Funkcja Eulera

Definicja

Jeśli $n \in \mathbb{N}_+$, to

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

Przykład

Dla $n = 12$ mamy

$$\{a \in [0, 11] : \gcd(a, 12) = 1\} = \{\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11\}.$$

Zatem $\varphi(12) = 4$.

Wzór

Jeśli $n = p_1^{m_1} \cdots p_k^{m_k}$ dla parami różnych liczb pierwszych $p_1, \ldots, p_k$ oraz dodatnich liczb całkowitych $m_1, \ldots, m_k$, to

$$\varphi(n) = n \cdot \left(1 - \tfrac{1}{p_1}\right) \cdots \left(1 - \tfrac{1}{p_k}\right)$$

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

Przykład

Ponieważ $1800 = 2^3 \cdot 3^2 \cdot 5^2$, więc

$$\varphi(1800) = 2^2 \cdot (2-1) \cdot 3^1 \cdot (3-1) \cdot 5^1 \cdot (5-1) = 480.$$

Problem

Dla danej liczby $m \in \mathbb{N}_+$ znaleźć wszystkie liczby $n \in \mathbb{N}_+$ takie, że $\varphi(n) = m$.

Metoda – część I

1. Wyznaczamy wszystkie dodatnie dzielniki $d_1, \ldots, d_r$ liczby m.

   Spośród liczb $d_1 + 1, \ldots, d_r + 1$ wybieramy wszystkie liczby pierwsze $p_1, \ldots, p_l$, przy czym zakładamy, że $p_1 > \cdots > p_l$. [W szczególności, $p_l = 2$.]

2. Tworzymy pomocniczą tabelę, której kolumny indeksowane są liczbami pierwszymi $p_1, \ldots, p_l$, a wiersze nieujemnymi liczbami całkowitymi.

   Na przecięciu kolumny indeksowanej liczbą p oraz wiersza k wpisujemy wartość funkcji Eulera $\varphi(p^k)$.

   Obliczając wartości funkcji $\varphi(p^k)$, warto skorzystać z następujących rekurencyjnych wzorów:

   $$\varphi(p^0) = 1, \qquad \varphi(p^1) = p - 1, \qquad \varphi(p^k) = p \cdot \varphi(p^{k-1}), \qquad \text{gdy } k > 1.$$

   Wypełnianie kolumny odpowiadającej liczbie pierwszej p kończymy, gdy $\varphi(p^k)$ nie jest dzielnikiem liczby m.

Równania z funkcją Eulera – przykład, część I

Zadanie

Wyznaczyć wszystkie liczby $n \in \mathbb{N}_+$ takie, że $\varphi(n) = 18$.

Rozwiązanie

1. Dzielnikami liczby 18 są: 18, 9, 6, 3, 2, 1.

   Po dodaniu do nich 1 otrzymujemy liczby: 19, 10, 7, 4, 3, 2.

   Po usunięciu liczb złożonych, otrzymujemy liczby: 19, 7, 3, 2.

2.

	19	7	3	2
0	1	1	1	1
1	18	6	2	1
2	~~342~~	~~42~~	6	2
3			18	~~4~~
4			~~×~~	

Metoda – część II

3. Tworzymy drzewo, z którego odczytamy odpowiedź, w następujący sposób:
   - W korzeniu drzewa (jedynym wierzchołku na poziomie 1) wpisujemy liczbę m.
   - Jeśli na poziomie $i = 1, \ldots, l-1$ mamy z wpisaną liczbą d, to z tego wierzchołka rysujemy krawędzie, których etykietami są nieujemne liczby całkowite k takie, że $\varphi(p_i^k)$ dzieli d.

     W wierzchołkach kończących te krawędzie, które znajdują się na poziomie $i+1$, wpisujemy liczby $\frac{d}{\varphi(p_i^k)}$.
   - Jeśli na poziomie l mamy wierzchołek z wpisaną liczbą d, to możemy mieć do czynienia z jedną z następujących dwóch sytuacji:
     - dla każdej liczby $k \in \mathbb{N}$ takiej, że $\varphi(2^k) = d$, rysujemy krawędź z etykietą k zakończoną wierzchołkiem znajdującym się na poziomie $l+1$, w którym wpisujemy znak $\checkmark$;
     - jeśli nie istnieje $k \in \mathbb{N}$ takie, że $\varphi(2^k) = d$, to rysujemy krawędź (bez etykiety) zakończoną wierzchołkiem na poziomie $l+1$, w którym wpisujemy znak $\times$.
   - Dla każdego wierzchołka z poziomu $l+1$ z wpisanym znakiem $\checkmark$ odczytujemy (od góry) etykiety $k_1, \ldots, k_l$ krawędzi prowadzących od korzenia do tego wierzchołka: każdy taki ciąg daje jedno z rozwiązań równe

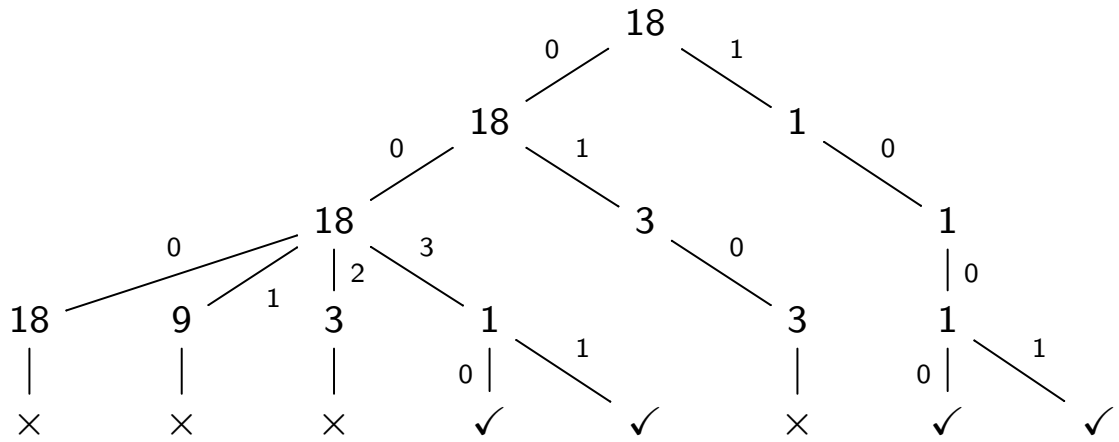
$$p_1^{k_1} \cdots p_l^{k_l}.$$

Równania z funkcją Eulera – przykład, część II

2.

	19	7	3	2
0	1	1	1	1
1	18	6	2	1
2	~~342~~	~~42~~	6	2
3			18	~~4~~
4			~~×~~	

3.



Dla wierzchołków z najniższego poziomu ze znakiem ✓ wypisujemy ciągi etykiet krawędzi prowadzących z korzenia:

$$(0,0,3,0), \qquad (0,0,3,1), \qquad (1,0,0,0), \qquad (1,0,0,1).$$

Powyższe ciągi odpowiadają następującym odpowiedziom:

$19^0 \cdot 7^0 \cdot 3^3 \cdot 2^0 = 27, \qquad 19^0 \cdot 7^0 \cdot 3^3 \cdot 2^1 = 54, \qquad 19^1 \cdot 7^0 \cdot 3^0 \cdot 2^0 = 19, \qquad 19^1 \cdot 7^0 \cdot 3^0 \cdot 2^1 = 38.$

Twierdzenie Eulera

Twierdzenie (Euler)

Jeśli $n \in \mathbb{N}_+$, $a \in \mathbb{Z}$ i $\gcd(a, n) = 1$, to

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