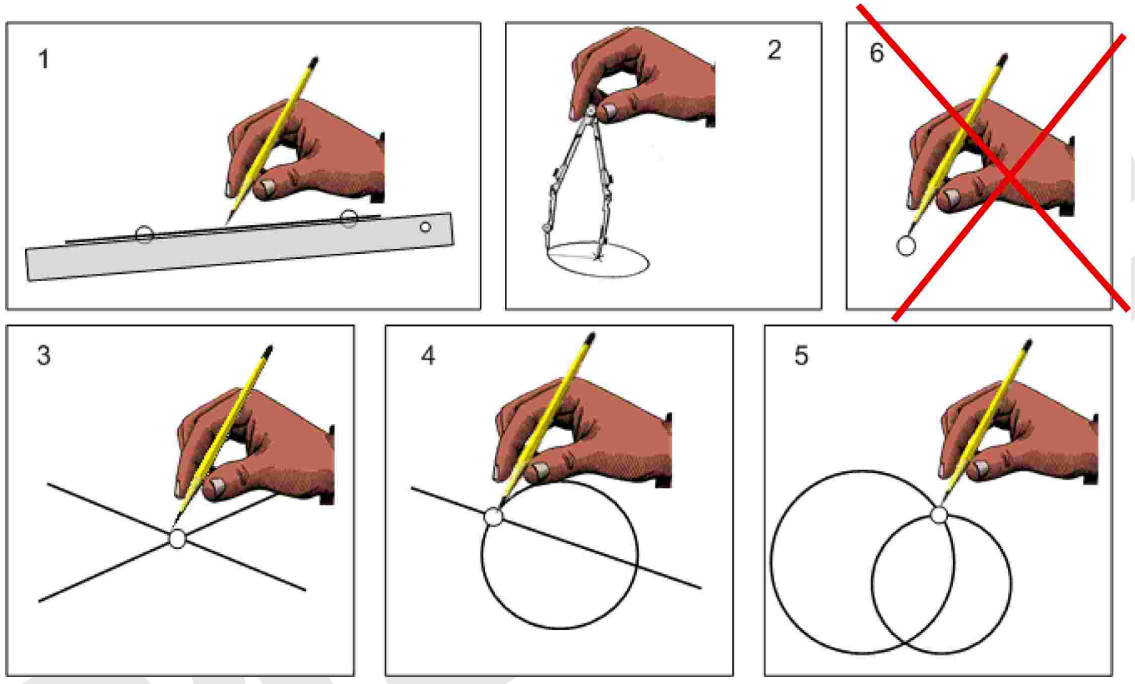
Geometriai szerkeszthetőség

Szerkesztési feladat

Adottak $P_1, \ldots, P_n$ pontok, ezekből szeretnénk egy Q pontot megszerkeszteni.



Szerkesztési lépések

Ha A, B, C, D már meg van szerkesztve akkor egy új E pontot szerkeszthetünk

- az AB és CD egyenesek metszéspontjaként,
- az AB egyenes és a C középpontú, D-n átmenő kör (egyik) metszéspontjaként, vagy
- az A középpontú B-n átmenő kör és a C középpontú, D-n átmenő kör (egyik) metszéspontjaként.

A szerkesztés menete

$$H = \{P_1, P_2, \ldots, P_n\} \rightsquigarrow \{P_1, P_2, \ldots, P_n, Q_1\} \rightsquigarrow$$
$$\rightsquigarrow \{P_1, P_2, \ldots, P_n, Q_1, Q_2\} \rightsquigarrow \ldots$$
$$\rightsquigarrow \{P_1, P_2, \ldots, P_n, Q_1, Q_2, \ldots, Q_\ell\} \quad Q_\ell = Q.$$

Megjegyzések

- A megadott $P_1, \ldots, P_n$ pontok *konkrét* pontok a síkon, pl. egy konkrét háromszög magasságpontját akarjuk megszerkeszteni. Amennyiben olyan eljárást akarunk adni, ami pl. tetszőleges háromszög magasságpontjának megszerkesztésére alkalmas, akkor *paraméteres* szerkesztési feladatról beszélünk. Az utóbbi nyilván nehezebb feladat: ha általános eljárást tudunk adni, akkor az minden speciális esetben is működni fog. Fordítva ez nem igaz, nincs például általános szerkesztési eljárás tetszőleges szög harmadolására, de ettől még speciális esetekben (pl. 90°) tudunk szöget harmadolni.
- Mindig feltesszük, hogy legalább két pont meg van adva ($n \geq 2$).
- Két pontból már lehet egy sűrű ponthalmazt szerkeszteni, ezért nem jelent megszorítást, hogy megtiltottuk, hogy „csak úgy” segédpontokat vegyünk fel.
- Kört csak adott középpontból adott kerületi ponton keresztül rajzolhatunk (euklideszi körző); nem lehet egy adott szakaszt (mint sugarat) körzőnyílásba venni, és máshol kört rajzolni vele. HF: Mutassuk meg, hogy ez sem jelent megszorítást!

Algebraizálás

Vegyünk fel egy derékszögű koordinátarendszert, amelynek origója $O \in H$, és az első tengelyen az egységnek az $E \in H$ pont felel meg. Ezután pontok helyett számokat szerkesztünk: minden valós szám megfelel az első tengely (mint valós számegyenes) egy pontjának. Könnyű belátni, hogy egy $Q = (x, y)$ pont akkor és csak akkor szerkeszthető meg, ha az x, y számok(nak megfelelő pontok az első tengelyen) megszerkeszthetőek.

Szerkesztési feladat

Adottak $c_1, \ldots, c_n$ valós számok, ezekből szeretnénk egy α valós számot megszerkeszteni.

Szerkesztési lépések

Ha $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{R}$ már meg vannak szerkesztve akkor egy új $\alpha \in \mathbb{R}$ számot szerkeszthetünk

- az AB és CD egyenesek metszéspontjának egyik koordinátájaként,
- az AB egyenes és a C középpontú, D-n átmenő kör (egyik) metszéspontjának egyik koordinátájaként, vagy
- az A középpontú B-n átmenő kör és a C középpontú, D-n átmenő kör (egyik) metszéspontjának egyik koordinátájaként,

ahol $A = (a_1, a_2)$, $B = (b_1, b_2)$, $C = (c_1, c_2)$, $D = (d_1, d_2)$.

A szerkesztés menete

$$\begin{aligned}\{c_1, c_2, \ldots, c_n\} &\rightsquigarrow \{c_1, c_2, \ldots, c_n, \alpha_1\} \rightsquigarrow \\ &\rightsquigarrow \{c_1, c_2, \ldots, c_n, \alpha_1, \alpha_2\} \rightsquigarrow \cdots \\ &\rightsquigarrow \{c_1, c_2, \ldots, c_n, \alpha_1, \alpha_2, \ldots, \alpha_\ell\} \quad \alpha_\ell = \alpha.\end{aligned}$$

Megjegyzés

A koordinátarendszer választása miatt az O és E pontok a 0 és 1 számoknak felelnek meg, tehát ez a két szám mindig adott.

A szerkesztés alapteste

A kiindulásul megadott $c_1, \ldots, c_n$ számok által generált $K = \mathbb{Q}(c_1, \ldots, c_n) \leq \mathbb{R}$ számtestet a szerkesztés **alaptestének** nevezzük.

Állítás

Az alaptest nem függ a koordinátarendszer választásától.

Tétel

Ha $\alpha \in \mathbb{R}$ szerkeszthető, akkor α algebrai K fölött, és $m_{\alpha,K}$ foka kettőhatvány.

Tétel (szögharmadolás)

Nem lehet adott szöghöz harmadakkora szöget szerkeszteni.

Bizonyítás

Ez egy paraméteres szerkesztési feladat; megmutatjuk, hogy nemcsak általános szögharmadolási eljárás nincs, de még olyan „ad hoc" eljárás sem, ami a 60°-os szög harmadát megszerkesztené. Ekkor $K = \mathbb{Q}$ és a megszerkesztendő szám $\alpha = \cos 20^\circ$. Node $m_{\alpha,K} = x^3 - \frac{3}{4}x - \frac{1}{8}$ foka nem kettőhatvány. □

Tétel (kockakettőzés)

Nem lehet adott kockához kétszerakkora térfogatú kockát szerkeszteni.

Bizonyítás

Igazából ez is paraméteres feladat; nézzük az egységkocka esetét. Ekkor $K = \mathbb{Q}$ és a megszerkesztendő szám $\alpha = \sqrt[3]{2}$. Node $m_{\alpha,K} = x^3 - 2$ foka nem kettőhatvány. □

Tétel (körnégyszögesítés)

Nem lehet adott körhöz vele azonos területű négyzetet szerkeszteni.

Bizonyítás

Nézzük az egységkör esetét. Ekkor $K = \mathbb{Q}$ és a megszerkesztendő szám $\alpha = \sqrt{\pi}$, ami még csak nem is algebrai K fölött. □

Ikerfeladatok

- Adott a derékszögű háromszög derékszögű csúcsból induló magassága és
  - a derékszögő csúcsból induló szögfelezője, vagy
  - egy másik csúcsból induló szögfelezője.

  Megszerkeszthető-e a háromszög?

- Adott az egyenlő szárú háromszög beírt körének sugara és
  - a szára, vagy
  - az alapja.

  Megszerkeszthető-e a háromszög?

A szerkeszthetőség elméletét fel lehet építeni úgy is, hogy egy pontnak nem egy valós számpárt, hanem egy komplex számot feleltetünk meg.

Algebraizálás

Vegyük fel a valós és a képzetes tengelyt úgy, hogy $O \in H$ feleljen meg a 0-nak és $E \in H$ az 1-nek. Ezután pontok helyett komplex számokat szerkesztünk

Szerkesztési feladat

Adottak $c_1, \ldots, c_n$ komplex számok, ezekből szeretnénk egy α komplex számot megszerkeszteni.

A szerkesztés alapteste

A kiindulásul megadott $c_1, \ldots, c_n$ számok és konjugáltjaik által generált $K = \mathbb{Q}\left(c_1, \ldots, c_n, \overline{c_1}, \ldots, \overline{c_n}\right) \leq \mathbb{C}$ számtestet a szerkesztés **alaptestének** nevezzük.

Állítás

Az alaptest nem függ a koordinátarendszer választásától.

4.30. Definíció

Az α komplex számot K feletti **négyzetgyökmennyiségnek** nevezzük, ha α megkapható K elemeiből a négy alapművelet és négyzetgyökvonás véges számú alkalmazásával.

4.31. Definíció

Az $L|K$ testbővítés **egyszerű négyzetgyökbővítés**, ha $\exists a \in K : L = K(\sqrt{a})$.
Az $L|K$ testbővítés **négyzetgyökbővítés**, ha megkapható véges sok egyszerű négyzetgyökbővítés egymásutánjaként:

$$K = T_0 \leq T_1 \leq \cdots \leq T_\ell = L \qquad\qquad T_{i+1} = T_i(\sqrt{a_i}), \text{ ahol } a_i \in T_i.$$

HF: Biz. be, hogy $L|K$ egyszerű négyzetgyökbővítés $\iff [L : K] \leq 2$.

4.32. Állítás

Négyzetgyökbővítés foka mindig kettőhatvány. (Fordítva ez általában nem igaz, de normális testbővítésekre igen.)

4.33. Tétel

Tetszőleges α komplex számra az alábbiak ekvivalensek:

(1) α megszerkeszthető (K-ból);

(2) α négyzetgyökmennyiség K felett;

(3) α benne van K valamely négyzetgyökbővítésében.

4.34. Következmény

Ha $\alpha \in \mathbb{C}$ megszerkeszthető, akkor α algebrai K fölött, és $m_{\alpha,K}$ foka kettőhatvány.

Bizonyítás

$$\begin{aligned} \alpha \text{ szerkeszthető} &\implies \exists L : \alpha \in L \text{ és } L|K \text{ négyzetgyökbővítés} \\ &\implies \deg m_{\alpha,K} \mid [L:K] = 2^{\ell} \\ &\implies \deg m_{\alpha,K} = 2^{*} \end{aligned}$$

□

4.35. Megjegyzés

A fenti következmény megfordítása nem igaz; például az $x^4 + 7x + 7$ polinom gyökei nem szerkeszthetőek meg a $K = \mathbb{Q}$ alaptestből.

4.36. Tétel

Az α komplex szám akkor és csak akkor szerkeszthető meg a K alaptestből kiindulva, ha α algebrai K fölött, és $m_{\alpha,K}$ felbontási testének foka kettőhatvány.

Az egységkörbe írt szabályos n-szög akkor és csak akkor szerkeszthető meg, ha az $\varepsilon_1 = \operatorname{cis}\frac{2\pi}{n}$ komplex szám (primitív n-edik egységgyök) megszerkeszthető.
Tehát az $m_{\varepsilon_1,\mathbb{Q}}$ polinomot kell meghatároznunk.

4.37. Definíció

Az n-edik **körosztási polinom** az a Φ_n polinom, amelynek gyökei éppen a primitív n-edik egységgyökök (mindegyik egyszeres gyök):

$$\Phi_n = \prod_{\substack{\varepsilon\in\mathbb{C}^* \\ o(\varepsilon)=n}} (x-\varepsilon) = \prod_{\substack{k=1,\dots,n \\ \mathrm{lnko}(k,n)=1}} (x-\varepsilon_k)\,.$$

(Itt $\varepsilon_k = \varepsilon_1^k = \operatorname{cis}\frac{2k\pi}{n}$.) Vegyük észre, hogy $\deg\Phi_n = \varphi(n)$.

Néhány példa körosztási polinomra

- $\Phi_1 = x - 1$
- $\Phi_2 = x - (-1) = x + 1$
- $\Phi_3 = \left(x - \operatorname{cis}\frac{2\pi}{3}\right)\left(x - \operatorname{cis}\frac{4\pi}{3}\right) = \frac{x^3-1}{x-1} = x^2 + x + 1$
- $\Phi_4 = (x - i)(x + i) = \frac{x^4-1}{(x-1)(x+1)} = x^2 + 1$
- $\Phi_5 = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$
- $\Phi_6 = \frac{x^6-1}{\Phi_1\Phi_2\Phi_3} = \frac{x^6-1}{x^4+x^3-x-1} = x^2 - x + 1$
- $\Phi_7 = \frac{x^7-1}{\Phi_1} = \frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $\Phi_8 = \frac{x^8-1}{\Phi_1\Phi_2\Phi_4} = \frac{x^8-1}{x^4-1} = x^4 + 1$
- $\Phi_9 = \frac{x^9-1}{\Phi_1\Phi_3} = \frac{x^9-1}{x^3-1} = x^6 + x^3 + 1$
- $\ldots$
- $\Phi_{105} = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1$

Tétel

$$\Phi_n = \frac{x^n - 1}{\prod\limits_{\substack{d|n \\ d<n}} \Phi_d}$$

Bizonyítás

A bizonyítandó egyenlőség azzal ekvivalens, hogy $x^n - 1 = \prod\limits_{d|n} \Phi_d$.

A bal oldali polinom gyökei éppen az n-edik egységgyökök (mindegyik egyszeres).
A jobb oldali polinom gyökei ugyanezek, mert

$$\forall z \in \mathbb{C}: \quad z^n = 1 \iff d := o(z) \mid n.$$

□

4.38. Tétel

A körosztási polinomok egész együtthatósak, és irreducibilisek $\mathbb{Q}$ felett.

Bizonyítás

Csak az $n = p$ és p^2 eseteket igazoljuk (p prímszám).

Bizonyítás (folyt.)

Ha p prím, akkor $\Phi_p = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$.
Vezessük be az $y = x - 1$ új határozatlant; ekkor a polinom így alakul:

$$\Phi_p(y+1) = \frac{(y+1)^p - 1}{(y+1) - 1} =$$

$$= \frac{y^p + py^{p-1} + \binom{p}{2}y^{p-2} + \cdots + \binom{p}{p-2}y^2 + py + 1 - 1}{y} =$$

$$= y^{p-1} + py^{p-2} + \binom{p}{2}y^{p-3} + \cdots + \binom{p}{p-2}y + p.$$

Erre a polinomra pedig már alkalmazható a Schönemann–Eisenstein-féle irreducibilitási kritérium (lásd a 4.22. Lemmát).

Ha ε egy p^2-edik egységgyök, akkor ε pontosan akkor primitív p^2-edik egységgyök, ha nem p-edik egységgyök, ezért

$$\Phi_{p^2} = \frac{x^{p^2} - 1}{x^p - 1} = \frac{(x^p)^p - 1}{x^p - 1} = \Phi_p(x^p) =$$

$$= x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1 \in \mathbb{Z}[x].$$

Erre a polinomra az $x = y + 1$ helyettesítés után szintén alkalmazható a Schönemann–Eisenstein-féle irreducibilitási kritérium... □

4.39. Következmény

Ha ε primitív n-edik egységgyök, akkor $m_{\varepsilon,\mathbb{Q}} = \Phi_n$.

4.40. Lemma

(1) Ha szerkeszthető szabályos n-szög, akkor minden $d \mid n$ esetén szerkeszthető szabályos d-szög is.

(2) Ha szerkeszthető szabályos n-szög, akkor minden $k \geq 0$ esetén szerkeszthető szabályos $2^k n$-szög is.

(3) Ha szerkeszthető szabályos n-szög és szabályos m-szög, akkor szerkeszthető szabályos $\operatorname{lkkt}(n, m)$-szög is.

Bizonyítás

Az első két állítás triviális (HF). A harmadikhoz keressünk olyan x, y egész számokat, amelyekre

$$x \cdot \frac{2\pi}{n} + y \cdot \frac{2\pi}{m} = \frac{2\pi}{\operatorname{lkkt}(n, m)}.$$

Rendezés után azt kapjuk, hogy

$$mx + ny = \frac{nm}{\operatorname{lkkt}(n, m)} = \operatorname{lnko}(n, m),$$

és ennek a diofantoszi egyenletnek van megoldása. □

4.41. Tétel (Gauss 1801, Wantzel 1837)

Szerkeszthető szabályos n-szög $\iff$ az n prímfelbontásában fellépő páratlan prímek mind Fermat-prímek, és mindegyik első hatványon lép fel.

Bizonyítás

$\Longrightarrow$ (Wantzel): Tfh. szerkeszthető szabályos n-szög.

Ha $p^2 \mid n$ valamely p ptl. prímre, akkor szerkeszthető szabályos p^2-szög (4.40), és így $\varepsilon = \operatorname{cis}\frac{2\pi}{p^2}$ minimálpolinomjának foka kettőhatvány.
Node $m_{\varepsilon,\mathbb{Q}} = \Phi_{p^2}$ foka $\varphi\left(p^2\right) = p\,(p-1)$, ami nem kettőhatvány.

Tehát n prímfelbontásában minden páratlan prím első hatványon szerepel.
Legyen p egy ilyen prím; ekkor szerkeszthető szabályos p-szög (4.40), ezért az előzőekhez hasonlóan $\deg \Phi_p = \varphi\,(p) = p-1$ kettőhatvány, azaz p Fermat-prím.

$\Longleftarrow$ (Gauss): Tfh. $n = 2^k \cdot p_1 \cdot \ldots \cdot p_t$, ahol $k \geq 0$ és $p_1, \ldots, p_t$ páronként különböző Fermat-prímek.

A 4.40. Lemma szerint elég megmutatnunk, hogy szerkeszthető szabályos p_i-szög $(i = 1, \ldots, t)$. A $p_i = 3$ eset HF, a $p_i = 5$ esetet lásd a táblán, a többit nem bizonyítjuk. □

Tény

Ha $2^n + 1$ prím, akkor n kettőhatvány.

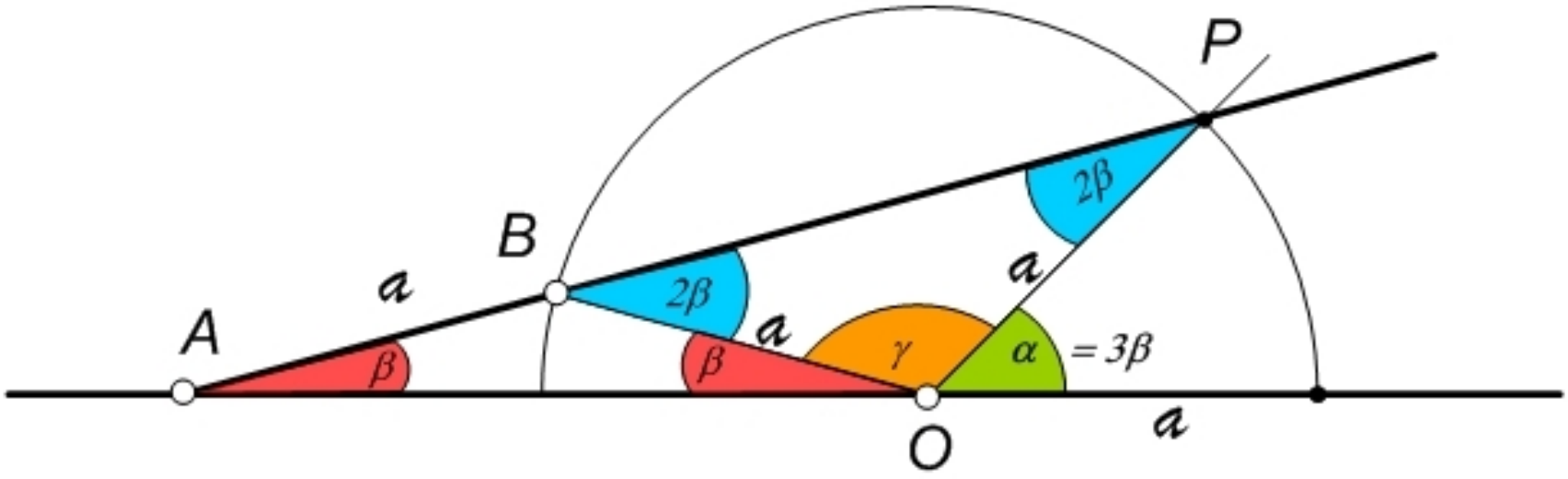
Fermat azt sejtette, hogy $F_n = 2^{2^n} + 1$ mindig prím, de ez nem igaz: Euler észrevette, hogy $F_5 = 641 \cdot 6700417$. Minden további Fermat-szám, amit megvizsgáltak szintén összetettnek bizonyult. Tehát csak öt Fermat-prímet ismerünk:

- $F_0 = 2^1 + 1 = 3$ (szerk.: ókori görögök)
- $F_1 = 2^2 + 1 = 5$ (szerk.: ókori görögök)
- $F_2 = 2^4 + 1 = 17$ (szerk.: Gauss 1796, Erchinger $\sim$1800)
  $\cos\frac{2\pi}{17} = \frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\right)$
- $F_3 = 2^8 + 1 = 257$ (szerk.: Richelot 1832)
- $F_4 = 2^{16} + 1 = 65537$ (szerk.: Hermes 1894; 10 év, 200 oldal)

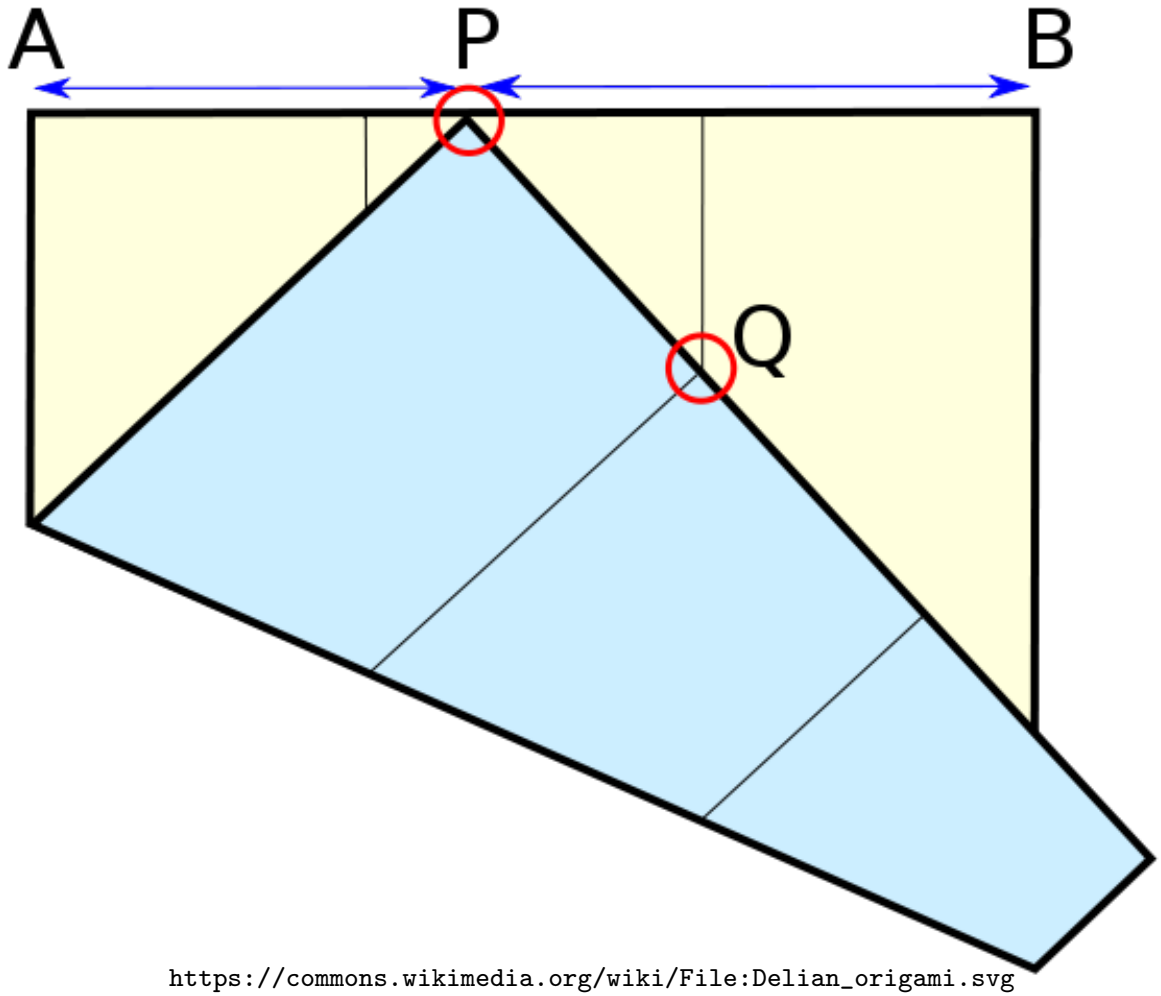
Nemeuklideszi szerkesztések

- Mohr 1672, Mascheroni 1797
  csak körző $\equiv$ körző és vonalzó
- Poncelet 1822, Steiner 1833
  csak vonalzó és egy megrajzolt kör a középpontjával együtt $\equiv$ körző és vonalzó
- köbös szerkesztések (fok$=2^k3^\ell$)
  betolóvonalzó, papírhajtogatás

Szögharmadolás betolóvonalzóval



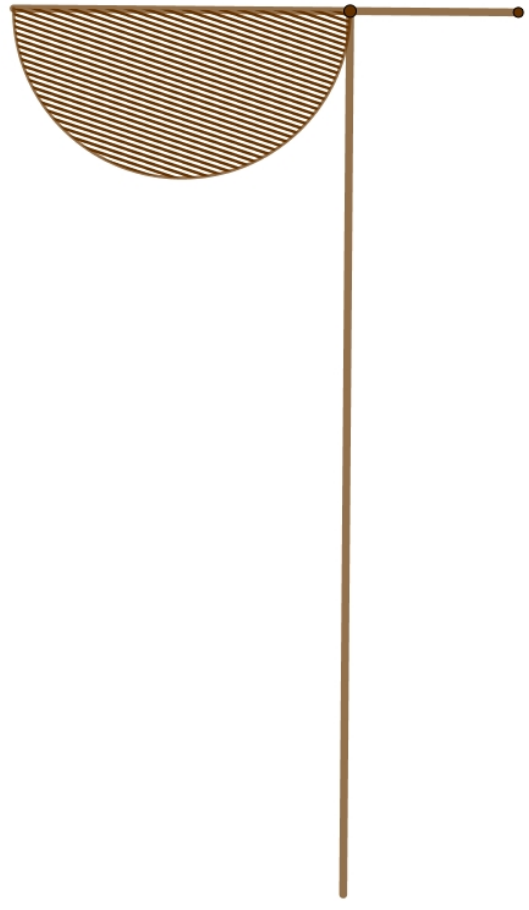
Kockakettőzés papírhajtogatással



https://commons.wikimedia.org/wiki/File:Delian_origami.svg

$$\frac{PB}{PA} = \sqrt[3]{2}$$

Szögharmadolás tomahawkkal



https://commons.wikimedia.org/wiki/File:Tomahawk-BHM_Ethno_1894.410.37-P8260256-white.jpg