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

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

1 Rozwiązania ćwiczeń

Rozwiązanie 1. Zauważmy, że $2^{50} = 2^{48+2} = 4 \cdot \left(2^6\right)^8$ oraz $2^6 \equiv 1 \pmod 7$, zatem $2^{50} \equiv 4 \cdot 1^8 = 4 \pmod 7$.

Rozwiązanie 2. Z MTF dostajemy, że

$$5n^{40} \equiv 5 \cdot \left(n^{12}\right)^3 \cdot n^4 \equiv 5n^4 \equiv 5 \cdot 7^4 \equiv 49^2 \cdot 5 \equiv (-3)^2 \cdot 5 = 45 \equiv 6 \pmod{13}.$$

Nie ma takiej liczby

Rozwiązanie 3. Zapiszmy wyrażenie w postaci

$$ab^p - a^p b = ab\left(b^{p-1} - a^{p-1}\right).$$

Jeżeli $p \mid a$ lub $p \mid b$, to zarówno ab^p, jak i $a^p b$ są podzielne przez p, a więc również ich różnica jest podzielna przez p. Załóżmy teraz, że $p \nmid a$ oraz $p \nmid b$. Wówczas na mocy MTF mamy

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

Stąd $b^{p-1} - a^{p-1} \equiv 0 \pmod p$. Wobec tego $ab\left(b^{p-1} - a^{p-1}\right) \equiv 0 \pmod p$, czyli $ab^p - a^p b \equiv 0 \pmod p$.
Zatem $p \mid ab^p - a^p b$, co kończy dowód.

Rozwiązanie 4. Zaczynamy od przekształcenia równania:

$$a^2 \equiv 1 \pmod p \iff a^2 - 1 \equiv 0 \pmod p \iff (a-1)(a+1) \equiv 0 \pmod p.$$

Ponieważ p jest liczbą pierwszą, jeśli iloczyn $(a-1)(a+1)$ jest podzielny przez p, to przynajmniej jeden z czynników musi być podzielny przez p. Stąd mamy dwa przypadki:

$$a - 1 \equiv 0 \pmod p \quad \text{lub} \quad a + 1 \equiv 0 \pmod p,$$

czyli

$$a \equiv 1 \pmod p \quad \text{lub} \quad a \equiv -1 \pmod p.$$

Rozwiązanie 5. Z definicji $s = \frac{p-1}{2}$ otrzymujemy:

$$a^{p-1} = a^{2s} \equiv 1 \pmod p.$$

Zatem

$$\left(a^s\right)^2 \equiv 1 \pmod p.$$

Z poprzedniego zadania wiemy, że jeśli $x^2 \equiv 1 \pmod p$, to $x \equiv 1 \pmod p$ lub $x \equiv -1 \pmod p$. Zatem w naszym przypadku:

$$a^s \equiv 1 \pmod p \quad \text{lub} \quad a^s \equiv -1 \pmod p.$$

2 Rozwiązania zadań

Rozwiązanie 1. Niech $p = 4n + 1$, oczywiście $p \nmid n$ oraz $p \neq 2$. Korzystając z MTF otrzymujemy

$$p \mid n^{4n} - 1 = (n^{2n} - 1)(n^{2n} + 1),$$

więc chcemy udowodnić, że $p \nmid n^{2n} + 1$. Zauważamy, że jeśli ta podzielność zachodzi, to (korzystamy z $p \perp 2$):

$$p \mid 4(n^{2n} + 1) - (4n + 1)n^{2n-1} = 4 - n^{2n-1}.$$

Postępując analogicznie dostajemy, że dla każdego k:

$$p \mid n^{2n-k} + (-1)^k \cdot 4^k.$$

W szczególności dla $k = 2n$ zachodzi $p \mid 1 + 4^{2n} = 1 + 2^{4n} \equiv 2 \neq 0 \pmod p$, gdzie w ostatnim przystawaniu ponownie użyliśmy MTF. Sprzeczność oznacza, że $p \mid n^{2n} - 1$.

Rozwiązanie 2. Jeżeli jedna z liczb a_i jest podzielna przez 23, to iloczyn $ba_1a_2 \ldots a_{20}$ jest podzielny przez 23 i dowód jest zakończony.
Załóżmy więc, że liczby $a_1, a_2, \ldots, a_{20}$ nie są podzielne przez 23. Wówczas dla każdego $1 \leqslant i \leqslant 20$, a_i^{11} jest liczbą całkowitą, której kwadrat a_i^{22} daje resztę 1 przy dzieleniu przez 23:

$$a_i^{22} \equiv 1 \pmod{23}.$$

Wobec tego

$$a_i^{11} \equiv \pm 1 \pmod{23} \quad \text{dla każdego } 1 \leqslant i \leqslant 20,$$

co wynika z ćwiczenia 4.
Jeżeli k składników sumy $a_1^{11} + a_2^{11} + \ldots + a_{20}^{11}$ przystaje do 1 modulo 23, a $20 - k$ pozostałych przystaje do -1 modulo 23, to

$$b^{11} = a_1^{11} + a_2^{11} + \ldots + a_{20}^{11} \equiv k - (20 - k) \equiv 2k - 20 \pmod{23}.$$

Zatem $b^{11} \equiv 2k - 20 \pmod{23}$. Liczba $2k - 20$ modulo 23 może przyjmować wartości parzyste w zakresie -20 do 20, ale niekoniecznie ± 1.
Ponieważ (z ćwiczenia 5) dla $p = 23$ i $s = \frac{23-1}{2} = 11$, mamy $b^{11} \equiv \pm 1 \pmod{23}$ o ile $23 \nmid b$, więc porównując z wyrażeniem $2k - 20$ otrzymujemy, że

$$2k - 20 \equiv \pm 1 \pmod{23}.$$

Można sprawdzić, że równanie to nie ma rozwiązania dla całkowitych k z zakresu $0 \leqslant k \leqslant 20$.
Wobec tego nasze założenie, że $23 \nmid b$, prowadzi do sprzeczności. Zatem $23 \mid b$, a to oznacza, że iloczyn $ba_1a_2 \ldots a_{20}$ jest podzielny przez 23.

Rozwiązanie 3. Używając MTF wiemy, że suma $x^6 + y^6 + z^6$ w zależności od podzielności poszczególnych wyrazów przez 7 może przyjmować wartości od 0 do 3. Ten fakt mówi, że 7 musi dzielić x, y i z żeby założenie zadania było spełnione, a iloczyn trzech liczb podzielnych przez 7 daje liczbę podzielną przez 343.

Rozwiązanie 4. Używając Małego Twierdzenia Fermata (MTF) dostajemy:

$$a^p \equiv a \Rightarrow (a^p)^q \equiv a^q \equiv a \Rightarrow a^{pq} \equiv a \pmod{p}$$
$$a^q \equiv a \Rightarrow (a^q)^p \equiv a^p \equiv a \Rightarrow a^{pq} \equiv a \pmod{q}$$

Wynika z tego, że $a^{pq} = px + a = qy + a$, ale z tego wnioskujemy, że $px = qy$. Można to zapisać jako $x = kq$, $y = kp$ dla $k \in \mathbb{Z}$, więc

$$a^{pq} = p(qk) + a = q(pk) + a = (pq)k + a \Rightarrow a^{pq} \equiv a \pmod{pq}.$$

Rozwiązanie 5. Dodatnie dzielniki n oznaczymy przez $d_1, d_2, \ldots, d_m$. Ponieważ $7 \nmid n$, mamy $d_i \perp 7$ dla każdego dzielnika d_i. Z Małego Twierdzenia Fermata dla $p = 7$:

$$d_i^6 \equiv 1 \pmod{7} \quad \Longrightarrow \quad (d_i^3)^2 \equiv 1 \pmod{7}.$$

Stąd

$$d_i^3 \equiv 1 \pmod{7} \quad \text{lub} \quad d_i^3 \equiv -1 \pmod{7}.$$

Liczba $n = 7k+3$ nie jest kwadratem, więc liczba dzielników m jest parzysta. Dzielniki możemy więc pogrupować w pary:

$$\left(d_i, \frac{n}{d_i}\right).$$

Zauważmy, że $n^3 \equiv 3^3 = 27 \equiv -1 \pmod{7}$, zatem

$$d_i^3 \equiv 1 \quad \text{oraz} \quad \left(\frac{n}{d_i}\right)^3 \equiv -1 \pmod{7} \qquad \text{lub} \qquad d_i^3 \equiv -1 \quad \text{oraz} \quad \left(\frac{n}{d_i}\right)^3 \equiv 1 \pmod{7}.$$

Dla każdej pary mamy:

$$d_i^3 + \left(\frac{n}{d_i}\right)^3 \equiv 1 + (-1) \equiv 0 \pmod{7}$$

lub odwrotnie:

$$d_i^3 + \left(\frac{n}{d_i}\right)^3 \equiv -1 + 1 \equiv 0 \pmod{7}.$$

Zatem suma wszystkich sześcianów dzielników jest podzielna przez 7:

$$\sum_{i=1}^{m} d_i^3 \equiv 0 \pmod{7}.$$

Rozwiązanie 6. Wszystkie przystawania będziemy rozważać modulo R. Zauważmy, że $x^R \equiv y^R$, ale na mocy Małego Twierdzenia Fermata mamy, że $x \equiv x^R$ oraz $y \equiv y^R$, więc dostajemy, że $x \equiv y$. Zatem $y - x$ jest podzielne przez R. Zauważmy, że:

$$x^{R-1} + x^{R-2}y + \cdots + xy^{R-2} + y^{R-1} \equiv R \cdot x^{R-1} \equiv 0$$

A zatem na mocy wzoru skróconego mnożenia $R^2 \mid y^R - x^R$, więc $R^2 \mid R \cdot pq$, czyli $R \mid pq$. Z pierwszości R, p, q wynika teza.

Rozwiązanie 7. Wykażemy, że dla $n = p - 1$, gdzie $p > 2$ jest dowolną liczbą pierwszą, podane równanie nie ma rozwiązania w liczbach całkowitych.
Załóżmy, że istnieją takie liczby całkowite x, y, że zachodzi równość

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

Z małego twierdzenia Fermata wynika, że

$$p \mid (x+1)^p - (x+1) \quad \text{oraz} \quad p \mid (x-1)^p - (x-1).$$

Wobec tego

$$p \mid (x+1)^p - (x+1) - \big((x-1)^p - (x-1)\big) = (x+1)^p - (x-1)^p - 2 = y^{p-1} - 2.$$

Stąd otrzymujemy podzielność

$$p \mid y(y^{p-1} - 2) = y^p - 2y.$$

Ponownie korzystając z małego twierdzenia Fermata dostajemy, że $p \mid y^p - y$, co wraz z poprzednią podzielnością daje $p \mid y$ — sprzeczność z tym, że $p \mid y^{p-1} - 2$.

Rozwiązanie 8. Dla dowolnej dodatniej liczby naturalnej k przyjmijmy $n_k = (p-1)(kp-1)$. Wówczas na podstawie małego twierdzenia Fermata otrzymujemy

$$2^{n_k} - n_k = 2^{(p-1)(kp-1)} - (p-1)(kp-1) \equiv 1^{kp-1} - (-1)\cdot(-1) \equiv 1 - 1 \equiv 0 \pmod{p},$$

skąd wynika, że ciąg liczb $\{n_k\}_{k\in\mathbb{N}}$ zdefiniowany powyższym wzorem spełnia warunki zadania.

Rozwiązanie 9. Liczby $n = 2$ i $n = 3$ spełniają warunki zadania, bowiem liczby

$$2^2 \cdot 2 - 1 = 7, \quad 2^2 \cdot 3 - 1 = 11, \quad 2^3 \cdot 3 - 1 = 23$$

są pierwsze. Poniżej wykażemy, że liczby $n \geqslant 4$ nie spełniają warunków zadania.
Jeśli $n \geqslant 4$ jest liczbą parzystą, to $n - 1$ jest nieparzystą liczbą większą lub równą 3, a więc ma nieparzysty dzielnik pierwszy p. Wówczas

$$2 \leqslant p - 1 \leqslant n.$$

Z małego twierdzenia Fermata wynika, że

$$2^{p-1} \cdot n - 1 \equiv 2^{p-1} - 1 \equiv 0 \pmod{p},$$

więc $2^{p-1} \cdot n - 1$ dzieli się przez p. Liczba ta jest większa od p, więc jest złożona. Stąd n nie spełnia warunków zadania.
Jeśli $n \geqslant 5$ jest liczbą nieparzystą, to liczba $n - 2$ jest nieparzystą liczbą większą lub równą 3, a więc ma nieparzysty dzielnik pierwszy p. Jeśli $p = 3$, to liczba $2^3 \cdot n - 1 = 8(n-2) + 15$ dzieli się przez 3 i jest większa od 3, jest więc złożona. W przeciwnym razie $p \geqslant 5$, wtedy $2 \leqslant p - 2 \leqslant n$. Z małego twierdzenia Fermata wynika, że

$$2^{p-2} \cdot n - 1 \equiv 2^{p-2} \cdot 2 - 1 \equiv 2^{p-1} - 1 \equiv 0 \pmod{p},$$

więc $2^{p-2} \cdot n - 1$ dzieli się przez p. Jest to liczba większa od p, więc jest złożona. Zatem n nie spełnia warunków zadania.

Rozwiązanie 10. Odpowiedzią jest 1. Pokażemy, że każda liczba pierwsza p dzieli pewien wyraz tego ciągu. Dla $p = 2$ wystarczy $n = 1$, a dla $p = 3$ wystarczy $n = 2$.
Dla $p \neq 2, 3$ rozważmy $n = p - 2$. Z Małego Twierdzenia Fermata mamy:

$$6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) = 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \equiv 3 + 2 + 1 - 6 \equiv 0 \pmod{p}.$$

Ponieważ p nie dzieli 6 (bo $p \neq 2, 3$), otrzymujemy:

$$p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1.$$

Zatem jedyną liczbą względnie pierwszą ze wszystkimi wyrazami ciągu jest 1.