**§ 4. Dowód twierdzenia Fermata o rozkładzie liczb pierwszych formy 4k+1 na sumę dwu kwadratów.** Udowodnimy przede wszystkim

**Lemat 1.** *Jeżeli $p$ jest liczbą pierwszą i istnieją dwie liczby całkowite niepodzielne przez $p$, których suma kwadratów jest podzielna przez $p$, to $p$ jest sumą dwu kwadratów.*

D o w ó d. Ponieważ suma kwadratów liczb całkowitych jest zawsze nieujemna, a zerem może być tylko wtedy, gdy te liczby są zerami, więc suma kwadratów dwu liczb niepodzielnych przez $p$ jest zawsze liczbą naturalną. W myśl założenia lematu, istnieje zatem liczba naturalna podzielna przez $p$ i rozkładająca się na sumę dwu kwadratów niepodzielnych przez $p$. Takich liczb naturalnych może być więcej. Niech $n$ będzie najmniejszą z nich. Jest więc przy pewnym naturalnym $m$:

$$n = mp, \tag{23}$$

$$n = a^2 + b^2, \tag{24}$$

gdzie $a$ i $b$ są dwiema liczbami całkowitymi niepodzielnymi przez $p$.

Jak wiemy z § 2, możemy wyznaczyć liczby $\alpha$ i $\beta$, spełniające warunki:

$$\begin{gathered} \alpha \equiv a(mod\ p), \qquad \beta \equiv b(mod\ p), \\ |\alpha| \leqslant \frac{p}{2}, \qquad |\beta| \leqslant \frac{p}{2}. \end{gathered} \tag{25}$$

Stąd:

$$\begin{gathered} \alpha^2 + \beta^2 \equiv a^2 + b^2 (mod\ p), \\ \alpha^2 + \beta^2 \leqslant \frac{p^2}{4} + \frac{p^2}{4} = \frac{p^2}{2} < p^2. \end{gathered} \tag{26}$$

Wobec niepodzielności liczb $a$ i $b$ przez $p$, kongruencje (25) dowodzą, że $\alpha$ i $\beta$ są też niepodzielne przez $p$, a kongruencja (26) dowodzi, że suma kwadratów $\alpha^2 + \beta^2$ jest podzielna przez $p$.

Również więc liczba $\alpha^2 + \beta^2$ jest naturalna, podzielna przez $p$ i rozkłada się na sumę kwadratów dwu liczb niepodzielnych przez $p$. Skoro jednak $n$ jest najmniejszą z takich liczb naturalnych, to

$$n \leqslant \alpha^2 + \beta^2,$$

a zatem w myśl (23) i nierówności (26)

$$mp < p^2,$$

skąd

$$m < p. \tag{27}$$

Jeżeli udowodnimy, że $m = 1$, to lemat będzie dowiedziony, gdyż w myśl wzorów (23) i (24) będziemy mieli wtedy

$$p = a^2 + b^2.$$

Przypuśćmy, że $m \neq 1$. Ponieważ $m$ jest liczbą naturalną spełmiającą nierówność (27), więc

$$1 < m < p. \tag{28}$$

Wyznaczmy liczby $a_1$ i $b_1$, spełniające warunki:

$$a_1 \equiv a(mod\ m), \qquad b_1 \equiv b(mod\ m), \tag{29}$$

$$|a_1| \leqslant \frac{m}{2}, \qquad |b_1| \leqslant \frac{m}{2}. \tag{30}$$

Warunki te dają:

$$a_1^2 + b_1^2 \equiv a^2 + b^2(mod\ m), \tag{31}$$

$$a_1^2 + b_1^2 \leqslant \frac{m^2}{4} + \frac{m^2}{4} = \frac{m^2}{2} < m^2. \tag{32}$$

Kongruencja (31) wskazuje wobec wzorów (20) i (19), że liczba $a_1^2 + b_1^2$ jest podzielna przez $m$; nierówność zaś (32) dowodzi, że liczba ta jest mniejsza niż $m^2$. Możemy więc przyjąć

$$a_1^2 + b_1^2 = lm, \tag{33}$$

gdzie $l$ jest liczbą całkowitą mniejszą niż $m$.

Liczba $l$ nie może być zerem, gdyż wtedy byłoby $a_1 = b_1 = 0$, wskutek czego liczby $a_1$ i $b_1$, a więc na mocy kongruencji (29) również liczby $a$ i $b$, byłyby podzielne przez $m$; pisząc wówczas $a = tm$ i $b = um$, mielibyśmy w myśl (24), $n = (t^2+u^2)m^2$, skąd w myśl (23) $p = (t^2+u^2)m$ i liczba pierwsza $p$ posiadałaby dzielnik $m$ spełniający nierówności (28), co niemożliwe.

Liczba $l$ jest więc naturalna i zachodzi nierówność

$$0 < l < m. \tag{34}$$

Weźmy teraz pod uwagę tożsamość

$$(a^2 + b^2)(a_1^2 + b_1^2) = (aa_1 + bb_1)^2 + (ab_1 - ba_1)^2. \tag{35}$$

Lewa strona tej tożsamości przedstawia w myśl (24), (23) i (33) liczbę

$$mp \cdot lm = lpm^2. \tag{36}$$

Obliczamy jej stronę prawą. Mnożąc pierwszą z kongruencji (29) przez $a$, a drugą przez $b$, otrzymujemy po dodaniu stronami $aa_1 + bb_1 \equiv a^2 + b^2 (mod\ m)$, skąd $aa_1 + bb_1 \equiv 0(mod\ m)$ czyli

$$aa_1 + bb_1 = cm, \tag{37}$$

gdzie $c$ jest liczbą całkowitą.

Mnożąc zaś pierwszą z kongruencji (29) przez $b$ i odejmując od drugiej, pomnożonej przez $a$, otrzymujemy $ab_1 - ba_1 \equiv 0(mod\ m)$, co dowodzi, że

$$ab_1 - ba_1 = dm, \tag{38}$$

gdzie $d$ jest liczbą całkowitą.

Tożsamość (32) daje więc na mocy (36), (37), (38)

$$lpm^2 = c^2m^2 + d^2m^2,$$

skąd po podzieleniu obu stron przez liczbę dodatnią $m^2$ otrzymujemy

$$lp = c^2 + d^2. \tag{39}$$

Wzór ten wskazuje, że liczby $c$ i $d$ są albo obie podzielne przez $p$, albo obie niepodzielne przez $p$. Gdyby obie liczby $c$ i $d$ były podzielne przez $p$, to przynajmniej jedna z nich byłaby co do bezwzględnej wartości nie mnieszja od $p$, gdyż obie zerem być nie mogą, skoro $l > 0$. Lecz wtedy kwadrat jej byłby nie mniejszy od $p^2$, a zatem $c^2 + d^2 \geqslant p^2$, skąd $l \geqslant p$ wbrew nierównościom (34) i (27).

Wzór (39) przedstawia więc rozkład liczby $lp$ na sumę kwadratów dwu liczb całkowitych niepodzielnych przez $p$. Skoro jednak $lp$ jest wielokrotnością naturalną liczby $p$, więc w myśl definicji liczby $n$ musiałoby być $n \leqslant lp$ czyli na mocy (23) $mp \leqslant lp$, skąd $m \leqslant l$ wbrew nierówności (34).

Tym sposobem przypuszczenie, że $m \neq 1$, doprowadza do sprzeczności i lemat został udowodniony.

**Twierdzenie 8** (Fermata)**.** *Każda liczba pierwsza formy $4k+1$ rozkłada się i to w jeden tylko sposób na sumę dwu kwadratów.*

D o w ó d. Niech $p$ będzie liczbą pierwszą formy $4k+1$. Jak dowiedliśmy w § 2, istnieje dla lcizby pierwszej $p$ formy $4k+1$ taka liczba całkowita $x$, że $x^2+1$ jest podzielne przez $p$. Wiemy też, że jeżeli suma kwadratów dwu liczb całkowitych jest podzielna przez liczbę pierwszą $p$, to albo obie te liczby są podzielne przez $p$, albo żadna z nich nie jest podzielna przez $p$. Wobec niepodzielności liczby 1 przez $p$ wnosimy stąd, że $p$ jest dzielikiem sumy kwadratów dwu liczb niepodzielnych przez $p$, mianowicie $x^2 + 1^2$ [1]. W myśl udowodnionego lematu liczba $p$ sama jest więc sumą dwu kwadratów:

$$p = a^2 + b^2.$$

[1] Można dowieść, opierając się na twierdzeniu Wilsona, że liczba $(1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2})^2 + 1$ jest podzielna przez $p$ (gdy $p$ jest liczbą pierwszą formy $4k+1$). Por. §3, ćwiczenie 26.

Pozostaje do udowodnienia, że istnieje tylko ejden taki rozkład, jeżeli nie zwracać uwagi na porządek oraz na znaki liczb $a$ i $b$.

Przypuśćmy, że $p$ ma dwa rozkłady na sumę dwu kwadratów:

$$p = a^2 + b^2, \qquad p = a_1^2 + b_1^2. \tag{40}$$

Żadna z liczb $a$ i $b$ nie może być zerem, gdyż liczba pierwsza $p$ nie jest kwadratem żadnej liczby całkowitej. Ponieważ zaś nie zwracamy uwagi na znaki liczb $a$ i $b$, więc możemy założyć, że obie są dodatnie. Są one przy tym względnie pierwsze, gdyż każdy ich wspólny dzielnik jest zarazem dzielnikiem liczby $p = a^2 + b^2$. Takie same uwagi możemy zrobić co do liczb $a_1$ i $b_1$.

Weźmy teraz pod uwagę tożsamości:

$$\begin{aligned} p^2 = (a^2+b^2)(a_1^2+b_1^2) &= (aa_1+bb_1)^2 + (ab_1-ba_1)^2 = \\ &= (ab_1+ba_1)^2 + (aa_1-bb_1)^2, \\ (aa_1+bb_1)(ab_1+ba_1) &= (a^2+b^2)a_1b_1 + (a_1^2+b_1^2)ab = \\ &= p((a_1b_1+ab). \end{aligned} \tag{41}$$

Iloczyn

$$(aa_1+bb_1)(ab_1+ba_1) \tag{42}$$

jest więc podzielny przez liczbę pierwszą $p$, skąd wnosimy, że przynajmniej jeden z jego czynników jest podzielny przez $p$.

Jeżeli pierwszy czynnik iloczynu (42) jest podzielny przez $p$, to ponieważ jest on liczbą naturalną, więc $aa_1 + bb_1 \geqslant p$ i przeto $(aa_1+bb_1)^2 \geqslant p^2$, wobec czego pierwszy z rozkładów (41) liczby $p^2$ na sumę dwu kwadratów daje

$$ab_1 - ba_1 = 0 \qquad \text{czyli} \qquad ab_1 = ba_1.$$

Ponieważ $(a_1b_1) = 1$ więc $a$ jest podzielne przez $a_1$, a ponieważ $(a,b) = 1$, więc $a_1$ jest podzielne przez $a$. Jest zatem $a = a_1$, wobec czego równość $ab_1 = ba_1$ daje $b_1 = b$. Rozkłady (40) są zatem w tym przypadku identyczne.

Jeżeli zaś pierwszy czynnik iloczynu (32) nie jest podzielny przez $p$, to w takim razie drugi czynnik musi być podzielny przez $p$, a zatem $ab_1 + ba_1 \geqslant p$. Jak wyżej, wnosimy z drugiego z rozkładów (41), że wtedy $aa_1 - bb_1 = 0$ czyli $aa_1 = bb_1$. Ponieważ $(a,b) = 1$, więc $a_1$ jest podzielne przez $b$, a ponieważ $(a_1,b_1) = 1$, więc $b$ jest podzielne przez $a_1$. Jest zatem $a_1 = b$, wobec czego równość $aa_1 = bb_1$ daje $b_1 = a$. W tym przypadku rozkłady różniłyby się tylko porządkiem składników.

Tym samym dowód twierdzenia 2 został zakończony.

*U w a g a.* Jeżeli uważać za różne takie rozkłady $x^2 + y^2$, które się różnią bądź porządkiem, bądź znakami liczb $x$ i $y$, to - jak łatwo widzieć - każda liczba pierwsza $p$ formy $4k+1$ będzie miała dokładnie 8 rozkładów na sumę dwu kwadratów, a mianowicie:

$$\begin{array}{llll} a^2+b^2, & a^2+(-b)^2, & (-a)^2+b^2, & (-a)^2+(-b)^2, \\ b^2+a^2, & (-b)^2+a^2, & b^2+(-a)^2, & (-b)^2+(-a)^2. \end{array}$$

Że wszystkie te rozkłady są różne, wynika stąd, że $a$ i $b$ są różnymi liczbami naturalnymi.

Oto rozkłady na sumę dwu kwadratów dla wszystkich liczb pierwszych formy $4k+1$, zawartych w pierwszej setce:

$$5=1^2+2^2, \quad 13=2^2+3^2, \quad 17=1^2+4^2, \quad 29=2^2+5^2$$
$$37=1^2+6^2, \quad 41=4^2+5^2, \quad 53=2^2+7^2, \quad 61=5^2+6^2,$$
$$73=3^2+8^2, \quad 89=5^2+8^2, \quad 97=4^2+9^2.$$

Mając dwa różne rozkłady liczby nieparzystej $n$ na sumę dwu kwadratów:

$$n=a^2+b^2=c^2+d^2,$$

gdzie $a \geqslant b > 0$, $a > c$ i $c \geqslant d > 0$, potrafimy rozłożyć $n$ na dwa czynniki naturalne większe od 1. Niech bowiem

$$\delta=(a-c,d-b), \qquad a-c=r\delta i d-b=s\delta.$$

Wówczas $(r,s)=1$, a ponieważ $a^2-c^2=d^2-b^2$, więc $r(a+c)=s(d+b)$; wnosimy stąd, że $a+c=st$, gdzie $t$ jest liczbą naturalną. Łatwo sprawdzić, że

$$n=\frac{(r^2+s^2)(t^2+\delta^2)}{4}$$

i że każdy z obu czynników licznika przewyższa 4. Stąd otrzymuje się od razu wspomniany rozkład liczby $n$. Czytelnik zechce zastosować tę metodę np. do rozkładów:

$$8^2+1^2=7^2+4^2, \qquad 9^2+2^2=7^2+6^2, \qquad 179^2+2^2=178^2+19^2.$$

**§ 5. Ilość liczb pierwszych formy 4k+1, 4k+3, 3k+2 i 8k+1.** Nasuwa się pytanie: ile jest liczb pierwszych formy $4k+1$? Gdyby się okazało, że jest ich skończenie wiele, to udowodnione twierdzenie Fermata straciłoby na swej wartości.

Zanim się zajmiemy tym zagadnieniem, udowodnimy

**Lemat 2.** *Żadna liczba formy $4k+3$ (pierwsza lub złożona) nie rozkłada się na subę dwu kwadratów.*

D o w ó d. Oczywiście wystarczy udowodnić, że żadna suma $a^2+b^2$ nie daje przy dzieleniu przez 4 reszty 3.

Jeżeli obie liczby $a$ i $b$ są parzyste, albo obie nieparzyste, to - jak łatwo widzieć - suma kwadratów jest liczbą parzystą i nie daje przy dzieleniu przez 4 reszty 3.

Jeżeli zaś jedna z liczb $a$ i $b$ jest parzysta, a druga nieparzysta, np. $a = 2t$ i $b = 2u + 1$, gdzie $t$ i $u$ są liczbami całkowitymi, to

$$a^2 + b^2 = (2t)^2 + (2u + 1)^2 = 4t^2 + 4u^2 + 4u + 1,$$

a więc $a^2 + b^2$ daje przy dzieleniu przez 4 resztę 1. Reszty 3 przy dzieleniu przez 4 nie otrzymujemy więc dla żadnej sumy dwu kwadratów. c. b. d. d.

**Twierdzenie 9.** *Istnieje nieskończenie wiele liczb pierwszych formy* $4k + 1$.

D o w ó d. Przypuśćmy, że wzystkich liczb pierwszych formy $4k + 1$ jest skończenie wiele: niech to będą liczby

$$p_1, p_2, \ldots, p_n. \tag{43}$$

Niech

$$N = (2p_1p_2 \ldots p_n)^2 + 1.$$

Jest to oczywiście liczba naturalna formy $4k + 1$. Liczba $N$ jako większa od jedności i nieparzysta, ma co najmniej jeden czynnik pierwszy $p$, oczywiście nie parzysty.

Liczba $p$ jest więc formy $4k + 1$ lub $4k + 3$, gdyż każda liczba nieparzysta jest jednej z tych dwu form. Ale $p$ nie może być formy $4k + 1$, gdyż - jak łatwo widzieć - $N$ daje resztę 1 przy dzieleniu przez każdą liczbę pierwszą formy $4k+1$, tj. przez każdą z liczb (43). A więc $p$ jest formy $4k + 3$, zatem różne od 2 i od każdej z liczb (43). Liczba $N$, podzielna przez liczbę pierwszą $p$, jest więc sumą kwadratów dwu liczb niepodzielnych przez $p$. W myśl lematu 1 wnosimy stąd, że $p$ samo jest sumą dwu kwadratów, a przeto nie jest liczbą formy $4k + 3$. Doszliśmy więc do sprzeczności.

**Wniosek.** *Forma* $x^2 + y^2$ *przy naturalnych* $x$ *i* $y$ *zawiera nieskończenie wiele liczb pierwszych (oczywiście nie same tylko liczby pierwsze).*

Udowodnimy teraz, że forma $4k + 3$ też zawiera nieskończenie wiele liczb pierwszych.

**Lemat 3.** *Każda liczba naturalna formy* $4k + 3$ *ma przynajmniej jeden dzielnik pierwszy tej samej formy.*

D o w ó d. Niech $n = 4k + 3$. Liczba ta ma oczywiście dzielniki naturalne formy $4t + 3$, gdyż sama jest jednym z nich. Oznaczmy przez $p$ najmniejszy z takich dzielników. Pokażemy, że $p$ jest liczbą pierwszą, W przeciwnym bowiem razie byłoby $p = d\delta$, gdzie $d$ i $\delta$ są liczbami naturalnymi mniejszymi od $p$ i nieparzystymi, skoro $p$ jest nieparzyste. Obie one nie mogą być formy $4t + 1$ gdyż wówczas - jak łatwo widzieć - iloczyn ich byłby liczbą formy $4t + 1$. Zatem co najmniej jedna z liczb $d$ i $\delta$ jest formy $4t + 3$. Ponieważ dzielniki liczby $p$ są zarazem dzielnikami liczby $n$, więc $n$ miałoby dzielnik naturalny formy $4t + 3$ mniejszy od $p$, wbrew określeniu liczby $p$.

**Twierdzenie 10.** *Istnieje nieskończenie wiele liczb pierwszych formy* $4k + 3$.

D o w ó d. Przypuśćmy, że jest ich skończenie wiele. Niech to będą liczby $p_1, p_2, \ldots, p_n$ i niech

$$N = 4p_1p_2 \ldots p_n - 1.$$

Jest to oczywiście liczba naturalna formy $4k + 3$. W myśl lematu 3 liczba ta musi mieć co najmniej jeden dzielnik pierwszy formy $4k + 3$. Atoli z definicji liczby $N$ wynika natychmiast, że liczba ta nie jest podzielna przez żadną z liczb $p_1, p_2, \ldots, p_n$, czyli przez żadną liczbę pierwszą formy $4k + 3$. Stąd sprzeczność.

Twierdzenia 9 i 10 można wypowiedzieć w postaci: w każdym z postępów arytmetycznych

$$1, 5, 9, 13, 17, 21, 25, 29, 33, 37, \ldots$$
$$3, 7, 11, 15, 19, 23, 27, 31, 35, 39, \ldots$$

jest nieskończenie wiele liczb pierwszych.

**Twierdzenie 11.** *Istnieje nieskończenie wiele liczb pierwszych formy* $8k + 1$.

D o w ó d. Przypuścmy, że jest ich skończenie wiele. Niech to będą liczby $p_1, p_2, \ldots, p_n$ i niech

$$N = 2p_1p_2 \ldots p_n$$

Oznaczamy przez $q$ jakikolwwiek dzielnik liczby $N^4 + 1$, który jest liczbą pierwszą. Oczywiście $(N, q) = 1$. Liczba $q$ jest nieparzysta, a więc musiałaby być jednej z postaci:

$$8k + 1, \quad 8k + 3, \quad 8k + 5 \quad 8k + 7.$$

Nie może ona jednak być postaci $8k + 1$, gdyż wtedy byłaby jedną z liczb $p_1, p_2, \ldots, p_n$, przez które oczywiście liczba $N^4 + 1$ nie jest podzielna. Liczba $q$ nie może też być postaci $8k + 3$ ani $8k + 7$, gdyż byłaby wtedy zarazem postaci $4t + 3$, skąd

$$N^4 \equiv -1 (mod\ q), \text{ a więc } N^{4(2t+1)} \equiv -1 (mod\ q)$$

czyli $N^{2(q-1)} \equiv -1 (mod\ q)$, wbrew małemu twierdzeniu Fermata (p. §1, str. 59). Wreszcie, liczba $q$ nie może być postaci $8k + 5$, gdyż wtedy byłoby $N^{4(2k+1)} \equiv -1 (mod\ q)$ czyli $a^{q-1} \equiv -1 (mod\ q)$, znowu wbrew małemu twierdzeniu Fermata.

Mamy więc sprzeczność, a tym samym twierdzenie 5 jest dowiedzione.

Podobnie dowodzi się, że *liczb pierwszych postaci* $16k + 1$ *i, ogólnie, postaci* $2^n k + 1$ *(przy każdym naturalnym $n$) jest nieskończenie wiele.*

Udowodnimy jeszcze analogicznie twierdzenie dla formy $6k + 1$.

**Lemat 4.** *Każda liczba naturalna $n$ formy* $6k + 5$ *ma przynajmniej jeden dzielnik pierwszy tej formy.*

D o w ó d. Wystarczy zauważyć, że liczbą $n = 6k + 5$, jako nieparzysta i niepodzielna przez 3, moż?e mieć tylko dzielniki formy $6k + 1$ i $6k + 5$. Gdyby w rozkładzie liczby $n$ (oczywiście większej od jedności) na czynniki pierwsze figurowały same tylko czynniki formy $6k+1$, to $n$ - jak łatwo widzieć - samo byłoby formy $6k+1$, wbrew założeniu. Wśród czynników pierwszych liczby $n$ (nie wyłączając przypadku, keidy $n$ samo jest liczbą pierwszą) znajdzie się więc co najmniej jeden czynnik formy $6k+5$, c. b. d. o.

**Twierdzenie 12.** *Istnieje nieskońćzenie wiele liczb pierwszych formy* $6k+5$.

D o w ó d. Przypuśćmy, że jest ich skończenie wiele. Niech to będą liczby $p_1, p_2, \dots, p_n$ i niech

$$N = 6p_1p_2 \dots p_n - 1$$

$N$ byłoby więc liczbą naturalną formy $6k+5$, niepodzielną przez żadną liczbę pierwszą tej formy, wbrew lematowi 4.

W postępie arytmetycznym

$$5, 11, 17, 23, 29, 35, 41, 47, \dots$$

istnieje więc nieskończenie wiele liczb pierwszych. Tym bardziej też istnieje nieskończenie wiele lcizb pierwszych w postępie arytmetycznym.

$$2, 5, 8, 11, 14, 17, 20, 23, \dots,$$

w którym figurują przecież wszystkie wyrazy postępu $6k+5$.

Mamy więc

**Wniosek.** *Istnieje nieskończenie wiele liczb pierwszych formy* $3k+2$.

Twierdzenia 9-12 są szczególnymi przypadkami tzw. *twierdzenia Lejeune-Dirichleta* o postępie arytmetycznym $ak+b$, tj. w każdym ciągu nieskończonym postaci

$$a, a+b, a+2b, \dots,$$

gdzie $(a, b) = 1$, jest *nieskończenie wiele liczb pierwszych.*

Dowód tego twierdzenia, podany po raz pierwszy przez `Lejeune-Dirichleta` w 1837 r., jest jednym z trudniejszych dowodów teorii liczb i środkami elementarnymi uzyskać się nie daje. Pewne jednak przypadki szczególne można udowodnić elementarnie. Prócz tych, które stanowią treść ostatnich czterech twierdzeń, udowodnimy jeszcze w Rozdziale XIV, §7, kilka innych przypadków tego ogólnego twierdzenia.

ĆWICZENIE. Dowieść, opierając się na twierdzeniu o postępie arytmetycznym, że istnieją liczby pierwsze, dowolnie daleko *izolowane* z obu stron, tj. że dla każdej liczby naturalnej $n$ istnieje taka liczba pierwsza $p > n$, że każda z liczb $p \pm i$, gdzie $i = 1, 2, \dots, n$, jest złożona.

*D o w ó d. Istnieje liczba pierwsza* $q > n+1$. *Niech*

$$a = \prod_{i=1}^{q-2} (q^2 - i^2).$$

*Ponieważ liczba* $(q-2)!$ *jest pierwsza względem liczby (pierwszej)* $q$*, więc - jak łatwo widzieć - liczby* $a$ *i* $q$ *są również względnie pierwsze. W myśl twierdzenia o postępie arytmetycznym istnieje liczba pierwsza* $p > q$ *postaci* $ak + q$*, skąd*

$$p \pm i = ak + q \pm i \qquad \text{dla } i = 1, 2, \ldots, n.$$

*Wobec* $q > n + 1$ *jest (dla tych* $i$*)* $q - 1 > i$ *czyli* $q + i > 1$*. Zarazem* $q \pm i$*, jako dzielnik liczby* $a$*, jest dzielnikiem liczby* $p \pm i$*, różnym od niej wobec* $p > q$*. Liczba* $p \pm i$ *jest więc złożona.*

**§ 6. Warunki rozkładalności na sumę dwu kwadratów.** Powróćmy do rozkładów na sumę dwu kwadratów. Zapytajmy, jakie są warunki konieczne i dostateczne na to, aby liczba naturalna $n$ rozkładała się na sumę kwadratów dwu liczb całkowitych.

Odpowiedź na to pytanie daje następujące

**Twierdzenie 13.** *Na to, żeby liczba naturalna* $n$ *była sumą kwadratów dwu liczb całkowitych, potrzeba i wystarcza, by* $n$ *nie zawierało w swym rozwinięciu na czynniki pierwsze żadnej liczby pierwszej formy* $4k + 3$ *w potędze o wykładniku nieparzystym.*

D o w ó d. Załóżmy, że liczba $n$ rozkłada się na sumę kwadratów dwu liczb całkowitych

$$n = a^2 + b^2 \tag{44}$$

i niech

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \tag{45}$$

będzie rozwinięciem liczby $n$ na czynniki pierwsze.

Udowodnimy, że wszystkie czynniki pierwsze formy $4k + 3$, o ile w ogóle wchodzą do rozwinięcia liczby $n$, są w nim w potęgach o wykładnikach parzystych.

Niech $p$ będzie czynnikiem pierwszym formy $4k + 3$, figurującym w rozwinięciu liczby $n$, i niech

$$d = (a, b), \quad a = da_1, \quad b = db_1;$$

liczby $a_1$ i $b_1$ są względnie pierwsze. Wobec (35) liczba $n$ musi być podzielna przez $d^2$; niech $n = d^2 n_1$. Gdyby liczba $n_1$ nie zawierała w swym rozwinięciu na czynniki pierwsze liczby $p$, to rozwinięcie liczby $n$ zawierałoby oczywiście $p$ w potędze o wykładniku parzystym.

Przypuśćmy więc, że $n_1$ jest jeszcze podzielne przez $p$. Wzór (44) daje

$$n_1 = a_1^2 + b_1^2, \tag{46}$$