

Twierdzenie Lagrange’a

Mikołaj Stańczyk

4 marca 2010

1. Początki

Rozważania dotyczące przedstawiania liczby jako **sumy czterech kwadratów** pojawiają się już w słynnym dziele *Arytmetyka*, autorstwa Diofantosa — aleksandryjskiego matematyka żyjącego w 3. wieku n. e. W 1621 roku, w przygotowanej przez francuskiego matematyka Claude’a Gasparda Bacheta łacińskiej edycji tego dzieła, zamieszczone zostało następujące twierdzenie:

Każda liczba naturalna jest sumą czterech kwadratów.

Zostało ono udowodnione przez znanego włoskiego matematyka **Josepha Louisa Lagrange’a** w 1770 roku — dlatego zostało nazwane jego imieniem.

Dowód twierdzenia Lagrange’a, który przedstawimy, opiera się na zastosowaniu metod algebraicznych. Zanim będziemy w stanie go przeprowadzić, musimy wprowadzić definicje kilku ważnych pojęć algebraicznych i omówić ich własności.

2. Kwaterniony Hamiltona

Przypomnijmy, że **liczbą zespoloną** nazywamy każdą liczbę postaci $a + bi$, gdzie a oraz b są liczbami rzeczywistymi, a i jest tak zwaną **jednostką urojoną**, która spełnia zależność $i^2 = -1$. Nie będziemy tutaj opisywać konstrukcji liczb zespolonych; ograniczymy się jedynie do stwierdzenia, że typowa konstrukcja zbioru liczb zespolonych \mathbb{C} opiera się na wprowadzeniu działań dodawania i mnożenia na parach uporządkowanych liczb rzeczywistych. Konstrukcja taka pozwala w prosty sposób uzasadnić najważniejsze własności algebraiczne liczb zespolonych.

Liczyby zespolone dają wyraźne korzyści, gdy zostaną wykorzystane w **geometrii płaszczyzny**. Fakt ten skłonił matematyków do poszukiwań podobnego systemu, który pozwoliłby w analogiczny sposób opisać **przestrzeń trójwymiarową**.

Sir William Rowan Hamilton, irlandzki matematyk, był jedną z osób, które poszukiwały odpowiedniego sposobu konstrukcji. Hamilton chciał zdefiniować działania na trójkach uporządkowanych, tak, aby otrzymać konstrukcję o podobnych własnościach do systemu \mathbb{C} . Z pewnych przyczyn okazało się to jednak niemożliwe.

W poniedziałek, 16 października 1843, podczas spaceru z żoną po rodzinnym Dublinie, Hamiltonowi przyszła do głowy koncepcja wprowadzenia działań na zbiorze czwórek — a nie trójek — uporządkowanych. Idea była dla niego tak ekscytująca, że wyrzucił reguły działań na kwaternionach na moście nad Kanałem Królewskim. Pomysł istotnie okazał się rewelacyjny — czwórki uporządkowane, nazwane później **kwaternionami**, odegrały znaczącą rolę w rozwoju nauki — przede wszystkim w matematyce, fizyce i astronomii, a ostatnio mają również szerokie zastosowanie w grafice komputerowej.

Nakreślmy teraz najważniejsze idee związane z pojęciem kwaternionów. Nie będziemy podawać formalnej konstrukcji — ograniczymy się jedynie do wymienienia podstawowych własności, które wystarczą do naszych bezpośrednich celów. Podkreślamy tutaj, że takie podejście nie daje nam informacji na temat tego, *czym* tak naprawdę jest kwaternion; niemniej jednak przy definiowaniu jakichkolwiek liczb ważne jest, aby definicja zapewniała nam pożądane własności — kwestia budowy nie odgrywa na ogół żadnej roli. W szczególności, kwaterniony można definiować zarówno jako uporządkowane pary liczb zespolonych, jak i pewne szczególne macierze kwadratowe — w obu przypadkach otrzymujemy **identyczny pod względem własności obiekt**.

Określenie kwaternionu, które przyjmujemy, jest podobne do określenia liczby zespolonej; jak się wkrótce przekonamy, każda liczba zespolona jest kwaternionem.

Określenie 2.1. **Kwaternionem** nazywamy wyrażenie $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, gdzie a, b, c, d są liczbami rzeczywistymi. Zbiór wszystkich kwaternionów oznaczamy symbolem \mathbb{H} .

Określenie 2.2. Niech $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ oraz $\xi' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$. Kwaterniony ξ, ξ' nazywamy **równymi** jeśli $a = a' \wedge b = b' \wedge c = c' \wedge d = d'$.

Wprowadzimy teraz **działanie dodawania i odejmowania kwaternionów**. Są one bardzo podobne do odpowiadających im działań na liczbach zespolonych.

Określenie 2.3. Niech $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ oraz $\xi' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$. **Sumą kwaternionów** ξ, ξ' nazywamy kwaternion $\xi + \xi' := (a + a') + (b + b')\mathbf{i} + (c + c')\mathbf{j} + (d + d')\mathbf{k}$. **Różnicą kwaternionów** ξ, ξ' nazywamy kwaternion $\xi - \xi' := (a - a') + (b - b')\mathbf{i} + (c - c')\mathbf{j} + (d - d')\mathbf{k}$.

Znacznie bardziej złożone jest wprowadzenie **działania mnożenia**. Zanim podamy ogólny sposób mnożenia kwaternionów, zatrzymamy się na

chwile nad określeniem **mnożenia jednostek i, j, k** . Jednostki te są oznaczane **kolejnymi trzema literami alfabetu łacińskiego**. Nie jest to przypadek — przy mnożeniu tych jednostek decydującą rolę odgrywa ich kolejność, częściowo określona przez kolejność alfabetyczną.

Przyjmujemy, że bezpośrednio po i następuje j , a bezpośrednio po j następuje k . Ponadto, dla naszych celów przyjmijmy, że bezpośrednio po k następuje i . Zefiniowaliśmy **quasi-alfabetyczną kolejność**; w przeciwieństwie do „zwykłej” kolejności alfabetycznej, każda jednostka ma jedną następującą bezpośrednio po niej.

... **ijkijkijkijkijkijkijkijk** ...

Jest oczywiste, że w podobny sposób możemy określić **odwrotną kolejność quasi-alfabetyczną**:

... **kjikjikjikjikjikjikjki** ...

Pokażemy teraz, jak powyższe rozważania mają się do **reguł mnożenia jednostek** w kwaternionach. Zauważmy, że iloczyn dwóch jednostek jest jednej z następujących postaci:

1. **Dwie kolejne w sensie kolejności quasi-alfabetycznej jednostki.** Są to iloczyny ij , jk oraz ki . W każdym z tych przypadków wynikiem będzie jednostka następująca bezpośrednio po drugim czynniku. Mówiąc inaczej, wynikiem będzie jednostka, która nie występowała w tym iloczynie. Na tej zasadzie mamy więc: $ij = k$, $jk = i$ oraz $ki = j$.
2. **Dwie kolejne w sensie odwrotnej kolejności quasi-alfabetycznej jednostki.** Są to iloczyny ji , kj oraz ik . W każdym z tych przypadków wynikiem będzie jednostka bezpośrednio poprzedzająca pierwszy czynnik, ale ze znakiem minus. Mówiąc inaczej, wynikiem będzie -1 razy jednostka, która nie występowała w tym iloczynie. Na tej zasadzie mamy więc: $ji = -k$, $kj = -i$ oraz $ik = -j$.
3. **Dwie identyczne jednostki.** Są to iloczyny $ii = i^2$, $jj = j^2$ oraz $kk = k^2$. Każdy z tych iloczynów jest równy -1 . Mamy więc: $i^2 = j^2 = k^2 = -1$.

Określone powyżej reguły nazywamy regułami mnożenia. Żeby pomnożyć dwa dowolne kwaterniony, mnożymy każdy składnik pierwszego przez każdy składnik drugiego i dodajemy wyniki — jak w przypadku mnożenia wielomianów. Następnie, korzystając z reguł mnożenia, zamieniamy wyrażenia w rodzaju $2ji$, $-k^2$, czy $5ki$ na prostsze wyrażenia — w tym przypadku byłyby to odpowiednio: $-2k$, 1 , $5j$. Następnie porządkujemy sumę, doprowadzając ją do postaci $\xi = a + bi + cj + dk$, gdzie $a, b, c, d \in \mathbb{R}$.

Przykład 2.4. $(3 + i - j + 2k)(1 - i + 3j - 2k) = 3(1 - i + 3j - 2k) + i(1 - i + 3j - 2k) - j(1 - i + 3j - 2k) + 2k(1 - i + 3j - 2k) = 3 - 3i + 9j - 6k + i - i^2 + 3ij - 2ik - j + ji - 3j^2 + 2jk + 2k - 2ki + 6kj - 4k^2 = 3 - 3i + 9j - 6k + i + 1 + 3k + 2j - j - k + 3 + 2i + 2k - 2j - 6i + 4 = 11 - 6i + 8j - 2k$

Przykład 2.5. $(i + j)(1 + k) = i(1 + k) + j(1 + k) = i + ik + j + jk = i - j + j + i = 2i$

$(1 + k)(i + j) = i + j + k(i + j) = i + j + ki + kj = i + j + j - i = 2j$

$2i = 0 + 2i + 0j + 0k$

$2j = 0 + 0i + 2j + 0k$

Kwaterniony $2i$ oraz $2j$ różnią się współczynnikami przy jednostce i (jak również przy j), dlatego nie są równe.

$(i + j)(1 + k) \neq (1 + k)(i + j)$

Wniosek 2.6. *Mnożenie kwaternionów nie jest przemienne.*

Uwaga 2.7. Każda liczba rzeczywista x jest kwaternionem: $x = x + 0i + 0j + 0k$.

Każda liczba zespolona z jest kwaternionem: $z = a + bi = a + bi + 0j + 0k$.

$\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$

Definicja 2.8. Kwaternion $\xi = a + bi + cj + dk$, którego wszystkie współczynniki a, b, c, d są liczbami całkowitymi, nazywamy **kwaternionem o współczynnikach całkowitych**. Zbiór wszystkich kwaternionów o współczynnikach całkowitych oznaczamy symbolem $\mathbb{H}(\mathbb{Z})$.

Definicja 2.9. Kwaternion $\xi = a + bi + cj + dk$, którego wszystkie współczynniki a, b, c, d są liczbami wymiernymi, nazywamy **kwaternionem o współczynnikach wymiernych**. Zbiór wszystkich kwaternionów o współczynnikach wymiernych oznaczamy symbolem $\mathbb{H}(\mathbb{Q})$.

Uwaga 2.10. Natychmiast z definicji wynikają dosyć oczywiste inkluzje: $\mathbb{Z} \subseteq \mathbb{H}(\mathbb{Z})$, $\mathbb{Q} \subseteq \mathbb{H}(\mathbb{Q})$ oraz $\mathbb{H}(\mathbb{Z}) \subseteq \mathbb{H}(\mathbb{Q}) \subseteq \mathbb{H}$.

3. Sprzężenie i wartość bezwzględna kwaternionu

Definicja 3.1. **Sprzężeniem kwaternionu** $\xi = a + bi + cj + dk$ nazywamy kwaternion $\xi^* := a - bi - cj - dk$. Kwaternion ξ^* nazywamy kwaternionem sprzężonym z ξ .

Uwaga 3.2. Jeżeli $z = a + bi$, to $z^* = a - bi - 0j - 0k = a - bi = \bar{z}$. Definicja sprzężenia dla kwaternionów jest zatem uogólnieniem definicji sprzężenia liczby zespolonej. W związku z tym, sprzężenie kwaternionu ξ będziemy również oznaczać symbolem $\bar{\xi}$.

Definicja 3.3. **Wartością bezwzględną kwaternionu** $\xi = a + bi + cj + dk$ nazywamy liczbę rzeczywistą $\|\xi\| := \sqrt{a^2 + b^2 + c^2 + d^2}$.

Uwaga 3.4. Jeżeli $x \in \mathbb{R}$, to $x = x+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}$, a więc $\|x\| = \sqrt{x^2 + 3 \cdot 0^2} = \sqrt{x^2} = |x|$.

Jeżeli $z \in \mathbb{C}$, czyli $z = a + b\mathbf{i}$, to $z = a + b\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$, a zatem $\|z\| = \sqrt{a^2 + b^2 + 0^2 + 0^2} = |z|$.

Wynika stąd, że definicja wartości bezwzględnej kwaternionu jest uogólnieniem definicji wartości bezwzględnej liczby rzeczywistej i zespolonej. W związku z tym wartość bezwzględną kwaternionu ξ będziemy oznaczać symbolem $|\xi|$.

Uwaga 3.5. Zbiór wszystkich kwaternionów postaci $x + y\mathbf{i} + z\mathbf{j} + 0\mathbf{k}$ możemy utożsamiać ze zbiorem wszystkich uporządkowanych trójek (x, y, z) o współrzędnych rzeczywistych, a więc również z **przestrzenią trójwymiarową**. $|x + y\mathbf{i} + z\mathbf{j}| = \sqrt{x^2 + y^2 + z^2}$ jest odległością punktu (x, y, z) od początku układu współrzędnych.

Twierdzenie 3.6. Dla każdego kwaternionu ξ prawdziwa jest równość:

$$\xi\bar{\xi} = \bar{\xi}\xi = |\xi|^2$$

Dowód. Niech $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$; $a, b, c, d \in \mathbb{R}$.

$$\bar{\xi} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

$$\begin{aligned} \xi\bar{\xi} &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = a^2 - ab\mathbf{i} - ac\mathbf{j} - ad\mathbf{k} + ab\mathbf{i} - b^2\mathbf{i}^2 - bc\mathbf{ij} - bd\mathbf{ik} + ac\mathbf{j} - bc\mathbf{ji} - c^2\mathbf{j}^2 - cd\mathbf{jk} + ad\mathbf{k} - bd\mathbf{ki} - cd\mathbf{kj} - d^2\mathbf{k}^2 = a^2 - ab\mathbf{i} - ac\mathbf{j} - ad\mathbf{k} + ab\mathbf{i} + b^2 - bck + bd\mathbf{j} + ac\mathbf{j} + bck + c^2 - cdi + ad\mathbf{k} - bd\mathbf{j} + cdi + d^2 = a^2 + b^2 + c^2 + d^2 \\ \bar{\xi}\xi &= (a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = a^2 + ab\mathbf{i} + ac\mathbf{j} + ad\mathbf{k} - ab\mathbf{i} - b^2\mathbf{i}^2 - bc\mathbf{ij} - bd\mathbf{ik} - ac\mathbf{j} - bc\mathbf{ji} - c^2\mathbf{j}^2 - cd\mathbf{jk} - ad\mathbf{k} - bd\mathbf{ki} - cd\mathbf{kj} - d^2\mathbf{k}^2 = a^2 + ab\mathbf{i} + ac\mathbf{j} + ad\mathbf{k} - ab\mathbf{i} + b^2 - bck + bd\mathbf{j} - ac\mathbf{j} + bck + c^2 - cdi - ad\mathbf{k} - bd\mathbf{j} + cdi + d^2 = a^2 + b^2 + c^2 + d^2 \\ |\xi|^2 &= (\sqrt{a^2 + b^2 + c^2 + d^2})^2 = a^2 + b^2 + c^2 + d^2 \quad \square \end{aligned}$$

Twierdzenie 3.7. Dla dowolnych kwaternionów ξ, ξ' prawdziwa jest równość:

$$\overline{\xi \cdot \xi'} = \bar{\xi}' \cdot \bar{\xi}$$

Dowód. Niech $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$; $a, b, c, d \in \mathbb{R}$.

$$\xi' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}; \quad a', b', c', d' \in \mathbb{R}$$

$$\begin{aligned} \xi\xi' &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = aa' + ab'\mathbf{i} + ac'\mathbf{j} + ad'\mathbf{k} + ba'\mathbf{i} + bb'\mathbf{i}^2 + bc'\mathbf{ij} + bd'\mathbf{ik} + ca'\mathbf{j} + cb'\mathbf{ji} + cc'\mathbf{j}^2 + cd'\mathbf{jk} + da'\mathbf{k} + db'\mathbf{ki} + dc'\mathbf{kj} + dd'\mathbf{k}^2 = \\ &= aa' + ab'\mathbf{i} + ac'\mathbf{j} + ad'\mathbf{k} + ba'\mathbf{i} - bb' + bc'\mathbf{k} - bd'\mathbf{j} + ca'\mathbf{j} - cb'\mathbf{k} - cc' + cd'\mathbf{i} + da'\mathbf{k} + db'\mathbf{j} - dc'\mathbf{i} - dd' = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')\mathbf{i} + \\ &+ (ac' - bd' + ca' + db')\mathbf{j} + (ad' + bc' - cb' + da')\mathbf{k} \end{aligned}$$

$$\bar{\xi}' \cdot \bar{\xi} = (aa' - bb' - cc' - dd') + (-ab' - ba' - cd' + dc')\mathbf{i} + (-ac' + bd' - ca' - db')\mathbf{j} + (-ad' - bc' + cb' - da')\mathbf{k}$$

$$\bar{\xi}' = a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k}$$

$$\bar{\xi} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

$$\bar{\xi}' \cdot \bar{\xi} = (a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = aa' - a'b\mathbf{i} - a'c\mathbf{j} - a'd\mathbf{k} - b'ai + b'bi^2 + b'cij + b'dik - c'aj + c'bji + c'cj^2 + c'djk - d'ak + d'bki + d'ckj + d'dk^2 =$$

$$\begin{aligned}
& aa' - ba'\mathbf{i} - ca'\mathbf{j} - da'\mathbf{k} - ab'\mathbf{i} - bb' + cb'\mathbf{k} - db'\mathbf{j} - ac'\mathbf{j} - bc'\mathbf{k} - cc' + dc'\mathbf{i} - \\
& ad'\mathbf{k} + bd'\mathbf{j} - cd'\mathbf{i} - dd' = (aa' - bb' - cc' - dd') + (-ab' - ba' - cd' + dc')\mathbf{i} + \\
& (-ac' + bd' - ca' - db')\mathbf{j} + (-ad' - bc' + cb' - da')\mathbf{k} \\
& \overline{\xi \cdot \xi'} = \overline{\xi'} \cdot \overline{\xi} \quad \square
\end{aligned}$$

Wniosek 3.8. Dla dowolnych kwaternionów ξ, ξ' prawdziwa jest równość:

$$|\xi\xi'|^2 = |\xi|^2|\xi'|^2$$

Dowód. $|\xi\xi'|^2 = \xi\xi'\overline{\xi\xi'} = \xi\xi'\overline{\xi'} \cdot \overline{\xi} = \xi|\xi'|^2\overline{\xi} = |\xi'|^2\xi\overline{\xi} = |\xi'|^2|\xi|^2 = |\xi|^2|\xi'|^2$ \square

4. Tożsamość Eulera

Sformułujemy teraz i udowodnimy jedną z ważniejszych tożsamości w teorii liczb; mianowicie, **tożsamość Eulera**.

Twierdzenie 4.1 (Tożsamość Eulera). Dla dowolnych $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ następująca równość jest prawdziwa: $(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = (aa' + bb' + cc' + dd')^2 + (ab' - ba' - cd' + dc')^2 + (ac' + bd' - ca' - db')^2 + (ad' - bc' + cb' - da')^2$

Dowód. Niech:

$$\xi = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

$$\xi' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$$

$$|\xi|^2|\xi'|^2 = (a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2)$$

$$\begin{aligned}
\xi\xi' &= (a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = aa' + ab'\mathbf{i} + ac'\mathbf{j} + ad'\mathbf{k} - ba'\mathbf{i} - \\
& bb'\mathbf{i}^2 - bc'\mathbf{ij} - bd'\mathbf{ik} - ca'\mathbf{j} - cb'\mathbf{ji} - cc'\mathbf{j}^2 - cd'\mathbf{jk} - da'\mathbf{k} - db'\mathbf{ki} - dc'\mathbf{kj} - dd'\mathbf{k}^2 = \\
& aa' + ab'\mathbf{i} + ac'\mathbf{j} + ad'\mathbf{k} - ba'\mathbf{i} + bb' - bc'\mathbf{k} + bd'\mathbf{j} - ca'\mathbf{j} + cb'\mathbf{k} + cc' - cd'\mathbf{i} - \\
& da'\mathbf{k} - db'\mathbf{j} + dc'\mathbf{i} + dd' = (aa' + bb' + cc' + dd') + (ab' - ba' - cd' + dc')\mathbf{i} + \\
& (ac' + bd' - ca' - db')\mathbf{j} + (ad' - bc' + cb' - da')\mathbf{k}
\end{aligned}$$

$$|\xi\xi'|^2 = (aa' + bb' + cc' + dd')^2 + (ab' - ba' - cd' + dc')^2 + (ac' + bd' - ca' - db')^2 + (ad' - bc' + cb' - da')^2$$

Ale $|\xi|^2|\xi'|^2 = |\xi\xi'|^2$, czyli

$$(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = (aa' + bb' + cc' + dd')^2 + (ab' - ba' - cd' + dc')^2 + (ac' + bd' - ca' - db')^2 + (ad' - bc' + cb' - da')^2 \quad \square$$

Z tożsamości Eulera wynika natychmiast niezwykle istotny wniosek.

Wniosek 4.2. Iloczyn sum czterech kwadratów jest sumą czterech kwadratów.

Kolejny wniosek odegra znaczącą rolę w dowodzie twierdzenia Lagrange'a.

Wniosek 4.3. Twierdzenie Lagrange'a jest równoważne następującemu twierdzeniu: **Każda liczba pierwsza jest sumą czterech kwadratów liczb całkowitych.**

Dowód. Implikacja (\Rightarrow) jest oczywista. Udowodnimy implikację odwrotną. Niech $m \in \mathbb{N}$. Rozważmy trzy możliwości:

1. $m = 1$

Wtedy $m = 1^2 + 0^2 + 0^2 + 0^2$.

2. $m \in \mathbb{P}$

Wtedy m jest sumą czterech kwadratów z założenia.

3. m jest liczbą złożoną.

$$m = p_1^{\alpha_1} \dots p_n^{\alpha_n}; p_1, \dots, p_n \in \mathbb{P}; \alpha_1, \dots, \alpha_n \in \mathbb{N}$$

Z założenia:

$$p_1 = a_1^2 + b_1^2 + c_1^2 + d_1^2; a_1, b_1, c_1, d_1 \in \mathbb{Z}$$

\vdots

$$p_n = a_n^2 + b_n^2 + c_n^2 + d_n^2; a_n, b_n, c_n, d_n \in \mathbb{Z}$$

Zatem:

$$m = (a_1^2 + b_1^2 + c_1^2 + d_1^2)^{\alpha_1} \dots (a_n^2 + b_n^2 + c_n^2 + d_n^2)^{\alpha_n}$$

Ale iloczyn sum czterech kwadratów jest sumą czterech kwadratów.

Wynika stąd, że m jest sumą czterech kwadratów.

□