# Wielkie Twierdzenie Fermata

Dorota Blinkiewicz

Uniwersytet im. Adama Mickiewicza w Poznaniu

*67. Szkoła Matematyki Poglądowej*

*Na początku było pytanie*

24 VIII 2024

# Wielkie Twierdzenie Fermata

Pierre de Fermat (17.08.1601r. – 12.01.1665r.) [1]

## WIELKIE TWIERDZENIE FERMATA
### – ORYGINALNE BRZMIENIE –

*„Nie można podzielić sześcianu na dwa sześciany ani czwartej potęgi na dwie czwarte potęgi, ani ogólniej żadnej potęgi wyższej niż druga na dwie takie same potęgi; znalazłem naprawdę zadziwiający dowód, który nie zmieści się na zbyt wąskim marginesie”*

P. de Fermat, ∼1637r., margines prac Diofantosa pt. *Arithmetica* wydanych przez Bacheta

## WIELKIE TWIERDZENIE FERMATA – ORYGINALNE BRZMIENIE –

*„Nie można podzielić sześcianu na dwa sześciany ani czwartej potęgi na dwie czwarte potęgi, ani ogólniej żadnej potęgi wyższej niż druga na dwie takie same potęgi; znalazłem naprawdę zadziwiający dowód, który nie zmieści się na zbyt wąskim marginesie”*

P. de Fermat, ∼1637r., margines prac Diofantosa pt. *Arithmetica* wydanych przez Bacheta

## WIELKIE TWIERDZENIE FERMATA – WSPÓŁCZEŚNIE

Niech $n > 2$ będzie liczbą naturalną. Niech $x, y, z \in \mathbb{Z}$. Wówczas:

$$x^n + y^n = z^n \implies xyz = 0.$$

## WIELKIE TWIERDZENIE FERMATA
### – ORYGINALNE BRZMIENIE –

*„Nie można podzielić sześcianu na dwa sześciany ani czwartej potęgi na dwie czwarte potęgi, ani ogólniej żadnej potęgi wyższej niż druga na dwie takie same potęgi; znalazłem naprawdę zadziwiający dowód, który nie zmieści się na zbyt wąskim marginesie”*

P. de Fermat, ∼1637r., margines prac Diofantosa pt. *Arithmetica* wydanych przez Bacheta

## WIELKIE TWIERDZENIE FERMATA – WSPÓŁCZEŚNIE

Niech $n > 2$ będzie liczbą naturalną. Niech $x, y, z \in \mathbb{Z}$. Wówczas:

$$x^n + y^n = z^n \implies xyz = 0.$$

## PO PROSTU TWIERDZENIE

Od teraz zamiast pisać Wielkie Twierdzenie Fermata, będziemy pisać po prostu TWIERDZENIE.

„W Konstytucji Państw i Narodów, w Rozdziale o Prawach Człowieka powinno być zapisane:

„W Konstytucji Państw i Narodów, w Rozdziale o Prawach Człowieka powinno być zapisane:

**Każdy ma niepodważalne prawo wymyślić dowód Wielkiego Twierdzenia Fermata.**

„W Konstytucji Państw i Narodów, w Rozdziale o Prawach Człowieka powinno być zapisane:

**Każdy ma niepodważalne prawo wymyślić dowód Wielkiego Twierdzenia Fermata.**

Jednak to uroczyście przyznane prawo dotyczące Wielkiego Twierdzenia Fermata (zwanego dalej TWIERDZENIEM) podlega następującym ograniczeniom:

„W Konstytucji Państw i Narodów, w Rozdziale o Prawach Człowieka powinno być zapisane:

**Każdy ma niepodważalne prawo wymyślić dowód Wielkiego Twierdzenia Fermata.**

Jednak to uroczyście przyznane prawo dotyczące Wielkiego Twierdzenia Fermata (zwanego dalej TWIERDZENIEM) podlega następującym ograniczeniom:

§1. *Żadna nowa próba udowodnienia TWIERDZENIA nie może być powtórzeniem jednej z poprzednich.*

„W Konstytucji Państw i Narodów, w Rozdziale o Prawach Człowieka powinno być zapisane:

**Każdy ma niepodważalne prawo wymyślić dowód Wielkiego Twierdzenia Fermata.**

Jednak to uroczyście przyznane prawo dotyczące Wielkiego Twierdzenia Fermata (zwanego dalej TWIERDZENIEM) podlega następującym ograniczeniom:

§1. *Żadna nowa próba udowodnienia TWIERDZENIA nie może być powtórzeniem jednej z poprzednich.*

§2. *Jest przestępstwem przesyłanie fałszywych dowodów TWIERDZENIA profesorom, którzy i tak z trudem zarabiają na życie ucząc, jak nie wymyślać fałszywych dowodów TWIERDZENIA.*

„W Konstytucji Państw i Narodów, w Rozdziale o Prawach Człowieka powinno być zapisane:

**Każdy ma niepodważalne prawo wymyślić dowód Wielkiego Twierdzenia Fermata.**

Jednak to uroczyście przyznane prawo dotyczące Wielkiego Twierdzenia Fermata (zwanego dalej TWIERDZENIEM) podlega następującym ograniczeniom:

§1. *Żadna nowa próba udowodnienia TWIERDZENIA nie może być powtórzeniem jednej z poprzednich.*

§2. *Jest przestępstwem przesyłanie fałszywych dowodów TWIERDZENIA profesorom, którzy i tak z trudem zarabiają na życie ucząc, jak nie wymyślać fałszywych dowodów TWIERDZENIA.*

„W Konstytucji Państw i Narodów, w Rozdziale o Prawach Człowieka powinno być zapisane:

**Każdy ma niepodważalne prawo wymyślić dowód Wielkiego Twierdzenia Fermata.**

Jednak to uroczyście przyznane prawo dotyczące Wielkiego Twierdzenia Fermata (zwanego dalej TWIERDZENIEM) podlega następującym ograniczeniom:

§1. *Żadna nowa próba udowodnienia TWIERDZENIA nie może być powtórzeniem jednej z poprzednich.*

§2. *Jest przestępstwem przesyłanie fałszywych dowodów TWIERDZENIA profesorom, którzy i tak z trudem zarabiają na życie ucząc, jak nie wymyślać fałszywych dowodów TWIERDZENIA.*

Naruszenie ostatniego zakazu prowadzi nieuchronnie do Piekła. Powrót do Raju będzie możliwy tylko wtedy, gdy wspomniany złoczyńca zrozumie dowód Wilesa i będzie w stanie go odtworzyć. (Jest to kara surowa).”

„W Konstytucji Państw i Narodów, w Rozdziale o Prawach Człowieka powinno być zapisane:

**Każdy ma niepodważalne prawo wymyślić dowód Wielkiego Twierdzenia Fermata.**

Jednak to uroczyście przyznane prawo dotyczące Wielkiego Twierdzenia Fermata (zwanego dalej TWIERDZENIEM) podlega następującym ograniczeniom:

§1. *Żadna nowa próba udowodnienia TWIERDZENIA nie może być powtórzeniem jednej z poprzednich.*

§2. *Jest przestępstwem przesyłanie fałszywych dowodów TWIERDZENIA profesorom, którzy i tak z trudem zarabiają na życie ucząc, jak nie wymyślać fałszywych dowodów TWIERDZENIA.*

Naruszenie ostatniego zakazu prowadzi nieuchronnie do Piekła. Powrót do Raju będzie możliwy tylko wtedy, gdy wspomniany złoczyńca zrozumie dowód Wilesa i będzie w stanie go odtworzyć. (Jest to kara surowa)."

P. Ribenboim, *Wielkie twierdzenie Fermata dla laików*, w tłumaczeniu J. Browkina [3, str. 7]

# Uwagi ogólne

Niech $p$ będzie liczbą pierwszą nieparzystą.

Niech $p$ będzie liczbą pierwszą nieparzystą.

1. Rozwiązanie równania $x^n + y^n = z^n$ nazywamy **trywialnym**, gdy $xyz = 0$.

Niech $p$ będzie liczbą pierwszą nieparzystą.

1. Rozwiązanie równania $x^n + y^n = z^n$ nazywamy **trywialnym**, gdy $xyz = 0$.

Niech $p$ będzie liczbą pierwszą nieparzystą.

1. Rozwiązanie równania $x^n + y^n = z^n$ nazywamy **trywialnym**, gdy $xyz = 0$. W przeciwnym przypadku rozwiązanie nazywamy **nietrywialnym**.

Niech $p$ będzie liczbą pierwszą nieparzystą.

1. Rozwiązanie równania $x^n + y^n = z^n$ nazywamy **trywialnym**, gdy $xyz = 0$. W przeciwnym przypadku rozwiązanie nazywamy **nietrywialnym**.
2. TWIERDZENIE wystarczy udowodnić dla $n = 4$ lub $n = p$.

Niech $p$ będzie liczbą pierwszą nieparzystą.

1. Rozwiązanie równania $x^n + y^n = z^n$ nazywamy **trywialnym**, gdy $xyz = 0$. W przeciwnym przypadku rozwiązanie nazywamy **nietrywialnym**.
2. TWIERDZENIE wystarczy udowodnić dla $n = 4$ lub $n = p$.

Niech $p$ będzie liczbą pierwszą nieparzystą.

1. Rozwiązanie równania $x^n + y^n = z^n$ nazywamy **trywialnym**, gdy $xyz = 0$. W przeciwnym przypadku rozwiązanie nazywamy **nietrywialnym**.
2. TWIERDZENIE wystarczy udowodnić dla $n = 4$ lub $n = p$.

   Istotnie, niech $n \in \mathbb{N}$ i $n > 2$. Wówczas $n = k \cdot l$, gdzie $k = 4$ lub $k = p$, $l \in \mathbb{N}$. Jeśli TWIERDZENIE nie zachodzi dla $n$, to istnieją $x, y, z \in \mathbb{Z} \setminus \{0\}$ takie, że $x^n + y^n = z^n$. Wówczas mamy:

   $$\left(x^l\right)^k + \left(y^l\right)^k = \left(z^l\right)^k.$$

   A zatem TWIERDZENIE nie zachodzi dla $k$.

3. Niech $X, Y, Z \in \mathbb{Z} \setminus \{0\}$ oraz $X^n + Y^n = Z^n$.

3. Niech $X, Y, Z \in \mathbb{Z} \setminus \{0\}$ oraz $X^n + Y^n = Z^n$.

3. Niech $X, Y, Z \in \mathbb{Z} \setminus \{0\}$ oraz $X^n + Y^n = Z^n$. Załóżmy, że $(X, Y, Z) = d > 1$. Możemy zapisać:

$$X = xd, \quad Y = yd, \quad Z = zd, \quad \text{gdzie} \quad (x, y, z) = 1.$$

Wówczas mamy:

$$X^n + Y^n = Z^n \iff (xd)^n + (yd)^n = (zd)^n \iff x^n + y^n = z^n.$$

Wystarczy zatem rozpatrywać tylko trójki liczb całkowitych względnie pierwszych.

3. Niech $X, Y, Z \in \mathbb{Z} \setminus \{0\}$ oraz $X^n + Y^n = Z^n$. Załóżmy, że $(X, Y, Z) = d > 1$. Możemy zapisać:

$$X = xd, \quad Y = yd, \quad Z = zd, \quad \text{gdzie} \quad (x, y, z) = 1.$$

Wówczas mamy:

$$X^n + Y^n = Z^n \iff (xd)^n + (yd)^n = (zd)^n \iff x^n + y^n = z^n.$$

Wystarczy zatem rozpatrywać tylko trójki liczb całkowitych względnie pierwszych.

4. Jeśli $2 \nmid n$, to równanie $x^n + y^n = z^n$ ma rozwiązanie nietrywialne wtedy i tylko wtedy, gdy równanie $x^n + y^n + z^n = 0$ ma rozwiązanie nietrywialne.

3. Niech $X, Y, Z \in \mathbb{Z} \setminus \{0\}$ oraz $X^n + Y^n = Z^n$. Załóżmy, że $(X, Y, Z) = d > 1$. Możemy zapisać:

$$X = xd, \quad Y = yd, \quad Z = zd, \quad \text{gdzie} \quad (x, y, z) = 1.$$

Wówczas mamy:

$$X^n + Y^n = Z^n \iff (xd)^n + (yd)^n = (zd)^n \iff x^n + y^n = z^n.$$

Wystarczy zatem rozpatrywać tylko trójki liczb całkowitych względnie pierwszych.

4. Jeśli $2 \nmid n$, to równanie $x^n + y^n = z^n$ ma rozwiązanie nietrywialne wtedy i tylko wtedy, gdy równanie $x^n + y^n + z^n = 0$ ma rozwiązanie nietrywialne.

5. Niech $n = 2^u m$, gdzie $u \in \mathbb{N} \cup \{0\}$ oraz $m \in \mathbb{N}$ i $2 \nmid m$. Mówimy, że zachodzi **I przypadek twierdzenia Fermata** dla wykładnika $n$, gdy zachodzi następująca implikacja:

$$\text{jeśli } x, y, z \in \mathbb{Z} \setminus \{0\} \text{ i } (m, xyz) = 1, \text{ to } x^n + y^n \neq z^n.$$

6. Niech $n = 2^u m$, gdzie $u \in \mathbb{N} \cup \{0\}$ oraz $m \in \mathbb{N}$ i $2 \nmid m$. Mówimy, że zachodzi **II przypadek twierdzenia Fermata** dla wykładnika $n$, gdy zachodzi następująca implikacja:
jeśli $x, y, z \in \mathbb{Z} \setminus \{0\}$ oraz $x, y, z$ są parami względnie pierwsze i $(m, xyz) > 1$, to $x^n + y^n \neq z^n$.

6. Niech $n = 2^u m$, gdzie $u \in \mathbb{N} \cup \{0\}$ oraz $m \in \mathbb{N}$ i $2 \nmid m$. Mówimy, że zachodzi **II przypadek twierdzenia Fermata** dla wykładnika $n$, gdy zachodzi następująca implikacja:
jeśli $x, y, z \in \mathbb{Z} \setminus \{0\}$ oraz $x, y, z$ są parami względnie pierwsze i $(m, xyz) > 1$, to $x^n + y^n \neq z^n$.
7. Jak wiadomo dla $n = 2$, równanie $x^2 + y^2 = z^2$ ma rozwiązania.

6. Niech $n = 2^u m$, gdzie $u \in \mathbb{N} \cup \{0\}$ oraz $m \in \mathbb{N}$ i $2 \nmid m$. Mówimy, że zachodzi **II przypadek twierdzenia Fermata** dla wykładnika $n$, gdy zachodzi następująca implikacja:
jeśli $x, y, z \in \mathbb{Z} \setminus \{0\}$ oraz $x, y, z$ są parami względnie pierwsze i $(m, xyz) > 1$, to $x^n + y^n \neq z^n$.
7. Jak wiadomo dla $n = 2$, równanie $x^2 + y^2 = z^2$ ma rozwiązania.

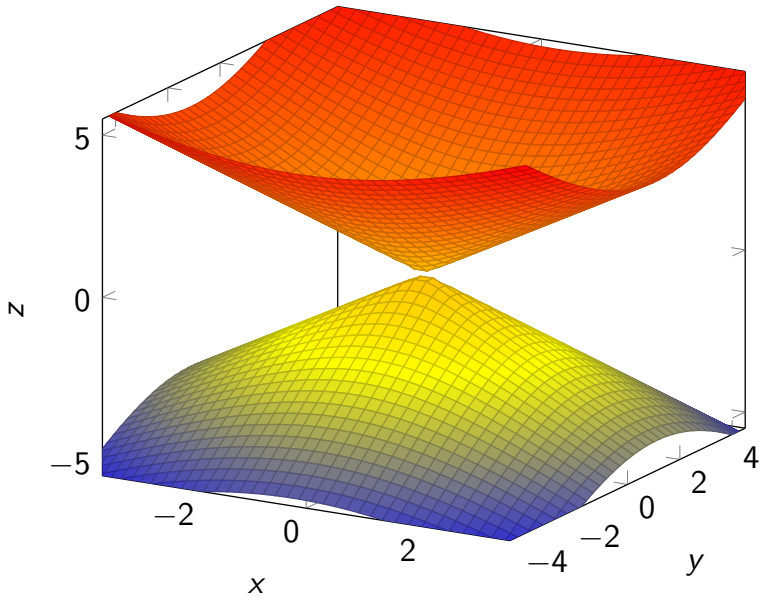
6. Niech $n = 2^u m$, gdzie $u \in \mathbb{N} \cup \{0\}$ oraz $m \in \mathbb{N}$ i $2 \nmid m$. Mówimy, że zachodzi **II przypadek twierdzenia Fermata** dla wykładnika $n$, gdy zachodzi następująca implikacja:
jeśli $x, y, z \in \mathbb{Z} \setminus \{0\}$ oraz $x, y, z$ są parami względnie pierwsze i $(m, xyz) > 1$, to $x^n + y^n \neq z^n$.
7. Jak wiadomo dla $n = 2$, równanie $x^2 + y^2 = z^2$ ma rozwiązania. Rozwiązania pierwotne (trójki liczb $x, y, z$ parami względnie pierwszych i takich, że $x, y, z > 0$) dane są wzorami:

$$\begin{cases} x = m^2 - n^2, \\ y = 2mn, \\ z = m^2 + n^2, \quad (m, n) = 1, m > n > 0 \text{ oraz } m, n \text{ różnej parzystości.} \end{cases}$$

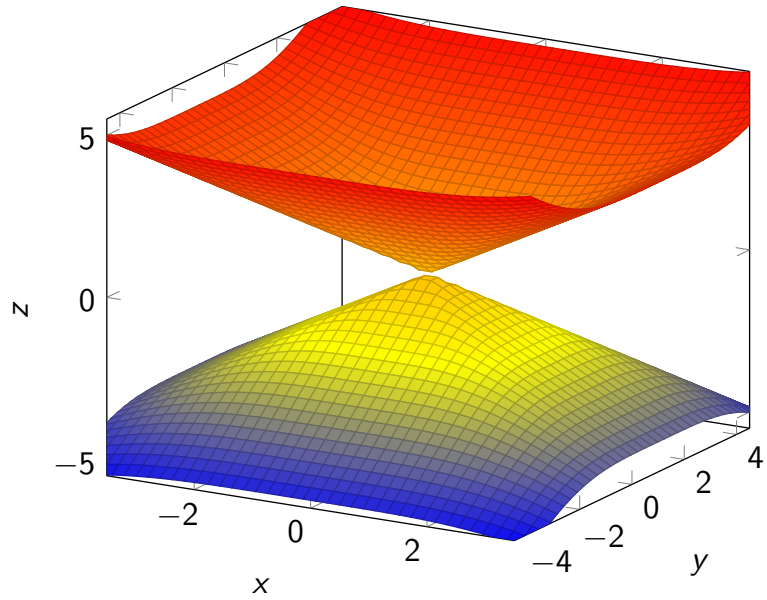
6. Niech $n = 2^u m$, gdzie $u \in \mathbb{N} \cup \{0\}$ oraz $m \in \mathbb{N}$ i $2 \nmid m$. Mówimy, że zachodzi **II przypadek twierdzenia Fermata** dla wykładnika $n$, gdy zachodzi następująca implikacja:
jeśli $x, y, z \in \mathbb{Z} \setminus \{0\}$ oraz $x, y, z$ są parami względnie pierwsze i $(m, xyz) > 1$, to $x^n + y^n \neq z^n$.
7. Jak wiadomo dla $n = 2$, równanie $x^2 + y^2 = z^2$ ma rozwiązania. Rozwiązania pierwotne (trójki liczb $x, y, z$ parami względnie pierwszych i takich, że $x, y, z > 0$) dane są wzorami:

$$\begin{cases} x = m^2 - n^2, \\ y = 2mn, \\ z = m^2 + n^2, \quad (m, n) = 1, m > n > 0 \text{ oraz } m, n \text{ różnej parzystości.} \end{cases}$$

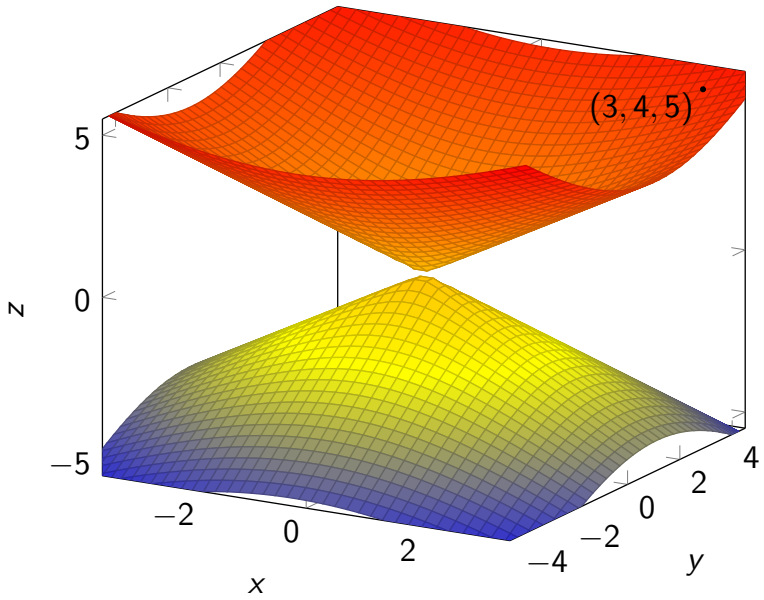
Tę parametryzację dał Leonardo z Pizy (Fibonacci) w 1225 roku.



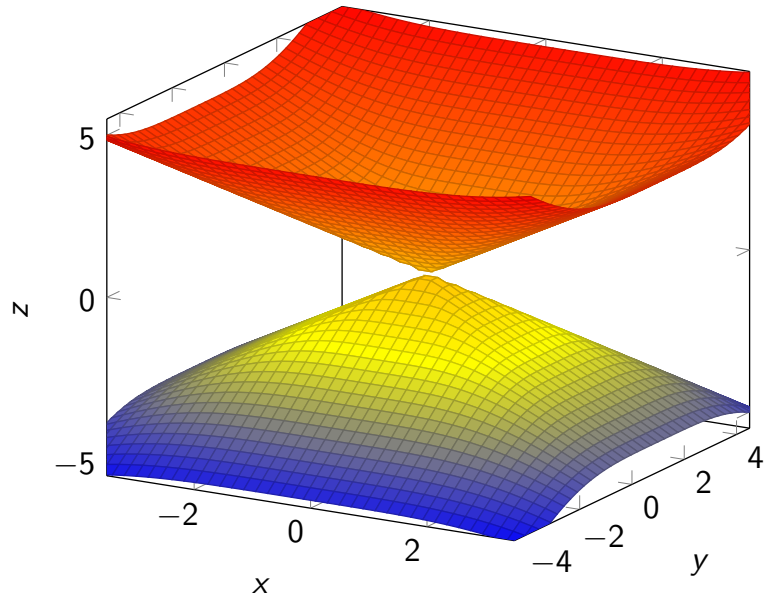

$$z^2 = x^2 + y^2$$




$$z^4 = x^4 + y^4$$




$$z^2 = x^2 + y^2$$




$$z^4 = x^4 + y^4$$

# Szczególne przypadki

Dla $n = 4$ sam Pierre de Fermat podał dowód TWIERDZENIA około 1640 roku.

Dla $n = 4$ sam Pierre de Fermat podał dowód TWIERDZENIA około 1640 roku. Wykorzystał on w nim odkrytą przez siebie **metodę regresji**.

Dla $n = 4$ sam Pierre de Fermat podał dowód TWIERDZENIA około 1640 roku. Wykorzystał on w nim odkrytą przez siebie **metodę regresji**.

## Metoda regresji

Jeśli trójka $x_0, y_0, z_0$ liczb całkowitych dodatnich jest rozwiązaniem naszego równania, to jesteśmy w stanie otrzymać trójkę $x_1, y_1, z_1$ liczb całkowitych dodatnich będących również rozwiązaniem naszego równania o własności $x_1 < x_0$.

Dla $n = 4$ sam Pierre de Fermat podał dowód TWIERDZENIA około 1640 roku. Wykorzystał on w nim odkrytą przez siebie **metodę regresji**.

## Metoda regresji

Jeśli trójka $x_0, y_0, z_0$ liczb całkowitych dodatnich jest rozwiązaniem naszego równania, to jesteśmy w stanie otrzymać trójkę $x_1, y_1, z_1$ liczb całkowitych dodatnich będących również rozwiązaniem naszego równania o własności $x_1 < x_0$.

Powtarzając to postępowanie otrzymalibyśmy nieskończony malejący ciąg $(x_n)_{n=0}^{\infty}$ liczb całkowitych dodatnich:

$$\ldots < x_2 < x_1 < x_0,$$

co jest sprzeczne.

## Twierdzenie 3.1

*Równanie $x^4 + y^4 = z^4$ nie ma całkowitych rozwiązań nietrywialnych.*

## Twierdzenie 3.1

*Równanie $x^4 + y^4 = z^4$ nie ma całkowitych rozwiązań nietrywialnych.*

**Dowód.**

**Twierdzenie 3.1**

*Równanie $x^4 + y^4 = z^4$ nie ma całkowitych rozwiązań nietrywialnych.*

**Dowód.**

Rozpatrzmy równanie diofantyczne:

$$X^4 - Y^4 = Z^2. \tag{3.1}$$

**Twierdzenie 3.1**

*Równanie $x^4 + y^4 = z^4$ nie ma całkowitych rozwiązań nietrywialnych.*

**Dowód.**

Rozpatrzmy równanie diofantyczne:

$$X^4 - Y^4 = Z^2. \tag{3.1}$$

Przypuśćmy, że równanie (3.1) ma rozwiązanie nietrywialne.

**Twierdzenie 3.1**

*Równanie $x^4 + y^4 = z^4$ nie ma całkowitych rozwiązań nietrywialnych.*

**Dowód.**

Rozpatrzmy równanie diofantyczne:

$$X^4 - Y^4 = Z^2. \tag{3.1}$$

Przypuśćmy, że równanie (3.1) ma rozwiązanie nietrywialne.
Niech trójka $X, Y, Z$ będzie rozwiązaniem nietrywialnym o następujących własnościach: $X, Y, Z > 0$ oraz $X$ ma minimalną możliwą wartość.

**Twierdzenie 3.1**

*Równanie $x^4 + y^4 = z^4$ nie ma całkowitych rozwiązań nietrywialnych.*

**Dowód.**

Rozpatrzmy równanie diofantyczne:

$$X^4 - Y^4 = Z^2. \tag{3.1}$$

Przypuśćmy, że równanie (3.1) ma rozwiązanie nietrywialne.
Niech trójka $X, Y, Z$ będzie rozwiązaniem nietrywialnym o następujących własnościach: $X, Y, Z > 0$ oraz $X$ ma minimalną możliwą wartość.
Niech $(X, Y) = d$. Pokażemy, że $d = 1$.

**Twierdzenie 3.1**

*Równanie $x^4 + y^4 = z^4$ nie ma całkowitych rozwiązań nietrywialnych.*

**Dowód.**

Rozpatrzmy równanie diofantyczne:

$$X^4 - Y^4 = Z^2. \tag{3.1}$$

Przypuśćmy, że równanie (3.1) ma rozwiązanie nietrywialne.
Niech trójka $X, Y, Z$ będzie rozwiązaniem nietrywialnym o następujących własnościach: $X, Y, Z > 0$ oraz $X$ ma minimalną możliwą wartość.
Niech $(X, Y) = d$. Pokażemy, że $d = 1$. Przypuśćmy, że istnieje liczba pierwsza $q \mid d$. Wówczas $X = qX'$, $Y = qY'$ i otrzymujemy:

$$q^4((X')^4 - (Y')^4) = Z^2 \implies q^4 \mid Z^2 \implies q^2 \mid Z \implies Z = q^2 Z'.$$

Otrzymujemy:

$(X')^4 - (Y')^4 = (Z')^2$ – sprzeczność z założeniem o minimalności $X$.

Zatem $(X, Y) = 1$.

Otrzymujemy:

$(X')^4 - (Y')^4 = (Z')^2$ – sprzeczność z założeniem o minimalności $X$.

Zatem $(X, Y) = 1$.

Mamy:

$$Z^2 = X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2).$$

Otrzymujemy:

$$(X')^4 - (Y')^4 = (Z')^2 \text{ – sprzeczność z założeniem o minimalności } X.$$

Zatem $(X, Y) = 1$.

Mamy:

$$Z^2 = X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2).$$

Niech teraz $q$ będzie liczbą pierwszą taką, że:

$$q \mid X^2 - Y^2 \quad \text{oraz} \quad q \mid X^2 + Y^2.$$

Otrzymujemy:

$(X')^4 - (Y')^4 = (Z')^2$ – sprzeczność z założeniem o minimalności $X$.

Zatem $(X, Y) = 1$.

Mamy:

$$Z^2 = X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2).$$

Niech teraz $q$ będzie liczbą pierwszą taką, że:

$$q \mid X^2 - Y^2 \quad \text{oraz} \quad q \mid X^2 + Y^2.$$

Wówczas

$$q \mid \underbrace{(X^2 - Y^2) + (X^2 + Y^2)}_{=2X^2} \quad \text{oraz} \quad q \mid \underbrace{(X^2 + Y^2) - (X^2 - Y^2)}_{=2Y^2}.$$

Otrzymujemy:

$(X')^4 - (Y')^4 = (Z')^2$ – sprzeczność z założeniem o minimalności $X$.

Zatem $(X, Y) = 1$.

Mamy:

$$Z^2 = X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2).$$

Niech teraz $q$ będzie liczbą pierwszą taką, że:

$$q \mid X^2 - Y^2 \quad \text{oraz} \quad q \mid X^2 + Y^2.$$

Wówczas

$$q \mid \underbrace{(X^2 - Y^2) + (X^2 + Y^2)}_{=2X^2} \quad \text{oraz} \quad q \mid \underbrace{(X^2 + Y^2) - (X^2 - Y^2)}_{=2Y^2}.$$

Zatem

$$(q \mid 2 \ \vee \ q \mid X^2) \quad \text{oraz} \quad (q \mid 2 \ \vee \ q \mid Y^2)$$

stąd

stąd

$$q \mid 2 \quad \text{lub} \quad \underbrace{(q \mid X^2 \ \wedge \ q \mid Y^2)}_{\text{sprzeczność z } (X,Y)=1}.$$

stąd

$$q \mid 2 \quad \text{lub} \quad \underbrace{(q \mid X^2 \ \wedge \ q \mid Y^2)}_{\text{sprzeczność z } (X,Y)=1}.$$

Zatem $(X^2 - Y^2, X^2 + Y^2) = 1 \ \vee \ 2$.

1. $(X^2 - Y^2, X^2 + Y^2) = 1$.

stąd

$$q \mid 2 \quad \text{lub} \quad \underbrace{(q \mid X^2 \ \wedge \ q \mid Y^2)}_{\text{sprzeczność z } (X,Y)=1}.$$

Zatem $(X^2 - Y^2, X^2 + Y^2) = 1 \ \vee \ 2$.

1. $(X^2 - Y^2, X^2 + Y^2) = 1$.

stąd

$$q \mid 2 \quad \text{lub} \quad \underbrace{(q \mid X^2 \ \wedge \ q \mid Y^2)}_{\text{sprzeczność z } (X,Y)=1}.$$

Zatem $(X^2 - Y^2, X^2 + Y^2) = 1 \ \vee \ 2$.

1. $(X^2 - Y^2, X^2 + Y^2) = 1$.
   Istnieją liczby całkowite dodatnie $m < n$ takie, że $(m, n) = 1$ oraz

$$\begin{cases} X^2 - Y^2 = m^2, \\ X^2 + Y^2 = n^2. \end{cases}$$

stąd

$$q \mid 2 \quad \text{lub} \quad \underbrace{(q \mid X^2 \ \wedge \ q \mid Y^2)}_{\text{sprzeczność z } (X,Y)=1}.$$

Zatem $(X^2 - Y^2, X^2 + Y^2) = 1 \ \vee \ 2$.

1. $(X^2 - Y^2, X^2 + Y^2) = 1$.
   Istnieją liczby całkowite dodatnie $m < n$ takie, że $(m, n) = 1$ oraz

$$\begin{cases} X^2 - Y^2 = m^2, \\ X^2 + Y^2 = n^2. \end{cases}$$

   Zauważmy, że $2X^2 = m^2 + n^2$, zatem $2 \mid m^2 + n^2$. Stąd $m, n$ muszą być tej samej parzystości. Ponieważ $(m, n) = 1$, więc $2 \nmid m$ oraz $2 \nmid n$.

stąd

$$q \mid 2 \quad \text{lub} \quad \underbrace{(q \mid X^2 \ \wedge \ q \mid Y^2)}_{\text{sprzeczność z } (X,Y)=1}.$$

Zatem $(X^2 - Y^2, X^2 + Y^2) = 1 \ \vee \ 2$.

1. $(X^2 - Y^2, X^2 + Y^2) = 1$.
   Istnieją liczby całkowite dodatnie $m < n$ takie, że $(m, n) = 1$ oraz

$$\begin{cases} X^2 - Y^2 = m^2, \\ X^2 + Y^2 = n^2. \end{cases}$$

   Zauważmy, że $2X^2 = m^2 + n^2$, zatem $2 \mid m^2 + n^2$. Stąd $m, n$ muszą być tej samej parzystości. Ponieważ $(m, n) = 1$, więc $2 \nmid m$ oraz $2 \nmid n$. Istnieją zatem liczby całkowite dodatnie $r, s$ takie, że

$$\begin{cases} r = \frac{m+n}{2}, \\ s = \frac{n-m}{2}. \end{cases}$$

Niech $q$ będzie liczbą pierwszą taką, że $q \mid r$ oraz $q \mid s$. Wówczas

Niech $q$ będzie liczbą pierwszą taką, że $q \mid r$ oraz $q \mid s$. Wówczas

$$q \mid \underbrace{r + s}_{=n} \quad \text{oraz} \quad q \mid \underbrace{r - s}_{=m} \text{ – sprzeczność.}$$

Niech $q$ będzie liczbą pierwszą taką, że $q \mid r$ oraz $q \mid s$. Wówczas

$$q \mid \underbrace{r + s}_{=n} \quad \text{oraz} \quad q \mid \underbrace{r - s}_{=m} \text{ – sprzeczność.}$$

Zatem $(r, s) = 1$.
Dalej mamy:

Niech $q$ będzie liczbą pierwszą taką, że $q \mid r$ oraz $q \mid s$. Wówczas

$$q \mid \underbrace{r+s}_{=n} \quad \text{oraz} \quad q \mid \underbrace{r-s}_{=m} \text{ – sprzeczność.}$$

Zatem $(r, s) = 1$.
Dalej mamy:

$$rs = \frac{n^2 - m^2}{4} = \frac{(X^2 + Y^2) - (X^2 - Y^2)}{4} = \frac{Y^2}{2} \implies Y^2 = 2rs.$$

Niech $q$ będzie liczbą pierwszą taką, że $q \mid r$ oraz $q \mid s$. Wówczas

$$q \mid \underbrace{r+s}_{=n} \quad \text{oraz} \quad q \mid \underbrace{r-s}_{=m} \text{ – sprzeczność.}$$

Zatem $(r, s) = 1$.
Dalej mamy:

$$rs = \frac{n^2 - m^2}{4} = \frac{(X^2 + Y^2) - (X^2 - Y^2)}{4} = \frac{Y^2}{2} \implies Y^2 = 2rs.$$

Zatem istnieją liczby całkowite dodatnie $t, u$ takie, że

Niech $q$ będzie liczbą pierwszą taką, że $q \mid r$ oraz $q \mid s$. Wówczas

$$q \mid \underbrace{r+s}_{=n} \quad \text{oraz} \quad q \mid \underbrace{r-s}_{=m} \text{ – sprzeczność.}$$

Zatem $(r, s) = 1$.
Dalej mamy:

$$rs = \frac{n^2 - m^2}{4} = \frac{(X^2 + Y^2) - (X^2 - Y^2)}{4} = \frac{Y^2}{2} \implies Y^2 = 2rs.$$

Zatem istnieją liczby całkowite dodatnie $t, u$ takie, że

$$\begin{cases} r = t^2, \\ s = 2u^2 \end{cases} \qquad \text{lub}$$

Niech $q$ będzie liczbą pierwszą taką, że $q \mid r$ oraz $q \mid s$. Wówczas

$$q \mid \underbrace{r+s}_{=n} \quad \text{oraz} \quad q \mid \underbrace{r-s}_{=m} \text{ – sprzeczność.}$$

Zatem $(r, s) = 1$.
Dalej mamy:

$$rs = \frac{n^2 - m^2}{4} = \frac{(X^2 + Y^2) - (X^2 - Y^2)}{4} = \frac{Y^2}{2} \implies Y^2 = 2rs.$$

Zatem istnieją liczby całkowite dodatnie $t, u$ takie, że

$$\begin{cases} r = t^2, \\ s = 2u^2 \end{cases} \qquad \text{lub} \qquad \begin{cases} r = 2t^2, \\ s = u^2. \end{cases}$$

Niech $q$ będzie liczbą pierwszą taką, że $q \mid r$ oraz $q \mid s$. Wówczas

$$q \mid \underbrace{r+s}_{=n} \quad \text{oraz} \quad q \mid \underbrace{r-s}_{=m} \text{ – sprzeczność.}$$

Zatem $(r, s) = 1$.
Dalej mamy:

$$rs = \frac{n^2 - m^2}{4} = \frac{(X^2 + Y^2) - (X^2 - Y^2)}{4} = \frac{Y^2}{2} \implies Y^2 = 2rs.$$

Zatem istnieją liczby całkowite dodatnie $t, u$ takie, że

$$\begin{cases} r = t^2, \\ s = 2u^2 \end{cases} \qquad \text{lub} \qquad \begin{cases} r = 2t^2, \\ s = u^2. \end{cases}$$

Rozpatrzmy pierwszy z przypadków. Mamy:

Niech $q$ będzie liczbą pierwszą taką, że $q \mid r$ oraz $q \mid s$. Wówczas

$$q \mid \underbrace{r+s}_{=n} \quad \text{oraz} \quad q \mid \underbrace{r-s}_{=m} \text{ – sprzeczność.}$$

Zatem $(r, s) = 1$.
Dalej mamy:

$$rs = \frac{n^2 - m^2}{4} = \frac{(X^2 + Y^2) - (X^2 - Y^2)}{4} = \frac{Y^2}{2} \implies Y^2 = 2rs.$$

Zatem istnieją liczby całkowite dodatnie $t, u$ takie, że

$$\begin{cases} r = t^2, \\ s = 2u^2 \end{cases} \qquad \text{lub} \qquad \begin{cases} r = 2t^2, \\ s = u^2. \end{cases}$$

Rozpatrzmy pierwszy z przypadków. Mamy:

$$2 \mid s, \quad (r, s, X) = 1.$$

Zauważmy, że

Zauważmy, że

$$r^2 + s^2 = \left(\frac{m+n}{2}\right)^2 + \left(\frac{n-m}{2}\right)^2 = \frac{m^2+n^2}{2} = X^2.$$

Zauważmy, że

$$r^2 + s^2 = \left(\frac{m+n}{2}\right)^2 + \left(\frac{n-m}{2}\right)^2 = \frac{m^2+n^2}{2} = X^2.$$

Istnieją więc liczby całkowite dodatnie $M > N > 0$, $(M, N) = 1$ takie, że:

Zauważmy, że

$$r^2 + s^2 = \left(\frac{m+n}{2}\right)^2 + \left(\frac{n-m}{2}\right)^2 = \frac{m^2+n^2}{2} = X^2.$$

Istnieją więc liczby całkowite dodatnie $M > N > 0$, $(M, N) = 1$ takie, że:

$$\begin{cases} s = 2u^2 = 2MN, & \Longrightarrow \ u^2 = MN. \\ r = t^2 = M^2 - N^2, \\ X = M^2 + N^2. \end{cases}$$

Zauważmy, że

$$r^2 + s^2 = \left(\frac{m+n}{2}\right)^2 + \left(\frac{n-m}{2}\right)^2 = \frac{m^2+n^2}{2} = X^2.$$

Istnieją więc liczby całkowite dodatnie $M > N > 0$, $(M, N) = 1$ takie, że:

$$\begin{cases} s = 2u^2 = 2MN, & \Longrightarrow \ u^2 = MN. \\ r = t^2 = M^2 - N^2, & \\ X = M^2 + N^2. & \end{cases}$$

Zatem istnieją liczby całkowite dodatnie $a, b$ takie, że

Zauważmy, że

$$r^2 + s^2 = \left(\frac{m+n}{2}\right)^2 + \left(\frac{n-m}{2}\right)^2 = \frac{m^2+n^2}{2} = X^2.$$

Istnieją więc liczby całkowite dodatnie $M > N > 0$, $(M, N) = 1$ takie, że:

$$\begin{cases} s = 2u^2 = 2MN, & \Longrightarrow \ u^2 = MN. \\ r = t^2 = M^2 - N^2, \\ X = M^2 + N^2. \end{cases}$$

Zatem istnieją liczby całkowite dodatnie $a, b$ takie, że

$$\begin{cases} M = a^2, \\ N = b^2 \end{cases}$$

Zauważmy, że

$$r^2 + s^2 = \left(\frac{m+n}{2}\right)^2 + \left(\frac{n-m}{2}\right)^2 = \frac{m^2+n^2}{2} = X^2.$$

Istnieją więc liczby całkowite dodatnie $M > N > 0$, $(M, N) = 1$ takie, że:

$$\begin{cases} s = 2u^2 = 2MN, & \Longrightarrow \ u^2 = MN. \\ r = t^2 = M^2 - N^2, \\ X = M^2 + N^2. \end{cases}$$

Zatem istnieją liczby całkowite dodatnie $a, b$ takie, że

$$\begin{cases} M = a^2, \\ N = b^2 \end{cases}$$

i $t^2 = M^2 - N^2 = a^4 - b^4$, ale $0 < a < M < X$ – sprzeczność z założeniem o minimalności $X$.

Zauważmy, że

$$r^2 + s^2 = \left(\frac{m+n}{2}\right)^2 + \left(\frac{n-m}{2}\right)^2 = \frac{m^2+n^2}{2} = X^2.$$

Istnieją więc liczby całkowite dodatnie $M > N > 0$, $(M, N) = 1$ takie, że:

$$\begin{cases} s = 2u^2 = 2MN, & \Longrightarrow \ u^2 = MN. \\ r = t^2 = M^2 - N^2, \\ X = M^2 + N^2. \end{cases}$$

Zatem istnieją liczby całkowite dodatnie $a, b$ takie, że

$$\begin{cases} M = a^2, \\ N = b^2 \end{cases}$$

i $t^2 = M^2 - N^2 = a^4 - b^4$, ale $0 < a < M < X$ – sprzeczność z założeniem o minimalności $X$.

2. $(X^2 - Y^2, X^2 + Y^2) = 2$.

2. $(X^2 - Y^2, X^2 + Y^2) = 2$.

2. $(X^2 - Y^2, X^2 + Y^2) = 2$.

$$Z^2 = X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2) \implies 2 \mid Z \wedge 2 \nmid X \wedge 2 \nmid Y.$$

2. $(X^2 - Y^2, X^2 + Y^2) = 2$.

$$Z^2 = X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2) \implies 2 \mid Z \wedge 2 \nmid X \wedge 2 \nmid Y.$$

Mamy, więc

$$Z^2 + \left(Y^2\right)^2 = \left(X^2\right)^2.$$

2. $(X^2 - Y^2, X^2 + Y^2) = 2$.

$$Z^2 = X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2) \implies 2 \mid Z \wedge 2 \nmid X \wedge 2 \nmid Y.$$

Mamy, więc

$$Z^2 + \left(Y^2\right)^2 = \left(X^2\right)^2.$$

Istnieją zatem liczby całkowite dodatnie $m > n > 0$, $(m, n) = 1$ takie, że:

$$\begin{cases} X^2 = m^2 + n^2, \\ Y^2 = m^2 - n^2, \\ Z = 2mn. \end{cases}$$

2. $(X^2 - Y^2, X^2 + Y^2) = 2$.

$$Z^2 = X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2) \implies 2 \mid Z \wedge 2 \nmid X \wedge 2 \nmid Y.$$

Mamy, więc

$$Z^2 + \left(Y^2\right)^2 = \left(X^2\right)^2.$$

Istnieją zatem liczby całkowite dodatnie $m > n > 0$, $(m, n) = 1$ takie, że:

$$\begin{cases} X^2 = m^2 + n^2, \\ Y^2 = m^2 - n^2, \\ Z = 2mn. \end{cases}$$

Otrzymujemy:

$$(XY)^2 = m^4 - n^4,$$

2. $(X^2 - Y^2, X^2 + Y^2) = 2$.

$$Z^2 = X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2) \implies 2 \mid Z \wedge 2 \nmid X \wedge 2 \nmid Y.$$

Mamy, więc

$$Z^2 + \left(Y^2\right)^2 = \left(X^2\right)^2.$$

Istnieją zatem liczby całkowite dodatnie $m > n > 0$, $(m, n) = 1$ takie, że:

$$\begin{cases} X^2 = m^2 + n^2, \\ Y^2 = m^2 - n^2, \\ Z = 2mn. \end{cases}$$

Otrzymujemy:

$$(XY)^2 = m^4 - n^4,$$

gdzie $0 < m < X$ – sprzeczność z minimalnością $X$.

Zatem nie istnieje nietrywialne rozwiązanie równania (3.1).

Zatem nie istnieje nietrywialne rozwiązanie równania (3.1).

Przypuśćmy teraz, że istnieje trójka liczb całkowitych różnych od zera $x, y, z$ takich, że

$$x^4 + y^4 = z^4.$$

Zatem nie istnieje nietrywialne rozwiązanie równania (3.1).

Przypuśćmy teraz, że istnieje trójka liczb całkowitych różnych od zera $x, y, z$ takich, że

$$x^4 + y^4 = z^4.$$

Wówczas $z^4 - y^4 = \left(x^2\right)^2$

Zatem nie istnieje nietrywialne rozwiązanie równania (3.1).

Przypuśćmy teraz, że istnieje trójka liczb całkowitych różnych od zera $x, y, z$ takich, że

$$x^4 + y^4 = z^4.$$

Wówczas $z^4 - y^4 = \left(x^2\right)^2$ – sprzeczność.

Zatem nie istnieje nietrywialne rozwiązanie równania (3.1).

Przypuśćmy teraz, że istnieje trójka liczb całkowitych różnych od zera $x, y, z$ takich, że

$$x^4 + y^4 = z^4.$$

Wówczas $z^4 - y^4 = \left(x^2\right)^2$ – sprzeczność.

□

Rozpatrzmy teraz TWIERDZENIE dla $n = 3$.

Rozpatrzmy teraz TWIERDZENIE dla $n = 3$.

W tym przypadku próby udowodnienia TWIERDZENIA podjął się Euler w latach ok. 1758-1770.

Rozpatrzmy teraz TWIERDZENIE dla $n = 3$.

W tym przypadku próby udowodnienia TWIERDZENIA podjął się Euler w latach ok. 1758-1770. Jednak okazało się, że zostawił pewne niekompletne wyjaśnienia, które to Pepin uzupełnił w 1875r.

Rozpatrzmy teraz TWIERDZENIE dla $n = 3$.

W tym przypadku próby udowodnienia TWIERDZENIA podjął się Euler w latach ok. 1758-1770. Jednak okazało się, że zostawił pewne niekompletne wyjaśnienia, które to Pepin uzupełnił w 1875r.

W tym momencie TWIERDZENIE może być przeformułowane następująco:

Rozpatrzmy teraz TWIERDZENIE dla $n = 3$.

W tym przypadku próby udowodnienia TWIERDZENIA podjął się Euler w latach ok. 1758-1770. Jednak okazało się, że zostawił pewne niekompletne wyjaśnienia, które to Pepin uzupełnił w 1875r.

W tym momencie TWIERDZENIE może być przeformułowane następująco:

**Wielkie Twierdzenie Fermata**

Niech $p > 3$ będzie liczbą pierwszą. Niech $x, y, z \in \mathbb{Z}$.

Rozpatrzmy teraz TWIERDZENIE dla $n = 3$.

W tym przypadku próby udowodnienia TWIERDZENIA podjął się Euler w latach ok. 1758-1770. Jednak okazało się, że zostawił pewne niekompletne wyjaśnienia, które to Pepin uzupełnił w 1875r.

W tym momencie TWIERDZENIE może być przeformułowane następująco:

**Wielkie Twierdzenie Fermata**

Niech $p > 3$ będzie liczbą pierwszą. Niech $x, y, z \in \mathbb{Z}$. Wówczas:

$$x^p + y^p = z^p \implies xyz = 0.$$

## Definicja 3.2

**Liczby Bernoulliego** $B_0, B_1, B_2, \ldots$ definiujemy rekurencyjnie wg następującego wzoru:

$$\sum_{k=0}^{n} \binom{n+1}{k} B_k = 0, \text{ dla } n \geqslant 1, \text{ gdzie } B_0 = 1.$$

## Definicja 3.2

**Liczby Bernoulliego** $B_0, B_1, B_2, \ldots$ definiujemy rekurencyjnie wg następującego wzoru:

$$\sum_{k=0}^{n} \binom{n+1}{k} B_k = 0, \text{ dla } n \geqslant 1, \text{ gdzie } B_0 = 1.$$

Zatem

## Definicja 3.2

**Liczby Bernoulliego** $B_0, B_1, B_2, \ldots$ definiujemy rekurencyjnie wg następującego wzoru:

$$\sum_{k=0}^{n} \binom{n+1}{k} B_k = 0, \text{ dla } n \geqslant 1, \text{ gdzie } B_0 = 1.$$

Zatem

$$n = 1 : 2B_1 + 1 = 0 \implies B_1 = -\frac{1}{2}$$
$$n = 2 : 3B_2 - \frac{3}{2} + 1 = 0 \implies B_2 = \frac{1}{6}$$
$$n = 3 : 4B_3 + 1 - 2 + 1 = 0 \implies B_3 = 0, \text{ itd.}$$

## Liczby Bernoulliego o nieparzystych indeksach

Można pokazać, że $B_{2k+1} = 0$, dla $k \in \mathbb{N}$.

## Definicja 3.3

Nieparzystą liczbę pierwszą $p$ nazywamy **regularną**, gdy $p$ nie dzieli licznika żadnej z liczb Bernoulliego $B_2, B_4, \ldots, B_{p-5}, B_{p-3}$.

**Definicja 3.3**

Nieparzystą liczbę pierwszą $p$ nazywamy **regularną**, gdy $p$ nie dzieli licznika żadnej z liczb Bernoulliego $B_2, B_4, \ldots, B_{p-5}, B_{p-3}$.

**Twierdzenie 3.4 (Kummer 1847r.)**

*Jeśli $p > 2$ jest liczbą pierwszą regularną, to zachodzi I przypadek twierdzenia Fermata dla wykładnika $p$.*

## O REGULARNOŚCI

## O regularności

Do dziś nie wiadomo, czy liczb pierwszych regularnych jest nieskończenie wiele.

## O regularności

Do dziś nie wiadomo, czy liczb pierwszych regularnych jest nieskończenie wiele.

Najmniejszą liczbą pierwszą nieregularną jest 37.

## O regularności

Do dziś nie wiadomo, czy liczb pierwszych regularnych jest nieskończenie wiele.

Najmniejszą liczbą pierwszą nieregularną jest 37.

Liczb pierwszych nieregularnych jest nieskończenie wiele.

## O regularności

Do dziś nie wiadomo, czy liczb pierwszych regularnych jest nieskończenie wiele.

Najmniejszą liczbą pierwszą nieregularną jest 37.

Liczb pierwszych nieregularnych jest nieskończenie wiele.

Korzystając z kryterium Lehmerów i Vandivera, Buhler at al. w 1993 roku pokazali, że twierdzenie to zachodzi dla wykładników pierwszych nieprzekraczających $4 \cdot 10^6$.

# Krzywe eliptyczne

Zajmiemy się tylko modelem afinicznym krzywej eliptycznej nad ciałem $K$.

Zajmiemy się tylko modelem afinicznym krzywej eliptycznej nad ciałem $K$. Załóżmy dla prostoty, że $\operatorname{char} K \neq 2, 3$.

Zajmiemy się tylko modelem afinicznym krzywej eliptycznej nad ciałem $K$. Załóżmy dla prostoty, że $\operatorname{char} K \neq 2, 3$.

## Definicja 4.1

**Krzywą eliptyczną** $E$ nad ciałem $K$ będziemy nazywać zbiór punktów spełniających poniższe równanie, zwane **równaniem Weierstrassa**:

Zajmiemy się tylko modelem afinicznym krzywej eliptycznej nad ciałem $K$. Załóżmy dla prostoty, że $\operatorname{char} K \neq 2, 3$.

## Definicja 4.1

**Krzywą eliptyczną** $E$ nad ciałem $K$ będziemy nazywać zbiór punktów spełniających poniższe równanie, zwane **równaniem Weierstrassa**:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

Zajmiemy się tylko modelem afinicznym krzywej eliptycznej nad ciałem $K$. Załóżmy dla prostoty, że char $K \neq 2, 3$.

## Definicja 4.1

**Krzywą eliptyczną** $E$ nad ciałem $K$ będziemy nazywać zbiór punktów spełniających poniższe równanie, zwane **równaniem Weierstrassa**:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdzie $a_1, \ldots, a_6 \in K$ oraz jej wyróżnik $\Delta \neq 0$ (który za moment zdefiniujemy) "wraz z punktem w nieskończoności $\infty$" .

Zajmiemy się tylko modelem afinicznym krzywej eliptycznej nad ciałem $K$. Załóżmy dla prostoty, że $\operatorname{char} K \neq 2, 3$.

**Definicja 4.1**

**Krzywą eliptyczną** $E$ nad ciałem $K$ będziemy nazywać zbiór punktów spełniających poniższe równanie, zwane **równaniem Weierstrassa**:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdzie $a_1, \ldots, a_6 \in K$ oraz jej wyróżnik $\Delta \neq 0$ (który za moment zdefiniujemy) "wraz z punktem w nieskończoności $\infty$" .

Możemy uprościć powyższe równanie.

Podstawiamy za $y = \frac{1}{2}(y - a_1x - a_3)$ i otrzymujemy równanie:

Podstawiamy za $y = \frac{1}{2}(y - a_1x - a_3)$ i otrzymujemy równanie:

$$E: \ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

gdzie:

Podstawiamy za $y = \frac{1}{2}(y - a_1x - a_3)$ i otrzymujemy równanie:

$$E: \ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

gdzie:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6. \end{aligned} \tag{4.1}$$

Zdefiniujmy również następujące wielkości:

Zdefiniujmy również następujące wielkości:

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24 b_4, \\ c_6 &= -b_2^3 + 36 b_2 b_4 - 21 b_6, \\ \Delta &= -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6, \\ j &= \frac{c_4^3}{\Delta}. \end{aligned} \tag{4.2}$$

Zdefiniujmy również następujące wielkości:

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24 b_4, \\ c_6 &= -b_2^3 + 36 b_2 b_4 - 21 b_6, \\ \Delta &= -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6, \\ j &= \frac{c_4^3}{\Delta}. \end{aligned} \tag{4.2}$$

Parę $(x, y)$ możemy zastąpić $\left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$, w ten sposób eliminujemy $x^2$ i otrzymujemy prostsze równanie:

Zdefiniujmy również następujące wielkości:

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24 b_4, \\ c_6 &= -b_2^3 + 36 b_2 b_4 - 21 b_6, \\ \Delta &= -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6, \\ j &= \frac{c_4^3}{\Delta}. \end{aligned} \tag{4.2}$$

Parę $(x, y)$ możemy zastąpić $\left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$, w ten sposób eliminujemy $x^2$ i otrzymujemy prostsze równanie:

$$E: \ y^2 = x^3 - 27 c_4 x - 54 c_6. \tag{4.3}$$

Zdefiniujmy również następujące wielkości:

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24 b_4, \\ c_6 &= -b_2^3 + 36 b_2 b_4 - 21 b_6, \\ \Delta &= -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6, \\ j &= \frac{c_4^3}{\Delta}. \end{aligned} \tag{4.2}$$

Parę $(x, y)$ możemy zastąpić $\left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$, w ten sposób eliminujemy $x^2$ i otrzymujemy prostsze równanie:

$$E: \ y^2 = x^3 - 27 c_4 x - 54 c_6. \tag{4.3}$$

**Definicja 4.2**

Wielkość $\Delta$ nazywamy **wyróżnikiem równania Weierstrassa**,

Zdefiniujmy również następujące wielkości:

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24 b_4, \\ c_6 &= -b_2^3 + 36 b_2 b_4 - 21 b_6, \\ \Delta &= -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6, \\ j &= \frac{c_4^3}{\Delta}. \end{aligned} \tag{4.2}$$

Parę $(x, y)$ możemy zastąpić $\left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$, w ten sposób eliminujemy $x^2$ i otrzymujemy prostsze równanie:

$$E: \ y^2 = x^3 - 27 c_4 x - 54 c_6. \tag{4.3}$$

**Definicja 4.2**

Wielkość $\Delta$ nazywamy **wyróżnikiem równania Weierstrassa**, $j$ nazywamy **$j$–niezmiennikiem krzywej eliptycznej** $E$.

Możemy zatem równanie Weierstrassa zapisać w postaci:

Możemy zatem równanie Weierstrassa zapisać w postaci:

$$E: \ y^2 = x^3 + Ax + B, \tag{4.4}$$

wówczas:

Możemy zatem równanie Weierstrassa zapisać w postaci:

$$E: \ y^2 = x^3 + Ax + B, \tag{4.4}$$

wówczas:

$$\Delta = -16\left(4A^3 + 27B^2\right),$$

$$j = -1728\frac{(4A)^3}{\Delta}.$$

Możemy zatem równanie Weierstrassa zapisać w postaci:

$$E: \ y^2 = x^3 + Ax + B, \tag{4.4}$$

wówczas:

$$\Delta = -16\left(4A^3 + 27B^2\right),$$

$$j = -1728\frac{(4A)^3}{\Delta}.$$

Równanie (4.4) nazywamy **krótkim równaniem Weierstrassa**.

Niech $E/K$ będzie krzywą zadaną długim równaniem Weierstrassa.

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

Niech $E/K$ będzie krzywą zadaną długim równaniem Weierstrassa.

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

wówczas stosując liniową zamianę zmiennych:

Niech $E/K$ będzie krzywą zadaną długim równaniem Weierstrassa.

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

wówczas stosując liniową zamianę zmiennych:

$$\begin{cases} X = u^2X' + r, \\ Y = u^3Y' + su^2X' + t, \quad \text{gdzie } u, r, s, t \in K, u \neq 0, \end{cases}$$

uzyskamy:

Niech $E/K$ będzie krzywą zadaną długim równaniem Weierstrassa.

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

wówczas stosując liniową zamianę zmiennych:

$$\begin{cases} X = u^2X' + r, \\ Y = u^3Y' + su^2X' + t, \quad \text{gdzie } u, r, s, t \in K, u \neq 0, \end{cases}$$

uzyskamy:

$$\begin{aligned} u^4c_4' &= c_4, \\ u^6c_6' &= c_6, \\ u^{12}\Delta' &= \Delta, \\ j' &= j. \end{aligned} \tag{4.5}$$

**Twierdzenie 4.3 ([2, Proposition 1.4(b), str. 45])**

*Dwie krzywe eliptyczne $E_1$, $E_2$ zadane nad tym samym ciałem są izomorficzne wtedy i tylko wtedy, gdy $j_{E_1} = j_{E_2}$*

**Twierdzenie 4.3 ([2, Proposition 1.4(b), str. 45])**

*Dwie krzywe eliptyczne $E_1$, $E_2$ zadane nad tym samym ciałem są izomorficzne wtedy i tylko wtedy, gdy $j_{E_1} = j_{E_2}$*

**Twierdzenie 4.4 ([2, Proposition 1.4(a), str. 45])**

*Krzywe dane za pomocą równania* (4.4) *(lub* (4.3)*) możemy podzielić w następujący sposób:*

**Twierdzenie 4.3 ([2, Proposition 1.4(b), str. 45])**

*Dwie krzywe eliptyczne $E_1$, $E_2$ zadane nad tym samym ciałem są izomorficzne wtedy i tylko wtedy, gdy $j_{E_1} = j_{E_2}$*

**Twierdzenie 4.4 ([2, Proposition 1.4(a), str. 45])**

*Krzywe dane za pomocą równania* (4.4) *(lub* (4.3)*) możemy podzielić w następujący sposób:*

1. *Krzywa E jest nieosobliwa wtedy i tylko wtedy, gdy $\Delta \neq 0$ (czyli E jest krzywą eliptyczną),*

**Twierdzenie 4.3** *([2, Proposition 1.4(b), str. 45])*

*Dwie krzywe eliptyczne $E_1$, $E_2$ zadane nad tym samym ciałem są izomorficzne wtedy i tylko wtedy, gdy $j_{E_1} = j_{E_2}$*

**Twierdzenie 4.4** *([2, Proposition 1.4(a), str. 45])*

*Krzywe dane za pomocą równania* (4.4) *(lub* (4.3)*) możemy podzielić w następujący sposób:*

1. *Krzywa $E$ jest nieosobliwa wtedy i tylko wtedy, gdy $\Delta \neq 0$ (czyli $E$ jest krzywą eliptyczną),*
2. *Krzywa $E$ ma tylko jeden punkt osobliwy – **węzeł** wtedy i tylko wtedy, gdy $\Delta = 0$ i $A \neq 0$ (lub $c_4 \neq 0$),*

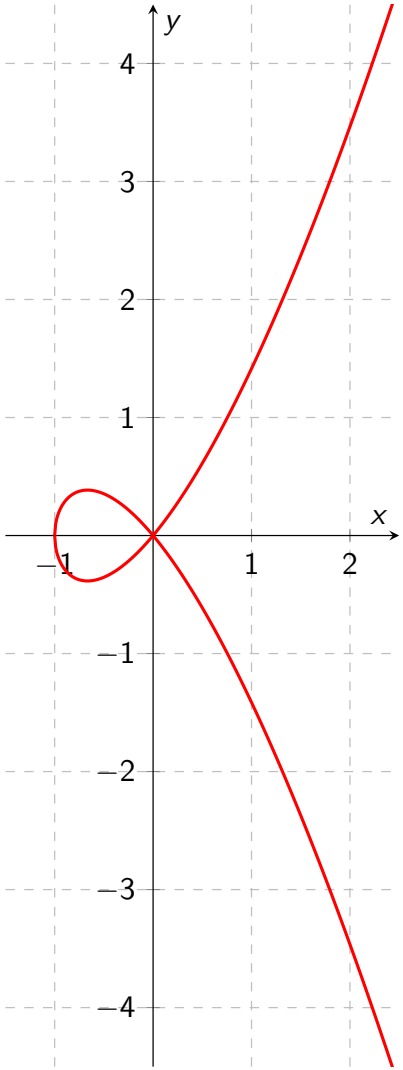
**Twierdzenie 4.3** *([2, Proposition 1.4(b), str. 45])*

*Dwie krzywe eliptyczne $E_1$, $E_2$ zadane nad tym samym ciałem są izomorficzne wtedy i tylko wtedy, gdy $j_{E_1} = j_{E_2}$*

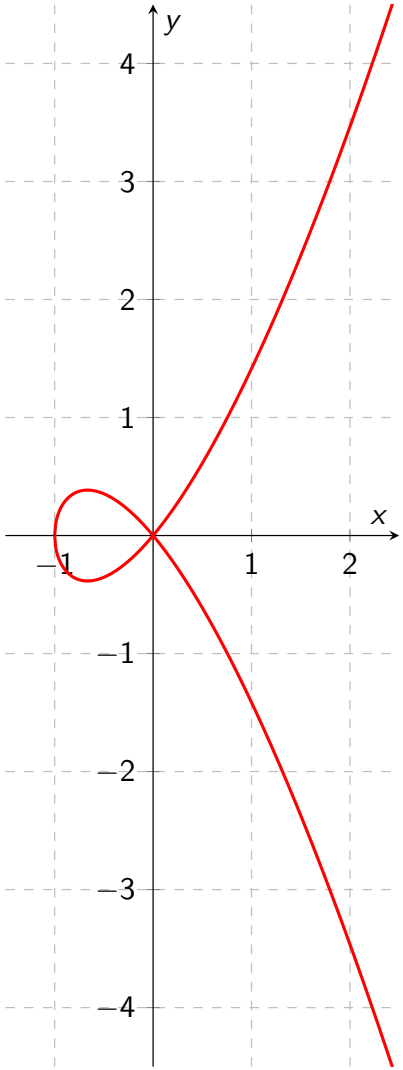
**Twierdzenie 4.4** *([2, Proposition 1.4(a), str. 45])*

*Krzywe dane za pomocą równania* (4.4) *(lub* (4.3)*) możemy podzielić w następujący sposób:*

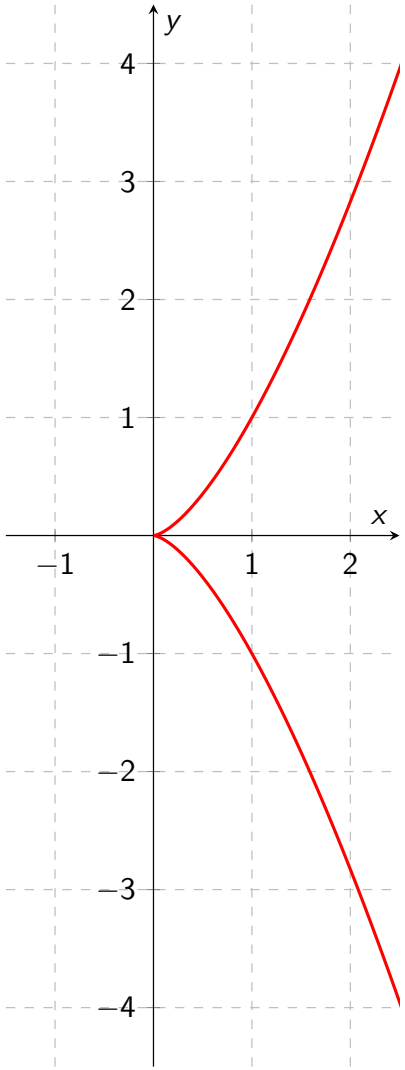
1. *Krzywa $E$ jest nieosobliwa wtedy i tylko wtedy, gdy $\Delta \neq 0$ (czyli $E$ jest krzywą eliptyczną),*
2. *Krzywa $E$ ma tylko jeden punkt osobliwy – **węzeł** wtedy i tylko wtedy, gdy $\Delta = 0$ i $A \neq 0$ (lub $c_4 \neq 0$),*
3. *Krzywa $E$ ma tylko jeden punkt osobliwy – **ostrze** wtedy i tylko wtedy, gdy $\Delta = 0$ i $A = 0$ (lub $c_4 = 0$).*




$y^2 = x^3 + x^2$ – węzeł




$y^2 = x^3 + x^2$ – węzeł




$y^2 = x^3$ – ostrze

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną zadaną równaniem Weierstrassa:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną zadaną równaniem Weierstrassa:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdzie $a_1, \ldots, a_6 \in \mathbb{Q}$.

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną zadaną równaniem Weierstrassa:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdzie $a_1, \ldots, a_6 \in \mathbb{Q}$. Poprzez liniową zamianę zmiennych zastąpimy parę $(x, y)$ przez $\left(u^2x', u^3y'\right)$,

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną zadaną równaniem Weierstrassa:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdzie $a_1, \ldots, a_6 \in \mathbb{Q}$. Poprzez liniową zamianę zmiennych zastąpimy parę $(x, y)$ przez $\left(u^2x', u^3y'\right)$, gdzie $u$ jest tak dobrane, by nowa krzywa $E'$ miała współczynniki $a_i' = \frac{a_i}{u^i}$ całkowite.

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną zadaną równaniem Weierstrassa:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdzie $a_1, \ldots, a_6 \in \mathbb{Q}$. Poprzez liniową zamianę zmiennych zastąpimy parę $(x, y)$ przez $\left(u^2x', u^3y'\right)$, gdzie $u$ jest tak dobrane, by nowa krzywa $E'$ miała współczynniki $a_i' = \frac{a_i}{u^i}$ całkowite.

**Waluacja $\ell$-adyczna**

Niech $\ell$ będzie liczbą pierwszą, oraz $\alpha \in \mathbb{Q}$, $\alpha = \frac{m}{n} \cdot \ell^e$, gdzie $m, n \in \mathbb{Z}$, $n \neq 0$ oraz $\ell \nmid mn$.

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną zadaną równaniem Weierstrassa:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdzie $a_1, \ldots, a_6 \in \mathbb{Q}$. Poprzez liniową zamianę zmiennych zastąpimy parę $(x, y)$ przez $\left(u^2x', u^3y'\right)$, gdzie $u$ jest tak dobrane, by nowa krzywa $E'$ miała współczynniki $a_i' = \frac{a_i}{u^i}$ całkowite.

### Waluacja $\ell$-adyczna

Niech $\ell$ będzie liczbą pierwszą, oraz $\alpha \in \mathbb{Q}$, $\alpha = \frac{m}{n} \cdot \ell^e$, gdzie $m, n \in \mathbb{Z}$, $n \neq 0$ oraz $\ell \nmid mn$. Zdefiniujmy **$\ell$-adyczną waluację** $v_\ell$ na $\mathbb{Q}$:

$$v_\ell(\alpha) = v_\ell\left(\frac{m}{n} \cdot \ell^e\right) = e \in \mathbb{Z}.$$

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną zadaną równaniem Weierstrassa:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

gdzie $a_1, \ldots, a_6 \in \mathbb{Q}$. Poprzez liniową zamianę zmiennych zastąpimy parę $(x, y)$ przez $\left(u^2x', u^3y'\right)$, gdzie $u$ jest tak dobrane, by nowa krzywa $E'$ miała współczynniki $a_i' = \frac{a_i}{u^i}$ całkowite.

### Waluacja $\ell$-adyczna

Niech $\ell$ będzie liczbą pierwszą, oraz $\alpha \in \mathbb{Q}$, $\alpha = \frac{m}{n} \cdot \ell^e$, gdzie $m, n \in \mathbb{Z}, n \neq 0$ oraz $\ell \nmid mn$. Zdefiniujmy **$\ell$-adyczną waluację** $v_\ell$ na $\mathbb{Q}$:

$$v_\ell(\alpha) = v_\ell\left(\frac{m}{n} \cdot \ell^e\right) = e \in \mathbb{Z}.$$

Przyjmijmy, że $v_\ell(0) = +\infty$.

## Definicja 4.5

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną. Równanie Weierstrassa o współczynnikach z $\mathbb{Z}$, którego wyróżnik $\Delta$ ma najmniejszą waluację w $\ell$ nazywamy **minimalnym równaniem dla krzywej $E$ w $\ell$**.

**Definicja 4.5**

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną. Równanie Weierstrassa o współczynnikach z $\mathbb{Z}$, którego wyróżnik $\Delta$ ma najmniejszą waluację w $\ell$ nazywamy **minimalnym równaniem dla krzywej $E$ w $\ell$**.

Teraz podamy proste kryterium sprawdzania, czy dane równanie jest minimalne.

## Fakt 4.6

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną równaniem Weierstrassa o współczynnikach z $\mathbb{Z}$:*

## Fakt 4.6

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną równaniem Weierstrassa o współczynnikach z $\mathbb{Z}$:*

1. *Jeśli $v_\ell(\Delta) < 12$, to równanie krzywej $E$ jest minimalne w $\ell$.*

## Fakt 4.6

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną równaniem Weierstrassa o współczynnikach z $\mathbb{Z}$:*

1. *Jeśli $v_\ell(\Delta) < 12$, to równanie krzywej $E$ jest minimalne w $\ell$.*
2. *Jeśli $v_\ell(c_4) < 4$, to równanie krzywej $E$ jest minimalne w $\ell$.*

## Fakt 4.6

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną równaniem Weierstrassa o współczynnikach z $\mathbb{Z}$:*

1. *Jeśli $v_\ell(\Delta) < 12$, to równanie krzywej $E$ jest minimalne w $\ell$.*
2. *Jeśli $v_\ell(c_4) < 4$, to równanie krzywej $E$ jest minimalne w $\ell$.*
3. *Jeśli $v_\ell(c_6) < 6$, to równanie krzywej $E$ jest minimalne w $\ell$.*

## Fakt 4.6

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną równaniem Weierstrassa o współczynnikach z $\mathbb{Z}$:*

1. *Jeśli $v_\ell(\Delta) < 12$, to równanie krzywej $E$ jest minimalne w $\ell$.*
2. *Jeśli $v_\ell(c_4) < 4$, to równanie krzywej $E$ jest minimalne w $\ell$.*
3. *Jeśli $v_\ell(c_6) < 6$, to równanie krzywej $E$ jest minimalne w $\ell$.*

## Fakt 4.6

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną równaniem Weierstrassa o współczynnikach z $\mathbb{Z}$:*

1. *Jeśli $v_\ell(\Delta) < 12$, to równanie krzywej $E$ jest minimalne w $\ell$.*
2. *Jeśli $v_\ell(c_4) < 4$, to równanie krzywej $E$ jest minimalne w $\ell$.*
3. *Jeśli $v_\ell(c_6) < 6$, to równanie krzywej $E$ jest minimalne w $\ell$.*

## Proof.

Wynika ze wzorów (4.5). □

## Fakt 4.6

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną równaniem Weierstrassa o współczynnikach z $\mathbb{Z}$:*

1. *Jeśli $v_\ell(\Delta) < 12$, to równanie krzywej $E$ jest minimalne w $\ell$.*
2. *Jeśli $v_\ell(c_4) < 4$, to równanie krzywej $E$ jest minimalne w $\ell$.*
3. *Jeśli $v_\ell(c_6) < 6$, to równanie krzywej $E$ jest minimalne w $\ell$.*

## Proof.

Wynika ze wzorów (4.5). □

## Definicja 4.7

Równanie Weierstrassa krzywej $E/\mathbb{Q}$ o współczynnikach z $\mathbb{Z}$, której wyróżnik $\Delta$ ma najmniejszą waluację w każdej liczbie pierwszej, nazywamy **globalnym równaniem minimalnym dla krzywej** $E$.

Niech krzywa $E/\mathbb{Q}$ będzie zadana przez globalne równanie minimalne:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.6}$$

Niech krzywa $E/\mathbb{Q}$ będzie zadana przez globalne równanie minimalne:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.6}$$

Mamy naturalne przekształcenie redukcji modulo $\ell$, $r_\ell : \mathbb{Z} \to \mathbb{F}_\ell = \mathbb{Z}/\ell$, przyporządkowujące $x \mapsto \tilde{x}$.

Niech krzywa $E/\mathbb{Q}$ będzie zadana przez globalne równanie minimalne:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.6}$$

Mamy naturalne przekształcenie redukcji modulo $\ell$, $r_\ell : \mathbb{Z} \to \mathbb{F}_\ell = \mathbb{Z}/\ell$, przyporządkowujące $x \mapsto \tilde{x}$. Możemy zatem współczynniki równania (4.6) zredukować modulo $\ell$ i otrzymamy krzywą o równaniu:

Niech krzywa $E/\mathbb{Q}$ będzie zadana przez globalne równanie minimalne:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.6}$$

Mamy naturalne przekształcenie redukcji modulo $\ell$, $r_\ell : \mathbb{Z} \to \mathbb{F}_\ell = \mathbb{Z}/\ell$, przyporządkowujące $x \mapsto \tilde{x}$. Możemy zatem współczynniki równania (4.6) zredukować modulo $\ell$ i otrzymamy krzywą o równaniu:

$$\tilde{E}: \ y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

Niech krzywa $E/\mathbb{Q}$ będzie zadana przez globalne równanie minimalne:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.6}$$

Mamy naturalne przekształcenie redukcji modulo $\ell$, $r_\ell : \mathbb{Z} \to \mathbb{F}_\ell = \mathbb{Z}/\ell$, przyporządkowujące $x \mapsto \tilde{x}$. Możemy zatem współczynniki równania (4.6) zredukować modulo $\ell$ i otrzymamy krzywą o równaniu:

$$\tilde{E}: \ y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

Krzywa $\tilde{E}/\mathbb{F}_\ell$ nazywana jest **redukcją krzywej $E$ w $\ell$**.

## Definicja 4.8

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną i niech $\tilde{E}$ będzie redukcją krzywej $E$ modulo $\ell$ (dla minimalnego równania krzywej $E$).

## Definicja 4.8

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną i niech $\tilde{E}$ będzie redukcją krzywej $E$ modulo $\ell$ (dla minimalnego równania krzywej $E$). Wówczas mówimy, że $E$ ma:

## Definicja 4.8

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną i niech $\tilde{E}$ będzie redukcją krzywej $E$ modulo $\ell$ (dla minimalnego równania krzywej $E$). Wówczas mówimy, że $E$ ma:

1. **Dobrą (stabilną) redukcję w** $\ell$, gdy $\tilde{E}$ jest nieosobliwa.

## Definicja 4.8

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną i niech $\tilde{E}$ będzie redukcją krzywej $E$ modulo $\ell$ (dla minimalnego równania krzywej $E$). Wówczas mówimy, że $E$ ma:

1. **Dobrą (stabilną) redukcję w** $\ell$, gdy $\tilde{E}$ jest nieosobliwa.

## Definicja 4.8

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną i niech $\tilde{E}$ będzie redukcją krzywej $E$ modulo $\ell$ (dla minimalnego równania krzywej $E$). Wówczas mówimy, że $E$ ma:

1. **Dobrą (stabilną) redukcję w** $\ell$, gdy $\tilde{E}$ jest nieosobliwa.
2. **Złą redukcję w** $\ell$, gdy $\tilde{E}$ jest osobliwa.

## Definicja 4.8

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną i niech $\tilde{E}$ będzie redukcją krzywej $E$ modulo $\ell$ (dla minimalnego równania krzywej $E$). Wówczas mówimy, że $E$ ma:

1. **Dobrą (stabilną) redukcję w** $\ell$, gdy $\tilde{E}$ jest nieosobliwa.
2. **Złą redukcję w** $\ell$, gdy $\tilde{E}$ jest osobliwa.

## Definicja 4.8

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną i niech $\tilde{E}$ będzie redukcją krzywej $E$ modulo $\ell$ (dla minimalnego równania krzywej $E$). Wówczas mówimy, że $E$ ma:

1. **Dobrą (stabilną) redukcję w** $\ell$, gdy $\tilde{E}$ jest nieosobliwa.
2. **Złą redukcję w** $\ell$, gdy $\tilde{E}$ jest osobliwa. Rozróżniamy dwa rodzaje złej redukcji:

## Definicja 4.8

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną i niech $\tilde{E}$ będzie redukcją krzywej $E$ modulo $\ell$ (dla minimalnego równania krzywej $E$). Wówczas mówimy, że $E$ ma:

1. **Dobrą (stabilną) redukcję w** $\ell$, gdy $\tilde{E}$ jest nieosobliwa.
2. **Złą redukcję w** $\ell$, gdy $\tilde{E}$ jest osobliwa. Rozróżniamy dwa rodzaje złej redukcji:
   - **złą addytywną redukcję (niestabilną) w** $\ell$, gdy $\tilde{E}$ ma ostrze,

## Definicja 4.8

Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną i niech $\tilde{E}$ będzie redukcją krzywej $E$ modulo $\ell$ (dla minimalnego równania krzywej $E$). Wówczas mówimy, że $E$ ma:

1. **Dobrą (stabilną) redukcję w** $\ell$, gdy $\tilde{E}$ jest nieosobliwa.
2. **Złą redukcję w** $\ell$, gdy $\tilde{E}$ jest osobliwa. Rozróżniamy dwa rodzaje złej redukcji:
   - **złą addytywną redukcję (niestabilną) w** $\ell$, gdy $\tilde{E}$ ma ostrze,
   - **złą multiplikatywną (semistabilną) redukcję w** $\ell$, gdy $\tilde{E}$ ma węzeł.

## Twierdzenie 4.9 ([2, Proposition 5.1, str. 180])

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną minimalnym równaniem Weierstrassa w $\ell$:*

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

## Twierdzenie 4.9 (*[2, Proposition 5.1, str. 180]*)

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną minimalnym równaniem Weierstrassa w $\ell$:*

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*Niech $\Delta$ będzie wyróżnikiem równania oraz $c_4$ obliczone zgodnie z formułą* (4.2).

## Twierdzenie 4.9 (*[2, Proposition 5.1, str. 180]*)

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną minimalnym równaniem Weierstrassa w $\ell$:*

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*Niech $\Delta$ będzie wyróżnikiem równania oraz $c_4$ obliczone zgodnie z formułą (4.2). Wówczas $E$ ma:*

## Twierdzenie 4.9 ([2, Proposition 5.1, str. 180])

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną minimalnym równaniem Weierstrassa w $\ell$:*

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*Niech $\Delta$ będzie wyróżnikiem równania oraz $c_4$ obliczone zgodnie z formułą (4.2). Wówczas $E$ ma:*

1. *Dobrą redukcję w $\ell$ wtedy i tylko wtedy, gdy $v_\ell(\Delta) = 0$.*

## Twierdzenie 4.9 ([2, Proposition 5.1, str. 180])

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną minimalnym równaniem Weierstrassa w $\ell$:*

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*Niech $\Delta$ będzie wyróżnikiem równania oraz $c_4$ obliczone zgodnie z formułą (4.2). Wówczas $E$ ma:*

1. *Dobrą redukcję w $\ell$ wtedy i tylko wtedy, gdy $v_\ell(\Delta) = 0$.*
2. *Multiplikatywną redukcję w $\ell$ wtedy i tylko wtedy, gdy $v_\ell(\Delta) > 0$ i $v_\ell(c_4) = 0$.*

**Twierdzenie 4.9** *([2, Proposition 5.1, str. 180])*

*Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną daną minimalnym równaniem Weierstrassa w $\ell$:*

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*Niech $\Delta$ będzie wyróżnikiem równania oraz $c_4$ obliczone zgodnie z formułą (4.2). Wówczas $E$ ma:*

1. *Dobrą redukcję w $\ell$ wtedy i tylko wtedy, gdy $v_\ell(\Delta) = 0$.*
2. *Multiplikatywną redukcję w $\ell$ wtedy i tylko wtedy, gdy $v_\ell(\Delta) > 0$ i $v_\ell(c_4) = 0$.*
3. *Addytywną redukcję w $\ell$ wtedy i tylko wtedy, gdy $v_\ell(\Delta) > 0$ oraz $v_\ell(c_4) > 0$.*

**Definicja 4.10**

Krzywą $E$ nad ciałem $\mathbb{Q}$ nazywamy **semistabilną**, gdy dla każdego $\ell$, krzywa ta ma dobrą lub multiplikatywną redukcję.

## Definicja 4.10

Krzywą $E$ nad ciałem $\mathbb{Q}$ nazywamy **semistabilną**, gdy dla każdego $\ell$, krzywa ta ma dobrą lub multiplikatywną redukcję.

## Definicja 4.11

**Przewodnikiem krzywej** $E/\mathbb{Q}$ nazywamy wielkość:

$$N = \prod_{\ell} \ell^{f_\ell},$$

gdzie $\ell$ jest liczbą pierwszą,

## Definicja 4.10

Krzywą $E$ nad ciałem $\mathbb{Q}$ nazywamy **semistabilną**, gdy dla każdego $\ell$, krzywa ta ma dobrą lub multiplikatywną redukcję.

## Definicja 4.11

**Przewodnikiem krzywej** $E/\mathbb{Q}$ nazywamy wielkość:

$$N = \prod_{\ell} \ell^{f_\ell},$$

gdzie $\ell$ jest liczbą pierwszą,

$$f_\ell = \begin{cases} 0, & \text{gdy } E \text{ ma dobrą redukcję modulo } \ell, \\ 1, & \text{gdy } E \text{ ma multiplikatywną redukcję modulo } \ell, \\ \geqslant 2, & \text{gdy } E \text{ ma addytywną redukcję modulo } \ell. \end{cases}$$

Gerhard Frey w 1985 roku, jako pierwszy zasugerował, że istnienie nietrywialnych rozwiązań problemu Fermata może przeczyć **hipotezie Shimury, Taniyamy i Weila (o modularności)**.

Gerhard Frey w 1985 roku, jako pierwszy zasugerował, że istnienie nietrywialnych rozwiązań problemu Fermata może przeczyć **hipotezie Shimury, Taniyamy i Weila (o modularności)**.

Frey rozważał krzywą eliptyczną daną wzorem:

$$E : y^2 = x(x - A)(x + B),$$

gdzie $A + B = C$ oraz $A = a^p$, $B = b^p$, $C = c^p$, gdzie $p \geqslant 5$ jest liczbą pierwszą.

Rozpatrzmy równanie:

$$a^p + b^p = c^p, \text{ gdzie } p \text{ jest liczbą pierwszą, } p \geqslant 5. \tag{4.7}$$

Rozpatrzmy równanie:

$$a^p + b^p = c^p, \text{ gdzie } p \text{ jest liczbą pierwszą, } p \geqslant 5. \tag{4.7}$$

Gdyby $(a, b, c) = d \neq 1$, to równanie (4.7) można by podzielić stronami przez $d^p$ i uzyskalibyśmy równanie $(a')^p + (b')^p = (c')^p$, gdzie $(a', b', c') = 1$.

Rozpatrzmy równanie:

$$a^p + b^p = c^p, \text{ gdzie } p \text{ jest liczbą pierwszą, } p \geqslant 5. \tag{4.7}$$

Gdyby $(a, b, c) = d \neq 1$, to równanie (4.7) można by podzielić stronami przez $d^p$ i uzyskalibyśmy równanie $(a')^p + (b')^p = (c')^p$, gdzie $(a', b', c') = 1$. Załóżmy zatem, że $(a, b, c) = 1$.

Rozpatrzmy równanie:

$$a^p + b^p = c^p, \text{ gdzie } p \text{ jest liczbą pierwszą, } p \geqslant 5. \tag{4.7}$$

Gdyby $(a, b, c) = d \neq 1$, to równanie (4.7) można by podzielić stronami przez $d^p$ i uzyskalibyśmy równanie $(a')^p + (b')^p = (c')^p$, gdzie $(a', b', c') = 1$. Załóżmy zatem, że $(a, b, c) = 1$.

Przypuśćmy teraz, że $a, b, c$ nie są parami względnie pierwsze. Niech na przykład $(a, b) = d \neq 1$. Rozważmy redukcję modulo $d$ równania (4.7). Mamy:

$$a^p + b^p \equiv 0 \,(\mathrm{mod}\, d)\,,$$
$$c^p \equiv 0 \,(\mathrm{mod}\, d)\,, \text{ sprzeczność, bo } (a, b, c) = 1.$$

Rozpatrzmy równanie:

$$a^p + b^p = c^p, \text{ gdzie } p \text{ jest liczbą pierwszą, } p \geqslant 5. \tag{4.7}$$

Gdyby $(a, b, c) = d \neq 1$, to równanie (4.7) można by podzielić stronami przez $d^p$ i uzyskalibyśmy równanie $(a')^p + (b')^p = (c')^p$, gdzie $(a', b', c') = 1$. Załóżmy zatem, że $(a, b, c) = 1$.

Przypuśćmy teraz, że $a, b, c$ nie są parami względnie pierwsze. Niech na przykład $(a, b) = d \neq 1$. Rozważmy redukcję modulo $d$ równania (4.7). Mamy:

$$\begin{aligned} a^p + b^p &\equiv 0 \,(\mathrm{mod}\, d)\,, \\ c^p &\equiv 0 \,(\mathrm{mod}\, d)\,, \text{ sprzeczność, bo } (a, b, c) = 1. \end{aligned}$$

Zatem, możemy założyć, że $a, b, c$ są parami względnie pierwsze.

Rozpatrzmy równanie:

$$a^p + b^p = c^p, \text{ gdzie } p \text{ jest liczbą pierwszą, } p \geqslant 5. \tag{4.7}$$

Gdyby $(a, b, c) = d \neq 1$, to równanie (4.7) można by podzielić stronami przez $d^p$ i uzyskalibyśmy równanie $(a')^p + (b')^p = (c')^p$, gdzie $(a', b', c') = 1$. Załóżmy zatem, że $(a, b, c) = 1$.

Przypuśćmy teraz, że $a, b, c$ nie są parami względnie pierwsze. Niech na przykład $(a, b) = d \neq 1$. Rozważmy redukcję modulo $d$ równania (4.7). Mamy:

$$a^p + b^p \equiv 0 \,(\mathrm{mod}\, d)\,,$$
$$c^p \equiv 0 \,(\mathrm{mod}\, d)\,, \text{ sprzeczność, bo } (a, b, c) = 1.$$

Zatem, możemy założyć, że $a, b, c$ są parami względnie pierwsze.

Rozpatrzmy teraz redukcję modulo 2 równania (4.7).

Rozpatrzmy równanie:

$$a^p + b^p = c^p, \text{ gdzie } p \text{ jest liczbą pierwszą, } p \geqslant 5. \tag{4.7}$$

Gdyby $(a, b, c) = d \neq 1$, to równanie (4.7) można by podzielić stronami przez $d^p$ i uzyskalibyśmy równanie $(a')^p + (b')^p = (c')^p$, gdzie $(a', b', c') = 1$. Załóżmy zatem, że $(a, b, c) = 1$.

Przypuśćmy teraz, że $a, b, c$ nie są parami względnie pierwsze. Niech na przykład $(a, b) = d \neq 1$. Rozważmy redukcję modulo $d$ równania (4.7). Mamy:

$$\begin{aligned} a^p + b^p &\equiv 0 \,(\mathrm{mod}\, d)\,, \\ c^p &\equiv 0 \,(\mathrm{mod}\, d)\,, \text{ sprzeczność, bo } (a, b, c) = 1. \end{aligned}$$

Zatem, możemy założyć, że $a, b, c$ są parami względnie pierwsze.

Rozpatrzmy teraz redukcję modulo 2 równania (4.7).

Gdyby $2 \nmid abc$, to mielibyśmy $0 \equiv 1 \,(\mathrm{mod}\, 2)$, więc byłaby sprzeczność.

Rozpatrzmy równanie:

$$a^p + b^p = c^p, \text{ gdzie } p \text{ jest liczbą pierwszą, } p \geqslant 5. \tag{4.7}$$

Gdyby $(a, b, c) = d \neq 1$, to równanie (4.7) można by podzielić stronami przez $d^p$ i uzyskalibyśmy równanie $(a')^p + (b')^p = (c')^p$, gdzie $(a', b', c') = 1$. Załóżmy zatem, że $(a, b, c) = 1$.

Przypuśćmy teraz, że $a, b, c$ nie są parami względnie pierwsze. Niech na przykład $(a, b) = d \neq 1$. Rozważmy redukcję modulo $d$ równania (4.7). Mamy:

$$\begin{aligned} a^p + b^p &\equiv 0 \,(\mathrm{mod}\, d)\,, \\ c^p &\equiv 0 \,(\mathrm{mod}\, d)\,, \text{ sprzeczność, bo } (a, b, c) = 1. \end{aligned}$$

Zatem, możemy założyć, że $a, b, c$ są parami względnie pierwsze.

Rozpatrzmy teraz redukcję modulo 2 równania (4.7).

Gdyby $2 \nmid abc$, to mielibyśmy $0 \equiv 1 \,(\mathrm{mod}\, 2)$, więc byłaby sprzeczność.

Załóżmy zatem bez straty ogólności, że $2 \mid a$.

Rozpatrzmy teraz redukcję modulo 4 wyjściowego równania.

Rozpatrzmy teraz redukcję modulo 4 wyjściowego równania.

Wiemy, że $a^p \equiv 0 \pmod 4$ oraz, że liczby $a, b, c$ są względnie pierwsze, mamy więc

$$b \equiv \pm 1 \pmod 4 \text{ i } c \equiv \pm 1 \pmod 4 .$$

Rozpatrzmy teraz redukcję modulo 4 wyjściowego równania.

Wiemy, że $a^p \equiv 0 \pmod 4$ oraz, że liczby $a, b, c$ są względnie pierwsze, mamy więc

$$b \equiv \pm 1 \pmod 4 \text{ i } c \equiv \pm 1 \pmod 4 .$$

Gdyby $b \equiv 1 \pmod 4$ i $c \equiv -1 \pmod 4$, to otrzymamy

$$1 \equiv -1 \pmod 4 \text{ – sprzeczność.}$$

Rozpatrzmy teraz redukcję modulo 4 wyjściowego równania.

Wiemy, że $a^p \equiv 0 \pmod 4$ oraz, że liczby $a, b, c$ są względnie pierwsze, mamy więc

$$b \equiv \pm 1 \pmod 4 \text{ i } c \equiv \pm 1 \pmod 4 .$$

Gdyby $b \equiv 1 \pmod 4$ i $c \equiv -1 \pmod 4$, to otrzymamy

$$1 \equiv -1 \pmod 4 \text{ – sprzeczność.}$$

Analogicznie na odwrót. Tak więc, $b \equiv c \equiv \pm 1 \pmod 4$.

Rozpatrzmy teraz redukcję modulo 4 wyjściowego równania.

Wiemy, że $a^p \equiv 0 \pmod 4$ oraz, że liczby $a, b, c$ są względnie pierwsze, mamy więc

$$b \equiv \pm 1 \pmod 4 \text{ i } c \equiv \pm 1 \pmod 4 .$$

Gdyby $b \equiv 1 \pmod 4$ i $c \equiv -1 \pmod 4$, to otrzymamy

$$1 \equiv -1 \pmod 4 \text{ – sprzeczność.}$$

Analogicznie na odwrót. Tak więc, $b \equiv c \equiv \pm 1 \pmod 4$.

Gdyby $b \equiv c \equiv -1 \pmod 4$, to podstawiając za parę $(b, c)$, parę $(-c, -b)$, otrzymamy: $b \equiv c \equiv 1 \pmod 4$.

Rozpatrzmy teraz redukcję modulo 4 wyjściowego równania.

Wiemy, że $a^p \equiv 0 \pmod 4$ oraz, że liczby $a, b, c$ są względnie pierwsze, mamy więc

$$b \equiv \pm 1 \pmod 4 \text{ i } c \equiv \pm 1 \pmod 4.$$

Gdyby $b \equiv 1 \pmod 4$ i $c \equiv -1 \pmod 4$, to otrzymamy

$$1 \equiv -1 \pmod 4 \text{ – sprzeczność.}$$

Analogicznie na odwrót. Tak więc, $b \equiv c \equiv \pm 1 \pmod 4$.

Gdyby $b \equiv c \equiv -1 \pmod 4$, to podstawiając za parę $(b, c)$, parę $(-c, -b)$, otrzymamy: $b \equiv c \equiv 1 \pmod 4$.

Z powyższego wynika, że bez straty ogólności możemy założyć, że $a, b, c$ są parami względnie pierwsze, $2 \mid a$ oraz $b \equiv c \equiv 1 \pmod 4$.

Rozważmy krzywą Freya (stowarzyszoną z równaniem (4.7)), tj. krzywą eliptyczną nad $\mathbb{Q}$ o równaniu Weierstrassa:

Rozważmy krzywą Freya (stowarzyszoną z równaniem (4.7)), tj. krzywą eliptyczną nad $\mathbb{Q}$ o równaniu Weierstrassa:

$$E: \ y^2 = x\left(x - a^p\right)\left(x + b^p\right) = x^3 + \left(b^p - a^p\right)x^2 - a^p b^p x.$$

Rozważmy krzywą Freya (stowarzyszoną z równaniem (4.7)), tj. krzywą eliptyczną nad $\mathbb{Q}$ o równaniu Weierstrassa:

$$E: \ y^2 = x\left(x - a^p\right)\left(x + b^p\right) = x^3 + \left(b^p - a^p\right)x^2 - a^p b^p x.$$

Mamy:

$$\begin{aligned} a_1 &= a_3 = a_6 = 0, \\ a_2 &= b^p - a^p, \\ a_4 &= -a^p b^p. \end{aligned}$$

Jako, że $\operatorname{char}\mathbb{Q} = 0$, możemy użyć wzorów (4.1) oraz (4.2) i obliczyć $\Delta$ oraz $c_4$.

Jako, że $\operatorname{char}\mathbb{Q} = 0$, możemy użyć wzorów (4.1) oraz (4.2) i obliczyć $\Delta$ oraz $c_4$.

$$
\begin{aligned}
b_2 &= 4\left(b^p - a^p\right), \\
b_4 &= -2a^p b^p, \\
b_6 &= 0, \\
b_8 &= -a^{2p} b^{2p}, \\
\Delta &= -b_2^2 b_8 - 8b_4^3 = \\
&= 16a^{2p} b^{2p} \left(b^p - a^p\right)^2 + 64a^{3p} b^{3p} c^{3p} = \\
&= 16a^{2p} b^{2p} \left(\left(b^p + a^p\right)^2 - 4a^p b^p\right) + 64a^{3p} b^{3p} c^{3p} = 16a^{2p} b^{2p} c^{2p}, \\
c_4 &= b_2^2 - 24b_4 = \\
&= 16\left(b^p - a^p\right) + 48a^p b^p = \\
&= 16\left(b^{2p} + a^{2p} - 2a^p b^p + 3a^p b^p\right) = 16\left(b^{2p} + a^{2p} + a^p b^p\right).
\end{aligned}
$$

Niech $\ell$ będzie liczbą pierwszą.

Niech $\ell$ będzie liczbą pierwszą.

Jeśli $\ell \nmid \Delta$, to krzywa $E$ z twierdzenia 4.9 ma dobrą redukcję modulo $\ell$.

Niech $\ell$ będzie liczbą pierwszą.

Jeśli $\ell \nmid \Delta$, to krzywa $E$ z twierdzenia 4.9 ma dobrą redukcję modulo $\ell$.

Warunek $\ell \nmid \Delta$ jest równoważny warunkowi $\ell \nmid abc$.

Niech $\ell$ będzie liczbą pierwszą.

Jeśli $\ell \nmid \Delta$, to krzywa $E$ z twierdzenia 4.9 ma dobrą redukcję modulo $\ell$.

Warunek $\ell \nmid \Delta$ jest równoważny warunkowi $\ell \nmid abc$.

Wykażemy teraz, że gdy $\ell \mid abc$, to krzywa $E$ ma złą multiplikatywną redukcję.

Niech $\ell$ będzie liczbą pierwszą.

Jeśli $\ell \nmid \Delta$, to krzywa $E$ z twierdzenia 4.9 ma dobrą redukcję modulo $\ell$.

Warunek $\ell \nmid \Delta$ jest równoważny warunkowi $\ell \nmid abc$.

Wykażemy teraz, że gdy $\ell \mid abc$, to krzywa $E$ ma złą multiplikatywną redukcję.

Dokonajmy najpierw liniowej zamiany zmiennych:

Niech $\ell$ będzie liczbą pierwszą.

Jeśli $\ell \nmid \Delta$, to krzywa $E$ z twierdzenia 4.9 ma dobrą redukcję modulo $\ell$.

Warunek $\ell \nmid \Delta$ jest równoważny warunkowi $\ell \nmid abc$.

Wykażemy teraz, że gdy $\ell \mid abc$, to krzywa $E$ ma złą multiplikatywną redukcję.

Dokonajmy najpierw liniowej zamiany zmiennych:

$$x = 4X,$$
$$y = 8Y + 4X.$$

Niech $\ell$ będzie liczbą pierwszą.

Jeśli $\ell \nmid \Delta$, to krzywa $E$ z twierdzenia 4.9 ma dobrą redukcję modulo $\ell$.

Warunek $\ell \nmid \Delta$ jest równoważny warunkowi $\ell \nmid abc$.

Wykażemy teraz, że gdy $\ell \mid abc$, to krzywa $E$ ma złą multiplikatywną redukcję.

Dokonajmy najpierw liniowej zamiany zmiennych:

$$x = 4X,$$
$$y = 8Y + 4X.$$

$$(8Y + 4X)^2 = 64X^3 + (-a^p + b^p)\,16X^2 - a^p b^p 4X,$$
$$64Y^2 + 64XY = 64X^3 + (b^p - a^p - 1)\,16X^2 - a^p b^p 4X,$$
$$Y^2 + XY = X^3 + \frac{(b^p - a^p - 1)}{4}X^2 - \frac{a^p b^p}{16}X,$$

$$E' : \ Y^2 + XY = X^3 + \frac{(b^p - a^p - 1)}{4}X^2 - \frac{a^p b^p}{16}X. \qquad (4.8)$$

$$E' : \ Y^2 + XY = X^3 + \frac{(b^p - a^p - 1)}{4}X^2 - \frac{a^p b^p}{16}X. \qquad (4.8)$$

Uzyskaliśmy krzywą $E'$ izomorficzną z $E$ nad $\mathbb{Q}$.

$$E' : \ Y^2 + XY = X^3 + \frac{(b^p - a^p - 1)}{4}X^2 - \frac{a^p b^p}{16}X. \qquad (4.8)$$

Uzyskaliśmy krzywą $E'$ izomorficzną z $E$ nad $\mathbb{Q}$.

Współczynniki krzywej $E'$ są całkowite, wynika to z przyjętych założeń ($2 \mid a$ oraz $b \equiv 1 \pmod 4$).

$$E' : \ Y^2 + XY = X^3 + \frac{(b^p - a^p - 1)}{4}X^2 - \frac{a^p b^p}{16}X. \qquad (4.8)$$

Uzyskaliśmy krzywą $E'$ izomorficzną z $E$ nad $\mathbb{Q}$.

Współczynniki krzywej $E'$ są całkowite, wynika to z przyjętych założeń ($2 \mid a$ oraz $b \equiv 1 \pmod 4$). Ze wzorów (4.5) mamy:

$$E' : \ Y^2 + XY = X^3 + \frac{(b^p - a^p - 1)}{4}X^2 - \frac{a^p b^p}{16}X. \qquad (4.8)$$

Uzyskaliśmy krzywą $E'$ izomorficzną z $E$ nad $\mathbb{Q}$.

Współczynniki krzywej $E'$ są całkowite, wynika to z przyjętych założeń ($2 \mid a$ oraz $b \equiv 1 \pmod 4$). Ze wzorów (4.5) mamy:

$$\Delta' = \frac{\Delta}{2^{12}} = 2^{-8} a^{2p} b^{2p} c^{2p},$$
$$c_4' = \frac{c_4}{2^4} = b^{2p} + a^{2p} + a^p b^p.$$

$$E' : \ Y^2 + XY = X^3 + \frac{(b^p - a^p - 1)}{4}X^2 - \frac{a^p b^p}{16}X. \qquad (4.8)$$

Uzyskaliśmy krzywą $E'$ izomorficzną z $E$ nad $\mathbb{Q}$.

Współczynniki krzywej $E'$ są całkowite, wynika to z przyjętych założeń ($2 \mid a$ oraz $b \equiv 1 \pmod 4$). Ze wzorów (4.5) mamy:

$$\Delta' = \frac{\Delta}{2^{12}} = 2^{-8} a^{2p} b^{2p} c^{2p},$$
$$c_4' = \frac{c_4}{2^4} = b^{2p} + a^{2p} + a^p b^p.$$

Sprawdzimy teraz, czy (4.8) jest równaniem minimalnym krzywej $E$ dla każdej liczby $\ell$.

Jeśli $\ell \nmid abc$, to jest oczywistym, że równanie krzywej $E'$ jest minimalne dla $E$.

Jeśli $\ell \nmid abc$, to jest oczywistym, że równanie krzywej $E'$ jest minimalne dla $E$.

Jeśli $\ell \mid abc$, to z tego, że $a, b, c$ są parami względnie pierwsze wynika, że $\ell$ dzieli tylko jedną spośród nich.

Jeśli $\ell \nmid abc$, to jest oczywistym, że równanie krzywej $E'$ jest minimalne dla $E$.

Jeśli $\ell \mid abc$, to z tego, że $a, b, c$ są parami względnie pierwsze wynika, że $\ell$ dzieli tylko jedną spośród nich.

1. Załóżmy, że $\ell \mid a$. Wykażemy, że $\ell \nmid c_4'$.

Jeśli $\ell \nmid abc$, to jest oczywistym, że równanie krzywej $E'$ jest minimalne dla $E$.

Jeśli $\ell \mid abc$, to z tego, że $a, b, c$ są parami względnie pierwsze wynika, że $\ell$ dzieli tylko jedną spośród nich.

1. Załóżmy, że $\ell \mid a$. Wykażemy, że $\ell \nmid c_4'$.

Jeśli $\ell \nmid abc$, to jest oczywistym, że równanie krzywej $E'$ jest minimalne dla $E$.

Jeśli $\ell \mid abc$, to z tego, że $a, b, c$ są parami względnie pierwsze wynika, że $\ell$ dzieli tylko jedną spośród nich.

1. Załóżmy, że $\ell \mid a$. Wykażemy, że $\ell \nmid c_4'$.
   Przypuśćmy, że $\ell \mid \left(b^{2p} + a^{2p} + a^p b^p\right)$, ale ponieważ $\ell \mid a$ mamy, że $\ell \mid \left(a^{2p} + a^p b^p\right)$, stąd $\ell \mid b^{2p}$ — sprzeczność, bo $a, b, c$ są parami względnie pierwsze.
2. Analogicznie jak wyżej dowodzimy, gdy $\ell \mid b$.

Jeśli $\ell \nmid abc$, to jest oczywistym, że równanie krzywej $E'$ jest minimalne dla $E$.

Jeśli $\ell \mid abc$, to z tego, że $a, b, c$ są parami względnie pierwsze wynika, że $\ell$ dzieli tylko jedną spośród nich.

1. Załóżmy, że $\ell \mid a$. Wykażemy, że $\ell \nmid c_4'$.
   Przypuśćmy, że $\ell \mid \left(b^{2p} + a^{2p} + a^p b^p\right)$, ale ponieważ $\ell \mid a$ mamy, że $\ell \mid \left(a^{2p} + a^p b^p\right)$, stąd $\ell \mid b^{2p}$ — sprzeczność, bo $a, b, c$ są parami względnie pierwsze.
2. Analogicznie jak wyżej dowodzimy, gdy $\ell \mid b$.
3. Załóżmy, że $\ell \mid c$. Wykażemy, że $\ell \nmid c_4'$.

Jeśli $\ell \nmid abc$, to jest oczywistym, że równanie krzywej $E'$ jest minimalne dla $E$.

Jeśli $\ell \mid abc$, to z tego, że $a, b, c$ są parami względnie pierwsze wynika, że $\ell$ dzieli tylko jedną spośród nich.

1. Załóżmy, że $\ell \mid a$. Wykażemy, że $\ell \nmid c_4'$.
   Przypuśćmy, że $\ell \mid \left(b^{2p} + a^{2p} + a^p b^p\right)$, ale ponieważ $\ell \mid a$ mamy, że $\ell \mid \left(a^{2p} + a^p b^p\right)$, stąd $\ell \mid b^{2p}$ — sprzeczność, bo $a, b, c$ są parami względnie pierwsze.
2. Analogicznie jak wyżej dowodzimy, gdy $\ell \mid b$.
3. Załóżmy, że $\ell \mid c$. Wykażemy, że $\ell \nmid c_4'$.

Jeśli $\ell \nmid abc$, to jest oczywistym, że równanie krzywej $E'$ jest minimalne dla $E$.

Jeśli $\ell \mid abc$, to z tego, że $a, b, c$ są parami względnie pierwsze wynika, że $\ell$ dzieli tylko jedną spośród nich.

1. Załóżmy, że $\ell \mid a$. Wykażemy, że $\ell \nmid c_4'$.
   Przypuśćmy, że $\ell \mid \left(b^{2p} + a^{2p} + a^p b^p\right)$, ale ponieważ $\ell \mid a$ mamy, że $\ell \mid \left(a^{2p} + a^p b^p\right)$, stąd $\ell \mid b^{2p}$ — sprzeczność, bo $a, b, c$ są parami względnie pierwsze.
2. Analogicznie jak wyżej dowodzimy, gdy $\ell \mid b$.
3. Załóżmy, że $\ell \mid c$. Wykażemy, że $\ell \nmid c_4'$.
   Przypuśćmy, że:

$$\ell \mid \left(b^{2p} + a^{2p} + a^p b^p\right) = \left(\left(b^p + a^p\right)^2 - a^p b^p\right) = \left(c^{2p} - a^p b^p\right),$$

   ale jako że $\ell \mid c$ mamy, że $\ell \mid c^{2p}$, stąd $\ell \mid a^p b^p$ – sprzeczność, bo $a, b, c$ są parami względnie pierwsze.

Z faktu 4.6 mamy, że równanie (4.8) jest równaniem minimalnym krzywej $E$,

Z faktu 4.6 mamy, że równanie (4.8) jest równaniem minimalnym krzywej $E$, natomiast z twierdzenia 4.9 mamy, że dla każdej liczby pierwszej $\ell \mid abc$, krzywa $E$ ma złą multiplikatywną redukcję w $\ell$.

Z faktu 4.6 mamy, że równanie (4.8) jest równaniem minimalnym krzywej $E$, natomiast z twierdzenia 4.9 mamy, że dla każdej liczby pierwszej $\ell \mid abc$, krzywa $E$ ma złą multiplikatywną redukcję w $\ell$.

**Zatem krzywa ta jest semistabilna**.

Następnym ważnym momentem było udowodnienie w 1986 roku, przez Kena Ribeta – **Hipotezy $\epsilon$ Serre'a**, spowodowało to sprowadzenie problemu Fermata do udowodnienia **hipotezy Shimury, Taniyamy i Weila (o modularności)** dla krzywych eliptycznych semistabilnych.

Jak wiemy szeregiem Dirichleta nazywamy szereg postaci:

Jak wiemy szeregiem Dirichleta nazywamy szereg postaci:

$$f(s) = \sum_{n \geqslant 1} \frac{a(n)}{n^s}, \ a(n) \in \mathbb{C}, s \in \mathbb{C}.$$

Jak wiemy szeregiem Dirichleta nazywamy szereg postaci:

$$f(s) = \sum_{n \geqslant 1} \frac{a(n)}{n^s}, \ a(n) \in \mathbb{C}, s \in \mathbb{C}.$$

Najprostszym przykładem szeregu Dirichleta jest funkcja dzeta Riemanna:

Jak wiemy szeregiem Dirichleta nazywamy szereg postaci:

$$f(s) = \sum_{n \geqslant 1} \frac{a(n)}{n^s}, \ a(n) \in \mathbb{C}, s \in \mathbb{C}.$$

Najprostszym przykładem szeregu Dirichleta jest funkcja dzeta Riemanna:

$$f(s) = \sum_{n \geqslant 1} n^{-s}.$$

## Definicja 4.12

**$L-$szeregiem krzywej eliptycznej** $E$ zdefiniowanej nad $\mathbb{Q}$ nazywamy szereg postaci:

## Definicja 4.12

**$L-$szeregiem krzywej eliptycznej** $E$ zdefiniowanej nad $\mathbb{Q}$ nazywamy szereg postaci:

$$L(E,s) = \prod_{p \text{ dobrej redukcji}} \frac{1}{1 - a_p p^{-s} + p^{1-s}} \prod_{p \text{ złej redukcji}} \frac{1}{1 - a_p p^{-s}} = \sum_{n \geqslant 1} \frac{a_n}{n^s},$$

## Definicja 4.12

**$L-$szeregiem krzywej eliptycznej** $E$ zdefiniowanej nad $\mathbb{Q}$ nazywamy szereg postaci:

$$L(E,s) = \prod_{p \text{ dobrej redukcji}} \frac{1}{1 - a_p p^{-s} + p^{1-s}} \prod_{p \text{ złej redukcji}} \frac{1}{1 - a_p p^{-s}} = \sum_{n \geqslant 1} \frac{a_n}{n^s},$$

gdzie $p$ przebiega liczby pierwsze, mamy:

## Definicja 4.12

**$L-$szeregiem krzywej eliptycznej** $E$ zdefiniowanej nad $\mathbb{Q}$ nazywamy szereg postaci:

$$L(E,s) = \prod_{p \text{ dobrej redukcji}} \frac{1}{1 - a_p p^{-s} + p^{1-s}} \prod_{p \text{ złej redukcji}} \frac{1}{1 - a_p p^{-s}} = \sum_{n \geqslant 1} \frac{a_n}{n^s},$$

gdzie $p$ przebiega liczby pierwsze, mamy:

$$a_p = \begin{cases} p + 1 - \#E(\mathbb{F}_p), & \text{gdy } E \text{ ma dobrą redukcję w } p, \\ 1 \vee -1, & \text{gdy } E \text{ ma złą multiplikatywną redukcję w } p, \\ 0, & \text{gdy } E \text{ ma addytywną redukcję w } p, \end{cases}$$

## kontynuacja Definicji 4.12

dla $r \geqslant 1$

## KONTYNUACJA DEFINICJI 4.12

dla $r \geqslant 1$

$$a_{p^{r+1}} = \begin{cases} a_p a_{p^r} - p a_{p^{r-1}}, & \text{gdy } E \text{ ma dobrą redukcję w } p, \\ a_p^{r+1}, & \text{gdy } E \text{ ma złą redukcję w } p, \end{cases}$$

## KONTYNUACJA DEFINICJI 4.12

dla $r \geqslant 1$

$$a_{p^{r+1}} = \begin{cases} a_p a_{p^r} - p a_{p^{r-1}}, & \text{gdy } E \text{ ma dobrą redukcję w } p, \\ a_p^{r+1}, & \text{gdy } E \text{ ma złą redukcję w } p, \end{cases}$$

$$a_n = \begin{cases} 1, & \text{gdy } n = 1, \\ a_p, & \text{gdy } n = p, \\ a_{p^{r+1}}, & \text{gdy } n = p^{r+1}, r \geqslant 1, \\ a_k a_l, & \text{gdy } n = lk \text{ oraz } (l,k) = 1. \end{cases}$$

# Bardzo krótko o formach modularnych

Niech $\mathfrak{h}$ oznacza górną półpłaszczyznę zespoloną:

$$\mathfrak{h} := \{z = x + iy : \ x, y, \in \mathbb{R}, y > 0\}.$$

Niech $\mathfrak{h}$ oznacza górną półpłaszczyznę zespoloną:

$$\mathfrak{h} := \{z = x + iy : \ x, y, \in \mathbb{R}, y > 0\}.$$

Niech $SL_2(\mathbb{Z})$ będzie grupą macierzy $2 \times 2$ o całkowitych współczynnikach i o wyznaczniku równym 1.

Niech $\mathfrak{h}$ oznacza górną półpłaszczyznę zespoloną:

$$\mathfrak{h} := \{z = x + iy : \ x, y, \in \mathbb{R}, y > 0\}.$$

Niech $\mathrm{SL}_2(\mathbb{Z})$ będzie grupą macierzy $2 \times 2$ o całkowitych współczynnikach i o wyznaczniku równym 1. Grupę $\mathrm{SL}_2(\mathbb{Z})$ nazywamy **pełną grupą modularną** (ang. full modular group) i oznaczamy $\Gamma(1)$.

Niech $\mathfrak{h}$ oznacza górną półpłaszczyznę zespoloną:

$$\mathfrak{h} := \{z = x + iy : \ x, y, \in \mathbb{R}, y > 0\}.$$

Niech $\mathrm{SL}_2(\mathbb{Z})$ będzie grupą macierzy $2 \times 2$ o całkowitych współczynnikach i o wyznaczniku równym 1. Grupę $\mathrm{SL}_2(\mathbb{Z})$ nazywamy **pełną grupą modularną** (ang. full modular group) i oznaczamy $\Gamma(1)$. Wówczas grupa $\Gamma(1)$ działa na $\mathfrak{h}$ w następujący sposób:

Niech $\mathfrak{h}$ oznacza górną półpłaszczyznę zespoloną:

$$\mathfrak{h} := \{z = x + iy : \ x, y, \in \mathbb{R}, y > 0\}.$$

Niech $\mathrm{SL}_2(\mathbb{Z})$ będzie grupą macierzy $2 \times 2$ o całkowitych współczynnikach i o wyznaczniku równym 1. Grupę $\mathrm{SL}_2(\mathbb{Z})$ nazywamy **pełną grupą modularną** (ang. full modular group) i oznaczamy $\Gamma(1)$. Wówczas grupa $\Gamma(1)$ działa na $\mathfrak{h}$ w następujący sposób:

$$\gamma z = \frac{az + b}{cz + d}, \text{ dla } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1).$$

Niech $\mathfrak{h}$ oznacza górną półpłaszczyznę zespoloną:

$$\mathfrak{h} := \{z = x + iy : \ x, y, \in \mathbb{R}, y > 0\}.$$

Niech $\mathrm{SL}_2(\mathbb{Z})$ będzie grupą macierzy $2 \times 2$ o całkowitych współczynnikach i o wyznaczniku równym 1. Grupę $\mathrm{SL}_2(\mathbb{Z})$ nazywamy **pełną grupą modularną** (ang. full modular group) i oznaczamy $\Gamma(1)$. Wówczas grupa $\Gamma(1)$ działa na $\mathfrak{h}$ w następujący sposób:

$$\gamma z = \frac{az + b}{cz + d}, \text{ dla } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1).$$

Przez $\mathfrak{h}^*$ będziemy oznaczać:

$$\mathfrak{h}^* := \mathfrak{h} \cup \mathbb{Q} \cup \{\infty\}.$$

Działanie grupy $\Gamma(1)$ można rozszerzyć w następujący sposób na $\mathfrak{h}^*$.

Działanie grupy $\Gamma(1)$ można rozszerzyć w następujący sposób na $\mathfrak{h}^*$.

Niech $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$:

Działanie grupy $\Gamma(1)$ można rozszerzyć w następujący sposób na $\mathfrak{h}^*$.

Niech $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a}{c}, \text{ gdzie } c \neq 0,$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \infty = \infty,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{r}{s} = \frac{ar + bs}{cr + ds}, \text{ gdzie } (r, s) = 1.$$

Działanie grupy $\Gamma(1)$ można rozszerzyć w następujący sposób na $\mathfrak{h}^*$.

Niech $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a}{c}, \text{ gdzie } c \neq 0,$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \infty = \infty,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{r}{s} = \frac{ar + bs}{cr + ds}, \text{ gdzie } (r, s) = 1.$$

Zauważmy, że $\gamma\left(-\frac{d}{c}\right) = \infty$.

Działanie grupy $\Gamma(1)$ można rozszerzyć w następujący sposób na $\mathfrak{h}^*$.

Niech $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a}{c}, \text{ gdzie } c \neq 0,$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \infty = \infty,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{r}{s} = \frac{ar + bs}{cr + ds}, \text{ gdzie } (r, s) = 1.$$

Zauważmy, że $\gamma\left(-\frac{d}{c}\right) = \infty$.

Zbiór $\mathbb{Q} \cup \{\infty\}$ nazywamy **ostrzami**.

Działanie grupy $\Gamma(1)$ można rozszerzyć w następujący sposób na $\mathfrak{h}^*$.

Niech $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a}{c}, \text{ gdzie } c \neq 0,$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \infty = \infty,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{r}{s} = \frac{ar + bs}{cr + ds}, \text{ gdzie } (r, s) = 1.$$

Zauważmy, że $\gamma\left(-\frac{d}{c}\right) = \infty$.

Zbiór $\mathbb{Q} \cup \{\infty\}$ nazywamy **ostrzami**.

Niech $N \in \mathbb{N}$. Określimy jedną z podgrup kongruencji poziomu $N$:

Działanie grupy $\Gamma(1)$ można rozszerzyć w następujący sposób na $\mathfrak{h}^*$.

Niech $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a}{c}, \text{ gdzie } c \neq 0,$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \infty = \infty,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{r}{s} = \frac{ar + bs}{cr + ds}, \text{ gdzie } (r, s) = 1.$$

Zauważmy, że $\gamma\left(-\frac{d}{c}\right) = \infty$.

Zbiór $\mathbb{Q} \cup \{\infty\}$ nazywamy **ostrzami**.

Niech $N \in \mathbb{N}$. Określimy jedną z podgrup kongruencji poziomu $N$:

$$\Gamma_0(N) := \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : \ N \mid c \right\}.$$

Niech $k \in \mathbb{N}$. Niech $f$ będzie funkcją funkcją holomorficzną $f : \mathfrak{h} \to \mathbb{C}$, która się "zachowuje całkiem przyzwoicie" względem działania grupy $\Gamma_0(N)$, tzn. funkcją spełniającą następujący warunek:

Niech $k \in \mathbb{N}$. Niech $f$ będzie funkcją funkcją holomorficzną $f : \mathfrak{h} \to \mathbb{C}$, która się "zachowuje całkiem przyzwoicie" względem działania grupy $\Gamma_0(N)$, tzn. funkcją spełniającą następujący warunek:

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \, \forall z \in \mathfrak{h} : \; f(\gamma z) = (cz + d)^k f(z).$$

Niech $k \in \mathbb{N}$. Niech $f$ będzie funkcją funkcją holomorficzną $f : \mathfrak{h} \to \mathbb{C}$, która się "zachowuje całkiem przyzwoicie" względem działania grupy $\Gamma_0(N)$, tzn. funkcją spełniającą następujący warunek:

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \, \forall z \in \mathfrak{h} : \; f(\gamma z) = (cz + d)^k f(z).$$

Zauważmy, że $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, zatem $f(z) = f(z+1)$ dla każdego $z \in \mathfrak{h}$.

Niech $k \in \mathbb{N}$. Niech $f$ będzie funkcją funkcją holomorficzną $f : \mathfrak{h} \to \mathbb{C}$, która się "zachowuje całkiem przyzwoicie" względem działania grupy $\Gamma_0(N)$, tzn. funkcją spełniającą następujący warunek:

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \, \forall z \in \mathfrak{h} : \; f(\gamma z) = (cz + d)^k f(z).$$

Zauważmy, że $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, zatem $f(z) = f(z+1)$ dla każdego $z \in \mathfrak{h}$. Możemy ją więc rozwinąć w szereg Fouriera:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n z}.$$

Niech $k \in \mathbb{N}$. Niech $f$ będzie funkcją funkcją holomorficzną $f : \mathfrak{h} \to \mathbb{C}$, która się "zachowuje całkiem przyzwoicie" względem działania grupy $\Gamma_0(N)$, tzn. funkcją spełniającą następujący warunek:

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \, \forall z \in \mathfrak{h} : \; f(\gamma z) = (cz + d)^k f(z).$$

Zauważmy, że $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, zatem $f(z) = f(z+1)$ dla każdego $z \in \mathfrak{h}$. Możemy ją więc rozwinąć w szereg Fouriera:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n z}.$$

Mówimy, że funkcja $f$ jest **holomorficzna w nieskończoności**, gdy $a_n = 0$, dla $n < 0$,

Niech $k \in \mathbb{N}$. Niech $f$ będzie funkcją funkcją holomorficzną $f : \mathfrak{h} \to \mathbb{C}$, która się "zachowuje całkiem przyzwoicie" względem działania grupy $\Gamma_0(N)$, tzn. funkcją spełniającą następujący warunek:

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \, \forall z \in \mathfrak{h} : \; f(\gamma z) = (cz + d)^k f(z).$$

Zauważmy, że $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, zatem $f(z) = f(z+1)$ dla każdego $z \in \mathfrak{h}$. Możemy ją więc rozwinąć w szereg Fouriera:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n z}.$$

Mówimy, że funkcja $f$ jest **holomorficzna w nieskończoności**, gdy $a_n = 0$, dla $n < 0$, natomiast mówimy, że funkcja $f$ **znika w nieskończoności**, gdy $a_n = 0$ dla $n \leqslant 0$.

## Definicja 5.1

**Formą modularną wagi** $k$ **poziomu** $N$ nazywamy funkcję j.w., która jest holomorficzna na $\mathfrak{h}^*$.

## Definicja 5.1

**Formą modularną wagi** $k$ **poziomu** $N$ nazywamy funkcję j.w., która jest holomorficzna na $\mathfrak{h}^*$.

Formę modularną, która znika we wszystkich ostrzach nazywamy **formą paraboliczną**.

### Definicja 5.1

**Formą modularną wagi** $k$ **poziomu** $N$ nazywamy funkcję j.w., która jest holomorficzna na $\mathfrak{h}^*$.

Formę modularną, która znika we wszystkich ostrzach nazywamy **formą paraboliczną**.

Przez $M_k(N)$ (odp. $S_k(N)$) będziemy oznaczać zbiór form modularnych (odp. parabolicznych) poziomu $N$ wagi $k$

## Definicja 5.1

**Formą modularną wagi** $k$ **poziomu** $N$ nazywamy funkcję j.w., która jest holomorficzna na $\mathfrak{h}^*$.

Formę modularną, która znika we wszystkich ostrzach nazywamy **formą paraboliczną**.

Przez $M_k(N)$ (odp. $S_k(N)$) będziemy oznaczać zbiór form modularnych (odp. parabolicznych) poziomu $N$ wagi $k$

**Nas będą interesowały formy wagi** 2.

### Definicja 5.1

**Formą modularną wagi** $k$ **poziomu** $N$ nazywamy funkcję j.w., która jest holomorficzna na $\mathfrak{h}^*$.

Formę modularną, która znika we wszystkich ostrzach nazywamy **formą paraboliczną**.

Przez $M_k(N)$ (odp. $S_k(N)$) będziemy oznaczać zbiór form modularnych (odp. parabolicznych) poziomu $N$ wagi $k$

**Nas będą interesowały formy wagi** 2.

### Fakt 5.2

*$M_2(N)$ jest skończenie wymiarową przestrzenią liniową nad $\mathbb{C}$.*

### Definicja 5.1

**Formą modularną wagi** $k$ **poziomu** $N$ nazywamy funkcję j.w., która jest holomorficzna na $\mathfrak{h}^*$.

Formę modularną, która znika we wszystkich ostrzach nazywamy **formą paraboliczną**.

Przez $M_k(N)$ (odp. $S_k(N)$) będziemy oznaczać zbiór form modularnych (odp. parabolicznych) poziomu $N$ wagi $k$

**Nas będą interesowały formy wagi** 2.

### Fakt 5.2

*$M_2(N)$ jest skończenie wymiarową przestrzenią liniową nad $\mathbb{C}$.*
*$S_2(N)$ jest podprzestrzenią przestrzeni $M_2(N)$.*

## Forma stara i nowa

Jeśli $M \mid N$, to mamy zanurzenie $S_2(M) \subseteq S_2(N)$: dla $f \in S_2(M)$, mamy $\tilde{f}(z) = f((N/M)z)$ dla każdego $z \in \mathfrak{h}^*$ oraz $\tilde{f} \in S_2(N)$.

## Forma stara i nowa

Jeśli $M \mid N$, to mamy zanurzenie $S_2(M) \subseteq S_2(N)$: dla $f \in S_2(M)$, mamy $\tilde{f}(z) = f((N/M)z)$ dla każdego $z \in \mathfrak{h}^*$ oraz $\tilde{f} \in S_2(N)$.

Formę $f \in S_2(N)$ nazywamy formą **starą**, gdy należy do powłoki liniowej generowanej przez obrazy wszystkich podprzestrzeni $S_2(M)$ dla każdego $M \mid N$ przy zanurzeniu określonym j.w.

## Forma stara i nowa

Jeśli $M \mid N$, to mamy zanurzenie $S_2(M) \subseteq S_2(N)$: dla $f \in S_2(M)$, mamy $\tilde{f}(z) = f((N/M)z)$ dla każdego $z \in \mathfrak{h}^*$ oraz $\tilde{f} \in S_2(N)$.

Formę $f \in S_2(N)$ nazywamy formą **starą**, gdy należy do powłoki liniowej generowanej przez obrazy wszystkich podprzestrzeni $S_2(M)$ dla każdego $M \mid N$ przy zanurzeniu określonym j.w.

Formę $f \in S_2(N)$ nazywamy formą **nową**, gdy należy do dopełnienia ortogonalnego względem iloczynu skalarnego Peterssona form starych.

Dla każdego $n \in \mathbb{N}$ takiego, że $(n, N) = 1$, Hecke określił przekształcenie liniowe, zwane dzisiaj **operatorem Hecke'go** $T_n : \ S_2(N) \to S_2(N)$.

Dla każdego $n \in \mathbb{N}$ takiego, że $(n, N) = 1$, Hecke określił przekształcenie liniowe, zwane dzisiaj **operatorem Hecke'go** $T_n : \ S_2(N) \to S_2(N)$. Operatory Hecke'go są przemienne oraz dla $(n, m) = 1$, mamy $T_{nm} = T_n \circ T_m$.

Dla każdego $n \in \mathbb{N}$ takiego, że $(n, N) = 1$, Hecke określił przekształcenie liniowe, zwane dzisiaj **operatorem Hecke'go** $T_n : S_2(N) \to S_2(N)$. Operatory Hecke'go są przemienne oraz dla $(n, m) = 1$, mamy $T_{nm} = T_n \circ T_m$.

Interesują nas wektory własne, które są wektorami własnymi dla każdego $n$, tzn. takie formy $f \in S_2(N)$, że:

$$T_n(f) = \lambda_n f, \text{ dla każdego } n, (n, N) = 1.$$

Dla każdego $n \in \mathbb{N}$ takiego, że $(n, N) = 1$, Hecke określił przekształcenie liniowe, zwane dzisiaj **operatorem Hecke'go** $T_n : S_2(N) \to S_2(N)$. Operatory Hecke'go są przemienne oraz dla $(n, m) = 1$, mamy $T_{nm} = T_n \circ T_m$.

Interesują nas wektory własne, które są wektorami własnymi dla każdego $n$, tzn. takie formy $f \in S_2(N)$, że:

$$T_n(f) = \lambda_n f, \text{ dla każdego } n, (n, N) = 1.$$

Takie wektory własne nazywamy **formami własnymi**.

Dla każdego $n \in \mathbb{N}$ takiego, że $(n, N) = 1$, Hecke określił przekształcenie liniowe, zwane dzisiaj **operatorem Hecke'go** $T_n : S_2(N) \to S_2(N)$. Operatory Hecke'go są przemienne oraz dla $(n, m) = 1$, mamy $T_{nm} = T_n \circ T_m$.

Interesują nas wektory własne, które są wektorami własnymi dla każdego $n$, tzn. takie formy $f \in S_2(N)$, że:

$$T_n(f) = \lambda_n f, \text{ dla każdego } n, (n, N) = 1.$$

Takie wektory własne nazywamy **formami własnymi**.

Zatem przypomnijmy dla $f \in S_2(N)$, $f$ ma rozwinięcie w szereg Fouriera postaci:

$$f(z) = \sum_{n=1}^{\infty} c_n e^{2\pi i n z}$$

## Hipoteza Shimury Taniyamy i Weila

Niech $E$ będzie krzywą eliptyczną określoną nad $\mathbb{Q}$ o przewodniku $N$.

## Hipoteza Shimury Taniyamy i Weila

Niech $E$ będzie krzywą eliptyczną określoną nad $\mathbb{Q}$ o przewodniku $N$. Niech $a_n$ będą liczbami, które pojawiają się w $L$-szeregu krzywej $E$ dla każdego $n$.

## Hipoteza Shimury Taniyamy i Weila

Niech $E$ będzie krzywą eliptyczną określoną nad $\mathbb{Q}$ o przewodniku $N$. Niech $a_n$ będą liczbami, które pojawiają się w $L$-szeregu krzywej $E$ dla każdego $n$. Wówczas istnieje nowa forma paraboliczna wagi 2, poziomu $N$,

## Hipoteza Shimury Taniyamy i Weila

Niech $E$ będzie krzywą eliptyczną określoną nad $\mathbb{Q}$ o przewodniku $N$. Niech $a_n$ będą liczbami, które pojawiają się w $L$-szeregu krzywej $E$ dla każdego $n$. Wówczas istnieje nowa forma paraboliczna wagi 2, poziomu $N$, która jest formą własną,

## Hipoteza Shimury Taniyamy i Weila

Niech $E$ będzie krzywą eliptyczną określoną nad $\mathbb{Q}$ o przewodniku $N$. Niech $a_n$ będą liczbami, które pojawiają się w $L$-szeregu krzywej $E$ dla każdego $n$. Wówczas istnieje nowa forma paraboliczna wagi 2, poziomu $N$, która jest formą własną, której szereg Fouriera jest postaci $\sum_n a_n e^{2\pi inz}$,

## Hipoteza Shimury Taniyamy i Weila

Niech $E$ będzie krzywą eliptyczną określoną nad $\mathbb{Q}$ o przewodniku $N$. Niech $a_n$ będą liczbami, które pojawiają się w $L$-szeregu krzywej $E$ dla każdego $n$. Wówczas istnieje nowa forma paraboliczna wagi 2, poziomu $N$, która jest formą własną, której szereg Fouriera jest postaci $\sum_n a_n e^{2\pi inz}$, tzn. każda krzywa eliptyczna nad $\mathbb{Q}$ jest modularna.

## Twierdzenie Wilesa i Taylora

Każda semistabilna krzywa eliptyczna nad $\mathbb{Q}$ jest modularna.

# Bardzo krótki szkic dowodu TWIERDZENIA:

## Bardzo krótki szkic dowodu TWIERDZENIA:

Udowodnienie hipotezy $\epsilon$ Serre'a przez K. Ribeta pozwoliło pokazać, że nie może istnieć nietrywialne rozwiązanie równania $x^n + y^n = z^n$,

## Bardzo krótki szkic dowodu TWIERDZENIA:

Udowodnienie hipotezy $\epsilon$ Serre'a przez K. Ribeta pozwoliło pokazać, że nie może istnieć nietrywialne rozwiązanie równania $x^n + y^n = z^n$, gdyż jego istnienie spowodowałoby, że istniałaby semistabilna krzywa eliptyczna – krzywa Freya,

## Bardzo krótki szkic dowodu TWIERDZENIA:

Udowodnienie hipotezy $\epsilon$ Serre'a przez K. Ribeta pozwoliło pokazać, że nie może istnieć nietrywialne rozwiązanie równania $x^n + y^n = z^n$, gdyż jego istnienie spowodowałoby, że istniałaby semistabilna krzywa eliptyczna – krzywa Freya, która jest modularna,

## Bardzo krótki szkic dowodu TWIERDZENIA:

Udowodnienie hipotezy $\epsilon$ Serre'a przez K. Ribeta pozwoliło pokazać, że nie może istnieć nietrywialne rozwiązanie równania $x^n + y^n = z^n$, gdyż jego istnienie spowodowałoby, że istniałaby semistabilna krzywa eliptyczna – krzywa Freya, która jest modularna, a wówczas musiałaby istnieć nowa forma paraboliczna własna wagi 2, poziomu 2,

## Bardzo krótki szkic dowodu TWIERDZENIA:

Udowodnienie hipotezy $\epsilon$ Serre'a przez K. Ribeta pozwoliło pokazać, że nie może istnieć nietrywialne rozwiązanie równania $x^n + y^n = z^n$, gdyż jego istnienie spowodowałoby, że istniałaby semistabilna krzywa eliptyczna – krzywa Freya, która jest modularna, a wówczas musiałaby istnieć nowa forma paraboliczna własna wagi 2, poziomu 2, a takich form nie ma,

## Bardzo krótki szkic dowodu TWIERDZENIA:

Udowodnienie hipotezy $\epsilon$ Serre'a przez K. Ribeta pozwoliło pokazać, że nie może istnieć nietrywialne rozwiązanie równania $x^n + y^n = z^n$, gdyż jego istnienie spowodowałoby, że istniałaby semistabilna krzywa eliptyczna – krzywa Freya, która jest modularna, a wówczas musiałaby istnieć nowa forma paraboliczna własna wagi 2, poziomu 2, a takich form nie ma, więc otrzymujemy sprzeczność.

□

# Źródła I

[1] Autorstwa Nieznany - https://web.archive.org/web/20191028044928/http://www-groups.dcs.st-and.ac.uk/ history/PictDisplay/Fermat.html, Domena publiczna, https://commons.wikimedia.org/w/index.php?curid=36804

[2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag New York, Inc., 1986.

[3] Paulo Ribenboim, *Wielkie twierdzenie Fermata dla laików*, z angielskiego przełożył Jerzy Browkin, Wydawnictwo Naukowo-Techniczne Warszawa, 2001.

[4] Fernando Q. Gouvêa, *A Marvelous Proof*, Amer. Math. Monthly 101, 1994, str. 203–222.

# Źródła II

[5] F. Diamond, J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics 228, Springer Science+Business Media, Inc., 2005.