Twierdzenie Eulera (teoria liczb)

Z Wikipedii, wolnej encyklopedii

Twierdzenie Eulera o liczbach względnie pierwszych to twierdzenie teorii liczb, które mówi, co następuje:

Spis treści

Treść twierdzenia

Jeżeli $m \in \mathbb{Z}_+$ i $a \in \mathbb{Z}$ są liczbami względnie pierwszymi, to *m* dzieli liczbę $a^{\varphi(m)} - 1$, gdzie φ(*m*) oznacza wartość funkcji Eulera, czyli liczbę tych liczb całkowitych dodatnich mniejszych od *m*, które są z *m* względnie pierwsze.

Innymi słowy, zachowując powyższe oznaczenia, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Słabszą wersją tego twierdzenia jest małe twierdzenie Fermata.

Przykład

Mamy φ(10) = 4 — np. liczby 7,21,133 są względnie pierwsze z 10 (7 jest liczbą pierwszą, $21 = 3 \cdot 7, 133 = 7 \cdot 19, 10 = 2 \cdot 5$), dlatego też liczby $7^4 - 1$, $133^4 - 1$, $21^4 - 1$, itd. są podzielne przez 10.

Dowód[1]

Niech $m \in \mathbb{Z}_+$ i $a \in \mathbb{Z}$ oraz $\mathrm{NWD}(m, a) = 1$.

Jeżeli *m* = 1, to φ(*m*) = 1, a więc $a^{\varphi(m)} = a$. Oczywiście 1 | *a* − 1. Zatem dla *m* = 1 twierdzenie jest prawdziwe.

Niech teraz *m* > 1.

Przez *A* oznaczmy zbiór $\{p_1, p_2, ..., p_{\varphi(m)}\}$ liczb należących do $\mathbb{Z}_+$, pierwszych względem *m* i mniejszych lub równych *m*.

Niech dla każdego $k \in \{1, 2, ..., \varphi(m)\}$, r_k oznacza resztę z dzielenia liczby ap_k przez *m*.

Niech $B = \{r_1, r_2, ..., r_{\varphi(m)}\}$.

Udowodnimy, że $A = B$. W tym celu wystarczy pokazać, że:

1. dla każdej liczby r_k, gdzie $k \in \{1, 2, ..., \varphi(m)\}$, zachodzi $0 < r_k \leq m$ i r_k jest względnie pierwsza względem m (czyli $B \subseteq A$),
2. funkcja $f\colon A \to B$ opisana wzorem $f(p_k) = r_k$, gdzie $k = 1, 2, ..., \varphi(m)$, jest różnowartościowa (wtedy zbiory A i B byłyby równoliczne, gdyż f jest z definicji suriekcją),

bowiem zbiory A i B są skończone (a więc nie mogą być równoliczne ze swoimi podzbiorami właściwymi).

Liczby r_k są resztami z dzielenia przez m, więc są większe lub równe 0 i mniejsze od m.

Jest też oczywiście zawsze: $r_k \equiv ap_k \pmod m$, a więc: (1) $r_k = ap_k + mt_k$ dla $k = 1, 2, ..., \varphi(m)$ i $t_k \in \mathbb{Z}$.

Ponieważ zarówno p_k jak i a są względnie pierwsze względem m, to również ap_k ma tą własność. Załóżmy, że pewna liczba całkowita d dzieli zarówno r_k jak i m. Ze wzoru (1) wynika, że d musi być równe 1, a więc r_k i m muszą być względnie pierwsze. Stąd też $r_k \neq 0$, co kończy dowód własności 1.

Załóżmy teraz, że dla pewnej pary $(k, l) \in \{1, 2, ..., \varphi(m)\}^2$ takiej, że $k \neq l$, zachodzi $f(p_k) = f(p_l)$. Byłoby wtedy $ap_k \equiv ap_l \pmod m$, a więc, ponieważ $a \neq 0$ jako liczba względnie pierwsza względem m, byłoby też wtedy $p_k \equiv p_l \pmod m$, co jest niemożliwe, skoro p_k, p_l są różnymi liczbami całkowitymi dodatnimi mniejszymi od m. Zatem dla każdej pary $(k, l) \in \{1, 2, ..., \varphi(m)\}^2$ takiej, że $k \neq l$, zachodzi $f(p_k) \neq (p_l)$, co kończy dowód własności 2.

Ponieważ $A = B$, zatem $\prod_{k=1}^{\varphi(m)} p_k = \prod_{k=1}^{\varphi(m)} r_k$. Skoro zaś $\prod_{k=1}^{\varphi(m)} r_k \equiv a^{\varphi(m)} \prod_{k=1}^{\varphi(m)} p_k \pmod m$, to również $\prod_{k=1}^{\varphi(m)} p_k \equiv a^{\varphi(m)} \prod_{k=1}^{\varphi(m)} p_k \pmod m$. Stąd, ponieważ $\prod_{k=1}^{\varphi(m)} p_k$ jest względnie pierwsze z m, zachodzi $a^{\varphi(m)} \equiv 1 \pmod m$ □

Inny dowód [2]

Niech $m \in \mathbb{Z}_+$ i $a \in \mathbb{Z}$ będą liczbami względnie pierwszymi, a $P = (a_1, a_2, \ldots, a_{\varphi(m)})$ będzie ciągiem liczb naturalnych mniejszych od m i względnie z nim pierwszych. Wtedy ciąg $P' = (aa_1, aa_2, \ldots, aa_{\varphi(m)})$ z wyrazami wziętymi $\pmod m$ jest permutacją ciągu P. Istotnie, dla każdego i, aa_i jest również względnie pierwsze z m, zatem zachodzi $aa_i \equiv a_k \pmod m$ dla pewnego k i ponieważ ponadto $aa_i \equiv aa_j \Leftrightarrow a_i \equiv a_j \pmod m$ (bo z założenia a i m są względnie pierwsze), a zatem elementy ciągu P' są różne, więc istotnie jest to permutacja.

W związku z tym:

$$\begin{aligned} a_1 a_2 \ldots a_{\varphi(m)} &\equiv (aa_1)(aa_2)\ldots(aa_{\varphi(m)}) \pmod m \\ a_1 a_2 \ldots a_{\varphi(m)} &\equiv a^{\varphi(m)} a_1 a_2 \ldots a_{\varphi(m)} \pmod m \\ 1 &\equiv a^{\varphi(m)} \pmod m \end{aligned}$$

QED.

Przypisy

1. ↑ Dowód ten jest przeredagowaną wersją dowodu zawartego w książce Wacława Sierpińskiego *Wstęp do teorii liczb*.
2. ↑ Naoki Sato: Number Theory (http://www.scribd.com/doc/9386316/Number-Theory) (ang.). [dostęp 03.06.2009]. ss. 14-15.