1.5 Funkcja i twierdzenie Eulera

Rozpoczniemy do definicji funkcji Eulera. Jeśli n jest dodatnią liczbą całkowitą, to przez $\varphi(n)$ oznaczamy liczbę elementów zbioru

$$U_n := \{a \in [0, n-1] : \gcd(a, n) = 1\},$$

a więc liczbę reszt z dzielenia przez n, które są względnie pierwsze z n. Zauważmy, że $\varphi(n) > 0$ dla każdej dodatniej liczby całkowitej n. Równoważnie, $U_n \neq \varnothing$ dla każdego n. Istotnie, jeśli $n > 1$, to $1 \in U_n$, gdyż oczywiście $\gcd(n, 1) = 1$ oraz z założenia $0 \leq 1 < n$. Gdy $n = 1$, to $0 \in U_n$, gdyż w tym przypadku $\gcd(0, n) = n = 1$ oraz oczywiście $0 \leq 0 < 1 = n$. Zatem otrzymujemy w ten sposób funkcję $\varphi\colon \mathbb{N}_+ \to \mathbb{N}_+$, którą nazywamy funkcją Eulera.

Dla małych liczb n wartość $\varphi(n)$ funkcji Eulera możemy znajdować bezpośrednio z definicji. Na przykład, $\varphi(8) = 4$, gdyż spośród liczb 0, 1, 2, 3, 4, 5, 6 i 7, tylko 1, 3, 5 i 7 są względnie pierwsze z 8 (w pozostałych przypadkach mamy $\gcd(0, 8) = 8$, $\gcd(2, 8) = 2 = \gcd(6, 8)$ i $\gcd(4, 8) = 4$). Dla większych wartości n powyższa metoda jest nieefektywna, będziemy więc chcieli znaleźć szybszy sposób liczenia wartości funkcji Eulera.

Pierwszą redukcję daje następująca obserwacja.

Lemma 1.43. *Jeśli $n_1, \ldots, n_k$ są dodatnimi liczbami całkowitymi, które są parami względnie pierwsze (tj. $\gcd(n_i, n_j) = 1$, dla wszystkich par (i, j) takich, że $1 \leq i < j \leq k$), to*

$$\varphi(n_1 \cdots n_k) = \varphi(n_1) \cdots \varphi(n_k).$$

Dowód. Przypomnijmy, że na mocy Chińskiego Twierdzenia o Resztach (Twierdzenie 1.40) funkcja

$$\Phi\colon [0, n-1] \to [0, n_1 - 1] \times \cdots \times [0, n_k - 1],$$

gdzie $n := n_1 \cdots n_k$, dana wzorem

$$\Phi(a) := (a \bmod n_1, \cdots, a \bmod n_k),$$

jest bijekcją. Aby udowodnić wzór

$$\varphi(n_1 \cdots n_k) = \varphi(n_1) \cdots \varphi(n_k)$$

wystarczy pokazać, że obrazem zbioru U_n przy bijekcji Φ jest zbiór $U_{n_1} \times \cdots \times U_{n_k}$, tzn.

$$\Phi(a) \in U_{n_1} \times \cdots \times U_{n_k} \iff a \in U_n.$$

Z definicji (funkcji Φ oraz zbiorów $U_{n_1}, \ldots, U_{n_k}$) wiemy, że $\Phi(a) \in U_{n_1} \times \cdots \times U_{n_k}$ wtedy i tylko wtedy, gdy

$$\gcd(a \bmod n_1, n_1) = 1, \ldots, \gcd(a \bmod n_k, n_k) = 1.$$

Z Lematu 1.21 wiemy jednak, że $\gcd(a \bmod m, m) = \gcd(a, m)$ dla każdego m, więc powyższy warunek jest równoważny warunkowi

$$\gcd(a, n_1) = 1, \ldots, \gcd(a, n_k) = 1.$$

Teraz jednak możemy skorzystać z Wniosku 1.24, który mówi, że w powyższej sytuacji

$$\gcd(a, n_1 \cdots n_k) = 1.$$

Ponieważ z definicji $n_1 \cdots n_k = n$, oznacza to, że $a \in U_n$, co kończy dowód. □

Z Podstawowego Twierdzenia Arytmetyki wiadomo, że jeśli n jest dodatnią liczbą całkowitą, to istnieją parami różne liczby pierwsze $p_1, \ldots, p_k$ oraz dodatnie liczby całkowite $m_1, \ldots, m_k$ takie, że

$$n = p_1^{m_1} \cdots p_k^{m_k}. \tag{1.1}$$

Jeśli

$$n_1 := p_1^{m_1}, \qquad , n_k := p_k^{m_k},$$

to równość (1.1) oznacza, że $n = n_1 \cdots n_k$. Ponadto, liczby $n_1, \ldots, n_k$ są parami względnie pierwsze (gdyż liczby $p_1, \ldots, p_k$ są pierwsze i parami różne), więc

$$\varphi(n) = \varphi(n_1) \cdots \varphi(n_k)$$

na mocy udowodnionego powyżej Lematu 1.43. Brakujące wartości funkcji Eulera $\varphi(n_1), \ldots, \varphi(n_k)$ można policzyć korzystając z następującego lematu.

Lemma 1.42. *Jeśli p jest liczbą pierwszą i m jest dodatnią liczbą całkowitą, to*

$$\varphi(p^m) = p^m - p^{m-1}.$$

Przed dowodem powyższego lematu sformułujemy płynący z niego wniosek.

Wniosek 1.44. *Jeśli $p_1, \ldots, p_k$ są wszystkimi parami różnymi liczbami pierwszymi dzielącymi dodatnią liczbę całkowitą n, to*

$$\varphi(n) = n \cdot \Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_k}\Big). \tag{1.2}$$

Dokładniej, jeśli

$$n = p_1^{m_1} \cdots p_k^{m_k}$$

dla dodatnich liczb całkowitych $m_1, \ldots, m_k$*, to*

$$\varphi(n) = (p_1^{m_1} - p_1^{m_1-1}) \cdots (p_k^{m_k} - p_k^{m_k-1}) \tag{1.3}$$

$$= (p_1 - 1)p_1^{m_1-1} \cdots (p_k - 1)p_k^{m_k-1}. \tag{1.4}$$

Dowód. Z rozważań poprzedzających sformułowanie Lematu 1.42 wiemy, że

$$\varphi(n) = \varphi(p_1^{m_1}) \cdots \varphi(p_k^{m_k}). \tag{1.5}$$

Ponieważ

$$\varphi(p_1^{m_1}) = p_1^{m_1} - p_1^{m_1-1}, \ldots, \varphi(p_k^{m_k}) = p_k^{m_k} - p_k^{m_k-1},$$

na mocy Lematu 1.43, więc otrzymujemy wzór (1.3). Wyłączając w powyższych wyrażeniach $p_1^{m_1-1}$, $\ldots$, $p_k^{m_k-1}$, odpowiednio, otrzymujemy, że

$$\varphi(p_1^{m_1}) = (p_1 - 1)p_1^{m_1-1}, \ldots, \varphi(p_k^{m_k}) = (p_k - 1)p_k^{m_k-1},$$

więc po podstawieniu do wzoru (1.5), otrzymujemy wzór (1.4). Podobnie, mamy

$$\varphi(p_1^{m_1}) = p_1^{m_1}\Big(1 - \frac{1}{p_1}\Big), \ldots, \varphi(p_k^{m_k}) = p_k^{m_k}\Big(1 - \frac{1}{p_k}\Big),$$

skąd

$$\varphi(n) = p_1^{m_1} \cdots p_k^{m_k}\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_k}\Big).$$

Ponieważ z założenia $p_1^{m_1} \cdots p_k^{m_k} = n$, więc otrzymujemy wzór (1.2). □

Wróćmy teraz do dowodu Lematu 1.42.

Dowód Lematu 1.42. Policzymy ile spośród liczb 0, 1, $\ldots$, $p^m - 1$ nie należy do zbioru U_{p^m}, a więc nie jest względnie pierwszych z p^m. Ponieważ p jest liczbą pierwszą, więc $\gcd(k, p) \neq 1$ wtedy i tylko wtedy, gdy $p \mid k$. Wśród liczb 1, 2, $\ldots$, $p^m - 1$ co p-ta liczba jest podzielna przez p, a więc takich liczb jest $\lfloor \frac{p^m-1}{p} \rfloor$. Ponadto $\gcd(0, p^m) = p^m > 1$, gdyż $m > 0$. Zatem 0 nie należy do U_{p^m}. Ostatecznie reszt nienależących do U_{p^m} jest

$$\Big\lfloor \frac{p^m - 1}{p} \Big\rfloor + 1 = \Big\lfloor p^{m-1} - \frac{1}{p} \Big\rfloor + 1 = (p^{m-1} - 1) + 1 = p^{m-1}.$$

Ponieważ reszt z dzielenia przez p^m jest p^m, więc wartość funkcji Eulera dla p^m jest równa $p^m - p^{m-1}$. □

Naszym drugim celem w tym wykładzie jest udowodnienie następującego twierdzenia.

Twierdzenie 1.46 (Euler)**.** *Jeśli n jest dodatnią liczbą całkowitą, a a jest liczbą całkowitą względnie pierwszą z n, to*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

W dowodzie korzystać będziemy między innymi z następującego faktu, który teraz przypomnimy bez dowodu.

Lemma 1.37. (2) *Jeśli n jest dodatnią liczbą całkowitą oraz x, y i z są liczbami całkowitymi takimi, że $x \cdot y \equiv x \cdot z \pmod{n}$ i $\gcd(x, n) = 1$, to $y \equiv z \pmod{n}$.*

Dowód. Oznaczmy $\varphi(n)$ przez m, tj. $m := \varphi(n)$. Niech $b_1, \ldots, b_m$ będą wszystkimi parami różnymi resztami z dzielenia przez n, które są względnie pierwsze z n, tzn.

$$U_n = \{b_1, \ldots, b_m\}. \tag{1.6}$$

Dla $i = 1, \ldots, m$, niech c_i będzie resztą z dzielenia $a \cdot b_i$ przez n, tzn. $c_i := (a \cdot b_i) \bmod n$. Pokażemy, że

$$\{c_1, \ldots, c_m\} = \{b_1, \ldots, b_m\}. \tag{1.7}$$

Ustalmy $i \in \{1, \ldots, m\}$. Ponieważ z założenia $\gcd(a, n) = 1 = \gcd(b_i, n)$, więc $\gcd(a \cdot b_i, n) = 1$ na mocy Wniosku 1.24. Ponieważ $\gcd((a \cdot b_i) \bmod n, n) = \gcd(a \cdot b_i, n)$ na mocy Lematu 1.21, więc otrzymujemy, że $\gcd(c_i, n) = 1$, a więc $c_i \in U_n$ (gdyż oczywiście $0 \leq c_i < n$). Podsumowując,

$$\{c_1, \ldots, c_m\} \subseteq U_n. \tag{1.8}$$

Aby dokończyć dowód równości (1.7) pokażemy teraz, że $c_i \neq c_j$, gdy $i \neq j$. Istotnie, jeśli $c_i = c_j$, tzn. $(a \cdot b_i) \bmod n = (a \cdot b_j) \bmod n$, to $a \cdot b_i \equiv a \cdot b_j \pmod{n}$ na mocy Faktu 1.35. Korzystając z Lematu 1.37(2) dla $x = a$, $y = b_i$ i $z = c_i$, otrzymujemy zatem, że $b_i \equiv b_j \pmod{n}$, co oznacza, że $b_i \bmod n = b_j \bmod n$, na mocy Faktu 1.35. Ponieważ, $0 \leq b_i, b_j < n$, więc $b_i \bmod n = b_i$ i $b_j \bmod n = b_j$ (na mocy Wniosku 1.15), zatem dostajemy $b_i = b_j$. Ponieważ jednak liczby $b_1, \ldots, b_m$ są parami różne, więc oznacza to, że $i = j$. Podsumowując, pokazaliśmy, że jeśli $c_i = c_j$, to $i = j$. Innymi słowy, jeśli $i \neq j$, to $c_i \neq c_j$, co chcieliśmy udowodnić.

Ponieważ, jak właśnie pokazaliśmy, liczby $c_1, \ldots, c_m$ są parami różne, więc

$$|\{c_1, \ldots, c_m\}| = m.$$

Zatem z definicji liczby m oraz funkcji Eulera mamy

$$|\{c_1, \ldots, c_m\}| = m = \varphi(n) = |U_n|.$$

Ponieważ dodatkowo

$$\{c_1, \ldots, c_m\} \subseteq U_n$$

(patrz (1.8)), więc ostatecznie

$$\{c_1, \ldots, c_m\} = U_n.$$

Wykorzystując dodatkowo równość

$$U_n = \{b_1, \ldots, b_m\}$$

(patrz (1.6)), mamy zapowiadaną równość

$$\{c_1, \ldots, c_m\} = \{b_1, \ldots, b_m\}.$$

Ponieważ liczby $c_1, \ldots, c_m$ są parami różne, podobnie jak liczby $b_1, \ldots, b_m$, więc powyższa równość implikuje, że

$$c_1 \cdots c_m = b_1 \cdots b_m.$$

Ale z definicji i Faktu 1.35 $c_1 \equiv a \cdot b_1 \pmod{n}$, $\ldots$, $c_m \equiv a \cdot b_m \pmod{n}$, więc

$$c_1 \cdots c_m \equiv (a \cdot b_1) \cdots (a \cdot b_m) = b_1 \cdots b_m a^m \pmod{m}$$

na mocy Lematu 1.37(1). Powyższe dwa równania prowadzą więc do wniosku, że

$$b_1 \cdots b_m a^m \equiv b_1 \cdots b_m \pmod{n}.$$

Korzystając z Lematu 1.37(2) dla $x = b_1$ (pamiętając, że $\gcd(b_1, n) = 1$), $y = b_2 \cdots b_m a^m$ i $z = b_2 \cdots b_m$, otrzymujemy, że

$$b_2 \cdots b_m a^m \equiv b_2 \cdots b_m \pmod{n}.$$

Analogicznie,

$$b_3 \cdots b_m a^m \equiv b_3 \cdots b_m \pmod{n}.$$

Kontynuując, otrzymujemy, że

$$a^m \equiv 1 \pmod{n},$$

co należało udowodnić, gdyż $m = \varphi(n)$. □