Eulerova funkcija

Behin, Andrea

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Andrea Behin

Eulerova funkcija

Završni rad

Osijek, 2016.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Andrea Behin

Eulerova funkcija

Završni rad

Voditelj: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2016.

Sadržaj

1. Uvod **1**

2. Eulerova funkcija **2**

2.1. Definicija i formula 2

2.2. Svojstva Eulerove funkcije 6

2.3. Neke ocjene za Eulerovu funkciju 7

3. Eulerov teorem **10**

3.1. Dokaz Eulerovog teorema 10

3.2. Primjene 10

3.2.1. Ostatci pri dijeljenju zadanim brojem 10

3.2.2. Rješavanje linearnih kongruencija 12

3.2.3. Fermatov test prostosti 12

3.2.4. Dokaz Wilsonovog teorema 12

3.2.5. RSA kriptosustav 13

4. Problemi vezani uz Eulerovu funkciju **15**

4.1. Konstrukcija pravilnog n-terokuta pomoću ravnala i šestara 15

4.2. Lehmerov problem 15

4.3. Carmichaelova slutnja 16

Literatura **17**

Sažetak: U ovom radu obradit ćemo Eulerovu funkciju i ukratko nešto reći o L. Euleru, matematičaru po kojemu je ta funkcija dobila ime. Definirat ćemo što je ta funkcija, navesti osnovna svojstva i neke ocjene te na primjerima pokazati kako se računa vrijednost te funkcije. Nadalje, navest ćemo primjene Eulerove funkcije i probleme usko vezane uz nju. Dokazat ćemo Eulerov teorem te također navesti njegove primjene.

Ključne riječi: kongruencije, reducirani sustav ostataka, Eulerova funkcija, multiplikativna funkcija, Eulerov teorem, Mali Fermatov teorem

Abstract: In this article we will cover the Euler's totient function and briefly focus on L. Euler, a mathematician after whom this function is named. We will define this function, specify the basic properties and some bounds, and give some examples that show how to calculate the value of this function. Furthermore, we will list the applications and problems closely related to. We will prove Euler's theorem and also indicate its application.

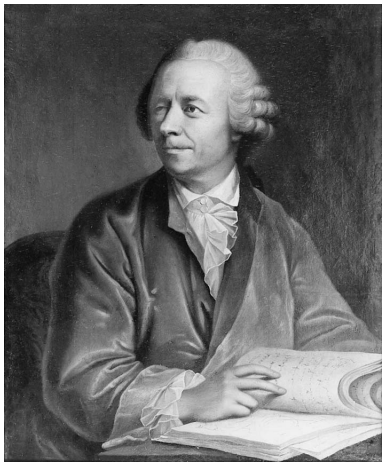
Key words: congruence, residue system, Euler's totient function or Euler's phi function, multiplicative function, Euler's theorem, Fermat's Little theorem

1. Uvod

U ovom radu bavit ćemo se Eulerovom funkcijom. Ta funkcija javnosti je predstavljena 1763. godine, međutim tada L. Euler nije odabrao simbol za njezinu oznaku. Euler je nastavio i dalje proučavati funkciju te je prvotno za njezinu oznaku odabrao grčko slovo π. Oznaka $\pi(D)$ predstavljala je "mnoštvo" brojeva manjih od broja D, a koji nemaju zajedničkih djelitelja s njim. Ta definicija Eulerove funkcije razlikuje se od "prave" jedino za $D = 1$ jer za Eulerovu funkciju koju označavamo s grčkim slovom φ vrijedi $\varphi(1) = 1$. Standardna oznaka φ za Eulerovu funkciju dolazi iz Gaussove knjige Disquisitiones Arithmeticae objavljene 1801. godine.
U ovom radu ćemo ukratko reći nešto o Leonhardu Euleru, švicarskom matematičaru, fizičaru i astronomu po kojemu je ta funkcija dobila ime. U radu ćemo definirati Eulerovu funkciju i navesti osnovna svojstva i primjere vezane uz tu funkciju te ćemo navesti neke ocjene. Dokazat ćemo Eulerov teorem, jedan od najbitnijih teorema u teoriji brojeva te navesti primjene tog teorema u RSA kriptosustavu i rješavanju linearnih kongruencija i zadataka u kojima želimo odrediti ostatak pri dijeljenju s nekim zadanim brojem. Nadalje, Wilsonov teorem ćemo dokazati koristeći Mali Fermatov teorem i ukratko ćemo opisati Fermatov test prostosti. Također ćemo opisati vezu Eulerove funkcije s konstruiranjem pravilnog n-terokuta pomoću šestara i ravnala te ukratko reći nešto o Lehmerovom problemu i Carmichaelovoj slutnji.

2. Eulerova funkcija

Prije svega, ukratko o Leonhardu Euleru, matematičaru koji je zaslužan za njezino postojanje i po kojemu je dobila ime.



Slika 1: Leonhard Euler

Leonhard Euler rođen je u Baselu 15. travnja 1707. godine. Umro je 18. rujna 1783. godine. Količina njegova znanja impresivna je kao i njegov doprinos matematici. Poznavao je više jezika i studirao je teologiju, medicinu, astronomiju i fiziku. Veliki period života posvetio je matematičkoj analizi te je 1748. godine objavio svoje najznačajnije djelo "Uvod u analizu beskonačnosti". Najpoznatiji je po svom doprinosu analizi i teoriji brojeva, posebice za korištenje beskonačnih suma i produkta, te za modernije zapise matematičkih pojmova.

2.1. Definicija i formula

U teoriji brojeva, možemo reći da Eulerova funkcija (engl. Euler's totient function) "broji" sve pozitivne cijele brojeve manje od zadanog prirodnog broja n koji su relativno prosti s n. Da bismo definirali što je to Eulerova funkcija, prije svega moramo definirati što je to reducirani sustav ostataka modulo n.

Definicija 2.1. *Reducirani sustav ostataka modulo n je skup cijelih brojeva $\{r_1, \ldots, r_m\}$ sa svojstvom da je $(r_i, n) = 1$, $\forall i = 1, \ldots, m$, $r_i \not\equiv r_j \pmod{n}$ za $i \neq j$, te da za svaki cijeli broj x takav da je $(x, n) = 1$ postoji r_i takav da je $x \equiv r_i \pmod{n}$.*

Primjer 2.1. *(a) Jedan reducirani sustav ostataka modulo n je skup svih brojeva $a \in \{1, 2, \ldots, n\}$ takvih da je $(a, n) = 1$.*

(b) Skup $S = \{1, 3, 7, 9\}$ je reducirani sustav ostataka modulo 10. Svaki element tog skupa je relativno prost s 10 i vrijedi $r_i \not\equiv r_j \pmod{m}$, $i \neq j$, za svaki r_i, $r_j \in S$.

Iz definicije je jasno da reducirani sustavi ostataka modulo n imaju isti broj elemenata.

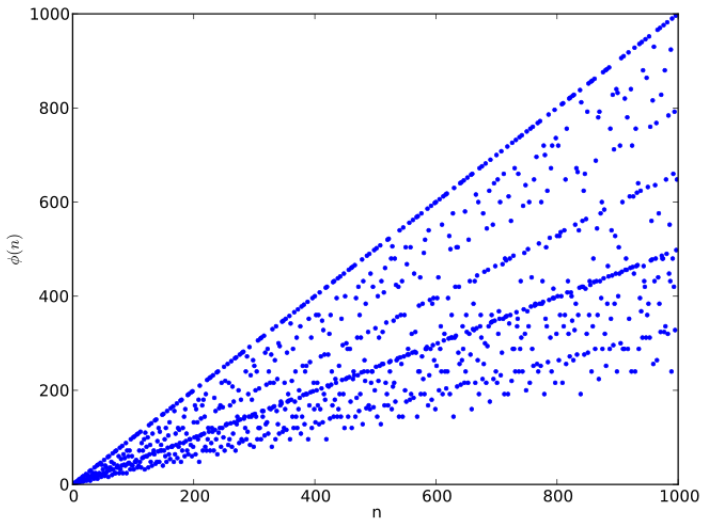
Definicija 2.2. *Funkcija $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ definirana s*

$$\varphi(n) = |\{k \in \mathbb{N} : 1 \leq k < n \ i \ (n, k) = 1\}|,$$

tj. $\varphi(n)$ = broj elemenata reduciranog sustava ostataka modulo n, naziva se Eulerova funkcija.

Primjer 2.2. *(a)* $\varphi(1) = 1$.

(b) Ako je p prost broj, tada je svaki prirodan broj j takav da je $j < p$ relativno prost s p pa vrijedi $\varphi(p) = p - 1$.



Slika 2: Graf koji prikazuje prvih 1000 vrijednosti Eulerove funkcije

Uočimo da za proste brojeve p funkcija φ postiže maksimalne vrijednosti (Slika 2).

Definicija 2.3. *Funkciju $f : \mathbb{N} \to \mathbb{C}$ za koju vrijedi*

1 $f(1) = 1$

2 $f(mn) = f(m)f(n)$ *za sve m, n takve da je $(m, n) = 1$,*

zovemo multiplikativna funkcija.

U nastavku teksta ćemo pokazati da je Eulerova funkcija multiplikativna. Najprije ćemo u jednoj lemi okarakterizirati potpuni sustav ostataka modulo n.

Definicija 2.4. *Skup $\{x_1, \ldots, x_n\}$ zove se potpuni sustav ostataka modulo n ako za svaki $y \in \mathbb{Z}$ postoji točno jedan x_j takav da je $y \equiv x_j \pmod{n}$.*

Lema 2.1. *Ako je $ax \equiv ay \pmod{n}$ i $(a, n) = 1$, onda je $x \equiv y \pmod{n}$.*

Dokaz. $ax \equiv ay \pmod{n}$ povlači da n dijeli $ax - ay$. Kako su a i n relativno prosti, n mora dijeliti $x - y$ i time je tvrdnja dokazana. □

Lema 2.2. *Ako je A potpun sustav ostataka modulo n, i m i c cijeli brojevi takvi da je $(m, n) = 1$, tada je i skup $Am + c = \{am + c : a \in A\}$ potpun sustav ostataka.*

Dokaz. Neka je $am + c \equiv a'm + c \pmod{n}$, gdje su $a, a' \in A$. Oduzimanjem broja c i dijeljenjem s m prema Lemi 2.1 slijedi da je $a \equiv a' \pmod{n}$ pa je $a = a'$. Prema tome, svih n elemenata $am + c$ nalaze se u različitim klasama ekvivalencije pa zajedno čine potpun sustav ostataka modulo n.

□

Teorem 2.1. *Eulerova funkcija je multiplikativna funkcija.*

Dokaz. Neka su m, n prirodni brojevi takvi da $(m, n) = 1$. Za $m = n = 1$ je $\varphi(1) = 1$. Ako je $m = 1$ i $n > 1$, tvrdnja vrijedi jer $\varphi(1 \cdot m) = \varphi(m) = 1 \cdot \varphi(m) = \varphi(1)\varphi(m)$. Slično se provjeri i za $n = 1$ pa još preostaje provjeriti slučaj kada je $m, n > 1$. Sada posložimo brojeve $1, 2, \ldots, mn$ u tablicu s n redova i m stupaca na sljedeći način:

$$\begin{array}{rrrcr} 1 & 2 & 3 & \ldots & m \\ m+1 & m+2 & m+3 & \ldots & 2m \\ \vdots & \vdots & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \ldots & nm \end{array}$$

Brojevi i iz tablice čine potpun sustav ostataka modulo mn pa postoji $\varphi(mn)$ brojeva koji su relativno prosti s mn, odnosno $(i, m) = (i, n) = 1$. Svi brojevi u danom stupcu su međusobno kongruentni modulo m, tj. u istom stupcu imamo brojeve koji pri dijeljenju s m daju isti ostatak, a svih m stupaca odgovara m klasa ekvivalencije modulo m. Dakle, brojevi u istom stupcu ili su svi relativno prosti s m ili nijedan nije relativno prost s m. Stoga, točno $\varphi(m)$ stupaca sastoji se od brojeva relativno prostih s m, dok ostali stupci sadrže brojeve i takve da je $(i, m) > 1$. Uzmimo sada jedan od tih $\varphi(m)$ stupaca. Neka je to k-ti stupac. Taj stupac sastavljen je od brojeva k, $m + k$, $2m + k$,..., $(n - 1)m + k$. Prema Lemi 2.2 brojevi tog stupca čine i potpun sustav ostataka modulo n, budući da svaki od tih brojeva daje različit ostatak pri dijeljenju s n i $(m, n) = 1$. Naime, kada bi dva broja $mx_1 + k$, $mx_2 + k$, $x_1, x_2 \in \{0, 1, \ldots, n - 1\}$, $(x_1 \neq x_2)$ davala isti ostatak pri dijeljenju s n, imali bismo da je

$$mx_1 + k \equiv mx_2 + k \pmod{n},$$

odnosno $mx_1 \equiv mx_2 \pmod{n}$. Kako je $(m, n) = 1$ slijedilo bi da je

$$x_1 \equiv x_2 \pmod{n}$$

što je nemoguće jer razlika dvaju različitih brojeva iz skupa $\{0, 1, \ldots, n - 1\}$ ne može biti djeljiva s n. Stoga, svaki od stupaca iz tablice sadrži $\varphi(n)$ brojeva relativno prostih s n pa tih $\varphi(m)$ stupaca daje $\varphi(m)\varphi(n)$ brojeva i relativno prostih i s m i s n. Stoga, $\varphi(mn) = \varphi(m)\varphi(n)$ i tvrdnja je dokazana. □

Primjer 2.3. *Brojevi $m = 3$ i $n = 5$ su relativno prosti i $\varphi(3) = 2$, $\varphi(5) = 4$. Znamo da je Eulerova funkcija multiplikativna pa vrijedi $\varphi(5 \cdot 3) = \varphi(5)\varphi(3) = 4 \cdot 2 = 8$.*

Propozicija 2.1. *Neka je p prost broj i $\alpha \in \mathbb{N}$. Tada vrijedi*

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

Dokaz. Neka je p prost broj i $\alpha \geq 1$. Pozitivni djelitelji broja p^α su $1, p, \ldots, p^\alpha$. Jedini brojevi i takvi da $1 \leq i \leq p^\alpha$ koji nisu relativno prosti s p^α su višekratnici broja p, a to su $1 \cdot p, 2 \cdot p, \ldots, p^{\alpha-1} \cdot p = p^\alpha$. Dakle, ima ih $p^{\alpha-1}$ pa je

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1) = p^\alpha \left(1 - \frac{1}{p}\right).$$

□

Primjer 2.4. *Odredimo koliko iznosi* $\varphi(2^{10})$.

Rješenje: Prema Propziciji 2.1 $\varphi(2^{10}) = 2^{10} - 2^9 = 2^9(2-1) = 2^9$.

Svojstvo multiplikativnosti Eulerove funkcije potrebno nam je da bismo odredili vrijednost funkcije za složene brojeve.

Propozicija 2.2. *Za* $n \in \mathbb{N}$, $n > 1$ *vrijedi*

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Dokaz. Prema Osnovnom teoremu aritmetike znamo da se svaki prirodan broj $n > 1$ može zapisati u obliku $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, gdje su $p_1 < \cdots < p_k$ prosti brojevi i svaki $\alpha_i \geq 1$. Uzastopnom primjenom svojstva multiplikativnosti funkcije φ i formule za $\varphi(p^\alpha)$ dobivamo

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) \\
&= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) \\
&= p_1^{\alpha_1} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

□

Napomena 2.1. *Prethodna formula može se zapisati i u ovim oblicima:*

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i - 1),$$

odnosno

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

U nastavku ćemo na nekoliko primjera pokazati kako računamo vrijednosti Eulerove funkcije.

Primjer 2.5. *Odredimo koliko iznosi* $\varphi(10^{10})$.

Rješenje: Budući je $10 = 2 \cdot 5$ prema Napomeni 2.1 imamo

$$\varphi(10^{10}) = \varphi((2 \cdot 5)^{10}) = \varphi(2^{10} \cdot 5^{10}) = 2^9(2-1)5^9(5-1) = 2^9 \cdot 5^9 \cdot 2^2 = 2^{11} \cdot 5^9.$$

Primjer 2.6. *Pokažimo da postoji beskonačno mnogo pozitivnih cijelih brojeva* n *takvih da je*

$$\varphi(n) = \frac{n}{3}.$$

Rješenje: Neka je $n = 2 \cdot 3^m$, gdje je m pozitivan cijeli broj. Tada zbog multiplikativnosti od φ i prema Propoziciji 2.1 imamo

$$\varphi(n) = \varphi(2 \cdot 3^m) = \varphi(2)\varphi(3^m) = 1(3^m - 3^{m-1}) = 2 \cdot 3^{m-1} = \frac{n}{3}$$

za beskonačno mnogo vrijednosti broja n.

Primjer 2.7. *Odredimo sve prirodne brojeve n za koje je $\varphi(n)$ neparan broj.*

Rješenje: Zbog svojstva multiplikativnosti Eulerove funkcije za $n = 1$ vrijedi $\varphi(1) = 1$. Za $n = 2$ vrijedi $\varphi(2) = 2 - 1 = 1$. Neka je sada $n > 2$ i $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Tada je prema Napomeni 2.1 $\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$. Imamo 2 slučaja:

- Ako postoji neparan faktor p_i od n (jedini paran prost broj je 2), onda je $p_i - 1$ paran broj te iz ovoga slijedi da je $\varphi(n)$ paran broj.
- Ako ne postoji neparan faktor p_i od n, onda je $n = 2^a$, $a \geq 2$ (zbog $n > 2$) pa je $\varphi(n) = 2^{a-1}(2 - 1) = 2^{a-1}$. Zbog $a \geq 2$ slijedi da je $a - 1 \geq 1$ pa je $\varphi(n)$ paran broj.

Dakle, $\varphi(n)$ je neparan broj samo za $n = 1$ i $n = 2$.

Primjer 2.8. *Odredimo sve prirodne brojeve n za koje vrijedi $\varphi(n) = 12$.*

Rješenje: Ako je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, onda je prema Napomeni 2.1 $\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$. Iz $(p_i - 1) \mid 12$ slijedi $p_i \in \{2, 3, 5, 7, 13\}$. Ako je $p_i = 2$, onda je $\alpha_i \leq 3$; ako je $p_i = 3$, onda je $\alpha_i \leq 2$, a ako je $p_i \neq 2, 3$, onda je $\alpha_i = 1$.
Dakle, imamo 4 mogućnosti (s k ćemo označiti broj oblika $2^\alpha 3^\beta$):

- $n = 13k$ pa je $\varphi(n) = 12\varphi(k) = 12$ odakle slijedi $\varphi(k) = 1$. Iz $\varphi(k) = 1$ slijedi $k = 1$ ili $k = 2$. Dakle, $n = 13$ ili $n = 26$;
- $n = 7k$ pa je $\varphi(n) = 6\varphi(k) = 12$ odakle slijedi $\varphi(k) = 2$. Iz $\varphi(k) = 2$ slijedi $k = 3$, $k = 4$ ili $k = 6$. Dakle, $n = 21$, $n = 28$ ili $n = 42$;
- $n = 5k$ pa je $\varphi(n) = 4\varphi(k) = 12$ odakle slijedi $\varphi(k) = 3$, što nema rješenja;
- $n = k$ pa je $\varphi(n) = 2^{\alpha-1}3^{\beta-1}2 = 12$. To vrijedi za $\alpha = 2$ i $\beta = 2$. Dakle, $n = 36$.

Dakle, za brojeve $n = 13, 21, 26, 28, 36, 42$ vrijedi $\varphi(n) = 12$.

2.2. Svojstva Eulerove funkcije

U ovom ćemo dijelu dokazati neka svojstva Eulerove funkcije.

Propozicija 2.3. *Ako $d \mid n$, onda $\varphi(d) \mid \varphi(n)$.*

Dokaz. Prema Napomeni 2.1 znamo

$$\varphi(d) = d \prod_{p \mid d} \left(1 - \frac{1}{p}\right) \quad \text{i} \quad \varphi(n) = n \prod_{q \mid n} \left(1 - \frac{1}{q}\right),$$

pa imamo

$$\frac{\varphi(n)}{\varphi(d)} = \frac{n}{d} \prod_r \left(1 - \frac{1}{r}\right),$$

gdje je r prost broj takav da $r \mid n$, ali $r \nmid d$. Stoga, $\dfrac{\varphi(n)}{\varphi(d)}$ je višekratnik od

$$\prod_r r \prod_r \left(1 - \frac{1}{r}\right) = \prod_r (r-1) \in \mathbb{Z},$$

pa je $\dfrac{\varphi(n)}{\varphi(d)}$ cijeli broj. □

Propozicija 2.4. *Za svaki prirodan broj m postoji konačno mnogo cijelih brojeva n takvih da je $\varphi(n) = m$.*

Dokaz. Ako neka potencija prostog broja p dijeli n, tj. $p^a \mid n$, prema Propoziciji 2.3 $(p-1)p^{a-1} \mid \varphi(n) = m$ i tada je $p^a \leq \dfrac{mp}{p-1} \leq 2m$. Postoji samo konačno mnogo brojeva p^a takvih da je $p^a \leq 2m$, stoga i konačno mnogo produkata takvih prostih potencija. Budući da se svaki $n > 1$ može zapisati u obliku produkta prostih potencija, slijedi tvrdnja. □

Propozicija 2.5. *Vrijedi*

$$\sum_{d \mid n} \varphi(d) = n.$$

Dokaz. Neka je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Zbog multiplikativnosti funkcije φ imamo

$$\sum_{d \mid n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{\alpha_i})). \tag{1}$$

Množenjem faktora na desnoj strani od (1) dobivamo sumu faktora oblika

$$\varphi(p_1^{\beta_1}) \cdots \varphi(p_k^{\beta_k}) = \varphi(p_1^{\beta_1} \cdots p_k^{\beta_k}),$$

gdje je $0 \leq \beta_i \leq \alpha_i$, $i = 1, \ldots, k$, a to je upravo lijeva strana od (1). Sada imamo

$$\sum_{d \mid n} \varphi(d) = \prod_{i=1}^{k} (1 + (p_i - 1) + (p_i^2 - p_i) + \cdots + (p_i^{\alpha_i} - p_i^{\alpha_i - 1})) = \prod_{i=1}^{k} p_i^{\alpha_i} = n$$

i time je tvrdnja dokazana. □

2.3. Neke ocjene za Eulerovu funkciju

Propozicija 2.6. *Ako je n složen prirodan broj, tada je*

$$\varphi(n) \leq n - \sqrt{n}.$$

Dokaz. Budući da je n složen broj, n ima prost faktor $p_j \leq \sqrt{n}$. Sada imamo

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \leq n \left(1 - \frac{1}{p_j}\right) \leq n \left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n}.$$

□

Propozicija 2.7. *Za prirodan broj n, $n \neq 2, 6$, vrijedi*

$$\varphi(n) \geq \sqrt{n}.$$

Dokaz. Ako je $n = 2^m$, gdje je $m \geq 2$, prema Propoziciji 2.1 imamo

$$\varphi(n) = 2^m - 2^{m-1} = 2^{m-1} \geq \sqrt{2^m} = \sqrt{n}.$$

Ako je $n = p^m$, gdje je p neparan prost broj i $m \geq 2$, imamo

$$\varphi(n) = p^m - p^{m-1} = p^{m-1}(p-1) \geq \sqrt{2p^m} = \sqrt{2n}.$$

Ako je $n = p^m$, gdje je p prost broj takav da je $p \geq 5$, tada je $\varphi(n) \geq \sqrt{2n}$. Ako je n neparan ili $4 \mid n$, imamo

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) \geq \sqrt{p_1^{\alpha_1}} \cdots \sqrt{p_k^{\alpha_k}} = \sqrt{n}.$$

Ako je $n = 2t$, gdje je t neparan, tada za $n \neq 6$ vidimo da t ima barem jedan prost faktor veći ili jednak 5. Stoga, $\varphi(n) = \varphi(t) \geq \sqrt{2t}$. □

Lema 2.3. *Neka je n prirodan broj, $n \geq 2$, i $\sigma(n)$ suma svih pozitivnih djelitelja broja n. Tada vrijedi*

$$\sigma(n) < n(1 + \ln n).$$

Dokaz. Imamo

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} \leq n \sum_{d \leq n} \frac{1}{d} < n \left(1 + \int_1^n \frac{1}{x} dx\right) = n(1 + \ln n).$$

□

Propozicija 2.8. *Za prirodan broj n, $n \geq 2$, vrijedi*

$$\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}.$$

Dokaz. Funkcija $f(n) = \dfrac{\sigma(n)\varphi(n)}{n^2}$ je multiplikativna i vrijedi

$$f(p^j) = \frac{(p^{j+1} - 1)p^{j-1}(p-1)}{(p-1)p^{2j}} = 1 - \frac{1}{p^{j+1}} \geq 1 - \frac{1}{p^2},$$

pa je

$$f(n) \geq \prod_{p|n} \left(1 - \frac{1}{p^2}\right) \geq \prod_{m=2}^{\infty} \left(1 - \frac{1}{m^2}\right) = \frac{1 \cdot 3}{2 \cdot 2} \cdot \frac{2 \cdot 4}{3 \cdot 3} \cdot \frac{3 \cdot 5}{4 \cdot 4} \cdots = \frac{1}{2}.$$

Prema tome, $\sigma(n)\varphi(n) \geq \frac{1}{2}n^2$. Prema Propoziciji 2.3 slijedi $\sigma(n) < 2n \ln n$ za $n \geq 2$, odakle slijedi

$$\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}.$$

□

U nastavku navodimo bez dokaza još neke ocjene Eulerove funkcije.

Propozicija 2.9. *Za svaki $\varepsilon > 0$ postoji prirodan broj n takav da vrijedi*

$$\frac{\varphi(n)}{n} \leq \varepsilon.$$

Dokaz. Vidi [4]. □

Teorem 2.2. *1. Za bilo koji $\varepsilon > 0$ i proizvoljno veliki prirodan broj n vrijedi*

$$\frac{\varphi(n)\ln(\ln n)}{n} \geq e^{-\gamma} - \varepsilon.$$

2. Postoji niz različitih prirodnih brojeva n_k takvih da vrijedi

$$\lim_{k\to\infty} \frac{\varphi(n_k)\ln(\ln n_k)}{n_j} = e^{-\gamma}.$$

Dokaz. Vidi [4]. □

Napomena 2.2. *Broj γ predstavlja Euler-Mascheroni konstantu za koju vrijedi*

$$\gamma = \lim_{n\to\infty} \left(-\ln n + \sum_{k=1}^{n} \frac{1}{k} \right) \approx 0.5772.$$

Teorem 2.2 govori nam da $\dfrac{n}{\varphi(n)}$ može imati vrijednost jednaku, za proizvoljno velike n, kao umnožak konstante i $\ln(\ln n)$, ali ne veću od toga.

Teorem 2.3. *Vrijedi*

$$\sum_{x\leq n} \varphi(x) = \frac{3}{\pi^2} n^2 + O(n \ln n).$$

Dokaz. Vidi [6]. □

3. Eulerov teorem

Eulerova funkcija sastavni je dio Eulerovog teorema, jednog od najvažnijih teorema u teoriji brojeva.

3.1. Dokaz Eulerovog teorema

Lema 3.1. *Neka je* $\{r_1, \ldots, r_{\varphi(n)}\}$ *reducirani sustav ostataka modulo* n *i neka je* $(a, n) = 1$. *Tada je* $\{ar_1, \ldots, ar_{\varphi(n)}\}$ *također reducirani sustav ostataka modulo* n.

Dokaz. Kako dani skupovi imaju jednak broj elemenata, dovoljno je provjeriti da među elementima skupa $\{ar_1, \ldots, ar_{\varphi(n)}\}$ nema međusobno kongruentnih elemenata. Ali, ako bi postojali i, j takvi da je $ar_i \equiv ar_j \pmod{n}$, onda prema Lemi 2.1 slijedi $r_i \equiv r_j \pmod{n}$ pa je $i = j$. Time je tvrdnja dokazana. □

Teorem 3.1. *(Eulerov teorem) Ako su* $n \in \mathbb{N}$ *i* $a \in \mathbb{Z}$ *takvi da* $(a, n) = 1$, *onda je*

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

Dokaz. Prema Lemi 3.1 znamo da ako je $S = \{r_1, \ldots, r_{\varphi(n)}\}$ reducirani sustav ostataka modulo n i vrijedi $(a, n) = 1$, tada je i $R = \{ar_1, \ldots, ar_{\varphi(n)}\}$ također reducirani sustav ostataka modulo n pa zaključujemo

$$\prod_{j=1}^{\varphi(n)} (ar_j) \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n},$$

odnosno

$$a^{\varphi(n)} \prod_{j=1}^{\varphi(n)} r_j \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n}.$$

Kako je $(r_i, n) = 1$, prema Lemi 2.1 slijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Sljedeća tvrdnja specijalan je slučaj Eulerovog teorema kada je n prost broj.

Korolar 3.1. *(Mali Fermatov teorem) Neka je* p *prost broj. Ako* $p \nmid a$, *onda je*

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

Za svaki cijeli broj a *vrijedi* $a^p \equiv a \pmod{p}$.

Dokaz. Očito je $\varphi(p) = p - 1$ pa tvrdnja slijedi iz Eulerovog teorema. □

3.2. Primjene

3.2.1. Ostatci pri dijeljenju zadanim brojem

Eulerov teorem i Mali Fermatov teorem vrlo su korisni u teoriji brojeva, posebice za proučavanje vrlo velikih brojeva zapisanih u obliku potencije.

Primjer 3.1. *Odredimo zadnje dvije znamenke u decimalnom zapisu broja* 3^{400}.

Rješenje: Budući da je $\varphi(25) = \varphi(5^2) = 5(5-1) = 20$, primjenom Eulerovog teorema imamo $3^{20} \equiv 1 \pmod{25}$, odakle slijedi $3^{400} \equiv 1 \pmod{25}$. Vrijedi i $3^2 \equiv 1 \pmod{4}$ pa je i $3^{400} \equiv 1 \pmod{4}$. Dakle, $3^{400} \equiv 1 \pmod{100}$ pa su zadnje dvije znamenke broja 3^{400} 01.

Primjer 3.2. *Odredite ostatak pri dijeljenju broja* 2016^{10^6} *sa 55.*

Rješenje: Kako je $\varphi(55) = \varphi(5 \cdot 11) = 4 \cdot 10 = 40$ i $(2016, 55) = 1$ iz Eulerovog teorema slijedi

$$2016^{40} \equiv 1 \pmod{55}.$$

No, onda je

$$2016^{10^6} \equiv 2016^{40 \cdot 25000} \equiv 1 \pmod{55}.$$

Stoga je traženi ostatak 1.

Primjer 3.3. *Dokažite da za svaki prirodan broj* n *brojevi oblika* n^{4k+1} $(k \in \mathbb{N})$ *i* n *imaju istu zadnju znamenku.*

Rješenje: Trebamo pokazati da je

$$n^{4k+1} \equiv n \pmod{10}, \quad \forall n \in \mathbb{N}.$$

Ako je $(n, 10) = 1$, onda tvrdnja slijedi iz Eulerovog teorema budući je

$$n^{\varphi(10)} = n^4 \equiv 1 \pmod{10},$$

pa vrijedi i

$$n^{4k+1} \equiv n \pmod{10}.$$

U slučaju kada je $(n, 10) \neq 1$ imamo sljedeće mogućnosti:

- $(n, 10) = 2$; tada je $n \equiv 0 \pmod{2}$ pa je i

  $$n^{4k+1} \equiv 0 \equiv n \pmod{2}. \tag{2}$$

  Kako je $(n, 5) = 1$, iz Malog Fermatovog teorema slijedi $n^4 \equiv 1 \pmod{5}$, odnosno

  $$n^{4k+1} \equiv n \pmod{5}. \tag{3}$$

  Iz (2) i (3) slijedi tvrdnja.

- $(n, 10) = 5$; tada je $n \equiv 1 \pmod{2}$ pa je i

  $$n^{4k+1} \equiv 1 \equiv n \pmod{2}, \tag{4}$$

  a $n \equiv 0 \pmod{5}$ povlači da je

  $$n^{4k+1} \equiv 0 \equiv n \pmod{5}. \tag{5}$$

  Iz (4) i (5) slijedi tvrdnja.

- $(n, 10) = 10$; tada je $n \equiv 0 \pmod{10}$ pa je i

  $$n^{4k+1} \equiv 0 \equiv n \pmod{10}.$$

3.2.2. Rješavanje linearnih kongruencija

U nastavku ćemo na primjeru pokazati primjenu Eulerovog teorema na rješavanje linearnih kongruencija, odnosno kongruencija oblika $ax \equiv b \pmod{n}$.

Teorem 3.2. *Neka su a i m prirodni, te b cijeli broj. Kongruencija $ax \equiv b \pmod{n}$ ima rješenja ako i samo ako $d = (a, n)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo n.*

Dokaz. Vidi [6]. □

Primjer 3.4. *Koristeći Eulerov teorem riješite kongruenciju*

$$25x \equiv 53 \pmod{62}.$$

Rješenje: Budući je $(25, 62) = 1$, prema Teoremu 3.2 znamo da ova kongruencija ima jedinstveno rješenje. Kako je $\varphi(62) = \varphi(31 \cdot 2) = 30 \cdot 1 = 30$ i $(25, 62) = 1$, prema Eulerovom teoremu slijedi

$$25^{30} \equiv 1 \pmod{62}. \tag{6}$$

Sada $25x \equiv 53 \pmod{62}$ pomnožimo s 25^{29} i dobijemo

$$25^{30}x \equiv 25^{29} \cdot 53 \pmod{62},$$

odakle zbog (6) slijedi

$$x \equiv 25^{29} \cdot 53 \pmod{62} \equiv 17 \pmod{62}.$$

3.2.3. Frematov test prostosti

Postoje važna svojstva prostih brojeva koja su vrlo jednostavna za provjeru, ali ih posjeduju i neki složeni brojevi. Tipičan primjer takvog svojstva dan je u Malom Fermatovu teoremu. 1640. godine Fermat je otkrio ono što su Kinezi znali oko 2000 godina prije njega. Takozvana Kineska slutnja glasi:

Prirodan broj p je prost ako i samo ako vrijedi $2^p \equiv 2 \pmod{p}$.

U Malom Fermatovom teoremu, zamijenimo li a s 2, i onda obje strane pomnožimo s 2, dobivamo upravo $2^p \equiv 2 \pmod{p}$. Mali Fermatov teorem je zbog jednostavnosti i brzine provjere odlična baza za puno testova prostosti, a kada bi vrijedio i obrat, imali bismo vrlo jednostavan test prostosti. Međutim, p može biti i složen broj, a da za neki ili čak i za svaki a vrijedi $a^{p-1} \equiv 1 \pmod{p}$. Sarrus je 1819. godine pronašao kontraprimjer: $2^{341} \equiv 2 \pmod{341}$, ali $341 = 11 \cdot 31$. Neparne složene brojeve za koje vrijedi kongruencija $a^{p-1} \equiv 1 \pmod{p}$ nazivamo pseudoprosti brojevi. Više o ovome može se naći u [9].

3.2.4. Dokaz Wilsonovog teorema

Sljedeći teorem potreban nam je da bismo dokazali Wilsonov teorem koristeći Mali Fermatov teorem.

Teorem 3.3. *(Lagrangeov teorem) Ako je $f(x)$ polinom stupnja d modulo p, tada polinom $f(x)$ ima najviše p međusobno različitih nultočaka modulo p.*

Dokaz. Vidi [6]. □

Teorem 3.4. *(Wilsonov teorem) Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod{p}$.*

Dokaz. Tvrdnja trivijalno vrijedi za $p = 2$, stoga možemo pretpostaviti da je p neparan prost broj. Prema Malom Fermatovom teoremu polinom $x^{p-1} - 1$ ima $p - 1$ različitih nultočaka modulo p, odnosno nultočke $1, 2, \ldots, p-1$. Sada prema Lagrangeovom teoremu imamo

$$(x-1)(x-2)\cdots(x-p+1) \equiv x^{p-1} - 1 \pmod{p}. \tag{7}$$

Sada u (7) uvrstimo $x = 0$ i dobivamo

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

Budući da je $p - 1$ paran broj, slijedi tvrdnja. □

3.2.5. RSA kriptosustav

Najpoznatiji kriptosustav s javnim ključem je RSA kriptosustav iz 1977. godine, nazvan po svojim tvorcima Rivestu, Shamiru i Adlemanu. Njegova sigurnost zasnovana je upravo na teškoći faktorizacije velikih prirodnih brojeva. Slijedi precizna definicija RSA kriptosustava.

Definicija 3.1. *Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, te*

$$\mathcal{K} = \{(n, p, q, d, e) : n = pq, de \equiv 1 \pmod{\varphi(n)}\}.$$

Za $K \in \mathcal{K}$ definiramo

$$e_K(x) = x^e \pmod{n},\ d_K(y) = y^d \pmod{n}.$$

Brojevi n i e (enkripcijski eksponent) su javni, odnosno poznati, dok je d (dekripcijski eksponent) tajan. Poruka, koju predstavlja cijeli broj m, gdje je $0 < m < n$, šifrirana je izrazom $S = m^e \pmod{n}$. Ta poruka dešifrira se računajući $t = S^d \pmod{n}$. Eulerov teorem govori nam da ako je $0 < t < n$ vrijedi $t = m$.

Teorem 3.5. *Za $1 \leq x < n$ vrijedi $d_K(e_K(x)) = x$, tj. e_K i d_K su jedna drugoj inverzne funkcije.*

Dokaz. Da bismo pokazali da to uistinu vrijedi, moramo pokazati da je $d_K(e_K(x)) = x$. Znamo

$$d_K(e_K(x)) \equiv x^{de} \pmod{n}.$$

Budući je $de \equiv 1 \pmod{\varphi(n)}$, postoji $t \in \mathbb{N}$ takav da je $de = t\varphi(n) + 1$ pa sada imamo

$$x^{de} = x^{t\varphi(n)+1} = [x^{\varphi(n)}]^t x. \tag{8}$$

Ako je $(n, x) = 1$, prema Eulerovom teoremu vrijedi $x^{\varphi(n)} \equiv 1 \pmod{n}$ te iz toga i (8) slijedi $x^{de} \equiv x \pmod{n}$. Ako je $(n, x) = n$, onda je $x^{\varphi(n)} \equiv 0 \pmod{n}$. Ako je $(n, x) = p$, onda je $x^{\varphi(n)} \equiv 0 \pmod{n}$, a budući da je $(n, x) = (pq, x) = p$ slijedi $(q, x) = 1$. Sada prema Eulerovom teoremu imamo

$$x^{\varphi(q)} = x^{q-1} \equiv 1 \pmod{q}.$$

Iz toga slijedi

$$x^{de} = [x^{q-1}]^{(p-1)t} x \equiv x \pmod{q}$$

pa je $x^{de} \equiv x \pmod{n}$. Analogno rješavamo slučaj kada je $(n, x) = q$. Sada vidimo da zaista $x^{de} \equiv x \pmod{n}$, što znači da je $d_K(e_K(x)) = x$. □

Sigurnost RSA kriptosustava leži u pretpostavci da je funkcija $e_K(x) = x^e \pmod{n}$ funkcija kod koje je relativno lako odrediti $y = e_K(x)$, ali je vrlo teško odrediti $x = e_K^{-1}(y)$. Dodatni podatak koji omogućava dešifriranje je poznavanje faktorizacije prirodnog broja n jer je u tom slučaju lako odrediti $\varphi(n)$ (za $n = pq$, gdje su p i q prosti, $\varphi(n) = \varphi(pq) = (p-1)(q-1)$) i dobiti eksponent d rješavajući linearnu kongruenciju $de \equiv 1 \pmod{\varphi(n)}$ pomoću Euklidovog algoritma.

Primjer 3.5. *Uzmimo $p = 3$ i $q = 11$. Tada je*

$$n = 3 \cdot 11 = 33 \quad i \quad \varphi(33) = (3-1)(11-1) = 20.$$

Za enkripcijski eksponent e mora vrijediti $(e, \varphi(33)) = (e, 20) = 1$ pa uzmemo $e = 7$. Budući da vrijedi $de \equiv 1 \pmod{\varphi(n)}$, odnosno $7d \equiv 1 \pmod{20}$, znamo da je $7d - 1 = 20l$, $l \in \mathbb{Z}$, te slijedi $d = 3$. Sada je $(n, e) = (33, 7)$ naš javni ključ. Pretpostavimo da nam netko želi poslati poruku $x = 17$. To znači da trebamo izračunati $e_K(x) = 17^7 \pmod{33}$. Kako je $17^7 \equiv 8 \pmod{33}$, šifrat je $y = e_K(x) = 8$. Kada primimo ovaj šifrat, dešifriramo ga pomoću dekripcijskog ključa d:

$$x = d_K(y) = 8^3 = 8 \cdot 8^2 \equiv 8 \cdot 31 \pmod{33} \equiv 17 \pmod{33}.$$

Dakle, $x = 17$.

4. Problemi vezani uz Eulerovu funkciju

U ovom dijelu opisat ćemo neke od poznatih problema usko vezanih uz Eulerovu funkciju.

4.1. Konstrukcija pravilnog n-terokuta pomoću ravnala i šestara

Konstruiranje pravilnog n-terokuta pomoću ravnala i šestara je moguće ako se duljina stranice tog n-terokuta može zapisati koristeći četiri osnovne aritmetičke operacije i korjenovanje. Gauss je 1736. godine primjetio kako brojevi $3, 9, \ldots, 3^{16}$ (potencije broja 3) pri dijeljenju sa 17 daju za ostatke sve brojeve $1, \ldots, 16$. To je dovelo do njegovog velikog otkrića - konstrukcije pravilnog 17-terokuta. Gauss je u Disquisitiones Arithmeticae objavljenoj 1801. godine dokazao uvjet dovoljnosti iz sljedećeg teorema, dok je nužnost dokazao Wantzel ([13]) 1837. godine.

Teorem 4.1. *(Gauss-Wantzel) Pravilan n-terokut, za $n > 2$, može se konstruirati sa šestarom i ravnalom ako i samo ako vrijedi:*

1. *n je Fermatov prost broj*
2. *n se može prikazati kao potencija broja 2*
3. *n je produkt potencije broja 2 i različitih Fermatovih prostih brojeva, tj. $n = 2^i F_{n_1} \cdots F_{n_j}$, gdje su $n \geq 3$, $i \geq 0$, $j \geq 0$ i $F_{n_1}, \ldots, F_{n_j}$ različiti Fermatovi prosti brojevi.*

Prosti brojevi oblika $F_n = 2^{2^n} + 1$ nazivaju se Fermatovi prosti brojevi i poznato ih je samo 5, a to su $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ i $F_4 = 65537$.
Teorem 4.1 može se izreći i na sljedeći način:

> *Pravilan n-terokut može se konstruirati sa šestarom i ravnalom ako i samo ako je n prirodan broj veći od 2 takav da je $\varphi(n)$ potencija broja 2.*

Dakle, pravilan n-terokut može se konstruirati za $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \ldots$.

4.2. Lehmerov problem

Prema Primjeru 2.2 znamo da ako je p prost broj, onda je $\varphi(p) = p - 1$. 1932. godine Lehmer je postavio pitanje postoje li složeni brojevi n takvi da $\varphi(n) \mid n - 1$. Pretpostavlja se da takvi brojevi ne postoje i danas je ta pretpostavka poznata kao *Lehmerov problem o Eulerovoj funkciji*:

> *Ne postoji složen prirodan broj n sa svojstvom da $\varphi(n) \mid n - 1$.*

1933. godine Lehmer je dokazao da ako takav n postoji, mora biti neparan, kvadratno slobodan i djeljiv s barem 7 prostih brojeva, odnosno $\omega(n) \geq 7$ (ω je funkcija koja "broji" sve proste djelitelje zadanog broja n). Cohen i Hagis dokazali su 1980. godine da je $n > 10^{20}$ i $\omega(n) \geq 14$. Nadalje, Hagis je pokazao da ako $3 \mid n$, tada je $n > 10^{1937042}$ i $\omega(n) \geq 298848$ (više o ovome može se pronaći u [5]). U sljedećem teoremu pokazat ćemo da tvrdnja vrijedi za sve n-ove takve da je $\omega(n) \leq 3$.

Teorem 4.2. *Ako za prirodan broj n vrijedi $\varphi(n) \mid (n-1)$ i $\omega(n) \leq 3$, onda je n prost broj.*

Dokaz. Neka je n prirodan broj takav da $\varphi(n) \mid (n-1)$ i $\omega(n) \leq 3$. Primjetimo da za prost broj p takav da $p^2 \mid n$ postoji cijeli broj a takav da je $n = p^2a$ i $\varphi(n) = \varphi(p^2a)$. Tada $p \mid \varphi(n)$, ali $p \nmid n-1$ što je kontradikcija. Stoga trebamo pokazati da je $n \neq pq$ i $n \neq pqr$, za proste brojeve $p < q < r$. Neka je $n = pq$. Prema pretpostavci slijedi $(p-1)(q-1) \mid pq-1$. Ako je $q \geq 3$, tada je $(p-1)(q-1)$ paran broj pa je i $(pq-1)$ paran broj i p i q su neparni prosti brojevi. Ali, za $p = 3$ i $q = 5$ imamo

$$\frac{pq-1}{(p-1)(q-1)} < 2.$$

Izraz na lijevoj strani ove nejednakosti je padajuća funkcija i uvijek je veći od 1 pa $\dfrac{pq-1}{(p-1)(q-1)}$ ne može biti neki pozitivan cijeli broj, a to je kontradikcija s $(p-1)(q-1) \mid pq-1$.
Neka je sada $n = pqr$. Analogno kao u prethodnom slučaju, p, q i r su neparni prosti brojevi. Ako je $p = 3$, $q = 7$ i $r = 11$ imamo

$$\frac{pqr-1}{(p-1)(q-1)(r-1)} < 2.$$

Budući da je lijeva strana uvijek veća od 1 i funkcija je padajuća, to je kontradikcija i isključuje sve mogućnosti osim za $p = 3$ i $q = 5$. Tada za $r = 7$

$$\frac{pqr-1}{(p-1)(q-1)(r-1)} < 3,$$

odakle slijedi $\dfrac{pqr-1}{(p-1)(q-1)(r-1)} = 2$. Međutim, iz $\dfrac{(15r-1)}{8(r-1)} = 2$ slijedi $r = 15$, a 15 nije prost broj i time smo eliminirali sve mogućnosti. Dakle, $n \neq pq$ i $n \neq pqr$, za sve proste brojeve $p < q < r$. □

4.3. Carmichaelova slutnja

1907. godine Robert Carmichael objavio je teorem u kojem tvrdi da ne postoji broj n takav da za sve druge brojeve m, $m \neq n$, je $\varphi(n) \neq \varphi(m)$. Međutim, već 1922. godine ustanovilo se da dokaz nije ispravan te se od tada pokušava razriješiti taj problem. Pretpostavlja se da takvi brojevi zaista ne postoje i danas je ta pretpostavka poznata kao *Carmichaelova slutnja:*

> *Ne postoji broj n sa svojstvom da za sve druge brojeve m, $m \neq n$, je $\varphi(n) \neq \varphi(m)$.*

Carmichaelova slutnja može se izreći i na sljedeći način:

> *Ako je $A(f)$ broj pozitivnih cijelih brojeva n takvih da je $\varphi(n) = f$, tada mora vrijediti $A(f) \neq 1$.*

Carmichael je dokazao da kontraprimjer njegovoj pretpostavci mora biti broj veći ili jednak 10^{37} ([3]) , a Victor Klee pokazao je da mora biti veći ili jednak 10^{400} ([10]). Kevin Ford je 1998. godine pokazao da slutnja vrijedi za sve brojeve manje od $10^{10^{10}}$ ([7]). Carl Pomerance pokazao je da je prirodan broj n kontraprimjer ovoj pretpostavci ako za svaki prost broj p takav da $p-1 \mid \varphi(n)$ vrijedi $p^2 \mid n$ ([12]).

Literatura

[1] T. Andreescu, D. Andrica, *Number theory*, Birkhäuser, Basel, 2009.

[2] R. D. Carmichael, *On Eulers φ-function*, The Bulletin of the American Mathematical Society **13** (1907), 241–243.

[3] R. D. Carmichael, *Note on Eulers φ-function*, The Bulletin of the American Mathematical Society **28** (1922), 109–110.

[4] P. L. Clark, *Number Theory: A Contemporary Introduction*, http://math.uga.edu/~pete/4400FULL.pdf

[5] Cohen, Graeme L, Hagis, *On the Number of Prime Factors of n if $\varphi(n) \mid (n-1)$*, Nieuw Arch. Wiskd. **28** (1980), 177–185.

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

[7] K. Ford, *The number of solutions of $\varphi(x) = m$*, Annals of Mathematics **150** (1999), 283–311.

[8] G.A. Jones, J.M. Jones, *Elementary Number Theory*, Springer, 2003.

[9] A. Jurasić, M. Rukavina, *Pseudoprosti brojevi*, (http://www.math.uniri.hr/∼ ajurasic/Pseudoprosti20%brojevi-clanak.pdf)

[10] V. L. Klee, *On a conjecture of Carmichael*, The Bulletin of the American Mathematical Society **53** (1947), 1183–1186. (http://www.ams.org/journals/bull/1947-53-12/S0002-9904-1947-08940-0 /S0002-9904-1947-08940-0.pdf)

[11] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, New York, 2008.

[12] C. Pomerance, *On Carmichael's conjecture*, Proceedings of the American Mathematical Society **43** (1974), 297–298. (https://math.dartmouth.edu/ carlp/PDF/carmichaelconjecture.pdf)

[13] P. Wantzel *Recherches sur les moyens de reconnaître si un problème de Géométrie peut se résoudre avec la règle et le compas*, Journal de Mathématiques Pures et Appliquées **1** (1837), 366–372. (http://sites.mathdoc.fr/JMPA/PDF/JMPA_1837_1_2_A31_0.pdf)