# Rzędy, Generatory i nie tylko

Antoni Łuczak

## 1 Rzędy

**Definicja 1** *Rzędem elementu a modulo m* nazwiemy taką najmniejszą liczbę naturalną $\mathrm{ord}_m(a)$, że

$$a^{\mathrm{ord}_m(a)} \equiv_m 1.$$

Dzięki twierdzeniu Eulera taka liczba istnieje.

Kilka fakcików:

- $m \mid a^k - 1 \iff \mathrm{ord}_m(a) \mid k$
- $\mathrm{ord}_m(a) \mid \varphi(m)$
- $a^x \equiv_m a^y \iff x \equiv_{\mathrm{ord}_m(a)} y$
- $m \mid n \implies \mathrm{ord}_m(a) \mid \mathrm{ord}_n(a)$
- $\mathrm{ord}_m(a^k) = \frac{\mathrm{ord}_m(a)}{\mathrm{NWD}(k, \mathrm{ord}_m(a))}$
- $\mathrm{ord}_m(a) \perp \mathrm{ord}_m(b) \implies \mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$

Pracując z rzędami warto rozpatrywać szczególne dzielniki pierwsze (np. najmniejsze). Warto też korzystać z faktu, że jeśli rząd modulo $m$ dzieli jakieś $n$, to rząd ten dzieli też $\mathrm{NWD}(n, \varphi(m))$. To często pozwala dobrze oszacować wielkość rzędu, co później pozwala ograniczyć zadanie do szczególnych przypadków. Tę technikę można wykorzystać w rozwiązaniu zadania 1. Warto też pamiętać o technikach takich jak sprawdzanie modulo, czy LTE.

**Zadania:**

1. Wyznaczyć wszystkie takie liczby naturalne $n$, że $n \mid 2^n - 1$.

2. Niech $p$ będzie liczbą pierwszą. Udowodnić, że wszystkie różne od 1 dzielniki liczby $2^p - 1$ są większe od $p$.

3. Udowodnij, że każdy dzielnik liczby $a^{2^n} + 1$ jest postaci $k \cdot 2^{n+1} + 1$

4. (OM) Udowodnić, że jeśli $k, n$ są liczbami naturalnymi, to nie istnieją takie liczby naturalne $a, b$, że

$$k \mid 2^a - 1, 2^b + 1 \text{ oraz } n \mid 2^a + 1, 2^b - 1$$

5. (Finał 54 OM zad 3) Wyznaczyć wszystkie wielomiany $W$ o współczynnikach całkowitych spełniające następujący warunek: Dla każdej liczby naturalnej $n$ liczba $2^n - 1$ jest podzielna przez $W(n)$.

6. Niech $p$ będzie liczbą pierwszą oraz $n$ liczbą naturalną. Załóżmy, że $2^n - 1$ jest podzielne przez $p$, ale nie przez $p^2$. Pokazać, że $2^{p-1} - 1$ jest podzielne przez $p$, ale nie przez $p^2$.

7. Znaleźć wszystkie takie liczby naturalne $n$, że

$$n^2 \mid 3^n + 1.$$

8 (IMO 1999). Znaleźć wszystkie takie liczby naturalne $n$, że

$$n^2 \mid 2^n + 1.$$

# 2 Generatory

**Definicja 2** *Generatorem modulo* $m$ nazywamy taką liczbę $g \perp m$, że $\mathrm{ord}_m(g) = \varphi(m)$. Innymi słowy potęgi generatora modulo $m$ (od $g^1$ do $g^{\varphi(m)}$) *generują* wszystkie reszty modulo $m$ względnie pierwsze z $m$.

**Twierdzenie 1** Generator modulo $m$ istnieje w następujących przypadkach:

$$m = 1,\ 2,\ 4,\ p^k,\ 2p^k$$

gdzie $p$ to nieparzysta liczba pierwsza, a $k$ to dowolna liczba naturalna.

**Zadania:**

1. Dana jest nieparzysta liczba pierwsza $p$ oraz liczba całkowita $k$, przy czym $p - 1$ nie dzieli $k$, pokazać, że

$$1^k + 2^k + \cdots + (p-1)^k \equiv_p 0$$

2. Pokazać, że jeśli istnieje generator modulo $m$, to elementów rzędu $k$ jest dokładnie $\varphi(k)$.

3. Kryterium Eulera: Dana jest nieparzysta liczba pierwsza $p$. Pokazać, że kongruencja $x \equiv_p a^2$ ma rozwiązanie wtedy i tylko wtedy gdy $x^{\frac{p-1}{2}} \equiv_p 1$.

4. Dana jest liczba naturalna $n$. Pokazać, że

$$n \mid 3^n + 4^n \implies 7 \mid n.$$

5. Udowodnić, że istnieje nieskończenie wiele takich liczb naturalnych $n$, że największy dzielnik pierwszy liczby $n^4 + 1$ jest większy od $2n$.

6. Udowodnić, że liczby

$$1^k,\ 2^k,\ \ldots,\ (p-1)^k$$

generują $\frac{p-1}{\mathrm{NWD}(k,p-1)}$ niezerowych reszt modulo $p$.

# 3 Dodatek: Wielomiany cyklotomiczne

W tej sekcji rozwiążemy problem rozkładu wielomianu $X^n - 1$ w $\mathbb{Z}[X]$.

**Definicja 3** Liczbę zespoloną $z$ nazwiemy *$n$-tym pierwotnym pierwiastkiem z jedności*, jeśli $z^n = 1$, ale $z^k \neq 1$ dla $1 \leqslant k \leqslant n$.

**Ćwiczenie 1** Niech $\zeta = e^{\frac{2\pi i}{n}}$. Pokazać, że $n$-te pierwotne pierwiastki z jedności to dokładnie liczby $\zeta^k$ dla $1 \leqslant k \leqslant n, k \perp n$.

**Definicja 4** *$n$-tym wielomianem cyklotomicznym* nazywamy wielomian

$$\Phi_n(X) = \prod_{k \perp n} (X - \zeta^k).$$

**Przykład:**

$$\Phi_1(X) = X - 1,\ \Phi_2(X) = X + 1,\ \Phi_3(X) = X^2 + X + 1,\ \Phi_4(X) = X^2 + 1$$

**Twierdzenie 2** Dla dowolnego naturalnego $n$, $\Phi_n$ ma współczynniki całkowite oraz jest nierozkładalny w $\mathbb{Z}[X]$.

**Twierdzenie 3** Dla dowolnego naturalnego $n$

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Niech $\mu(n)$ oznacza funkcję Möbiusa

$$\mu(n) = \begin{cases} 0, \text{ jeśli } n \text{ jest podzielne przez kwadrat} \\ (-1)^{\omega(n)} \text{ w przeciwnym przypadku} \end{cases}$$

gdzie $\omega(n)$ oznacza liczbę dzielników liczby $n$. Wtedy

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}.$$

**Twierdzenie 4** Niech $p$ będzie liczbą pierwszą, $n$ liczbą naturalną, $a$ liczbą całkowitą. Załóżmy, że

$$\Phi_n(a) \equiv_p 0$$

Wtedy $p|n$ lub $\mathrm{ord}_p(a) = n$.

**Przykład (Słaby Dirichlet):** niech $a$ będzie liczbą naturalną. Udowodnić, że w ciągu arytmetycznym $an + 1$ jest nieskończenie wiele liczb pierwszych.

*Dowód:* Załóżmy, że ciąg ten zawiera jedynie skończenie wiele liczb pierwszych, nazwijmy je $p_1, \ldots, p_k$. Rozważmy liczbę

$$K = \Phi_a(ap_1 \cdots p_k)$$

(w przypadku gdy w ciągu nie ma liczb pierwszych bierzemy $K = \Phi_a(a)$). Niech $p$ będzie dowolnym dzielnikiem pierwszym liczby $K$. Oczywiście Wyraz wolny $\Phi_a$ jest równy $\pm 1$, zatem $p$ nie dzieli

$ap_1 \cdots p_k$. Z twierdzenia wiemy, że $a = \mathrm{ord}_p(ap_1 \cdots p_k) \mid p-1 \implies p = an+1$ dla pewnego $n \in \mathbb{N}$. Otrzymaliśmy nową liczbę pierwszą w naszym ciągu, co oznacza sprzeczność.

Innym ważnym faktem, który da się udowodnić za pomocą wielomianów cyklotomicznych jest następujące twierdzenie:

**Twierdzenie Zsigmondy'ego:** Niech $a > b$ będą względnie pierwszymi liczbami naturalnymi. Wówczas dla każdego naturalnego $n$, $a^n - b^n$ posiada taki dzielnik pierwszy $p$, że $\forall_{0<k<n}\ p \nmid a^k - b^k$. Twierdzenie nie działa w następujących przypadkach:

- $a = 2,\ b = 1,\ n = 6$
- $n = 2$ oraz $a + b$ jest potęgą dwójki

Takie dzielniki pierwsze $p$ nazwiemy dzielnikami pierwotnymi liczby $a^n - b^n$.

**Twierdzenie (Wersja plusowa):** Twierdzenie Zsigmondy'ego działa nawet jeśli $a^n - b^n, a^k - b^k$ zamienimy na $a^n + b^n, a^k + b^k$. Ten wariant przestaje działać wtedy i tylko wtedy gdy $a = 2, b = 1, n = 3$.

**Przykład (OM):** Dane są różne liczby pierwsze $p, q$ większe od 2. Udowodnić, że liczba $2^{pq} - 1$ ma co najmniej 3 różne dzielniki pierwsze.

*Dowód:* Z twierdzenia Zsigmondy'ego dla $2^p - 1, 2^q - 1, 2^{pq} - 1$ dostajemy, że każda z tych liczb posiada pierwotny dzielnik pierwszy. Jednak $2^p - 1, 2^q - 1$ są dzielnikami $2^{pq} - 1$ - koniec. Czytelnik powinien sprawdzić, że w każdym z tych przypadków twierdzenie Zsigmondy'ego zadziała.

Jak zaraz zobaczymy, Twierdzenie Zsigmondy'ego trywializuje wiele dość ciężkich zadań.

**Zadania:**

1. Dane są liczby naturalne $a > 1, m \neq n$. Udowodnić, że jeśli liczby $a^m - 1, a^n - 1$ posiadają dokładnie te same dzielniki pierwsze, to $a + 1$ jest potęgą 2.

2. Pokazać, że nie istnieją takie liczby naturalne $x^{2009} + y^{2009} = 7^z$.

3. (ISL 2000 N4) Znaleźć wszystkie trójki liczb naturalnych $(a, m, n)$ spełniające

$$a^m + 1 \mid (a+1)^n$$

4. (IMO 2000 P5) Rozstrzygnąć czy istnieje taka liczba naturalna $n$, że $n$ ma dokładnie 2000 parami różnych dzielników pierwszych oraz $n \mid 2^n + 1$.

5. Niech $p_1, p_2, \ldots, p_n$ będą parami różnymi liczba mi pierwszymi większymi od 3. Udowodnij, że liczba $2^{p_1 \cdots p_n} + 1$ ma co najmniej $2^{2^n}$ dzielników.

6. Rozwiązać równanie

$$x^n + y^n = p^n,$$

gdzie $x, y, n$ są liczbami naturalnymi, a $p$ jest liczbą pierwszą (bez WTF).

# 4 Rozwiązania

## 4.1 Rzędy

1. Niech $p$ to najmniejszy dzielnik pierwszy liczby $n$. Wtedy $p \mid 2^n - 1 \implies \mathrm{ord}_p(2) \mid n \implies \mathrm{ord}_p(2) \mid \mathrm{NWD}(n, p-1) = 1$, czyli $\mathrm{ord}_p(2) = 1$, co nie jest możliwe.

2. Niech $q$ to najmniejszy dzielnik pierwszy liczby $2^p - 1$. Mamy $\mathrm{ord}_q(2) \mid p$, więc korzystając z faktu, że $\mathrm{ord}_q(2) \neq 1$ dostajemy $\mathrm{ord}_q(2) = p$. Mamy zatem $p \mid \varphi(q) \implies p \leqslant \varphi(q) < q$. Skoro najmniejszy dzielnik liczby $2^p - 1$ jest większy od $p$, to każdy jej dzielnik jest większy od $p$.

3. Tezę wystarczy pokazać dla dzielników pierwszych. Niech $p \mid a^{2^n} + 1$ będzie liczbą pierwszą. Mamy $p \mid a^{2^{n+1}} - 1$, czyli $\mathrm{ord}_p(a) \mid 2^{n+1}$, ale $\mathrm{ord}_p(a)$ nie dzieli $2^n$. To oznacza, że $\mathrm{ord}_p(a) = 2^{n+1} \implies 2^{n+1} \mid p - 1 \implies p = k \cdot 2^{n+1} + 1$.

4. Załóżmy, że takie $k, n$ istnieją. Wtedy $\mathrm{ord}_k(2) \mid 2b$, ale $\mathrm{ord}_k(2) \nmid b$, czyli $v_2(\mathrm{ord}_k(2)) = v_2(b) + 1$. Ponadto $\mathrm{ord}_k(2) \mid a$, czyli $v_2(b) + 1 = v_2(\mathrm{ord}_k(2)) \leqslant v_2(a)$. Jeżeli jednak zrobimy to samo dla $n$, to dostaniemy $v_2(a) + 1 \leqslant v_2(b)$ - sprzeczność.

5. Zauważmy, że $p \mid W(n) \implies p \mid W(n+p)$, czyli $p \mid 2^n - 1,\ 2^{n+p} - 1 \implies \mathrm{ord}_p(2) \mid n,\ n+p \implies \mathrm{ord}_p(2) \mid p \implies \mathrm{ord}_p(2) \mid \mathrm{NWD}(p, p-1) = 1$. To oznacza, że jedynymie wielomianami spełniającymi warunki zadania są $W(x) \equiv \pm 1$.

6. Niech $m = \mathrm{ord}_p(2)$. Mamy $p \mid 2^m - 1 \mid 2^n - 1$, czyli $p^2$ nie dzieli $2^m - 1$. Oczywiście $m \mid p - 1 \implies 2^m - 1 \mid 2^{p-1} - 1$. Mamy zatem

$$\frac{2^{p-1} - 1}{2^m - 1} = 1 + 2^m + (2^m)^2 + \cdots + (2^m)^{\frac{p-1}{m} - 1} \equiv_p 1 + 1 + \cdots + 1 \equiv \frac{p-1}{m},$$

czyli $2^{p-1} - 1$ jest podzielne przez $p$ ale nie przez $p^2$.

7. Gdyby $n$ było parzyste, to $4 \mid 3^n + 1 \equiv_4 2$, co nie jest możliwe. Pokażemy, że dla nieparzystego $n > 1$ podzielność

$$n \mid 3^n + 1$$

nie może zajść. Załóżmy, że jest inaczej i niech $p$ to najmniejszy dzielnik pierwszy liczby $n$. Wtedy $p \mid 3^{2n} - 1 \implies \mathrm{ord}_p(3) \mid \mathrm{NWD}(2n, p-1) = 2$. To oznacza, że $p \mid 3^2 - 1 = 8 \implies p = 2$, co nie jest możliwe. W takim razie jedynym rozwiązaniem jest $n = 1$.

8. Oczywiście $n = 1$ spełnia warunki zadania. Załóżmy, że $n > 1$ oraz niech $p$ to najmniejszy dzielnik pierwszy liczby $n$. Mamy $p \mid 2^{2n} - 1 \implies \mathrm{ord}_p(2) \mid 2n \implies \mathrm{ord}_p(2) \mid \mathrm{NWD}(2n, p-1) = 2$. Mamy zatem $p \mid 2^2 - 1 = 3 \implies p = 3$. Oczywiście $n$ jest nieparzyste, więc możemy zastosować LTE

$$v_3(2^n + 1) = v_3(n) + 1.$$

Skoro $n^2 \mid 2^n + 1$, to $2v_3(n) \leqslant v_3(n) + 1 \implies v_3(n) = 1$. Niech $q$ to drugi najmniejszy dzielnik pierwszy liczby $n$. Podobnie $\mathrm{ord}_q(2) \mid \mathrm{NWD}(2n, q-1) \leqslant 6$. Skoro $q \neq 3$, to $\mathrm{ord}_q(2) = 6 \implies q \mid 2^6 - 1 = 63 \implies q = 7$. Zauważmy jednak, że $2^3 \equiv_7 1 \implies (2^3)^{\frac{n}{3}} + 1 \equiv_7 2$, co nie jest możliwe. To oznacza, że $q$ nie istnieje, czyli $n = 3$. Łatwo zauważyć, że takie $n$ spełnia warunki zadania.

## 4.2 Generatory

1. Niech $g$ będzie generatorem modulo $p$. Niech ponadto $1 = g^{\alpha_1}, \ldots, p-1 = g^{\alpha_{p-1}}$. Zauważmy, że $g^{kx} \equiv_p g^{ky} \iff kx \equiv_{p-1} ky \iff x \equiv_{p-1} y$, ponieważ $p-1$ nie dzieli $k$. To oznacza, że $g^{k\alpha_1}, \ldots, g^{k\alpha_{p-1}}$ jest permutacją reszt $g^{\alpha_1}, \ldots, g^{\alpha_{p-1}}$. Możemy zatem napisać

$$\sum_{i=1}^{p-1} i^k = \sum_{i=1}^{p-1} g^{k\alpha_i} \equiv_p \sum_{i=1}^{p-1} g^{\alpha_i} \equiv_p \sum_{i=1}^{p-1} i \equiv_p \frac{p(p-1)}{2} \equiv_p 0.$$

2. Niech $a$ będzie dowolnym elementem rzędu $k$. Zapiszmy $a = g^{\frac{\varphi(m)x}{k}}$. Gdyby $d = \mathrm{NWD}(k,x) \neq 1$, to $a^{\frac{k}{d}} \equiv_p 1$, co nie jest możliwe. Mamy zatem $x \perp k$. Takich liczb $x$ mniejszych od $k$ jest $\varphi(k)$, zatem dokładnie tyle jest elementów rzędu $k$.

3. Jeżeli $x \equiv_p a^2$, to $x^{\frac{p-1}{2}} \equiv_p a^{p-1} \equiv 1$. Niech $x^{\frac{p-1}{2}} \equiv_p 1$. Zapiszmy $x = g^y$. Wtedy $g^{\frac{y(p-1)}{2}} \equiv_p 1 \implies p-1 \mid \frac{y(p-1)}{2} \implies 2 \mid y \implies x \equiv_p (g^{\frac{y}{2}})^2$.

4. Niech $p$ to najmniejszy dzielnik pierwszy liczby $n$. Niech $g$ będzie generatorem modulo $p$ oraz niech $3 \equiv_p g^a,\ 4 \equiv_p g^b$ dla pewnych naturalnych $a, b < p-1$. Wtedy $g^{an} \equiv_p -g^{bn} \implies g^{2n|a-b|} \equiv_p 1$. To oznacza że $p-1 \mid 2n|a-b|$. Skoro $p$ to najmniejszy dzielnik $n$, to $\mathrm{NWD}(n, p-1) = 1 \implies p-1 \mid 2|a-b|$. Skoro $a \neq b$ oraz $2|a-b| < 2(p-1)$, to $a = b \pm \frac{p-1}{2}$. Mamy zatem $3 \equiv_p g^a \equiv_p g^b g^{\pm\frac{p-1}{2}} = 4g^{\frac{p-1}{2}} \equiv_p -4$. Dostaliśmy $p \mid 7 \implies p = 7$, co kończy dowód.

5. Niech $p$ będzie taką liczbą pierwszą, że $8 \mid p-1$ (takich liczb jest nieskończenie wiele z twierdzenia Dirichleta). Niech $g$ to generator modulo $p$. Niech $k \equiv_p g^{\frac{p-1}{8}}$. Skoro $g$ jest generatorem, to $g^{\frac{p-1}{2}} \equiv_p -1$, czyli $p \mid k^4 + 1$. Zauważmy, że jedna z liczb $k, p-k$ jest mniejsza od $\frac{p}{2}$, czyli istnieje takie $n$, że $p \mid n^4 + 1$ oraz $p > 2n$.

6. Niech $g$ będzie generatorem modulo $p$. Zauważmy, że

$$g^{kx} \equiv_p g^{lx} \iff kx \equiv_{p-1} lx \iff k \equiv_{\frac{p-1}{\mathrm{NWD}(k,p-1)}} l.$$

Liczby $1^k, \ldots, (p-1)^k$ generują te same reszty co $g^k, \ldots, g^{(p-1)k}$, czyli $\frac{p-1}{\mathrm{NWD}(k,p-1)}$ reszt.

## 4.3 Zsigmondy

1. Bez straty ogólności niech $m > n$. Przypadek gdy $m = 6$ sprawdzamy ręcznie. Załóżmy teraz, że $m \neq 6$ oraz $a+1$ nie jest potęgą 2. Wtedy $2^m - 1$ posiada dzielnik pierwotny, który nie dzieli $2^n - 1$ - sprzeczność.

2. Skoro 2009 dzieli się przez 7, to $x^7 + y^7 \mid x^{2009} + y^{2009}$. Jednak z twierdzenia Zsigmondy'ego $x^{2009} + y^{2009}$ posiada dzielnik pierwotny, który nie jest dzielnikiem $x^7 + y^7$, co nie jest możliwe, gdyż obie te liczby są potęgami siódemki.

3. Oczywiście trójki $(a, 1, n),\ (1, m, n)$ spełniają warunki zadania. Trójka $(2, 3, n)$ również spełnia warunki zadania dla $n \geqslant 2$. Teraz twierdzenie Zsigmondy'ego mówi nam, że jeśli $(a, m, n)$ nie jest żadną z powyższych trójek, to $a^m + 1$ posiada dzielnik pierwotny, który nie dzieli $a + 1$.

4. liczbę $n$ nazwiemy *kociarską*, jeśli $n \mid 2^n + 1$. Pokażemy indukcyjnie, że dla dowolnego $k \geqslant 9$ istnieje liczba kociarska posiadająca dokładnie $k$ różnych dzielników pierwszych. Zauważmy, że 9 jest kociarska. Teraz załóżmy, że liczba $n \geqslant 9$ posiada dokładnie $k$ różnych dzielników pierwszych oraz jest kociarska. Na mocy twierdzenia Zsigmondy'ego $2^{2n} - 1$ posiada dzielnik pierwotny $p$. Skoro $\varphi(n) < 2n$, to $p$ nie dzieli $2^{\varphi(n)} - 1$, czyli $p$ nie dzieli $n$. Skoro $p$ dzieli $2^{2n} - 1$, ale nie dzieli już $2^n - 1$, to musi dzielić $2^n + 1$. Mamy zatem

$$pn \mid 2^n + 1 \mid 2^{np} + 1,$$

czyli liczba $pn$ jest kociarska oraz posiada dokładnie $k + 1$ dzielników pierwszych, co kończy dowód indukcyjny.

5. Liczby $p_1, \ldots, p_n$ są większe od 3, więc dla każdej z liczb

$$2^{p_1} + 1, \ldots, 2^{p_n} + 1, 2^{p_1 p_2} + 1, \ldots, 2^{p_{n-1} p_n} + 1, \ldots, 2^{p_1 \cdots p_n} + 1$$

Możemy zastosować twierdzenie Zsigmondy'ego. Skoro każda z tych liczb posiada dzielnik pierwotny oraz jest dzielnikiem $2^{p_1 \cdots p_n} + 1$, to $2^{p_1 \cdots p_n} + 1$ posiada co najmniej $2^n$ dzielników pierwszych, czyli posiada co najmniej $2^{2^n}$ dzielników naturalnych.

6. Zauważmy, że dla $n = 1$ wystarczy wybrać $y = p - x$ dla $x \in \mathbb{N}, 1 \leqslant x < p$. Przypadek $x = 2, y = 1, n = 3$ łatwo wykluczyć, gdyż wtedy $p^3 = 9$, co nie jest możliwe. Załóżmy teraz, że $n > 1$ oraz $n$ posiada nieparzysty dzielnik $d$. Wtedy $x^d + y^d \mid x^n + y^n$, zatem $x^d + y^d$ jest potęgą liczby $p$. Jednak na mocy twierdzenia Zsigmondy'ego $x^n + y^n$ posiada dzielnik, który nie dzieli $x^d + y^d$, co nie jest możliwe. To oznacza, że $n = 2^k$ dla pewnego naturalnego $k$. Jeżeli $k \geqslant 2$ to chcemy rozwiązać równanie postaci

$$(x^{\frac{n}{4}})^4 + (y^{\frac{n}{4}})^4 = (p^{\frac{n}{2}})^2.$$

Pokażemy, że równanie

$$a^4 + b^4 = c^2$$

nie ma rozwiązania w liczbach naturalnych. Załóżmy nie wprost, że $a, b, c$ spełniają to równanie i załóżmy, że $c$ jest minimalne. Wtedy $a, b, c$ są parami względnie pierwsze i $(a^2, b^2, c)$ jest pierwotną trójką pitagorejską, zatem możemy zapisać (ewentualnie zamieniając $a, b$ miejscami)

$$a^2 = m^2 - n^2,\ b^2 = 2mn,\ c = m^2 + n^2$$

Dla względnie pierwszych $m, n$. Z pierwszego równania dostajemy, że $(a, n, m)$ również jest pierwotną trójką pitagorejską, czyli możemy zapisać

$$a = r^2 - s^2,\ n = 2rs,\ m = r^2 + s^2$$

dla względnie pierwszych $r, s$. To w szczególności oznacza, że $m, r, s$ są parami względnie pierwsze. Jednak $b^2 = 2mn = 4mrs$, czyli $m = c_1^2,\ r = a_1^2,\ s = b_1^2$ dla pewnych liczb naturalnych $a_1, b_1, c_1$. Jednak wstawiając to do równania $m = r^2 + s^2$ dostajemy

$$a_1^4 + b_1^4 = c_1^2.$$

Jednak $c_1 < c$, co przeczy minimalności $c$. To oznacza, że $n = 2$, czyli szukamy rozwiązań równania

$$x^2 + y^2 = p^2.$$

Oczywiście $x, y, p$ są parami względnie pierwsze, zatem (ewentualnie zamieniając $x, y$ miejscami)

$$x = m^2 - n^2,\ y = 2mn,\ p = m^2 + n^2.$$

Jak dobrze wiadomo liczbę pierwszą da się zapisać jako sumę kwadratów wtedy i tylko wtedy gdy daje ona resztę 1 z dzielenia przez 4. Dodatkowo taki zapis jest unikalny z dokładnością do znaku oraz kolejności liczb $m, n$. Podsumowując jedynymi rozwiązaniami są

$$(n, x, y, p) = (1, x, p - x, p),\ (2, m^2 - n^2, 2mn, m^2 + n^2),\ (2, 2mn, m^2 - n^2, m^2 + n^2)$$