# Małe twierdzenie Fermata

Bartosz Chomiński

## 1 Twierdzenie

Niech $p$ będzie liczbą pierwszą oraz niech $a$ będzie liczbą całkowitą niepodzielną przez $p$. Wtedy $a^{p-1}$ daje resztę 1 z dzielenia przez $p$.

## 2 Dowód (wersja bijekcyjna)

Zacznijmy od pewnego prostego lematu, który pomoże nam w pokazaniu, że mnożenie modulo jest bijekcyjne.

### 2.1 Lemat o różnowartościowości mnożenia

Niech $a \neq b$ i $c$ będą resztami z dzielenia przez $p$ i niech $c$ nie będzie podzielna przez $p$. Wtedy $a \cdot c$ i $b \cdot c$ dają różne reszty z dzielenia przez $p$.

**Dowód.** Załóżmy nie wprost, że $a \cdot c$ i $b \cdot c$ dają te same reszty z dzielenia przez $p$. Wtedy ich różnica, czyli $a \cdot c - b \cdot c$ jest liczbą podzielną przez $p$. Tę liczbę możemy również zapisać jako $(a-b) \cdot c$. Z własności liczb pierwszych wnioskujemy, że $(a-b)$ jest podzielne przez $p$ lub $c$ jest podzielne przez $p$. Żadna z tych opcji nie jest możliwa, ponieważ założenia lematu są z nimi sprzeczne. Z tej sprzeczności wnioskujemy, że $a \cdot c$ i $b \cdot c$ dają różne reszty z dzielenia przez $p$, a więc tezę lematu.

### 2.2 Bijekcja

Niech $f_a : \{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\}$ będzie funkcją zdefiniowaną jako

$$f_a(n) = (a \cdot n) \bmod p,$$

czyli mówiąc wprost $f_a$ to operacja mnożenia przez $a$ modulo $p$.

Ta funkcja dla $a \not\equiv 0 \pmod p$ jest bijekcją, ponieważ jej dziedzina jest skończona i równoliczna ze zbiorem wartości, a ponadto ta funkcja jest różnowartościowa, co pokazaliśmy w lemacie o różnowartościowości mnożenia.

### 2.3 Podsumowanie

Skoro $f_a$ jest bijekcją (a nawet *automorfizmem*), to zbiory

$$\{1, 2, 3, \ldots, p-1\}$$

oraz

$$\{f_a(1), f_a(2), f_a(3), \ldots, f_a(p-1)\}$$

są równe.

Skoro zbiory są równe, to iloczyny wszystkich ich elementów również, a więc

$$1 \cdot 2 \cdot \ldots \cdot (p-1) = f_a(1) \cdot f_a(2) \cdot \ldots \cdot f_a(p-1).$$

Rozwińmy napisy typu „$f_a(n)$” zgodnie z definicją $f_a$:

$$1 \cdot 2 \cdot \ldots \cdot (p-1) = (a \cdot 1 \bmod p) \cdot \ldots \cdot (a \cdot (p-1) \bmod p).$$

Rozważmy reszty z dzielenia przez $p$ obu stron. To pozwoli nam pozbyć się „mod $p$” z prawej strony równości:

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv (a \cdot 1) \cdot (a \cdot 2) \cdot \ldots \cdot (a \cdot (p-1)) \pmod p.$$

Wyłączmy z nawiasów po prawej stronie wystąpienia $a$:

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a^{p-1} \cdot (1 \cdot 2 \cdot \ldots \cdot (p-1)) \pmod p.$$

Zauważmy, że $a^{p-1}$ musi dawać resztę 1 z dzielenia przez $p$, ponieważ w przeciwnym razie powyższa *kongruencja* nie byłaby spełniona (por. lemat). To kończy dowód małego twierdzenia Fermata w wersji bijekcyjnej.

## 3 Dowód (wersja indukcyjna)

### 3.1 Indukcja matematyczna

Indukcja matematyczna to pewna metoda dowodzenia twierdzeń, która sprawdza się, gdy mamy do udowodnienia prawdziwość pewnej formuły dla wszystkich liczb naturalnych. Niech $\varphi(n)$ będzie formułą, której prawdziwość mamy udowodnić dla wszystkich liczb naturalnych $n$. Plan działania wygląda następująco:

1. Dowodzimy prawdziwości zdania $\varphi(0)$.

2. Dowodzimy prawdziwości zdania: dla każdej liczby naturalnej $n$ zachodzi implikacja

$$\varphi(n) \implies \varphi(n+1).$$

Jeśli wypełnimy oba punkty planu, to na podstawie zasady indukcji matematycznej możemy wnioskować prawdziwość formuły $\varphi(n)$ dla każdej liczby naturalnej $n$.

### 3.2 Zastosowanie

Ustalmy jedną konkretną liczbę pierwszą $p$.

W przypadku dowodu małego twierdzenia Fermata za formułę $\varphi(a)$ możemy przyjąć:

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

To sformułowanie wygląda trochę inaczej, niż teza twierdzenia podana wyżej, ale Dociekliwy Czytelnik z pewnością będzie w stanie się przekonać, że obecna wersja twierdzenia implikuje wersję podaną na początku.

### 3.3 Pierwszy krok indukcji

Na początek zrealizujemy pierwszy punkt z planu wyżej. Zdanie $\varphi(1)$ brzmi:

Zachodzi kongruencja $1^p \equiv 1 \pmod{p}$.

To zdanie jest w oczywisty sposób prawdziwe, zatem pierwszy punkt planu mamy za sobą.

### 3.4 Drugi krok indukcji

Implikacja, którą mamy udowodnić brzmi:

Jeśli zachodzi kongruencja $a^p \equiv a \pmod{p}$, to zachodzi kongruencja $(a+1)^p \equiv a+1 \pmod{p}$.

Zatem przystąpmy do pracy: wyrażenie $(a+1)^p$ można zapisać korzystając z *wzorów skróconego mnożenia*. Pisząc wprost, mamy

$$(a+1)^p = a^p\binom{p}{0} + a^{p-1}\binom{p}{1} + \cdots + a^0\binom{p}{p}.$$

Przyjrzyjmy się symbolom Newtona $\binom{p}{k}$. Możemy zapisać wprost z definicji

$$\binom{p}{k} = \frac{1\cdot 2\cdot 3\cdot \ldots \cdot p}{(1\cdot 2\cdot \ldots \cdot k)\cdot(1\cdot 2\cdot \ldots \cdot (p-k))}.$$

Gdy $k$ jest różne od 0 i od $p$, to ta liczba będzie podzielna przez $p$, ponieważ żaden czynnik z mianownika „nie skróci się" z czynnikiem $p$ z licznika, a więc skoro przy okazji wiemy, że będzie to liczba całkowita, to będzie również podzielna przez $p$.

Wróćmy do $(a+1)^p$, a w zasadzie do reszty z dzielenia tej liczby przez $p$ (bo to reszta nas interesuje). Skoro liczby $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ są podzielne przez $p$, to składniki sumy, które zawierają te liczby jako czynniki, również będą podzielne przez $p$, a zatem nie wpłyną na resztę z dzielenia całej sumy przez $p$. Mamy

$$\begin{aligned}
(a+1)^p &\equiv_p a^p\binom{p}{0} + a^{p-1}\binom{p}{1} + \cdots + a^0\binom{p}{p} \\
&\equiv_p a^p\binom{p}{0} + a^{p-1}\cdot 0 + \cdots + a^1\cdot 0 + a^0\binom{p}{p} \\
&\equiv_p a^p\binom{p}{0} + \underbrace{0+\cdots+0}_{0} + a^0\binom{p}{p} \\
&\equiv_p a^p + a^0 \\
&\equiv_p a^p + 1 \\
&\equiv_p a + 1.
\end{aligned}$$

Ostatnie przejście w powyższym rachunku wynika wprost z założenia indukcyjnego i w ten sposób uzyskujemy tezę implikacji, a więc dowodzimy drugiego kroku indukcyjnego, co w połączeniu z pierwszym krokiem daje pełny dowód indukcyjny.

## 4 Czytaj też


- J. Wróblewski, Materiały ligi zadaniowej OMG 2012/2013, Opowieści o indukcji. `http://math.uni.wroc.pl/~jwr/2022-23/Analiza1/indukcja.pdf`
- L. Newelski, Wstęp do matematyki. `http://math.uni.wroc.pl/~newelski/dydaktyka/wdm-A/skrypt3/skrypt/node14.html`
- T. Kazana, Małe twierdzenie Fermata. `https://www.deltami.edu.pl/temat/matematyka/teoria_liczb/2017/03/27/Male_Twierdzenie_Fermata/`