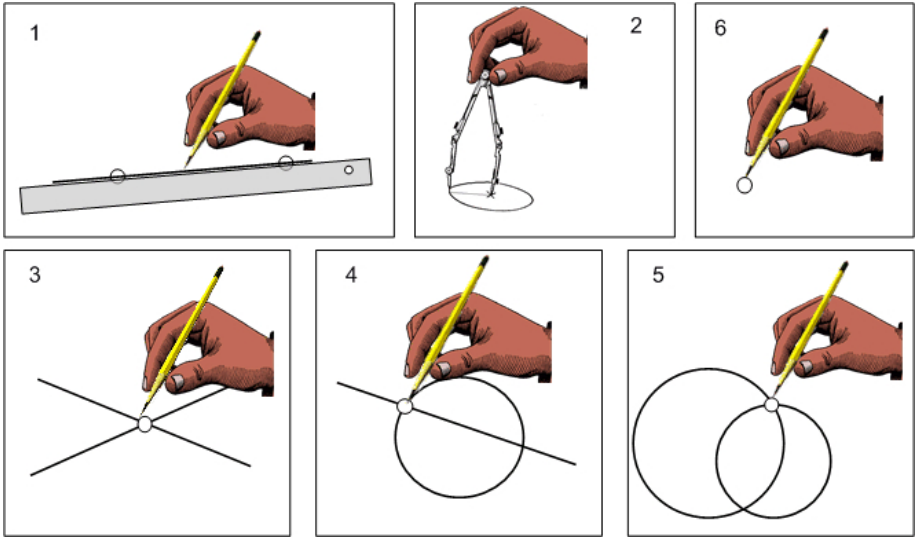
Nem kell Gaussnak lennünk a matematikai kutatáshoz

Kunos Ádám
PhD hallgató

Doktori Nyílt Nap, Bolyai Intézet
Szeged, 2015. 10. 02.

Carl Friedrich Gauss (1777-1855)

Egy barátságos téma



Forrás: https://hu.wikipedia.org/wiki/Euklideszi_szerkeszt%C3%A9s

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).
- Tudunk szöget felezni.

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).
- Tudunk szöget felezni.
- Tudunk gyököt vonni (ha adott az egység).

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).
- Tudunk szöget felezni.
- Tudunk gyököt vonni (ha adott az egység).

Kell ennél több?

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).
- Tudunk szöget felezni.
- Tudunk gyököt vonni (ha adott az egység).

Kell ennél több?
A görögöknek kellett:

- Mely szabályos sokszögek szerkeszthetőek?

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).
- Tudunk szöget felezni.
- Tudunk gyököt vonni (ha adott az egység).

Kell ennél több?
A görögöknek kellett:

- Mely szabályos sokszögek szerkeszthetőek?
- Tudunk-e szöget harmadolni?

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).
- Tudunk szöget felezni.
- Tudunk gyököt vonni (ha adott az egység).

Kell ennél több?
A görögöknek kellett:

- Mely szabályos sokszögek szerkeszthetőek?
- Tudunk-e szöget harmadolni?
- $\sqrt[3]{2}$ megszerkeszthető (kockakettőzés)?

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).
- Tudunk szöget felezni.
- Tudunk gyököt vonni (ha adott az egység).

Kell ennél több?
A görögöknek kellett:

- Mely szabályos sokszögek szerkeszthetőek?
- Tudunk-e szöget harmadolni?
- $\sqrt[3]{2}$ megszerkeszthető (kockakettőzés)?
- Tudunk-e (sugarával adott) körrel egyenlő területű négyzetet szerkeszteni? (kör négyszögesítése)

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).
- Tudunk szöget felezni.
- Tudunk gyököt vonni (ha adott az egység).

Kell ennél több?
A görögöknek kellett:

- Mely szabályos sokszögek szerkeszthetőek?
- Tudunk-e szöget harmadolni?
- $\sqrt[3]{2}$ megszerkeszthető (kockakettőzés)?
- Tudunk-e (sugarával adott) körrel egyenlő területű négyzetet szerkeszteni? (kör négyszögesítése)

Ezekre évezredekig nem sikerült válaszolni.

Barátságos?

- Tudunk szakaszt n részre osztani ($n \in \mathbb{Z}^+$).
- Tudunk szöget felezni.
- Tudunk gyököt vonni (ha adott az egység).

Kell ennél több?
A görögöknek kellett:

- Mely szabályos sokszögek szerkeszthetőek?
- Tudunk-e szöget harmadolni?
- $\sqrt[3]{2}$ megszerkeszthető (kockakettőzés)?
- Tudunk-e (sugarával adott) körrel egyenlő területű négyzetet szerkeszteni? (kör négyszögesítése)

Ezekre évezredekig nem sikerült válaszolni.

Barátságos???

Aki végül kihúzta a kérdéskör méregfogát

Évariste Galois

Aki végül kihúzta a kérdéskör méregfogát

Évariste Galois
1811. október 25. — 1832. május 31.

Gauss-Wantzel tétel

Legyen $n > 2$ egész. Szabályos n szög akkor és csakis akkor szerkeszthető (oldalhosszából), ha $n = 2^k p_1 p_2 \dots p_r$, ahol $p_1, p_2, \dots, p_r$ különböző Fermat-prímek.

Gauss-Wantzel tétel

Legyen $n > 2$ egész. Szabályos n szög akkor és csakis akkor szerkeszthető (oldalhosszából), ha $n = 2^k p_1 p_2 \dots p_r$, ahol $p_1, p_2, \dots, p_r$ különböző Fermat-prímek.

Tétel

Szöget harmadolni lehetetlen.

Méregfog kihúzva

Gauss-Wantzel tétel

Legyen $n > 2$ egész. Szabályos n szög akkor és csakis akkor szerkeszthető (oldalhosszából), ha $n = 2^k p_1 p_2 \dots p_r$, ahol $p_1, p_2, \dots, p_r$ különböző Fermat-prímek.

Tétel

Szöget harmadolni lehetetlen.

Tétel

$\sqrt[3]{2}$ nem szerkeszthető.

Méregfog kihúzva

Gauss-Wantzel tétel

Legyen $n > 2$ egész. Szabályos n szög akkor és csakis akkor szerkeszthető (oldalhosszából), ha $n = 2^k p_1 p_2 \dots p_r$, ahol $p_1, p_2, \dots, p_r$ különböző Fermat-prímek.

Tétel

Szöget harmadolni lehetetlen.

Tétel

$\sqrt[3]{2}$ nem szerkeszthető.

Tétel

Lehetetlen (sugarával adott) körrel egyenlő területű négyzetet szerkeszteni.

Manapság

Az elmélet tananyag lett

Az elmélet tananyag lett:

Az elmélet tananyag lett:

A dolog lezártnak tekintett, kutatás nem folyik a témában

Az elmélet tananyag lett:

A dolog lezártnak tekintett, kutatás nem folyik a témában, KIVÉVE:
Schreiber, P.: *On the existence and constructibility of inscribed polygons*, Beiträge zur Algebra und Geometrie **34**, 195–199 (1993)

Schreiber „tétele”

Az n oldalú húrsokszög általában nem szerkeszthető az oldalaiból, ha $n \geq 5$.

Schreiber „tétele”

Az n oldalú húrsokszög általában nem szerkeszthető az oldalaiból, ha $n \geq 5$.

A bizonyítása HIBÁS!

Az n oldalú húrsokszög általában nem szerkeszthető az oldalaiból, ha $n \geq 5$.

A bizonyítása HIBÁS!

2013 tavaszán Czédli professzor a *Testelmélet és Galois-elmélet* kurzuson arra bíztat, hogy a hallgatóság próbáljon keresni egy helyes bizonyítást. Meg is adja a kezdő lökést.

Az n oldalú húrsokszög általában nem szerkeszthető az oldalaiból, ha $n \geq 5$.

A bizonyítása HIBÁS!

2013 tavaszán Czédli professzor a *Testelmélet és Galois-elmélet* kurzuson arra bíztat, hogy a hallgatóság próbáljon keresni egy helyes bizonyítást. Meg is adja a kezdő lökést.

Hamarosan megszületik a bizonyítás páros n-ekre.

Az n oldalú húrsokszög általában nem szerkeszthető az oldalaiból, ha $n \geq 5$.

A bizonyítása HIBÁS!

2013 tavaszán Czédli professzor a *Testelmélet és Galois-elmélet* kurzuson arra bíztat, hogy a hallgatóság próbáljon keresni egy helyes bizonyítást. Meg is adja a kezdő lökést.

Hamarosan megszületik a bizonyítás páros n-ekre.

A cikk kalandos utat jár be

Az n oldalú húrsokszög általában nem szerkeszthető az oldalaiból, ha $n \geq 5$.

A bizonyítása HIBÁS!

2013 tavaszán Czédli professzor a *Testelmélet és Galois-elmélet* kurzuson arra bíztat, hogy a hallgatóság próbáljon keresni egy helyes bizonyítást. Meg is adja a kezdő lökést.

Hamarosan megszületik a bizonyítás páros n-ekre.

A cikk kalandos utat jár be, de végül révbe ér:
G. Czédli and Á. Kunos: *Geometric constructibility of cyclic polygons and a limit theorem*, Acta Sci. Math., accepted

Az n oldalú húrsokszög általában nem szerkeszthető az oldalaiból, ha $n \geq 5$.

A bizonyítása HIBÁS!

2013 tavaszán Czédli professzor a *Testelmélet és Galois-elmélet* kurzuson arra bíztat, hogy a hallgatóság próbáljon keresni egy helyes bizonyítást. Meg is adja a kezdő lökést.

Hamarosan megszületik a bizonyítás páros n-ekre.

A cikk kalandos utat jár be, de végül révbe ér:
G. Czédli and Á. Kunos: *Geometric constructibility of cyclic polygons and a limit theorem*, Acta Sci. Math., accepted

Ebben már Schreiber állítása teljes egészében bizonyítva van.

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)
A szerkesztési feladatunk ekvivalens a kör R sugarának megszerkesztésével.

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)
A szerkesztési feladatunk ekvivalens a kör R sugarának megszerkesztésével.
MSc-s tananyag: A szerkesztés nem végezhető el, ha R-nek létezik $\mathbb{Q}(a_1, \ldots, a_n)$ felett minimálpolinomja és az nem 2-hatvány fokú.

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)
A szerkesztési feladatunk ekvivalens a kör R sugarának megszerkesztésével.
MSc-s tananyag: A szerkesztés nem végezhető el, ha R-nek létezik $\mathbb{Q}(a_1, \ldots, a_n)$ felett minimálpolinomja és az nem 2-hatvány fokú.
Ha minden a_i egyenlő, akkor Gauss-Wantzel.

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)
A szerkesztési feladatunk ekvivalens a kör R sugarának megszerkesztésével.
MSc-s tananyag: A szerkesztés nem végezhető el, ha R-nek létezik $\mathbb{Q}(a_1, \ldots, a_n)$ felett minimálpolinomja és az nem 2-hatvány fokú.
Ha minden a_i egyenlő, akkor Gauss-Wantzel.
Próbáljuk meg az $|\{a_1, \ldots, a_n\}| = 2$ esetet!

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)
A szerkesztési feladatunk ekvivalens a kör R sugarának megszerkesztésével.
MSc-s tananyag: A szerkesztés nem végezhető el, ha R-nek létezik $\mathbb{Q}(a_1, \ldots, a_n)$ felett minimálpolinomja és az nem 2-hatvány fokú.
Ha minden a_i egyenlő, akkor Gauss-Wantzel.
Próbáljuk meg az $|\{a_1, \ldots, a_n\}| = 2$ esetet!
Írjunk fel egy ($\mathbb{Q}(a_1, \ldots, a_n)$ feletti) polinomot, melynek R gyöke.

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)
A szerkesztési feladatunk ekvivalens a kör R sugarának megszerkesztésével.
MSc-s tananyag: A szerkesztés nem végezhető el, ha R-nek létezik $\mathbb{Q}(a_1, \ldots, a_n)$ felett minimálpolinomja és az nem 2-hatvány fokú.
Ha minden a_i egyenlő, akkor Gauss-Wantzel.
Próbáljuk meg az $|\{a_1, \ldots, a_n\}| = 2$ esetet!
Írjunk fel egy ($\mathbb{Q}(a_1, \ldots, a_n)$ feletti) polinomot, melynek R gyöke.
Az a és b hosszúságú oldalakhoz tartozó középponti szögek felét jelölje rendre α, β.

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)
A szerkesztési feladatunk ekvivalens a kör R sugarának megszerkesztésével.
MSc-s tananyag: A szerkesztés nem végezhető el, ha R-nek létezik $\mathbb{Q}(a_1, \ldots, a_n)$ felett minimálpolinomja és az nem 2-hatvány fokú.
Ha minden a_i egyenlő, akkor Gauss-Wantzel.
Próbáljuk meg az $|\{a_1, \ldots, a_n\}| = 2$ esetet!
Írjunk fel egy ($\mathbb{Q}(a_1, \ldots, a_n)$ feletti) polinomot, melynek R gyöke.
Az a és b hosszúságú oldalakhoz tartozó középponti szögek felét jelölje rendre α, β.
Ha k db a hosszúságú oldal van, akkor $k\alpha + (n-k)\beta = \pi$, melyből

$$\sin(k\alpha) - \sin((n-k)\beta) = 0.$$

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)
A szerkesztési feladatunk ekvivalens a kör R sugarának megszerkesztésével.
MSc-s tananyag: A szerkesztés nem végezhető el, ha R-nek létezik $\mathbb{Q}(a_1, \ldots, a_n)$ felett minimálpolinomja és az nem 2-hatvány fokú.
Ha minden a_i egyenlő, akkor Gauss-Wantzel.
Próbáljuk meg az $|\{a_1, \ldots, a_n\}| = 2$ esetet!
Írjunk fel egy ($\mathbb{Q}(a_1, \ldots, a_n)$ feletti) polinomot, melynek R gyöke.
Az a és b hosszúságú oldalakhoz tartozó középponti szögek felét jelölje rendre α, β.
Ha k db a hosszúságú oldal van, akkor $k\alpha + (n-k)\beta = \pi$, melyből

$$\sin(k\alpha) - \sin((n-k)\beta) = 0.$$

Legyen $u := 1/(2R)$. Világos, hogy a húrsokszögünk akkor és csak akkor szerkeszthető, ha u szerkeszthető.

Nem kell Gaussnak lennünk

Adottak az oldalhosszak: $a_1, \ldots, a_n \in \mathbb{R}^+$ (lehetnek köztük egyenlőek is)
A szerkesztési feladatunk ekvivalens a kör R sugarának megszerkesztésével.
MSc-s tananyag: A szerkesztés nem végezhető el, ha R-nek létezik $\mathbb{Q}(a_1, \ldots, a_n)$ felett minimálpolinomja és az nem 2-hatvány fokú.
Ha minden a_i egyenlő, akkor Gauss-Wantzel.
Próbáljuk meg az $|\{a_1, \ldots, a_n\}| = 2$ esetet!
Írjunk fel egy ($\mathbb{Q}(a_1, \ldots, a_n)$ feletti) polinomot, melynek R gyöke.
Az a és b hosszúságú oldalakhoz tartozó középponti szögek felét jelölje rendre α, β.
Ha k db a hosszúságú oldal van, akkor $k\alpha + (n-k)\beta = \pi$, melyből

$$\sin(k\alpha) - \sin((n-k)\beta) = 0.$$

Legyen $u := 1/(2R)$. Világos, hogy a húrsokszögünk akkor és csak akkor szerkeszthető, ha u szerkeszthető. A bevezetett jelölésekkel

$$\sin\alpha = au,\ \sin\beta = bu,\ \cos\alpha = \sqrt{1-a^2u^2},\ \text{és}\ \cos\beta = \sqrt{1-b^2u^2}.$$

Nem kell Gaussnak lennünk

Felhasználva, hogy

$$\sin(m\gamma) = \sum_{2\nmid j=1}^{m} (-1)^{(j-1)/2} \binom{m}{j} (\cos\gamma)^{m-j} \cdot (\sin\gamma)^{j},$$

Nem kell Gaussnak lennünk

Felhasználva, hogy

$$\sin(m\gamma) = \sum_{2\nmid j=1}^{m} (-1)^{(j-1)/2} \binom{m}{j} (\cos\gamma)^{m-j} \cdot (\sin\gamma)^j,$$

adódik, hogy u gyöke a

$$q(x) =: \sum_{2\nmid j=1}^{k} (-1)^{(j-1)/2} \binom{k}{j} (1-a^2x^2)^{(k-j)/2} \cdot (ax)^j - \sum_{2\nmid j=1}^{n-k} (-1)^{(j-1)/2} \binom{n-k}{j} (1-b^2x^2)^{(n-k-j)/2} \cdot (bx)^j$$

kifejezésnek.

Nem kell Gaussnak lennünk

Felhasználva, hogy

$$\sin(m\gamma) = \sum_{2\nmid j=1}^{m} (-1)^{(j-1)/2} \binom{m}{j} (\cos\gamma)^{m-j} \cdot (\sin\gamma)^j,$$

adódik, hogy u gyöke a

$$q(x) =: \sum_{2\nmid j=1}^{k} (-1)^{(j-1)/2} \binom{k}{j} (1-a^2x^2)^{(k-j)/2} \cdot (ax)^j - \sum_{2\nmid j=1}^{n-k} (-1)^{(j-1)/2} \binom{n-k}{j} (1-b^2x^2)^{(n-k-j)/2} \cdot (bx)^j$$

kifejezésnek. Ha k páratlan és n páros, akkor $q(x)$ polinom.

Nem kell Gaussnak lennünk

Felhasználva, hogy

$$\sin(m\gamma) = \sum_{2\nmid j=1}^{m} (-1)^{(j-1)/2} \binom{m}{j} (\cos\gamma)^{m-j} \cdot (\sin\gamma)^j,$$

adódik, hogy u gyöke a

$$q(x) =: \sum_{2\nmid j=1}^{k} (-1)^{(j-1)/2} \binom{k}{j} (1-a^2x^2)^{(k-j)/2} \cdot (ax)^j - \sum_{2\nmid j=1}^{n-k} (-1)^{(j-1)/2} \binom{n-k}{j} (1-b^2x^2)^{(n-k-j)/2} \cdot (bx)^j$$

kifejezésnek. Ha k páratlan és n páros, akkor $q(x)$ polinom. Figyeljük meg, hogy a konstans tag 0.

Nem kell Gaussnak lennünk

Felhasználva, hogy

$$\sin(m\gamma) = \sum_{2\nmid j=1}^{m} (-1)^{(j-1)/2} \binom{m}{j} (\cos\gamma)^{m-j} \cdot (\sin\gamma)^j,$$

adódik, hogy u gyöke a

$$q(x) =: \sum_{2\nmid j=1}^{k} (-1)^{(j-1)/2} \binom{k}{j} (1-a^2x^2)^{(k-j)/2} \cdot (ax)^j - \sum_{2\nmid j=1}^{n-k} (-1)^{(j-1)/2} \binom{n-k}{j} (1-b^2x^2)^{(n-k-j)/2} \cdot (bx)^j$$

kifejezésnek. Ha k páratlan és n páros, akkor $q(x)$ polinom. Figyeljük meg, hogy a konstans tag 0. Úgy szeretnénk megválasztani k, a és b paramétereinket, hogy a $q(x)/x$ polinom (irreducibilis legyen és) irreducibilitását meg tudjuk mutatni a Schönemann-Eisenstein irreducibilitási kritériummal.

Nem kell Gaussnak lennünk

Felhasználva, hogy

$$\sin(m\gamma) = \sum_{2\nmid j=1}^{m} (-1)^{(j-1)/2} \binom{m}{j} (\cos\gamma)^{m-j} \cdot (\sin\gamma)^j,$$

adódik, hogy u gyöke a

$$q(x) =: \sum_{2\nmid j=1}^{k} (-1)^{(j-1)/2} \binom{k}{j} (1-a^2x^2)^{(k-j)/2} \cdot (ax)^j - \sum_{2\nmid j=1}^{n-k} (-1)^{(j-1)/2} \binom{n-k}{j} (1-b^2x^2)^{(n-k-j)/2} \cdot (bx)^j$$

kifejezésnek. Ha k páratlan és n páros, akkor $q(x)$ polinom. Figyeljük meg, hogy a konstans tag 0. Úgy szeretnénk megválasztani k, a és b paramétereinket, hogy a $q(x)/x$ polinom (irreducibilis legyen és) irreducibilitását meg tudjuk mutatni a Schönemann-Eisenstein irreducibilitási kritériummal. Mi a $q(x)$ polinom főegyütthatója?

Nem kell Gaussnak lennünk

Válasszuk úgy k-t, hogy $n/2 < k < n$ teljesüljön.

Nem kell Gaussnak lennünk

Válasszuk úgy k-t, hogy $n/2 < k < n$ teljesüljön. Érdemes volna $k = p$ prímet választani?

Nem kell Gaussnak lennünk

Válasszuk úgy k-t, hogy $n/2 < k < n$ teljesüljön. Érdemes volna $k = p$ prímet választani?

$$q(x) =: \sum_{2\nmid j=1}^{p} (-1)^{(j-1)/2} \binom{p}{j} (1 - a^2x^2)^{(p-j)/2} \cdot (ax)^j -$$
$$\sum_{2\nmid j=1}^{n-p} (-1)^{(j-1)/2} \binom{n-p}{j} (1 - b^2x^2)^{(n-p-j)/2} \cdot (bx)^j$$

Nem kell Gaussnak lennünk

Válasszuk úgy k-t, hogy $n/2 < k < n$ teljesüljön. Érdemes volna $k = p$ prímet választani?

$$q(x) =: \sum_{2\nmid j=1}^{p} (-1)^{(j-1)/2} \binom{p}{j} (1 - a^2x^2)^{(p-j)/2} \cdot (ax)^j -$$
$$\sum_{2\nmid j=1}^{n-p} (-1)^{(j-1)/2} \binom{n-p}{j} (1 - b^2x^2)^{(n-p-j)/2} \cdot (bx)^j$$

A főegyüttható $\equiv \pm 1$ (p), ha a-t $a \equiv 1$ (p^2) módon választjuk.

Nem kell Gaussnak lennünk

Válasszuk úgy k-t, hogy $n/2 < k < n$ teljesüljön. Érdemes volna $k = p$ prímet választani?

$$q(x) =: \sum_{2\nmid j=1}^{p} (-1)^{(j-1)/2} \binom{p}{j} (1-a^2x^2)^{(p-j)/2} \cdot (ax)^j - \sum_{2\nmid j=1}^{n-p} (-1)^{(j-1)/2} \binom{n-p}{j} (1-b^2x^2)^{(n-p-j)/2} \cdot (bx)^j$$

A főegyüttható $\equiv \pm 1$ (p), ha a-t $a \equiv 1$ (p^2) módon választjuk.
A konstans tag $q(x)/x$-ben:

$$\binom{p}{1} a - \binom{n-p}{1} b = pa - (n-p)b$$

Nem kell Gaussnak lennünk

Válasszuk úgy k-t, hogy $n/2 < k < n$ teljesüljön. Érdemes volna $k = p$ prímet választani?

$$q(x) =: \sum_{2\nmid j=1}^{p} (-1)^{(j-1)/2} \binom{p}{j} (1-a^2x^2)^{(p-j)/2} \cdot (ax)^j - \sum_{2\nmid j=1}^{n-p} (-1)^{(j-1)/2} \binom{n-p}{j} (1-b^2x^2)^{(n-p-j)/2} \cdot (bx)^j$$

A főegyüttható $\equiv \pm 1$ (p), ha a-t $a \equiv 1$ (p^2) módon választjuk.
A konstans tag $q(x)/x$-ben:

$$\binom{p}{1} a - \binom{n-p}{1} b = pa - (n-p)b \equiv p, \quad (p^2)$$

ha b-t $b \equiv 0$ (p^2) módon választjuk.

Nem kell Gaussnak lennünk

Válasszuk úgy k-t, hogy $n/2 < k < n$ teljesüljön. Érdemes volna $k = p$ prímet választani?

$$q(x) =: \sum_{2\nmid j=1}^{p} (-1)^{(j-1)/2} \binom{p}{j} (1 - a^2x^2)^{(p-j)/2} \cdot (ax)^j - \sum_{2\nmid j=1}^{n-p} (-1)^{(j-1)/2} \binom{n-p}{j} (1 - b^2x^2)^{(n-p-j)/2} \cdot (bx)^j$$

A főegyüttható $\equiv \pm 1$ (p), ha a-t $a \equiv 1$ (p^2) módon választjuk.
A konstans tag $q(x)/x$-ben:

$$\binom{p}{1} a - \binom{n-p}{1} b = pa - (n-p)b \equiv p, \quad (p^2)$$

ha b-t $b \equiv 0$ (p^2) módon választjuk. Ezekkel a választásokkal működik a Schönemann-Eisenstein kritérium!

Nem kell Gaussnak lennünk

Ott tartunk, hogy a $q(x)/x$ egy olyan $p-1$-ed fokú polinom, melynek gyöke a szerkesztendő mennyiség, irreducibilis $\mathbb{Q}$ (a szerkesztési feladatunk alapteste) felett.

Nem kell Gaussnak lennünk

Ott tartunk, hogy a $q(x)/x$ egy olyan $p-1$-ed fokú polinom, melynek gyöke a szerkesztendő mennyiség, irreducibilis $\mathbb{Q}$ (a szerkesztési feladatunk alapteste) felett. Ha tehát $p-1$ nem 2-hatvány, azaz p nem Fermat-prím, készen vagyunk.

Nem kell Gaussnak lennünk

Ott tartunk, hogy a $q(x)/x$ egy olyan $p-1$-ed fokú polinom, melynek gyöke a szerkesztendő mennyiség, irreducibilis $\mathbb{Q}$ (a szerkesztési feladatunk alapteste) felett. Ha tehát $p-1$ nem 2-hatvány, azaz p nem Fermat-prím, készen vagyunk. p-ről eddig csak annyit tettünk fel, hogy $n/2 < p < n$. Van-e ebben az intervallumban olyan prím, ami nem Fermat-prím?

Nem kell Gaussnak lennünk

Ott tartunk, hogy a $q(x)/x$ egy olyan $p-1$-ed fokú polinom, melynek gyöke a szerkesztendő mennyiség, irreducibilis $\mathbb{Q}$ (a szerkesztési feladatunk alapteste) felett. Ha tehát $p-1$ nem 2-hatvány, azaz p nem Fermat-prím, készen vagyunk. p-ről eddig csak annyit tettünk fel, hogy $n/2 < p < n$. Van-e ebben az intervallumban olyan prím, ami nem Fermat-prím? A Fermat-prímek nagyon ritkán vannak...

Nem kell Gaussnak lennünk

Ott tartunk, hogy a $q(x)/x$ egy olyan $p-1$-ed fokú polinom, melynek gyöke a szerkesztendő mennyiség, irreducibilis $\mathbb{Q}$ (a szerkesztési feladatunk alapteste) felett. Ha tehát $p-1$ nem 2-hatvány, azaz p nem Fermat-prím, készen vagyunk. p-ről eddig csak annyit tettünk fel, hogy $n/2 < p < n$. Van-e ebben az intervallumban olyan prím, ami nem Fermat-prím? A Fermat-prímek nagyon ritkán vannak...

Tétel (J. Nagura, 1952)

Minden $25 \leq x$ valós számra van prímszám a nyitott $(x, 6x/5)$ intervallumban.

Nem kell Gaussnak lennünk

Ott tartunk, hogy a $q(x)/x$ egy olyan $p-1$-ed fokú polinom, melynek gyöke a szerkesztendő mennyiség, irreducibilis $\mathbb{Q}$ (a szerkesztési feladatunk alapteste) felett. Ha tehát $p-1$ nem 2-hatvány, azaz p nem Fermat-prím, készen vagyunk. p-ről eddig csak annyit tettünk fel, hogy $n/2 < p < n$. Van-e ebben az intervallumban olyan prím, ami nem Fermat-prím? A Fermat-prímek nagyon ritkán vannak...

Tétel (J. Nagura, 1952)

Minden $25 \leq x$ valós számra van prímszám a nyitott $(x, 6x/5)$ intervallumban.

Ezzel a tétellel kaphatunk két prímet az $(x, 36x/25)$ intervallumban, így $k \geq 25$ esetén van legalább két különböző prím a $(k, 2k)$ intervallumban.

Nem kell Gaussnak lennünk

Ott tartunk, hogy a $q(x)/x$ egy olyan $p-1$-ed fokú polinom, melynek gyöke a szerkesztendő mennyiség, irreducibilis $\mathbb{Q}$ (a szerkesztési feladatunk alapteste) felett. Ha tehát $p-1$ nem 2-hatvány, azaz p nem Fermat-prím, készen vagyunk. p-ről eddig csak annyit tettünk fel, hogy $n/2 < p < n$. Van-e ebben az intervallumban olyan prím, ami nem Fermat-prím? A Fermat-prímek nagyon ritkán vannak...

Tétel (J. Nagura, 1952)

Minden $25 \leq x$ valós számra van prímszám a nyitott $(x, 6x/5)$ intervallumban.

Ezzel a tétellel kaphatunk két prímet az $(x, 36x/25)$ intervallumban, így $k \geq 25$ esetén van legalább két különböző prím a $(k, 2k)$ intervallumban. Addig pedig kézzel könnyen kereshetünk:

n	5	8–13	14–25	26–45	46–85
p	3	7	13	23	43

Köszönöm a figyelmet!