

Na odwrót — jak łatwo widzieć — jeżeli liczby x i $-x$ są równoważne właściwie, to każda z nich jest sama sobie równoważna niewłaściwie.

Tak więc, aby stwierdzić, czy niewymierność 2-go stopnia x jest sama sobie równoważna niewłaściwie, wystarczy rozstrzygnąć, czy liczby x i $-x$ są równoważne właściwie, a to zagadnienie potrafimy już rozstrzygnąć za pomocą twierdzenia 13.

Zauważymy tu jeszcze, że — jak można dowieść — na to, żeby niewymierność 2-go stopnia była sama sobie równoważna niewłaściwie, potrzeba i wystarczy żeby okres jej rozwinięcia na ułamek łańcuchowy składał się z nieparzystej liczby ogniw¹⁾.

ROZDZIAŁ XVI

TEORIA LICZB CAŁKOWITYCH ZESPOLONYCH

§ 1. Liczby całkowite zespolone i ich norma. Liczby stowarzyszone. Przez *liczby całkowite zespolone* rozumiemy liczby zespolone $a+bi$, gdzie a i b są liczbami całkowitymi.

Wartość teorii liczb całkowitych zespolonych polega nie tyle na tym, że jest ona uogólnieniem teorii zwykłych liczb całkowitych, ile na tym, że jako jej proste zastosowanie otrzymujemy dowody różnych twierdzeń o zwykłych liczbach całkowitych, które na innej drodze są o wiele trudniejsze.

Z definicji działań arytmetycznych na liczbach zespolonych wynika natychmiast, że suma, różnica i iloczyn dwu lub więcej liczb zespolonych całkowitych jest liczbą zespoloną całkowitą.

ĆWICZENIA. 1. Znaleźć wszystkie rozkłady liczby 0 na sumę kwadratów dwu liczb całkowitych zespolonych.

Odpowiedź: $0 = (a+bi)^2 + (\pm b \mp ai)^2$, gdzie a i b są dowolnymi liczbami całkowitymi rzeczywistymi, a znaki należy użyć wszędzie górne lub wszędzie dolne.

2. Zbadać jakie liczby całkowite zespolone $x+yi$ są sumami dwu kwadratów liczb całkowitych zespolonych.

Rozwiązanie. Na to, by liczba całkowita zespolona $x+yi$ była sumą dwu kwadratów liczb całkowitych zespolonych, potrzeba i wystarczy, żeby y było liczbą parzystą oraz w przypadku, gdy x jest postaci $4t+2$, żeby y było podzielne przez 4.

Warunek jest konieczny, bo jeżeli

$$x+yi = (a+bi)^2 + (c+di)^2,$$

to

$$x = a^2 - b^2 + c^2 - d^2, \quad y = 2(ab + cd).$$

Jak łatwo stąd widzieć, x jest postaci $4t+2$ tylko wtedy, gdy co najmniej jedna z liczb a i b , a jednocześnie co najmniej jedna z liczb c i d jest parzysta. Lecz wówczas liczba $ab+cd$ jest parzysta, więc liczba y jest podzielna przez 4.

Warunek jest dostateczny, bo jeżeli $x = 2t+1$ i $y = 2u$, to

$$x+yi = (t+1+ui)^2 + (u-ti)^2,$$

¹⁾ Ob. 2-e wydanie tej książki, Warszawa 1925, str. 215.

jeżeli $x = 4t + 2$ i $y = 4u$, to

$$x + yi = [t + u + 1 + (u - t)i]^2 + [t - u + 1 + (t + u)i]^2,$$

jeżeli $x = 4t$ i $y = 4u$, to

$$x + yi = (t + 1 + ui)^2 + (u + (1 - t)i)^2,$$

wreszcie, jeżeli $x = 4t$ i $y = 4u + 2$, to

$$x + yi = [t + u + 1 + (u + 1 - t)i]^2 + [t - u + (t + u)i]^2.$$

5. Dowieść, że na to, by liczba całkowita zespolona $x + yi$ była sumą trzech kwadratów liczb całkowitych zespolonych, potrzeba i wystarcza, żeby y było liczbą parzystą.

Wskazówka. Oprzeć się na ćwiczeniu 2 i na tożsamości

$$4t + 2 + 2ui = 4t + 1 + 2ui + 1^2.$$

4. Dowieść, że na to, by liczba całkowita zespolona $a + bi \neq 0$ była kwadratem liczby całkowitej zespolonej, potrzeba i wystarcza, żeby było

$$a^2 + b^2 = c^2, \quad c + a = 2x^2 \quad \text{i} \quad c - a = 2y^2,$$

gdzie c jest liczbą naturalną, a x i y — liczbami całkowitymi. Okazać, że wówczas

$$a + bi = (\pm x \pm yi)^2,$$

gdzie znaki należy brać jednakowe, gdy $b > 0$, i różne, gdy $b < 0$.

Uwaga. Jest to zarazem sposób zbadania, czy dana liczba całkowita zespolona jest kwadratem liczby całkowitej zespolonej, i ewentualnego znalezienia jej pierwiastków kwadratowych (zespolonych)¹⁾.

5. Opierając się na ćwiczeniu 4, zbadać, czy liczby $5 + 4i$ i $4 + 3i$ są kwadratami liczb całkowitych zespolonych, i znaleźć ich ewentualne pierwiastki kwadratowe.

Odpowiedź: $5 + 4i = (2 + i)^2 = (-2 - i)^2$. Liczba zaś $4 + 3i$ nie jest kwadratem liczby całkowitej zespolonej.

Dla liczby zespolonej $z = a + bi$ oznaczamy przez z' liczbę zespoloną sprzężoną czyli liczbę $z' = a - bi$.

Z definicji działań arytmetycznych na liczbach zespolonych wynika w jednej chwili, że dla wszelkich liczb zespolonych t, u :

$$(1) \quad \text{jeżeli } z = t + u, \text{ to } z' = t' + u',$$

$$(2) \quad \text{jeżeli } z = t - u, \text{ to } z' = t' - u',$$

$$(3) \quad \text{jeżeli } z = tu, \text{ to } z' = t'u'.$$

Liczy sprzężone z i z' są zawsze obie całkowite lub obie niecałkowite. Liczbą (z') , sprzężoną z , jest zawsze liczba z .

¹⁾ Por. moją książkę *Zasady algebry wyższej*, Monografie Matematyczne, Warszawa-Wrocław 1946, str. 172.

Iloczyn zz' dwu liczb sprzężonych nazywamy *normą* liczby z i oznaczamy przez $N(z)$:

$$N(z) = zz';$$

zatem, jeżeli $z = a + bi$ (gdzie a i b są liczbami rzeczywistymi), to

$$N(z) = a^2 + b^2.$$

Norma liczby zespolonej jest więc zawsze liczbą rzeczywistą nieujemną, równą zero tylko w razie $a = b = 0$, tj. dla $z = 0$.

Norma liczby zespolonej całkowitej, różnej od zera, jest zawsze liczbą naturalną.

Liczy sprzężone mają tę samą normę. O liczbie całkowitej zespolonej z mówimy, że jest *podzielna* przez liczbę t , jeżeli istnieje taka liczba całkowita zespolona u , że

$$(4) \quad z = tu.$$

Piszemy też wówczas $t|z$.

Badanie, czy liczba zespolona $a + bi$ jest podzielna przez liczbę zespoloną $c + di$ różną od zera, sprowadza się z łatwością do badania podzielności liczb całkowitych rzeczywistych. Ze wzoru bowiem

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i$$

wynika natychmiast, że na to, by

$$c + di | a + bi,$$

potrzeba i wystarcza, żeby

$$c^2 + d^2 | ac + bd \quad \text{i} \quad c^2 + d^2 | bc - ad.$$

Tak np.

$$\begin{array}{llll} 3 + 5i | 21 + i, & \text{gdź} & 34 | 68 & \text{i} & 34 | -102, \\ 1 + i | 2, & \text{gdź} & 2 | 2 & \text{i} & 2 | -2. \end{array}$$

Natomiast

$$1 - 2i \text{ non} | 1 + 2i, \quad \text{gdź} \quad 5 \text{ non} | -3.$$

Z (5) wynika, że jeżeli $t|z$, to również $t'|z'$ i jeżeli $z = tu$, to

$$zz' = tu t'u' = t't'uu',$$

skąd na mocy definicji normy:

$$(5) \quad N(z) = N(t)N(u).$$

Zatem: *norma iloczynu jest iloczynem norm.*

Twierdzenie to uogólniamy przez indukcję na iloczyn dowolnej skończonej liczby czynników.

Wzór (5) dowodzi też, że $N(t)|N(z)$, a zatem:

Jeżeli liczba całkowita zespolona t jest dzielnikiem liczby z , to norma liczby t jest dzielnikiem normy liczb z .

Ale nie jest na odwrót, gdyż np. $N(1-2i)=N(1+2i)$, lecz $1-2i \nmid 1+2i$.

Dwie liczby całkowite zespolone (różne od zera), które są wzajemnie przez siebie podzielne, nazywamy *stowarzyszonymi*.

Na to więc, by liczby z i t były stowarzyszone, potrzeba i wystarcza, żeby $t|z$ i $z|t$. Wówczas mamy też $N(t)|N(z)$ i $N(z)|N(t)$, co z uwagi na to, że norma liczby całkowitej zespolonej różnej od 0 jest liczbą naturalną, daje $N(t)=N(z)$.

Zatem: *liczby stowarzyszone mają równe normy* (ale nie na odwrót, gdyż np. liczby $1-2i$ i $1+2i$, które mają równe normy, nie są stowarzyszone, gdyż jak widzieliśmy, $1-2i \nmid 1+2i$).

Zajmiemy się teraz wyznaczeniem wszystkich liczb stowarzyszonych z daną liczbą całkowitą zespoloną $z \neq 0$.

Niech t będzie jedną z nich. Jest więc $t=zu$ przy pewnym całkowitym zespolonym u , skąd

$$(6) \quad N(t)=N(z)N(u),$$

a ponieważ liczby stowarzyszone mają równe normy, przeto $N(z)=N(t)$; zarazem $N(z) \neq 0$, gdyż $z \neq 0$. Równość (6) daje więc $N(u)=1$.

Niech $u=a+bi$, skąd

$$a^2+b^2=1,$$

a więc albo $a=\pm 1$ i $b=0$, albo $a=0$ i $b=\pm 1$. Zatem u jest jedną z czterech liczb

$$1, \quad -1, \quad i, \quad -i,$$

a więc $t=zu$ — jedną z czterech liczb

$$(7) \quad z, \quad -z, \quad iz, \quad -iz.$$

Każda liczba stowarzyszona z liczbą z jest przeto jedną z liczb (7). Na odwrót — jak łatwo widzieć — każda z liczb (7) jest stowarzyszona z liczbą z , gdyż $z=(-1)(-z)=(-i)iz=i(-iz)$. Mamy zatem

Twierdzenie 1. *Dla każdej liczby całkowitej zespolonej z , różnej od 0, istnieją cztery i tylko cztery liczby z nią stowarzyszone, mianowicie liczby (7).*

Jak łatwo widzieć (wobec $z \neq 0$), wszystkie te cztery liczby są różne.

W zagadnieniach dotyczących podzielności liczb, można oczywiście liczby stowarzyszone zastępować jedne przez drugie. Jeżeli bowiem z jest podzielne przez t , to — jak łatwo widzieć — każda liczba stowarzyszona z z , jest podzielna przez każdą liczbę stowarzyszoną z t .

Łatwo też widzieć, że jeżeli liczba z jest stowarzyszona z liczbą t , to liczba z' jest stowarzyszona z liczbą t' .

Jeżeli liczby zespolone całkowite z_1 i z_2 są podzielne przez t , to ich suma i różnica też jest podzielna przez t . Jeżeli bowiem $z_1=tu$ i $z_2=tv$, to $z_1 \pm z_2=t(u \pm v)$.

Jeżeli liczba całkowita zespolona z jest podzielna przez t , a t przez u , to z jest podzielne przez u . Jeżeli bowiem $z=tw$ i $t=uv$, to $z=uvw$.

Wynika stąd dalej, że jeżeli liczba zespolona całkowita t jest wspólnym dzielnikiem liczb zespolonych całkowitych $z_1, z_2, \dots, z_n$ i jeżeli $u_1, u_2, \dots, u_n$ są liczbami całkowitymi zespolonymi, to t jest dzielnikiem liczby $z_1u_1+z_2u_2+\dots+z_nu_n$.

§ 2. Algorytm kolejnych dzielen i największy wspólny dzielnik liczb całkowitych zespolonych. Udowodnimy

Twierdzenie 2. *Jeżeli z i $t \neq 0$ są liczbami całkowitymi zespolonymi, to istnieją takie liczby całkowite zespolone c i r , że*

$$(8) \quad z=ct+r,$$

oraz

$$(9) \quad N(r) \leq \frac{1}{2}N(t),$$

a więc też $N(r) < N(t)$.

Dowód. Niech

$$(10) \quad z/t = x + yi,$$

gdzie x i y są liczbami rzeczywistymi wymiernymi. Oznaczając przez ξ i η odpowiednio najbliższe do x i y liczby całkowite, możemy napisać:

$$(11) \quad x = \xi + x_1, \quad y = \eta + y_1,$$

gdzie x_1 i y_1 są liczbami rzeczywistymi wymiernymi o wartościach bezwzględnych

$$(12) \quad |x_1| \leq \frac{1}{2}, \quad |y_1| \leq \frac{1}{2}.$$

Niech

$$(13) \quad c = \xi + \eta i, \quad r = z - ct;$$

są to liczby całkowite zespolone i spełniają one wzór (8). Zarazem na mocy (10), (11) i (13)

$$r = z - ct = (x + yi)t - (\xi + \eta i)t = (x_1 + y_1 i)t.$$

Ponieważ norma iloczynu jest iloczynem norm, więc na mocy (12)

$$N(r) = N(x_1 + y_1 i)N(t) = (x_1^2 + y_1^2)N(t), \quad x_1^2 + y_1^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2},$$

skąd nierówność (9), c. b. d. d.

Udowodnione twierdzenie 2 daje dla liczb całkowitych zespolonych algorytm analogiczny do algorytmu Euklidesa.

Wyznamy bowiem dla liczb całkowitych zespolonych z i $t \neq 0$ liczby całkowite zespolone c i r , spełniające warunki twierdzenia 2. Ze wzoru (8) wynika natychmiast, że liczby z i t mają te same wspólne dzielniki co liczby t i r . Zarazem w myśl wzoru (5) jest $N(r) < N(t)$. Znajdowanie więc wszystkich wspólnych dzielników liczb z i t sprowadza się do znajdowania wszystkich wspólnych dzielników liczb t i r , przy czym $N(r) < N(t)$.

Jeżeli $r = 0$, to wspólne dzielniki liczb z i t pokrywają się oczywiście z dzielnikami liczby t .

Jeżeli zaś $r \neq 0$, to możemy postąpić z liczbami t i r jak poprzednio z liczbami z i t , przez co znajdowanie wspólnych dzielników liczb t i r sprowadza się do znajdowania wspólnych dzielników liczb r i r_1 , gdzie $N(r_1) < N(r)$.

Jeżeli $r_1 \neq 0$, wyznaczamy nową liczbę r_2 itd.

Ciąg liczb $r, r_1, r_2, \dots$ nie może być nieskończony, gdyż normy tych liczb tworzą ciąg malejący liczb naturalnych. Dojdziemy więc do liczby $r_n = 0$, a wówczas wspólne dzielniki liczb r_{n-2} i r_{n-1} pokrywają się z dzielnikami liczby r_{n-1} . Ostatecznie więc dochodzimy do wniosku, że istnieje taka liczba całkowita zespolona g , której dzielniki pokrywają się ze wspólnymi dzielnikami liczb z i t .

Wynika stąd natychmiast, że dla każdych dwu liczb całkowitych zespolonych różnych od 0 istnieje co najmniej jeden taki ich wspólny dzielnik, który jest podzielny przez każdy ich wspólny dzielnik. Naturalną więc rzeczą jest nazywać go *największym wspólnym dzielnikiem* liczb całkowitych zespolonych.

Zbadamy teraz, ile takich największych wspólnych dzielników mają dwie liczby całkowite zespolone. Niech d i δ będą dwoma takimi wspólnymi dzielnikami liczb z i t , które są podzielne przez każdy ich wspólny dzielnik. Liczby d i δ są więc wzajemnie przez siebie podzielne: są zatem liczbami stowarzyszonymi. Wynika stąd na mocy twierdzenia 2

Wniosek. Dla każdych dwu liczb zespolonych całkowitych różnych od 0 istnieją cztery największe wspólne dzielniki: są one ze sobą stowarzyszone.

Właściwie i liczby całkowite wymierne mają zawsze dwa różniące się znakiem wspólne dzielniki, podzielne przez każdy wspólny dzielnik tych liczb, ale przy obliczaniu liczby wspólnych dzielników nie uwzględniamy dzielników, różniących się tylko znakiem. Podobnie można by i dla liczb całkowitych zespolonych nie uwzględniać czterech dzielników stowarzyszonych i mówić wobec tego tylko o jednym największym wspólnym dzielniku. Jest to oczywiście tylko sprawa mniej lub więcej dogodnej umowy.

PRZYKŁADY. 1. Wyznamy za pomocą powyższego algorytmu największe wspólne dzielniki liczb $6 - 17i$ i $18 + i$. Znajdujemy tu kolejno:

$$\frac{6 - 17i}{18 + i} = \frac{(6 - 17i)(18 - i)}{18^2 + 1} = \frac{91 - 312i}{325} = -i + \frac{91 + 13i}{325},$$

$$6 - 17i = -i(18 + i) + (5 + i),$$

$$\frac{18 + i}{5 + i} = \frac{(18 + i)(5 - i)}{5^2 + 1} = \frac{91 - 13i}{26} = 3 + \frac{1 - i}{2},$$

$$18 + i = 3(5 + i) + 3 - 2i,$$

$$\frac{5 + i}{3 - 2i} = \frac{(5 + i)(3 + 2i)}{3^2 + 2^2} = 1 + i.$$

Największymi wspólnymi dzielnikami liczb $6 - 17i$ i $18 + i$ są więc: liczba $3 - 2i$ oraz liczby z nią stowarzyszone: $-3 + 2i$, $2 + 3i$ i $-2 - 3i$.

2. Wyznaczmy największe wspólne dzielniki liczb $2+3i$ i $2-3i$. Znajdujemy tu kolejno:

$$\begin{aligned}\frac{2+3i}{2-3i} &= \frac{(2+3i)^2}{2^2+3^2} + \frac{5+12i}{13} = i + \frac{5-i}{13}, \\ \frac{2+3i}{2-3i} &= i(2-3i) + i - 1, \\ \frac{2+3i}{i-1} &= \frac{-(2-3i)(i+1)}{2} = \frac{-5+i}{2} = -3 + \frac{1+i}{2}, \\ 2-3i &= -3(i-1) - 1.\end{aligned}$$

Największymi wspólnymi dzielnikami liczb $2+3i$ i $2-3i$ są więc: liczba 1 oraz liczby z nią stowarzyszone: -1 , i i $-i$.

3. Wyznaczmy największe wspólne dzielniki liczb $31+i$ i $5+i$. Znajdujemy:

$$\frac{31+i}{5+i} = \frac{31+i(5-i)}{5^2+1^2} = \frac{156-26i}{26} = 6-i.$$

Największymi wspólnymi dzielnikami liczb $31+i$ i $5+i$ są więc: liczba $5+i$ oraz liczby z nią stowarzyszone:

$$-5-i, \quad -1+3i \quad i \quad 1-3i.$$

Łatwo widzieć, że największe wspólne dzielniki dwu liczb całkowitych zespolonych mają wśród wszystkich wspólnych dzielników tych liczb największą normę i na odwrót. Można by więc też tę własność przyjąć za definicję największych wspólnych dzielników, ale wtedy dowód zasadniczej ich własności (podzielności przez każdy wspólny dzielnik) byłby trudniejszy.

Można też z łatwością oprzeć teorię największego wspólnego dzielnika dwu lub więcej liczb całkowitych zespolonych na rozważaniu form liniowych, podobnie jak dla liczb całkowitych wymiernych. Niech mianowicie $a_1, a_2, \dots, a_m$ będą liczbami całkowitymi zespolonymi różnymi od zera, a Z — zbiorem wszystkich różnych od zera liczb postaci

$$a_1 z_1 + a_2 z_2 + \dots + a_m z_m,$$

gdzie $z_1, z_2, \dots, z_m$ są liczbami całkowitymi zespolonymi. Wreszcie, niech N będzie zbiorem norm liczb należących do zbioru Z ; jest to więc pewien zbiór liczb naturalnych. Oznaczmy przez n najmniejszą spośród liczb należących do zbioru N . Istnieje więc w zbiorze Z taka liczba ξ , dla której $N(\xi) = n$, a przeto istnieją w nim też takie liczby całkowite zespolone $\xi_1, \xi_2, \dots, \xi_m$, że

$$(14) \quad \xi = a_1 \xi_1 + a_2 \xi_2 + \dots + a_m \xi_m.$$

Okażemy, że każda liczba zbioru Z jest podzielna przez ξ . Istotnie, niech z będzie jakąkolwiek liczbą ze zbioru Z . Istnieją więc takie liczby całkowite zespolone $z_1, z_2, \dots, z_m$, że

$$(15) \quad z = a_1 z_1 + a_2 z_2 + \dots + a_m z_m.$$

Ponadto w myśl twierdzenia 2 istnieją takie liczby całkowite zespolone c i r , że

$$(16) \quad z = c\xi + r \quad i \quad N(r) < N(\xi).$$

Gdyby było $r \neq 0$, to liczba r należałaby do zbioru Z , ponieważ wobec (14), (15) i (12) jest

$$r = z - c\xi = a_1(z_1 - c\xi_1) + a_2(z_2 - c\xi_2) + \dots + a_m(z_m - c\xi_m),$$

a liczby $z_j - c\xi_j$, dla $j=1, 2, \dots, m$ są całkowite. Lecz w takim razie r byłoby wobec (16) liczbą ze zbioru Z o normie mniejszej od normy n liczby ξ , wbrew określeniu liczby n . Musi więc być $r=0$, skąd na mocy (16), $z=c\xi$, a przeto $\xi|z$.

Ponieważ — jak łatwo widzieć — każda z liczb $a_1, a_2, \dots, a_m$ należy do zbioru Z , więc z udowodnionej własności liczb należących do tego zbioru wynika, że liczba ξ jest wspólnym dzielnikiem liczb $a_1, a_2, \dots, a_m$.

Niech teraz δ będzie jakimkolwiek wspólnym dzielnikiem tych liczb. Istnieją wobec tego takie liczby całkowite zespolone $t_1, t_2, \dots, t_m$, że $a_j = t_j \delta$ dla $j=1, 2, \dots, m$, skąd na mocy (14)

$$\xi = (t_1 \xi_1 + t_2 \xi_2 + \dots + t_m \xi_m) \delta,$$

a przeto $\delta|\xi$. Liczba ξ jest więc takim wspólnym dzielnikiem liczb $a_1, a_2, \dots, a_m$, który jest podzielny przez każdy wspólny dzielnik tych liczb. Dowiedliśmy zarazem, że dzielnik ten daje się przedstawić w postaci (14), gdzie $\xi_1, \xi_2, \dots, \xi_m$ są liczbami całkowitymi zespolonymi.

Każde dwie liczby całkowite zespolone a i b mają oczywiście co najmniej 4 wspólne dzielniki, mianowicie 1, -1 , i , $-i$.

Jeżeli nie mają one prócz tych 4 liczb żadnych innych wspólnych dzielników, to mówimy, że są *względnie pierwsze* i piszemy $(a, b) = 1$.

Łatwo widzieć, że istnieją wtedy liczby całkowite zespolone x i y , spełniające równanie

$$(17) \quad ax + by = 1.$$

Jeżeli bowiem $(a, b) = 1$, to liczba ζ , wyznaczona ze wzoru (14) dla $a = a_1$, $b = a_2$ i $m = 2$, musi być jedną z liczb $1, -1, i, -i$; wobec tego jedna z liczb $\zeta, -\zeta, i\zeta, -i\zeta$ musi być równa 1, skąd wnosimy w jednej chwili, że dla pewnych całkowitych zespolonych x i y musi zachodzić równość (17).

Na odwrót z (17) wynika, że każdy wspólny dzielnik liczb a i b jest dzielnikiem liczby 1, a więc że liczby a i b nie mają wspólnego dzielnika różnego od liczb $1, -1, i, -i$, czyli że $(a, b) = 1$.

Udowodniliśmy zatem

Twierdzenie 3. *Na to, by liczby zespolone całkowite a i b były względnie pierwsze, potrzeba i wystarczy żeby istniały takie liczby całkowite zespolone x i y , dla których $ax + by = 1$.*

Niech teraz a, b i c będą liczbami całkowitymi zespolonymi; dla których $(a, b) = 1$ i $b|ac$. Okażemy, że wówczas $b|c$.

Istotnie, wobec $(a, b) = 1$ istnieją na mocy twierdzenia 3 liczby całkowite zespolone x i y , spełniające równanie (17), skąd mnożąc przez c ,

$$(18) \quad acx + bcy = c.$$

Alc $b|ac$ w myśl założenia i $b|bc$ dla wszelkich b . Wobec (18) jest zatem $b|c$. Udowodniliśmy więc

Twierdzenie 4. *Dla wszelkich liczb całkowitych zespolonych a, b i c z $(a, b) = 1$ i $b|ac$ wynika $b|c$.*

Innym wnioskiem z twierdzenia 3 jest

Twierdzenie 5. *Jeżeli $(a, b) = 1$ i $(a, c) = 1$, to $(a, bc) = 1$.*

Dowód. Jeżeli $(a, b) = 1$ i $(a, c) = 1$, to istnieją takie liczby całkowite zespolone x, y, u i v , że $ax + by = 1$ i $au + cv = 1$. Mnożąc stronami, otrzymujemy $a[x(au + cv) + buy] + bcyv = 1$, skąd $(a, bc) = 1$, c. b. d. o.

§ 3. Najmniejsza wspólna wielokrotność liczb całkowitych zespolonych. Niech $a_1, a_2, \dots, a_m$ będą liczbami całkowitymi zespolonymi różnymi od zera. Istnieją oczywiście różne od zera wspólne wielokrotności tych liczb, np. ich iloczyn. Wśród tych wielokrotności istnieją oczywiście najmniejsze, tj. takie, których normy są niewiększe od normy żadnej innej wspólnej wielokrotności tychże liczb. Niech ν będzie jedną z nich. Okażemy, że każda wspólna wielokrotność liczb $a_1, a_2, \dots, a_m$ jest podzielna przez ν .

Istotnie, niech z będzie jakąkolwiek wspólną wielokrotnością tych liczb. W myśl twierdzenia 2 istnieją takie liczby całkowite zespolone c i r , że $z = c\nu + r$ i $N(r) < N(\nu)$.

Gdyby było $r \neq 0$, to r byłoby — jak łatwo widzieć — wspólną wielokrotnością liczb $a_1, a_2, \dots, a_m$ o normie mniejszej od normy liczby ν wbrew określeniu tej liczby. Musi więc być $r = 0$, skąd $z = c\nu$, a przeto $\nu|z$. Wynika stąd natychmiast, że wśród wspólnych wielokrotności liczb całkowitych zespolonych $a_1, a_2, \dots, a_m$ istnieje co najmniej jedna taka, która jest dzielnikiem każdej wspólnej wielokrotności tych liczb.

Norma takiej wielokrotności nie jest większa od żadnej różnej od zera wspólnej wielokrotności liczb $a_1, a_2, \dots, a_m$. Nazywamy taką wielokrotność *najmniejszą wspólną wielokrotnością liczb $a_1, a_2, \dots, a_m$* .

Łatwo widzieć, że wszystkie najmniejsze wspólne wielokrotności liczb $a_1, a_2, \dots, a_m$ są stowarzyszone oraz że norma ich jest najmniejsza wśród wspólnych wielokrotności tych liczb.

§ 4. Liczby zespolone pierwsze. Ponieważ każda liczba całkowita zespolona ma co najmniej 4 różne dzielniki (mianowicie $1, -1, i, -i$), każda zaś liczba całkowita zespolona z , która nie jest stowarzyszona z liczbą 1, ma oczywiście prócz nich jeszcze 4 inne dzielniki (mianowicie $z, -z, iz, -iz$), więc każda taka liczba całkowita zespolona ma co najmniej 8 różnych dzielników.

Liczby całkowite zespolone, mające dokładnie 8 dzielników, nazywamy *pierwszymi*.

Innymi słowy, liczba zespolona pierwsza z jest to taka liczba całkowita zespolona, która nie jest stowarzyszona z liczbą 1 i nie ma żadnego dzielnika nie stowarzyszonego ani z liczbą 1, ani z liczbą z .

Jak łatwo widzieć, definicja ta jest równoważna następującej:

Liczba zespolona pierwsza jest to liczba całkowita zespolona o normie większej od 1, która nie jest iloczynem dwu liczb całkowitych zespolonych o normach większych od 1.

Istotnie, jeżeli ζ jest liczbą zespoloną całkowitą i $N(\zeta) > 1$ oraz jeżeli $\zeta = \mu\nu$, gdzie $N(\mu) > 1$ i $N(\nu) > 1$, to liczba μ nie może być stowarzyszona ani z 1, bo wtedy byłoby $N(\mu) = 1$, ani z ζ , bo wtedy byłoby $N(\mu) = N(\zeta)$, skąd wobec $N(\zeta) = N(\mu)N(\nu)$ wynikałoby $N(\nu) = 1$ wbrew założeniu.

Taka liczba ζ ma więc dzielnik μ nie stowarzyszony ani z 1, ani z ζ , a zatem nie jest liczbą pierwszą.

Na odwrót, jeżeli liczba zespolona ζ o normie $N(\zeta) > 1$ nie jest pierwsza, to ma ona w myśl definicji dzielnik μ nie stowarzyszony ani z 1, ani z ζ . Jest więc wówczas $\zeta = \mu\nu$, gdzie ν jest liczbą całkowitą zespoloną.

Gdyby było $N(\mu) = 1$, to liczba μ byłaby stowarzyszona z 1, wbrew założeniu (jeżeli bowiem dla liczby całkowitej zespolonej $a + bi$ jest $N(a + bi) = 1$, to $a^2 + b^2 = 1$ i wobec tego, że liczby a i b są całkowite wymierne, musiałyby być albo $a = \pm 1$ i $b = 0$, albo $a = 0$ i $b = \pm 1$).

Gdyby zaś było $N(\nu) = 1$, to liczba ν byłaby stowarzyszona z 1, a wtedy wobec $\zeta = \mu\nu$ liczba μ byłaby stowarzyszona z liczbą ζ wbrew założeniu.

Jest więc $N(\mu) > 1$ i $N(\nu) > 1$, a zatem liczba ζ jest iloczynem dwu liczb całkowitych zespolonych o normach większych od 1.

Jak łatwo widzieć, każda liczba zespolona całkowita, która jest stowarzyszona lub sprzężona z liczbą zespoloną pierwszą, jest liczbą zespoloną pierwszą.

Twierdzenie 6. Każda liczba zespolona całkowita o normie większej od 1 jest iloczynem skończenie wielu liczb zespolonych pierwszych.

Dowód. Przypuśćmy, że tak nie jest i zaliczmy do zbioru M liczbę naturalną $n > 1$ wtedy i tylko wtedy, gdy istnieje liczba całkowita zespolona o normie n , nie będąca iloczynem skończenia wielu liczb zespolonych pierwszych. Niech m będzie najmniejszą liczbą naturalną, należącą do zbioru M . Istnieje więc liczba całkowita zespolona z o normie m , nie będąca iloczynem skończenia wielu liczb zespolonych pierwszych. Liczba z , mająca w myśl założenia normę $m > 1$, nie jest więc pierwsza; przeto — jak dowiedliśmy — jest ona iloczynem dwu liczb całkowitych zespolonych μ i ν o normach większych od 1, a zarazem — wobec $m = N(z) = N(\mu\nu) = N(\mu)N(\nu)$ — o normach mniejszych od m . Z określenia liczby m wynika jednak, że wtedy każda z liczb μ i ν jest iloczynem skończenia wielu liczb zespolonych pierwszych. Zatem też liczba $z = \mu\nu$ byłaby takim iloczynem wbrew określeniu tej liczby. Tym samym twierdzenie jest dowiedzione.

Każda liczba zespolona pierwsza π ma na mocy definicji dokładnie 8 dzielników zespolonych:

$$1, \quad -1, \quad i, \quad -i, \quad \pi, \quad -\pi, \quad i\pi, \quad -i\pi.$$

Wynika stąd natychmiast, że jeżeli liczba zespolona całkowita λ nie jest podzielna przez liczbę zespoloną pierwszą π , to $(\lambda, \pi) = 1$.

Liczba naturalna, która jest pierwsza w dziedzinie liczb zespolonych, jest też oczywiście pierwsza w dziedzinie liczb naturalnych. Natomiast liczba pierwsza w dziedzinie liczb naturalnych może nie być pierwsza w dziedzinie liczb zespolonych.

Taka jest np. już liczba 2, gdyż

$$2 = (1+i)(1-i), \quad \text{ale} \quad N(1+i) = N(1-i) = 2 > 1.$$

Co do liczb $1+i$ i $1-i$, to są one pierwsze w dziedzinie liczb zespolonych. Istotnie, z $1 \pm i = \mu\nu$ wynika, że

$$N(\mu)N(\nu) = N(\mu\nu) = N(1 \pm i) = 2,$$

a więc (wobec tego, że norma liczby całkowitej zespolonej jest liczbą naturalną) musi być $N(\mu) = 1$ lub $N(\nu) = 1$, co dowodzi (p. str. 390), że μ lub ν byłoby liczbą stowarzyszoną z 1.

Liczby $1+i$ i $1-i$ są stowarzyszone, gdyż $1-i = -i(1+i)$. Liczba 2 jest więc stowarzyszona z kwadratem liczby pierwszej zespolonej.

Opierając się na twierdzeniu 4, można łatwo dowieść, że jeżeli dwu rozkładów liczby całkowitej zespolonej na czynniki całkowite zespolone nie uważać za różne, gdy różnią się one tylko porządkiem czynników lub czynnikami stowarzyszonymi, to każda liczba całkowita zespolona (o normie większej od 1) ma dokładnie jeden rozkład na czynniki zespolone pierwsze.

Nasuwa się pytanie, które z liczb całkowitych zespolonych są pierwsze.

Zbadamy przede wszystkim, które z liczb naturalnych są pierwsze w dziedzinie liczb zespolonych. Muszą to być oczywiście liczby pierwsze w dziedzinie liczb naturalnych, a przy tym nieparzyste, gdyż liczba 2 — jak okazaliśmy — nie jest pierwsza w dziedzinie liczb zespolonych. Mamy więc do rozpatrzenia liczby naturalne pierwsze formy $4k+1$ i formy $4k+3$.

Niech p będzie liczbą naturalną pierwszą formy $4k+1$. W myśl twierdzenia Fermata z Rozdziału IV (§ 4, str. 73) istnieją takie liczby naturalne a i b , że $p = a^2 + b^2$, skąd $p = (a+bi)(a-bi)$, a zarazem $N(a+bi) = a^2 + b^2 = p > 1$. Liczba p nie jest więc pierwsza w dziedzinie liczb zespolonych.

Natomiast — jak łatwo widzieć — czynniki $a+bi$ i $a-bi$ są już liczbami zespolonymi pierwszymi. Istotnie, gdyby było $a+bi = \mu\nu$, gdzie

$$(19) \quad N(\mu) > 1 \quad \text{i} \quad N(\nu) > 1,$$

to mielibyśmy $a-bi = \mu'\nu'$, skąd

$$p = (a+bi)(a-bi) = \mu\mu'\nu\nu' = N(\mu)N(\nu),$$

co wobec (19) jest niemożliwe, ponieważ liczba p jest pierwsza w dziedzinie liczb naturalnych.

Zatem *czynniki liczb naturalnych pierwszych formy $4k+1$ są liczbami zespolonymi pierwszymi.*

Łatwo widzieć, że czynniki te nie są ze sobą stowarzyszone. Istotnie, nie może być $a+bi = a-bi$, gdyż wynikałoby stąd, że $b=0$, a więc $p=a^2$. Nie może też być $a+bi = -(a-bi)$, gdyż wtedy byłoby $a=0$, a więc $p=b^2$. Niemożliwe jest również, żeby było $a+bi = i(a-bi)$, gdyż wówczas byłoby $a=b$, a więc $p=2a^2$. Wreszcie nie jest także $a+bi = -i(a-bi)$, gdyż dałoby to $a=-b$, skąd znowu $p=2a^2$.

Natomiast *liczby naturalne pierwsze formy $4k+3$ są pierwsze w dziedzinie liczb zespolonych.*

Istotnie, gdyby dla takiej liczby p istniał rozkład na dwa czynniki całkowite zespolone o normach większych od 1

$$p = (a+bi)(c+di),$$

to normując obie strony tej równości, otrzymalibyśmy

$$p^2 = (a^2 + b^2)(c^2 + d^2),$$

gdzie $a^2 + b^2 > 1$ i $c^2 + d^2 > 1$, a ponieważ p jest liczbą pierwszą w dziedzinie liczb naturalnych, więc musiałoby być $p = a^2 + b^2$, co dla $p = 4k+3$ jest niemożliwe (ob. Rozdział IV, § 5, lemat 2, str. 76).

Pośród liczb naturalnych pierwszymi w dziedzinie liczb zespolonych są więc tylko liczby pierwsze formy $4k+3$; pierwszymi są też: liczba $1+i$ oraz czynniki zespolone sprzężone liczb pierwszych formy $4k+1$.

Okażemy, że prócz tych liczb, jak też liczb z nimi stowarzyszonych, nie ma w dziedzinie liczb zespolonych żadnych innych liczb pierwszych.

Istotnie, niech π będzie liczbą pierwszą w dziedzinie liczb zespolonych.

Jeżeli jest ona stowarzyszona z liczbą naturalną n , to — jak łatwo widzieć — liczba n też musi być pierwsza w dziedzinie liczb zespolonych, a zatem, jako liczba naturalna, musi ona być liczbą pierwszą formy $4k+3$.

Jeżeli natomiast π nie jest liczbą stowarzyszoną z żadną liczbą naturalną, to $\pi = a+bi$, gdzie a i b są liczbami całkowitymi wymiernymi i $b \neq 0$. Ale skoro π jest liczbą zespoloną pierwszą, to jest nią również sprzężona z nią liczba $\pi' = a-bi$; zarazem $a^2 + b^2 = \pi\pi'$. Otóż gdyby liczba $N(\pi) = a^2 + b^2$ nie była pierwsza w dziedzinie liczb naturalnych, to (z uwagi, że $N(\pi) > 1$, skoro π jest liczbą pierwszą zespoloną) byłoby $\pi\pi' = a^2 + b^2 = kl$, gdzie k i l są liczbami naturalnymi większymi od 1. W iloczynie kl , jako podzielnym przez liczbę zespoloną pierwszą π , przynajmniej jeden z czynników musiałby być podzielny przez π ; niech np. $k = \pi\tau$. Liczba τ nie byłaby stowarzyszona z 1, skoro liczba π nie jest stowarzyszona z żadną liczbą naturalną. Ale w takim razie z równości $\pi\pi' = kl$ wynikałoby, że $\pi' = l\tau$, gdzie ani l , ani τ nie jest liczbą stowarzyszoną z 1, co niemożliwe, gdyż π' jest liczbą pierwszą. Zatem liczba $a^2 + b^2 = \pi\pi'$ jest pierwsza w dziedzinie liczb naturalnych i przeto, jako suma dwu kwadratów, jest ona bądź liczbą 2, bądź liczbą pierwszą formy $4k+1$. Liczba π jest więc czynnikiem zespolonym bądź liczby 2, bądź liczby pierwszej formy $4k+1$.

Udowodniliśmy w ten sposób

Twierdzenie 7. *Liczbami pierwszymi w dziedzinie liczb całkowitych zespolonych są tylko:*

$$1^0 \quad 1+i,$$

$$2^0 \quad \text{czynniki zespolone sprzężone liczb pierwszych formy } 4k+1.$$

$$3^0 \quad \text{liczby naturalne pierwsze formy } 4k+3$$

oraz liczby stowarzyszone z liczbami 1^0 , 2^0 i 3^0 .

Oto wszystkie liczby zespolone pierwsze, po jednej z każdej czwórki liczb stowarzyszonych, o normie niewiększej od 100:

$$\begin{array}{cccccc} 1+i, & 1\pm 2i, & 3, & 2\pm 3i, & 1\pm 4i, & 2\pm 5i, & 1\pm 6i, \\ 4\pm 5i, & 7, & 2\pm 7i, & 5\pm 6i, & 3\pm 8i, & 5\pm 8i, & 4\pm 9i. \end{array}$$

§ 5. Rozkład liczb całkowitych zespolonych na czynniki pierwsze. Okażemy teraz, jak można liczbę całkowitą zespoloną z rozłożyć na czynniki zespolone pierwsze.

Niech $N(z) = n$. Każdy czynnik pierwszy liczby z jest też oczywiście czynnikiem pierwszym jej normy $n = zz'$, czynniki zaś zespolone pierwsze liczby naturalnej n możemy wyznaczyć z łatwością, wychodząc z jej rozkładu na czynniki naturalne pierwsze. Niech bowiem

$$(20) \quad n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l},$$

gdzie p_j dla $j = 1, 2, \dots, k$ są liczbami pierwszymi formy $4t+1$, a q_j dla $j = 1, 2, \dots, l$ są liczbami pierwszymi formy $4t+3$. Oznaczmy przez π_j i π'_j dla $j = 1, 2, \dots, k$ czynniki zespolone sprzężone liczby p_j ; znajdziemy je jako $\pi = a+bi$ i $\pi' = a-bi$, rozkładając liczbę p na sumę dwu kwadratów $p = a^2 + b^2$. Wówczas rozkład liczby n na czynniki zespolone pierwsze jest następujący:

$$(21) \quad n = (-i)^{\alpha} (1+i)^{2\alpha} \pi_1^{\alpha_1} \pi_1'^{\alpha_1} \pi_2^{\alpha_2} \pi_2'^{\alpha_2} \dots \pi_k^{\alpha_k} \pi_k'^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}.$$

Wobec $n = zz'$ widzimy stąd, że musi być

$$(22) \quad z = i^r (1+i)^{\lambda} \pi_1^{\lambda_1} \pi_1'^{\lambda_1'} \pi_2^{\lambda_2} \pi_2'^{\lambda_2'} \dots \pi_k^{\lambda_k} \pi_k'^{\lambda_k'} q_1^{\mu_1} q_2^{\mu_2} \dots q_l^{\mu_l},$$

gdzie r jest jedną z liczb 1, 2, 3, 4, wszystkie zaś pozostałe wykładniki $\lambda, \lambda_1, \lambda'_1, \dots, \lambda_k, \lambda'_k, \mu_1, \dots, \mu_l$ są liczbami całkowitymi nieujemnymi. Normując obie strony równości (22), otrzymamy z uwagi na to, że $N(\pi_j) = p_j$ i $N(q_j) = q_j^2$

$$N(z) = 2^{\lambda} p_1^{\lambda_1 + \lambda_1'} p_2^{\lambda_2 + \lambda_2'} \dots p_k^{\lambda_k + \lambda_k'} q_1^{2\mu_1} q_2^{2\mu_2} \dots q_l^{2\mu_l},$$

skaż wobec $N(z) = n$ i (21) otrzymujemy przez porównanie wykładników przy jednakowych liczbach pierwszych:

$$(23) \quad \begin{aligned} \lambda &= \alpha, & \lambda_1 + \lambda'_1 &= \alpha_1, & \lambda_2 + \lambda'_2 &= \alpha_2, & \dots, & \lambda_k + \lambda'_k &= \alpha_k, \\ 2\mu_1 &= \beta_1, & 2\mu_2 &= \beta_2, & \dots, & 2\mu_l &= \beta_l. \end{aligned}$$

Równości (23) wskazują, że wszystkie wykładniki β muszą być parzyste.

A więc, jeżeli liczba naturalna n jest normą liczby całkowitej zespolonej, to w rozkładzie liczby n na czynniki naturalne pierwsze, które są formy $4k+3$, muszą być w potęgach parzystych.

Z równości (23) znajdujemy dalej:

$$\lambda = \alpha, \quad \mu_1 = \beta_1/2, \quad \mu_2 = \beta_2/2, \quad \dots, \quad \mu_l = \beta_l/2.$$

Wykładniki $\lambda, \mu_1, \mu_2, \dots, \mu_l$ są w ten sposób wyznaczone.

W celu wyznaczenia wykładników λ_j i λ'_j , gdzie $j = 1, 2, \dots, k$, użyjemy osobnej reguły, którą obecnie wyprowadzimy.

Niech π_j będzie wykładnikiem najwyższej potęgi liczby p_j , dla której $p_j^{\pi_j} | z$, czyli dla której $p_j^{\pi_j}$ jest jeszcze wspólnym dzielnikiem liczb a i b , gdzie $z = a + bi$. Wówczas:

$$(24) \quad \left. \begin{aligned} \lambda_j &= a_j - \pi_j \\ \lambda'_j &= a_j \end{aligned} \right\} \text{ gdy } p_j^{\pi_j} \pi_j | z, \quad \left. \begin{aligned} \lambda'_j &= a_j - \pi_j \\ \lambda_j &= \pi_j \end{aligned} \right\} \text{ gdy } p_j^{\pi_j} \pi_j \nmid z.$$

Istotnie, z określenia wykładnika π_j wynika natychmiast, że liczba całkowita zespolona $z/p_j^{\pi_j}$ nie może być podzielna jednocześnie przez π_j i przez π'_j , gdyż wobec $(\pi_j, \pi'_j) = 1$ byłaby wówczas podzielna przez $\pi_j \pi'_j = p_j$, a zatem byłoby $p_j^{\pi_j+1} | z$, wbrew określeniu liczby π_j .

Jeżeli więc $\pi_j | (z/p_j^{\pi_j})$, to liczba $z/p_j^{\pi_j}$ nie jest podzielna przez π'_j i wobec $p_j^{\pi_j} = \pi_j^{\pi_j} \pi_j'^{\pi_j}$ z rozwinięcia (22) wynika, że wówczas $\lambda'_j = \pi_j$, a zatem $\lambda_j = a_j - \pi_j$ na mocy (23).

Jeżeli zaś liczba $z/p_j^{\pi_j}$ nie jest podzielna przez π_j , to — jak łatwo widzieć — mamy $\lambda_j = \pi_j$ i $\lambda'_j = a_j - \pi_j$.

Reguła (24) została tym samym dowiedziona.

Wreszcie, wykładnik potęgi i^r znajdujemy za pomocą zwykłego dzielenia, znając liczbę z i pozostałe czynniki rozwinięcia (22).

PRZYKŁADY. 1. Niech $z = 22 + 7i$. Mamy tu:

$$N(z) = 484 + 49 = 533 = 13 \cdot 41, \quad p_1 = 13 = 2^2 + 3^2, \quad p_2 = 41 = 4^2 + 5^2.$$

Jest tu więc

$$z = i^r \pi_1^{\lambda_1} \pi_1'^{\lambda_1'} \pi_2^{\lambda_2} \pi_2'^{\lambda_2'},$$

gdzie

$$\pi_1 = 2 + 3i, \quad \pi_1' = 2 - 3i, \quad \pi_2 = 4 + 5i, \quad \pi_2' = 4 - 5i.$$

Oczywiście $\pi_1 = \pi_2 = 0$. Liczba

$$z/\pi_1 = (22 + 7i)/(2 + 3i) = (22 + 7i)(2 - 3i)/13 = 5 - 4i$$

jest całkowita, zatem $\lambda_1 = a_1 - 0 = 1$ i $\lambda'_1 = 0$. Można by oczywiście zbadać w podobny sposób iloraz z/π_2 , ale wystarczy tu zauważyć, że otrzymany iloraz $5 - 4i$ jest liczbą zespoloną pierwszą, co daje od razu rozkład badanej liczby z na czynniki zespolone pierwsze:

$$22 + 7i = (2 + 3i)(5 - 4i).$$

2. Niech $z=19+17i$. Mamy tu:

$$N(z)=361+289=650=2\cdot 5^3\cdot 13=2\cdot p_1^2\cdot p_2.$$

Jest tu więc

$$z=i^v(1+i)\pi_1^{\lambda_1}\pi_1'^{\lambda_1'}\pi_2^{\lambda_2}\pi_2'^{\lambda_2'},$$

gdzie

$$\pi_1=1+2i, \pi_1'=1-2i, \pi_2=2+3i, \pi_2'=2-3i, \alpha_1=2, \alpha_2=1.$$

Ponieważ nie jest ani $5|z$, ani $13|z$, więc $\alpha_1=\alpha_2=0$. Liczba $(19+17i)/(1+2i)$ nie jest całkowita, zatem $\lambda_1=0$ i $\lambda_1'=2$. Liczba $(19+17i)/(2+3i)$ też nie jest całkowita, zatem $\lambda_2=0$ i $\lambda_2'=1$. Mamy więc

$$z=i^v(1+i)(1-2i)^2(2-3i)$$

i przez proste dzielenie znajdujemy $v=2$. Rozwinięcie badanej liczby na czynniki zespolone pierwsze jest więc następujące:

$$19+17i=(1+i)(1-2i)^2(-2+3i).$$

3. Niech $z=10+100i$. Możemy napisać $z=10(1+10i)$ i rozwinąć tylko $1+10i$, gdyż

$$10=2\cdot 5=-i(1+i)^2(1+2i)(1-2i).$$

Mamy $N(1+10i)=101$. Jest to liczba pierwsza formy $4k+1$, a ponieważ w myśl twierdzenia 7 liczba, której norma jest liczbą naturalną pierwszą, jest liczbą zespoloną pierwszą, więc ostatecznie

$$10+100i=-i(1+i)^2(1+2i)(1-2i)(1+10i).$$

ĆWICZENIE. Rozłóż na czynniki zespolone pierwsze następujące liczby:

$$1+7i, \quad 9+i, \quad 7+9i, \quad 107+198i, \quad 10+i, \quad 7+24i.$$

$$\text{Odpowiedź: } \begin{aligned} 1+7i &= -i(1+i)(1+2i)^2, & 9+i &= -i(1+i)(4+5i), \\ 7+9i &= (1+i)(1+2i)(3-2i), & 107+198i &= -(1+6i)^2, \\ 10+i &= 10+i, & 7+24i &= -(1+2i)^4. \end{aligned}$$

§ 6. Ilość liczb całkowitych zespolonych o danej normie. Zbadamy obecnie, ile jest, dla liczby naturalnej n , liczb całkowitych zespolonych o normie n .

Jest to ciekawe nie tylko samo przez się, ale jeszcze z innego względu. Zagadnienie, ile jest liczb całkowitych zespolonych $z=x+yi$, dla których $N(z)=n$ (przy danym n naturalnym), jest — jak łatwo widzieć — równoważne zagadnieniu, ile jest układów dwu liczb całkowitych wymiernych x, y , dla których

$x^2+y^2=n$. Innymi słowy, liczba $\tau(n)$ liczb całkowitych zespolonych o normie n jest zarazem liczbą rozkładów liczby naturalnej n na sumę kwadratów dwu liczb całkowitych rzeczywistych. Jest to więc funkcja liczbową, którą badaliśmy na innej drodze w Rozdziale IV (§ 8, str. 84).

Niech więc (20) będzie, jak w § 5, rozkładem liczby n na czynniki naturalne pierwsze, a (21) jej rozkładem na czynniki zespolone pierwsze. Warunkiem koniecznym na to, by równanie $N(z)=n$ było rozwiązywalne w liczbach całkowitych zespolonych, jest — jak dowiedliśmy w § 5 (str. 594) — żeby wykładniki β_j (dla $j=1, 2, \dots, l$) były wszystkie parzyste.

Żałujemy naprzód, że warunek ten jest spełniony. Wówczas — jak widzieliśmy — liczba z o normie n daje rozwinięcie (22) i dla wykładników mamy równości (23), a v jest jedną z liczb 1, 2, 3, 4. Na odwrót — jak łatwo widzieć — jeżeli

$$\lambda, \lambda_1, \lambda_1', \lambda_2, \lambda_2', \dots, \lambda_k, \lambda_k', \mu_1, \mu_2, \dots, \mu_l$$

jest jakimkolwiek układem liczb całkowitych nieujemnych, spełniających równości (23), a v — jedną z liczb 1, 2, 3, 4, to liczba z wyznaczona ze wzoru (22) ma normę n . Pytanie, ile jest liczb całkowitych zespolonych z o normie n , jest więc równoważne pytaniu, ile jest układów liczb całkowitych nieujemnych $v, \lambda_1, \lambda_1', \lambda_2, \lambda_2', \dots, \lambda_k, \lambda_k'$ spełniających warunki:

$$1 \leq v \leq 4, \quad \lambda_1 + \lambda_1' = a_1, \quad \lambda_2 + \lambda_2' = a_2, \quad \dots, \quad \lambda_k + \lambda_k' = a_k,$$

gdź liczby $\lambda, \mu_1, \mu_2, \dots, \mu_l$ są przez warunki (23) określone jednoznacznie.

Dla v mamy 4 możliwe wartości (1, 2, 3, 4), a dla układu liczb λ_1, λ_1' możliwe są tylko następujące układy wartości:

$$0, a_1, \quad 1, a_1-1, \quad 2, a_1-2, \quad \dots, \quad a_1, 0,$$

których jest a_1+1 ; podobnie mamy a_2+1 możliwych układów wartości dla układu λ_2, λ_2' itd. Wynika stąd, że

$$(25) \quad \tau(n) = 4(a_1+1)(a_2+1)\dots(a_k+1).$$

Wzór ten wyprowadziliśmy przy założeniu, że liczba n zawiera wszystkie dzielniki pierwsze formy $4t+3$ w potęgach parzystych. W przeciwnym razie — jak widzieliśmy (ob. str. 594) — równanie $N(z)=n$ nie jest rozwiązywalne w liczbach całkowitych zespolonych z i mamy $\tau(n)=0$. Zachodzi więc następujące

Twierdzenie 8. Jeżeli liczba naturalna n ma rozkład (20) na czynniki naturalne pierwsze, to liczba $\tau(n)$ jej rozkładów na sumę kwadratów dwu liczb całkowitych rzeczywistych jest równa $4(a_1+1)(a_2+1)\dots(a_k+1)$, gdy wszystkie czynniki pierwsze liczby n formy $4t+3$ wchodzą do rozwinięcia (20) w potęgach parzystych; w przeciwnym razie $\tau(n)=0$.

Natychmiastowym wnioskiem stąd jest twierdzenie 13 z Rozdziału IV (§ 7, str. 80), udowodnione tam na innej drodze.

W szczególności, jeżeli n jest liczbą pierwszą formy $4k+1$, to $\tau(n)=8$, skąd natychmiast wynika twierdzenie Fermata, udowodnione w Rozdziale IV (§ 4, str. 73).

Niech teraz $f(h)$ będzie funkcją określoną, jak następuje:

$$(26) \quad f(h) = \begin{cases} 0 & \text{dla } h \text{ parzystych,} \\ +1 & \text{dla } h \text{ formy } 4t+1, \\ -1 & \text{dla } h \text{ formy } 4t+3. \end{cases}$$

Łatwo widzieć, że dla a i b całkowitych rzeczywistych jest zawsze

$$f(ab) = f(a)f(b).$$

Stąd jeżeli

$$n = h_1^{a_1} \cdot h_2^{a_2} \cdot \dots \cdot h_k^{a_k}$$

jest rozkładem liczby n na czynniki pierwsze, to — jak łatwo widzieć — zachodzi wzór następujący:

$$\sum_{d|n} f(d) = [f(1)+f(h_1)+f(h_1^2)+\dots+f(h_1^{a_1})] \dots [f(1)+f(h_k)+\dots+f(h_k^{a_k})].$$

Mamy oczywiście w myśl definicji (26)

$$f(1) = f(1) + f(2) + f(2^2) + \dots + f(2^a) = 1.$$

Jeżeli zaś $h = 4t+1$, to

$$f(1) + f(h) + f(h^2) + \dots + f(h^a) = a+1,$$

Wreszcie, jeżeli $h = 4t+3$, to

$$(27) \quad f(1) + f(h) + f(h^2) + \dots + f(h^a) = 1 - 1 + 1 - \dots + (-1)^a = \frac{1 + (-1)^a}{2}.$$

Na mocy wzoru dla $\sum_{d|n} f(d)$ mamy zatem

$$\sum_{d|n} f(d) = (a_1+1)(a_2+1)\dots(a_k+1);$$

skąd na mocy twierdzenia 8

$$(28) \quad \tau(n) = 4 \sum_{d|n} f(d),$$

jeżeli n nie zawiera żadnego czynnika pierwszego formy $4t+3$ w potęgze nieparzystej, w przeciwnym zaś razie w myśl (27)

$$\sum_{d|n} f(d) = 0,$$

a że wtedy też jest $\tau(n)=0$ na mocy twierdzenia 8, więc znowu zachodzi wzór (28). Wzór ten zachodzi przeto przy wszelkim naturalnym n .

Wynika stąd od razu następujące twierdzenie Jacobiego:

Twierdzenie 9. Liczba rozkładów liczby naturalnej n na sumę kwadratów dwu liczb całkowitych rzeczywistych jest równa pochwórną różnicy między liczbą wszystkich dzielników liczby n , mających formę $4t+1$, a liczbą wszystkich tych dzielników liczby n , które mają formę $4t+3$.

Istotnie, w sumie (28) składnik $+1$ figuruje w myśl definicji (26) funkcji f tyle razy, ile liczba n ma dzielników formy $4t+1$, składnik zaś -1 tyle razy, ile liczba n ma dzielników formy $4t+3$.

Zc wzoru (28) otrzymujemy

$$(29) \quad \frac{1}{4} \sum_{n=1}^{E(x)} \tau(n) = \sum_{k=1}^{E(x)} f(k) E\left(\frac{x}{k}\right),$$

gdyż każdy składnik $f(d)$ występuje w sumie $\sum_{n=1}^{E(x)} \sum_{d|n} f(d)$ tyle razy,

ile jest liczb $n \leq x$, dla których $d|n$, zatem $E\left(\frac{x}{d}\right)$ razy. Ponieważ zaś na mocy wzoru (58) z Rozdziału IV (str. 86) jest

$$\frac{1}{4} \sum_{n=1}^{E(x)} \tau(n) = \sum_{k=0}^{E(\sqrt{x})} E(\sqrt{x-k^2}),$$

więc zachodzi tożsamość

$$(30) \quad \sum_{k=0}^{E(\sqrt{x})} E(\sqrt{x-k^2}) = \sum_{k=1}^{E(x)} f(k) E\left(\frac{x}{k}\right)$$

czyli

$$\begin{aligned} & E(\sqrt{x}) + E(\sqrt{x-1^2}) + E(\sqrt{x-2^2}) + E(\sqrt{x-3^2}) + \dots = \\ & = E\left(\frac{x}{1}\right) - E\left(\frac{x}{3}\right) + E\left(\frac{x}{5}\right) - E\left(\frac{x}{7}\right) + \dots, \end{aligned}$$

gdzie po lewej stronie składniki należy wypisywać dopóty, dopóki pod pierwiastkiem otrzymujemy liczbę dodatnią, po prawej zaś — dopóki mianownik nie przewyższa licznika.

Jest to tak zwana *tożsamość Liouville'a*.

Np. dla $x=10$:

$$\begin{aligned} & E(\sqrt{10}) + E(\sqrt{9}) + E(\sqrt{6}) + E(\sqrt{1}) = \\ & = E\left(\frac{10}{1}\right) - E\left(\frac{10}{3}\right) + E\left(\frac{10}{5}\right) - E\left(\frac{10}{7}\right) + E\left(\frac{10}{9}\right); \end{aligned}$$

jakoż istotnie $3+3+2+1=10-3+2-1+1$.

Na odwrót, z tożsamości Liouville'a można z łatwością drogą elementarną wyprowadzić twierdzenie Jacobiego.

Z tożsamości Liouville'a można też na drodze czysto elementarnej wyprowadzić za pomocą nierówności (62) z Rozdziału IV (str. 89) wzór Leibniza dla liczby π :

$$\frac{\pi}{4} = \frac{1}{1} - \frac{1}{5} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \dots^1).$$

Godna uwagi jest w tym rozwinięciu rola liczb nieparzystych, które występują kolejno w mianownikach. Starożytni mawiali: „Numero impari deus gaudet”. Tak rachunek na wskroś arytmetyczny, przenikając do geometrii, pozwala określić jej najważniejszą stałą — stosunek obwodu koła do średnicy — za pomocą prostego szeregu odwrotności kolejnych liczb nieparzystych z naprzemiennymi znakami.

Innym wzorem dla liczby π , w którym występują liczby nieparzyste, jest wzór Eulera

$$\frac{\pi^2}{8} = \frac{1}{1^2} + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \frac{1}{9^2} + \dots,$$

który też można otrzymać na drodze elementarnej z pewnych twierdzeń Teorii liczb²⁾.

Spośród znanych w Analizie wzorów dla π , w których występują liczby nieparzyste, przytoczymy jeszcze wzór Wallisa³⁾

$$\frac{\pi}{4} = \left(1 - \frac{1}{3^2}\right) \left(1 - \frac{1}{5^2}\right) \left(1 - \frac{1}{7^2}\right) \left(1 - \frac{1}{9^2}\right) \dots,$$

¹⁾ Szczegółowy dowód znajduje się w poprzednich wydaniach tej książki (z 1914 r. i 1925 r.), str. 349-351.

²⁾ Ob. tamże, str. 371.

³⁾ Ob. np. mój *Rachunek różniczkowy*, Monografie Matematyczne, Warszawa-Wrocław 1948, str. 75.

wzór Eulera¹⁾.

$$\frac{\pi^3}{32} = \frac{1}{1^3} - \frac{1}{3^3} + \frac{1}{5^3} - \frac{1}{7^3} + \frac{1}{9^3} - \dots$$

i wzór Brounckera²⁾

$$\frac{4}{\pi} = 1 + \frac{1^2}{2} + \frac{3^2}{2} + \frac{5^2}{2} + \frac{7^2}{2} + \frac{9^2}{2} + \dots$$

W czasopiśmie hiszpańskim *Matematica Elemental*, tom 5 (1936), znajduje się na str. 48 wzmianka, iż Euler w karcie do Stirlinga napisał, że

$$\frac{\pi}{4} = \prod_{n=2}^{\infty} \frac{p_n}{f(p_n)},$$

gdzie p_n jest n -tą z kolei liczbą pierwszą, a $f(p_n)$ — najbliższą do p_n wielokrotności liczby 4. Zatem

$$\frac{\pi}{4} = \frac{5}{4} \cdot \frac{5}{4} \cdot \frac{7}{8} \cdot \frac{11}{12} \cdot \frac{13}{12} \cdot \frac{17}{16} \dots$$

Nie wiem, czy wzór ten został dowiedziony lub obalony.

§ 7. Twierdzenie Jacobiego o rozkładach na sumę czterech kwadratów. Zajmiemy się teraz innym twierdzeniem Jacobiego, dotyczącym liczby rozkładów na sumę czterech kwadratów.

Rozpatrzmy przede wszystkim przypadek, kiedy n jest czterokrotną liczbą nieparzystą, $n=4u$, i weźmy pod uwagę rozkłady liczby n na sumę kwadratów czterech liczb całkowitych nieparzystych:

$$(51) \quad 4u = x^2 + y^2 + z^2 + t^2.$$

Ponieważ liczby x, y, z i t są nieparzyste więc — jak łatwo widzieć —

$$(52) \quad x^2 + y^2 = 2u' \quad \text{ i } \quad z^2 + t^2 = 2u'',$$

gdzie u' i u'' są liczbami naturalnymi nieparzystymi. Na mocy (51) i (52) jest

$$(53) \quad 2u = u' + u''.$$

¹⁾ Ob. tamże, str. 99.

²⁾ Ob. tamże, str. 97 oraz moje *Działania nieskończone*, Monografie Matematyczne, Warszawa-Wrocław 1948, str. 140 (wzór 20).

Z drugiej strony, jeżeli n jest liczbą nieparzystą i $2n = a^2 + b^2$, to a i b są nieparzyste. Gdyby bowiem liczby a i b były obie parzyste, to $2n$ byłoby podzielne przez 4 wbrew założeniu, że, n jest nieparzyste. Gdyby zaś jedna z liczb a i b była parzysta, a druga nieparzysta, to $2n$ byłoby nieparzyste, co niemożliwe.

Widzimy więc, że na to, aby wyznaczyć wszystkie rozkłady liczby $4u$ na sumę kwadratów czterech liczb nieparzystych — oznaczmy ich liczbę przez $\theta(4u)$ — wystarczy wyznaczyć wszystkie rozkłady liczby $2u$ na sumę dwu liczb nieparzystych u' i u'' i następnie wszystkimi możliwymi sposobami rozłożyć liczby $2u'$ i $2u''$ na sumy dwu kwadratów, kombinując te rozkłady między sobą.

Dla każdej pary liczb nieparzystych u', u'' , spełniających równość (33), będziemy mieli, — jak łatwo widzieć (na mocy (28) i wynikającej z (25) równości $\tau(2m) = \tau(m)$ dla $m = 1, 2, \dots$) —

$$\tau(2u') \cdot \tau(2u'') = 16 \sum_{d'|u'} f(d') \cdot \sum_{d''|u''} f(d'')$$

rozkładów liczby $4u$ na sumę kwadratów czterech liczb nieparzystych. Stąd ogólna liczba rozkładów

$$(34) \quad \theta(4u) = 16 \sum_{u'+u''=2u} \left(\sum_{d'|u'} f(d') \cdot \sum_{d''|u''} f(d'') \right),$$

gdzie suma przed nawiasem jest rozciągnięta na wszystkie układy liczb naturalnych u', u'' , spełniających równość (33). Ponieważ każdy dzielnik d' liczby nieparzystej u' jest nieparzysty, więc wobec (26) jest

$$\sum_{d'|u'} f(d') = \sum_{d'|u'} (-1)^{\frac{d'-1}{2}}$$

i podobnie

$$\sum_{d''|u''} f(d'') = \sum_{d''|u''} (-1)^{\frac{d''-1}{2}},$$

wobec czego wzór (34) daje

$$(35) \quad \theta(4u) = 16 \sum_{u'+u''=2u} \left(\sum_{d'|u'} (-1)^{\frac{d'-1}{2}} \cdot \sum_{d''|u''} (-1)^{\frac{d''-1}{2}} \right).$$

Iloczyn sum w nawiasie możemy przekształcić na sumę podwójną w myśl wzoru

$$\sum_{m=1}^p a_m \sum_{n=1}^q b_n = (a_1 + a_2 + \dots + a_p)(b_1 + b_2 + \dots + b_q) = \sum_{m=1}^p \sum_{n=1}^q a_m b_n.$$

Otrzymamy w ten sposób ze wzoru (35)

$$(36) \quad \theta(4u) = 16 \sum_{u'+u''=2u} \sum_{d'|u'} \sum_{d''|u''} (-1)^{\frac{d'-1}{2} + \frac{d''-1}{2}}.$$

Na mocy tożsamości

$$\frac{d'-1}{2} + \frac{d''-1}{2} = \frac{d'-d''}{2} + d''-1$$

i nieparzystości liczby d'' (jako dzielnika liczby nieparzystej u'') jest oczywiście

$$(-1)^{\frac{d'-1}{2} + \frac{d''-1}{2}} = (-1)^{\frac{d'-d''}{2}},$$

tak iż wzór (36) daje

$$(37) \quad \theta(4u) = 16 \sum_{u'+u''=2u} \sum_{d'|u'} \sum_{d''|u''} (-1)^{\frac{d'-d''}{2}}.$$

Dla każdej pary liczb naturalnych nieparzystych u', u'' , spełniających równość (33) i dla każdej pary dzielników d', d'' są też określone ich dzielniki dopełniające δ', δ'' przez równości

$$(38) \quad u' = d' \delta', \quad u'' = d'' \delta''.$$

Zatem w myśl (33)

$$(39) \quad 2u = d' \delta' + d'' \delta'';$$

przy tym liczby δ' i δ'' (jako dzielniki liczb nieparzystych u' i u'') są nieparzyste. Każdemu składnikowi sumy potrójnej (37) odpowiada więc jednoznacznie układ czterech liczb naturalnych nieparzystych

$$(40) \quad d', d'', \delta', \delta'',$$

spełniających równość (39). Ale — jak łatwo widzieć — i na odwrót: każdemu układowi liczb naturalnych nieparzystych (40), spełniających równość (39), odpowiada jednoznacznie pewien składnik sumy potrójnej (37), ponieważ wskaźniki d', d'', u', u'' , charakteryzujące ten składnik, są określone pierwszymi dwoma bezpośrednio, a ostatnie dwa wzorami (38).

Możemy więc napisać

$$(41) \quad \theta(4u) = 16 \sum_{d'\delta' + d''\delta'' = 2u} (-1)^{\frac{d'-d''}{2}},$$

gdzie suma po stronie prawej jest rozciągnięta na wszystkie układy (40) czterech liczb naturalnych nieparzystych, spełniających równość (39).

Podzielmy teraz składniki sumy (41) na dwie klasy: do pierwszej zaliczmy wszystkie te, dla których $d' = d''$, do drugiej zaś wszystkie te, dla których $d' \neq d''$.

Dla każdej liczby naturalnej nieparzystej d obliczmy sumę wszystkich tych składników sumy (41), dla których $d' = d'' = d$. Jak wynika z (39), d jest wówczas dzielnikiem liczby $2u$, a przeto i liczby u , gdyż d jest nieparzyste. Niech więc $u = d\delta$, skąd na mocy (39)

$$2\delta = \delta' + \delta''.$$

Wszystkich składników sumy (41), dla których $d' = d'' = d$, jest zatem tyle, ile jest rozkładów liczby 2δ na sumę dwu liczb naturalnych nieparzystych. Składników tych jest więc δ , a że każdy składnik jest w danym razie równy $+1$, przeto suma wszystkich składników jest równa $\delta = u/d$.

Stąd jako sumę wszystkich składników klasy pierwszej otrzymujemy z łatwością liczbę

$$\sum_{d|u} \frac{u}{d} = \sum_{d|u} d = \sigma(u),$$

gdzie $\sigma(u)$ jest znaną nam z Rozdziału V (§ 2, str. 115) sumą wszystkich dzielników liczby u .

Składniki klasy drugiej rozbijemy na dwie grupy, zaliczając do pierwszej wszystkie te, dla których $d' > d''$, a do drugiej wszystkie te, dla których $d' < d''$. Każdemu składnikowi pierwszej grupy, wyznaczonemu przez układ (40), odpowiada — jak łatwo widzieć — równy mu składnik drugiej grupy, wyznaczony przez układ $d'', d', \delta'', \delta'$, i na odwrót. Wystarczy więc obliczyć sumę składników pierwszej grupy i podwoić ją.

Niech

$$(42) \quad \vartheta = E\left(\frac{d''}{d' - d''}\right).$$

Każdemu składnikowi pierwszej grupy, wyznaczonemu przez układ (40), przyporządkujemy składnik, wyznaczony przez układ

$$(43) \quad d_1, d_2, \delta_1, \delta_2,$$

gdzie:

$$(44) \quad \begin{aligned} d_1 &= \delta' + (\vartheta + 1)(\delta' + \delta''), & d_2 &= \delta' + \vartheta(\delta' + \delta''), \\ \delta_1 &= d'' - \vartheta(d' - d''), & \delta_2 &= (\vartheta + 1)(d' - d'') - d''. \end{aligned}$$

Okażemy przede wszystkim, że układ (43), określony wzorami (44), rzeczywiście wyznacza pewien składnik pierwszej grupy. Wobec całkowitości liczby ϑ i nieparzystości liczb (40), a więc parzystości liczb $\delta' + \delta''$ i $d' - d''$, ze wzorów (44) widać w jednej chwili, że liczby (43) są całkowite nieparzyste.

Na mocy (42) liczba ϑ jest nieujemna, ponieważ w pierwszej grupie jest $d' > d''$. Zatem w myśl wzorów (44) liczby d_1 i d_2 są dodatnie. Ponadto w myśl (42) jest

$$\frac{d''}{d' - d''} - 1 < \vartheta \leq \frac{d''}{d' - d''},$$

skąd mnożąc przez $d' - d'' > 0$, otrzymujemy

$$d'' - (d' - d'') < \vartheta(d' - d'') \leq d'',$$

co dowodzi wobec (44), że $\delta_1 \geq 0$ i $\delta_2 > 0$. Ponieważ zaś δ_1 , jako liczba nieparzysta, nie może być zerem, więc również $\delta_1 > 0$.

Wszystkie cztery liczby (43) są więc naturalne nieparzyste.

Ze wzorów (44) znajdujemy dalej

$$(45) \quad d_1 - d_2 = \delta' + \delta''$$

(co dowodzi, że $d_1 > d_2$) oraz

$$(46) \quad d_1 + d_2 = d' - d'',$$

skąd na mocy (45) i tożsamości

$$d_1\delta_1 + d_2\delta_2 = d_1(\delta_1 + \delta_2) - (d_1 - d_2)\delta_2$$

otrzymujemy

$$d_1\delta_1 + d_2\delta_2 = d_1(d' - d'') - (\delta' + \delta'')\delta_2,$$

a przeto na podstawie wzorów (44)

$$d_1\delta_1 + d_2\delta_2 = \delta'(d' - d'') + (\delta' + \delta'')d'' = d'\delta' + d''\delta'',$$

czyli wobec (39)

$$d_1\delta_1 + d_2\delta_2 = 2u.$$

Widzimy więc, że układ (43) istotnie wyznacza pewien składnik pierwszej grupy.

Układ (43) jest ponadto różny od układu (40), gdyż w razie tożsamości obu układów mielibyśmy w myśl (45) $d' - d'' = \delta' + \delta''$ i przeto według (39)

$$2u = (d' - d'')\delta' + (\delta' + \delta'')d'' = (\delta' + \delta'')(\delta' + d''),$$

skąd wywnioskowalibyśmy wobec parzystości liczb $\delta' + \delta''$ i $\delta' + d''$, że $2u$ jest podzielne przez 4, wbrew nieparzystości liczby u .

Rozwiązując równania (44) względem niewiadomych (40), otrzymujemy z łatwością według (45) i (46):

$$\begin{aligned}\delta' &= d_1 - (\vartheta + 1)(d_1 - d_2) = d_2 - \vartheta(d_1 - d_2), \\ d'' &= \delta_1 + \vartheta(\delta_1 + \delta_2),\end{aligned}$$

skąd dalej według (45) i (46):

$$\begin{aligned}\delta'' &= d_1 - d_2 - \delta' = (\vartheta + 1)(d_1 - d_2) - d_2, \\ d' &= \delta_1 + \delta_2 + d'' = \delta_1 + (\vartheta + 1)(\delta_1 + \delta_2).\end{aligned}$$

Ponieważ zaś na podstawie wzorów (44) i (42) jest

$$(47) \quad \vartheta_1 = E\left(\frac{d_2}{d_1 - d_2}\right) = E\left(\frac{\delta' + \vartheta(\delta' + \delta'')}{\delta' + \delta''}\right) = E\left(\frac{\delta'}{\delta' + \delta''} + \vartheta\right) = \vartheta,$$

gdyż ϑ jest liczbą całkowitą, a $\frac{\delta'}{\delta' + \delta''}$ ułamkiem właściwym, więc mamy ostatecznie:

$$(48) \quad \begin{aligned}d' &= \delta_1 + (\vartheta_1 + 1)(\delta_1 + \delta_2), & d'' &= \delta_1 + \vartheta_1(\delta_1 + \delta_2), \\ \delta' &= d_2 - \vartheta_1(d_1 - d_2), & \delta'' &= (\vartheta_1 + 1)(d_1 - d_2) - d_2.\end{aligned}$$

Przez porównanie wzorów (47) i (48) ze wzorami (42) i (44) dochodzimy do wniosku, że w myśl przyjętego przyporządkowania układowi (45) odpowiada znowu układ (40). Przyporządkowanie to łączy zatem wszystkie składniki pierwszej grupy w pary, i to w taki sposób, że do jednej pary należą składniki, wyznaczone przez dwa różne układy (40) i (45), związane ze sobą wzorami (44).

Obliczmy więc sumę dwu składników jednej i tej samej pary czyli sumę

$$(49) \quad (-1)^{\frac{d' - d''}{2}} + (-1)^{\frac{d_1 - d_2}{2}},$$

gdzie d' , d'' , d_1 i d_2 są związane między sobą wzorami (44).

Wobec (39) i (45) jest $2u = (d' - d'')\delta' + (d_1 - d_2)d''$ czyli

$$\frac{d' - d''}{2}\delta' + \frac{d_1 - d_2}{2}d'' = u,$$

skąd wobec nieparzystości liczb δ' , d'' i u

$$\frac{d' - d''}{2} + \frac{d_1 - d_2}{2} \equiv 1 \pmod{2}.$$

Dowodzi to, że suma (49) jest zerem. Składniki każdej pary znoszą się więc wzajemnie.

Wynika stąd, że suma wszystkich składników pierwszej grupy, a więc też suma składników całej klasy drugiej, jest zerem. Ponieważ zaś — jak dowiedliśmy — suma składników klasy pierwszej wynosi $\sigma(u)$, więc w myśl (41) otrzymujemy

Twierdzenie 10. Jeżeli u jest liczbą naturalną nieparzystą, to

$$\theta(4u) = 16\sigma(u).$$

Twierdzenie, wyrażone tym wzorem, zostało wypowiedziane (w nieco innym brzmieniu) i udowodnione przez Jacobiego ¹⁾. Powyższy zaś dowód, prostszy od dowodu Jacobiego, zawdzięczamy Dirichletowi ²⁾.

Niech teraz

$$(50) \quad u = \xi^2 + \eta^2 + \zeta^2 + \vartheta^2$$

będzie jakimkolwiek rozkładem liczby nieparzystej u na sumę kwadratów czterech liczb całkowitych i niech:

$$(51) \quad \begin{aligned}x' &= \xi + \eta + \zeta + \vartheta, & y' &= \xi + \eta - \zeta - \vartheta, \\ z' &= \xi - \eta + \zeta - \vartheta, & t' &= \xi - \eta - \zeta + \vartheta.\end{aligned}$$

Na mocy oczywistej kongruencji $m^2 \equiv m \pmod{2}$, zachodzącej dla wszelkich m całkowitych, jest na mocy (50) $x' \equiv u \pmod{2}$, co wobec nieparzystości liczby u dowodzi, że liczba x' też jest nieparzysta. Ponieważ dalej ze wzorów (51) wynika, że

$$y' = x - 2(\zeta + \vartheta), \quad z' = x - 2(\eta + \vartheta), \quad t' = x - 2(\eta + \zeta),$$

więc wszystkie cztery liczby x' , y' , z' , t' są nieparzyste. Na podstawie wzorów (50) i (51) sprawdzamy dalej z łatwością, że

$$x'^2 + y'^2 + z'^2 + t'^2 = 4u.$$

Układ

$$(52) \quad x', y', z', t',$$

wyznaczony ze wzorów (50), przedstawia zatem pewien rozkład liczby $4u$ na sumę kwadratów czterech liczb nieparzystych.

Niech z drugiej strony:

$$(53) \quad \begin{aligned}x'' &= -\xi + \eta + \zeta + \vartheta, & y'' &= \xi - \eta + \zeta + \vartheta, \\ z'' &= \xi + \eta - \zeta + \vartheta, & t'' &= \xi + \eta + \zeta - \vartheta.\end{aligned}$$

¹⁾ C. Jacobi, *De compositione numerorum e quatuor quadratis*, Journal für reine und angewandte Mathematik, tom 12 (1834) str. 167.

²⁾ Ob. L. Dirichlet, *Journal des Mathématiques*, 2-a seria, tom 1 (1856), str. 210; ob. też P. Bachmann, *Niedere Zahlentheorie*, tom II, Lipsk 1910, str. 349-354.

I tu — jak łatwo widzieć — liczby

$$(54) \quad x'', y'', z'', t''$$

są wszystkie nieparzyste i znowu

$$x''^2 + y''^2 + z''^2 + t''^2 = 4u.$$

Układy (52) i (54) są różne, gdyż ze wzorów (51) i (53) znajdujemy

$$(55) \quad x' + y' + z' + t' = 4\xi, \quad x'' + y'' + z'' + t'' = 2(\xi + \eta + \zeta + \theta),$$

skąd wynika wobec nieparzystości liczby $\xi + \eta + \zeta + \theta$, że suma liczb (52) jest podzielna przez 4, a suma liczb (54) jest niepodzielna przez 4.

W myśl wzorów (51) i (53) każdemu rozkładowi (50) liczby nieparzystej u na sumę czterech kwadratów odpowiadają zatem dwa różne rozkłady liczby $4u$ na sumę kwadratów czterech liczb nieparzystych.

Okażemy, że w ten sposób każdy rozkład (31) liczby $4u$ na sumę kwadratów czterech liczb nieparzystych jest przyporządkowany wzajemnie jednoznacznie pewnemu rozkładowi (50) liczby u na sumę czterech kwadratów.

Istotnie, liczba

$$s = x + y + z + t,$$

jako suma czterech liczb nieparzystych z rozkładu (31), jest w każdym razie parzysta. Rozróżnimy dwa przypadki:

1° $s \equiv 0 \pmod{4}$. Wzory (53), które pociągają za sobą wzór (55), nie mogą wówczas dla żadnych całkowitych ξ, η, ζ, θ , spełniających wzór (50), dać układu

$$x'' = x, \quad y'' = y, \quad z'' = z, \quad t'' = t,$$

gdyż suma s wypadłaby niepodzielna przez 4 wbrew założeniu. Natomiast istnieje jeden i tylko jeden układ liczb całkowitych ξ, η, ζ, θ , spełniających równość (50), dla których (por. wzory (51)):

$$(56) \quad \begin{aligned} x &= \xi + \eta + \zeta + \theta, & y &= \xi + \eta - \zeta - \theta, \\ z &= \xi - \eta + \zeta - \theta, & t &= \xi - \eta - \zeta + \theta, \end{aligned}$$

gdyż zakładając, że wzory (56) zachodzą, otrzymujemy z nich w jednej chwili:

$$(57) \quad \begin{aligned} \frac{x+y+z+t}{4} &= \xi, & \frac{x+y-z-t}{4} &= \eta, \\ \frac{x-y+z-t}{4} &= \zeta, & \frac{x-y-z+t}{4} &= \theta, \end{aligned}$$

co dowodzi, że układ x, y, z, t odpowiada co najwyżej jednemu układowi ξ, η, ζ, θ , i to takiemu, dla którego zachodzą wzory (57); zakładając zaś wzory (57) i wyznaczając z nich liczby ξ, η, ζ, θ , łatwo sprawdzić, że w rozpatrywanym przypadku 1° liczby te są całkowite, spełniają wzory (56), a wobec (31) również wzór (50), co dowodzi, że układ x, y, z, t odpowiada co najmniej jednemu takiemu układowi ξ, η, ζ, θ .

Tak więc w przypadku 1° rozkład (31) odpowiada wzajemnie jednoznacznie pewnemu rozkładowi (50) liczby u na sumę czterech kwadratów.

2° $s \equiv 2 \pmod{4}$. W tym przypadku wzory (51), które pociągają za sobą wzór (55), nie mogą dla żadnych ξ, η, ζ, θ całkowitych dać układu

$$x' = x, \quad y' = y, \quad z' = z, \quad t' = t,$$

gdyż suma s wypadłaby podzielna przez 4 wbrew założeniu. Natomiast istnieje jeden i tylko jeden układ liczb całkowitych ξ, η, ζ, θ , spełniających równość (50), dla których (por. wzory (53)):

$$(58) \quad \begin{aligned} x &= -\xi + \eta + \zeta + \theta, & y &= \xi - \eta + \zeta + \theta, \\ z &= \xi + \eta - \zeta + \theta, & t &= \xi + \eta + \zeta - \theta, \end{aligned}$$

gdyż zakładając, że wzory (58) zachodzą, otrzymujemy z nich w jednej chwili:

$$(59) \quad \begin{aligned} \frac{-x+y+z+t}{4} &= \xi, & \frac{x-y+z+t}{4} &= \eta, \\ \frac{x+y-z+t}{4} &= \zeta, & \frac{x+y+z-t}{4} &= \theta, \end{aligned}$$

co dowodzi, że układ x, y, z, t odpowiada co najwyżej jednemu układowi ξ, η, ζ, θ , i to takiemu, dla którego zachodzą wzory (59); zakładając zaś wzory (59) i wyznaczając z nich liczby ξ, η, ζ, θ , łatwo sprawdzić, że w rozpatrywanym przypadku 2° liczby te są wobec nieparzystości liczb x, y, z, t całkowite, spełniają wzory (58), a wobec (31) również wzór (50), co dowodzi, że układ x, y, z, t odpowiada co najmniej jednemu takiemu układowi ξ, η, ζ, θ .

Tak więc w przypadku 2° rozkład (31) znowu odpowiada wzajemnie jednoznacznie pewnemu rozkładowi (50) liczby u na sumę czterech kwadratów.

Dochodzimy zatem do wniosku, że liczba rozkładów liczby $4u$ na sumę kwadratów czterech liczb nieparzystych jest dwa razy większa niż liczba $\tau_4(u)$ rozkładów liczby (nieparzystej) u na sumę kwadratów czterech liczb całkowitych.

Stąd na mocy twierdzenia 10

$$(60) \quad \tau_4(u) = 8\sigma(u)$$

dla wszelkiej liczby nieparzystej u . Mamy więc

Twierdzenie 11. *Liczba rozkładów liczby naturalnej nieparzystej na sumę kwadratów czterech liczb całkowitych równa jest ośmiokrotnej sumie jej dzielników.*

Ponieważ suma dzielników liczby nieparzystej większej od 1 jest niemniejsza niż 4, więc na mocy twierdzenia 11 każda taka liczba nieparzysta ma co najmniej 32 rozkłady na sumę czterech kwadratów liczb całkowitych. Ponieważ zaś liczba nieparzysta kwadratowa ma dokładnie 8 różnych rozkładów na sumę czterech liczb całkowitych, z których trzy są zerami, więc wynika stąd, że każda liczba nieparzysta kwadratowa większa od 1 jest sumą kwadratów czterech liczb całkowitych, z których co najmniej dwie są różne od 0. Stąd już łatwo wynika za pomocą twierdzenia Lagrange'a (Rozdział IV, § 10, str. 93) następujący

Wniosek. *Każda liczba naturalna większa od 1 jest sumą kwadratów czterech liczb całkowitych, z których co najmniej dwie są różne od 0.*

Wniosek ten został wyprowadzony w Rozdziale IV (§ 10, str. 101, ćwiczenie 8) z nieudowodnionego w tej książce twierdzenia Gauss'a.

Obliczmy teraz liczbę rozkładów liczby $4u$ (gdzie u nieparzyste) na sumę kwadratów czterech liczb całkowitych. Niech

$$(61) \quad 4u = x^2 + y^2 + z^2 + t^2$$

będzie jednym z takich rozkładów.

Gdyby jedna z liczb x, y, z, t była parzysta, a pozostałe trzy nieparzyste, albo jedna nieparzysta, a pozostałe trzy parzyste, to suma ich kwadratów byłaby nieparzysta, wbrew (61).

Gdyby zaś dwie z tych liczb były parzyste, a dwie nieparzyste, to suma kwadratów wypadłaby formy $4k+2$, znowu wbrew (61).

Liczy x, y, z, t muszą więc być albo wszystkie cztery nieparzyste, albo wszystkie cztery parzyste.

Ponieważ w myśl twierdzenia 10 znamy już liczbę rozkładów liczby $4u$ na sumę kwadratów czterech liczb nieparzystych, więc wystarczy jeszcze obliczyć liczbę rozkładów tej liczby na sumę kwadratów czterech liczb parzystych.

Otóż łatwo widzieć, że każdemu takiemu rozkładowi

$$4u = (2\xi)^2 + (2\eta)^2 + (2\zeta)^2 + (2\vartheta)^2$$

odpowiada pewien rozkład liczby u na sumę kwadratów czterech liczb całkowitych

$$u = \xi^2 + \eta^2 + \zeta^2 + \vartheta^2,$$

i na odwrót. Stąd wniosek, że liczba rozkładów liczby $4u$ na sumę kwadratów czterech liczb parzystych jest równa liczbie rozkładów liczby u na sumę kwadratów czterech liczb całkowitych, która w myśl (60) wynosi $8\sigma(u)$.

Liczba rozkładów liczby $4u$ (gdzie u nieparzyste) na sumę kwadratów czterech liczb całkowitych wynosi więc razem

$$16\sigma(u) + 8\sigma(u) = 24\sigma(u).$$

Mamy zatem wzór

$$(62) \quad \tau_4(4u) = 24\sigma(u)$$

przy wszelkim u nieparzystym.

Obliczmy jeszcze liczbę rozkładów liczby $2u$ na sumę czterech kwadratów. Okażemy, że

$$(63) \quad \tau_4(2u) = \tau_4(4u).$$

Istotnie, jeżeli (61) jest jakimkolwiek rozkładem liczby $4u$ (gdzie u nieparzyste) na sumę czterech kwadratów, to — jak dowiedliśmy — liczby x, y, z, t są albo wszystkie cztery parzyste, albo wszystkie cztery nieparzyste. W każdym więc razie liczby

$$(64) \quad \xi = \frac{x+y}{2}, \quad \eta = \frac{x-y}{2}, \quad \zeta = \frac{z+t}{2}, \quad \vartheta = \frac{z-t}{2}$$

są całkowite, a że wzór (61) możemy napisać w postaci

$$2u = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2,$$

więc mamy rozkład

$$(65) \quad 2u = \xi^2 + \eta^2 + \zeta^2 + \vartheta^2.$$

Każdemu rozkładowi (61) liczby $4u$ na sumę czterech kwadratów odpowiada zatem pewien rozkład (65) liczby $2u$ na sumę

czterech kwadratów. Z drugiej strony łatwo widzieć, że każdemu rozkładowi (65) liczby $2u$ na sumę czterech kwadratów odpowiada tylko jeden rozkład (61) liczby $4u$ na sumę czterech kwadratów, ponieważ w założeniu, że odpowiada on w myśl powyższego przyporządkowania rozkładowi (61), otrzymujemy wzory (64), które dają:

$$\xi + \eta = x, \quad \xi - \eta = y, \quad \zeta + \vartheta = z, \quad \zeta - \vartheta = t,$$

i przeto wyznaczają rozkład (61) jednoznacznie.

Powyższe przyporządkowanie ustala zatem odpowiedniość wzajemnie jednoznaną między wszystkimi rozkładami liczby $4u$ oraz wszystkimi rozkładami liczby $2u$. Tym samym udowodniłszy wzór (65), skąd w myśl (62) mamy wzór

$$(66) \quad \tau_4(2u) = 24\sigma(u)$$

przy wszelkim u nieparzystym.

Obliczymy teraz liczbę rozkładów na sumę czterech kwadratów liczby $2^h u$ dla $h=3, 4, \dots$ (gdzie u nieparzyste). Niech

$$(67) \quad 2^h u = x^2 + y^2 + z^2 + t^2$$

będzie jakimkolwiek rozkładem liczby $2^h u$ na sumę czterech kwadratów. Liczby x, y, z, t nie mogą być wszystkie nieparzyste, gdyż wtedy prawa strona wzoru (67) przystawałaby do 4 modulo 8, gdy tymczasem lewa strona tego wzoru jest (wobec $h \geq 3$) podzielna przez 8. Podobnie, dwie z liczb x, y, z, t nie mogą być parzyste, a drugie dwie nieparzyste, gdyż wówczas prawa strona wzoru (67) przystawałaby do 2 modulo 4, co niemożliwe. Stąd łatwo wniosek, że liczby x, y, z, t są wszystkie cztery parzyste.

Niech więc

$$x = 2\xi, \quad y = 2\eta, \quad z = 2\zeta, \quad t = 2\vartheta,$$

gdzie $\xi, \eta, \zeta, \vartheta$ są liczbami całkowitymi. Na mocy (67) jest zatem

$$(68) \quad 2^{h-2}u = \xi^2 + \eta^2 + \zeta^2 + \vartheta^2.$$

Każdemu rozkładowi (67) liczby $2^h u$ na sumę czterech kwadratów odpowiada tym sposobem pewien rozkład (68) liczby $2^{h-2}u$ na sumę czterech kwadratów. Z drugiej strony — jak łatwo widzieć — każdemu rozkładowi (68) liczby $2^{h-2}u$ odpowiada jeden tylko rozkład liczby $2^h u$, mianowicie rozkład

$$2^h u = (2\xi)^2 + (2\eta)^2 + (2\zeta)^2 + (2\vartheta)^2.$$

Stąd wzór

$$(69) \quad \tau_4(2^h u) = \tau_4(2^{h-2} u)$$

przy wszelkim $h \geq 3$ naturalnym i wszelkim u naturalnym nieparzystym.

Niech teraz s będzie jakąkolwiek liczbą naturalną, a u — liczbą naturalną nieparzystą. Dla $s=1$ mamy w myśl (66), a dla $s=2$ w myśl (62)

$$(70) \quad \tau_4(2^s u) = 24\sigma(u).$$

Dla $s > 2$ rozróżnimy dwa przypadki:

1° $s=2k$. W myśl (69) możemy napisać dla kolejnych wartości $h=2k, 2k-2, \dots$

$$\tau_4(2^s u) = \tau_4(2^{2k} u) = \tau_4(2^{2k-2} u) = \tau_4(2^{2k-4} u) = \dots = \tau_4(2^2 u),$$

skąd znowu wynika wzór (70) na mocy (62).

2° $s=2k+1$. W myśl (69) mamy

$$\tau_4(2^s u) = \tau_4(2^{2k+1} u) = \tau_4(2^{2k-1} u) = \dots = \tau_4(2^3 u) = \tau_4(2u)$$

i odnajdujemy wzór (70) na mocy (66).

Tak więc wzór (70) zachodzi przy wszelkim s naturalnym i wszelkim u naturalnym nieparzystym.

Wzory (60) i (70) dają się ująć w jedno twierdzenie.

Niech mianowicie n będzie jakąkolwiek liczbą naturalną. Obliczmy sumę $\sigma^*(n)$ wszystkich tych dzielników naturalnych liczby n , które nie są podzielne przez 4.

Dla nieparzystego $n=u$ żaden z dzielników liczby n nie jest podzielny przez 4 i wtedy

$$(71) \quad \sigma^*(n) = \sigma(u).$$

Załóżmy więc, że n jest liczbą parzystą. Niech $n=2^s u$, gdzie s jest liczbą naturalną, a u — liczbą nieparzystą. Jasne jest, że każdy niepodzielny przez 4 dzielnik liczby $2^s u$ jest dzielnikiem liczby $2u$ i, na odwrót, każdy dzielnik liczby $2u$ jest niepodzielny przez 4 dzielnikiem liczby $2^s u$. Zatem

$$\sigma^*(n) = \sigma^*(2^s u) = \sigma(2u),$$

a że wobec $(2, u) = 1$ jest oczywiście

$$\sigma(2u) = \sigma(2)\sigma(u) = 3\sigma(u),$$

więc

$$(72) \quad \sigma^*(n) = 3\sigma(u).$$

Łącząc wzory (71) i (72) ze wzorami (60) i (70), otrzymujemy wzór

$$(73) \quad \tau_4(n) = 8\sigma^*(n),$$

zachodzący przy wszelkim n naturalnym. Udowodniliśmy więc

Twierdzenie 12. *Liczba rozkładów liczby naturalnej n na sumę kwadratów czterech liczb całkowitych jest równa ośmiokrotnej sumie wszystkich tych dzielników liczby n , które nie są podzielne przez 4.*

Ponieważ każda liczba naturalna ma co najmniej jeden dzielnik niepodzielny przez 4 (mianowicie liczbę 1), więc jako szczególny przypadek twierdzenia 12 otrzymujemy twierdzenie, udowodnione na innej drodze w Rozdziale IV (§ 10, str. 93), że każda liczba naturalna rozkłada się na sumę czterech kwadratów.

PRZYKŁADY. Mamy w myśl (70)

$$\tau_4(100) = 24\sigma(25) = 24 \frac{5^3-1}{5-1} = 24 \cdot 31 = 744.$$

Liczba 100 rozkłada się więc 744 sposobami na sumę czterech kwadratów.

W taki sam sposób znajdujemy

$$\tau_4(90) = 24\sigma(45) = 24 \frac{5^3-1}{5-1} \cdot \frac{3^2-1}{3-1} = 24 \cdot 13 \cdot 6 = 1872.$$

Jest to największa liczba rozkładów na sumę czterech kwadratów dla liczb pierwszej setki ¹⁾.

Podobnie:

$$\begin{aligned} \tau_4(7) &= 8\sigma(7) = 8 \cdot 8 = 64, & \tau_4(6) &= 24\sigma(3) = 24 \cdot 4 = 96, \\ \tau_4(96) &= 24\sigma(3) = 24 \cdot 4 = 96, & \tau_4(1024) &= \tau_4(2^{10}) = 24\sigma(1) = 24. \end{aligned}$$

Ze wzoru (73) otrzymuje się z łatwością wzór

$$\sum_{n=1}^{E(x)} \tau_4(n) = 8S(x) - 32S\left(\frac{x}{4}\right),$$

gdzie

$$S(x) = \sum_{k=1}^{E(x)} k E\left(\frac{x}{k}\right) = \frac{1}{2} \sum_{k=1}^{E(x)} E\left\{\frac{x}{k} \left[E\left(\frac{x}{k}\right) + 1 \right] \right\}$$

¹⁾ Tabliczkę wartości funkcji $\tau_4(n)$ dla $n < 100$ podałem w Pracach Matematyczno-Fizycznych, tom 18 (1908), str. 59.

(por. str. 133), z którego można wyprowadzić drogą elementarną dla x całkowitych nierówność

$$\left| \sum_{n=1}^x \tau_4(n) - \frac{\pi^2 x^2}{2} \right| < 100x\sqrt{x},$$

jako też na drodze arytmetycznej uzyskać wzór Eulera ¹⁾

$$\frac{\pi^2}{6} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots$$

¹⁾ Ob. poprzednie wydanie tej książki z 1925 r., str. 365-370.