Osnovni teorem aritmetike

Špiranec, Sara

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

Sara Špiranec

Osnovni teorem aritmetike

Završni rad

Osijek, 2017.

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

Sara Špiranec

Osnovni teorem aritmetike

Završni rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2017.

Sažetak

Tema ovog završnog rada bila je osnovni teorem aritmetike. U prvom dijelu rada upoznajemo se s osnovnim strukturama brojeva koje su nam potrebne za daljnju razradu osnovnog teorema aritmetike. Također, potreban nam je pojam djeljivosti u skupu cijelih bojeva te prosti brojevi koje uvodimo neposredno nakon podjele brojeva na prirodne i cijele. Zatim, uz pomoć prostih brojeva navodimo osnovni teorem aritmetike i njegov dokaz. Teorem je vrlo koristan rezultat u matematici. Primjenjuje se u mnogim područjima teorije brojeva. Veoma je važan u raznim primjenama kongruencija, kao i u primjeni metoda za šifriranje i dešifriranje poruka kojima se bavi znanstvena disciplina kriptografija.

Ključne riječi

Prosti brojevi, faktorizacija, djeljivost

Fundamental theorem of arithmetic

Summary

The theme of this final work was the fundamental theorem of arithmetic. In the first part of the paper, we will get acquainted with the basic structure of numbers that we need to further elaborate the fundamental theorem of arithmetic. Also, we need the notion of divisibility in the set of whole numbers and the prime numbers that we introduce immediately after the division of numbers into the natural and the whole. Then, with the help of prime numbers, we state the fundamental theorem of arithmetic and its proof. The theorem is a very useful result in mathematics. Applies to many areas of the theory of numbers. It is very important in various applications of congruence, as well as in the application of methods for encryption and decryption of messages dealing with scientific discipline cryptography.

Key words

Prime numbers, factorization, divisibility

Sadržaj

Uvod

Svestrani matematički genij i jedan od najvećih matematičara uopće, Nijemac Johann Carl Friedrich Gauss izjavio je kako je "matematika kraljica znanosti, a teorija brojeva kraljica matematike". Engleski matematičar Godfrey Harold Hardy ohrabren tom izjavom, u svom djelu *Isprike jednog matematičara* objavljenom 1940. godine, istaknuo je kako smatra da je najljepša matematika upravo čista, teorijska matematika, koja je lišena mogućnosti praktične primjene, u čemu prednjači upravo teorija brojeva. Teorija brojeva je češći naziv za aritmetiku, što je grana matematike koja se bavi brojevima (najčešće prirodnim i cijelim). Hardy smatra kako se ishodište Gaussova stava očituje u činjenici da su temeljni pojmovi i koncepti teorije brojeva mnogo čišći, dublji i elegantniji od istih u drugim granama matematike. Među glavne oslonce te teze pripada i pojam djeljivosti koji nas dovodi do osnovnog teorema aritmetike. Osnovni teorem aritmetike kaže nam da se svaki prirodan broj može prikazati kao produkt prostih brojeva na jedinstven način do na poredak pripadnih prostih faktora. Iako se osnovni teorem aritmetike ponekad pripisuje Euleru. Početkom 19. stoljeća, Carl Friedrich Gauss prvi je iznio pravilan i detaljan iskaz i dokaz ovog rezultata. Najbliže što se Euklid približio navedenom rezultatu je propozicija koja glasi:

"Ako je broj izmjeren prostim brojevima, onda ne može biti izmjeren niti jednim prostim brojem izuzev onih kojima je izvorno izmjeren."

Euklid nije mogao doći do općenitog iskaza osnovnog teorema aritmetike zbog nemogućnosti da prikaže produkt u kome broj faktora nije određen. Često je i mišljenje kako se tada jednostavno nije moglo doći do rezultata o egzistenciji prikaza prirodnog broja kao produkta prostih brojeva jer Grci nisu mogli pojmiti egzistenciju nečega što nije konstruktibilno metodama elementarne geometrije. U ovome radu prezentiramo osnovni teorem aritmetike te opisujemo njegovu primjenu u pojedinim područjima matematike.

1 Brojevi

U suvremenoj matematici brojevi se dijele na prirodne, cijele, racionalne, iracionalne, realne i kompleksne. U ovom poglavlju malo ćemo se bolje upoznati sa prirodnim i cijelim brojevima.

1.1 Prirodni brojevi

U neprestupnoj jednoj godini ima dvanaest mjeseci ili tristo šezdeset pet dana. U razrednom odjeljenju ima dvadeset šest učenika. Mario je uštedio sto trideset i pet kuna. Brojevi $1, 12, 365, 26, 135$ koji su se pojavili u tim rečenicama nazivaju se prirodni brojevi. Njih upotrebljavamo pri prebrojavanju raznovrsnih objekata iz naše okoline.

Skup svih prirodnih brojeva označavamo s $\mathbb{N}$:

$$\mathbb{N} = \{1, 2, 3, \ldots, n, n+1, \ldots\}.$$

On se često proširuje borjem 0 te ga u tom slučaju označavamo s $\mathbb{N}_0$.

Za dva prirodna broja a i b vrijedi jedna od sljedeće tri mogućnosti:

a) $a < b$ - relacija *"biti manji od"* (npr. $11 < 13$)

b) $a = b$ - relacija *"biti jednak"* (npr. $18 = 18$)

c) $a > b$ - reklacija *"biti veći od"* (npr. $6 > 5$)

Broj 1 je najmanji prirodni broj. Svaki prirodan broj ima svog sljedbenika, tj. broj koji je za jedan veći od zadanog broja (npr. broj 12 je sljedbenik broja 11).

Svaki prirodan broj manji je od svog sljedbenika.

Napomena 1. *Ako je $m \in \mathbb{N}$, tada je $m + 1 \in \mathbb{N}$ njegov sljedbenik.*

Svi prirodni brojevi, osim broja 1, imaju svog prethodnika, tj. broj koji je za jedan manji od zadanog broja (npr. broj 12 je prethodnik broja 13).

Svaki prirodni broj veći je od svog prethodnika.

Napomena 2. *Ako je $m \in \mathbb{N}$, tada je $m - 1 \in \mathbb{N}_0$ njegov prethodnik.*

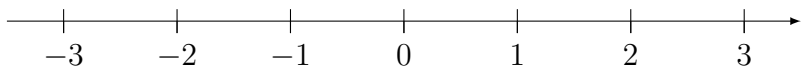
Najveći prirodni broj ne postoji, tj. skup prirodnih brojeva je beskonačan.

1.2 Cijeli brojevi

Često u skupu prirodnih brojeva ne možemo izvršiti operaciju oduzimanja. Naime, ako su $a, b, c \in \mathbb{N}$ i $a - b = c$, pri čemu je $a < b$, takav prirodan broj c ne postoji.
Zbog toga uvodimo negativne prirodne brojeve te 0, koji zajedno s pozitivnim prirodnim brojevima čine skup cijelih brojeva. Označavamo ga sa $\mathbb{Z}$.

$$\mathbb{Z} = \{\ldots, -m-1, -m, \ldots, -2, -1, 0, 1, 2, \ldots, m, m+1, \ldots\}$$

Na brojevnom pravcu desno od 0 nalaze se pozitivni cijeli brojevi, dok se lijevo od 0 nalaze negativni cijeli brojevi.



Cijeli brojevi koji su simetrično smješteni na pravcu u odnosu na nulu međusobno su suprotni.

Modul cijelog broja (apsolutna vrijednost) je udaljenost cijeloga broja od ishodišta na pravcu. Ona je uvijek pozitivni broj ili 0. Označava se s $|z|$.

Primjer 1. $|0| = 0,\ |1| = 1,\ |-27| = 27$

Cijeli broj a manji je od cijelog broja b ako se na brojevnom pravcu nalazi lijevo od broja b. Od dva negativna broja manji je onaj koji ima veću apsolutnu vrijednost.

Primjer 2. $13 < 18,\ 0 < 11,\ -31 < -11,\ -5 < 10$

Analogno kao i kod prirodnih brojeva, za cijeli broj z definiramo prethodnika $z - 1$ i sljedbenika $z + 1$.
Također, ne postoji najveći niti najmanji cijeli broj, tj. skup cijelih brojeva je beskonačan.

2 Djeljivost

Pojam djeljivosti jedan je od najjednostavnijih, ali ujedno i najvažnijih pojmova u teoriji brojeva. Stoga ćemo ga malo bolje promotriti.

2.1 Osnovni pojmovi

Definicija 1. *Neka su $a, b \in \mathbb{Z}$, $a \neq 0$. Ako postoji $d \in \mathbb{Z}$ takav da vrijedi $b = a \cdot d$, onda kažemo da a dijeli b. Oznaka: $a \mid b$. Tada se a naziva djelitelj broja b, a b se naziva višekratnik broja a. Ako a ne dijeli b, pišemo $a \nmid b$.*

Primjer 3.

a) $6 = 2 \cdot 3$, *očito* $2 \mid 6$ *i* $3 \mid 6$

b) $2 \mid -10$ *jer je* $-10 = 2 \cdot (-5)$.

Napomena 3.

a) $0 \cdot a = 0 \Rightarrow a \mid 0, \forall a \in \mathbb{Z}$

b) $1 \cdot b = b \Rightarrow 1 \mid b, \forall b \in \mathbb{Z}$

c) $a \in \mathbb{Z}$ *i* $a \mid 1 \Rightarrow a \in \{-1, 1\}$.

Propozicija 1 (vidi [5, Propozicija 1.1.1.])**.**

1) Ako $a \mid b$ i $b \neq 0$, onda je $|a| \leq |b|$.

2) Ako $a \mid b$, onda a dijeli svaki višekratnik od b.

3) Ako $a \mid b$ i $a \mid c$, onda $a \mid (b \pm c)$ i $a \mid bc$.

Dokaz:

1) Neka $a \mid b$ i $b \neq 0$. Iz toga slijedi da postoji $d \in \mathbb{Z}$ takav da vrijedi $b = a \cdot d$, $d \neq 0$. Tada vrijedi i $|b| = |a| \cdot |d|$. Jer je $|d| \geq 1$ slijedi $|a| \leq |b|$.

2) Neka $a \mid b$ i neka je c višekratnik broja b, tj. $c = b \cdot d$. Kako $a \mid b$ postoji $d' \in \mathbb{Z}$ takav da je $b = a \cdot d'$.
Prema tome je $c = b \cdot d = a \cdot (d' \cdot d)$, pa po definiciji $a \mid c$.

3) Neka $a \mid b$, tj. $b = a \cdot d$ i $a \mid c$, tj. $c = a \cdot d'$, pri čemu su $d, d' \in \mathbb{Z}$.

$$b \pm c = ad \pm ad' = a(d \pm d') \quad \Rightarrow \quad a \mid (b \pm c)$$

$$b \cdot c = ad \cdot ad' = a(add') \quad \Rightarrow \quad a \mid bc$$

.

□

Iz tvrdnje 1) prethodne propozicije možemo uočiti da ako $a \mid b$ i $b \mid a$, vrijedi da je $a \in \{-b, b\}$.

Slijedi nam jedan od osnovnih teorema čitave teorije brojeva:

Teorem 1 (**Teorem o dijeljenju s ostatkom**, vidi [2, Teorem 1.1.]). *Za $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ postoje jedinstveni cijeli brojevi q i r takvi da je*

$$b = aq + r, \quad 0 \leq r < a.$$

Dokaz:

- Egzistencija:
  Neka je q cijeli broj sa svojstvom

  $$q \leqslant \frac{b}{a} < q + 1$$
  $$0 \leqslant \frac{b}{a} < 1.$$

  Definiramo cijeli broj r kao $r = a\left(\frac{b}{a} - q\right) = b - aq$ iz čega slijedi da je $b = aq + r$. Pomnožimo li dobivenu nejednakost $0 \leqslant \frac{b}{a} < 1$ s a dobivamo da je $0 \leq r < a$.

- Jedinstvenost:
  Pretpostavimo suprotno, tj. da postoje cijeli brojevi q_1 i r_1 takvi da je $b = aq_1 + r_1$, $0 \leq r_1 < a$.
  Imamo da je $aq + r = aq_1 + r_1$, tj. $a(q - q_1) = r_1 - r$.
  Ako je $r_1 = r$, onda je i $q_1 = q$ jer je $a \neq 0$, pa pretpostavimo suprotno. Neka je $r_1 \neq r$, pa je i $q_1 \neq q$.
  Kako je $a(q - q_1) = r_1 - r$, vrijedi i $|a(q - q_1)| = |r_1 - r| \geq a$, ali zbog $0 \leq r_1, r < a$ vrijedi da je $|r_1 - r| < a$ što nas dovodi do kontradikcije iz čega slijedi jedinstvenost.

□

Broj r iz teorema o dijeljenju s ostatkom nazivamo ostatak pri dijeljenju broja a brojem b, dok q nazivamo kvocijent cjelobrojnog dijeljenja.

Neka je $\lfloor\rfloor : \mathbb{R} \to \mathbb{R}$ funkcija definirana s $\lfloor x \rfloor$ = najveći cijeli broj koji nije veći od x, $x \in \mathbb{R}$. Takva funckija zove se "pod od x". Ponekad se kaže i "najveće cijelo od x" (zanemaruje se s koje strane omeđujemo x). Tada se kvocijent cjelobrojnog dijeljenja q može zapisati u obliku $q = \lfloor \frac{b}{a} \rfloor$. Više o cjelobrojnim funkcijama može se naći u [6] .

Primjer 4.

a) $36 = 5 \cdot 7 + 1 \;\Rightarrow\; q = \lfloor \frac{36}{7} \rfloor = 5, \;\; r = 1$

b) $-12 = 5 \cdot (-3) + 3 \;\Rightarrow\; q = \lfloor \frac{-12}{5} \rfloor = -3, \;\; r = 3$

Korolar 1. *Za neki $a \in \mathbb{N}$, svaki cijeli broj b može se prikazati u jednom od sljedećih oblika: aq, $aq+1$, $\ldots$, $aq+a-1$.*

Dokaz: Dokaz se može vidjeti u [3, Representations of Integers]. □

Primjer 5. *$b \in \mathbb{Z}$ je jednog od oblika $3q, 3q+1, 3q+2$.*

Definicija 2. *Ako $a \mid b$ i $a \mid c$ kažemo da je a zajednički djelitelj brojeva b i c, pri čemu su $a, b, c \in \mathbb{Z}$, $a \neq 0$. Ukoliko je barem jedan od brojeva b i c različit od 0, onda postoji samo konačno mnogo zajedničkih djelitelja od b i c. (Ako su i b i c jednaki nuli, onda oni imaju beskonačno mnogo djelitelja.) Najveći među njima zove se najveći zajednički djelitelj brojeva b i c. Njega označavamo s (b, c).*
Slično se definira i najveći zajednički djelitelj cijelih brojeva $b_1, b_2, \ldots, b_n$ koji nisu svi jednaki nula. Oznaka: $(b_1, b_2, \ldots, b_n)$.

Napomena 4. *Broj (b, c) je uvijek prirodan broj. Dadatno još vrijedi i*

$$(b, c) = (c, b) = (-b, c).$$

Primjer 6.

a) $(40, 13) = 1$
$(40, 30) = 10$

b) $(a, a \cdot b) = |a|$

c) $(40, 30, 2) = 2$
$(40, 30, 3) = 1.$

Definicija 3. *Ako je najveći zajednički djelitelj cijelih brojeva a i b jednak 1 kažemo da su a i b relativno prosti. Analogno, za $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, ako je $(b_1, b_2, \ldots, b_n) = 1$, kažemo da su $b_1, b_2, \ldots, b_n$ relativno prosti.*
Ako je $(b_i, b_j) = 1$, $i \neq j$, $i.j \in \{1, \ldots, n\}$ kažemo da su brojevi $b_1, b_2, \ldots, b_n$ u parovima relativno prosti.

Primjer 7.

a) *40 i 13 su relativno prosti;*

b) *40, 30 i 3 nisu u parovima relativno prosti jer je npr.* $(40, 30) = 10 \neq 1$, *ali jesu relativno prosti.*

2.2 Euklidov algoritam

Najprije promotrimo sljedeći primjer:

Primjer 8. *Odredite* $(70, 32)$.

Rješenje:

Prema Propoziciji 1, svaki zajednički djelitelj brojeva 70 i 32 dijeli i njihovu razliku. Prema tome $(70, 32) \mid 70-32 = 38$. Dakle, $(70, 32)$ je i zajednički djelitelj brojeva 32 i 38. No, kako je svaki zajednički djelitelj brojeva 32 i 38 ujedno i djelitelj broja 70, dobivamo jednakost $(70, 32) = (32, 38)$. Slično vidimo da vrijedi i $(70, 32) \mid 70 - 2 \cdot 32 = 6$. Time se problem sveo na određivanje broja $(32, 6)$ koji je očito jednak 2. Dakle, $(70, 32) = (6, 32) = (6, 2) = 2$.

Lema 1 (vidi [5, Euklidov algoritam 1.2.]). *Ako su $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ takvi da postoje jedinstveni cijeli brojevi q i r takvi da je $b = aq + r$, $0 \leq r < a$, onda je $(a, b) = (a, r)$.*

Dokaz:

Označimo $(a, b) = d_1$, $(a, r) = d_2$. Iz jednakosti $r = b - aq$ i $d_1 \mid a$ i $d_1 \mid b$ slijedi da $d_1 \mid r$. Vidimo da d_1 dijeli i a i r pa je $d_1 \leq d_2$.
Iz jednakosti $b = aq + r$ i $d_2 \mid a$ i $d_2 \mid r$ slijedi da $d_2 \mid b$. Vidimo da d_2 dijeli i a i b pa je $d_2 \leq d_1$.
Kako je $d_1 \leq d_2$ i $d_2 \leq d_1$ slijedi da je $d_1 = d_2$.

□

Pretpostavimo da smo uzastopnom primjenom teorema o dijeljenju s ostatkom dobili sljedeći niz jednakosti:

$$\begin{aligned}
b &= aq_1 + r_1, \quad 0 < r_1 < a && (1)\\
a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 && (2)\\
r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 && (3)\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1} && (\mathrm{n})\\
r_{n-1} &= r_nq_{n+1} + 0, && (\mathrm{n}{+}1)
\end{aligned}$$

Kako je $a > r_1 > r_2 > \ldots > r_n > 0$ postupak će završiti u konačno mnogo koraka. Iz Leme 1. slijedi da je $(a, b) = (a, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$, $r_n > 0$, $r_n \mid r_{n-1}$. Ujedno r_n je posljednji ostatak različit od 0 u Euklidovom algoritmu.

Primjer 9. *Odredite* $(53357, 547)$.

Rješenje:

$$\begin{aligned}
53357 &= 547 \cdot 97 + 298\\
547 &= 298 \cdot 1 + 249\\
298 &= 249 \cdot 1 + 49\\
249 &= 49 \cdot 5 + 4\\
49 &= 4 \cdot 12 + 1\\
4 &= 1 \cdot 4.
\end{aligned}$$

Odatle je $(53357, 547) = 1$.

Napomena 5. *Primijetimo da iz prve jednakosti Euklidova algoritma možemo zapisati* $r_1 = b - q_1 a$. *Uvrštavanjem u idući redak dobivamo* $r_2 = (1 + q_1 q_2)a - q_2 b$. *Nastavljajući na isti način možemo zaključiti da postoje cijeli brojevi* x *i* y *za koje vrijedi*

$$ax + by = r_n = (a, b).$$

Taj identitet se naziva Bezoutov identitet.

Dakle, Euklidovim algoritmom može se odrediti rješenje linearne algebarske jednadžbe s cjelobrojnim koeficijentima $ax + by = (a, b)$. Općenito se takve jednadžbe zovu i linearne diofantske jednadžbe. Neki algoritmi za rješavanje različitih tipova diofantskih jednadžbi mogu se vidjeti npr. u [4].

Primjer 10. *Riješimo diofantsku jednadžbu*

$$53357x + 547y = (53357, 547).$$

Na prethodno opisani način imali bi:

$$\begin{aligned} 298 &= 53357 - 547 \cdot 97 \\ 249 &= 98 \cdot 547 - 1 \cdot 53357 \\ 49 &= 2 \cdot 53357 - 195 \cdot 547 \\ 4 &= 1073 \cdot 547 - 11 \cdot 53357 \\ 1 &= 134 \cdot 53357 - 13071 \cdot 547 \\ (53357, 547) &= 1. \end{aligned}$$

Time smo dobili da je $x = 134$ i $y = -13071$.

Teorem 2 (vidi [1, Korolar 2.2.])**.** *Neka su* $a, b \in \mathbb{Z}$ *i* $m \in \mathbb{Z}\backslash\{0\}$. *Jednadžba* $ax + by = m$ *ima cjelobrojno rješenje ako i samo ako* $(a, b) \mid m$.

Dokaz:

($\Longrightarrow$) Pretpostavimo da postoje $x, y \in \mathbb{Z}$ takvi da je $ax + by = m$. Kako $(a, b) \mid a$ i $(a, b) \mid b$ slijedi da i $(a, b) \mid m$.

($\Longleftarrow$) Pretpostavimo da $(a, b) \mid m$. Tada postoji cijeli broj t takav da je $m = (a, b) \cdot t$. Iz Euklidovog algoritma znamo da postoje cijeli brojevi x i y takvi da vrijedi $ax + by = (a, b)$. Pomnožimo li tu jednakost sa t imamo $a(xt) + b(yt) = (a, b) \cdot t = m$. Dakle, postoje $X, Y \in \mathbb{Z}$ takvi da je $aX + bY = m$.

□

Teorem 3 (vidi [5, Teorem 1.2.1.])**.**

1) Najmanji prirodni broj m za koji jednadžba $ax + by = m$ ima rješenje je (a, b).

2) Za $(a, b) = 1$ jednadžba $ax + by = 1$ ima cjelobrojno rješenje. Također, ako $ax + by = 1$ ima cjelobrojno rješenje, tada je $(a, b) = 1$.

Dokaz: Dokaz se može vidjeti u [5]. □

Primjer 11. *Neka je $a = 31$ i $b = 15$.*

$$\begin{aligned} 31 \cdot 2 + 15 \cdot (-4) = 2 \quad &\Rightarrow \quad (31, 15) \mid 2 \\ 31 \cdot 1 + 15 \cdot (-2) = 1 \quad &\Rightarrow \quad (31, 15) = 1. \end{aligned}$$

Vidimo da jednadžba $31x + 15y = 1$ ima rješenje $x = 1$, $y = -2$, pa teorem implicira da je $(31, 15) = 1$.

U sljedećem teoremu vidjet ćemo koliki je broj mogućih koraka u Euklidovom algoritmu. U tu svrhu prisjetimo se:

Definicija 4. *Niz (F_n) zadan početnim vrijednostima $F_0 = 0$, $F_1 = 1$, te rekurzivnom relacijom*

$$F_{n+1} = F_n + F_{n-1},$$

za sve $n \geq 1$, $n \in \mathbb{N}$, naziva se Fibonaccijev niz. Opći član niza F_n još zovemo n-ti Fibonaccijev broj. Također, za Fibonaccijeve brojeve vrijedi tzv. Binetova formula:

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right].$$

Teorem 4 (**Lameov teorem**, vidi [5, Propozicija 1.2.2.])**.** *Neka su a i b prirodni brojevi takvi da je $b \geq a$. Broj koraka Euklidova algoritma manji je ili jednak od 5 ($\lfloor \log a \rfloor + 1$).*

Dokaz: Neka su $a, b \in \mathbb{N}$ i $b \geq a$. Najprije pokažimo da je broj znamenki broja a upravo $\lfloor \log a \rfloor + 1$.
Označimo broj znamenki broja a (u dekadskom zapisu) s n. Očito vrijedi da je $10^{n-1} \leqslant a < 10^n$. Logaritmiranjem toga izraza dobivamo $n - 1 \leqslant \log a < n$, odakle direktno slijedi da je $n = \lfloor \log a \rfloor + 1$.

Pretpostavimo kako smo primjenom Euklidovog algoritma dobili sljedeći niz jednakosti:

$$\begin{aligned} b &= q_{n-1}a + r_{n-1}, \quad 0 < r_{n-1} < a \\ a &= q_{n-2}r_{n-1} + r_{n-2}, \quad 0 < r_{n-2} < r_{n-1} \\ &\vdots \\ r_3 &= q_1 r_2 + r_1, \quad 0 < r_1 < r_2 \\ r_2 &= q_0 r_1. \end{aligned}$$

Dakle, imamo n koraka u provedbi algoritma te smo, samo za potrebe ovog dokaza, označili dobivene ostatke redom s $a = r_n > r_{n-1} > \ldots > r_1$. Kako je za svaki i, $q_i \geqslant 1$, dobivamo $r_{i+1} \geqslant r_i + r_{i-1}$. Osim toga, $r_1 \geqslant 1$ i $r_2 \geqslant 2$. Iz toga dobivamo:

$$r_3 \geqslant r_2 + r_1 \geqslant 3$$
$$r_4 \geqslant r_3 + r_2 \geqslant 5$$
$$r_5 \geqslant r_4 + r_3 \geqslant 8.$$

Možemo zaključiti kako je $r_i \geqslant F_i$, gdje je F_i i-ti Fibonaccijev broj. Dakle, $a \geqslant F_n$ i broj znamenki od a je veći ili jednak broju znamenki od F_n. Kako bi ocijenili broj znamenki Fibonaccijevog broja potrebna nam je prethodna definicija, iz koje slijedi $F_n \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}$. Odatle je $\log F_n \geqslant (n-1)\log\left(\frac{1+\sqrt{5}}{2}\right)$. Kako je $\log\left(\frac{1+\sqrt{5}}{2}\right) > \frac{1}{5}$, slijedi $\log F_n > \frac{n-1}{5}$ te je broj znamenki od F_n barem $\frac{n}{5}$.
Prema tome, broj koraka algoritma je manji ili jednak od broja znamenki broja a uvećanog 5 puta, odnosno $\lfloor \log a \rfloor + 1 \geqslant \frac{n}{5}$.

□

2.3 Prosti brojevi

Neka je $n \in \mathbb{N}$, $n > 1$. Ako n nema niti jednog djelitelja d za koji vrijedi $1 < d < n$ kažemo da je n prost broj. U suprotnom je n složen broj.
Ako je p prost broj tada on ima točno dva pozitivna djelitelja, a to su 1 i p. Obrat također vrijedi.

Primjer 12. *Broj* 11 *je prost, dok je* $143 = 11 \cdot 13$ *složen.*

Vidimo da su prirodni brojevi podijeljeni u tri klase - broj 1, prosti brojevi i složeni brojevi.

Jedan od mehaničih postupaka pronalaženja prostih brojeva manjih od n je tzv. Eratostenovo sito. Ispišemo sve brojeve od 2 do n. Krenemo od broja 2 te prekrižimo svaki njegov višekratnik. Zatim krećemo od 3 te prekrižimo svaki treći broj s time da brojimo i one već prekrižene brojeve. Ovaj postupak ponavljamo dok ne dođemo do broja p za koji je $p^2 > n$. Brojevi koji su ostali neprekriženi su prosti.

Primjer 13. $n = 20$

Rješenje:
$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}$
$2, 3, 4, 5, \cancel{6}, 7, 8, \cancel{9}, 10, 11, \cancel{12}, 13, 14, \cancel{15}, 16, 17, \cancel{18}, 19, 20$

$\Rightarrow 2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}$

$\Rightarrow 2, 3, 5, 7, 11, 13, 17$ i 19 su prosti brojevi.

Propozicija 2 (vidi [2, Djeljivost]). *Svaki složen prirodan broj n ima prost faktor* $p \leq \sqrt{n}$, $p \in \mathbb{N}$.

Dokaz: Neka je $n \in \mathbb{N}$ i neka je $p \in \mathbb{N}$ najmanji prost faktor od n. Tada postoji $m \in \mathbb{N}$ takav da je $n = mp$. Kako je p najmanji prost faktor od n vrijedi da je $m \geq p$. Množeći tu nejednakost sa p slijedi $n = mp \geq p^2$. Korjenovanjem dobivene nejednakosti slijedi tvrdnja, tj. $p \leq \sqrt{n}$. □

Napomena 6. *Prethodna propozicija može se iskoristiti za generiranje tablice prostih brojeva. Npr. ako želimo napraviti tablicu prostih brojeva manjih ili jednakih 200, napišemo brojeve od 2 do 200 pa prekrižimo sve višekratnike od 2, zatim od 3 i tako dalje. U svakom koraku prvi neprekriženi broj je prost te u idućem koraku križamo njegove višekratnike. U ovom slučaju nakon križanja višekratnika broja 13 tablica je gotova budući da je 17 prvi prost broj nakon 13, a vrijedi da je* $17 > \sqrt{200}$ *i time smo završili.*

Važnost prostih brojeva očituje se u činjenici da se svaki prirodan broj veći od 1 može prikazati u obliku produkta potencija prostih brojeva, što ćemo i dokazati. Za to će nam biti potreban aksiom dobre uređenosti koji glasi: *"Svaki neprazan podskup skupa prirodnih brojeva ima najmanji element."*

Označimo skup svih prirodnih brojeva koji se ne mogu prikazati u obliku produkta prostih brojeva sa S. Neka je a najmanji element toga skupa.
Očito a nije prost broj jer bi inače na trivijalan način bio prikazan kao produkt prostih brojeva. Prema tome, postoje prirodni brojevi b i c, oba veća od 1, takvi da je $a = b \cdot c$. Kako su b i c oba manji od a, ne mogu biti elementi skupa S, te se oba mogu napisati kao produkt prostih brojeva. No, tada se i a može zapisati u obliku produkta prostih brojeva, što nije moguće. Dakle, skup S je prazan.

Primjer 14. $28 = 7 \cdot 4 = 7 \cdot 2 \cdot 2 = 7 \cdot 2^2$

Jedinstvenost ovakvog rastava prokomentirat ćemo u sljedećem podnaslovu.

2.3.1 Osnovni teorem aritmetike

Korolar 2 (vidi [1, Korolar 2.3, Korolar 2.4.]). *Neka su* $a, b \in \mathbb{N}$. *Ako je p prost broj takav da* $p \mid ab$, *onda* $p \mid a$ *ili* $p \mid b$.
Općenitije: Neka su $a_i \in \mathbb{N}, i \in \{1, 2, \ldots, n\}$, $n \in \mathbb{N}$. *Ako* $p \mid a_1 \cdot \ldots \cdot a_n$, *onda postoji i takav da* $p \mid a_i$, $i \in \{1, 2, \ldots, n\}$.

Dokaz:

Pretpostavimo da $p \mid ab$ i da $p \nmid a$. Kako $p \nmid a$, a i p su relativno prosti pa po Euklidovom algoritmu postoje x i y takvi da je $ax + py = 1$. Pomnožimo li tu jednakost sa b dobivamo da je $abx + pby = b$. Kako $p \mid ab$ i $p \mid pby$ slijedi da $p \mid b$.
Općeniti slučaj dokazuje se metodom matematičke indukcije:

(B): $p \mid ab \;\Rightarrow\; p \mid a$ ili $p \mid b$ što znamo iz prvog dijela dokaza.

(P): Pretpostavimo da ako $p \mid a_1 \cdot \ldots \cdot a_{n-1}$, da postoji i takav da $p \mid a_i$, $i \in \{1, 2, \ldots, n-1\}$.

(K): $p \mid (a_1 \cdot \ldots \cdot a_{n-1})a_n$; prema bazi indukcije $p \mid a_1 \cdot \ldots \cdot a_{n-1}$ ili $p \mid a_n$ pa prema pretpostavci slijedi tvrdnja.

□

Teorem 5 (**Osnovni teorem aritmetike**, vidi [5, Teorem 1.4.3.]). *Svaki $n \in \mathbb{N}$, $n > 1$, može se faktorizirati, tj. prikazati u obliku produkta potencija prostih brojeva. Faktorizacija je jedinstvena do na poredak prostih faktora.*

Dokaz:

- Egzistencija:
  Metoda matematičke indukcije po prirodnom broju n.

  (B): $n = 2$ - ovo je trivijalni produkt i 2 je prost broj.

  (P): Pretpostavimo da se svi $k < n$ mogu faktorizirati.

  (K): Pretpostavimo sada broj n:
  Ako je n prost broj, onda je to opet trivijalni produkt $(1 \cdot n)$.
  Ako je n složen broj, onda postoje d i d' takvi da je $1 < d, d' < n$ i $n = d \cdot d'$.
  Sada iz pretpostavke slijedi tvrdnja, tj. n se može faktorizirati.

- Jedinstvenost:
  Pretpostavimo da postoje prosti brojevi $p_1, \ldots, p_k$ i $q_1, \ldots, q_l$ ne nužno različiti takvi da je $n = p_1 \cdot \ldots \cdot p_k$ i $n = q_1 \cdot \ldots \cdot q_l$. Slijedi $p_1(p_2 \cdot \ldots \cdot p_k) = q_1 \cdot \ldots \cdot q_l$.
  Kako $p_1 \mid q_1 \cdot \ldots \cdot q_l$ prema Korolaru 2. postoji $j \in \{1, \ldots, l\}$ takav da $p_1 \mid q_j$. Slijedi da su p_1 i q_j jednaki jer su oba prosti brojevi i $p_1 \mid q_j$.
  Permutiranjem faktora $q_1, \ldots, q_l$ možemo dobiti da je $j = 1$ pa nakon kraćenja dobivamo $p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_l$. Sličnim zaključivanjem dobivamo $p_2 = q_2, \ldots, p_k = q_l$ i $k = l$ (da je $l > k$, $q_l = 1$, a q_l je prost broj).
  Slijedi da je faktorizacija jedinstvena do na poredak faktora.

□

Time smo pokazali da svaki prirodan nroj $n \geqslant 2$ možemo na jedinstven način do na poredak faktora prikazati u obliku $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, gdje je $k \in \mathbb{N}$, $p_1, p_2, \ldots, p_k \in \mathbb{N}$

različiti prosti brojevi te $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$.

Prema tome, proste brojeve možemo smatrati temeljnim gradivnim blokovima pomoću kojih se može prikazati svaki prirodan broj.

Osnovni teorem aritmetike koristimo pri dokazivanju mnogih tvrdnji te pri samom definiranju nekih pojmova. Nešto od toga vidjet ćemo u nastavku.

2.3.2 Skup prostih brojeva

Sa $\mathcal{P}$ označavamo skup svih prostih brojeva. Osnovno svojstvo toga skupa daje nam idući teorem.

Teorem 6 (**Euklid**, vidi [2, Teorem 1.12.]). *Skup prostih brojeva $\mathcal{P}$ je beskonačan.*

Dokaz:

Pretpostavimo suprotno, tj. $\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$, $k \in \mathbb{N}$. Definirajmo $q = p_1 \cdot \ldots \cdot p_k + 1$. Vidimo da je $q > p_i$, $i = 1, \ldots, k$, pa slijedi da $q \notin \mathcal{P}$, tj. q je složen broj. Prema osnovnom teoremu aritmetike postoji $i \in \{1, \ldots, k\}$ takav da $p_i \mid q$. Kako je $q = p_1 \cdot \ldots \cdot p_k + 1$ i $p_i \mid q$ slijedi i da $p_i \mid 1$ što nije moguće.
$\Rightarrow$ Skup $\mathcal{P}$ je beskonačan.

□

Iduća propozicija daje nam koristan kriterij djeljivosti:

Propozicija 3 (vidi [5, Skup prostih brojeva 1.4.2.]). *Neka su $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ i $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}$ prirodni brojevi dani rastavom na proste faktore. Broj a je djeljiv brojem b ako i samo ako za svaki q_j, $j \in \{1, \ldots, l\}$ postoji neki $i \in \{1, \ldots, k\}$ tako da je $q_j = p_i$ i $\alpha_i \geqslant \beta_j$.*

Primjer 15. $18 = 2 \cdot 3^2 \mid 54 = 2 \cdot 3^3$, *no* $36 = 2^2 \cdot 3^2 \nmid 54$.

Također, svaki prirodan broj n možemo zapisati u obliku $n = \prod_{p \in \mathcal{P}} p^{\alpha_p}$, gdje je $\alpha_p \in \mathbb{N} \cup \{0\}$ te su svi osim konačno mnogo brojeva α_p jednaki nuli.

Propozicija 4. *vidi [2, Napomena 1.1.] Neka je $a = \prod_{p \in \mathcal{P}} p^{\alpha_p}$ i $b = \prod_{p \in \mathcal{P}} p^{\beta_p}$. Tada $a \mid b$ ako i samo ako je $\alpha_p \leqslant \beta_p$.*

Možemo zaključiti kako se najveći zajednički djelitelj može lako odrediti ukoliko je poznata njihova faktorizacija, tj. ako je $a = \prod_{p \in \mathcal{P}} p^{\alpha_p}$ i $b = \prod_{p \in \mathcal{P}} p^{\beta_p}$ vidimo da je

$$(a, b) = \prod_{p \in \mathcal{P}} p^{\min\{\alpha_p, \beta_p\}}.$$

Definicija 5. *Ukoliko su a i b cijeli brojevi različiti od nule, definiramo njihov najmanji zajednički višekratnik kao najmanji prirodan broj koji je djeljiv i s a i s b. Označavamo ga s $[a, b]$. Analogno se definira i najmanji zajednički višekratnik brojeva $a_1, \ldots, a_n \in \mathbb{Z}\backslash\{0\}$. Oznaka: $[a_1, \ldots, a_n]$.*

Ako b dijeli a, lako se može vidjeti da vrijedi $[a, b] = |a|$, odnosno ako a dijeli b, onda je $[a, b] = |b|$. Također, ukoliko $a \mid m$ i $b \mid m$, tada i $[a, b] \mid m$.

Konačno, ako su $a = \prod_{p \in \mathcal{P}} p^{\alpha_p}$ i $b = \prod_{p \in \mathcal{P}} p^{\beta_p}$ prirodni brojevi, tada vrijedi $[a, b] = \prod_{p \in \mathcal{P}} p^{\max\{\alpha_p, \beta_p\}}$. Odatle slijedi i $(a, b) \cdot [a, b] = ab$.

Definicija 6. *Kažemo da je prirodan broj n potpun kvadrat ako postoji prirodan broj m takav da je $n = m^2$.*

Iz same definicije vidimo da niti jedan prost broj ne može biti potpun kvadrat. Može se lako vidjeti da je prirodan broj $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $n \geqslant 2$, potpun kvadrat ako i samo ako $2 \mid \alpha_i$, $\forall i \in \{1, \ldots, k\}$.

Definicija 7. *Kažemo da je prirodan broj n kvadratno slobodan ako je 1 najveći potpun kvadrat koji ga dijeli, tj. ukoliko iz $m^2 \mid n$, $m \in \mathbb{N}$, slijedi $m = 1$.*

Vidimo iz definicije da je svaki prost broj kvadratno slobodan. Prirodan broj $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $n \geqslant 2$, je kvadratno slobodan ako i samo ako je $\alpha_i = 1$, $\forall i \in \{1, \ldots, k\}$.

Primjer 16.

- $1, 4, 16, 49$ *su potpuni kvadrati.*
- 10 *je kvadratno slobodan, dok* 12 *nije kvadratno slobodan jer* $2^2 \mid 12$.

2.3.3 Broj djelitelja i suma djelitelja prirodnog broja

Neka je n prirodan broj veći ili jednak od 1. Sa $\delta(n)$ označavamo sumu svih pozitivnih djelitelja broja n, dok sa $\tau(n)$ označavamo broj svih pozitivnih djelitelja od n.

Primjer 17.

a) $\tau(1) = 1$
$\delta(1) = 1$

b) Neka je p prost broj. Tada je $\delta(p) = 1 + p$ te $\tau(p) = 2$.
Također primjenom svojstava geometrijskog niza, lako se vidi da je $\delta(p^k) = 1+p+p^2+\ldots+p^k = \frac{1-p^{k-1}}{1-p}$ te $\tau(p^k) = k+1$.

Definicija 8. *Funkcija $f : \mathbb{N} \to \mathbb{C}$ za koju vrijedi*

1) $f(1) = 1$

2) $f(m \cdot n) = f(m) \cdot f(n)$, $(m, n) = 1$

naziva se multiplikativna funkcija.

Teorem 7 (vidi [5, Broj djelitelja i suma djelitelja prirodnog broja 1.4.3]). *τ i δ su multiplikativne funkcije.*

Dokaz:

Vidimo da su funkcije τ i δ aritmetičke funkcije, tj. $\tau : \mathbb{N} \to \mathbb{N} \subseteq \mathbb{C}$ te $\delta : \mathbb{N} \to \mathbb{N} \subseteq \mathbb{C}$.
Pokažimo prvo da funkcija τ zadovoljava svojstva multiplikativne funkcije.
Znamo da je $\tau(1) = 1$. Neka je sada $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ prirodan broj veći od 1. Tada prirodan broj $d = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$ dijeli n ako i samo ako je $0 \leqslant \beta_j \leqslant \alpha_j$ za $j = 1, \ldots, k$.
Kako svaki β_j možemo odabrati na $\alpha_j + 1$ načina, prema principu produkta slijedi da je $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$. Neka su sada a i b dva relativno prosta prirodna broja, $a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $b = q_1^{\beta_1} \cdot \ldots \cdot q_l^{\beta_l}$, takvi da je $p_i \neq q_j$, $\forall i, j \in \{1, 2, \ldots, k\}$.
Tada je $ab = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} q_1^{\beta_1} \cdot \ldots \cdot q_l^{\beta_l}$ te je $\tau(ab) = (\alpha_1+1) \cdot \ldots \cdot (\alpha_k+1)(\beta_1+1) \cdot \ldots \cdot (\beta_l+1) = \tau(a) \cdot \tau(b)$.
Time smo pokazali da je τ multiplikativna funkcija.

Isto pokažimo i za funkciju δ. Znamo da je $\delta(1) = 1$. Neka su a i b dva relativno prosta broja takvi da su $a_1, \ldots, a_k$ svi pozitivni djelitelji od a, tj. $k = \tau(a)$ te $b_1, \ldots, b_l$ svi pozitivni djelitelji od b, tj. $l = \tau(b)$. Iz toga slijedi da je

$$\delta(a) \cdot \delta(b) = (a_1 + \ldots + a_k)(b_1 + \ldots + b_l) = a_1(b_1 + \ldots + b_l) + \ldots + a_k(b_1 + \ldots + b_l).$$

Kako je $(a, b) = 1$, svaki $a_i b_j$ je djelitelj od ab. Pretpostavimo da postoje i, j, m i n takvi da je $a_i b_j = a_m \cdot b_n$. Iz toga vidimo da $a_m \mid a_i$ i $a_i \mid a_m$ pa je $a_m = a_i$. Analognim zaključivanjem dolazimo do toga da je i $b_j = b_n$. Zaključujemo da su svi $a_i b_j$ međusobno različiti djelitelji od ab te je $\delta(a) \cdot \delta(b) = \delta(ab)$.

□

Iz dokaza prethodnog teorema slijedi da je

$$\delta(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) = \delta(p_1^{\alpha_1}) \cdot \ldots \cdot \delta(p_k^{\alpha_k}) = \prod_{j=1}^{k} \frac{1 - p_j^{\alpha_j+1}}{1 - p_j}.$$

Primjer 18. *Neka je* $n = 100$. *Kako je* $100 = 2^2 \cdot 5^2$, *dobivamo* $\tau(100) = (2+1)(2+1) = 9$ *te* $\delta(100) = \delta(2^2 \cdot 5^2) = \frac{1-2^3}{1-2} \cdot \frac{1-5^3}{1-5} = \frac{-7}{-1} \cdot \left(\frac{-124}{-4}\right) = 7 \cdot 31 = 217$.

2.3.4 Fermatovi i Mersennovi brojevi

Pierre de Fermat je bio francuski pravnik te matematičar iz hobija koji se posebno ističe svojim rezultatima u teoriji brojeva. Dokažimo za početak bitnu propoziciju.

Propozicija 5 (vidi [2, Primjer 1.9.]). *Ako je* $2^k + 1$ *prost broj, onda je* $k = 0$ *ili* $k = 2^n$ *za neki* $n \geqslant 0$.

Dokaz:

Ako je $k = 0$ slijedi da je $2^k + 1 = 2$ što je prost broj. Pretpostavimo sada da je $k \neq 0$ i da k ima neparan prosti faktor p. Tada je $k = p \cdot m$, $m \neq 1$. Sada imamo da je $2^{pm} + 1 = (2^m)^p + 1^p = (2^m + 1)\left((2^m)^{p-1} - (2^m)^{p-2} + \ldots + 1\right)$. Kako $2^m + 1$ dijeli cijelu desnu stranu jednakosti, mora dijeliti i lijevu, tj. $(2^m + 1) \mid 2^{pm} + 1 = 2^k + 1$ što ne može biti jer je $2^k + 1$ prost broj. Iz toga slijedi da je k oblika 2^n.

□

Definicija 9. *Fermatovi brojevi su brojevi oblika* $F_n = 2^{2^n} + 1$, $n \geqslant 0$.

Prvih nekoliko Fermatovih brojeva su $3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, \ldots$ Među njima ima i složenih i prostih brojeva, a zanimljivo je da su jedini do sada poznati prosti Fermatovi brojevi F_0, F_1, F_2, F_3 i F_4. Najveći poznat složen broj je upravo Fermatov broj $F_{3329780}$.

Napomena 7. *Fermatovi brojevi zadovoljavaju sljedećih nekoliko rekurzivnih relacija:*

$$F_n = (F_{n-1} - 1)^2 + 1$$
$$F_n = F_{n-1} + 2^{2n-1} F_0 F_1 \cdots F_{n-2}$$
$$F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$$
$$F_n = F_0 F_1 \cdots F_{n-1} + 2.$$

Definicija 10. *Mersennovi brojevi su brojevi oblika* $M_n = 2^n - 1$, $n \in \mathbb{N}$.

Ti brojevi su nazvani prema francuskom redovniku i matematičaru Marinu Mersenneu. Prvih nekoliko Mersennovih brojeva su $1, 3, 7, 15, 31, 63, 127, 255, \ldots$ iz čega vidimo da su neki Mersennovi brojevi prosti, a neki složeni.

Napomena 8. *Ako je* n *prost broj oblika* $4k + 3$, $k \in \mathbb{N}$ *takav da je broj* $q = 2n + 1$ *prost, onda* $q \mid M_n$.

Propozicija 6 (vidi [5, Propozicija 1.4.8.]). *Ako je Mersennov broj M_n prost, onda je i n prost broj.*

Dokaz:

Ako je n složen broj možemo ga zapisati u obliku $n = rs$, za neke prirodne brojeve r i s koji su veći od 1. Tada je $2^{rs} - 1 = (2^s - 1)(2^{s(r-1)} + 2^{s(r-2)} + \ldots + 2^s + 1)$ te je M_n složen broj jer je djeljiv s $2^s - 1$.

□

Deset najvećih poznatih prostih brojeva su Mersennovi prosti brojevi. Najveći od njih je $2^{74207281} - 1$ koji ima 22338618 znamenaka.

Definicija 11. *Za prirodan broj n kažemo da je savršen ako je $\delta(n) = 2n$.*

Neki od savršenih brojeva su $6, 28, 498, 8128, \ldots$

Teorem 8 (vidi [4, Teorem 5.]). *Paran broj n je savršen ako i samo ako se može prikazati u obliku $n = 2^{k-1}(2^k - 1)$ gdje je $2^k - 1$ prost, $k \in \mathbb{N}$.*

Dokaz:

Neka je $n = 2^{k-1}(2^k - 1)$, gdje je $2^k - 1$ prost. Direktno slijedi

$\delta(2^{k-1}) = 1 + 2 + 4 + \ldots + 2^{k-1} = \frac{2^{k-1+1}-1}{2-1} = 2^k - 1$ te $\delta(2^k - 1) = 1 + 2^k - 1 = 2^k$.

Kako su 2^{k-1} i $2^k - 1$ relativno prosti, multiplikativnost funkcije δ povlači

$$\delta(n) = \delta(2^{k-1}) \cdot \delta(2^k - 1) = (2^k - 1)2^k = 2n,$$

pa je broj n savršen.

Obratno, neka je n savršen. Zapišimo ga u obliku $n = 2^k \cdot m$, gdje je $k \geqslant 0$ i m neparan. Kako je $\delta(n) = 2n$ dobivamo

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

Iz prethodnih jednakosti zaključujemo da $2^{k+1} - 1$ dijeli $2^{k+1} \cdot m$. Kako su 2^{k+1} i $2^{k+1} - 1$ relativno prosti, $2^{k+1}-1$ dijeli m. Prema tome, postoji $m' \in \mathbb{Z}$ takav da je $m = (2^{k+1}-1) \cdot m'$. Sada je $\delta(m) = 2^{k+1} \cdot m'$ te $n = (2^{k+1} - 1)2^k \cdot m'$. Preostaje još dokazati da je $m' = 1$ i da je $2^{k+1} - 1$ prost broj.
Ako je $m' \neq 1$, slijedi da je $\delta(m) \geqslant 1 + m' + m$. No,

$$\delta(m) = 2^{k+1} \cdot m' = (2^{k+1} - 1)m' + m' = m + m' < 1 + m + m'.$$

Prema tome, $m' = 1$ te $m = 2^{k+1} - 1$. S druge strane, $\delta(m) = m + m' = m + 1$ pa je m, tj. $2^{k+1} - 1$ prost broj. □

Primjer 19. *Broj 6 je savršen broj.*

Rješenje:
Znamo da su djelitelji broja 6 su $1, 2, 3$ i 6, pa je $\delta(6) = 1+2+3+6 = 12$, što je $2 \cdot 6$. Prema definiciji je 6 savršen broj.

Primjer 20. *Broj 28 je savršen broj.*

Rješenje:
Po prethodnom Teoremu 8. postoji $k \in \mathbb{N}$ takav da je $28 = 2^{k-1}(2^k - 1)$ gdje je $2^k - 1$ prost. Traženi broj k je 3.

Literatura

[1] G. E. Andrews, *Number Theory*, W. B. Saunders company, Philadelphia, 1971.

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

[3] S. S. Epp, *Discrete mathematics with applications*, Elm Street Publishing Services, Boston, 2011.

[4] W. Sierpinski, *Elementary Theory of numbers*, North-Holand, Amsterdam, 1988.

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

[6] R. L. Graham, D. E. Knuth, O. Patashink, *Concrete mathematics: A Foundation for computer science*, 2nd Edition, Addison Wesley publishing company, Boston, 1994.