Neke aritmetičke funkcije

Bencetić, Doris

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Doris Bencetić

Neke aritmetičke funkcije

Završni rad

Osijek, 2017.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Doris Bencetić

Neke aritmetičke funkcije

Završni rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2017.

Sadržaj

Uvod **i**

1 Broj i suma djelitelja **1**

1.1 Broj djelitelja 1

1.2 Suma djelitelja 6

1.3 Savršeni i prijateljski brojevi i aritmetičke funkcije 8

2 Eulerova funkcija **11**

2.1 Definicija i svojstva 11

2.2 Eulerov teorem i primjene 16

Literatura **19**

Sažetak

U ovome radu proučit ćemo aritmetičke funkcije broj i suma djelitelja te Eulerovu funkciju. Upoznat ćemo se s njihovim osnovnim svojstvima, objasniti kako se računa vrijednost pojedine funkcije za bilo koji prirodan broj n te sve upotpuniti odgovarajućim primjerima. Također, iskazat ćemo i dokazati Eulerov teorem koji je usko vezan uz Eulerovu funkciju, a ima primjene u mnogim područjima teorije brojeva i kriptografije.

Ključne riječi

Broj djelitelja, suma djelitelja, Eulerova funkcija, Eulerov teorem, Mali Fermatov teorem, multiplikativna funkcija, kongruencije, prosti brojevi.

Summary

In this paper, we will consider some arithmetic functions such as sum and number of divisors of positive integer and Euler's function. We will talk about their basic properties, explain how to calculate their value for any positive integer n and illustrate all of that with suitable examples. Moreover, we will state and prove the Euler's theorem whose constituent part is Euler's function. It has lots of applications in many areas of number theory and cryptography.

Key words

Number of divisors function, sum of divisors function, Euler's function, Euler's theorem, Fermat's little theorem, multiplicative function, congruences, prime numbers.

Uvod

Od davnina, znanstvenici iz područja teorije brojeva proučavaju mnoge različite aritmetičke funkcije poznate i pod nazivom *funkcije teorije brojeva*. Ovaj skup čine sve funkcije koje za domenu imaju skup pozitivnih cijelih brojeva $\mathbb{Z}^+$, a kodomena im je neki podskup skupa kompleksnih brojeva $\mathbb{C}$. Aritmetičke funkcije opisuju aritmetička svojstva brojeva, a od ostalih funkcija razlikuju se u tome što ne mogu biti opisane jednostavnim formulama već se ocjenjuju u terminima prosječne vrijednosti i asimptotskog ponašanja. Imaju široku primjenu u svim granama matematike, a jedna od najbitnih primjena je u kriptografiji. Naime, aritmetičke funkcije baza su raznih metoda šifriranja i dešifriranja poruka.
U prvom poglavlju ovoga rada upoznat ćemo se s funkcijama *broj* i *suma djelitelja*. Navest ćemo njihova najznačajnija svojstva, objasniti kako se računa vrijednost tih funkcija te pokazati kako zadovoljavaju svojstvo multiplikativnosti. Osim toga, uvest ćemo pojmove *prijateljski* i *savršeni brojevi*.
U drugom poglavlju bavit ćemo se *Eulerovom funkcijom*, u oznaci φ. Iskazat ćemo i dokazati *Eulerov teorem* čiji sastavni dio je upravo *Eulerova funkcija*, te na primjeru pokazati primjenu ovoga teorema u rješavanju linearnih kongruencija. Spomenut ćemo i *Carmichaelove* i *pseudoproste brojeve*.

1 Broj i suma djelitelja

Prije same definicije funkcijâ *broj djelitelja* i *suma djelitelja* definirat ćemo neke osnovne pojmove potrebne za razumijevanje sadržaja ovog završnog rada te iskazati *Osnovni teorem artimetike* koji je jako bitan u proučavanju svojstava navedenih funkcija.

Definicija 1. *Neka su* $m, n \in \mathbb{Z}, m \neq 0$. *Ako postoji* $d \in \mathbb{Z}$ *takav da vrijedi*

$$n = m \cdot d$$

kažemo da m *dijeli* n *i označavamo* $m|n$. *Broj* n *nazivamo višekratnikom broja* m, *a broj* m *djeliteljem broja* n.

Primjer 1. *Broj* 6 *dijeli broj* 48 *(pišemo* $6|48$*), tj. postoji* $d = 8$ *takav da je*

$$48 = 6 \cdot 8.$$

Broj 48 *nazivano višekratnikom broja* 6, *a broj* 6 *djeliteljem broja* 48 .

Definicija 2. *Prirodan broj* $n, n > 1$ *je prost broj ako nema djelitelja* d *takvog da vrijedi* $1 < d < n$; *u suprotnom je broj* n *složen broj.*

Primjer 2. *Broj* 37 *je prost broj,a broj* $49 = 7 \cdot 7$ *nije prost broj.*

Više o svojstvima djeljivosti i prostim brojevima može se vidjeti primjerice u [2].

Teorem 1 (Osnovni teorem aritmetike, vidi [6, Teorem 1.4.3.])**.** *Prikaz svakog prirodnog broja većeg od* 1 *u obliku produkta potencija prostih brojeva je jedinstven do na poredak faktora.*

Primjer 3. *Broj* 1200 *zapisan u obliku produkta potencija prostih brojeva izgleda ovako:*

$$1200 = 2^4 \cdot 3 \cdot 5^2.$$

1.1 Broj djelitelja

Definicija 3. *Neka je* $n \in \mathbb{N}$. *Brojem* $\tau(n)$ *definiramo broj svih pozitivnih djelitelja broja* n.

Koristeći modifikaciju Eratostenovog sita, algoritma za dobivanje svih prostih brojeva manjih od unaprijed izabranog prirodnog broja, možemo napisati tablicu koja odgovara funkciji τ. Kako bismo pronašli vrijednost naše funkcije τ, za $n \leq a$ zapišemo brojeve $1, 2, \ldots, a$ i podvučemo crticu ispod svakog od njih. U sljedećem koraku podvučemo drugu crticu ispod broja 2 te svih onih brojeva koji su djeljivi s 2; zatim podvučemo treću crticu ispod broja 3 te ispod svih brojeva djeljivih s 3. Postupak nastavljamo na ovaj način i na kraju podvučemo crticu ispod broja a. Vrijednost funkcije $\tau(n)$ jednaka je broju crtica ispod broja n.

Pogledajmo kako navedena metoda izgleda na primjeru broja $a = 10$:

$$\underline{1}, \underline{\underline{2}}, \underline{\underline{3}}, \underline{\underline{\underline{4}}}, \underline{\underline{5}}, \underline{\underline{\underline{6}}}, \underline{\underline{7}}, \underline{\underline{\underline{8}}}, \underline{\underline{9}}, \underline{\underline{\underline{10}}}.$$

Dakle,

$$\tau(1) = 1, \tau(2) = 2, \tau(3) = 2, \tau(4) = 3, \tau(5) = 2,$$
$$\tau(6) = 4, \tau(7) = 2, \tau(8) = 4, \tau(9) = 3, \tau(10) = 4.$$

Navedimo sada nekoliko važnih rezultata o djeliteljima i broju djelitelja proizvoljnog prirodnog broja n.

Teorem 2 (vidi, [2, Theorem 1,CH IV]). *Ako je n prirodan broj čija je faktorizacija dana s*

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}, \quad k \in \mathbb{N} \tag{1}$$

i ako su

$$\lambda_1, \lambda_2, \dots, \lambda_k \tag{2}$$

međusobno različiti skalari iz $\mathbb{N}$ ili $\mathbb{Z}$ ili $\mathbb{R}$ koji zadovoljavaju svojstvo

$$0 \leq \lambda_i \leq \alpha_i, i = 1 \dots n, \tag{3}$$

onda su svi djelitelji broja n oblika

$$d = q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_k^{\lambda_k}. \tag{4}$$

Nadalje, svakom skupu brojeva $\{\lambda_1, \lambda_2, \dots, \lambda_k\}$ odgovara točno jedan djelitelj d.

Dokaz.

Neka je $n \in \mathbb{N}$ veći od 1 i neka je (1) prikaz prirodnog broja n u obliku produkta potencija prostih brojeva. Neka je d djelitelj broja n. Kako je svaki djelitelj broja d ujedno i djelitelj broja n, tada se u faktorizaciji broja d, mogu pojaviti samo oni faktori koji su i u (1). Prema tome, svaki djelitelj broja d je oblika (4) i vrijedi $0 \leq \lambda_i \leq \alpha_i$, $i = 1, 2, \dots, k$. S druge strane, očito je da svaki broj d koji se može napisati u obliku (4), za koji je $0 \leq \lambda_i \leq a_i$, $i = 1, 2, \dots, k$, ujedno i djelitelj broja n. Naime, (3) povlači

$$\frac{n}{d} = q_1^{\alpha_1 - \lambda_1} q_2^{\alpha_2 - \lambda_2} \cdots q_k^{\alpha_k - \lambda_2}$$

i to je cijeli broj.
Na kraju, očito je da za različit izbor brojeva $\lambda_1, \lambda_2, \dots, \lambda_k$ koji zadovoljavaju (3) dobivamo različite brojeve u (4). □

Primjer 4. *Uzmimo broj iz prethodnog primjera*

$$1200 = 2^4 \cdot 3 \cdot 5^2.$$

i pogledajmo neke njegove djelitelje. Imamo:

$$600 = 2^3 \cdot 5^2 \cdot 3$$
$$400 = 2^4 \cdot 5^2$$
$$40 = 2^3 \cdot 5$$
$$4 = 2^2.$$

Zaista uočavamo da su svi djelitelji broja 1200 *u obliku produkta potencija brojeva* $2, 3$ *i* 5.

Teorem 3 (vidi [2, Theorem 2,CH IV])**.** *Broj djelitelja prirodnog broja* n *čiji je rastav na proste faktore dan kao u* (1) *je oblika*

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1). \tag{5}$$

Dokaz.

Broj djelitelja prirodnog broja n čija je faktorizacija dana s (1) jednaka je broju skupova cijelih brojeva $\{\lambda_1, \lambda_2, \ldots, \lambda_k\}$, $k \in \mathbb{N}$ koji zadovoljavaju nejednakost (3). Jednostavim računom zaključimo koliko tih sustava ima. Kako bi cijeli broj λ_i zadovoljavao nejednakost (3) nužno je i dovoljno da λ_i pripada skupu

$$0, 1, 2, \ldots, \alpha_i,$$

pa za dani $i = 1, 2, \ldots, k$ broj λ_i može imati $\alpha_i + 1$ različitih vrijednosti.

□

Primjer 5. *Rastavimo broj* 540 *na proste faktore.*
Rješenje:
Imamo

$$540 = 2^2 \cdot 3^3 \cdot 5.$$

Iz (3) *slijedi kako je broj djelitelja broja* 540 *jednak*

$$\tau(540) = (2 + 1)(3 + 1)(1 + 1) = 24.$$

Primjer 6. *Pronađimo najmanji prirodan broj koji ima točno 24 djelitelja.*
Rješenje:
Ako je $\tau(n) = 24$*, iz* (3) *slijedi* $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1) = 24$*, Postoji samo 6 načina rastava broja 24 na proste faktore:* $3 \cdot 2 \cdot 2 \cdot 2 = 4 \cdot 3 \cdot 2 = 6 \cdot 4 = 6 \cdot 2 \cdot 2 = 8 \cdot 3 = 12 \cdot 2 = 24$.

Naši kandidati su oblika:

$$\begin{aligned} 2^{3-1}\cdot 3^{2-1}\cdot 5^{2-1}\cdot 7^{2-1} &= 420\\ 2^{4-1}\cdot 3^{3-1}\cdot 5^{2-1} &= 360\\ 2^5\cdot 3^3 &= 2592\\ 2^5\cdot 3\cdot 5 &= 480\\ 2^{11}\cdot 3 &= 6144\\ 2^{23} &= 8388608. \end{aligned}$$

Izaberemo najmanji, dakle broj 360 je naše rješenje.

Funkcija τ ima puno korisnih svojstava. Primjerice, može se pokazati da je za bilo koji prirodan broj n, $\tau(n)$ neparan broj ako i samo ako je n potpun kvadrat. Naime, ako je $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, $k \in \mathbb{N}$ tada je

$$\tau(n) = \prod_{j=1}^{k}(\alpha_{j+1}) = (\alpha_1+1)\cdots(\alpha_k+1).$$

Broj n je potpun kvadrat ako i samo ako vrijedi $n = m^2, m \in \mathbb{Z}$. Prethodna jednakost vrijedi ako i samo ako su sve potencije α_i parni brojevi za $i = 1,\ldots,k$, a to vrijedi ako i samo ako su svi $\alpha_i + 1$ neparni. Dakle, polazna jednakost vrijedi ako i samo ako je $\tau(n)$ neparan broj.

Osim toga, za svaki prirodan broj n vrijedi sljedeća jednakost

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}.$$

Zaista, ako n nije potpun kvadrat, onda je $\tau(n)$ paran pa imamo

$$\prod_{d|n} d = 1\cdot d_1\cdot d_2\cdots d_l\cdot\frac{n}{d_l}\cdots\frac{n}{d_1}\cdot n.$$

Grupiramo prvi i posljednji član pa dobivamo $1\cdot\frac{n}{1} = n$, zatim grupiramo drugi i pretposljednji član $d_1\cdot\frac{n}{d_1}$ i analogno nastavimo. Kako se s desne strane jednakosti nalazi $\tau(n)$ elemenata vrijedi sljedeće

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}.$$

Obratno, ako je n potpun kvadrat, onda je $\tau(n)$ neparan i vrijedi

$$\prod_{d|n} d = 1\cdot d_1\cdot d_2\cdots d_l\cdot\sqrt{n}\cdot\frac{n}{d_l}\cdot\frac{n}{d_l-1}\cdots\frac{n}{d_2}\cdot\frac{n}{d_1}\cdot\frac{n}{1}.$$

Analogno prethodnom zaključujemo da s desne strane jednakosti imamo $\frac{\tau(n)-1}{2}$ elemenata

plus središnji element $\sqrt{n}$ pa slijedi

$$\begin{aligned}\prod_{d|n} d &= n^{\frac{\tau(n)-1}{2}} \cdot \sqrt{n} \\ &= n^{\frac{\tau(n)-1}{2}+\frac{1}{2}} \\ &= n^{\frac{\tau(n)}{2}}.\end{aligned}$$

Nadalje, jedno od važnijih svojstava funkcije $\tau(n)$ je njena multiplikativnost. Naime, općenito vrijedi:

Definicija 4. *Funkcija $f : \mathbb{N} \to \mathbb{C}$ takva da vrijedi $f(x \cdot y) = f(x) \cdot f(y)$, gdje su x i y relativno prosti te $f(1) = 1$ naziva se multiplikativna funkcija.*

Multiplikativne funkcije su od velikog značaja u razvoju modernih kriptografskih sustava kojima je cilj omogućiti slanje poruka u takvom obliku da ih samo onaj kojem su namjenjene može pročitati. Naime, mnoge kriptografske aplikacije oslanjaju se na korištenje jako velikih brojeva, koji imaju i po tisuće znamenki, kako bi šifrirale informacije. Sigurnost informacija često ovisi o težini izokretanja vrijednosti pojedinih brojeva i upravo zbog toga se uzimaju multiplikativne funkcije s obzirom da one omogućavaju brzo i efikasno računanje.
Pokažimo da je $\tau(n)$ zaista multiplikativna funkcija.
Neka su x i y relativno prosti prirodni brojevi tj. vrijedi $(x, y) = 1$. Rastavimo ih na proste faktore na sljedeći način:

$$\begin{aligned}x &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \\ y &= q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}.\end{aligned}$$

Budući da su x i y relativno prosti, mora biti $p_i \neq q_j$, za svaki $i, j = 1, \ldots, k$. Tada je

$$x \cdot y = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k},$$

pa prema Teoremu 1 slijedi:

$$\tau(xy) = (\alpha_1 + 1) \cdots (\alpha_k + 1)(\beta_1 + 1) \cdots (\beta_k + 1) = \tau(x) \cdot \tau(y).$$

Pokažimo to i na primjeru:

Primjer 7. *Jer je $(7, 3) = 1$, imamo*

$$\tau(7 \cdot 3) = (1 + 1)(1 + 1) = 4.$$

S druge strane,

$$\tau(7) \cdot \tau(3) = 2 \cdot 2 = 4.$$

Sljedećim primjerom naglasit ćemo nužnost uvjeta $(x, y) = 1$. Naime, ako je $(x, y) \neq 1$, ne mora biti $\tau(xy) = \tau(x) \cdot \tau(y)$.

Primjer 8. *Neka je $x = 3$, $y = 4$. Vrijedi:*

$$\tau(x) \cdot \tau(y) = \tau(3) \cdot \tau(3 \cdot 4^2) = 2 \cdot 2 \cdot 3 = 12.$$

Osim toga,

$$\tau(x) \cdot \tau(y) = \tau(3^2 \cdot 4^2) = 3 \cdot 3 = 9,$$

pa zaključujemo da je $\tau(xy) \neq \tau(x) \cdot \tau(y)$.

Kao što smo već i napomenuli, aritmetičke funkcije imaju različite primjene. Primjerice, funkcija τ pojavljuje se u razvoju specifičnih funkcija u beskonačne redove. Pogledajmo Lambertov red potencija

$$\sum_{n=1}^{\infty} a_n \frac{x^n}{1-x^n}, \quad |x| < 1.$$

Za $a_n = 1$ imamo

$$\sum_{n=1}^{\infty} \frac{x^n}{1-x^n} = \frac{x}{1-x} + \frac{x^2}{1-x^2} + \dots$$

Jer je $x^n + x^{2n} + x^{3n} + \dots = \frac{x^n}{1-x^n}$, dobivamo

$$\sum_{n=1}^{\infty} \frac{x^n}{1-x^n} = \sum_{k=1}^{\infty} \sum_{l=1}^{\infty} x^{kl}.$$

U toj dvostrukoj sumi za svaki prirodan broj n, potencija x^n pojavljuje se onoliko puta koliko i rješenje jednadžbe $k \cdot l = n$ u prirodnim brojevima k i l, tj. pojavljuje se $\tau(n)$ puta. Dakle, za $|x| < 1$ imamo

$$\sum_{n=1}^{\infty} \frac{x^n}{1-x^n} = \sum_{n=1}^{\infty} \tau(n) x^n.$$

Vidimo da je naša funkcija $\tau(n)$ koeficijent uz x^n u razvoju Lambertovog reda u red potencija.

1.2 Suma djelitelja

Nakon prvog djela rada u kojem smo se bavili brojem djelitelja nekog prirodnog broja n, priodno je zapitati se kolika je njihova suma.

Definicija 5. *Neka je $n \in \mathbb{N}$. Sa $\sigma(n)$ definiramo sumu svih pozitivnih djelitelja prirodnog broja n.*

Iskazati ćemo i dokazati teroem koji nam govori o tome na koji se način računa vrijednost $\sigma(n)$, $n \in \mathbb{N}$.

Teorem 4 (vidi, [2, Theorem 3,CH IV])**.** *Suma prirodnih djelitelja $\sigma(n)$ prirodnog broja n čija je faktorizacija dana s*

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}, \quad k \in \mathbb{N}$$

je oblika:

$$\sigma(n) = \frac{q_1^{\alpha_1+1} - 1}{q_1 - 1} \cdot \frac{q_2^{\alpha_2+1} - 1}{q_2 - 1} \cdots \frac{q_k^{\alpha_k+1} - 1}{q_k - 1}. \tag{6}$$

Dokaz.

Iz Teorema 2 slijedi: ako je $n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_k^{\alpha_k}$, tada vrijedi

$$\sigma(n) = \sum q_1^{\lambda_1} \cdot q_2^{\lambda_2} \cdots q_k^{\lambda_k}, \tag{7}$$

gdje sumacija ide po svim sustavima od k cijelih brojeva $\lambda_1, \ldots, \lambda_k$ koji zadovoljavaju $0 \leq \lambda_i \leq \alpha_i$.

Lako se vidi da je svaki pribrojnik iz (7) sadržan u proširenju produkta

$$(1 + q_1 + q_1^2 + \cdots + q_1^{\alpha_1})(1 + q_2 + q_2^2 + \cdots + q_2^{\alpha_2}) \ldots (1 + q_k + q_k^2 + \cdots + q_k^{\alpha_k})$$

točno jednom. S druge strane svaki član proširenja produkta je jedan od pribrojnika u (7). □

Pogledajmo kako to izgleda na primjeru:

Primjer 9. *Izračunajmo* $\sigma(540)$.
Rješenje:
Rastavimo broj 540 *na proste faktore. Imamo*

$$540 = 2^2 \cdot 3^3 \cdot 5.$$

Iz (6) *slijedi*

$$\sigma(540) = \sigma(2^2 \cdot 3^3 \cdot 5) = \frac{2^{2+1} - 1}{2 - 1} \cdot \frac{3^{3+1} - 1}{3 - 1} \cdot \frac{5^{1+1} - 1}{5 - 1} = 1680.$$

Funkcija $\sigma(n)$ je također multiplikativna funkcija. Pokažimo to:

Za bilo koji $p \in \mathbb{N}$ je $p^0 = 1$, pa prema formuli (6) vrijedi $\sigma(p^0) = \frac{p-1}{p-1} = 1$, tj. $\sigma(1) = 1$. Nadalje, iz definicije funkcije σ vidimo da za prost broj p vrijedi

$$\sigma(p^m) = 1 + p + p^2 + \cdots + p^m = \frac{p^{m+1} - 1}{p - 1}.$$

Najprije, promotrimo slučaj u kojem je prirodan broj n zapisan kao produkt potencija dva prosta broja p i q odnosno $n = p^m q^r$, $m, r > 0$.

$$\sigma(p^m q^r) = 1 + p + p^2 + \cdots + p^m + q + pq + p^2 q + \cdots + p^m q + \cdots + q^r + pq^r + p^2 q^r + \cdots + p^m q^r.$$

Ako ove brojeve grupiramo, dobivamo

$$\begin{aligned} \sigma(p^m q^r) &= (1 + p + p^2 + \cdots + p^m)(1 + q + q^2 + \cdots + q^r) \\ &= \frac{p^{m+1} - 1}{p - 1} \cdot \frac{q^{r+1} - 1}{q - 1} \\ &= \sigma(p^m)\sigma(q^r). \end{aligned}$$

To upravo znači da je σ multiplikativna funkcija. Generalizacijom ovog postupka dobivamo:

$$\sigma(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}) = \prod_{i=1}^{k}\frac{p_i^{\alpha_{i+1}}-1}{p_i-1} = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})\cdots\sigma(p_k^{\alpha_k}).$$

Koristeći Teorem 4 i multiplikativnost funkcije σ odredimo prvih nekoliko njenih vrijednosti:

$$\sigma(1)=1, \sigma(2)=3, \sigma(3)=4, \sigma(4)=7, \sigma(5)=6$$
$$\sigma(6)=12, \sigma(7)=8, \sigma(8)=15, \sigma(9)=13, \sigma(10)=18.$$

Uočavamo da je $\sigma(n) > n$ za $n > 1$, pa mora vrijediti i $\sigma(n) > 5$ za $n > 4$. Vidimo i da vrijednost funkcije σ za $n \leq 4$ iznosti 1, 3, 4 i 7. Stoga, ne postoji prirodan broj n za koji je $\sigma(n) = 5$. Tu slutnju nam potvrđuje i sljedeći teorem koji navodimo bez dokaza.

Teorem (vidi, [2, Theorem 4, CH IV]). *Postoji beskonačno mnogo prirodnih brojeva koji nisu vrijednost funkcije $\sigma(n)$, za dani prirodan broj n.*

Funkcija σ, slično kao i funkcija τ, pojavljuje se kao koeficijent u raznim razvojima u beskonačne redove. Primjerice, vrijedi

$$\sum_{k=1}^{\infty}\frac{kx^k}{1-x^k} = \sum_{n=1}^{\infty}\sigma(n)x^n, \quad |x|<1.$$

Postoje i razne druge aritmetičke funkcije, poput Möbiusove funkcije, funkcijâ pod $\lfloor\rfloor$ i strop $\lceil\rceil$, Smarandacheove funkcije , itd. Neka njihova svojstva mogu se vidjeti u [8] i [4].

1.3 Savršeni i prijateljski brojevi i aritmetičke funkcije

Definicija 6. *Za prirodan broj n kažemo da je savršen ako vrijedi*

$$\sigma(n) = 2n.$$

Poznato je samo 30 savršenih brojeva i svih 30 su parni brojevi. Još uvijek nije poznato postoji li neparan savršen broj no dokazano je da u slučaju da postoji tada on mora biti veći od 10^{50} i mora imati najmanje 8 različitih prostih faktora (vidi [2]).
Najveći poznat savršen broj je $2^{216090}(2^{216091}-1)$ i ima 1301000 znamenki.
Najmanji savršen broj je $6 = 1+2+3$, sljedeći je $28 = 1+2+4+7+14$, odmah iza njega $496 = 1+2+4+8+16+31+62+124+248$, itd.

Prvih osam savršenih brojeva rezimirano je u Tablici 1.

n	P_n
1	6
2	28
3	496
4	8128
5	33550336
6	8589869056
7	137438691328
8	2305843008139952128

Tablica 1: *Prvih osam savršenih brojeva* P_n

Navedimo sada jednu od najbitnijih karakterizacija savršenih brojeva.

Teorem 5 (vidi, [2, Theorem 5, CH IV])**.** *Paran broj n je savršen ako i samo ako se može prikazati u obliku*

$$n = 2^{s-1}(2^s - 1), \quad s > 1,$$

gdje je $2^s - 1$ *prost broj.*

Dokaz.

Neka je n paran prirodan broj. Tada ga možemo zapisati kao $n = 2^{s-1}l$, gdje je $s > 1$ i l neparan broj. Stoga slijedi

$$\sigma(n) = (2^s - 1)\sigma(l).$$

Prema definiciji savršenog broja slijedi $(2^s - 1)\sigma(l) = 2^s l$. Kako vrijedi $(2^s - 1, 2^s) = 1$ vidimo da je $\sigma(l) = 2^s q$, gdje je q prirodan broj. Dakle, $(2^s - 1)q = l$ što zbog $\sigma(l) = 2^s q$ implicira $\sigma(l) = l + q$. No kako je $(2^s - 1)q = l$ i $s > 1$ imamo $q|l$ i $q < l$. Stoga, broj l ima barem 2 različita prirodna djelitelja, q i l, i formula $\sigma(l) = l + q$ dokazuje da drugih djelitelja nema pa je l prost broj. No, $l = (2^s - 1)q = 2^s - 1$. Stoga, $n = 2^{s-1}l = 2^{s-1}(2^s - 1)$ pa je $2^s - 1$ prost broj. Time smo dokazali nužnost uvjeta.
S druge strane, neka je $2^s - 1$ neparan prirodan broj veći od 2. Nadalje, neka je $n = 2^{s-1}(2^s - 1)$. Sada imamo $\sigma(n) = (2^s - 1)\sigma(2^s - 1) = (2^s - 1)2^s$ jer je $2^s - 1$ prost broj. Dakle, $\sigma(n) = 2n$ što dokazuje da je n savršen broj. Time smo dokazali dovoljnost uvjeta te dokazali teorem.

□

Osim toga, može se pokazati i da broj oblika $2^{m-1}(2^m - 1)$, $m \in \mathbb{N}$ nije savršen, ako je $2^m - 1$ složen broj. Zaista, neka je $N = 2^{m-1}(2^m - 1)$. Pokažimo da $\sigma(N) \neq 2N$.

$$\begin{aligned}\sigma(n) &= \sigma(2^{m-1})\sigma(2^m - 1) \\ &= \frac{2^m - 1}{2 - 1}\sigma(2^m - 1) \\ &= (2^m - 1)\sigma(2^m - 1).\end{aligned}$$

Jer je $\sigma(2^m-1)$ zbroj jedinice, samog broja 2^m-1 i još nekih djelitelja koji sigurno postoje zbog toga što je 2^m-1 složen broj, a to je u sumi neki broj koji je veći od 2^m pa slijedi

$$\sigma(N) > 2 \cdot 2^{m-1} \cdot (2^m - 1) = 2N.$$

Napomena 1. *Ako je broj 2^s-1 prost, tada i broj s mora biti prost.*
Naime, ako je s=ab gdje su a i b prirodni brojevi veći od 1 tada imamo

$$2^s - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a}),$$

s obzirom da je $a > 1$ i $2^a - 1 \geq 2^2 - 1 \geq 3$, broj 2^s-1 je složen.

Još jedna korisna implikacija koja savršen broj n povezuje s njegovim djeliteljima d kaže da je prirodan broj n savršen ako i samo ako vrijedi $\sum_{d|n} d^{-1} = 2$. Naime, kako vrijedi $d|n \iff$ postoji d_1 takav da je $n = d_1 \cdot d \iff d = \frac{n}{d_1}$ slijedi

$$\sum_{d|n} d^{-1} = \sum_{d|n} \frac{1}{d} = \sum_{d_1|n} \frac{1}{\frac{n}{d_1}} = \sum_{d|n} \frac{d}{n} = \frac{1}{n} \sum_{d|n} d.$$

Dakle, vrijedi

$$\sum_{d|n} d^{-1} = 2 \iff \frac{1}{n} \sum_{d|n} d = 2 \iff \sum_{d|n} d = 2n.$$

Kako je $\sum_{d|n} d = \sigma(n) = 2n$, time smo pokazali da jednakost vrijedi ako i samo ako je n savršen.

Osim toga, može se pokazati i da je broj oblika $2 \cdot 3^\alpha$ savršen ako i samo ako je $\alpha = 1$. Naime, pokažimo da je $\sigma(2 \cdot 3^\alpha) = 2 \cdot (2 \cdot 3^\alpha) \iff \alpha = 1$. S jedne strane, pretpostavimo da je broj $2 \cdot 3^\alpha$ savršen, tada vrijedi

$$\sigma(2 \cdot 3^\alpha) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^{\alpha+1} - 1}{3 - 1} = \frac{3}{2}(3^{\alpha+1} - 1) = 2 \cdot 2 \cdot 3^\alpha.$$

Iz posljednje dvije jednakosti slijedi

$$3^{\alpha+1} - 1 = 8 \cdot 3^{\alpha-1} \iff 3^\alpha \cdot 3 - 1 = 8 \cdot 3^\alpha \cdot 3^{-1}.$$

Uzmemo li supstituciju $3^\alpha = t$ dobivamo $3t - 1 = \frac{8}{3}t$, tj. $8t = 9t - 3$, pa je $t = 3$. Konačno, uvrstimo li t nazad u supstituciju dobivamo $\alpha = 1$. S druge strane, ukoliko je $\alpha = 1$ tada je $2 \cdot 3 = 6$ a to je savršen broj.

Direktna posljedica prethodnog teorema je i sljedeći korolar:

Korolar 1. *Svi parni savršeni brojevi dani su izrazom $2^{p-1}(2^p - 1)$ gdje su p i $2^p - 1$ prosti brojevi.*

Upoznati ćemo se s još jednom skupinom brojeva koja je usko vezana uz aritmetičke funkcije.

Definicija 7. *Za dva prirodna broja m i n kažemo da su prijateljska ako vrijedi*
$\sigma(m) = \sigma(n) = m + n$.

Prvi par prijateljskih brojeva 220 i 284 otkrio je Pitagora, par savršenih brojeva $2^4 \cdot 23 \cdot 47$ i $2^4 \cdot 1151$ otkrio je Fermat, Euler ih je otkrio 59 a u novijim radovima autora Borho, Hoffman i Riele prezentirano ih je puno više (vidi [10] i [11]). Poznati su nam parovi u kojima su oba člana parna i oni u kojima su oba člana neparna, no još nije otkriven par savršenih brojeva u kojem je jedan član paran a drugi neparan, osim toga upitno je i to ima li savršenih brojeva beskonačno mnogo. Nadalje, L. E. Dickson uvodi i pojam uređen skup prijateljskih brojeva (više u [12]). Naime, uređen skup od n prirodnih brojeva je uređen skup prijateljskih brojeva ako vrijedi

$$\sigma(n_1) = \sigma(n_2) = \cdots = \sigma(n_k) = n_1 + n_2 + \cdots + n_k.$$

Primjetimo da se za $k = 2$ definicija svodi na definiciju uređenog para prijateljskih brojeva.

2 Eulerova funkcija

Eulerovu funkciju, u oznaci φ prvi je istraživao Euler još davne 1760. godine. Oznaku funkcije imamo zahvaljujući Gaussu koji ju je predstavio 1801. godine i iz toga razloga neki je autori nazivaju Gaussovom funkcijom.

2.1 Definicija i svojstva

Prije same definicije funkcije upoznajmo se s nekim pojmovima potrebnim za razumijevanje sljedećeg gradiva.

Definicija 8. *Neka je n prirodan broj, a i b cijeli brojevi. Ako n dijeli razliku $(a-b)$ kažemo da je a kongruentan b modulo n i pišemo*

$$a \equiv b (\bmod n).$$

Primjer 10.
a) $38 \equiv 14 (\bmod 6)$ *jer 6 dijeli razliku* $38 - 14 = 24$.
b) $-25 \equiv -1 (\bmod 4)$ *jer 4 dijeli razliku* $-25 - (-1) = -24$.

Navedimo neka bitna svojstva kongruencija:

Propozicija 1 (vidi, [6, Propozicija 2.1.3.])**.**
1) *Neka su a, a', b, b' cijeli brojevi te n prirodan broj. Neka je* $a \equiv a' (\bmod n)$ *i* $b \equiv b' (\bmod n)$. *Tada vrijedi*

$$a + b \equiv a' + b' (\bmod n)$$
$$a - b \equiv a' - b' (\bmod n)$$
$$ab \equiv a'b' (\bmod n).$$

2)*Neka su a,b,c cijeli brojevi i n prirodan broj. Neka su brojevi a i n relativno prosti. Ako je*

$$ab \equiv ac (\bmod n)$$

tada vrijedi i

$$b \equiv c (\bmod n).$$

Tvrdnja 2) prethodne propozicije ne vrijedi bez uvjeta $(a, n) = 1$, pa stoga uvodimo općenitiju tvrdnju:

Propozicija 2 (vidi, [6, Propozicija 2.1.4.]). *Neka je* $ax \equiv ay (\mathrm{mod}\ n)$. *Tada vrijedi i* $x \equiv y (\mathrm{mod}\ \frac{n}{d})$, *gdje je* $d = (a, n)$.

Definicija 9. *Neka je* n *prirodan broj veći od 1. Skup* $S = \{a_1, a_2, \ldots, a_n\}$ *naziva se potpun sustav ostataka modulo* n *ako za svaki cijeli broj* b *postoji jedinstveni* a_i *iz* S, *za neki* $i \in \{1, \ldots, n\}$, *takav da vrijedi*

$$b \equiv a_i (\mathrm{mod}\ n).$$

Primjer 11. *Za* $n = 6$, *potpun sustav ostataka modulo 6 je skup* $\{0, 1, 2, 3, 4, 5\}$.

Definicija 10. *Neka je* n *prirodan broj veći od* 1. *Skup* $S = \{a_1, \ldots, a_k\}$ *naziva se reducirani sustav ostataka modulo* n *ako za svaki cijeli broj* b *koji je relativno prost s* n *postoji jedinstveni* a_i *iz skupa* S, *za neki* $i \in \{1, \ldots, n\}$, *takav da vrijedi*

$$b \equiv a_i (\mathrm{mod}\ n).$$

Primjer 12. *Za* $n = 6$, *reducirani sustav ostataka modulo* 6 *je* $\{1, 5\}$, *ali i skup* $\{-5, 5\}$. *Naime, reduciranih sustava ostataka modulo* n *ima beskonačno mnogo i svi imaju isti broj elemenata.*

Sada navedimo preciznu definiciju Eulerove funkcije.

Definicija 11. *Neka je* n *prirodan broj. Broj prirodnih brojeva u nizu* $1, 2, \ldots, n$ *koji su relativno prosti s* n *označavamo s* $\varphi(n)$, *a funkciju* $f : \mathbb{N} \to \mathbb{N}$ *zovemo Eulerova funkcija.*

Napomena 2. *Broj elemenata reduciranog skupa ostataka modulo* n *jednak je vrijednosti funkcije* $\varphi(n)$.

Sada ćemo navesti jedan koristan rezultat čiji se dokaz može vidjetu u [6].

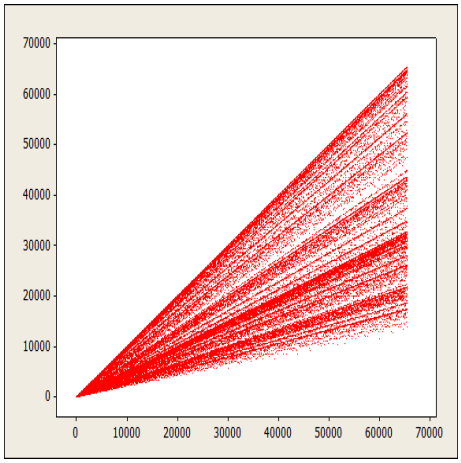
Lema 1 (vidi, [6, Lema 2.1.8.]). *Neka je* $S = \{a_1, a_2, \ldots, a_{\varphi(n)}\}$ *potpuni sustav ostataka modulo* n. *Tada je i skup* $\{b \cdot a_1, b \cdot a_2, \ldots, b \cdot a_{\varphi(n)}\}$ *potpuni sustav ostataka modulo* n, *za svaki cijeli broj* b *za koji vrijedi* $(b, n) = 1$.

Primjer 13. *Pogledajmo vrijednost funkcije* φ *za prvih nekoliko prirodnih brojeva* n.

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

Tablica 2: *Vrijednosti funkcije* $\varphi(n)$

Primjer 14. *Pogledajmo kako izgleda graf Eulerove funkcije φ:*



Slika 1: *Graf funkcije $\varphi(n)$ gdje je $n \in [1, 7000]$*

Najgornja linija na grafu predstavlja vrijednost funkcije φ u svim prostim brojevima p, a vrijednost funkcije u tim točkama iznosi $p-1$. Uočimo da funkcija φ postiže maksimalne vrijednostu upravo u prostim brojevima.

Primjer 15. *Ako je p prost broj, tada je svaki prirodan broj manji od p relativno prost sa p iz čega slijedi $\varphi(p) = p - 1$.*

Sada ćemo iskazati i dokazom potkrijepiti još općenitiji rezultat:

Teorem 6 (vidi, [2, Theorem 1, CH VI])**.** *Neka je p prost i k prirodan broj. Tada vrijedi*

$$\varphi(p^k) = p^{k-1}(p-1).$$

Dokaz.

Jedini brojevi u skupu $1, 2, \ldots, p^k$ koji nisu relativno prosti s p^k su oni koji su djeljivi s p^k. To su brojevi oblika pt, gdje je t prirodan broj takav da vrijedi $pt \leq p^k$ tj. $t \leq p^{k-1}$. dakle, broj t-ova jednak je p^{k-1}. Stoga u nizu $1, 2, \ldots, p^k$ postoji točno p^{k-1} brojeva koji nisu relativno prosti s p^k. Dakle, $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. □

Za određivanje vrijednosti Eulerove funkcije važno nam je i njeno svojstvo multiplikativnosti koje ćemo u nastavku i dokazati.

Teorem 7 (vidi, [6, Theorem 2.2.7])**.** *Eulerova funkcija je multiplikativna.*

Dokaz.

Znamo da je $\varphi(1) = 1$. Uzmimo relativno proste cijele brojeve m i n i definirajmo skupove $S_1 = \{a \in \mathbb{N} : a \leq mn, (a, mn) = 1\}, S_2 = \{a \in \mathbb{N} : a \leq m, (a, m) = 1\}$, $S_3 = \{a \in \mathbb{N} : a \leq n, (a, n) = 1\}$. Očito je $|S_1| = \varphi(mn), |S_2| = \varphi(m), |S_3| = \varphi(n)$.

Promatrajmo preslikavanje

$$i : \{0, 1, \ldots, mn-1\} \to \{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\}$$

dano s $i(t) = (t \mod m, t \mod n)$. Trebamo pokazati da je prelikavanje i bijekcija. Kako su domena i kodomena prelikavanja i jednakobrojne, dovoljno je pokazati da je i injekcija. Neka su $t_1, t_2 \in \{0, 1, \ldots, mn-1\}$ takvi da je $i(t_1) = i(t_2)$. Tada je $t_1 \equiv t_2 (\mod m)$ i $t_1 \equiv t_2 (\mod n)$ tj. $m|t_1 - t_2$ i $n|t_1 - t_2$. Kako su m i n relativno prosti, slijedi $mn|t_1 - t_2$ te (zbog $-mn + 1 \leq t_1 - t_2 \leq mn - 1$) vrijedi $t_1 = t_2$. Prema tome i je injekcija odnosno i je bijekcija.

Za $t \in \{0, 1, \ldots, mn-1\}$ neka je $i(t) = (a, b)$. Primjetimo da je $(t, mn) = 1$ ako i samo ako je $(a, m) = (b, n) = 1$. Naime, kako je $t = k_1 m + a = k_2 n + b$, za neke $k_1, k_2 \in \mathbb{Z}$ slijedi da je svaki zajednički prost djelitelj brojeva t i m (odnosno t i n) ujedno i zajednički prost djelitelj brojeva a i m (odnosno b i n).
Prema tome, restrikcija preslikavanja i na skup S_1 daje bijekciju sa skupa S_1 na skup $S_2 \times S_3$, što povlači $\varphi(mn) = \varphi(m)\varphi(n)$.

□

Direktna posljedica prethodnog teorema je sljedeći korolar.

Korolar 2 (vidi, [2, Corollary, CH VI, 1]). *Ako su $m_1, m_2, \ldots, m_k$ u parovima relativno prosti prirodni brojevi, tada vrijedi*

$$\varphi(m_1 m_2 \ldots m_k) = \varphi(m_1)\varphi(m_2) \cdots \varphi(m_k).$$

Konačno, došli smo do teorema koji nam govori kako računamo vrijednost $\varphi(n)$, za bilo koji $n \in \mathbb{N}, n > 1$:

Teorem 8 (vidi, [2, Theorem 3, CH VI]). *Neka je $n \in \mathbb{N}, n > 1$ dan faktorizacijom $n = q_1^{\alpha 1} q_2^{\alpha 2} \cdots q_k^{\alpha k}$, tada je*

$$\varphi(n) = q_1^{\alpha_1 - 1}(q_1 - 1) q_2^{\alpha_2 - 1}(q_2 - 1) \cdots q_k^{\alpha_k - 1}(q_k - 1)$$

što možemo zapisati kao

$$\varphi(n) = n\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_k}\right).$$

Dokaz ovog teorema može se pronaći u [2].

Primjer 16. *Odredimo koliko je pozitivnih cijelih brojeva manjih od 900 relativno prostih sa 900.*
Rješenje:
Imamo $\varphi(900) = \varphi(2^2 \cdot 3^2 \cdot 5^2) = 900(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 240$. *Dakle, takvih brojeva je* 240.

Primjer 17. *Odredimo koliko je brojeva u skupu* $\{1, 2, \ldots, 100\}$ *relativno prostih s* 50.
Rješenje:
Kako je $\varphi(50) = 2^{1-1}(2-1) \cdot 5^{2-1} \cdot (5-1) = 20$, *relativno prostih brojeva sa* 50 *u skupu* $\{1, 2, \ldots, 50\}$ *je* 20. *Kako vrijedi* $(a, b) = (a - b, b)$ *slijedi:*

$$\begin{aligned}(51, 50) &= (1, 50)\\ (52, 50) &= (2, 50)\\ &\vdots\\ (100, 50) &= (50, 50).\end{aligned}$$

Dakle, i u skupu $\{101, 102, \ldots, 200\}$ *postoji* $\varphi(50) = 20$ *relativno prostih brojeva sa* 50, *pa je konačan odgovor* $20 + 20 = 40$, *tj. u skupu* $\{1, 2, \ldots, 100\}$ *nalazi se* 40 *brojeva relativno prostih s* 50.

Već se iz prethodnih primjera da naslutiti da je u većini slučajeva $\varphi(n)$ paran broj. Odredimo stoga sve $n \in \mathbb{N}$ za koje je $\varphi(n)$ neparan broj. Znamo $\varphi(1) = \varphi(2)$, pa neka je $n > 2$ i $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Ako postoji neparan faktor p_i od n, tada je $p_i - 1$ paran broj pa je i $\varphi(n)$ paran. Ukoliko ne postoji neparan p_i tada je n oblika $n = 2^\alpha$ i $\alpha \geq 2$ zbog uvjeta $n > 2$ pa je $\varphi(n) = 2^{\alpha-1}$, $\alpha - 1 \geq 1$ tj. $\varphi(n)$ je paran broj. Slijedi da je vrijednost Eulerove funkcije paran broj samo za $n = 1$ ili $n = 2$.
Osim toga, može se pokazati da za bilo koji prost broj p vrijedi

$$1 + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^k) = p^k.$$

Zaista, ako je p prost broj imamo

$$\begin{aligned}\varphi(p) &= p - 1\\ \varphi(p^2) &= p(p-1) = p^2 - p\\ \varphi(p^3) &= p^2(p-1) = p^3 - p^2\\ &\vdots\\ \varphi(p^k) &= p^{k-1}(p-1) = p^k - p^{k-1}.\end{aligned}$$

Zbrojimo li sve jednadžbe, s desne strane će se pokratiti svi članovi osim p^k tj. dobivamo $1 + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^k) = p^k$.
Dakle, Eulerova funkcija ima mnoga korisna svojstva i puno toga može se vidjetu u npr. [2]. Primjerice, za svaki prirodan broj veći od 1 postoji beskonačno mnogo prirodnih brojeva m takvih da je

$$\frac{\varphi(m)}{m} = \frac{\varphi(n)}{n}.$$

To se može lagano i pokazati. Naime, kako svaki prirodan broj veći od 1 ima prost djelitelj možemo pisati $n = p^\alpha \cdot n_1$, $\alpha \in \mathbb{N}$, $(n_1, p) = 1$. Stoga slijedi,

$$\frac{\varphi(n)}{n} = \frac{p^{\alpha-1}(p-1)\varphi(n_1)}{p^\alpha n_1} = \frac{p-1}{p} \cdot \frac{\varphi(n_1)}{n_1}.$$

Analogno, zapišimo $m = p^{\beta} n_1$, $\beta \in \mathbb{N}$. Slijedi

$$\frac{\varphi(m)}{m} = \frac{p-1}{p} \cdot \frac{\varphi(n_1)}{n_1}.$$

Iz tih dviju jednakosti očito je da vrijedi $\frac{\varphi(m)}{m} = \frac{\varphi(n)}{n}$.

2.2 Eulerov teorem i primjene

Leonhard Euler 1736. godine objavio je dokaz Malog Fermatovog teorema kojeg je Fermat predstavio bez dokaza u obliku:

Teorem 9 (vidi, [6, Teorem 2.2.3]). *Neka je p prost broj i $a \in \mathbb{Z}$. Tada je*

$$a^p \equiv a (\bmod\ p).$$

Ako $p \nmid a$, onda je

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

Napomena 3. *Ako za prirodan broj n vrijedi*

$$a^{n-1} \equiv 1 (\bmod\ n),$$

za svaki a iz skupa $\{2, 3, \ldots, n+1\}$, to ne znači da je n prost broj!

Neparan složen broj n takav da za sve prirodne brojeve a koji su relativno prosti s n vrijedi $a^{n-1} \equiv 1 (\bmod\ n)$ naziva se pseudoprost broj u bazi a.
Primjerice, $3^{90} \equiv 1 (\bmod\ 91)$, ali $91 = 7 \cdot 13$ i to je složen broj. Prema tome, 91 je pseudoprost broj u bazi 3.
Složen broj n naziva se apsolutno pseudoprost ako za svaki cijeli broj a vrijedi da je $a^n - a$ djeljivo s n. Svaki apsolutno pseudoprost broj je ujedno i pseudoprost, no obrat ne vrijedi.

Složen prirodan broj n takav da za sve prirodne brojeve a koji su relativno prosti s n vrijedi $a^{n-1} \equiv 1 (\bmod\ n)$ naziva se Carmichaelov broj. Najmanji takav je 561. Svaki Carmichaelov broj je ujedno i pseuduprost, vrijedi i obrat. Detaljnije o ovim brojevima može se pronaći u [2, CH 5,7]

Nakon toga, Euler je objavio i druge verzije dokaza ovog teorema, a rezultat jednog od tih bio je i Eulerov teorem koji je nastao u pokušaju pronalska najmanje potencije za koju Mali Fermatov teorem vrijedi. Sastavni dio ovog teorema je Eulerova funkcija φ i upravo iz tog razloga nam je on u ovom radu jako zanimljiv.

Teorem 10 (Eulerov teorem, vidi [6, Teorem 2.2.2.]). *Neka je $a \in \mathbb{Z}$ i $n \in \mathbb{N}$. Ako su brojevi a i n relativno prosti, tj. $(a, n) = 1$, tada vrijedi*

$$a^{\varphi(n)} = 1(\bmod n).$$

Dokaz.

Neka je $S = \{a_1, a_2, \ldots, a_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. Prema Lemi 2 i skup $\{a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_{\varphi(n)}\}$ je reducirani sustav ostataka modulo n. Prema tome, za svaki a_i, $1 \leq i \leq \varphi(n)$ postoji jedinstveni $a_j \in S$ takav da je $a_i \equiv a \cdot a_j (\bmod n)$.
Primjenom Propozicije 1, svojstvo 1 dobivamo $a_1 \cdot a_2 \cdots a_{\varphi(n)} \equiv aa_1 \cdot aa_2 \cdots aa_{\varphi(n)} (\bmod n)$ odnosno $a_1 \cdot a_2 \cdots a_{\varphi(n)} \equiv a^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)} (\bmod n)$.
Kako je $(a_i, n) = 1$, za sve $a_i \in S$, uzastopnom primjenom Propozicije 1, svojstvo 2 dobivamo

$$a^{\varphi(n)} \equiv 1(\bmod n).$$

□

Eulerov i Mali Fermatov teorem imaju razne zanimljive primjene. Pogledajmo sada neke od njih preuzete iz kolegija *Uvod u teoriju brojeva* koji se izvodi na studijima Odjela za matematiku sveučilišta u Osijeku.

Primjer 18. *Dokažimo da su prirodni brojevi oblika $n^{24} + 17$ djeljivi s 18 za sve prirodne brojeve n za koje je (n,18)=1.*
Rješenje:
Za $(n, 18) = 1$ primjenom Eulerovog teorema dobivamo

$$n^{\varphi(18)} \equiv n^6 \equiv 1(\bmod 18),$$

pa je

$$n^{24} + 17 \equiv (n^6)^4 + 17 \equiv 1 + 17 \equiv 0(\bmod 18).$$

Time je tvrdnja dokazana.

Primjer 19. *Odredimo sve moguće ostatke pri djeljenju stote potencije cijelog broja sa 125.*
Rješenje:
Izračunajmo najprije $\varphi(125) = \varphi(5^3) = 5^2 \cdot 4 = 100$. Neka je $a \in \mathbb{Z}$. Ako vrijedi $(a, 125) = 1$, tada primjenom Eulerovog teorema slijedi

$$a^{100} \equiv 1(\bmod 125).$$

Dakle, jedan ostatak je 1. U drugom slučaju je $(a, 125) \neq 1$, a tada i $(a, 5) \neq 1$. Stoga, postoji $b \in \mathbb{Z}$ takav da $b = 5b$. Slijedi

$$a^{100} = (5b)^{100} = 5^{100} \cdot b^{100} = 5^{33} \cdot 5 \cdot b^{100}.$$

Pogledajmo taj izraz modulo 125

$$\begin{aligned} a^{100} &\equiv 125^{33} \cdot 5 \cdot b^{100} (\bmod 125) \\ &\equiv 0(\bmod 125). \end{aligned}$$

Dakle, drugi mogući ostatak je 0.

Primjer 20. *Dokažimo da je za sve prirodne brojeve m i n, $m^{61}n - mn^{61}$ djeljivo s* 2015.
Rješenje:
S obzirom da je $2015 = 5 \cdot 13 \cdot 31$, *treba pokazati da je* $m^{61}n - mn^{61}$ *djeljivo s* 5,13 *i* 31.
Dokažimo najprije da je $m^{61}n - mn^{61} = mn(m^{60} - n^{60})$ *djeljivo s* 31. *Ako je neki od brojeva m i n djeljiv s* 31 *onda smo gotovi, a ako nije, prema malom Fermatovom teoremu slijedi da je* $m^{30} \equiv 1 (\mathrm{mod}\ 31)$ *i* $n^{30} \equiv 1 (\mathrm{mod}\ 31)$, *a onda i* $m^{60} \equiv 1 (\mathrm{mod}\ 31)$ *i* $n^{60} \equiv 1 (\mathrm{mod}\ 31)$, *pa je* $m^{60} - n^{60}$ *djeljivo s* 31.
Analogno, ako je neki od brojeva m i n djeljiv s 5, *onda smo gotovi. U suprotnom, prema malom Fermatovom teoremu imamo* $m^4 \equiv 1 (\mathrm{mod}\ 5)$, $n^4 \equiv 1 (\mathrm{mod}\ 5)$, *pa onda i* $m^{60} \equiv 1 (\mathrm{mod}\ 5)$, $n^{60} \equiv 1 (\mathrm{mod}\ 5)$ *i* $m^{60} - n^{60}$ *djeljivo s* 5.
Na sličan način pokaže se da je $m^{60} - n^{60}$ *djeljivo s* 13. *Kako su* $(5, 13, 31) = 1$, *slijedi* $2015 | m^{61}n - mn^{61}$.

Primjer 21. *Primjenom Eulerovog teorem rješimo kongruenciju* $25x \equiv 53 (\mathrm{mod}\ 62)$.
Rješenje:
Izračunajmo najprije $\varphi(62) = \varphi(2 \cdot 31) = (2-1)(31-1) = 30$. *Primjenom Eulerovog teorema slijedi* $a^{30} \equiv 1 (\mathrm{mod}\ 62)$, *za svaki a za koji vrijedi* $(a, 62) = 1$. *Kako je* $(25, 62) = 1$ *možemo pisati* $25^{30} \equiv 1 (\mathrm{mod}\ 62)$. *Pomnožimo li početnu jednadžbu s* 25^{29} *dobivamo*

$$\begin{aligned} 25^{30}x &\equiv 25^{29} \cdot 53 (\mathrm{mod}\ 62) \\ x &\equiv 25^{3 \cdot 9 + 2} \cdot 53 (\mathrm{mod}\ 62). \end{aligned}$$

Kako je $25^3 \equiv 1 (\mathrm{mod}\ 62)$ *slijedi*

$$\begin{aligned} x &\equiv 25^2 \cdot 53 (\mathrm{mod}\ 62) \\ &\vdots \\ x &\equiv 17 (\mathrm{mod}\ 62). \end{aligned}$$

Primjer 22. *Odredimo zadnje dvije znamenke broja* 3^{1000}.
Rješenje:
Budući da je $\varphi(25) = 20$, *imamo* $3^{20} \equiv 1 (\mathrm{mod}\ 25)$. *A onda je i* $3^{1000} \equiv 1 (\mathrm{mod}\ 25)$. *Također,* $3^2 \equiv 1 (\mathrm{mod}\ 4)$, *pa je i* $3^{1000} \equiv 1 (\mathrm{mod}\ 4)$. *Kako je* $(4, 25) = 1$, *zaključujemo da je* $3^{1000} \equiv 1 (\mathrm{mod}\ 100)$, *pa su zadnje dvije znamenke broja* 3^{1000} *znamenke* 01.

Osim u teoriji brojeva, Eulerov i Mali Fermatov teorem imaju različite primjene i u drugim granama matematike, razne metode šifriranja i dešifriranja bazirane su na tim rezultatima. Primjerice, najpoznatiji kriptosustav s javnim ključem, RSA kriptosustav, u svom funkcioniranju koristi Eulerovu funkciju i njena svojstva (vidi [7]).
Osim toga, razni testovi za ispitivanje prostosi prirodnih brojeva zasnovani su na tvrdnji Malog Fermatovog teorema (više o tome može se vidjeti u [8]).

Literatura

[1] A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu, skripta.

[2] W. Sierpinski, *Elementary theory of numbers*, North Holland, Amsterdam, 1988.

[3] T. Nagel, *Introduction to number theory*, John Wiley and sons, New York, 1950.

[4] J. Sandor, *Geometric theorems, diophantine equations and arithemtic functions*, American research press, Rehoboth, 2002.

[5] G. E. Andrews, *Number theory*, W. B. Saunders company, Philadelphia, 1971.

[6] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište u Osijeku, Osijek, 2014.

[7] B. Ibrahimpašić, *RSA kriptosustav*, Osječki matematički list **5**(2005), 101–112.

[8] H. Riesel, *Prime numbers and computer methods for factorization*, Birkhäuser, Boston, 1985.

[9] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete mathematics*, Addison-Wesley publishing company, Boston, 1998.

[10] H. J. J. Riele, *Computation of all the amicable pairs below* 10^{10}, Math. Comput. **47**(1986), 361–368.

[11] H. J. J. Riele, W. Borho, S. Battiato, H. Hoffmann, E. J. J. Lee *Table of amicable pairs between* 10^{10} *and* 10^{52}, Centrum voor Wiskunde en Informatica, Amsterdam, 1986.

[12] L. E. Dickson, *Amicable number triples*, Amer. Math. Monthly **20**(1913), 84–91.