Funkcja Eulera

Celem tej notki jest zaznajomienie czytelnika z pojęciem fukcji Eulera i jej podstawowymi własnościami. Niech $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ oznacza zbiór liczb naturalnych włączając liczbę 0, przez $\mathbb{Z}$ rozumiemy zbiór wszystkich liczb całkowitych. Natomiast dla ustalonej dodatniej liczby naturalnej n określamy zbiór $\mathbb{Z}_n = \{0, \ldots, n-1\} \subseteq \mathbb{N}$.

W zbiorze liczb naturalnych ustalamy porządek liniowy $\mathbb{N}, \leq)$, taki że 0 jest elementem najmniejszym wzblędem relacji $\leq$ oraz dla każdej liczby $n \in \mathbb{N}$ mamy $n < n+1$ tzn. $n \leq n+1 \wedge \neg(n = n+1)$.

Dla uproszczenia wprowadzimy oznaczenie $[n] = \{1, \ldots, n\}$ dla ustalonej liczby naturalnej $n \in \mathbb{N} \setminus \{0\}$.

Więc zaczynamy, ma sie rozumieć od definicji. W zbiorze $\mathbb{Z}$ wprowadzamy relację podzielności

$$(\forall a, b \in \mathbb{Z})\ a|b \longleftrightarrow (\exists d \in \mathbb{Z})b = a \cdot d.$$

Oczywiście wprost z definicji wynika ze relacja podzielnoeści w zbiorze $\mathbb{Z}$ jest relacją zwrotną i przechodnią oraz liczba 1 jest elementem minimalnym a nawet najmniejszym w $(\mathbb{Z}, |)$. Relacja podzielności nie jest symetryczna bo np. $1|2$ ale $\neg(\ 2|1\ )$ i nie jest słabo antysymetryczna np. $1|-1$ i $-1|1$ ale $\neg(1 = -1)$.

Przez $\mathscr{P}$ oznaczamy zbiór liczb pierwszych tj,

$$\mathscr{P} = \{n \in \mathbb{N} \setminus \{0, 1\} :\ (\forall d \in \mathbb{N})\ d|n \longrightarrow (d = 1 \vee d = n)\}.$$

Definicja 0.1 (NWD) *Niech $A \subseteq \mathbb{Z} \setminus \{0\}$ będzie skończonym niepustym podzbiórem liczb całkowitych różnych od zera, to*

$$NWD(A) = \max\{d \in \mathbb{N} :\ (\forall a \in A)\ d|a\},$$

tutaj maksimum jest wzięte względem relacji wpomnianego wcześniej porządku liniowego $(\mathbb{N}, \leq)$. Wartość funkcji NWD na zbiorze A jest nazywana największym wspólnym dzielnikiem w zbiorze A.

Uwaga 0.1 *Zazwyczaj pojęcie NWD wprowadza się na skończonych ciagach liczb całkowitych ale dowodzi się że definicja ta nie zalezy od kolejności występowania tych liczb w ciagu.*

Jezeli $A = \{a, b\}$ to zamiast pisać $NWD(A)$, czy $NWD(\{a, b\})$ używać będziemy uproszczenia $NWD(a, b)$ a nawet (a, b) o ile to nie prowadzi do komplikacji w interpretacji tego napisu.

Powiemy, że dwie liczby całkowite $a, b \in \mathbb{Z}$ są względnie pierwsze wtedy i tylko wtedy gdy $(a, b) = 1$. Każde dwie liczby względnie pierwsze mają różne dzielniki pierwsze, dokładniej:

$$\{p \in \mathbb{N} : p|a \wedge p \in \mathscr{P}\} \cap \{p \in \mathbb{N} : p|b \wedge p \in \mathscr{P}\} = \emptyset.$$

Wprowadzimy definicję na tytułowy obiekt, mianowicie:

Definicja 0.2 (funkcja Eulera) *Niech* $n \in \mathbb{N} \setminus \{0\}$ *to*

$$\varphi(n) = |\{k \in [n] : (k, n) = 1\}|.$$

Możemy wypisać kilka wartości funkcji Eulera $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, ...$

Zachodzi następujący fakt.

Fakt 0.1 $(\forall p \in \mathscr{P})(\forall n \in \mathbb{N} \setminus \{0\})\ \varphi(p^n) = p^n - p^{n-1}$.

Dowòd. *Z definicji funcji Eulera mamy*

$$\begin{aligned}\varphi(p^n) =& |\{k \in [p^n] :\ (k, p^n) = 1\}| = |\{k \in [p^n] :\ \neg(p|k)\}| \\ =& |[p^n] \setminus \{k \in [p^n] :\ p|k\}|.\end{aligned}$$

Zauważmy, że

$$A := \{k \in [p^n] :\ p|k\} = \{p \cdot l : l \in \{1, \ldots, p^{n-1}\}\} \subseteq [p^n],$$

co daje tezę $\varphi(p^n) = |[p^n] - A| = |[p^n]| - |A| = p^n - p^{n-1}$. ■

Twierdzenie 0.1 $(\forall m, n \in \mathbb{N} \setminus \{0\})\ (m, n) = 1 \longrightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Dowòd. *Wypiszmy elementy zbioru* $[m \cdot n]$ *w postaci nastepującej tablicy:*

$$\begin{array}{ccccccc} 1 & m+1 & \ldots & k \cdot m + 1 & \ldots & & (n-1) \cdot m + 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ r & m+r & \ldots & k \cdot m + r & \ldots & & (n-1) \cdot m + r \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ m & m+m & \ldots & k \cdot m + m & \ldots & (n-1) \cdot m + m = n \cdot m. & \end{array}$$

Do dowodu naszego twierdzenia wykorzystamy kilka przydatnych faktów.

Claim 0.1 $(\forall k \in [m \cdot n])\ (k, m \cdot n) = 1 \longleftrightarrow ((k, m) = 1 \wedge (k, n) = 1)$.

Dowód. " $\rightarrow$" Niech $\neg((k,m)=1 \wedge (k,n)=1)$, to jest $d>1$ takie że $d|k$ i ($d|m$ lub $d|n$), to $d|k$ i $d|m\cdot n$ więc $\neg\,(k,m\cdot n)=1$.

" $\leftarrow$ " Jeżeli $\neg((k,m\cdot n)=1)$, to istnieje liczba pierwsza $p\in\mathscr{P}$ taka że $p|k\wedge p|m\cdot n$ ale $(m,n)=1$ więc $p|m\vee p|n$ oraz $p|k$ a więc $(k,m)\neq 1\vee(k,n)\neq 1$ a więc $\neg((k,m)=1\wedge(k,n)=1)$. ■

Claim 0.2 $(\forall x,n\in\mathbb{N}\setminus\{0\})(x,n)=1\longleftrightarrow((x)_n,n)=1$. *Tutaj* $(x)_n$ *oznacza resztę z dzielenia* x *przez* n.

Dowód. Niech $x\in\mathbb{N}\setminus\{0\}$ będzie dodatnia liczbą naturalną, to instnieją $q\in\mathbb{N}$ i $r\in\mathbb{Z}_n$ takie że $x=q\cdot n+r$ i wtedy $(x)_n=r$. Jeśli więc $d>1$ jest takie że $d|n\wedge d|r$, to oczywiscie $d|x$ i na odwrót, jesli dla $d>1$ zachodzi $d|n\wedge d|x$, to $d|x-q\cdot n$ a wiec $d|r$ ale $r=(x)_n$ co daje $d|(x)_n$. ■

Claim 0.3 $(\forall r\in[m])(r,m)=1\longleftrightarrow(\forall k\in\mathbb{Z}_n)(k\cdot m+r,m)=1$.

Dowód. " $\leftarrow$" *Dowód jest niemal oczywisty, kładąc* $k=0$.

" $\rightarrow$ " *Niech* $(km+r,m)\neq 1$ *dla pewnego* $k\in\mathbb{Z}_n$, *to istnieje liczba pierwsza* $p\in\mathscr{P}$ *taka że* $p|m\wedge p|km+r$. *Niech* $x=km+r$, *to* $p|x$ *a stąd* $p|x-km$ *a więc* $p|r$ *oraz* $p|m$ *a stąd* $(r,m)\neq 1$. ■

Claim 0.4 $(\forall r\in[m])\ \{(k\cdot m+r)_n:\ k\in\mathbb{Z}_n\}=\mathbb{Z}_n$.

Dowód. *Pokażemy, że zbiór* $\{(k\cdot m+r)_n:\ k\in\mathbb{Z}_n\}\subseteq\mathbb{Z}_n$ *jest* n*-elementowy. Niech* $0\leq k'\leq k<n$ *będą liczbami naturalnymi, dla których* $(k'\cdot m+r)_n=(k\cdot m+r)_n$, *więc* $k'\cdot m+r\equiv k\cdot m+r \mod n$ *a stąd* $(k-k')m\equiv 0 \mod n$ *czyli* $n|(k-k')m$ *ale* $(m,n)=1$ *więc* $n|k-k'$. *Ponieważ* $0\leq k-k'\leq k<n$, *więc* $k-k'=0$ *a stąd* $k=k'$. ■

Wyliczmy wartość fukcji Eulera w $m\cdot n$:

$$\begin{aligned}
\varphi(m\cdot n) =& |\{x\in[mn]:\ (x,mn)=1\}| \\
\overset{Claim0.1}{=}& |\{x\in[mn]:\ (x,m)=1\wedge(x,n)=1\}| \\
\overset{Claim0.3}{=}& \Big|\dot{\bigcup_{r\in\{r\in[m]:(r,m)=1\}}}\{k\cdot m+r:k\in\mathbb{Z}_n\wedge(k\cdot m+r,n)=1\}\Big| \\
=& \sum_{r\in\{r\in[m]:(r,m)=1\}}|\{k\cdot m+r:k\in\mathbb{Z}_n\wedge(k\cdot m+r,n)=1\}| \\
\overset{Claim0.2}{=}& \sum_{r\in\{r\in[m]:(r,m)=1\}}|\{(k\cdot m+r)_n:k\in\mathbb{Z}_n\wedge((k\cdot m+r)_n,n)=1\}| \\
\overset{Claim0.4}{=}& \sum_{r\in\{r\in[m]:(r,m)=1\}}|\{x\in\mathbb{Z}_n:\ (x,n)=1\}| \\
=& \sum_{r\in\{r\in[m]:(r,m)=1\}}\varphi(n)=\varphi(m)\cdot\varphi(n).
\end{aligned}$$

■

Dowòd. *Dla zadanej liczby naturalnej k niech $\mathbb{Z}_k^* = \{x \in \mathbb{Z}_k : nwd(x,k) = 1\}$. Udowodnimy, że istnieje bijekcja pomiędzy $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ a zbiorem $\mathbb{Z}_{mn}^*$. Dla zadanej pary $(k,l) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ niech $f(k,l) = z$ będzie elementem zbioru $\mathbb{Z}_{mn}$ spełniające równania*

$$z \equiv k \mod m \text{ oraz } z \equiv l \mod n.$$

Ponieważ liczby m i n są względnie pierwsze, to z chińskiego twierdzenia o resztach, istnieje jedyna liczba naturalna z, taka że $0 \leq z < mn$ i która spełnia powyższe kongruencje. Ponieważ k jest względnie pierwsza z liczbą m, to na podstawie pierwszej kongruencji, liczba z jest względnie pierwsza z m, podobnie z jest względnie pierwsza z liczbą n, więc z jest liczbą względnie pierwszą z iloczynem mn. Więc $f : \mathbb{Z}_m^* \times \mathbb{Z}_n^* \to \mathbb{Z}_{mn}^*$.

Pokażemy, że f jest różnowartościowa. Niech $f(k,l) = z = f(k',l')$ dla $k, k' \in \mathbb{Z}_m^*, l, l' \in \mathbb{Z}_n^*$. Z pierwszwj kongruencji mamy $k \equiv z \equiv k' \mod m$, a co za tym idzie $k = k'$, podobnie mamy $l = l'$. Następnie pokażemy, że f jest surjekcją na zbiór $\mathbb{Z}_{mn}^*$. Niech $z \in \mathbb{Z}_{mn}^*$ będzie dowolną liczbą, niech $k = (z \mod m)$ a $l = (z \mod n)$. Ponieważ z jest względnie pierwsza z mn, to w szczególności z jest względnie pierwsza z m, co na mocy definicji liczby k również liczba k jest względnie pierwsza z m. Podobnie l jest względnie pierwsza z n, więc $(k,l) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ i $f(k,l) = z$, co dowodzi surjektywności funkcji f na zbiór $\mathbb{Z}_{mn}^*$. Ostatecznie mamy

$$\varphi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m) \cdot \varphi(n).$$

■

Na mocy Twierdzenia i Faktu mamy następujący wniosek.

Wniosek 0.1 *Jeśli $n = p_1^{m_1} \cdots p_k^{m_k}$ jest rozkładem liczby naturalnej n na czynniki pierwsze ($p_i \neq p_j$, dla różnych $i, j \in [k]$), to wtedy*

$$\varphi(n) = \prod_{i \in [k]} \left(p_i^{m_i} - p_i^{m_i - 1}\right) = n \cdot \prod_{i \in [k]} \left(1 - \frac{1}{p_i}\right).$$

Robert Rałowski