Pravilni sedamnaesterokut

Fabijančić, Krešimir

Master's thesis / Diplomski rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:161274

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Krešimir Fabijančić

PRAVILNI SEDAMNAESTEROKUT

Diplomski rad

Osijek, 2017.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Krešimir Fabijančić

PRAVILNI SEDAMNAESTEROKUT

Diplomski rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2017.

zaručnici Mateji, mami Slavici i sestri Nadi
Si consistant adversum me castra, non timebit cor meum. Ps. 27,3

Sadržaj

Uvod

Još od antike su geometrijske konstrukcije bile privlačne matematičarima. Konstrukcije figura i dužina bile su ograničene instrumentima. Zahtijevalo se da konstrukcije budu izvođene isključivo ravnalom i šestarom na način da ravnalo bude jednobridno bez mjernih oznaka. Za šestar se čak zahtijevalo da se ne smije koristiti za označavanja udaljenosti, odnosno prenošenje dužina, već se pretpostavljalo da se mora sklopiti kada nije u procesu crtanja kružnice. Platon je zahtijevao upotrebu isključivo šestara pri konstrukcijama. Metode konstrukcija pravilnih n-terokuta dao je Euklid ali samo za $n = 2, 3, 5$, te za udvostručeni broj stranica konstruiranog n-terokuta. Prvi matematičar koji je napravio značajan pomak pri konstrukciji pravilnih n-terokuta bio je Carl Friedrich Gauss koji je pokazao za koje sve vrijednosti prirodnog broja n je pravilni n-terokut konstruktibilan.

U prvom poglavlju dana je kraća Gaussova biografija i značajnija dostignuća na području matematike iako ih ima još mnogo koja su možda i značajnija.

Drugo poglavlje donosi kratak pregled konstrukcija - elementarnih i algebarskih onako kako su poznate još od antike. Dani su aksiomi konstruktivne geometrije te iskaz teorema o konstruktibilnosti algebarskih izraza.

Treće poglavlje donosi poveznicu kompleksnih brojeva i konstrukcije pravilnih n-terokuta preko n-tih korijena iz jedinice. Pokazuje se kako je za konstrukciju pravilnog n-terokuta dovoljno moći konstruirati $\cos\frac{2\pi}{n}$ što je povezano s rješavanjem jednadžbe oblika $x^n - 1 = 0$. Opisuje se kako je Gauss došao do konstrukcije pravilnog sedamnaesterokuta i do konstrukcije pravilnih n-terokuta općenito te kako je iskoristio prijašnje poznate rezultate na vrlo lukav način.

Zadnje, četvrto poglavlje povezuje Gaussov teorem o konstrukciji pravilnih n-terokuta s algebarskim strukturama i Fermatovim brojevima. Daje se kako iskaz tako i dokaz teorema koji odgovara na pitanje za koji prirodni broj n je pravilni n-terokut konstruktibilan.

1 Carl Friedrich Gauss

Potkraj 18. stoljeća Njemačka je preuzela vodstvo kao središte matematičkih zbivanja. Najveći matematičar modernog doba, Carl Friedrich Gauss (1777. - 1855.), je bio toliki veliki Nijemac da Njemačku nije napuštao nikada u svom životu. Gauss je rođen u siromašnoj obitelji i roditelji su mu bili nepismeni. Otac ih je uspio izvući iz siromaštva napornim poslovima klesara, vrtlara, kopanjem kanala te nadzornika u jednoj zidarskoj tvrtki u rodnom Braunschweigu. Da je bilo po očevoj volji, Gauss bi slijedio obiteljske poslove i postao vrtlar ili zidar. Protiv svoje volje i nakon mnogo nagovaranja otac ga daje u školu jer je bio vrlo nadaren. Vrlo brzo se Gauss počeo isticati u školi i njegova nadarenost za matematiku je dolazila na vidjelo. Njegove aritmetičke sposobnosti su toliko prerasle njegove školske kolege da su u dobi od 9 godina nastavnici priznali kako ga nemaju više čemu poučavati. Govori se da je već na prvom satu aritmetike Gauss zapanjio nastavnika gotovo odmah zbrojivši sve brojeve od 1 do 100 što se činilo kao mukotrpan i dugačak posao. Sam Gauss kasnije je priznao da je uočio uzorak:

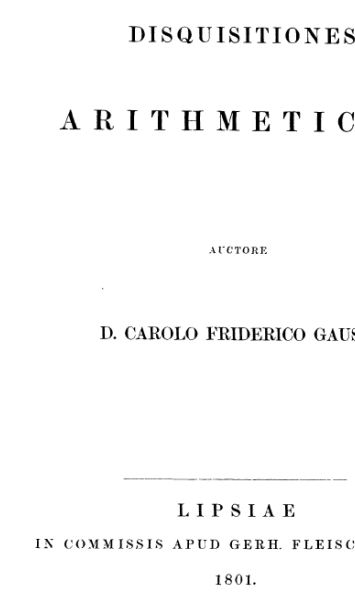
Slika 1: Carl Friedrich Gauss

$$1 + 100 = 101,\ 2 + 99 = 101,\ 3 + 98 = 101,\ \ldots\ ,\ 50 + 51 = 101.$$

Jer je ukupno 50 parova brojeva od kojih svaki par daje sumu 101, suma svih brojeva mora biti $50 \cdot 101 = 5\,050$. Ovim principom dolazimo i do općenite formule za sumu prvh n prirodnih brojeva: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Njegova briljantnost je privukla pažnju uglednih ljudi, osobito Ferdinanda vojvode od Braunschweiga koji je bio Gaussov zaštitnik i mecena kroz dugi niz godina. Vojvodina velikodušnost je omogućila Gaussu pohađanje najboljih škola te na kraju i sveučilišta u Göttingenu gdje se zadržao samo tri godine te otišao bez diplome po koju se vratio nakon godinu dana. Kada je došao na sveučilište, još uvijek je bio neodlučan - postati matematičar ili loviti karijeru s klasičnim jezicima. 30. ožujak 1796. označio je prekretnicu u izboru studija. Toga dana, kad još nije napunio ni 20 godina, Gauss je došao do zapanjujućeg rezultata koji ga je obilježio kao matematičara.

Problem konstrukcija pravilnih poligona koristeći isključivo ravnalo i šestar je u svijetu matematike dugo ležao po strani. Naime, vjerovalo se da su antički matematičari iscrpili sve mogućnosti i da se već sve zna o konstrukcijama pravilnih poligona. Međutim, Gauss je pokazao da je moguće konstruirati pravilni poligon sa 17 strana što je bio prvi takav rezultat još od Euklida. Gauss je bio toliko ponosan na to otkriće da je želio da mu se na nadgrobni spomenik ukleše pravilni sedamnaesterokut. Iako mu nisu ispunili želju, ipak su uklesali zvijezdu sa sedamnaest krakova na spomeniku podignutom njemu u čast u njegovom rodnom mjestu. Navodno je klesar odbio uklesati pravilni sedamnaesterokut jer se bojao da se ta figura neće puno razlikovati od kružnice.


DISQUISITIONES

ARITHMETICAE

AUCTORE

D. CAROLO FRIDERICO GAUSS.

LIPSIAE

IN COMMISSIS APUD GERH. FLEISCHER Jun.

1801.

Slika 2: Početna stranica Gaussove knjige

Kasnije, u svojoj impresivnoj knjizi Disquisitiones Arithmeticae, koju je izdao 1801., Gauss daje dokaz da se pravilni poligon sa p strana (gdje je p neparan prost broj) može konstruirati ravnalom i šestarom ako je broj p oblika $2^{2^k}+1$. Za $k = 0, 1, 2, 3, 4$ dobivamo redom $p = 3, 5, 17, 257, 65\ 537$ što su sve prosti brojevi. Za $k = 5$ Euler je pokazao da broj $2^{2^5}+1$ nije prost i da sadrži faktor 641. Matematičari danas vjeruju da je $2^{2^k}+1$ složen broj za $k \geq 5$ iako za to ne postoji formalni dokaz.

U Göttingenu je Gauss studirao matematiku pod vodstvom profesora Abrahama Kastnera. Budući da Kastner nije pokazivao zanimanje za Gaussova istraživanja, Gauss je radio samostalno i neovisno o profesorima. Postoji priča koja kaže da je Gauss pokušao zainteresirati Kastnera za konstrukciju pravilnog sedamnaesterokuta ističući da je do konstrukcije došao tako što je riješio algebarsku jednadžbu sedamnaestog stupnja. Profesor je, tražeći način da se riješi Gaussa, jednostavno rekao da je takvo što nemoguće. Vrativši se sa sveučilišta u rodni grad, Gauss je pokušavao davati privatne poduke iz matematike ali to mu nije išlo za rukom. Stoga mu je vojvoda Ferdinand dao mirovinu kako bi se posvetio istraživačkom radu. U tom vremenu Gauss je napisao svoju doktorsku disertaciju na temelju koje mu je dan doktorat bez ikakvog dodatnog ispitivanja koje je bilo uobičajeno. Disertacija naslova: *"Novi dokaz teorema da svaka integrabilna racionalna funkcija jedne varijable može biti rastavljena na realne faktore prvog ili drugog stupnja"* daje prvi značajan dokaz fundamentalnog teorema algebre, iako nije zapisan današnjim matematičkim jezikom. Fundamentalni teorem algebre kaže da svaka algebarska jednadžba n-tog stupnja ima barem jedno kompleksno rješenje. Nakon disertacije Gaussovi uspjesi su se nizali jedan za drugim. Ideje iz teorije brojeva još od studentskih dana skupio je i objavio u knjizi Disquisitiones Arithmeticae u kojoj se, između ostalog, nalaze i rješenja jednadžbe sedamnaestog stupnja kojima je moguće konstruirati pravilni sedamnaesterokut. Ova knjiga dala mu je neoborivu titulu matematičkog genija.

Do sredine 19. st. matematika je bila uvelike razvijena i podijeljena u više područja za koje su se pojedini matematičari specijalizirali. Gauss je bio zadnji potpuni matematičar i nije pretjerano reći da je imao udjela u gotovo svim područjima matematike. Njegova predanost matematici dala mu je titulu *princ matematike* rame uz rame s Arhimedom i Isaacom Newtonom. Iako je volio svu matematiku, Gaussu je najveće polje interesa bila teorija brojeva. U svojoj knjizi Disquisitiones Arithmeticae prvi je uveo pojam kongruencije i uveo simbol "$\equiv$". U znak zahvalnosti vojvodi Ferdinandu za sve što mu je omogućio, Gauss je knjigu Disquisitiones Arithmeticae posvetio upravo njemu. U svojoj posveti Gauss je između ostalog napisao: "*Da nije bilo Vaše nesebične potpore mojim studijima, ne bih se mogao posvetiti svojoj strasnoj ljubavi - proučavanju matematike.*".

2 Euklidske konstrukcije

Još od samih početaka matematike, ravnalo i šestar su korišteni kao geometrijski instrumenti. Pod pojmom *ravnalo* podrazumijevamo da se radi o jednobridnom ravnalu bez mjernih oznaka. Platon (429. – 347. pr. Kr.) je pri rješavanju konstruktivnih zadaća koristio isključivo ravnalo i šestar. Nakon njega je Euklid (300. pr. Kr.) izdao zbirku od 13 knjiga pod nazivom *Elementi* u kojima je sustavno obrađena sva do tada poznata geometrija, osim krivulja drugog reda. U Elementima Euklid daje aksiome kojima opisuje mogućnosti izvođenja konstrukcija ravnalom i šestarom. Ti aksiomi su poznati kao aksiomi ravnala i šestara.

Euklidskim konstrukcijama nazivat ćemo one konstrukcije koje su izvodive isključivo šestarom i ravnalom bez mjernih oznaka. Također, za neku figuru ćemo reći da je konstruktibilna ako ju se može konstruirati pomoću konačnog broja fundamentalnih konstrukcija.

Aksiomi konstruktivne geometrije

AKSIOM 1. *Svaka zadana figura je konstruirana.*

AKSIOM 2. *Ako su konstruirane dvije ili više figura, tada je konstruirana i njihova unija.*

AKSIOM 3. *Ako su konstruirane dvije figure, tada se može ustanoviti je li njihova razlika prazan skup ili ne i u slučaju da ta razlika nije prazan skup ta razlika je konstruirana.*

AKSIOM 4. *Ako su konstruirane dvije ili više figura tada se može ustanoviti je li njihov presjek prazan skup ili ne i u slučaju da taj presjek nije prazan skup taj presjek je konstruiran.*

AKSIOM 5. *Ako je dana neprazna figura tada je moguće konstruirati točku koja pripada toj figuri.*

Aksiomi ravnala

Ravnalom se mogu vršiti ove konstrukcije:

AKSIOM 6 (R1)**.** *Ravnalom možemo konstruirati dužinu ako su dani krajevi te dužine.*

AKSIOM 7 (R2)**.** *Ravnalom možemo konstruirati polupravac s danom početnom točkom koji prolazi kroz drugu danu točku.*

AKSIOM 8 (R3)**.** *Ravnalom možemo konstruirati pravac koji prolazi kroz dvije dane točke.*

Aksiomi šestara

Šestarom se mogu vršiti ove konstrukcije:

AKSIOM 9 (S1)**.** *Šestarom možemo konstruirati kružnicu ako je dano njeno središte i polumjer.*

AKSIOM 10 (S2)**.** *Šestarom možemo konstruirati bilo koji od dva luka kružnice određen s dvije točke kružnice ako je dano središte kružnice i krajnje točke tog luka.*

Fundamentalne konstrukcije

Pod fundamentalne konstrukcije ubrajamo aksiome ravnala (**R1**, **R2**, **R3**), aksiome šetara (**S1**, **S2**) i dodatno

- konstrukciju konačnog broja zajedničkih točaka dvaju danih likova
- konstrukciju točke koja pripada danom liku.

Elementarne konstrukcije

1. simetrala dužine
2. simetrala kuta
3. prenošenje dužine
4. prenošenje kuta
5. paralela s danim pravcem povučena kroz danu točku
6. okomica povučena iz dane točke na dani pravac
7. dijeljenje dužine u zadanom omjeru
8. konstrukcija trokuta korištenjem poučaka o sukladnosti trokuta
   ($S-S-S$, $S-K-S$, $K-S-K$, $S^{>}-S-K$)

Kao što možemo vidjeti, ravnalom i šestarom smo vrlo ograničeni i možemo izvršiti samo neke konstrukcije. Pretpostavimo stoga da su nam zadane dužine određene duljinama $a, b, c, \ldots, k$. Treba konstruirati dužinu duljine x dane algebarskim izrazom $x = f(a, b, c, \ldots, k)$. U ovom slučaju (uz određene uvjete) kažemo da smo konstruirali dani izraz x. Varijable u ovom izrazu su duljine dužina, a kako su to uvijek pozitivne vrijednosti to i izraz x ima smisla samo ako poprima pozitivne vrijednosti.

Definicija 2.1. *Za izraz $f(d_1, d_2, d_3, \ldots, d_n)$ kažemo da je homogen izraz dimenzije n ako za svaki $k \in \mathbb{N}$ vrijedi*

$$f(kd_1, kd_2, kd_3, \ldots, kd_n) = k^n f(d_1, d_2, d_3, \ldots, d_n).$$

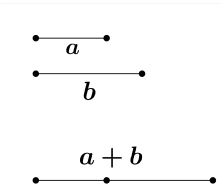
Za konstruiranje homogenih izraza dimenzije 1 nemamo problema, međutim ako je homogeni izraz dimenzije različite od 1 ili je nehomogen, tada je potrebno uvesti dužinu jedinične duljine $e = 1$. Svaki zadani algebarski izraz najprije je potrebno rastaviti na najjednostavnije algebarske izraze koristeći konačan broj zbrajanja, oduzimanja, množenja i dijeljenja te određivanja drugih korijena. Bitno je da rastav bude takav da svaki pojedini član znamo konstruirati (konstrukcije ćemo navesti kasnije). Prirodno je postaviti pitanje kada se pomoću ravnala i šestara može konstruirati izraz $f(d_1, d_2, d_3, \ldots, d_n)$? Odgovor daje idući teorem.

Teorem 2.1. *Svaki pozitivni algebarski izraz $f(d_1, d_2, d_3, \ldots, d_n)$ koji se iz danih veličina $d_1, d_2, d_3, \ldots, d_n$ dobiva konačnim brojem racionalnih operacija (zbrajanje, oduzimanje, množenje, dijeljenje) i određivanjem drugih korijena može se konstruirati ravnalom i šestarom.*

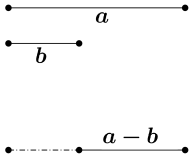
Uvodeći ovu, takozvanu algebarsku metodu konstruiranja, dobivamo malo veći opseg mogućih konstrukcija ravnalom i šestarom.

2.1 Najjednostavnije algebarske konstrukcije

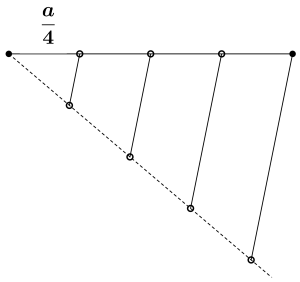
Među najjednostavnije algebarske konstrukcije ubrajamo konstrukcije zbroja, razlike, dijeljenje dužine na n jednakih dijelova te određivanje drugog korijena. Ostale algebarske konstrukcije se svode na ove (uključujući i konstrukcije izraza za koje uvodimo dužinu jedinične duljine). Napomenimo samo da se konstrukcija izraza $x = \dfrac{a^2}{c}$ svodi na konstrukciju sa Slike 6 za $b = a$, $x = \sqrt{a^2 - b^2}$ za $a > b$ se svodi na konstrukciju sa Slike 7, te $x = \sqrt{n} \cdot a$ se svodi na konstrukciju sa Slike 8. Treba imati na umu da konstrukcije u kojima se pojavljuje drugi korijen nisu jedinstvene. Na primjer, izraz $x = a\sqrt{5}$ možemo konstruirati kao što je prikazano na Slici 8 za $a = 5a$ te $b = a$, ali možemo napraviti i rastav prema Pitagorinom poučku $(2a)^2 + a^2 = (\sqrt{5}a)^2$ što se konstruira kao što je prikazano na Slici 7.



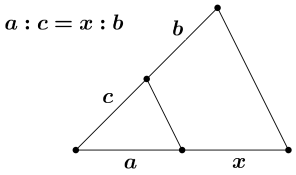
Slika 3: $x = a + b$



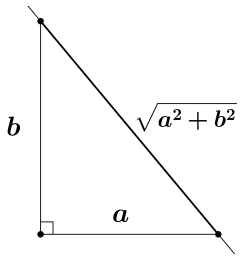
Slika 4: $x = a - b$



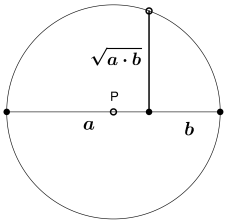
Slika 5: $x = \dfrac{a}{n}, n \in \mathbb{N}$



Slika 6: $x = \dfrac{a \cdot b}{c}$



Slika 7: $x = \sqrt{a^2 + b^2}$



Slika 8: $x = \sqrt{a \cdot b}$

Konstruktivna zadaća

Pri izvođenju geometrijskih konstrukcija nezaobilazan pojam su konstruktivne zadaće. Konstruktivna zadaća sastoji se u konstrukciji neke figure s danim instrumentima ako su dane druge figure i opisani odnosi između elemenata tražene figure i danih figura.

Rješenje konstruktivne zadaće je svaka figura koja zadovoljava sve uvjete koje mora zadovoljavati tražena figura. Naći rješenje konstruktivne zadaće znači svesti danu zadaću na konačan niz fundamentalnih konstrukcija danih instrumenata nakon čega smatramo da je tražena figura i sama konstruirana. Konstruktivna zadaća općenito ima više rješenja.

Pri rješavanju konstruktivne zadaće slijedimo određeni niz rješavanja:

$$analiza \rightarrow konstrukcija \rightarrow dokaz \rightarrow rasprava$$

U analizi tražimo način rješavanja zadaće. Ispitujemo vezu dane i tražene figure uz pomoć pomoćnih figura koje se najprije konstruiraju. U analizi se koriste ranije poznati teoremi i konstrukcije te se obično radi skica.

Konstrukcija se radi na temelju analize. Istakne se niz osnovnih i fundamentalnih konstrukcija ili poznatih konstrukcija i ranije riješenih zadaća. Taj niz daje traženu figuru.

Dokazom pokazujemo da dobivena figura zadovoljava sve uvjete zadaće i da je svaki korak u konstrukciji moguć.

Rasprava obično odgovara na pitanja je li uvijek moguće izvršiti konstrukciju, koliko ima rješenja uz svaki mogući izbor danih elemenata,... Također ispitujemo sve moguće položaje danih elemenata koji mogu doći u obzir.

2.2 Pravilni poligoni

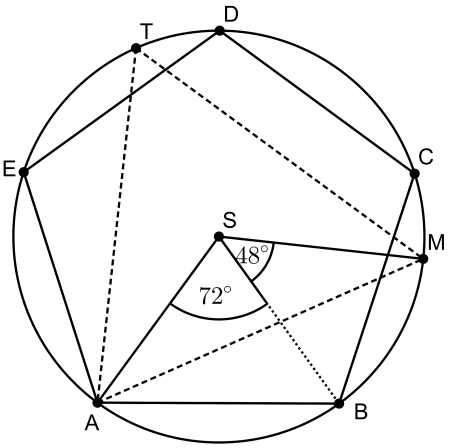
Još od Euklidovog doba poznato je koji mnogokuti su konstruktibilni. Zasigurno svatko tko je završio barem osnovnoškolsko obrazovanje vidio je (ako ne i upamtio) konstrukcije pravilnog trokuta, četverokuta i peterokuta.

Kako bi konstruirali pravilni $2n$-terokut iz pravilnog n-terkuta potrebno je povući simetrale svih stranica pravilnog n-terokuta. One će sijeći kružnicu opisanu pravilnom n-terokutu u točkama koje određuju pravilni $2n$-terokut. Dakle, ako krenemo od pravilnih trokuta, četverokuta i peterokuta možemo konstruirati poligone s $3, 6, 12, \ldots$ strana, $4, 8, 16, \ldots$ strana, $5, 10, 20, \ldots$ strana.

Međutim, što ako želimo konstruirati pravilni petnaesterokut? I to je moguće i također poznato još od antike.

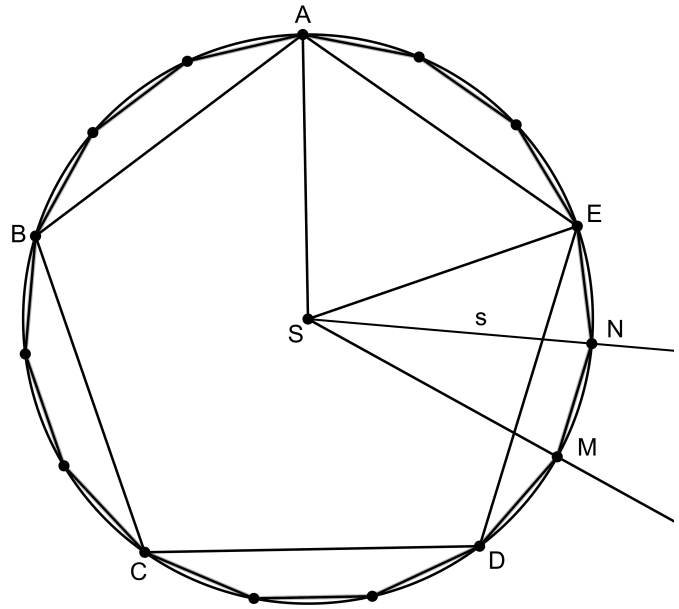
Zadatak. *Zadan je pravilni peterokut $ABCDE$ upisan kružnici $k(S, |SA|)$. Konstruirati pravilni petnaesterokut koji je upisan danoj kružnici.*

Analiza: Središnji kut pravilnog peterokuta iznosi $\alpha = 72°$. Ako bi u istoj kružnici konstruirali pravilne (jednakostranične) trokute (na poseban način) koji svaki sa danim peterokutom dijele po jedan vrh, dobili bi trisekciju središnjeg kuta pravilnog peterokuta. Odnosno, dobili bi središnji kut pravilnog n-terokuta od $\alpha' = 24°$ što u konačnici daje pravilni petnaesterokut.



Slika 9: Skica

Konstrukcija: Prema analizi i skici radimo konstrukciju:



Koraci konstrukcije:

1. $\overline{AS}$
2. $M \in k$, $\angle ASM = 120°$
3. s, s simetrala kuta $\angle ESM$
4. $s \cap k = N$
5. $\overline{MN}$ je stranica petnaesterokuta

Slika 10: Pravilni petnaesterokut

Dokaz: Ako uzmemo u obzir formulu za središnji kut pravilnog n-terokuta $\alpha = \dfrac{360°}{n}$, onda je kut $\angle ASE = \dfrac{360°}{5} = 72°$. Prema konstrukciji je $\angle ASM = 120°$, a to je središnji kut jednakostraničnog trokuta. Tada je

$$\angle ESM = \angle ASM - \angle ASE = 120° - 72° = 48°.$$

Kako simetrala kuta $\angle ESM$ dijeli taj kut na dva sukladna kuta, to je $\angle ESN = \angle NSM = 24°$. Prema $\alpha = \dfrac{360°}{n}$ je $n = \dfrac{360°}{24°} = 15$.
Jer su $\overline{SM}$ i $\overline{SN}$ polumjeri iste kružnice te $\angle NSM = \angle ESN$ prema poučku o sukladnosti trokuta $S - K - S$ je $\overline{MN} \cong \overline{NE}$. Analogno vrijedi i za ostale stranice petnaesterokuta. □

Rasprava: Rješenje zadaće je jedinstveno.

Sada iz petnaesterokuta možemo konstruirati mnogokut s $15, 30, 60 \ldots$ strana.

Ovoj listi konstruktibilnih pravilnih poligona koja se nije mijenjala gotovo 2000 godina, Gauss je nadodao pravilni sedamnaesterokut. I ne samo nadodao sedamnaesterokut već odgovorio na pitanje: "*Za koje vrijednosti $n \in \mathbb{N}$ je pravilni n-terokut konstruktibilan?*".

3 Konstrukcija pravilnih n-terokuta

Skup $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$, gdje i ima svojstvo $i^2 = -1$ se zove skup kompleksnih brojeva. Ako je $z = a + bi$, onda a nazivamo realni dio kompleksnog broja z te b nazivamo imaginarni dio kompleksnog broja z. Broj i nazivamo imaginarna jedinica.

Svaki kompleksni broj je potpuno zadan s dva realna broja i pri tome je važno koji je prvi (realni) a koji drugi (imaginarni). Obratno, svakom uređenom paru realnih brojeva (a, b) možemo pridružiti kompleksni broj $z = a + bi$. Tako je dano obostrano jednoznačno pridruživanje između skupova $\mathbb{C}$ i $\mathbb{R}^2$. To pridruživanje nam omogućava da se kompleksni brojevi crtaju u ravnini kao točke. Razlika je u tome što u ravnini u kojoj crtamo kompleksne brojeve točke možemo zbrajati i množiti. Ta ravnina ima posebno ime: kompleksna ili Gaussova ravnina.

Neka je u Gaussovoj ravnini na jediničnoj kružnici dana točka ξ. Neka ξ zatvara kut φ sa pozitivnim dijelom realne osi. Tada možemo pisati: $\xi = \cos\varphi + i\sin\varphi$. Ako je $\varphi = \dfrac{2k\pi}{n}$ za neke $k, n \in \mathbb{Z}$ prema pravilima za množenje kompleksnih brojeva je $\xi^n = 1$. Drugim riječima, ξ je kompleksno rješenje (korijen) jednadžbe $x^n - 1 = 0$. Za $k = 0, 1, 2, \ldots, n-1$ dobivamo n različitih rješenja (korijena) te jednadžbe.

Definicija 3.1. *Kažemo da je $\xi \in \mathbb{C}$ n-ti korijen iz jedinice ako je $\xi^n = 1$.*
Ako je ξ n-ti korijen iz jedinice onda je red *od ξ najmanji $k \in \mathbb{N}$ takav da je $\xi^k = 1$ i označavamo ga s $ord(\xi) = k$.*

Geometrijski gledano, n-ti korijeni iz jedinice su zapravo točke jednako raspoređene na trigonometrijskoj kružnici; svake dvije susjedne točke sa središtem zatvaraju jednaki središnji kut kružnice.

Kako bi konstruirali pravilni n-terokut dovoljno je konstruirati $\cos\dfrac{2\pi}{n}$, odnosno $\sin\dfrac{2\pi}{n}$. Budući da je kompleksni broj $\xi = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$ n-ti korijen iz jedinice, konstrukcija pravilnog n-terokuta u Gaussovoj ravnini povezana je s rješavanjem jednadžbe $x^n - 1 = 0$ u kompleksnim brojevima i prikazu rješenja u obliku konačnog broja racionalnih operacija i određivanja drugih korijena.

Primjer za $n = 5$ (pravilni peterokut)

Uzmimo da je $n = 5$. Neka je $\varphi = \dfrac{2\pi}{5}$ te $\xi = \cos\dfrac{2\pi}{5} + i\sin\dfrac{2\pi}{5}$ kompleksni broj koji predstavlja prvi vrh peterokuta nakon vrha 1. Pet vrhova peterokuta bit će u točkama $1, \xi, \xi^2, \xi^3, \xi^4$.

Primijetimo da je $\xi^4 = \xi^{-1}$, odnosno, ξ^4 je kompleksno-konjugirani par od ξ. Zato je:

$$\xi + \xi^4 = 2\cos\frac{2\pi}{5}.$$

S druge strane, ξ je korijen jednadžbe $x^5 - 1 = 0$. Izraz $x^5 - 1$ možemo faktorizirati kao

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1).$$

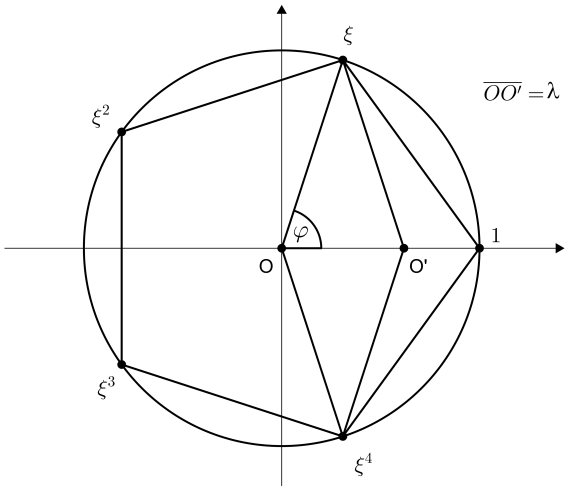
Budući da $\xi \neq 1$, on ne poništava prvi faktor što znači da poništava drugi faktor, tj. $\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$ što nam daje $\xi^4 + \xi^3 + \xi^2 + \xi = -1$. Neka je $\lambda = \xi + \xi^4$. Uzimajući u obzir da je $\xi^5 = 1$ slijedi da je $\lambda^2 = \xi^2 + 2 + \xi^3$. Sada zbrojimo λ i λ^2 te dobivamo:

$$\lambda^2 + \lambda = \xi^4 + \xi^3 + \xi^2 + \xi + 2 = 1.$$

Sada možemo zaključiti da je λ korijen jednadžbe $x^2 + x - 1 = 0$ koja ima rješenja $x_{1,2} = \dfrac{-1 \pm \sqrt{5}}{2}$. Kako je λ pozitivan realan broj, mora biti $\lambda = \dfrac{\sqrt{5}-1}{2}$. Sada možemo zaključiti da je

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$$

a to prema Teoremu 2.1 možemo konstruirati.



Slika 11: Pet korijena iz jedinice koji čine petrokut

3.1 Gaussov sedamnaesterokut

Povijesne knjige svjedoče da se mladi 19-godišnji Gauss probudio u rano jutro 30. ožujka 1796. jer mu je na pamet pala nevjerojatna metoda kako konstruirati pravilni sedamnaesterokut.

Ako bi samo trebalo pokazati da je pravilni sedamnaesterokut moguće konstruirati, rješenje je vrlo jasno i jednostavno. Uzmimo da je $2\pi = 17\varphi$. Kada bi se $\cos\varphi$ mogao izraziti konačnim brojem racionalnih operacija i određivanja drugih korijena, tada je moguće konstruirati dužinu te duljine. Kako smo već rekli, $\cos\varphi$ predstavlja x koordinatu točke na jediničnoj kružnici. Gauss je pronašao način kako $\cos\varphi$ izraziti konačnim brojem racionalnih operacija i određivanja drugih korijena. To je učinio rješavajući jednadžbu sedamnaestog stupnja $x^{17} - 1 = 0$ tražeći rješenja na poseban način.

Definirajmo:

$$\begin{aligned} a &= \cos\varphi + \cos 4\varphi \\ b &= \cos 2\varphi + \cos 8\varphi \\ c &= \cos 3\varphi + \cos 5\varphi \\ d &= \cos 6\varphi + \cos 7\varphi. \end{aligned}$$

Ovakve jednakosti nisu postavljene slučajno, i imaju veze s Gaussovom teorijom o rješavanju jednadžbi oblika $x^n - 1 = 0$ o kojoj će biti više u idućem poglavlju.

Nadalje, zbrojimo i označimo ovako:

$$\begin{aligned} e &= a+b \\ f &= c+d \end{aligned}$$

te zbrojimo i $e+f$. Rezultat zbrajanja bit će

$$e+f = \cos\varphi + \cos 2\varphi + \ldots + \cos 8\varphi.$$

Kako bi našli rezultat ovog zbrajanja, označimo $e+f = S_8$ te lijevu i desnu stranu pomnožimo s $2\sin\frac{\varphi}{2}$. Slijedi:

$$2S_8 \sin\frac{\varphi}{2} = 2\cos\varphi\sin\frac{\varphi}{2} + 2\cos 2\varphi\sin\frac{\varphi}{2} + \ldots + 2\cos 8\varphi\sin\frac{\varphi}{2}.$$

Primjenom adicijske formule $\sin x - \sin y = 2\cos\frac{x+y}{2}\sin\frac{x-y}{2}$ na svaki od članova desne strane, formula se znatno pojednostavi. Uvrštavajući $\varphi = \frac{2\pi}{17}$ u pojednostavljenu jednadžbu

$$S_8 = \frac{\sin\frac{17\varphi}{2} - \sin\frac{\varphi}{2}}{2\sin\frac{\varphi}{2}}$$

dobijemo

$$e+f = S_8 = -\frac{1}{2}.$$

Sada možemo računati produkte od a, b, c, d svaki sa svakim. Kraćim računom i uzimajući u obzir da vrijedi $\cos n\varphi = \cos(17-n)\varphi$, što se može provjeriti raspisivanjem desne strane, imamo slijedeće:

$$\begin{aligned} 2ab &= e+f = -\frac{1}{2} \\ 2ac &= 2a+b+d \\ 2ad &= b+c+2d \\ 2bc &= a+2c+d \\ 2bd &= a+2b+c \\ 2cd &= e+f = -\frac{1}{2}. \end{aligned}$$

Pokazat ćemo samo jedno množenje. Ostala se mogu izvesti analogno.

$$\begin{aligned} 2ab &= 2(\cos\varphi + \cos 4\varphi)(\cos 2\varphi + \cos 8\varphi) \\ &= 2\cos\varphi\cos 2\varphi + 2\cos\varphi\cos 8\varphi + 2\cos 4\varphi\cos 2\varphi + 2\cos 4\varphi\cos 8\varphi \\ &= (\cos 3\varphi + \cos\varphi) + (\cos 9\varphi + \cos 7\varphi) + (\cos 6\varphi + \cos 2\varphi) + (\cos 12\varphi + \cos 4\varphi). \end{aligned}$$

Zbog $\cos n\varphi = \cos(17-n)\varphi$ možemo uvesti supstituciju $\cos 9\varphi = \cos 8\varphi$ te $\cos 12\varphi = \cos 5\varphi$. Preslagivanjem članova i uvrštavanjem supstitucije imamo:

$$\begin{aligned} 2ab &= (\cos\varphi + \cos 4\varphi) + (\cos 2\varphi + \cos 8\varphi) + (\cos 3\varphi + \cos 5\varphi) + (\cos 6\varphi + \cos 7\varphi) \\ &= a+b+c+d \\ &= e+f = -\frac{1}{2}. \end{aligned}$$

Još nas zanima koliko je ef. Uvrštavajući izraze za e i f imamo:

$$\begin{aligned} 2ef &= 2(a+b)(c+d) \\ &= 2ac+2ad+2bc+2bd \\ &= 2a+b+d+b+c+2d+a+2c+d+a+2b+c \\ &= 4a+4b+4c+4d \\ &= 4(e+f) = -2 \end{aligned}$$

odakle slijedi da je $ef = -1$. Sada kada imamo $e+f = -\frac{1}{2}$ te $ef = -1$, zbog Viéteovih formula možemo zaključiti da su e i f korijeni kvadratne jednadžbe

$$x^2 + \frac{1}{2}x - 1 = 0.$$

Rješenja ove jednadžbe su $x_{1,2} = \dfrac{-1 \pm \sqrt{17}}{4}$. Koje rješenje je e a koje f procijenit ćemo numerički. Jer je

$$e = a + b = \cos\varphi + \cos 4\varphi + \cos 2\varphi + \cos 8\varphi \overset{\varphi=\frac{2\pi}{17}}{\approx} 0.7807764$$

možemo zaključiti da je $e = \dfrac{-1+\sqrt{17}}{4} \approx 0.7807764$, te da je $f = \dfrac{-1-\sqrt{17}}{4}$. Valja napomenuti da numerička procjena nije sredstvo dokaza, ali je dobro oruđe i u ovom slučaju može poslužiti pri zaključivanju.

Jer je $a + b = e$ te $ab = \dfrac{e+f}{2} = -\dfrac{1}{4}$, a i b su rješenja jednadžbe

$$x^2 - ex - \frac{1}{4} = 0.$$

Prema formuli za rješenja kvadratne jednadžbe imamo $x_{1,2} = \dfrac{1}{2}e \pm \sqrt{\dfrac{1}{4} + \dfrac{1}{4}e^2}$. Uvrštavanjem vrijednosti od e slijedi da je

$$x_{1,2} = -\frac{1}{8} + \frac{1}{8}\sqrt{17} \pm \frac{1}{8}\sqrt{34 - 2\sqrt{17}}.$$

Ovdje ćemo se opet poslužiti numeričkom procjenom kako bi odredili koje rješenje je a te koje rješenje je b. Jer je

$$a = \cos\varphi + \cos 4\varphi \overset{\varphi=\frac{2\pi}{17}}{\approx} 1.024741$$

možemo zaključiti da je

$$\begin{aligned} a &= -\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{34 - 2\sqrt{17}} \\ b &= -\frac{1}{8} + \frac{1}{8}\sqrt{17} - \frac{1}{8}\sqrt{34 - 2\sqrt{17}}. \end{aligned}$$

Na potpuno analogan način je

$$\begin{aligned} c &= -\frac{1}{8} - \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{34 + 2\sqrt{17}} \\ d &= -\frac{1}{8} - \frac{1}{8}\sqrt{17} - \frac{1}{8}\sqrt{34 + 2\sqrt{17}}. \end{aligned}$$

Konačno, jer je produkt[1] $\cos\varphi\cos 4\varphi = \frac{1}{2}c$ te $\cos\varphi + \cos 4\varphi = a$, $\cos\varphi$ i $\cos 4\varphi$ su rješenja jednadžbe

$$x^2 - ax + \frac{1}{2}c = 0.$$

Stoga je

$$\begin{aligned}\cos\varphi &= \frac{1}{2}a + \sqrt{\frac{1}{4}a^2 - \frac{1}{2}c}\\ \cos 4\varphi &= \frac{1}{2}a - \sqrt{\frac{1}{4}a^2 - \frac{1}{2}c}.\end{aligned}$$

Nadalje je

$$\begin{aligned}2a^2 &= 2\cos^2\varphi + 4\cos\varphi\cos 4\varphi + 2\cos^2 4\varphi\\ &= 2\frac{1+\cos 2\varphi}{2} + 2\cos 3\varphi + 2\cos 5\varphi + 2\frac{1+\cos 8\varphi}{2}\\ &= 2 + \cos 2\varphi + \cos 8\varphi + 2(\cos 4\varphi + \cos 5\varphi)\\ &= 2 + b + 2c.\end{aligned}$$

Budući da od samog početka tražimo vrijednost $\cos\varphi$, odnosno $\cos\frac{2\pi}{17}$, sada imamo:

$$\cos\frac{2\pi}{17} = \frac{1}{2}a + \sqrt{\frac{1}{4}a^2 - \frac{1}{2}c} = \frac{1}{2}a + \frac{1}{2}\sqrt{1 + \frac{1}{2}b - c}.$$

Nakon uvrštavanja i sređivanja, za $\cos\frac{2\pi}{17}$ se dobije vrijednost

$$\frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\right)$$

koja je zapisana konačnim brojem racionalnih operacija i određivanja drugih korijena, te je prema Teoremu 2.1 ovaj izraz konstruktibilan ravnalom i šestarom. Takav rezultat je dobio Gauss.

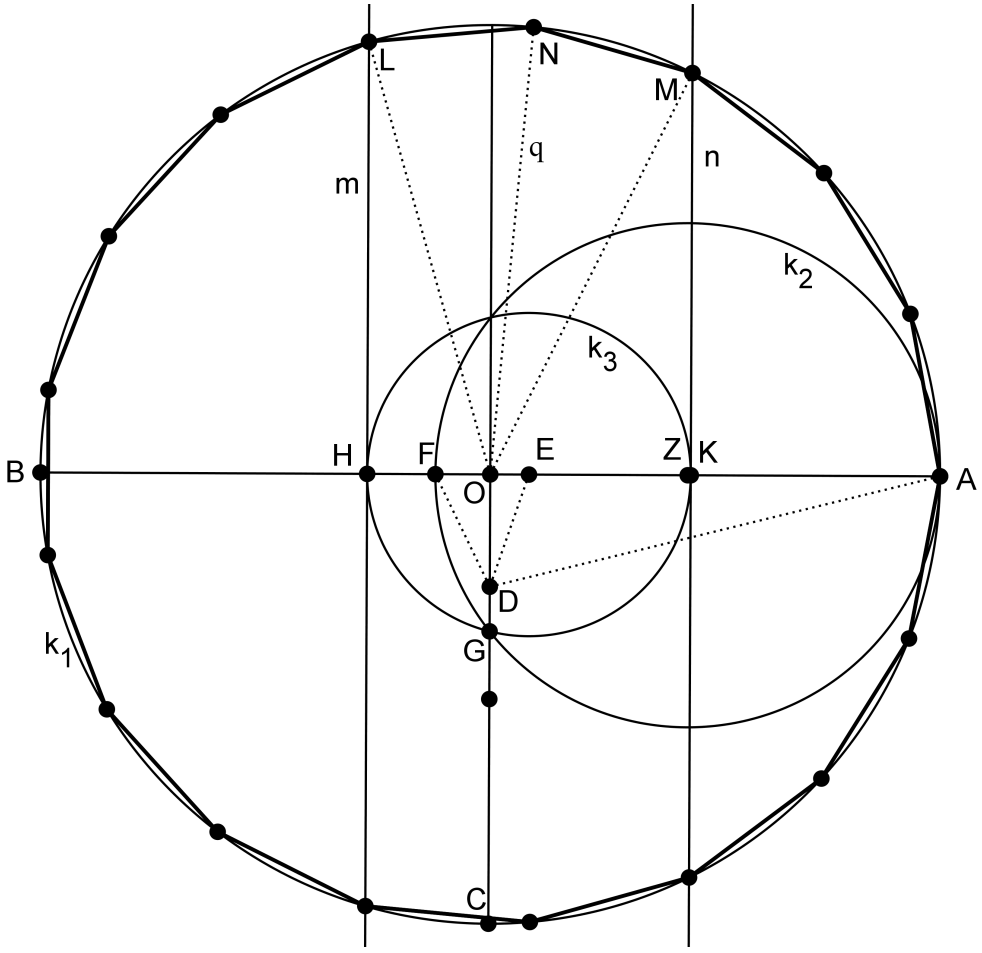
3.2 Konstrukcija pravilnog sedamnaesterokuta ravnalom i šestarom

Analiza: analizu smo proveli u prethodnom potpoglavlju, te ju s toga ne treba ponavljati. Konstruirat ćemo dobiveni izraz za $\cos\frac{2\pi}{17}$ koji će ujedno dati i stranicu pravilnog sedamnaesterokuta.

[1] $2\cos\varphi\cos 4\varphi = \cos(\varphi - 4\varphi) + \cos(\varphi + 4\varphi) = \cos 3\varphi + \cos 5\varphi = c$

Konstrukcija: najprije ćemo navesti korake konstrukcije a zatim sliku koja slijedi korake. Konstrukcija izraza za $\cos\frac{2\pi}{17}$ slijedi nakon dokaza.

1. $k_1(O, |OA|)$
2. $B \in k_1$,
   $\overline{AB}$ promjer kružnice k_1
3. $C \in k_1,\ \overline{OC} \perp \overline{AB}$
4. $D \in \overline{OC},\ |OD| = \frac{1}{4}|OC|$
5. $E \in \overline{OA},\ \angle ODE = \frac{1}{4}\angle ODA$
6. $F \in \overline{AB},\ \angle FDE = 45°$
7. Z polovište $\overline{AF}$
8. $k_2(Z, |AZ|),\ k_2 \cap \overline{OC} = G$
9. $k_3(E, |EG|),\ k_3 \cap \overline{AB} = H, K$
10. $m, n;\ H \in m,\ K \in n,$
    $m, n \perp \overline{AB}$
11. $m \cap k_1 = L,\ n \cap k_1 = M$
12. q simetrala kuta $\angle LOM$
    $q \cap k_1 = N$
13. $|LN|$ je stranica pravilnog sedamnaesterokuta



Slika 12: Konstrukcija pravilnog sedamnaesterokuta

Dokaz: Treba pokazati da je konstrukcijom dobiven kut $\angle LOM = \dfrac{4\pi}{17}$. Simetralom se taj kut raspolovi i dobije se traženi unutrašnji kut pravilnog sedamnaesterokuta $\dfrac{2\pi}{17}$.

Zapravo, treba pokazati da je $\pi - \angle HOL - \angle MOK = \dfrac{4\pi}{17}$ ili da je $\pi - \arccos\dfrac{|OH|}{|LO|} - \arccos\dfrac{|OK|}{|MO|} = \dfrac{4\pi}{17}$.

Bez smanjenja općenitosti, neka je konstrukcija rađena na jediničnoj kružnici. Tada je $|MO| = |LO| = 1$ jer su to polumjeri. Sada je još potrebno naći duljine $|OK|$ i $|OH|$. To ćemo učiniti primjenom trigonometrije pravokutnog trokuta. Svi razmatrani trokuti su pravokutni prema konstrukciji.

Iz $\triangle AOD$ slijedi $\angle ODA = \operatorname{arctg} 4$.

Prema konstrukciji je $\angle ODE = \dfrac{\operatorname{arctg} 4}{4}$. Označimo taj kut s α. Iz $\triangle ODE$ imamo da je $|OE| = \dfrac{1}{4}\operatorname{tg}\angle ODE$. Označimo tu dužinu sa b.

Prema konstrukciji je $\angle ODF = 45° - \alpha$. Iz $\triangle ODF$ slijedi da je $|OF| = \dfrac{1}{4}\operatorname{tg}(45° - \alpha)$. Označimo tu duljinu s c.

Prema konstrukciji je $|FA| = c + |OA| = c + 1$. Ovu duljinu označimo s d.

Prema konstrukciji je $|EG| = |EK|$ jer su to radijusi iste kružnice k_3. Stoga je dovoljno naći jedan od njih, npr. $|EG|$.

Primijetimo da je $|OZ| = \dfrac{1}{2}|AF| - |OF| = \dfrac{d}{2} - c$. Označimo ovaj izraz s e. Također je $|ZG|$ radijus kružnice k_2 pa je $|ZG| = \dfrac{d}{2}$. Označimo ovaj izraz s f.

Iz $\triangle ZOG$ možemo zaključiti da je $\cos\angle GZO = \dfrac{|OZ|}{|ZG|} = \dfrac{\frac{d}{2} - c}{\frac{d}{2}} = 1 - \dfrac{2c}{d}$. Označimo $\cos\angle GZO$ s g. Sada je $\angle GZO = \arccos g$. Taj kut označimo s h.

Sada možemo zaključiti da je $|OG| = f\sin h$. Označimo tu duljinu s i.

Iz $\triangle OGE$ je $\operatorname{tg}\angle OGE = \dfrac{|OE|}{|OG| = \frac{b}{i}}$. Odavdje je $\angle OGE = \operatorname{arctg}\dfrac{b}{i}$. Ovu vrijednost označimo s j.

Sada je $|EG| = \dfrac{|OE|}{\sin\angle OGE} = \dfrac{b}{\sin j} = |EK|$. Ovu vrijednost označimo s k.

Očito je $|OK| = |OE| + |EK| = b + k$. Ovu duljinu označimo s l.

Primjetimo da je $|HK| = 2k$ jer je to promjer kružnice kojoj je $|EK| = k$ polumjer. To nam daje $|OH| = |HK| - l$.

Sada je iz trokuta $\triangle MOK$ i $\triangle OLH$ lako naći vrijednosti kuteva $\angle MOK$ i $\angle HOL$. Konačno je $\pi - \arccos\dfrac{|OH|}{|LO|} - \arccos\dfrac{|OK|}{|MO|} = \dfrac{4\pi}{17}$ pa se bisekcijom tog kuta dobije traženi kut. □

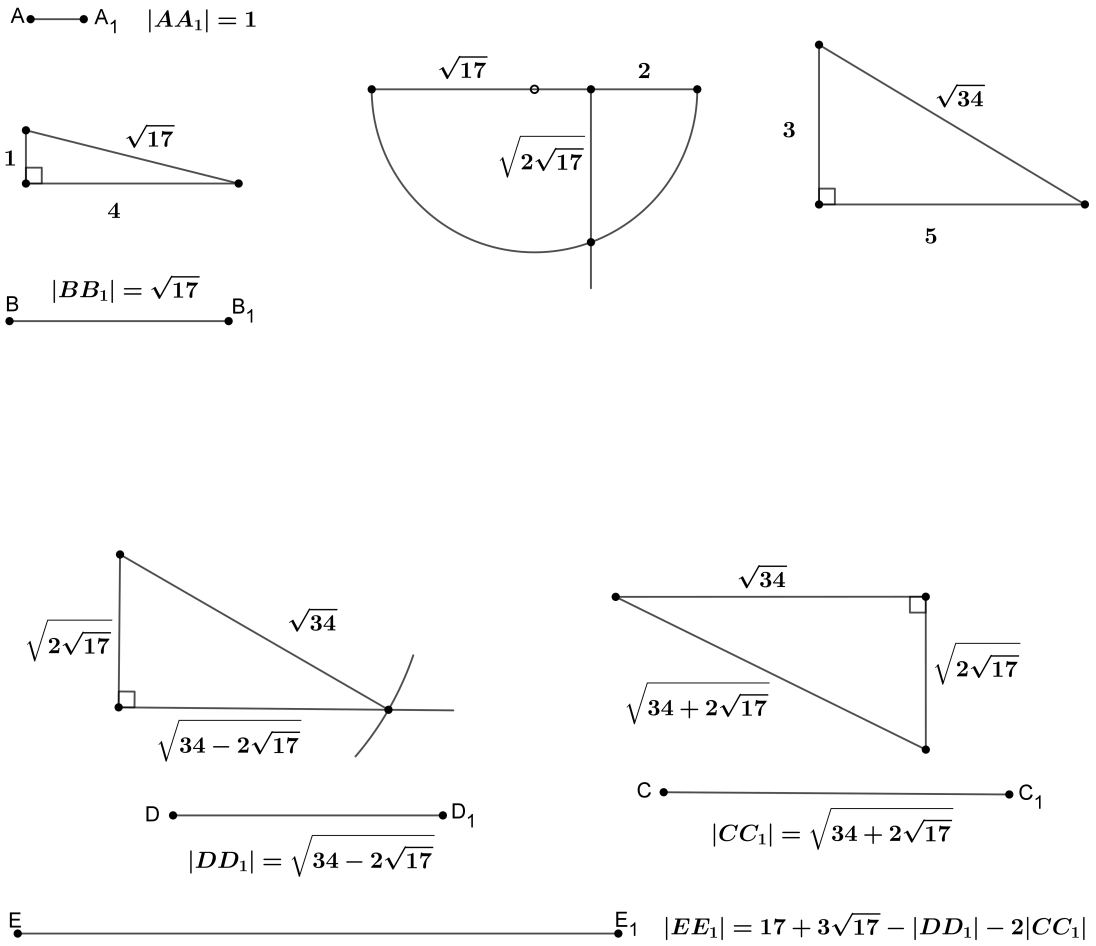
Rasprava: Rješenje je jedinstveno.

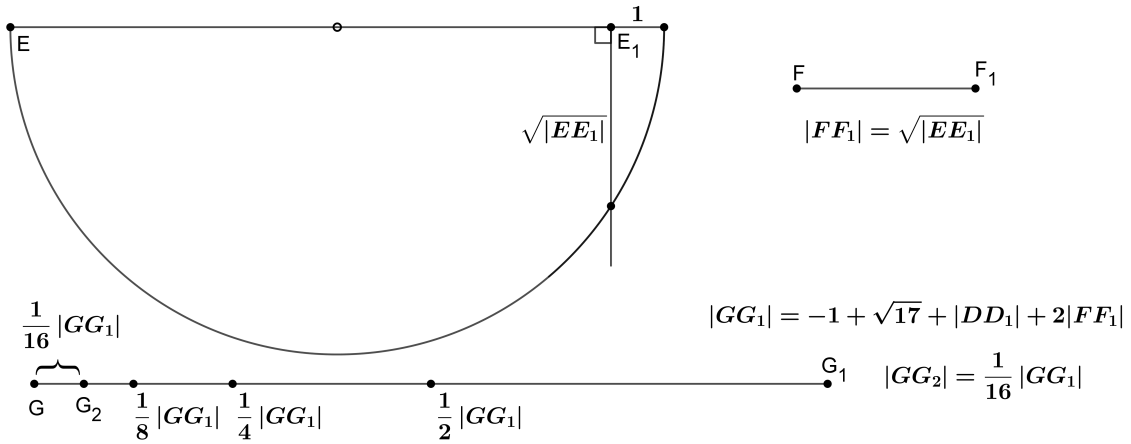
Slijedeća konstrukcija napravljena je direktno konstruiranjem dobivenog algebarskog izraza za $\cos\dfrac{2\pi}{17}$.

Analiza:

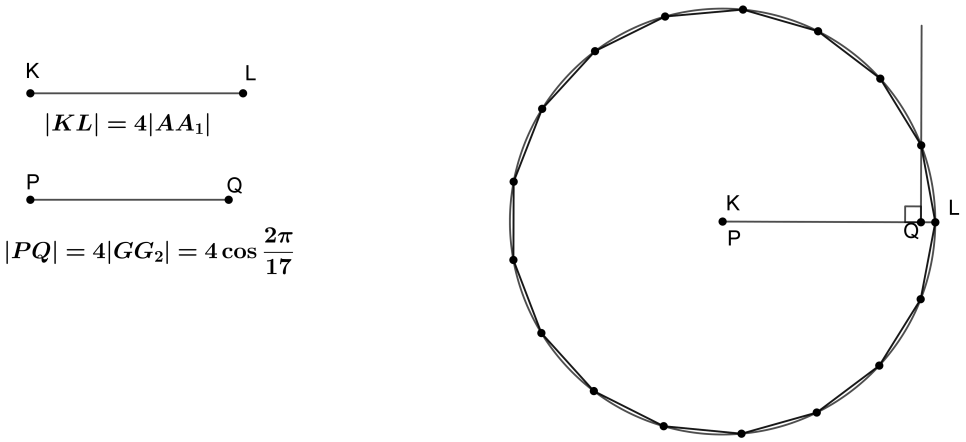
1. $|AA_1| = 1$
2. $|BB_1| = \sqrt{4^2+1^2} = \sqrt{17}$
3. $|CC_1| = \sqrt{34+2\sqrt{17}} = \sqrt{\sqrt{34}^2+\sqrt{2\sqrt{17}}^2}$
4. $\sqrt{34} = \sqrt{3^2+5^2}$
5. $|DD_1| = \sqrt{34-2\sqrt{17}}$
6. $|EE_1| = 17+3|BB_1|-|DD_1|-2|CC_1|$
7. $|FF_1| = \sqrt{|EE_1|}$
8. $|GG_1| = |BB_1|-1+|DD_1|+2|FF_1|$
9. $|GG_2| = \dfrac{1}{16}|GG_1|$

Konstrukcija: prema osnovnim algebarskim konstrukcijama iz poglavlja 2 slijedi konstrukcija:





Kako bi konstrukcija sedamnaesterokuta bila preglednija, povećajmo četiri puta duljinu jedinične dužine. Tada se i dobivena tražena duljina $|GG_2|$ poveća četiri puta.



Dokaz: Dokaz slijedi iz analize i konstrukcije te Teorema 2.1.

Rasprava: Rješenje je jedinstveno.

3.3 Gaussova teorija

Prije Gaussa su problem konstrukcija pravilnih n-terokuta razmatrali Vandermonde i Lagrange. Oni su nezavisno jedan od drugog predstavili zašto postoje opća rješenja jednadžbi trećeg i četvrtog stupnja. Zaključili su da je mogućnost pronalaska rješenja jednadžbe jednaka pronalasku vrijednosti određenih izraza vezanih za rješenja i to bez poznavanja samih rješenja.

Njihovu metodu pokušat ćemo objasniti na osnovu jednadžbe $x^2 - px + q = 0$. Neka su toj jednadžbi rješenja $x_1 = a$ i $x_2 = b$. Sada možemo reći da je $p = a + b$ te $q = ab$. Sada uzmimo neku funkciju koja ovisi o a i b. Neke funkcije, kao što je $f(r_1, r_2) = r_1 + r_2$ imaju istu vrijednost bez obzira koju varijablu označimo s r_1 a koje s r_2. Neka je zato $f(a, b) = f(b, a) = p$.

S druge strane, funkcije oblika $g(r_1, r_2) = r_1 - r_2$ imaju različite vrijednosti obzirom na to što je proglašeno za r_1 a što za r_2. Zato funkcija g može poprimiti jednu ili dvije

moguće vrijednosti: $a-b$ ili $a+b$. Kako bi se našle točne vrijednosti, Lagrange je dozvolio da k različitih vrijednosti budu korijeni jednadžbe k-tog stupnja. Odnosno, u našem primjeru, dvije vrijednosti za g bit će korijeni jednadžbe

$$(y-(a-b))(y-(b-a)) = y^2-(a-b)^2.$$

Očito je $(a-b)^2 = (a+b)^2-4ab$. Budući da znamo vrijednosti od $a+b$ i ab možemo odrediti da je

$$(a-b)^2 = p^2-4q$$

i to bez poznavanja rješenja a i b.

Dakle, možemo zaključiti da će dvije različite vrijednosti od $a-b$ biti rješenja jednadžbe $y^2-(p^2-4q)=0$. Odatle je $a-b=\sqrt{p^2-4q}$ ili $a-b=-\sqrt{p^2-4q}$. Ono što odaberemo neće praviti nikakvu razliku. Na primjer, mogli bi uzeti $a-b=\sqrt{p^2-4q}$. Da bi našli a i b treba nam još jedna jednadžba koju možemo dobiti kao $a+b=p$ što nam daje sustav

$$\begin{aligned} a+b &= p \\ a-b &= \sqrt{p^2-4q} \end{aligned}$$

iz čega slijedi da je $a=\dfrac{p+\sqrt{p^2-4q}}{2}$, $b=\dfrac{p-\sqrt{p^2-4q}}{2}$.

Obojica, Vandermonde i Lagrange, razmatrali su problem pronalaska n-tih korijena iz jedinice, odnosno rješavanje jednadžbi oblika $x^n-1=0$. Lagrange je spoznao da ako je n prost, sva rješenja jednadžbe mogu se izgenerirati sukcesivnim potenciranjem svakog korijena jednadžbe osim $x=1$. Tako je Lagrange ovu metodu upotrijebio kako bi našao korijene iz jedinice za $n=3,4,5,6$ dok je Vandermonde koristeći slične metode došao do $n=11$.

Kako smo već pokazali i konstruirali, možemo naslutiti kako je Gauss koristio slične metode kao i Vandermonde i Lagrange. Gaussovo otkriće bilo je bez presedana. On je izravno ali pametno upotrijebio Vandermondeove i Lagrangeove ideje.

Kako smo ranije naveli, n-ti korijeni iz jedinice su rješenja jednadžbe $x^n-1=0$. Očito je da svaki korijen r te jednadžbe mora zadovoljavati $r^n=1$. Ako je n najmanji takav da je $r^n=1$, onda kažemo da je r primitivni n-ti korijen iz jedinice. Na primjer, korijeni jednadžbe $x^4-1=0$ su $\pm 1, \pm i$. Budući da je $1^1=1$ te $(-1)^2=1$ onda ± 1 nisu primitivni. S druge strane, najmanja potencija od i i $-i$ koja daje 1 je 4, pa su $\pm i$ primitivni korijeni iz jedinice i njihove potencije generiraju sva rješenja:

$$i, \qquad i^2=-1, \qquad i^3=-i, \qquad i^4=1.$$

Općenito, Lagrange je napomenuo da ako je n prost tada jednadžba ima $n-1$ primitivnih korijena iz jedinice.

Također, ranije smo istaknuli da konstrukcija pravilnog n-terokuta odgovara konstrukciji korijena jednadžbe $x^n-1=0$. Zbog jednostavnosti, pristupit ćemo problemu tražeći rješenja jednadžbe $x^5-1=0$. Ova jednadžba ima jedan neprimitivni korijen $x=1$. Dijeleći jednadžbu s $x-1$ dobijemo jednadžbu

$$x^4+x^3+x^2+x+1=0$$

koju nazivamo ciklotomska jednadžba. Svi primitivni peti korijeni moraju zadovoljavati ovu jednadžbu.

Gauss je za razmatranje uzeo niz čiji je prvi član primitivni korijen, a svaki idući član je neka potencija prethodnog. Na primjer, ako uzmemo r i kubiramo ga sukcesivno, dobivamo niz

$$r, r^3, r^9, r^{27}, r^{81}, \ldots$$

Budući da je r korijen jednadžbe $x^5 - 1 = 0$, tada je $r^5 = 1$. Dakle, prethodni niz potencija možemo zapisati kao

$$r, r^3, r^4, r^2, r, \ldots$$

i u tom nizu se pojavljuju svi korijeni. S druge strane, pretpostavimo da smo uzeli r i sukcesivno ga potencirali potencijom 4. Opet, budući da je r korijen jednadžbe $x^5 - 1 = 0$, tada je $r^5 = 1$. Dakle, dobijemo niz

$$r, r^4, r^{16}, r^{64}, \ldots$$

U ovome slučaju jedini različiti brojevi u nizu su r i r^4. Primijetimo da su ostala dva korijena r^2 i r^3 kvadrati dvaju različitih članova prethodnog niza

$$(r)^2 = r^2 \qquad (r^4)^2 = r^8 = r^3.$$

Općenitije, pretpostavimo da je n prost broj te r primitivni n-ti korijen iz jedinice. Gauss je pokazao da će niz potencija imati k različitih elemenata, gdje je k djelitelj od $n-1$. Štoviše, preostali korijeni (ako je $k \neq n-1$) mogu se separirati u dva skupa od po k različitih elemenata od kojih je svaki potencija korijena originalnog skupa.

Na primjer, neka je $n = 7$ te p primitivni korijen. Niz $p, p^6, p^{36}, p^{216}, \ldots$ sadrži samo dva različita korijena: p i p^6. Njihovi kvadrati su $p^2, p^{12} = p^5$ a kubovi p^3, p^4. Dakle, 6 korijena smo particionirali u tri skupa: $\{p, p^6\}$, $\{p^2, p^5\}$ i $\{p^3, p^4\}$. Primijetimo da ovo particioniranje nije jedinstveno. Mogli smo uzeti niz $p, p^2, p^4, p^8, \ldots$. On sadrži tri različita korijena p, p^2, p^4 a ostali korijeni su kubovi ovih korijena. Tako smo 6 korijena particionirali u dva skupa: $\{p, p^2, p^4\}$ i $\{p^3, p^5, p^6\}$.

Vratimo se sada našem problemu za $n = 5$. Skup korijena smo particionirali na dva dijela: $\{r, r^4\}$ i $\{r^2, r^3\}$. Gauss je zatim razmatrao zbroj korijena u svakom skupu (označavajući sume kao "periodi") te je stavio te sume kao korijene jednadžbe. U našem slučaju to izgleda ovako:

$$\begin{aligned}
(y - (r + r^4))(y - (r^2 + r^3)) &= y^2 - (r^4 + r^3 + r^2 + r)y + (r + r^4)(r^2 + r^3) \\
&= y^2 - (r^4 + r^3 + r^2 + r)y + (r^3 + r^4 + r^6 + r^7) \\
&= y^2 - (r^4 + r^3 + r^2 + r)y + (r^4 + r^3 + r^2 + r) \\
&= y^2 + y - 1
\end{aligned}$$

gdje smo uzeli u obzir činjenicu da r zadovoljava jednadžbu $x^4 + x^3 + x^2 + x + 1 = 0$. Sada možemo zaključiti da izrazi $r + r^4$ i $r^2 + r^3$ odgovaraju korijenima kvadratne jednadžbe $y^2 + y - 1 = 0$. Lako se izračuna da su to $y_{1,2} = \dfrac{-1 \pm \sqrt{5}}{2}$. Jedan od tih korijena odgovara izrazu $r + r^4$ a drugi izrazu $r^2 + r^3$. U principu nema razlike koji ćemo dodijeliti kojem, međutim u praksi je zgodnije kada bi r bio vodeći peti korijen iz jedinice $\cos\dfrac{2\pi}{5} + i \sin\dfrac{2\pi}{5}$. Gauss je napomenuo kako bi se taj korijen mogao naći numerički, odnosno približno, te tako vidjeti koji od dva korijena jednadžbe $y^2 + y - 1 = 0$ je jednak $r + r^4$. Alternativna solucija bi bila primijetiti kako $r + r^4$ ima pozitivan realni dio pa će biti $r + r^4 = \dfrac{-1 + \sqrt{5}}{2}$.

Za pronalazak korijena r možemo konstruirati kvadratnu jednadžbu kojoj su r i r^4 korijeni:

$$(z-r)(z-r^4) = z^2 - (r+r^4)z + r^5 = z^2 - \left(\frac{-1+\sqrt{5}}{2}\right)z + 1$$

i koeficijenti ove jednadžbe se mogu konstruirati. Stoga će i korijeni jednadžbe biti konstruktibilni. Korijeni jednadžbe su:

$$z_{1,2} = \frac{\left(\frac{-1+\sqrt{5}}{2}\right) \pm \sqrt{\left(\frac{-1+\sqrt{5}}{2}\right)^2 - 4}}{2} = \frac{-1+\sqrt{5}}{4} \pm i\frac{\sqrt{10+2\sqrt{5}}}{4}.$$

Jedno od tih rješenja bit će vodeći peti korijen iz jedinice a drugo rješenje bit će četvrta potencija prvog rješenja. Budući da je vodeći peti korijen iz jedinice $\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$, možemo (kako je Gauss sugerirao) aproksimirati sinus i kosinus te odrediti koji od dva korijena odgovara vodećem korijenu. Kada provedemo račun dobit ćemo da je $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$ te da je $\sin\frac{2\pi}{5} = \frac{\sqrt{10+2\sqrt{5}}}{4}$. Obzirom da su ove vrijednosti konstruktibilne, to je i pravilni peterokut konstruktibilan. To smo, naravno, znali i ranije, ali cilj je bio na jednostavnijem primjeru pokazati što je zapravo Gauss radio i kako je došao do pravilnog sedamnaesterokuta.

Pogledajmo još jedan primjer. Neka je to pravilni sedmerokut. Kao i ranije možemo separirati korijene jednadžbe $x^7 - 1 = 0$ u dva skupa: $\{p, p^2, p^4\}$ te $\{p^3, p^5, p^6\}$. Neka su sume elemenata iz pojedinog skupa korijeni kvadratne jednadžbe. Sada kao i ranije imamo

$$(y - (p + p^2 + p^4))(y - (p^3 + p^5 + p^6)) = y^2 + y + 2.$$

Korijeni jednadžbe $y^2 + y + 2 = 0$ su $y_{1,2} = \frac{-1 \pm \sqrt{-1}}{2}$. Ako je p vodeći korijen, tada $p + p^2 + p^4$ ima pozitivni imaginarni dio pa je $\frac{-1+\sqrt{-1}}{2} = p + p^2 + p^4$ te $\frac{-1-\sqrt{-1}}{2} = p^3 + p^5 + p^6$. Idući korak bi bio postavljanje p, p^2, p^4 za korijene kubne jednadžbe $(z-p)(z-p^2)(z-p^4) = 0$. Ovu jednadžbu možemo riješiti i znamo joj naći rješenja ali problem nam stvara određivanje trećeg korijena koje je neizbježno. Stoga je jasno da pravilni sedmerokut nije konstruktibilan.

Ovaj primjer nam je pokazao puno toga. Pretpostavimo da želimo konstruirati pravilni n-terokut za n prost broj. Ako $n-1$ ima prostih faktora različitih od 2 tada ćemo u nekom koraku separiranja korijena morati riješiti jednadžbu stupnja većeg od 2. Stoga konstrukcija pravilnog n-terokuta pokazanom metodom zahtjeva da je n oblika $n = 2^k + 1$. Možemo otići i korak dalje. Ako k ima barem jedan neparan faktor tada je $2^k - 1$ složen broj. To vrijedi, jer ako je $k = pq$ i, bez smanjenja općenitosti, q je neparan, tada $x^{pq} + 1$ sadrži faktor $x^p + 1$. Možemo zaključiti da je pravilni n-terokut, za n prost, moguće konstruirati ako je n posebnog oblika. Taj posebni oblik su zapravo Fermatovi brojevi $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}_0$. Poznati Fermatovi brojevi su $3, 5, 17, 257, 65\,537$.

U svakom slučaju, za $n = 17$ odgovarajuća ciklotomska jednadžba ima 16 korijena. Budući da u procesu niti jednom nije morao riješiti jednadžbu stupnja većeg od 2, Gauss je dobio da se korijeni mogu konstruirati. Raspodjela u skupove bila je prema opisanim koracima i zbog preglednosti prikazana je na Slici 13.

Gauss je uzeo p kao primitivni korijen ciklotomske jednadžbe šesnaestog stupnja $x^{16} + x^{15} + \ldots + x + 1 = 0$. Pri prvoj podjeli je p sukcesivno potencirao na devetu potenciju i dobio niz

$$p, p^9, p^{81}, p^{729}, \ldots, p^{4\ 782\ 969}, \ldots$$

te, jer je $p^{17} = 1$, dobio ponavljanja. Slijedi prvi skup

$$\{p, p^2, p^4, p^8, p^9, p^{13}, p^{15}, p^{16}\}.$$

Kubiranjem članova tog skupa dobije se skup preostalih rješenja

$$\{p^3, p^5, p^6, p^7, p^{10}, p^{11}, p^{12}, p^{14}\}.$$

Nastavak raspodjele može se pratiti na Slici 13.

$p, p^2, p^3, p^4, \ldots, p^{16}$

<table>
<tr><td colspan="4">$p, p^9, p^{81}, p^{729}, \ldots, p^{4782969}$
$\Rightarrow p, p^9, p^{13}, p^{15}, p^{16}, p^8, p^4, p^2$
$\boldsymbol{\{p, p^2, p^4, p^8, p^9, p^{13}, p^{15}, p^{16}\}}$</td><td colspan="4">$p^3, p^{2\cdot3}, p^{4\cdot3}, p^{8\cdot3}, p^{9\cdot3}, p^{13\cdot3}, p^{15\cdot3}, p^{16\cdot3}$
$\boldsymbol{\{p^3, p^5, p^6, p^7, p^{10}, p^{11}, p^{12}, p^{14}\}}$</td></tr>
<tr><td colspan="2">p, p^4, p^{16}, p^{64}
$\boldsymbol{\{p, p^4, p^{13}, p^{16}\}}$</td><td colspan="2">$p^2, p^{2\cdot4}, p^{2\cdot16}, p^{2\cdot64}$
$\boldsymbol{\{p^2, p^8, p^9, p^{15}\}}$</td><td colspan="2">$p^3, p^{3\cdot4}, p^{3\cdot16}, p^{3\cdot64}$
$\boldsymbol{\{p^3, p^5, p^{12}, p^{14}\}}$</td><td colspan="2">$p^6, p^{6\cdot4}, p^{6\cdot16}, p^{6\cdot64}$
$\boldsymbol{\{p^6, p^7, p^{10}, p^{11}\}}$</td></tr>
<tr><td>p, p^{16}
$\boldsymbol{\{p, p^{16}\}}$</td><td>$p^4, p^{4\cdot16}$
$\boldsymbol{\{p^4, p^{13}\}}$</td><td>$p^2, p^{2\cdot16}$
$\boldsymbol{\{p^2, p^{15}\}}$</td><td>$p^8, p^{8\cdot16}$
$\boldsymbol{\{p^8, p^9\}}$</td><td>$p^3, p^{3\cdot16}$
$\boldsymbol{\{p^3, p^{14}\}}$</td><td>$p^5, p^{5\cdot16}$
$\boldsymbol{\{p^5, p^{12}\}}$</td><td>$p^6, p^{6\cdot16}$
$\boldsymbol{\{p^6, p^{11}\}}$</td><td>$p^7, p^{7\cdot16}$
$\boldsymbol{\{p^7, p^{10}\}}$</td></tr>
</table>

Slika 13: Particioniranje skupa korijena jednadžbe $x^{16} + x^{15} + \cdots + x + 1 = 0$

Jer je $\varphi = \dfrac{2\pi}{17}$ vrijedi: $\cos\varphi = \cos 16\varphi$, $\cos 4\varphi = \cos 13\varphi$, $\cos 2\varphi = \cos 15\varphi$, $\cos 8\varphi = \cos 9\varphi$,$\cos 3\varphi = \cos 14\varphi$, $\cos 5\varphi = \cos 12\varphi$, $\cos 6\varphi = \cos 11\varphi$, $\cos 7\varphi = \cos 10\varphi$ što se lako provjeri oduzimanjem i primjenom trigonometrijskih identiteta.

Dakle, sada je jasno odakle Gaussu izbor za a, b, c, d iz potpoglavlja 3.1.

4 Gaussov teorem i algebra

Još nam je ostalo otvoreno pitanje za koje $n \in \mathbb{N}$ se može konstruirati pravilni n-terokut. Odgovor na ovo pitanje dat će nam Gaussov teorem, no najprije ćemo iskazati osnovnu teoriju koja nam je potrebna za razumijevanje dokaza teorema.

4.1 Grupe i polja

Definicija 4.1. *Skup G s binarnom operacijom $*$ se zove grupa ako vrijedi*

1. *asocijativnost: za sve $a, b, c \in G$: $a * (b * c) = (a * b) * c$*
2. *postoji $e \in G$ takav da je $e * a = a * e = a$, za svaki $a \in G$*
3. *za svaki $a \in G$ postoji $a^{-1} \in G$ takav da je $a * a^{-1} = a^{-1} * a = e$*

Grupu nazivamo komutativna ili Abelova ako za svaki $a, b \in G$ vrijedi $a * b = b * a$.

Definicija 4.2. *Red grupe G, u oznaci $|G|$ je broj elemenata grupe G. Ako je broj elemenata grupe konačan tada je i grupa konačnog reda. U suprotnom je grupa beskonačnog reda.*

Definicija 4.3. *Neka je G grupa i $H \subseteq G$. H se zove podgrupa grupe G ako je H grupa obzirom na istu operaciju kao i G.*

Definicija 4.4. *Neka je p prost broj. Za grupu ćemo reći da je p-grupa ako je ona konačna grupa čiji red je potencija broja p.*

Definicija 4.5. *Komutativni prsten s jedinicom je skup R na kojem su definirane dvije binrne opracije, $+$ i $\cdot$ takve da vrijedi:*

1. *R je Abelova grupa obzirom na opraciju $+$*
2. *komutativnost: $a \cdot b = b \cdot a$, za sve $a, b \in R$*
3. *asocijativnost: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, za sve $a, b, c \in R$*
4. *postoji $1 \in R$ takav da je $1 \cdot a = a$, za sve $a \in R$*
5. *distributivnost: $a \cdot (b + c) = a \cdot b + a \cdot c$, za sve $a, b, c \in R$*

Definicija 4.6. *Polje je komutativni prsten s jedinicom u kojem svaki ne-nul element ima multiplikativni inverz, tj.tj. za svaki $a \in R \setminus \{0\}$, gdje je 0 neutralni element grupe R postoji $x \in R$ takav da je $a \cdot x = x \cdot a = 1$.*

4.2 Proširenje polja

Ideja o ireducibilnosti polinoma nad poljem racionalnih brojeva dovela je do pitanja o tome koje je najmanje polje nad kojim je dani polinom reducibilan. Osnovni teorem algebre kaže da su svi polinomi reducibilni nad poljem kompleksnih brojeva, ali zadani polinom je možda potpuno reducibilan i nad nekim manjim poljem. To je razvilo koncepte proširenja polja.

Definicija 4.7. *Neka su K i L polja. Ako je $K \subseteq L$, L se naziva proširenje polja K.*

Kažemo da je L jednostavno proširenje polja K ako je L proširenje polja K te postoji a iz L takav da je L najmanje polje koje sadrži i K i a. Posebno, u polje možemo dodati korijene polinoma i tako napraviti veće polje nad kojim je polinom reducibilan. U slučaju polinoma, na primjer $x^2 - 2$, veće polje nad kojim je on reducibilan je $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$.

Definicija 4.8. *Ako je L proširenje polja K, L možemo promatrati kao vektorski prostor nad poljem K te ako je taj vektorski prostor konačnodimenzionalan kažemo da je L konačno proširenje polja K. Prirodni broj $dim_K L$ zovemo stupanj proširenja polja K i označavamo s $[L : K]$.*

Stupanj proširenja, dakle, možemo naći tražeći dimenziju vektorskog prostora L nad poljem K.

Dokaz idućeg rezultata nije nam toliko bitan, ali može ga se naći u knjizi [5, str. 85]

Teorem 4.1. *Neka su $K \subseteq L \subseteq M$ polja. Tada je $[M : K] = [M : L]\,[L : K]$, pri čemu smatramo da je $\infty \cdot n = n \cdot \infty = \infty \cdot \infty = \infty$.*

Definicija 4.9. *Neka su G_1 i G_2 grupe. Preslikavanje $\varphi : G_1 \longrightarrow G_2$ naziva se homomorfizam grupa ako je $\varphi(ab) = \varphi(a)\varphi(b)$ za svaki $a, b \in G_1$. Izomorfizam grupa je homomorfizam koji je bijekcija.*

Definicija 4.10. *Neka je K polje. Automorfizam polja K je svaki izomorfizam polja K na samog sebe. Skup svih automorfizama polja K označavamo s $Aut(K)$.*

Definicija 4.11. *Neka je L proširenje polja K ($K \subseteq L$). K-automorfizam polja L je automorfizam $\sigma \in Aut(L)$ za koji vrijedi $\sigma(x) = x$, za svaki $x \in K$.*

Definicija 4.12. *Označimo s $Aut_K(L)$ skup svih K-automorfizama polja L. $Aut_K(L)$ je potpolje od $Aut(L)$ i $Aut_K(L)$ naziva se Galoisova grupa proširenja L polja K. Označavamo ju s $Gal(L, K)$.*

4.3 Polinomi

Jedan od važnijih rezultata algebre je da ako je R komutativni prsten s jedinicom tada je $R[x]$, skup polinoma u jednoj varijabli s koeficijentima iz R, komutativni prsten s jedinicom. U algebri se često govori o ireducibilnim polinomima. Ireducibilan polinom je takav polinom kod kojeg ne postoji polinom manjeg stupnja od njega koji ga dijeli u istom prstenu polinoma. Drugim riječima, ako je polinom $p(x)$ ireducibilan tada ne postoje netrivijalni polinomi manjeg stupnja takvi da je $p(x) = a(x)b(x)$. Također, postoji jedinstvena faktorizacija svih polinoma u produkt ireducibilnih polinoma.

Definicija 4.13. *Neka je K polje i $P \in K[x]$ nekonstantan polinom. Kažemo da se polinom P cijepa nad proširenjem L polja K ako postoji $a \in K$ te $\alpha_1, \ldots, \alpha_n \in L$ takvi da je*

$$P(x) = a(x - \alpha_1) \cdots (x - \alpha_n),$$

odnosno ako polinom P možemo faktorizirati kao produkt linearnih faktora.

Definicija 4.14. *Neka je K polje i $P \in K[x]$ nekonstantan polinom. Ako se P cijepa nad L, tj. ako je $P(x) = a(x-\alpha_1) \cdots (x-\alpha_n)$, $a \in K$, $\alpha_1, \ldots, \alpha_n \in L$ te ako je k tome $L = K(\alpha_1, \ldots, \alpha_n)$, onda se L naziva polje cijepanja polinoma P nad poljem K.*

4.4 Ciklotomsko polje

Kako bi preveli ideju o n točaka jednako raspoređenih po trigonometrijskoj kružnici iz euklidske konstrukcije u nešto s čime možemo raditi algebarski potrebno nam je ciklotomsko polje . Navesti ćemo još jednom definicije vezane za ciklotomska polja.

Definicija 4.15. *Neka je $n \in \mathbb{N}$. Polje $\mathbb{Q}(\xi_n)$ koje se dobije proširenjem polja racionalnih brojeva primitivnim n-tim korijenima iz jedinice ξ_n naziva se ciklotomsko polje reda n.*

Ciklotomsko polje $\mathbb{Q}(\xi_n)$ je polje korijena polinoma $x^n - 1$. Zaista, svaki korijen od $x^n - 1$ je potencija primitivnog korijena ξ_n i te potencije generiraju $\mathbb{Q}(\xi_n)$. Odatle je $\mathbb{Q}(\xi_n)$ Galoisova grupa proširenja polja $\mathbb{Q}$.

Može se pokazati([6, lema 6.1.]) da je $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$, gdje je $\varphi(n)$ Eulerova funkcija koja daje broj elemenata skupa $1, 2, \ldots, n$ koji su relativno prosti s n.

Definicija 4.16. *Polinom oblika*

$$\Phi_n(x) = \prod_{\xi \in \omega_n} (x - \xi)$$

gdje je ω_n skup primitivnih n-tih korijena iz jedinice, naziva se ciklotomski polinom. Ciklotomski polinom je normirani polinom najmanjeg stupnja čiji su svi korijeni primitivni n-ti korijeni iz jedinice.

4.5 Konstruktibilni brojevi

Kako smo ranije rekli, duljinu neke dužine, tj. neki broj, možemo konstruirati ravnalom i šestarom ako ju možemo dobiti konačnim brojem racionalnih operacija i određivanja drugih korijena. Možemo reći: broj je konstruktibilan ako ga se može dobiti konačnim brojem presjeka pravaca i kružnica. Primijetimo, ako kružnice i pravce prebacimo u koordinatni sustav i radimo s njihovim jednadžbama, svaki presjek pravca i kružnice će imati jednadžbu stupnja dva ili manje. Dakle, sve te jednadžbe mogu se riješiti samo racionalnim operacijama i uzimanjem drugih korijena. Također, algebarski to možemo reći ovako: kompleksni broj je konstruktibilan ako i samo ako postoji niz proširenja polja $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = \mathbb{Q}(z)$ takav da je svako proširenje $K_i \subseteq K_{i+1}$ kvadratno, odnosno $[K_{i+1} : K_i] = 2$.

Ovi iskazi su ekvivalentni jer je proširenje polja $F \subseteq K$ kvadratno ako i samo ako je $K = F(\sqrt{a})$ za neki $a \in F$ takav da $\sqrt{a} \notin F$. Dakle, konstruirati drugi korijen ekvivalentno je najviše kvadratnom proširenju polja, dok zbrajanje, oduzimanje, množenje i dijeljenje polju ne doprinose ni na koji način.

4.6 Fermatovi brojevi

Brojevi oblika $F_n = 2^{2^n} + 1$ gdje je $n \in \mathbb{N}_0$, zovu se Fermatovi brojevi. Poznato je da su prvih pet Fermatovih brojeva prosti. Ti brojevi su 3, 5, 17, 257 i 65 537. Idući Fermatov broj je $F_5 = 4\ 294\ 967\ 297$ i za njega ni sam Fermat nije mogao dokazati da je prost. Tek 80 godina nakon Fermatove smrti Euler je pokazao da je taj broj zapravo složen te da su mu djelitelji 641 i 6 700 417. Petnaestak godina kasnije Euler je objavio i dokaz idućeg teorema, koji je zapravo poopćenje malog Fermatovog teorema, koji kaže da ako cijeli broj a nije djeljiv prostim brojem p onda je $a^{p-1} - 1$ djeljiv s p,:

Teorem 4.2. *Ako brojevi a i b nisu djeljivi prostim brojem p tada je svaki broj oblika $a^{p-1} - b^{p-1}$ djeljiv s p.*

Euler je to iskoristio kako bi dokazao da svaki djelitelj broja oblika $a^{2m} + b^{2m}$ (među kojima su i Fermatovi brojevi) mora biti oblika $k2^{m+1} + 1$, gdje je $k \geq 0$. Lucas je ovo proširio na brojeve oblika $k2^{m+2} + 1$ što mu je dalo početnu točku za testiranje vrijednosti n koje daju proste brojeve te ih testirao jesu li djelitelji od F_5. Bilo mu je potrebno samo šest pokušaja da nađe prikladni n. Ovakvim istraživanjem došlo se do zaključka da su brojevi od F_6 do F_{11} složeni. Nije poznato postoje li veći prosti Fermatovi brojevi.

4.7 Gaussov teorem

Teorem 4.3 (Gauss)**.** *Pravilni n-terokut može se konstruirati ravnalom i šestarom ako i samo ako je n broj oblika*

$$n = 2^a p_1 p_2 p_3 \cdots p_i$$

gdje je $a \geq 0$ te $p_1, p_2, \ldots, p_i$ različiti Fermatovi brojevi.

Dokaz. Najprije primijetimo da je konstrukcija pravilnog n-terokuta ekvivalentna konstrukciji n-tih korijena iz jedinice u kompleksnoj ravnini.

Pogledajmo primitivni n-ti korijen iz jedinice $\xi_n = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$. Sada su svi n-ti korijeni iz jedinice $1, \xi_n, \ldots, \xi_n^{n-1}$. Budući da je skup konstruktibilnih brojeva polje, ti brojevi će biti konstruktibilni ako i samo ako je ξ_n konstruktibilan. Dakle, pravilni n-terokut je konstruktibilan ako i samo ako je ξ_n konstruktibilan.

Prema karakterizaciji konstruktibilnih brojeva iz potpoglavlja 4.5, ξ_n će biti konstruktibilan ako i samo ako postoji niz proširenja polja $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = \mathbb{Q}(z)$ takav da je svako proširenje $K_i \subseteq K_{i+1}$ kvadratno, odnosno $[K_{i+1} : K_i] = 2$. Jer je $\mathbb{Q}(\xi_n)$ ciklotomsko polje, ranije smo naveli da je $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$.

Pretpostavimo sada da niz proširenja $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = \mathbb{Q}(z)$ postoji. Prema Teoremu 4.1 slijedi:

$$\varphi(n) = [\mathbb{Q}(\xi_n) : \mathbb{Q}] = [K_m : K_{m-1}]\,[K_{m-1} : K_{m-2}] \cdots [K_1 : K_0] = \underbrace{2 \cdot 2 \cdots 2}_{m \text{ puta}} = 2^m$$

što smo i tražili.

Pretpostavimo sada da je $\varphi(n) = 2^m$ za neki m. Polje $\mathbb{Q}(\xi_n)$ je polje cijepanja ciklotomskog polinoma $\Phi_n(x)$ te je $\mathbb{Q}(\xi_n)$ Galoisova grupa proširenja polja $\mathbb{Q}$. Red Galoisove grupe $Gal(\mathbb{Q}(\xi_n), \mathbb{Q})$ je jednak $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = 2^m$. Stoga je $G = Gal(\mathbb{Q}(\xi_n), \mathbb{Q})$ 2-grupa te mora postojati niz podgrupa

$$G = G_m > G_{m-1} > \cdots > G_0 = \{e\}$$

takav da je $[G_{i+1} : G_i] = 2$ za sve i. Fundamentalni teorem Galoisove teorije kaže da postoji bijekcija između podgrupa od $Gal(\mathbb{Q}(\xi_n), \mathbb{Q})$ i niza proširenja polja K_i: $\mathbb{Q} = K_m \subseteq K_{m-1} \subseteq \cdots \subseteq K_0 = \mathbb{Q}(\xi_n)$; takvih da je stupanj svakog proširenja 2, odnosno da je $[K_i : K_{i+1}] = [G_{i+1} : G_i] = 2$. Stoga je ξ_n konstruktibilan.

Sada smo pokazali da je pravilni n-terokut konstruktibilan ako i samo ako je $\varphi(n) = 2$. Još treba pokazati da su brojevi koji to zadovoljavaju u točnom obliku, tj. oblika $n = 2^a p_1 p_2 p_3 \cdots p_i$ gdje je $a \geq 0$ te $p_1, p_2, \ldots, p_i$ različiti Fermatovi brojevi.

Neka je n faktoriziran na način da je $n = 2^a p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_i^{e_i}$, gdje su $p_1, p_2, \ldots, p_n$ različiti neparni prosti brojevi, $e_k \geq 1$ za sve k, te $a \geq 0$. Prema definiciji od $\varphi(n)$ imamo:

$$\varphi(n) = 2^{a-1} p_1^{e_1-1} p_2^{e_2-1} p_3^{e_3-1} \ldots p_i^{e_i-1} (p_1 - 1)(p_2 - 1) \cdots (p_n - 1)$$

ili

$$\varphi(n) = p_1^{e_1-1} p_2^{e_2-1} p_3^{e_3-1} \cdots p_i^{e_i-1} (p_1 - 1)(p_2 - 1) \cdots (p_n - 1) \text{ ako je } a = 0.$$

Pretpostavimo da je $\varphi(n) = 2^m$. Potencija broja 2 ne može biti djeljiva neparnim prostim brojem pa ne može biti $e_k > 1$ ni za koji k jer bi inače p_k dijelio 2^m. Stoga je $e_1 = e_2 = \cdots = e_i = 1$. Također, bilo koji djelitelj potencije broja 2 mora biti potencija broja 2 te je tako $p_k - 1$ potencija broja 2 za svaki k. Sada je jasno da je svaki p_k Fermatov broj. Dakle, n je traženog oblika.

Obratno, pretpostavimo da je $n = 2^a p_1 p_2 p_3 \cdots p_i$, gdje su $p_1, p_2, \ldots, p_i$ različiti Fermatovi brojevi $p_k = 2^{2^{\gamma_k}} + 1$. Tada je

$$\varphi(n) = 2^{a-1}(p_1 - 1)(p_2 - 1) \cdots (p_n - 1) = 2^{a-1} 2^{2^{\gamma_1}} 2^{2^{\gamma_2}} \cdots 2^{2^{\gamma_i}}$$

ili

$$\varphi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_n - 1) = 2^{2^{\gamma_1}} 2^{2^{\gamma_2}} \cdots 2^{2^{\gamma_i}} \text{ ako je } a = 0.$$

U oba slučaja to su potencije broja 2 kako se i zahtijevalo. □

U knjizi Disquisitiones Arithmeticae na kraju sedmog poglavlja *Sectio septima de aequationibus circuli sectiones definientibus* (o jednadžbama koje definiraju odjeljke kruga), Gauss navodi slijedeće: "*Općenito, dakle, kako bi mogli podijeliti kružnicu geometrijski na N dijelova, N mora biti* 2 *ili neka veća potencija od* 2*, ili prost broj oblika* $2^m + 1$*, ili produkt nekoliko prostih brojeva tog oblika, ili jednog ili nekoliko takvih prostih brojeva s* 2 *ili nekom većom potencijom od* 2*. Ukratko, potrebno je da N ne sadrži neparni prosti faktor koji nije oblika* $2^m + 1$ *niti prosti faktor oblika* $2^m + 1$ *više od jednom. Ovdje su navedene* 38 *vrijednosti broja N ispod* 300*:*
2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272."[2, str. 463]

Literatura

[1] D. M. BURTON, *The History of Mathematics: An Introduction*, McGraw-Hill, New York, 2006.

[2] C. F. GAUSS, *Disquisitiones Arithmeticae*, Lipsiae, in Comissis apud Gerh. Fleischer, 1801.

[3] R. HARTSHORNE, *Geometry: Euclid and Beyond*, Springer, New York, 2000.

[4] A. JONES, S. A. MORRIS, K. R. PEARSON, *Abstract Algebra and Famous Imposibilities*, Springer-Verlag, Harrisonburg Virginia, 1994.

[5] H. KRALJEVIĆ, *Algebra*, Odjel za matematiku, Osijek, 2007.

[6] D. KUH, *Constructible Regular n-gons*, Whitman College - senior project archive, 2013.

[7] Y. NISHIYAMA, *Gauss' Method of Constructing a Regular Heptadecagon*, International Journal of Pure and Applied Mathematics, vol. 82 no. 5, 2013., 695-707

[8] D. PALMAN, *Geometrijske konstrukcije*, Element, Zagreb, 1996.

[9] C. C. PINTER, *A book of abstract algebra*, Dover Publications, Inc., Mineola, New York, 1990.

[10] D. SAVITT, *The Matematics of Gauss*, Cornell University New York, 2007.

[11] J. SUZUKI, *A Brief History of Impossibility*, Mathematics magazine, vol. 81 no. 1, 2008., 27-38

[12] J. VILLANUEVA, *The cyclotomic equation and its significance to solving the quintic equation*, International Conference on Technology in Collegiate Mathematics (ICTCM),vol. 25, 2013., 293-299

Sažetak

Geometrijske ili euklidske konstrukcije, kako im samo ime kaže, poznate su još od antičke Grčke. Smatralo se da se sve zna i da su iscrpljene sve mogućnosti. Međutim, Carl Friedrich Gauss nije smatrao tako. On je uspio pokazati da uz konstrukcije poznatih pravilnih n-terokuta kao što su trokut, četverokut i peterokut, postoje još neki koji su konstruktibilni. Gauss je smjestio pravilne n-terokute u kompleksnu ravninu. Vrhove pravilnih n-terokuta shvatio je kao koordinate točaka u kompleksnoj ravnini. Obzirom da se tako svaki vrh može prikazati kao kompleksni broj $z = x + yi$, odnosno u trigonometrijskom obliku $z = \cos\varphi + i\sin\varphi$, za konstrukciju pravilnog n-terokuta dovoljno je moći konstruirati dužinu duljine $\cos\dfrac{2\pi}{n}$ ili $\sin\dfrac{2\pi}{n}$. To je moguće ukoliko se riješenja jednadžbe n-tog stupnja $x^n - 1 = 0$ mogu zapisati konačnim brojem racionalnih operacija i određivanja drugih korijena. Rješenja takve jednadžbe nazivaju se n-ti korijeni iz jedinice.

Koristeći se Vandermondeovim i Lagrangeovim prijašnjim rezultatima, Gauss je vrlo vješto riješio jednadžbu sedamnaestog stupnja $x^{17} - 1 = 0$ i jedno njeno rješenje prikazao konačnim brojem racionalnih operacija i određivanja drugih korijena te tako pokazao da je moguće konstruirati pravilni sedamnaesterokut. Rješavanje jednadžbe $x^{17} - 1 = 0$ sveo je na traženje korijena ciklotomskog polinoma $x^{16} + x^{15} + \cdots + x + 1 = 0$. Ne znajući unaprijed rješenja, korijene polinoma je separirao u osam skupova po dva korijena i tako traženje korijena polinoma šesnaestog stupnja sveo na traženje korijena polinoma drugog stupnja. Svoje ideje i detaljne raspise postupka objavio je u knjizi Disquisitiones Arithmeticae sa nepune 24 godine.

Općenitije, Gauss je dao točan opis brojeva n za koje je pravilni n-terokut konstruktibilan. Ti n-ovi su usko povezani s Fermatovim brojevima i potencijama broja dva. Formalno govoreći, Gauss je pokazao da se pravilni n-terokut može konstruirati ravnalom i šestarom ako je n oblika $2^a p_1 p_2 p_3 \cdots p_i$ gdje je $a > 0$ te $p_1, p_2, p_3, \ldots, p_i$ različiti Fermatovi brojevi.

Ključne riječi: Gauss, Disquisitiones Arithmeticae, pravilni sedamnaesterokut, pravilni poligoni, ciklotomski polinom, korijen iz jedinice, ciklotomsko polje, Gaussov teorem

Title and summary

Regular heptadecagon

Geometric or Euclidean constructions, as their name suggest, are known from antic Greece. It was considered that all is known and all possibilities are exhausted. But, Carl Friedrich Gauss didn't thought so. He managed to prove that along constructions of regular n-gons like triangle, square and pentagon, there are more of them which are constructible. Gauss settled regular n-gons in complex plane. He imagined vertices of regular n-gons as coordinates of points in complex plane. Considering that every vertex can be written as complex number $z = x + yi$, that is in trigonometric form $z = \cos\varphi + i\sin\varphi$, for construction of regular n-gon it is enough to be able to construct segment with length of $\cos\dfrac{2\pi}{n}$ or $\sin\dfrac{2\pi}{n}$. That is possible if roots of equation of n-th degree $x^n - 1 = 0$ can be written with finite number of rational operations and taking of square roots. Roots of such equation are called n-th roots of unity.

Using Vandermonde and Lagrange earlier results, Gauss was very cleverly solved equation of 17th degree $x^{17} - 1 = 0$ and one of their roots wrote using finite number of rational operations and taking of square roots and by doing so showed that it is possible to construct regular heptadecagon. Solving of equation $x^{17} - 1 = 0$ he reduced on finding roots of cyclotomic polynomial $x^{16} + x^{15} + \cdots + x + 1 = 0$. Not knowing solutions in advance, he separated roots of polynomial in eight sets by two roots and by doing so he reduced finding roots of polynomial of 16th degree into finding roots of polynomial of 2nd degree. His ideas and detailed descriptions Gauss published in book Disquisitiones Arithmeticae not even being 24 years old.

Generally, Gauss gave exact description of numbers n for which regular n-gon is constructible. Those n-s are closely related to Fermat numbers and powers of number two. Formally speaking, Gauss showed that regular n-gon can be constructed with ruler and compass if n has form $2^a p_1 p_2 p_3 \cdots p_i$ where $a > 0$ and $p_1, p_2, p_3, \ldots, p_i$ different Fermat numbers.

Key words: Gauss, Disquisitiones Arithmeticae, regular heptadecagon, regular polygon, cyclotomic polynomial, root of unity, cyclotomic field, Gauss theorem

Životopis

Rođen sam 18.6.1991. u Osijeku. Od 1998. do 2006. pohađao sam Osnovnu školu Ivan Goran kovačić u Đakovu te nakon toga upisao Prirodoslovno-matematičku gimnaziju A. G. Matoša također u Đakovu. Gimnaziju sam završio položenom Državnom maturom školske godine 2009./2010. te iste 2010. upisao Integrirani sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku Sveučilišta J. J. Strossmayera u Osijeku.