Małe Twierdzenie Fermata

Tomasz Kossakowski

12 grudnia 2025

Rys historyczny

Małe twierdzenie Fermata zostało sformułowane w 1640 roku przez Pierre'a de Fermata w liście do jego przyjaciela, Frénicle'a de Bessy. Sam Fermat nie podał jednak dowodu, twierdząc, że jest on zbyt długi, by go zapisać w formie notatki. Przez wiele lat twierdzenie pozostawało bez formalnego uzasadnienia, aż w 1736 roku pierwszy poprawny dowód opublikował Leonhard Euler. Dopiero na początku XX wieku, około 1913 roku, zaczęto powszechnie używać nazwy „małe twierdzenie Fermata".

Krótkie przypomnienie kongruencji

Definicja 1 (kongruencja)

Niech $a, b \in \mathbb{Z}$ oraz niech $m \in \mathbb{Z}_+$. Mówimy, że a przystaje do b modulo m, jeśli liczba $a - b$ dzieli się przez m. Stosujemy oznaczenie

$$a \equiv b \pmod{m}$$

i nazywamy je kongruencją. Oznacza to również, że liczby a i b dają taką samą resztę z dzielenia przez m.

Kongruencje mają wiele przydatnych właściwości.

Twierdzenie 1 (własności kongruencji)

Dla $a, b, c, d \in \mathbb{Z}$ oraz $m, n \in \mathbb{Z}_+$ zachodzą poniższe zależności.

1. $a \equiv a \pmod{m}$.
2. Jeśli $a \equiv b \pmod{m}$, to $b \equiv a \pmod{m}$.
3. Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$.
4. Jeśli $a \equiv b \pmod{m}$, to $a \pm c \equiv b \pm c \pmod{m}$.
5. Jeśli $a \equiv b \pmod{m}$, to $ac \equiv bc \pmod{m}$.
6. Jeśli $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$, to $a \pm c \equiv b \pm d \pmod{m}$.
7. Jeśli $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$, to $ac \equiv bd \pmod{m}$.
8. Jeśli $a \equiv b \pmod{m}$, to $a^n \equiv b^n \pmod{m}$.

Twierdzenie i jego dowód

Twierdzenie 2 (MTF)

Jeżeli p jest liczbą pierwszą, to dla dowolnej liczby całkowitej a zachodzi

$$a^p \equiv a \pmod{p}.$$

Innymi słowy, jeśli p jest liczbą pierwszą, a a jest taką liczbą całkowitą, że liczby a i p są względnie pierwsze, to

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dowód. Gdy $p = 2$, sprawa jest oczywista. Załóżmy więc, że $p > 2$. Kongruencję $a^p \equiv a \pmod{p}$ udowodnimy najpierw dla $a = n \in \mathbb{N}$ przez indukcję względem n.

Dla $n = 1$ sprawdzenie jest trywialne. Z założenia indukcyjnego $n^p \equiv n \pmod p$, wzoru dwumiennego oraz faktu, że dla $1 \leqslant k \leqslant p-1$ liczba $\binom{p}{k}$ jest podzielna przez p dostajemy, że:

$$(n+1)^p = n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + \binom{p}{p-1}n + 1 \equiv n^p + 1 \equiv n + 1 \pmod p.$$

To dowodzi kongruencji dla wszystkich liczb naturalnych n.
Jeśli a jest ujemną liczbą całkowitą, to wobec nieparzystości p (gdy $p > 2$) mamy:

$$a^p = -(-a)^p \equiv -(-a) \equiv a \pmod p.$$

Mając $a^p \equiv a \pmod p$, czyli $p \mid a^p - a$, po wykorzystaniu założenia $p \nmid a$ (gdy chcemy przejść do postaci $a^{p-1} \equiv 1 \pmod p$), otrzymujemy $p \mid a(a^{p-1} - 1)$, a stąd $p \mid a^{p-1} - 1$, co daje $a^{p-1} \equiv 1 \pmod p$. □

Ćwiczenie 1. Wyznacz resztę $2^{50} \pmod 7$.

Ćwiczenie 2. Czy istnieje liczba całkowita n taka, że $n \equiv 7 \pmod{13}$ oraz $5n^{40} \equiv 12 \pmod{13}$?

Ćwiczenie 3. Niech $a, b \in \mathbb{Z}$ oraz $p \in \mathbb{P}$. Udowodnić, że $p \mid ab^p - a^p b$.

Ćwiczenie 4. Niech $p \in \mathbb{P}$ oraz $a \in \mathbb{Z}$. Udowodnić, że jeśli $a^2 \equiv 1 \pmod p$, to $a \equiv \pm 1 \pmod p$.

Ćwiczenie 5. Niech $p \in \mathbb{P}$, $p > 2$ oraz $s = \frac{p-1}{2}$. Udowodnić, że jeśli $p \nmid a$, to $a^s \equiv \pm 1 \pmod p$.

Zadania

Zadanie 1 (Obóz MIKO, gr. młodsza, P4)**.** Niech $n \geqslant 3$ będzie taką liczbą naturalną, że $4n + 1$ jest liczbą pierwszą. Udowodnij, że $4n + 1$ dzieli $n^{2n} - 1$.

Zadanie 2. Dla danych liczb całkowitych b i $a_1, a_2, \ldots, a_{20}$ zachodzi równość

$$b^{11} = a_1^{11} + a_2^{11} + a_3^{11} + \ldots + a_{20}^{11}.$$

Udowodnić, że iloczyn $ba_1a_2 \cdot \ldots \cdot a_{20}$ jest liczbą podzielną przez 23.

Zadanie 3. Udowodnić, że jeżeli $7 \mid x^6 + y^6 + z^6$ dla pewnych liczb całkowitych x, y, z, to $343 \mid xyz$.

Zadanie 4. Załóżmy, że p i q to liczby pierwsze, $a^p \equiv a \pmod q$ i $a^q \equiv a \pmod p$. Udowodnić, że

$$a^{pq} \equiv a \pmod{pq}.$$

Zadanie 5 (75OM-I-5)**.** Dana jest dodatnia liczba całkowita dająca resztę 3 z dzielenia przez 7. Udowodnić, że suma sześcianów jej dodatnich dzielników dzieli się przez 7.

Zadanie 6 (Rabka 2018, gr. średnia)**.** Dane są liczby całkowite x, y oraz liczby pierwsze p, q, R, które spełniają równość

$$x^R + R \cdot pq = y^R.$$

Udowodnić, że przynajmniej jedna z liczb p, q jest równa R.

Zadanie 7 (69OM-I-9)**.** Wykazać, że dla nieskończenie wielu liczb całkowitych $n > 1$ równanie

$$(x+1)^{n+1} - (x-1)^{n+1} = y^n$$

nie ma rozwiązania w liczbach całkowitych x, y.

Zadanie 8 (Obóz OMJ 2013, poziom OM, P14)**.** Dana jest liczba pierwsza $p > 2$. Wykaż, że istnieje nieskończenie wiele takich dodatnich liczb całkowitych n, że liczba $2^n - n$ jest podzielna przez p.

Zadanie 9 (76OM-II-2)**.** Wyznaczyć wszystkie liczby całkowite $n \geqslant 2$ o następującej własności: liczba $2^k \cdot n - 1$ jest pierwsza dla każdego $k \in \{2, 3, \ldots, n\}$.

Zadanie 10 (IMO 2005, P4)**.** Wyznacz wszystkie dodatnie liczby całkowite, które są względnie pierwsze ze wszystkimi wyrazami nieskończonego ciągu

$$2^n + 3^n + 6^n - 1, \quad n \geqslant 1.$$