УНИВЕРЗИТЕТ ЦРНЕ ГОРЕ

Природно-математички факултет Подгорица

Маријана Ђурнић

Примитивни коријени и аритметичке функције

СПЕЦИЈАЛИСТИЧКИ РАД

Подгорица, 2020.

УНИВЕРЗИТЕТ ЦРНЕ ГОРЕ

Природно-математички факултет Подгорица

Примитивни коријени и аритметичке функције

СПЕЦИЈАЛИСТИЧКИ РАД

Математика

Ментор: Владимир Божовић

Маријана Ђурнић

Студијски програм: Математика и рачунарске науке

Подгорица, децембар 2020.

Апстракт

Циљ овог рада је упознавање са примитивним коријенима и аритметичким функцијама. У уводу ћемо се подсјетити појма конгруенција и неких њених својстава. У првом поглављу ћемо усвајањем појма *реда броја a по модулу m*, упознати се и са појмом *примитивног коријена*. За сваки природан број моћи ћемо рећи постоји ли његов примитивни коријен и колико их тачно има. Алгоритмом ћемо провјерити да ли је дати број примитивни коријен задатог броја. Такође, посматраћемо примитивне коријене из угла алгебре и утврдити да су они генератори цикличних група. На крају овог поглавља, упознаћемо се са *Артиновом претпоставком*. У другом поглављу ћемо се бавити аритметичким функцијама, нарочито мултипликативним функцијама. Као представника оваквих функција, изучићемо Мебијусову функцију и нека њена основна својства.

Abstract

The aim of this research is to get more familiar with the primitive roots and arithmetic functions. In the introduction I will talk about congruence and its properties. In the first chapter I will focus more on terms *order of a modulo m* and *primitive root*. For every natural number I will be able to tell whether there is a primitive root to it and how many primitive roots are there. With the algorithm I will check whether the number is the primitive root of the previously given number. Also, I will focus on the primitive root and whether they are generators of cyclic groups, but from the perspective of algebra. At the end of this chapter, I will present *Artin's conjecture*. In the second chapter, I will talk about arithmetic functions, particularly about multiplicative functions. As for the representative of these functions I will consider *Möbius function* and some of its basic properties.

Садржај

Глава 1

Увод

Ријеч конгруенција потиче од латинске ријечи *congruentia*, што значи сагласност, сличност, подударност. У свијету математике, конгруенција је бинарна операција која нам даје остатак при дијељењу два цијела броја и ову операцију је увео њемачки математичар Карл Фридрих Гаус [9]. Да би боље разумјели ову операцију, прво ћемо уочити њену примјену у свакодневном животу.

Знамо да је дан подијељен на 24 сата. Ако је тренутно у Канади $21h$, код нас је $6h$ више, односно добијамо сабирањем $21h + 6h = 27h$. Закључујемо да је то заправо $3h$ послије поноћи, јер послије поноћи часови се опет почињу рачунати од $00 - 24h$. Посматрањем из угла конгруенција - рачуна остатака, $3h$ добијамо као остатак при дијељењу броја 27 са 24.

Дефиниција 1. *Нека су a и b произвољни цијели бројеви и $m \in \mathbb{N}$. Кажемо да је* ***a конгруентно са b по модулу m****, у ознаци $a \equiv b \pmod{m}$, ако важи $m \mid a - b$.*

Осврћући се на уводни примјер, добијамо $27 \equiv 3 \pmod{24}$, јер $24 \mid 27 - 3$.

Примјер 1. *Можемо рећи да је $71 \equiv 7 \pmod{8}$, јер $8 \mid 71 - 7$ или $13 \equiv -2 \pmod{3}$, јер $3 \mid 13 - (-2)$. Међутим, $23 \not\equiv 4 \pmod{5}$, јер $5 \nmid 23 - 4$.*

Следеће леме нам дају нека основна својства конгруенција.

Лема 1. *Нека су* $a, b, c, d \in \mathbb{Z}$ *и* $m \in \mathbb{N}$. *Тада важи:*

1. *Ако је* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m} \implies a \pm c \equiv b \pm d \pmod{m}$.
2. *Ако је* $a \equiv b \pmod{m} \implies a \cdot c \equiv b \cdot c \pmod{m}$.
3. *Ако је* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m} \implies a \cdot c \equiv b \cdot d \pmod{m}$.
4. *Ако је* $a \equiv b \pmod{m} \wedge d \mid m \implies a \equiv b \pmod{d}$.

Лема 2. *Нека је* $f(x)$ *полином са цјелобројним коефицијентима. Ако је* $a \equiv b \pmod{m}$, *тада је* $f(a) \equiv f(b) \pmod{m}$.

Примјер 2. *Користећи наведене леме, израчунаћемо* $7^7 \pmod{5}$. *Почињемо од* 7^2, $7^2 = 49 \equiv 4 \pmod{5}$. *Ако претходну конгруенцију степенујемо бројем 3, добијамо* $(7^2)^3 = 7^6 \equiv 4^3 = 64 \pmod{5}$, *односно* $7^6 \equiv 4 \pmod{5}$. *Последњу конгруенцију ћемо помножити са конгруенцијом* $7 \equiv 2 \pmod{5}$. *Слиједи,* $7^6 \cdot 7 \equiv 4 \cdot 2 \pmod{5}$, *што је еквивавлентно са* $7^7 \equiv 8 \pmod{5}$. *Закључујемо да је* $7^7 \equiv 3 \pmod{5}$.

Теорема 1. *Конгруенција по модулу* $m, m \in \mathbb{N}$, *је релација еквиваленције на скупу* $\mathbb{Z}$, *тј:*

i) $a \equiv a \pmod{m}, \forall a \in \mathbb{Z}$ *(рефлексивност)*

ii) Ако је $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}, \forall a, b \in \mathbb{Z}$ *(симетричност)*

iii) Ако је $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \implies a \equiv c \pmod{m}, \forall a, b, c \in \mathbb{Z}$ *(транзитивност)*

Дефиниција 2. *Скуп* $\{x_1, x_2, \ldots, x_m\}$ *цијелих бројева се зове* ***потпуни систем остатака по модулу m*** *ако и само ако за свако* $y \in \mathbb{Z}$ *постоји тачно један* x_j *из датог скупа, тако да је* $y \equiv x_j \pmod{m}$.

Класу еквиваленције цијелог броја m, можемо представити канонским скупом $\mathbb{Z}_m = \{0, 1, 2, 3, \ldots, m-1\}$. Тако потпуни систем остатака по модулу 5, можемо представити као $\{0, 1, 2, 3, 4\}$ или $\{-2, -1, 0, 1, 2\}$ или на још много других начина. Ако посматрамо из угла алгебре, скуп $\mathbb{Z}_m$ је прстен цијелих бројева по модулу m, са сабирањем и множењем по модулу m. Ово су само неке основне особине конгруенција. Њихова примјена је огромна, како у теорији бројева, теорији прстенова, криптографији, рачунарству, тако и у економији, музици, визуелним умјетностима.

Формулисаћемо Ојлерову функцију и теореме које ћемо користити у даљем раду.

Дефиниција 3. *Скуп свих елемената потпуног система остатака по модулу m, који су узајамно прости са m, назива се* ***редукован систем остатака по модулу m****. Ознака R_m, $R_m = \{a \in \mathbb{Z}_m \mid \textbf{нзд}(a, m) = 1\}$*

Дефиниција 4. *Нека је $\phi : \mathbb{N} \to \mathbb{N}$, $\phi(1) = 1$ и $\phi(m) = |R_m|$. Тада је ϕ-****Ојлерова функција****.*

Теорема 2. ***(Ојлер)*** *Ако је* **нзд**$(a, m) = 1$*, онда је* $a^{\phi(m)} \equiv 1 \pmod{m}$.

Посљедица 1. ***(Мала Фермаова теорема)*** *Ако је p прост број,* **нзд**$(a, p) = 1$*, онда је $\phi(p) = p - 1$.*

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

Теорема 3. *Ојлерова функција је мултипликативна.*

Доказе формулисаних теорема и лема, заинтересовани читалац може наћи у [2].

Глава 2

Примитивни коријени

Израчунајмо степене 3^i по модулу 7, за $0 \leq i < \phi(7) = 6$. Добијамо,

$$3^0 \equiv 1 \pmod 7$$
$$3^1 \equiv 3 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$
$$3^3 \equiv 6 \pmod 7$$
$$3^4 \equiv 4 \pmod 7$$
$$3^5 \equiv 5 \pmod 7$$

Отуда је скуп $\{3^i \mid 0 \leq i < \phi(7)\}$ редуковани систем остатака по модулу 7. Односно сваки цио број a, који није дјељив са 7, је конгруентан са 3^i за јединствени цио број i који добијамо по модулу $\phi(7)$. Ова чињеница нам омогућава да замијенимо рачунање у којем користимо само множење и степеновање по модулу 7, са рачунањем у којем ћемо користити сабирање по модулу $\phi(7)$, што ћемо и примијенити у сљедећем примјеру.

Примјер 3. *Ријешите једначину* $x^5 \equiv 6 \pmod 7$. *Нека је* $x \equiv 3^y \pmod 7$, *јер* x *није дјељиво са* 7. *Како је* $6 \equiv 3^3 \pmod 7$, *задату једначину можемо записати у облику* $3^{5y} \equiv 3^3 \pmod 7$, *која је еквивалентна са конгруенцијом* $5y \equiv 3 \pmod 6$.

Задња конгруенција има јединствено рјешење $y \equiv 3 \pmod 6$, *па слиједи да је рјешење наше једначине* $x \equiv 6 \pmod 7$, *односно* $6^5 \equiv 6 \pmod 7$.

Подстакнути *примјером 3*, посматраћемо све бројеве m са својством да постоји број g тако да је скуп $\{g^i \mid 0 \leq i < \phi(m)\}$ редуковани систем остатака по модулу m. Да сви бројеви m немају ово својство показује следећи примјер.

Примјер 4. *Како је* $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$ *и* $\phi(8) = 4$, *слиједи да* $\{a^i \mid 0 \leq i < 4\}$ *никада није једнак редукованом систему остатака по модулу* 8.

Теорема 4. *Нека је* m *природан број и* a *произвољан цио број тако да важи* **нзд**$(a, m) = 1$. *Дефинишимо скуп* A,

$$A = \{k \in \mathbb{Z} \mid a^{|k|} \equiv 1 \pmod m\}.$$

Тада је A *идеал у* $\mathbb{Z}$.

Доказ. Морамо показати да је скуп A затворен у односу на одузимање, тј. да за $j, k \in A \implies j - k \in A$. Претпоставимо да је $j \geq k$, јер $j - k \in A$ ако и само ако $k - j \in A$.

Нека су $j, k \in A$. Ако је $j \geq k \geq 0$ тада $a^j \equiv a^k \equiv 1 \pmod m$, и отуда је $a^{j-k} \equiv a^{j-k}a^k = a^j \equiv 1 \pmod m$. Ако је $j \geq 0 > k$, тада $a^j \equiv a^{-k} \equiv 1 \pmod m$, и добијамо $a^{j-k} = a^j a^{-k} \equiv 1 \cdot 1 = 1 \pmod m$. На крају, ако је $0 > j \geq k$, тада $a^{-j} \equiv a^{-k} \equiv 1 \pmod m$ и закључујемо $a^{j-k} \equiv a^{-j}a^{j-k} = a^{-k} \equiv 1 \pmod m$. Према томе, у сваком случају $j - k \in A$. □

Примијетимо да A садржи ненулте цијеле бројеве, јер $\phi(m)$ припада A по Ојлеровој теореми. Према теореми о идеалима, идеал A је генерисан јединственим природним бројем h, који је најмањи природан број који припада A тако да

$a^h \equiv 1 \pmod{m}$, док $a^j \not\equiv 1 \pmod{m}$ за $1 \leq j < h$. Управо тај цио број h који припада скупу A је *ред броја a по модулу m*. Слиједи дефиниција.

Дефиниција 5. *Позитиван генератор h од A, тј. најмањи природан број тако да $a^h \equiv 1 \pmod{m}$, се зове* ***ред броја*** a ***по модулу*** m *и означавамо са* $\mathbf{ord}\, a$.

Ред $\mathbf{ord}\, a$ наравно зависи од модула m, али пошто је овдје модул m фиксиран, ту зависност ћемо занемарити јер неће имати утицаја на даље излагање. Такође, за било који модул важи $\mathbf{ord}\, 1 = 1$.

Примјер 5. *По модулу 8 имамо* $\mathbf{ord}\, 3 = \mathbf{ord}\, 5 = \mathbf{ord}\, 7 = 2$.

Примјер 6. *Израчунајмо ред бројева 2, 3 и 6 по модулу 7. У уводном примјеру смо видјели да* $\mathbf{ord}\, 3 = 6$. *Како је* $2^2 \equiv 4 \pmod{7}, 2^3 \equiv 1 \pmod{7}$ *то је* $\mathbf{ord}\, 2 = 3$. *И на крају, како је* $6^2 \equiv 1 \pmod{7}$, *то је* $\mathbf{ord}\, 6 = 2$.

Сљедећа теорема је директна посљедица чињенице да је идеал A генерисан са h, $h = \mathbf{ord}\, a$.

Теорема 5. *Претпоставимо да је* $\mathbf{нзд}(a, m) = 1$ *и* $h = \mathbf{ord}\, a$ *по модулу m. Тада:*

i) $a^n \equiv 1 \pmod{m}$ *ако и само ако* $h \mid n$;

ii) $h \mid \phi(m)$;

iii) $a^j \equiv a^k \pmod{m}$ *ако и само ако* $j \equiv k \pmod{h}$;

iv) бројеви $1, a, a^2, \ldots, a^{h-1}$ *су неконгруентни по модулу m, и сваки степен* a^n *је конгруентан са једним од њих по модулу m;*

v) $\mathbf{ord}\, a^k = \frac{h}{\mathbf{нзд}(h,k)}$.

Доказ. i) Слиједи из дефиниције генератора идеала.

ii) Слиједи из i) и Ојлерове теореме.

iii) Претпоставимо да је $k \geq j \geq 0$. Тада $a^k \equiv a^j \pmod{m}$ важи ако и само ако $a^{k-j} \equiv 1 \pmod{m}$, зато што можемо подијелити претходну конгруенцију са a^j како је $\textbf{нзд}(a, m) = 1$. Доказ сада слиједи из *i)*.

iv) Посљедица је од iii).

v) По i), $(a^k)^n \equiv 1 \pmod{m} \iff kn \equiv 0 \pmod{h}$. Подијелимо десну страну конкгруенције са k под условом да промијенимо модул у $\frac{h}{\textbf{нзд}(h,k)}$. Према томе,

$$(a^k)^n \equiv 1 \pmod{m} \iff n \equiv 0 \pmod{\frac{h}{\textbf{нзд}(h,k)}}.$$

Најмањи позитиван број n који задовољава посљедњу конгруенцију је $n = \frac{h}{\textbf{нзд}(h,k)}$. По дефиницији, ово је ред броја a^k по модулу m.

□

На основу тврдње *ii)* из последње теореме, закључујемо да је $\textbf{ord}\, a \leq \phi(m)$, за сваки број a који је узајамно прост са m. Сада се поставља очигледно питање: За које m постоји цио број чији је ред што је могуће већи, рецимо $\phi(m)$? Одговор на ово питање слиједи у сљедећој дефиницији.

Дефиниција 6. *Претпоставимо да* $\textbf{нзд}(g, m) = 1$. *Ако је ред елемента* g *по модулу* m *једнак* $\phi(m)$, *тада је* g ***примитивни коријен по модулу*** m *или* ***примитивни коријен од*** m.

Примјер 7. *Већ смо раније рачунали ред броја* 3 *по модулу* 7 *и добили смо да је* $\textbf{ord}\, 3 = 6 = \phi(7)$. *Слиједи,* 3 *је примитивни коријен по модулу* 7.

Да нема сваки цио број примитивни коријен, показаће нам сљедећи примјер.

Примјер 8. *Ако је* $m = 8$*, тада је* $a^2 \equiv 1$ *за сваки непаран цио број и отуда* $\mathbf{ord}\, a \leq 2 < 4 = \phi(8)$*, за сваки број* a *који је узајамно прост са* 8*. Према томе,* 8 *нема примитивних коријена.*

Теорема 6. *Нека је* g *примитивни коријен по модулу* m*. Тада:*

i) $\{1, g, g^2, \ldots, g^{\phi(m)-1}\}$ *је редуковани систем остатака по модулу* m*;*

ii) $g^j \equiv g^k \pmod{m}$ *ако и само ако* $j \equiv k \pmod{\phi(m)}$*;*

iii) g^k *је примитивни коријен по модулу* m *ако и само ако* $\mathbf{нзд}(k, \phi(m)) = 1$*. Специјално, ако постоји примитивни коријен по модулу* m*, тада постоји тачно* $\phi(\phi(m))$ *примитивних коријена.*

Доказ. Теорема 5 је специјалан случај *Теореме 4.* □

Ова теорема нам, између осталог, говори да ако постоји примитивни коријен по модулу m, онда можемо да израчунамо колико их тачно има. У сљедећем примјеру ћемо показати како одредити све примитивне коријене, уколико их има више.

Примјер 9. *Установили смо да је* 3 *примитивни коријен по модулу* 7*. Како је* $\phi(\phi(7)) = \phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3) = 1 \cdot 2 = 2$*, имамо* 2 *примитивна коријена. Знамо један примитивни коријен по модулу* 7 *и то је* 3*, а да би одредили који је други, испитујемо који број из скупа* $R_7 = \{1, 2, 3, 4, 5, 6\}$ *има ред једнак* $\phi(7) = 6$ *по модулу* 7*. Закључујемо да је то број* 5*. Тако су* 3 *и* 5 *примитивни коријени по модулу* 7*.*

Показаћемо да су једини позитивни цијели бројеви који имају примитивне коријене $1, 2, 4, p^k$ и $2p^k$, гдје је p непаран прост број и k произвољан природан број. Прво ћемо доказати да сваки прост број има примитивне коријене за шта су нам прво потребне сљедеће двије леме.

Лема 3. *Ако a има ред h и b има ред k по модулу m, и ако* **нзд**$(h,k)=1$*, тада ab има ред hk по модулу m.*

Доказ. Нека је r ред броја ab. Како је $(ab)^{hk}=(a^h)^k\cdot(b^k)^h\equiv 1^k\cdot 1^h=1 \pmod m$, закључујемо да $r \mid hk$. Да би доказ био комплетан, остаје још да докажемо да $hk \mid r$.

Примијетимо да $b^{rh}\equiv (a^h)^r b^{rh}=(ab)^{rh}\equiv 1 \pmod m$, и отуда слиједи $k \mid rh$. Како је **нзд**$(h,k)=1$, то повлачи да $k \mid r$. На сличан анчин се доказује да $h \mid r$. Како је **нзд**$(h,k)=1$, слиједи да $hk \mid r$. □

Примјер 10. *Радећи по модулу 7, имамо* $\mathbf{ord}\,2=3$ *и* $\mathbf{ord}\,6=2$*. Како је* **нзд**$(2,3)=1$*, тада* $\mathbf{ord}(2\cdot 6)=2\cdot 3=6$.

Лема 4. *Нека су p и q прости бројеви и претпоставимо да $q^k \mid (p-1)$. Тада постоји број a реда q^k по модулу p.*

Доказ. Заинтересовани читалац може наћи у [1], лема 15.7. □

Теорема 7. *Ако је p прост број, постоји тачно $\phi(p-1)$ примитивних коријена по модулу p.*

Доказ. На основу последње теореме, имамо да постоји најмање један примитивни коријен по модулу p. Нека је $p-1={q_1}^{k_1}{q_2}^{k_2}\ldots{q_r}^{k_r}$ факторизација по различитим простим бројевима. На основу последње леме, слиједи да постоје цијели бројеви a_i реда ${q_i}^{k_i}, i=1,2,\ldots r$. Бројеви ${q_i}^{k_i}$ су у паровима узајамно прости, тако да опет употребом *Леме 3*, видимо да $g=a_1,a_2,\ldots,a_r$ има ред $p-1$, те је g примитивни коријен по модулу p. □

Претпоставимо да је g примитивни коријен по модулу m. Ако је $\textbf{нзд}(a, m) = 1$, тада *Теорема 5* имплицира да постоји јединствени цио број $i, 0 \leq i \leq \phi(m) - 1$ такав да $g^i \equiv a \pmod{m}$. Ова чињеница нас доводи до сљедеће дефиниције.

Дефиниција 7. *Нека је g примитивни коријен по модулу m и претпоставимо да је $\textbf{нзд}(a, m) = 1$. Најмањи ненегативан цио број i, такав да $g^i \equiv a \pmod{m}$ се зове* ***дискретни логаритам a у односу на примитивни коријен g.*** *Означава се са $\textbf{длог}_g(a)$ или само са $\textbf{длог}(a)$ уколико је из контекста јасно на који се примитивни коријен мисли.*

Треба напоменути да дискретни логаритам зависи и од модула m и од коријена g, али како су m и g увијек фиксирани, ову чињеницу можемо занемарити у даљем излагању.

Дискретни логаритам се помиње у теорији коначних група и можемо га примијенити на произвољну цикличну групу. За неке коначне групе, веома је тешко израчунати дискретни алгоритам. Његову примјену налазимо у криптографији.[8]

Постоји доста сличности између дискретних логаритама и логаритама. Сљедећа теорема нам доноси најважнија својства. Доказ је једноставан и препуштамо га читаоцу.

Теорема 8. *Нека је g примитивни коријен по модулу m, и нека је $\textbf{длог}(a)$ ознака за дискретни логаритам a у односу на g.*

i) $\textbf{длог}(1) = 0$ *и* $\textbf{длог}(g) = 1$.

ii) $a \equiv b \pmod{m}$ *ако и само ако* $\textbf{длог}(a) = \textbf{длог}(b) \pmod{\phi(m)}$.

iii) $\textbf{длог}(ab) = \textbf{длог}(a) + \textbf{длог}(b) \pmod{\phi(m)}$.

iv) $\textbf{длог}(a^k) \equiv k\,\textbf{длог}(a) \pmod{\phi(m)}$, *за сваки ненегативан цио број k.*

Теорема 9. *Нека је m природан број са примитивним коријеном и нека је* **нзд**$(a, m) = 1$. *Тада конгруенција* $x^n \equiv a \pmod{m}$ *има рјешење ако и само ако*

$$a^{\frac{\phi(m)}{\textbf{нзд}(n,\phi(m))}} \equiv 1 \pmod{m}. \tag{1}$$

Ако је конгруенција $x^n \equiv a \pmod{m}$ *рјешива, тада она има тачно* **нзд**$(n, \phi(m))$ *неконгруентних рјешења.*

Доказ. Нека је g примитивни коријен по модулу m и нека је $d =$ **нзд**$(n, \phi(m))$. Посматрано из угла дискретног логаритма, видимо да конгруенција $x^n \equiv a \pmod{m}$ важи ако и само ако $n\,$**длог**$(x) \equiv$ **длог**$(a) \pmod{\phi(m)}$. Ова конгруенција је рјешива ако и само ако $d \mid$ **длог**(a), и ако рјешење постоји, тада постоји тачно d неконгруентних рјешења.

Да би довршили доказ, показаћемо да (1) важи ако и само ако $d \mid$ **длог**(a). Како је конгруенција (1) еквивалентна са $\frac{\phi(m)}{d}$ **длог**$(a) \equiv 0 \pmod{\phi(m)}$, она важи ако и само ако $d \mid$ **длог**(a). □

Ако m има примитивни коријен, тада рјешења конгруенције $x^n \equiv a \pmod{m}$ се могу одредити користећи дискретан логаритам, под условом да израчунамо (или имамо на располагању) табелу дискретних логаритама за дати модул m. Како сваки прост модул има примитивни коријен, слиједи посљедица *Теореме 8.*

Посљедица 2. *Нека је p прост број и* **нзд**$(a, p) = 1$. *Тада конгруенција* $x^n \equiv a \pmod{p}$ *је рјешива ако и само ако*

$$a^{\frac{p-1}{\textbf{нзд}(n,p-1)}} \equiv 1 \pmod{p}.$$

Доказ ове посљедице можете наћи у [1].

Ова посљедица нам даје ефикасан поступак за утврђивање да ли је конгруенција $m\ x^n \equiv a \pmod{p}$ рјешива, док је одређивање рјешења још теже. Међутим, ако је $\mathbf{нзд}(n, p-1) = 1$, тада је релативно лако. Користећи Еуклидов алгоритам за одређивање природних бројева s и t имамо да $sn = t(p-1)+1$. Тада је $a^{sn} = a^{t(p-1)} \cdot a \equiv a \pmod{p}$, па је a^s рјешење конгруенције $x^n \equiv a \pmod{p}$.

Слиједи још једна посљедица.

Посљедица 3. *Претпоставимо да m има примитивни коријен и да $n \mid \phi(m)$. Тада конгруенција $x^n - 1 \equiv 0 \pmod{m}$ има тачно n коријена.*

Доказ. Конгруенција $x^n \equiv 1 \pmod{m}$ је очигледно рјешива. Отуда, према *Теореми 8*, има $\mathbf{нзд}(n, \phi(m)) = n$ неконгруентних рјешења. □

У наставку ћемо доказати да ако је p непаран прост број, тада p^k има примитивне коријене за свако k.

Теорема 10. *Нека је p непаран прост број.*

i) Ако је g примитиван коријен по модулу p, тада $g + np$ је примитиван коријен по модулу p^2 за тачно $p-1$ вриједности броја n по модулу p.

ii) Ако је g примитиван коријен по модулу p^2, тада је g примитиван коријен по модулу p^k, за свако $k \geq 2$.

Доказ. i) Означимо са h ред од $g+np$ по модулу p^2 (h може зависити од n). Тада $h \mid \phi(p^2)$, односно $h \mid p(p-1)$.

Међутим $(g+np)^h \equiv 1 \pmod{p^2}$ имплицира $(g+np)^h \equiv 1 \pmod{p}$, па према биномној теореми $(g+np)^h = g^h + \sum_{j=1}^{h} \binom{h}{j} (np)^j g^{h-j} \equiv g^h \pmod{p}$. Отуда $g^h \equiv 1 \pmod{p}$. Како g има ред $p-1$, то повлачи да $p-1 \mid h$.

Према томе, $h = p-1$ или $h = p(p-1)$. У другом случају $g+np$ је примитивни коријен од p^2, а у првом случају није. Доказаћемо да први случај се дешава једино за једну од p могућих вриједности од n.

Нека је $f(x) = x^{p-1} - 1$, тада је g рјешење конгруенције $f(x) \equiv 0 \pmod{p}$ и $f'(g) = (p-1)g^{p-2} \not\equiv 0 \pmod{p}$ како је **нзд**$(g^{p-2}, p) = 1$. Отуда постоји јединствено рјешење облика $g + np$ конгруенције $f(x) \equiv 0 \pmod{p^2}$. То доказује нашу тврдњу.

ii) Треба доказати да ако је g примитиван коријен по модулу $p^k, k \geq 2$, тада је g такође и примитиван коријен по модулу p^{k+1}. Нека је h ред од g по модулу p^{k+1}. Тада $h \mid \phi(p^{k+1})$, односно $h \mid p^k(p-1)$.

Како $g^h \equiv 1 \pmod{p^{k+1}}$ имплицира $g^h \equiv 1 \pmod{p^k}$ и g је примитиван коријен по модулу p^k, $\phi(p^k)$ мора да дијели h, односно $p^{k-1}(p-1) \mid h$.

Према томе или $h = p^{k-1}(p-1)$ или $h = p^k(p-1) = \phi(p^{k+1})$. У другом случају g је примитиван коријен по модулу p^{k+1}, као што се и тврди. Морамо показати да је први случај искључен.

Нека је $t = \phi(p^{k-1})$, тада $g^t \equiv 1 \pmod{p^{k-1}}$ по Ојлеровој теореми и зато $g^t = 1 + np^{k-1}, n \in \mathbb{Z}$. Ако $p \mid n$ тада имамо $g^t \equiv 1 \pmod{p^k}$, што је контрадикторно са чињеницом да је g примитиван коријен по модулу p^k. Према томе $p \nmid n$.

По биномној теореми,

$g^{pt} = (g^t)^p = (1 + np^{k-1})^p = 1 + np^k + \frac{p(p-1)}{2}n^2p^{2k-1} + \cdots \equiv 1 + np^k \pmod{p^{k+1}}$.

Овдје смо користили чињеницу да цио број $\frac{p(p-1)}{2}n^2p^{2k-2} = \frac{p-1}{2}n^2p^{2k-1}$ је дјељив са p^{k+1}, јер $2k-1 \geq k+1$ када $k \geq 2$ и преостали изостављени чланови у развоју имају веће степене од p. Како $p \nmid n$, закључујемо да $g^{pt} \not\equiv 1 \pmod{p^{k+1}}$. Дакле, $h \neq pt = p\phi(p^{k-1}) = p^{k-1}(p-1)$ и доказ је комплетан.

□

Примјер 11. *Како је* $2^2 \equiv -1 \not\equiv 1 \pmod 5$*, закључујемо да ред броја* 2 *по модулу* 5 *мора бити* 4*, па је* 2 *примитиван корије од 5. Према Теореми 9,* $2 + 5n$ *је примитиван корије од* $5^2 = 25$*, за тачно четири вриједности од* n*,* $0 \leq n \leq 4$*. Како је* $\phi(25) = \phi(5^2) = 5^2 - 5 = 20$*, примитивни корије од* 25 *имају ред* 20*. Добијамо,*

$$\begin{aligned} &\textit{за } n = 0, && 2^{20} \equiv 1 \pmod{25}\textit{;} \\ &\textit{за } n = 1, && 7^{20} \equiv 1 \pmod{25}\textit{;} \\ &\textit{за } n = 2, && 12^{20} \equiv 1 \pmod{25}\textit{;} \\ &\textit{за } n = 3, && 17^{20} \equiv 1 \pmod{25}\textit{;} \\ &\textit{за } n = 4, && 22^{20} \equiv 1 \pmod{25}. \end{aligned}$$

Испитајмо које 4 *од горе наведених* 5 *конгруенција је тачно. Ред* h *по модулу* 25 *произвољног броја* a *је дјелилац броја* 20*. Ако је* $h < 20$*, тада или* $h \mid 4$ *или* $h \mid 10$*, што повлачи да* $a^4 \equiv 1 \pmod{25}$ *или* $a^{10} \equiv 1 \pmod{25}$*. Дакле, да би одредили да ли број* a *има ред* 20*, довољно је израчунати* a^4 *и* a^{10} *по модулу 25. Ред је* 20 *ако и само ако ниједан од ова два степена није конгруентан са* 1*. За* $a = 2$*, добијамо* $2^2 \equiv 4, 2^4 \equiv 16, 2^8 \equiv 6$ *и* $2^{10} \equiv 24$*. Дакле, ред броја* 2 *је* 20*, тј.* 2 *је примитивни корије од* 25*.*

За $a = 7$ *добијамо* $7^2 \equiv -1$ *и* $7^4 \equiv 1 \pmod{25}$*, па је ред броја* 7 *једнак* 4 *и* 7 *није притмитивни корије од* 25*. Наравно то сада повлачи да су* 12*,* 17 *и* 22 *примитивни корије од* 25*.*

По Теореми 9, 2 *је примитивни корије од* 5^k *за свако* k*.*

Из овог примјера смо увидјели како можемо испитати да ли је број a примитивни корије од задатог броја m. Примијенићемо исти поступак и у сљедећем примјеру.

Примјер 12. *Већ смо израчунали да је* 3 *примитивни коријен од* 7*, јер* $3^6 \equiv 1 \pmod 7$. *Одредимо примитивне коријене по модулу* 7^2.

Кандидати за примитивне коријене по модулу 7^2 *су коријени облика* $3 + 7n$*, за тачно* 6 *вриједности од* n*,* $0 \leq n \leq 6$. *То су бројеви* $3, 10, 17, 24, 31, 38, 45$. *Ред примитивних коријена по модулу* $7^2 = 49$ *је* $\phi(7^2) = 7^2 - 7 = 49 - 7 = 42$.

Ред h *примитивног броја по модулу* 49*, мора бити* 42. *Ако је* $h < 42$*, тада* h *мора бити неки од дјелилаца броја* 42*,* $42 = 2 \cdot 3 \cdot 7$. *Ред је* 42 *ако и само ако ниједан од степена* a^b*, гдје је* $a \in \{3, 10, 17, 24, 31, 38, 45\}$*,* $b \in \{2, 3, 7, 6, 14, 21\}$*, није конгруентан са* 1 *по модулу* 49. *Како је,* $31^3 \equiv -1 \pmod{49}$*, то је* $31^6 \equiv 1 \pmod{49}$. *Закључујемо,* 31 *није примитивни коријен од* 49. *То повлачи да су* $3, 10, 17, 24, 38$ *и* 45 *примитивни коријени по модулу* $7^2 = 49$.

Закључујемо да би се алгоритам који провјера да ли је број a примитивни коријен по модулу m, састојао од сљедећих корака:

- израчунамо ред h, $h = \phi(m)$, који мора да има примитивни коријен по модулу m;
- извршимо просту факторизацију броја $\phi(m)$, $\phi(m) = {p_1}^{q_1} \cdot {p_2}^{q_2} \cdot \ldots \cdot {p_k}^{q_k}$;
- провјеримо да ли је број a^b, гдје је b дјелилац броја $\phi(m)$ и $b < \phi(m)$, конгруентан са 1 по модулу m;
- ред броја a је $\phi(m)$ ако и само ако ниједан од бројева облика a^b, гдје је b дјелилац броја $\phi(m)$ и $b < \phi(m)$, није конгруентан са 1 по модулу m.

Теорема 11. *Претпоставимо да је* p *непаран прост број и нека је* g *примитивни коријен по модулу* p^k. *Ако је* g *непаран, тада је* g *примитивни коријен по модулу* $2p^k$*, а ако је* g *паран, тада је* $g + p^k$ *примитивни коријен по модулу* $2p^k$.

Доказ. Ако је g непаран, тада $g^j \equiv 1 \pmod 2$, $\forall j \geq 1$. Тако $g^j \equiv 1 \pmod{2p^k}$ ако и само ако $g^j \equiv 1 \pmod{p^k}$. Отуда ред броја g по модулу $2p^k$ је једнак са редом

броја g по модулу p^k, а то је $\phi(p^k)$. Како је $\phi(2p^k) = \phi(2) \cdot \phi(p^k) = \phi(p^k)$, g је примитивни коријен од $2p^k$.

Ако је g паран, тада g не може бити примитивни коријен од $2p^k$, јер примитивни коријен је увијек узајамно прост са модулом. Али $g + p^k$ је непаран, и како је конгруентан са g по модулу p^k, оно је такође и примитивни коријен по модулу p^k. Отуда, $g + p^k$ је примитивни коријен од $2p^k$ због већ наведеног аргумента $\phi(p^k) = \phi(2p^k)$. □

Примјер 13. *Из Примјера 11 имамо да је* 2 *примитивни коријен од* 5^k*, за свако* k*. Како је* 2 *паран, тада је* $2 + 5^k$ *примитивни коријен од* $2 \cdot 5^k$*, за свако* k*.*

За $k = 1$*, слиједи да је* 7 *примитивни коријен од 10, тј.* $7^{\phi(10)} \equiv 1 \pmod{10}$*. Како је* $\phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(5) = 1 \cdot 4 = 4$*, то је* $7^4 \equiv 1 \pmod{10}$*.*
На сличан начин, за $k = 2$ *добијамо да је* 27 *примитивни коријен од* 50*.*

Примјер 14. *Већ смо имали прилике да видимо да је* 17 *примитивни коријен од* $25 = 5^2$*. На тај начин,* 17 *је примитивни коријен од* 5^k*, за свако* k*. Како је* 17 *непаран, то повлачи да је* 17 *примитивни коријен од* $2 \cdot 5^k$*, за свако* k*.*

Теорема 12. *Примитивни коријен по модулу* m *постоји ако и само ако је* $m = 1, 2, 4, p^k$ *или* $2p^k$*, гдје је* p *непаран прост број и* k *произвољан природан број.*

Доказ. Примијетимо прво да $1, 2$ и 4 имају примитивне коријене ($1, 1$ и 3 редом).

$$1^{\phi(1)} \equiv 1 \pmod{1}, \qquad \phi(1) = 1;$$
$$1^{\phi(2)} \equiv 1 \pmod{2}, \qquad \phi(2) = 1;$$
$$3^{\phi(4)} \equiv 1 \pmod{4}, \qquad \phi(4) = 2.$$

Из претходних теорема већ смо видјели да p^k и $2p^k$ имају примитивне коријене кад год је p непаран прост број и k произвољан природан број.

Обратно, докажимо да су ово једини позитивни цијели бројеви који имају примитивне коријене. Претпоставимо да $m > 2$ има примитивни коријен. Конгруенција $x^2 \equiv 1 \pmod{m}$ има тачно 2 неконгруентна рјешења (јер $2 \mid \phi(m)$ за све $m \geq 3$). На основу теореме која нам говори о броју рјешења конгруенције $x^2 \equiv a \pmod{m}$, закључујемо да m мора бити 4, p^k или $2p^k$, гдје је p непаран прост број. □

Читаоци са основним знањем из теорије група могли су примијетити да доста појмова из овог поглавља су специјални случајеви општих појмова група.

Ако је G коначна група са неутралним елементом e, тада ред $\mathbf{ord}\, a$ елемента a је дефинисан као најмањи природан број, тако да $a^n = e$, док је ред групе $\mathbf{ord}\, G$ дефинисан као број елемената групе G. Ако $h = \mathbf{ord}\, a$, тада $h \mid \mathbf{ord}\, G$ и $\{e, a, a^2, \ldots, a^{h-1}\}$ је подгрупа групе G. Ова подгрупа се поклапа са G ако $\mathbf{ord}\, a = \mathbf{ord}\, G$, и G је тада циклична група са генератором a.

Примијенимо ове опште појмове на случај када је G група $\mathbb{Z}_m^*$ свих класа остатака по модулу m, који су узајамно прости са m. Видимо да, ред h цијелог броја a по модулу m се поклапа са редом класе остатака $\overline{a}$ у $\mathbb{Z}_m^*$. Како $h \mid \phi(m)$, то је g примитивни коријен по модулу m ако и само ако класа остатака $\overline{g}$ генерише $\mathbb{Z}_m^*$. Тада постоји примитивни коријен по модулу m ако и само ако је група $\mathbb{Z}_m^*$ циклична група.

Служећи се језиком група, *Теорему 11* ћемо преформулисати: Група $\mathbb{Z}_m^*$ је циклична ако и само ако је $m = 1, 2, 4, p^k$ или $2p^k$, гдје је p непаран прост број и k произвољан природан број.

2.1 Артинова претпоставка

До сада смо одређивали примитивне коријене a по модулу p. Покушаћемо да одговоримо на питање, постоји ли бесконачно много простих бројева p за које је a примитивни коријен. Овим питањем се бавио и њемачки математичар Гаус, који је поставио питање колико често је 10 примитивни коријен по модулу p, али није изнио конкретну претпоставку. Прецизнију претпоставку је изнио аустријски математичар Е.Артин 1927. године.[5]

Артинова претпоставка: *За било који ненулти цијели број a, осим $1, -1$ или потрпуног квадрата, постоји бесконачно много простих бројева p за које је a примитивни коријен по модулу p.*

Није познато да Артинова претпоставка постоји за јединствени цијели број a, али је познато да постоје највише два проста броја за које претпоставка не важи. На примјер, бар један од бројева 3, 5 и 7 је примитивни коријен по модулу сваког другог простог броја , али је тренутно непознато за које претпоставка важи.[3]

Артин је имао дубљи утицај на обликовање математике нашег времена. Његов дубљи увид у класу теорије поља, водили су до развоја модерне теорије бројева. Артинова претпоставка је један познати примјер његове математичке интуиције и креативности. Она је кључна тачка разних области математике као што је теорија група, алгебарска и аналитичка теорија бројева, алгебарска геометрија. У ствари, Артинова мотивација потиче од алгебарске теорије бројева. Његова интуиција је била следећа.

Ако је a примитивни коријен по модулу p, тада је неопходно и довољно да

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p},$$

за сваки прост дјелилац q од $p-1$. Ако је k ред броја a по модулу p, тада $k \mid p-1$ и ако $k \neq p-1$, тада $k \mid \frac{p-1}{q}$ за неки прости дјелилац q од $p-1$. Дакле, a је примитивни коријен по модулу p, ако се "догађаји"

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

не догоде, односно ако не постоји прост број q који задовољава оба услова. Да би преокренули проблем, фиксирајмо q и нађимо вјероватноћу да прост број p задовољава оба услова. По Дирихлеовој теореми, $p \equiv 1 \pmod{q}$ важи за просте бројева p са вјероватноћом $\frac{1}{q-1}$. Могло би се очекивати, да $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ се јавља са вјероватноћом $\frac{1}{q}$. Вјероватноћа оба догађаја је $\frac{1}{q(q-1)}$, будући да се може претпоставити да су они независни. Да би се увјерили да је a примитивни коријен по модулу p, оба догађаја се не смију догодити за свако q. Долазимо до вјероватноће $\prod_q \left(1 - \frac{1}{q(q-1)}\right)$ за такве просте бројеве. Управо овај производ

$$\mathcal{C}_{Artin} = \prod_q \left(1 - \frac{1}{q(q-1)}\right) = 0,3739558136\ldots$$

је познат као **Артинова константа**.

Неколико година касније, 1983. године, доказано је да постоји скуп од 13 бројева таквих да за најмање један од 13 таквих бројева, Артинова претпоставка је тачна. Касније је тај скуп смањен на 7 бројева. Међутим, прецизнији резултат је дат у сљедећој теореми.

Теорема 13. *Један од бројева* 2,3,5 *је примитивни коријенпо модулу* p*, за бесконачно много простих бројева* p*.*

Доказ. Да би a био примитивни коријен по модулу p, неопходно је и довољно да за сваки прост број q важи

$$p \equiv 1 \pmod{q} \implies a^{\frac{p-1}{q}} \not\equiv 1 \pmod{q}. \tag{1}$$

Користећи овај критеријум, неколико математичара 19. вијека примијетило је да је 2 примитивни коријен по модулу p, кад год је p облика $4q+1$, гдје је q прост број. У том случају, $p-1$ има једино два проста дјелиоца 2 и q. Како је q непаран,

$$p = 4q + 1 = 4(2k+1) + 1 = 8k + 5 \equiv 5 \pmod{8}$$

и

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

као посебан случај квадратног остатка. Такође, важи да $2^{\frac{p-1}{q}} = 2^4 \equiv 1 \pmod{p}$ што даље имплицира да је p једнако 3 или 5 и ниједан од ових бројева није облика $4q+1$. Дакле, (1) је задовољен и 2 је примитивни коријен по модулу p. Проблем израчунавања да ли постоји бесконачно много простих бројева облика $\frac{p-1}{4}$ је нерјешив. Међутим, познато је по методи сита да је $\frac{p-1}{4}$ често производ највише два проста броја и оба та проста броја су већа од p^θ, $\theta > \frac{1}{4}$. Према томе, нема много услова одређених условима (1) који би обезбиједили да је a примитивни коријен по модулу p за све просте бројеве. Ово је суштинска чињеница која нам омогућава да докажемо теорему.

□

Примјер 15. *У претходној теореми показано је да је* 2 *примитивни коријен по модулу* p*, за бесконачно много простих бројева* p*. Навешћемо првих* 50 *простих бројева за које је* 2 *примитивни коријен. То су бројеви:* 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197, 211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461, 467, 491, 509, 523, 541, 547, 557, 563, 587, 613, 619, 653, 659, 661.

Глава 3

Аритметичке функције

Функције које су дефиницисане на скупу природних бројева а чији је кодомен подскуп скупа $\mathbb{R}(\mathbb{C})$ зову се **аритметичке функције**. Међу аритметичким функцијама разликујемо двије врсте: мултипликативне и адитивне функције.

Ми смо до сада већ разматрали неке аритметичке функције, а то је Ојлерова функција. Друге битне аритметичке функције које ћемо разматрати у овом поглављу су:

- $\tau(n)$ - број позитивних дјелилаца броја n;
- $\sigma(n)$ - збир позитивних дјелилаца броја n;
- $\sigma_k(n)$ - збир k-тих степена позитивних дјелилаца броја n.

Означимо са $\sum_{d|n} f(d)$ и $\prod_{d|n} f(d)$ збир и производ од $f(d)$, гдје је d позитивни дјелилац од n. Тако је, $\sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$.

Користећи ове ознаке, имамо

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

Примијетимо да су функције $\tau(n)$ и $\sigma(n)$ специјални случајеви од $\sigma_k(n)$, како је $\tau(n) = \sigma_0(n)$ и $\sigma(n) = \sigma_1(n)$.

Дефиниција 8. *Аритметичка функција $f(n)$ је* ***мултипликативна*** *ако није идентички једнака нули и задовољава услов $f(mn) = f(m)f(n)$, за сваки пар узајамно простих бројева m и n. Ако је $f(mn) = f(m)f(n)$ за сваки пар m и n, били узајамно прости или не, тада је $f(n)$* ***потпуно мултипликативна****.*

Ако је f мултипликативна функција, тада је $f(n) = f(n) \cdot f(1)$ за сваки позитиван цио број n. Како за n важи $f(n) \neq 0$, то повлачи да $f(1) = 1$. Користећи математичку индукцију, лако је доказати да ако су $m_1, m_2, \ldots, m_r$ у паровима прости бројеви, тада је $f(m_1 m_2 \ldots m_r) = f(m_1)f(m_2)\ldots f(m_r)$.

Нарочито ово важи кад год су $m_1, m_2, \ldots, m_r$ степени различитих простих бројева. Ако је $n = {p_1}^{k_1}{p_2}^{k_2}\ldots{p_r}^{k_r}$ факторизација цијелог броја n, $n > 1$, као производ степена различитих простих бројева, тада $f(n) = f({p_1}^{k_1})f({p_2}^{k_2})\ldots f({p_r}^{k_r})$. Дакле, вриједност од $f(n)$, за свако n је у потпуности дјељива са вриједношћу $f(p^k)$, за све степене простих бројева.

Већ знамо да је функција $\phi(n)$ мултипликативна и користили смо ову чињеницу за добијање формуле за $\phi(n)$. Наша сљедећа теорема доноси општи метод за конструкцију мултипликативних функција.

Теорема 14. *Нека је $f(n)$ мултипликативна функција, и нека је $F(n) = \sum_{d|n} f(d)$. Тада је $F(n)$ мултипликативна.*

Доказ. Нека је $\mathbf{нзд}(m, n) = 1$. Ако $d \mid mn$, тада $d = d_1 d_2$, гдје $d_1 \mid m$ и $d_2 \mid n$. Штавише, $d_1 = \mathbf{нзд}(m, d)$, $d_2 = \mathbf{нзд}(n, d)$ и $\mathbf{нзд}(d_1, d_2) = 1$, и факторизација је јединствена. Због тога,

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) = \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) =$$

$$= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = F(m)F(n).$$

□

Посљедица 4. *i) Функције $\tau(n)$, $\sigma(n)$ и генерално $\sigma_k(n)$ су мултипликативне.*

ii) Ако $n = {p_1}^{k_1} {p_2}^{k_2} \dots {p_r}^{k_r}$, тада

$$\tau(n) = \prod_{j=1}^{r} (k_j + 1) \qquad и \qquad \sigma(n) = \prod_{j=1}^{r} \left(\frac{{p_j}^{k_j+1} - 1}{p_j - 1} \right).$$

Доказ. i) Како $\sigma_k(n) = \sum_{d|n} d^k$ и функција $f(n) = n^k$ је (потпуно) мултипликативна, то повлачи претходна теорема да је $\sigma_k(n)$ мултипликатовна. Функције $\tau(n)$ и $\sigma(n)$ су специјални случајеви.

ii) Позитивни дјелиоци од p^k су $1, p, p^2, \dots, p^k$ и отуда $\tau(p^k) = k + 1$ и $\sigma(p^k) = \sum_{j=0}^{k} p^j = \frac{p^{k+1} - 1}{p - 1}$. Одавде слиједе формуле за $\tau(n)$ и $\sigma(n)$. □

Теорема 15. *За сваки природан број n, важи $\sum_{d|n} \phi(d) = n$.*

Доказ. Нека је $F(n) = \sum_{d|n} \phi(d)$. Тада је $F(n)$ мултипликативна, *по Теореми 12.* Како је функција $G(n) = n$ такође мултипликативна, довољно је доказати да је $F(p^k) = p^k$, за све степене простих бројева p^k, да би се доказало да је $F(n) = n$, за свако n. Како је $\phi(p^j) = p^j - p^{j-1}$ за $j \geq 1$, отуда

$$F(p^k) = \sum_{d|p^k} \phi(d) = \sum_{j=0}^{k} \phi(p^j) = 1 + \sum_{j=1}^{k} (p^j - p^{j-1}) = p^k.$$

Овим је теорема доказана. □

Нека је $f(n)$ аритметичка функција и дефинишимо $F(n) = \sum_{d|n} f(n)$. Да ли је функција f јединствено одређена функцијом F ? Имамо:

$$\begin{cases} F(1) = f(1) \\ F(2) = f(1) + f(2) \\ F(3) = f(1) + f(3) \\ F(4) = f(1) + f(2) + f(4) \\ F(5) = f(1) + f(5) \\ \quad \vdots \\ F(n) = f(1) + \cdots + f(n), \qquad \text{за } f(d), \text{кад } d \mid n. \end{cases}$$

Ово се може посматрати као систем линеарних једначина, гдје су $f(1)$, $f(2)$,..., $f(n)$ непознате. Очигледно је да је $f(n)$ линеарна комбинација $F(1), F(2), \ldots, F(n)$ са цјелобројним коефицијентима. Функција f је јединствено одређена функцијом F. Наш сљедећи циљ је да изведемо формулу за $f(n)$, за шта ће нам бити потребна сљедећа дефиниција.

Дефиниција 9. *Дефинишимо*

$$\mu(n) = \begin{cases} 1, & \textit{ако } n = 1 \\ 0, & \textit{ако је } n \textit{ дјељиво са } p^2, \textit{ гдје је } p \textit{ прост број} \\ (-1)^r, & \textit{ако је } n = p_1 p_2 \ldots p_r, \textit{ гдје су } p_1, p_2, \ldots, p_r \textit{ различити прости} \\ & \textit{бројеви.} \end{cases}$$

Функција μ је ***Мебијусова μ-функција****.*

Примјер 16. *Вриједности Мебијусове функције за првих 10 природних бројева.[7]*

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

Теорема 16. *Функција $\mu(n)$ је мултипликативна и*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{за } n = 1 \\ 0, & \text{за } n > 1. \end{cases}$$

Доказ. Мултипликативност је очигледна. Дефинишимо $F(n) = \sum_{d|n} \mu(d)$. Тада је $F(n)$ мултипликативна, по *Теореми 12.* Како је $\mu(p) = -1$ и $\mu(p^j) = 0$ за $j \geq 2$, имамо да важи $F(p^k) = \sum_{j=0}^{k} \mu(p^j) = \mu(1) + \mu(p) = 1 - 1 = 0$, за све просте бројеве p и за све $k \geq 1$. Отуда, $F(n) = 0$ за све $n > 1$, и важи $F(1) = \mu(1) = 1$. □

Примјер 17. *Израчунајмо вриједност Мебијусове функције за* 45, 102 *и* 2805.

$\mu(45) = \mu(3^2 \cdot 5) = \mu(3^2) \cdot \mu(5) = 0 \cdot (-1) = 0$

$\mu(102) = \mu(2 \cdot 3 \cdot 17) = \mu(2) \cdot \mu(3) \cdot \mu(17) = (-1)(-1)(-1) = -1$

$\mu(2805) = \mu(3 \cdot 5 \cdot 11 \cdot 17) = \mu(3) \cdot \mu(5) \cdot \mu(11) \cdot \mu(17) = (-1)^4 = 1$

Теорема 17. ***(Мебијусова инверзна формула)*** *Нека је f произвољна аритметичка функција. Ако је $F(n) = \sum_{d|n} f(d)$ за сваки природан број n, тада је*

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

Доказ. Користећи дефиницију функције F, добијамо

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{k|\left(\frac{n}{d}\right)} f(k) = \sum_{\substack{dk|n \\ \forall d,k}} \mu(d) f(k).$$

Сада можемо промијенити редосљед сумирања и задњу суму написати у облику,

$$\sum_{\substack{dk|n \\ \forall d,k}} \mu(d) f(k) = \sum_{k|n} f(k) \sum_{d|\left(\frac{n}{k}\right)} \mu(d).$$

Према *Теореми 14*, $\sum_{d|\left(\frac{n}{k}\right)} \mu(d) = 0$, осим за $k = n$, када је вриједност 1. Отуда,

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

Овим је теорема доказана. □

Такође важи и сљедећа супротност. Слиједи теорема.

Теорема 18. *Ако је* $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$ *за свако* $n \in \mathbb{N}$, *тада је*

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

Доказ. Дефинишимо $G(n) = \sum_{d|n} f(d)$. Тада је $f(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$ по претходној теореми. Према томе,

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

важи за свако n. Индукцијом ћемо показати да је $F(n) = G(n)$, за свако $n \in \mathbb{N}$.

Нека је $n = 1$, тада $\mu(1)F\left(\frac{1}{1}\right) = \mu(1)G\left(\frac{1}{1}\right)$, па је $F(1) = G(1)$. Претпоставимо да је $F(m) = G(m)$, за свако $m < n$. Како је $\frac{n}{d} < n$, за све позитивне дјелиоце d од n, осим за $d = 1$, израз (1) сада поједностављујемо па $\mu(1)F\left(\frac{n}{1}\right) = \mu(1)G\left(\frac{n}{1}\right)$ и закључујемо да $F(n) = G(n)$. Овим завршавамо индукцију. □

Табела примитивних коријена за првих 20 природних бројева

n	**Примитивни коријени по модулу n**	**Ред**
1	0	1
2	1	1
3	2	2
4	3	2
5	2, 3	4
6	5	2
7	3, 5	6
8	/	/
9	2, 5	6
10	3, 7	4
11	2, 6, 7, 8	10
12	/	/
13	2, 6, 7, 11	12
14	3, 5	6
15	/	/
16	/	/
17	3, 5, 6, 7, 10, 11, 12, 14	16
18	5, 11	6
19	2, 3, 10, 13, 14, 15	18
20	/	/

Библиографија

[1] Lars-Ake Lindahl, *Lectures on Number Theory*, 2002.

[2] М.Станић, Н.Икодиновић, *Теорија бројева*, збирка задатака, 2004.

[3] Andrew Kobin, *Elementary Number Theory*, spring 2013.

[4] Michael Rosen, *Number Theory in Function Fields*, 2002.

[5] M.Ram Murty, *Artin's conjecture for primitive roots*, 2009.

[6] Rajiv Gupta, M.Ram Murty, *A remark on Artin's conjecture*, 1984.

[7] https://sr.wikipedia.org/sr-el/

[8] https://sh.wikipedia.org/wiki/Logaritam

[9] https://sh.wikipedia.org/wiki/Modularna$_a$*ritmetika*