Zanimljivi brojevi

Štivić, Ira

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

Ira Štivić

Zanimljivi brojevi

Završni rad

Osijek, 2019.

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

Ira Štivić

Zanimljivi brojevi

Završni rad

Mentor: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2019.

Sažetak

U ovom radu proučit ćemo nekoliko klasa zanimljivih brojeva koji imaju važnu ulogu u teoriji brojeva. Poglavlja ovog rada bazirat ćemo na opisu, svojstvima i primjeni pojedinih klasa brojeva. U radu ćemo obraditi sljedeće klase brojeva: figurativni brojevi, Eulerovi brojevi, Fibonaccijev niz brojeva, Mersenneovi brojevi, savršeni brojevi, Fermatovi brojevi, pseudoprosti brojevi i Carmichaelovi brojevi. Na kraju rada ćemo navesti nekoliko definicija i primjera još nekih zanimljivih klasa brojeva koje u ovom radu nećemo detaljnije obrađivati.

Ključne riječi

Prost broj, mnogokut, Fibonaccijev niz, Lucasov broj, Eulerov broj, Fermatov broj, mali Fermatov teorem, Mersenneov broj, pseudoprost broj, Carmichaelov broj.

Interesting numbers

Abstract

In this paper we will consider a few different classes of interesting numbers which have an important role in number theory. The chapters of this paper will be based on the description, properties and use of each of these classes of numbers. In the paper we will process the next classes of numbers: figurative numbers, Euler's number, Fibonacci number sequence, Mersenne's number, perfect number, Fermat's number, pseudoprime number and Carmichael's number. At the end of this paper we will list a few definitions and examples of other interesting clasess of numbers which we will not process in detail.

Key words

Prime number, polygon, Fibonacci sequence, Lucas number, Euler's number, Fermat's number, Fermat's little theorem, Mersenne number, pseudoprime number and Carmichael number.

Sadržaj

Uvod

Teorija brojeva je grana matematike koja se bavi proučavanjem prirodnih, cijelih i racionalnih brojeva. Stariji naziv za teoriju brojeva je aritmetika. Problemima ovog područja bavili su se još u starom Babilonu i Egiptu, a posebice u staroj Grčkoj. Tijekom povijesti pojavljuju se razne klase brojeva koje se ističu po svojim svojstvima, značaju ili primjenama te zbog toga dobivaju istaknuta imena. Ponekad su to konstruktivna imena, a ponekad imena dobivena prema znanstvenicima koji su proučavali problematiku te klase brojeva.

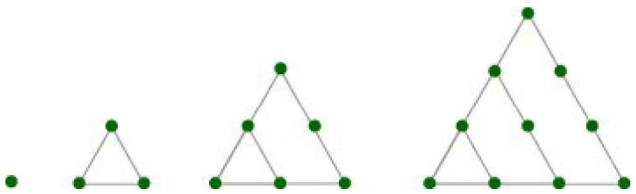
U ovom radu pručit ćemo nekoliko klasa zanimljivih brojeva, detaljnije opisati njihova svojstva te primjenu, što ćemo pokazati i na nekoliko primjera. Na kraju ćemo navesti još nekoliko definicija i primjera drugih zanimljivih klasa brojeva koje nećemo detaljnije obrađivati.

1 Figurativni brojevi

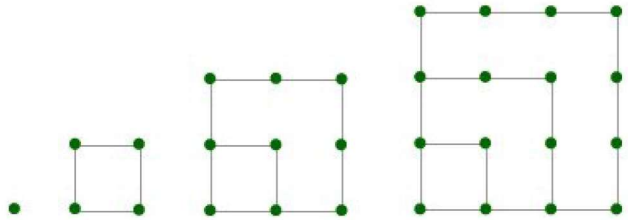
Figurativni brojevi prvi put su se pojavili u Pitagorinoj školi u 6. stoljeću prije Krista u pokušaju povezivanja geometrije i aritmetike. Pitagorejci su, vjerujući da je "sve broj", smatrali svaki pozitivni cijeli broj skupom točaka u ravnini. Teorija figurativnih brojeva, iako ne pripada središnjoj domeni matematike, pridobila je pažnju mnogih znanstvenika tijekom više tisuća godina. Među matematičarima koji su proučavali figurativne brojeve nalaze se Pitagora, Diofant, Fibonacci, Pell, Fermat, Euler i brojni drugi.

Figurativni broj je u suštini onaj broj koji se može prikazati pomoću geometrijskog uzorka različitih točaka u ravnini. Najpoznatija vrsta figurativnih brojeva su ravninski figurativni brojevi koji se reprezentiraju kao mnogokuti.

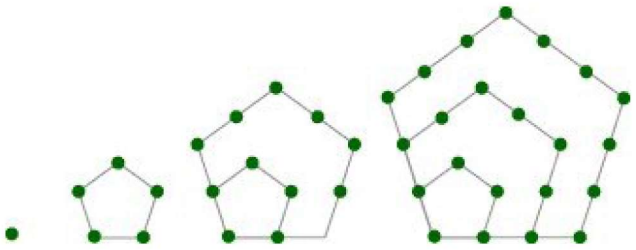
Mnogokutni brojevi obuhvaćaju brojeve koji se mogu urediti tako da tvore trokut, kvadrat i bilo koji drugi m-terokut za cijeli broj $m \geq 3$. Niz mnogokutnih brojeva sastoji se od trokutnih brojeva $1, 3, 6, 10, 15, \ldots$ (Slika 1), kvadratnih brojeva $1, 4, 9, 16, 25, \ldots$ (Slika 2), peterokutnih brojeva $1, 5, 12, 22, 35, \ldots$ (Slika 3), itd.



Slika 1: Trokutni figurativni brojevi [8]



Slika 2: Kvadratni figurativni brojevi [8]



Slika 3: Peterokutni figurativni brojevi [8]

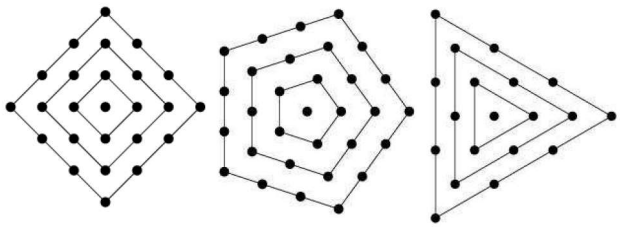
Ako je m broj strana u mnogokutu, onda se može pokazati ([2]) da je formula za n-ti i m-gonalni broj dana s

$$S_m(n) = \frac{1}{2}m(n^2 - n) - n^2 + 2n.$$

Također, može se pokazati da vrijede sljedeće relacije:

- Theonova formula:
$$S_3(n) + S_3(n-1) = S_4(n),$$
- Diofantova formula:
$$S_4(2n+1) = 8S_3(n) + 1,$$
- Teorem o heksagonalnim brojevima:
$$S_6(n) = S_3(2n-1),$$
- Teorem o oktagonalnim brojevima:
$$S_8(n) = 6S_3(n-1) + n,$$
- Nicomachusova formula:
$$S_m(n) = S_{m-1}(n) + S_3(n-1),$$
- te Bachet de Meziriacova formula:
$$S_m(n) = S_3(n) + (m-3)S_3(n-1).$$

Osim klasičnih mnogokutnih brojeva, proučavani su i pravilni mnogokutni brojevi koji mogu biti konstruirani u ravnini iz točaka. Svaki takav broj formira se iz središnje točke koju okružuju mnogokutni slojevi s konstantnim brojem strana. Svaka strana jednog sloja sadrži jednu točku više od bilo koje druge strane prethodnog sloja. Tako postoje, jednako kao i klasični, pravilni trokutni brojevi $1, 4, 10, 19, 31, \ldots$, pravilni kvadratni brojevi $1, 5, 13, 25, 41, \ldots$, pravilni peterokutni brojevi $1, 6, 16, 31, 51, \ldots$ itd. [2]. Konstrukcija ovakvih brojeva prikazana je na Slici 4.



Slika 4: Konstrukcija pravilnog kvadratnog, peterokutnog i trokutnog broja

Pravilni trokutni brojevi su brojevi oblika
$$T_3(n) = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2},$$
pravilni kvadratni brojevi su brojevi oblika
$$T_4(n) = 1 + 3 + 5 + \cdots + (2n-1) = n^2,$$
pravilni peterokutni brojevi su brojevi oblika
$$T_5(n) = 1 + 4 + 7 + \cdots + (3n-2) = 3T_3(n) - 2n = \frac{n(3n-1)}{2}.$$
Formule za ostale pravilne figurativne brojeve izvode se analogno.

2 Eulerovi brojevi

Znamo li koliko je "cik-cak uređaja", u oznaci $\mathbb{Z}_n$, brojeva $1, 2, \ldots, n$, tj. uređaja u kojima brojevi naizmjenično rastu, a zatim padaju?

Sljedeća tablica pokazuje prvih nekoliko takvih uređaja:

n	$\mathbb{Z}_n$	Uređaj
1	1	1
2	1	12
3	2	231;132
4	5	3412;1423,2413;1324,2314

Točke zarezi u ovakvom uređaju razdvajaju brojeve u redoslijedu prema njihovoj zadnjoj znamenci, tzv. r-toj znamenci. Brojevi oblika $\mathbb{Z}_{2n}$ nazivaju se Eulerovim brojevima [1]. Poznati su još i kao *sekantni brojevi* iz aspekta formule za sekans:

$$\sec x = 1 + \frac{1x^2}{2!} + \frac{5x^4}{4!} + \frac{61x^6}{6!} + \cdots \tag{1}$$

Desna granica cik-cak trokuta predstavlja tzv. *tangens brojeve*, $\mathbb{Z}_{2n+1}$, jer je:

$$\operatorname{tg} x = \frac{x}{1!} + \frac{2x^3}{3!} + \frac{16x^5}{5!} + \frac{272x^7}{7!} + \cdots \tag{2}$$

Ukupan broj uređaja brojeva $1, 2, \ldots, n$ u kojemu je $k-1$ porasta, također je dobio ime po Euleru i naziva se *Eulerski broj* u oznaci $A(n, k)$.

$$A(n,k) = \sum_{j=0}^{k} (-1)^j \binom{n+1}{j} (k-j)^n. \tag{3}$$

3 Fibonaccijevi brojevi

Fibonaccijevi brojevi ime su dobili po talijanskom matematičaru Leonardu iz Pise (1175.-1250.) poznatijem kao Fibonacci (skraćeno od *tal. fillius Bonacci*-"Bonaccijev sin"). Fibonaccija se smatralo najdarovitijim zapadnjačkim matematičarem srednjeg vijeka. Niz brojeva koji je otkrio postao je jedan od najzanimljivijih matematičkih nizova čije je postojanje otkriveno u prirodi, a zatim se nastavio koristiti i u drugim područjima matematike gdje je svoju primjenu našao u pojašnjenjima prirodnih pojava. Fibonacci je promatrao par zečeva i pitao se koliko će parova zečeva biti u n-toj generaciji potomstva prvotnog para zečeva. Za pretpostavku je uzeo da će svaki par zečeva iz svake generacije dobiti potomstvo svakog prvog dana u mjesecu, ali tek nakon navršena dva mjeseca. Također, pretpostavio je da parovi zečeva nakon reprodukcije ne umiru. Ono što je iz ove pretpostavke zaključio, opisao je sljedećom formulom. Ako postoji f_n parova zečeva u n-toj generaciji, onda vrijedi:

$$\begin{aligned} f_1 &= 1, \\ f_2 &= 1, \\ f_{n+2} &= f_n + f_{n+1}. \end{aligned}$$

Tako je nastao niz brojeva koji danas nazivamo *Fibonaccijev niz* [1]:

$$f_0 = 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

Iz niza vidimo da je svaki sljedeći broj u nizu jednak zbroju dvaju prethodnih brojeva. Može se pokazati da je Fibonaccijev niz brojeva dan sljedećom eksplicitnom formulom:

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \tag{4}$$

Primjer 1. *[4] Stubište se sastoji od n stuba. U jednom koraku možemo preskočiti jednu ili dvije stube. Na koliko načina možemo prijeći cijelo stubište ?*

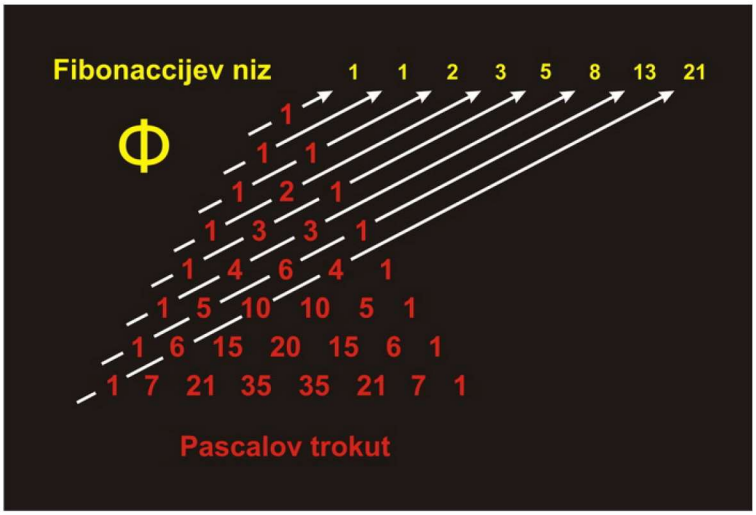
Rješenje:
Stubište od jedne stube možemo prijeći na samo jedan način, ono od dvije na dva načina. Tri stube možemo prijeći koracima 1,1,1 ili 1,2 ili 2,1, dakle, na tri načina.
Međutim, četiri stube možemo prijeći na pet načina. Za mali n lako možemo ispisati sve odgovarajuće nizove:

n	nizovi	broj
1	1	1
2	11,2	2
3	111,12,21	3
4	1111,112,121,211,22	5
5	11111,1112,1121,1211,2111,122,212,221	8
	...	

Fibonaccijev niz brojeva ima široku primjenu u matematici. Francuski matematičar Edouard Lucas (1842.-1891.) otkrio je da se Fibonaccijev niz može iščitati pomoću Pascalovog trokuta koristeći sljedeću relaciju:

$$f_{n+1} = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots$$

Primjer 2. *Zbrojimo li elemente Pascalovog trokuta duž rastućih dijagonala, suma će biti Fibonaccijev broj. Nekoliko prvih vrijednosti naznačeno je na sljedećoj slici gdje su Fibonaccijevi brojevi napisani na gornjoj desnoj strani trokuta.*



Slika 5: Veza između Fibonaccijevog niza i Pascalovog trokuta
[1]

Izaberemo li u relaciji za Fibonaccijev niz par brojeva koji nisu uzastopni članovi Fibonaccijeva niza, dobit ćemo niz različit od Fibonaccijevog. Iako imaju potpuno različite vrijednosti, ti nizovi će imati neka identična svojstva [1]. Uz Fibonaccijeve, sljedeći dobar odabir parova brojeva je onaj koji daje Lucasove brojeve.

Lucasovi brojevi (l_n) definirani su rekurzivnom relacijom

$$l_n = l_{n-1} + l_{n-2}$$

uz početne vrijednosti

$$l_0 = 2, l_1 = 1.$$

Prvih nekoliko Lucasovih brojeva su:

$$2,1,3,4,7,11,18,29,47,\ldots$$

Nešto kasnije, njemački matematičar Johannes Kepler (1571.-1630.) otkrio je da je omjer uzastopnih Fibonaccijevih brojeva približno jednak 1.618. Točnije, limes omjera jednak je 1.61803398874989..., što se još od antičke Grčke naziva *zlatnim rezom*:

$$\varphi = \frac{1+\sqrt{5}}{2}$$

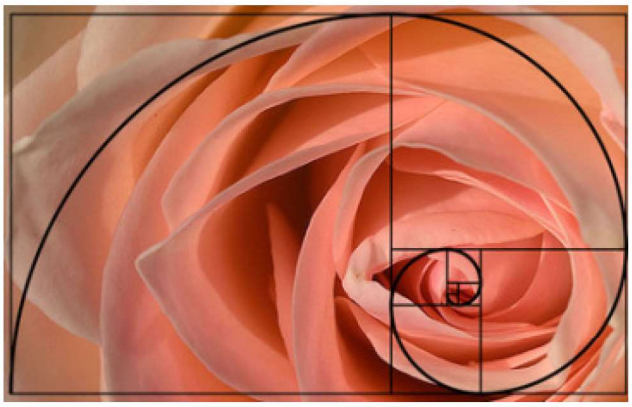
[1] `http://fotoklub-cakovec.hr/wp/2012/02/geometricnost-fotografije-ii`

Pravilo zlatnog reza:

Omjer manjeg dijela prema većem jednak je omjeru većeg dijela prema cjelini.

Omjer uzastopnih Lucasovih brojeva ima isti limes kao i omjer Fibonaccijevih brojeva, dok omjer Lucasovih i Fibonaccijevih brojeva, $\frac{l_n}{f_n}$, teži ka $\sqrt{5}$.

Iako se pokazalo da Fibonaccijevo pravilo nije primjenjivo na parovima zečeva u stvarnom životu, Fibonaccijev niz brojeva prisutan je u mnogim drugim prirodnim elementima, npr. može se pokazati da je raspored žila na listovima biljaka ili raspored latica cvijeća kao npr. ruža (Slika 6) određen upravo ovim nizom brojeva [1].



Slika 6: Prikaz rasporeda latica ruže pomoću pravila zlatnog reza
[2]

[2] https://fibonacijevniz.wordpress.com/2016/06/03/fibonacijev-niz-u-prirodi/

4 Mersenneovi brojevi

Francuski teolog, filozof i matematičar Marin Mersenne (1588.-1648.) bio je jedan od prvih matematičara koji je svoja otkrića zabilježio u dnevnike i pisma. 1536. godine, u pismu Frenicleu de Bessyju, Mersenne navodi mogućnost postojanja prostih brojeva oblika $M_n = 2^n - 1$, gdje je n prirodan broj. Mersenne je tvrdio da su za n=2,3,5,7,13,17,19,31,67,127,257 brojevi $2^n - 1$ zaista prosti, te da ova tvrdnja ne vrijedi ni za jedan drugi broj manji od 257.

Ova tvrdnja je pobudila veliko zanimanje kod drugih matematičara upravo zbog toga što su navedeni brojevi toliko veliki. Dugi niz godina niti jedan matematičar nije mogao potvrditi ni opovrgnuti Mersenneovu tvrdnju. Tek 1722. godine je Euler uspio dokazati da je broj M_{31} prost, a 1876. godine E. Lucas je došao do zaključka da je i M_{127} usitinu prost broj.

Prvih nekoliko Mersenneovih brojeva su 1,3,7,15,31,63,127,255 iz čega je vidljivo da su neki Mersenneovi brojevi prosti, a neki složeni. Do tog zaključka je došao američki matematičar Cole 1903. godine pokazavši da je

$$2^{67} - 1 = 193707721 \cdot 761838257287$$

složen broj, odakle slijedi da M_{67} nije prost broj [1].

Propozicija 1. *[5] Ako je Mersenneov broj M_n prost, tada je i n prost broj.*

Dokaz. Ako je broj n složen, možemo ga zapisati u obliku $n = rs$, za neke prirodne brojeve r,s koji su oba veći od 1. Tada je

$$2^{rs} - 1 = (2^s - 1)(2^{s(r-1)} + 2^{s(r-2)} + \cdots + 2^s + 1)$$

te je M_n složen broj jer je djeljiv s $2^s - 1$. □

Danas postoje mnoge tehnike i testovi koji donekle olakšavaju provjeru je li broj oblika $2^n - 1$ zaista prost. Jedan od najpouzdanijih kriterija za ispitivanje prostosti Mersenneovih brojeva je tzv. *Lucas-Lehmerov test*:

Teorem 1. *[5] Definirajmo niz prirodnih brojeva (s_n) sa s_1=4, $s_{n+1} = s_n^2 - 2$. Neka je p neparan prost broj. Mersenneov broj M_p je prost ako i samo ako M_p dijeli s_{p-1}.*

5 Savršeni brojevi

Za prirodan broj n kažemo da je savršen ako je jednak sumi svojih djelitelja manjih od njega samog. U matematici to zapisujemo na sljedeći način: $\sigma(n) = 2n$. Naziv savršeni brojevi potječe još iz antičke Grčke, točnije od Pitagorejaca. Drugi znanstvenici i filozofi su, slično kao Pitagorejci, objašnjavali značenje savršenih brojeva pomoću religije. Sveti Augustin smatrao je da je Bog stvorio svijet u šest dana, a u ranom Starom zavjetu spominje se i savršenstvo svemira koje je simbolizirano brojem 28 jer je toliko dana potrebno Mjesecu da obiđe Zemlju. Sljedeći raspisi pokazuju da su 6 i 28 savršeni brojevi:

$$6 = 1 + 2 + 3$$
$$28 = 1 + 2 + 4 + 7 + 14.$$

Gotovo dvije tisuće godine prije M. Mersennea, Euklid (330.pr.Kr.-275.pr.Kr.) je otkrio zanimljivu poveznicu između savršenih brojeva i onoga što danas nazivamo Mersenneovim brojevima. Pokazao je da činjenica da je broj $2^n - 1$ prost povlači da je broj $2^{n-1}(2^n - 1)$ savršen.

Na osnovi poznavanja samo četiri savršena broja nastala je slutnja da n-ti savršeni broj ima točno n znamenki, te da parni savršeni brojevi završavaju naizmjence na znamenke 6 i 8.

Obje pretpostavke, Eulerova i ona starih Grka, pokazale su se netočnima nakon što je Pietro Cataldi (1548.-1626.) dokazao da su peti, šesti i sedmi savršeni brojevi jednaki 33550336, 8589869056 i 137438691328. Oko dvije tisuće godina nakon Euklida, Euler je dopunio njegovu tvrdnju koju ćemo iskazati i dokazati u sljedećem teoremu.

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

Dokaz. Neka je

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

gdje je $2^k - 1$ prost. Direktno slijedi

$$\sigma(2^{k-1}) = 1 + 2 + 4 + \cdots + 2^{k-1} = \frac{2^{k-1+1}}{2 - 1} = 2^k - 1$$

te

$$\sigma(2^k - 1) = 1 + 2^k - 1 = 2^k.$$

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

$$\sigma(n) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)2^k = 2n$$

pa je broj n savršen.

Obratno, neka je n savršen; zapišimo ga u obliku $n = 2^k m$, gdje je $k \geq 0$ i m neparan. Kako je $\sigma(n) = 2n$, dobivamo

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

Iz prethodnih jednakosti zaključujemo da $2^{k+1}-1$ dijeli $2^{k+1}m$. Kako su 2^{k+1} i $2^{k+1}-1$ relativno prosti, $2^{k+1}-1$ dijeli m. Zapišimo sada m u obliku $m=(2^{k+1}-1)m'$. Dobivamo da je

$$\sigma(m)=2^{k+1}m',$$

te

$$n=(2^{k+1}-1)2^km'.$$

Preostaje još dokazati da je m'=1 i da je $2^{k+1}-1$ prost broj.
Ako je $m'\neq 1$, slijedi

$$\sigma(m)\geq 1+m+m'.$$

No, vidjeli smo da je

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

Prema tome, m'=1 te m=$2^{k+1}-1$. S druge strane,

$$\sigma(m)=m+m'=m+1$$

pa je m, tj. $2^{k+1}-1$ prost broj. □

O neparnim savršenim brojevima ne znamo mnogo, osim da moraju imati najmanje 1500 znamenki [6] i velik broj faktora pa se nameće pretpostavka da neparni savršeni brojevi ne postoje.

6 Fermatovi brojevi

Pierre de Fermat (1607.-1665.) bio je francuski pravnik kojemu je matematika bila hobi. Kasnije će postati veoma značajan znanstvenik upravo u tom području. Uglavnom se bavio analitičkom geometrijom i teorijom vjerojatnosti, ali najviše se istaknuo svojim doprinosom teoriji brojeva.

1640. godine dolazi do spoznaje da su brojevi oblika $F_n = 2^{2^n} + 1$, gdje je n prirodan broj, prosti brojevi. Ovi brojevi danas se nazivaju Fermatovi brojevi.

Prvih nekoliko Fermatovih brojeva su:

$$F_0 = 2^{2^0} + 1 = 3$$
$$F_1 = 2^{2^1} + 1 = 5$$
$$F_2 = 2^{2^2} + 1 = 17$$
$$F_3 = 2^{2^3} + 1 = 257$$
$$F_4 = 2^{2^4} + 1 = 65537$$

i svi ovi brojevi su prosti.

Međutim, 1732. godine Euler je otkrio da je sljedeći Fermatov broj, F_5 složen:

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

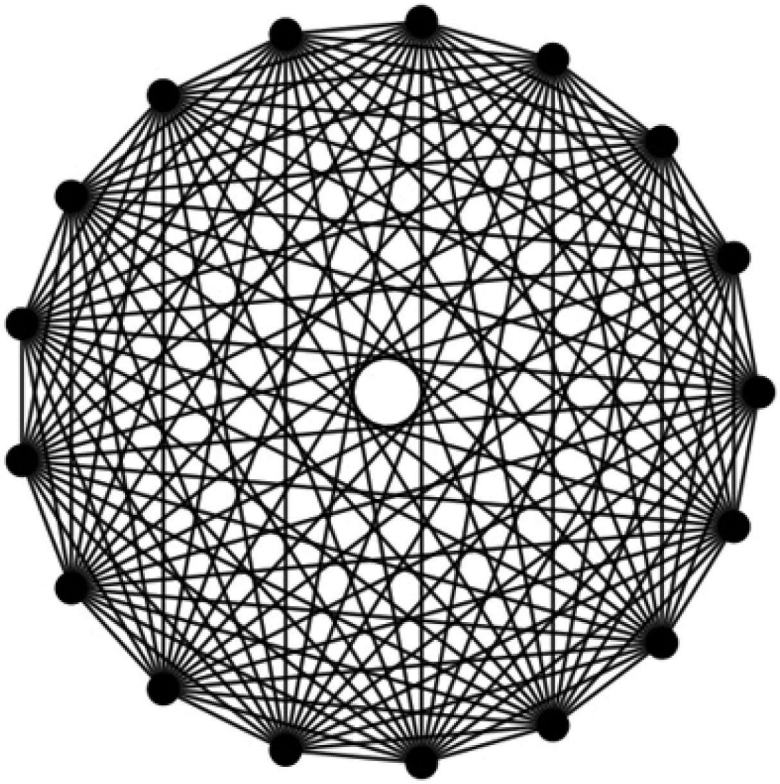
Također, 1880. godine F. Landry je pokazao da je $2^{2^6} + 1$ složen broj, 1975. godine Brillhart i Morrison isto su pokazali za broj $2^{2^7} + 1$, a 1981. R. Brent i J. Pollard faktorizirali su broj $2^{2^8} + 1$. Poznato je i da su brojevi $2^{2^9} + 1$, $2^{2^{10}} + 1$,...,$2^{2^{32}} + 1$ složeni [10].

Matematičar koji je najviše pozornosti pridao Fermatovim brojevima, i postigao najveće rezultate, bio je Carl Friedrich Gauss (1777.-1855.). Gauss je još kao mladić uspio dokazati da ukoliko je p Fermatov prost broj, onda se ravnalom i šestarom može konstruirati pravilan mnogokut s p strana. Euklid je konstruirao trokut i peterokut, ali prije Gaussa nitko nije uspio konstruirati veći mnogokut s prostim brojem strana.

Dokazano je da je lako konstruirati pravilan 85-terokut koristeći konstrukcije za peterokut i 17-terokut (Slika 7), a obzirom da se kutovi u mnogokutu mogu prepoloviti, također je moguće konstruirati pravilni 170-terokut, 340-terokut itd. Općenito, mogu se konstruirati mnogokuti oblika

$$2^k pqr \cdots,$$

gdje su p,q,r,... različiti Fermatovi prosti brojevi. Gauss je tvrdio da su ovo jedini mnogokuti koji se mogu konstruirati ravnalom i šestarom. Jedini takvi poznati mnogokuti s neparnim brojem strana su oni čiji je broj strana djelitelj broja $2^{2^5} - 1$. Takvih brojeva ima 32, a najveći djelitelj je upravo sam $2^{2^5} - 1 = 4294967295$.



Slika 7: Konstruirani pravilni 17-terokut

Primjer 3. *Pokažimo da je* $2^{2^5}+1$ *složen broj koristeći kongruencije modulo p=641.*

Rješenje: Vrijedi

$$\begin{aligned} p &= 625+16 \equiv 5^4+2^4 \\ p-1 &= 5\cdot 128 = 5\cdot 2^7 \\ 5\cdot 128 &\equiv -1 \pmod{p} \\ 2^4 &\equiv -5^4 \pmod{p}. \end{aligned}$$

Iz toga slijedi:

$$2^{2^5} = 2^{32} = 2^4\cdot 2^{28} \equiv -5^4\cdot 128^4 \equiv -(-1)^4 \equiv -1 \pmod{p}.$$

Fermatovi brojevi zadovljavaju nekoliko rekurzivnih relacija koje se mogu dokazati induktivno:

$$\begin{aligned} F_n &= (F_{n-1}-1)^2+1 \\ F_n &= F_{n-1}+2^{2n-1}F_0F_1\ldots F_{n-2} \\ F_n &= F_{n-1}^2-2(F_{n-2}-1)^2 \\ F_n &= F_0F_1\ldots F_{n-1}+2 \end{aligned}$$

Posljednju od navedenih relacija iskoristiti ćemo u dokazu iduće propozicije:

Propozicija 2. *[5] Neka su i,j nenegativni cijeli brojevi. Ako je i≠j, tada je* $(F_i,F_j)=1$.

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti $i>j$. Prema navedenoj relaciji, vrijedi $F_i = F_0 \cdots F_j \cdots F_{i-1} + 2$. Kako $(F_i, F_j)|F_i$ i $(F_i, F_j)|F_0 \cdots F_j \cdots F_{i-1}$, slijedi da $(F_i, F_j)|2$. No, svi Fermatovi brojevi su neparni, odakle dobivamo $(F_i,F_j)=1$. □

7 Pseudoprosti brojevi i Carmichaelovi brojevi

Koristeći Mali Fermatov teorem, moguće je pokazati da je neki cijeli broj složen. Prisjetimo se Malog Fermatovog teorema:

Teorem 3. *[5] Neka je p prost broj i a cijeli broj. Tada je $a^p \equiv a \pmod{p}$ te ako $p \nmid a$ vrijedi i $a^{p-1} \equiv 1 \pmod{p}$.*

Na primjeru ćemo pokazati kako ovaj test radi.

Primjer 4. *Ispitajte je li broj 91 prost koristeći Mali Fermatov teorem.*

Rješenje:
Ispitajmo je li $2^{90} \equiv 1 \pmod{91}$?
Kako je

$$2^6 = 64 \equiv -27 \pmod{91}$$
$$2^{12} = (-27)^2 = 729 \equiv 1 \pmod{91}$$

dobivamo

$$2^{84} = (2^{12})^7 \equiv 1^7 \equiv 1 \pmod{91}$$

pa je

$$2^{90} = 2^{84} \cdot 2^6 \equiv 1 \cdot (-27) \pmod{91}$$

Iz prethodnih kongruencija slijedi da 91 nije prost broj!

Prethodni primjer pokazuje da Fermatov test zadovoljava nužne uvjete provjere prostosti brojeva, ali ne i dovoljne uvjete. Test koji zadovoljava i dovoljne uvjete provjere prostosti brojeva uveo je Sir J. Wilson (1741.-1793.).

Teorem 4. *[5] Ako je p prost broj, tada je $(p-1)! \equiv -1 \pmod{p}$.*

Također vrijedi i obrat Wilsonova teorema:

Propozicija 3. *[5] Ako prirodan broj n zadovoljava kongruenciju $(n-1)! \equiv -1 \pmod{n}$, tada je n prost.*

Kako je Wilsonov test neefikasan, u svrhu testiranja prostosti brojeva češće se koristi Mali Fermatov teorem.

Ono što je u Fermatovom testu nedostajalo je metoda provjeravanja je li broj prost. U staroj Kini se vjerovalo da ako je $2^n \equiv 2 \pmod{n}$, onda n mora biti prost broj. Postavlja se pitanje kako možemo pokazati da su brojevi složeni ako ne možemo pronaći njihovu faktorizaciju? U tu svrhu promatrat ćemo složene brojeve koji zadovoljavaju relaciju iz Malog Fermatovog teorema, što dovodi do sljedeće definicije:

Definicija 1. *[7] Neka je b pozitivan cijeli broj. Ako je n složen pozitivan cijeli broj i vrijedi $b^n \equiv b \pmod{n}$, onda se n naziva pseudoprostim brojem u bazi b.*

Uočimo, ukoliko vrijedi $(b, n) = 1$, onda je kongruencija $b^n \equiv b \pmod{n}$ ekvivalentna kongruenciji $b^{n-1} \equiv 1 \pmod{n}$.

Primjer 5. *Cijeli brojevi 341=11·31, 561=3·11·17 i 645=3·5·43 su svi pseudoprosti brojevi u bazi 2 jer se lako provjeri da vrijedi* $2^{340} \equiv 1 \pmod{341}$, $2^{560} \equiv 1 \pmod{561}$ *i* $2^{644} \equiv 1 \pmod{645}$.

Provjera je li zadovoljena kongruencija $b^n \equiv b \pmod{n}$ je učinkovita ukoliko postoji relativno mali broj pseudoprostih brojeva u bazi b, međutim, vrlo mali broj složenih brojeva zadovoljava ovu kongruenciju. Pokazalo se da je broj pseudoprostih brojeva u bazi b znatno manji od broja poznatih prostih brojeva. Preciznije, postoji beskonačno mnogo prostih brojeva, dok je poznato samo 14884 pseudoprostih brojeva u bazi 2. Iako su pseudoprosti brojevi u bilo kojoj danoj bazi rijetki, neosporivo je da postoji beskonačno mnogo takvih pseudoprostih brojeva. Pokazati ćemo ovu tvrdnju za bazu 2.

Lema 1. *[7] Ako su d i n pozitivni cijeli brojevi takvi da d dijeli n, onda $2^d - 1$ dijeli $2^n - 1$.*

Dokaz. Budući da $d|n$, postoji pozitivan cijeli broj t takav da $dt{=}n$. Ukoliko u izrazu

$$x^t - 1 = (x - 1)(x^{t-1} + x^{t-2} + \cdots + 1)$$

postavimo $x = 2^d$, dobit ćemo da vrijedi

$$2^n - 1 = (2^d - 1)(2^{d(t-1)} + 2^{d(t-2)} + \cdots + 2^d + 1)$$

iz čega slijedi $(2^d - 1)|(2^n - 1)$. □

Sada uz pomoć prethodne leme možemo dokazati sljedeći teorem.

Teorem 5. *[7] Postoji beskonačno mnogo pseudoprostih brojeva u bazi 2.*

Dokaz. Pokazat ćemo da ako je n neparan pseudoprost broj u bazi 2, onda je $m = 2^n - 1$ također pseudoprost broj u bazi 2. Obzirom da znamo da postoji barem jedan neparan pseudoprost broj, označimo ga s $n_0{=}341$, možemo konstruirati beskonačno mnogo pseudoprostih brojeva u bazi 2 uzimajući n_0 i $n_{k+1} = 2^{n_k} - 1$ za $k{=}0,1,2,\ldots$. Svi ovi neparni cijeli brojevi su različiti obzirom da je $n_0 < n_1 < \cdots < n_k < n_{k+1} < \cdots$.

Neka je n neparan, složen pseudoprost broj takav da vrijedi $2^{n-1} \equiv 1 \pmod{n}$. Kako je n složen, znamo da je $n = dt$ i da vrijedi $1 < d < n$ i $1 < t < n$. Pokazat ćemo da je broj $m = 2^n - 1$ također pseudoprost broj tako što ćemo prvo dokazati da je složen, a zatim da vrijedi $2^{m-1} \equiv 1 \pmod{m}$.

Kako bismo pokazali da je m složen broj, koristimo prethodnu lemu iz koje je jasno uočljivo da je $(2^d - 1)|(2^n - 1) = m$. Zatim, da bismo pokazali kako vrijedi $2^{m-1} \equiv 1 \pmod{m}$, prvo moramo uočiti da, s obzirom da vrijedi $2^n \equiv 2 \pmod{n}$, postoji cijeli broj k takav da je $2^n - 2 = kn$. Dakle, $2^{m-1} = 2^{2^n-2} = 2^{kn}$. Prema prethodnoj lemi znamo da vrijedi $m = (2^n - 1)|(2^{kn} - 1) = 2^{m-1} - 1$. Iz toga slijedi da je $2^{m-1} - 1 \equiv 0 \pmod{m}$ i $2^{m-1} \equiv 1 \pmod{m}$ pa možemo zaključiti da je m pseudoprost broj u bazi 2. □

Ukoliko želimo provjeriti je li cijeli broj n prost, a znamo da je $2^{n-1} \equiv 1 \pmod{n}$, možemo zaključiti da je n ili prost broj ili pseudoprost broj u bazi 2. Nešto drukčiji pristup je provjeravanje broja n u drugim bazama, tj. provjeravamo vrijedi li $b^{n-1} \equiv 1 \pmod{n}$ za različite pozitivne cijele brojeve b. Ako pronađemo bilo koji b takav da je $(b, n) = 1$ i $b^{n-1} \not\equiv 1 \pmod{n}$, onda slijedi da je n složen.

Primjer 6. *Obzirom da vrijedi*

$$7^3 = 343 \equiv 2 \pmod{341}$$

i

$$2^{10} = 1024 \equiv 1 \pmod{341},$$

slijedi da je

$$\begin{aligned} 7^{340} = (7^3)^{113}7 \equiv 2^{113}7 = (2^{10})^{11} \cdot 2^3 \cdot 7 \\ \equiv 8 \cdot 7 \equiv 56 \not\equiv 1 \pmod{341}. \end{aligned}$$

Dakle, obzirom da $7^{340} \not\equiv 1 \pmod{341}$*, možemo zaključiti kako je 341 složen broj.*

Postoje složeni cijeli brojevi takvi da je $b^{n-1} \equiv 1 \pmod{n}$ za sve b takve da je $(b,n)=1$, za koje se ne može pokazati da su složeni koristeći metodu iskorištenu u prethodnom primjeru.

Definicija 2. *[7] Složen cijeli broj takav da je* $b^{n-1} \equiv 1 \pmod{n}$ *za sve pozitivne cijele brojeve b za koje vrijedi (b,n)=1, naziva se Carmichaelov broj.*

Primjer 7. *561=3·11·17 je Carmichaelov broj.*

Rješenje: Primijetimo, ako je $(b,561)=1$, onda je $(b,3)=(b,11)=(b,17)=1$. Dakle, iz Malog Fermatovog teorema slijedi:

$$\begin{aligned} b^2 &\equiv 1 \pmod{3}, \\ b^{10} &\equiv 1 \pmod{11}, \\ b^{16} &\equiv 1 \pmod{17}. \end{aligned}$$

Posljedično gledajući, slijedi da je $b^{560} = (b^2)^{280} \equiv 1 \pmod{3}$, $b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$ i $b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$. Dakle, slijedi da je $b^{560} \equiv 1 \pmod{561}$ za sve b takve da je $(b,n)=1$.

Pretpostavlja se da postoji beskonačno mnogo Carmichaelovih brojeva, ali to još nije dokazano. U sljedećem teoremu dokazati ćemo uvjete koje zadovoljavaju Carmichaelovi brojevi.

Teorem 6. *Ako je* $n = q_1 q_2 \cdots q_k$*, gdje su* q_j *različiti prosti brojevi za koje vrijedi* $(q_j - 1)/(n-1)$ *za sve j, onda je n Carmichaelov broj.*

Dokaz. Neka je b pozitivan cijeli broj takav da je $(b,n)=1$. Tada vrijedi $(b,q_j)=1$ za $j=1,2,\ldots,k$ pa iz Malog Fermatovog teorema slijedi da je $b^{q_j-1} \equiv 1 \pmod{q)_j}$ za $j=1,2,\ldots,k$. Budući da za sve cijele brojeve $j=1,2,\ldots,k$ vrijedi $(q_j-1)|(n-1)$, postoje cijeli brojevi t_j takvi da je $t_j(q_j-1)=n-1$. Dakle, za svaki j vrijedi $b^{n-1} = b^{(q_j-1)t_j} \equiv 1 \pmod{q)_j}$. Sada možemo zaključiti da je $b^{n-1} \equiv 1 \pmod{n}$ pa je n Carmichaelov broj. □

Također vrijedi i obrat ovog teorema:

Teorem 7. *Svi Carmichaelovi brojevi su oblika $q_1q_2\cdots q_k$, gdje su q_j različiti prosti brojevi i vrijedi $(q_j-1)/(n-1), \forall j$.*

Druga zanimljiva svojstva i primjene Carmichaelovih brojeva mogu se pronaći u [7].

8 Drugi zanimljivi brojevi

U ovom poglavlju navesti ćemo definicije još nekih zanimljivih klasa brojeva [9].

Definicija 3. *Cunninghamov broj je pozitivan cijeli broj oblika* $n2^n + 1$.

Prvih nekoliko takvih brojeva su: 1,3,9,25,65,161,385,. . ..

Definicija 4. *Euklidov broj je prirodan broj oblika* $E_n = p_n\# + 1$, *gdje je* $p_n\#$ *umnožak prvih n prostih brojeva.*

Prvih nekoliko takvih brojeva su: 2,3,7,31,211,2311,30031,. . ..

Definicija 5. *n-ti Hardy-Ramanujanov broj, u oznaci* $T_a(n)$ *je najmanji pozitivan broj koji se može izraziti kao suma dva kuba na n različitih načina.*

Prvih nekoliko takvih brojeva su: 2,1729,87539319,6963472309248, ...

Definicija 6. *Pellove brojeve čini niz brojeva,* (P_n), *kojeg definiramo sljedećom rekurzivnom relacijom:*

$$P(n) = \begin{cases} 0 & , n = 0 \\ 1 & , n = 1 \\ 2P_{n-1} + P_{n-2} & , n \in \mathbb{N} \setminus \{0, 1\} \end{cases}$$

Prvih nekoliko takvih brojeva su: 0,1,2,5,12,29,70,169,408,. . ..

Definicija 7. *Prothov broj je prirodan broj oblika* $N = k2^n + 1$, *gdje je k neparan cijeli broj, n pozitivan cijeli broj i* $2^n > k$.

Prvih nekoliko takvih brojeva su: 3,5,9,13,17,25,33,41,49,. . ..

Definicija 8. *Neka je k neparan, pozitivan cijeli broj. Tada je k Rieselov broj ako i samo ako je za sve pozitivne cijele brojeve n, broj* $k2^n - 1$ *složen.*

Prvih nekoliko takvih brojeva su: 509203,762701, 777149,790841,. . ..

Definicija 9. *Brojevi Sierpinskog 1. vrste su cijeli brojevi* S_n *oblika* $S_n = n^n + 1$, *za sve cijele brojeve n. Brojevi Sierpinskog 2. vrste su neparni, pozitivni cijeli brojevi k takvi da su brojevi oblika* $k2^n + 1$ *složeni za sve cijele brojeve n.*

Definicija 10. *Smithovi brojevi su oni složeni brojevi čija je suma znamenki jednaka sumi znamenki njihovih prostih faktora.*

Prvih nekoliko takvih brojeva su: 4,22,27,58,85,94,121,166,. . ..

Definicija 11. *Sternov broj je neparan broj koji se ne može zapisati u obliku* $2a^2 + p$, *gdje je a pozitivan cijeli broj, a p prost broj.*

Prvih nekoliko takvih brojeva su: 1,3,17,137,227,. . ..

Definicija 12. *Prost broj Sophie Germain je prost broj p takav da je $2p+1$ također prost.*

Prvih nekoliko takvih brojeva su: 2,3,5,11,23,29,41,53,83,....

Definicija 13. *Wieferichov prost broj je prost broj p takav da $p^2|2^{p-1}-1$.*

Niz Wieferichovih brojeva započinje s: 1093,3511,....

Definicija 14. *Wilsonov prost broj je prost broj p takav da $p^2|(p-1)!+1$.*

Prvih nekoliko takvih brojeva su: 5,13,563,....

Literatura

[1] J. H. Conway, R. K. Guy, *The book of numbers*, Copernicus, New York, 1996.

[2] E. Deza, M. Deza, *Figurate numbers*, World Scientific, Singapore, 2011.

[3] A. Dujella, *Uvod u teoriju brojeva*, PMF, Zagreb (skripta).

[4] *Fibonaccijev niz*, FER, Zagreb,
URL: https://www.fer.unizg.hr/_download/repository/diskont1-06.pdf

[5] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Osijek, 2013.

[6] P. Ochem, M. Rao, *Odd Perfect Numbers Are Greater than* 10^{1500}, Mathematics of Computation **81** (2012), 1869–1877.

[7] K. H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, 1984.

[8] *Figurate numbers*,
URL: https://www.learner.org/courses/learningmath/algebra/sesion7/index.html

[9] *Number sequence*,
URL: https://en.wikipedia.org/wiki/List_of_recreational_number_theory_topics#Number_sequences

[10] *Summary of factoring status for Fermat numbers Fm as of March 27, 2019*,
URL: https://www.prothsearch.com/fermat.html#Summary