

Przed półwieczem rozpowszechniło się skojarzenie pojęć
odpowieź i **matematyk** w następującym żarcie:

*Gdy po wielogodzinnym błędzeniu w chmurach
lecący balonem ujrzeni pod sobą łąd,
zakrzyknęli do przechodzącego człowieka*

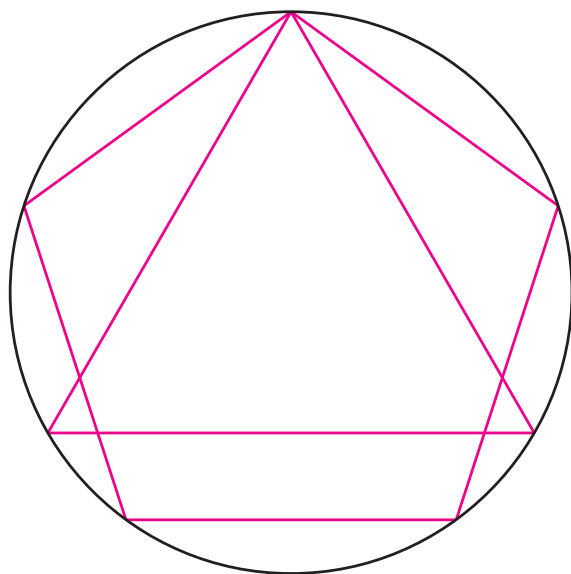
Gdzie jesteśmy?

Ten popatrzył na nich, zastanowił się i odparł:

W balonie!

*Był to bowiem **matematyk**,
a oni zawsze udzielają **odpowiedzi**
przemyślanej, precyzyjnej i do niczego nieprzydatnej.*

Konstrukcja wielokątów foremnych i wywołane przez nią problemy



Rysunek ten Euklides potraktował jako konstrukcję 15-kąta foremnego. Istotnie $2 \cdot \frac{1}{5} - \frac{1}{3} = \frac{1}{15}$.

Wysnuł z tego wniosek, że, gdybyśmy potrafili skonstruować wszystkie p_i -kąty foremne dla różnych liczb pierwszych $p_1, p_2, \dots, p_n$, to potrafilibyśmy skonstruować $2^k \cdot p_1 \cdot p_2 \cdot \dots \cdot p_n$ -kąta foremnego dla dowolnego k .

Rozumowanie to opiera się na tym, że dla dowolnych liczb naturalnych m i n istnieją takie liczby całkowite a i b , że $a \cdot m + b \cdot n = \text{nwd}(n, m)$.

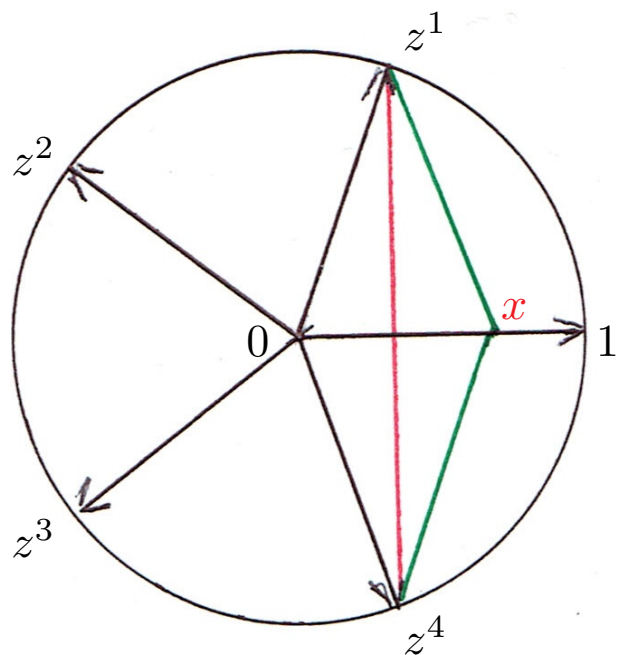
Zatem gdy n i m są względnie pierwsze, mamy $a \cdot m + b \cdot n = 1$, czyli $a \cdot \frac{1}{n} + b \cdot \frac{1}{m} = \frac{1}{m \cdot n}$.

Euklides podał konstrukcję trójkąta równobocznego i pięciokąta foremnego, ale na 3 i 5 lista wymienionych wyżej liczb pierwszych kończyła się. Lista wielokątów foremnego, jakie umiano skonstruować – acz nieskończona – była mocno ograniczona.

Dopiero dwa tysiące lat później sprawę skutecznie zaatakował 19-letni Carl Friedrich Gauss, biorąc na warsztat liczbę 17. Użył w tym celu liczb zespolonych.

Uwaga ogólna: Konstrukcje, o których mowa, to konstrukcje cyrklem i linijką bez podziałki, co analitycznie oznacza, że możemy posługiwać się jedynie równaniami stopnia 1 i 2.

Pierwiastki stopnia n z jedności są wierzchołkami n -kąta foremnego wpisanego w okrąg jednostkowy.



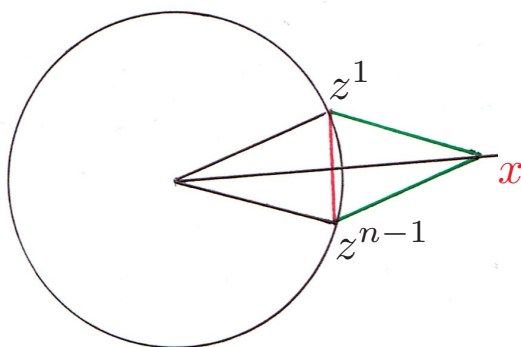
Z symetrii mamy

$$z^{n-1} + z^{n-2} + \dots + z + 1 = 0$$

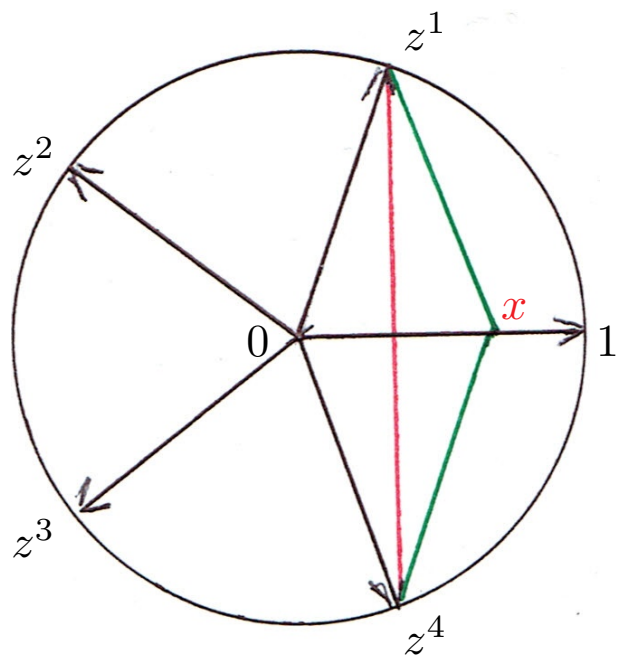
oraz fakt, że

dla każdego k suma $z^k + z^{n-k}$ jest liczbą rzeczywistą.

Gdybyśmy umieli obliczyć za pomocą równań stopnia nie wyższego niż 2 liczbę $x = z + z^{n-1}$, to kreśląc prostopadłą do osi rzeczywistej w odległości $\frac{1}{2}x$ od zera, otrzymalibyśmy zarówno z , jak z^{n-1} , czyli skonstruowalibyśmy n -kąć foremny.



Pierwiastki stopnia n z jedności są wierzchołkami n -kąta foremnego wpisanego w okrąg jednostkowy.



Z symetrii mamy

$$z^{n-1} + z^{n-2} + \dots + z + 1 = 0$$

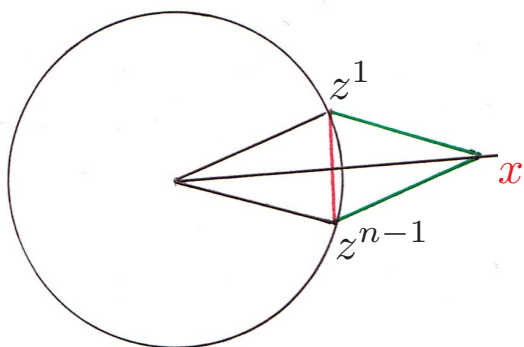
oraz fakt, że

dla każdego k suma $z^k + z^{n-k}$ jest liczbą rzeczywistą.

Gdybyśmy umieli obliczyć za pomocą równań stopnia nie wyższego niż 2 liczbę $x = z + z^{n-1}$, to kreśląc prostopadłą do osi rzeczywistej w odległości $\frac{1}{2}x$ od zera, otrzymalibyśmy zarówno z , jak z^{n-1} , czyli skonstruowalibyśmy n -kąć foremny.

Gauss zrobił to dla $n = 5$ i – w analogiczny sposób – dla $n = 17$.

Idąc dalej pokazał, że metoda ta stosuje się do wszystkich liczb pierwszych postaci $2^{2^k} + 1$.



Najpierw rozdził pierwiastki z jedności:

z^k będzie reprezentowane jako punkt ε_k i jako obrót δ_k ;

mnożenie liczb zespolonych to iloczyn ich modułów i suma ich argumentów
– w przypadku pierwiastków z jedności to po prostu obrót, stąd

$$\delta_i(\varepsilon_j) = \varepsilon_{i \cdot j}.$$

indeks $i \cdot j$ należy brać modulo n , co będzie dalej nie zaznaczane,
podobnie mówiąc o pierwiastkach z jedności będziemy pomijali 1.

Jak łatwo zauważyć poddanie wszystkich pierwiastków z jedności jednemu obrotowi δ_i zachowuje ten zbiór.

Podobnie poddanie jednego pierwiastka ε_i wszystkim obrotom daje nam wszystkie pierwiastki.

Gaussa interesowało, **jakie są inne zbiory niezmiennicze**, czyli jakie podzbiory pierwiastków z jedności dana funkcja δ_i przeprowadza na nie same.

Okazało się, że takie podzbiory istnieją, a łatwiej je zaobserwować, gdy przenumeruje się pierwiastki w skali wykładniczej (lub, jak kto woli, logarytmicznej), czyli

ε_k ma nowy numer **l** , gdy $a^l \equiv k \pmod{n}$,

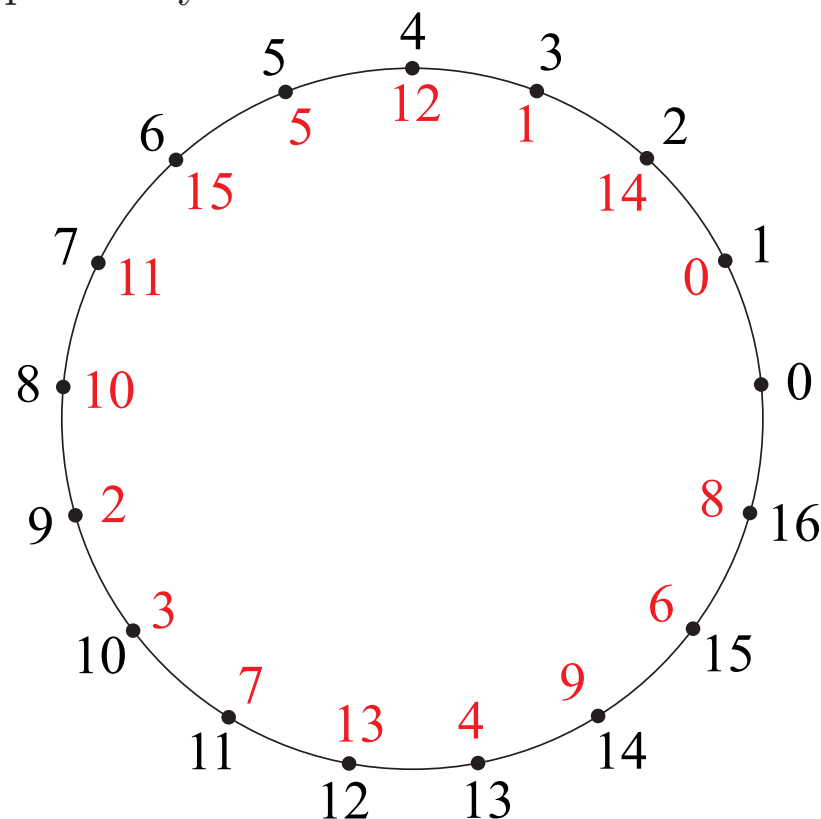
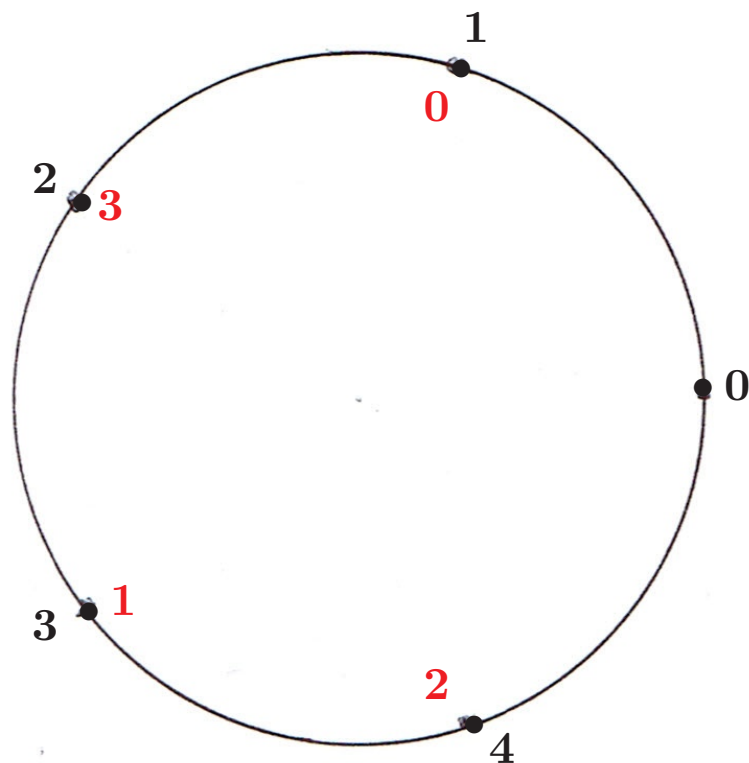
i podobnie δ_i .

Powstaje pytanie, dla jakiej liczby a wszystkie pierwiastki z jedności (różne od 1) otrzymają nowe, różne numery.

pierwszy problem otwarty

Aby takie przenieumerowanie dało wszystkie pierwiastki z jedynki (oprócz 1), potrzeba, by potęgi a dawały $n - 1$, czyli wszystkie reszty modulo n . O takiej sytuacji mówimy, że a jest pierwiastkiem pierwotnym dla n .

Łatwo (?) sprawdzić, że 3 jest pierwiastkiem pierwotnym dla $n = 5$ i dla $n = 17$.



$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 4 + 1 \cdot 5, \\ 3^3 = 2 + 5 \cdot 5, \quad 3^4 = 1 + 18 \cdot 5;$$

$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 10 + 1 \cdot 17, \\ 3^4 = 13 + 4 \cdot 17, \quad 3^5 = 5 + 14 \cdot 17, \quad \dots\dots$$

Dalej będę dla jasności (i daltonistów) będę używał innego zapisu: zamiast k będę pisał (k) .

Dygresja

pierwszy problem otwarty

Dokładniej: a jest pierwiastkiem pierwotnym dla n , gdy potęgi a dają modulo n wszystkie reszty względnie pierwsze z n ;
w przypadku, gdy n jest liczbą pierwszą, reszt tych jest $n - 1$.

Posługując się funkcją φ Eulera

$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot \dots \cdot (1 - \frac{1}{p_k})$, gdzie $p_1, \dots, p_k$ to wszystkie różne dzielniki pierwsze n (ona zlicza liczby nie większe i względnie pierwsze z n),

można wykazać, że **liczba n ma pierwiastki pierwotne wtw** gdy jest potęgą nieparzystej liczby pierwszej, podwojeniem takiej liczby, bądź jest równa 2 lub 4.

Nie jest jednak znana procedura pozwalająca na stwierdzenie, dla jakich n dana liczba a jest pierwiastkiem pierwotnym.

Można, oczywiście, sprawdzić to w każdym konkretnym przypadku (mniej niż n kroków),
podobnie jak do sprawdzenia, czy liczba p jest pierwsza, wystarczy wykonać dzielenia jej przez wszystkie liczby mniejsze od $\sqrt{p}$.

Tu widać, jak zmyślnie został obrany temat tej Szkoły:

nie wszystkiemu, co formalnie jest odpowiedzią, rangę odpowiedzi chcemy przyznać.

Bo chciałoby się mieć jakąś "maszynkę" do odpowiadania na pytania, czy a jest pierwiastkiem pierwotnym dla n , w stylu np. cechy podzielności przez 9 czy 13.

Dygresja

pierwszy problem otwarty

Pierwiastki pierwotne interesowały zresztą Gaussa jeszcze w szkole powszechnej.

Karolek (nudząc się w szkole) sprawdził, dla których liczb mniejszych od 1000 liczba 10 jest pierwiastkiem pierwotnym. Są wśród nich np. 7, 17, 19, 23, 29, 97, 337, a nie ma np. 3, 11, 13.

Różni popularyzatorzy w miejsce tego faktu wstawiają historyjkę o tym, jak uczeń–Gauss zręcznie zsumował liczby od 1 do 100.

Gauss zresztą korzystał z pozornie innej metody niż potęgowanie: sprawdzał, kiedy $\frac{1}{n}$ ma rozwinięcie okresowe $(n - 1)$ -miejscowe.

Tak np. $\frac{1}{7} = 0, (142857)$, a przenumerowując wierzchołki 7-kąta za pomocą liczby 10 otrzymalibyśmy kolejno 1, 3, 2, 6, 4, 5.

Ale nawet odpowiedź dla jakich n liczba 10 jest pierwiastkiem pierwotnym nie jest znana.

Po przenieumerowaniu łatwo zobaczyć zbiory niezmiennicze, bo

$$\delta_{(i)}(\varepsilon_{(j)}) = \varepsilon_{(i+j)}.$$

Np. dla parzystego (i) funkcja $\delta_{(i)}$ zachowuje zbiór punktów o (nowych) indeksach parzystych i zbiór punktów o indeksach nieparzystych., a dla nieparzystego (i) te zbiory zamienia.

Łatwo zauważyć, że gdy mamy punktów więcej (jak np. dla $n = 17$) podobnie będzie dla zbiorów punktów o indeksach mających tę samą resztę z dzielenia przez 4, czy przez 8.

A gdybyśmy rozważali inne liczby pierwsze p , dla których $p - 1$ jest potęgą dwójki, to samo pojawiłoby się dla reszt z 16, 32,...

Te **zbiory niezmiennicze posłużą do wyprodukowania równań kwadratowych** prowadzących do znalezienia odpowiednio liczb rzeczywistych $\varepsilon_{(0)} + \varepsilon_{(2)}$ w przypadku $n = 5$, a także $\varepsilon_{(0)} + \varepsilon_{(8)}$ dla $n = 17$, czyli do konstrukcji odpowiednio 5-kąta foremnego i 17-kąta foremnego, bo pierwsza z tych sum to $z^1 + z^4$, a druga to $z^1 + z^{16}$.

Po przenieumerowaniu łatwo zobaczyć zbiory niezmiennicze, bo

$$\delta_{(i)}(\varepsilon_{(j)}) = \varepsilon_{(i+j)}.$$

Np. dla parzystego (i) funkcja $\delta_{(i)}$ zachowuje zbiór punktów o (nowych) indeksach parzystych i zbiór punktów o indeksach nieparzystych., a dla nieparzystego (i) te zbiory zamienia.

Łatwo zauważyć, że gdy mamy punktów więcej (jak np. dla $n = 17$) podobnie będzie dla zbiorów punktów o indeksach mających tę samą resztę z dzielenia przez 4, czy przez 8.

A gdybyśmy rozważali inne liczby pierwsze p , dla których $p - 1$ jest potęgą dwójki, to samo pojawiłoby się dla reszt z 16, 32,...

Te **zbiory niezmiennicze posłużą do wyprodukowania równań kwadratowych** prowadzących do znalezienia odpowiednio liczb rzeczywistych $\varepsilon_{(0)} + \varepsilon_{(2)}$ w przypadku $n = 5$, a także $\varepsilon_{(0)} + \varepsilon_{(8)}$ dla $n = 17$, czyli do konstrukcji odpowiednio 5-kąta foremnego i 17-kąta foremnego, bo pierwsza z tych sum to $z^1 + z^4$, a druga to $z^1 + z^{16}$.

W tym celu wprowadzimy kilka nowych symboli. Definiujemy:

$\sigma_{i,j}$ to suma tych pierwiastków, których nowe indeksy dają przy dzieleniu przez i resztę j .

$$s_2 := \sigma_{2,0} + \sigma_{2,1}, \quad t_2 := \sigma_{2,0} \cdot \sigma_{2,1}$$

a w przypadku $n = 17$ także

$$s_4 := \sigma_{4,0} + \sigma_{4,2}, \quad t_4 := \sigma_{4,0} \cdot \sigma_{4,2} \quad \text{ i } \quad s_8 := \sigma_{8,0} + \sigma_{8,4}, \quad t_8 := \sigma_{8,0} \cdot \sigma_{8,4}.$$

Gdy obliczymy te liczby, to (wobec wzorów Viète'a) obliczymy te sigmy z równań

$$x^2 - s_k x + t_k = 0.$$

skąd ten pomysł?

To **standardowe obliczenia** dla $n = 5$:

$$1 + z + z^2 + z^3 + z^4 = 0,$$

$$1 + z + z^2 + \frac{1}{z^2} + \frac{1}{z} = 0,$$

$$1 + (z + \frac{1}{z}) + (z^2 + \frac{1}{z^2}) = 0,$$

$$\text{ale ponieważ } (z + \frac{1}{z})^2 = z^2 + 2 + \frac{1}{z^2},$$

$$\text{mamy } 1 + (z + \frac{1}{z}) + (z + \frac{1}{z})^2 - 2 = 0.$$

Porządkując i podstawiając $x = z + \frac{1}{z}$ otrzymujemy $x^2 + x - 1 = 0$,

skąd $x = \frac{\sqrt{5}-1}{2}$ (bierzemy pierwiastek dodatni).

Metoda zaproponowaną przez **Gaussa** liczylibyśmy tak:

$$\sigma_{2,0} = \varepsilon_{(0)} + \varepsilon_{(2)}, \quad \sigma_{2,1} = \varepsilon_{(1)} + \varepsilon_{(3)},$$

$$s_2 = \sigma_{2,0} + \sigma_{2,1} = (\varepsilon_{(0)} + \varepsilon_{(2)}) + (\varepsilon_{(1)} + \varepsilon_{(3)}) = \varepsilon_{(0)} + \varepsilon_{(1)} + \varepsilon_{(2)} + \varepsilon_{(3)} = -1,$$

$$\begin{aligned} t_2 &= \sigma_{2,0} \cdot \sigma_{2,1} = (\varepsilon_{(0)} + \varepsilon_{(2)}) \cdot (\varepsilon_{(1)} + \varepsilon_{(3)}) = \varepsilon_{(0)} \cdot \varepsilon_{(1)} + \varepsilon_{(0)} \cdot \varepsilon_{(3)} + \varepsilon_{(2)} \cdot \varepsilon_{(1)} + \varepsilon_{(2)} \cdot \varepsilon_{(3)} = \\ &= \varepsilon_{(0)} \cdot \varepsilon_{(1)} + \varepsilon_{(1)} \cdot \varepsilon_{(2)} + \varepsilon_{(2)} \cdot \varepsilon_{(3)} + \varepsilon_{(3)} \cdot \varepsilon_{(0)} = \\ &= \delta_{(0)}(\varepsilon_{(0)} \cdot \varepsilon_{(1)}) + \delta_{(1)}(\varepsilon_{(0)} \cdot \varepsilon_{(1)}) + \delta_{(2)}(\varepsilon_{(0)} \cdot \varepsilon_{(1)}) + \delta_{(3)}(\varepsilon_{(0)} \cdot \varepsilon_{(1)}) = \\ &= \varepsilon_{(0)} + \varepsilon_{(1)} + \varepsilon_{(2)} + \varepsilon_{(3)} = -1. \end{aligned}$$

A więc równanie $x^2 - s_2x + t_2 = 0$ przybiera postać $x^2 + x - 1 = 0$.

Zysk techniczny jest wątpliwy.

Ale stosując pierwszą metodę do $n = 17$ mielibyśmy do czynienia z równaniem stopnia 8.

Liczmy metodą Gaussa

$$\sigma_{2,0} = \varepsilon_{(0)} + \varepsilon_{(2)} + \dots + \varepsilon_{(14)}, \quad \sigma_{2,1} = \varepsilon_{(1)} + \varepsilon_{(3)} + \dots + \varepsilon_{(15)},$$

$$s_2 = \sigma_{2,0} + \sigma_{2,1} = -1 \text{ jak poprzednio,}$$

$$\begin{aligned} t_2 &= \sigma_{2,0} \cdot \sigma_{2,1} = \varepsilon_{(0)}\varepsilon_{(1)} + \varepsilon_{(0)}\varepsilon_{(3)} + \dots + \varepsilon_{(14)}\varepsilon_{(13)} + \varepsilon_{(14)}\varepsilon_{(15)} = \\ &= \varepsilon_{(0)}\varepsilon_{(1)} + \varepsilon_{(1)}\varepsilon_{(2)} + \dots + \varepsilon_{(14)}\varepsilon_{(15)} + \varepsilon_{(15)}\varepsilon_{(0)} + \\ &\quad + \varepsilon_{(0)}\varepsilon_{(3)} + \varepsilon_{(1)}\varepsilon_{(4)} + \dots + \varepsilon_{(14)}\varepsilon_{(1)} + \varepsilon_{(15)}\varepsilon_{(2)} + \\ &\quad + \varepsilon_{(0)}\varepsilon_{(5)} + \varepsilon_{(1)}\varepsilon_{(6)} + \dots + \varepsilon_{(14)}\varepsilon_{(3)} + \varepsilon_{(15)}\varepsilon_{(4)} + \\ &\quad + \varepsilon_{(0)}\varepsilon_{(7)} + \varepsilon_{(1)}\varepsilon_{(8)} + \dots + \varepsilon_{(14)}\varepsilon_{(5)} + \varepsilon_{(14)}\varepsilon_{(6)} = \end{aligned}$$

Liczymy metodą Gaussa

$$\sigma_{2,0} = \varepsilon_{(0)} + \varepsilon_{(2)} + \dots + \varepsilon_{(14)}, \quad \sigma_{2,1} = \varepsilon_{(1)} + \varepsilon_{(3)} + \dots + \varepsilon_{(15)},$$

$$s_2 = \sigma_{2,0} + \sigma_{2,1} = -1 \text{ jak poprzednio,}$$

$$\begin{aligned} t_2 &= \sigma_{2,0} \cdot \sigma_{2,1} = \varepsilon_{(0)}\varepsilon_{(1)} + \varepsilon_{(0)}\varepsilon_{(3)} + \dots + \varepsilon_{(14)}\varepsilon_{(13)} + \varepsilon_{(14)}\varepsilon_{(15)} = \\ &= \varepsilon_{(0)}\varepsilon_{(1)} + \varepsilon_{(1)}\varepsilon_{(2)} + \dots + \varepsilon_{(14)}\varepsilon_{(15)} + \varepsilon_{(15)}\varepsilon_{(0)} + \\ &\quad + \varepsilon_{(0)}\varepsilon_{(3)} + \varepsilon_{(1)}\varepsilon_{(4)} + \dots + \varepsilon_{(14)}\varepsilon_{(1)} + \varepsilon_{(15)}\varepsilon_{(2)} + \\ &\quad + \varepsilon_{(0)}\varepsilon_{(5)} + \varepsilon_{(1)}\varepsilon_{(6)} + \dots + \varepsilon_{(14)}\varepsilon_{(3)} + \varepsilon_{(15)}\varepsilon_{(4)} + \\ &\quad + \varepsilon_{(0)}\varepsilon_{(7)} + \varepsilon_{(1)}\varepsilon_{(8)} + \dots + \varepsilon_{(14)}\varepsilon_{(5)} + \varepsilon_{(14)}\varepsilon_{(6)} = \\ &= \left(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(1)}) + \delta_{(1)}(\varepsilon_{(0)}\varepsilon_{(1)}) + \dots + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(1)}) + \delta_{(15)}(\varepsilon_{(0)}\varepsilon_{(1)}) \right) + \\ &\quad + \left(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(3)}) + \delta_{(1)}(\varepsilon_{(0)}\varepsilon_{(3)}) + \dots + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(3)}) + \delta_{(15)}(\varepsilon_{(0)}\varepsilon_{(3)}) \right) + \\ &\quad + \left(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(5)}) + \delta_{(1)}(\varepsilon_{(0)}\varepsilon_{(5)}) + \dots + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(5)}) + \delta_{(15)}(\varepsilon_{(0)}\varepsilon_{(5)}) \right) + \\ &\quad + \left(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(7)}) + \delta_{(1)}(\varepsilon_{(0)}\varepsilon_{(7)}) + \dots + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(7)}) + \delta_{(15)}(\varepsilon_{(0)}\varepsilon_{(7)}) \right) = \\ &= 4 \cdot (\varepsilon_{(0)} + \varepsilon_{(1)} + \dots + \varepsilon_{(14)} + \varepsilon_{(15)}) = 4 \cdot (-1) = -4. \end{aligned}$$

Stąd mamy równanie $x^2 + x - 4 = 0$ na $\sigma_{2,0}$ (dodatni) i $\sigma_{2,1}$.

Konkretnie $\sigma_{2,0} = \frac{\sqrt{17}-1}{2}$, ale wartościami liczbowymi nie będziemy się zajmowali – podam tylko wartość liczbową końcowego wyniku.

rachunki dla $n = 17$ cd.

Idziemy dalej:

$$\sigma_{4,0} = \varepsilon_{(0)} + \varepsilon_{(4)} + \varepsilon_{(8)} + \varepsilon_{(12)}, \quad \sigma_{4,2} = \varepsilon_{(2)} + \varepsilon_{(6)} + \varepsilon_{(10)} + \varepsilon_{(14)},$$

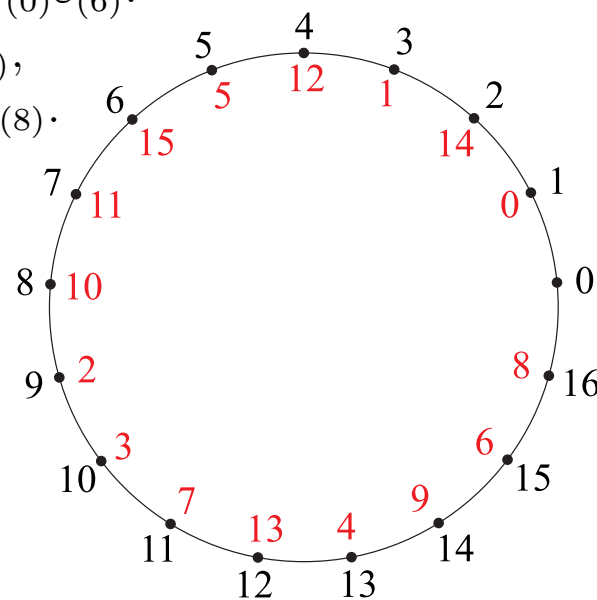
$$s_4 = \sigma_{4,0} + \sigma_{4,2} = \sigma_{2,0}, \text{ co przed chwilą obliczyliśmy,}$$

$$\begin{aligned} t_4 &= \sigma_{4,0} \cdot \sigma_{4,2} = \varepsilon_{(0)}\varepsilon_{(2)} + \varepsilon_{(0)}\varepsilon_{(6)} + \dots + \varepsilon_{(12)}\varepsilon_{(10)} + \varepsilon_{(12)}\varepsilon_{(14)} = \\ &= \varepsilon_{(0)}\varepsilon_{(2)} + \varepsilon_{(2)}\varepsilon_{(4)} + \dots + \varepsilon_{(12)}\varepsilon_{(14)} + \varepsilon_{(14)}\varepsilon_{(0)} + \\ &\quad + \varepsilon_{(0)}\varepsilon_{(6)} + \varepsilon_{(2)}\varepsilon_{(8)} + \dots + \varepsilon_{(12)}\varepsilon_{(2)} + \varepsilon_{(14)}\varepsilon_{(4)} = \\ &= \left(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(2)}) + \delta_{(2)}(\varepsilon_{(0)}\varepsilon_{(2)}) + \dots + \delta_{(12)}(\varepsilon_{(0)}\varepsilon_{(2)}) + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(2)}) \right) + \\ &\quad + \left(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(6)}) + \delta_{(2)}(\varepsilon_{(0)}\varepsilon_{(6)}) + \dots + \delta_{(12)}(\varepsilon_{(0)}\varepsilon_{(6)}) + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(6)}) \right). \end{aligned}$$

I nie ma rady, trzeba dowiedzieć się, co to jest $\varepsilon_{(0)}\varepsilon_{(2)}$ i $\varepsilon_{(0)}\varepsilon_{(6)}$:

$$\varepsilon_{(0)} \cdot \varepsilon_{(2)} = \varepsilon_1 \cdot \varepsilon_9 = z^1 \cdot z^9 = z^{10} = \varepsilon_{10} = \varepsilon_{(3)},$$

$$\varepsilon_{(0)} \cdot \varepsilon_{(6)} = \varepsilon_1 \cdot \varepsilon_{15} = z^1 \cdot z^{15} = z^{16} = \varepsilon_{16} = \varepsilon_{(8)}.$$



rachunki dla $n = 17$ cd.

Idziemy dalej:

$$\sigma_{4,0} = \varepsilon_{(0)} + \varepsilon_{(4)} + \varepsilon_{(8)} + \varepsilon_{(12)}, \quad \sigma_{4,2} = \varepsilon_{(2)} + \varepsilon_{(6)} + \varepsilon_{(10)} + \varepsilon_{(14)},$$

$$s_4 = \sigma_{4,0} + \sigma_{4,2} = \sigma_{2,0}, \text{ co przed chwilą obliczyliśmy,}$$

$$\begin{aligned} t_4 &= \sigma_{4,0} \cdot \sigma_{4,2} = \varepsilon_{(0)}\varepsilon_{(2)} + \varepsilon_{(0)}\varepsilon_{(6)} + \dots + \varepsilon_{(12)}\varepsilon_{(10)} + \varepsilon_{(12)}\varepsilon_{(14)} = \\ &= \varepsilon_{(0)}\varepsilon_{(2)} + \varepsilon_{(2)}\varepsilon_{(4)} + \dots + \varepsilon_{(12)}\varepsilon_{(14)} + \varepsilon_{(14)}\varepsilon_{(0)} + \\ &\quad + \varepsilon_{(0)}\varepsilon_{(6)} + \varepsilon_{(2)}\varepsilon_{(8)} + \dots + \varepsilon_{(12)}\varepsilon_{(2)} + \varepsilon_{(14)}\varepsilon_{(4)} = \\ &= \left(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(2)}) + \delta_{(2)}(\varepsilon_{(0)}\varepsilon_{(2)}) + \dots + \delta_{(12)}(\varepsilon_{(0)}\varepsilon_{(2)}) + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(2)}) \right) + \\ &\quad + \left(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(6)}) + \delta_{(2)}(\varepsilon_{(0)}\varepsilon_{(6)}) + \dots + \delta_{(12)}(\varepsilon_{(0)}\varepsilon_{(6)}) + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(6)}) \right). \end{aligned}$$

I nie ma rady, trzeba dowiedzieć się, co to jest $\varepsilon_{(0)}\varepsilon_{(2)}$ i $\varepsilon_{(0)}\varepsilon_{(6)}$:

$$\varepsilon_{(0)} \cdot \varepsilon_{(2)} = \varepsilon_1 \cdot \varepsilon_9 = z^1 \cdot z^9 = z^{10} = \varepsilon_{10} = \varepsilon_{(3)},$$

$$\varepsilon_{(0)} \cdot \varepsilon_{(6)} = \varepsilon_1 \cdot \varepsilon_{15} = z^1 \cdot z^{15} = z^{16} = \varepsilon_{16} = \varepsilon_{(8)}.$$

Zatem

$$\begin{aligned} t_4 &= \left(\delta_{(0)}(\varepsilon_{(3)}) + \delta_{(2)}(\varepsilon_{(3)}) + \dots + \delta_{(12)}(\varepsilon_{(3)}) + \delta_{(14)}(\varepsilon_{(3)}) \right) + \\ &\quad + \left(\delta_{(0)}(\varepsilon_{(8)}) + \delta_{(2)}(\varepsilon_{(8)}) + \dots + \delta_{(12)}(\varepsilon_{(8)}) + \delta_{(14)}(\varepsilon_{(8)}) \right) = \sigma_{2,1} + \sigma_{2,0} = -1. \end{aligned}$$

Wobec tego równanie na $\sigma_{4,0}$ i $\sigma_{4,2}$ ma postać $x^2 - \sigma_{2,0}x - 1 = 0$,

co chętny może sobie obliczyć.

rachunki dla $n = 17$ cd.

Kolej na ostatnie równanie, które niestety okaże się przedostatnim.

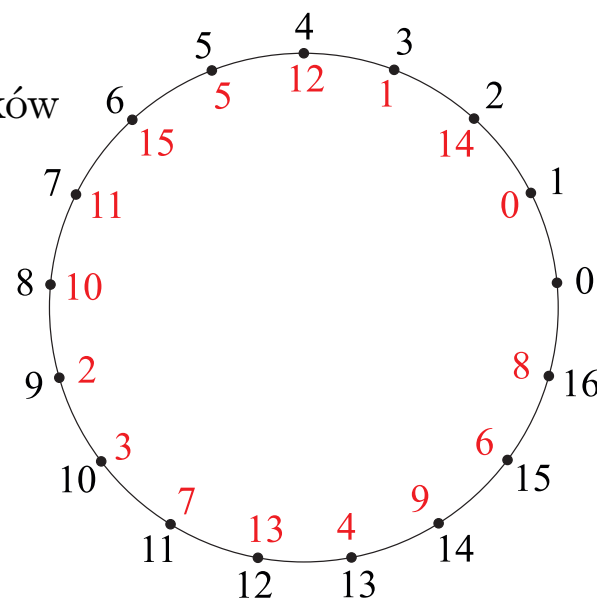
Oczywiście $s_8 = \sigma_{8,0} + \sigma_{8,4} = \sigma_{4,0}$.

$$\begin{aligned} t_8 &= \sigma_{8,0} \cdot \sigma_{8,4} = (\varepsilon_{(0)} + \varepsilon_{(8)}) \cdot (\varepsilon_{(4)} + \varepsilon_{(12)}) = \\ &= \varepsilon_{(0)}\varepsilon_{(4)} + \varepsilon_{(4)}\varepsilon_{(8)} + \varepsilon_{(8)}\varepsilon_{(12)} + \varepsilon_{(12)}\varepsilon_{(0)} = \\ &= \left(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(4)}) + \delta_{(4)}(\varepsilon_{(0)}\varepsilon_{(4)}) + \delta_{(8)}(\varepsilon_{(0)}\varepsilon_{(4)}) + \delta_{(12)}(\varepsilon_{(0)}\varepsilon_{(4)}) \right) = \\ &= \left(\delta_{(0)}(\varepsilon_{(9)}) + \delta_{(4)}(\varepsilon_{(9)}) + \delta_{(8)}(\varepsilon_{(9)}) + \delta_{(14)}(\varepsilon_{(9)}) \right) = \sigma_{4,1} \end{aligned}$$

$$\text{bo } \varepsilon_{(0)}\varepsilon_{(4)} = \varepsilon_1\varepsilon_{13} = z^1 \cdot z^{13} = z^{14} = \varepsilon_{14} = \varepsilon_{(9)}.$$

Zatem poszukiwane przez nas $\sigma_{8,0}$ to większy z pierwiastków równania $x^2 - \sigma_{4,0}x + \sigma_{4,1} = 0$.

Ale $\sigma_{4,1}$ dopiero trzeba obliczyć.



rachunki dla $n = 17$ cd.

A więc liczymy

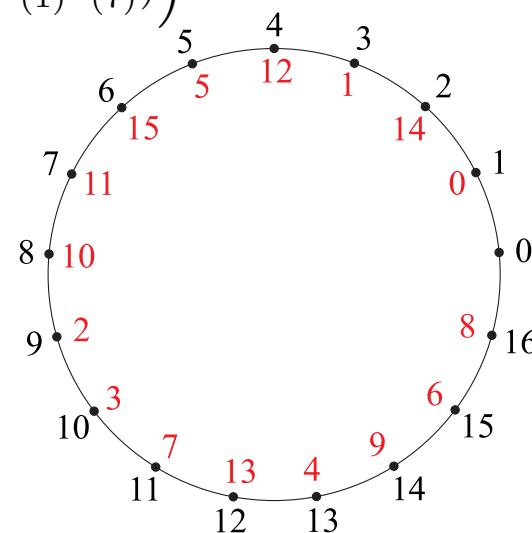
$$\sigma_{4,1} + \sigma_{4,3} = \sigma_{2,1}$$

$$\begin{aligned} \sigma_{4,1} \cdot \sigma_{4,3} &= (\varepsilon_{(1)} + \varepsilon_{(5)} + \varepsilon_{(9)} + \varepsilon_{(13)}) \cdot (\varepsilon_{(3)} + \varepsilon_{(7)} + \varepsilon_{(11)} + \varepsilon_{(15)}) = \\ &= \varepsilon_{(1)}\varepsilon_{(3)} + \varepsilon_{(1)}\varepsilon_{(7)} + \dots + \varepsilon_{(13)}\varepsilon_{(11)} + \varepsilon_{(13)}\varepsilon_{(15)} = \\ &= \varepsilon_{(1)}\varepsilon_{(3)} + \varepsilon_{(3)}\varepsilon_{(5)} + \dots + \varepsilon_{(13)}\varepsilon_{(15)} + \varepsilon_{(15)}\varepsilon_{(1)} + \\ &\quad + \varepsilon_{(1)}\varepsilon_{(7)} + \varepsilon_{(3)}\varepsilon_{(9)} + \dots + \varepsilon_{(13)}\varepsilon_{(3)} + \varepsilon_{(15)}\varepsilon_{(5)} = \\ &= \left(\delta_{(0)}(\varepsilon_{(1)}\varepsilon_{(3)}) + \delta_{(2)}(\varepsilon_{(1)}\varepsilon_{(3)}) + \dots + \delta_{(12)}(\varepsilon_{(1)}\varepsilon_{(3)}) + \delta_{(14)}(\varepsilon_{(1)}\varepsilon_{(3)}) \right) + \\ &\quad + \left(\delta_{(0)}(\varepsilon_{(1)}\varepsilon_{(7)}) + \delta_{(2)}(\varepsilon_{(1)}\varepsilon_{(7)}) + \dots + \delta_{(12)}(\varepsilon_{(1)}\varepsilon_{(7)}) + \delta_{(14)}(\varepsilon_{(1)}\varepsilon_{(7)}) \right) = \\ &= \left(\delta_{(0)}(\varepsilon_{(4)}) + \delta_{(2)}(\varepsilon_{(4)}) + \dots + \delta_{(12)}(\varepsilon_{(4)}) + \delta_{(14)}(\varepsilon_{(4)}) \right) + \\ &\quad + \left(\delta_{(0)}(\varepsilon_{(9)}) + \delta_{(2)}(\varepsilon_{(9)}) + \dots + \delta_{(12)}(\varepsilon_{(9)}) + \delta_{(14)}(\varepsilon_{(9)}) \right) = \\ &= \sigma_{2,0} + \sigma_{2,1} = -1 \end{aligned}$$

$$\begin{aligned} \text{bo } \varepsilon_{(1)} \cdot \varepsilon_{(3)} &= \varepsilon_3 \cdot \varepsilon_{10} = z^3 \cdot z^{10} = z^{13} = \varepsilon_{13} = \varepsilon_{(4)}, \\ \varepsilon_{(1)} \cdot \varepsilon_{(7)} &= \varepsilon_3 \cdot \varepsilon_{11} = z^3 \cdot z^{11} = z^{14} = \varepsilon_{16} = \varepsilon_{(9)}. \end{aligned}$$

Mamy więc równanie $x^2 - \sigma_{2,1}x - 1 = 0$ na $\sigma_{4,1}$ i $\sigma_{4,3}$,

co pozwala rozwiązać końcowe równanie $x^2 - \sigma_{4,0}x + \sigma_{4,1} = 0$.



rachunki dla $n = 17$ – koniec, i co dalej?

Równanie $x^2 - \sigma_{4,0}x + \sigma_{4,1} = 0$. ma rozwiązanie o wartości liczbowej (uzyskanej po obliczeniu wartości liczbowych poprzednich czterech równań) dość niebanalnej

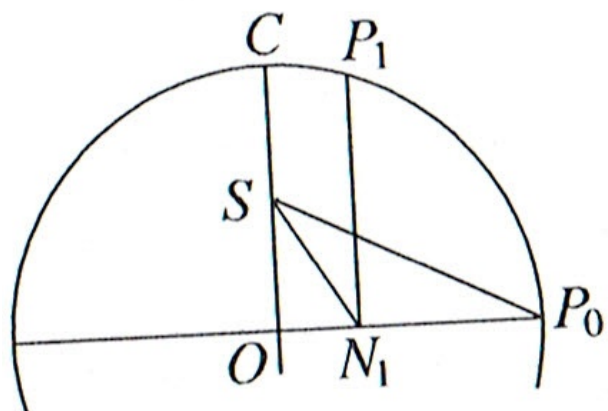
$$\sigma_{8,0} = \frac{1}{8} \left(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}} \right) + \frac{1}{4} \sqrt{17 + 3\sqrt{17} - \sqrt{170 + 38\sqrt{17}}}.$$

Nasuwa to kilka pytań.

- Trudno sobie wyobrazić, jak skonstruować odcinek o takiej długości. Ale skoro dowiedliśmy istnienia konstrukcji 17-kąta foremnego, to jak machać linijką i cyrklem, by go efektywnie nakreślić?
- Metoda Gaussa daje się uogólnić na wszystkie liczby pierwsze p , takie że $p - 1$ jest potęgą dwójki. Ile jest takich liczb pierwszych?
- Czy można skonstruować wielokąty foremne dla liczb pierwszych, których metoda Gaussa nie chwyta (i, ewentualnie, dla jakich)?
- I wreszcie, czy można skonstruować m -kąty foremne, gdy m nie jest liczbą postaci podanej przez Euklidesa (czyli $2^k \cdot p_1 \cdot p_2 \cdot \dots \cdot p_n$, gdzie p_i są pierwsze i różne)?

Kolejno na nie odpowiemy.

Zaczniemy od najłatwiejszego.



Efektywna konstrukcja 5-kąta

jakoby od Ptolemeusza

Dany okrąg o .

O, P_0, C : OP_0 i OC to połowy
prostopadłych średnic,

S : środek OC ,

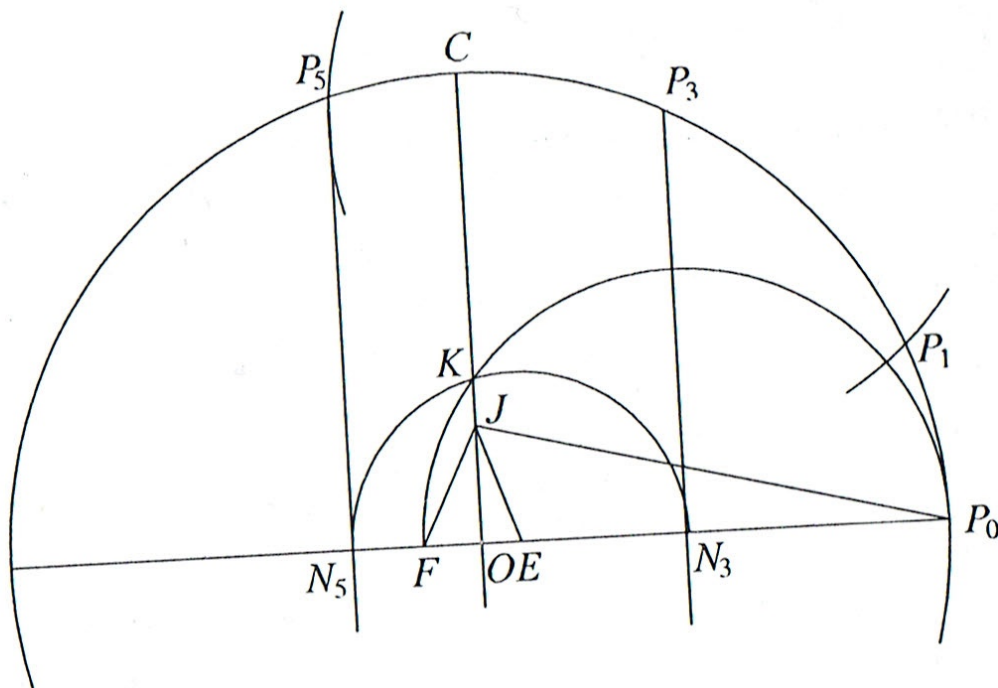
N_1 : na OP_0 i dwusiecznej $\sphericalangle OSP_0$,

P_1 : na o i $P_1N_1 \perp P_0O$.

P_0P_1 to kolejne wierzchołki pięciokąta foremnego.

Istotnie, posługując się twierdzeniem Pitagorasa i twierdzeniem o dwusiecznej,

łatwo stwierdzamy, że $|ON_1| = \frac{\sqrt{5} - 1}{4}$.



Efektywna konstrukcja 17-kąta

Dany okrąg o .

O, P_0, C : OP_0 i OC to połowy
prostopadłych średnic,

J : $|OJ| = \frac{1}{4}|OC|$ na OC ,

E : $\sphericalangle OJE = \frac{1}{4}\sphericalangle OJP_0$ na OP_0 ,

F : $\sphericalangle FJE = 45^\circ$ na prostej OP_0 ,

K : na OC i półokręgu o średnicy P_0F ,

N_3, N_5 : na prostej OP_0 i półokręgu o środku E przez K (N_3 bliżej P_0),

P_3, P_5 : odpowiednio na okręgu o i prostopadłych do OP_0 przez N_3 i N_5 ,

P_1 : $|P_1P_3| = |P_5P_3|$ na okręgu o .

Wszystkie punkty P_i są wierzchołkami 17-kąta wpisanego w o ,
ale stwierdzenie tego jest dość niebanalne.

drugi problem otwarty

Jeśli p jest liczbą pierwszą i $p - 1$ jest potęgą dwójki, to $p = 2^{2^k} + 1$ dla pewnego k ,
albowiem $2^{2q+1} + 1 = (2 + 1)(2^{2q} - 2^{2q-1} + 2^{2q-2} - \dots + 2^2 - 2 + 1)$.

Pozostaje problem,

które liczby postaci $p = 2^{2^k} + 1$ dla pewnego k (zwane liczbami Fermata) są pierwsze?

Do listy Euklidesa, złożonej z 3 i 5 dopisano 17, 257 i 65537, czyli mamy liczby Fermata dla $k = 0, 1, 2, 3, 4$ i – mimo starań – nic więcej.

Na początku XVIII wieku (dopiero!) Euler udowodnił, że nie wszystkie liczby Fermata są pierwsze, rozkładając liczbę Fermata dla $k = 5$, czyli $2^{2^5} + 1 = 4294967297$.

$$\begin{aligned} 2^{2^5} + 1 &= 2^{32} + 5^4 \cdot 2^{28} - (5^4 \cdot 2^{28} - 1) = 2^{28}(2^4 + 5^4) - (5^2 \cdot 2^{14} + 1)(5 \cdot 2^7 + 1)(5 \cdot 2^7 - 1) = \\ &= 641 \cdot (2^{28} - (5^2 \cdot 2^{14} + 1) \cdot 639). \end{aligned}$$

Jak widać, metoda Eulera nie sugeruje uogólnienia, podobnie jak sposoby, jakimi później powiększono sporą (ale skończoną) listę "niepierwszych" liczb Fermata.

Są wśród nich np. liczby dla k równego 6, 7, 8, 9, ale też np. 21, 23, 36, 38, 73 (tu najmniejszym dzielnikiem jest $5 \cdot 2^{75} + 1$), czy 1945.

Tak więc **nie wiemy, czy istnieje więcej niż pięć liczb pierwszych Fermata.**

Oczywiście (?) rachunki metodą Gaussa dla wielokątów foremnych o 257 i 65537 wierzchołkach przeprowadzono, co można sprawdzić w muzeum w Getyndze.

inaczej się nie da

Na ostatnie dwa pytania odpowiedź jest **NIE**.

Udowodnił to (41 lat po wyniku Gaussa) **Pierre Laurent Wantzel** (1814–1848).

Dziś dowodzimy tego posługując się teorią Galois, której Wantzel nie znał, ale którą w potrzebnym zakresie skonstruował.

Zauważył, że rozwiązania kolejnych równań kwadratowych należą do kolejnych rozszerzeń ciała liczb wymiernych $\mathfrak{F}_0$ o potrzebny (ta "delta") pierwiastek kwadratowy.

Oto przykład rozumowania, jakim się posługiwał.

Mamy równanie $x^3 + ax^2 + bx + c = 0$ o pierwiastkach x_1, x_2, x_3 . Równanie to pojawiło się w $\mathfrak{F}_{k+1}$, które jest rozszerzeniem $\mathfrak{F}_k$ o pierwiastek z w , czyli składa się z liczb postaci $p + q\sqrt{w}$, gdzie p, q, w należą do $\mathfrak{F}_k$.

W tej sytuacji (co najmniej) jeden z pierwiastków też należy do $\mathfrak{F}_k$.

Jeśli bowiem jednym z pierwiastków jest $s + t\sqrt{w}$, to również jest nim $s - t\sqrt{w}$.

Podstawiając do równania pierwszy z nich otrzymujemy

$$s^3 + 3s^2t\sqrt{w} + 3st^2w + t^3w\sqrt{w} + as^2 + 2ast\sqrt{w} + at^2w + bs + bt\sqrt{w} + c = 0,$$

$$\text{czyli } (s^3 + 3st^2w + as^2 + at^2w + bs + c) + \sqrt{w}(3s^2t + t^3w + 2ast + bt) = 0,$$

a więc oba te nawiasy muszą być równe 0, wobec czego wszystko jedno, czy łączy je $+$ czy $-$.

Z wzorów Viète'a $x_1 + x_2 + x_3 = -a$, a więc $x_3 = -a - (s + t\sqrt{w} + s - t\sqrt{w}) = -a - 2s \in \mathfrak{F}_k$.

Ale teraz sytuacja powtarza się dla $\mathfrak{F}_k$ i jeden z pierwiastków musi być w $\mathfrak{F}_{k-1}$,

Iterując to postępowanie otrzymujemy wniosek, że jeden z pierwiastków musi być wymierny.

Podkreślmy: jest tak, gdy równanie to zostało uzyskane z rozwiązywania równań kwadratowych.

niekonstruowalność 7-kąta foremnego

Zobaczmy, jak to działa na przykładzie pytania o konstrukcję 7-kąta foremnego.

Mamy $z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$,

czyli $z^3 + z^2 + z + 1 + \frac{1}{z} + \frac{1}{z^2} + \frac{1}{z^3} = 0$.

ale $(z + \frac{1}{z})^3 = z^3 + 3z^2 + 3\frac{1}{z} + \frac{1}{z^3} = (z^3 + \frac{1}{z^3}) + 3(z + \frac{1}{z})$,

skąd $z^3 + \frac{1}{z^3} = (z + \frac{1}{z})^3 - 3(z + \frac{1}{z})$,

oraz $(z + \frac{1}{z})^2 = z^2 + 2 + \frac{1}{z^2}$,

skąd $z^2 + \frac{1}{z^2} = (z + \frac{1}{z})^2 - 2$.

Podstawiając otrzymujemy

$(z + \frac{1}{z})^3 - 3(z + \frac{1}{z}) + (z + \frac{1}{z})^2 - 2 + (z + \frac{1}{z}) + 1 = 0$.

porządkując i podstawiając $y = z + \frac{1}{z}$ mamy $y^3 + y^2 - 2y - 1 = 0$.

Równanie to nie ma pierwiastka wymiernego, bo podstawiając $\frac{r}{s}$, gdzie $nwd(r, s) = 1$ otrzymujemy sprzeczność:

$$\left(\frac{r}{s}\right)^3 + \left(\frac{r}{s}\right)^2 - 2\frac{r}{s} + 1 = 0,$$

skąd $r^3 + r^2s - 2rs^2 - s^3 = 0$, więc $-r^3 = s(r^2 - 2rs - s^2)$, wbrew $nwd(r, s) = 1$.

Zatem 7-kąta foremnego cyrklem i linijką bez podziałki skonstruować nie można.

3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34		
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49		
50	51	52	53	54	55	56	57	58	59	60	61	62	63	64		
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79		
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94		
95	96	97	98	99	100	101	102	103	104	105	106					
107	108	109	110	111	112	113	114	115	116	117						
118	119	120	121	122	123	124	125	126	127	128						
129	130	131	132	133	134	135	136	137	138	139						
140	141	142	143	144	145	146	147	148	149	150						
151	152	153	154	155	156	157	158	159	160	161						
162	163	164	165	166	167	168	169	170	171	172						
173	174	175	176	177	178	179	180	181	182	183						
184	185	186	187	188	189	190	191	192	193	194						
195	196	197	198	199	200	201	202	203	204	205						
206	207	208	209	210	211	212	213	214	215	216						
217	218	219	220	221	222	223	224	225	226	227						
228	229	230	231	232	233	234	235	236	237	238						
239	240	241	242	243	244	245	246	247	248	249						
250	251	252	253	254	255	256	257	258	.	.	.	.	.	.	.	.

Czy będą dalsze trójki?

Jedna na pewno: **65535, 65536, 65537.**

Czy będą dalsze trójki?

Jedna na pewno: **65535, 65536, 65537**.

Czy można było to odgadnąć? – tak, bo

$$5 = 2^{2^1} + 1, \quad 4 = 2^{2^1}, \quad 3 = 2^{2^1} - 1 = 2^{2^0} + 1;$$

$$17 = 2^{2^2} + 1, \quad 16 = 2^{2^2}, \quad 15 = 2^{2^2} - 1 = 5 \cdot 3 = (2^{2^1} + 1) \cdot (2^{2^0} + 1);$$

$$257 = 2^{2^3} + 1, \quad 256 = 2^{2^3}, \quad 255 = 2^{2^3} - 1 = 17 \cdot 5 \cdot 3 = (2^{2^2} + 1) \cdot (2^{2^1} + 1) \cdot (2^{2^0} + 1);$$

a więc można się było spodziewać, że będzie

$$\begin{aligned} 65537 = 2^{2^4} + 1, \quad 65536 = 2^{2^4}, \quad 65535 = 2^{2^4} - 1 &= 257 \cdot 17 \cdot 5 \cdot 3 = \\ &= (2^{2^3} + 1) \cdot (2^{2^2} + 1) \cdot (2^{2^1} + 1) \cdot (2^{2^0} + 1) \end{aligned}$$

i rzeczywiście tak jest!

Czy będą dalsze trójki?

Jedna na pewno: **65535, 65536, 65537**.

Czy można było to odgadnąć? – tak, bo

$$5 = 2^{2^1} + 1, \quad 4 = 2^{2^1}, \quad 3 = 2^{2^1} - 1 = 2^{2^0} + 1;$$

$$17 = 2^{2^2} + 1, \quad 16 = 2^{2^2}, \quad 15 = 2^{2^2} - 1 = 5 \cdot 3 = (2^{2^1} + 1) \cdot (2^{2^0} + 1);$$

$$257 = 2^{2^3} + 1, \quad 256 = 2^{2^3}, \quad 255 = 2^{2^3} - 1 = 17 \cdot 5 \cdot 3 = (2^{2^2} + 1) \cdot (2^{2^1} + 1) \cdot (2^{2^0} + 1);$$

a więc można się było spodziewać, że będzie

$$\begin{aligned} 65537 = 2^{2^4} + 1, \quad 65536 = 2^{2^4}, \quad 65535 = 2^{2^4} - 1 &= 257 \cdot 17 \cdot 5 \cdot 3 = \\ &= (2^{2^3} + 1) \cdot (2^{2^2} + 1) \cdot (2^{2^1} + 1) \cdot (2^{2^0} + 1) \end{aligned}$$

i rzeczywiście tak jest!

Nasuwa to sugestię, żeby (wobec trudności z liczbami pierwszymi Fermata) oderwać się od konstrukcji wielokątów foremnych i zapytać, czy faktycznie dla dowolnego n jest

$$2^{2^n} - 1 = (2^{2^{n-1}} + 1) \cdot (2^{2^{n-2}} + 1) \cdot \dots \cdot (2^{2^1} + 1) \cdot (2^{2^0} + 1).$$

Znaczyłoby to, że liczby Mersenne'a o wykładniku postaci 2^n są iloczynami wszystkich liczb Fermata o niższych wykładnikach.

Czy będą dalsze trójki?

Jedna na pewno: **65535, 65536, 65537**.

Czy można było to odgadnąć? – tak, bo

$$5 = 2^{2^1} + 1, \quad 4 = 2^{2^1}, \quad 3 = 2^{2^1} - 1 = 2^{2^0} + 1;$$

$$17 = 2^{2^2} + 1, \quad 16 = 2^{2^2}, \quad 15 = 2^{2^2} - 1 = 5 \cdot 3 = (2^{2^1} + 1) \cdot (2^{2^0} + 1);$$

$$257 = 2^{2^3} + 1, \quad 256 = 2^{2^3}, \quad 255 = 2^{2^3} - 1 = 17 \cdot 5 \cdot 3 = (2^{2^2} + 1) \cdot (2^{2^1} + 1) \cdot (2^{2^0} + 1);$$

a więc można się było spodziewać, że będzie

$$\begin{aligned} 65537 = 2^{2^4} + 1, \quad 65536 = 2^{2^4}, \quad 65535 = 2^{2^4} - 1 &= 257 \cdot 17 \cdot 5 \cdot 3 = \\ &= (2^{2^3} + 1) \cdot (2^{2^2} + 1) \cdot (2^{2^1} + 1) \cdot (2^{2^0} + 1) \end{aligned}$$

i rzeczywiście tak jest!

Nasuwa to sugestię, żeby (wobec trudności z liczbami pierwszymi Fermata) oderwać się od konstrukcji wielokątów foremnych i zapytać, czy faktycznie dla dowolnego n jest

$$2^{2^n} - 1 = (2^{2^{n-1}} + 1) \cdot (2^{2^{n-2}} + 1) \cdot \dots \cdot (2^{2^1} + 1) \cdot (2^{2^0} + 1) \cdot (2^{2^0} - 1).$$

Faktycznie tak jest. Okazuje się, że wystarczyło dopisać jedynekę.

Fakt okazał się banalny,

ale można go spożytkować na okoliczność konstruowania wielokątów foremnych:

niezależnie bowiem od tego, czy dla $n > 4$ istnieją liczby pierwsze Fermata $2^{2^n} + 1$,
czy też nie,

trzech konstruowalnych wielokątów foremnych "pod rząd" więcej już nie ma,

albowiem wszystkie liczby Mersenne'a postaci $2^{2^n} - 1$ dla $n > 5$ dzielą się przez $2^{2^5} + 1$
i w konsekwencji nawet przez 641.

a wielokąt foremny dla $2^{2^5} + 1$ nie jest konstruowalny, co też rozбивa ewentualną trójkę
(szkoda , bo 4294967295 i 4294967296 są konstruowalne).

Tak więc, jedynymi trójkami są **(3, 4, 5)** (6 się przyplątała), **(15, 16, 17)**,
(255, 256, 257) i **(65535, 65536, 65537)**.