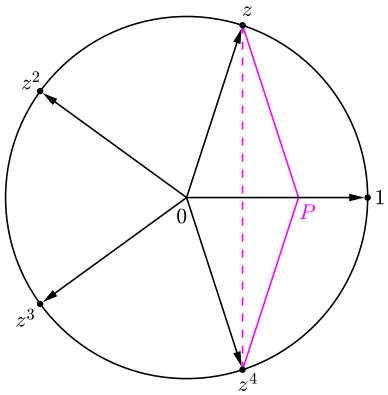
Jak Gauss skonstruował siedemnastokąt foremny

Marek KORDOS



Zespolone pierwiastki z 1.

Liczby zespolone są to wektory o początku w ustalonym punkcie 0 (ustalamy też jakiś punkt 1), które dodaje się oczywiście tak, jak wektory, a mnoży w ten sposób, że iloczyn ma długość będącą iloczynem długości czynników i z wektorem $\overline{01}$ tworzy kąt będący sumą kątów, jakie czynniki tworzą z tym wektorem.

Już Euklides wiedział, że
jeśli konstruowalne są foremne p_i-kąty dla $i = 1, 2, \ldots, k$, gdzie p_i są różnymi nieparzystymi liczbami pierwszymi, to konstruowalny jest foremny n-kąt dla $n = 2^m \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k$, gdzie $m = 0, 1, 2, \ldots$.
(*dla $k = 0$ liczba m jest równa co najmniej* 2),
ale była to przewaga formy nad treścią, bo p-kąty foremne umiano skonstruować tylko dla dwóch liczb pierwszych: 3 i 5. I taki stan meczu trwał przez z górą 2 000 lat.

Sprawa ruszyła do przodu za sprawą 19-letniego Carla Gaussa. Na znaną (może i Tobie, Czytelniku?) konstrukcję pięciokąta foremnego spojrzał on w inny sposób, poprzez liczby zespolone. Spójrzmy bowiem na rysunek: są na nim narysowane wszystkie zespolone pierwiastki stopnia 5 z jedności (proszę sprawdzić z umieszczoną na marginesie definicją działań). Widzimy też, że są one wszystkie potęgami pierwszego z nich. A także (ciągle korzystamy z definicji), że są one wierzchołkami pięciokąta foremnego i wobec tego (symetrie, równość kątów!) dają w sumie zero, czyli spełniają równanie

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

co można jednak sprytnie uporządkować, korzystając z tego, że $z^5 = 1$,

$$z^4 + z^3 + z^2 + z + 1 = \frac{1}{z} + \frac{1}{z^2} + z^2 + z + 1 = \left(z^2 + \frac{1}{z^2}\right) + \left(z + \frac{1}{z}\right) + 1 =$$
$$= \left(z + \frac{1}{z}\right)^2 - 2 + \left(z + \frac{1}{z}\right) + 1 = \left(z + \frac{1}{z}\right)^2 + \left(z + \frac{1}{z}\right) - 1 = 0$$

Zatem, aby znaleźć punkt P, potrzeba tylko rozwiązać równanie

$$x^2 + x - 1 = 0,$$

co każdy potrafi, a potem narysować symetralną odcinka $0P$ – w jej przecięciu z okręgiem jednostkowym będzie szukane z. Czyli do konstrukcji pięciokąta foremnego potrzebne jest rozwiązanie (jednego) równania kwadratowego, co można zrealizować cyrklem i linijką. Ale jak to naśladować dla innych liczb pierwszych? I dla których się da?

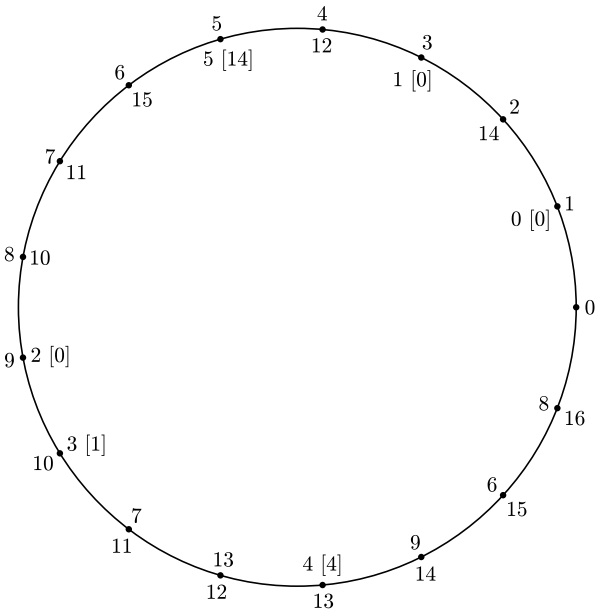
Gauss wiedział już, że należy poszukać tych liczb wśród takich liczb pierwszych, które są potęgami dwójki plus 1. Takie liczby muszą być postaci $2^{2^k} + 1$; nazywa się je liczbami Fermata. Takie są 3 i 5. Kolejna liczba to 17. Weźmy się więc za pierwiastki z jedności 17 stopnia.

Jeśli wykładnik k liczby $2^k + 1$ ma czynnik nieparzysty m (czyli jest postaci $k = n \cdot m$), to daje się ona rozłożyć:
$2^{n\cdot m} + 1 = (2^n + 1)\cdot$
$\cdot(2^{n\cdot(m-1)} - 2^{n\cdot(m-2)} + \cdot - 2^n + 1)$,
nie jest więc pierwsza.

Jednak tutaj takie proste sztuczki, jak dla 5, nie wychodzą. Gauss zauważył, że każdy, różny od 1, pierwiastek stopnia p, będącego liczbą pierwszą, ma tę własność, że potęgowany, zanim stanie się jedynką, będzie kolejno (choć nie po kolei) wszystkimi pozostałymi pierwiastkami (np. dla 5 potęgowany pierwiastek z^2 będzie dawał kolejno z^4, potem z i potem z^3). Podobnie, podnosząc kolejno wszystkie pierwiastki do jakiejkolwiek mniejszej od p potęgi, znów otrzymamy zbiór wszystkich pierwiastków. Taka symetria nasunęła pomysł, by z każdym pierwiastkiem związać też funkcję wykładniczą z jego numerem jako potęgą. Numerujemy więc pierwiastki od 0 do $p - 1$. Będą to zatem ε_i i odpowiadające im funkcje wykładnicze δ_i. Mamy, jak łatwo zauważyć, $\delta_i(\varepsilon_j) = \varepsilon_{\langle i\cdot j\rangle}$, gdzie $\langle\cdot\rangle$ oznacza, że należy zamiast iloczynu brać resztę z jego dzielenia przez p.

Z definicji liczba g jest pierwiastkiem pierwotnym dla liczby pierwszej p, gdy najmniejszym wykładnikiem naturalnym n, dla którego g^n daje z dzielenia przez p resztę 1, jest $p - 1$. Np. 10 jest pierwiastkiem pierwotnym dla 7 (co – inaczej niż przez dzielenie kolejnych potęg 10 przez 7 – możemy sprawdzić, np. rozwijając w ułamek dziesiętny $\frac{1}{7}$ - okres będzie sześciomiejscowy), jest też np. dla 17, 19, 23, 29, 97, 337, a nie jest np. dla 3 (okres długości 1), 11 (2), 13 (6). Wszystko to Gauss obliczył w szkole. Gdy zajmował się siedemnastokątem, wykazał, że 3 jest pierwiastkiem pierwotnym dla wszystkich liczb pierwszych Fermata.

Aby lepiej obserwować zachowanie się pierwiastków przy potęgowaniu, zastosował Gauss znany sposób: logarytmy – wtedy mnożenie staje się dodawaniem, może wówczas będzie lepiej widać. Przenumerował więc pierwiastki logarytmicznie. Konkretnie pierwiastek ε_k otrzymywał nowy numer l, gdy reszta z dzielenia 3^l przez 5 czy 17 była równa k. Okazuje się, że w tym przypadku wszystkie pierwiastki (poza jedynką) otrzymają różne numery. O takiej własności liczby 3 wobec liczby 5 czy liczby 17 mówimy, że 3 jest *pierwiastkiem pierwotnym dla tych liczb* (słowo pierwiastek, jak widać, jest tu używane w dwóch znaczeniach). Dla odróżnienia pierwiastki i funkcje z nowym numerem i będziemy oznaczali przez $\varepsilon_{(i)}$ i $\delta_{(i)}$.



Dla 17 stare numery na zewnątrz, nowe wewnątrz; dla małych numerów w nawiasach prostokątnych liczba pełnych owinięć.

Przenumerowywanie można sobie wyobrazić, jak nawijanie na okrąg o obwodzie p nici, której kolejne punkty są umieszczane w odległości 3^n od początku. Dla 5 mamy więc $\varepsilon_{(0)} = \varepsilon_1$, $\varepsilon_{(1)} = \varepsilon_3$, $\varepsilon_{(2)} = \varepsilon_4$ (i jedno pełne owinięcie), $\varepsilon_{(3)} = \varepsilon_2$ (i pięć pełnych owinięć). Zauważmy, że rozwiązując równanie, zebraliśmy razem parzyste i nieparzyste nowe numery.

Obok jest pokazana zmiana numeracji dla 17. Na pierwszy rzut oka nic nie wskazuje, aby tutaj też zbierać razem numery parzyste i nieparzyste. Ale rozum może pokazać więcej niż oko. Teraz mamy

$$\delta_{(i)}(\varepsilon_{(j)}) = \varepsilon_{(\langle i+j\rangle)}, \text{ ale nie } \varepsilon_{(i)} \cdot \varepsilon_{(j)} = \varepsilon_{(\langle i+j\rangle)}.$$

Mamy też

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

Pierwsza z tych równości pokazuje, że jeśli np. pierwiastki o nowych parzystych (nieparzystych) numerach poddamy przekształceniom o nowych numerach parzystych, to ich numery pozostaną parzyste (nieparzyste). Gdy poddamy je przekształceniom o nowych numerach nieparzystych, to się zamienią, ale też się nie pomieszają.

Dalej posługujemy się tylko nowymi numerami, więc nie będziemy pisać, że są nowe.

Podobnie np. reszta z dzielenia nowych numerów przez 4 jest zachowywana przy przekształceniach o nowych numerach podzielnych przez 4 itd. Gauss podzielił wobec tego wszystkie pierwiastki na takie właśnie grupy i postanowił obliczać sumę pierwiastków w tych grupach. Na początek zatem podzielił wszystkie pierwiastki na te o numerach parzystych i te o numerach nieparzystych – oznaczmy sumę pierwiastków w tych grupach odpowiednio przez $\sigma_{2,0}$ i $\sigma_{2,1}$ (z dzielenia przez 2 dają resztę 0 lub 1). Spróbujmy obliczyć te sumy. Oczywiście $\sigma_{2,0} + \sigma_{2,1} = -1$ – to suma wszystkich pierwiastków oprócz 1. Okazuje się, że i iloczyn daje się obliczyć.

$$\sigma_{2,0} = \varepsilon_{(0)} + \varepsilon_{(2)} + \ldots + \varepsilon_{(14)} \quad \text{i} \quad \sigma_{2,1} = \varepsilon_{(1)} + \varepsilon_{(3)} + \ldots + \varepsilon_{(15)}.$$

Wobec tego

$$\begin{aligned}
\sigma_{2,0} \cdot \sigma_{2,1} &= \varepsilon_{(0)}\varepsilon_{(1)} + \varepsilon_{(0)}\varepsilon_{(3)} + \ldots + \varepsilon_{(14)}\varepsilon_{(13)} + \varepsilon_{(14)}\varepsilon_{(15)} =_\star \\
&= \varepsilon_{(0)}\varepsilon_{(1)} + \varepsilon_{(1)}\varepsilon_{(2)} + \ldots + \varepsilon_{(14)}\varepsilon_{(15)} + \varepsilon_{(15)}\varepsilon_{(0)} + \\
&\quad + \varepsilon_{(0)}\varepsilon_{(3)} + \varepsilon_{(1)}\varepsilon_{(4)} + \ldots + \varepsilon_{(14)}\varepsilon_{(1)} + \varepsilon_{(15)}\varepsilon_{(2)} + \\
&\quad + \varepsilon_{(0)}\varepsilon_{(5)} + \varepsilon_{(1)}\varepsilon_{(6)} + \ldots + \varepsilon_{(14)}\varepsilon_{(3)} + \varepsilon_{(15)}\varepsilon_{(4)} + \\
&\quad + \varepsilon_{(0)}\varepsilon_{(7)} + \varepsilon_{(1)}\varepsilon_{(8)} + \ldots + \varepsilon_{(14)}\varepsilon_{(5)} + \varepsilon_{(15)}\varepsilon_{(6)} = \\
&= \Big(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(1)}) + \delta_{(1)}(\varepsilon_{(0)}\varepsilon_{(1)}) + \ldots + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(1)}) + \delta_{(15)}(\varepsilon_{(0)}\varepsilon_{(1)})\Big) + \\
&+ \Big(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(3)}) + \delta_{(1)}(\varepsilon_{(0)}\varepsilon_{(3)}) + \ldots + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(3)}) + \delta_{(15)}(\varepsilon_{(0)}\varepsilon_{(3)})\Big) + \\
&+ \Big(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(5)}) + \delta_{(1)}(\varepsilon_{(0)}\varepsilon_{(5)}) + \ldots + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(5)}) + \delta_{(15)}(\varepsilon_{(0)}\varepsilon_{(5)})\Big) + \\
&+ \Big(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(7)}) + \delta_{(1)}(\varepsilon_{(0)}\varepsilon_{(7)}) + \ldots + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(7)}) + \delta_{(15)}(\varepsilon_{(0)}\varepsilon_{(7)})\Big) = \\
&= 4 \cdot \big(\varepsilon_{(0)} + \varepsilon_{(1)} + \ldots + \varepsilon_{(14)} + \varepsilon_{(15)}\big) = 4 \cdot (-1) = -4.
\end{aligned}$$

Najbardziej podejrzanym momentem tego rachunku jest chyba równość oznaczona $\star$, ale zauważmy, że po obu jej stronach są 64 różne iloczyny, czyli akurat tyle, ile być powinno. I nie było potrzebne, aby się dowiedzieć, któremu pierwiastkowi są równe przekształcane iloczyny pierwiastków – cztery razy skorzystaliśmy z faktu, że zastosowanie wszystkich $\delta_{(i)}$ do jakiegokolwiek pierwiastka daje wszystkie pierwiastki.

Otrzymaliśmy zatem (wobec wzorów Viète'a) na $\sigma_{2,0}$ i $\sigma_{2,1}$ równanie

$$x^2 + x - 4 = 0, \quad \text{zatem} \quad \sigma_{2,0} = \frac{\sqrt{17}-1}{2} \quad \text{i} \quad \sigma_{2,1} = \frac{-\sqrt{17}-1}{2}.$$

To, że akurat tak należy przyporządkować pierwiastki równania, stwierdzamy geometrycznie, czyli dodając (na oko wystarczy) odpowiednie wektory na rysunku: większość mających numery parzyste jest z prawej strony rysunku, a większość mających numery nieparzyste – z lewej (precyzyjnie byłoby dodawać rzuty wektorów na prostą 01); zatem $\sigma_{2,0} > 0 > \sigma_{2,1}$.

Z kolei podzielimy $\sigma_{2,0}$ na dwie części $\sigma_{4,0}$ i $\sigma_{4,2}$. Ich suma to oczywiście $\sigma_{2,0}$. Obliczenie iloczynu jest trochę bardziej kłopotliwe, ale możliwe. Mamy

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

Zatem

$$\begin{aligned}
\sigma_{4,0} \cdot \sigma_{4,2} &= \varepsilon_{(0)}\varepsilon_{(2)} + \varepsilon_{(0)}\varepsilon_{(6)} + \ldots + \varepsilon_{(12)}\varepsilon_{(10)} + \varepsilon_{(12)}\varepsilon_{(14)} = \\
&= \varepsilon_{(0)}\varepsilon_{(2)} + \varepsilon_{(2)}\varepsilon_{(4)} + \ldots + \varepsilon_{(12)}\varepsilon_{(14)} + \varepsilon_{(14)}\varepsilon_{(0)} + \\
&\quad + \varepsilon_{(0)}\varepsilon_{(6)} + \varepsilon_{(2)}\varepsilon_{(8)} + \ldots + \varepsilon_{(12)}\varepsilon_{(2)} + \varepsilon_{(14)}\varepsilon_{(4)} = \\
&= \Big(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(2)}) + \delta_{(2)}(\varepsilon_{(0)}\varepsilon_{(2)}) + \ldots + \delta_{(12)}(\varepsilon_{(0)}\varepsilon_{(2)}) + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(2)})\Big) + \\
&\quad + \Big(\delta_{(0)}(\varepsilon_{(0)}\varepsilon_{(6)}) + \delta_{(2)}(\varepsilon_{(0)}\varepsilon_{(6)}) + \ldots + \delta_{(12)}(\varepsilon_{(0)}\varepsilon_{(6)}) + \delta_{(14)}(\varepsilon_{(0)}\varepsilon_{(6)})\Big)
\end{aligned}$$

i nie ma rady, trzeba się dowiedzieć, co to za elementy są przekształcane przez wszystkie $\delta_{(i)}$ o parzystym i. Tu niezbędne jest odwołanie się do pierwotnej numeracji, gdzie mnożenie wyraża się bardzo prosto:

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

i podobnie

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

patrząc na liczby 3 i 8, warto zauważyć jedynie, że jedna jest nieparzysta, a druga parzysta. Możemy więc kontynuować obliczanie.

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

Tym sposobem otrzymaliśmy równanie na $\sigma_{4,0}$ i $\sigma_{4,2}$, a mianowicie

$$x^2 - \sigma_{2,0}x - 1 = 0.$$

Analogicznie dzielimy $\sigma_{4,0}$ na $\sigma_{8,0}$ i $\sigma_{8,4}$. Zauważmy, że obliczenie tej pierwszej sumy kończy sprawę, bo jest to odpowiednik punktu P z obliczeń dla pięciokąta (spójrzmy na oba rysunki). Odpowiednim, analogicznie uzyskanym równaniem, okazuje się jednak

$$x^2 + \sigma_{4,0}x + \sigma_{4,1} = 0,$$

więc trzeba rozważyć wcześniej rozbicie $\sigma_{2,1}$ na $\sigma_{4,1}$ i $\sigma_{4,3}$, do czego jest potrzebne równanie

$$x^2 - \sigma_{2,1}x - 1 = 0.$$

Ostatecznie, po rozwiązaniu czterech równań kwadratowych otrzymujemy

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

Gauss udowodnił, że jego metoda jest dobra dla każdej liczby pierwszej Fermata. Pierre Wanzel udowodnił, że dla żadnej innej liczby pierwszej rozwiązania poprzez rozwiązywanie równań kwadratowych, a więc konstrukcji cyrklem i linijką, nie ma. Sprawa jednak nie posunęła się zbyt daleko poza wynik Euklidesa: wiemy, że liczbami pierwszymi Fermata są jeszcze 257 i 65537, ale żadnej innej liczby pierwszej Fermata nie znamy, a nawet nie wiemy, czy takie w ogóle istnieją. Następna liczba Fermata, dla $k = 5$, dzieli się przez 641. Rzeczywiście

$$\begin{aligned}
4294967297 &= 2^{2^5} + 1 = 2^{32} + 5^4 \cdot 2^{28} - \big(5^4 \cdot 2^{28} - 1\big) = \\
&= 2^{28}\big(2^4 + 5^4\big) - \big(5^2 \cdot 2^{14} + 1\big)\big(5 \cdot 2^7 + 1\big)\big(5 \cdot 2^7 - 1\big) = \\
&= 641\big(2^{28} - \big(5^2 \cdot 2^{14} + 1\big) \cdot 639\big).
\end{aligned}$$

Metodę zastosowaną na początku do przypadku pięciokąta można stosować również w innych przypadkach. Np. zauważmy, że

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

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

Wobec tego rozwiązując równanie opisujące siedmiokąt foremny, mamy

$$\begin{aligned}
0 &= z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = \\
&= \frac{1}{z} + \frac{1}{z^2} + \frac{1}{z^3} + z^3 + z^2 + z + 1 = \\
&= \Big(z + \frac{1}{z}\Big)^3 + \Big(z + \frac{1}{z}\Big)^2 - \\
&\quad - 2\Big(z + \frac{1}{z}\Big) - 1,
\end{aligned}$$

co sprowadza problem do rozwiązania równania

$$x^3 + x^2 - 2x - 1 = 0.$$

Jest to jednak pozorny sukces, bo równanie to nie da się zastąpić żadną liczbą równań kwadratowych.

Ale to już inna bajka.