Konstruktibilna števila

Gal Zajc, Živa Kocijan, Matija Likar
Mentorica: Klara Drofenik

Povzetek

Pri projektu smo iskali števila, ki jih lahko konstruiramo zgolj z ravnilom in šestilom. Spoznali smo probleme *kvadrature kroga*, *trisekcije kota*, *podvojitve kocke* in *konstrukcije pravilnega n-kotnika.*

1 Uvod

Antična matematika je še danes zelo zanimiva in nekateri njihovi problemi so še vedno dobro znani. Primeri teh so *problem kvadrature kroga*, *trisekcija kota* in *podvojitev kocke.* Med drugim je antične probleme obravnaval tudi nemški matematik Carl Friedrich Gauss, ki je že pri 17-tih ukvarjal s konstruktibilnostjo pravilnih n-kotnikov.

Konstruktibilna števila so števila, ki jih lahko narišemo le z ravnilom in šestilom. V članku bomo najprej opisali, kako lahko konstruiramo nova konstruktibilna števila iz starih. V 3. poglavju bomo predstavili nekaj antičnih problemov, katerih rešljivost oziroma nerešljivost bomo dokazali v poglavju 7. Spoznali bomo matematični struktruri grupe in obsega ter si ogledali razširitve obsegov.

2 Konstruktibilnost

Definicija 1. *Konstruktibilna števila so:*

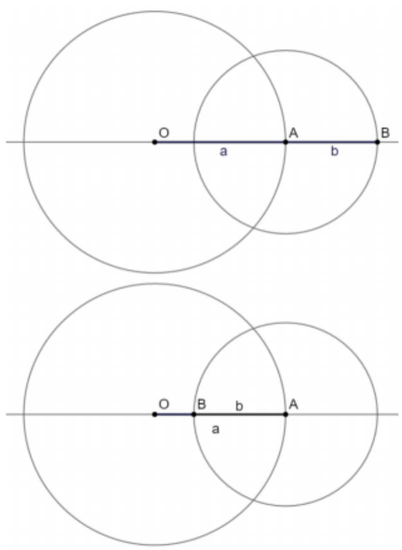
- *Enota, ki jo najprej določimo.*
- *x in y natanko tedaj, ko je točka (x, y) konstruktibilna.*

Konstruktibilne objekte definiramo:

- *Če imamo dve konstruktibilni točki, potem je konstruktibilna tudi premica, ki gre skozi obe.*
- *Če imamo dve konstruktibilni točki, potem je konstruktibilna tudi krožnica, ki ima središče v prvi točki in gre skozi drugo točko.*
- *Presečišča konstruktibilnih krožnic in premic so konstruktibilna.*

2.1 Seštevanje in odštevanje koonstruktibilnih števil

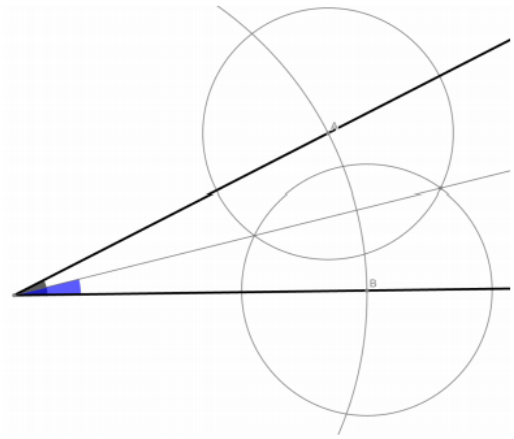
Dani imamo konstruktibilni števili a in b, ki ju želimo sešteti. Kot vidimo na sliki 1, lahko to naredimo tako, da na premici konstruiramo daljico OA dolžine a in daljico AB dolžine b tako, da je točka B na drugi strani točke A kot točka O. Razdalja OB je enaka $a + b$, torej je $a + b$ konstruktibilno. Odštevanje naredimo podobno, le da je točka B na isti strani točke A kot točka O.



Slika 1: Zgoraj: vsota intervalov a in b; Spodaj: razlika intervalov a in b

2.2 Razpolavljanje kota

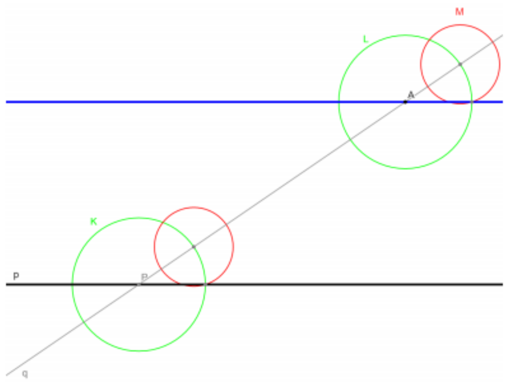
Poglejmo si, kako razpolovimo kot. Začnimo s kotom. Šestilo zapičimo v vrh kota in narišemo lok, kot je razvidno na sliki 2, ki seka oba kraka kota v točkah A in B. Narišemo krožnici s središčema v točkah A in B s poljubnima enakima polmeroma. Potegnemo premico skozi presečišči novonastalih krožnic in vrh kota. Ta premica razplolavlja začetni kot.



Slika 2: Primer razpolavljanja kota

2.3 Konstrukcija vzporednic

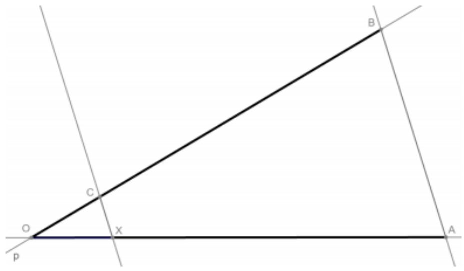
Oglejmo si, kako konstruiramo vzporednico dani premici p in točki A ($A \notin p$). Kot opisano na sliki 3, skozi A potegnemo premico q, ki seka p v točki P. Narišemo krožnici enakega radija s središčem v točki P in v točki A. Označimo ju s K in L. Vzamemo zgornje presešišče K s q ter odmerimo razdaljo do desnega presečišča K in p. V zgornjem presečišču q in L narišemo krožnico M s prejšnjim polmerom. Nato potegnemo premico skozi A in spodnje presečišče krožnic M in L. Ta premica je vzporedna premici p.



Slika 3: Primer konstrukcije vzporednic

2.4 Deljenje konstruktibilnega števila z naravnim številom

Denimo, da želimo daljico OA razdeliti na b enakih delov, kjer je $b \in \mathbb{N}$. Skozi krajišče O potegnemo poljubno premico p, na katero b-krat nanesemo razdaljo $|OC|$, kjer je C točka na premici p. Kot je razvidno na sliki 4, je razdalja $|OB| = b \cdot |OC|$. Nato narišemo premico skozi A in B. Tej premici narišemo vzporednico skozi C. Naj bo X presečišče te vzporednice z daljico OA. Razdalja $|OX|$ je enaka $\frac{|OA|}{|OB|}$.

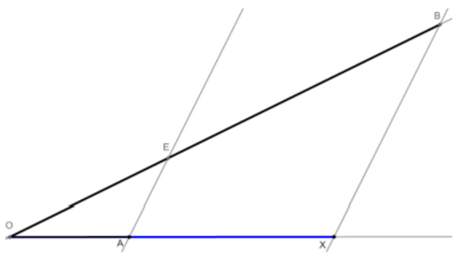


Slika 4: Primer deljenja intervala dolžine a na b enakih delov intervalov

2.5 Množenje intervalov

Podani imamo števili a in b, s katerima želimo konstruirati razdaljo $a \cdot b$. Narišemo daljico OA dolžine a, kot je razvidno iz slike 5. Skozi O potegnemo poljubno premico p in nanjo nanesemo enoto ter dolžino b. Na p postavimo točki E in B, tako da velja $|OE| = 1; |OB| = b$. Narišemo daljico AE in njeno vzporednico skozi B. Presečišče te vzporednice in noslike daljice OA naj bo X, ki leži na razdalji x od izhodšča.

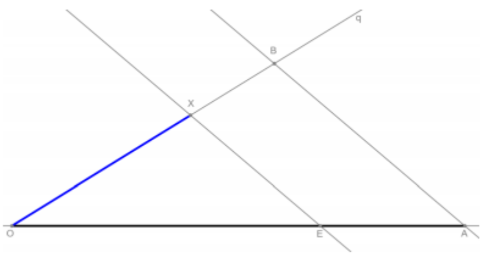
$$\frac{a}{1} = \frac{x}{b}$$
$$a \cdot b = x$$



Slika 5: Primer množenja intervalov

2.6 Konstrukcija obratne vrednosti

Imamo podano konstruktibilno število a različno od 0 in želimo dobiti število $\frac{1}{a}$. Na številsko premico nanesemo razdaljo a in krajišča označimo s točkama O in A, kot je prikazano na sliki 6. Skozi krajišče O potegnemo poljubno premico q in na njej označimo točko B, da velja $|OB| = 1$. Povežemo točki A in B in skozi točko E, ki leži na daljici OA in za katero velja $|EO| = 1$, potegnemo vzporednico AB. Presečišče vzporednice in premice q označimo z X, razdalja $|OX|$ je enaka $1/a$, kar je obratna vrednost od števila a.



Slika 6: Primer konstrukcije obratne vrednosti

2.7 Korenjenje števil

Želimo konstruirati koren števila a, vidnega na sliki 7. Naj bo premica p nosilka daljice OA, tako da velja $|OA| = a$. Točka B je na dolžini 1 od točke A in je na nasprotni strani od O. Razpolovimo OB in s S označimo razpolovišče. Narišemo krožni lok s središčem v S in radijem $|OS|$. Na OB narišemo pravokotnico skozi A, ki seka lok v točki C. Dokažimo, da je $|AC| = \sqrt{a}$. Po Talesovem izreku je kot $\angle BCO$ pravi. Velja: $\angle COA + \angle OBC = \frac{\pi}{2}$. Prav tako je $\angle BCA + \angle ACO = \frac{\pi}{2}$. Ker sta trikotnika CAO in CBA pravokotna, lahko ugotovimo, da sta si trikotnika AOC in ACB podobna, saj se ujemata v dveh (torej vseh) kotih. Od kod dobimo:

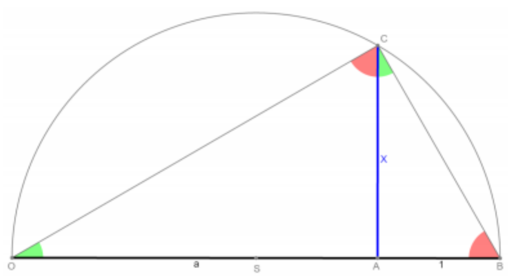
$$\frac{|OA|}{|AC|} = \frac{|AC|}{|AB|}$$
$$|OA||AB| = |AC|^2$$

Ker je $|AB| = 1$, sledi

$$|AC| = \sqrt{|OA|} = \sqrt{a}$$

.

□



Slika 7: Primer korenjenja števila

3 Predstavitev problemov

3.1 Kvadratura kroga

Imamo podan krog z nekim radijem r, kjer je r konstruktibilno število. Ali je mogoče konstruirati kvadrat z isto ploščino le z uporabo neoznačenega ravnila in šestila?

Naj ima ta kvadrat stranico a.

$$a^2 = \pi r^2$$
$$a = \sqrt{\pi} r$$

Če želimo, da bo a konstruktibilen, mora biti produkt $\sqrt{\pi} r$, konstruktibilen. r je po predpostavki konstruktibilno število. Torej mora biti $\sqrt{\pi}$ konstruktibilen. Ker znamo narisati koren kaeregakoli konstruktibilnega števil, bo mogoče narediti kvadraturo kroga natanko tedaj, ko bo π konstruktibilen.

π.

3.2 Trisekcija kota

Imamo podan poljuben kot θ. Ali je mogoče konstruirati kot velikosti $\frac{\theta}{3}$, torej razdeliti prvotni kot na tri enake dele. Trivialno je, da lahko kota π in $\frac{\pi}{2}$ razdelimo na tri enake dele, saj sta kota $\frac{\pi}{3}$ in $\frac{\pi}{6}$ konstruktibilna.

3.3 Podvojitev kocke

Dano imamo kocko s konstruktiblinimi stranicami a. Ali je mogoče konstruirati kocko z dvakrat večjo prostornino? Naj ima večja kocka stranico b.

$$b^3 = 2a^3$$
$$b = a\sqrt[3]{2}$$

Kocka s stranico b je torej konstruktibilna natanko tedaj, ko je konstruktibilno število $\sqrt[3]{2}$.

3.4 Konstruktibilni pravilni n-kotniki

Ali je mogoče konstruirati poljuben pravilni n-kotnik zgolj z uporabo neoznačenega ravnila in šestila? Pokažimo primer konstukcije za $n = 3, 4, 6$.

Narišemo poljubno krožnico. Polmer krožnice šestkrat prenesmo po krožnici, tako da šestilo zapišemo na poljubno mesto na krožnici, in zarišemo presečišče z krožnico. Šestilo zapičimo na to presečišče in to še petkrat ponovimo.Novonastale točke so oglišča našega pravilnega šestkotnika, kot vidimo na sliki 8a.

Pravilni trikotnik konstruiramo tako, da povežemo vsako drugo oglišče šestkotnika.

Želimo konstruirati kvadrat. Konstrukcija je vidna na sliki 8b. Narišemo daljico dolžine a. V krajišču te daljice konstruiramo pravokotnico in nanjo prenesemo dolžino stranice. Postopek ponovimo za ostali dve stranici in tako dobimo pravilni štirikotnik.

(a) Konstrukcija pravilnega šestkotnika in trikotnika

(b) Konstrukcija pravilnega kvadrata

Slika 8: Pravilni n-kotniki

4 Polinomi

Definicija 2. *Polinomi so vsota produktov spremenljivk in koeficientov. Splošna oblika polinoma je*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0,$$

kjer je a_n je vodilni člen polinoma, a_0 pa je prosti člen. Stopnja polinoma je največji i, da velja $a_i \neq 0$.

Izrek 1. ***Eisensteinov kriterij***
Imejmo polinom $q(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$

Če obstaja praštevilo p, tako da p deli vsak koeficient a_i, razen vodilnega člena a_n, kvadrat praštevila pa ne deli prostega člena a_0, potem je $q(x)$ nerazcepen nad $\mathbb{Q}$ - to pomeni, da nima racionalnih ničel.

5 Množica konstruktibilnih števil

5.1 Grupa

Grupa je par $(G, *)$, kjer je G neprazna množica in $*$ asociativna binarna operacija $G \times G \to G$, ki vsakemu urejenemu paru $(a, b) \in G$ priredi element $a * b \in G$. Operacija $*$ mora zadoščati aksiomom grupe:

1. **Zaprtost:** Za vsak $a, b \in G$ velja $a * b \in G$.
2. **Asociativnost:** Za vsake $a, b, c \in G$ velja $(a * b) * c = a * (b * c)$.
3. **Obstoj nevtralnega elementa:** Obstaja tak element $e \in G$, da za vsak $a \in G$ velja $e * a = a = a * e$.
4. **Obstoj inverza:** Za vsak $a \in G$ obstaja tak $b \in G$, da velja $a * b = b * a = e$.

5.2 Obseg

Definicija 3. *$(A, +, \cdot)$ **je obseg**, če sta $(A, +)$ ter $(A - \{0\}, \cdot)$ grupi in velja distributivnost:*

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Definicija 4. *K je **podobseg** F, če je K podmnožica F in je $(K, +, \cdot)$ obseg.*

5.3 Razširitev obsegov

Obseg F je **razširitev** obsega K natanko tedaj, ko je K podobseg F.

Definicija 5. *Razširitev obsega K z a je najmanjši podobseg F, ki vsebuje obseg K in $a; a \notin K$:*

$$K(a) = \{\frac{p(a)}{q(a)}; p(x), q(x) \in K[x]; q(x) \neq 0\}$$

Z razširitvijo $K(a)$ dodamo obsegu K ničlo nekega nerazcepnega polinoma s koeficienti iz K.

Definicija 6. *Stopnja razširitve je enaka stopnji nerazcepnega polinoma za a.*

Stopnja razširitve nekega $F = K(a)$ je enaka 1, natanko tedaj, ko $F = K$. Takšno razširitev imenujemo **trivialna razširitev**. Razširitvi stopnje 2 in 3 imeujemo **kvadratna razširitev** in **kubična razširitev**.
Primer razširitve $\mathbb{Q}$ s $\sqrt{2}$:

$$\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \middle| a, b \in \mathbb{Q}\right\},$$

Denimo, da imamo polinom druge stopnje oblike $x^2 - 2$. Ker gledeamo polinom nad $\mathbb{Q}$, je ta polinom narezcepen po Eisensteinovem kriteriju. Zato je stopnja razširitve $\mathbb{Q}$ z $\sqrt{2}$ enaka 2. Stopnjo razširitve $F = K(a)$ označimo z $[F : K]$.

5.4 Algebraična in transcendentna števila

Definicija 7. *Število x je* ***algebraično*** *nad K natanko tedaj, ko obstaja polinom s koeficienti v K, tako da je x ničla tega polinoma. V nasprotnem primeru je število* ***transcendentno****.*

Če naredimo razširitev $\mathbb{Q}(\lambda)$, kjer je λ transcendentno število, je stopnja razširitve ∞.

Lastnosti transcendentnih in algrebraičnih števil so:

Algebraična števila	Transcendentna števila
števno neskončna	neštevno neskončna
vsako racionalno število je tudi algebraično	vsa realna transcendentna število so iracionalna
so konstruktibilna	niso konstruktibilna

Primer: π je transcendentno število.

6 Razširitev konstruktibilnih števil

Naj bo K množica vseh konstrkutibilnih števil.

Trditev 1. *Množica vseh konstruktibilnih števil K je obseg.*

Dokaz: Po definiciji obsega je dovolj dokazati, da sta seštevanje in množenje notranji operaciji.
V poglavjih 2.1 ter 2.5 smo pokazali, da če sta a, b konstruktibilni števili, so tudi $a + b$, $a - b$, $\frac{a}{b}$ in $a \cdot b$ konstruktibilna števila. Iz tega sledi, da velja $\mathbb{Q} \subseteq K$

Definirajmo enoto in pokažimo, katera števila je mogoče konstruirati.

Naj bo K_0 naša prvotna množica konstruktibilnih števil, $K_0 = \{0, 1\}$.

Naj bo $K_i(a)$ neka razširitev K_i in podobseg K.

V poglavju 2 smo pokazali, da lahko točko konstruiramo oziroma z njo razširimo K_i na 3 načine.

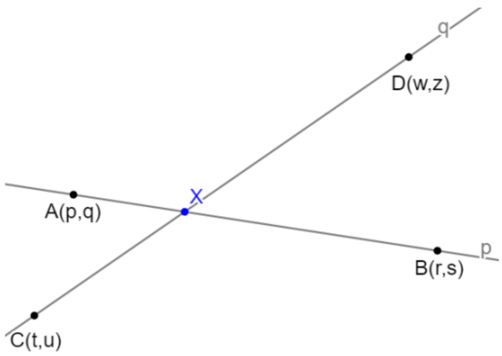
1. Dodamo presečišče dveh premic
2. Dodamo presečišče dveh krožnic
3. Dodamo presečišče krožnice in premice

Trditev 2. *Naj bo a število, ki smo ga tako dodali. Potem ima vsaka prej opisana razširitev stopnjo 1 ali 2.*

Dokažimo, da lahko s predpisanimi načini konstruiranja dosežemo samo razširitve take stopnje.

6.1 Presečišče dveh premic

Imamo podani dve premici. Prvo definirata konstruktibilni točki $A(p,q)$ in $B(r,s)$, drugo pa konstruktibilni točki $C(t,u)$ ter $D(w,z)$. Števila p,q,r,s,t,u,w,z morajo biti vsa konstruktibilna. Želimo najti koordinate presečišča in ugotoviti, katere stopnje je razširitev (glej sliko 9).



Slika 9: Konstrukcija presečišča dveh premic

Zapišimo obe premici v eksplicitni obliki $y = k_i x + n_i$, potem velja:

Opomba: Če je premica navpična, torej je oblike x = a za vsak y, je ne moremo izraziti v eksplicitni obliki. Dokaz v tem primeru prepustimo bralcu.

$$k_1 = \frac{s-q}{r-p}$$
$$k_2 = \frac{z-u}{w-t}$$
$$n_1 = q - p \cdot \frac{s-q}{r-p}$$
$$n_2 = z - w \cdot \frac{z-u}{w-t}$$

Tako dobimo sistem enačb:

$$y = \frac{s-q}{r-p}x + (q - p \cdot \frac{s-q}{r-p})$$
$$y = \frac{z-u}{w-t}x + (z - w \cdot \frac{z-u}{w-t})$$

.

Enačimo y in izpostavimo x

$$\frac{s-q}{r-p}x + (q - p \cdot \frac{s-q}{r-p}) = \frac{z-u}{w-t}x + (z - w \cdot \frac{z-u}{w-t})$$
$$(q - p \cdot \frac{s-q}{r-p}) - (z - w \cdot \frac{z-u}{w-t}) = (\frac{z-u}{w-t} - \frac{s-q}{r-p})x$$
$$\frac{(q - p \cdot \frac{s-q}{r-p}) - (z - w \cdot \frac{z-u}{w-t})}{(\frac{z-u}{w-t} - \frac{s-q}{r-p})} = x$$
$$x - \frac{(q - p \cdot \frac{s-q}{r-p}) - (z - w \cdot \frac{z-u}{w-t})}{(\frac{z-u}{w-t} - \frac{s-q}{r-p})} = 0$$

Vidimo, da je polinom nerazcepen s stopnjo 1, torej je iskanje presečišča premic ekvivalentno razširitvi množice K_i prve stopnje.

6.2 Presečišče dveh krožnic

Dani imamo dva kroga K_1 in K_2 s konstruktibilnima polmeroma in konstruktibilnima koordinatama središč (glej sliko 10). Redefiniramo enotna vektorja koordinatnega sistema, tako da enega izmed krogov postavimo v središče, drugega pa na abscisno os. To je dovoljeno, saj sta v našem primeru koordinati vektorja konstruktibilni števili.

Krog v središču koordiatnega sistema naj ima radij r_1, drugi krog r_2. K_2 leži na razdalji k od izhodišča.

Zapišimo njuni enačbi:

$$r_1^2 = x^2 + y^2$$

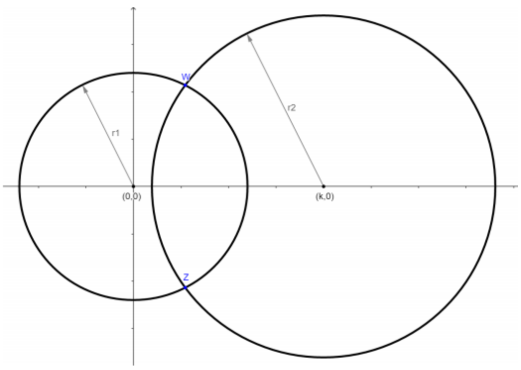
in

$$r_2^2 = (x-k)^2 + y^2.$$

Iz enačb izrazimo y, ju enačimo in nato izpostavimo x:

$$\begin{aligned}
r_1^2 - r_2^2 &= x^2 - (x-k)^2, \\
r_1^2 - r_2^2 &= x^2 - x^2 + 2kx - k^2, \\
r_1^2 - r_2^2 &= 2kx - k^2, \\
\frac{r_1^2 - r_2^2 + k^2}{2k} &= x.
\end{aligned}$$

Tako kot pri presečišču premic je tudi tukaj polinom prve stopnje, kar pomeni, da je razširitev s presečišči dveh krožnih prve stopnje.



Slika 10: Konstrukcija presečišča dveh krožnic

6.3 Presečišče krožnice in premice

Podani imamo dve konstruktibilni točki $A(p,q)$ in $B(r,s)$, ki definirata premico. Imamo tudi konstruktibilno krožnico s središčem v $C(t,u)$ in radijem R (glej sliko 11).

Zapišimo enačbo krožnice in enačbo premice:

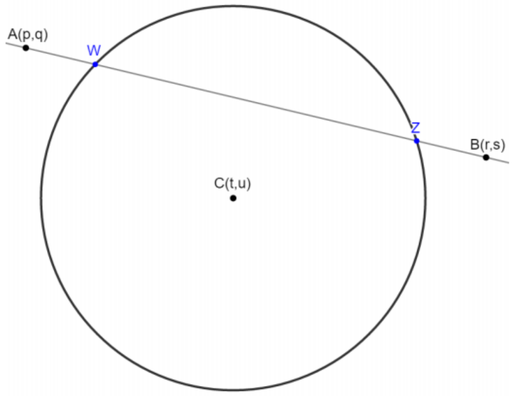
$$R^2 = (x-t)^2 + (y-u)^2$$

$$y = \frac{s-q}{r-p}x + (q - p \cdot \frac{s-q}{r-p})$$

iz druge enačbe izrazimo y in ga vstavimo v prvo enačbo ter izpostavimo x:

$$R^2 = (x-t)^2 + (\frac{s-q}{r-p}x + q - p \cdot \frac{s-q}{r-p} - u)^2$$

očitno je to polinom druge stopnje v x. Če je ta polinom nerazcepen, je razširitev druge stopnje, če pa je razcepen, pa prve stopnje.



Slika 11: Konstrukcija presečišča premice in krožnice

6.4 Posledica

Ugotovili smo, da lahko s konstrukcijo para premic, krogov ali premice in kroga, dosežemo razširitev ali prve ali druge stopnje. Če uporabimo hkrati več krožnic ter premic, se razširitve množijo, kar pomeni, da je razširitev v našem primeru stopnje $2^k; k \in \mathbb{Z}^+$.

7 Rešitve problemov

7.1 Konstruktibilni pravilni n-kotniki

Definicija 8. *Naravno število n je **marsovsko**, če je pravilni n-kotnik konstruktibilen, kar pomeni, da ga lahko konstruiramo z ravnilom in šestilom.*

Če $m|n$, lahko konstruiramo pravilen m-kotnik s povezovanjem vsakega d-tega oglišča pravilnega n kotnika ($d = \frac{n}{m}$).

Iz tega sledi:

Izrek 2. *Če je n marsovsko in m deli n, potem je m marsovsko.*

Če sta števili n in m tuji, obstajata celi števili a in b, za kateri velja: $am + bn = 1$. Iz tega sledi $\frac{a}{n} + \frac{b}{m} = \frac{1}{mn}$. Tako lahko iz $\frac{2\pi}{m}$ in $\frac{2\pi}{n}$ konstruiramo $\frac{2\pi}{mn}$.
Iz tega sledi:

Izrek 3. *Če sta m in n marsovski in tuji števili, potem je tudi $m \cdot n$ marsovsko.*

Pogoj za konstruktibilnost pravilnega n-kotnika je leta 1781 definiral Friedrich Gauss, leta 1837 pa jo je dokazal Pierre Wantzel.

Izrek 4. *Pravilen n-kotnik je konstruktibilen, če in samo če velja:* $n = 2^r \cdot p_1 \cdot \ldots \cdot p_s; r, s \geq 0; r, s \in \mathbb{Z}$. $p_1, \ldots p_s$ *so liha števila oblike* $p_j = 2^{2^{r_j}} + 1$.

Števila oblike $p = 2^{2^r} + 1$ imenujemo **Fermatova števila**: $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. Posledica: Če je p praštevilo, potem je p-kotnik konstruktibilen za $p = 2, 3, \ldots 17, 257, 65537$.

7.2 Podvojitev kocke

Že v razdelku 3.3 smo omenili, da lahko konstruiramo kocko z dvojno prostornino natanko tedaj, ko lahko konstruiramo $\sqrt[3]{2}$.
Želimo torej razširiti naš obseg K s številom $\sqrt[3]{2}$. Če želimo, da bi razširitev ustrezala našim kriterijem konstruktibilnosti, mora biti stopnja razširitve enaka 2^k, za nek $k \in \mathbb{N}$. Najdimo torej polinom z koeficienti iz K, da bo $\sqrt[3]{2}$ ena izmed njegovih ničel.

$$\begin{aligned} x &= \sqrt[3]{2} \\ x^3 &= 2 \\ x^3 - 2 &= 0 \end{aligned}$$

Ta polinom je nerazcepen po Eisensteinovem kriteriju za praštevilo $p = 3$. Torej je stopnja razširitve 3, kar pomeni da takšna razširitev ni potenca števila 2. Zaradi tega ne moremo konstruirati števila $x = \sqrt[3]{2}$ zgolj z ravnilom in šestilom. Podvojitev kocke je zato nemogoča. $\square$

7.3 Kvadratura kroga

Izrek 5. *Za poljuben krog ne moremo konstruirati kvadrata z isto ploščino le z uporabo šestila in ravnila.*

Dokaz: Takšna konstrukcija je ekvivalentna konstrukciji točke $(0, \sqrt{\pi})$ iz začetnih točk {(0,0),(1,0)}.
Če znamo konstruirati $(0, \sqrt{\pi})$, lahko enostavno konstruiramo$(0, \pi)$.
Če bi takšna konstrukcija obstajala, potem bi veljalo $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^n$, kar pa ni res, saj je π transcendentno. Iz tega sledi, da π ne moremo konstruirati.

7.4 Trisekcija kota

Izrek 6. *Kot $\frac{\pi}{3}$ se ne da razdeliti na 3 eneake dele z ravnilom in šestilom.*

Dokaz:

1. Znamo konstruirati kot $\frac{\pi}{3}$ iz $(0,0)$ in (1,0).

2. Narediti trisekcijo kota $\frac{\pi}{3}$ je ekvivalentno konstrukciji (α,0); $\alpha = cos\frac{\pi}{9}$ iz (0,0) in (1,0). Iz $\cos\frac{\pi}{9}$ lahko konstruiramo tudi (β,0); $\beta = 2\cos\frac{\pi}{9}$
Za vsak α velja: $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$.
Če vstavimo $\alpha =\frac{\pi}{9}$ v kubično enačbo, dobimo: $\cos\frac{\pi}{3} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9}$
Če upoštevamo $\cos 3\alpha = cos\frac{\pi}{3} = \frac{1}{2}$, dobimo: $\frac{1}{2} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9}$. S substitucijo $\beta = 2\cos\frac{\pi}{9}$, dobimo: $0 = 4\frac{\beta^3}{8} - 3\frac{\beta}{2} - \frac{1}{2}$, oziroma: $0 = \beta^3 - 3\beta - 1$.

Pripadajoči polinom$f(t) = t^3 - 3t - 1$ ne uztreza Eisensteinovemu kriteriju, saj nobeno praštevilo ne deli 1, ki je prosti člen. Zato poskusimo namesto t vstaviti t+1:

$$f(t+1) = t^3 + 3t^2 - 3 = 0$$

Vidimo, da ta polinom ustreza kriteriju za praštevilo 3, torej je ta polinom nerazcepen. Zatoje trisekcija kota ekvivalentna razširitvi stopnje 3, število 3 pa ni oblike 2^k. Trisekcija kota zato ni mogoča. □

8 Literatura

Literatura

[1] Richard Courant, Herbet Robbins, *An Elementary approach to ideas and methods*, Second edition, Oxford University Press, USA, 1996.

[2] Ian Stewart, *Galois Theory*, Third edition, Chapman & Hall/CRC mathematics, United States of America, 2003.

[3] Constructible polygon, v: Wikipedia: The Free Encyclopedia, [ogled 1. 8. 2019], dostopno na `https://en.wikipedia.org/wiki/Constructible_polygon.html`.

[4] Field extension, v: Wikipedia: The Free Encyclopedia, [ogled 1. 8. 2019], dostopno na `https://en.wikipedia.org/wiki/Field_extension.html`.

[5] Polynomial, v: Wikipedia: The Free Encyclopedia, [ogled 1. 8. 2019], dostopno na
https://en.wikipedia.org/wiki/Polynomial.