Osječki matematički list 13 (2013), 21-31

Fermatovi brojevi

Ljubica Baćić*

Sažetak

U ovom članku opisani su Fermatovi brojevi. Zanimljiv je geometrijski prikaz ovih brojeva pomoću kojih možemo vidjeti je li broj prost ili složen. Navedena su i osnovna svojstva koja se lako dokazuju metodom matematičke indukcije.

Ključne riječi: *Fermatovi brojevi, geometrijski prikaz*

Fermat Numbers

Abstract

Fermat numbers are described in this article. It is particulary interesting to see how the geometric interpretation of these numbers can be used to determine whether the number is prime or composite. Basic properties of Fermat numbers, which can be easily proved by mathematical induction, are listed.

Keywords: *Fermat numbers, geometric interpretation*

Pierre de Fermat (1601. - 1665.), *francuski matematičar.*

1 Uvod

Francuski pravnik Pierre de Fermat postao je nadaleko poznat po svojim postignućima u matematici. Bio je jedan od začetnika diferencijalnog računa, te je dao znatan doprinos analitičkoj geometriji i vjerojatnosti. Posebno se istaknuo teoremima u teoriji brojeva, gdje su kasnije po njemu

*OŠ Nikole Andrića, Vukovar, Hrvatska, e-mail: ljubica.bacic@skole.hr

nazvani "Veliki Fermatov teorem" i "Mali Fermatov teorem". Pored toga pretpostavio je da su brojevi oblika

$$F_n = 2^{2^n} + 1, \qquad \text{za } n = 0, 1, 2, \ldots \tag{1}$$

prosti. Nakon njegove smrti ovi brojevi nazvani su *Fermatovi brojevi*.

Ako je F_n prost, onda kažemo da je on Fermatov prost broj. Fermat je smatrao da su svi takvi brojevi prosti. Prvih 5 članova niza

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

su prosti. Međutim, F_5 nije prost. 1732. godine Leonhard Euler našao je da je $F_5 = 641 \cdot 6700417$ i tako opovrgnuo Fermatovu pretpostavku.

1796. godine njemački matematičar Carl Friedrich Gauss našao je zanimljivu vezu između euklidske konstrukcije[1] pravilnih n-terokuta i Fermatovih prostih brojeva. Pokazao je da se pravilni n-terokut može konstruirati ravnalom i šestarom ako je broj stranica

$$n = 3,\ 4,\ 5,\ 6,\ 8,\ 10,\ 12,\ 15,\ 16,\ 17, \ldots$$

Preciznije, dokazao je da postoji euklidska konstrukcija pravilnog n-terokuta s n stranica ako je

$$n = 2^i F_{n_1} F_{n_2} \cdots F_{n_j}$$

gdje su $n \geq 3, i \geq 0, j \geq 0$ i $F_{n_1}, F_{n_2}, \ldots, F_{n_j}$ različiti Fermatovi prosti brojevi.

2 Geometrijski prikaz

Iz Gaussovih otkrića vidimo da Fermatovi brojevi mogu biti usko povezani s nekim geometrijskim problemima. Stoga je korisno uočiti njihovo geometrijsko značenje.

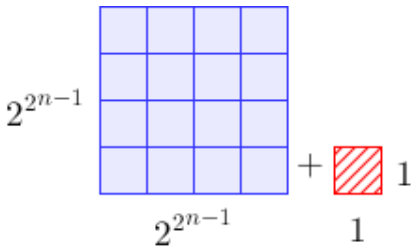
Fermatov broj $F_n = 2^{2^n} + 1$ za $n \geq 1$ može se geometrijski prikazati kao kvadrat s duljinom stranice $2^{2^{n-1}}$ uvećan za jedinični kvadrat. Zaista

$$F_n = (2^{2^{n-1}})^2 + 1.$$

Pitanje je mogu li se jedinični kvadratni blokovi preraspodijeliti kako bi činili pravokutan oblik. Važno je napomenuti da duljine stranica pravokutnika moraju biti različite od 1. Ako mogu, onda postoje prirodni brojevi $a, b \neq 1$ takvi da je

$$F_n = a \cdot b.$$

[1] Konstrukcije pomoću ravnala (bez oznake mjerne jedinice) i šestara zovemo euklidskim konstrukcijama.



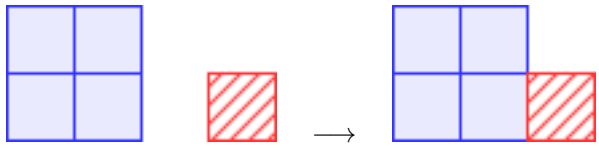
Slika 1: Geometrijski prikaz za F_n.

To zapravo znači da je broj F_n složen. Ako ne postoje takvi prirodni brojevi, onda je F_n prost. Stoga vidimo da je ovo jedna interesantna geometrijska metoda ispitivanja prostosti Fermatovih brojeva, koja je pogodna za male n.

Primjer 1. Fermatov broj $F_1 = 5$ može se shvatiti kao kvadrat s duljinom stranice 2 uvećan za jedinični kvadrat tj.

$$F_1 = 2^2 + 1 = 5.$$

Preraspodjelom jediničnih kvadratnih blokova nikako ne možemo dobiti pravokutnik (s duljinama stranica različitim od 1) što zapravo znači da je F_1 prost.

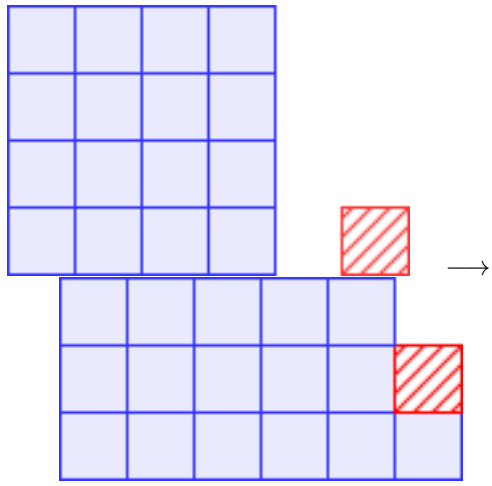


Slika 2: Preraspodjela jediničnih kvadratnih blokova za F_1.

Primjer 2. Treći Fermatov broj $F_2 = 17$ može se shvatiti kao kvadrat s duljinom stranice 4 uvećan za jedinični kvadrat tj.

$$F_2 = 4^2 + 1 = 17.$$

Preraspodjelom jediničnih kvadratnih blokova nikako ne možemo dobiti pravokutnik (s duljinama stranica različitim od 1) što zapravo znači da je F_2 prost.



Slika 3: Preraspodjela jediničnih kvadratnih blokova za F_2.

3 Osnovna svojstva

Fermatovi brojevi zadovoljavaju nekoliko rekurzivnih relacija koje ćemo ovdje navesti. Posebnu pažnju posvetit ćemo geometrijskim interpretacijama rekurzivnih relacija.

Teorem 3.1. Za svaki $n \geq 1$ vrijedi

$$F_n = (F_{n-1} - 1)^2 + 1.$$

Dokaz. Provedimo najprije dokaz metodom matematičke indukcije.

1.) Baza indukcije: Provjerimo vrijedi li tvrdnja za $n = 1$.

$$\begin{aligned} F_1 &= (F_0 - 1)^2 + 1 \\ F_1 &= (3 - 1)^2 + 1 \\ F_1 &= 2^2 + 1 \\ F_1 &= 4 + 1 \\ F_1 &= 5 \end{aligned}$$

2.) Pretpostavimo da tvrdnja vrijedi za $n = k$ tj. pretpostavimo da vrijedi

$$F_k = (F_{k-1} - 1)^2 + 1. \tag{2}$$

3.) Korak indukcije: Dokažimo da tvrdnja vrijedi za $n = k+1$ tj. dokažimo da vrijedi

$$F_{k+1} = (F_k - 1)^2 + 1. \tag{3}$$

Primjenom formule (2) dobivamo

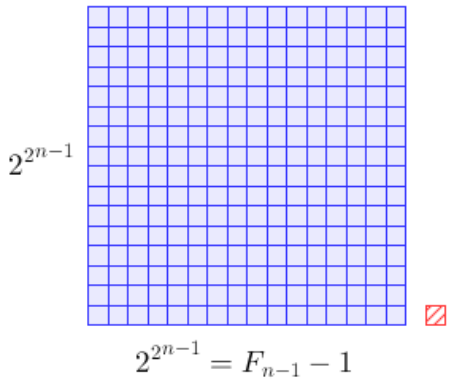
$$\begin{aligned}
(F_k - 1)^2 + 1 &= \left((F_{k-1} - 1)^2 + 1 - 1\right)^2 + 1 \\
&= \left((F_{k-1} - 1)^2\right)^2 + 1 \\
&= (F_{k-1} - 1)^4 + 1 \\
&= \left(2^{2^{k-1}} + 1 - 1\right)^4 + 1 \\
&= \left(2^{2^{k-1}}\right)^4 + 1 \\
&= 2^{4 \cdot 2^{k-1}} + 1 \\
&= 2^{2^{k+1}} + 1 \\
&= F_{k+1},
\end{aligned}$$

čime smo dokazali formulu (3). □

Pogledajmo sada i drugi dokaz.

$$(F_{n-1} - 1)^2 + 1 = (2^{2^{n-1}} + 1 - 1)^2 + 1 = (2^{2^{n-1}})^2 + 1 = 2^{2^n} + 1 = F_n.$$

Zgodno je spomenuti geometrijsku interpretaciju ovog teorema. Naime, svaki Fermatov broj F_n jednak je površini kvadrata duljine stranice $F_{n-1} - 1$ uvećanoj za jedinični kvadrat.



Slika 4: Geometrijska interpretacija Teorema 1.

Teorem 3.2. Za svaki $n \geq 2$ vrijedi

$$F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2.$$

Dokaz. Pogledajmo prvi dokaz.

1.) Baza indukcije: Provjerimo vrijedi li tvrdnja za $n = 2$.

$$\begin{aligned} F_2 &= F_1^2 - 2(F_0 - 1)^2 \\ F_2 &= 5^2 - 2(3-1)^2 \\ F_2 &= 25 - 2 \cdot 4 \\ F_2 &= 17 \end{aligned}$$

2.) Pretpostavimo da tvrdnja vrijedi za $n = k$ tj. pretpostavimo da vrijedi

$$F_k = F_{k-1}^2 - 2(F_{k-2} - 1)^2. \tag{4}$$

3.) Korak indukcije: Dokažimo da tvrdnja vrijedi za $n = k + 1$ tj. dokažimo da vrijedi

$$F_{k+1} = F_k^2 - 2(F_{k-1} - 1)^2. \tag{5}$$

Primjenom formule (4) dobivamo

$$\begin{aligned}
F_k^2 - 2(F_{k-1}-1)^2 &= \left(F_{k-1}^2 - 2(F_{k-2}-1)^2\right)^2 - 2(F_{k-1}-1)^2 \\
&= \left(\left(2^{2^{k-1}}+1\right)^2 - 2\left(2^{2^{k-2}}+1-1\right)^2\right)^2 - 2\left(2^{2^{k-1}}+1-1\right)^2 \\
&= \left(2^{2^k} + 2\cdot 2^{2^{k-1}} + 1 - 2\left(2^{2^{k-2}}\right)^2\right)^2 - 2\left(2^{2^{k-1}}\right)^2 \\
&= \left(2^{2^k} + 2\cdot 2^{2^{k-1}} + 1 - 2\cdot 2^{2^{k-1}}\right)^2 - 2\cdot 2^{2^k} \\
&= \left(2^{2^k}+1\right)^2 - 2\cdot 2^{2^k} \\
&= 2^{2^{k+1}} + 2\cdot 2^{2^k} + 1 - 2\cdot 2^{2^k} \\
&= 2^{2^{k+1}} + 1 \\
&= F_{k+1},
\end{aligned}$$

čime smo dokazali formulu (5).

Pogledajmo sada i drugi dokaz. Dovoljno je uočiti da izjednačavanjem izraza

$$F_n = (F_{n-1}-1)^2 + 1 \qquad \text{i} \qquad F_n = F_{n-1}^2 - 2(F_{n-2}-1)^2$$

lako dobivamo formulu koja povezuje F_{n-1} i F_{n-2}

$$(F_{n-2}-1)^2 = F_{n-1} - 1. \tag{6}$$

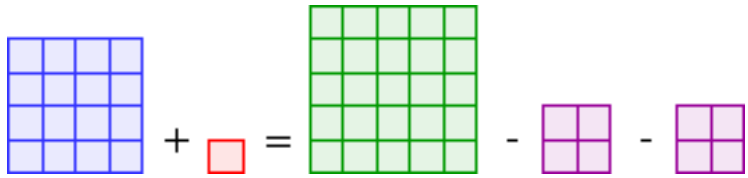
Stoga, primjenom Teorema 1 slijedi

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

□

Geometrijsko interpretacija ovog teorema je da svaki Fermatov broj F_n predstavlja površinu kvadrata duljine stranice F_{n-1} umanjenu za dvije površine kvadrata duljine stranice $F_{n-2}-1$. U slučaju $F_2 = 17$ imamo

$$4^2 + 1 = 5^2 - 2\cdot 2^2.$$



Slika 5: Geometrijska interpretacija Teorema 2 za $F_2 = 17$.

Teorem 3.3. Za svaki $n \geq 1$ vrijedi

$$F_n = F_0 \cdots F_{n-1} + 2.$$

Dokaz. Dokaz provodimo metodom matematičke indukcije.

1.) Baza indukcije: Provjerimo vrijedi li tvrdnja za $n = 1$.

$$\begin{aligned} F_1 &= F_0 + 2 \\ F_1 &= 3 + 2 \\ F_1 &= 5 \end{aligned}$$

2.) Pretpostavimo da tvrdnja vrijedi za $n = k$ tj. pretpostavimo da vrijedi

$$F_k = F_0 \cdots F_{k-1} + 2. \tag{7}$$

3.) Korak indukcije: Dokažimo da tvrdnja vrijedi za $n = k + 1$ tj. dokažimo da vrijedi

$$F_{k+1} = F_0 \cdots F_k + 2. \tag{8}$$

Primjenom formule (7) dobivamo

$$\begin{aligned} F_0 \cdots F_k + 2 &= F_0 \cdots F_{k-1} \cdot F_k + 2 \\ &= (F_k - 2) \cdot F_k + 2 \\ &= (2^{2^k} - 1) \cdot (2^{2^k} + 1) + 2 \\ &= 2^{2^{k+1}} - 1 + 2 \\ &= 2^{2^{k+1}} + 1 \\ &= F_{k+1}, \end{aligned}$$

čime smo dokazali formulu (8).

□

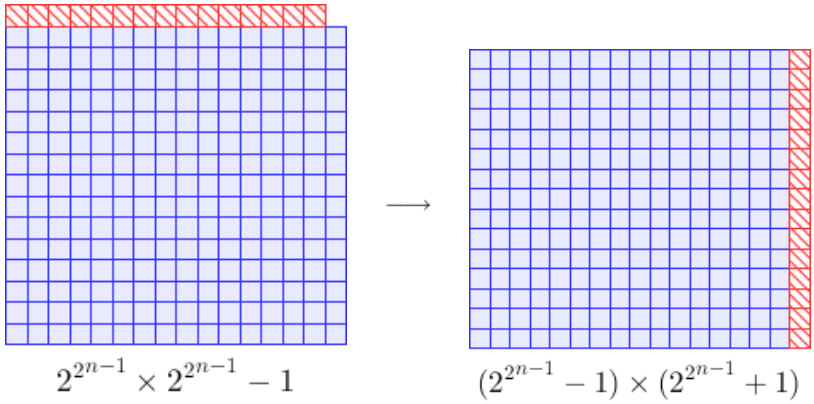
Kako bi razumjeli geometrijski dokaz ovog teorema, uočimo prvo da iz Teorema 3.1 oduzimanjem broja 2 s obje strane lako dobivamo

$$F_n - 2 = (F_{n-1} - 1)^2 - 1.$$

Uvrštavanjem formule (1)

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

To zapravo znači da $F_n - 2$ predstavlja površinu kvadrata s duljinom stranice F_{n-1} umanjenu za jedinični kvadrat. Preraspodjelom jediničnih kvadratnih blokova dobije se pravokutnik što je i prikazano na Slici 6.



Slika 6: Geometrijska interpretacija Teorema 3.

Teorem 3.4. Za svaki $n \geq 1$ vrijedi

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

Dokaz. Teorem dokazujemo metodom matematičke indukcije.

1.) Baza indukcije: Provjerimo vrijedi li tvrdnja za $n = 1$.

$$\begin{aligned} F_2 &= F_1 + 2^{2^1} \cdot F_0 \\ F_2 &= 5 + 4 \cdot 3 \\ F_2 &= 17 \end{aligned}$$

2.) Pretpostavimo da tvrdnja vrijedi za $n = k$ tj. pretpostavimo da vrijedi

$$F_{k+1} = F_k + 2^{2^k} F_0 \cdots F_{k-1}. \tag{9}$$

3.) Korak indukcije: Dokažimo da tvrdnja vrijedi za $n = k+1$ tj. dokažimo da vrijedi

$$F_{k+2} = F_{k+1} + 2^{2^{k+1}} F_0 \cdots F_k. \tag{10}$$

Primjenom formule (9) dobivamo

$$\begin{aligned} F_{k+1} + 2^{2^{k+1}} F_0 \cdots F_k &= F_{k+1} + 2^{2^k} \cdot (2^{2^k} F_0 \cdots F_{k-1}) \cdot F_k \\ &= F_{k+1} + 2^{2^k} \cdot F_k \cdot (F_{k+1} - F_k) \\ &= 2^{2^{k+1}} + 1 + 2^{2^k} \cdot (2^{2^k} + 1) \cdot (2^{2^{k+1}} - 2^{2^k}) \\ &= 2^{2^{k+1}} + 1 + 2^{2^k} \cdot (2^{2^k} + 1) \cdot 2^{2^k} \cdot (2^{2^k} - 1) \\ &= 2^{2^{k+1}} + 1 + 2^{2^{k+1}} \cdot (2^{2^{k+1}} - 1) \\ &= 2^{2^{k+1}} + 1 + 2^{2^{k+2}} - 2^{2^{k+1}} \\ &= 2^{2^{k+2}} + 1 \\ &= F_{k+2}, \end{aligned}$$

čime smo dokazali formulu (10).

□

Na kraju, istaknimo kako je geometrijska interpretacija Fermatovih brojeva pogodna i prilikom obrade prostih brojeva u 5. razredu osnovne škole. Velik dio dokaza može se iskoristiti i kod obrade principa matematičke indukcije u 4. razredu gimnazije.

Ali i dalje postoje neka otvorena pitanja! Naglasimo da su jedini do sada poznati prosti Fermatovi brojevi upravo $F_0, \ldots, F_4$. Je li F_n složen za svaki $n > 4$? Postoji li beskonačno mnogo prostih Fermatovih brojeva? Postoji li beskonačno mnogo složenih Fermatovih brojeva?

Literatura

[1] M. Križek, F. Luca and L. Somer, *17 Lectures on Fermat Numbers – From Number Theory to Geometry, Springer-Verlag, New York, 2001.*

[2] I. Matić, *Uvod u teoriju brojeva*, Skripta, Odjel za matematiku, Sveučilište J. J. Strossmayera u Osijeku, Osijek, 2011.

[3] C. Tsang, *Fermat Numbers*, završni projekt iz kolegija Math414 Number Theory, profesora Williama Steina na University of Washington, 2010. http://modular.math.washington.edu/edu/2010/414/projects/tsang.pdf

[4] *Wikipedia*, http://hr.wikipedia.org/wiki/Pierre_de_Fermat