Funkcja Eulera

Bartłomiej BZDĘGA

Niech n będzie liczbą całkowitą dodatnią. Przez $\varphi(n)$ oznaczamy liczbę tych reszt z dzielenia przez n, które są względnie pierwsze z n. Jest to tytułowa funkcja Eulera.

Zachodzi równość $\varphi(1) = 1$, gdyż $\mathtt{NWD}(0,1) = 1$. Dalej będziemy rozważać wyłącznie $n > 1$.

Jeżeli $n > 1$ i znamy wszystkie dzielniki pierwsze liczby n – niech będą nimi $p_1, p_2, \ldots, p_k$ – to wartość funkcji Eulera możemy wyrazić jawnym wzorem. Aby go wyprowadzić, wykorzystamy regułę włączeń i wyłączeń (zob. kącik 43. w Δ^7_{22}). Niech A_d oznacza zbiór tych reszt z dzielenia przez n, które są podzielne przez d. Jeśli $d \mid n$, to $|A_d| = n/d$. Ze zbioru reszt z dzielenia przez n należy wyeliminować te liczby, które mają wspólny dzielnik z n, więc

$$\varphi(n) = n - |A_{p_1} \cup A_{p_2} \cup \ldots \cup A_{p_k}|\,.$$

Nietrudno zauważyć, że $A_{p_{i_1}} \cap \ldots \cap A_{p_{i_j}} = A_{p_{i_1}\ldots p_{i_j}}$ dla $i_1 < \ldots < i_j$. Na mocy reguły włączeń i wyłączeń

$$(*) \quad \varphi(n) = n - \sum_{j=1}^{k} (-1)^{j-1} \sum_{1 \leqslant i_1 < \ldots < i_j \leqslant k} |A_{p_{i_1}\ldots p_{i_j}}|$$

$$= n - \sum_{j=1}^{k} (-1)^{j-1} \sum_{1 \leqslant i_1 < \ldots < i_j \leqslant k} \frac{n}{p_{i_1}\ldots p_{i_j}} = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_n}\right).$$

Ze wzoru $(*)$ wynika, że jeśli m i n są liczbami względnie pierwszymi, to $\varphi(mn) = \varphi(m)\varphi(n)$. O funkcji spełniającej taki warunek mówimy, że jest multiplikatywna. Można podać niezależny dowód multiplikatywności funkcji φ za pomocą chińskiego twierdzenia o resztach, o którym jeszcze kiedyś napiszę.

Zwróćmy uwagę, że dla liczby pierwszej p mamy $\varphi(p) = p - 1$. Małe twierdzenie Fermata (zob. kącik 44. w Δ^8_{22}) można więc zapisać następująco: jeśli a jest liczbą całkowitą względnie pierwszą z p, to $a^{\varphi(p)} \equiv 1 \pmod{p}$. Naturalnym uogólnieniem tego twierdzenia jest

Twierdzenie Eulera. Niech $n > 1$ będzie liczbą naturalną. Jeżeli a jest liczbą całkowitą względnie pierwszą z n, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód jest bardzo podobny do przedstawionego w poprzednim kąciku dowodu małego twierdzenia Fermata, trzeba tylko znaleźć odpowiednik lematu o ciągu arytmetycznym.

Lemat. Przy założeniach z twierdzenia Eulera – niech $r_1 < r_2 < \ldots < r_{\varphi(n)}$ będą wszystkimi resztami z dzielenia przez n względnie pierwszymi z n i niech s_i oznacza resztę z dzielenia przez n liczby ar_i dla $i = 1, 2, \ldots, \varphi(n)$. Wówczas

$$\{s_1, s_2, \ldots, s_{\varphi(n)}\} = \{r_1, r_2, \ldots, r_{\varphi(n)}\}.$$

Dowód lematu. Ponieważ a oraz r_i są względnie pierwsze z n, liczba ar_i, a w konsekwencji również s_i jest względnie pierwsza z n. Pozostaje wykazać, że $ar_i \not\equiv ar_j \pmod{n}$ dla $1 \leqslant i < j \leqslant \varphi(n)$. Gdyby było inaczej, to mielibyśmy podzielność $n \mid a(r_j - r_i)$, z której wynika, że $n \mid r_j - r_i$, gdyż a i n są względnie pierwsze. Jednak $0 < r_j - r_i < n$ – sprzeczność.

Dowód twierdzenia Eulera. Z lematu wynika, że

$$a^{\varphi(n)} r_1 r_2 \ldots r_{\varphi(n)} = (ar_1)(ar_2)\ldots(ar_{\varphi(n)}) \equiv s_1 s_2 \ldots s_{\varphi(n)} = r_1 r_2 \ldots r_{\varphi(n)} \pmod{n},$$

wystarczy więc podzielić obie strony kongruencji przez $r_1 r_2 \ldots r_{\varphi(n)}$, co można uczynić, gdyż jest to liczba względnie pierwsza z n.

Wskazówki do zadań

1. $2^{16} - 2^4 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$. Sprawdzając podzielność przez niepierwsze czynniki przedstawionego iloczynu, korzystamy z twierdzenia Eulera, natomiast dowodząc podzielności przez 2^4, warto wykorzystać wzory skróconego mnożenia.
2. Najmniejszy dzielnik pierwszy liczby złożonej n nie przekracza $\sqrt{n}$.
3. Jeśli liczb pierwszych jest skończenie wiele i n jest ich iloczynem, to z definicji $\varphi(n) = 1$, ale to się nie zgadza ze wzorem $(*)$.
4. Niech x będzie największym dzielnikiem liczby n względnie pierwszym z a oraz $y = n/x$. Wystarczy wykazać, że $y \mid a^\alpha$ oraz $x \mid a^{\varphi(n)} - 1$. W ostatniej podzielności skorzystać z multiplikatywności funkcji φ oraz twierdzenia Eulera.
5. Jeśli a_n jest liczbą pierwszą, to $a_{n+1} = a_n + c - 1$, więc wśród 2c kolejnych wyrazów tego ciągu musi wystąpić liczba złożona podzielna przez c. Jeśli a_n jest złożona, to szacujemy a_{n+1} za pomocą nierówności z zadania 2. Reszta jest kwestią techniki – dowodzimy, że ciąg (a) ma nieskończenie wiele wyrazów nieprzekraczających pewnej dużej liczby M, więc pewne dwa jego wyrazy muszą być równe, a to w połączeniu z indukcją daje tezę.
6. Rozważmy $n > 2$. Podobnie jak w dowodzie twierdzenia Wilsona w poprzednim kąciku, parujemy reszty z ich odwrotnościami modulo n – iloczyn sparowanych reszt da nam jedynkę modulo n. Pozostają reszty, które są swoimi własnymi odwrotnościami – parujemy każdą taką resztę r z resztą $n - r$. Jeśli t jest liczbą par $\{r, n - r\}$, to $r_1 r_2 \cdots r_{\varphi(n)} \equiv (-1)^t \pmod{n}$. (Można wykazać, że otrzymamy -1 wtedy i tylko wtedy, gdy $n \in \{4, p^\alpha, 2p^\alpha\}$ dla pewnej liczby pierwszej $p > 2$ i liczby całkowitej dodatniej α.)

Zadania

1. Udowodnić, że $2^{16} - 2^4 \mid n^{16} - n^4$ dla każdego naturalnego n.
2. Wykazać, że $\varphi(n) \leqslant n - \sqrt{n}$ dla liczb złożonych n.
3. Za pomocą definicji funkcji φ i wzoru $(*)$ wykazać, że liczb pierwszych jest nieskończenie wiele.
4. Niech $n \geqslant 2$ będzie liczbą naturalną, a $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ jej rozkładem na czynniki pierwsze. Połóżmy $\alpha = \max\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. Wykazać, że $n \mid a^{\varphi(n)+\alpha} - a^\alpha$ dla każdej liczby całkowitej a. (Dla liczb pierwszych otrzymujemy $p \mid a^p - a$ – jest to alternatywna wersja małego twierdzenia Fermata).
5. Ciąg $(a_1, a_2, a_3, \ldots)$ spełnia następujące warunki: a_1 jest liczbą całkowitą dodatnią oraz $a_{n+1} = \varphi(a_n) + c$ dla $n \geqslant 1$, przy czym $c \geqslant 2$ jest pewną ustaloną liczbą naturalną. Dowieść, że ten ciąg jest od pewnego miejsca okresowy.
6. Wykaż, że iloczyn $r_1 r_2 \ldots r_{\varphi(n)}$ z dowodu twierdzenia Eulera przystaje do 1 lub -1 modulo n. (Jest to uogólnienie twierdzenia Wilsona).