Fermatovi brojevi

Sedlar, Antonija

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Antonija Sedlar

Fermatovi brojevi

Završni rad

Osijek, 2019.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Antonija Sedlar

Fermatovi brojevi

Završni rad

Voditelj: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2019.

Sažetak:

U ovom radu se bavimo Fermatovim brojevima, svojstvima prostih i složenih Fermatovih brojeva, njihovom geometrijskom interpretacijom te osnovnim alatima za razumijevanje navedenih svojstava.

Ključne riječi:

Fermatovi brojevi, testovi prostosti, konstrukcija pravilnih mnogokuta, Mersennovi brojevi, geometrijska interpretacija

Fermat numbers

Abstract: In this work, we will discuss Fermat numbers, properties of the Fermat primes and composites, its geometric interpretation and basic tools for understanding mentioned properties.

Key words: Fermat numbers, primality tests, constrution of regular polygons, Mersenne numbers, geometric interpretation

Sadržaj

Uvod

Pierre de Fermat francuski je matematičar s početka 17. stoljeća. Često ga nazivaju osnivačem moderne teorije brojeva. Također, zbog njegovih metoda za pronalaženje tangente na krivulju te točke u kojoj postiže minimum i maksimum smatra se začetnikom diferencijalnog računa. Postavio je i temelje teorije vjerojatnosti te analitičke geometrije.
U ovom radu ćemo se usredotočiti na dio njegovog doprinosa teoriji brojeva.

Slika 1: Pierre de Fermat[1]

1640. godine u pismima svojim suvremenicima, uključujući i Blaisea Pascala, Fermat navodi kako vjeruje da su brojevi oblika $2^{2^n}+1$ prosti. Takvi brojevi su kasnije nazvani Fermatovi brojevi. Formalno:

Definicija. *Fermatovi brojevi su brojevi oblika* $F_n = 2^{2^n}+1$, $n \in \mathbb{N}_0$.

Stoljeće kasnije, Euler je pobio Fermatovu slutnju, pokazavši da je 641 prost djelitelj Fermatovog broja $2^{2^5}+1$. Zaista:

$$\begin{aligned} 2^{32}+1 &= 2^4 \cdot 2^{28}+1 = (641-5^4)\cdot 2^{28}+1 \\ &= 641\cdot 2^{28} - (5\cdot 2^7)^4 + 1 = 641\cdot 2^{28} - (641-1)^4 + 1 \\ &= 641\cdot(2^{28} - 641^3 + 4\cdot 641^2 - 6\cdot 641 + 4). \end{aligned}$$

Usprkos tome, Fermatovi brojevi nastavljaju biti predmetom istraživanja brojnih matematičara. Do danas se ne zna postoji li prost Fermatov broj za $n > 4$.

U nastavku rada bavit ćemo se otkrićima matematičara vezanih uz Fermatove brojeve. Proučit ćemo njihova svojstva općenito, ali i ona vezana samo uz proste Fermatove brojeve. Navest ćemo pregled faktorizacije Fermatovih brojeva do $n = 200$. Također, pokazat ćemo geometrijsko značenje Fermatovih brojeva i nekih njihovih svojstava te ćemo utvrditi vezu između Fermatovih i Mersennovih brojeva.

[1]Izvor: [11]

1. Fermatovi brojevi

1.1. Osnovna svojstva Fermatovih brojeva

Proučavajući Fermatove brojeve, matematičari su kroz stoljeća otkrivali njihova brojna svojstva. U ovom potpoglavlju navest ćemo svojstva zajednička svim Fermatovim brojevima.

Teorem 1.1. *Za $n \geq 1$ vrijedi*

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

Dokaz. Za $n-1$ dobivamo

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

Kada to uvrstimo u desnu stranu jednakosti (1), dobivamo

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

a to je upravo jednako n-tom Fermatovom broju, pa je tvrdnja dokazana. □

Osim što se n-ti Fermatov broj može dovesti u relaciju sa svojim Fermatovim prethodnikom, možemo uočiti njegovu vezu sa svim njegovim Fermatovim prethodnicima. Nju ćemo navesti u sljedeća dva teorema.

Teorem 1.2. *Za $n \geq 1$ vrijedi*

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

Dokaz. Dokaz ovog teorema provodi se indukcijom.
Za $n = 1$ uvrstimo:

$$F_0 + 2 = 3 + 2 = 5 = F_1.$$

Pretpostavimo da vrijedi

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

U koraku indukcije, u $F_0 \cdots F_n + 2$ umjesto prvih $n-1$ Fermatovih brojeva uvrštavamo $F_n - 2$ što smo pretpostavili u drugom koraku dokaza tj. pišemo

$$\begin{aligned} F_0 \cdots F_{n-1} F_n + 2 &= (F_n - 2)F_n + 2 \\ &= (2^{2^n} - 1)(2^{2^n} + 1) + 2. \end{aligned}$$

Dobiveni izraz je razlika kvadrata, pa vrijedi

$$2^{2^{n+1}} - 1 + 2 = 2^{2^{n+1}} + 1,$$

a to je upravo F_{n+1}. □

Teorem 1.3. *Za $n \geq 2$ vrijedi*

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

Dokaz. Dokaz se provodi indukcijom.
Za $n = 2$, vrijedi

$$F_1 + 2^2 F_0 = 5 + 2^2 \cdot 3 = 17 = F_2.$$

Pretpostavimo da vrijedi

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

Tada, ako krenemo od izraza kojeg trebamo dobiti, i uvrstimo jednakost iz pretpostavke, dobivamo

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

čime je ova tvrdnja dokazana. □

Korolar 1.1. *Za $m \leq 2^n - 1$ vrijedi*

$$F_m \mid 2^{F_n} - 2.$$

Dokaz. Primjenom Teorema 1.2. dobivamo

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

odakle slijedi tvrdnja. □

Korolar 1.2. *Za $n \geq 1$ i sve $k = 0, 1, \ldots n-1$ vrijedi*

$$F_n \equiv 2 \pmod{F_k}.$$

Dokaz. Ekvivalentno je reći da $F_k \mid F_n - 2$. Zbog Teorema 1.2 vrijedi $F_n = F_0 \cdots F_{n-1} + 2$, odnosno

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

a odavde odmah slijedi tvrdnja. □

Korolar 1.3. *Za $n \geq 2$, zadnja znamenka od F_n je 7.*

Dokaz ovog teorema provest ćemo rješavajući sustav linearnih kongruencija. Kako bismo to učinili, iskoristit ćemo Kineski teorem o ostacima, kojeg ćemo najprije navesti.

Teorem 1.4 (Kineski teorem o ostacima)**.** *Neka su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti prirodni brojevi. Neka su $a_1, a_2, \ldots, a_r$ cijeli brojevi. Tada sustav kongruencija*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

ima rješenje. Ako je jedno rješenje dano s x_0, onda su sva rješenja tog sustava dana s

$$x \equiv x_0 \pmod{m_1 m_2 \ldots m_r}.$$

Dokaz Korolara 1.3. Iz Korolara 1.2 slijedi da je $F_n \equiv 2 \pmod 5$. Kako su svi Fermatovi brojevi neparni, vrijedi $F_n \equiv 1 \pmod 2$. Primjenjujući Kineski teorem o ostacima, dobivamo:

$$5F_n \equiv 1 \pmod 2,$$
$$2F_n \equiv 2 \pmod 5.$$

Slijedi

$$F_n \equiv 1 \cdot 2 + 1 \cdot 5 \pmod{10},$$

tj.

$$F_n \equiv 7 \pmod{10},$$

čime smo dokazali traženo. □

Korolar 1.4. *Ni jedan Fermatov broj nije potpun kvadrat.*

Dokaz. Očito $F_0 = 3$ i $F_1 = 5$ nisu potpuni kvadrati. Za F_n, gdje je $n \geq 2$, po Korolaru 1.3 vrijedi $F_n \equiv 7 \pmod{10}$. S druge strane, samo brojevi koji su kongruentni s 0,1,4,5,6 ili 9 (mod 10) mogu biti potpuni kvadrati, pa je time tvrdnja dokazana. □

Korolar 1.5. *Svaki Fermatov broj F_n, za $n \geq 1$ je oblika $6m - 1$.*

Dokaz. Ekvivaletno je pokazati da $6 \mid F_n + 1$. Prema Teoremu 1.2 vrijedi

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

Ako s obje strane dodamo 1 i umjesto F_0 uvrstimo 3, dobivamo:

$$F_n + 1 = 3F_1 \cdots F_n + 2 + 1 = 3(F_1 \cdots F_n + 1),$$

gdje je $F_1 \cdots F_n + 1$ paran broj (svi Fermatovi brojevi su neparni, pa je i njihov umnožak neparan). Kako je $F_n + 1$ istovremeno djeljiv s 2 i 3, $F_n + 1$ je djeljiv sa 6. □

Teorem 1.5. *Za $n \geq 2$ vrijedi*

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

Dokaz. Krenut ćemo od desne strane i raspisati ju po binomnoj formuli:

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

što je upravo jednako F_n. □

Teorem 1.6. *Za $n \geq 2$, svaki Fermatov broj se može napisati na beskonačno mnogo načina u obliku $x^2 - 2y^2$, gdje su x i y prirodni brojevi.*

Dokaz. Teorem 1.5 nam daje jedan takav zapis, pri čemu je

$$(x, y) = (F_{n-1}, F_{n-2} - 1).$$

Primjetimo sada da vrijedi

$$\begin{aligned} (3x + 4y)^2 - 2(2x + 3y)^2 &= 9x^2 + 24xy + 16y^2 - 2(4x^2 + 12xy + 9y^2) \\ &= x^2 - 2y^2. \end{aligned}$$

Ako su x i y oboje pozitivni, $3x + 4y > x$ i $2x + 3y > y$ su također pozitivni. To znači da (x_i, y_i) možemo pronaći rekurzivno, postavljajući

$$(x_i, y_i) = (3x_{i-l} + 4y_{i-l}, 2x_{i-l} + 3y_{i-l}).$$

Skup svih točaka ovog oblika je beskonačan, a svaki par (x_i, y_i) daje jedan prikaz broja F_n u traženom obliku. □

Teorem 1.7. *Svaka dva međusobno različita Fermatova broja su relativno prosta.*

Dokaz. Pretpostavimo suprotno: postoje Fermatovi brojevi F_i, F_j i $a > 1$ takvi da $a \mid F_i$ i $a \mid F_j$. Možemo, bez smanjenja općenitosti, pretpostaviti da vrijedi $F_j > F_i$.
Zbog Teorema 1.3 znamo da vrijedi

$$F_j = F_{j-1} + 2^{2j-1} \cdot F_0 \cdots F_i \cdots F_{j-2}.$$

Kako a dijeli F_i i F_j, a dijeli i F_{j-1}, a samim time i $F_0 \cdots F_i \cdots F_{j-1}$. No onda $a \mid F_j - F_0 \cdots F_{j-1}$, što je prema Teoremu 1.2 jednako 2. Slijedi $a = 2$, ali kako su svi Fermatovi brojevi neparni, dolazimo do kontradikcije. □

Osim što Teorem 1.7 daje jednu karakteristiku Fermatovih brojeva, možemo ga iskoristiti u jednom od dokaza beskonačnosti skupa prostih brojeva.

Korolar 1.6. *Skup prostih brojeva je beskonačan.*

Dokaz. Definiramo:

$$p_i = \begin{cases} F_i, & \text{ako je } F_i \text{ prost} \\ \text{prost faktor od } F_i, & \text{ako je } F_i \text{ složen} \end{cases}$$

Svi brojevi p_i su po Teoremu 1.7 različiti, pa slijedi da skup $\{p_i : i = 1, 2, 3 \dots\}$ sadrži beskonačno mnogo prostih brojeva. □

Teorem 1.8. *Ni jedan Fermatov broj F_n za $n \geq 2$ se ne može prikazati kao zbroj dva prosta broja.*

Dokaz. Pretpostavimo suprotno. Koristeći činjenicu da je F_n neparan, kako bismo došli do kontradikcije, jedan od dva prosta broja mora biti broj 2. Tada drugi pribrojnik mora biti jednak

$$F_n - 2 = 2^{2^n} - 1.$$

Taj izraz možemo rastaviti na razliku kvadrata:

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

Kako je $n \geq 2$, $F_n - 2$ nije prost broj. □

1.2. Svojstva prostih Fermatovih brojeva

Iako smo do sada Fermatove brojeve promatrali kao brojeve oblika $2^{2^n} + 1$, gdje je $n \in \mathbb{N}$, koristi se još jedna definicija Fermatovih brojeva ([9]).

Definicija 1.1. *Fermatovi brojevi su brojevi oblika $2^n + 1$, gdje je $n \in \mathbb{N}$.*

Primarno se držimo definicije koje smo naveli u Uvodu jer je uvriježenija. Osim toga, svojstva koja smo naveli i dokazali u prethodnom poglavlju odnose se upravo na brojeve oblika $2^{2^n}+1$.

Primjetimo, ako koristimo Definiciju 1.1, Teorem 1.7 ne vrijedi.

Primjer 1.1. *Za brojeve* $2^3+1=9$ *i* $2^5+1=33$ *vrijedi* $(9,33)=3$.

Ako promatramo samo proste Fermatove brojeve, tada je svejedno koju definiciju koristimo. To nam ilustrira sljedeći teorem.

Teorem 1.9. *Ako je* 2^n+1 *prost broj, tada je* n *potencija broja 2.*

Dokaz. Teorem dokazujemo po kontrapoziciji. Pretpostavimo da je n prirodni broj koji nije potencija broja 2. Tada n možemo prikazati kao $n=2^r s$, gdje je r nenegativan cijeli broj i s neparan prirodan broj. Također, prisjetimo se da vrijedi:

$$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-1}+b^{n-1}).$$

Iz toga slijedi da $a-b$ dijeli razliku a^n-b^n. Ako uvedemo supstituciju $a=2^r$, $b=-1$ i $n=s$, dobivamo da 2^r+1 dijeli $2^{rs}-(-1)^s=2^n+1$. S druge strane, $r<n$ iz čega slijedi da 2^n+1 nije prost. Dakle, n mora biti potencija broja 2 kako bi 2^n+1 bio prost. □

Teorem 1.10. *Ni jedan prost Fermatov broj ne može se prikazati kao razlika dvaju p-tih potencija, gdje je p neparan prost broj.*

U dokazu gore navedenog svojstva bit će nam potreban Mali Fermatov teorem pa ćemo najprije njega navesti.

Teorem 1.11. *(Mali Fermatov teorem) Neka je p prost broj i a cijeli broj. Tada je* $a^p\equiv a \pmod p$, *te ako p ne dijeli a vrijedi i* $a^{p-1}\equiv 1 \pmod p$.

Dokaz Teorema 1.10. Dokaz provodimo kontradikcijom. Pretpostavimo da postoji takav Fermatov broj. Tada vrijedi

$$F_n=a^p-b^p=(a-b)(a^{p-1}+a^{p-2}b+\cdots+ab^{p-1}+b^{p-1}),$$

gdje je $a>b$ i p je neparan prost broj. Kako je F_n prost, mora vrijediti da je $a-b=1$. Nadalje, zbog Malog Fermatovog teorema vrijedi

$$a^p\equiv a \pmod p$$

i

$$b^p\equiv b \pmod p.$$

Slijedi,

$$F_n=a^p-b^p\equiv a-b=1 \pmod p.$$

Odavde slijedi

$$p \mid F_n-1=2^{2^n}$$

čime smo došli do kontradikcije, jer je očito jedini prost djelitelj broja 2^{2^n} broj 2. □

1.3. Testovi prostosti Fermatovih brojeva

Osim Malog Fermatovog teorema, postoji još nekoliko različitih testova kojima provjeravamo prostost Fermatovih brojeva (ali i brojeva općenito). U ovom poglavlju susrest ćemo se sa Selfridgovim testom (Teorem 1.14) i generaliziranom verzijom Pepinovog testa (Teorem 1.16). U dokazima ovih teorema pojavljuje se Jacobijev simbol, pa ćemo prvo njega uvesti.

Definicija 1.2. *Neka je p neparan prost broj i a cijeli broj. Legendrov simbol $\left(\frac{a}{p}\right)$ definiran je s*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ako je } a \text{ kvadratni ostatak modulo } p, \\ 0, & \text{ako } p \mid a, \\ -1, & \text{ako je } a \text{ kvadratni neostatak modulo } p. \end{cases}$$

Definicija 1.3. *Neka je P neparan prirodan broj, te zapišimo P u obliku $P = p_1 p_2 \cdots p_n$, gdje su p_1, p_2, ..., p_n prosti brojevi, koji su nužno neparni. Jacobijev simbol $\left(\frac{a}{P}\right)$ definiran je s $\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_n}\right)$, gdje je $\left(\frac{a}{p_i}\right)$ Legendreov simbol.*

Jacobijev simbol je direktna generalizacija Legendreova simbola. U slučaju kada je P prost, Legendreov i Jacobijev simbol se podudaraju.

Teorem 1.12 (Eulerov kriterij)**.** *Ako je p neparan prost broj, tada vrijedi*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Prema tome, a je kvadratni ostatak modulo p ako i samo ako

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Dokazi ovog i teorema koji slijedi mogu se naći u [6].

Teorem 1.13. *Neka su $m > 1$ i $n > 1$ neparni cijeli brojevi i neka su $a, b \in \mathbb{Z}$. Tada vrijedi:*

i) ako je $a \equiv b \pmod{n}$, onda je $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$;

ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$;

iii) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$;

iv) $\left(\frac{1}{n}\right) = 1$, $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$;

v) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$;

vi) $\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}\left(\frac{n}{m}\right)$.

Teorem 1.14. *Neka je $N > 1$ i $\prod_{i=1}^{r} p_i^{k_i}$ faktorizacija broja $N-1$ na proste faktore. Tada je N prost ako i samo ako za svaki p_i, $i = 1, \ldots, r$ postoji $a_i \in \mathbb{N}$ takav da $a_i^{N-1} \equiv 1 \pmod{N}$ i $a_i^{\frac{N-1}{p_i}} \not\equiv 1 \pmod{N}$.*

Kako bismo razumjeli dokaz ovog teorema, uvodimo nekoliko definicija i pomoćni teorem bez dokaza.

Definicija 1.4. *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se red od a modulo n.*

Definicija 1.5. *Ako je red od a modulo n jednak $\varphi(n)$, onda se a zove primitivni korijen modulo n.*

Teorem 1.15 (Eulerov teorem)**.** *Ako je $(a, m) = 1$, onda je*

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

Dokaz Teorema 1.14. Ako je N prost broj, postoji primitivan korijen a koji zadovoljava oba uvjeta. Pretpostavimo sada da je N složen. Preostaje pokazati da je $\varphi(N) = N - 1$. Neka je e_i takav da je $a_i^{e_i} \equiv 1 \pmod{N}$. Tada e_i dijeli razliku $N - 1$, ali ne i $\frac{N-1}{p_i}$. Dakle, $p_i^{k_i} \mid e_i$. Također, zbog Eulerovog teorema vrijedi

$$a_i^{\varphi(N)} \equiv 1 \pmod{N}$$

iz čega slijedi $e_i \mid \varphi(N)$.
Iz $p_i^{k_i} \mid e_i$ i $e_i \mid \varphi(N)$ zaključujemo $p_i^{k_i} \mid \varphi(N)$ za sve $i = 1, 2, \ldots r$, pa $N - 1 \mid \varphi(N)$. Ali, kako je $\varphi(N) \leq N - 1$ vrijedi $\varphi(N) = N - 1$. □

Teorem 1.16. *Za $n \geq 2$, Fermatov broj F_n je prost ako i samo ako*

$$a^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n},$$

gdje je a cijeli broj takav da Jacobijev simbol $\left(\frac{a}{F_n}\right) = -1$ za sve.

Dokaz. Za početak, pretpostavimo da je F_n prost broj. Tada je Jacobijev simbol $\left(\frac{a}{F_n}\right)$ Legendreov simbol, pa po Eulerovom kriteriju znamo

$$a^{\frac{F_n-1}{2}} \equiv \left(\frac{a}{F_n}\right) \equiv -1 \pmod{F_n}.$$

Sada pretpostavimo da kongruencija vrijedi tj.

$$a^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

No, onda je

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

Kako je 2 jedini prost djelitelj broja $F_n - 1$, prema Teoremu 1.14, F_n je prost broj. □

Korolar 1.7. *Za $n \geq 2$, Fermatov broj F_n je prost ako i samo ako*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Dokaz. Dovoljno je pokazati da je

$$\left(\frac{3}{F_n}\right) = -1.$$

Iz Korolara 1.2 slijedi

$$F_n \equiv 2 \pmod{3}.$$

Nadalje, kako je

$$F_n \equiv 1 \pmod{4},$$

prema Teoremu 1.13 vrijedi

$$\left(\frac{3}{F_n}\right) = (-1)^{\frac{(3-1)(4k+1-1)}{4}} \left(\frac{F_n}{3}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

□

2. Faktorizacije Fermatovih brojeva

2.1. Tablica faktorizacije Fermatovih brojeva

U ovom poglavlju prikazat ćemo status faktorizacije prvih 201 ($0 \leq n \leq 1$) Fermatovih brojeva. Kako bismo bolje i zornije razumjeli razlog velikog broja nepotpune faktorizacije Fermatovih brojeva, dat ćemo pregled prvih 11 Fermatovih brojeva.

$$
\begin{aligned}
F_0 &= 3,\\
F_1 &= 5,\\
F_2 &= 17,\\
F_3 &= 257,\\
F_4 &= 65537,\\
F_5 &= 4294967297,\\
F_6 &= 18446744073709551617,\\
F_7 &= 340282366920938463463374607431768211457,\\
F_8 &= 115792089237316195423570985008687907853\\
&\quad 269984665640564039457584007913129639937,\\
F_9 &= 134078079299425970995740249982058461274\\
&\quad 793658205923933777235614437217640300735\\
&\quad 469768018742981669034276900318581864860\\
&\quad 508537538828119465699464336490060840 97,\\
F_{10} &= 179769313486231590772930519078902473361\\
&\quad 797697894230657273430081157732675805500\\
&\quad 963132708477322407536021120113879871393\\
&\quad 357658789768814416622492847430639474124\\
&\quad 377767893424865485276302219601246094119\\
&\quad 453082952085005768838150682342462881473\\
&\quad 913110540827237163350510684586298239947\\
&\quad 245938479716304835356329624224137217.
\end{aligned}
$$

Primjećujemo da broj znamenki Fermatovih brojeva vrlo brzo raste: već F_{10} ima 308 znamenki. Točnije, broj znamenki n-tog Fermatovog broja dan je formulom:

$$
\begin{aligned}
D(n) &= \lfloor [\log (2^{2^n} + 1)] + 1 \rfloor\\
&\approx \lfloor [\log (2^{2^n})] + 1 \rfloor\\
&= 1 + \lfloor 2^n \log 2 + 1 \rfloor,
\end{aligned}
$$

što znači da je broj znamenki eksponencijalnog rasta. To objašnjava nepotpune ili nepostojeće faktorizacije Fermatovih brojeva. Detaljnije o faktorizaciji Fermatovih brojeva možemo razmotriti o sljedećoj tablici.

									0
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Prost	
Složen bez poznatih faktora	
Složen s nepotpunom faktorizacijom	
Potpuno faktoriziran složen broj	
Nepoznato je li prost ili složen	

Slika 2: Tablica faktorizacije Fermatovih brojeva do $n = 200$[2]

[2]Izvor [9]

3. Geometrijski prikaz Fermatovih brojeva

3.1. Geometrijsko značenje Fermatovih brojeva

Kao što je već spomenuto, Fermatovi brojevi su bili objekt velikog interesa raznih matematičara. 1796. godine (prisjetimo se, Fermat uvodi pojam Fermatovih brojeva 1640.) njemački matematičar Carl Friedrich Gauss pronalazi vezu između Fermatovih prostih brojeva i euklidske konstrukcije (konstrukcija pomoću ravnala (bez oznake mjerne jedinice) i šestara) pravilnih $n-terokuta$ ([4]). Došao je do zaključka da se pravilni $n-terokut$ može konstruirati ravnalom i šestarom ako je broj stranica

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

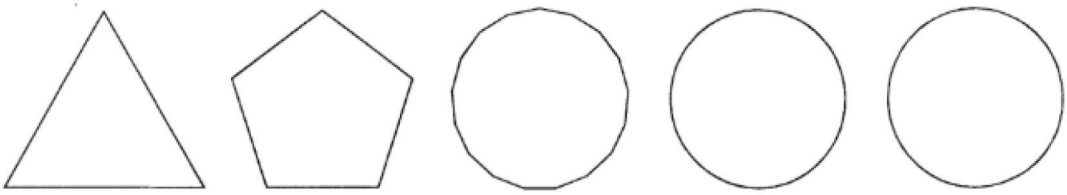
Preciznije, dokazao je da postoji euklidska konstrukcija pravilnog n-terokuta s n stranica ako je

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

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. Kako do sada poznajemo točno 5 Fermatovih prostih brojeva, zbog

$$\binom{5}{1} + \binom{5}{2} + \binom{5}{3} + \binom{5}{4} + \binom{5}{5} = 31$$

znamo da postoji barem 31 pravilan $n-terokut$ (i samo 5 pravilnih $n-terokuta$ čiji broj stranica je prost broj (Slika 3)) koje znamo euklidski konstruirati. Napomenimo da vrijedi i obrat ovog teorema. Njega je dokazao Wantzel, a dokaz se može pronaći u [10].



Slika 3: Pravilan trokut, pentagon, heptadekagon, 257-gon i 65537-gon[3]

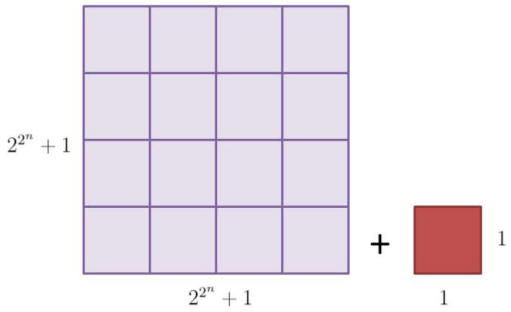
Iz ovoga vidimo da Fermatovi brojevi mogu biti povezani s nekim geometrijskim problemima. Zbog toga ćemo u nastavku promotriti njihovo geometrijsko značenje i interpretaciju. Fermatov broj F_n geometrijski se može prikazati kao kvadrat duljine stranice $2^{2^{n-1}}$ uvećan za jedinični kvadrat (Slika 4). Zaista

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

Dolazimo do problema preraspodjele jediničnih kvadratnih blokova u pravokutan oblik. Napomenimo da duljine stranica kvadrata moraju biti različite od 1. Ako postoji riješenje ovog problema, onda postoje prirodni brojevi a i b različiti od 1, takvi da je

$$F_n = a \cdot b.$$

[3]Izvor: [5]



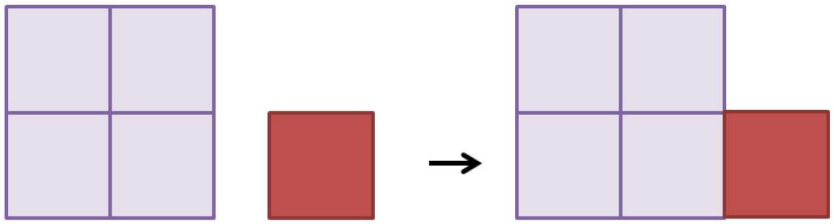
Slika 4: Geometrijski prikaz broja F_n[4]

Ovakav zapis Fermatovog broja F_n nam govori da je on složen. Ako ne postoje takvi a i b, odnosno, ako se F_n ne može prikazati kao pravokutnik, slijedi da je F_n prost Fermatov broj. Možemo primjetiti da smo našli još jednu, ilustrativnu, metodu za ispitivanje prostosti Fermatovih brojeva, koja je pogodna za provođenje za male n.

Primjer 3.1. *Fermatov broj $F_1 = 5$ možemo shvatiti kao kvadrat s duljinom stranice 2 uvećan za jedinični kvadrat, tj.*

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

Primjetimo da neovisno o tome kako pokušamo preraspodijeliti jedinične kvadratne blokove, nikada nećemo dobiti pravokutnik, zbog čega zaključujemo da je F_1 prost broj.

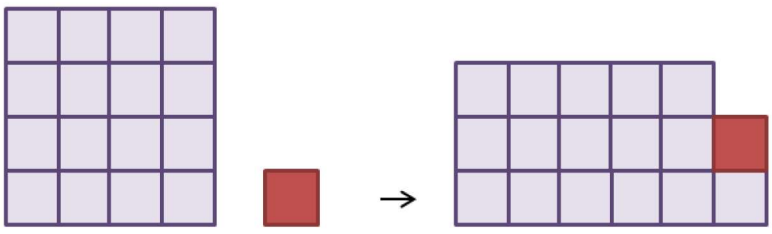


Slika 5: Preraspodjela jediničnih kvadratnih blokova za F_1

Primjer 3.2. *Treći Fermatov broj $F_2 = 17$ može se shvatiti kao kvadrat s duljinom stranice 4 uvećan za jedinični kvadrat tj.*

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

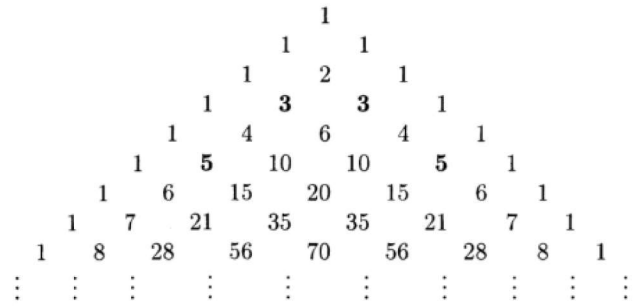
Preraspodjelom jediničnih kvadratnih blokova ni na koji način ne možemo dobiti pravokutnik (s duljinama stranica različitim od 1) što implicira da je F_2 prost.



Slika 6: Preraspodjela jediničnih kvadratnih blokova za F_2

Još jedna zanimljiva poveznica između teorije brojeva i geometrije leži u vezi Pascalovog trokuta i Fermatovih brojeva.
Promotrimo Pascalov trokut i položaj Fermatovih brojeva u njemu.

[4]Slike s ove stranice preuzete su iz [1]

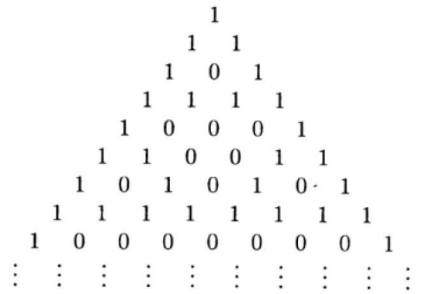


Slika 7: Položaj Fermatovih brojeva u Pascalovom trokutu[5]

Ako sada ispišemo Pascalov trokut modulo 2, interpretirajući prva 32 reda kao brojeve u binarnom sustavu, dobivamo monotono rastući niz

$$1, 3, 5, 15, 17, 51, 85, 255, 257 \ldots$$

.

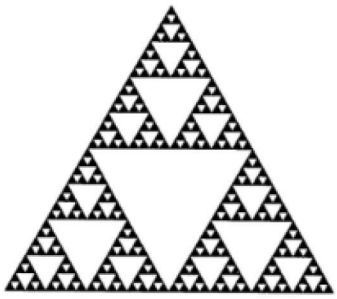


Slika 8: Pascalov trokut modulo 2

Primjetimo da redovi čije rubove čini po jedna jedinica sa svake strane, a između njih se nalazi niz nula (osim u 2. redu u kojem rubovi čine cijeli red) daju Fermatove brojeve. Zaista:

$$\begin{aligned} 11 &= 3 \\ 101 &= 5 \\ 10001 &= 17 \\ 10000001 &= 257 \\ 1000000000000001 &= 65537. \end{aligned}$$

Ako sada "zacrnimo" mjesta jedinice, i ostavimo bijelo na mjestima 0, u prvih 31 red dobivamo pravilne poligone s prostim brojem stranica koje znamo konstruirati:



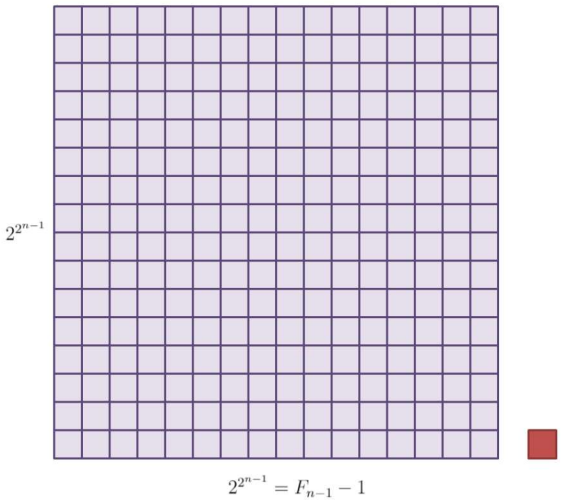
Slika 9: Geometrijska interpretacija Pascalovog trokuta modulo 2 (trokut Sierpińskog)

[5]Slike s ove stranice preuzete su iz [5]

3.2. Geometrijska interpretacija svojstava Fermatovih brojeva

Iako smo već naveli i dokazali svojstva Fermatovih brojeva, u ovom poglavlju neka od njih objasnit ćemo koristeći se njihovom geometrijskom interpretacijom.

Prisjetimo se, Teorem 1.1 tvrdi da za $n \geq 1$, $F_n = (F_{n-1} - 1)^2 + 1$.
Geometrijski, ovaj teorem tumačimo na način da je svaki Fermatov broj F_n jednak površini kvadrata duljine stranice $F_{n-1} - 1$ uvećanoj za jedinični kvadrat.



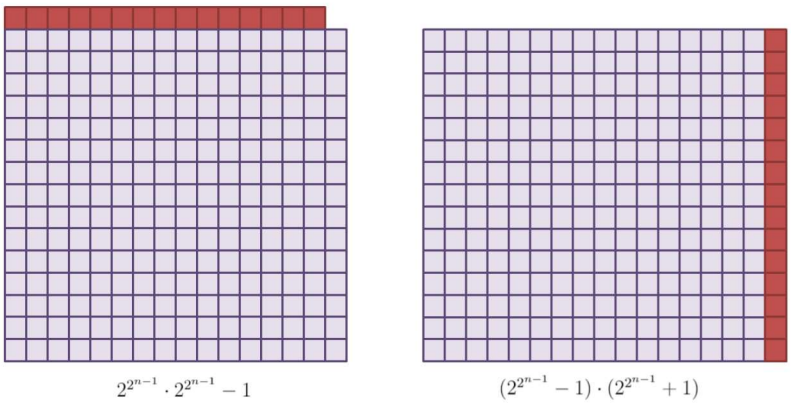
Slika 10: Geometrijska interpretacija Teorema 1.1[6]

Drugo svojstvo (Teorem 1.2) govori da vrijedi $F_n = F_0 \cdots F_{n-1} + 2$.
Kako bismo ovo svojstvo interpretirali geometrijski, osvrnut ćemo se na prethodnu jednakost:

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

Ako s obje strane te jednakosti dodamo -2 dobivamo:

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



Slika 11: Geometrijska interpretacija Teorema 1.2

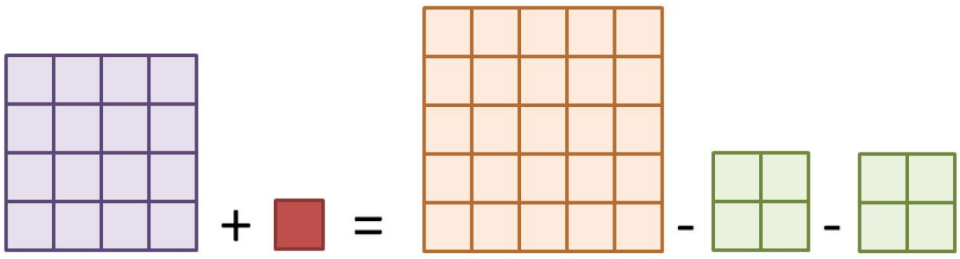
[6]Slike iz ovog dijela su preuzete iz [1]

Dakle, $F_n - 2$ predstavlja površinu kvadrata stranice F_{n-1} umanjenu za jedinični kvadrat. Njegove jedinične kvadratne blokove možemo prerasporediti tako da dobijemo pravokutnik (Slika 11).

Teorem 1.5 kaže: $F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$.
Geometrijski govoreći, svaki Fermatov broj F_n predstavlja površinu kvadrata duljine stranice F_{n-1} umanjenu za dvije površine kvadrata duljine stranice $F_{n-2} - 1$. Pogledajmo na konkretnom primjeru.

Primjer 3.3. *Za* $F_2 = 17$ *imamo*

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



Slika 12: Geometrijska interpretacija Teorema 1.5 za $F_2 = 17$

4. Mersennovi i Fermatovi brojevi

4.1. Veza između Mersennovih i Fermatovih brojeva

Definicija 4.1. *Brojevi oblika 2^n-1 nazivaju se Mersennovi brojevi, gdje je n prirodan broj.*

Brojevi ovog oblika nazvani su prema francuskom redovniku i matematičaru s kraja 16. i početka 17. stoljeća, Marinu Mersennu.
Mersenne i Fermat komunicirali su putem pisama, raspravljajući o matematičkim problemima, a tema njihovih rasprava često je bila upravo prostost brojeva oblika 2^n-1 i 2^n+1.

U nekim definicijama Mersennovih brojeva se zahtjeva da je n prost broj. No, kao i u slučaju Fermatovih brojeva, ako promatramo samo proste brojeve tog oblika, svejedno je koje definicije se držimo, što dokazuje sljedeći teorem.

Teorem 4.1. *Mersennov broj $M_n = 2^n - 1$ je prost samo ako je n prost.*

Dokaz. Vrijedi

$$2^{ab} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a}),$$

gdje je $a > 1$ neparan prirodan broj. Slijedi, ako je $n = ab$ složen, onda je $M_n = 2^n - 1$ djeljiv s $2^a - 1$, što je različito od 1. □

Sljedeća dva teorema dovode u vezu Mersennove brojeve i prostost pripadnih Fermatovih brojeva. Navedimo najprije definiciju pseudoprostih brojeva.

Definicija 4.2. *Ako je n neparan složen broj, te a cijeli broj za koji vrijedi $(n, a) = 1$ i $a^{n-1} \equiv 1 \pmod{n}$, kažemo da je n pseudoprost u bazi a.*

Lema 4.1. *Ako je p prost, onda su svi Mersennovi brojevi M_p prosti ili pseudo prosti u bazi 2.*

Dokaz. Neka je $M_p = 2^p - 1$ Mersennov broj, gdje je p prost. Ako je M_p složen, onda je p neparan. Zbog Malog Fermatovog teorema vrijedi

$$\frac{M_p - 1}{2} = 2^{p-1} \equiv 0 \pmod{p}.$$

Dakle, $\frac{M_p-1}{2} = kp$ za prirodni broj k. Slijedi

$$M_p = 2^p - 1 \mid 2^{kp} - 1 = 2^{\frac{M_p-1}{2}} - 1.$$

Ekvivalentno je napisati

$$2^{\frac{M_p-1}{2}} \equiv 1 \pmod{M_p}$$

iz čega slijedi

$$2^{M_p-1} \equiv 1 \pmod{M_p},$$

čime je tvrdnja dokazana. □

Teorem 4.2. *Neka je p prost broj takav da vrijedi $p \equiv 3 \pmod 4$. Tada je Fermatov broj F_p prost ako i samo ako je $M_p^{\frac{F_p-1}{2}} \equiv -1 \pmod{F_p}$, gdje je M_p pripadni Mersennov broj.*

Dokaz. Prema Teoremu 1.16, dovoljno je pokazati da je $\left(\frac{M_p}{F_p}\right) = -1$. Prema Lemi 4.1,

$$2^{2^p-2} \equiv 1 \pmod{M_p}.$$

Kada pomnožimo obje strane kongruencije s 2, dobivamo

$$2^{2^p-1} \equiv 2 \pmod{M_p}.$$

Iz toga slijedi

$$F_p = 2 \cdot 2^{2^p-1} + 1 \equiv 5 \pmod{M_p}.$$

Nadalje, kako je $p \equiv 3 \pmod 4$,

$$M_p = 2^p - 1 = 2^{4k+3} - 1 = 8 \cdot 2^{4k} - 1 = 3 \cdot 1 - 1 = 2 \pmod 5.$$

Dakle, prema Teoremu 1.13,

$$\left(\frac{M_p}{F_p}\right) = \left(\frac{F_p}{M_p}\right) = \left(\frac{5}{M_p}\right) = \left(\frac{M_p}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

□

Teorem 4.3. *Neka je p prost broj takav da $p \equiv 3$ ili $5 \mod 8$. Tada je Fermatov broj F_{p+1} prost ako i samo ako $M_p^{\frac{F_{p+1}-1}{2}} \equiv -1 \pmod{F_{p+1}}$, gdje je M_p pripadni Mersennov broj.*

Dokaz. Prema Teoremu 1.16, dovoljno je pokazati $\left(\frac{M_p}{F_{p+1}}\right) = -1$. U Teoremu 4.2 smo pokazali da je $F_p \equiv 5 \pmod{M_p}$. Nadalje, zbog Teorema 1.1 vrijedi

$$F_{p+1} = (F_p - 1)^2 + 1 = 4^2 + 1 \equiv 17 \pmod{M_p}.$$

Ako pretpostavimo $p \equiv 3 \pmod 8$, vrijedi

$$M_p = 2^{8k+3} - 1 = 8 \cdot 16^{2k} - 1 \equiv 8 - 1 = 7 \pmod{17}.$$

Dakle,

$$\left(\frac{M_p}{F_{p+1}}\right) = \left(\frac{F_{p+1}}{M_p}\right) = \left(\frac{17}{M_p}\right) = \left(\frac{M_p}{17}\right) = \left(\frac{7}{17}\right) = -1.$$

Sada, ako pretpostavimo da je $p \equiv 5 \pmod 8$, onda je

$$M_p = 2^{8k+5} - 1 \equiv 2^5 - 1 = -1 \equiv 14 \pmod{17}.$$

Dakle,

$$\left(\frac{M_p}{F_{p+1}}\right) = \left(\frac{M_p}{17}\right) = \left(\frac{14}{17}\right) = -1.$$

□

Literatura

[1] Lj. Bačić, *Fermatovi brojevi*, Osječki matematički list 13 (2013), 21-31.

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

[3] *Encyclopædia Britannica, Pierre de Fermat*,
URL: `https://www.britannica.com/biography/Pierre-de-Fermat`

[4] C. F. Gauss, *Mathematisches Tagebuch 1796-1814. Leipzig: Ostwalds Klassiker der exacten Wissenschaften 256*, (Gauß, Werke, Band 10), 1976.

[5] M. Křížek, F. Luca, L. Somer, *17 Lectures on Fermat Numbers From Number Theory to Geometry*, Canadian Mathematical Society, 2001.

[6] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište J.J. Strossmajera u Osijeku, 2013.

[7] *Opća enciklopedija Jugoslavenskog leksikografskog zavoda*, Grafički zavod Hrvatske, Zagreb, 1977.

[8] *Proth Search Page*,
URL: `http://www.prothsearch.com/fermat.html#Search`

[9] C. Tsang, *Fermat numbers*, University of Washington, 2010.
URL: `https://wstein.org/edu/2010/414/projects/tsang.pdf`

[10] 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., 1, (1836), 366-372.

[11] *Wikipedia, Pierre de Fermat*,
URL: `https://hr.wikipedia.org/wiki/Pierre_de_Fermat`

[12] *Wolfram Math World, Fermat Number*,
URL: `http://mathworld.wolfram.com/FermatNumber.html`