \cdot b_t = a_s \cdot \sigma(b).$$

Prej nga duke i mbledhur anë për anë të gjitha barazitë kemi:

$$\sigma(n) = \sigma(b) + a_1 \cdot \sigma(b) + \dots + a_s \cdot \sigma(b)$$

$= (1 + a_1 + a_2 + \dots + a_s) \sigma(b) = \sigma(a) \cdot \sigma(b)$ , gjë që duhej treguar.

**Lema 2.** Nëse  $p$  është numër i thjeshtë dhe  $k \geq 0$ , kemi:

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

**Vërtetim.** Meqë  $p$  është i thjeshtë, pjesëtuesit e  $p^k$  janë  $1 + p, p^2, \dots, p^k$ .

$$\text{Kështu } \sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

Le t'i kthehemi tani vërtetimit të teoremës. Me këtë rast do të përdorim metodën e induksionit matematik. Le të jetë  $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_r^{e_r}$ .

Nëse  $r = 1$ ,  $n = p_1^{e_1}$ . Nga Lema 2 kemi vërtetimin.

Supozojmë se rezultati është i vërtetë për  $1 \leq r \leq k$ . Tegojmë  $r = k + 1$ .

D.m.th. le të jetë  $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k} \cdot p_{k+1}^{e_{k+1}}$ , ku  $p_1, p_2, \dots, p_k, p_{k+1}$  janë të ndryshëm dhe  $e_i \geq 0$ . Le të jetë  $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$ ,  $b = p_{k+1}^{e_{k+1}}$ . Është e qartë se  $(a, b) = 1$ .

Kështu nga Lema 1 kemi  $\sigma(n) = \sigma(a) \cdot \sigma(b)$ .

Nga hipoteza induktive kemi:

$$\sigma(a) = \left( \frac{p_1^{e_1+1} - 1}{p_1 - 1} \right) \cdot \dots \cdot \left( \frac{p_k^{e_k+1} - 1}{p_k - 1} \right)$$

dhe nga Lema 2,  $\sigma(b) = \frac{p_{k+1}^{e_{k+1}+1} - 1}{p_{k+1} - 1}$ .

Prej nga

$$\sigma(n) = \left( \frac{p_1^{e_1+1} - 1}{p_1 - 1} \right) \cdot \dots \cdot \left( \frac{p_{k+1}^{e_{k+1}+1} - 1}{p_{k+1} - 1} \right) \text{ gjë që duhej treguar.}$$

Nga vërtetimi i teoremës 1 rrjedh pohimi vijues.

**Pohimi 1.** Funkzionet  $\tau: \mathbb{N} \rightarrow \mathbb{C}$  dhe  $\sigma: \mathbb{N} \rightarrow \mathbb{C}$  janë multiplikative.

**Vërtetim.**

## 10. NUMRAT PERFEKT DHE NUMRAT E THJESHTË TË MERSEN-IT

**Përkufizimi:** Pjesëtuesi pozitiv  $d$  i numrit  $n$  quhet **pjesëtues (vërtetë)** i  $n$ -it nëse  $d < n$ . Shumën e të gjithë pjesëtuesve të thjeshtë të  $n$ -it e shënojmë me  $\sigma^*(n)$ . Vërejmë se nëse  $n \geq 2$ , atëherë

$$\sigma^*(n) = \sigma(n) - n.$$

**Përkufizim.**  $n > 1$  është perfekt nëse  $\sigma^*(n) = n$ .

Pra  $n$  është perfekt nëse  $\sigma(n) = 2n$ .

**Përkufizim.** Numrat e formës  $M_n = 2^n - 1$ ,  $n \geq 2$  quhen numra të Mersentit.

Nëse  $M_n$  është i thjeshtë, ai quhet numër i thjeshtë i Mersentit.

Nëse kërkojmë numra perfekt deri në 10 000 do të gjejmë vetëm numrat:

$$6 = 2 \cdot 3$$

$$28 = 2^2 \cdot 7$$

$$496 = 2^4 \cdot 31$$

$$8128 = 2^6 \cdot 127.$$

Vërejmë se  $2^2 = 4$ ,  $2^3 = 8$ ,  $2^5 = 32$ ,  $2^7 = 128$ , pra

$$6 = 2 \cdot (2^2 - 1)$$

$$28 = 2^2 \cdot (2^3 - 1)$$

$$496 = 2^4 \cdot (2^5 - 1)$$

$$8128 = 2^6 \cdot (2^7 - 1).$$

Poashtu vërejmë se  $2^2 - 1$ ,  $2^3 - 1$ ,  $2^5 - 1$ ,  $2^7 - 1$  janë numra të thjeshtë të Mersentit. Në lidhje më këtë vlen:

**Teorema 2.** Nëse  $2^p - 1$  është numër i thjeshtë i Mersentit atëherë  $2^{p-1}(2^p - 1)$  është perfektë.

**Vërtetim.** Le të shenojmë  $q = 2^p - 1$  dhe le të jetë  $n = 2^{p-1} \cdot q$ . Meqë  $q$  është numër tek dhe i thjeshtë, nga teorema 1 kemi:

$$\begin{aligned}\sigma(n) &= \sigma(2^{p-1} \cdot q) = \left(\frac{2^p - 1}{2 - 1}\right) \cdot \left(\frac{q^2 - 1}{q - 1}\right) = (2^p - 1) \cdot (q + 1) = \\ &= (2^p - 1) \cdot 2^p = 2n.\end{aligned}$$

Pra  $\sigma(n) = 2n$  dhe  $n$  është perfekt.

**Teorema 3.** Nëse  $n$  është çift dhe perfekt atëherë ekziston numri i thjeshtë i Mersenit  $2^p - 1$  i tillë që  $n = 2^{p-1}(2^p - 1)$ .

**Vërtetim.** Le të jetë  $n$  numër çift dhe perfekt. Atëherë për ndonjë me  $Z$  vlen,  $n = 2m$ . Numrin  $n$  mund ta shkruajmë në trajtën  $n = 2^k \cdot q$ ,  $k \geq 1$ ,  $q$  tek. Pse?

Meqë  $n$  është perfekt  $\sigma^*(n) = n$ , pra  $\sigma(n) = 2n$ . Meqë  $q$  është numër tek atëherë  $(2^k \cdot q) = 1$ . Pse? Në bazë të lemave 1 dhe 2 kemi:

$$\sigma(n) = \sigma(2^k) \sigma(q) = (2^{k+1} - 1) \cdot \sigma(q).$$

Kështu kemi:

$$2^k \cdot q = n \Rightarrow 2^{k+1} \cdot q = 2n = \sigma(n) = (2^{k+1} - 1) \cdot \sigma(q).$$

D.m.th.

$$2^{k+1} \cdot q = (2^{k+1} - 1) \cdot \sigma(q). \quad (1)$$

$$\text{Tani } \sigma^*(q) = \sigma(q) - q \Rightarrow \sigma(q) = \sigma^*(q) + q.$$

Duke zëvendësuar në (1) merret:

$$\begin{aligned}2^{k+1} \cdot q &= (2^{k+1} - 1)(\sigma^*(q) + q) \\ 2^{k+1} \cdot q &= (2^{k+1} - 1)\sigma^*(q) + 2^{k+1} - q - q.\end{aligned}$$

Pra

$$\sigma^*(q)(2^{k+1} - 1) = q.$$

D.m.th.  $\sigma^*(q)$  është pjesëtues i  $q$ -së.

Meqë  $k \geq 1$ ,  $2^{k+1} - 1 \geq 4 - 1 = 3$  përfundojmë se  $\sigma^*(q)$  është pjesëtues i vërtetë i  $q$ -së. Por  $\sigma^*(q)$  është shuma e të gjithë faktorëve të vërtetë të  $q$ -së.

Kjo është e mundur vetëm nëse  $q$  ka vetëm një faktor të vërtetë. D.m.th.  $q$  duhet të jetë numër i thjeshtë dhe  $\sigma^*(q) = 1$ .

D.m.th.

$$q = 2^{k+1} - 1.$$

Pra  $q$  duhet të jetë numër i thjeshtë i Mersenit dhe  $k + 1 = p$  është i thjeshtë. Pra

$$n = 2^{p-1} \cdot (2^p - 1), \text{ gjë që duhej treguar.}$$