3⁰ Liczba a nie jest podzielna przez p. W tym przypadku mamy $(a,p)=1$ wobec założenia, że p jest liczbą pierwszą. Możemy więc (ob. Rozdział II, § 2) wyznaczyć takie dwie liczby całkowite ξ i η, iż

$$a\xi+p\eta=1;$$

pisząc $x_0=b\xi$, będziemy mieli $ax_0=ab\xi=b-bp\eta\equiv b\pmod p$ czyli

$$ax_0\equiv b\pmod p. \tag{9}$$

Kongruencja (9) ma więc w tym przypadku co najmniej jeden pierwiastek. Załóżmy, że liczba x_1 jest również pierwiastkiem kongruencji (9). Mielibyśmy $ax_1\equiv ax_0\pmod p$, skąd wnosilibyśmy, że różnica $a(x_1-x_0)$ jest podzielna przez p.

Lecz wobec $(a,p)=1$ musiałoby x_1-x_0 być wtedy podzielne przez p, czyli

$$x_1\equiv x_0\pmod p.$$

Liczby x_0 i x_1 przedstawiają więc ten sam pierwiastek kongruencji (9). Udowodniliśmy zatem

Twierdzenie 2. *Jeżeli a jest liczbą niepodzielną przez liczbę pierwszą p, to kongruencja*

$$ax\equiv b\pmod p$$

ma jeden i tylko jeden pierwiastek.

Zauważmy na zakończenie, że liczenie pierwiastków kongruencji $f(x)\equiv 0\pmod m$, jakie stosujemy w przypadku, gdy $f(x)$ jest wielomianem całkowitym o spółczynnikach całkowitych, nie daje się zastosować w innych przypadkach, np. do kongruencji wykładniczej $2^x\equiv 1\pmod 7$, gdyż np. liczba 10, choć przystaje według modułu 7 do pierwiastka 3 tej kongruencji, nie jest jej pierwiastkiem (por. str. 43).

ROZDZIAŁ IV

TWIERDZENIA WILSONA, EULERA I FERMATA TWIERDZENIA O ROZKŁADACH NA SUMĘ KWADRATÓW

§ 1. Reszty i niereszty kwadratowe. Dowód twierdzeń Wilsona, Eulera i małego twierdzenia Fermata. Symbol Legendre'a. Niech p oznacza liczbę pierwszą nieparzystą, D zaś liczbę całkowitą niepodzielną przez p.

Będziemy nazywać liczbami *odpowiednimi* każde dwie liczby m i n z ciągu

$$1,\ 2,\ \ldots,\ p-1, \tag{1}$$

dla których zachodzi kongruencja

$$mn\equiv D\pmod p. \tag{2}$$

Z definicji tej wynika bezpośrednio, że jeżeli n jest liczbą odpowiednią dla m, to i na odwrót, m jest liczbą odpowiednią dla n.

Udowodnimy, że każda z liczb ciągu (1) ma jedną i przy tym tylko jedną liczbę odpowiednią.

Istotnie, niech m będzie liczbą z ciągu (1). Na to, żeby liczba x z ciągu (1) była odpowiednią dla m, potrzeba i wystarcza, by zachodziła kongruencja

$$mx\equiv D\pmod p. \tag{3}$$

Jest to kongruencja 1-go stopnia o module pierwszym i spółczynnik m przy niewiadomej jest niepodzielny przez moduł, gdyż — jak zakładamy — m jest jednym z wyrazów ciągu (1). Kongruencja (3) ma zatem jeden i tylko jeden pierwiastek. W ciągu wszystkich reszt według modułu p, tj. w ciągu

$$0,\ 1,\ 2,\ \ldots,\ p-1, \tag{4}$$

jest więc jedna i tylko jedna liczba, spełniająca kongruencję (3). Liczbą tą nie może być 0, gdyż prawa strona kongruencji (3),

tj. liczba D, jest niepodzielna przez p. Wnosimy stąd natychmiast, że w ciągu (1) istnieje jedna i tylko jedna liczba, spełniająca kongruencję (3), c. b. d. o.

Może się zdarzyć, że liczby odpowiednie m i n są równe. Kongruencja (2) daje wówczas

$$m^2 \equiv D \pmod p,$$

co jest możliwe oczywiście tylko wtedy, gdy istnieje kwadrat, dający przy dzieleniu przez p tę samą resztę co i liczba D. W tym przypadku przyjęto mówić, że D jest *resztą* (lub *pozostałością*) *kwadratową* dla modułu p. W przeciwnym razie, tj. kiedy żaden kwadrat nie daje według modułu p tej samej reszty co liczba D, powiadamy, że D jest *niereszta*ą (lub *niepozostałością*) *kwadratową* dla p. Innymi słowy, *liczbę D, niepodzielną przez liczbę pierwszą nieparzystą p, nazywamy resztą albo niereszta*ą *kwadratową dla p zależnie od tego, czy kongruencja*

$$x^2 \equiv D \pmod p$$

jest rozwiązalna, czy nie.

Zajmiemy się najpierw przypadkiem, kiedy D jest niereszta*ą* kwadratową dla p. Wówczas każda para liczb odpowiednich m i n składa się z dwu różnych liczb. Wszystkie liczby ciągu (1) będziemy więc mogli w tym przypadku podzielić na pary liczb odpowiednich; par tych będzie oczywiście $\frac{p-1}{2}$. Dla każdej pary wypiszemy kongruencję (2); otrzymamy w ten sposób ciąg $\frac{p-1}{2}$ kongruencji:

$$\begin{aligned} m_1 n_1 &\equiv D \pmod p, \\ m_2 n_2 &\equiv D \pmod p, \\ &\cdots\cdots\cdots \\ m_{\frac{p-1}{2}} n_{\frac{p-1}{2}} &\equiv D \pmod p. \end{aligned}$$

Mnożąc te kongruencje stronami i zważywszy, że iloczyn

$$m_1 n_1 m_2 n_2 \ldots m_{\frac{p-1}{2}} n_{\frac{p-1}{2}}$$

różni się co najwyżej porządkiem czynników od iloczynu wszystkich wyrazów ciągu (1), otrzymamy kongruencję

$$(5) \qquad (p-1)! \equiv D^{\frac{p-1}{2}} \pmod p.$$

Zajmijmy się teraz przypadkiem, gdy D jest resztą kwadratową dla p. Wówczas kongruencja

$$(6) \qquad x^2 \equiv D \pmod p$$

jest rozwiązalna. Zapytajmy, ile wyrazów ciągu (1) spełnia tę kongruencję. Skoro kongruencja (6) jest rozwiązalna, to w ciągu (4) istnieje co najmniej jedna liczba, która ją spełnia; niech to będzie liczba k. Nie może być $k=0$, gdyż D nie jest podzielne przez p. Jest więc k jedną z liczb ciągu (1) czyli liczbą całkowitą, spełniającą nierówność $0<k<p$, a więc $l=p-k$ jest również liczbą spełniającą tę nierówność. Przy tym jest $l \neq k$, gdyż w razie $l=k$ mielibyśmy $k=p-k$, skąd $p=2k$ wbrew założeniu, że p jest liczbą nieparzystą. Z drugiej strony, mamy oczywiście

$$l^2 = (p-k)^2 \equiv (-k)^2 \equiv k^2 \pmod p,$$

a że — jak założyliśmy — k spełnia kongruencję (6), więc też l ją spełnia czyli $l^2 \equiv D \pmod p$.

Jeżeli więc D jest resztą kwadratową dla p, to w ciągu (1) istnieją c o n a j m n i e j dwie liczby spełniające kongruencję (6). Udowodnimy, że t y l k o dwie liczby ciągu (1) spełniają tę kongruencję.

Istotnie, niech liczba x z ciągu (1) spełnia kongruencję (6). Wobec $k^2 \equiv D \pmod p$, kongruencja (6) daje $x^2 \equiv D \equiv k^2 \pmod p$, co dowodzi, że różnica x^2-k^2 jest podzielna przez p. Lecz $x^2-k^2=(x-k)(x+k)$, a że p jest liczbą pierwszą, więc iloczyn ten może być przez p podzielny tylko wtedy, jeżeli przynajmniej jeden z czynników jest podzielny przez p.

Niech najpierw $x-k$ będzie podzielne przez p. Skoro liczby x i k są wyrazami ciągu (1), to mamy nierówności:

$$(7) \qquad 0<x<p, \qquad 0<k<p,$$

skąd $-p<x-k<p$.

Lecz między $-p$ a p tylko liczba 0 jest podzielna przez p; mamy więc tutaj $x-k=0$ czyli $x=k$.

Niech teraz $x+k$ będzie podzielne przez p. Wobec nierówności (7) mamy $0<x+k<2p$, a że między liczbą 0 a $2p$ tylko liczba p jest podzielna przez p, więc $x+k=p$ czyli $x=p-k=l$.

Dowiedliśmy zatem, że oprócz liczb k i l żaden inny wyraz ciągu (1) nie spełnia kongruencji (6). Mamy więc

Twierdzenie 1. *Jeżeli D jest resztą kwadratową dla p, to kongruencja* (6) *ma dokładnie dwa pierwiastki.*

Usuńmy teraz liczby k i l z ciągu (1). Pozostałe $p-3$ wyrazy tego ciągu będziemy mogli znowu podzielić na pary liczb odpowiednich. Par tych będzie $\frac{p-3}{2}$ i dla każdej z nich znowu będziemy mogli wypisać kongruencję (2). Otrzymamy w ten sposób ciąg $\frac{p-3}{2}$ kongruencyj:

$$\begin{aligned} m_1 n_1 &\equiv D \pmod p, \\ m_2 n_2 &\equiv D \pmod p, \\ &\cdots\cdots\cdots \\ m_{\frac{p-3}{2}} n_{\frac{p-3}{2}} &\equiv D \pmod p. \end{aligned} \tag{8}$$

Gdybyśmy teraz kongruencje te pomnożyli stronami, to po lewej stronie nie otrzymalibyśmy iloczynu wszystkich liczb (1), brakłoby bowiem liczb k i l.

Możemy jednak do ciągu kongruencji (7) dopisać jeszcze kongruencję

$$kl \equiv -D \pmod p, \tag{9}$$

gdyż $kl = k(p-k) \equiv -k^2 \equiv -D \pmod p$.

Mnożąc teraz stronami iloczyn kongruencji (8) przez kongruencję (9), otrzymamy już po lewej stronie, po ewentualnej zmianie porządku czynników, iloczyn $(p-1)!$. Stąd kongruencja

$$(p-1)! \equiv -D^{\frac{p-1}{2}} \pmod p, \tag{10}$$

gdyż liczba mnożonych kongruencji wynosi znowu $\frac{p-1}{2}$.

Mamy więc bądź wzór (5), bądź wzór (10) zależnie od tego, czy D nie jest, czy jest resztą kwadratową dla p.

Oba te wzory możemy połączyć w jeden:

$$(p-1)! \equiv \mp D^{\frac{p-1}{2}} \pmod p, \tag{11}$$

gdzie po stronie prawej należy wziąć znak górny albo dolny zależnie od tego, czy D jest resztą, czy nieresztą kwadratową dla p.

Przyjmijmy w szczególności $D=1$. Jedność jest oczywiście resztą kwadratową dla każdego modułu p, musimy zatem wziąć znak górny, co daje

$$(p-1)! \equiv -1 \pmod p. \tag{12}$$

Kongruencję tę wyprowadziliśmy wprawdzie w założeniu, że p jest liczbą pierwszą nieparzystą, łatwo jednak sprawdzić bezpośrednio, że jest ona prawdziwa i dla $p=2$. Mamy bowiem

$$(2-1)! = 1! = 1 \equiv -1 \pmod 2.$$

Kongruencja (12) jest zatem prawdziwa dla każdej liczby pierwszej. Mamy więc

Twierdzenie 2. *Jeżeli p jest liczbą pierwszą, to liczba $(p-1)!+1$ jest podzielna przez p.*

Jest to tzw. *twierdzenie Wilsona* (odkryte około 1770 r.).

Godne uwagi jest, że twierdzenie to daje się odwrócić. Mianowicie, jeżeli $p>1$ i liczba $(p-1)!+1$ jest podzielna przez p, to p jest liczbą pierwszą. Istotnie jeżeli $p>1$ nie jest liczbą pierwszą, to p ma dzielnik q, spełniający nierówności $1<q<p$. Liczba $(p-1)!+1$, jako podzielna przez p, musiałaby tym bardziej być podzielna przez q. Lecz q, jako liczba naturalna mniejsza od p, jest jednym z czynników iloczynu

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-1) = (p-1)!$$

Liczba $(p-1)!+1$ daje zatem przy dzieleniu przez q resztę 1.

A więc na to, żeby liczba $p>1$ była liczbą pierwszą, potrzeba i wystarcza, by liczba $(p-1)!+1$ była podzielna przez p. Mamy tu pewną *charakterystyczną* własność liczb pierwszych.

Np. $4!+1=25$ jest podzielne przez 5; $6!+1=721$ jest podzielne przez 7, lecz $5!+1=121$ nie jest podzielne przez 6.

W związku z twierdzeniem Wilsona zauważymy, że zachodzi następujące

Twierdzenie Leibniz'a [1]. *Na to, by liczba $p>1$ była pierwszą, potrzeba i wystarcza, żeby było*

$$(p-2)! \equiv 1 \pmod p.$$

Pozostawiamy czytelnikowi łatwe wyprowadzenie tego twierdzenia z twierdzenia Wilsona.

Łatwo też wyprowadzić następujące uogólnienie tych twierdzeń [2]:

---

[1]) G. W. Leibniz, *Manuscrits inédits conservés à la Bibliothèque de Hannover et publiés dans le Formulaire de Mathématiques t. 2, N. 3 (1899) par M. Vacca*, t. 3, B. 11, fol. 10.

[2]) Ob. X. Smitgoud, Intermédiaire des Recherches Mathématiques 1 (1945), p. 104, 0320.

Na to, by liczba całkowita $p>1$ była pierwsza, potrzeba i wystarcza, żeby dla każdej liczby całkowitej n, takiej że $0\leqslant n\leqslant p-1$, zachodziła kongruencja

$$(p-1-n)!\,n!+(-1)^n\equiv 0 \pmod p.$$

Zauważmy jeszcze, że jeżeli liczba p jest złożona i $p\neq 4$, to

$$(*)\qquad (p-1)!\equiv 0 \pmod p.$$

Istotnie, jeżeli liczba p jest złożona, to istnieją takie liczby naturalne q i r, iż $p=qr$, $1<q<p$ i $1<r<p$.

W przypadku, gdy $q\neq r$, liczby q i r są różnymi czynnikami iloczynu $1\cdot 2\cdot\ldots\cdot(p-1)$, który zatem jest podzielny przez $qr=p$, stąd wzór (*).

W przypadku zaś, gdy $q=r$, jest $p=q^2$, a ponieważ p jest liczbą złożoną i $p\neq 4$, więc $p>4$ i przeto $q>2$. Wynika stąd, że $p=q^2>2q$, a więc q i $2q$ są różnymi czynnikami iloczynu $(p-1)!$, który zatem jest podzielny przez $q\cdot 2q$, a tym bardziej przez $q^2=p$, co znowu daje wzór (*).

Natomiast dla $p=4$ mamy

$$(p-1)!=3!=6=2 \pmod 4.$$

Podajemy tu bez dowodu następujące uogólnienie twierdzenia Wilsona:

Iloczyn wszystkich liczb naturalnych pierwszych względem m i zarazem mniejszych od m jest przystający do -1 według modułu m tylko wtedy, gdy liczba m może być przedstawiona w jednej z dwu postaci: p^α, $2p^\alpha$, gdzie p jest liczbą pierwszą, a zaś liczbą naturalną; w pozostałych przypadkach powyższy iloczyn przystaje do $+1$ według modułu m [1]).

Jako ćwiczenie pozostawiamy czytelnikowi bezpośrednie sprawdzenie tego twierdzenia dla wszystkich liczb naturalnych od 1 do 10.

Spośród liczb $n!+1$ dla $n\leqslant 14$ tylko liczby:

$1!+1=2$; $2!+1=3$, $3!+1=7$ i $11!+1=39\,916\,801$

są pierwsze [2]). Natomiast:

$4!+1=5^2$, $5!+1=11^2$, $6!+1=7\cdot 103$,
$7!+1=71^2$, $8!+1=61\cdot 661$, $9!+1=19\cdot 71\cdot 269$,

[1]) C. F. Gauss, *Disquisitiones Arithmeticae*, Lipsk 1801, n° 78.

[2]) Dowód, że liczba $11!+1$ jest pierwszą, znajduje się w książce A. Ferrier, *Les nombres premiers*, Paryż 1947, str. 30.

$10!+1\equiv 0 \pmod{11}$, $12!+1\equiv 0 \pmod{13}$,
$13!+1\equiv 0 \pmod{83}$, $14!+1\equiv 0 \pmod{23}$.

Z twierdzenia Wilsona wynika, że liczb naturalnych n, dla których $n!+1$ jest liczbą złożoną, jest nieskończenie wiele: są to bowiem wszystkie liczby $n=p-1$, gdzie p jest liczbą pierwszą większą od 3.

Łatwo też wysnuć z twierdzenia Wilsona, że nieskończenie wiele jest również liczb naturalnych n, dla których $n!-1$ jest liczbą złożoną. Mianowicie, wobec $p-1\equiv -1 \pmod p$ każda liczba pierwsza p spełnia na mocy twierdzenia Wilsona kongruencję $(p-2)!\equiv 1 \pmod p$ i przeto dla każdego $p>5$ pierwszego liczba $(p-2)!-1>p$ jest złożona.

Ze wzorów (11) i (12) otrzymujemy bezpośrednio

Twierdzenie 3. *Jeżeli liczba całkowita D jest niepodzielna przez liczbę pierwszą p, to*

$$(13)\qquad D^{\frac{p-1}{2}}\equiv \pm 1 \pmod p,$$

przy czym po prawej stronie należy wziąć $+$ lub $-$ zależnie od tego, czy D jest, czy nie jest resztą kwadratową dla p.

Jest to t. zw. *twierdzenie Eulera.*

Podnosząc obie strony kongruencji (13) do kwadratu, otrzymujemy

Twierdzenie 4. *Jeżeli liczba całkowita D jest niepodzielna przez liczbę pierwszą p, to*

$$(14)\qquad D^{p-1}\equiv 1 \pmod p.$$

Jest to t. zw. *małe* [1]) *twierdzenie Fermata.* Zostało ono podane przez P. Fermata bez dowodu w 1670 r. Pierwszy dowód podał Euler w 1741 r.

Wzór (14) wyprowadziliśmy w założeniu, że p jest liczbą pierwszą nieparzystą, ale prawdziwość jego dla $p=2$ jest widoczna, gdyż skoro D jest niepodzielne przez p, a więc nieparzyste, to $D\equiv 1 \pmod 2$.

Zatem dla każdej liczby całkowitej D, niepodzielnej przez liczbę pierwszą p, liczba $D^{p-1}-1$ jest podzielna przez p.

[1]) Dla odróżnienia od dotąd jeszcze nie dowiedzionego tzw. *wielkiego twierdzenia Fermata* (p. Rozdział XIX).

Np. $2^{10}-1=1023$ jest podzielne przez 11, $3^4-1=80$ jest podzielne przez 5, $10^2-1=99$ jest podzielne przez 3 itp.

Małe twierdzenie Fermata daje się — jak łatwo widzieć — odwrócić, jak następuje:

Jeżeli dla każdej liczby całkowitej a, niepodzielnej przez liczbę $p>1$, jest $a^{p-1}\equiv 1 \pmod p$, to p jest liczbą pierwszą.

Istotnie, gdyby liczba $p>1$ nie była pierwsza, mielibyśmy $p=mn$ gdzie m i n są liczbami naturalnymi większymi od 1. Liczba m nie jest oczywiście podzielna przez p, a jednak nie może być $m^{p-1}\equiv 1 \pmod p$, gdyż wtedy byłoby też $m^{p-1}\equiv 1 \pmod m$, co niemożliwe, ponieważ $m^{p-1}\equiv 0 \pmod m$.

Dla poszczególnych liczb a może jednak być $a^{p-1}\equiv 1 \pmod p$, mimo że p jest liczbą złożoną. Np. $3^{120}\equiv 1 \pmod{121}$, mimo że $121=11^2$; a także $3^{670}\equiv 1 \pmod{671}$, mimo że $671=11\cdot 61$, jak to łatwo czytelnik sprawdzi. Więcej nawet:

Istnieją takie liczby złożone n, iż dla każdej liczby całkowitej a, pierwszej względem n, mamy

$$a^{n-1}\equiv 1 \pmod n. \tag{15}$$

Istotnie, taka jest np. liczba $n=561=3\cdot 11\cdot 17$. Jeżeli bowiem $(a, 561)=1$, to tym bardziej $(a, 3)=(a, 11)=(a, 17)=1$; wynika stąd w myśl małego twierdzenia Fermata, że:

$$a^2\equiv 1 \pmod 3, \qquad a^{10}\equiv 1 \pmod{11}, \qquad a^{16}\equiv 1 \pmod{17},$$

co daje przez podnoszenie do potęgi odpowiednio o wykładnikach 40, 8 i 5 kongruencje $a^{80}\equiv 1 \pmod{3, 11, 17}$. Z uwagi na to, że liczby 3, 11 i 17 są pierwsze oraz że ich iloczyn wynosi 561, otrzymujemy

$$a^{560}\equiv 1 \pmod{561}.$$

A zatem liczba $n=561$ spełnia kongruencję (15). Tę samą własność ma też liczba $n=5\cdot 13\cdot 17=1105$.

W tym więc sensie małe twierdzenie Fermata nie daje się odwrócić [1]).

Sispanov nazywa liczbę naturalną m *pseudo-pierwszą*, gdy $a^{m-1}\equiv 1 \pmod m$ dla $(a, m)=1$, oraz dowodzi, że na to, aby liczba naturalna m była *pseudo-pierwszą*, potrzeba i wystarcza, żeby była postaci $m=p_1p_2\ldots p_k$, gdzie $k\geqslant 3$ i gdzie p_i (dla $i=1, 2, \ldots, k$) są różnymi liczbami pierwszymi nieparzystymi, takimi iż $(p_i-1)\mid(m-1)$ [1]).

[1]) Por. P. Bachmann, Archiv der Mathematik und Physik (3), tom 21 (1913), str. 185-187.

Z małego twierdzenia Fermata wynika

Wniosek 1. *Jeżeli n jest liczbą pierwszą, to*

$$2^n\equiv 2 \pmod n. \tag{16}$$

Istnieją jednak liczby złożone n, spełniające warunek (16), np. liczba $341=11\cdot 31$. Istotnie, w myśl małego twierdzenia Fermata mamy $D^{10}\equiv 1 \pmod{11}$, skąd $2^{341}\equiv 2^{340}\cdot 2\equiv 2 \pmod{11}$; dalej $2^{30}\equiv 1 \pmod{31}$, skąd $2^{341}=2^{30\cdot 11}\cdot 2^{11}\equiv 2^{11}\equiv 2 \pmod{31}$, gdyż $2^{11}=2048=66\cdot 31+2$. Liczba $2^{341}-2$ jest zatem podzielna przez liczby pierwsze 11 i 31, a więc i przez 341, c. b. d. o.

Jak udowodnił Banachiewicz, 341 jest najmniejszą liczbą złożoną n o własności (16).

Następną jest liczba $561=3\cdot 11\cdot 17$, po niej $645=3\cdot 5\cdot 43$, dalej $1105=5\cdot 13\cdot 17$, $1387=19\cdot 73$, $1729=7\cdot 13\cdot 19$ i $1905=3\cdot 5\cdot 127$. Spośród liczb złożonych $n\leqslant 2000$ tylko tych 7 liczb spełnia kongruencję (16). Można jednak dowieść, że takich liczb złożonych jest nieskończenie wiele (ob. str. 66, ćwiczenie 15). Istnienie takich liczb obala przypuszczenie matematyków chińskich, że liczba $(2^n-2)/n$ nie może być całkowita dla n złożonych [2]).

Nie wiemy jednak, czy istnieją liczby złożone *parzyste* n, spełniające warunek (16). Innymi słowy: nie wiadomo, czy istnieją liczby naturalne $m>1$, spełniające kongruencję

$$2^{2m-1}\equiv 1 \pmod m.$$

Łatwo widzieć, że kongruencja (16) zachodzi też dla wszystkich liczb n postaci $n=2^{2^k}+1$. Istotnie, z samej postaci liczby n widzimy, że $2^{2^k}\equiv -1 \pmod n$; podnosząc obie strony tej kongruencji do potęgi parzystej $(n-1)\cdot 2^{-k}=2^{2^k-k}$, otrzymujemy $2^{n-1}\equiv 1 \pmod n$, skąd (16), c. b. d. o.

Więc np. kongruencja (16) zachodzi dla liczby złożonej $n=2^{2^5}+1$ (podzielnej przez 641).

[1]) S. Sispanov, Bolletino di Matematica 14 (1941), str. 99-106.

[2]) T. Banachiewicz, Sprawozdania Towarzystwa Naukowego Warszawskiego, tom 2 (1901) str. 9, gdzie podano tylko 5 liczb $n\leqslant 2000$ o własności (16).

D. H. Lehmer podał wszystkie 526 liczb złożonych $n<10^8$, spełniających kongruencję (16), których wszystkie dzielniki pierwsze są większe od liczby 313. Wyprowadził on stąd praktyczny sposób rozpoznawania, czy dana liczba naturalna $n<10^8$ jest pierwsza [1]).

Wniosek 2. *Jeżeli liczba p jest pierwsza, to dla każdej liczby całkowitej x zachodzi kongruencja*

$$x^p \equiv x \pmod p.$$

Z twierdzenia Fermata wynika dalej natychmiast, że każda z liczb ciągu (1) spełnia kongruencję dwumienną o module pierwszym

$$x^{p-1} \equiv 1 \pmod p,$$

a ponieważ liczba 0 oczywiście tej kongruencji nie spełnia, więc kongruencja ta ma $p-1$ pierwiastków czyli dokładnie tyle, ile jest jedności w jej stopniu. Z uwagi tej skorzystamy w Rozdziale VIII.

Zauważymy tu jeszcze, że na podstawie twierdzenia Fermata możemy z łatwością (przynajmniej teoretycznie) wyznaczyć pierwiastek kongruencji pierwszego stopnia (o module pierwszym)

$$ax \equiv b \pmod p.$$

Kongruencja ta ma — jak wiemy z twierdzenia 2 — jeden pierwiastek, jeżeli a jest niepodzielne przez p. Jest nim mianowicie $x=a^{p-2}b$.

Istotnie, wobec założenia, że a jest niepodzielne przez p, i w myśl twierdzenia Fermata mamy

$$ax = a^{p-1}b \equiv b \pmod p.$$

Powróćmy jeszcze do wzoru (13). Zakładając, że D jest liczbą niepodzielną przez liczbę pierwszą nieparzystą p, oznaczmy tak zwanym *symbolem Legendre'a*

$$\left(\frac{D}{p}\right)$$

liczbę 1 lub -1 zależnie od tego, czy D jest, czy nie jest resztą kwadratową dla p. Wzór (13) będziemy teraz mogli napisać w postaci:

$$\left(\frac{D}{p}\right) \equiv D^{\frac{p-1}{2}} \pmod p. \tag{17}$$

[1]) D. H. Lehmer, American Mathematical Monthly, tom 43 (1936), str. 347-353.

Otrzymany wynik wyrazimy jeszcze inaczej w § 2.

§ 2. Reszty bezwzględnie najmniejsze. Symbol Legendre'a $\left(\frac{D}{p}\right)$ jako reszta bezwzględnie najmniejsza liczby $D^{\frac{p-1}{2}}$ według modułu p. Udowodnimy następujące

Twierdzenie 5. *Dla każdej liczby całkowitej a i naturalnej m istnieje jedna i tylko jedna liczba całkowita ϱ, spełniająca warunki:*

$$\varrho \equiv a \pmod m \qquad i \qquad -\frac{m}{2} < \varrho \leqslant \frac{m}{2}. \tag{18}$$

Dowód. Niech r będzie resztą liczby a według modułu m:

$$r \equiv a \pmod m \qquad \text{i} \qquad 0 \leqslant r < m. \tag{19}$$

Jeżeli $r \leqslant \frac{m}{2}$, to liczba $\varrho = r$ spełnia oczywiście warunki (18).

Jeżeli zaś $r > \frac{m}{2}$, to liczba $\varrho = r - m$ spełnia warunki (18), gdyż w myśl (19) jest $\varrho \equiv r \equiv a \pmod m$ i $\frac{m}{2} - m < \varrho < m - m$ czyli $-\frac{m}{2} < \varrho < 0$.

Aby udowodnić, że istnieje tylko jedna liczba ϱ, spełniająca warunki (18), przypuśćmy, że spełniają je dwie różne liczby ϱ i ϱ'. Wtedy $\varrho - \varrho'$ byłoby podzielne przez m i $-m < \varrho - \varrho' < m$, co jest niemożliwe, gdyż między $-m$ a m tylko liczba 0 jest podzielna przez m.

Wniosek 1. *Jeżeli m jest liczbą nieparzystą, to dla każdego całkowitego a istnieje jedna i tylko jedna liczba całkowita ϱ, spełniająca warunki:*

$$\varrho \equiv a \pmod m, \qquad |\varrho| < \frac{m}{2}. \tag{20}$$

Dla każdej innej liczby r przystającej do a według modułu m będzie więc $|r| > \frac{m}{2}$, a zatem $|r| > |\varrho|$. Z tej racji nazywamy liczbę ϱ *resztą bezwzględnie najmniejszą* liczby a według modułu m.

Ponieważ wartością symbolu Legendre'a $\left(\frac{D}{p}\right)$ jest zawsze $+1$ lub -1, więc skoro p jest liczbą pierwszą nieparzystą (zatem $p \geqslant 3$), mamy nierówność:

$$\left|\left(\frac{D}{p}\right)\right| < \frac{p}{2}.$$

Wobec (17) możemy więc wypowiedzieć

Twierdzenie 6. $\left(\frac{D}{p}\right)$ *jest resztą bezwzględnie najmniejszą liczby* $D^{\frac{p-1}{2}}$ *według modułu pierwszego nieparzystego* p.

Niech np. $p=19$ i $D=2$; mamy $D^{\frac{p-1}{2}}=2^9=512$; resztą bezwzględnie najmniejszą liczby 512 według modułu 19 jest więc -1 czyli $\left(\frac{2}{19}\right)=-1$, a więc 2 jest nieresztą kwadratową dla modułu 19.

Niech teraz $p=11$ i $D=3$; mamy $D^{\frac{p-1}{2}}=3^5=243$; resztą bezwzględnie najmniejszą liczby $243 \pmod{11}$ jest tu $+1$ czyli $\left(\frac{3}{11}\right)=+1$, a więc 3 jest resztą kwadratową dla liczby 11.

Zajmiemy się teraz jeszcze pewnym ogólniejszym przykładem, z którego skorzystamy w Rozdziale XIV. Niech mianowicie $D=-1$. Resztą bezwzględnie najmniejszą liczby $(-1)^{\frac{p-1}{2}}$ jest oczywiście sama ta liczba; zatem

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

Ponieważ p jest liczbą nieparzystą, więc jest formy $4k+1$ lub $4k+3$. W przypadku pierwszym $\frac{p-1}{2}$ jest oczywiście liczbą parzystą, w drugim — nieparzystą. Wnosimy stąd, że

$$\left(\frac{-1}{p}\right)=+1$$

dla liczb pierwszych p formy $4k+1$, natomiast

$$\left(\frac{-1}{p}\right)=-1$$

dla liczb pierwszych p formy $4k+3$.

Dla liczb pierwszych formy $4k+1$ jest tedy -1 resztą kwadratową; dla liczb tych można więc wyznaczyć takie całkowite x, by liczba x^2+1 była podzielna przez p. Natomiast dla liczb pierwszych formy $4k+3$ liczba -1 nie jest resztą kwadratową.

ĆWICZENIA. 1. Dowieść, że 10-a potęga każdej liczby całkowitej jest postaci $11k$ lub $11k+1$ (gdzie k jest całkowite).

Dowód. Jeżeli a jest liczbą całkowitą niepodzielną przez 11, to w myśl małego twierdzenia Fermata jest $11 \mid (a^{10}-1)$, a zatem $a^{10}=11k+1$.

2. Dowieść, że 12-a potęga każdej liczby całkowitej jest postaci $13k$ lub $13k+1$.

3. Dowieść, że 20-a potęga każdej liczby całkowitej jest postaci $25k$ lub $25k+1$.

Dowód. Jeżeli $5 \mid a$, to $25 \mid a^2$ i tym bardziej $25 \mid a^{20}$. Jeżeli zaś $(a,5)=1$, to w myśl małego twierdzenia Fermata jest $a^4 \equiv 1 \pmod 5$; stąd $a^{4n} \equiv 1 \pmod 5$ dla $n=1,2,3,4$ i $1+a^4+a^8+a^{12}+a^{16} \equiv 0 \pmod 5$; a ponieważ

$$a^{20}-1=(a^4-1)(a^{16}+a^{12}+a^8+a^4+1),$$

więc $5^2 \mid (a^{20}-1)$.

4. Dowieść, że setna potęga każdej liczby całkowitej jest postaci $125k$ lub $125k+1$.

Dowód. Jeżeli $5 \mid a$, to $5^4 \mid a^4$ i tym bardziej $5^4 \mid a^{100}$. Jeżeli zaś $(a,5)=1$, to (w myśl ćwiczenia 3) jest $5^2 \mid a^{20}-1$ i $a^{20n} \equiv 1 \pmod{25}$ dla $n=1,2,3,4$: stąd $25 \mid (a^{80}+a^{60}+a^{40}+a^{20}+1)$, a ponieważ $a^{100}-1=(a^{20}-1)(a^{80}+a^{60}+a^{40}+a^{20}+1)$, więc $125 \mid a^{100}-1$.

5. Dowieść, że 9-a potęga każdej liczby całkowitej jest postaci $19k$ lub $19k \pm 1$.

Dowód. Jeżeli $19 \mid a$, to $a=19k$. Jeżeli $(a,19)=1$, to $a^{18} \equiv 1 \pmod{19}$; zatem $19 \mid (a^9-1)(a^9+1)$ i przeto jeżeli nie jest $19 \mid a^9-1$, to musi być $19 \mid a^9+1$ czyli $a^9=19k-1$.

6. Dowieść, że dla każdej liczby całkowitej x jest $x^8 \equiv 0, 1$ lub $-1 \pmod{17}$.

7. Dowieść, że dla wszelkich x całkowitych jest $42 \mid (x^7-x)$.

Dowód. Dla x całkowitych mamy oczywiście $2 \mid x^7-x$; w myśl zaś wniosku 2 z małego twierdzenia Fermata jest $x^3 \equiv x \pmod 3$, skąd $x^7 \equiv x^5 \equiv x^3 \equiv x \pmod 3$, a zatem $3 \mid x^7-x$; dalej $x^7 \equiv x \pmod 7$, zatem $7 \mid x^7-x$, a ponieważ $(2,3,7)=1$, więc $42 \mid x^7-x$, c. b. d. o.

8. Dowieść, że kwadrat liczby całkowitej jest zawsze postaci $5k$ lub $5k \pm 1$.

9. Dowieść, że jeżeli $(k,6)=1$, to $6 \mid (k^2+5)$.

10. Dowieść, że dla x całkowitych liczba $\frac{x^5}{120}-\frac{x^3}{24}+\frac{x}{30}$ jest całkowita.

11. Dowieść, że jeżeli p jest liczbą pierwszą, to $p \mid (5^p-2\cdot 3^p+1)$.

Dowód. Dla $p=2,3$ i 5 z łatwością sprawdzamy to bezpośrednio. Dla $p>5$ jest $(5,p)=1$, zatem w myśl wniosku z małego twierdzenia Fermata jest $5^p \equiv 5 \pmod p$; podobnie $3^p \equiv 3 \pmod p$, zatem $5^p-2\cdot 3^p+1 \equiv 5-2\cdot 3+1 \equiv 0 \pmod p$, c. b. d. o.

12. Dowieść, że $33^4+34^4\equiv 58^4+59^4 \pmod{100}$.

13. Dowieść, że jeżeli liczby $p>5$ i $2p+1$ są pierwsze, to liczba $4p+1$ jest złożona.

Dowód. Jeżeli liczby $p>3$ i $2p+1$ są pierwsze, to nie może być $3|(2p+1)$; a zatem nie może być $p\equiv 1 \pmod 3$. Lecz również nie może być $p\equiv 0 \pmod 3$, skoro $p>3$ jest liczbą pierwszą. Jest zatem $p\equiv 2 \pmod 3$, a więc $4p+1\equiv 0 \pmod 3$ czyli $3|(4p+1)$, co dowodzi, że liczba $4p+1$ jest złożona.

14. Dowieść, że jeżeli p jest liczbą pierwszą i $n=2^p-1$, to $2^n\equiv 2 \pmod n$.

Dowód. Dla $p=2$ jest to oczywiste. Jeżeli zaś p jest liczbą pierwszą nieparzystą, to na mocy twierdzenia 4 jest $2^{p-1}\equiv 1 \pmod p$, skąd $2^{p-1}-1=kp$, a zatem $2^{n-1}=2^{2(2^{p-1}-1)}=2^{2kp}=(2^p)^{2k}$; lecz ponieważ $n=2^p-1$, więc $2^p\equiv 1 \pmod n$, a zatem $2^{n-1}=(2^p)^{2k}\equiv 1 \pmod n$, skąd $2^n\equiv 2 \pmod n$, c. b. d. o.

15. Dowieść, że istnieje nieskończenie wiele liczb złożonych n, spełniających kongruencję (16) $2^n-2\equiv 0 \pmod n$.

Dowód. Jak wiemy (p. str. 61), istnieją takie liczby n złożone nieparzyste; jest nią np. liczba 341. Wystarczy więc okazać, że dla każdej takiej liczby złożonej nieparzystej n istnieje liczba złożona nieparzysta m od niej większa i spełniająca kongruencję (16).

Otóż jeżeli liczba złożona nieparzysta n spełnia kongruencję (16), to $2^{n-1}\equiv 1 \pmod n$. Wtedy $m=2^n-1$ jest liczbą złożoną większą od n i oczywiście nieparzystą. Jeżeli bowiem $n=rs$, gdzie $r>1$ i $s>1$, to zachodzą nierówności $1<r<n$ i $1<2^r-1<2^n-1$; przy tym 2^r-1 jest dzielnikiem liczby $m=2^n-1$.

Ponieważ $2^{n-1}\equiv 1 \pmod n$, więc $2^{n-1}-1=kn$, skąd $2^{m-1}=2^{2(2^{n-1}-1)}=2^{2kn}=(2^n)^{2k}$. Lecz wobec tego, że $m=2^n-1$, mamy $2^n\equiv 1 \pmod m$: zatem także $(2^n)^{2k}\equiv 1 \pmod m$ czyli $2^{m-1}\equiv 1 \pmod m$, skąd kongruencja (16), c. b. d. o.

16. Dowieść, że dla wszelkich naturalnych $n>1$ jest $25^n\equiv 76 \pmod{100}$.

17. Dowieść, że dla wszelkich naturalnych n jest

$$24^{2n-1}\equiv 24 \pmod{100} \quad \text{i} \quad 24^{2n}\equiv 76 \pmod{100}.$$

18. Dowieść, że dla wszelkich całkowitych x jest

$$x^7-x^5-x^3+x\equiv 0 \pmod{15}.$$

Dowód. W myśl małego twierdzenia Fermata mamy dla wszelkich x całkowitych $x^5\equiv x \pmod 5$, skąd $x^7\equiv x^3 \pmod 5$, a zatem

$$x^7-x^5-x^3+x\equiv 0 \pmod 5;$$

podobnie $x^3\equiv x \pmod 3$, skąd $x^7\equiv x^5 \pmod 3$, a zatem

$$x^7-x^5-x^3+x\equiv 0 \pmod 3.$$

Kongruencje $a\equiv 0 \pmod 5$ i $a\equiv 0 \pmod 3$ dają $a\equiv 0 \pmod{15}$.

19. Dowieść, że każda liczba pierwsza $p>5$ jest dzielnikiem liczby $n_p=111\ldots1$, napisanej w układzie dziesiętnym za pomocą $p-1$ jedynek.

Dowód. Niech p będzie liczbą pierwszą większą od 5. Jak łatwo widzieć, jest $(10,p)=1$ i $9n_p=10^{p-1}-1$. Lecz w myśl małego twierdzenia Fermata

jest $10^{p-1}\equiv 1 \pmod p$, a więc $p|9n_p$, a ponieważ $(p,9)=1$, bo p jest liczbą pierwszą większą od 5, więc $p|n_p$, c. b. d. o.

20. Dowieść, że dla każdej liczby naturalnej n liczba n^5-n jest podzielna przez 30.

Dowód. Z małego twierdzenia Fermata wynika, że przy każdym naturalnym n jest $n^5\equiv n \pmod 2$, $\pmod 3$ i $\pmod 7$. Liczba n^5-n jest więc podzielna przez 2, 3 i 5, a zatem również przez 30.

21. Dowieść, że dla naturalnych $n\geqslant 2$ ostatnią cyfrą liczby $2^{2^n}+1$ jest 7.

22. Dowieść, że dla żadnego układu liczb całkowitych x i y nie może być $x^2+1=3y^2$.

Dowód wynika natychmiast z uwagi, że -1 nie jest resztą kwadratową dla modułu 3.

23 Dowieść, że największym wspólnym dzielnikiem wszystkich liczb $n^3(n^6-1)$, gdzie $n=1,2,3,\ldots$, jest liczba 504.

24. Iloma sposobami można liczbę naturalną $n>1$, mającą rozkład na czynniki pierwsze $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, rozbić na iloczyn dwu czynników względnie pierwszych, jeżeli nie uważać za różne rozkłady, różniące się tylko porządkiem czynników?

Odpowiedź: 2^{k-1} sposobami.

25. Ile rozwiązań w liczbach naturalnych x,y ma równanie $xy=10^n$ przy danym naturalnym n?

Odpowiedź: $(n+1)^2$.

26. Udowodnić, że dla każdej liczby naturalnej nieparzystej n i liczb całkowitych względnie pierwszych a i b jest $(a+b)^2|a^n+b^n$ wtedy i tylko wtedy, gdy $(a+b)|n$. (T. Boncler).

Dowieść, że twierdzenie to nie zachodzi dla n parzystych.

Dowód. Ze wzoru na dwumian Newtona mamy

$$(m+k)^n\equiv nmk^{n-1}+k^n \pmod{m^2};$$

podstawiając $m=a+b$ i $k=-b$, otrzymujemy dla n nieparzystego

$$a^n\equiv n(a+b)\,b^{n-1}-b^n \pmod{(a+b)^2},$$

a zatem

$$a^n+b^n\equiv n(a+b)\,b^{n-1} \pmod{(a+b)^2}.$$

Na to więc, żeby było $a^n+b^n\equiv 0 \pmod{(a+b)^2}$, potrzeba i wystarcza, by

$$nb^{n-1}\equiv 0 \pmod{(a+b)};$$

z uwagi, że wobec $(a,b)=1$ jest $(b,a+b)=1$, daje to $n\equiv 0 \pmod{(a+b)}$, c. b. d. o.

Twierdzenie nie jest prawdziwe dla n parzystych, gdyż np. $3|6$, lecz

$$2^6+1^6\not\equiv 0 \pmod 9.$$

Jednakże również dla n parzystych warunek twierdzenia jest konieczny.

27. Dowieść, że liczba $\frac{2^{152}+1}{5}$ jest złożona.

Dowód. Jest

$$(*) \qquad 2^{122}+1=(2^{61}-2^{31}+1)(2^{61}+2^{31}+1).$$

Lecz $2^2\equiv -1 \pmod 5$, skąd:

$2^{60}\equiv 1 \pmod 5$, $2^{61}\equiv 2 \pmod 5$, $2^{30}\equiv -1 \pmod 5$, $2^{31}\equiv -2 \pmod 5$,

zatem $2^{61}-2^{31}+1\equiv 0 \pmod 5$. Z równości (*) wynika więc, że $2^{61}+2^{31}+1$ jest dzielnikiem liczby $\frac{2^{122}+2}{5}$; liczba ta jest więc złożona, c. b. d. o.

Uwaga. Jak dowiódł Kraïtchik, liczba $2^{61}+2^{31}+1$ też jest złożona (mianowicie podzielna przez 3456749). Podał on też rozkład liczby $2^{122}+1$ na czynniki pierwsze [1]).

28. Dowieść, że jeżeli p jest liczbą pierwszą nieparzystą, to

$$(*_*) \qquad \left[\left(\frac{p-1}{2}\right)!\right]^2+(-1)^{\frac{p-1}{2}}\equiv 0 \pmod p \qquad \text{(Waring).}$$

Dowód. Dla nieparzystych p jest oczywiście $(p-1)!=\prod_{k=1}^{\frac{p-1}{2}} k(p-k)$, skąd $(p-1)!\equiv(-1)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p$.

Dla otrzymania kongruencji $(*_*)$ wystarczy więc zastosować twierdzenie Wilsona.

29. Dowieść, że jeżeli p jest liczbą pierwszą i $q=2^p-1$, to $2^{q-1}\equiv 1 \pmod q$, oraz pokazać na przykładach, że dla liczb p złożonych kongruencja ta może zachodzić lub nie.

30. Dowieść, że $2^{70}+3^{70}\equiv 0 \pmod{13}$. (Kraïtchik).

31. Dowieść, że $3^{7380}\equiv 1 \pmod{7381}$.

Wskazówka: $7381=11^2\cdot 61$.

32. Dać przykłady liczb a naturalnych i p pierwszych, dla których $a^{p-1}\equiv 1 \pmod{p^2}$.

Odpowiedź: $10^2\equiv 1 \pmod{3^2}$, $3^{10}\equiv 1 \pmod{11^2}$.

§ 3. Reszty kwadratowe dla modułu pierwszego. Ich wyznaczanie i liczba. Zapytamy obecnie, ile dla modułu pierwszego nieparzystego p mamy reszt oraz niereszt kwadratowych. Najprostszą drogą dla otrzymania wszystkich reszt kwadratowych dla modułu p jest oczywiście wypisanie reszt kolejnych kwadratów:

$$1^2,\ 2^2,\ 3^2,\ \ldots,\ (p-1)^2$$

[1]) M. Kraïtchik, *Théorie des nombres*, tom I, Paryż 1922, str. 151-160.

według modułu p. Liczbę 0 pomijamy, gdyż w kongruencji $x^2\equiv D \pmod p$ zakładamy zawsze, że D jest niepodzielne przez p.

Tak więc np. dla modułu $p=7$ wypisujemy kwadraty:

$$1,\ 4,\ 9,\ 16,\ 25,\ 36$$

i wyznaczamy ich reszty według modułu 7:

$$1,\ 4,\ 2,\ 2,\ 4,\ 1.$$

Moduł $p=7$ ma zatem trzy reszty kwadratowe, mianowicie 1, 2 i 4.

Pozostałe liczby naturalne mniejsze od 7, czyli liczby 3, 5 i 6, są nieresztami kwadratowymi dla modułu 7. Moduł ten ma zatem także trzy niereszty kwadratowe.

Równie łatwo czytelnik obliczy, że np. liczba 11 ma 5 reszt kwadratowych, mianowicie

$$1,\ 3,\ 4,\ 5 \text{ i } 9,$$

oraz tyleż niereszt, którymi są liczby 2, 6, 7, 8 i 10.

Twierdzenie 7. *Każdy moduł pierwszy nieparzysty p ma $\frac{p-1}{2}$ reszt kwadratowych i tyleż niereszt. Wszystkie reszty kwadratowe otrzymamy, obliczając reszty według modułu p liczb*

$$(21) \qquad 1^2,\ 2^2,\ 3^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2.$$

Dowód. Oznaczmy przez

$$(22) \qquad r_1, r_2, r_3, \ldots, r_{\frac{p-1}{2}}$$

reszty $(\text{mod } p)$ liczb ciągu (21).

Udowodnimy przede wszystkim, że każda reszta kwadratowa liczby p jest zawarta w ciągu (22).

Jeżeli liczba D (jak zakładamy, niepodzielna przez p) jest resztą kwadratową liczby p, to istnieje liczba całkowita x również niepodzielna przez p i spełniająca kongruencję

$$x^2\equiv D \pmod p.$$

Niech ϱ będzie resztą według modułu p liczby x. Jest to liczba naturalna mniejsza od p i oczywiście

$$\varrho^2\equiv D \pmod p, \qquad (p-\varrho)^2\equiv D \pmod p.$$

Jedna z liczb ϱ i $p-\varrho$ na pewno jest naturalna i nie większa od $\frac{p}{2}$ lub — co na jedno wychodzi wobec nieparzystości liczby p — nie większa od $\frac{p-1}{2}$. Kwadrat jej, przystający według modułu p do liczby D, jest więc na pewno zawarty w ciągu (21), a zatem przystaje według modułu p do jednej z liczb ciągu (22). Będzie więc też do jednej z tych liczb przystawała liczba D.

Że — na odwrót — wszystkie wyrazy ciągu (22) są resztami kwadratowymi dla p, wynika ze sposobu ich otrzymania.

Pozostaje więc tylko do okazania, że są one r ó ż n y m i resztami kwadratowymi dla p, innymi słowy, że wszystkie wyrazy ciągu (22) są różne.

Przypuśćmy przeciwnie, że dwa wyrazy ciągu (22), r_i i r_j, o różnych wskaźnikach są równe. Oznaczając przez x'^2 wyraz ciągu (21) dający resztę r_i, a przez x''^2 wyraz tegoż ciągu dający resztę r_j, mielibyśmy

$$x'^2 \equiv x''^2 \pmod p,$$

co dowodziłoby podzielności przez p różnicy

$$x'^2 - x''^2 = (x'+x'')(x'-x'').$$

Jeden przynajmniej z czynników po prawej stronie musiałby więc być podzielny przez p. Lecz dla liczb x' i x'' mamy nierówności:

$$0 < x' \leqslant \frac{p-1}{2}, \qquad 0 < x'' \leqslant \frac{p-1}{2},$$

z których wynika, że

$$0 < x'+x'' \leqslant p-1 \quad \text{i} \quad -\frac{p-1}{2} < x'-x'' < \frac{p-1}{2}.$$

Pierwsza z tych nierówności dowodzi, że $x'+x''$ nie jest podzielne przez p, druga zaś — że $x'-x''$ jest podzielne przez p jedynie, gdy $x'=x''$. Lecz wtedy mielibyśmy $x'^2=x''^2$, a więc też $r_i=r_j$, wbrew założeniu.

Ciąg (22) zawiera zatem wszystkie różne reszty kwadratowe dla p, których tedy jest dokładnie $\frac{p-1}{2}$. Ponieważ zaś wszystkich liczb naturalnych mniejszych od p jest $p-1$, więc niereszt kwadratowych dla p mamy $p-1-\frac{p-1}{2}$ czyli również $\frac{p-1}{2}$, c. b. d. o.

§ 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 n a j m n i e j s z ą 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 α i β, spełniające warunki:

$$\alpha \equiv a \pmod p, \qquad \beta \equiv b \pmod p,$$
$$|\alpha| \leqslant \frac{p}{2}, \qquad |\beta| \leqslant \frac{p}{2}. \tag{25}$$

Stąd:

$$\alpha^2+\beta^2 \equiv a^2+b^2 \pmod p,$$
$$\alpha^2+\beta^2 \leqslant \frac{p^2}{4}+\frac{p^2}{4} = \frac{p^2}{2} < p^2. \tag{26}$$

Wobec niepodzielności liczb a i b przez p, kongruencje (25) dowodzą, że α i β 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 spełniającą nierówność (27), więc

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

Wyznaczmy liczby a_1 i b_1, spełniające warunki:

$$a_1\equiv a \pmod m, \qquad b_1\equiv b \pmod m, \tag{29}$$

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

Warunki te dają:

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

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

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

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

Obliczmy jej stronę prawą. Mnożąc pierwszą z kongruencji (29) przez a, a drugą przez b, otrzymujemy po dodaniu stronami $aa_1+bb_1\equiv a^2+b^2 \pmod m$, skąd $aa_1+bb_1\equiv 0 \pmod m$ 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 $ab_1-ba_1\equiv 0 \pmod m$, co dowodzi, że

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

gdzie d jest liczbą całkowitą.

Tożsamość (32) daje więc na mocy (36), (37) i (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 mniejsza 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.*

Dowód. Niech p będzie liczbą pierwszą formy $4k+1$. Jak dowiedliśmy w § 2, istnieje dla liczby 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 dzielnikiem 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:

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

Pozostaje do udowodnienia, że istnieje tylko jeden 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:

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

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

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

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

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

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.

Uwaga. 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:

$$\begin{array}{llll} 5=1^2+2^2, & 13=2^2+3^2, & 17=1^2+4^2, & 29=2^2+5^2,\\ 37=1^2+6^2, & 41=4^2+5^2, & 53=2^2+7^2, & 61=5^2+6^2,\\ 73=3^2+8^2, & 89=5^2+8^2, & 97=4^2+9^2. & \end{array}$$

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

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

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 sumę dwu kwadratów.*

Dowód. 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 ich 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* $4k+1$.

Dowód. Przypuśćmy, że wszystkich 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 nieparzysty.

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.*

Dowód. 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 δ 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 δ 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* $4k+3$.

Dowód. 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* $8k+1$.

Dowód: Przypuśćmy, że jest ich skończenie wiele. Niech to będą liczby $p_1, p_2, \ldots, p_n$ i niech

$$N = 2p_1 p_2 \ldots p_n.$$

Oznaczmy przez q jakikolwiek 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

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

czyli $N^{2(q-1)} \equiv -1 \pmod q$, wbrew małemu twierdzeniu Fermata (p. § 1, str. 59). Wreszcie, liczba q nie może być postaci $8k+5$, gdyż wtedy byłoby $N^{4(2k+1)} \equiv -1 \pmod q$ czyli $a^{q-1} \equiv -1 \pmod q$, 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 analogiczne twierdzenie dla formy $6k+1$.

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

Dowód. Wystarczy zauważyć, że liczbą $n=6k+5$, jako nieparzysta i niepodzielna przez 3, może 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, kiedy n samo jest liczbą pierwszą) znajdzie się więc co najmniej jeden czynnik formy $6k+5$, c. b. d. o.

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

Dowód. Przypuśćmy, że jest ich skończenie wiele. Niech to będą liczby $p_1, p_2, \ldots, p_n$ i niech

$$N = 6p_1 p_2 \ldots p_n - 1.$$

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

W postępie arytmetycznym

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

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

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

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 t. zw. *twierdzenia Lejeune-Dirichleta o postępie arytmetycznym*:

W każdym postępie arytmetycznym $ak+b$, tj. w każdym ciągu nieskończonym postaci

$$a, \quad a+b, \quad a+2b, \quad \ldots,$$

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 $i=1, 2, \ldots, n$, jest złożona.

Dowód. 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.

§ 7. 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.*

Dowód. 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

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

liczby a_1 i b_1 są względnie pierwsze. Wobec (35) liczba n musi być podzielna przez d^2; niech $n=d^2n_1$. 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

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

zatem wobec $p|n_1$

$$a_1^2+b_1^2 \equiv 0 \pmod p.$$

Mamy $(a_1,b_1)=1$; jedna więc przynajmniej z liczb a_1 i b_1 jest niepodzielna przez p, a więc wobec $p|n_1$ i (46) — również i druga. W myśl lematu 1 liczba p byłaby więc sumą dwu kwadratów wbrew lematowi 2.

Nie może więc n_1 być podzielne przez p; zatem p wchodzi do rozwinięcia liczby n w potędze o wykładniku parzystym. Tym samym udowodniliśmy że warunek jest konieczny.

Na odwrót, załóżmy teraz, że w rozwinięciu (45) liczby n na czynniki pierwsze wszystkie czynniki pierwsze formy $4k+3$ — o ile w nim figurują — wchodzą w potęgach o wykładnikach parzystych.

Oznaczmy przez $\beta_1,\beta_2,\ldots,\beta_n$ odpowiednie reszty liczb $\alpha_1,\alpha_2,\ldots,\alpha_n$ według modułu 2. Każda z liczb β jest więc albo zerem, albo jednością; oznaczając przez $k_1,k_2,\ldots,k_r$ liczby całkowite, będziemy mogli przyjąć

$$\alpha_1=2k_1+\beta_1, \qquad \alpha_2=2k_2+\beta_2, \qquad \ldots, \qquad \alpha_r=2k_r+\beta_r. \tag{47}$$

W myśl (45) i (47)

$$n=(p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r})^2 p_1^{\beta_1}p_2^{\beta_2}\ldots p_r^{\beta_r}. \tag{48}$$

Niech

$$p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}=m$$

(nie wyłączamy tu przypadku $m=1$). Opuszczając w iloczynie $p_1^{\beta_1}p_2^{\beta_2}\ldots p_r^{\beta_r}$ czynniki, dla których $\beta=0$ (jako równe jedności), otrzymamy wobec (48)

$$n=m^2p'p''\ldots p^{(s)}, \tag{49}$$

gdzie $p',p'',\ldots,p^{(s)}$ są oczywiście tymi czynnikami pierwszymi rozwinięcia (45), które wchodzą do niego w potęgach o wykładnikach nieparzystych (może być też $s=0$).

Wśród czynników $p',p'',\ldots,p^{(s)}$ może się więc znajdować tylko liczba 2 oraz liczby pierwsze formy $4k+1$.

Udowodnimy, że każdy z $s+1$ czynników prawej strony wzoru (49) rozkłada się na sumę kwadratów dwu liczb całkowitych. Istotnie, mamy

$$m^2=m^2+0^2,$$

a co do czynników $p',p'',\ldots,p^{(s)}$, to wystarczy zauważyć, że zarówno $2=1^2+1^2$ jak i liczby pierwsze formy $4k+1$ rozkładają się (w myśl twierdzenia Fermata) na sumę dwu kwadratów.

Liczba n daje się więc przedstawić jako iloczyn liczb, z których każda rozkłada się na sumę dwu kwadratów. Łatwo jednak widzieć, że iloczyn taki sam rozkłada się na sumę dwu kwadratów. Dla dwu czynników wynika to z tożsamości

$$(50) \qquad (a^2+b^2)(a_1^2+b_1)^2=(aa_1+bb_1)^2+(ab_1-ba_1)^2;$$

uogólnienie na większą liczbę czynników jest natychmiastowe. Dowiedliśmy więc, że warunek jest dostateczny.

PRZYKŁADY. Niech $n=19557$. Rozwijając na czynniki pierwsze, dostajemy

$$n=3^2\cdot 41\cdot 53.$$

Warunek twierdzenia 7 jest więc spełniony. Dla liczb 41 i 53 wypisujemy z łatwością rozkłady:

$$41=4^2+5^2, \qquad 53=2^2+7^2.$$

Stosując tożsamość (50) do $a=4$, $b=5$, $a_1=2$ i $b_1=7$, otrzymujemy z łatwością

$$41.53=(4.2+5.7)^2+(4.7-5.2)^2=43^2+18^2.$$

Jest zatem $3^2\cdot 41\cdot 53=(3\cdot 43)^2+(3\cdot 18)^2$ czyli

$$19557=129^2+54^2.$$

Inny rozkład otrzymalibyśmy, pisząc rozkłady dla 41 i 53 w postaci

$$41=5^2+4^2, \qquad 53=2^2+7^2$$

i stosując tożsamość (50), co daje $41\cdot 53=(5\cdot 2+4\cdot 7)^2+(5\cdot 7-4\cdot 2)^2=38^2+27^2$, zatem $3^2\cdot 41\cdot 53=(3\cdot 38)^2+(3\cdot 27)^2$ czyli

$$19557=114^2+81^2.$$

Niech teraz $n=105$. Rozwijając na czynniki pierwsze, dostajemy

$$105=3\cdot 5\cdot 7.$$

Warunek twierdzenia 7 nie jest więc spełniony, a zatem liczba 105 nie rozkłada się na sumę dwu kwadratów.

ĆWICZENIA. 1. Dowieść, że jeżeli liczba naturalna nie jest sumą kwadratów dwu liczb całkowitych, to nie jest też sumą kwadratów dwu liczb wymiernych.

Dowód. Jeżeli liczba naturalna n nie jest sumą kwadratów dwu liczb całkowitych, to w myśl twierdzenia 7 istnieje liczba pierwsza q postaci $4k+3$, która w rozwinięciu liczby n na czynniki pierwsze występuje z wykładnikiem nieparzystym. Gdyby było $n=\left(\frac{l}{m}\right)^2+\left(\frac{l_1}{m_1}\right)^2$, to mielibyśmy

$$(mm_1)^2n=(lm_1)^2+(l_1m)^2$$

wbrew twierdzeniu 7, gdyż q występuje w rozwinięciu liczby $(mm_1)^2n$ na czynniki pierwsze z wykładnikiem nieparzystym.

2. Dowieść, że liczba $\sqrt[1]{3}$ nie jest sumą kwadratów dwu liczb wymiernych.

3. Znając rozkład liczby n na sumę dwu kwadratów, znaleźć rozkład liczby $2n$ na sumę dwu kwadratów.

Rozwiązanie. Jeżeli $n=a^2+b^2$, to $2n=(a+b)^2+(a-b)^2$.

4. Dowieść, że na to, by ułamek nieprzywiedlny l/m o naturalnym liczniku i mianowniku był sumą kwadratów dwu liczb wymiernych, potrzeba i wystarcza, aby każda z liczb l i m była sumą kwadratów dwu liczb całkowitych.

§ 8. Wyznaczanie rozkładów na sumę dwu kwadratów i średnia ich ilość. Zapytajmy obecnie, w jaki sposób — przynajmniej teoretycznie — można by wyznaczyć wszystkie rozkłady danej liczby na sumę dwu kwadratów.

Jeżeli liczba n rozkłada się na sumę dwu kwadratów liczb całkowitych

$$(51) \qquad n=x^2+y^2,$$

to musi być $n\geqslant x^2$, jako też $n\geqslant y^2$; zatem $|x|\leqslant\sqrt{n}$ i $|y|\leqslant\sqrt{n}$.

Wystarczy więc podstawiać do wzoru (51) na x wartości całkowite, nie większe co do wartości bezwzględnej od $\sqrt{n}$. Jeżeli liczba $n-x^2$ nie będzie kwadratem, to dla danej wartości x nie otrzymamy rozkładu; w przeciwnym razie, biorąc $y=\pm\sqrt{n-x^2}$, otrzymamy układ liczb całkowitych x,y, spełniający równanie (51).

Zauważmy, że przy badaniu wyrażenia $n-x^2$ wystarczy uwzględniać tylko nieujemne wartości x, gdyż zmiana znaku przed x nie wpływa na wartość liczby $n-x^2$.

Przydać się może też uwaga, że liczby

$$n, \qquad n-1^2, \qquad n-2^2, \qquad n-3^2, \qquad \ldots$$

różnią się kolejno o

$$1, \qquad 3, \qquad 5, \qquad 7, \qquad \ldots,$$

t. j. o kolejne liczby nieparzyste.

PRZYKŁAD. Niech $n=10$. Tworzymy ciąg liczb 10, 9, 6, 1.

Z tych tylko druga i ostatnia są kwadratami. Możemy więc przyjąć $x=\pm 1$, $y=\pm 3$ albo $x=\pm 3$, $y=\pm 1$. W ten sposób dla liczby 10 otrzymujemy 8 rozkładów:

$$10=(+1)^2+(+3)^2=(+1)^2+(-3)^2=(-1)^2+(+3)^2=(-1)^2+(-3)^2=$$
$$=(+3)^2+(+1)^2=(-3)^2+(+1)^2=(+3)^2+(-1)^2=(-3)^2+(-1)^2.$$

Niech teraz $n=25$. Tworzymy ciąg liczb 25, 24, 21, 16, 9, 0.

Kwadratami są tu liczby 25, 16, 9 i 0. Mamy więc dla x i y wartości:

$$x=0, \quad y=\pm 5, \qquad x=\pm 3, \quad y=\pm 4,$$
$$x=\pm 4, \quad y=\pm 3, \qquad x=\pm 5, \quad y=0.$$

Stąd z łatwością znajdujemy 12 rozkładów liczby 25 na sumę dwu kwadratów.

Oznaczmy ogólnie symbolem $\tau(n)$ liczbę rozkładów liczby n na sumę kwadratów dwu liczb całkowitych. Obliczając jak wyżej, znajdujemy z łatwością:

$$\tau(1)=4, \quad \tau(2)=4, \quad \tau(3)=0, \quad \tau(4)=4, \quad \tau(5)=8,$$
$$\tau(6)=0, \quad \tau(7)=0, \quad \tau(8)=4, \quad \tau(9)=4, \quad \tau(10)=8,$$

przy czym, naturalnie, przypadek $\tau(n)=0$ przewidzieć można z góry, na podstawie twierdzenia 7.

Wartości funkcji liczbowej $\tau(n)$ — jak to widać już z powyższej tabliczki — zmieniają się nieprawidłowo: trudno dostrzec jakieś prawo, któremu podlegają. Np. dla (nieskończenie wielu) liczb pierwszych formy $4k+1$ będziemy mieli stale na podstawie twierdzenia Fermata $\tau(n)=8$, dla wszystkich zaś liczb formy $4k+3$ — stale $\tau(n)=0$.

Ciekawe jest jednak, że jeżeli zamiast oddzielnych wartości funkcji $\tau(n)$ rozpatrywać ich średnią arytmetyczną:

$$\frac{\tau(1)+\tau(2)+\tau(3)+\ldots+\tau(n)}{n}, \tag{52}$$

to przy wzrastaniu liczby n wyrażenie to zachowuje się już znacznie prawidłowiej, tak jak gdyby nieprawidłowości przebiegu funkcji $\tau(n)$ znosiły się wzajemnie. Okażemy mianowicie, że średnia arytmetyczna (52) zmierza przy nieograniczonym wzrastaniu liczby n do pewnej granicy. Sprawdzimy to najpierw praktycznie, a później podamy uzasadnienie teoretyczne tego zjawiska.

Dla pierwszych dziesięciu wartości funkcji $\tau(n)$ znajdujemy bezpośrednio z wyżej wypisanej tabliczki sumę 36; średnia arytmetyczna jest więc 3,6. Dla większych wartości n bezpośrednie obliczanie składników sumy

$$T(n)=\tau(1)+\tau(2)+\tau(3)+\ldots+\tau(n) \tag{53}$$

staje się coraz uciążliwsze. Wobec tego postaramy się znaleźć inną drogę dla wyznaczania tej sumy. Rozumowanie, jakie przy tym przeprowadzimy, da się z pewnymi zmianami zastosować w wielu innych podobnych przypadkach.

Liczba $\tau(k)$ jest liczbą rozwiązań w liczbach całkowitych x i y równania

$$x^2+y^2=k;$$

suma $\tau(0)+\tau(1)+\tau(2)+\ldots+\tau(n)$ jest zatem liczbą rozwiązań w liczbach całkowitych x i y nierówności

$$0\leqslant x^2+y^2\leqslant n. \tag{54}$$

Wszystkie układy liczb całkowitych x, y, spełniające nierówności (54), podzielimy na klasy, zaliczając do jednej i tej samej klasy te układy, dla których wartość x jest jednakowa. Policzmy, ile będzie układów w każdej klasie.

Jeżeli x ma oznaczoną wartość $x=k$, to y na mocy nierówności (54) może przyjmować tylko takie wartości, dla których

$$0-k^2\leqslant y^2\leqslant n-k^2.$$

Lewa część tej nierówności jest spełniona dla każdego y, prawa zaś daje $|y|\leqslant\sqrt{n-k^2}$ czyli

$$-\sqrt{n-k^2}\leqslant y\leqslant\sqrt{n-k^2} \tag{55}$$

i wskazuje na to, że musi być $n\geqslant k^2$ czyli

$$-\sqrt{n}\leqslant k\leqslant\sqrt{n}. \tag{56}$$

Ponieważ y musi być liczbą całkowitą, więc nierówności (55) można zastąpić przez nierówności

$$-\mathrm{E}(\sqrt{n-k^2})\leqslant y\leqslant\mathrm{E}(\sqrt{n-k^2}).$$

Zmienna y może zatem przy danym $x=k$ (nie większym co do wartości bezwzględnej od $\sqrt{n}$) przyjmować wartości:

$$0, \quad \pm 1, \quad \pm 2, \quad \ldots, \quad \pm\mathrm{E}(\sqrt{n-k^2}),$$

których jest dokładnie $2\mathrm{E}(\sqrt{n-k^2})+1$.

Oznaczmy ogólnie przez L_k liczbę wszystkich układów x, y, spełniających nierówności (54), w których x ma wartość k; będzie więc:

$$L_k=2\mathrm{E}(\sqrt{n-k^2})+1, \tag{57}$$

samo zaś k może — jak widzieliśmy — przyjmować wartości całkowite, spełniające nierówności (56), czyli wartości:

$$0, \quad \pm 1, \quad \pm 2, \quad \ldots, \quad \pm\mathrm{E}(\sqrt{n}).$$

Mamy więc oczywiście

$$\tau(0)+\tau(1)+\tau(2)+\ldots,+\tau(n)=$$
$$=L_0+L_1+L_2+\ldots+L_{\mathrm{E}(\sqrt{n})}+L_{-1}+L_{-2}+\ldots+L_{-\mathrm{E}(\sqrt{n})}.$$

Ze wzoru (57) wnosimy, że

$$L_{-k}=L_k;$$

możemy więc napisać

$$\tau(0)+\tau(1)+\tau(2)+\ldots+\tau(n)=L_0+2L_1+\ldots 2L_{(\mathrm{E}\sqrt{n})}.$$

Wstawmy tu zamiast L_k ich wartości ze wzoru (57) i połączmy razem wszystkie składniki $+1$ (których jest dokładnie $2\mathrm{E}(\sqrt{n})+1$). Otrzymamy w ten sposób

$$\tau(0)+\tau(1)+\tau(2)+\ldots+\tau(n)=2\mathrm{E}(\sqrt{n})+1+2\mathrm{E}(\sqrt{n})+$$
$$+4\mathrm{E}(\sqrt{n-1^2})+4\mathrm{E}(\sqrt{n-2^2})+\ldots+4\mathrm{E}(\sqrt{n-[\mathrm{E}(\sqrt{n})]^2}),$$

a stąd, zważywszy, że $\tau(0)=1$, gdyż 0 daje jedyny rozkład na sumę dwu kwadratów $0=0^2+0^2$, otrzymujemy według (53):

$$T(n)=4\mathrm{E}(\sqrt{n})+4\mathrm{E}(\sqrt{n-1^2})+4\mathrm{E}(\sqrt{n-2^2})+4\mathrm{E}(\sqrt{n-3^2})+\ldots,$$

gdzie składniki szeregu po prawej stronie należy wypisywać dopóty, dopóki pod pierwiastkiem otrzymujemy wartość dodatnią. Piszemy to w zwięzłej postaci:

$$T(n)=4\sum_{k=0}^{\mathrm{E}(\sqrt{n})}\mathrm{E}(\sqrt{n-k^2}). \tag{58}$$

Obliczmy na podstawie tego wzoru $T(100)$. Dostaniemy:

$$T(100)=4[\mathrm{E}(\sqrt{100})+\mathrm{E}(\sqrt{99})+\mathrm{E}(\sqrt{96})+\mathrm{E}(\sqrt{91})+\mathrm{E}(\sqrt{84})+$$
$$+\mathrm{E}(\sqrt{75})+\mathrm{E}(\sqrt{64})+\mathrm{E}(\sqrt{51})+\mathrm{E}(\sqrt{36})+\mathrm{E}(\sqrt{19})]=$$
$$=4(10+9+9+9+9+8+8+7+6+4)=4\cdot 79=316.$$

Stąd jako średnią liczbę rozkładów na sumę dwu kwadratów dla pierwszych 100 liczb otrzymujemy 3,16.

Obliczmy jeszcze $T(400)$. W myśl wzoru (58) dostajemy:

$$\tfrac{1}{4}T(400)=\mathrm{E}(\sqrt{400})+\mathrm{E}(\sqrt{399})+\mathrm{E}(\sqrt{396})+\mathrm{E}(\sqrt{391})+\mathrm{E}(\sqrt{384})+$$
$$+\mathrm{E}(\sqrt{375})+\mathrm{E}(\sqrt{364})+\mathrm{E}(\sqrt{351})+\mathrm{E}(\sqrt{336})+\mathrm{E}(\sqrt{319})+\mathrm{E}(\sqrt{300})+$$
$$+\mathrm{E}(\sqrt{279})+\mathrm{E}(\sqrt{256})+\mathrm{E}(\sqrt{231})+\mathrm{E}(\sqrt{204})+\mathrm{E}(\sqrt{175})+\mathrm{E}(\sqrt{144})+$$
$$+\mathrm{E}(\sqrt{111})+\mathrm{E}(\sqrt{76})+\mathrm{E}(\sqrt{39})=$$
$$=20+19+19+19+19+19+19+18+18+17+17+$$
$$+16+16+15+14+13+12+10+8+6=314.$$

Stąd $T(400)=4\cdot 314=1256$ czyli $T(400)/400=3{,}14$.

Uderza nas tu, że *przy wzrastaniu liczby n średnia wartość funkcji $\tau(n)$ zmierza do liczby π.*

Uzasadnimy to obecnie na drodze geometrycznej. Poprowadźmy na płaszczyźnie dwie proste względem siebie prostopadłe, np. proste Ox i Oy. Proste te nazywać będziemy *osiami* (fig. 1). Po obu stronach każdej z nich poprowadźmy szereg równoległych, kolejno odległych o jednostkę długości. Równoległe te ponumerujemy w następujący sposób: równoległe do osi Ox opatrzymy kolejnymi numerami 1, 2, 3, ... idąc ku górze, numerami zaś -1, -2, -3, ... idąc ku dołowi; podobnie równoległe do osi Oy opatrzymy po prawej stronie kolejno numerami 1, 2, 3, ..., po lewej zaś — numerami -1, -2, -3, ... Same osie opatrzymy numerem 0.

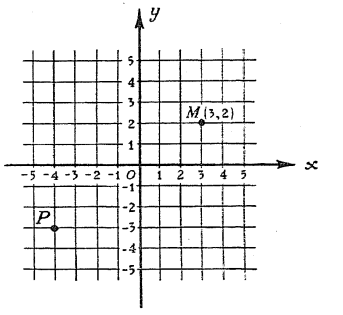

Fig. 1.

Odwzorowaniem (albo *obrazem*) *rozkładu* x^2+y^2 będziemy nazywali ten punkt M płaszczyzny, który leży na przecięciu się prostopadłej x do osi Ox z prostopadłą y do osi Oy.

Tak np. odwzorowaniem rozkładu 3^2+2^2 będzie punkt M, oznaczony na fig. 1; odwzorowaniem rozkładu $(-4)^2+(-3)^2$ jest punkt P, a odwzorowaniem rozkładu 0^2+0^2 — punkt O. Punkty leżące na przecięciu dwu którychkolwiek prostych (nie wyłączając osi), czyli punkty o współrzędnych całkowitych, nazywamy *punktami sieciowymi*. Jasne jest, że każdemu rozkładowi x^2+y^2 odpowiada pewien punkt sieciowy i na odwrót, każdy punkt sieciowy jest obrazem jakiegoś rozkładu x^2+y^2.

Weźmy pod uwagę punkt sieciowy M, który jest obrazem rozkładu x^2+y^2. Na podstawie twierdzenia Pytagorasa odległość OM równa jest $\sqrt{x^2+y^2}$ (fig. 2). Wnosimy stąd dalej, że rozkładom x, y, spełniającym nierówność $x^2+y^2\leqslant n$, odpowiadają punkty sieciowe, leżące wewnątrz lub na obwodzie koła zatoczonego promieniem $\sqrt{n}$ dokoła punktu O.

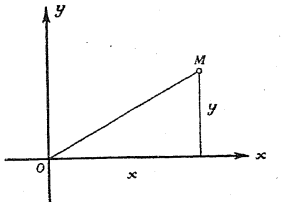

Fig. 2.

Tak np. dla $n=400$ wobec znalezionego $T(400)=1256$, wewnątrz i na kole zatoczonym promieniem $R=20$ dokoła punktu O, znajduje się dokładnie 1257 punktów sieciowych.

Przyporządkujmy każdemu punktowi sieciowemu kwadrat o jednostce pola, mający ów punkt za środek, a boki równoległe do osi (fig. 3). Pole P, zajęte przez kwadraty odpowiadające punktom sieciowym, nie wychodzącym poza obwód koła K, jest więc dokładnie równe liczbie takich punktów czyli sumie $1+T(n)$. Z łatwością jednak spostrzegamy, że pole P jest równe w przybliżeniu polu koła K, i możemy nawet bliżej określić stopień tego przybliżenia.

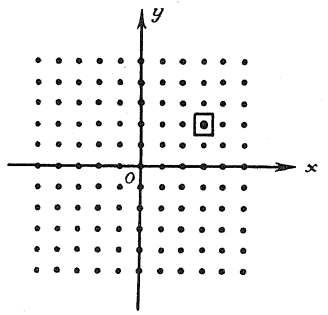

Fig. 3.

Jeżeli mianowicie zakreślimy z punktu O koło o promieniu $\sqrt{n}+\frac{1}{\sqrt{2}}$, to zważywszy, że $\frac{1}{\sqrt{2}}$ jest największą odległością punktów kwadratu o jednostce pola od jego środka, wnosimy, że wszystkie kwadraty tworzące pole P będą leżały wewnątrz takiego koła, co najwyżej dotykając jego obwodu. Pole zajęte przez nie będzie więc mniejsze od pola koła:

$$P<\pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2. \tag{59}$$

Z drugiej strony, gdybyśmy z punktu O zakreślili koło promieniem $\sqrt{n}-\frac{1}{\sqrt{2}}$, to wywnioskowalibyśmy podobnie, że pole tego koła jest mniejsze od pola zajętego przez kwadraty:

$$P>\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2. \tag{60}$$

Nierówności (59) i (60) dają wobec równości $P=1+T(n)$:

$$\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2-1<T(n)<\pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2-1. \tag{61}$$

Zważywszy, że $\pi\sqrt{2}<5$ i że przy naturalnym n mamy

$$0<\frac{\pi}{2}-1<1\leqslant\sqrt{n},$$

możemy napisać nierówności:

$$\pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2-1=\pi n+\pi\sqrt{2}\cdot\sqrt{n}+\frac{\pi}{2}-1<\pi n+6\sqrt{n},$$

$$\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2-1=\pi n-\pi\sqrt{2}\cdot\sqrt{n}+\frac{\pi}{2}-1>\pi n-6\sqrt{n},$$

na mocy których (61) daje $\pi n-6\sqrt{n}<T(n)<\pi n+6\sqrt{n}$, czyli $|T(n)-\pi n|<6\sqrt{n}$ przy wszelkim naturalnym n, skąd natychmiast:

$$\left|\frac{T(n)}{n}-\pi\right|<\frac{6}{\sqrt{n}}. \tag{62}$$

Niech ε będzie dowolną liczbą dodatnią. Dla dostatecznie wielkich n, mianowicie dla wszystkich $n\geqslant\frac{36}{\varepsilon^2}$ będzie $\frac{6}{\sqrt{n}}\leqslant\varepsilon$; zatem lewa strona wzoru (62) jest mniejsza od ε. Możemy więc powiedzieć, że dla dostatecznie wielkich n średnia arytmetyczna

$$\frac{T(n)}{n}=\frac{\tau(1)+\tau(2)+\tau(3)+\ \ldots\ +\tau(n)}{n}$$

różni się od liczby π dowolnie mało. Wyrażamy to, mówiąc, że ta średnia arytmetyczna *zmierza do granicy* π, gdy n wzrasta nieograniczenie, i piszemy:

$$\lim_{n=\infty}\frac{\tau(1)+\tau(2)+\ \ldots\ +\tau(n)}{n}=\pi.$$

Jeżeli dla danej funkcji liczbowej średnia arytmetyczna z jej n kolejnych wartości zmierza do granicy (skończonej) a, gdy n wzrasta nieograniczenie, to mówimy, że a jest *wartością średnią* tej funkcji liczbowej. Możemy więc powiedzieć, że wartością średnią funkcji $\tau(n)$ jest liczba π albo że *liczby naturalne dają średnio* π *rozkładów na sumę dwu kwadratów.*

Do rozkładów na sumę dwu kwadratów powrócimy jeszcze w Rozdziale XVI [1]). Obecnie przejdziemy do rozkładów na sumę trzech i więcej kwadratów.

[1]) W związku z rozkładem liczb naturalnych na sumę dwu kwadratów zauważymy, że badano też rozkłady wielomianów całkowitych o spółczynnikach całkowitych na sumę kwadratów dwu takich wielomianów; ob. np. Th. Skolem, Norsk Matematisk Tidsskrift, tom 21 (1939), str. 154-159.

§ 9. Rozkłady liczb naturalnych na sumę trzech kwadratów.

Twierdzenie 14. *Na to, aby liczba naturalna n rozkładała się na sumę kwadratów trzech liczb całkowitych, potrzeba, aby nie była ona postaci $4^l(8k+7)$ dla żadnych k i l całkowitych nieujemnych.*

Dowód. Okażemy najpierw, że żadna liczba całkowita postaci $8k+7$ nie rozkłada się na sumę trzech kwadratów.

Przypuśćmy przeciwnie, że przy pewnym całkowitym k oraz pewnych całkowitych x, y, z jest

$$8k+7=x^2+y^2+z^2.$$

Po lewej stronie mamy liczbę nieparzystą; wnosimy stąd natychmiast, że albo wszystkie trzy liczby x, y, z są nieparzyste, albo dwie z nich są parzyste, a jedna nieparzysta.

Niech m będzie liczbą nieparzystą, a więc $m=2t+1$, gdzie t jest liczbą całkowitą. Zatem

$$m^2=4t(t+1)+1.$$

Jeżeli t jest parzyste, to $4t$ jest podzielne przez 8; jeżeli zaś t jest nieparzyste, to $t+1$ jest parzyste i $4(t+1)$ jest podzielne przez 8. W każdym więc razie iloczyn $4t(t+1)$ jest podzielny przez 8. Oznaczając go przez $8u$, gdzie u jest całkowite, otrzymujemy

$$m^2=8u+1.$$

Dowiedliśmy zatem, że kwadrat liczby nieparzystej zawsze przystaje do 1 według modułu 8. Co się zaś tyczy kwadratu liczby parzystej, to, jako podzielny przez 4, przystaje on zawsze do 0 lub 4 według modułu 8. Biorąc to pod uwagę, wnosimy z łatwością, że suma kwadratów trzech liczb nieparzystych zawsze przystaje do $3 \pmod 8$, suma zaś kwadratów trzech liczb, z których dwie są parzyste, a jedna nieparzysta, przystaje albo do $1 \pmod 8$, albo do $5 \pmod 8$; pierwszy przypadek zachodzi, gdy obie liczby parzyste są podzielne lub obie niepodzielne przez 4, drugi zaś — gdy jedna z liczb parzystych jest podzielna, a druga niepodzielna przez 4.

W żadnym atoli z tych przypadków nie otrzymujemy liczby przystającej do $7 \pmod 8$, czyli liczby postaci $8k+7$. Dowiedliśmy więc, że żadna liczba tej postaci nie rozkłada się na sumę trzech kwadratów.

Przypuśćmy teraz, że dla liczby całkowitej k istnieje przynajmniej jedna taka liczba naturalna l, że liczba $4^l(8k+7)$ rozkłada się na sumę trzech kwadratów. Niech l_0 będzie najmniejszą z takich właśnie liczb naturalnych l. Jest więc:

$$4^{l_0}(8k+7)=x^2+y^2+z^2. \tag{63}$$

Lewa strona tej równości musi być podzielna przez 4, skoro $l_0 \geqslant 1$. Stąd łatwy wniosek, że liczby x, y, z albo są wszystkie trzy parzyste, albo jedna z nich parzysta, a dwie nieparzyste. Lecz w ostatnim przypadku suma $x^2+y^2+z^2$ byłaby — jak łatwo widzieć — postaci $8t+2$ albo postaci $8t+6$ (zależnie od tego, czy owa liczba parzysta jest podzielna, czy niepodzielna przez 4), a więc w każdym razie liczbą niepodzielną przez 4, co niemożliwe. Muszą więc wszystkie trzy liczby x, y, z być parzyste, a zatem:

$$x=2\xi, \qquad y=2\eta, \qquad z=2\zeta,$$

gdzie ξ, η, ζ są całkowite. Wstawiając te wartości do wzoru (63), otrzymalibyśmy skracając przez 4:

$$4^{l_0-1}(8k+7)=\xi^2+\eta^2+\zeta^2.$$

Rozkład ten nie może zachodzić dla $l_0=1$, gdyż dowiedliśmy wyżej, że żadna liczba postaci $8k+7$ nie rozkłada się na sumę trzech kwadratów. Jeżeli jednak $l_0>1$, to l_0-1 jest liczbą naturalną, co przeczy założeniu, że l_0 jest najmniejszą liczbą naturalną l, dla której $4^l(8k+7)$ rozkłada się na sumę trzech kwadratów.

Twierdzenie 14 jest więc dowiedzione.

Godne uwagi jest, że twierdzenie 14 daje się odwrócić: można mianowicie dowieść, że *każda liczba naturalna, nie mająca postaci $4^l(8k+7)$ dla żadnych całkowitych k i l, rozkłada się na sumę kwadratów trzech liczb całkowitych.*

Dowód tego twierdzenia jest długi. Podał go Gauss, a następnie uprościli Lejeune-Dirichlet i Landau [1]). Przytoczenie tego dowodu przekraczałoby jednak ramy niniejszego dzieła.

---

[1]) Ob. E. Landau, *Vorlesungen über Zahlentheorie I*, Lipsk 1927, str. 114-125.

W szczególności, z twierdzenia tego wynika, że dla każdego naturalnego n istnieją takie liczby całkowite x, y, z, iż

$$8n+3=x^2+y^2+z^2;$$

jak łatwo widzieć, liczby te muszą być wszystkie nieparzyste, zatem:

$$x=2a+1, \qquad y=2b+1, \qquad z=2c+1,$$

skąd $8n+3=(2a+1)^2+(2b+1)^2+(2c+1)^2$, co daje od razu

$$n=\frac{a(a+1)}{2}+\frac{b(b+1)}{2}+\frac{c(c+1)}{2}.$$

Liczby postaci $\frac{t(t+1)}{2}$, gdzie t jest liczbą naturalną, noszą nazwę *trójkątnych.*

Z twierdzenia udowodnionego przez Gaussa wynika więc twierdzenie (wypowiedziane przez Fermata), że *każda liczba naturalna jest sumą co najwyżej trzech liczb trójkątnych.*

Łatwo jest dowieść, że każda liczba całkowita daje się przedstawić w postaci $x^2+y^2-z^2$, gdzie x, y i z są liczbami naturalnymi. Dowód wynika natychmiast z tożsamości:

$$2k-1=2^2+(k-2)^2-(k-3)^2=4^2+(k-8)^2-(k-9)^2,$$
$$2k=1^2+k^2-(k-1)^2=3^2+(k-4)^2-(k-5)^2.$$

ĆWICZENIE. Dowieść twierdzenia Lagrange'a, że dla każdej liczby całkowitej m istnieje nieskończenie wiele różnych rozwiązań równania $m=x^2+y^2-z^2$ w liczbach całkowitych.

Dowód. Dla $x\not\equiv m \pmod 2$ liczba $m-x^2$ jest nieparzysta i wystarczy przyjąć $y=\frac{m-x^2+1}{2}$, $z=\frac{m-x^2-1}{2}$. W ten sposób dla t całkowitych otrzymujemy tożsamości:

$$2k-1=(2t)^2+(k-2t^2)^2-(k-2t^2-1)^2,$$
$$2k=(2t+1)^2+(k-2t^2-2t)^2-(k-2t^2-2t-1)^2.$$

Oznaczmy teraz przez $\tau(n)$ liczbę rozkładów liczby n na sumę kwadratów *trzech* liczb całkowitych. Pierwszymi wartościami funkcji $\tau(n)$ są:

$$\tau(1)=6, \quad \tau(2)=12, \quad \tau(3)=8, \quad \tau(4)=6, \quad \tau(5)=24,$$
$$\tau(6)=34, \quad \tau(7)=0, \quad \tau(8)=12, \quad \tau(9)=30, \quad \tau(10)=24.$$

Twierdzenie 14 poucza nas, że dla nieskończenie wielu liczb naturalnych jest $\tau(n)=0$.

Co się zaś tyczy liczby $T(n)=\tau(1)+\tau(2)+\ldots+\tau(n)$, to podobnie jak dla rozkładów na sumę dwu kwadratów (ob. § 7) moglibyśmy z łatwością wyprowadzić na drodze geometrycznej pewną nierówność, rozważając kulę i sześciany zamiast koła i kwadratów, mianowicie nierówność:

$$^4/_3\pi\left(\sqrt{n}-\frac{\sqrt{3}}{2}\right)^2-1<T(n)<{}^4/_3\pi\left(\sqrt{n}+\frac{\sqrt{3}}{2}\right)^3-1,$$

z której z łatwością wynika, że przy wszelkim naturalnym n jest

$$|T(n)-{}^4/_3\pi n\sqrt{n}|<10n.$$

Można stąd wywnioskować, że

$$\lim_{n=\infty}\frac{T(n)}{{}^4/_3\pi n\sqrt{n}}=1.$$

ĆWICZENIA. 1. Dowieść, że liczba 7 nie jest sumą kwadratów trzech liczb wymiernych.

Dowód. Gdyby liczba 7 była sumą kwadratów trzech liczb wymiernych, to sprowadzając je do wspólnego mianownika $2^{l-1}(2s-1)$, mielibyśmy przy całkowitych l, s, x, y i z równość $4^l-17(2s-1)^2=x^2+y^2+z^2$, co jest niemożliwe, gdyż $(2s-1)^2\equiv 1 \pmod 8$, a liczba $7(2s-1)^2$ jest postaci $8k+7$.

Uwaga. Można dowieść, że każda liczba naturalna, która nie jest sumą kwadratów trzech liczb całkowitych, nie jest też sumą kwadratów trzech liczb wymiernych.

2. Dowieść, że 1/7 nie jest sumą kwadratów trzech liczb wymiernych.

Dowód sprowadza się do ćwiczenia 1 wobec równości $1/7=7/49$.

3. Dowieść przez podanie przykładu, że iloczyn dwu liczb, z których każda jest sumą kwadratów trzech liczb naturalnych, może nie być sumą kwadratów trzech liczb całkowitych.

Dowód: $63=3\cdot 21=(1^2+1^2+1^2)(1^2+2^2+4^2)$; przy tym 63, jako liczba postaci $8k+7$, nie jest sumą trzech kwadratów.

§ 10. Rozkłady liczb naturalnych na sumę czterech kwadratów. Twierdzenie Lagrange'a. Zajmiemy się teraz rozkładami na sumę czterech kwadratów. Udowodnimy następujące twierdzenie, znane pod nazwą *twierdzenia Lagrange'a* [1]).

Twierdzenie 15. *Każda liczba całkowita nieujemna rozkłada się na sumę kwadratów czterech liczb całkowitych.*

[1]) Twierdzenie to wypowiedział bez dowodu Bachet w 1621 roku; dowody podali Fermat i (w 1770 r.) Lagrange.

Udowodnimy wpierw

Lemat I. *Liczba pierwsza nieparzysta p, będąca dzielnikiem sumy kwadratów czterech liczb całkowitych, z których jedna przynajmniej nie jest podzielna przez p, jest sama sumą czterech kwadratów,*

Dowód. Załóżmy, że p spełnia założenia lematu. Istnieją więc liczby naturalne, podzielne przez p, rozkładające się na sumę kwadratów czterech liczb całkowitych, z których jedna przynajmniej nie jest podzielna przez p. Niech n będzie najmniejszą z takich właśnie liczb naturalnych. Jest więc

$$n = mp, \tag{64}$$

gdzie m jest liczbą naturalną, oraz

$$n = a^2+b^2+c^2+d^2, \tag{65}$$

gdzie a, b, c, d są liczbami całkowitymi, z których jedna przynajmniej, np. liczba a, nie jest podzielna przez p.

Oznaczmy przez $\alpha, \beta, \gamma, \delta$ odpowiednio najmniejsze co do wartości bezwzględnej reszty liczb a, b, c, d według modułu p. Zatem:

$$a \equiv \alpha \pmod p, \qquad \beta \equiv b \pmod p, \qquad \gamma \equiv c \pmod p, \qquad \delta \equiv d \pmod p,$$

$$|\alpha| < \frac{p}{2}, \qquad |\beta| < \frac{p}{2}, \qquad |\gamma| < \frac{p}{2}, \qquad |\delta| < \frac{p}{2}. \tag{66}$$

Z kongruencji tych wynika, że α jest niepodzielne przez p oraz

$$\alpha^2+\beta^2+\gamma^2+\delta^2 \equiv a^2+b^2+c^2+d^2 \equiv 0 \pmod p.$$

Wobec definicji liczby n, wnosimy stąd natychmiast, że

$$n \leqslant \alpha^2+\beta^2+\gamma^2+\delta^2.$$

Biorąc pod uwagę, że prawa strona tej nierówności jest wobec (66) mniejsza od $4\frac{p^2}{4}$, otrzymujemy

$$n < p^2,$$

a zatem wobec (64) jest $mp < p^2$, skąd

$$m < p. \tag{67}$$

Pozostaje dowieść, że $m = 1$, ponieważ wtedy wobec (64) i (65) mielibyśmy już rozkład liczby p na sumę czterech kwadratów i lemat byłby udowodniony.

Przypuśćmy więc, że $m \neq 1$. Ponieważ m jest liczbą naturalną, więc wobec (67) jest

$$1 < m < p. \tag{68}$$

Oznaczmy przez a_1, b_1, c_1, d_1 liczby, spełniające warunki:

$$a_1 \equiv a \pmod m, \qquad b_1 \equiv b \pmod m, \qquad c_1 \equiv c \pmod m, \qquad d_1 \equiv d \pmod m,$$

$$|a_1| \leqslant \frac{m}{2}, \qquad |b_1| \leqslant \frac{m}{2}, \qquad |c_1| \leqslant \frac{m}{2}, \qquad |d_1| \leqslant \frac{m}{2}. \tag{69}$$

Z kongruencji tych wynika, że

$$a_1^2+b_1^2+c_1^2+d_1^2 \equiv a^2+b^2+c^2+d^2 \pmod m,$$

a że prawa strona jest w myśl (64) i (65) podzielna przez m, więc możemy przyjąć, że

$$a_1^2+b_1^2+c_1^2+d_1^2 = lm, \tag{70}$$

gdzie l jest liczbą całkowitą, oczywiście nieujemną. Gdyby było $l=0$, to mielibyśmy $a_1 = b_1 = c_1 = d_1 = 0$ i w myśl kongruencji dla liczb a_1, b_1, c_1, d_1 wszystkie cztery liczby a, b, c, d byłyby podzielne przez m. Wynikałoby stąd, że suma kwadratów tych liczb, czyli liczba n, jest podzielna przez m^2, a zatem wobec (64), że liczba p jest podzielna przez m, co niemożliwe, gdyż p jest liczbą pierwszą, m zaś spełnia nierówności (68). Liczba l musi więc być naturalna.

Przypuśćmy, że

$$|a_1| = |b_1| = |c_1| = |d_1| = \frac{m}{2}; \tag{71}$$

jest to możliwe oczywiście tylko dla m parzystego; niech więc będzie

$$m = 2q \tag{72}$$

czyli $m/2 = q$. Kongruencja $a_1 \equiv a \pmod m$ daje $a = a_1 + mt$, gdzie t jest liczbą całkowitą; zatem w myśl (71) i (72) jest

$$a = \pm q + 2tq = (2t \pm 1)q$$

czyli

$$a = k_1 q,$$

gdzie k_1 jest liczbą nieparzystą. Podobnie znaleźlibyśmy

$$b = k_2 q, \qquad c = k_3 q, \qquad d = k_4 q,$$

gdzie k_2, k_3 i k_4 są liczbami nieparzystymi. Stąd w myśl (64), 65) i (72) jest $n=2qp=q^2(k_1^2+k_2^2+k_3^2+k_4^2)$, a zatem

$$2p=q(k_1^2+k_2^2+k_3^2+k_4^2).$$

Kwadrat liczby nieparzystej daje — jak wiemy — przy dzieleniu przez 4 resztę 1; zatem prawa strona otrzymanej równości jest podzielna przez 4, gdy tymczasem lewa strona nie jest podzielna przez 4, gdyż p jest liczbą pierwszą nieparzystą.

Równości (71) zachodzić więc nie mogą. Znaczy to, że w jednej przynajmniej z nierówności (69) jest wyłączony znak równości. Pociąga to za sobą — jak łatwo widzieć — nierówność

$$a_1^2+b_1^2+c_1^2+d_1^2<4\frac{m^2}{4},$$

czyli wobec (70) nierówność $lm<m^2$, skąd

$$l<m. \tag{73}$$

Weźmy teraz pod uwagę *tożsamość Eulera*:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1^2)=\\ =(aa_1+bb_1+cc_1+dd_1)^2+(ab_1-ba_1+cd_1-dc_1)^2+\\ +(ac_1-ca_1+db_1-bd_1)^2+(ad_1-da_1+bc_1-cb_1)^2.\end{aligned} \tag{74}$$

Lewa strona tej tożsamości równa jest w myśl (65), (64) i (70) liczbie m^2lp.

Z kongruencji dla a_1, b_1, c_1, d_1 wynika, że możemy przyjąć:

$$\begin{aligned}a_1&=a+ma_2, & c_1&=c+mc_2,\\ b_1&=b+mb_2, & d_1&=d+md_2,\end{aligned} \tag{75}$$

gdzie a_2, b_2, c_2, i d_2 są liczbami całkowitymi.

Wzory (75) dają w jednej chwili

$$\begin{aligned}aa_1+bb_1+cc_1+dd_1=\\ =a^2+b^2+c^2+d^2+m(aa_2+bb_2+cc_2+dd_2)=\\ =m(p+aa_2+bb_2+cc_2+dd_2)=mt_1,\\ ab_1-ba_1+cd_1-dc_1=m(ab_2-ba_2+cd_2-dc_2)=mt_2,\\ ac_1-ca_1+bd_1-db_1=m(ac_2-ca_2+bd_2-db_2)=mt_3,\\ ad_1-da_1+bc_1-cb_1=m(ad_2-da_2+bc_2-ca_2)=mt_4,\end{aligned}$$

gdzie liczby t_1, t_2, t_3 i t_4 są całkowite.

Wstawiając te wartości do prawej strony wzoru (74), otrzymujemy $m^2lp=m^2(t_1^2+t_2^2+t_3^2+t_4^2)$, skąd

$$lp=t_1^2+t_2^2+t_3^2+t_4^2. \tag{76}$$

Ponieważ lewa strona tej równości jest liczbą naturalną, więc przynajmniej jedna z liczb t nie jest zerem. Gdyby wszystkie cztery liczby t były podzielne przez p, to jedna przynajmniej z nich — ta mianowicie, która nie jest zerem — byłaby co do bezwzględnej wartości niemniejsza od p, zatem jej kwadrat — od p^2. Byłoby więc $lp\geqslant p^2$, skąd $l\geqslant p$, wbrew (73) i (67). Przynajmniej jedna z liczb t nie jest zatem podzielna przez p.

Wzór (76) przedstawia więc rozkład liczby naturalnej podzielnej przez p na sumę kwadratów czterech liczb całkowitych, z których jedna przynajmniej nie jest podzielna przez p. W myśl definicji liczby n musi więc być $n\leqslant lp$, czyli wobec (64) $mp\leqslant lp$, skąd $m\leqslant l$, wbrew (73). Nie może więc być $m\neq 1$.

Jest zatem $m=1$, skąd wobec (74) i (75) dostajemy równość $p=a^2+b^2+c^2+d^2$, c. b. d. d.

Uwaga. Zastępując w tożsamości Eulera (74) odpowiednio b,c,d, b_1,c_1,d_1 przez $b\sqrt{x}$, $c\sqrt{y}$, $d\sqrt{xy}$, $b_1\sqrt{x}$, $c_1\sqrt{y}$, $d_1\sqrt{xy}$, otrzymujemy ogólniejszą *tożsamość Lagrange'a*:

$$\begin{aligned}(a^2+b^2x+c^2y+d^2xy)(a_1^2+b_1^2x+c_1^2y+d_1^2xy)=\\ =(aa_1+bb_1x+cc_1y+dd_1xy)^2+(ab_1-ba_1+cd_1y-dc_1y)^2x+\\ +(ac_1-ca_1+db_1x-bd_1x)^2y+(ad_1-da_1+bc_1-cb_1)^2xy.\end{aligned}$$

M. Brioschi[1]) podał tożsamość, wyrażającą iloczyn dwu sum 8 kwadratów przez sumę 8 kwadratów, mianowicie

$$\begin{aligned}(a^2+b^2+c^2+d^2+e^2+f^2+g^2+h^2)\cdot\\ \cdot(a_1^2+b_1^2+c_1^2+d_1^2+e_1^2+f_1^2+g_1^2+h_1^2)=\\ =(aa_1+bb_1+cc_1+dd_1+ee_1+ff_1+gg_1+hh_1)^2+\\ +(ab_1-ba_1-cd_1+dc_1-ef_1+fe_1-gh_1+hg_1)^2+\\ +(ac_1+bd_1-ca_1-db_1+eg_1-fh_1-ge_1+hf_1)^2+\\ +(ad_1-bc_1+cb_1-da_1-eh_1-fg_1+gf_1+he_1)^2+\\ +(ae_1+bf_1-cg_1+dh_1-ca_1-fb_1+gc_1-hd_1)^2+\\ +(af_1-be_1+ch_1+dg_1+eb_1-fa_1-gd_1-hc_1)^2+\\ +(ag_1+bh_1+ce_1-df_1-ec_1+fd_1-ga_1-hb_1)^2+\\ +(ah_1-bg_1-cf_1-de_1+ed_1+fc_1+gb_1-ha_1)^2.\end{aligned}$$

[1]) Ob. książkę: V.-A. Le Besgue, *Introduction à la théorie des nombres*, Paris 1862; ob. też książkę: G. Peano, *Formulaire de Mathématiques*, Turyn 1901, str. 67, gdzie wzór ten jest przypisany Degenowi (1822).

Istnieje analogiczna tożsamość, wyrażająca iloczyn dwu sum 2^m kwadratów jako sumę 2^m kwadratów [1]).

Badano też, dla jakich układów liczb naturalnych a, b, c, d każda liczba naturalna n daje się przedstawić w postaci

$$ax^2+by^2+cz^2+du^2$$

przy x, y, z i u całkowitych. Matematyk hinduski Ramanujan [2]) dowiódł, że istnieją tylko 54 takie układy. Jednym z nich jest np. układ postaci $x^2+2y^2+4z^2+14u^2$.

Lemat II. *Każda liczba pierwsza rozkłada się na sumę kwadratów czterech liczb całkowitych.*

Dowód. Dla liczby 2 prawdziwość lematu jest oczywista, gdyż

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

Załóżmy więc $p>2$. A zatem p jest liczbą pierwszą nieparzystą. W myśl lematu I wystarczy okazać, że p jest dzielnikiem pewnej sumy kwadratów czterech liczb całkowitych, z których jedna przynajmniej nie jest podzielna przez p.

Wyznaczamy reszty według modułu p liczb

$$(77) \qquad 1+0^2, \quad 1+1^2, \quad 1+2^2, \quad \ldots, \quad 1+\left(\frac{p-1}{2}\right)^2.$$

Wszystkie te reszty są różne, gdyż w przeciwnym razie istniałyby dwie różne liczby całkowite u i v, spełniające nierówności:

$$(78) \qquad 0\leqslant u\leqslant\frac{p-1}{2}, \qquad 0\leqslant v\leqslant\frac{p-1}{2}$$

oraz kongruencję

$$1+u^2\equiv 1+v^2 \pmod p.$$

Z kongruencji tej wynika, że $u^2-v^2=(u+v)(u-v)$ jest podzielne przez liczbę pierwszą p, tymczasem nierówności (78) dają:

$$0\leqslant u+v\leqslant p-1, \qquad -\frac{p-1}{2}\leqslant u-v\leqslant\frac{p-1}{2}.$$

[1]) A. Genocchi, Annali di Matematica, Seria 1, tom 3 (1860), str. 202-206.

[2]) S. Ramanujan, Proceedings of the Cambridge Philosophical Society, tom 19, I (1916), str. 11-21.

Aby $u+v$ było podzielne przez p, potrzeba więc, iżby było $u+v=0$, co wobec $u\geqslant 0$ i $v\geqslant 0$ daje $u=v=0$; aby zaś $u-v$ było podzielne przez p, potrzeba, iżby było $u-v=0$ czyli znowu $u=v$. W każdym więc razie byłoby $u=v$, wbrew założeniu.

Liczby w ciągu (77) dają zatem $1+\frac{p-1}{2}=\frac{p+1}{2}$ różnych reszt przy dzieleniu przez p.

Wyznaczamy dalej reszty według modułu p liczb

$$(79) \qquad -0^2, \quad -1^2, \quad -2^2, \quad \ldots, \quad -\left(\frac{p-1}{2}\right)^2.$$

Zupełnie tak samo jak dla ciągu (77) udowodnilibyśmy, że liczby (79) dają też $\frac{p+1}{2}$ różnych reszt przy dzieleniu przez p.

Reszty liczb ciągu (77) według modułu p nie mogą być wszystkie różne od każdej z reszt liczb ciągu (79) według tegoż modułu, gdyż wtedy mielibyśmy $\frac{p+1}{2}+\frac{p+1}{2}=p+1$ różnych reszt według modułu p, gdy tymczasem różnych reszt według modułu p jest tylko p. Znajdzie się więc w ciągu (77) przynajmniej jeden wyraz, np $1+x^2$, który da według modułu p taką samą resztę, jaką daje pewien wyraz ciągu (79), np. $-y^2$. Mamy więc przy pewnych całkowitych x i y

$$1+x^2\equiv -y^2 \pmod p,$$

czyli liczba $1^2+x^2+y^2$ jest podzielna przez p. Lecz liczba ta, napisana w formie $1+x^2+y^2+0^2$, jest oczywiście sumą kwadratów czterech liczb całkowitych, z których przynajmniej jedna (mianowicie pierwsza) nie jest podzielna przez p, c. b. d. o.

Możemy teraz już przejść do dowodu samego twierdzenia 15.

W myśl tożsamości (74), iloczyn dwu liczb, z których każda rozkłada się na sumę czterech kwadratów, sam jest sumą czterech kwadratów. Twierdzenie to uogólniamy natychmiast na dowolną liczbę czynników. Ponieważ zaś każda liczba naturalna większa od 1 albo sama jest pierwsza, albo rozwija się na iloczyn samych czynników pierwszych, więc w myśl lematu II każda liczba naturalna większa od 1 rozkłada się na sumę czterech kwadratów. Liczby 0 i 1 również rozkładają się na sumę czterech kwadratów:

$$0=0^2+0^2+0^2+0^2, \quad 1=1^2+0^2+0^2+0^2.$$

Twierdzenie 15 jest zatem dowiedzione.

Ponieważ zmiana znaku liczby x nie wpływa na wartość liczby x^2, więc z udowodnionego twierdzenia wynika następujący

Wniosek. *Każda liczba naturalna jest sumą kwadratów czterech liczb całkowitych nieujemnych.*

Można dowieść (choć nie jest to rzeczą łatwą), że każda liczba nieparzysta jest sumą czterech kwadratów liczb całkowitych, z których co najmniej dwie są równe (czytelnik zechce to sprawdzić dla liczb nieparzystych mniejszych od 30, wypisując odpowiednie rozkłady). Turski dowiódł, że każda liczba naturalna jest sumą dziesięciu lub mniej kwadratów liczb nieparzystych[1]). Pozostawiamy czytelnikowi do udowodnienia, że liczba 66 nie jest sumą mniej niż dziesięciu kwadratów liczb nieparzystych.

Znane są dowody twierdzenia Lagrange'a, przy pomocy kwaternionów[2]).

Badano też rozkłady liczb naturalnych na sumy $a^2+b^3+c^4$, gdzie a i c są liczbami całkowitymi, a b — liczbą naturalną [3]).

ĆWICZENIA. 1. Dowieść, że liczby 9, 11, 14 i 17 nie są sumami czterech kwadratów liczb naturalnych.

2. Dowieść, że każda liczba naturalna mniejsza od 112 jest sumą kwadratów czterech liczb całkowitych, z których co najmniej jedna jest równa 0 lub 1, oraz że liczba 112 nie ma już tej własności.

3. Dowieść, że każda liczba wymierna nieujemna jest sumą kwadratów czterech liczb wymiernych.

Dowód wynika z twierdzenia Lagrange'a i z tego, że $\frac{l}{m}=\frac{lm}{m^2}$.

4. Dowieść, że każda liczba naturalna mniejsza od 448 jest sumą kwadratów czterech liczb całkowitych, z których co najmniej jedna ma wartość bezwzględną niewiększą od 2, oraz że liczba 448 już nie ma tej własności.

5. Dowieść, że w każdym rozkładzie liczby $4^m\cdot 7$ na sumę kwadratów czterech liczb całkowitych każdy ze składników ma wartość bezwzględną niemniejszą od 2^{m-1}.

---

[1]) S. Turski, Bulletin de la Société Royale des Sciences de Liège 1933, nr 3. Por. też ćwiczenie 7, str. 101.

[2]) Ob. np. D. Barbilian, Mathematica 22 (1946), str. 159-169.

[3]) Ob. K. F. Roth, *Proof that almost all positive integers are sums of square, a positive cube and a fourth power*, Journal of London Mathematical Society, tom 24 (1949), str. 4-13.

Dowód wynika stąd, że dla $k\leqslant m-2$ jest

$$4^m\cdot 7-[2^k(2t-1)]^2=4^k[4^{m-k}\cdot 7-(8u+1)]=4^k(8x+7)$$

i że żadna liczba postaci $4^k(8x+7)$ nie jest sumą trzech kwadratów liczb całkowitych.

6. Dowieść za pomocą twierdzenia Lagrange'a, że każda liczba naturalna podzielna przez 8 jest sumą ośmiu kwadratów liczb nieparzystych.

Dowód. Jeżeli n jest liczbą naturalną, to w myśl twierdzenia Lagrange'a istnieją takie liczby całkowite a, b, c, d, że $n-1=a^2+b^2+c^2+d^2$, skąd

$$8n=(2a-1)^2+(2b-1)^2+(2c-1)^2+(2d-1)^2+$$
$$+(2a+1)^2+(2b+1)^2+(2c+1)^2+(2d+1)^2.$$

7. Wyprowadzić twierdzenie Turskiego[1]) z twierdzenia Gaussa, orzekającego, że każda liczba naturalna, nie będąca postaci $4^{k-1}(8t+7)$, jest sumą trzech kwadratów.

Dowód. W myśl twierdzenia Gaussa każda liczba naturalna postaci $8k+3$ jest sumą trzech kwadratów $x^2+y^2+z^2$; łatwo widzieć, że liczby x, y i z muszą być nieparzyste. Z drugiej strony, każda liczba naturalna większa od 3 jest postaci $8k+3+r$, gdzie $r=0, 1, 2, \ldots, 7$, a więc r jest sumą co najwyżej 7 kwadratów z jedności.

8. Z twierdzenia Gaussa o rozkładalności liczb postaci $8k+5$ na sumę trzech kwadratów wyprowadzić następujące twierdzenie K. Zarankiewicza i M. Schiffera[2]):

Każda liczba naturalna $n>1$ jest sumą kwadratów czterech liczb całkowitych, z których co najmniej dwie są różne od zera.

Dowód. Wobec twierdzenia 15 wystarczy ograniczyć się do liczb naturalnych $n>1$, będących kwadratami.

Jeżeli n jest kwadratem liczby parzystej, $n=(2m)^2$, to oczywiście $n=m^2+m^2+m^2+m^2$, gdzie m jest liczbą naturalną.

Jeżeli zaś n jest kwadratem liczby nieparzystej, $n=(2m+1)^2$, gdzie wobec $n>1$ liczba m jest naturalna, to $n\geqslant 3^2$ i liczba $n-4=(2m+1)^2-2^2$ jest naturalna postaci $8k+5$, a zatem w myśl twierdzenia Gaussa jest sumą kwadratów trzech liczb całkowitych nieujemnych, z których co najmniej dwie są dodatnie (gdyż liczba postaci $8k+5$ nie może być kwadratem). Liczba n jest więc wtedy sumą czterech kwadratów liczb całkowitych, z których co najmniej trzy są dodatnie.

9. Dowieść, że żadna liczba postaci 2^{2k+1}, gdzie $k=0, 1, 2, \ldots$, nie jest sumą kwadratów czterech liczb naturalnych.

Dowód Przypuśćmy, że istnieją liczby tej postaci, będące sumami kwadratów czterech liczb naturalnych. Niech 2^{2k+1} będzie najmniejszą

---

[1]) p. str. 100.

[2]) W rozdziale XVI, § 6, podamy inny dowód tego twierdzenia, nie oparty na twierdzeniu Gaussa.

z nich. Musi tu być $k>0$, a zatem $2^{2k+1}\equiv 0 \pmod 8$. Mamy więc $2^{2k+1}=n_1^2+n_2^2+n_3^2+n_4^2$, gdzie liczby n_1, n_2, n_3, n_4 są naturalne. Gdyby nie wszystkie one były parzyste, mielibyśmy $n_1^2+n_2^2+n_3^2+n_4^2\equiv 4$ lub $\equiv 2 \pmod 8$, co niemożliwe. Jest więc $n_i=2l_i$ dla $i=1,2,3,4$, gdzie liczby l_i są naturalne, skąd $2^{2k-1}=l_1^2+l_2^2+l_3^2+l_4^2$, wbrew określeniu liczby 2^{2k+1}.

10. Dowieść, że żadna liczba naturalna postaci 2^{2k+1} nie jest sumą kwadratów trzech liczb naturalnych.

Dowód jest analogiczny do dowodu z ćwiczenia 9,

11. Dowieść, że liczba naturalna 89 nie jest postaci $11x^2+y^2$ dla x i y całkowitych, lecz jest tej postaci dla x i y wymiernych.

Wskazówka: $89=11\left(\frac{5}{2}\right)^2+\left(\frac{9}{2}\right)^2=11\left(\frac{4}{3}\right)^2+\left(\frac{25}{3}\right)^2$.

12. Dowieść, że każda potęga naturalna sumy trzech kwadratów jest sumą trzech kwadratów.

Dowód. Twierdzenie jest oczywiste dla potęg pierwszej i drugiej. Jeżeli zaś $n\geqslant 3$, to $n=2k$ lub $n=2k+3$, gdzie k jest liczbą całkowitą nieujemną. Wobec tożsamości Catalana

$$(x^2+y^2+z^2)^3=x^2(3z^2-x^2-y^2)^2+y^2(3z^2-x^2-y^2)^2+z^2(z^2-3x^2-3y^2)^2$$

mamy więc

$$(x^2+y^2+z^2)^{2k+3}=(x^2+y^2+z^2)^{2k}(t^2+u^2+w^2)=$$
$$=[(x^2+y^2+z^2)^k t]^2+[(x^2+y^2+z^2)^k u]^2+[(x^2+y^2+z^2)^k w]^2;$$

zarazem

$$(x^2+y^2+z^2)^{2k}=[(x^2+y^2+z^2)^k]^2+0^2+0^2.$$

§ 11. Twierdzenie Waringa. E. Waring w 1782 r. wypowiedział bez dowodu następujące twierdzenie [1]):

Do każdego wykładnika naturalnego s można dobrać taką liczbę naturalną k, że każda liczba naturalna n jest sumą k składników, z których każdy jest s-tą potęgą liczby całkowitej nieujemnej.

Dla $s=1$ twierdzenie to jest oczywiście prawdziwe, ale nic ciekawego nie daje. Dla $s=2$ możemy przyjąć $k=4$ w myśl twierdzenia Lagrange'a (str. 93), udowodnionego w § 10.

Dla $s=3$ Waring twierdził, że można przyjąć $k=9$, tj. że każda liczba naturalna jest sumą dziewięciu (lub mniej) sześcianów liczb naturalnych. Twierdzenie to udowodnił dopiero A. Wieferich w 1909 r.

Dla $s=4$ Waring twierdził, że można przyjąć $k=19$ tj. że każda liczba naturalna jest sumą dziewiętnastu (lub mniej) bi-

[1]) Twierdzenie to udowodnił D. Hilbert (w 1909 r).

kwadratów. Twierdzenia tego dotąd jednak nie udowodniono ani nie obalono. G. H. Hardy i J. E. Littlewood dowiedli, że jest ono prawdziwe dla wszystkich liczb naturalnych niewiększych od $10^{10^{90}}$.

Wiadomo też, że każda dostatecznie wielka liczba naturalna jest sumą 17 czwartych potęg liczb całkowitych. Dowiedli tego jednocześnie Estermann[1]) oraz Davenport i Heilbronn[2]).

Zajmiemy się tutaj przypadkiem $s=4$; można wówczas przyjąć $k=53$. Udowodnimy mianowicie

Twierdzenie 16. *Każda liczba naturalna jest sumą 53 czwartych potęg liczb całkowitych nieujemnych.*

Dowód oparty jest na następującej ciekawej tożsamości E. Lucasa, podanej w 1876 r.:

$$\begin{aligned}6(x_1^2+x_2^2+x_3^2+x_4^2)^2=&\\ =(x_1+x_2)^4+(x_1-x_2)^4+(x_1+x_3)^4+(x_1-x_3)^4+&\\ +(x_1+x_4)^4+(x_1-x_4)^4+(x_2+x_3)^4+(x_2-x_3)^4+&\\ +(x_2+x_4)^4+(x_2-x_4)^4+(x_3+x_4)^4+(x_3-x_4)^4.&\end{aligned}\tag{80}$$

Niech n będzie liczbą naturalną, która przy dzieleniu przez 6 daje resztę r:

$$n=6m+r,\tag{81}$$

gdzie m jest liczbą całkowitą nieujemną, r zaś — jedną z liczb

$$0,\ 1,\ 2,\ 3,\ 4,\ 5.\tag{82}$$

W myśl twierdzenia Lagrange'a istnieją takie cztery liczby całkowite nieujemne a, b, c, d, że

$$m=a^2+b^2+c^2+d^2.$$

Wobec (81) możemy napisać:

$$n=6a^2+6b^2+6c^2+6d^2+6r.\tag{83}$$

W myśl tegoż twierdzenia Lagrange'a istnieją takie cztery liczby całkowite x_1, x_2, x_3, x_4, że

$$a=x_1^2+x_2^2+x_3^2+x_4^2.$$

Wobec tożsamości (80) możemy napisać:

$$6a^2=\alpha_1^4+\alpha_1^4+\alpha_3^4+\ldots+\alpha_{12}^4,\tag{84}$$

[1]) T. Estermann, Proceedings of the London Mathematical Society, seria II, tom 41 (1936), str. 126-142.

[2]) H. Davenport i H. Heilbronn, tamże, str. 143-150.

gdzie $a_1, a_2, \ldots, a_{12}$ są liczbami całkowitymi nieujemnymi (mianowicie $a_1=|x_1+x_2|$, $a_2=|x_1-x_2|$, ..., $a_{12}=|x_3-x_4|$). Podobnie, istnieją liczby całkowite nieujemne $\beta_i, \gamma_i, \delta_i$ (gdzie $i=1, 2, \ldots, 12$) takie, że:

$$\begin{aligned} 6b^2&=\beta_1^4+\beta_2^4+\ldots.+\beta_{12}^4,\\ 6c^2&=\gamma_1^4+\gamma_2^4+\ldots.+\gamma_{12}^4,\\ 6d^2&=\delta_1^4+\delta_2^4+\ldots.+\delta_{12}^4. \end{aligned} \tag{85}$$

Dla każdej zaś liczby r z ciągu (82) istnieje pięć takich liczb całkowitych nieujemnych ε_i $(i=1,2,\ldots,5)$, że

$$r=\varepsilon_1^4+\varepsilon_2^4+\varepsilon_3^4+\varepsilon_4^4+\varepsilon_5^4. \tag{86}$$

Istotnie:

$$\begin{aligned} 0&=0^4+0^4+0^4+0^4+0^4,\\ 1&=1^4+0^4+0^4+0^4+0^4,\\ 2&=1^4+1^4+0^4+0^4+0^4,\\ &\cdots\cdots\cdots\\ 5&=1^4+1^4+1^4+1^4+1^4. \end{aligned}$$

Wobec (83)-(86) możemy zatem napisać:

$$n=a_1^4+a_2^4+\ldots+a_{12}^4+\beta_1^4+\beta_2^4+\ldots+\beta_{12}^4+\gamma_1^4+\gamma_2^4+\ldots+\gamma_{12}^4+ +\delta_1^4+\delta_2^4+\ldots+\delta_{12}^4+\varepsilon_1^4+\varepsilon_2^4+\ldots+\varepsilon_5^4.$$

Liczba n jest więc sumą $4\cdot 12+5=53$ czwartych potęg liczb całkowitych nieujemnych, c. b. d. o.

Pierwszy dowód tego twierdzenia podał J. Liouville w połowie ubiegłego stulecia.

Twierdzenie 17. *Każda liczba całkowita jest sumą algebraiczną 12 czwartych potęg liczb całkowitych*[1]).

Dowód. Każdą liczbę całkowitą x możemy przedstawić w postaci $x=24t+r$, gdzie t jest liczbą całkowitą, r zaś jest jedną z liczb $0, 1, \ldots, 23$. Wnosimy stąd, że $x=24t+12+(r-12)$, gdzie $r-12=-12, -11, \ldots, -1, -0, 1, 2, \ldots, 11$. Wobec tożsamości

$$24k+12=(k+2)^4-3(k+1)^4+3k^4-(k-1)^4 \tag{87}$$

[1]) E. L. Dickson, *Modern Elementary Theory of Numbers*, The University of Chicago Press (1939), str. 262.

dla dowodu twierdzenia wystarczy więc okazać, że każda z liczb $1, 2, \ldots, 12$ przystaje według modułu 24 do sumy algebraicznej czterech bikwadratów. Wówczas bowiem będzie

$$r-12=24u\pm a_1^4\pm a_2^4\pm a_3^4\pm a_4^4,$$

gdzie u, a_1, a_2, a_3 i a_4 są liczbami całkowitymi, skąd otrzymamy

$$x=24(t+u)+12\pm a_1^4\pm a_2^4\pm a_3^4\pm a_4^4;$$

a ponieważ wobec (87) jest

$$24(t+u)+12=\sum_{i=5}^{12}\pm a_i^4,$$

gdzie $a_5, a_6, \ldots, a_{12}$ są liczbami całkowitymi, więc będzie

$$x=\sum_{i=1}^{12}\pm a_i^4.$$

Pozostaje więc jedynie sprawdzić, że istotnie:

$5=24-2^4-1^4-1^4-1^4$, $6=24-2^4-1^4-1^4$, $7=24-2^4-1^4$,

$8=24-2^4$, $9=24-2^4+1^4$, $10=24-2^4+1^4+1^4$,

$11=24-2^4+1^4+1^4+1^4$, $12=-3\cdot 24+3^4+1^4+1^4+1^4$.

Hunter[1]) dowiódł, że każda liczba całkowita daje się na nieskończenie wiele sposobów przedstawić jako suma algebraiczna dziesięciu czwartych potęg liczb całkowitych.

ĆWICZENIE. Stosując metodę dowodu twierdzenia 17, przedstawić liczby 79 i 100 jako sumy algebraiczne 12 bikwadratów.

Odpowiedź: $79=4^4-3\cdot 3^4+3\cdot 2^4-1^4+6\cdot 0^4$, $100=5^4-3\cdot 4^4+3\cdot 3^4+5\cdot 0^4$. Ale mamy też inne rozkłady:

$79=3^4-1^4-1^4+9\cdot 0^4$, $100=3^4+2^4+3\cdot 1^4+7\cdot 0^4$.

Twierdzenie Waringa orzeka, że dla każdej liczby naturalnej s istnieje taka liczba naturalna k, że dla wszelkiej liczby naturalnej n równanie nieoznaczone

$$n=x_1^s+x_2^s+x_3^s+\ldots.+x_k^s \tag{88}$$

jest rozwiązalne w liczbach całkowitych nieujemnych x_i.

Jeżeli przy ustalonym s liczba naturalna k spełnia ten warunek, to oczywiście każda liczba naturalna większa od k spełnia

[1]) H. Hunter, Journal of the London Mathematical Society, tom 16 (1941), str. 171-179; por. też H. Davenport, tamże, str. 3-4.

go tym bardziej, gdyż z rozwiązalności (w liczbach całkowitych nieujemnych) równania (88) wynika tym bardziej rozwiązalność (w takich liczbach) równania

$$n=x_1^s+x_2^s+\ldots+x_k^s+x_{k+1}^s+\ldots+x_{k+l}^s.$$

Mianowicie wystarczy wyznaczyć liczby $x_1, x_2, \ldots, x_k$ z równania (88) i przyjąć $x_{k+1}=x_{k+2}=\ldots=x_{k+l}=0$.

Wobec tego dla każdego wykładnika naturalnego s istnieje nieskończenie wiele odpowiednich liczb naturalnych k; oznaczmy przez k_s najmniejszą z nich.

Tak więc liczba naturalna k_s jest wyznaczona przez następujące dwie własności:

1° Każda liczba naturalna n rozkłada się na sumę k_s składników, z których każdy jest s-tą potęgą liczby całkowitej nieujemnej.

2° Istnieje przynajmniej jedna liczba naturalna, nie rozkładająca się na sumę k_s-1 składników, które są s-tymi potęgami liczb całkowitych nieujemnych.

Obliczmy np. k_2. Ponieważ każda liczba naturalna jest sumą czterech kwadratów oraz istnieją liczby naturalne, które nie są sumami trzech kwadratów, wnosimy, że $k_2=4$. Dla $s>2$ znamy dotychczas jedną tylko wartość k_s, mianowicie $k_3=9$ (Wiefe-rich, p. str. 102). Dla niektórych $s>3$ znamy jedynie granice, w których liczby k_s są zawarte.

Tak np. na podstawie dowiedzionego twierdzenia 17 możemy twierdzić, że $k_4\leqslant 53$.

Jest to górna granica dla liczby k_4. Pokażemy teraz w jaki sposób obliczać można dolne granice dla liczb k_s.

Weźmy pod uwagę liczbę

$$n=2^s\mathrm{E}\left(\frac{3^s}{2^s}\right)-1. \tag{89}$$

Na mocy definicji symbolu $\mathrm{E}(x)$ (str. 49) jest zawsze $\mathrm{E}(x)\leqslant x$; wzór (89) daje więc w jednej chwili

$$n<3^s; \tag{90}$$

n jest oczywiście liczbą naturalną. Na mocy określenia liczby k_s możemy powiedzieć, że istnieją takie liczby całkowite nieujemne x_i $(i=1,2,\ldots,k_s)$, iż

$$n=x_1^s+x_2^s+\ldots+x_{k_s}^s. \tag{91}$$

Z nierówności (90) wynika, że każda z liczb x_i jest mniejsza od 3; liczby te mogą więc być równe tylko 0, 1 lub 2. Załóżmy, że wśród k_s składników prawej strony wzoru (91) mamy l równych 2^s, m równych 1, oraz q równych 0; liczby l, m i q są oczywiście całkowite nieujemne. Będziemy mogli napisać:

$$k_s=l+m+q\geqslant l+m, \tag{92}$$

$$n=2^s l+m, \tag{93}$$

skąd $n\geqslant 2^s l$ czyli $l\leqslant\frac{n}{2^s}$, a że w myśl (89) jest $n<2^s\mathrm{E}\left(\frac{3^s}{2^s}\right)$, więc $l<\mathrm{E}\left(\frac{3^s}{2^s}\right)$ czyli

$$l\leqslant\mathrm{E}\left(\frac{3^s}{2^s}\right)-1. \tag{94}$$

Wobec (93) mamy $m=n-2^s l$, a zatem

$$l+m=l+(n-2^s l)=n-(2^s-1)l. \tag{95}$$

Ponieważ s jest liczbą naturalną, więc 2^s-1 jest liczbą dodatnią. Mnożąc przez tę liczbę nierówność (94), dostajemy

$$(2^s-1)l\leqslant(2^s-1)\left[\mathrm{E}\left(\frac{3^s}{2^s}\right)-1\right],$$

skąd na mocy (95)

$$l+m\geqslant n-(2^s-1)\left[\mathrm{E}\left(\frac{3^s}{2^s}\right)-1\right].$$

Prawa strona tej nierówności równa jest na mocy (89)

$$2^s\mathrm{E}\left(\frac{3^s}{2^s}\right)-1-(2^s-1)\left[\mathrm{E}\left(\frac{3^s}{2^s}\right)-1\right]=\mathrm{E}\left(\frac{3^s}{2^s}\right)+2^s-2.$$

Wobec (92) możemy więc ostatecznie napisać

$$k_s\geqslant\mathrm{E}\left(\frac{3^s}{2^s}\right)+2^s-2. \tag{96}$$

Prawa strona tej nierówności jest właśnie dolną granicą dla liczb k_s.

Dla $s=2$ nierówność (96) daje $k_s\geqslant\mathrm{E}\left(\frac{9}{4}\right)+2^2-2=2+4-2$ czyli $k_2\geqslant 4$ (wyżej dowiedliśmy nawet, że $k_2=4$).

Dla $s=3$ nierówność (96) daje $k_3 \geqslant E\left(\frac{27}{8}\right)+2^3-2=3+8-2$

czyli $k_3 \geqslant 9$. Istnieją zatem liczby naturalne — np. liczba 23 — które nie rozkładają się na sumę ośmiu sześcianów liczb całkowitych nieujemnych, a jak wspomnieliśmy (na str. 102), Wieferich dowiódł nawet, że $k_3=9$.

Dla $s=4$ nierówność (96) daje $k_4 \geqslant E\left(\frac{81}{16}\right)+2^4-2=5+16-2$

czyli $k_4 \geqslant 19$. Istnieją więc w myśl wzoru (89) liczby naturalne — np. liczba 79 — które się nie rozkładają na sumę 18 bikwadratów. Waring twierdził, że $k_4=19$.

Dla $s=5$ nierówność (96) daje, jak łatwo obliczyć, $k_5 \geqslant 37$, a wzór (89) wskazuje, że liczba 223 nie rozkłada się na sumę 36 składników, z których każdy jest 5-tą potęgą liczby całkowitej nieujemnej. Dotąd nie rozstrzygnięto, czy $k_5=37$, czy $k_5>37$.

Dla $s=6$ nierówność (96) daje $k_6 \geqslant 73$.

W związku z twierdzeniem, że $k_3=9$, zauważymy, że — jak łatwo dowieść — *każda liczba całkowita jest sumą pięciu sześcianów liczb całkowitych*[1]).

Istotnie, każda liczba całkowita t, podzielna przez 6, jest sumą czterech sześcianów liczb całkowitych (a więc też i pięciu, gdyż możemy dodać 0^3), ponieważ — jak łatwo sprawdzić —

$$6k=(k+1)^3+(k-1)^3+(-k)^3+(-k)^3.$$

Dla innych zaś liczb całkowitych mamy

$$6k+1=6k+1^3, \quad 6k+2=6(k-1)+2^3, \quad 6k+3=6(k-4)+3^3,$$

$$6k+4=6(k+2)+(-2)^3, \quad 6k+5=6(k+1)+(-1)^3.$$

Bang[2]) przypuszcza, że każda liczba całkowita jest sumą czterech sześcianów liczb całkowitych.

Chao Ko ułożył tablice rozkładów wszystkich liczb naturalnych niewiększych od 100 na sumę czterech sześcianów liczb całkowitych. W szczególności

$$76=(-11)^3+10^3+7^3+4^3, \quad 100=5^3+(-3)^3+1^3+1^3.$$

[1]) S. Lubelski, *Zadania i twierdzenia z ogólnej teorii liczb*, Warszawa 1932, str. 10 i 52-53.

[2]) A. S. Bang, Mathematisk Tidsskrift (1940), str. 25-42.

Można dowieść z łatwością, że każda liczba całkowita, która rozkłada się na sumę sześcianów dwu liczb całkowitych, ma skończoną liczbę takich rozkładów (ob. ćwiczenie 1, str. 111), natomiast nie każda liczba naturalna, rozkładająca się na sumę trzech sześcianów liczb całkowitych, ma skończoną liczbę takich rozkładów; np. liczba 1 ma nieskończenie wiele rozkładów

$$1=1^3+n^3+(-n)^3 \qquad \text{dla } n=1,2,\ldots,$$

albo jeżeli nie chcemy, żeby dwa sześciany się znosiły,

$$1=(9n^4)^3+(1-9n^3)^3+(3n-9n^4)^3 \quad \text{dla } n=1,2,\ldots$$

Liczba 0 nie rozkłada się na sumę trzech sześcianów liczb całkowitych różnych od zera; dowód tego nie jest bynajmniej łatwy (podamy go w Rozdziale XVII, § 9). Natomiast 0 ma nieskończenie wiele rozkładów na sumę czterech sześcianów liczb całkowitych różnych od zera, np.

$$0=(3n)^3+(4n)^3+(5n)^3+(-6n)^3 \quad \text{dla } n=1,2,\ldots$$

H. W. Richmond dowiódł na drodze elementarnej (w 1923 r.), że każda liczba wymierna dodatnia jest sumą trzech sześcianów liczb wymiernych[1]). Z wielkiego twierdzenia Fermata dla trzecich potęg (Rozdział XVII, § 9) wynika natychmiast, że liczba 1 nie jest sumą dwu sześcianów liczb wymiernych.

Twierdzenie 18. *Każda liczba wymierna jest sumą trzech sześcianów liczb wymiernych.*

Dowód. W tożsamości

$$(a-b)^3+(b-c)^3+c^3=3b^2(a-c)+[a^3-3b(a^2-c^2)]$$

podstawmy

$$a=12t(t+1), \quad b=(t+1)^3, \quad c=12t(t-1).$$

Otrzymamy

$$72t(t+1)^6=(a-b)^3+(b-c)^3+c^3.$$

W przypadku, gdy $t\neq-1$, wnosimy, że liczba $w=72t$ jest sumą trzech sześcianów liczb, wyrażających się wymiernie przez t. Każda więc liczba wymierna $w\neq-72$ jest sumą trzech sześcianów liczb wymiernych.

W przypadku, gdy $t=-1$, mamy $-72=(-4)^3+(-2)^3+0^3$.

[1]) Ob. I. Arnold, *Tieoria czisieł*, Moskwa 1939, str. 136.

Twierdzenie 19. *Każda liczba całkowita jest sumą dziesięciu piątych potęg liczb całkowitych*[1]).

Dowód. Wobec tożsamości

$$720k-360=(k+3)^5-2(k+2)^5+k^5+(k-1)^5-2(k-3)^5+(k-4)^5$$

wystarczy dowieść, że *każda liczba całkowita k przystaje według modułu 720 do sumy dwu piątych potęg liczb całkowitych.*

Okażemy przede wszystkim, że

$$x\equiv x^{25}\pmod{720} \quad \text{dla} \quad (x,720)=1.$$

Rzeczywiście, dla $(x,720)=1$ mamy w myśl małego twierdzenia Fermata $x^5\equiv x\pmod 5$, skąd $x^{25}\equiv x\pmod 5$. W myśl zaś twierdzenia Eulera[2]) jest $x^6\equiv 1\pmod 9$, skąd $x^{24}\equiv 1\pmod 9$ oraz $x^{25}\equiv x\pmod 9$. Podobnie, w myśl twierdzenia Eulera jest $x^8\equiv 1\pmod{16}$, skąd $x^{24}\equiv 1\pmod{16}$ oraz $x^{25}\equiv x\pmod{16}$. Mamy więc $x\equiv x^{25}\pmod{5,9,16}$, skąd $x\equiv x^{25}\pmod{720}$, gdyż $720=5\cdot 9\cdot 16$ i $(5,9)=(5,16)=(9,16)=1$.

Niech teraz k będzie dowolną liczbą całkowitą. Możemy ją przedstawić w postaci $k=ab$, gdzie $a=2^\alpha 3^\beta 5^\gamma$, a $(b,720)=1$.

Jeżeli $\alpha>0$, $\beta>0$ i $\gamma>0$, to $a=1+c$, gdzie $(c,720)=1$; zatem $a\equiv 1+c^{25}\pmod{720}$, a że wobec $(b,720)=1$ mamy $b\equiv b^{25}\pmod{720}$, więc $k=ab\equiv b^{25}+(c^5b^5)^5\pmod{720}$.

Jeżeli zaś jedna z liczb α,β,γ jest równa zeru, np. $\alpha>0$, $\beta>0$ i $\gamma=0$, to $a=5^5+c$, gdzie — jak łatwo widzieć — jest $(c,720)=1$; zatem $c\equiv c^{25}\pmod{720}$, skąd znowu wnosimy, że k przystaje według modułu 720 do sumy dwu piątych potęg.

Jeżeli dwie z liczb α,β,γ są równe zeru, np. $\alpha>0$, $\beta=0$ i $\gamma=0$, to $a=(3.5)^5+c$, gdzie $(c,720)=1$ i dalej rozumujemy jak poprzednio.

Jeżeli wreszcie $\alpha=\beta=\gamma=0$, to $a=1$ i $k=b$, gdzie $(b,720)=1$; zatem $k\equiv(b^5)^5+0^5\pmod{720}$.

Tym samym twierdzenie 19 zostało udowodnione.

Dickson ogłosił[3]) dla naturalnych $n<300000$ tablice najmniejszych liczb k (zależnych od n) takich, że n rozkłada się na sumę k piątych potęg. Z tablic tych widać, że każda liczba mniejsza od $3\cdot 10^5$ jest sumą co najwyżej 37 piątych potęg. Metodą przez niego podaną można dowieść, że jest tak dla $n<10^{183}$.

Dickson dowiódł również, że każda liczba naturalna jest sumą 4223 dwunastych potęg liczb całkowitych natomiast liczba $2^{12}\mathrm{E}\left(\frac{3}{2}\right)^{12}-1$ nie jest sumą mniej niż 4223 dwunastych potęg liczb całkowitych.

[1]) E. L. Dickson, *Modern Elementary Theory of Numbers*, The University of Chicago Press (1939), str. 263.

[2]) Ob. dalej Rozdział VIII, § 1.

[3]) E. L. Dickson, *Minimum decompositions into fifth powers*, Mathematical Tables, tom 3, Londyn 1933

ĆWICZENIA. 1. Dowieść, że liczba rozkładów liczby naturalnej na sumę sześcianów dwu liczb całkowitych nie przewyższa podwójnej liczby jej dzielników naturalnych.

Dowód. Jeżeli $n=x^3+y^3$, to $n=(x+y)(x^2-xy+y^2)$, zatem $x+y=\pm d$, gdzie $d|n$, A więc $y=\pm d-x$ i $x^2-xy+y^2=\pm\frac{n}{d}$, skąd $3x^2\mp 3dx+d^2\mp\frac{n}{d}=0$.

Aby równanie to posiadało pierwiastki rzeczywiste, potrzeba, żeby było $9d^2-12(d^2\mp\frac{n}{d})\geqslant 0$ czyli $\pm\frac{12n}{d}-3d^2\geqslant 0$, co jest możliwe tylko przy znaku górnym. Otrzymamy w ten sposób (dla danego $d|n$) co najwyżej dwie wartości na x, a wartości na y będą wyznaczone przez wzór $y=d-x$. Każdemu dzielnikowi naturalnemu d liczby n odpowiadają więc co najwyżej dwa różne rozkłady liczby n na sumę dwu sześcianów liczb całkowitych.

2. Dowieść, że żadna liczba formy $7k+3$ ani $7k+4$ (gdzie k jest całkowite) nie jest sumą sześcianów dwu liczb całkowitych.

Wskazówka: sześcian każdej liczby całkowitej jest formy $7t$ lub $7t\pm 1$.

3. Dowieść, że żadna liczba formy $9k+4$ ani $9k+5$ nie jest sumą sześcianów trzech liczb całkowitych.

Dowód. Z rozwinięcia $(3t\pm 1)^3$ wynika, że sześcian liczby całkowitej jest formy $9t$ lub $9t\pm 1$, suma zaś trzech liczb tych form nie może być liczbą formy $9k+4$ ani $9k+5$.

4. Przedstawić liczbę 1729 dwoma różnymi sposobami jako sumę sześcianów dwu liczb naturalnych.

Odpowiedź: $1729=10^3+9^3=12^3+1^3$. (Ramanujan)

Uwaga. Można dowieść, że jest to najmniejsza liczba naturalna, rozkładająca się dwoma różnymi sposobami na sumę sześcianów dwu liczb naturalnych (jeżeli rozkładów różniących się tylko porządkiem składników nie uważać za różne).