PIERŚCIENIE I CIAŁA
Wykład 3

Leonhard Euler był jednym z najwybitniejszych matematyków. Dokonał licznych odkryć w tak różnych gałęziach matematyki jak rachunek różniczkowy i całkowy oraz teoria grafów.

Rysunek 1. Leonhard Euler (1707–1783)

Euler urodził się w Bazylei, w Szwajcarii w 1707 r. Mając 13 lat rozpoczął studia na Uniwersytecie Bazylejskim, a w wieku 16 lat otrzymał stopień magistra filozofii. Przez pewien okres mieszkał w Petersburgu, a także w Berlinie. Trzy lata po przejściu niemal śmiertelnej gorączki, która dotknęła go w roku 1735 Euler prawie całkowicie stracił wzrok w prawym oku, a katarakta w drugim, dotychczas zdrowym oku doprowadziła go już w kilka tygodni po jej odkryciu do niemal całkowitej ślepoty. Kłopoty ze wzrokiem kompensował swoją fotograficzną pamięcią i umiejętnościami dokonywania obliczeń pamięciowych. Był na przykład zdolny do powtórzenia bez najmniejszego wahania słowo w słowo Eneidy Wergiliusza, co więcej był w stanie wskazać jakim wersem zaczyna się i jakim kończy dowolna stronica tej książki.

Funkcja Eulera

Dla liczby naturalnej $n \geqslant 2$ przez $\varphi(n)$ oznaczamy liczbę wszystkich liczb $k \in \mathbb{N}$ takich, że $1 \leqslant k < n$ i k jest względnie pierwsze z n. Dodatkowo przyjmujemy $\varphi(1) = 1$. Funkcja $\varphi : \mathbb{N} \to \mathbb{N}$ nosi nazwę ***funkcji Eulera***.

Mamy

$$\varphi(1) = \varphi(2) = 1, \quad \varphi(3) = \varphi(4) = \varphi(6) = 2, \quad \varphi(5) = \varphi(8) = \varphi(10) = \varphi(12) = 4$$

i ogólnie $\varphi(n) = n - 1$, jeśli $n > 1$ jest liczbą pierwszą.

Twierdzenie 1. *Jeżeli liczby $m, n \in \mathbb{N}$ są względnie pierwsze, to*

$$\varphi(mn) = \varphi(m)\varphi(n). \tag{1}$$

Jeśli $n = p^k$ jest potęgą liczby pierwszej p, to

$$\varphi\left(p^k\right) = p^k\left(1 - \frac{1}{p}\right) = p^{k-1}(p-1). \tag{2}$$

Stąd i ze wzoru (1) wynika, że jeśli $n = p_1^{k_1}p_2^{k_2}...p_m^{k_m}$ jest rozkładem liczby $n \in \mathbb{N}$ na czynniki pierwsze, czyli $p_1, p_2, ..., p_m \in \mathbb{N}$ są parami różnymi liczbami pierwszymi i $k_1, k_2, ..., k_m \in \mathbb{N}$, to

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_m}\right). \tag{3}$$

Wzory na wartości funkcji φ dla początkowych liczb naturalnych sugerują, że dla $n \geqslant 3$, $\varphi(n)$ jest liczbą parzystą. Jest to rzeczywiście prawdą.

Twierdzenie 2. *Dla $n \geqslant 3$, $\varphi(n)$ jest liczbą parzystą.*

Dowód. Załóżmy, że n ma nieparzysty czynnik p w rozkładzie na czynniki pierwsze. Wtedy $n = p^k m$, gdzie $k \in \mathbb{N}$ i liczba m jest względnie pierwsza z p. Ze wzorów (1) i (2) otrzymujemy

$$\varphi(n) = \varphi(p^k)\varphi(m) = (p-1)p^{k-1}\varphi(m),$$

przy czym $p - 1$ jest liczbą parzystą. Stąd $\varphi(n)$ jest liczbą parzystą.

Załóżmy teraz, że n nie ma żadnego nieparzystego czynnika w rozkładzie na czynniki pierwsze, czyli jedynym czynnikiem pierwszym jest 2. Oznacza to, że $n = 2^k$ dla pewnego $k > 1$. Korzystając ze wzoru (2) dostajemy

$$\varphi(n) = \varphi(2^k) = 2^{k-1},$$

więc jest to liczba parzysta. □

Mamy następującą charakteryzację liczb względnie pierwszych.

Twierdzenie 3. *Liczby $m, n \in \mathbb{Z}$ są względnie pierwsze wtedy i tylko wtedy, gdy istnieją $x, y \in \mathbb{Z}$ takie, że*

$$mx + ny = 1. \tag{4}$$

Dla danych liczb względnie pierwszych $m, n \in \mathbb{Z}$ rozwiązanie $x, y \in \mathbb{Z}$ równania (4) można znaleźć korzystając z algorytmu Euklidesa wyznaczania największego wspólnego dzielnika liczb m, n (który jest równy 1). Rozwiązań tych jest nieskończenie wiele i jeśli x_0, y_0 jest jednym z nich, to pozostałe rozwiązania są dane wzorami

$$x = x_0 + kn, \quad y = y_0 - km,$$

gdzie $k \in \mathbb{Z}$.

Funkcja Eulera pojawia się w naturalny sposób przy rozważaniu pierwiastków z 1. Przypomnijmy, że zespolone pierwiastki stopnia n z 1 są dane wzorem

$$\omega_k = e^{\frac{2k\pi i}{n}} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},$$

gdzie $k = 0, 1, ..., n-1$.

Pierwiastkiem pierwotnym stopnia n z 1 nazywamy taki pierwiastek ω_m, że każdy pierwiastek jest jego potęgą. Zauważmy, że pierwiastkiem pierwotnym jest

$$\omega_1 = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},$$

gdyż

$$\omega_k = e^{\frac{2k\pi i}{n}} = \left(e^{\frac{2\pi i}{n}}\right)^k = \omega_1^k$$

dla $k = 0, 1, ..., n-1$. Fakt, że ω_m jest pierwiastkiem pierwotnym oznacza, że dla dowolnego $k = 0, 1, ..., n-1$ istnieje $l \in \mathbb{Z}$ takie, że $\omega_k = \omega_m^l$. Wtedy $\omega_k = \omega_m^l = (\omega_m^{-1})^{-l}$, co pokazuje, że także ω_m^{-1} jest też pierwiastkiem pierwotnym.

Korzystając z twierdzenia 3 możemy otrzymać charakteryzację pierwiastków pierwotnych.

Twierdzenie 4. *Niech ω_m będzie pierwiastkiem stopnia n z 1. Pierwiastek ω_m jest pierwiastkiem pierwotnym wtedy i tylko wtedy, gdy liczba m jest względnie pierwsza z n. W szczególności, jeśli n jest liczbą pierwszą, to dla każdego $m = 1, 2, ..., n-1$ pierwiastek ω_m jest pierwiastkiem pierwotnym.*

Dowód. Załóżmy, że ω_m jest pierwiastkiem pierwotnym. Wtedy $\omega_m^l = \omega_1$ dla pewnego $l \in \mathbb{Z}$. Z równości tej wynika, że różnica argumentów liczb ω_m^l i ω_1 jest wielokrotnością 2π. Zatem

$$\frac{2lm\pi}{n} - \frac{2\pi}{n} = 2k\pi$$

dla pewnego $k \in \mathbb{Z}$, co prowadzi do równości $lm - 1 = kn$, czyli

$$ml - nk = 1$$

i z twierdzenia 3 wynika, że liczby m, n są względnie pierwsze.

Załóżmy teraz, że liczby m, n są względnie pierwsze. Wobec twierdzenia istnieją liczby $x, y \in \mathbb{Z}$ takie, że

$$mx + ny = 1.$$

Niech $k \in \{1, 2, ..., n-1\}$. Wtedy $mkx + nky = k$ i oznaczając $p = kx$, $q = -ky$ dostajemy równość $mp - nq = k$, czyli $mp - k = nq$. Stąd

$$\frac{2mp\pi}{n} - \frac{2k\pi}{n} = 2q\pi,$$

co oznacza, że argumenty liczb $e^{\frac{2mp\pi i}{n}} = \omega_m^p$ i $e^{\frac{2k\pi i}{n}} = \omega_k$ różnią się o wielokrotność 2π. Zatem $\omega_k = \omega_m^p$. □

Przypomnijmy, że jeśli G jest grupą z działaniem $*$, to przyjmujemy $a^0 = e$, gdzie e jest elementem neutralnym,

$$a^n = \underbrace{a * a * ... * a}_{n \text{ razy}},$$

gdy $n \in \mathbb{N}$ i $a^n = (a^{-1})^{-n}$, gdy $n \in \mathbb{Z}$, $n < 0$. Zbiór $(a) = \{a^n : n \in \mathbb{Z}\}$ jest podgrupą grupy G, którą nazywamy grupą cykliczną generowaną przez element a. W szczególności jeśli $G = (a)$, to dla każdego $b \in G$ istnieje $n \in \mathbb{Z}$ taki, że $b = a^n$.

Standardowym przykładem grupy cyklicznej jest zbiór $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ dla $n \in \mathbb{N}$, $n \geqslant 2$ rozważany z dodawaniem modulo n, czyli działaniem $\oplus_n$ określonym wzorem

$$a \oplus_n b = r_n(a + b),$$

gdzie $r_n : \mathbb{Z} \to \mathbb{Z}_n$ oznacza funkcję, która liczbie $x \in \mathbb{Z}$ przyporządkowuje resztę $r_n(x)$ z dzielenia x przez n. Grupa $\mathbb{Z}_n$ jest oczywiście generowana przez liczbę 1.

Niech U_n oznacza zbiór wszystkich zespolonych pierwiastków stopnia n z 1. Jeśli $\omega_k, \omega_l \in U_n$, to

$$(\omega_k \omega_l)^n = \omega_k^n \omega_l^n = 1,$$

więc iloczyn $\omega_k \omega_l$ należy do U_n. Ponadto

$$(\omega_k^{-1})^n = \frac{1}{\omega_k^n} = 1,$$

więc $\omega_k^{-1} \in U_n$. Wynika stąd, że zbiór U_n z mnożeniem jest grupą. Fakt, że ω_m jest pierwiastkiem pierwotnym oznacza, że ω_m generuje grupę U_n, czyli $U_n = (\omega_m)$.

Grupa U_n jest izomorficzna z $\mathbb{Z}_n$, co oznacza, że istnieje wzajemnie jednoznaczna funkcja $F : \mathbb{Z}_n \to U_n$ taka, że

$$F(x \oplus_n y) = F(x) \cdot F(y)$$

dla dowolnych $x, y \in \mathbb{Z}_n$. Funkcją tą jest

$$F(x) = e^{\frac{2x\pi i}{n}} = \omega_x.$$

Rzeczywiście, $x \oplus_n y = r_n(x + y)$, więc zgodnie ze wzorem na dzielenie z resztą $x + y = nq + x \oplus_n y$ dla pewnego $q \in \mathbb{Z}$. Zatem $x \oplus_n y = (x + y) - nq$

$$F(x \oplus_n y) = e^{\frac{2(x \oplus_n y)\pi i}{n}} = e^{\frac{2(x+y)\pi i}{n}} \cdot e^{-\frac{2nq\pi i}{n}} = e^{\frac{2x\pi i}{n}} \cdot e^{\frac{2y\pi i}{n}} \cdot e^{-2q\pi i} = F(x) \cdot F(y),$$

gdyż $e^{-2q\pi i} = \cos(-2q\pi) + i \sin(-2q\pi) = 1$.

Izomorfizm przeprowadza generator grupy na generator grupy. Rozważając funkcję $F^{-1} : U_n \to \mathbb{Z}_n$, która także jest izomorfizmem z twierdzenia 4 widzimy, że liczba $m \in \mathbb{Z}_n$ jest generatorem grupy Z_n wtedy i tylko wtedy, gdy m jest względnie pierwsza z n. W szczególności jeśli n jest liczbą pierwszą, to każda liczba $m = 1, 2, ..., n-1$ jest generatorem grupy $\mathbb{Z}_n$.

Przykład 1. Liczby 1,5 są generatorami grupy $\mathbb{Z}_6$. Dla $m = 2$ mamy

$$2 \oplus_6 2 = 4, \quad 2 \oplus_6 2 \oplus_6 2 = 0, \quad 2 \oplus_6 2 \oplus_6 2 \oplus_6 2 = 2,$$

więc $(2) = \{0, 2, 4\}$. Dla $m = 3$ mamy

$$3 \oplus_6 3 = 0, \quad 3 \oplus_6 3 \oplus_6 3 = 3,$$

więc $(3) = \{0, 3\}$. Dla $m = 4$ mamy

$$4 \oplus_6 4 = 2, \quad 4 \oplus_6 4 \oplus_6 4 = 0, \quad 4 \oplus_6 4 \oplus_6 4 \oplus_6 4 = 4,$$

więc $(4) = \{0, 2, 4\}$. Widzimy więc, że liczby 2,3,4 nie generują całej grupy $\mathbb{Z}_6$.

Wielomiany cyklotmiczne

Wielomianem cyklotomicznym nazywamy wielomian postaci

$$\Phi_n(x) = \prod_{\substack{1\leqslant k\leqslant n\\ \mathrm{NWD}(k,n)=1}} \left(x - e^{\frac{2k\pi i}{n}}\right) = \prod_{\substack{1\leqslant k\leqslant n\\ \mathrm{NWD}(k,n)=1}} (x-\omega_k)\,, \tag{5}$$

gdzie $n > 1$ i ω_k jest pierwiastkiem stopnia n z 1. Liczba czynników w tym iloczynie jest równa $\varphi(n)$, więc $\operatorname{st}\Phi_n = \varphi(n)$. Z twierdzenia 2 wiemy, że dla $n \geqslant 3$ jest to liczba parzysta. Dodatkowo przyjmujemy $\Phi_1(x) = x - 1$.

Jeśli k nie jest względnie pierwsze z n, to $d = \mathrm{NWD}(k,n) > 1$ i biorąc $l = \frac{k}{d}$, $m = \frac{n}{d}$ otrzymujemy liczby względnie pierwsze l, m. Stąd $e^{\frac{2l\pi i}{m}}$ jest pierwiastkiem pierwotnym stopnia m z 1. Mamy $\frac{k}{n} = \frac{l}{m}$, zatem

$$x^n - 1 = \prod_{k=0}^{n-1} \left(x - e^{\frac{2k\pi i}{n}}\right) = \prod_{\substack{1\leqslant m\leqslant n\\ m|n}} \prod_{\substack{1\leqslant l\leqslant m\\ \mathrm{NWD}(l,m)=1}} \left(x - e^{\frac{2l\pi i}{m}}\right) = \prod_{\substack{1\leqslant m\leqslant n\\ m|n}} \Phi_m(x), \tag{6}$$

gdzie zapis $m|n$ oznacza, że m dzieli n. Używając tego wzoru można rekurencyjnie wyznaczać kolejne wielomiany Φ_n. Mamy $\Phi_1(x) = x - 1$, więc

$$\Phi_2(x) = \frac{x^2-1}{\Phi_1(x)} = \frac{x^2-1}{x-1} = x+1,$$
$$\Phi_3(x) = \frac{x^3-1}{\Phi_1(x)} = \frac{x^3-1}{x-1} = x^2+x+1,$$
$$\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4-1}{(x-1)(x+1)} = x^2+1,$$
$$\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1,$$
$$\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{(x^3-1)(x^3+1)}{\Phi_1(x)\Phi_3(x)(x+1)} = \frac{(x^3-1)(x^3+1)}{(x^3-1)(x+1)} = x^2-x+1.$$

Ogólny wzór możemy otrzymać w przypadku, gdy $p > 1$ jest liczbą pierwszą. Wtedy wzór (6) przyjmuje postać

$$x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x).$$

Stąd

$$\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Twierdzenie 5. *Dla każdego $n \in \mathbb{N}$, wielomian Φ_n ma współczynniki całkowite.*

Dowód. Zastosujemy indukcję względem n. W pierwszym kroku stwierdzamy, że $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Załóżmy, że $\Phi_k \in \mathbb{Z}[x]$ dla $k < n$. Niech

$$f(x) = \prod_{\substack{1\leqslant m<n\\ m|n}} \Phi_m(x).$$

Z założenia wynika, że wszystkie wielomiany występujące w tym iloczynie mają współczynniki całkowite, więc $f \in \mathbb{Z}[x]$. Ze wzoru (6) wiemy, że

$$x^n - 1 = f(x)\Phi_n(x). \tag{7}$$

Ponadto f jest wielomianem unormowanym, więc można podzielić $x^n - 1$ przez f zgodnie z algorytmem Euklidesa. W ten sposób otrzymujemy wzór

$$x^n - 1 = f(x)q(x) + r(x)$$

dla pewnych wielomianów $q, r \in \mathbb{Z}[x]$ takich, że $\operatorname{st} r < \operatorname{st} f$. Zatem $f(x)\Phi_n(x) = f(x)q(x) + r(x)$, czyli

$$f(x)(\Phi_n(x) - q(x)) = r(x)$$

i ponieważ $\operatorname{st} r < \operatorname{st} f$, więc $\Phi_n(x) - q(x) = 0$, gdyż w przeciwnym przypadku wielomian po lewej stronie miałby stopień co najmniej $\operatorname{st} f$. Stąd $\Phi_n = q \in \mathbb{Z}[x]$. □

Trzeba jednak zaznaczyć, że nie wszystkie wielomiany Φ_n mają współczynniki równe 1, 0 lub -1. Pierwszym wielomianem, w którym występują także inne współczynniki jest

$$\begin{aligned}\Phi_{105}(x) = 1 &+ x + x^2 - x^5 - x^6 - 2x^7 - x^8 - x^9 + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} \\ &- x^{20} - x^{22} - x^{24} - x^{26} - x^{28} + x^{31} + x^{32} + x^{33} + x^{34} + x^{35} + x^{36} \\ &- x^{39} - x^{40} - 2x^{41} - x^{42} - x^{43} + x^{46} + x^{47} + x^{48}.\end{aligned}$$

Twierdzenie 6. *Dla każdego $n > 1$, Φ_n jest wielomianem palindromicznym.*

Dowód. Wielomian Φ_n ma stopień $\varphi(n)$ i zgodnie ze wzorem (5) liczba jego pierwiastków jest także równa $\varphi(n)$. Zatem

$$x^{\varphi(n)}\Phi_n\left(\frac{1}{x}\right) = x^{\varphi(n)} \prod_{\substack{1 \leqslant k \leqslant n \\ \mathrm{NWD}(k,n)=1}} \left(\frac{1}{x} - e^{\frac{2k\pi i}{n}}\right) = \prod_{\substack{1 \leqslant k \leqslant n \\ \mathrm{NWD}(k,n)=1}} x\left(\frac{1}{x} - e^{\frac{2k\pi i}{n}}\right) = g(x),$$

gdzie

$$g(x) = \prod_{\substack{1 \leqslant k \leqslant n \\ \mathrm{NWD}(k,n)=1}} \left(1 - xe^{\frac{2k\pi i}{n}}\right).$$

Zauważmy, że wielomian g ma też $\varphi(n)$ pierwiastków i są one odwrotnościami pierwiastków wielomianu Φ_n. Jak wiemy odwrotności te są również pierwiastkami pierwotnymi stopnia n z 1. Stąd g ma takie same pierwiastki jak Φ_n i ich liczba jest równa stopniowi tych wielomianów. Zatem $g = \Phi_n$ i otrzymujemy równość

$$x^{\varphi(n)}\Phi_n\left(\frac{1}{x}\right) = \Phi_n(x),$$

która dowodzi, że Φ_n jest wielomianem palindromicznym. □