1 Sumy kwadratów

Bartłomiej Błoniarz

1.1 Teoria

Definicja 1.1 (Tożsamość Brahmagupty)

$$(x^2 + cy^2)(u^2 + cv^2) = (xu \pm cyv)^2 + c(xv \mp yu)^2,$$

Dla $c = 1$ jest to tożsamość Fibonacci'ego.

Dowód $(x^2+cy^2)(u^2+cv^2) = x^2u^2+x^2cv^2+cy^2u^2+c^2y^2v^2 = x^2u^2 \pm 2xucyv + c^2y^2v^2 + x^2cv^2 \mp 2xucyv + cy^2u^2 = (xu \pm cyv)^2 + c(x^2v^2 \mp 2xvyu + y^2u^2) = (xu \pm cyv)^2 + c(xv \mp yu)^2$

□

Definicja 1.2 (Zbiór $\mathcal{W}_{(a,b,c)}$)

$$\mathcal{W}_{(a,b,c)} = \{ax^2 + bxy + cy^2 : a, b, c, x, y \in \mathbb{Z}\}$$

$$\mathcal{W}_{(1,0,c)} = \{x^2 + cy^2 : c, x, y \in \mathbb{Z}\}$$

Definicja 1.3 (Multiplikatywna zamkniętość zbioru $\mathcal{W}_{(1,0,c)}$)

$$m \in \mathcal{W}_{(1,0,c)} \wedge n \in \mathcal{W}_{(1,0,c)} \implies m \cdot n \in \mathcal{W}_{(1,0,c)}$$

Wynika z tożsamości Brahmagupty.

Twierdzenie 1.1 (Twierdzenie Dirichlet'a o aproksymacji) *Dana jest liczba rzeczywista α i liczba naturalna N. Wtedy istnieje taki mianownik k, że $1 \leqslant k \leqslant N$ oraz*

$$\left|\alpha - \frac{h}{k}\right| \leqslant \frac{1}{k(N+1)}$$

dla odpowiednio dobranego licznika $h \in \mathbb{Z}$

Lemat 1.1
Jeżeli $n, a, b \in \mathbb{N}$, $\mathrm{NWD}(a, b) = 1$ oraz $n \mid a^2 + b^2$, to istnieją takie liczby całkowite x, y, że $n = x^2 + y^2$.

Dowód Udowodnimy to najpierw w przypadku, gdy $b = 1$. Zastosujemy w tym celu Twierdzenie Dirichlet'a o aproksymacji do liczb $\alpha = \frac{a}{n}$ i $N = \lfloor\sqrt{n}\rfloor$. Znajdziemy wówczas takie h, k, że

$$\left|\frac{a}{n} - \frac{h}{k}\right| \leqslant \frac{1}{k(N+1)} \text{ oraz } k \leqslant N. \tag{1}$$

Twierdzimy, że $x = ak - nh$ i $y = k$ są dobre. Aby to sprawdzić pokażemy $x^2 + y^2$ jest niezerową wielokrotnością liczby n mniejszą niż $2n$. To, oczywiście, skończy dowód w przypadku $b = 1$. Mamy

$$x^2+y^2 = (ak-nh)^2+k^2 = a^2k^2-2ahkn+n^2h^2+k^2 = k^2(a^2+1)+n(nh^2-2ahk).$$

Założenie $n|a^2+1$ daje $n|x^2+y^2$. Z drugiej strony mnożąc nierówność (1) przez nk i podnosząc do kwadratu dostajemy

$$x^2 = |ak-nh|^2 \leqslant \left(\frac{n}{N+1}\right)^2 < n$$

Ostatnia nierówność wynika z oczywistej nierówności $n < (N+1)^2$. Ponadto, ponieważ $1 \leqslant k \leqslant N$, więc $y^2 = k^2 \leqslant N^2 = \lfloor\sqrt{n}\rfloor^2 \leqslant \sqrt{n}^2 = n$. Zatem $0 < x^2 + y^2 < 2n$.

Jeżeli $b \neq 1$, to dobieramy takie $u, v \in \mathbb{Z}$ by $au + bv = 1$. Wówczas, na mocy tożsamości Fibonacci'ego:

$$(a^2+b^2)(u^2+v^2) = (av-bu)^2+(au+bv)^2 = A^2+1.$$

Zatem $n|A^2+1$, więc n jest sumą dwóch kwadratów.

□

Lemat 1.2 *Jeżeli liczba pierwsza $p \equiv 1 \pmod 4$, to istnieje $0 < m < p$ i takie liczby $x, y \in \mathbb{Z}$, że $x^2 + y^2 = mp$.*

Dowód Z twierdzenia Wilsona mamy:

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

Widzimy stąd, że jeżeli $p \equiv 1 \pmod 4$, to istnieje taka $a \in \mathbb{Z}$, że $a^2 \equiv -1 \pmod p$, czyli $a^2 + 1 = sp$ dla pewnego $s \in \mathbb{N}$. Wybierzmy takie x, by $a \equiv x \pmod p$ i by $|x| < \frac{p}{2}$. Wówczas $x^2 + 1 = mp$ dla pewnej liczby naturalnej m. Ponadto $mp = x^2 + 1 < \left(\frac{p}{2}\right)^2 + 1 < p^2$. Stąd $0 < m < p$. Wystarczy teraz przyjąć y=1.

□

Twierdzenie 1.2 (Twierdzenie Thue'go) *Jeżeli $m \geqslant 2$ jest liczbą naturalną i liczba całkowita a jest względnie pierwsza z m, to istnieją różne od zera liczby całkowite x, y spełniające warunki:*

$$x \equiv ay \pmod m \qquad \textit{oraz} \qquad |x|, |y| \leqslant \sqrt{m}.$$

Dowód Niech $A = \lfloor\sqrt{m}\rfloor$. Rozważmy dowolnie ustawione w ciąg liczby $x + ay$, gdzie x i y przebiegają zbiór $\{0, 1, \ldots, A\}$. Ponieważ w tym ciągu jest $(A+1)^2$

wyrazów, a $(A+1)^2 > m$, to możemy wybrać dwa różne wyrazy dające tę samą resztę z dzielenia przez m. Niech to będą $x_1 + ay_1$ i $x_2 + ay_2$. Wówczas,

$$(x_1 - x_2) + a(y_1 - y_2) \equiv 0 \pmod{m}. \tag{2}$$

Ponieważ $0 \leqslant x_1, x_2 \leqslant A$, więc $|x_1 - x_2| \leqslant A \leqslant \sqrt{m}$. Podobnie, $|y_1 - y_2| \leqslant \sqrt{m}$. Kładziemy $x = x_1 - x_2$, $y = y_2 - y_1$. Pozostaje nam sprawdzić, że $x \neq 0$ i $y \neq 0$. Otóż, gdyby y=0, to, wobec (2), mielibyśmy $m \mid x_1 - x_2$. Jednocześnie $|x_1 - x_2| \leqslant \sqrt{m} < m$. Stąd $x_1 - x_2 = 0$, więc $(x_1, y_1) = (x_2, y_2)$ wbrew dokonanemu wyborowi różnych wyrazów ciągu. Gdyby zaś $x_1 = x_2$, to kongruencja (2) dałaby $m \mid a(y_1 - y_2)$. W takim przypadku założona względna pierwszość m i a oraz ZTA dają podzielność $m \mid y_1 - y_2$, która, tak jak przed chwilą, prowadzi do równości $y_1 = y_2$. Uzyskane sprzeczności dowodzą, że $x \neq 0$ i $y \neq 0$.

□

Twierdzenie 1.3 *Jeżeli p jest liczbą pierwszą, $p \nmid c$ i $p \in \mathcal{W}_{(1,0,c)}$, to liczba $(-c)$ jest resztą kwadratową modulo p.*

Dowód Z założenia wiemy, że istnieją takie $x, y \in \mathbb{Z}$, że $x^2 + cy^2 = p$. Oznacza to, że $x^2 + cy^2 \equiv 0 \pmod{p}$. Załóżmy, że $p|y$, z czego wynika, że $p|x$. Oznaczałoby to, że $p^2|x^2 + cy^2 = p$, co jest niemożliwe. Oznacza to, że $p \nmid y$. Możemy więc przez u oznaczyć odwrotność y modulo p. Mnożymy kongruencję $x^2 \equiv -cy^2 \pmod{p}$ przez u^2. Wtedy $(xu)^2 \equiv -c \pmod{p}$.

□

Twierdzenie 1.4 *Jeżeli liczba naturalna n jest dzielnikiem liczby*

$$34x^2 - 42xy + 13y^2,$$

gdzie $x, y \in \mathbb{Z}$ są względnie pierwsze, to n jest sumą dwóch kwadratów (liczb całkowitych).

Dowód Zauważmy, że $34x^2 - 42xy + 13y^2 = (5x - 3y)^2 + (3x - 2y)^2$. Powołując się na L1 otrzymujemy tezę.

□

Twierdzenie 1.5 *Jeśli $2n$ jest sumą kwadratów dwóch liczb całkowitych, to n również.*

Źródło: Stefan Straszewicz - "Zadania z Olimpiad Matematycznych"

Dowód Dla pewnych $x, y \in \mathbb{Z} : x^2 + y^2 = 2n$. Oznacza to, że $x \equiv y \pmod{2}$. Wynika z tego, że liczby $p = \frac{x+y}{2}$ i $q = \frac{x-y}{2}$ są całkowite. Wtedy:

$$p^2 + q^2 = \frac{x^2 + 2xy + y^2 + x^2 - 2xy + y^2}{4} = \frac{x^2 + y^2}{2} = \frac{2n}{2} = n.$$

□

Twierdzenie 1.6 *Niech $m, n \in \mathbb{N}$. Jeżeli $5m = n^2 + 49$, to m jest sumą dwóch kwadratów liczb całkowitych.*

Źródło: Andrzej Nowicki - "Podróże po Imperium Liczb"

Dowód Załóżmy, że $n = 7k$, $k \in \mathbb{N}$, wtedy $5m = 49(k^2+1)$. Skoro $k^2+1 \in \mathbb{N}$ to $49|m$. Bierzemy $x = \frac{m}{49}$, wtedy $5x = k^2 + 1$. NWD(k, 1)=1 więc na mocy L1 mamy, że $x = p^2+q^2$, gdzie $p, q \in \mathbb{Z}$. Mnożymy stronami przez 49 i mamy $m = (7p)^2+(7q)^2$. Jeżeli zaś $7 \nmid n$ wtedy NWD(n, 49)=1, więc od razu z L1 otrzymujemy tezę.

□

Twierdzenie 1.7 *Jeśli każda z liczb n, $n+1$, $n+2$ jest sumą dwóch kwadratów liczb całkowitych, to własność tę mają również liczby m, $m+1$, $m+2$, dla $m = n(n+2)$.*

Źródło: Andrzej Nowicki - "Podróże po Imperium Liczb"

Dowód Skoro liczby n i $n+2$ są sumami dwóch kwadratów to korzystając z D3 liczba $m = n(n+2)$ również jest sumą dwóch kwadratów. Mamy ponadto $m+1 = n^2+2n+1 = (n+1)^2+0^2$, $m+2 = n^2+2n+2 = (n+1)^2+1^2$.

□

Twierdzenie 1.8 *Dla każdej liczby naturalnej $n > 1$ istnieją różne liczby naturalne a, b, c, leżące pomiędzy n^2 i $(n+1)^2$ takie, że $c|a^2+b^2$.*

Źródło: Olimpiada Matematyczna Mołdawia 2001

Dowód Niech $c = n^2+1$, $a = n^2+2$, $b = n^2+n+1$. Liczby te są parami rożne oraz leżą pomiędzy n^2 i $(n+1)^2$. Ponadto, $a \equiv 1 \pmod{c}$, $b \equiv n \pmod{c}$, więc $a^2+b^2 \equiv c \equiv 0 \pmod{c}$

□

Twierdzenie 1.9 *Równanie $x^2+y^2 = z^2+3$ ma nieskończenie wiele rozwiązań całkowitych.*

Źródło: Olimpiada Matematyczna Włochy 1996

Dowód Przyjmijmy $z = 2n^2+4n+1$ dla dowolnego $n \in \mathbb{N}$. Wtedy

$$z^2+3 = 4n^4+16n^3+20n^2+8n+4 = (2n^2+4n)^2+(2n+2)^2.$$

Dobieramy więc $x = 2n^2+4n$ oraz $y = 2n+2$.

□

Twierdzenie 1.10 *Nie ma takich liczb całkowitych $x_1, x_2, \ldots, x_{2011}$, ani $y_1, y_2, \ldots, y_{2011}$, dla których liczba*

$$L = (2x_1^2 + 3y_1^2)(2x_2^2 + 3y_2^2) \cdot \ldots \cdot (2x_{2011}^2 + 3y_{2011}^2),$$

byłaby kwadratem liczby naturalnej.

Źródło: LXII Olimpiada Matematyczna - II etap

Dowód Załóżmy, nie wprost, że wskazana liczba L jest kwadratem. Wówczas $2^{2012}L$ również jest kwadratem. Czyli

$$M^2 = 2^{2012}L = 2 \cdot ((2x_1)^2 + 6y_1^2)((2x_2)^2 + 6y_2^2) \cdot \ldots \cdot ((2x_{2011})^2 + 6y_{2011}^2).$$

Korzystając wielokrotnie z multiplikatywnej zamkniętości zbioru $\mathcal{W}_{(1,0,6)}$, możemy zapisać powyższą równość skrótowo tak: $M^2 = 2(A^2+6C^2)$ przy pewnych $A, C \in \mathbb{Z}$. Kładąc $B = 2C$, dostajemy

$$M^2 = 2A^2 + 3B^2.$$

To jest niemożliwe, wystarczy rozważyć $\pmod 3$.

□

Twierdzenie 1.11 *Nieparzysta liczba pierwsza p da się przedstawić w postaci $x^2 + y^2$ wtedy i tylko wtedy, gdy $p \equiv 1 \pmod 4$.*

Dowód Korzystając z tego że p jest nieparzyste mamy $p \equiv 1, 3 \pmod 4$, ale ponieważ reszty kwadratowe $\pmod 4$ to 0 i 1 to musi być $p \equiv 1 \pmod 4$. Dla dowodu dostateczności dla $p = 4k + 1$ bierzemy $a = (2k)!$. Z twierdzenia Wilsona:

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

Oznacza to, że $a^2 \equiv -1 \pmod p$. Wtedy $p|a^2 + 1$. Zatem, na mocy L1, p jest sumą dwóch kwadratów.

□

Twierdzenie 1.12 *Przedstawienie $p = x^2 + y^2$ liczby pierwszej w postaci sumy dwóch kwadratów jest jednoznaczne (z dokładnością do zamiany x^2 na y^2).*

Dowód Niech

$$p = x_1^2 + y_1^2 = x_2^2 + y_2^2, \tag{3}$$

będą dwoma przedstawieniami liczby pierwszej p w postaci sumy kwadratów. Wówczas $\mathrm{NWD}(x_i, y_i) = 1$ (bo kwadrat wspólnego dzielnika x_i i y_i jest dzielnikiem p) oraz $p \nmid x_i$ i $p \nmid y_i$. Mnożąc obustronnie kongruencję $x_i^2 + y_i^2 \equiv 0 \pmod p$ przez odwrotność (y_i^2) otrzymamy $(x_i y_i^{-1})^2 \equiv -1 \pmod p$. Widzimy więc, że $x_1 y_1^{-1}$ i $x_2 y_2^{-1}$ są rozwiązaniami kongruencji $z^2+1 \equiv 0 \pmod p$. Ale kongruencja ta ma co najwyżej dwa rozwiązania (jeżeli $a \pmod p$ jest rozwiązaniem, to drugim jest $-a \pmod p$).

Zatem $x_1 y_1^{-1} \equiv \pm x_2 y_2^{-1} \pmod{p}$, co, po obustronnym pomnożeniu przez $y_1 y_2$, daje $x_1 y_2 \equiv \pm x_2 y_1 \pmod{p}$. Zmieniając ewentualnie y_1 na $-y_1$, mamy $x_1 y_2 \equiv x_2 y_1 \pmod{p}$. Równości (3) i tożsamość Fibonacci'ego dają $p^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2$. Ponieważ $p | x_1 y_2 - x_2 y_1$, więc też $p | x_1 x_2 + y_1 y_2$. Po podzieleniu przez p^2 otrzymamy

$$1 = \left(\frac{x_1 x_2 + y_1 y_2}{p}\right)^2 + \left(\frac{x_1 y_2 - x_2 y_1}{p}\right)^2.$$

Stąd $x_1 x_2 = -y_1 y_2$ lub $x_1 y_2 = x_2 y_1$. Jeżeli zachodzi pierwsza z tych równości, to, wobec względnej pierwszości x_1 i y_1, na mocy ZTA, mamy $x_1 | y_2$, a wobec względnej pierwszości x_2 i y_2, $y_2 | x_1$. Zatem $x_1 = \pm y_2$ i wtedy $x_2 = \pm y_1$. Podobnie rozpatrujemy drugi przypadek i dostajemy: $x_1 = \pm x_2$ i $y_1 = \pm y_2$. To kończy rozwiązanie.

□

Twierdzenie 1.13 *Liczba naturalna jest sumą dwóch kwadratów liczb całkowitych wtedy i tylko wtedy, gdy w jej rozkładzie na czynniki pierwsze nie ma żadnej liczby pierwszej postaci $4k+3$ w potędze nieparzystej.*

Źródło: Wacław Sierpiński - "Teoria liczb"

Dowód ($\Leftarrow$) Przedstawmy n w postaci $n = d^2 m$, gdzie m jest iloczynem różnych liczb pierwszych postaci $4k+1$ i dwójki. Dzięki temu, że $p = 4k+1$ można przedstawić w postaci sumy dwóch kwadratów, równości $2 = 1^2 + 1^2$ i wielokrotnemu zastosowaniu tożsamości Fibonacci'ego możemy napisać $m = x^2 + y^2$. Stąd $n = (dx)^2 + (dy)^2$.

($\Rightarrow$) Załóżmy teraz, że $n = x^2 + y^2$ jest sumą dwóch kwadratów i że liczba pierwsza $p \equiv 3 \pmod{4}$ dzieli n. Twierdzimy, że wówczas $p | x$ i $p | y$. Gdyby bowiem $p \nmid x$, to, oznaczając przez u odwrotność x modulo p, mielibyśmy

$$nu^2 = (xu)^2 + (yu)^2,$$

skąd $1 + (yu)^2 \equiv 0 \pmod{p}$, co jest niemożliwe (bo -1 jest niereszą kwadratową modulo $p \equiv 3 \pmod{4}$). Podobnie sprawdzamy, że $p | y$. Otrzymujemy $n = x^2 + y^2 = (pa)^2 + (pb)^2$, więc $p^2 | n$. Dokończenie rozumowania jest teraz natychmiastowe.

□

Twierdzenie 1.14 *Nieparzysta liczba pierwsza p da się przedstawić w postaci $x^2 + 2y^2$ wtedy i tylko wtedy, gdy $p \equiv 1, 3 \pmod{8}$.*

Dowód Ponieważ kwadraty modulo 8 to 0, 1, 4, a podwojone kwadraty to 0, 2, więc jasne, że suma kwadratu i podwojonego kwadratu może dawać resztę 0, 1, 2, 3, 4, 6, nigdy zaś reszty 5, 7. Stąd wynika, że nie tylko liczby pierwsze $\equiv 5, 7 \pmod{8}$ ale w ogóle żadne liczby naturalne $\equiv 1, 3 \pmod{8}$ nie mogą być sumami kwadratu

i podwojonego kwadratu. Niech więc $p \equiv 1, 3 \pmod 8$ będzie liczbą pierwszą. To, na mocy symbolu Legendre'a, oznacza, że istnieje liczba całkowita a spełniająca kongruencję:

$$a^2 \equiv -2 \pmod p. \tag{4}$$

Jasne, że $p \nmid a$. Stosując twierdzenie Thue'go ($m = p$ i $a = a$), znajdujemy takie niezerowe liczby całkowite x, y, że $x \equiv ay \pmod p$, a ponadto $|x|, |y| < \sqrt{p}$. Wówczas, na mocy (4),

$$x^2 + 2y^2 \equiv x^2 - a^2y^2 \equiv (x - ay)(x + ay) \equiv 0 \pmod p,$$

a, ponieważ $|x|$ i $|y|$ są "małe", więc $x^2 + 2y^2 < (\sqrt{p})^2 + 2(\sqrt{p})^2 = 3p$. Zatem $x^2 + 2y^2$ jest dodatnią wielokrotnością liczby p ściśle mniejszą od $3p$, co oznacza, że $x^2 + 2y^2 = p$ lub $2p$. Jeżeli $x^2 + 2y^2 = p$, to koniec. Jeżeli zaś $x^2 + 2y^2 = 2p$, to zachodzi równość $x = 2z$ dla pewnego $z \in \mathbb{Z}$. Skąd $2z^2 + y^2 = p$, co kończy rozwiązanie.

□

Twierdzenie 1.15 *Liczba naturalna n da się przedstawić w postaci $x^2 + 2y^2$ wtedy i tylko wtedy, gdy dla każdej liczby pierwszej $p \equiv 5, 7 \pmod 8$ wykładnik $v_p(n)$ jest liczbą parzystą.*

Dowód ($\Leftarrow$) Przedstawiając liczbę naturalną n w postaci d^2m, gdzie m jest iloczynem różnych liczb pierwszych postaci 2, 8k+1, 8k+3 i pisząc (dzięki wielokrotnemu zastosowaniu faktu, że 2, $8k + 1$, $8k + 3$ da się zapisać jako $x^2 + 2y^2$ i tożsamości Brahmagupty dla $c = 2$, jest to możliwe) $m = x^2 + 2y^2$ otrzymamy $n = (dx)^2 + (dy)^2$.

($\Rightarrow$) Załóżmy teraz, że

$$n = x^2 + 2y^2, \tag{5}$$

jest sumą kwadratu i podwojonego kwadratu i że liczba pierwsza $p \equiv 5, 7 \pmod 8$ dzieli n. Twierdzimy, że wówczas $p|x$ i $p|y$. Gdyby bowiem $p \nmid y$, to oznaczając przez u odwrotność y modulo p mielibyśmy

$$nu^2 = (xu)^2 + 2(yu)^2,$$

skąd $0 \equiv (xu)^2 + 2 \pmod p$ co jest niemożliwe, bo -2 jest niereszą kwadratową modulo $p \equiv 5, 7 \pmod 8$. Zatem $p|y$. Równość (5) pokazuje wtedy, że również $p|x$. Stąd $n = x^2 + 2y^2 = (pa)^2 + 2(pb)^2$, więc $p^2|n$. Dokończenie rozumowania jest oczywiste.

□

Twierdzenie 1.16 *Liczba pierwsza p da się przedstawić w postaci $x^2 + 3y^2$ wtedy i tylko wtedy, gdy $p \equiv 1 \pmod 3$.*

Dowód Ponieważ kwadraty modulo 3 to 0, 1, a potrojone kwadraty to 0, więc jasne, że suma kwadratu i potrojonego kwadratu może dawać resztę 0, 1. Nie może to być 0 ponieważ liczba pierwsza inna niż 3 nie może być wielokrotnością 3, a dla $p = 3$ nie ma takiego x i y. Niech więc $p \equiv 1 \pmod 3$ będzie liczbą pierwszą. To, na mocy symbolu Legendre'a, oznacza, że istnieje liczba całkowita a spełniająca kongruencję:

$$a^2 \equiv -3 \pmod p. \tag{6}$$

Jasne, że $p \nmid a$. Stosując twierdzenie Thue'go ($m = p$ i $a = a$), znajdujemy takie niezerowe liczby całkowite x, y, że $x \equiv ay \pmod p$, a ponadto $|x|, |y| < \sqrt{p}$. Wówczas, na mocy (6),

$$x^2 + 3y^2 \equiv x^2 - a^2y^2 \equiv (x - ay)(x + ay) \equiv 0 \pmod p,$$

a, ponieważ $|x|$ i $|y|$ są "małe", więc $x^2 + 3y^2 < (\sqrt{p})^2 + 3(\sqrt{p})^2 = 4p$. Zatem $x^2 + 3y^2$ jest dodatnią wielokrotnością liczby p ściśle mniejszą od $4p$, co oznacza, że $x^2 + 3y^2 = p$ lub $2p$ lub $3p$. Jeżeli $x^2 + 3y^2 = p$, to koniec. Jeżeli zaś $x^2 + 3y^2 = 3p$, to zachodzi równość $x = 3z$ dla pewnego $z \in \mathbb{Z}$. Skąd $3z^2 + y^2 = p$, co kończy, a dla $x^2 + 3y^2 = 2p$ mamy skoro $p \equiv 1 \pmod 3$ to $2 \equiv 2p \equiv x^2 + 3y^2 \equiv 0, 1 \pmod p$ co jest oczywiście sprzeczne.

□

Twierdzenie 1.17 *Jeżeli liczba pierwsza $p \equiv 3 \pmod 4$ jest dzielnikiem liczby $s^2 + 5t^2$ przy pewnych względnie pierwszych $s, t \in \mathbb{Z}$, to istnieją takie względnie pierwsze x, y, że $2p = x^2 + 5y^2$.*

Źródło: LIX Olimpiada Matematyczna - Finał

Dowód Warunek $p|s^2+5t^2$, czyli kongruencja $s^2 \equiv -5t^2 \pmod p$ przy względnie pierwszych s, t, implikuje, że $p \nmid t$. Więc $t \pmod p$ jest odwracalne. Niech u będzie odwrotnością t modulo p. Wtedy $(su)^2 \equiv -5 \pmod p$. To oznacza, że $a = su$ spełnia kongruencję:

$$a^2 \equiv -5 \pmod p.$$

Ponieważ $p \nmid a$, więc możemy przywołać twierdzenie Thue'go i znaleźć takie $x, y \in \mathbb{Z} \setminus \{0\}$ spełniające warunki: $x \equiv ay \pmod p$ i $|x|, |y| \leqslant \sqrt{p}$. Wówczas sprawdzamy, że

$$x^2 + 5y^2 \equiv x^2 - a^2y^2 \equiv (x - ay)(x + ay) \equiv 0 \pmod p,$$

czyli, że $x^2 + 5y^2$ jest niezerową wielokrotnością p. Ponadto $|x|, |y| < \sqrt{p}$, więc

$$x^2 + 5y^2 < (\sqrt{p})^2 + 5(\sqrt{p})^2 = 6p.$$

Widzimy stąd, że $x^2 + 5y^2 = p$, $2p$, $3p$, $4p$ lub $5p$. Korzystając z tego, że $p \equiv 3 \pmod 4$ mamy:

$$p \equiv 5p \equiv x^2 + 5y^2 \equiv x^2 + y^2 \equiv 0, 1, 2 \pmod 4.$$

Co jest sprzeczne, odrzucamy więc możliwości p oraz $5p$.

Załóżmy więc, że $x^2+5y^2 = 4p$. Wtedy $x^2+5y^2 \equiv 0 \pmod 4$. Załóżmy że $4 \nmid x^2$. Wtedy jako u oznaczamy odwrotność x modulo 4 mnożąc poprzednią kongruencję stronami przez u^2 otrzymujemy $1 + 5(yu)^2 \equiv 0 \pmod 4$ czyli $(yu)^2 \equiv -1 \pmod 4$ co jest niemożliwe. Jeśli zaś dzieli wtedy także $4|5y^2$ więc kładziemy $g, h \in \mathbb{Z}$, takie że $x^2 = 4g^2$ oraz $y^2 = 4h^2$, skąd otrzymujemy $g^2 + 5h^2 = p$ co, jak wykazaliśmy wcześniej, jest niemożliwe.

Załóżmy teraz $x^2+5y^2 = 3p$, 3 nie może dzielić x i y, ponieważ wtedy 9 dzieliłoby x^2 i y^2, czyli $9|3p$ co zachodzi tylko dla $p = 3$, które nie spełnia warunków zadania. Możemy więc przyjąć $x, y \equiv 1 \pmod 3$ (ponieważ $-2 \equiv 1 \pmod 3$). Zapiszmy teraz

$$18p = 6 \cdot 3p = 6(x^2 + 5y^2) = (x + 5y)^2 + 5(x - y)^2. \tag{7}$$

Korzystając z tego, że $x+5y \equiv x-y \equiv 0 \pmod 3$, możemy zapisać $x+5y = 3g$ oraz $x-y = 3h$, dla pewnych $g, h \in \mathbb{Z}$. Wstawiając to do (7) otrzymujemy $2p = g^2+5h^2$. Co spełnia tezę.

Dla przypadku $x^2 + 5y^2 = 2p$ teza oczywiście zachodzi.

□