math.e

Hrvatski matematički elektronički časopis

Eulerova funkcija

Eulerov teorem **Eulerova funkcija** **kongruencije** **Mali Fermatov teorem**

Sažetak

Eulerova funkcija je jedna od najvažnijih funkcija u teoriji brojeva. U članku ćemo izvesti formulu za određivanje vrijednosti ove funkcije te ćemo dokazati neka od njezinih svojstava. Na primjerima ćemo pokazati neke od primjena dobivenih rezultata, a na kraju ćemo opisati nekoliko problema koji su usko vezani uz Eulerovu funkciju.

1 Uvod

Leonhard Euler izložio je na skupovima iz 1758. i 1759., a u članku [8] iz 1763. godine i objavio svoje rezultate vezane uz funkciju koja "broji broj prirodnih brojeva manjih od prirodnog broja n koji nemaju zajedničkih djelitelja s n". Kao što ćemo vidjeti, ova definicija razlikuje se od današnje samo utoliko što se umjesto izraza "manjih" koristi izraz "manjih ili jednakih". Godine 1784. Euler je za ovako definiranu funkciju koristio oznaku π, a danas se koristi oznaka φ koju je uveo Gauss u *Disquisitiones Arithmeticae* [11] objavljenim 1801. godine. U teoriji brojeva standardno se koristi termin Eulerova funkcija (ili Eulerova φ funkcija), dok se u engleskoj literaturi najčešće koristi termin Euler's totient function koji je 1879. godine uveo Sylvester [17].

U članku ćemo dokazati neka svojstva Eulerove funkcije i Eulerov teorem, jedan od najvažnijih teorema u kojemu se javlja Eulerova funkcija. Dokazane tvrdnje ćemo primijeniti na primjerima, a na kraju ćemo opisati neke od poznatih problema u kojima se pojavljuje Eulerova funkcija.

2 Eksplicitna formula

Ukoliko sa U_n označimo skup svih prirodnih brojeva koji nisu veći od n i relativno su prosti s n, tj.

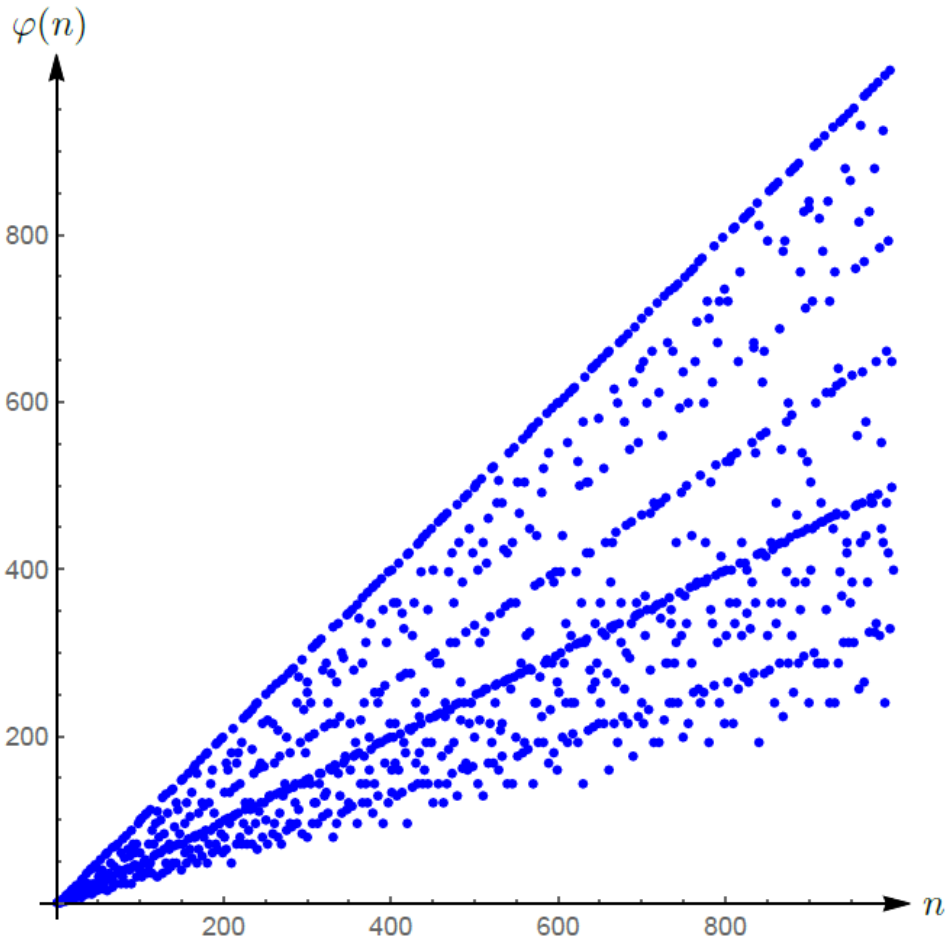
$$U_n = \{k \in \mathbb{N} : 1 \leq k \leq n \text{ i } (n,k) = 1\},$$

tada Eulerovu funkciju možemo definirati kao funkciju $\varphi : \mathbb{N} \to \mathbb{N}$ zadanu s $\varphi(n) = \#U_n$.

Uočimo da se vrijednosti ovako definirane funkcije razlikuju u odnosu na spomenutu Eulerovu definiciju samo za broj 1 - ovdje je $\varphi(1) = 1$, dok bi primjenom Eulerove definicije dobili vrijednost 0 u broju 1.

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

Grafički prikaz Eulerove funkcije dan je na Slici 1.



Slika 1: Graf Eulerove funkcije

Vrijednosti Eulerove funkcije usko su vezane uz broj elemenata u tzv. reduciranom sustavu ostataka modulo n.

Reducirani sustav ostataka modulo n je skup $R \subseteq \mathbb{Z}$ koji sadrži po točno jedan element iz svake od $\varphi(n)$ klasa ekvivalencije od U_n.

U nastavku ćemo dokazati jedno važno svojstvo Eulerove funkcije, a to je tzv. svojstvo multiplikativnosti. Multiplikativne funkcije su funkcije $f : \mathbb{N} \to \mathbb{C}$ za koje vrijedi:

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

Teorem 2. *Eulerova funkcija je multiplikativna funkcija.*

Proof. Iz definicije je jasno da je $\varphi(1) = 1$. Neka su m, n prirodni brojevi sa svojstvom da je $(m, n) = 1$. Posložimo brojeve $1, 2, \ldots, mn$ u tablicu s n redova i m stupaca na sljedeći način:

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

U ovom nizu brojeva postoji, prema definiciji, $\varphi(mn)$ brojeva koji su relativno prosti s mn. Uočimo da su svi brojevi u pojedinom stupcu međusobno kongruentni modulo m, a svih m stupaca odgovaraju m klasa ekvivalencije modulo m. Stoga su brojevi u istom stupcu ili svi relativno prosti s m ili nijedan nije relativno prost s m. Zaključujemo da se točno $\varphi(m)$ stupaca sastoji od brojeva relativno prostih s m, dok ostali stupci sadrže brojeve koji nisu relativno prosti s m.

Promotrimo jedan od tih $\varphi(m)$ stupaca. Neka je to k-ti stupac. Označimo sa S_k skup koji sadrži sve elemente toga stupca, tj. $S_k = \{k, m+k, 2m+k, \ldots, (n-1)m+k\}$ Dokažimo da su u skupu S_k svi elementi međusobno nekongruentni. Ako bi postojali $i, j \in \{0, 1, \ldots, n-1\}$takvi da vrijedi

$$im + k \equiv jm + k \pmod{n},$$

onda oduzimanjem broja k i korištenjem činjenice da je $(m, n) = 1$ dobivamo da je $i \equiv j \pmod{n}$ pa je $i = j$.

Kako S_k ima n međusobno nekongruentnih elemenata modulo n zaključujemo da u S_k imamo predstavnike svih mogućih klasa modulo n (tj. S_k je potpun sustav ostataka modulo n). Neka je R_k skup koji sadrži

elemente skupa S_k koji su relativno prosti s n. Tada je R_k reducirani sustav ostataka modulo n i ima $\varphi(n)$ elemenata.

Zaključujemo da svaki od $\varphi(m)$ stupaca iz gornje tablice sadrži $\varphi(n)$ brojeva relativno prostih s n pa je u gornjoj tablici $\varphi(m)\varphi(n)$ brojeva koji su relativno prosti i sa m i sa n, a onda i s mn.

Stoga je $\varphi(mn) = \varphi(m)\varphi(n)$ i tvrdnja je dokazana. ■

Primjer 3. *Odredimo $\varphi(1111)$. Kako je $1111 = 11 \cdot 101$, primjenom svojstva multiplikativnosti Eulerove funkcije i činjenice da su 11 i 101 prosti brojevi dobivamo*

$$\varphi(1111) = \varphi(11 \cdot 101) = \varphi(11)\varphi(101) = 10 \cdot 100 = 1000.$$

Propozicija 4. *Neka je p prost broj i $\alpha \in \mathbb{N}$. Tada vrijedi*

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

Proof. 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

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

■

Kako se svaki prirodan broj veći od 1 može prikazati u obliku $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $\alpha_i \in \mathbb{N}$, p_i prosti brojevi, $i \in \{1, \ldots, k\}$, primjenom svojstva multiplikativnosti Eulerove funkcije i upravo dokazane propozicije, dobivamo

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

Primjer 5. *Odredimo broj prirodnih brojeva koji su relativno prosti s brojem googol tj. s brojem 10^{100} i manji su od njega.*

Rješenje: Trebamo odrediti $\varphi(10^{100})$. Primjenom prethodne formule dobivamo

$$\varphi(10^{100}) = \varphi(2^{100}5^{100}) = 2^{99}5^{99}4 = 4 \cdot 10^{99}.$$

\hfill $\diamondsuit$

Primjer 6. *Odredimo sve prirodne brojeve n za koje je $\varphi(n)$ neparan broj.*

Rješenje: Već smo komentirali da je $\varphi(1) = 1$, a lako se vidi i da je $\varphi(2) = 1$.

Pretpostavimo da je $n > 2$. Ako postoji neparan faktor p_i od n, onda je $p_i - 1$ paran broj pa je $\varphi(n)$ paran broj zbog (1). Ako ne postoji neparan faktor p_i od n, onda je $n = 2^\alpha$, $\alpha \geq 2$, pa je

$$\varphi(n) = 2^{a-1}(2-1) = 2^{a-1}.$$

Kako je $\alpha - 1 \geq 1$ slijedi da je $\varphi(n)$ paran broj.

Zaključujemo da je $\varphi(n)$ neparan broj samo za $n \in \{1, 2\}$. \hfill $\diamondsuit$

Primjer 7. *Pokažimo da postoji beskonačno mnogo pozitivnih cijelih brojeva n takvih da je*

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

Rješenje: Za sve $n = 2 \cdot 3^m$, $m \in \mathbb{N}$, vrijedi

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

Time je tvrdnja dokazana. \hfill $\diamondsuit$

3 Svojstva Eulerove funkcije

U ovom ćemo dijelu dokazati još neka svojstva Eulerove funkcije.

Propozicija 8. *Neka je n prirodan broj. Ako $d \mid n$, onda $\varphi(d) \mid \varphi(n)$.*

Proof. Neka je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Ako $d \mid n$, onda je $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$, gdje je $0 \leq \beta_i \leq \alpha_i$, $i = 1, \ldots, k$. Uvrštavanjem u formulu (1) dobije se da je

$$\frac{\varphi(n)}{\varphi(d)} = \prod_{i=1}^{k} p^{\alpha_i - \beta_i}.$$

Kako je, zbog $\alpha_i - \beta_i \geq 0$, broj s desne strane ove jednakosti prirodan, time je tvrdnja dokazana. ■

Propozicija 9. *[Gauss] Za sve prirodne brojeve n vrijedi*

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

Proof. Neka je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Promatrajmo sljedeći produkt

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

Množenjem faktora ovog produkta dobivamo sumu pribrojnika oblika

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

gdje je $0 \leq \beta_i \leq \alpha_i$, $i = 1, \ldots, k$. Kako su s $p_1^{\beta_1} \cdots p_k^{\beta_k}$, $0 \leq \beta_i \leq \alpha_i$, $i = 1, \ldots, k$, dani svi djelitelji broja n, zaključujemo da je

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{\alpha_i})). \tag{3}$$

Stoga je

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

i time je tvrdnja dokazana. ■

Propozicija 10. *Za svaki prirodan broj m postoji konačno mnogo prirodnih brojeva n takvih da je $\varphi(n) = m$.*

Proof. Ako neka potencija prostog broja p dijeli n, tj. $p^{\alpha} \mid n$, prema Propoziciji (8) vrijedi $p^{\alpha-1}(p-1) \mid \varphi(n) = m$. No, onda je

$$p^{\alpha} \leq \frac{mp}{p-1} \leq 2m.$$

Kako postoji samo konačno mnogo brojeva p^{α} takvih da je $p^{\alpha} \leq 2m$, postoji i konačno mnogo produkata takvih potencija prostih brojeva. Stoga postoji i konačno mnogo prirodnih brojeva s danim svojstvom. ■

U nastavku donosimo dvije ocjene za Eulerovu funkciju.

Propozicija 11. *Ako je n složen prirodan broj, tada je*

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

Proof. 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 12. *Za sve prirodne brojeve n, $n \neq 2, 6$, vrijedi*

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

Proof. Za $n = p^m$, gdje je p prost broj i $m \geq 2$, vrijedi $\frac{m}{2} \leq m - 1$ pa slijedi

$$\varphi(n) = p^{m-1}(p-1) \geq p^{m-1} \geq \sqrt{p^m} = \sqrt{n}. \tag{4}$$

U slučaju kada je $p \neq 2$ vrijedi i

$$\varphi(n) = p^{m-1}(p-1) \geq p^{m-1}\sqrt{2} \geq \sqrt{2p^m} = \sqrt{2n}. \tag{5}$$

Neka je $n = p$, $p \geq 3$, gdje je p prost broj. Lako se vidi da je kvadratna funkcija $f(x) = x^2 - x - 1$ pozitivna za $x > \frac{1+\sqrt{5}}{2}$. Uz supstituciju $x = \sqrt{t}$ dobivamo da za $t > \left(\frac{1+\sqrt{5}}{2}\right)^2$ vrijedi $\sqrt{t} < t - 1$. Stoga za $p \geq 3$ vrijedi $\sqrt{p} < p - 1$ pa je

$$\varphi(n) = p - 1 > \sqrt{p} = \sqrt{n}. \tag{6}$$

Za $p \geq 5$ analogno se može pokazati da je

$$\varphi(n) = p - 1 > \sqrt{2p} = \sqrt{2n}. \tag{7}$$

Ako je n neparan ili $4 \mid n$, (4) i (6) povlače da vrijedi

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

Ako je $n = 2k$, gdje je k neparan broj, tada za $n \neq 6$ slijedi da 9 dijeli k ili k ima barem jedan prost faktor $p \geq 5$. Iz (5)–(7) slijedi

$$\varphi(n) = \varphi(k) \geq \sqrt{2k} = \sqrt{n}.$$

■

4 Eulerov teorem

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

Teorem 13. *{(Eulerov teorem)} Ako su $n \in \mathbb{N}$ i $a \in \mathbb{Z}$ takvi da $(a, n) = 1$, onda je*

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

Proof. Ako je $\{r_1, \ldots, r_{\varphi(n)}\}$ reducirani sustav ostataka modulo n, onda je, za $(a, n) = 1$, i $\{ar_1, \ldots, ar_{\varphi(n)}\}$ reducirani sustav ostataka modulo n (jer iz $ar_i \equiv ar_j \pmod{n}$ i $(a, n) = 1$ slijedi $i = j$). No, onda mora vrijediti

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

odnosno

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

Kako je $(r_i, n) = 1$, $i = 1, \ldots, n$, odavde slijedi

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

■

Ako je n prost broj, onda iz Eulerovog teorema direktno slijedi Mali Fermatov teorem.

Korolar 14. *(Mali Fermatov teorem) Neka je p prost broj. Ako $p \nmid a$, onda je*

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

Primjer 15. *Odredimo ostatak pri dijeljenju broja 2017^{10^6} sa 55.*

Rješenje: Kako je $\varphi(55) = \varphi(5)\varphi(11) = 40$ i $(2017, 55) = 1$, iz Eulerovog teorema slijedi

$$2017^{40} \equiv 1 \pmod{55}.$$

No, onda je

$$2017^{10^6} \equiv 2017^{40 \cdot 25000} \equiv 1 \pmod{55}.$$

Stoga je traženi ostatak 1. \hfill $\diamondsuit$

Primjer 16. *Odredimo posljednje tri znamenke u decimalnom zapisu broja 3^{4004}.*

Rješenje: Uočimo da rješenje možemo dobiti određivanjem ostatka pri dijeljenju danog broja s 1000. Budući da je $\varphi(1000) = \varphi(2^3)\varphi(5^3) = 400$ i $(3, 1000) = 1$ primjenom Eulerovog teorema dobivamo

$$3^{400} \equiv 1 \pmod{1000},$$

odakle slijedi

$$3^{4004} \equiv 3^{400 \cdot 10 + 4} \equiv 3^4 \equiv 81 \pmod{1000}.$$

Odavde zaključujemo da su zadnje tri znamenke broja 3^{400} jednake 081. \hfill $\diamondsuit$

Primjer 17. *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

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

pa je

$$n^{24}+17 \equiv 1+17 \equiv 0 \pmod{18}$$

i time je tvrdnja dokazana. \hfill $\diamondsuit$

Spomenimo samo da Eulerov teorem i Mali Fermatov teorem imaju dvije važne primjene:

- Najpoznatiji kriptosustav s javnim ključem, RSA kriptosustav, bazira se na Eulerovom teoremu (vidi npr. [12]).
- Iako obrat Malog Fermatovog teorema ne vrijedi (može se pokazati da je npr. $2^{340} \equiv 1 \pmod{341}$, ali $341 = 11 \cdot 31$), Mali Fermatov teorem je baza za razne testove prostosti (vidi npr. [16]).

5 Problemi vezani uz Eulerovu funkciju

U ovom dijelu opisat ćemo neke od poznatih problema koji su vezani uz Eulerovu funkciju.

5.1 Gauss-Wantzelov teorem

Kažemo da je pravilni n-terokut konstruktibilan ako se može konstruirati samo pomoću ravnala i šestara. Gauss je 1796. godine pokazao da je pravilni 17-terokut konstruktibilan, a u Disquisitiones Arithmeticae je poopćio ovaj rezultat te je dokazao uvjet dovoljnosti iz teorema koji ćemo navesti. Uvjet nužnosti dokazao

dokazao je Wantzel [18] 1837. godine.

Tvrdnja teorema u uskoj je vezi s Fermatovim prostim brojevima tj. prostim brojevima oblika $F_n = 2^{2^n} + 1$. Poznato je samo 5 prostih Fermatovih brojeva (to su $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ i $F_4 = 65537$) i otvoreni je problem ima li ih još.

Teorem 18. *Pravilan n-terokut može se konstruirati ravnalom i šestarom ako i samo ako se n može prikazati u obliku produkta neke potencije broja dva 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 $F_{n_1}, \ldots, F_{n_j}$ su različiti Fermatovi prosti brojevi.*

Wantzel je pokazao da se Teorem (18) može izreći i na sljedeći način:

Teorem 19. *Pravilan n-terokut može se konstruirati ravnalom i šestarom ako i samo ako je n prirodan broj veći od 2 takav da je $\varphi(n)$ potencija broja 2.*

5.2 Lehmerov problem

Znamo da za prost broj p vrijedi $\varphi(p) = p - 1$. Lehmer je 1932. godine 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/slutnja 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 [6] dokazali su 1980. godine da je $n > 10^{20}$ i $\omega(n) \geq 14$. Burcsi, Czirbusz i Farkas su 2011. pokazali da ako $3 \mid n$, onda je $n > 10^{360000000}$ i $\omega(n) \geq 40000000$.

5.3 Carmichaelova slutnja i Fordov teorem

1907. godine Carmichael [3] je objavio teorem u kojem je tvrdio da ne postoji broj n takav da za sve $m \neq n$ vrijedi $\varphi(n) \neq \varphi(m)$. Međutim, 1922. godine pronađena je greška u dokazu. Iako tvrdnja još uvijek nije

dokazana, pretpostavlja se da je točna i danas je ta pretpostavka poznata kao *Carmichaelova slutnja*. Često se iskazuje i u sljedećem obliku:

> *Za sve prirodne brojeve* n jednadžba $\varphi(x) = n$ ne može imati jedinstveno rješenje.}

Carmichael [4] je dokazao da kontraprimjer njegovoj pretpostavci mora biti broj veći ili jednak od 10^{37}. Pomerance [15] je pokazao 1974. da je prirodan broj n kontraprimjer ovoj pretpostavci ako za svaki prost broj p takav da $p-1 \mid \varphi(n)$ vrijedi $p^2 \mid n$. Ford [9] je 1998. godine pokazao da eventualni kontraprimjer mora biti veći od $10^{10^{10}}$.

Vezano uz broj rješenja jednadžbe $\varphi(x) = n$ poznata je i slutnja koju je iznio Sierpiński:

> *Za svaki prirodni broj* $k \geq 2$ postoji prirodni broj n takav da jednadžba $\varphi(x) = n$ ima točno k rješenja.}

Ford [10] je 1998. dokazao da je slutnja točna.

Bibliografija

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

[2] P. Burcsi, S. Czirbusz, G. Farkas, *Computational investigation of Lehmer's totient problem*, Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Comput. {\bf 35} (2011), 43–49.

[3] R. D. Carmichael, *On Eulers*φ-function}, Bull. Amer. Math. Soc. (N.S.) {\bf 13} (1907), 241–243.

[4] R. D. Carmichael, *Note on Eulers*φ-function}, Bull. Amer. Math. Soc. (N.S.) {\bf 28} (1922), 109–110.

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

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

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

[8] L. Euler, *Theoremata arithmetica nova methodo demonstrata*, Novi commentarii academiae scientiarum imperialis Petropolitanae {\bf 8} (1763), 74–104.

[9] K. Ford, *The number of solutions of*$\varphi(x) = m$}, Ann. of Math. {\bf 150} (1999), 283–311.

[10] K. Ford, *The distribution of totients*, Ramanujan J. {\bf 2} (1998), 67–151.

[11] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, Germany, 1801, (Yale University Press, New Haven, 1965).

[12] B. Ibrahimpašić, *RSA kriptosustav*, Osječki matematički list {\bf 5} (2005), 101–112.

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

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

[15] C. Pomerance, *On Carmichael's conjecture*, Proc. Amer. Math. Soc. {\bf 43} (1974), 297–298.

[16] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1994.

[17] J. J. Sylvester, *On certain ternary cubic-form equations*, Amer. J. Math. {\bf 2} (1879), 357–393.

[18] P. L. Wantzel, *Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas*, J. Math. Pures Appliq. {\bf 1} (1836), 366–372.

ISSN 1334-6083