

TEORIA LICZB

Czym się zajmuje teoria liczb



CZEŚĆ PIERWSZA

NIEKTÓRE ZAGADNIENIA ADDYTYWNEJ TEORII LICZB

Jak wiadomo z arytmetyki, każda liczba naturalna jest sumą samych jedynek (jeżeli jako sumy uważamy i takie, które mają tylko jeden składnik). Więc na przykład

$$1 = 1, 2 = 1 + 1, 3 = 1 + 1 + 1, 4 = 1 + 1 + 1 + 1, \dots$$

Tak więc, jeżeli chodzi o budowę liczb naturalnych przy pomocy dodawania, to jest ona niezmiernie prosta: każdą liczbę naturalną otrzymujemy za pomocą dodawania do siebie samych jedynek, i każdą liczbę naturalną > 1 otrzymujemy z poprzedzającej ją liczby naturalnej przez dodanie do tej ostatniej jedynki. Można by więc powiedzieć, że pod tym względem liczby naturalne zachowują się jednolicie, że nie ma między nimi istotnych różnic, poza tą, że dla otrzymania liczb naturalnych potrzebna jest mniejsza lub większa liczba jedynek. Nie wynika stąd jednak, żeby wszystkie zagadnienia dotyczące otrzymywania liczb naturalnych za pomocą dodawania były łatwe. Rozpatrzmy tu kilka takich zagadnień o różnym stopniu trudności. Na początek postawmy sobie pytanie: iloma różnymi sposobami można daną liczbę naturalną $n > 1$ przedstawić jako sumę dwóch składników naturalnych? Należy tu oczywiście ustalić, czy mamy uważać za różne rozkłady różniące się tylko porządkiem składników, jak na przykład rozkłady $5 = 2 + 3$ i $5 = 3 + 2$. Jeżeli takie rozkłady będziemy uważali za różne, to, jak łatwo zauważyć, wszystkimi rozkładami liczby naturalnej $n > 1$ na sumę dwóch liczb naturalnych będą $1 + (n - 1)$,

$2 + (n - 2)$, $3 + (n - 3)$, . . . , $(n - 2) + 2$ i $(n - 1) + 1$ (gdyż pierwszym składnikiem może tu być dowolna liczba naturalna mniejsza od n , a rozkład danej liczby na sumę dwóch składników jest znany, gdy znamy pierwszy składnik). A więc rozkładów liczby naturalnej $n > 1$ na sumę dwóch składników naturalnych, jeżeli uważamy za różne rozkłady takie, które różnią się chociażby tylko porządkiem składników, jest $n - 1$. Nie tak już prostą będzie odpowiedź, jeżeli nie uważamy za różne rozkłady różniące się tylko porządkiem składników. Tutaj rozkłady takie jak $1 + (n - 1)$ i $(n - 1) + 1$ nie będziemy uważali za różne, a więc przy obliczaniu liczby rozkładów trzeba będzie je liczyć raz tylko. Podobnie będzie z każdymi dwoma wyrazami wypisanego wyżej ciągu $n - 1$ rozkładów, zajmującymi odpowiednio te same miejsca od początku i od końca (więc na przykład z rozkładami $2 + (n - 2)$ i $(n - 2) + 2$ itd.

Czy jednak w ten sposób każdy rozkład $k + (n - k)$ (gdzie k jest liczbą naturalną $< n$) będzie miał swoją parę $(n - k) + k$? Jeżeli n jest liczbą nieparzystą, to tak będzie istotnie, gdyż liczby k i $n - k$ będą wtedy różne (dla naturalnych $k < n$), bowiem z równości $k = n - k$ wynikałoby, że $n = 2k$, a więc, że liczba n jest parzysta. Ale jeśli n będzie liczbą parzystą, $n = 2k$, to oczywiście środkowy wyraz naszego ciągu rozkładów, $k + k$, nie będzie miał swojej pary. Stąd łatwy wniosek, że liczba rozkładów liczby naturalnej $n > 1$ na sumę dwóch składników naturalnych, jeżeli nie uważamy za różne rozkładów różniących się tylko porządkiem składników, wynosi przy n nieparzystym $n - 1/2$, zaś przy n parzystym $n / 2$.

Przejdźmy teraz do rozkładów liczb naturalnych > 2 na sumy trzech składników naturalnych. Jeżeli uważać za różne rozkłady różniące się tylko porządkiem składników, to liczbę rozkładów liczby n można obliczyć w sposób następujący. Pierwszym składnikiem może tu być oczywiście dowolna liczba naturalna $k \leq n - 2$. Przy takim danym k należy już tylko przedstawić liczbę $n - k \geq 2$ jako sumę dwóch składników naturalnych, a takich rozkładów (jeżeli uważać za różne rozkłady różniące się tylko porządkiem składników) jest, jak wiemy,

$n - k - 1$. Tak więc wszystkich rozkładów liczby naturalnej $n > 2$ na sumę trzech liczb naturalnych (jeżeli uważać za różne rozkłady różniące się tylko porządkiem składników) będzie $(n - 1 - 1) + (n - 2 - 1) + (n - 3 - 1) + \dots + [n - (n - 2) - 1] = n(n-3) / 2 + 1$

Na przykład dla liczby $n = 5$ będziemy mieli 6 rozkładów. Są to rozkłady $5 = 1 + 1 + 3 = 1 + 2 + 2 = 1 + 3 + 1 = 2 + 1 + 2 = 2 + 2 + 1 = 3 + 1 + 1$.

Jeżeli zaś nie uważać za różne rozkładów różniących się tylko porządkiem składników, to liczba 5 daje tylko dwa rozkłady na sumę trzech liczb naturalnych: $5 = 1 + 1 + 3 = 1 + 2 + 2$. Trudniej byłoby obliczyć, ile rozkładów na sumę trzech liczb naturalnych daje liczba naturalna $n > 2$, jeżeli nie uważać za różne rozkładów różniących się tylko porządkiem składników.

Badano też ogólniej, dla danej liczby naturalnej s , ile rozkładów na sumę s składników naturalnych daje liczba naturalna $n > s - 1$. Trudniejsze jeszcze jest następujące zagadnienie klasyczne, znane pod nazwą *partitio numerorum*: Iloma sposobami można liczbę naturalną n przedstawić jako sumę liczb naturalnych (jeżeli nie zwracać uwagi na liczbę składników)? I tu są również różne warianty tego zagadnienia, zależnie od tego, czy zwracamy uwagę na porządek składników, czy też nie.

Dla niewielkich n łatwo podać wszystkie rozkłady. Jeżeli na przykład nie uważać za różne rozkładów różniących się tylko porządkiem składników, to liczby 1, 2, 3, 4, 5 dają odpowiednio tylko rozkłady

$$1 = 1, 2 = 2 = 1 + 1, 3 = 3 = 1 + 2 = 1 + 1 + 1, 4 = 4 = 1 + 3 = 2 + 2 = 1 + 1 + 2 = 1 + 1 + 1 + 1, 5 = 5 = 1 + 4 = 2 + 3 = 1 + 1 + 3 = 1 + 1 + 1 + 2 = 1 + 1 + 1 + 1 + 1.$$

Jeżeli więc oznaczymy dla liczby naturalnej n przez $p(n)$ liczbę rozkładów liczby n na składniki naturalne, gdzie obojętną jest liczba składników, lecz nie uważamy za różne rozkładów różniących się tylko porządkiem składników, to będzie $p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5, p(5) = 7$. Łatwo byłoby jeszcze obliczyć, że $p(6) = 11, p(7) = 15, p(8) = 22, p(9) = 30, p(10) = 42$; ogólnego jednak wzoru na $p(n)$ dla naturalnych n nie znamy.

Za pomocą znanych z algebry własności współczynników rozwinięcia dwumianu łatwo jest dowiedzieć, że jeżeli n i k są dane liczby naturalne, to liczba wszystkich rozkładów liczby k na sumę n składników całkowitych ≥ 0 , gdzie rozkłady różniące się porządkiem składników uważamy za różne wynosi

$$\binom{n+k-1}{k} = \frac{(n+k-1)(n+k-2)\dots n}{1*2\dots k}$$

Mianownik jest tu iloczynem kolejnych liczb naturalnych od jedności aż do k , licznik zaś jest iloczynem kolejnych liczb naturalnych zaczynających się od liczby n , a kończących na liczbie $n+k-1$. (Więc na przykład liczba 4 daje na sumę dwóch składników

$$\binom{2+4-1}{4} = \frac{5}{4} = 5$$

takich rozkładów, mianowicie $4 = 0 + 4 = 4 + 0 = 1 + 3 = 3 + 1 = 2 + 2$.)

Zagadnienia, w których sformułowaniu mamy do czynienia tylko z dodawaniem i odejmowaniem liczb, należą do tak zwanej *addytywnej teorii liczb*. Niektóre z nich są trudne, jak na przykład *partitio numerorum*. A oto pewne twierdzenie z addytywnej teorii liczb, którego dowód jest wprawdzie elementarny, ale niezbyt łatwy:

Jeżeli wszystkie liczby naturalne rozbijemy na skończoną liczbę klas, to jedna co najmniej z tych klas zawiera pewne dwie różne liczby oraz ich sumę. Udowodniono też, że jeżeli k jest liczbą naturalną, $n = 3^{(k+1)!}$ i jeżeli liczby $1, 2, \dots, n$ rozbijemy na k klas, to jedna co najmniej z tych klas będzie zawierała pewne dwie różne liczby oraz ich sumę. W związku z tym twierdzeniem nasuwa się pytanie, jaka jest dla danej liczby naturalnej k najmniejsza liczba naturalna $n = n(k)$ taka, że jeżeli liczby $1, 2, \dots, n$ rozbijemy na k klas, to jedna co najmniej z tych klas zawierać będzie dwie różne liczby oraz ich sumę. Mamy tu oczywiście $n(1) = 3$. Można też dowiedzieć, że $n(2) = 9$. Że mamy tu $n(2) \geq 9$ wynika z uwagi, że zbiór wszystkich liczb naturalnych ≤ 8 można rozbić na dwa zbiory: jeden złożony z liczb 1, 2, 4, 8, a drugi z liczb 3, 5, 6, 7, przy czym, jak łatwo sprawdzić, żaden z tych dwóch zbiorów nie zawiera dwóch różnych liczb i ich sumy. Dla dowodu, że $n(2) = 9$ wystarczy więc udowodnić, że jeżeli liczby 1, 2, 3, 4, 5, 6, 7, 8, 9 podzielimy w dowolny sposób na dwie klasy, to co najmniej jedna z nich zawierać będzie dwie różne liczby oraz ich sumę. Dowód

nie jest trudny, ale nie natychmiastowy, gdyż wymaga rozpatrzenia kilku przypadków.

Wartość liczby $n(4)$ nie znam, ani też nie znam żadnej z liczb $n(k)$ dla $k \geq 4$. Z przytoczonego wyżej twierdzenia wynika tylko, że $n(k) \leq 3^{(k+1)!}$, więc w szczególności $n(3) \leq 3^{24}$. Podobnie wynika stąd, że $n(2) \geq 3^6$, ale wiemy, że $n(2) = 3^2$, zaś $n(3) = 24$.

Do addytywnej teorii liczb należy też zagadnienie tak zwanych kwadratów magicznych. Kwadratem magicznym nazywamy ustawienie liczb $1, 2, \dots, n^2$ w kwadrat, tak aby suma każdego wiersza, suma każdej kolumny i suma każdej z dwóch przekątnych głównych były równe. Jak łatwo obliczyć, każda z tych sum musi wtedy być równa liczbie $1/2 n (n^2 + 1)$.

Przypadek $n = 1$ jest trywialny. Dla $n = 2$, jak łatwo się przekonać, nie ma kwadratu magicznego.

Dla $n = 3$ mamy tylko jeden kwadrat magiczny, jeżeli nie uważać za różne tych, które powstają z danego przez obrót lub symetryczne odbicie. Jest to kwadrat:

| | | |
|---|---|---|
| 8 | 1 | 6 |
| 3 | 5 | 7 |
| 4 | 9 | 2 |

Ten kwadrat magiczny (w którym suma liczb każdego wiersza, suma liczb każdej kolumny i suma liczb każdej z dwóch przekątnych głównych wynosi 15) był znany już w starożytności.

Frenicle w XVI wieku obliczył, że dla $n = 4$ istnieje 880 różnych kwadratów magicznych.

Oto kilka z nich:

| | | | |
|----|----|----|----|
| 16 | 3 | 2 | 13 |
| 5 | 10 | 11 | 8 |
| 9 | 6 | 7 | 12 |
| 4 | 15 | 14 | 1 |

| | | | |
|----|----|----|----|
| 10 | 5 | 11 | 8 |
| 3 | 16 | 2 | 13 |
| 6 | 9 | 7 | 12 |
| 15 | 4 | 14 | 1 |

| | | | |
|----|----|----|----|
| 1 | 15 | 10 | 8 |
| 14 | 4 | 5 | 11 |
| 7 | 9 | 16 | 2 |
| 12 | 6 | 3 | 13 |

| | | | |
|----|----|----|----|
| 4 | 10 | 15 | 5 |
| 7 | 13 | 12 | 2 |
| 14 | 8 | 1 | 11 |
| 9 | 3 | 6 | 16 |

| | | | |
|----|----|----|----|
| 2 | 13 | 8 | 11 |
| 12 | 7 | 14 | 1 |
| 15 | 4 | 9 | 6 |
| 5 | 10 | 3 | 16 |

| | | | |
|----|----|----|----|
| 1 | 14 | 15 | 4 |
| 12 | 7 | 6 | 9 |
| 8 | 11 | 10 | 5 |
| 13 | 2 | 3 | 16 |

Dla $n = 5$ według Mac Mahona można zbudować około 60 000 różnych kwadratów magicznych.

Oto jeden z nich:

| | | | | |
|----|----|----|----|----|
| 17 | 24 | 1 | 8 | 15 |
| 23 | 5 | 7 | 14 | 16 |
| 4 | 6 | 13 | 20 | 22 |
| 10 | 12 | 19 | 21 | 3 |
| 11 | 18 | 25 | 2 | 9 |

A oto jeszcze kwadrat magiczny dla $n = 6$:

| | | | | | |
|----|----|----|----|----|----|
| 1 | 35 | 4 | 33 | 32 | 6 |
| 25 | 11 | 9 | 28 | 8 | 30 |
| 24 | 14 | 18 | 16 | 17 | 22 |
| 13 | 23 | 19 | 21 | 20 | 15 |
| 12 | 26 | 27 | 10 | 29 | 7 |
| 36 | 2 | 34 | 3 | 5 | 31 |

W X VI wieku Michał Stiffel budował kwadraty magiczne o n^2 elementach takie, że jeżeli przy dowolnym naturalnym $k \leq n-3/2$ usuniemy z nich k pierwszych wierszy górnych, k ostatnich wierszy dolnych i k pierwszych lewych kolumn i k ostatnich prawych kolumn, to otrzymamy kwadrat o $(n-2k)^2$ elementach taki, że jeżeli od każdego z tych elementów odejmiemy pewną stałą liczbę, to otrzymamy kwadrat magiczny o $(n - 2k)^2$ elementach. Oto kwadrat magiczny Stiffela o 9 wierszach:

| | | | | | | | | |
|----|----|----|----|----|----|----|----|----|
| 16 | 81 | 79 | 77 | 75 | 11 | 13 | 15 | 2 |
| 78 | 28 | 65 | 63 | 61 | 25 | 27 | 18 | 4 |
| 76 | 62 | 36 | 53 | 51 | 35 | 30 | 20 | 6 |
| 74 | 60 | 50 | 40 | 45 | 38 | 32 | 22 | 8 |
| 9 | 23 | 33 | 39 | 41 | 43 | 49 | 59 | 73 |
| 10 | 24 | 34 | 44 | 37 | 42 | 48 | 58 | 72 |
| 12 | 26 | 52 | 29 | 31 | 47 | 46 | 56 | 70 |
| 14 | 64 | 17 | 19 | 21 | 57 | 55 | 54 | 68 |
| 80 | 1 | 3 | 5 | 7 | 71 | 69 | 67 | 66 |

Usuając tu skrajne wiersze i kolumny otrzymamy kwadrat utworzony z siedmiu wierszy i tyłuż kolumn; odejmując od każdej z liczb tego kwadratu liczbę 16 otrzymamy kwadrat magiczny o siedmiu wierszach. Usuając zaś z naszego kwadratu dwa skrajne wiersze górne i dwa skrajne dolne, jako też dwie skrajne kolumny lewe i dwie skrajne prawe, otrzymamy kwadrat taki, że odejmując od każdego jego elementu liczbę 28 otrzymamy kwadrat magiczny o pięciu wierszach. Gdybyśmy wreszcie usunęli z naszego kwadratu o dziewięciu wierszach po trzy skrajne wiersze z góry i z dołu i po trzy skrajne kolumny z lewej i prawej strony, otrzymamy kwadrat z dziewięciu elementami, a odejmując od każdego z nich liczbę 36, otrzymamy kwadrat magiczny o trzech wierszach. Udowodniono, że istnieją kwadraty magiczne Stiffela o dowolnej > 4 liczbie wierszy, ale dowód jest trudny. W roku 1742 Ch. Goldbach wyraził przypuszczenie, że każda liczba parzysta większa od 4 jest sumą dwóch liczb pierwszych nieparzystych. Przypuszczenie to zostało sprawdzone dla liczb parzystych < 100000 , ogólnego dowodu jednak dotąd nie znaleziono. Na przykład $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7 = 5 + 5$, $12 = 5 + 7$, $14 = 7 + 7$, $16 = 3 + 13 = 5 + 11$. Liczba 100 daje aż 6 rozkładów na sumę dwóch liczb pierwszych (jeżeli nie zwracać uwagi na porządek składników): $100 = 3 + 97 = 11 + 89 = 17 + 83 = 29 + 71 = 41 + 59 = 47 + 53$. Liczba 1000 daje 28 takich rozkładów. Udowodniono, że z liczb parzystych ≤ 1000 największą liczbę takich rozkładów, mianowicie 52, daje liczba 990. Istnieje przypuszczenie, że liczba rozkładów liczby parzystej $2n$ na sumę dwóch liczb pierwszych wzrasta nieograniczenie wraz z n .

Udowodniono natomiast twierdzenie słabsze, że dla każdej liczby naturalnej s istnieje liczba parzysta, dająca więcej niż s różnych rozkładów na sumę dwóch liczb pierwszych.

Z przypuszczenia Goldbacha wynika z łatwością twierdzenie Czebyszewa: dla każdej liczby naturalnej $n > 1$ między n i $2n$ leży co najmniej jedna liczba pierwsza. W samej rzeczy, jeżeli n jest liczbą naturalną > 1 , to w myśl przypuszczenia Goldbacha, $2n + 2$ jako liczba parzysta > 4 jest sumą dwóch liczb pierwszych nieparzystych, $2n + 2 = p + q$, i możemy założyć, że $3 \leq p \leq q$ skąd $q < 2n$ oraz $2n + 2 \leq 2q$, zatem $q > n$. Liczba q jest więc liczbą pierwszą, zawartą między n i $2n$.

Przypuszczenia Goldbacha dotąd nie udowodniono, natomiast istnieją dowody elementarne (choć dość skomplikowane) twierdzenia Czebyszewa. Można nawet dowiedzieć, że liczba liczb pierwszych zawartych między n i $2n$ wzrasta nieograniczenie wraz z n . Nie wiadomo, czy każda liczba parzysta jest różnicą dwóch liczb pierwszych. (Mamy na przykład $2 = 5 - 3$, $4 = 11 - 7$, $6 = 29 - 23$, $8 = 97 - 89$, $10 = 149 - 139$.) Wyrażono przypuszczenie, że każda liczba parzysta daje się przedstawić nieskończenie wieloma sposobami jako różnica dwóch liczb pierwszych. Dla liczb 2, 4, 6 łatwo na przykład podać po 10 takich rozkładów:

$2 = 5 - 3 = 7 - 5 = 13 - 11 = 19 - 17 = 31 - 29 = 43 - 41 = 61 - 59 = 73 - 71 = 103 - 101 = 139 - 137$,
 $4 = 7 - 3 = 11 - 7 = 17 - 13 = 23 - 19 = 41 - 37 = 47 - 43 = 71 - 67 = 83 - 79 = 107 - 103 = 113 - 109$,
 $6 = 11 - 5 = 19 - 13 = 23 - 17 = 29 - 23 = 37 - 31 = 47 - 41 = 53 - 47 = 59 - 53 = 67 - 61 = 73 - 67$.

Przeszło sto lat temu wyrażono też mocniejsze przypuszczenie, że każda liczba parzysta daje się na nieskończenie wiele sposobów przedstawić jako różnica kolejnych liczb pierwszych. Przypuszczenie to nie zostało dotąd udowodnione ani też obalone. Dla liczby 2 jest ono równoważne przypuszczeniu, że istnieje nieskończenie wiele par liczb pierwszych bliźniaczych, tj. liczb pierwszych p , dla których liczba $p + 2$ też jest pierwszą. Największą znaną parę liczb bliźniaczych otrzymujemy dla $p = 1000000009649$. Łatwo jest dowiedzieć, że jeżeli liczby $p > 3$ i $p + 2$ są obie pierwsze, to liczba p przy dzieleniu przez 6 musi dawać resztę 5, zaś jeżeli $p > 5$, to przy dzieleniu liczby p przez 10 resztą jej musi być jedna z trzech liczb: 1, 7 lub 9. Tak więc pary liczb pierwszych bliźniaczych (poza parami 3 i 5 oraz 5 i 7) możemy podzielić na trzy klasy, zależnie od tego, czy ostatnią cyfrą mniejszej z tych liczb jest 1, 7 czy też 9. Na przykład do pierwszej klasy należą pary liczb bliźniaczych 11 i 13, 41 i 43, 71 i 73, 101 i 103, 311 i 313, 521 i 523; do drugiej klasy należą pary 17 i 19, 107 i 109, 137 i 139, 197 i 199, 227 i 229, 617 i 619; do trzeciej klasy należą pary 29 i 31, 59 i 61, 179 i 181, 239 i 241, 269 i 271, 419 i 421. Istnieje przypuszczenie, że w każdej z tych trzech klas mamy nieskończenie wiele par liczb pierwszych bliźniaczych.

Wyrażono też przypuszczenie, że istnieje nieskończenie wiele trójek liczb pierwszych postaci $(p, p + 2, p + 6)$, jak na przykład $(5, 7, 11)$, $(11, 13, 17)$ albo $(17, 19, 23)$ jako też trójek postaci $(p, p + 4, p + 6)$, jak na przykład $(7, 11, 13)$, $(13, 17, 19)$ albo $(37, 41, 43)$, a wreszcie czwórek postaci $(p, p + 2, p + 6, p + 8)$, jak $(11, 13, 17, 19)$ lub $(191, 193, 197, 199)$.

Gdyby przypuszczenie Goldbacha było prawdziwe, to, jak łatwo stwierdzić, prawdziwe byłoby też przypuszczenie, że każda liczba nieparzysta > 7 jest sumą trzech liczb pierwszych nieparzystych (i to takich, z których co najmniej jedną jest 3). Czy tak jest, dotąd nie wiemy, ale w 1937 r. I. Winogradow dowiódł, że każda dostatecznie wielka liczba nieparzysta jest sumą trzech liczb pierwszych nieparzystych. Udowodniono, że każda liczba naturalna > 11 jest sumą dwóch lub więcej różnych liczb pierwszych. Na przykład $12 = 5 + 7$, $13 = 2 + 11$, $14 = 3 + 11$, $15 = 2 + 13$, $16 = 3 + 13$, $17 = 2 + 3 + 5 + 7$, $23 = 5 + 7 + 11$, $25 = 3 + 5 + 19$, $29 = 3 + 7 + 19$.

Nie wiadomo, czy każda liczba parzysta > 6 jest sumą dwóch różnych liczb pierwszych. Gdyby tak było, to, jak można dowiedzieć, stąd wynikałoby, że każda liczba naturalna > 17 jest sumą trzech różnych liczb pierwszych. Co do liczby 17, to łatwo dowiedzieć, że nie jest ona sumą dwóch ani też trzech różnych liczb pierwszych. W ostatnich latach zajmowano się liczbą $P(n)$ rozkładów liczby naturalnej n na sumę liczb pierwszych, gdzie nie uważamy za różne rozkładów, różniących się tylko porządkiem składników. Mamy tu oczywiście $P(1) = 0$, $P(2) = P(3) = P(4) = 1$, lecz już $P(5) = 2$ (gdyż 5 daje dwa takie rozkłady: $5 = 5$ oraz $5 = 2 + 3$), $P(6) = 2$ (gdyż 6 daje rozkłady $6 = 3 + 3$ i $6 = 2 + 2 + 2$), $P(7) = 3$ (gdyż $7 = 7$, $7 = 2 + 5$ i $7 = 2 + 2 + 3$), $P(8) = 3$ (gdyż $8 = 3 + 5 = 2 + 3 + 3 = 2 + 2 + 2 + 2$), $P(9) = 4$ (gdyż $9 = 2 + 7 = 2 + 2 + 5 = 3 + 3 + 3 = 2 + 2 + 2 + 3$), $P(10) = 5$ (gdyż 10

$= 3 + 7 = 5 + 5 = 2 + 3 + 5 = 2 + 2 + 3 = 2 + 2 + 2 + 2 + 2$). P. T. B a t e m a n i P. Erdős dowiedli, że dla naturalnych n mamy zawsze $P(n+1) \geq P(n)$ oraz że różnica $P(n+1) - P(n)$ zmierza do nieskończoności wraz z n . Dowody tych twierdzeń nie są łatwe, Łatwo natomiast jest dowieść, że $P(n+2) \geq P(n)$ dla naturalnych n , oraz że $P(n)$ zmierza do nieskończoności wraz z n . Znany historyk matematyki Moritz C a n t o r wypowiedział w 1861 r. przypuszczenie, że trzy kolejne liczby pierwsze, z których żadna nie jest liczbą 3, nie mogą tworzyć postępu arytmetycznego. Przypuszczenie to było powtarzane przez innych matematyków i dopiero w 1956 roku Andrzej Schinzel zwrócił uwagę na to, że jest ono błędne, gdyż 47, 53 i 59 są kolejnymi liczbami pierwszymi, tworzącymi postęp arytmetyczny o różnicy 6. Inną taką trójką liczb pierwszych jest 151, 157, 163. Znamy też postęp arytmetyczny utworzony z czterech kolejnych liczb pierwszych: 251, 257, 263, 269. Wbrew przypuszczeniu Cantora można by wyrazić przypuszczenie, że istnieje nieskończenie wiele trójek kolejnych liczb pierwszych, dających postęp arytmetyczny. Znamy postęp arytmetyczny, utworzony z dziesięciu liczb pierwszych, na przykład postęp $199 + 210k$, gdzie $k = 0, 1, 2, \dots, 9$. Nie wiemy natomiast, czy istnieje postęp arytmetyczny utworzony ze stu liczb pierwszych. Można dowieść, że gdyby taki postęp istniał, to różnica jego wyrazów byłaby liczbą o co najmniej kilkudziesięciu cyfrach (w układzie dziesiętnym). Udowodniono, że istnieje nieskończenie wiele postępów arytmetycznych trójwyrazowych, utworzonych z różnych liczb pierwszych. Pytanie czy takich postępów jest nieskończenie wiele, jest, jak łatwo zauważyć, równoważne pytaniu, czy równanie $p + r = 2q$ ma nieskończenie wiele rozwiązań w liczbach pierwszych p, q, r , gdzie $p \neq r$. Oto przykłady takich postępów o pierwszym wyrazie 3: 3, 7, 11; 3, 11, 19; 3, 13, 23; 3, 17, 31; 3, 23, 43; 3, 31, 59; 3, 37, 71; 3, 41, 79; 3, 43, 83; 3, 53, 103. Nie wiemy natomiast, czy równanie $p + r = q$ ma nieskończenie wiele rozwiązań w liczbach pierwszych p, q, r . Znamy jednak dużo takich rozwiązań, na przykład $2 + 3 = 5$, $2 + 11 = 13$, $2 + 71 = 73$. Natomiast można dowieść, że równanie $p + q + r = s$ ma nieskończenie wiele rozwiązań w liczbach pierwszych p, q, r, s , ale dowód jest trudny. Oto przykłady takich rozwiązań: $2 + 2 + 3 = 7$, $2 + 2 + 7 = 11$, $3 + 5 + 11 = 19$, $3 + 3 + 23 = 29$, $7 + 11 + 13 = 31$. Nie wiemy, czy istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + 1$, gdzie x jest liczbą naturalną. (Spośród liczb pierwszych ≤ 1000 takimi są liczby 2, 5, 17, 37, 101, 197, 257, 401, 577 i 677.) Nie wiemy też, czy istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + y^2 + 1$, gdzie x i y są liczbami naturalnymi. (Spośród liczb pierwszych 100 takimi są liczby $3 = 1^2 + 1^2 + 1$, $11 = 1^2 + 3^2 + 1$, $19 = 3^2 + 3^2 + 1$, $41 = 2^2 + 6^2 + 1$, $53 = 4^2 + 6^2 + 1$, $73 = 6^2 + 6^2 + 1$ i $83 = 1^2 + 9^2 + 1$). Natomiast można dowieść, chociaż nie jest to łatwe, że istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + y^2 + z^2 + 1$, gdzie x, y i z są liczbami naturalnymi. (W szczególności takimi są wszystkie liczby pierwsze postaci $8k + 7$.) Co się tyczy liczb pierwszych postaci $x^2 + 1$, to L. Euler dał tablice takich liczb dla $x \leq 1500$, zaś W. A. G o ł u b i e w dla $x \leq 3500$, prostując przy tym kilka błędów w tablicy Eulera (który na przykład pominął liczbę pierwszą $1080^2 + 1$, podając mylnie, że jest ona złożoną, podzielną przez 773, przez którą to liczbę jest podzielna liczba $1090^2 + 1$. Euler zaliczył też błędnie do liczb pierwszych liczbę $1234^2 + 1 = 1522757$, podzielną przez 421). Dla $x \leq 1000$, jak obliczył Gołubiew, mamy 110 liczb pierwszych postaci $x^2 + 1$; dla $x \leq 2000$ mamy 207 takich liczb, dla $x \leq 3000$ mamy ich 301, dla $x \leq 3500$ jest ich 342.

CZEŚĆ DRUGA

ZAGADNIENIA DOTYCZĄCE PODZIELNOŚCI LICZB CAŁKOWITYCH

Jeżeli chodzi o mnożenie liczb, w której mamy do czynienia z mnożeniem liczb i jego działaniem odwrotnym, dzieleniem, to pewne trudności napotykamy tu już na początku. O ile bowiem działanie odwrotne do dodawania, tj. odejmowanie, było w sferze liczb całkowitych zawsze wykonalne, to działanie odwrotne do mnożenia, czyli dzielenie, nie zawsze jest w sferze liczb całkowitych wykonalne. Wynikiem dzielenia liczby a przez liczbę b nazywamy każdą liczbę c taką iż $a = bc$. Wynik dzielenia liczby całkowitej a przez liczbę całkowitą b może nie istnieć (gdy a

nie jest zerem, zaś b jest zerem); może być dowolną liczbą (jeżeli $a = 0$ i $b = 0$) i wreszcie może być określoną liczbą, ale niekoniecznie całkowitą. W tym i tylko w tym przypadku, gdy dla danych liczb całkowitych a i b istnieje liczba całkowita c , taka iż $a = bc$, nazywamy liczbę b dzielnikiem liczby a i mówimy, że liczba a jest podzielna (bez reszty) przez liczbę b . Na piśmie wyrażamy to wzorem

$$b|a$$

co czytamy: b jest dzielnikiem a .

Łatwo dowieść, że jeżeli x , y i z są liczbami całkowitymi i jeżeli $x|y$ jako też $y|z$, to $x|z$. Jeżeli bowiem $x|y$, to istnieje liczba całkowita t taka iż $y = xt$; jeżeli zaś $y|z$, to istnieje liczba całkowita u taka iż $z = yu$. Stąd $z = (xt)u = x(tu)$, a więc z jest iloczynem liczby x przez liczbę całkowitą tu , zatem $x|z$, c.b.d.o

Zatem: dzielnik dzielnika liczby całkowitej jest jej dzielnikiem. Dla danych liczb całkowitych a i b arytmetyka daje nam sposoby przekonania się, czy b jest dzielnikiem liczby a , czy też nie.

Trudniejsza jest sprawa, gdy chodzi o znalezienie wszystkich dzielników danej liczby całkowitej. W tym przypadku wystarczy znaleźć wszystkie dzielniki naturalne liczby a , gdyż z równoważności wzorów $a = bc$ i $a = (-b) \cdot (-c)$ wynika natychmiast, że jeżeli liczba b jest dzielnikiem liczby a , to i liczba $-b$ jest dzielnikiem liczby a . Dzielniki liczby całkowitej różnej od zera rozpadają się więc na pary dzielników różniących się tylko znakiem. (Dla liczby 0 oczywiście każda liczba całkowita jest jej dzielnikiem.) Jasne jest też, że liczby a i $-a$ mają te same dzielniki. Wystarczy więc znajdowanie dzielników naturalnych liczb naturalnych. Teoretycznie wystarczy tu dzielić kolejno daną liczbę naturalną n przez liczby $1, 2, 3, \dots, n$ i wypisać te z tych liczb, przez które dzielenie wypadnie bez reszty. Tę liczbę n dzielić można nawet zmniejszyć. Jeżeli bowiem d jest dzielnikiem naturalnym liczby naturalnej n , to iloraz $n : d$ jest liczbą naturalną d' , i mamy $n = dd'$, skąd wynika, że d' też jest dzielnikiem naturalnym liczby n ; nazywamy go dzielnikiem dopełniającym dla dzielnika d liczby n . Oczywiście dzielnikiem dopełniającym dla dzielnika d' będzie dzielnik d . W ten sposób dzielniki naturalne liczby n rozpadają się na pary dzielników wzajemnie się dopełniających. Nie zawsze jednak dzielnik dopełniający dla dzielnika d liczby n jest różny od dzielnika d . Jeżeli $d' = d$, to wobec $n = dd'$ mamy $n = d^2$, co dowodzi, że n jest kwadratem liczby naturalnej. Na odwrót, jeżeli n jest kwadratem liczby naturalnej, to n ma wśród swych dzielników taki, który jest równy swemu dopełniającemu. Dzielnik d liczby n i jego dopełniający d' nie mogą być oba większe od \sqrt{n} , gdyż wtedy byłoby $dd' > \sqrt{n} * \sqrt{n} = n$, wbrew równaniu $dd' = n$. Podobnie wnosimy, że dzielnik d liczby n i jego dopełniający d' nie mogą być oba mniejsze od \sqrt{n} . Zatem z dwóch dopełniających się dzielników liczby n jeden jest zawsze $\leq \sqrt{n}$, a drugi $\geq \sqrt{n}$. Dla otrzymania wszystkich dzielników naturalnych liczby naturalnej n wystarczy więc wyznaczyć wszystkie dzielniki naturalne liczby n nie większe od \sqrt{n} , a potem dopisać do nich ich dopełniające, pamiętając o tym, że jeżeli n jest kwadratem liczby naturalnej d , to w ten sposób dzielnik d byłby wypisany dwukrotnie (jako dzielnik $= \sqrt{n}$ i jako swój dopełniający). Wynika stąd też natychmiast, że liczby kwadratowe, i tylko takie liczby, mają nieparzystą liczbę dzielników naturalnych. Przypuśćmy na przykład, że chcemy wypisać wszystkie dzielniki naturalne liczby 60. Ponieważ $7 < \sqrt{60} < 8$, więc wystarczy wypisać wszystkie dzielniki naturalne liczby 60 nie większe od 7, a więc liczby 1, 2, 3, 4, 5 i 6 i dopisać dzielniki dopełniające, czyli liczby 60, 30, 20, 15, 12 i 10. W ten sposób liczba 60 ma 12 dzielników naturalnych: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 i 60.

Przypuśćmy teraz, że chcemy wypisać wszystkie dzielniki naturalne liczby 100. Ponieważ $\sqrt{100} = 10$ i 100 jest liczbą kwadratową, więc wystarczy wypisać wszystkie dzielniki naturalne liczby 100 nie większe od 10, tj. liczby 1, 2, 4, 5, 10, a następnie dopisać dzielniki dopełniające dla nich, z pominięciem dzielnika 10, a więc dopisać tylko liczby 100, 50, 25 i 20. W ten sposób liczba 100 ma 9 dzielników naturalnych: 1, 2, 4, 5, 10, 20, 25, 50 i 100.

Postępowanie to, teoretycznie bardzo proste, może się jednak w praktyce okazać uciążliwym, albo nawet technicznie niewykonalnym, gdy n jest wielką liczbą. Na przykład nie potrafimy wypisać wszystkich dzielników naturalnych liczby $n = 2^{101} - 1$, mającej 31 cyfr. Oczywiście potrafimy wypisać dwa dzielniki tej liczby: 1 i n , ale ciekawą jest rzeczą, że udowodniono, iż nasza liczba n ma oprócz tych dwóch dzielników jeszcze inne, których jednak nie potrafimy wypisać ani nawet

podać, ile ich jest. Później wyjaśnimy, jak to mogą zachodzić podobne sytuacje. Podobnie jest z liczbą $2^{128} + 1$. Natomiast co do liczby

$$2^{2^u} + 1$$

to nie wiemy, czy ma ona jeszcze inne dzielniki naturalne poza dwoma oczywistymi. Są jednak liczby wielocyfrowe, których wszystkie dzielniki potrafimy wypisać. Ma przykład wszystkimi dzielnikami naturalnymi liczby 2^{102} są liczby 1, 2, 22, 23, ..., 2^{101} , 2^{102} (jest ich więc 103). A oto w jaki sposób mając daną liczbę naturalną n można by obliczać liczbę dzielników kolejnych liczb naturalnych od 1 do n . Wypiszmy kolejne liczby naturalne od 1 do n . Liczba 1 jest dzielnikiem każdej liczby naturalnej: każdą więc z naszych liczb podkreślmy raz. Liczba 2 jest dzielnikiem liczb parzystych, i tylko takich: podkreślmy więc jeszcze raz każdą liczbę parzystą. Podkreślmy także jeszcze raz liczbę 3 i każdą co trzecią liczbę licząc od niej, następnie podkreślmy jeszcze raz liczbę 4 i dalej każdą co czwartą liczbę itd., aż dojdziemy do liczby n . Jasną jest rzeczą, że każda liczba naszego ciągu 1, 2, ..., n będzie miała tyle dzielników naturalnych, ile razy została podkreślona. Oto na przykład dla $n = 50$ wynik naszych czynności będzie wyglądał następująco:



Daje nam to możliwość ułożenia dla liczb naturalnych $n \leq 50$ tabliczki liczb $\Theta(n)$, gdzie $\Theta(n)$ oznacza liczbę dzielników naturalnych liczby n :

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|----|---|
| 0 | | 1 | 2 | 2 | 3 | 2 | 4 | 2 | 4 | 3 |
| 1 | 4 | 2 | 6 | 2 | 4 | 4 | 5 | 2 | 6 | 2 |
| 2 | 6 | 4 | 4 | 2 | 8 | 3 | 4 | 4 | 6 | 2 |
| 3 | 8 | 2 | 6 | 4 | 4 | 4 | 9 | 2 | 4 | 4 |
| 4 | 8 | 2 | 8 | 2 | 6 | 6 | 4 | 2 | 10 | 3 |
| 5 | 6 | | | | | | | | | |

Już ta mała tabliczka pozwala wysnuć pewne wnioski i przypuszczenia co do liczb $\Theta(n)$, a także nasuwa pewne pytania, z których nie na wszystkie potrafimy odpowiedzieć. Przede wszystkim już z naszej tabliczki widać, że bieg liczb $\Theta(n)$ dla $n = 1, 2, \dots$ (czyli bieg tak zwanej funkcji liczbowej $\Theta(n)$) jest nader nieprzewidywalny. Tak na przykład po wartości $\Theta(3) = 2$ następuje większa wartość $\Theta(4) = 3$, ale po niej znów mniejsza wartość $\Theta(5) = 2$, po której znów następuje większa wartość $\Theta(6) = 4$, a po niej znów mniejsza wartość $\Theta(7) = 2$, po niej większa $\Theta(8) = 4$, po niej znów mniejsza $\Theta(9) = 3$, po niej większa $\Theta(10) = 4$, po niej mniejsza $\Theta(11) = 2$, po niej większa $\Theta(12) = 6$, po niej znów mniejsza $\Theta(13) = 2$. Ale błędnym byłoby przypuszczenie, że tak będzie wciąż dalej na przemian: po większej wartości mniejsza, a po niej znów większa. Spotkamy tu obok siebie stojące liczby naturalne, mające jednakową liczbę dzielników: na przykład 2 i 3 (gdyż $\Theta(2) = \Theta(3) = 2$) albo 14 i 15 (gdyż $\Theta(14) = \Theta(15) = 4$), 21 i 22 (gdyż $\Theta(21) = \Theta(22) = 4$), 38 i 39 (gdyż $\Theta(38) = \Theta(39) = 4$), 44 i 45 (gdyż $\Theta(44) = \Theta(45) = 6$).

Nasuwa się pytanie, czy takich liczb n , dla których $\Theta(n) = \Theta(n + 1)$, jest nieskończenie wiele. Na to pytanie nie potrafimy dać odpowiedzi. Wypowiedziano natomiast przypuszczenie, że istnieje dowolna ilość kolejnych liczb naturalnych mających jednakową liczbę dzielników. Z tablicy naszej

wnosimy, że trzema takimi kolejnymi liczbami są 33, 34 i 35 (gdyż $\Theta(33) = \Theta(34) = \Theta(35) = 4$). Mamy też $\Theta(242) = \Theta(243) = \Theta(244) = \Theta(245) = 6$ oraz $\Theta(n) = \Theta(n + 1) = \Theta(n + 2) = \Theta(n + 3) = \Theta(n + 4) = 8$ dla $n = 40311$ i dla $n = 99655$ (jak znalazł J. M y c i e l s k i). W tabliczce naszej nie ma trzech kolejnych wyrazów rosnących; istnieje jednak i więcej takich wyrazów dla $n > 50$, na przykład mamy $\Theta(61) < \Theta(62) < \Theta(63) < \Theta(64)$, gdyż $\Theta(61) = 2$, $\Theta(62) = 4$, $\Theta(63) = 6$, $\Theta(64) = 7$. Istnieją natomiast w naszej tabliczce trzy kolejne wyrazy malejące, gdyż $\Theta(45) > \Theta(46) > \Theta(47)$. Trudniejsze byłoby pytanie, czy istnieje nieskończenie wiele liczb naturalnych n takich iż $\Theta(n) < \Theta(n + 1) < \Theta(n + 2)$, albo takich iż $\Theta(n) > \Theta(n + 1) > \Theta(n + 2)$. Nasuwają się tu inne pytania podobne, na przykład, czy istnieje nieskończenie wiele liczb naturalnych n takich iż $\Theta(n) < \Theta(n + 1) > \Theta(n + 2)$, albo czy dla każdej liczby naturalnej s istnieje liczba naturalna n taka iż $\Theta(n) < \Theta(n + 1) < \dots < \Theta(n + s)$. Zagadnienia te są przeważnie trudne. Do pewnych z tych zagadnień jeszcze później powrócimy. Istnieją tablice dające wartości $\Theta(n)$ dla $n < 10000$. Tablice te zostały wydane w 1940 r. w Cambridge (Anglia) pt. J. W. L. Glaisher Number-divisor Tables (stron X + 100).

Łatwo dowieść, że $\Theta(n) = 1$ tylko dla $n = 1$. Jeżeli bowiem liczba naturalna n jest > 1 , to ma co najmniej dwa różne dzielniki, 1 i n , zatem $\Theta(n) \geq 2$ dla $n > 1$. Liczby naturalne n , dla których $\Theta(n) = 2$ nazywamy liczbami pierwszymi. Są to więc liczby naturalne większe od jednośc, nie mające innych dzielników naturalnych prócz jednośc i samych siebie. Liczby 1 nie zaliczamy do liczb pierwszych. Czynili to wprawdzie niektórzy dawniejsi matematycy, ale okazało się to niewygodne, gdyż komplikowało wysłowienie wielu ważnych twierdzeń. Jak wynika z podanej wyżej tabliczki funkcji $\Theta(n)$, wszystkimi liczbami pierwszymi < 50 są liczby 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 i 47. Nasuwa się pytanie, czy liczb pierwszych jest nieskończenie wiele, innymi słowy, czy dla każdej liczby naturalnej n istnieje liczba pierwsza od niej większa?

Aby tego dowieść, zastanówmy się naprzód, co wynika z założenia, że dana liczba naturalna $n > 1$ nie jest pierwszą. Skoro $n > 1$, to, jak wiemy, mamy $\Theta(n) \geq 2$. Ale skoro liczba n nie jest pierwszą, to nie może być $\Theta(n) = 2$, zatem $\Theta(n) > 2$, czyli $\Theta(n) \geq 3$. Liczba n ma więc co najmniej trzy różne dzielniki naturalne, a więc w każdym razie ma dzielnik naturalny d różny od 1 i od n , zatem $1 < d < n$. Oznaczając dopełniający (do n) dzielnik dla d przed d' będziemy więc mieli $n = dd'$ i, wobec $1 < d < n$, wynika stąd, że również $1 < d' < n$. Tak więc n jest iloczynem dwóch liczb naturalnych d i d' , obu mniejszych od n . Dowiedliśmy więc, że jeżeli liczba naturalna > 1 nie jest pierwszą, to jest ona iloczynem dwóch liczb naturalnych od niej mniejszych. Takie liczby nazywamy złożonymi.

Jasną jest rzeczą, że na to, by liczba naturalna n była złożoną, potrzeba i wystarcza żeby było $\Theta(n) \geq 3$. Każda więc liczba naturalna > 1 jest albo pierwszą, albo złożoną. Niech teraz n oznacza jakąkolwiek liczbę naturalną > 1 . Ma ona więc co najmniej jeden dzielnik naturalny większy od 1, na przykład samo n . Oznaczmy przez p najmniejszy ze wszystkich większych od jednośc dzielników liczby n . Liczba p jest więc > 1 . Gdyby liczba p nie była pierwszą, byłaby złożoną, a więc stanowiłaby iloczyn dwóch liczb od niej mniejszych: $p = dd'$, gdzie $d' < p$, zatem $1 < d < p$. Lecz d jest oczywiście dzielnikiem liczby p , zatem i liczby n (gdyż p jest dzielnikiem liczby n), a więc d byłoby dzielnikiem liczby n większym od 1, a mniejszym od p , wbrew definicji liczby p . Założenie, że liczba p nie jest pierwszą, doprowadza zatem do sprzeczności. Liczba p jest więc pierwszą. Dowiedliśmy w ten sposób, że jeżeli n jest liczbą naturalną > 1 , to najmniejszy ze wszystkich większych od jednośc dzielników liczby n jest liczbą pierwszą. Wynika stąd natychmiast, że każda liczba naturalna > 1 ma co najmniej jeden dzielnik pierwszy. Niech teraz n oznacza jakąkolwiek liczbę naturalną. Liczba $m = n! + 1$ (gdzie $n!$ oznacza iloczyn 1, 2 ... n) jest oczywiście > 1 , a więc ma dzielnik pierwszy p . Liczba p nie może być żadną z liczb 1, 2, 3, ..., n , gdyż przy dzieleniu liczby m przez każdą z nich otrzymujemy oczywiście resztę 1, a więc nie są one dzielnikami liczby m (która jest > 1). Musi więc być $p > n$. Dowiedliśmy zatem, że dla każdej liczby naturalnej n istnieje liczba pierwsza p większa od n . Wynika stąd, że liczb pierwszych jest nieskończenie wiele. Z liczb $n! + 1$ dla naturalnych $n < 26$ pierwszymi są tylko cztery, dla $n = 1, 2, 3$ i 11. O liczbie $27! + 1$ nie wiemy, czy jest pierwszą, czy nie. Łatwo dowieść, że $n! > 10$ dla $n \geq 28$. Liczba $3!!! = 720!$ ma przeszło 1000 cyfr. W 1876 r. H. Brocard postawił pytanie, dla jakich wartości naturalnych n liczby $n! + 1$ są kwadratami liczb naturalnych. Pytaniem tym zajmowało się wielu matematyków. Dla $n < 1020$ znaleziono tylko trzy liczby n , dla których $n! + 1$ jest

kwadratem: są to liczby $n = 4, 5$ i 7 . (Mamy $4! + 1 = 5^2$, $5! + 1 = 11^2$, $7! + 1 = 71^2$.)

Liczby $n! - 1$ są dla $n \leq 22$ pierwsze tylko gdy $n = 3, 4, 6, 7, 12, 14$ i 20 . O liczbach $24! - 1$ i $25! - 1$ nie wiemy, czy są pierwsze, czy nie. Liczba $26! - 1$ jest złożoną, podzieloną przez 149 . O równaniu $x!y! = z!$ łatwo dowieść, że ma nieskończenie wiele rozwiązań w liczbach naturalnych x, y, z . Ma ono na przykład rozwiązanie $x = n, y = n! - 1, z = n!$, gdzie $n = 1, 2, \dots$ (więc $3!5! = 6!$, $4!23! = 24!$, $5!119! = 120!$ itd.). Z innych rozwiązań znamy tylko jedno: $6!7! = 10!$. Stąd, że każda liczba naturalna > 1 ma co najmniej jeden dzielnik pierwszy, wyprowadzamy z łatwością przez indukcję twierdzenie, że każda liczba naturalna > 1 jest iloczynem skończonej ilości liczb pierwszych (niekoniecznie różnych). Twierdzenie takie jest bowiem prawdziwe dla liczby 2 (iloczyn ma tu jeden tylko czynnik, 2). Przypuśćmy, że twierdzenie jest słuszne dla liczb naturalnych > 1 oraz mniejszych od liczby naturalnej $n > 2$. Liczba n ma dzielnik pierwszy p , skąd $n = mp$, gdzie m jest liczbą naturalną. Jeżeli $m = 1$, to $n = p$ i twierdzenie jest prawdziwe dla liczby n , jeżeli zaś $m > 1$, wobec $m = n/p < n$ twierdzenie jest prawdziwe dla liczby m , zatem m , a więc też $n = mp$ jest iloczynem skończonej liczby liczb pierwszych. Łatwo byłoby też dowieść przez indukcję, że każda liczba naturalna > 1 rozkłada się tylko w jeden sposób na czynniki pierwsze, jeżeli nie uważać za różne rozkładów, różniących się tylko porządkiem czynników. Teoretycznie znalezienie rozkładu danej liczby naturalnej n na czynniki pierwsze jest rzeczą prostą. Za pomocą kolejnych dzieleń liczby n przez liczby $2, 3, \dots, n$ znajdujemy najmniejszy z większych od jednośc dzielników liczby n : będzie to, jak wiemy, pewna liczba pierwsza q_1 i będzie $n = q_1 n_1$, gdzie n_1 jest liczbą naturalną mniejszą od n . Jeżeli $n = 1$, to będzie $n = q_1$ i rozkład liczby n na czynniki pierwsze będzie znaleziony (przy czym będziemy tu mieli tylko jeden czynnik). Jeżeli $n_1 > 1$, to z liczbą n_1 postępujemy, jak postąpiliśmy z liczbą n , co da nam $n_1 = q_2 n_2$, gdzie q_2 jest liczbą pierwszą, zaś n_2 liczbą naturalną $< n_1$. Rozumowanie to możemy powtarzać dalej, ale tylko skończoną liczbę razy, gdyż liczby naturalne n, n_1, n_2, \dots stale maleją. Musimy więc przy pewnym naturalnym s dojść do liczby $n_s = 1$, a wówczas równości $n = q_1 n_1, n_1 = q_2 n_2, \dots, n_{s-1} = q_s n_s$ dają rozkład liczby n na s czynników pierwszych: $n = q_1 q_2 \dots q_s$, przy czym, jak łatwo stwierdzić, będzie tu $q_1 \leq q_2 \leq \dots \leq q_s$. Tą drogą otrzymujemy więc rozkład każdej liczby naturalnej > 1 na iloczyn skończonej liczby czynników pierwszych nie malejących. Trudności mogą tu być tylko natury technicznej, jeżeli chodzi o rozkład wielkiej liczby, wymagający wielu dzieleń. Toteż istnieją liczby naturalne (oczywiście wielocyfrowe), których rozkłady na czynniki pierwsze nie zostały dotąd znalezione. Taką jest na przykład liczba $2^{101} - 1$, mająca 31 cyfr. Jeżeli w rozkładzie liczby naturalnej $n > 1$ na czynniki pierwsze iloczyn równych czynników będziemy przedstawiali jako potęgę jednego z nich, to rozwinięcie każdej liczby naturalnej $n > 1$ będziemy mogli przedstawić w postaci

$$(1) \quad n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$$

gdzie q_1, q_2, \dots, q_k są to różne liczby pierwsze, zaś liczba k oraz wykładniki $\alpha_1, \alpha_2, \dots, \alpha_k$ są naturalne. Jeżeli liczba naturalna d jest dzielnikiem liczby n , to każdy jej dzielnik pierwszy jest zarazem dzielnikiem liczby n i nie może wchodzić do rozwinięcia liczby d na czynniki pierwsze w wyższej potędze niż do rozwinięcia liczby n . Stąd łatwy wniosek, że

$$(2) \quad d = q_1^{\lambda_1} q_2^{\lambda_2} \dots q_k^{\lambda_k}$$

gdzie wykładnik $\lambda_1, \lambda_2, \dots, \lambda_k$ są całkowite nieujemne, odpowiednio nie większe od wykładników $\alpha_1, \alpha_2, \dots, \alpha_k$ czyli że są to liczby całkowite, spełniające nierówności

$$(3) \quad 0 \leq \lambda_1 \leq \alpha_1, 0 \leq \lambda_2 \leq \alpha_2, \dots, 0 \leq \lambda_k \leq \alpha_k$$

Zdrugiej strony jasną jest rzeczą, że obierając jako $\lambda_1, \lambda_2, \dots, \lambda_k$ dowolne liczby całkowite spełniające nierówności (3) i wyznaczając liczbę d ze wzoru (2), otrzymamy dzielnik liczby (1), gdyż będzie

$$n/d = q_1^{\alpha_1 - \lambda_1} q_2^{\alpha_2 - \lambda_2} \dots q_k^{\alpha_k - \lambda_k}$$

a wykładniki $\alpha_1 - \lambda_1, \alpha_2 - \lambda_2, \dots, \alpha_k - \lambda_k$ są tu wszystkie liczbami całkowitymi nieujemnymi

A więc wszystkie dzielniki naturalne liczby n są zawarte we wzorze (2), gdzie $\lambda_1, \lambda_2, \dots, \lambda_k$ są liczbami całkowitymi spełniającymi nierówności (3). Ponieważ liczba λ_1 może tu przyjmować $\alpha_1 + 1$ wartości

0, 1, 2, ..., α_1 (podobnie liczba λ_2 może tu przyjmować α_2+1 wartości itd., wreszcie liczba λ_k może przyjmować α_k+1 wartości, więc kombinując z sobą dowolnie te wartości otrzymujemy $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$ układów liczb $\lambda_1, \lambda_2, \dots, \lambda_k$, spełniających nierówności (3). Wnosimy stąd, że jeżeli liczba naturalna n daje rozwinięcie (1) na czynniki pierwsze, to

$$\Theta(n) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$$

W szczególności wynika stąd, że jeżeli $n = p^{m-1}$, gdzie p jest liczbą pierwszą, zaś m liczbą naturalną > 1 , to $\Theta(n) = m$. Ponieważ liczb pierwszych jest nieskończenie wiele, wynika stąd natychmiast, że dla każdej liczby naturalnej $m > 1$ równanie $\Theta(x) = m$ ma nieskończenie wiele rozwiązań w liczbach naturalnych x . Znalezienie najmniejszej liczby naturalnej n , mającej daną liczbę m dzielników, na ogół nie jest rzeczą łatwą. Łatwe to jest w przypadku, gdy m jest liczbą pierwszą: można dowieść, że wówczas najmniejszą liczbą naturalną, mającą m dzielników jest liczba 2^{m-1} . Łatwo też dowieść, że jeżeli m jest iloczynem dwóch różnych liczb pierwszych p i q , gdzie $p < q$, to najmniejszą liczbą naturalną, mającą m dzielników jest $2^{q-1} 3^{p-1}$. W szczególności więc najmniejszą liczbą naturalną mającą 10 dzielników jest liczba 48.

Przy dowodzeniu różnych własności liczb naturalnych często stosujemy tak zwaną zasadę indukcji matematycznej. Niedawno zasadę tę, nie mówiąc w niej o liczbach naturalnych, tak wyraził prof. Hugo Steinhaus: orzeka ona, że jeżeli jakaś własność dziedziczna przypada protoplaście rodu, to przypada jego całej progeniturze po wszystkie pokolenia.

Wyrazimy teraz tę zasadę, mówiąc w niej o własnościach liczb naturalnych. Umówmy się nazywać dziedziczną każdą własność liczb naturalnych polegającą na tym, że skoro ma ją dana liczba naturalna, to ma ją też liczba naturalna o jedność od niej większa. Łatwo jest dać przykłady własności dziedzicznych liczb naturalnych. Taką jest na przykład własność, że liczba jest większa od stu. Jeżeli bowiem dana liczba naturalna jest większa od stu, to i liczba o jedność od niej większa będzie większa od stu. Ale nie każda liczba naturalna jest większa od stu: własność dziedziczna liczb naturalnych niekoniecznie więc jest własnością każdej liczby naturalnej. Przykładem własności liczb naturalnych, która nie jest dziedziczna (w podanym przez nas wyżej znaczeniu), jest własność, że liczba naturalna jest mniejsza od stu, gdyż liczba 99 jest mniejsza od stu, ale większa od niej o jedność liczba 100 już nie jest mniejsza od stu. Otóż zasadę indukcji można tak wysłowić: Jeżeli jakąś własność dziedziczną liczb naturalnych ma liczba 1, to ma ją każda liczba naturalna.

Nasuwa się pytanie, skąd wiemy, że zasada ta jest prawdziwa, że możemy ją stosować bez obawy dojścia do sprzeczności. Ogólniej można by zapytać: skąd wiemy, że jakieś dane twierdzenie matematyczne jest prawdziwe? Za prawdziwe uważamy w matematyce pewne twierdzenia zwane pewnikami oraz te, które dadzą się z przyjętych pewników wyprowadzić drogą logicznego wnioskowania. Jeżeli za jeden z pewników przyjmujemy, że w każdym nie pustym zbiorze liczb naturalnych istnieje liczba najmniejsza, to zasadę indukcji można stąd łatwo wy prowadzić.

Przypuśćmy bowiem, że daną własność dziedziczną W ma liczba 1, ale że nie jest prawdą, iż ma ją każda liczba naturalna. W takim razie zbiór Z tych wszystkich liczb naturalnych, które nie mają własności W , jest nie pusty i przeto istnieje w nim liczba najmniejsza n . Liczba n nie jest równa 1, gdyż, w myśl założenia, liczba 1 ma własność W , a liczba n jej nie ma. Zatem liczba naturalna n jest większa od jedności i liczba $n - 1$ jest naturalna. Ponieważ liczba n jest najmniejszą liczbą naturalną, nie mającą własności W , więc liczba naturalna $n - 1$ (jako mniejsza od n) ma własność W . Ponieważ zaś własność W jest dziedziczna, więc skoro ma ją liczba $n - 1$, to ma ją też liczba $(n-1)+1 = n$, skąd wynika sprzeczność, gdyż liczba n nie ma własności W . Założenie, że zasada indukcji nie jest prawdziwa, doprowadza więc do sprzeczności. Jako przykład zastosowania zasady indukcji udowodnimy własność W , że dla każdej liczby naturalnej n jest $2^n > n$. Własność tę ma oczywiście liczba $n = 1$, gdyż $2^1 > 1$. Nadto w własność W jest dziedziczna, bo jeżeli ma ją liczba naturalna n , czyli jeżeli $2^n > n$, to (mnożąc obie strony tej nierówności przez 2) mamy $2^n \cdot 2 > n \cdot 2$, czyli $2^{n+1} > n + n$, a ponieważ, przy naturalnym n jest $n + n \geq n + 1$, więc mamy $2^{n+1} > n + 1$, zatem własność W ma też liczba $n + 1$. Przez indukcję wnosimy więc, że własność W ma każda liczba naturalna, czyli, że $2^n > n$ dla $n = 1, 2, 3, \dots$

CZEŚĆ TRZECIA

NAJWIĘKSZY WSPÓLNY DZIELNIK. RÓWNANIA LINIOWE W LICZBACH CAŁKOWITYCH

Niech m będzie daną liczbą naturalną i niech będą dane m liczb całkowitych a_1, a_2, \dots, a_m . Gdyby każda z tych liczb była zerem, to każda liczba całkowita byłaby wspólnym dzielnikiem naszych m liczb i nie byłoby największego wspólnego ich dzielnika. Przypuśćmy więc, że jedna co najmniej z naszych liczb, na przykład liczba a_1 , nie jest zerem.

Oznaczmy przez Z zbiór wszystkich liczb naturalnych n , które dają się przedstawić w postaci

$$(1) \quad n = a_1x_1 + a_2x_2 + \dots + a_mx_m$$

gdzie x_1, x_2, \dots, x_m są to liczby całkowite.

Nasuwa się tu przede wszystkim pytanie, czy istnieją liczby naturalne n , należące do zbioru Z . Łatwo dowieść, że takie liczby istnieją, a nawet je wskazać. Skoro bowiem $a_1 \neq 0$, to $a_1 > 0$ lub $a_1 < 0$. Jeżeli $a_1 > 0$, to dla liczb całkowitych $x_1 = 1, x_2 = x_3 = \dots = x_m = 0$ wzór (1) daje $n = a_1 \cdot 1 + a_2 \cdot 0 + a_3 \cdot 0 + \dots + a_m \cdot 0 = a_1$ i a_1 jest liczbą zbioru Z . Jeżeli zaś $a_1 < 0$, to dla $x_1 = -1, x_2 = x_3 = \dots = x_m = 0$ wzór (1) daje $n = a_1 \cdot (-1) + a_2 \cdot 0 + \dots + a_m \cdot 0 = -a_1$ i ponieważ a_1 jest liczbą całkowitą ujemną, więc $n = -a_1$ jest liczbą naturalną postaci (1), (gdzie x_1, x_2, \dots, x_m są to liczby całkowite) i przeto należy do zbioru Z . Zbiór Z jest więc zbiorem nie pustym liczb naturalnych. Ale, jak wiadomo z arytmetyki, w każdym nie pustym zbiorze liczb naturalnych istnieje liczba najmniejsza. Zatem i w zbiorze Z istnieje liczba najmniejsza: oznaczmy ją przez d . Stąd, że d należy do zbioru Z i z określenia tego zbioru wynika, że istnieją liczby całkowite t_1, t_2, \dots, t_m takie, że

$$(2) \quad d = a_1t_1 + a_2t_2 + \dots + a_mt_m.$$

Niech teraz k oznacza dowolną liczbę całkowitą postaci

$$(3) \quad k = a_1x_1 + a_2x_2 + \dots + a_mx_m$$

gdzie x_1, x_2, \dots, x_m są to liczby całkowite. Okażemy, że liczba k jest podzielna bez reszty przez d . Przypuśćmy, dla dowodu, że przy dzieleniu liczby k przez d otrzymujemy resztę dodatnią r . Będzie więc r liczbą naturalną mniejszą od d i przy pewnym całkowitym u będzie $k = du + r$, skąd wobec (3) i (2) $r = k - du = a_1(x_1 - t_1u) + a_2(x_2 - t_2u) + \dots + a_m(x_m - t_mu)$. Połóżmy $y_i = x_i - t_iu$ dla $i = 1, 2, \dots, m$: będą to liczby całkowite i będzie

$$r = a_1y_1 + a_2y_2 + \dots + a_my_m$$

a ponieważ r jest liczbą naturalną, więc (w myśl definicji zbioru Z) będzie to liczba zbioru Z . Ale, jak wiemy, $r < d$, zaś d jest najmniejszą liczbą zbioru Z . Stąd sprzeczność. Założenie, że liczba k nie jest podzielna przez d doprowadza więc do sprzeczności.

Dowiedliśmy więc, że każda liczba całkowita k postaci (3), gdzie x_1, x_2, \dots, x_m są to liczby całkowite, jest podzielna przez d . Ale jak łatwo dowieść, każda z liczb a_1, a_2, \dots, a_m jest postaci (3) przy pewnych całkowitych x_1, x_2, \dots, x_m . Istotnie, jeżeli i jest jedną z liczb $1, 2, \dots, m$ i jeżeli przyjmiemy $x_i = 1$, zaś pozostałe z liczb x_1, x_2, \dots, x_m przyjmiemy równe zeru, to oczywiście będziemy mieli $a_i = a_1x_1 + a_2x_2 + \dots + a_mx_m$. Z tego, cośmy wyżej dowiedli o liczbach postaci (3) wynika, że każda z liczb a_1, a_2, \dots, a_m jest podzielna przez d . Liczba d jest więc wspólnym dzielnikiem wszystkich tych liczb.

Niech teraz δ oznacza jakikolwiek dzielnik wspólny liczb a_1, a_2, \dots, a_m . Istnieją więc liczby całkowite

k_1, k_2, \dots, k_m takie, iż $a_i = k_i \delta$ dla $i = 1, 2, \dots, m$. Stąd, wobec (2):

$$(4) d = (k_1 t_1 + k_2 t_2 + \dots + k_m t_m) \delta,$$

(5)

a ponieważ liczba $k_1 t_1 + k_2 t_2 + \dots + k_m t_m$ jest całkowitą, więc wzór (4) dowodzi, że liczba d jest podzielna przez δ .

Dowiedliśmy zatem, że liczba d jest takim dzielnikiem wspólnym liczb a_1, a_2, \dots, a_m , który jest podzielny przez każdy wspólny dzielnik tych liczb. Jest to więc największy ze wspólnych dzielników liczb a_1, a_2, \dots, a_m , czyli ich największy wspólny dzielnik.

Dowiedliśmy więc, że największy wspólny dzielnik m liczb całkowitych a_1, a_2, \dots, a_m , z których co najmniej jedna nie jest zerem, jest podzielny przez każdy wspólny dzielnik tych liczb, oraz daje się przedstawić w postaci (2), gdzie t_1, t_2, \dots, t_m są to pewne liczby całkowite. Udowodnione twierdzenie zastosujemy teraz do znalezienia warunku koniecznego i dostatecznego na to, żeby dla danych liczb całkowitych a_1, a_2, \dots, a_m i b równanie

$$(5) a_1 x_1 + a_2 x_2 + \dots + a_m x_m = b$$

miało co najmniej jedno rozwiązanie w liczbach całkowitych

x_1, x_2, \dots, x_m .

Jeżeli równanie (5) ma takie rozwiązanie i jeżeli $a_1 = a_2 = \dots = a_m = 0$, to oczywiście musi być $b = 0$, a jeżeli $a_1 = a_2 = \dots = a_m = 0 = b = 0$, to oczywiście każdy układ liczb całkowitych x_1, x_2, \dots, x_m spełnia równanie (5).

Przypuśćmy więc dalej, że nie wszystkie liczby a_1, a_2, \dots, a_m są równe zeru i niech d oznacza ich największy wspólny dzielnik. Wówczas istnieją liczby całkowite k_1, k_2, \dots, k_m takie, iż $a_i = k_i d$ dla $i = 1, 2, \dots, m$ i jeżeli przy pewnych całkowitych x_1, x_2, \dots, x_m równanie (5) jest spełnione, to

$$(k_1 x_1 + k_2 x_2 + \dots + k_m x_m) d = b,$$

skąd wynika, że b jest podzielne przez d .

Z drugiej strony, jeżeli liczba b jest podzielna przez d , $b = kd$, gdzie k jest liczbą całkowitą, to, wobec (2), liczby $x_i = kt_i$ ($i = 1, 2, \dots, m$), jak łatwo sprawdzić, spełniają równanie (5).

Jeżeli więc co najmniej jedna z liczb całkowitych a_1, a_2, \dots, a_m jest różna od zera, to na to, żeby równanie (5) miało choć jedno rozwiązanie w liczbach całkowitych x_1, x_2, \dots, x_m , potrzeba i wystarcza, żeby liczba b była podzielna przez największy wspólny dzielnik liczb a_1, a_2, \dots, a_m .

Dotychczasowe nasze rozważania nie dają jednak możliwości znalezienia choćby jednego rozwiązania równania (5) w razie jego rozwiązalności, gdyż nie dają żadnych wskazówek co do tego jak można obliczyć największy wspólny dzielnik d liczb a_1, a_2, \dots, a_m ani też, jak można znaleźć liczby całkowite t_1, t_2, \dots, t_m spełniające wzór (2).

W teorii liczb, aby rozwiązać dane zagadnienie dotyczące liczb naturalnych, często stosuje się metodę polegającą na tym, że zagadnienie to sprowadzamy do takiegoż zagadnienia dotyczącego liczb mniejszych. Ponieważ ciąg liczb naturalnych malejących musi być skończony, więc metoda ta (zwana metodą regresji) doprowadza do rozwiązania rozważanego zagadnienia. Wyjaśnimy to bliżej na przykładzie znajdowania największego wspólnego dzielnika liczb naturalnych.

Mamy na przykład dwie dane liczby naturalne a i b . Gdyby liczby te były równe, to oczywiście największym wspólnym dzielnikiem liczb a i b byłaby liczba a i dzielnik ten byłby znaleziony. Oznaczając przez (a, b) największy wspólny dzielnik liczb a i b mielibyśmy więc $(a, b) = a$. Możemy więc dalej przypuścić, że liczby a i b są różne, że na przykład $a > b$. Każdy dzielnik wspólny liczb a i b jest oczywiście też dzielnikiem liczby $a - b$, a każdy dzielnik wspólny liczb b oraz $a - b$ jest dzielnikiem $a = b + (a - b)$. Wynika stąd, że liczby a i b mają te same wspólne dzielniki co liczby $a - b$ i b , skąd wynika natychmiast, $(a, b) = (a - b, b)$. Lecz, skoro liczby a i b są naturalne, to $a + b > (a - b) + b = a$. Tak więc (w razie $a \neq b$) znajdowanie największego wspólnego dzielnika liczb naturalnych a i b sprowadziliśmy do znajdowania największego wspólnego dzielnika

liczb naturalnych $a - b$ i b o mniejszej sumie niż suma liczb a i b . Gdyby było $a - b = b$, największy wspólny dzielnik tych liczb byłby, jak wiemy, znaleziony ($= b$). W razie $a - b \neq b$ sprowadzilibyśmy, jak wyżej, znajdowanie największego wspólnego dzielnika liczb $a - b$ i b do znajdowania największego wspólnego dzielnika dwóch liczb naturalnych o mniejszej jeszcze sumie itd. Ponieważ nie ma ciągu nieskończonego liczb naturalnych malejących, więc po pewnej skończonej liczbie kroków musimy dojść do przypadku, w którym obie liczby, dla których szukamy ich największego wspólnego dzielnika, będą równe, a więc też równe ich największemu wspólnemu dzielnikowi, który w ten sposób będzie znaleziony.

Stosowane tu postępowanie można by przyspieszyć wyznaczając w razie $a > b$ resztę r z dzielenia liczby a przez b . Będzie tu $0 \leq r < b$. W razie $r = 0$ będzie oczywiście $(a, b) = b$, zaś w razie $r > 0$ będzie $(a, b) = (b, r)$, przy czym $b < a$ i $r < b$, a więc mamy do czynienia z liczbami mniejszymi odpowiednio niż a i b . W tym przypadku metoda ta jest znana pod nazwą metody kolejnych dzieleń, algorytmu Euklidesa, lub wreszcie algorytmu ułamka ciągłego.

Niech teraz m oznacza liczbę naturalną > 1 i przypuśćmy, że chcemy znaleźć największy wspólny dzielnik danych liczb naturalnych a_1, a_2, \dots, a_m . Gdyby wszystkie te liczby były równe, mielibyśmy oczywiście $(a_1, a_2, \dots, a_m) = a_1$ i największy ich wspólny dzielnik byłby znaleziony. Przypuśćmy więc, że nie wszystkie liczby a_1, a_2, \dots, a_m są równe, że więc na przykład $a_1 > a_m$. Jak łatwo dowieść, liczby a_1, a_2, \dots, a_m mają te same wspólne dzielniki co liczby $a_1 - a_m, a_2, \dots, a_m$, skąd wynika, że $(a_1, a_2, \dots, a_m) = (a_1 - a_m, a_2, \dots, a_m)$, a ponieważ $(a_1 - a_m) + a_2 + \dots + a_m = a_1 + a_2 + \dots + a_m - 1 < a_1 + a_2 + \dots + a_m$, więc znajdowanie największego wspólnego dzielnika liczb a_1, a_2, \dots, a_m sprowadziliśmy do znajdowania największego wspólnego dzielnika liczb naturalnych o mniejszej sumie. Możemy tu więc zastosować metodę regresji, która doprowadzi do znalezienia największego wspólnego dzielnika danych liczb naturalnych a_1, a_2, \dots, a_m . Można też dowieść, że obliczanie największego wspólnego dzielnika dowolnej skończonej liczby liczb całkowitych sprowadza się do kolejnego obliczania największego wspólnego dzielnika dwóch liczb całkowitych. Jeżeli mianowicie mamy $m > 2$ liczb całkowitych a_1, a_2, \dots, a_m i oznaczymy $d_k = (a_1, a_2, \dots, a_k)$ dla $k = 2, 3, \dots, m$, to będzie $d_2 = (a_1, a_2), d_3 = (d_2, a_3), d_4 = (d_3, a_4), \dots, d_m = (d_{m-1}, a_m)$, skąd kolejno obliczamy d_2, d_3 i wreszcie $d_m = (a_1, a_2, \dots, a_m)$.

Przypuśćmy teraz, że m jest liczbą naturalną, a_1, a_2, \dots, a_m i b są dane liczby całkowite, i chodzi o znalezienie wszystkich układów liczb całkowitych x_1, x_2, \dots, x_m spełniających równanie (5). Jak dowiedliśmy wyżej, na to żeby równanie to miało i choć jedno rozwiązanie w liczbach całkowitych x_1, x_2, \dots, x_m , potrzeba i wystarcza żeby liczba b była podzielna przez największy wspólny dzielnik liczb a_1, a_2, \dots, a_m . Przypuśćmy, że warunek ten jest spełniony. Okażemy jak wówczas, stosując metodę regresji można znaleźć wszystkie rozwiązania równaniu (5) w liczbach całkowitych x_1, x_2, \dots, x_m .

Zauważymy przede wszystkim, że można założyć, iż w równaniu (5) wszystkie współczynniki a_1, a_2, \dots, a_m są naturalne,

gdyż składniki o współczynnikach 0 można opuścić, zaś współczynnik ujemny możemy zastąpić przez równy mu co do wartości bezwzględnej dodatni, zmieniając znak przy niewiadomej. Gdyby wszystkie współczynniki a_1, a_2, \dots, a_m były równe, mielibyśmy równani:

$$a_1(x_1 + x_2 + \dots + x_m) = b$$

Jeżeli równanie to jest rozwiązalne w liczbach całkowitych x_1, x_2, \dots, x_m , to oczywiście liczba b musi być podzielna przez a_1 , a jeżeli warunek ten jest spełniony i $b = a_1 c$, gdzie c jest liczbą całkowitą, to otrzymujemy równanie

$$x_1 + x_2 + \dots + x_m = c,$$

którego wszystkie rozwiązania w liczbach całkowitych x_1, x_2, \dots, x_m , jak łatwo zauważyć, otrzymamy biorąc za x_2, x_3, \dots, x_m dowolne liczby całkowite i wyznaczając x_1 ze wzoru $x_1 = c - x_2 - x_3 - \dots - x_m$. Możemy więc dalej przy dopuścić, że nie wszystkie współczynniki a_1, a_2, \dots, a_m są równe,

że więc na przykład $a_1 \neq a_2$, przypuśćmy $a_1 > a_2$. Przypuśćmy, że liczba a_1 przy dzieleniu przez a_2 daje iloraz całkowity oraz resztę b_2 : będzie więc $a_1 = a_2k + b_2$, gdzie k jest liczbą naturalną, zaś b_2 liczbą całkowitą, taką iż $0 \leq b_2 < a_2$.

Położmy $y_1 = kx_1 + x_2$, $y_2 = x_1$, $b_1 = a_2$. Będzie $a_1x_1 + a_2x_2 = a_2(kx_1 + x_2) + b_2x_1 = b_1y_1 + b_2y_2$ i równanie (5) przejdzie na równanie

$$(6) \quad b_1y_1 + b_2y_2 + a_3x_3 + \dots + a_mx_m = b.$$

Z każdego rozwiązania równania (5) w liczbach całkowitych x_1, x_2, \dots, x_n otrzymujemy rozwiązanie w liczbach całkowitych $y_1, y_2, x_3, \dots, x_m$ równania (6), kładąc $y_1 = kx_1 + x_2$, $y_2 = x_1$. Na odwrót, z każdego rozwiązania w liczbach całkowitych $y_1, y_2, x_3, \dots, x_m$ równania (6) otrzymujemy rozwiązanie w liczbach całkowitych x_1, x_2, \dots, x_m równania (5) kładąc $x_1 = y_1$, $x_2 = y_1 - ky_2$.

Ponieważ $a_1 > a_2 = b_1 > b_2$, więc $a_1 + a_2 > b_1 + b_2$ i przeto suma wszystkich współczynników przy niewiadomych w równaniu (6) jest mniejsza niż w równaniu (5). Możemy więc tutaj zastosować metodę regresji. Opuszczając ewentualne wyrazy o współczynnikach $= 0$ musimy więc dojść albo do równania o jednej niewiadomej, które potrafimy rozwiązać, albo do równania, w którym wszystkie współczynniki przy niewiadomych są równe; i w tym przypadku wiemy, jak postąpić.

Zauważmy tu jeszcze, że gdyby w równaniu (5) jeden ze współczynników przy niewiadomych, na przykład a_1 , był równy 1, to natychmiast znaleźlibyśmy wszystkie rozwiązania tego równania w liczbach całkowitych x_1, x_2, \dots, x_m , biorąc za x_2, x_3, \dots, x_m dowolne liczby całkowite i kładąc

$$x_1 = b - a_2x_2 - a_3x_3 - \dots - a_mx_m.$$

Przykład. Znajdziemy wszystkie rozwiązania w liczbach całkowitych x, y, z , równania

$$(7) \quad 6x + 10y - 7z = 11.$$

Kładąc $z' = -z$, otrzymujemy równanie $6x + 10y + 7z' = 11$. Wobec $10 = 7 + 3$ mamy stąd $6x + 7(y + z') + 3y = 11$ i kładąc $y + z' = t$, otrzymujemy równanie $6x + 7t + 3y = 11$. Wobec $7 = 6 + 1$ mamy stąd $6(x + t) + t + 3y = 11$ i, kładąc $x + t = u$ otrzymujemy równanie $6u + t + 3y = 11$. Wszystkie rozwiązania w liczbach całkowitych u, t, y tego równania otrzymamy oczywiście obierając jako y i u dowolne liczby całkowite i kładąc $t = 11 - 3y - 6u$. Wobec $x + t = u$ otrzymujemy stąd: $x = u - t = 3y + 7u - 11$, zaś wobec $z' = -z$ i $y + z' = t$, znajdujemy $z = y - t = 4y + 6u - 11$. Wszystkie rozwiązania równania (7) w liczbach całkowitych x, y, z są więc zawarte we wzorach $x = 3y + 7u - 11$, $z = 4y + 6u - 11$, gdzie y i u są to dowolne liczby całkowite. Jakoż sprawdzamy: $6(3y + 7u - 11) + 10y - 7(4y + 6u - 11) = 11$. Łatwo jest dowieść, że jeżeli równanie (5) jest rozwiązalne w liczbach całkowitych, to takich rozwiązań, w razie $m > 1$, jest nieskończenie wiele. Jeżeli bowiem istnieją liczby całkowite y_1, y_2, \dots, y_m takie, że

$$a_1y_1 + a_2y_2 + \dots + a_my_m = b,$$

to kładąc $x_i = y_i + a_it_i$, dla $i = 1, 2, \dots, m - 1$, zaś $x_m = y_m - a_1t_1 - \dots - a_{m-1}t_{m-1}$, gdzie t_1, t_2, \dots, t_{m-1} są dowolnymi liczbami całkowitymi, otrzymamy, jak łatwo sprawdzić, liczby całkowite x_1, x_2, \dots, x_m spełniające równanie (5). Można by też dowieść, że jeśli równanie (5) jest rozwiązalne w liczbach całkowitych x_1, x_2, \dots, x_m , to liczby te wyrażają się liniowo (o współczynnikach całkowitych) przez $m-1$ dowolnych parametrów. (W podanym wyżej przykładzie niewiadome x, y, z wyrażają się za pomocą dwóch dowolnych parametrów y i u .) Uwaga ta pozwala rozwiązywać w liczbach całkowitych układ n równań liniowych o m niewiadomych. W tym celu z pierwszego równania wyrażamy każdą z niewiadomych przez $m-1$ parametrów i otrzymane wyrażenie wstawiamy do każdego z pozostałych $n - 1$ równań. Uważając $m - 1$ parametrów jako nowe niewiadome, otrzymamy w ten sposób $n - 1$ równań liniowych (o współczynnikach całkowitych) o $m - 1$ niewiadomych. Postępując w ten sposób dalej dojdziemy albo do jednego równania (o jednej lub

więcej niewiadomej), a to już wiemy, jak rozwiązać, albo do jednego lub więcej równania u jednej niewiadomej.

CZEŚĆ CZWARTA

RÓWNANIA DIOFANTYCZNE

Dział teorii liczb zajmujący się rozwiązywaniem równań w liczbach całkowitych nazywa się analizą diofantyczną, ponieważ matematyk grecki Diofant z Aleksandrii (który żył w III wieku n. e.) zajmował się zagadnieniami prowadzącymi do rozwiązywania równań o dwóch lub więcej niewiadomych w liczbach całkowitych. Zaczniemy tu od równania dowolnego stopnia o jednej niewiadomej. Przypuśćmy, że lewą stroną równania jest wielomian jednej zmiennej o współczynnikach całkowitych, że zatem równaniem jest

$$(1) \quad a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m = 0,$$

gdzie m jest daną liczbą naturalną, zaś a_0, a_1, \dots, a_m - dane liczby całkowite, przy czym $a_m \neq 0$. Jeżeli liczba całkowita x spełnia równanie (1), to mamy

$$(a_0x^{m-1} + a_1x^{m-2} + \dots + a_{m-1})x = -a_m,$$

skąd wynika, że liczba x musi być dzielnikiem liczby a_m . Ponieważ liczba całkowita, różna od zera, a_m , ma skończoną liczbę dzielników, więc wszystkie rozwiązania w liczbach całkowitych x równania (1) możemy znaleźć za pomocą skończonej ilości prób, podstawiając do równania (1) kolejno wszystkie dzielniki liczby a_m (zarówno dodatnie, jak i ujemne) i wybierając tylko te z nich, które spełniają nasze równanie. Gdyby było $a_m = 0$, to oczywiście jednym z pierwiastków naszego równania byłoby $x = 0$, a dla innych jego pierwiastków mielibyśmy równanie

$$a_0x^{m-1} + a_1x^{m-2} + \dots + a_{m-2}x + a_{m-1} = 0$$

z którym, w razie $a_{m-1} \neq 0$, postąpilibyśmy jak poprzednio z równaniem (1), zaś w razie $a_{m-1} = 0$ otrzymalibyśmy równanie $m - 2$ -go stopnia itd. Znajdziemy na przykład wszystkie rozwiązania w liczbach całkowitych równania

$$x^5 - 5x^4 - 3x^3 + 15x^2 + 2x - 10 = 0.$$

Ponieważ dzielnikami liczby 10 są tylko liczby 1, 2, 5, 10 oraz -1, -2, -5, -10, więc musimy za x podstawiać do naszego równania kolejno te 8 liczb. Z łatwością stwierdzamy, że spośród tych liczb tylko liczby 1, 2, 5, -1 i -2 spełniają nasze równanie: one więc dają wszystkie rozwiązania naszego równania w liczbach całkowitych. Jako drugi przykład weźmy równanie

$$x^7 + x + 2 = 0$$

Tu musimy za x podstawiać do naszego równania tylko dzielniki liczby -2, czyli liczby 1, -1, 2 i -2. W ten sposób stwierdzamy z łatwością, że tylko liczba -1 jest rozwiązaniem naszego równania w liczbach całkowitych. Tak więc znajdowanie wszystkich liczb całkowitych, będących pierwiastkami danego wielomianu o współczynnikach całkowitych, nawet dla wielomianów wyższych stopni, nie przedstawia innych trudności poza technicznymi; inaczej jest ze znajdowaniem wszystkich pierwiastków danego wielomianu, z którym mamy do czynienia w algebrze, gdzie, jak wiadomo, już wzory na pierwiastki wielomianów trzeciego lub czwartego stopnia są skomplikowane, a pierwiastki wielomianów stopnia wyższego niż czwarty tylko w pewnych szczególnych przypadkach mogą być znalezione algebraicznie. Jeżeli chodzi o rozwiązywanie danych równań o dwóch lub więcej niewiadomych w liczbach całkowitych, to możemy sobie uluwać następujące pytania, których stopień trudności jest coraz większy.

1. Czy dane równanie ma choćby jedno rozwiązanie w liczbach całkowitych?

2. Czy rozwiązań danego równania w liczbach całkowitych jest ilość skończona, czy też jest ich nieskończenie wiele?

3. Wyznaczyć wszystkie rozwiązania danego równania w liczbach całkowitych.

Znane są przypadki, w których już na pierwsze pytanie nie potrafimy dać odpowiedzi. Nie wiemy na przykład czy równanie $x^3 + y^3 + z^3 = 30$ ma choćby jedno rozwiązanie w liczbach całkowitych x, y, z . O równaniu $x^4 + y^4 + z^4 = t^4$ wiemy, że ma rozwiązania w liczbach całkowitych x, y, z, t (np. $x = y = 0, z = t$), ale nie wiemy, czy ma rozwiązanie w liczbach naturalnych ani też, czy jest ich liczba skończona. Dla równania $x^3 + y^3 + z^3 = 3$ znamy cztery rozwiązania w liczbach całkowitych x, y, z , mianowicie $(a, y, z) = (1, 1, 1), (4, 4, -5), (4, -5, 4)$ i $(-5, 4, 4)$, ale nie wiemy, czy są jeszcze inne.

O równaniu $x^3 + y^3 + z^3 = 3$ natomiast wiemy, że ma nieskończenie wiele rozwiązań w liczbach całkowitych, na przykład, jak łatwo sprawdzić, $(x, y, z) = (1 + 6n^3, 1 - 6n^3, -6n^2)$, gdzie n jest dowolną liczbą naturalną, ale nie znamy wszystkich rozwiązań tego równania w liczbach całkowitych. Natomiast łatwo jest dowieść, że równanie $x^3 + y^3 + z^3 = 4$ nie ma rozwiązań w liczbach całkowitych x, y, z . W samej rzeczy, sześcián liczby całkowitej przy dzieleniu przez 9 może dawać tylko resztę 0, 1 lub 8, skąd wynika, że suma dwóch sześciánów liczb całkowitych może przy dzieleniu przez 9 dawać tylko resztę 0, 1, 2, 7 lub 8, zatem suma trzech sześciánów tylko reszty 0, 1, 2, 3, 6, 7 lub 8, a więc nigdy nie daje reszty 4 ani reszty 5.

Nie tylko więc równanie $x^3 + y^3 + z^3 = 4$, ale i równanie $x^3 + y^3 + z^3 = 5$ nie ma rozwiązań w liczbach całkowitych x, y, z (i ogólniej, nie ma takich rozwiązań równania $x^3 + y^3 + z^3 = k$, gdzie k jest liczbą całkowitą, dającą przy dzieleniu przez 9 resztę 4 lub 5).

O równaniu $x^3 + y^3 + z^3 = 6$ wiemy, że ma rozwiązania w liczbach całkowitych x, y, z na przykład $(x, y, z) = (-1, -1, 2), (-43, -58, 65), (-55, -235, 236)$, ale nie wiemy, czy jest ich ilość skończona.

Niekiedy na przeszkodzie znalezieniu wszystkich rozwiązań danego równania w liczbach całkowitych stoją tylko trudności techniczne: długość potrzebnych na to rachunków. Na przykład, gdyby chodziło o znalezienie wszystkich rozwiązań w liczbach całkowitych x, y równania $xy = 2^{101} - 1$. Wiemy, że ma nimi rozwiązanie w liczbach naturalnych x, y większych od 1, ale nie potrafimy go znaleźć, chociaż byłoby to teoretycznie możliwe przez dokonywanie dzielenia liczby $2^{101} - 1$ przez kolejne liczby naturalne $< 2^{101} - 1$, lecz liczba prób byłaby tu zbyt wielka, aby je można było przy dzisiejszym stanie techniki wykonać.

Natomiast nie znamy żadnego postępowania, które by mogło, choćby po bardzo długich rachunkach, doprowadzić nas do rozstrzygnięcia, czy równanie $x^3 + y^3 + z^3 = 30$ ma rozwiązanie w liczbach całkowitych x, y, z . Łatwo jednak byłoby dowieść, że nie ma ono rozwiązań w liczbach naturalnych, co pozostawiamy czytelnikowi. Łatwo dać przykłady równań drugiego stopnia o dwóch niewiadomych i o współczynnikach całkowitych, które nie mają żadnego rozwiązania w liczbach całkowitych, na przykład równanie $x^2 + y^2 - 3 = 0$. Łatwo też dać przykład takich równań, które mają skończoną liczbę rozwiązań w liczbach całkowitych: na przykład równanie $x^2 + y^2 - 5 = 0$ ma osiem rozwiązań liczbach całkowitych: $(x, y) = (1, 2), (2, 1), (-1, 2), (2, -1), (1, -2), (-2, 1), (-1, -2), (-2, -1)$. Nie jest też rzeczą trudną danie przykładu równania drugiego stopnia o dwóch niewiadomych i o współczynnikach całkowitych, mającego nieskończenie wiele rozwiązań w liczbach całkowitych. Takim jest na przykład równanie

$$(2) \quad x^2 + x - 2y^2 = 0$$

Równanie to ma w liczbach naturalnych x, y rozwiązanie oczywiste $x = y = 1$.

Z drugiej strony łatwo dowieść, że jeżeli liczby x i y dają rozwiązanie równania (2) w liczbach naturalnych, to liczby (oczywiście naturalne)

$$(3) \quad \xi = 3x + 4y + 1, \eta = 2x + 3y + 1$$

też dają rozwiązanie naszego równania, gdyż jak łatwo obliczyć:

$$\xi^2 + \xi - 2\eta^2 = (3x + 4y + 1)(3x + 4y + 2) - 2(2x + 3y + 1)^2 = x^2 + x - 2y^2$$

Z każdego rozwiązania równania (2) w liczbach naturalnych możemy więc otrzymać rozwiązanie

tegoż równania w większych liczbach naturalnych. Na przykład z rozwiązania $x = y = 1$ otrzymujemy w ten sposób rozwiązanie $\xi = 8, \eta = 6$, z tego zaś nowe rozwiązanie $(49, 35)$, z niego zaś $(288, 204)$ itd. Równanie nasze ma więc nieskończenie wiele rozwiązań w liczbach naturalnych x, y . Można by dowieść, że wychodząc z rozwiązania $x = y = 1$ i wyznaczając wciąż nowe rozwiązania za pomocą wzorów (3) można otrzymać wszystkie rozwiązania równania (2) w liczbach naturalnych x, y . Liczbę $n(n+1)/2$, gdzie n jest liczbą naturalną, nazywamy n -tą liczbą trójkątną i oznaczamy przez t_n . Równanie (2) możemy więc napisać w postaci

$$t_x = y^2$$

Wyznacza ona wszystkie liczby kwadratowe y^2 , które są zarazem trójkątne. Podane wyżej wzory pozwalają więc wyznaczyć kolejno wszystkie takie liczby. Istnieje zatem nieskończenie wiele liczb kwadratowych, które są zarazem trójkątnymi. Udowodniono, że nie ma liczby trójkątnej > 1 , która by była bikwadratem, tj. równanie $x^2 + x - 2y^4 = 0$ nie ma rozwiązań w liczbach naturalnych > 1 . Można natomiast dowieść, że równanie to ma nieskończenie wiele rozwiązań w liczbach wymiernych x, y . Jednym z nich jest $x = 32/49, y = 6/7$, innym $x = 1/239^2, y = 13/239$

Rozważmy teraz równanie $x^2 + x - y^2 = 0$. Dla naturalnych x liczby x i $x + 1$ są, jak wiadomo, względnie pierwsze (tj. nie mają wspólnego dzielnika większego od jednośc, gdyż taki dzielnik byłby dzielnikiem ich różnicy, czyli liczby 1, co jest niemożliwe). Gdyby istniały liczby naturalne x, y takie iż $x^2 + x - y^2 = 0$, mielibyśmy $x(x + 1) = y^2$ i liczba kwadratowa y^2 byłaby iloczynem dwóch liczb względnie pierwszych x i $x + 1$. Lecz, jak wiadomo z arytmetyki, jeżeli liczba kwadratowa jest iloczynem dwóch liczb naturalnych względnie pierwszych, to każdy z czynników musi być kwadratem liczby naturalnej. Istniałyby więc liczby naturalne k i l , takie iż $x = k^2, x + 1 = l^2$, skąd $1 = l^2 - k^2 = (l + k)(l - k)$, co jest niemożliwe gdyż pierwszy czynnik prawej strony jest ≥ 2 . Założenie, że równanie $x^2 + x - y^2 = 0$ ma rozwiązanie w liczbach naturalnych x, y doprowadza więc do sprzeczności. Równanie to nie ma przeto rozwiązań w liczbach naturalnych: innymi słowy, iloczyn dwóch kolejnych liczb naturalnych nie jest nigdy kwadratem liczby naturalnej. Zauważymy jednak, że równanie $x^2 + x - y^2 = 0$ ma rozwiązania w liczbach wymiernych dodatnich, na przykład $x = 1/3, y = 2/3$ lub $x = 1/8, y = 3/8$

Podobnie łatwo mogliśmy dowieść, że dla naturalnych $m > 1$ równanie $x^2 + x - y^m = 0$ nie ma rozwiązań w liczbach naturalnych x i y , a więc że iloczyn dwóch kolejnych liczb naturalnych nie jest potęgą liczby naturalnej o wykładniku większym od jednośc. Od dwustu przeszło lat jest znane zagadnienie: Czy iloczyn dowolnej ilości kolejnych liczb naturalnych może być potęgą liczby naturalnej. Dotąd udowodniono tylko, że iloczyn dwóch, trzech, . . ., aż do siedemnastu kolejnych liczb naturalnych nie jest potęgą liczby naturalnej o wykładniku > 1 , tj. że równanie

$$x(x + 1) \dots (x + k - 1) = y^m$$

gdzie k jest liczbą naturalną, taką iż $2 \leq k \leq 17$, zaś m liczbą naturalną > 1 , nie ma rozwiązań w liczbach naturalnych x i y . Zajmiemy się teraz równaniem $x^2 + x + 1 = 3y^2$, które ma już swoją historię. W 1950 r. matematyk węgierski R. O b l a t h przypuszczał, że poza rozwiązaniem $x = y = 1$ nie ma ono innych rozwiązań w liczbach naturalnych x, y , gdzie x jest liczbą nieparzystą. W tymże roku T. N a g e 11 podał rozwiązanie $x = 313, y = 181$.

Łatwo dowieść, że równanie nasze ma nieskończenie wiele rozwiązań w liczbach naturalnych x, y , a wśród nich nieskończenie wiele takich, gdzie x jest liczbą nieparzystą. Jeżeli bowiem liczby naturalne x i y spełniają nasze równanie, to, jak łatwo sprawdzić, liczby $\xi = 7x + 12y + 3, \eta = 4x + 7y + 2$ również są naturalne i spełniają nasze równanie, gdyż

$$\xi^2 + \xi + 1 - 3\eta^2 = (7x + 12y + 3)^2 + (7x + 12y + 3) + 1 - 3(4x + 7y + 2)^2 = x^2 + x + 1 - 3y^2.$$

Z każdego więc rozwiązania naszego równania w liczbach naturalnych możemy otrzymać rozwiązanie tegoż równania w liczbach naturalnych większych. Tak na przykład z rozwiązania $(1, 1)$ otrzymujemy kolejno rozwiązania

$$(x, y) = (1, 1), (22, 13), (313, 181), (4366, 2521), (60817, 35113), \dots$$

Łatwo byłoby dowieść, że w rozwiązaniach tych liczby x są na przemian nieparzyste i parzyste, zaś liczby y zawsze nieparzyste. Trudniej byłoby dowieść, że w ten sposób otrzymujemy wszystkie

rozwiązania naszego równania w liczbach naturalnych. Andrzej Rotkiewicz zauważył, że z każdego rozwiązania w liczbach naturalnych $x > 1$ i y równania $x^2 + x + 1 = 3y^2$ można otrzymać rozwiązanie w liczbach naturalnych y, z równania

$$(4) (z + 1)^3 - z^3 = y^2.$$

Jeżeli bowiem liczby naturalne $x > 1$ i y spełniają równanie $x^2 + x + 1 = 3y^2$ to, jak łatwo sprawdzić, mamy $(x - 1)^2 = 3(y^2 - x)$, skąd wynika, że liczba (naturalna) $x - 1$ jest podzielna przez 3, zatem $x - 1 = 3z$, gdzie z jest liczbą naturalną, przy czym będzie $3z^2 = y^2 - x = y^2 - 3z - 1$, co dowodzi, że liczby x i y spełniają równanie (4).

Tuk więc z rozwiązań (22, 13), (313, 181), (4366, 2521), równania $x^2 + x + 1 = 3y^2$ otrzymujemy rozwiązania (7, 13), (104, 181), (1455, 2521) równania (4). Można dowiedzieć, że w ten sposób otrzymujemy wszystkie rozwiązania równania (4) w liczbach naturalnych y i z .

Przejdźmy teraz do równania

$$(5) x^2 - Dy^2 = 1,$$

które przez pomyłkę Eulera nazwane zostało równaniem Pella, choć Pell się nim nie zajmował. Gdyby tu D było kwadratem liczby naturalnej, $D = n^2$, równanie (5) można by napisać w postaci

$$(x - ny)(x + ny) = 1$$

skąd wynika z łatwością, że wówczas równanie (5) ma w liczbach całkowitych x, y tylko rozwiązanie $x = \pm 1, y = 0$. Przypuśćmy więc, że D jest liczbą naturalną, nie będącą kwadratem liczby naturalnej, albo, co na to samo wychodzi, że liczba \sqrt{D} jest niewymierna. Powstaje pytanie: czy wówczas równanie (7) ma rozwiązania w liczbach naturalnych x, y . Gdyby takie rozwiązanie istniało, istniałoby też oczywiście rozwiązanie w liczbach naturalnych najmniejszych x, y . Łatwo też dowiedzieć, że jeżeli równanie (5) ma choć jedno rozwiązanie w liczbach naturalnych x, y , to ma takich rozwiązań nieskończenie wiele. Jeżeli bowiem (a, b) i (c, d) są dwa (różne lub nie) rozwiązania równania (7), to wobec tożsamości

$$(ac + Dbd)^2 - D(bc + ad)^2 = (a^2 - Db^2)(c^2 - Dd^2)$$

wnosimy, że liczby $x = ac + Dbd$ i $y = bc + ad$ też dają rozwiązania równania (5). Można dowiedzieć, że wszystkie rozwiązania równania (5) w liczbach naturalnych x, y zawarte są w ciągu nieskończonym (x_n, y_n) ($n = 1, 2, \dots$), gdzie (x_1, y_1) jest rozwiązaniem w liczbach naturalnych najmniejszych, zaś

$$x_{n+1} = x_1 x_n + Dy_1 y_n, y_{n+1} = y_1 x_n + x_1 y_n \text{ dla } n = 1, 2, \dots$$

Na przykład, ponieważ rozwiązaniem równania $x^2 - 2y^2 = 1$ w liczbach naturalnych najmniejszych jest $x_1 = 3, y_1 = 2$, więc wszystkie rozwiązania (x_n, y_n) tego równania w liczbach naturalnych otrzymamy ze wzorów

$$x_{n+1} = 3x_n + 4y_n, y_{n+1} = 2x_n + 3y_n \text{ dla } n = 1, 2, \dots$$

W ten sposób otrzymujemy kolejno rozwiązania: $x_2 = 17, y_2 = 12, x_3 = 99, y_3 = 70, x_4 = 577, y_4 = 408$. Można dowiedzieć, że jeżeli liczba \sqrt{D} jest niewymierna, to istnieje rozwiązanie równania (5) w liczbach naturalnych. Ale jak można takie rozwiązanie znaleźć? Sprawa bynajmniej nie jest łatwa. Zdawałoby się, że dla znalezienia rozwiązania równania (5) w liczbach naturalnych x, y , i to w liczbach naturalnych najmniejszych, wystarczy podstawiać za y kolejne liczby naturalne i badać, czy liczba $Dy^2 + 1$ jest kwadratem liczby naturalnej. Jeżeli y będzie najmniejszą liczbą naturalną, dla której $Dy^2 + 1$ będzie kwadratem, powiedzmy, liczby naturalnej x , to (x, y) będzie rozwiązaniem równania (5) w liczbach naturalnych najmniejszych. W ten sposób łatwo byłoby znaleźć dla $D = 2, 3, 5, 6, 7, 8, 10, 11, 12$ rozwiązania w liczbach naturalnych najmniejszych $(3, 2), (2, 1), (9, 4), (5, 2), (8, 3), (3, 1), (19, 6), (10, 3), (7, 2)$.

Trudniej byłoby tą drogą znaleźć rozwiązanie równania (5) w liczbach naturalnych najmniejszych dla $D = 13$, gdyż jest nim układ $(649, 180)$, albo dla $D = 29$, gdzie takim układem jest $(4901, 1820)$. A już całkiem niemożliwa byłaby ta droga, gdy byśmy chcieli znaleźć rozwiązanie w liczbach naturalnych najmniejszych równania (5) dla $D = 991$, gdyż jest nim układ liczb x, y , gdzie x ma 30, zaś y ma 29 cyfr. Toteż dla znajdowania rozwiązań w liczbach naturalnych najmniejszych równania (5) znaleziono inną drogę, polegającą na rozwijaniu liczby niewymiernej \sqrt{D} na ułamek łańcuchowy i obliczania licznika i mianownika odpowiedniego reduktu tego rozwiązania. Jest rzeczą godną uwagi, że łatwo jest znaleźć wszystkie rozwiązania równania (5) w liczbach wymiernych różnych od zera. W samej rzeczy, przypuśćmy, że x i y są to liczby wymierne, różne od zera, spełniające nasze równanie. Mamy tu więc $x \neq 1$, gdyż w razie $x = 1$ mielibyśmy $Dy^2 = 0$, skąd $y = 0$, wbrew założeniu. Połóżmy $r = 1 - x / y$: będzie to liczba wymierna, różna od zera. Stąd $x = 1 - ry$ i, wstawiając do naszego równania, otrzymujemy $(1 - ry)^2 - Dy^2 = 1$, skąd $-2ry + r^2y^2 - Dy^2 = 0$, co wobec $y \neq 0$ daje $-2r + (r^2 - D)y = 0$; a ponieważ, jak wiemy, $r^2 - D \neq 0$, gdyż D nie jest kwadratem liczby wymiernej więc $y = 2r / (r^2 - D)$, skąd $x = 1 - ry = - (r^2 + D) / (r^2 - D)$. Z drugiej strony jeżeli dla dowolnej liczby wymiernej r różnej od zera położymy $x = - (r^2 + D) / (r^2 - D)$, $y = 2r / (r^2 - D)$ to otrzymamy liczby wymierne różne od zera, spełniające równanie (7), co wynika natychmiast z tożsamości $(r^2 + D)^2 - D(2r)^2 = (r^2 - D)^2$. Wszystkie rozwiązania równania (5) (gdzie D jest liczbą naturalną i, nie będącą kwadratem) w liczbach wymiernych różnych od zera otrzymujemy więc z wzorów

$$x = \frac{r^2 + D}{r^2 - D}, y = \frac{2r}{r^2 - D}$$

gdzie r jest liczbą wymierną $\neq 0$. Przejdźmy z kolei do równań drugiego stopnia o więcej niż dwóch niewiadomych. Przede wszystkim nasuwa się tu równanie

$$(6) \quad x^2 + y^2 = z^2.$$

Liczby naturalne x, y, z , spełniające to równanie, tworzą tak zwany trójkąt pitagorejski. Ograniczę się tu tylko do podania, że wszystkie rozwiązania równania (6) w liczbach naturalnych x, y, z otrzymujemy z wzorów

$$x = (m^2 - n^2)l, y = 2mnl, z = (m^2 + n^2)l$$

gdzie $m, n < m$ i l są to liczby naturalne, po dołączeniu rozwiązań z przestawionymi liczbami x i y . Trudniejsza jest sprawa, gdy chodzi o rozwiązywanie układów dwóch lub więcej równań drugiego stopnia w liczbach naturalnych, na przykład o dowód twierdzenia, że układ dwóch równań

$$x^2 + y^2 = z^2, \quad x^2 - y^2 = t^2$$

nie ma rozwiązań w liczbach naturalnych x, y, z, t , czego dowiódł już Fermat. Udowodniono, że istnieje nieskończenie wiele rozwiązań w liczbach naturalnych x, y, z, t, u, v układu trzech równań

$$(7) \quad x^2 + y^2 = t^2, \quad x^2 + z^2 = u^2, \quad y^2 + z^2 = v^2,$$

na przykład $x = 44, y = 117, z = 240, t = 125, u = 244, v = 267$, ale nie wiemy, czy istnieje choć jedno rozwiązanie w liczbach naturalnych x, y, z, t, u, v , w układzie czterech równań, które otrzymamy dołączając do układu (7) jeszcze równanie

$$x^2 + y^2 + z^2 = w^2$$

Innymi słowy, nie wiemy, czy istnieje prostopadłościan, którego krawędzie, przekątne ścian bocznych i przekątna wewnętrzna byłyby liczbami naturalnymi. Około roku 1220 postawiono

zagadnienie znalezienia liczb wymiernych r , dla których liczby $r^2 + 5$ oraz $r^2 - 5$ byłyby kwadratami liczb wymiernych. Wkrótce po tym Leonardo Pisano znalazł taką liczbę $r = 41/12$. W roku 1931 J. D. Hill znalazł inne takie liczby, na przykład $r = 3344161 / 1494696$. Dziś wiemy, że takich liczb wymiernych jest nieskończenie wiele. Napiszmy liczbę wymierną r w postaci ułamka nieprzywiedlnego x/y . Jeżeli liczby $r^2 + 5$ i $r^2 - 5$ są kwadratami liczb wymiernych, to wynika stąd z łatwości, że liczby $x^2 + 5y^2$ oraz $x^2 - 5y^2$ muszą być kwadratami liczb naturalnych, czyli mamy rozwiązanie w liczbach naturalnych x, y, z i t układu równań

$$(8) \quad x^2 + 5y^2 = z^2, \quad x^2 - 5y^2 = t^2,$$

gdzie liczby x i y są względnie pierwsze. Z drugiej strony jasną jest rzeczą, że z każdego rozwiązania układu równań (8) w liczbach naturalnych x, y, z, t , gdzie liczby x i y są względnie pierwsze, otrzymamy liczbę wymierną $r = x/y$, dla której liczby $r^2 + 5$ i $r^2 - 5$ będą kwadratami liczb wymiernych. Ogólniej zajęto się układem równań

$$(9) \quad x^2 + ky^2 = z^2, \quad x^2 - ky^2 = t^2,$$

gdzie k jest liczbą naturalną > 1 , niepodzielną przez żaden i kwadrat liczby naturalnej > 1 . Można dowieść, że jeżeli liczby x i y są względnie pierwsze i jedna z nich jest parzysta, i jeżeli liczby naturalne x, y, z, t , spełniają równania (9), to wyznaczając liczby x_1, y_1, z_1, t_1 ze wzorów

$$(10) \quad x_1 = x^4 + k^2y^4, \quad y_1 = 2xyzt, \quad z_1 = x^4 + 2kx^2y^2 - k^2y^4, \quad t_1 = |x^4 - 2kx^2y^2 - k^2y^4|$$

otrzymamy liczby naturalne, spełniające równania $x_1^2 + ky_1^2 = z_1^2$, $x_1^2 - ky_1^2 = t_1^2$ gdzie liczby x_1 i y_1 będą względnie pierwsze, y_1 parzyste, oraz $x_1 > x$, $y_1 > y$. Wynika stąd, że jeżeli układ równań (9) ma choć jedno rozwiązanie w liczbach naturalnych x, y, z, t , gdzie liczby x i y są względnie pierwsze i jedna z nich parzysta, to ma on takich rozwiązań nieskończenie wiele. W ten sposób na przykład dla $k = 5$, z rozwiązania $x = 41$, $y = 12$, $z = 49$, $t = 31$ przy pomocy wzorów (10) otrzymujemy rozwiązanie

$$x_1 = 3344161, \quad y_1 = 1494696, \quad z_1 = 4728001, \quad t_1 = 113279,$$

z którego otrzymujemy podaną wyżej liczbę r znaną przez Hilla. Stosując jeszcze raz wzory (10) otrzymalibyśmy liczby x_2, y_2, z_2, t_2 , gdzie liczba x_2 miałaby już 27 cyfr. Przejdźmy teraz do równań stopnia trzeciego. Tu już dla równań o dwóch niewiadomych napotykamy duże trudności. Weźmy na przykład jedno z najprostszych takich równań

$$(11) \quad x^2 - y^3 = 1.$$

Od dawna wiadano, że nie ma ono innych rozwiązań w liczbach naturalnych x, y poza $x = 3$, $y = 2$, ale dowody były nieelementarne. Dopiero niedawno prof. A. W a k u l i c z znalazł dowód elementarny, ale dosyć długi. Można dowieść, że twierdzenie, iż równanie (11) nie ma innych rozwiązań w liczbach naturalnych x, y poza $x = 3$, $y = 2$, jest równoważne twierdzeniu, że żadna liczba trójkątna > 1 nie jest sześcianiem liczby naturalnej, jako też jest równoważne twierdzeniu, że żadne z równań

$$u^3 - 2v^3 = 1, \quad u^3 - 2v^3 = -1$$

nie ma rozwiązań w liczbach naturalnych u i v , gdzie $v > 1$. Nielatwo jest dowieść, że równanie

$$(12) \quad x^2 + 2 = y^3$$

nie ma innych rozwiązań w liczbach naturalnych x, y prócz $x = 5$, $y = 3$, o czym wiedział już w

XVII wieku P. Fermat. Równanie (12) ma jednak inne rozwiązania w liczbach wymiernych, na przykład

$$x = 383 / 1000, y = 129 / 100$$

Trudny jest dowód, że równanie $x^2 - 2 = y^3$ nie ma rozwiązań w liczbach naturalnych x, y . Potrafimy natomiast dowieść w sposób elementarny, że żadne z równań $x^2 + 3 = y^3$ oraz $x^2 - 7 = y^3$ nie ma rozwiązań w liczbach całkowitych x, y . Natomiast równanie $x^2 + 7 = y^3$ ma rozwiązania w liczbach naturalnych, na przykład $x = 1, y = 2$ lub $x = 181, y = 32$. L. J. Mordell dowiódł, że dla każdej liczby całkowitej k równanie $x^2 + k = y^3$ ma skończoną ≥ 0 liczbę rozwiązań w liczbach całkowitych x, y . Udowodniono, że równanie

$$(13) \quad x^3 + y^3 = z^3$$

nie ma rozwiązań w liczbach naturalnych x, y, z ; dowód jest jednak trudny i długi. Łatwiej znacznie jest dowieść, że równanie

$$(14) \quad x^4 + y^4 = z^4$$

nie ma rozwiązań w liczbach naturalnych x, y, z . Równania (13) i (14) są przypadkami szczególnymi równania

$$(15) \quad x^n + y^n = z^n$$

o którym Fermat twierdził już w 1672 r., że nie ma ono rozwiązań w liczbach naturalnych x, y, z , gdy n jest liczbą naturalną > 2 . To tak zwane ostatnie lub wielkiego twierdzenia Fermata udowodnił w 1994 roku angielski matematyk Andrew Wiles w związku z wielkim twierdzeniem Fermata dla wykładnika 3 zauważymy, że można łatwo dowieść, iż dla każdej liczby naturalnej $n \neq 2$ istnieje sześcian liczby naturalnej, będący sumą n sześciąt różnych liczb naturalnych.

Twierdzenie to jest oczywiście prawdziwe dla $n = 1$. Przypuśćmy teraz, że n jest liczbą naturalną i że twierdzenie jest prawdziwe dla liczby $2n - 1$. Istnieją więc liczby naturalne $a_1, a_2, \dots, a_{2n-1}$ takie, iż $a_1 < a_2 < \dots < a_{2n-1}$ oraz $a^3 = a_1^3 + \dots + a_{2n-1}^3$. Stąd i wobec równości $6^3 = 3^3 + 4^3 + 5^3$ mamy $(6a)^3 = (3a_1)^3 + (4a_1)^3 + (5a_1)^3 + (6a_2)^3 + (6a_3)^3 + \dots + (6a_{2n-1})^3$, przy czym wobec $a_1 < a_2 < \dots < a_{2n-1}$, po prawej stronie wypisanej równości mamy $2n + 1$ składników rosnących. Stąd, przez indukcję, wynika prawdziwość naszego twierdzenia dla każdej liczby nieparzystej n . Niech teraz n będzie liczbą parzystą > 2 . Mamy $13^3 = 5^3 + 7^3 + 9^3 + 11^3$: twierdzenie jest więc prawdziwe dla $n = 4$. Niech dalej n będzie liczbą parzystą > 4 , $n = 2k + 2$, gdzie k jest liczbą naturalną > 1 , i przypuśćmy, że twierdzenie jest prawdziwe dla liczby $n - 2 = 2k > 2$. Istnieją więc liczby naturalne $a, a_1, a_2, \dots, a_{2k}$ takie, iż $a_1 < a_2 < \dots < a_{2k}$ oraz $a^3 = a_1^3 + a_2^3 + \dots + a_{2k}^3$. Stąd

$$(6a)^3 = (3a_1)^3 + (4a_1)^3 + (5a_1)^3 + (6a_2)^3 + (6a_3)^3 + \dots + (6a_{2k})^3,$$

gdzie po prawej stronie mamy $2k + 2 = n$ składników rosnących. Przez indukcję wynika stąd, że twierdzenie jest prawdziwe dla każdej liczby parzystej $n > 2$.

Można też dowieść elementarnie, że dla wszelkich liczb naturalnych m i $n > m$ z wyjątkiem układów $m = n = 1$ i $m = 1, n = 2$, istnieje $m + n$ różnych liczb naturalnych $a_1, a_2, \dots, a_m, b_1, b_2, \dots, b_n$ takich, iż

$$a_1^3 + a_2^3 + \dots + a_m^3 = b_1^3 + b_2^3 + \dots + b_n^3.$$

Więc na przykład mamy $9^3 + 10^3 = 1^3 + 12^3$, $7^3 + 8^3 = 1^3 + 5^3 + 9^3$, $1^3 + 12^3 + 15^3 = 2^3 + 10^3 + 16^3$.

Łatwo jest dowieść, że istnieje nieskończenie wiele liczb naturalnych, które są jednocześnie sumami dwóch sześciątów liczb naturalnych i różnicami dwóch sześciątów liczb naturalnych, co wynika natychmiast z tożsamości

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

Trudniej nieco jest dowieść, że istnieje nieskończenie wiele liczb naturalnych będących jednocześnie sumą dwóch sześciątów liczb naturalnych względnie pierwszych jako też różnicą dwóch sześciątów liczb naturalnych względnie pierwszych. Wynika to z tożsamości

$$(i) (27n^3 + 1)^3 + (81n^4 - 6n)^3 = (81n^4 + 3n)^3 - (54n^3 - 1)^3 \text{ dla } n = 1, 2, \dots \text{ i uwagi, że dla}$$

naturalnych n liczby $27n^3 + 1$ i $81n^4 - 6n$ są względnie pierwsze, jako też liczby $81n^4 + 3n$ i $54n^3 - 1$ na względnie pierwsze.

(Że liczby $27n^3 + 1$ i $81n^4 - 6n$ są względnie pierwsze wynika natychmiast z tożsamości $3n^2(81n^4 - 6n) - (9n^3 - 1)(27n^3 + 1) = 1$, że zaś liczby $81n^4 + 3n$ i $54n^3 - 1$ są względnie pierwsze wynika z tożsamości $12n^2(81n^4 + 3n) - (18n^3 + 1)(54n^3 - 1) = 1$.)

Z tożsamości (i) wyprowadzamy też wniosek, że istnieje nieskończenie wiele liczb naturalnych, których sześciąt jest sumą trzech sześciątów liczb naturalnych, z których każde dwie są względnie pierwsze.

Dla dowodu wystarczy jeszcze okazać, że dla $n = 1, 2$, liczba $54n^3 - 1$ jest pierwszą względem każdej z liczb $27n^3 + 1$ i $81n^4 - 6n$, co wynika z tożsamości

$$36n^3(27n^3 + 1) - (18n^3 + 1)(54n^3 - 1) = 1 \text{ i } (18n^3 - 1)(54n^3 - 1) - 12n^2(81n^4 - 6n) = 1.$$

Euler wyraził przypuszczenie, że równanie $x^4 + y^4 + z^4 = t^4$ nie ma rozwiązań w liczbach naturalnych x, y, z, t . W 1945 i, M. Ward dowiódł, że nie ma takich rozwiązań dla $t < 10^4$.

Matematyk węgierski P. Erdős wyraził przypuszczenie, że dla każdej liczby naturalnej $n > 1$ równanie $4xyz = n(xy + yz + zx)$ jest rozwiązalne w liczbach naturalnych x, y . Udowodniono, że przypuszczenie to jest prawdziwe dla każdej liczby naturalnej n takiej iż $1 < n < 141649$ oraz dla nieskończenie wielu innych wartości n ; dowodu jednak dla każdej liczby naturalnej n dotąd nie znamy. Podobne przypuszczenie można by wyrazić dla równania $5xyz = n(xy + yz + zx)$. Zagadnienia te są związane z rozkładaniem liczb wymiernych na tak zwane ułamki proste

Szukanie liczb trójkątnych, których kwadraty są również liczbami trójkątnymi, doprowadza do równania

$$(x^2 + x)^2 = 2(y^2 + y).$$

Nie wiemy, czy ma ono rozwiązanie w liczbach naturalnych x i y inne niż $x = y = 1$ oraz $x = 3, y = 8$. Udowodniono, że jeżeli są takie rozwiązania, to dla nich liczba x musi mieć więcej niż 330 cyfr. Układ dwu równań o czterech niewiadomych

$$x^2 + y^2 = u^4, x + y = v^2$$

ma nieskończenie wiele rozwiązań w liczbach naturalnych x, y, u, v ; rozwiązaniem w liczbach naturalnych najmniejszych [jest znalezione już przez Fermata rozwiązanie, w którym liczby x i y mają po 13 cyfr.

Powiemy jeszcze parę słów o równaniach wykładniczych. Do prostych równań wykładniczych o dwóch niewiadomych doprowadza badanie wymierności czy też niewymierności logarytmów liczb naturalnych, na przykład przy zasadzie 10. Przypuśćmy, że chodzi o logarytm liczby 2 przy zasadzie 10. Gdyby ten logarytm, który, jak wiadomo, jest liczbą dodatnią, był liczbą wymierną, byłby postaci x/y , gdzie x i y są liczbami naturalnymi, i w myśl definicji logarytmów mielibyśmy $10^{x/y} = 2$ skąd $10^x = 2^y$.

Równanie to nie ma, jak łatwo zauważyć, rozwiązań w liczbach naturalnych, gdyż lewa jego strona

jest dla każdej liczby naturalnej x podzielna przez 5, prawa zaś strona, jako potęga liczby 2 o naturalnym wykładniku, podzielna przez 5 być nie może. Wnosimy stąd, że logarytm liczby 2 przy zasadzie 10 jest liczbą niewymierną. Ogólniej można by dowiedzieć, że tylko liczby 10^k , gdzie k jest liczbą całkowitą ($>$, $=$ lub < 0), są liczbami wymiernymi dodatnimi, których logarytmy przy zasadzie 10 są wymierne.

W związku ze znaną równością $3^2 + 4^2 = 5^2$ postawiono pytanie jakie są rozwiązania równania

$$3^x + 4^y = 5^z$$

w liczbach naturalnych x, y, z . Można dowiedzieć elementarnie, że jedynym rozwiązaniem tego równania w liczbach naturalnych x, y, z jest $x = y = z = 2$. Leon Jeśmanowicz dowiódł, że podobną własność mają równania

$$5^x + 12^y = 13^z, 7^x + 24^y = 25^z, 9^x + 40^y = 41^z, 11^x + 60^y = 61^z$$

i postawił pytanie, dotąd nie rozstrzygnięte, czy istnieją liczby naturalne a, b, c , takie iż $a^2 + b^2 = c^2$ i dla których równanie $a^x + b^y = c^z$ miałyby rozwiązanie w liczbach naturalnych x, y, z inne niż $x = y = z = 2$.

A. W a k u l i c z dowiódł, że równanie $5^x + 3 = 2^y$ ma w liczbach naturalnych x, y tylko dwa rozwiązania $x = 1, y = 3$ oraz $x = 3, y = 7$, skąd wynika, że ułamek $1/n(n + 3)$ nie jest ułamkiem dziesiętnym skończonym dla liczb naturalnych n różnych od 1, 3, 5 i 125.

Udowodniono, że równanie

$$(16) \quad x^x y^y = z^z$$

ma nieskończenie wiele rozwiązań w liczbach naturalnych x, y, z różnych od jednośc. Jednym z nich jest $x = 2^{12}3^6, y = 2^83^8, z = 2^{11}3^7$. P. E r d o s przypuszcza, że równanie (16) nie ma rozwiązań w liczbach naturalnych x, y, z większych od jednośc, gdzie liczby x i y są względnie pierwsze.

Od stuleci nie jest rozwiązane zagadnienie, czy równanie

$$(17) \quad x^z - y^t = 1$$

ma rozwiązanie w liczbach całkowitych x, y, z, t większych od 1, różne od $x = 3, y = 2, z = 2, t = 3$. Przypuszczenie, że takich rozwiązań nie ma, znane jest pod nazwą twierdzenia Catalana. R. Hampel dowiódł, że poza podanym wyżej równanie (1) nie ma rozwiązań w liczbach całkowitych x, y, z, t większych od 1, gdzie $x - y = \pm 1$. W. Mnich zapytuje, czy istnieją trzy liczby wymierne, których zarówno suma, jak i iloczyn są równe jednośc. Na to proste pytanie, należące zdawałoby się do zakresu arytmetyki elementarnej, nie potrafimy dać odpowiedzi, chociaż w ostatnich czasach zajmowało się nim wielu wybitnych matematyków. Łatwo natomiast dowiedzieć, że pytanie W. Mnicha jest równoważne pytaniu, czy istnieją trzy liczby całkowite a, b, c , takie iż

$$(a + b + c)^3 = abc \neq 0,$$

a także, że jest ono równoważne pytaniu, czy istnieją trzy liczby całkowite x, y, z , takie iż

$$x^3 + y^3 + z^3 = xyz \neq 0.$$

Jest ono też równoważne pytaniu czy istnieją liczby całkowite u, w, v takie iż

$$u/v + v/w + w/u = 1$$

Z łatwością można dowiedzieć, że nie ma dwóch liczb wymiernych, których zarówno suma, jak i iloczyn są równe jednośc. Natomiast A. Schinzel dowiódł, że dla każdej liczby naturalnej $s > 3$ istnieje nieskończenie wiele układów s liczb wymiernych, których zarówno suma, jak i iloczyn są równe jednośc. Aby na przykład otrzymać nieskończenie wiele układów liczb wymiernych x_1, x_2, x_3, x_4 : takich iż $x_1 + x_2 + x_3 + x_4 = x_1 x_2 x_3 x_4 = 1$ wystarczy przyjąć $x_1 = n^2/n^2 - 1, x_2 = -(1/n^2 - 1), x_3 = n^2 - 1/n, x_4 = -(n^2 - 1)/n$ gdzie $n = 2, 3, \dots$, aby zaś otrzymać nieskończenie wiele układów liczb wymiernych x_1, x_2, x_3, x_4, x_5 gdzie $x_1 + x_2 + x_3 + x_4 + x_5 = x_1 x_2 x_3 x_4 x_5 = 1$, wystarczy przyjąć $x_1 = 1, x_2 = n, x_3 = 1/n, x_4 = -n, x_5 = -1/n$ gdzie $n = 1, 2, \dots$

CZĘŚĆ PIĄTA

BADANIE OKRESOWOŚCI PEWNYCH CIĄGÓW NIESKOŃCZONYCH

Jeżeli każdej liczbie naturalnej n jest przyporządkowana pewna liczba naturalna $f(n)$, to mówimy, że określona jest pewna funkcja liczbowa $f(n)$. Funkcja liczbowa będzie znana, jeżeli znane są wartości $f(n)$ dla każdej liczby naturalnej n , zatem jeżeli znany jest ciąg nieskończony

$$f(1), f(2), f(3), \dots$$

Każda funkcja liczbowa wyznacza więc pewien ciąg nieskończony o wyrazach naturalnych. Z drugiej strony każdy ciąg nieskończony o wyrazach naturalnych

$$(1) \quad u_1, u_2, u_3, \dots$$

określa pewną funkcję liczbową $f(n) = u_n$ (dla $n = 1, 2, \dots$).

Jeżeli wyrazy pewnego ciągu skończonego a_1, a_2, \dots, a_s (mającego s wyrazów) będziemy dalej kolejno wypisywali, nie zmieniając ich porządku, to otrzymany w ten sposób ciąg nieskończony

$$(2) \quad a_1, a_2, \dots, a_s, a_1, a_2, \dots, a_s, a_1, a_2, \dots, a_s \dots$$

nazywamy okresowym, o okresie czystym a_1, a_2, \dots, a_s . Okresowym, o okresie czystym $1, 2, 3, 4, 5$, będzie więc ciąg nieskończony

$$1, 2, 3, 4, 5, 1, 2, 3, 4, 5, 1, 2, 3, 4, 5, \dots$$

Okresowym też, o okresie czystym $1, 4, 2, 8, 5, 7$, będzie ciąg kolejnych cyfr po przecinku w rozwinięciu liczby $1/7$ na ułamek dziesiętny nieskończony:

$$1, 4, 2, 8, 5, 7, 1, 4, 2, 8, 5, 7, 1, 4, 2, 8, 5, 7, \dots$$

Jeżeli przed ciągiem okresowym o okresie czystym dopiszemy dowolną skończoną liczbę $r - 1$ wyrazów, gdzie r jest liczbą naturalną > 1 , na przykład przed ciągiem (2) wyrazy b_1, b_2, \dots, b_{r-1} , to otrzymamy w ten sposób ciąg $b_1, b_2, \dots, b_{r-1}, a_1, a_2, \dots, a_s, a_1, a_2, \dots, a_s, a_1, a_2, \dots, a_s, a_1, a_2, \dots, a_s, \dots$ nazywany ciągiem okresowym o okresie mieszanym a_1, a_2, \dots, a_s .

Wyrazy b_1, b_2, \dots, b_{r-1} nazywamy wyrazami poprzedzającymi okres i mówimy, że okres zaczyna się od r -go wyrazu. Tak na przykład ciąg kolejnych cyfr po przecinku w rozwinięciu liczby $3333/9000$ na ułamek dziesiętny nieskończony, czyli ciąg nieskończony

$$3, 5, 8, 1, 1, 1, \dots$$

będzie okresowym o okresie mieszanym jednowyrazowym 1 , zaczynającym się od czwartego wyrazu, gdzie wyrazami poprzedzającymi okres są $3, 5, 8$. Krócej moglibyśmy powiedzieć: Jeżeli dla danego ciągu nieskończonego (1) istnieją liczby naturalne r i s , takie iż

$$u_{n+s} = u_n \text{ dla } n = r, r + 1, r + 2, \dots,$$

to mówimy, że ciąg (1) jest okresowy i że w nim okres ma s wyrazów $u_r, u_{r+1}, \dots, u_{r+s-1}$ i zaczyna się od r -go wyrazu. Jeżeli w szczególności $r = 1$, to mówimy, że okres jest czysty, w przeciwnym zaś razie, że okres jest mieszany i że poprzedza go $r - 1$ wyrazów ciągu. Niech na przykład, dla naturalnych n , u_n oznacza ostatnią cyfrę liczby 2^n . Mamy tu, dla naturalnych n , $2^{n+4} - 2^n = 2^n(2^4 - 1) =$

$2^n \cdot 15 = 2^{n-1} \cdot 3 \cdot 10$. Liczby 2^{n+4} i 2^n różnią się więc o wielokrotność dziesięciu, a więc mają tę samą ostatnią cyfrę, skąd wynika, że $u_{n+4} = u_n$ dla $n = 1, 2, \dots$. Ciąg (1), czyli ciąg

2, 4, 8, 6, 2, 4, 8, 6, 2, 4, 8, 6, ...

jest tu więc okresowy, o okresie czystym, mającym cztery wyrazy. Niech teraz u_n oznacza resztę z dzielenia liczby 2^n przez 100. Mamy tu dla naturalnych $n \geq 2$

$$2^{n+20} - 2^n = 2^n(2^{20-1}) = 2^n(2^{10-1})(2^{10+1}) = 2^n \cdot 1023 \cdot 1025 = 2^{n-2} \cdot 1023 \cdot 41 \cdot 100.$$

Liczby 2^{n+20} i 2^n różnią się więc o wielokrotność liczby 100, skąd wynika, że $u_{n+20} = u_n$ dla $n \geq 2$. Dla $n = 1$ równość ta nie za chodzi, gdyż $u_{21} - u_1 = 2^{21} - 2 = 2(2^{20} - 1)$ jest (jako podwojona liczba nieparzysta) liczbą niepodzielną przez 4, a więc też, niepodzielną przez 100, skąd $u_{21} \neq u_1$. Ciąg (1), czyli ciąg 2, 4, 1, 8, 16, 32, 64, 28, 56, 12, 24, 48, 96, 92, 84, 68, 36, 72, 44, 88, 76, 52, 4, 8, 16, ... jest okresowym, o okresie mieszanym, mającym 20 wyrazów, poprzedzonym jednym wyrazem 2.

Można dowieść, że gdybyśmy oznaczyli przez u_n resztę z dzielenia liczby 2^n przez 1000, to ciąg (1) byłby okresowym, o okresie mieszanym, mającym 100 wyrazów, poprzedzonych dwoma wyrazami: 2 i 4. Niech teraz $f(n)$ będzie dowolną funkcją liczbową u_1 - dowolną liczbą naturalną, i połączmy, dla naturalnych n , $u_{n+1} = f(u_n)$. Okażemy, że ciąg (1) będzie okresowym wtedy i tylko wtedy, gdy znajdą się w nim dwa wyrazy równe (o różnych wskaźnikach). Z jednej bowiem strony jasną jest rzeczą, że jeżeli ciąg (1) jest okresowy, to muszą się w nim znaleźć dwa wyrazy równe o różnych wskaźnikach. Z drugiej zaś strony, jeżeli takie dwa wyrazy w ciągu (1) istnieją, na przykład $u_{r+s} = u_r$, gdzie r i s są liczbami naturalnymi, to mamy $u_{n+s} = u_n$, dla $n = r$. Ale jeśli przy pewnym naturalnym n mamy $u_{n+s} = u_n$, to $u_{n+1+s} = u_{(n+s)+1} = f(u_{n+s})$, $u_{n+1} = f(u_n)$ i, wobec $u_{n+s} = u_n$, znajdujemy $u_{n+1+s} = u_{n+1}$. Stąd przez indukcję wynika, że $u_{n+s} = u_n$ dla $n \geq r$, a więc ciąg (1) jest okresowy.

W szczególności niech m będzie daną liczbą naturalną i niech $f(n)$ oznacza resztę z dzielenia liczby $10n$ przez m . Ciąg (1), gdzie $u_{n+1} = f(u_n)$ dla $n = 1, 2, \dots$, będzie okresowym, o okresie mającym $\leq m$ wyrazów, gdyż przy naturalnych n liczby $u_{n+1} = f(u_n)$, jako reszty z dzielenia przez m , są nieujemne $\leq m-1$, a więc w ciągu u_2, u_3, \dots, u_{m+2} (mającym $m + 1$ wyrazów) muszą się znaleźć dwie jednakowe liczby. Na przykład dla $u_1 = 2$, $m = 13$ pierwszymi $m + 2 = 15$ wyrazami są

2, 7, 5, 11, 6, 8, 2, 7, 5, 11, 6, 8, 2, 7, 5,

i pierwszymi równymi wyrazami są tu u_1 i u_7 . Ciąg nasz jest zatem okresowy, o okresie czystym, mającym 6 wyrazów 2, 7, 5, 11, 6, 8

Niech teraz $f(n)$ oznacza liczbę, którą otrzymamy, odwracając porządek cyfr liczby $n + 5$ (napisanej w układzie dziesiętnym). Będzie tu więc na przykład $f(4) = 9$, $f(5) = 1$, $f(97) = 201$, $f(405) = 14$. Połączmy $u_1 = 1$, $u_{n+1} = f(u_n)$ dla $n = 1, 2, \dots$. Ciąg (1) będzie więc, jak dowiedliśmy wyżej, okresowym wtedy i tylko wtedy, jeżeli znajdą się w nim dwa jednakowe wyrazy o różnych wskaźnikach. Aby więc zbadać, czy ciąg nasz jest okresowy, możemy szukać w nim dwóch równych wyrazów o różnych wskaźnikach. Jeżeli je znajdziemy, będzie to dowodem okresowości naszego ciągu. Ale gdybyśmy obliczając kolejne wyrazy naszego ciągu, na przykład dwieście pierwszych wyrazów takich równych wyrazów nie znaleźli, nie byłoby to jeszcze dowodem, że ciąg nasz nie jest okresowym, gdyż wyraz równy któremuś z wcześniejszych wyrazów mógłby się znaleźć gdzieś na dalszym miejscu. Dla dowodu, że ciąg nasz nie jest okresowy, należałoby dowieść, że żadnych dwóch równych wyrazów o różnych wskaźnikach w nim nie ma; w przypadku ogólnym nie wiemy, jak można by taki dowód przeprowadzić. Obliczając pierwsze dwieście wyrazów określonego wyżej ciągu (1), otrzymujemy ciąg

1, 6, 11, 61, 66, 17, 22, 72, 77, 28, 33, 83, 88, 39, 44, 94, 99, 401, 604, 906, 119, 921, 624, 926, 139, 441, 644, 946, 159, 461, 664, 966, 179, 481, 684, 986, 199, 402, 704, 907, 219, 422, 724, 927, 239, 442, 744, 947, 259, 462, 764, 967, 279, 482, 784, 987, 299, 403, 804, 908, 319, 423, 824, 928, 339, 443, 844, 948, 359, 463, 864, 968, 379, 483, 884, 988, 399, 404, 904, 909, 419, 424, 924, 929, 439, 444, 944, 949, 459, 464, 964, 969, 479, 484, 984, 989, 499, 405, 14, 19, 69, 47, 25, 3, 8, 31, 63, 86, 19, 42, 74, 97, 201, 602, 706, 117, 221, 622, 726, 137, 241, 642, 746, 157, 261, 662, 766, 177, 281, 682, 786, 197, 202, 702, 707, 217, 222, 722, 727, 237, 242, 742, 747, 257, 262, 762, 767, 277, 282, 782, 787, 297, 203, 802, 708, 217, 223, 822, 728, 337, 243, 842, 748, 357, 263, 862, 768, 377, 283, 882, 788, 397, 204, 902, 709, 417, 224, 922, 729, 437, 244, 942, 749, 457, 264, 962, 769, 477, 284, 982, 789, 497, 205, 12, 71, 67, 27, 23, 82, 78,

w którym żaden wyraz się nie powtarza. Błędny byłby jednak stąd wniosek, że ciąg nasz nie jest okresowy, gdyż obliczając dalsze wyrazy znajdujemy:

38, 34, 93, 89, 49, 45, 5, 1,

a więc powtórzył się wyraz 1. Ciąg nasz jest więc okresowy o okresie czystym, mającym 207 wyrazów.

Gdybyśmy zaś przyjęli $u_1 = 2$, $u_{n+1} = f(u_n)$, dla $n = 1, 2, \dots$ przy tej samej co wyżej funkcji f , otrzymalibyśmy ciąg

2, 7, 21, 62, 76, 18, 32, 73, 87, 29, 43, 84, 98, 301, 603, 806, 118, 321, 623, 826, 138, 341, 643, 846, 158, 361, 663, 866, 178, 381, 683, 886, 198, 302, 703, 807, 218, 322, 723, 827, 238, 342, 743, 847, 258, 362, 763, 867, 278, 382, 783, 887, 298, 303, 803, 808, 318, 323, 823, 828, 338, 343, 843, 848, 358, 863, 868, 378, 383, 883, 888, 398, 304, 903, 809, 418, 324, 923, 829, 438, 344, 943, 849, 458, 364, 963, 869, 478, 384, 983, 889, 498, 305, 13, 81, 68, 37, 24, 92, 79, 48, 35, 4, 9, 41, 64, 96, 101, 601, 606, 116, 121, 621, 626, 136, 141, 641, 646, 156, 161, 666, 176, 181, 681, 686, 196, 102, 701, 607, 216, 122, 721, 627, 236, 142, 741, 647, 256, 162, 761, 667, 276, 182, 781, 687, 296, 103, 801, 608, 316, 123, 821, 628, 336, 143, 841, 648, 356, 163, 861, 668, 376, 183, 881, 688, 396, 104, 901, 609, 416, 124, 921, 629, 436, 144, 941, 649, 456, 164, 961, 669, 476, 184, 981, 689, 496, 105, 11,

a liczba 11 była trzecim wyrazem okresu, rozpoczynającego się od liczby 1. Stąd łatwy wniosek, że ciąg nasz jest okresowy, o okresie mieszanym mającym 207 wyrazów (rozpoczynającym się od liczb 11, 61, 66, . . . , a kończącym się liczbami 45, 5, 1, 6) poprzedzonym przez 186 wyrazów.

Łatwo natomiast można by dać odpowiedź na pytanie, jaki ciąg otrzymamy wychodząc z liczby $u_1 = 3$ i postępując jak wyżej. Ponieważ liczba 3 figurowała w okresie dla $u_1 = 1$, więc otrzymamy tu okres czysty o 207 wyrazach, rozpoczynający się liczbami 3, 8, 31, . . . , a kończący się liczbami 69, 47, 25. Jak więc widzimy, niekiedy dowód okresowości ciągu jest łatwy teoretycznie, ale wymaga długich rachunków. Nie znana jednak dotąd jest odpowiedź na pytanie, czy wychodząc z dowolnej liczby naturalnej u_1 i kładąc $u_{n+1} = f(u_n)$ dla $n = 1, 2, \dots$, gdzie f oznacza określoną wyżej funkcję liczbową otrzymamy zawsze ciąg okresowy o okresie czystym lub mieszanym mającym 207 wyrazów (co udowodniono dla wszystkich naturalnych $n \leq 100$). Jako ćwiczenie polecamy

czytelnikowi dowód, że jeżeli $f(n)$ oznacza liczbę otrzymaną przez odwrócenie porządku cyfr liczby $n + 2$ i jeżeli położymy $u_1 = 1$, zaś $u_{n+1} = f(u_n)$ dla $n = 1, 2, \dots$, to ciąg (1) będzie okresowy o czystym, mającym 81 wyrazów. Niech teraz $f(n)$ oznacza liczbę otrzymaną przez odwrócenie porządku cyfr liczby $n+10$ i niech $u_1 = 1$, zaś $u_{n+1} = f(u_n)$ dla $n = 1, 2, \dots$, Można dowieść (choć nie jest to rzeczą łatwą), że ciąg (1), czyli w danym przypadku ciąg

1, 11, 12, 22, 23, 33, 34, 44, 45, 55, 56, 66, 67, 77, 78, 88, 89, 99, 901, 119, 921, 139, 941, 159, 961, ...

nie jest okresowy i że nie byłby też okresowym ciągiem, który otrzymalibyśmy biorąc jako u_1 dowolną liczbę naturalną ≤ 1010 . Natomiast dla $u_1 = 1011$ otrzymujemy ciąg okresowy o okresie czystym, mającym 18 wyrazów:

1011, 1201, 1121, 1311, 1231, 1421, 1341, 1531, 1451, 1641, 1561, 1751, 1671, 1861, 1781, 1971, 1891, 1091.

Wychodząc z liczby $u_1 = 11000$ otrzymalibyśmy tu okres mieszany o 18 wyrazach, poprzedzony jedną liczbą 11000.

Ogólnej metody badania okresowości dowolnych ciągów liczb całkowitych nie znamy. Powtórzenie się wyrazu ciągu na ogół inie dowodzi jeszcze jego okresowości. W poszczególnych przypadkach stosowane bywają różne metody. Weźmy na przykład ciąg (1), gdzie u_n jest ostatnią cyfrą liczby n^n (napisanej w układzie dziesiętnym), czyli ciąg 1, 4, 7, 6, 5, 6, 3, 6, 9, 0, 1, 6, 3, 6, 5, 6, 7, 4, 9, 0, 1, 4, ...

Można dowieść, że ciąg ten jest okresowy o okresie czystym, mającym 20 wyrazów. Aby tego dowieść, wystarczy okazać, że $u_{n+20} = u_n$ dla $n = 1, 2, \dots$, czyli że dla $n = 1, 2, \dots$ liczby

$(n + 20)^{n+20}$ i n^n mają tę samą ostatnią cyfrę, to zaś będzie udowodnione, jeżeli okażemy, że dla naturalnych n liczb $(n + 20)^{n+20} - n^n$ jest podzielna przez 10. Otóż mamy $(n + 20)^{n+20} - n^n = (n + 20)^{n+20} - n^{n+20} + n^{n+20} - n^n$. Jak wiadomo z algebry, dla naturalnych m, n i k liczba $m^k - n^k$ jest podzielna przez $m - n$: liczba $(n + 20)^{n+20} - n^{n+20}$ jest więc podzielna przez 20 i tym bardziej przez 10.

Wystarczy więc dalej dowieść, że dla naturalnych n liczba $n^{n+20} - n^n$ jest podzielna przez 10, albo, co na to samo wychodzi, że jest podzielna przez 2 i przez 5. Jeżeli n jest liczbą nieparzystą, to liczby n^{n+20} i n^n są obie nieparzyste, jeżeli zaś n jest liczbą parzystą, to liczby te są obie parzyste. W każdym razie różnica ich jest parzysta, a więc po dzielną przez 2. Mamy $n^{n+20} - n^n = n^n (n^{20} - 1)$.

Jeżeli liczba n jest podzielna przez 5, to oczywiście i liczba $n^{n+20} - n^n$ jest podzielna przez 5. Jeżeli zaś liczba n nie jest podzielna przez 5, to przy dzieleniu przez 5 daje resztę 1, 2, 3, lub 4, a wtedy liczba n^4 przy dzieleniu przez 5 daje odpowiednio taką samą resztę, jak liczby $1^4 = 1$, $2^4 = 16$, $3^4 = 81$, lub $4^4 = 256$, a więc zawsze resztę 1, skąd też wynika natychmiast, że liczba $n^{20} = (n^4)^5$ daje przy dzieleniu przez 5 resztę 1, a więc liczba $n^{20} - 1$ jest podzielna przez 5, jak również liczba $n^{n+20} - n^n$ jest podzielna przez 5. Jest ona więc przy wszelkim naturalnym n podzielna przez 5 i przez 2, a więc i przez 10, skąd, jak wiemy, wynika, że $u_{n+20} = u_n$ dla $n = 1, 2, \dots$, a więc, że ciąg nasz jest okresowy, o okresie czystym 20-wyrazowym, c. b. d. o.

Zauważmy, że można dowieść, iż ostatnie cyfry ciągu. $u_n = n^n$ ($n = 1, 2, \dots$) dają okres czysty 20-wyrazowy:

1, 6, 7, 6, 5, 6, 3, 6, 9, 0, 1, 6, 7, 6, 5, 6, 7, 6, 9, 0.

Niech teraz v_1, v_2, v_3, \dots oznacza tak zwany ciąg Fibonacciego, określony przez warunki $v_1 = v_2 = 1$, zaś $v_{n+2} = v_n + v_{n+1}$ dla $n = 1, 2, \dots$ Będzie to więc ciąg

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233,

w którym, poczynając od trzeciego wyrazu, każdy wyraz jest sumą dwóch poprzedzających go wyrazów. Niech dalej m będzie daną liczbą naturalną > 1 , zaś u_n niech oznacza resztę z dzielenia liczby v_n przez m . Okażemy, że ciąg (1) okresowym. Ponieważ liczby u_n ($n = 1, 2, \dots$), jako reszty dzielenia przez liczbę naturalną m , są liczbami całkowitymi nieujemnymi $< m$, więc różnych układów (u_n, u_{n+1}) , ($n = 1, 2, \dots$) jest $\leq m^2$, gdyż są to układy dwóch liczb w ciągu $0, 1, 2, \dots, m - 1$.

Zatem w ciągu $m^2 + 1$ układów

$$(u_1, u_2), (u_2, u_3), (u_3, u_4), \dots, (u_{m^2+1}, u_{m^2+2})$$

co najmniej jeden układ musi się powtórzyć. Istnieją więc liczby naturalne r i s , gdzie $r < s \leq m^2 + 1$, takie iż (u_r, u_{r+1}) jest tym samym układem co (u_s, u_{s+1}) , zatem $u_r = u_s$ i $u_{r+1} = u_{s+1}$. Lecz z definicji ciągu v_1, v_2, \dots wynika, że $v_{r+2} = v_r + v_{r+1}$, zaś $v_{s+2} = v_s + v_{s+1}$; a ponieważ $u_r = u_s$, więc liczba v_r przy dzieleniu przez m daje tę samą resztę co liczba v_s i podobnie wobec $u_{r+1} + u_{s+1}$, liczba v_{r+1} daje przy dzieleniu przez m tę samą resztę co liczba v_{s+1} . Z równości $v_{r+2} = v_r + v_{r+1}$ i $v_{s+2} = v_s + v_{s+1}$ i wynika więc, że liczba v_{r+2} przy dzieleniu przez m daje tę samą resztę co liczba v_{s+2} . Dowodzi to, że $u_{r+2} = u_{s+2}$. Tak więc z równości $u_r = u_s$ i $u_{r+1} = u_{s+1}$ wyprowadziliśmy równość $u_{r+2} = u_{s+2}$. W ten sam sposób z równości $u_{r+1} = u_{s+1}$ i $u_{r+2} = u_{s+2}$ wyprowadzilibyśmy równość $u_{r+3} = u_{s+3}$. Przez indukcję ogólnie wynika stąd równość $u_{r+n} = u_{s+n}$ dla $n = 1, 2, \dots$, skąd natychmiast wynika, że ciąg (1) jest okresowy. Jeżeli $r > 1$, to wobec $v_{r+1} = v_{r-1} + v_r$ oraz $v_{s+1} = v_{s-1} + v_s$ mamy $v_{r-1} = v_{r+1} - v_r$ oraz $v_{s-1} = v_{s+1} - v_s$ skąd wnosimy, że liczba v_{r-1} daje przy dzieleniu przez m tę samą resztę co liczba v_{s-1} , zatem $u_{r-1} = u_{s-1}$. Gdyby było $r - 1 > 1$, to podobnie, wobec $u_r = u_s$ i $u_{r-1} = u_{s-1}$, znaleźlibyśmy $u_{r-2} = u_{s-2}$. W ten sposób dojdziemy do równości $u_1 = u_{s-r+1}$, co dowodzi, że ciąg (1) jest okresowy o okresie czystym, mającym $s - r$ wyrazów. Tak więc, określony przez nas ciąg (1) jest dla każdej liczby naturalnej $m > 1$ okresowy, o okresie czystym, mającym co najwyżej m^2 wyrazów. Okres tworzą wszystkie kolejne wyrazy (1), poprzedzające dwie obok siebie stojące jedynki (dalsze niż dwie pierwsze). W szczególności niech $m = 2$. Ciągiem (1) będzie tu ciąg $1, 1, 0, 1, 1, \dots$, a więc mamy tu $u_4 = u_1 = 1$, $u_5 = u_2 = 1$ skąd, jak wiemy, wynika, że ciąg nasz jest okresowy, o okresie czystym trzy wyrazowym: $1, 1, 0$. Wynika stąd, że w ciągu Fibonacciego v_1, v_2, \dots te i tylko te wyrazy v_n są parzyste, których wskaźnik n jest podzielny przez 3. Niech teraz $m = 3$. Ciągiem (1) będzie tu ciąg $1, 1, 2, 0, 2, 2, 1, 0, 1, 1, \dots$, skąd wynika, że ciąg (1) jest okresowy, o okresie czystym ośmiowyrazowym $1, 1, 2, 0, 2, 2, 1, 0$. Wynika stąd, że w ciągu Fibonacciego te i tylko te wyrazy v_n są podzielne przez 3, których wskaźnik n jest podzielny przez 4. Dla $m = 5$ jako ciąg (1) mamy ciąg $1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1$: jest on więc okresowy o okresie czystym 20-wyrazowym. Wnosimy też, że w ciągu Fibonacciego te i tylko te wyrazy v_n są podzielne przez 5, których wskaźnik jest podzielny przez 5. Dla $m = 6$ czytelnik z łatwością obliczy, że ciąg (1) będzie miał okres czysty o 24 wyrazach oraz że w ciągu Fibonacciego te i tylko te wyrazy są podzielne przez 6, których wskaźnik jest podzielny przez 12. Dla $m = 7$ otrzymujemy okres czysty o 16 wyrazach, a w ciągu Fibonacciego te i tylko te wyrazy są podzielne przez 7, których wskaźnik jest podzielny przez 8. Dla $m = 8$ mamy okres czysty o 12 wyrazach, a w ciągu Fibonacciego te i tylko te wyrazy są podzielne przez 8, których wskaźnik jest podzielny przez 6. Dla $m = 9$ znajdujemy okres czysty o 24 wyrazach, a w ciągu Fibonacciego te i tylko te wyrazy są podzielne przez 9, których wskaźnik jest podzielny przez 12.

Niech teraz $m = 10$. Ciągiem (1) będzie tu ciąg

$1, 1, 2, 3, 5, 8, 3, 1, 4, 5, 9, 4, 3, 7, 0, 7, 7, 4, 1, 5, 6, 1, 7, 8, 5, 3, 8, 1, 9, 0, 9, 9, 8, 7, 5, 2, 7, 9, 6, 5, 1, 6, 7, 3, 0, 3, 3, 6, 9, 5, 4, 9, 3, 2, 5, 7, 2, 9, 1, 0, 1, 1$.

Mamy tu $u_{61} = u_1 = 1$ i $u_{62} = u_2 = 1$, skąd wynika, że ciąg nasz jest okresowy, o okresie czystym mającym 60 wyrazów. W ciągu Fibonacciego natomiast te i tylko te wyrazy są podzielne przez 10, których wskaźnik jest podzielny przez 15. Pozostawiamy czytelnikowi do udowodnienia, że dla $m = 100$ otrzymujemy tu ciąg okresowy o okresie czystym, mającym 300 wyrazów. Co się tyczy ciągu Fibonacciego, to łatwo byłoby dowieść przez indukcję, że dla $n = 1, 2, \dots$ mamy

$$v_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

Natomiast dla ciągu $u_n (n = 1, 2, \dots)$, określonego przez warunki $u_1 = 1, u_2 = 2, u_{n+2} = 5 u_{n+1} = 6 u_n$ dla $n = 1, 2, \dots$, łatwo dowieść przez indukcję, że $u_n = 2^{n-1}$ dla $n = 1, 2, \dots$. Jest bowiem prawdą

dla $n=1$ i $n=2$, zaś w razie prawdziwości dla wzoru dla n i dla $n+1$, znajdujemy $u_{n+2} = 5u_{n+1} - 6u_n = 5 \cdot 2^n - 6 \cdot 2^{n-1} = 2^{n+1}$, co dowodzi prawdziwości wzoru dla $n+2$.

CZĘŚĆ SZÓSTA

JAK ZNALEZIONO NAJWIĘKSZE ZNANE LICZBY PIERWSZE

Na początku XIX wieku największą znaną liczbą pierwszą była liczba $2_{31} - 1 = 2147483647$ mająca 10 cyfr (znaleziona przez Eulera), na początku zaś 1951 roku największą znaną liczbą pierwszą była liczba $2^{127} - 1$, mająca 39 cyfr, a podana jeszcze przez Lucasa, o której w 1914 roku matematyk francuski Fauquemberge dowiódł, że jest pierwszą. We wrześniu 1952 roku stwierdzono za pomocą elektronowych maszyn do liczenia SWAC, że liczba $2^{1279} - 1$, mająca 386 cyfr, jest liczbą pierwszą: była to największa znana wówczas liczba pierwsza. 7 i 9 października 1952 r. stwierdzono za pomocą tychże maszyn, że liczby $2^{2203} - 1$ i $2^{2281} - 1$, mające odpowiednio 634 i 687 cyfr, są pierwsze. Największą znaną dziś liczbą pierwszą jest $2^{2281} - 1 = 4460875 \dots 8132836351$.

Przez znaną liczbę rozumiemy tu taką, której wszystkie kolejne cyfry (w układzie dziesiętnym) potrafimy wypisać. Podkreślamy to dlatego, że mógłby ktoś tak rozumować. Ponieważ, jak wiemy, liczb pierwszych jest nieskończenie wiele, więc istnieją liczby pierwsze większe od liczby $2^{2281} - 1$: oznaczmy przez p najmniejszą z nich. Liczba p jest określoną w zupełności liczbą pierwszą, większą od $2^{2281} - 1$. Wiemy nawet, ile cyfr (w układzie dziesiętnym) ma liczba p . W myśl bowiem twierdzenia Czebyszewa dla naturalnych $n > 1$, między n i $2n$ leży co najmniej jedna liczba pierwsza. Liczba p musi więc leżeć między $2^{2281} - 1$ a $2 \cdot (2^{2281} - 1)$, a ponieważ obie te liczby mają po 687 cyfr (gdyż pierwszą cyfrą liczby $2^{2281} - 1$ jest, jak obliczono, 4), więc i liczba p ma 687 cyfr. Jednakże wszystkich cyfr liczby p nie potrafimy obecnie wypisać i dlatego, w naszym rozumieniu, nie uważamy jej za liczbę znaną (jakkolwiek jest liczbą w zupełności określoną). W tym sensie nie znamy też żadnej liczby pierwszej, mającej dokładnie sto cyfr. Można by jednak dowieść, że takie liczby istnieją, a więc też można określić najmniejszą liczbę pierwszą o stu cyfrach. Ogólniej, z twierdzenia Czebyszewa można z łatwością wyprowadzić, że dla każdej liczby naturalnej s istnieje liczba pierwsza, a nawet więcej niż dwie liczby pierwsze o s cyfrach. W samej rzeczy liczby 10^{s-1} , $2 \cdot 10^{s-1}$, $4 \cdot 10^{s-1}$ i $8 \cdot 10^{s-1}$ mają każda s cyfr, a w myśl twierdzenia Czebyszewa dla $s > 1$ istnieją liczby pierwsze p , q i r takie, iż $10^{s-1} < p < 2 \cdot 10^{s-1} < q < 4 \cdot 10^{s-1} < r < 8 \cdot 10^{s-1}$, i jasną jest rzeczą, że liczby p , q , r mają każda s cyfr. W przypadku zaś $s = 1$ mamy dokładnie cztery liczby pierwsze jednocyfrowe: 2, 3, 5 i 7. Liczb pierwszych dwucyfrowych jest 21, trzycyfrowych jest 143. Można dowieść (choć jest to trudne), że liczba liczb pierwszych s -cyfrowych wzrasta nieograniczenie wraz z s . Nie jest rzeczą przypadku, że największe znane liczby pierwsze mają postać $2^p - 1$, gdzie p jest liczbą pierwszą, a więc są tak zwanymi liczbami Mersenne'a (który się liczbami tej postaci zajmował w połowie XVII stulecia). Przyczyną tego jest to, że dla liczb Mersenne'a znamy twierdzenie pozwalające stosunkowo łatwo (przy użyciu wielkich maszyn do liczenia) sprawdzać, czy liczby takie, mające nawet kilkaset cyfr, są pierwsze, czynnie. Oto to twierdzenie:

Niech m oznacza daną liczbę Mersenne'a $m = 2^p - 1$, gdzie p jest liczbą pierwszą > 2 . Dla liczby naturalnej n oznaczmy przez $f_m(n)$ resztę z dzielenia liczby $n^2 - 2$ przez m . Na to, żeby liczba to była pierwszą, potrzeba i wystarcza, żeby $(q-1)$ -szy wyraz ciągu

$$(1) \quad 4, f_m(4), f_m f_m(4), f_m f_m f_m(4), \dots$$

był równy zero. Dowód tego twierdzenia jest wprawdzie elementarny, ale długi i skomplikowany, więc go tutaj nie podajemy.

A oto jak stosujemy to twierdzenie. Weźmy na przykład liczbę Mersenne'a $m = 2^7 - 1 = 127$. Mamy tu więc $p = 7$. Ciągiem (1), jak łatwo obliczyć, będzie tu ciąg u_1, u_2, \dots , gdzie

$$u_1 = 4, u_2 = 14, u_3 = 67, u_4 = 42, u_5 = 115, u_6 = 0$$

(gdyż $4^2 - 2 = 14$ przy dzieleniu przez 127 daje resztę 14, dalej $14^2 - 2 = 194$ przy tymże dzieleniu daje resztę 67, $67^2 - 2 = 4487$ daje resztę 42, $42^2 - 2 = 1762$ daje resztę 111, zaś $111^2 - 2 = 12319$

przy dzieleniu przez 127 daje resztę 0). A więc $(p - 1)$ -szy wyraz ciągu (1) jest tu zerem, skąd w myśl przytoczonego twierdzenia wnosimy, że liczba 127 jest pierwszą. Oczywiście w tym przypadku łatwiej byłoby stwierdzić, że liczba 127 jest pierwszą, sprawdzając, że nie jest podzielna przez żadną z liczb pierwszych $\sqrt{127}$, to jest przez żadną z liczb 2, 3, 5, 7, 11; ale inaczej byłoby w przypadku, gdyby liczba Mersenne'a m miała kilkaset cyfr, a więc pierwiastek kwadratowy z niej miałby co najmniej sto cyfr (bo przecież nie byłibyśmy w możności dzielić naszej liczby przez wszystkie liczby pierwsze aż do stycyfrowych). Jako drugi przykład weźmy liczbę Mersenne'a $m = 2^{11} - 1 = 2047$. Mamy tu więc $p = 11$. Ciągiem (1), jak łatwo obliczyć, jest tu ciąg u_1, u_2, \dots , gdzie $u_1 = 4, u_2 = 14, u_3 = 194, u_4 = 788, u_5 = 701, u_6 = 119, u_7 = 1877, u_8 = 945, u_9 = 1279, u_{10} = 286$.

A więc $(p - 1)$ -szy wyraz ciągu (1) jest tu różny od zera, co w myśl naszego twierdzenia, dowodzi, że liczba 2047 jest złożoną. Godny uwagi jest fakt, że o pewnej liczbie dowiedliśmy, iż jest złożoną, nie wyznaczając jej rozkładu na dwa mniejsze od niej czynniki naturalne, ani też nie wyznaczając żadnego jej dzielnika pierwszego. Oczywiście w danym przypadku łatwo byłoby znaleźć dzielnik pierwszy liczby 2047, dzieląc ją przez kolejne liczby pierwsze $\sqrt{2047} < 46$, i w ten sposób znaleźlibyśmy dzielnik pierwszy 23 liczby 2047, co, jak podaje I.E. Dickson, jeszcze w XVII wieku znalazł nasz rodak Stanisław Pudłowski. Inaczej jednak byłoby z liczbą $2^{101} - 1$. I tutaj, stosując nasze twierdzenie, przekonano się, że $(p - 1)$ -wszy (a więc setny) wyraz ciągu (1) jest różny od zera, skąd wynika, że liczba $2^{101} - 1$ (mająca 31 cyfr) jest złożoną. Nie znamy jednak dotąd żadnego jej dzielnika pierwszego, ani też żadnego jej rozkładu na dwa czynniki naturalne od niej mniejsze. Oczywiście próbowano tu dzielić naszą liczbę przez kolejne liczby pierwsze, ale widocznie najmniejszy dzielnik pierwszy tej liczby jest bardzo duży (może ma kilkanaście cyfr) i dlatego nie można go było dotąd znaleźć. Podobna sytuacja zachodzi dla liczb Mersenne'a $M_n = 2^n - 1$, gdzie $n = 103, 109, 137, 149, 157, 193, 199, 227, 241$ i 257. Liczba $m = 2^{2281} - 1$ ma 687 cyfr i dla niej trzeba obliczyć 686-ty wyraz ciągu (1), co wymaga 686-ciu podnoszeń do kwadratu liczb mniejszych od m (a więc co najwyżej 687-cyfrowych) oraz tyluż dzieleń tych kwadratów (zmniejszonych o liczbę 2) przez liczbę 687-cyfrową m . Są to rachunki, które istniejące wielkie maszyny elektronowe do liczenia były w stanie wykonać i stwierdzić, że 2280-ty wyraz ciągu (1) jest równy zeru, skąd w myśl naszego twierdzenia wynika, że liczba $M_{2281} = 2^{2281} - 1$ jest liczbą pierwszą. Zbadano też wszystkie liczby Mersenne'a M_n o wskaźnikach $n \leq 2281$ i stwierdzono, że pierwszymi są tylko te z nich, które odpowiadają wskaźnikom $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 617, 1279, 2203$ i 2281.

Do dziś znamy tylko 17 liczb pierwszych Mersenne'a, odpowiadających wypisanym przed chwilą wskaźnikom. Nie wiemy, czy wśród liczb Mersenne'a jest nieskończenie wiele liczb pierwszych. Nie wiemy też, czy wśród liczb M_p o wskaźnikach p pierwszych istnieje nieskończenie wiele złożonych. Poznaliśmy wyżej liczby złożone, dla których nie znamy żadnego ich dzielnika pierwszego (na przykład liczba $2^{101} - 1$). Tu jednak dowód, że ta liczba jest złożoną, wymagał długich rachunków (no i znajomości twierdzenia, na któreśmy się powoływali). Gdyby chodziło tylko o podanie przykładu liczby, o której potrafimy łatwo dowieść, że jest złożoną, ale przy dzisiejszym stanie nauki nie znamy żadnego jej dzielnika pierwszego, to można by podać jako taki przykład liczbę $(2^{101} - 1)^2$. Jest ona złożona, bo jest kwadratem liczby naturalnej większej od jedności, a nie znamy żadnego jej dzielnika pierwszego (oczywiście tego, że czegoś nie znamy, nie trzeba dowodzić: wystarczy to skonstatować, a kto inie wierzy, niech poda taki dzielnik). Znamy tu natomiast rozkład naszej liczby na dwa czynniki naturalne od niej mniejsze. Dla liczb Mersenne'a M_n o wskaźnikach parzystych łatwo jest dać rozkład ich na dwa czynniki naturalne od nich mniejsze, co wynika ze wzoru $M_{2k} = 2^{2k} - 1 = (2^k - 1)(2^k + 1)$: liczby takie są więc złożone. Ogólniej, złożonymi są wszystkie liczby Mersenne'a o wskaźnikach złożonych, jeżeli bowiem a i b są liczbami naturalnymi > 1 , to jak wiadomo z algebry,

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1),$$

przy czym, wobec $ab > a > 1$, mamy $2^{ab} - 1 > 2^a - 1 > 1$, skąd wynika, że liczba $2^{ab} - 1$ (podzielna przez $2^a - 1$) jest złożoną. Ale i niektóre liczby Mersenne'a o wskaźnikach pierwszych są złożone, jak na przykład liczby $M_{11} = 23 \cdot 89$ lub $M_{23} = 47 \cdot 178481$.

Największą liczbą Mersenne'a złożoną o wskaźniku nieparzystym, której rozkład na czynniki

pierwsze jest znany, jest liczba M_{183} , będąca, jak znalazł w 1953 r. E. Gabard, iloczynem pięciu różnych liczb pierwszych, z których trzema najmniejszymi są 7376 i 55633, pozostałe zaś dwie mają odpowiednio 19 oraz 29 cyfr. F. Jakóbczyk wyraził przypuszczenie, że jeżeli p jest liczbą pierwszą, to liczba M_p nie ma żadnego dzielnika będącego kwadratem liczby naturalnej >1 , zaś N. G. W. H. Beeger, dowiódł (w 1939 r.), że dla p pierwszych < 16000 liczba M_{p-1} jest podzielna przez p^2 tylko dla $p = 1093$ i $p = 3511$, obalając w ten sposób przypuszczenie innego matematyka, że liczb takich w ogóle nie ma.

Przed 25 wiekami matematycy chińscy wyrazili przypuszczenie, że dla naturalnych $n > 1$ liczba $2^n - 2$ jest podzielna przez n wtedy i tylko wtedy, gdy n jest liczbą pierwszą. Być może, że sprawdzili to bezpośrednio dla kilkuset kolejnych wartości n , imna przykład dla $1 < n \leq 300$, i ponieważ ich przypuszczenie sprawdzało się w tak wielu przypadkach, wnioskowali, że tak jest zawsze. Przypuszczenie chińskie okazało się jednak fałszywe dla liczby $n = 341$, mianowicie liczba $2^{341} - 2$ jest podzielna przez 341, mimo że liczba $341 = 11 \cdot 31$ jest złożoną. Aby przekonać się, że liczba $2(2^{340} - 1)$ jest podzielna przez 341, zauważymy, że $2^{10} - 1 = 1023 = 3 \cdot 341$, przy tym, jak wiemy z algebry, jeżeli liczba naturalna a jest podzielna przez liczbę naturalną b , to liczba $2^a - 1$ jest podzielna przez liczbę $2^b - 1$. Liczba $2^{340} - 1$ jest więc podzielna przez liczbę $2^{10} - 1$, a więc tym bardziej przez liczbę 341. Warto tu zaznaczyć, że w latach 1680—1681 słynny matematyk Leibniz, opierając się na fałszywym rozumowaniu utrzymywał, że przypuszczenie Chińczyków jest prawdziwe. Tak to więc błędy popełniali i wielcy matematycy. Udowodniono później, że liczb naturalnych n , dla których twierdzenie chińskie jest fałszywe, jest nieskończenie wiele. Dla każdej bowiem liczby naturalnej n , dla której twierdzenie chińskie jest fałszywe, łatwo podać liczbę większą, dla której jest ono również fałszywe. Jeżeli bowiem n jest liczbą złożoną, dzielącą się bez reszty liczbę $2^n - 2$, to, jak wiemy, liczba $2^{2n-2} - 1$ jest podzielna przez $2^n - 1$ (gdyż wykładnik $2^n - 2$ jest podzielny przez n), przy czym liczba $2^n - 1$ jest złożona (gdyż n jest złożone). Tak więc jeżeli twierdzenie chińskie jest fałszywe dla liczby naturalnej n , to jest ono fałszywe dla liczby $2^n - 1$ (oczywiście większej od n , gdyż n , jako liczba złożona, jest > 1). Aż, do roku 1950 nie znano żadnej liczby parzystej n , dla której liczba $2^n - 2$ byłaby podzielna przez n . Pierwszą taką liczbę $n = 101038$ znalazł D. H. Lehmer. Później znaleziono więcej takich liczb parzystych i udowodniono, że jest ich nieskończenie wiele. Znaleźć liczbę n Lehmera było trudno, ale sprawdzenie, że dzieli, bez reszty liczbę $2^n - 2$, nie wymaga długich rachunków. Istotnie łatwo sprawdzić, że $n = 2 \cdot 73 \cdot 1103$, zaś $n - 1 = 9 \cdot 29 \cdot 817$, skąd wnosimy, że liczba $2^{n-1} - 1$ jest podzielna przez $2^9 - 1$ oraz przez $2^{29} - 1$, a ponieważ $2^9 - 1 = 7 \cdot 73$, zaś $2^{29} - 1 = 1103 \cdot 486737$, więc liczba $2^{n-1} - 1$ jest podzielna przez liczby pierwsze 73 i 1103, natomiast liczba $2^n - 2$ przez różne liczby pierwsze 2, 73 i 1103, a więc też przez ich iloczyn $u, c \cdot b \cdot d \cdot o$.

Zauważymy tu jeszcze, że udowodniono $M_{M_{13}}$ istnienie nieskończenie wielu par różnych liczb pierwszych p i q takich, iż liczba $2^{pq} - 2$ jest podzielna przez pq . Wypowiadano przypuszczenie, że jeżeli liczba Mersenne'a M_n jest pierwszą, to i liczba M_{M_n} jest pierwszą. Pięcioma najmniejszymi liczbami pierwszymi Mersenne'a są $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ i $M_{13} = 8191$. Dla pierwszych czterech z tych liczb przypuszczenie jest prawdziwe, gdyż liczby M_3 , M_7 , M_{31} i M_{127} są pierwsze. Lecz dla liczby M_{13} przypuszczenie okazało się błędne, gdyż jak obliczył w 1953 r. D. J. Wheeler liczba $M_{M_{13}} = 2^{8191} - 1$ (mająca 2468 cyfr) jest złożona. Wypowiedziano też przypuszczenie, że każdy wyraz ciągu nieskończonego q_1, q_2, q_3, \dots , gdzie $q_1 = 3$, zaś $q_{k+1} = 2^{q_k} - 1$ dla $k = 1, 2, \dots$ jest liczbą pierwszą. Pierwsze cztery wyrazy tego ciągu istotnie są liczbami pierwszymi, gdyż $q_1 = 3$, $q_2 = 7$, $q_3 = 127$, $q_4 = 2^{127} - 1$. Mamy $2^{10} = 1024 > 10^3$, skąd $2^{120} > 10^{36}$, a ponieważ $2^7 = 128 > 102$, więc $2^{127} > 10^{38}$ oraz $q_4 = 2^{127} - 1 \geq 10^{38}$, skąd $q_5 = 2^{q_4} - 1 \geq 2^{10^{38}} - 1 = 2^{10 \cdot 10^{38}} - 1 \geq 10^{3 \cdot 10^{37}}$. Liczba q_5 ma więc więcej niż 10^{37} cyfr i niepodobna jej wypisać, a cóż dopiero badać, czy jest pierwszą. Łatwo jest stawiać przypuszczenia, dotyczące olbrzymich liczb, dla których nie mogą być sprawdzone. Co się tyczy dzielników liczb Mersenne'a, to udowodniono że jeżeli p jest liczbą pierwszą, to każdy dzielnik liczby $2^p - 1$ musi mieć postać $2kp + 1$, gdzie k jest liczbą całkowitą ≥ 0 . Twierdzenie to, którego dowód podamy na końcu części VII, pozwala dla niewielkich wartości p łatwo znaleźć wszystkie dzielniki liczby M_p , a więc i jej rozkład na czynniki

pierwsze. Weźmy na przykład $p = 23$, czyli liczbę $M_{23} = 2^{23} - 1$. W myśl przytoczonego twierdzenia, dzielniki jej muszą mieć postać $46k + 1$, gdzie $k = 0, 1, 2, \dots$. Dla $k = 0$ otrzymujemy dzielnik trywialny 1. Dla $k = 1$ sprawdzamy, czy liczba 47 jest dzielnikiem liczby M_{23} . Dzieląc M_{23} przez 47 otrzymujemy iloraz naturalny $m = 178481$. Wystarczy więc dalej rozkładać tę ostatnią liczbę na czynniki pierwsze. Oczywiście jej dzielniki są dzielnikami liczby M_{23} , a więc też muszą mieć postać $46k + 1$ ($k = 0, 1, 2, \dots$). O ileby liczba m była złożoną, to jak wiemy, miałaby dzielnik pierwszy $\leq \sqrt{m} < 410$: wystarczy więc dzielić liczbę m przez liczby pierwsze postaci $46k + 1$, mniejsze od 410. Jak łatwo sprawdzić, liczbami takimi są tylko 47, 139 i 277. Przez żadną z nich liczba m nie dzieli bez reszty. Dowodzi to, że liczba m jest pierwszą. Liczba M_{23} jest więc iloczynem dwóch liczb pierwszych 17 i 178481.

Dla liczb Mersenne'a łatwo sprawdzić wzór

$$M_n = 1 + 2 + 2^2 + \dots + 2^{n-1} \text{ dla } n = 1, 2, 3, \dots$$

Liczby Mersenne'a są więc sumami cząstkowymi szeregu geometrycznego

$$1 + 2 + 2^2 + 2^3 + \dots$$

W związku z tym nasuwa się pytanie, czy i wśród sum cząstkowych szeregu arytmetycznego, utworzonego z kolejnych liczb naturalnych, $1 + 2 + 3 + 4 + \dots$ znajdują się liczby Mersenne'a. Mamy tu oczywiście: $1 = M_1$, $1 + 2 = M_2$, $1 + 2 + 3 + 4 + 5 = M_4$, a łatwo też sprawdzić, że $M_{12} = 1 + 2 + 3 + \dots + 90$. Dwaj młodzi matematycy polscy, Jerzy Browkin i Andrzej Schinze, udowodnili, że innych liczb Mersenne'a takiej własności nie ma: dowód ich ukazał się w Comptes rendus (sprawozdaniach) Paryskiej Akademii Nauk.

Liczbę $1 + 2 + \dots + n = n(n+1) / 2$, gdzie n jest liczbą naturalną nazywamy trójkątną. Istnieją więc tylko cztery liczby Mersenne'a trójkątne. Można dowieść, że istnieje jedna tylko liczba Mersenne'a kwadratowa, M_1 . Jeżeli a i n są liczbami naturalnymi > 1 , to liczba $a^n - 1$ ma, jak wiadomo, dzielnik $a - 1$, taki iż $1 \leq a - 1 < a^n - 1$. Wynika stąd, że $a^n - 1$ może być pierwszą tylko dla $a = 2$. Nie ma więc liczb pierwszych postaci $a^n - 1$ (gdzie a i n są to liczby naturalne > 1), które nie byłyby liczbami Mersenne'a. Natomiast dla naturalnych $a > 2$ i $n > 1$ istnieją liczby pierwsze postaci $a^n - 1 / a - 1$. W szczególności dla $a = 10$ istnieją liczby pierwsze postaci $10^n - 1 / 9$, a więc których rozwinięcie dziesiętne jest utworzone z samych jedynek, na przykład liczby 11, $10^{23} - 1 / 9$ (dla tej ostatniej liczby dowód, znaleziony przez M. Kraitchika, jest dosyć długi). Nie wiemy, czy takich liczb pierwszych jest nieskończenie wiele.

Liczby Fermata. Badano też liczby postaci $2^{2^n} + 1$, gdzie $n = 1, 2, \dots$. Jeżeli liczba n ma dzielnik nieparzysty $b > 1$, zatem $n = ab$, gdzie a jest liczbą naturalną, to, jak wiemy, liczba $2^n + 1 = (2^a)^b + 1$ jest (wobec nieparzystości b) podzielna przez $2^a + 1$, przy czym $1 < 2^a + 1 < 2^{ab} + 1 = 2^n + 1$, co dowodzi, że liczba $2^n + 1$ jest złożoną. Wynika stąd, że jeżeli liczba $2^n + 1$ jest pierwszą, to liczba n nie może mieć żadnego dzielnika nieparzystego większego od jedności: jest więc n potęgą liczby 2 o wykładniku całkowitym nieujemnym: $n = 2^k$, gdzie k jest liczbą całkowitą ≥ 0 , zatem $2^n + 1 =$

$$2^{2^k} + 1$$

Słynny matematyk P. Fermat w XVII wieku przypuszczał że i twierdzenie odwrotne jest prawdziwe, a więc że wszystkie liczby $F_k = 2^{2^k} + 1$, gdzie $k = 0, 1, 2, \dots$, są pierwsze. Liczby $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, jak łatwo sprawdzić, są pierwsze. Dziwić się należy, że Fermat wypowiadając swe przypuszczenie nie próbował dzielić liczby $F_5 = 4294967297$ przez kolejne liczby pierwsze mniejsze od tysiąca: gdyby był to uczynił (co w czasach Fermata, gdy nie było maszyn do liczenia, było rzeczą uciążliwą, ale wykonalną), byłby stwierdził, że liczba F_5 dzieli się przez 641 i przeto jest złożoną. Później udowodniono, że również liczby F_6 , F_7 , F_8 i F_9 są złożone. Do roku 1953 nie wiedziano, czy liczba F_{10} (mająca 309 cyfr) jest pierwszą, czy też nie. W 1953 r. udowodniono, że jest ona złożoną, podzielna przez liczbę $45592577 = 212 \cdot 11131 + 1$. Udowodniono też (już wcześniej), że liczby F_{11} i F_{12} są złożone. Liczba F_{13} jest najmniejszą liczbą

Fermata, o której dotąd nie wiemy, czy jest pierwszą, czy nie. Podobnie jest z liczbą F_{14} . Natomiast dowiedziano, że liczby F_{15} , F_{16} , F_{18} , F_{23} , F_{36} , F_{38} i F_{73} , są złożone. Liczba F_{73} jest największą liczbą Fermata, o której w r. 1956 wiedziano, że jest złożoną. Znamy też najmniejszy dzielnik pierwszy tej liczby, którym jest liczba $2^{75} \cdot 5 + 1$, mająca 24 cyfry. A ile cyfr ma liczba F_{73} ? Z nierówności $2^{10} > 10^3$ wynika z łatwością, że

$$2^{2^{73}} = 2^{16 \cdot 2^{69}} > 2^{10 \cdot 2^{69}} = (2^{10})^{2^{69}} > (10^3)^{2^{69}} > 10^{2^{70}} = 10^{(2^{10})^7} > 10^{(10^3)^7} = 10^{10^{21}}$$

zatem $F_{73} > 10^{10^{21}}$, skąd wynika, że liczba F_{73} ma więcej niż 10^{21} cyfr (w układzie dziesiętnym).

Ile miejsca by to zajęło, gdybyśmy ją chcieli wypisać? Na jednej stronie druku mieści się przeciętnie 2000 cyfr. Wydrukowanie miliona cyfr zajęłoby więc tom pięćsetstronicowy. Dla wydrukowania 10^{11} cyfr potrzeba by 10^5 , czyli stu tysięcy takich tomów, które wypełniłyby dużą bibliotekę. A więc wydrukowana liczba F_{73} zajęłaby nie mniej niż 10^{10} , czyli miliard dużych bibliotek. Nie podobna więc liczby F_{73} napisać. Jak więc mimo to stwierdzono, że jest podzielna przez liczbę $m = 2^{75} \cdot 5 + 1$? Na to, żeby stwierdzić, że dana liczba a jest podzielna przez liczbę b , niekoniecznie trzeba dokonać dzielenia liczby a wypisanej w układzie dziesiętnym przez liczbę b . Na przykład bez dokonywania takiego dzielenia wiemy, że liczba $2^{2^{73}}$ jest podzielna przez liczbę 2^{100} , gdyż $2^{73} > 100$. Dla stwierdzenia, że liczba F_{73} jest podzielna przez liczbę m , możemy tak postąpić. Przypuśćmy ogólniej, że dla danych liczb naturalnych s i $m > 1$ chodzi nam o zbadanie, czy liczba F_s jest podzielna przez m . Jasną jest rzeczą, że liczba

$F_s = 2^{2^s} + 1$ będzie wtedy i tylko wtedy podzielna przez m , gdy liczba przy 2^{2^s} dzieleniu przez m da resztę $m - 1$. Sprowadza się więc wszystko do tego, jak można obliczyć resztę z dzielenia liczby 2^{2^s} przez m .

Oznaczmy, dla $k = 1, 2, \dots, s$, przez r_k resztę z dzielenia liczby 2^{2^k} przez m . Istnieje więc dla $k = 1, 2, \dots, s$ liczba całkowita $t_k \geq 0$, taka iż $2^{2^k} = t_k m + r_k$, skąd podnosząc do kwadratu, znajdujemy $2^{2^{k+1}} = (t_k^2 m + 2t_k r_k) m + r_k^2$

Wynika stąd natychmiast, że r_{k+1} jest resztą z dzielenia liczby r_k^2 przez m . Jeżeli $m > 4$, to $r_1 = 2^2 = 4$, a każdą z liczb r_2, r_3, \dots, r_s obliczamy kolejno jako resztę z dzielenia kwadratu poprzedzającej liczby przez m .

W szczególności dla $s = 73$, $m = 2^{75} \cdot 5 + 1$ celem obliczenia liczby r_{73} będziemy musieli kilkadziesiąt razy podnosić do kwadratu, a następnie dzielić przez 24-cyfrową liczbę m liczby mniejsze od m , a więc co najwyżej 24-cyfrowe. Przy użyciu współczesnych maszyn do liczenia jest to zadanie wykonalne. W ten sposób stwierdzono podzielność liczby F_{73} przez m . Pozostaje jeszcze do wyjaśnienia pytanie, w jaki sposób natrafiono właśnie na dzielnik m .

Otóż można dowieść, że każdy dzielnik naturalny liczby F_s ma postać $2^{s+2k} + 1$, gdzie k jest liczbą całkowitą nieujemną. Stąd w szczególności dla $s = 73$ wynika, że dzielnikami liczby F_{73} mogą być tylko liczby postępu arytmetycznego $2^{75} k + 1$, gdzie $k = 0, 1, 2, \dots$. Pierwszy wyraz tego postępu daje dzielnik trywialny 1. Wyłożoną wyżej metodą stwierdzamy dalej, że liczba F_{73} , nie jest podzielna przez drugi, trzeci ani czwarty wyraz naszego postępu, natomiast jest podzielna przez piąty jego wyraz, czyli naszą liczbę m . Wynika stąd zarazem, że m jest najmniejszym z większych od jedności dzielników liczby F_{73} , zatem że m jest liczbą pierwszą. W ten sposób znaleziono najmniejszy dzielnik pierwszy liczby F_{73} . Podobnie już w 1878 r., bez pomocy maszyn do liczenia, duchowny rosyjski I. Pierwuszyn znalazł, że liczba F_{12} jest złożona, podzielna przez $2^{14} \cdot 7 + 1$, zaś liczba F_{23} jest złożona, podzielna przez $2^{25} \cdot 5 + 1$. W roku zaś 1953 stwierdzono przy pomocy maszyn elektronowych, że liczba F_{10} (mająca 309 cyfr) jest złożona i podzielna przez $2^{12} \cdot 11131 + 1$. Rachunki dla liczby F_{10} dlatego były znacznie trudniejsze niż dla większej od niej liczby F_{12} , ponieważ najmniejszy dzielnik pierwszy liczby F_{10} okazał się dalekim (11131-szym) wyrazem postępu arytmetycznego, o którym mówiliśmy wyżej: wykrycie go wymagało więc wielu tysięcy

podnoszeń do kwadratu liczb co najwyżej ośmiocyfrowych i dzielen tych kwadratów przez liczbę ośmiocyfrową. W tymże roku 1953 stwierdzono, że liczba F_{16} jest złożona, podzielna przez $2^{18} \cdot 3150 + 1$. Ten ostatni wynik był ciekawy z tego względu, że po obaleniu przez Eulera przypuszczenia Fermata że wszystkie liczby F_n są pierwsze, wysunięto przypuszczenie, iż wszystkie liczby ciągu nieskończonego

$$2 + 1, 2^2 + 1, 2^{2^2} + 1, 2^{2^{2^2}} + 1, 2^{2^{2^{2^2}}} + 1, \dots$$

są pierwsze. Otóż piątym wyrazem tego ciągu jest właśnie liczba F_{16} , a więc przypuszczenie to jest błędne. Liczba F_7 jest najmniejszą liczbą Fermata, dla której nie znamy najmniejszego jej dzielnika pierwszego. Wiemy wprawdzie, że taki dzielnik musi się znajdować w postępie arytmetycznym $512k+1$ ($k = 1, 2, \dots$) i oczywiście próbowano dzielić F_7 , (mającą 39 cyfr) przez wiele kolejnych liczb pierwszych tego postępu ale na dzielnik nie natrafiono: widocznie jest on bardzo dalekim wyrazem tego postępu. Mimo to jednak udowodniono, że liczba F_7 jest złożona. Znane jest bowiem takie twierdzenie:

Na to, żeby liczba Fermata F_s (gdzie s jest daną liczbą naturalną) była pierwszą, potrzeba i wystarcza, żeby liczba

$$3^{F_s-1/2} + 1$$

była podzielna przez F_s . Aby więc stwierdzić, że liczba F_7 nie jest pierwsza, wystarczy się przekonać, że liczba

$$3^{2^{127}} + 1$$

nie jest podzielna przez liczbę $F_7 = 2^{128} + 1$ (mającą 39 cyfr). W tym celu wystarczy znać resztę z dzielenia liczby $3^{2^{127}} + 1$ przez F_7 i okazać, że jest $\neq F_7 - 1$. Reszty zaś r_k z dzielenia liczb

3^{2^k} przez daną liczbę m wyznaczamy (dla $k = 1, 2, \dots$) podobnie, jak wyznaczaliśmy wyżej reszty z dzielenia liczb 2_{2k} przez m . Łatwo tu bowiem dowieść, że r_{k+1} jest resztą z dzielenia r_k przez m . Dla stwierdzenia, że liczba F_7 jest złożona, trzeba więc dokonać 125 podnoszeń do kwadratu liczb mających co najwyżej 39 cyfr, oraz dzielen tych liczb przez liczbę F_7 o 39 cyfrach. Rachunki te wykonali Morehead i Western jeszcze w roku 1909 i w ten sposób stwierdzili, że liczba F_7 jest złożona, w podobny też sposób stwierdzili, że liczba F_8 , mająca 78 cyfr, jest złożona. Nie znamy natomiast dotąd żadnych rozkładów tych liczb na iloczyn dwóch liczb naturalnych większych od jednośc, gdyż podana tu metoda nie daje możności znalezienia takich rozkładów. Można by też powiedzieć, że mamy tu tak zwany nieefektywny dowód istnienia takich rozkładów, mianowicie dowód ich istnienia bez podania konkretnego ich przykładu. Opisana tu metoda mogłaby też być zastosowana do stwierdzenia, że liczba F_{10} jest złożona. Ale dla liczby F_{10} znamy uzyskany inną drogą jej rozkład na iloczyn dwóch liczb naturalnych, większych od jednośc (z których jedną jest $2^{12} \cdot 11131 + 1$). Rozkład taki, jak mówiliśmy wyżej, znany jest i dla liczby F_{16} . Natomiast twierdzenie, które z powodzeniem daje się stosować do badania liczb F_7, F_8 i F_{10} , nie mogłoby być, ze względów technicznych, zastosowane do stwierdzenia, że liczba F_{16} jest złożona, ponieważ liczba F_{16} ma około dwudziestu tysięcy cyfr, a nawet największe obecnie istniejące maszyny do liczenia nie mogą wykonywać dziesiątków tysięcy mnożeń liczb mających około 20 000 cyfr, oraz dzielen kwadratów takich liczb przez liczbę mającą około 20 000 cyfr. Jeżeli zaś metoda, którą wyłożyliśmy przedtem, pozwoliła znaleźć najmniejszy dzielnik pierwszy liczby F_{16} , to tylko dlatego, że był on stosunkowo niewielki (dziewięciocyfrowy). Gdyby najmniejszy dzielnik pierwszy liczby F_{16} miał na przykładowo sto cyfr, nie wiedzielibyśmy dzisiaj czy liczba F_{16} jest pierwszą, czy nie. Dzisiejszy stan naszej wiedzy o liczbach Fermata jest więc luki: znamy tylko pięć liczb pierwszych Fermata F_n , mianowicie dla $n = 0, 1, 2, 3$ i 4 , które zresztą były znane i

Fermatowi. Poza tym nie znamy żadnej innej liczby pierwszej Fermata, natomiast znamy aż 29 liczb złożonych Fermata (dla $n = 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 18, 23, 36, 38, 39, 55, 63, 73, 117, 125, 144, 150, 207, 226, 228, 268, 284, 316, 452$), dla których, z wyjątkiem liczb F_7 i F_8 , znamy co najmniej jeden ich dzielnik pierwszy. Toteż zaryzykowano niedawno przypuszczenie (nie udowodnione ani też nie obalone dotąd), wręcz przeciwne przypuszczeniu Fermata, że wszystkie liczby F_n dla naturalnych $n \geq 5$ są złożone. W każdym razie możemy powiedzieć, że jeżeli chodzi o liczby F_n to wielki Fermat miał tu złą intuicję. W związku z badaniem rozmieszczenia liczb pierwszych nasuwa się pytanie, które z postępów arytmetycznych o naturalnym wyrazie pierwszym a i naturalnej różnicy r zawierają liczby pierwsze i ile ich zawierają. Jeżeli liczby a i r mają największy wspólny dzielnik $d > 1$, i" oczywiście wszystkie wyrazy postępu $a, a + r, a + 2r, \dots$ są podzielne przez d , skąd z łatwością wynika, że najwyżej tylko pierwszy wyraz tego postępu jest liczbą pierwszą. Takie postępy zawierają więc najwyżej jedną liczbę pierwszą. Natomiast, jak tego dowiódł Lejeune-Dirichlet jeszcze w 1837 r., jeżeli liczby naturalne a i r są względnie pierwsze, to postęp arytmetyczny nieskończony

$$(2) a, a + r, a + 2r, a + 3r, \dots$$

zawiera nieskończenie wiele liczb pierwszych. Pierwsze dowody tego twierdzenia były nieelementarne dopiero w ostatnich czasach je zelementaryzowano. Dla pewnych postępów arytmetycznych dowód twierdzenia Lejeune-Dirichleta jest łatwy. Oczywiście jest on na przykład dla postępów $1, 2, 3, 4, \dots$ oraz $1, 3, 5, 7, \dots$ a łatwym dla postępów $2, 5, 8, 13, \dots$ oraz $3, 7, 11, 15, \dots$

Można łatwo okazać, że dla dowodu twierdzenia Lejeune-Dirichleta w całej jego rozciągłości wystarczyłoby udowodnić, że w każdym postępie arytmetycznym (2), gdzie a i r są to liczby naturalne względnie pierwsze, istnieje co najmniej jedna liczba pierwsza. A oto pewne proste, zdawałoby się, pytanie dotyczące liczb pierwszych, na które nie potrafimy dać odpowiedzi.

Wypiszmy w pierwszym wierszu wszystkie kolejne liczby naturalne, pod nimi zaś w drugim wierszu wszystkie kolejne liczby nieparzyste:

$$\begin{array}{l} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots \\ 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, \dots \end{array}$$

W pierwszych kolumnach mogą się znajdować dwie liczby pierwsze, na przykład w drugiej kolumnie liczby 2 i 3, w trzeciej liczby 3 i 5, w siódmej liczby 7 i 13. Następnymi takimi kolumnami byłyby 31-sza, 37-ma, 97-ma, 127-ma, 139-ta, 157-ma, 199-ta, 211-ta i wiele innych. Nie wiemy jednak, czy takich kolumn (w których obie liczby są pierwsze) jest nieskończenie wiele. Pierwszy wiersz jest tu postępowaniem arytmetycznym o pierwszym wyrazie 1 i o różnicy 1, drugi — postępowaniem arytmetycznym o pierwszym wyrazie 1 i o różnicy 2. Dopiszmy jeszcze trzeci wiersz, będący postępowaniem arytmetycznym o pierwszym wyrazie 1 i o różnicy 3, a więc ciąg 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, . - I teraz istnieją kolumny, zawierające we wszystkich trzech wierszach liczby pierwsze, na przykład trzecia (3, 5 i 7), siódma (7, 13 i 19), 37-ma (37, 73 i 109), 271-sza (271, 541, 841). Gdybyśmy jednak dopisali jeszcze czwarty postęp arytmetyczny o pierwszym wyrazie 1 i różnicy 4, czyli postęp

$$1, 5, 9, 13, 17, 21, 25, 29, 33, 37, \dots$$

to niełatwo byłoby znaleźć pierwszą kolumnę, zawierającą cztery liczby pierwsze, innymi słowy, znaleźć najmniejszą liczbę naturalną k , dla której liczby $k + 1, 2k + 1, 3k + 1$ i $4k + 1$ byłyby wszystkie cztery pierwsze: byłoby tu $k = 1530$. Najmniejszą zaś liczbą k , dla której liczby $k + 1, 2k + 1, 3k + 1, 4k + 1$ i $5k + 1$ są pierwsze, jest $k = 10830$. Łatwo natomiast jest znaleźć liczbę naturalną k , dla której liczby $k - 1, 2k - 1, 3k - 1, 4k - 1$ i $5k - 1$ są wszystkie pierwsze: taką jest na przykład liczba $k = 6$. Nasuwa się pytanie, dla jakich naturalnych m istnieją liczby naturalne k , dla których liczby $k - 1, 2k - 1, 3k - 1, \dots, mk - 1$ są wszystkie pierwsze. Odpowiedzi na to pytanie nie

znamy.

CZĘŚĆ SIÓDMA

MAŁE TWIERDZENIE FERMATA

Małe twierdzenie Fermata. Dla każdej liczby całkowitej a oraz liczby pierwszej liczba $a^p - a$ jest podzielna przez p . Dowód. Niech p oznacza daną liczbę pierwszą, a dowolną liczbę całkowitą. Jeżeli liczba a jest podzielna przez p , to twierdzenie jest oczywiście prawdziwe: możemy więc dalej zakładać, że a jest liczbą całkowitą niepodzielną przez p . Wówczas oczywiście przy naturalnym k niepodzielnym przez p liczba $a_k = a^k$ też będzie niepodzielna przez p , a więc będzie przy dzieleniu przez p dawała resztę będącą jednym z wyrazów ciągu

$$(1) \quad 1, 2, 3, p-1$$

Liczby

$$(2) \quad r_1, r_2, \dots, r_{p-1}$$

są więc liczbami ciągu (1), przy czym łatwo dowieść, że jeżeli i i j są to dwie różne liczby ciągu (1), to liczby r_i oraz r_j są różne. Gdyby bowiem było $r_i = r_j$ wynikałoby stąd, że liczby $a_i = a^i$ oraz $a_j = a^j$ dają przy dzieleniu przez p jednakowe reszty, zatem ich różnica, czyli liczba $a_i - a_j = a^i - a^j$ byłaby podzielna przez p i, wobec niepodzielności przez liczbę pierwszą p liczby a , liczba $i - j$ musiałaby być podzielna przez p , co oczywiście jest nie możliwe, skoro i i j są różnymi liczbami ciągu (1).

Wyrazy ciągu (2) o różnych wskaźnikach są więc różnymi wyrazami ciągu (1), a ponieważ w obu ciągach jest ta sama liczba $p - 1$ wyrazów, wynika stąd, że wyrazy ciągu (2) co najwyżej porządkiem różnią się od wyrazów ciągu (1). Zatem

$$(3) \quad 1 \cdot 2 \cdot 3 \dots (p-1) = r_1 \cdot r_2 \dots r_{p-1}$$

Ponieważ a_k przy dzieleniu przez p daje resztę r_k (dla $k = 1, 2, \dots$), więc a_1, a_2, \dots, a_{p-1} przy dzieleniu przez p daje tę samą resztę co r_1, r_2, \dots, r_{p-1} , a wobec (3) tę samą resztę co $(p-1)!$, skąd wniosek, że liczba $a_1, a_2, \dots, a_{p-1} \cdot (p-1)!$ jest podzielna przez p . Lecz $a_1, a_2, \dots, a_{p-1} = 1 \cdot a \cdot 2 \cdot a \cdot 3 \cdot a \cdot \dots \cdot (p-1) \cdot a = (p-1)! \cdot a^{p-1}$; liczba $(p-1)! \cdot a^{p-1} - (p-1)! = (p-1)! [a^{p-1} - 1]$ jest więc podzielna przez p . Lecz pierwszy czynnik tej liczby, $(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1)$, jako iloczyn liczb naturalnych mniejszych od p , nie jest podzielny przez liczbę pierwszą p , skąd wniosek, że drugi czynnik, czyli liczba $a^{p-1} - 1$, dzieli się przez p . Tym bardziej więc liczba $a^p - a = a(a^{p-1} - 1)$ jest podzielna przez p , co dowodzi prawdziwości twierdzenia. Dowiedliśmy też zarazem twierdzenia:

Jeżeli p jest liczbą pierwszą, zaś a liczbą całkowitą niepodzielną przez p , to liczba $a^{p-1} - 1$ jest podzielna przez p . Więc na przykład, dla $p = 11$ wnosimy, że każda z liczb $1^{10} - 1, 2^{10} - 1, 3^{10} - 1, \dots, 10^{10} - 1$ jest podzielna przez 11, innymi słowy, że każda z liczb $1^{10}, 2^{10}, 3^{10}, \dots, 10^{10}$ przy dzieleniu przez 11 daje resztę 1.

Z dowiedzionego przed chwilą twierdzenia wynika, że jeżeli dla liczby naturalnej n i pewnej liczby całkowitej a niepodzielnej przez n liczba $a^n - a$ nie jest podzielna przez n , to n jest liczbą złożoną. Uwaga ta pozwala niekiedy na stwierdzenie, że dana liczba jest złożona. W ten sposób na przykład stwierdzono, że liczba $n = (10^{37} - 1)/9$ (której rozwinięcie dziesiętne składa się z 37 jedynek) jest złożona, gdyż, jak obliczono, liczba $7^{n-1} - 1$ nie jest podzielna przez n . Taki dowód nie daje żadnego rozkładu badanej liczby na iloczyn liczb od niej mniejszych.

Z małego twierdzenia Fermata wynika w szczególności, że jeśli n jest liczbą pierwszą, to $2^n - 2$ jest podzielne przez n . Jak wiemy, przypuszczenie Chińczyków, że twierdzenie to daje się odwrócić, jest błędne, gdyż na przykład liczba $341 = 11 \cdot 31$ nie jest liczbą pierwszą, a jednak liczba $2^{341} - 2$ jest podzielna przez 341. W związku z małym twierdzeniem Fermata zauważymy, że jeżeli dla

pewnej liczby naturalnej $n > 1$ liczba $a^n - a$ jest podzielna przez n przy każdym całkowitym a (co w myśl twierdzenia Fermata zachodzi zawsze, gdy n jest liczbą pierwszą), to liczba n niekoniecznie jest pierwszą. Liczby złożone, mające tę własność, nazwano liczbami bezwzględnie pseudopierwszymi (zachowując nazwę pseudopierwszych dla takich liczb złożonych n , dla których liczba $2^n - 2$ jest podzielna przez n). Liczbami bezwzględnie pseudopierwszymi są na przykład liczby $561 = 3 \cdot 11 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$, $2821 = 7 \cdot 13 \cdot 31 \cdot 61$, $7 \cdot 13 \cdot 31 \cdot 61 \cdot 181$.

Nie wiemy, czy liczb bezwzględnie pseudopierwszych jest nie skończenie wiele. Istnieją liczby pierwsze p oraz liczby całkowite a , dla których $a^{p-1} - 1$ jest podzielne przez p^2 , na przykład $p = 11$, $a = 3$ lub 9 ; $p = 29$, $a = 14$; $p = 37$, $a = 18$; $p = 43$, $a = 19$; $p = 487$, $a = 10$; $p = 1093$, $a = 2$; $p = 3511$, $a = 2$. Udowodniono, że istnieją tylko dwie liczby pierwsze $p < 25000$, dla których $2^{p-1} - 1$ jest podzielne przez p^2 , mianowicie $p = 1093$ i $p = 3511$. Wykładnik, do którego należy dana liczba całkowita według danego modułu. Niech p oznacza daną liczbę pierwszą, zaś a - liczbę całkowitą, niepodzielną przez p . Reszty z dzielenia przez p liczb ciągu

$$(4) a, a^2, a^3, \dots, a^p$$

są (wobec niepodzielności liczby a przez p) liczbami naturalnymi mniejszymi od p : różnych reszt jest więc co najwyżej $p-1$, a ponieważ w ciągu (4) mamy p liczb, więc istnieją wśród nich dwie dające jednakowe reszty przy dzieleniu przez p , na przykład a^k oraz a^{k+h} , gdzie k i h są liczbami naturalnymi, przy czym $k + h \leq p$, zatem $h \leq p - 1$.

Różnica $a^{k+h} - a^k$ jest więc podzielna przez p , a ponieważ $a^{k+h} - a^k = a^k(a^h - 1)$ oraz a^k nie jest podzielne przez liczbę pierwszą p , więc $a^h - 1$ musi być podzielne przez p , czyli a^h przy dzieleniu przez p daje resztę 1. Dowiedliśmy więc, że jeżeli p jest liczbą pierwszą, zaś a liczbą całkowitą niepodzielną przez p , to istnieje liczba naturalna $h \leq p-1$ taka, że liczba a^h przy dzieleniu przez p daje resztę 1. Najmniejszą z takich liczb naturalnych h nazywamy wykładnikiem, do którego liczba a należy według modułu pierwszego p .

Przyjmijmy $p = 7$. Liczba 1 należy oczywiście (według każdego modułu naturalnego) do wykładnika 1. Liczby $2, 2^2, 2^3$ przy dzieleniu przez 7 dają odpowiednio reszty 4 i 1, skąd wnosimy, że liczba 2 należy według modułu 7 do wykładnika 3. Liczby $3, 3^2, 3^3, 3^4, 3^5, 3^6$ przy dzieleniu przez 7 dają odpowiednio reszty 3, 2, 6, 4, 5, 1, zatem liczba 3 należy według modułu 7 do wykładnika 6. Liczby $4, 4^2, 4^3$ przy dzieleniu przez 7 dają odpowiednio reszty 4, 2, 1, zatem liczba 4 należy według modułu 7 do wykładnika 3. Liczby $5, 5^2, 5^3, 5^4, 5^5, 5^6$ przy dzieleniu przez 7 dają odpowiednio reszty 5, 4, 6, 2, 3, 1, zatem liczba 5 należy według modułu 7 do wykładnika 6; Liczby 6 i 6^2 przy dzieleniu przez 7 dają odpowiednio reszty 6 i 1, zatem liczba 6 należy według modułu 7 do wykładnika 2. Twierdzenie 1. Jeżeli p jest liczbą pierwszą, a - liczbą całkowitą, s - liczbą naturalną, i jeżeli liczba $a^s - 1$ jest podzielna przez p , to liczba s jest podzielna przez wykładnik h , do którego należy liczba a według modułu p . Dowód. Przypuśćmy, że liczba s nie jest podzielna przez h , że więc przy dzieleniu liczby s przez h otrzymujemy resztę dodatnią r , oczywiście mniejszą od h . Istnieje więc liczba całkowita nieujemna k taka, iż $s = kh + r$, skąd $a^s - 1 = a^{kh+r} - 1 = (a^{kh} - 1) a^r + (a^r - 1)$. W myśl założenia, lewa strona tego wzoru jest podzielna przez p ; również pierwszy składnik prawej strony jest podzielny przez p , gdyż liczba $a^{kh} - 1 = (a^h)^k - 1$ jest, jak wiadomo, podzielna przez liczbę $a^h - 1$, która jest podzielna przez p , gdyż h jest wykładnikiem, do którego należy a według modułu p . Wynika stąd, że i drugi składnik prawej strony naszego wzoru, czyli liczba $a^r - 1$ jest podzielna przez p , co jest niemożliwe, gdyż r jest liczbą naturalną, mniejszą od h , zaś h jako wykładnik, do którego należy liczba a według modułu p , jest najmniejszą liczbą naturalną, dla której liczba $a^h - 1$ jest podzielna przez p . Założenie, że liczba s nie jest podzielna przez h doprowadza więc do sprzeczności. Udowodniliśmy zatem nasze twierdzenie.

Ponieważ, jak dowiedliśmy wyżej, dla liczby pierwszej p oraz liczby całkowitej a niepodzielnej przez p liczba $a^{p-1} - 1$ jest podzielna przez p , więc w szczególności dla $s = p - 1$, z dowiedzonego przed chwilą twierdzenia wynika: Twierdzenie. Wykładnik h , do którego należy liczba całkowita a niepodzielna przez p według modułu pierwszego p , jest dzielnikiem liczby $p - 1$. Więc na przykład, jak znaleźliśmy wyżej, liczby 1, 2, 3, 4, 5 i 6 należą według modułu pierwszego $p = 7$ do

wykładników 1, 2, 3, lub 6, a te cztery liczby są dzielnikami liczby $p - 1 = 6$. Z dowiedzonego przed chwilą twierdzenia wynika też natychmiast, że wykładnik h , do którego należy liczba całkowita a niepodzielna przez p według modułu pierwszego p , jest $\leq p - 1$. Jeżeli, w szczególności, tym wykładnikiem jest $p - 1$, to mówimy, że liczba a jest pierwiastkiem pierwotnym dla modułu p . Więc na przykład liczby 3 i 5 są pierwiastkami pierwotnymi dla modułu 7. Można dowieść, że dla każdego modułu pierwszego p istnieje co najmniej jeden pierwiastek pierwotny. Pierwiastki pierwotne odgrywają ważną rolę przy różnych badaniach z teorii liczb. Wyprowadzimy teraz następujący wniosek z twierdzenia 1. Wniosek. Jeżeli q jest liczbą pierwszą nieparzystą, to każdy dzielnik naturalny liczby $2^q - 1$ ma postać $2kq + 1$, gdzie k jest liczbą całkowitą nieujemną. Dowód. Iloczyn dwóch liczb postaci $2kq + 1$, gdzie $k = 0, 1, 2, \dots$, jest liczbą tejże postaci, co wynika natychmiast z równości $(2k_1q + 1)(2k_2q + 1) = 2(2k_1k_2q + k_1 + k_2)q$. Stąd zaś wynika przez indukcję, że iloczyn dowolnej skończonej liczby liczb naszej postaci jest również liczbą naszej postaci. Ponieważ liczba 1 jest naszej postaci (przy $k = 0$), zaś każda liczba naturalna > 1 jest iloczynem skończonej liczby liczb pierwszych, więc wystarczy udowodnić nasz wniosek dla dzielników pierwszych liczby $2^q - 1$. Niech, więc p oznacza dzielnik pierwszy liczby $2^q - 1$ i niech h oznacza wykładnik, do którego należy liczba q według modułu p . Liczba $2^q - 1$ jest więc podzielna przez p i z twierdzenia wynika, że liczba q jest podzielna przez h , a ponieważ q jest liczbą pierwszą, więc może tu być tylko $h = 1$ lub $h = q$. Gdyby było $h = 1$, liczba $2^h - 1 = 1$ byłaby podzielna przez p , co jest niemożliwe. A więc $h = q$. Lecz, w myśl twierdzenia, wykładnik h jest dzielnikiem liczby $p - 1$, zatem $p - 1 = tq$, gdzie t jest liczbą naturalną, przy tym parzystą, gdyż liczba q jest, w myśl założenia, nieparzystą, jak również liczba $2^q - 1$, a więc też jej dzielnik p , skąd wynika, że liczba $p - 1$ jest parzysta. Jest więc $t = 2k$, gdzie k jest liczbą naturalną, zatem $p = 2kq + 1$, c.b.d.o. Wniosek nasz został więc udowodniony. Udowodniony wniosek ma zastosowanie przy znajdowaniu dzielników liczb Mersenne'a oraz ich rozkładu na czynniki pierwsze, o czym była mowa w Części VI.

CZĘŚĆ ÓSMA

ROZWINIĘCIE LICZB WEDŁUG ZASADY 10 I INNYCH

Przypuśćmy, że mamy w układzie dziesiętnym wypisaną liczbę naturalną o m cyfrach, którymi, licząc od końca, są c_1, c_2, \dots, c_m , a więc liczbę $x = c_m c_{m-1} \dots c_2 c_1$. Mamy tu oczywiście $c_m c_{m-1} \dots c_2 c_1 = c_m c_{m-1} \dots c_2 \cdot 10 + c_1 = c_m c_{m-1} \dots c_2 \cdot 10 + c_1$ i ostatnia cyfra c_1 jest resztą z dzielenia liczby x przez 10. Oznaczając całość ilorazu z tego dzielenia, czyli liczbę $c_m c_{m-1} \dots c_2$ przez x_1 będziemy więc mieli $x = 10x_1 + c_1$. Z liczbą x_1 możemy postąpić podobnie jak postąpiliśmy z liczbą x , co daje wzór $x_1 = 10x_2 + c_2$, gdzie $x_2 = c_m c_{m-1} \dots c_3$. Podobnie znajdziemy dalej $x_2 = 10x_3 + c_3$ itd., wreszcie $x_{m-2} = 10x_{m-1} + c_{m-1}$, gdzie $x_{m-1} = c_m$. Z wzorów tych znajdujemy z łatwością

$$x = c_1 + 10c_2 + 10^2c_3 + \dots + 10^{m-1}c_m$$

Więc na przykład niech będzie $x = 730151$. Jest tu więc $m = 6$, $730151 = 730150 + 1 = 73015 \cdot 10 + 1$, dalej $x_1 = 73015 = 73010 + 5 = 7301 \cdot 10 + 5$, następnie $x_2 = 7301 = 7300 + 1 = 730 \cdot 10 + 1$, $x_3 = 730 = 73 \cdot 10 + 0$, $x_4 = 73 = 70 + 3 = 7 \cdot 10 + 3$, $x_5 = 7$, stąd $730151 = 1 + 10 \cdot 5 + 10^2 \cdot 1 + 10^3 \cdot 0 + 10^4 \cdot 3 + 10^5 \cdot 7$.

Przypuśćmy teraz, że zamiast liczby 10 wzięliśmy jakąś inną liczbę naturalną $g > 1$. Dla danej liczby naturalnej x podobnie jak wyżej wyznaczmy resztę r_1 z dzielenia liczby x przez g i połączmy $x = gx_1 + r_1$. x_1 będzie tu liczbą całkowitą ≥ 0 . Jeżeli $x_1 > 0$, to postąpmy z liczbą x_1 jak przedtem z liczbą x wyznaczając resztę r_1 z dzielenia x_1 przez g , i połączmy $x_1 = gx_2 + r_2$ itd. Dojdziemy w ten sposób przy pewnym naturalnym m to do wzoru

$$(1) \quad x = r_1 + gr_2 + g^2r_3 + \dots + g^{m-1}r_m$$

gdzie r_1, r_2, \dots, r_m są to liczby całkowite, takie iż $0 \leq r_i \leq g-1$ dla $i = 1, 2, \dots, m$. Liczby takie

nazywamy cyframi przy zasadzie g a rozwinięcie (1) piszemy w postaci

$$(2) \quad x = (r_m r_{m-1} \dots r_2 r_1)_g$$

i nazywamy rozwinięciem liczby x przy zasadzie g .

Każda więc liczba naturalna daje określone w zupełności rozwinięcie przy każdej danej zasadzie naturalnej $g > 1$, a wyżej podaliśmy sposób otrzymania takiego rozwinięcia. Z drugiej strony, mając rozwinięcie (2) liczby x przy zasadzie g , łatwo możemy według wzoru (1) obliczyć jej wartość. Rozwinięcia dziesiętne są tylko przypadkiem szczególnym rozwinięć przy zasadzie g .

Znajdziemy na przykład rozwinięcie liczby 1000, czyli liczby $(1000)_{10}$ przy zasadzie $g = 7$. Dzielimy więc liczbę 1000 przez 7 i otrzymujemy $1000 = 7 \cdot 142 + 6$, zatem resztę 6 (która będzie ostatnią cyfrą przy zasadzie 7) i całość ilorazu 142. Dalej dzielimy 142 przez 7 i otrzymujemy $142 = 7 \cdot 20 + 2$, zatem resztę 2 (która będzie przedostatnią cyfrą przy zasadzie 7) i całość ilorazu 20. Dalej dzielimy 20 przez 7 i otrzymujemy $20 = 7 \cdot 2 + 6$: trzecią od końca cyfrą przy zasadzie 7 będzie więc 6, a czwartą od końca 2 i będzie

$$(1000)_{10} = (2626)_7.$$

Z drugiej strony, w myśl wzoru (2) łatwo byłoby obliczyć, że $(1000)_7 = 7^3 = (343)_{10}$. Czytelnik łatwością też obliczy, że

$$(1000)_{10} = (1111101000)_2 = (1101001)_3 = (33220)_4 = (13000)_5 = (4344)_6 = (2626)_7 = (1750)_8 = (1331)_9$$

$$(1000)_2 = (8)_{10}, (1000)_3 = (27)_{10}, (1000)_4 = (64)_{10}, (1000)_5 = (125)_{10}.$$

Zasada g może być i większa od 10: wówczas wśród cyfr 0, 1, 2, ..., $g-1$ są też i nie mniejsze od 10, które wówczas oznaczać należy albo literami, albo też liczbami wypisanymi w nawiasie. Więc na przykład przy zasadzie $g = 12$ będziemy mieli cyfry 0, 1, 2, ..., 9, (10) i (11). W ten sposób liczba $(1000)_{10}$ da rozwinięcie przy zasadzie 12: $(1000)_{10} = (6(11)4)_{12}$. Każdą liczbę rzeczywistą x , taką iż $0 \leq x < 1$ możemy też rozwinąć na ułamek nieskończony przy każdej danej zasadzie naturalnej $g > 1$ w następujący sposób. Niech $c_1 = E(gx)$ oznacza największą liczbę całkowitą $\leq gx$, zatem liczbę całkowitą c_1 , taką, iż $c_1 \leq gx$, lecz $c_1 + 1 > gx$, skąd $gx - 1 < c_1 \leq gx$, a ponieważ $0 \leq x < 1$, skąd $0 \leq gx < g$, więc $-1 < c_1 < g$, czyli wobec całkowitości liczby c_1 , $0 \leq c_1 \leq g - 1$, co dowodzi, że c_1 jest cyfrą przy zasadzie g . Połóżmy $x_1 = gx - c_1$: będzie więc (wobec $gx - 1 < c_1 \leq gx$) $0 \leq x_1 < 1$ i z liczbą x możemy postąpić jak postąpiliśmy wyżej z liczbą x , kładąc teraz $c_2 = E(gx_1)$, gdzie c_2 będzie cyfrą przy zasadzie g . Dalej położymy $x_2 = gx_1 - c_2$, gdzie będzie $0 \leq x_2 < 1$ i z liczbą x_2 postąpimy podobnie jak wyżej, itd. W ten sposób otrzymamy ciąg nieskończony cyfr c_1, c_2, c_3, \dots przy zasadzie g , oraz ciąg nieskończony liczb rzeczywistych x_1, x_2, \dots , przy czym będzie $x_k = gx_{k-1} - c_k$, dla $k = 0, 1, 2, \dots$, gdzie jako x_0 należy przyjąć x , oraz będzie $0 \leq x_k < 1$ dla $k = 0, 1, 2, \dots$. Z n kolejnych równości

$$x_1 = gx - c_1, x_2 = gx_1 - c_2, \dots, x_n = gx_{n-1} - c_n,$$

które dają

$$x = c_1/g + x_1/g; \quad x_1 = c_2/g + x_2/g, \dots, x_{n-1} = c_n/g + x_n/g,$$

otrzymujemy

$$x = c_1/g + c_2/g^2 + \dots + c_n/g^n + x_n/g^n,$$

skąd, wobec $0 \leq x_n < 1$

$$0 \leq x - (c_1/g^2 + c_2/g^2 + \dots + c_n/g^n) < 1/g^n$$

Liczbę $c_1/g + c_2/g^2 + \dots + c_n/g^n$ oznaczamy przez $(0, c_1, c_2, \dots, c_n)_g$ i nazywamy ułamkiem n-cyfrowym przy zasadzie g. Ułamek ten (w powyższy sposób otrzymany) różni się więc od liczby x mniej niż $1/g^n$, czyli mniej niż $(0,00\dots01)_g$, gdzie po przecinku mamy n-1 zer.

Piszemy też $x = (0, c_1, c_2, c_3, \dots)_g$ i wzór ten nazywamy rozwinięciem liczby x na ułamek nieskończony przy zasadzie g.

Przykłady. Niech $g = 2, x = 1/3$. Mamy tu $c_1 = E2/3 = 0$,

$$x_1 = 2/3, c_2 = E4/3 = 1, x_2 = 4/3 - 1 = 1/3 = x$$

skąd wynika,

że ciąg x, x_1, x_2, \dots jest okresowy, o okresie czystym, złożonym z dwóch wyrazów $1/3$ i $2/3$, a więc ciąg $c_n = E2x_{n-1}$ ($n = 1, 2, \dots$) jest okresowy, o okresie czystym dwu wyrazowym 0 i 1. Mamy więc

$$1/3 = (0,10101\dots)_2$$

Jakoż ze znanego z algebry wzoru na sumę szeregu geometrycznego łatwo sprawdzić, że

$$1/3 = 1/2^2 + 1/2^4 + 1/2^6 + \dots$$

Niech teraz $g = 7, x = 1/2$. Mamy tu $c_1 = E7/2 = 3, x_1 = 7/2 - 3 = 1/2 = x$. Ciąg x, x_1, x_2, \dots jest więc okresowy o okresie czystym, jednowyrazowym $1/2$ zatem i ciąg c_1, c_2, \dots jest okresowy o okresie czystym, jednowyrazowym 3 i mamy rozwinięcie

$$1/2 = (0,333\dots)_7$$

które też łatwo sprawdzić, gdyż w myśl wzoru na sumę szeregu geometrycznego mamy

$$1/2 = 3/7 + 3/7^2 + 3/7^3 + \dots$$

Niech dalej $g = 3, x = 1/11$ Mamy tu

$c_1 = E3/11 = 0, x_1 = 3/11, c_2 = E9/11 = 0, x_2 = 9/11, c_3 = E27/11 = 2, x_3 = 27/11 - 2 = 5/11, c_4 = E15/11 = 1, x_4 = 15/11 - 1 = 4/11, c_5 = E12/11 = 1, x_5 = 12/11 - 1 = 1/11 = x$. Ciąg x, x_1, x_2, \dots jest tu więc okresowy o okresie czystym pięciowyrazowym 0,0, 2,1,1 Mamy więc rozwinięcie

$$1/11 = (0,002110021100211\dots)_3$$

Wzór ten można by sprawdzić dodając do siebie trzy szeregi geometryczne. Łatwo dowieść, że liczby wymierne przy każdej zasadzie naturalnej $g > 1$ dają rozwinięcia okresowe (o okresie czystym lub mieszanym). W samej rzeczy, jeżeli $x = k/m$, gdzie m jest liczbą naturalną, zaś k liczbą całkowitą, taką iż $0 \leq k < m$, to $x_1 = gk/m - E gk/m = k_1/m$, gdzie k_1 jest liczbą całkowitą, taką iż $0 \leq k_1 < m$, a stąd wynika, że dla każdej liczby naturalnej n mamy $x_n = k_n/n$, gdzie k_n jest liczbą całkowitą, taką iż $0 \leq k_n < m$. W ciągu k, k_1, k_2, \dots, k_m co najmniej jeden z wyrazów musi się powtórzyć: to samo dotyczy więc i ciągu x, x_1, x_2, \dots, x_m , a stąd wynika, jak wiemy, okresowość ciągu nieskończonego x, x_1, x_2, \dots , jak też okresowość ciągu c_1, c_2, \dots . Łatwo jest dowieść, że na to aby liczba niecałkowita dawała rozwinięcie skończone przy zasadzie naturalnej $g > 1$, potrzeba i wystarcza, żeby była liczbą wymierną równą ułamkowi nieprzywiedlnemu, którego mianownik ma tylko dzielniki pierwsze, będące dzielnikami zasady g. W szczególności więc te i tylko te liczby niecałkowite dają rozwinięcie skończone na ułamek dziesiętny, które są równe ułamkowi nieprzywiedlnemu o mianowniku, nie mającym innych dzielników pierwszych prócz 2 i 5.

Dla liczb wymiernych zbadano długość okresów ich rozwinięć na ułamki przy zasadzie g, ale odnośne twierdzenia nie są tu zbyt proste. Dla przykładu podamy, że okres rozwinięcia liczby $1/61$ na ułamek dziesiętny ma 60 cyfr, zaś dla liczby $1/1913$ okres ma 1912 cyfr. Okres zaś rozwinięcia dziesiętnego liczby $1/99^2 = 0,00010203...080910111213...969799 \dots$ składa się ze 198 cyfr, a otrzymujemy go wypisując jako dwucyfrowe (a więc uzupełniając jednocyfrowe zerem na początku) kolejne liczby całkowite od 0 do 99, z pominięciem liczby 98. Można dowieść, że w każdym rozwinięciu dziesiętnym nieskończonym występują dowolnie długie ciągi następujących po sobie cyfr, występujące w rozwinięciu (w tym samym porządku) nieskończenie wiele razy. W szczególności w każdym ułamku dziesiętnym nieskończonym co najmniej jedna cyfra występuje nieskończenie wiele razy. Nie potrafimy jednak powiedzieć, która cyfra występuje nieskończenie wiele razy w rozwinięciu dziesiętnym liczby $\sqrt{2}$ albo liczby π . Niech $cc \dots c$ oznacza liczbę, której wszystkie cyfry (w układzie dziesiętnym) są jednakowe, równe c . Więc na przykład $66\dots6$ oznacza którąkolwiek z liczb ciągu $6, 66, 666, 6666, \dots$. Przed dwudziestu laty postawiono pytanie, kiedy liczba $cc\dots c$ jest potęgą liczby naturalnej większej od jednościci o wykładniku większym od jednościci, czyli jest postaci m^n , gdzie m i n są to liczby naturalne > 1 . Dla niektórych cyfr c odpowiedź na to pytanie jest łatwa. Na przykład liczby $22\dots2$ oraz $66\dots6$ nie są takimi potęgami, gdyż, jako kończące się cyfrą 2 lub 6, są to liczby parzyste, niepodzielne przez 4, zaś każda potęga o wykładniku > 1 liczby parzystej musi być podzielna przez 4.

Również łatwo jest rozstrzygnąć nasze pytanie dla liczb $55\dots5$ gdyż liczba 5 nie jest potęgą żadnej liczby naturalnej o wykładniku > 1 , zaś w razie więcej niż jednej cyfry mamy tu liczbę kończącą się na 55, a więc podzielną przez 5, ale niepodzielną przez $5^2 = 25$. Liczba 4 jest postaci $4 = 2^2$, ale liczba $44\dots4$, mająca więcej niż jedną cyfrę, nie jest żądanej postaci, czego można tak dowieść. Liczba ta nie może być potęgą o wykładniku > 2 , gdyż wtedy, jako parzysta, musiałaby być podzielna przez 8, co nie zachodzi, gdyż kończy się na 44. Gdyby zaś nasza liczba była kwadratem, byłaby kwadratem liczby parzystej $(2k)^2$, skąd znaleźlibyśmy $11\dots1 = k^2$. Ale liczba $11\dots1$, jako kończąca się na 11, jak łatwo sprawdzić, nie może być kwadratem liczby naturalnej. Udowodniono też, że liczby $99\dots9$, w razie gdy cyfr jest więcej niż jedna, oraz liczby $33\dots3$, $77\dots7$ jak też $88\dots8$ nie są postaci m^n , gdzie m i n są liczbami naturalnymi > 1 , ale dowody są trudne, natomiast o liczbach $11 \dots 1$ (gdzie cyfr jest więcej niż jedna) wiemy jeszcze tylko, że nie są sześcianami liczb naturalnych.

CZEŚĆ DZIEWIĄTA

TWIERDZENIE WILSONA. TWIERDZENIE THUE'GO. ROZKŁAD LICZBY NA SUMĘ KWADRATÓW, SZESZCIANÓW I BIKWADRATÓW

Twierdzenie Wilsona. Przy dowodzie małego twierdzenia Fermata dowiedliśmy, że jeżeli p jest liczbą pierwszą, zaś a jedną z liczb $1, 2, \dots, p-1$, to reszty z dzielenia przez p liczb $a, 2a, 3a, \dots, (p-1)a$ są wszystkie różne, a więc co najwyżej porządkiem różnią się od liczb ciągu $1, 2, \dots, p-1$. Wynika stąd, że dla każdej liczby a ciągu $1, 2, \dots, p-1$ istnieje jedna i tylko jedna liczba b tego ciągu taka, że ab przy dzieleniu przez p daje resztę 1. Nazwijmy liczbę b odpowiednią dla a . Oczywiście, jeżeli liczba b jest odpowiednią dla a , to liczba a będzie odpowiednią dla b . Niekoniecznie jednak liczba b odpowiednia dla a jest różną od a , bo na przykład liczbą odpowiednią dla $a = 1$ jest oczywiście liczba 1. Liczbą odpowiednią dla $p-1$ jest $p-1$, gdyż $(p-1)^2 = p^2 - 2p + 1$ przy dzieleniu przez p daje resztę 1, a każda liczba ma , jak wiemy, tylko jedną dla niej odpowiednią. Łatwo też dowieść, że poza liczbami 1 i $p-1$ nie ma w ciągu $1, 2, \dots, p-1$ innej, która była równa swej odpowiedniej. Gdyby bowiem a było taką liczbą, to liczba $a^2 - 1 = (a-1)(a+1)$ byłaby podzielna przez p , a więc liczba $a-1$ lub liczba $a+1$ byłaby podzielna przez p , co jest niemożliwe, gdyż $1 \leq a \pm 1 \leq p-1$, a p jest liczbą pierwszą. Tak więc poza liczbami 1 i $p-1$ wszystkie inne liczby ciągu $1, 2, \dots, p-1$, gdzie p jest liczbą pierwszą > 2 , a więc nieparzystą, rozpadają się na pary różnych liczb odpowiednich: $m_1, n_1; m_2, n_2; \dots, m_{p-3/2}, n_{p-3/2}$. Iloczyn $m_i n_i$, gdzie $i = 1, 2, \dots, p-$

$3/2$, przy dzieleniu przez p daje resztę 1 , zaś iloczyn $1 * (p - 1) = p - 1$ przy dzieleniu przez p daje resztę $p - 1$. Stąd łatwy wniosek, że iloczyn $m_1 n_1 m_2 n_2 \dots m_{p-3} / 2 n_{p-3} / 2 \cdot 1 \cdot (p - 1)$ przy dzieleniu przez p daje resztę $p - 1$, a ponieważ iloczyn ten tylko porządkiem czynników różni się od iloczynu $1, 2, 3, \dots (p - 1) = (p - 1)!$, więc liczba $(p - 1)!$ przy dzieleniu przez p daje resztę $p - 1$, zatem liczba $(p - 1)! + 1$ jest podzielna przez p . Udowodniliśmy więc Twierdzenie Wilsona: Jeżeli p jest liczbą pierwszą, to liczba $(p - 1)! + 1$ jest podzielna przez p . Wprawdzie przy dowodzie zakładaliśmy, że p jest, liczbą pierwszą nieparzystą, ale twierdzenie jest oczywiście prawdziwe i dla liczby $p = 2$.

Łatwo dowieść, że twierdzenie to daje się odwrócić: jeżeli dla liczby naturalnej $p > 1$ liczba $(p - 1)! + 1$ jest podzielna przez p , to liczba p jest pierwszą. Gdyby bowiem liczba p była złożoną, zatem $p = ab$, gdzie a i b są liczby naturalne, $a > 1$ i $b > 1$, to liczba $(p - 1)! + 1$, będąc podzielną przez p , byłaby też podzielną przez a , co jest niemożliwe, gdyż liczba $(p - 1)! = 1 \cdot 2 \dots (p - 1)$, wobec $1 < a < p$ (gdyż $b > 1$ i $p = ab > a$) zawiera czynnik a , a więc jest podzielna przez a , i liczba $(p - 1)! + 1$ przy dzieleniu przez a daje resztę 1 . Tak więc na to, żeby liczba naturalna $p > 1$ była pierwszą, potrzeba i wystarcza, żeby liczba $(p - 1)! + 1$ była podzielną przez p . Twierdzenie to jest ważnym twierdzeniem teorii liczb i ma różne zastosowania, ale do praktycznego sprawdzania, czy dana liczba jest pierwszą, nie nadaje się, gdyż już nawet dla dwucyfrowych liczb p wymagałoby to wielkich rachunków. Na przykład dla sprawdzenia, czy liczba 19 jest pierwszą, trzeba by liczbę $18! + 1$ dzielić przez 19 , co byłoby dość uciążliwe. Z twierdzenia Wilsona wyprowadzimy teraz następujący wniosek, z którego skorzystamy później.

Wniosek. Jeżeli p jest liczbą pierwszą postaci $4k + 1$, gdzie k jest liczbą naturalną, to liczba

$$\left[\left(\frac{p-1}{2} \right)! \right]^2 + 1$$

jest podzielna przez p . Dla dowodu zauważymy, że wobec parzystości liczby $p-1/2=2k$ mamy $1 \cdot 2 \cdot 3 \dots p-1/2 = (-1) (-2) \dots (-(p-1/2))$, co przy dzieleniu przez p daje oczywiście taką samą resztę co liczba $(p-1)(p-2) \dots (p-(p-1/2)) = p+1/2(p+1/2 + 1) \dots (p-2)(p-1)$, skąd wnosimy, że liczba

$$\left[\left(\frac{p-1}{2} \right)! \right]^2 + 1, \text{ przy dzieleniu przez } p \text{ daje taką samą resztę co liczba}$$

$$(p-1/2)! p+1/2(p+1/2 + 1) \dots (p-1) = (p-1)!$$

a więc, w myśl twierdzenia Wilsona, resztę $p-1$.

Udowodnimy teraz następujące Twierdzenie Thue'go. Jeżeli m jest liczbą naturalną, zaś a liczbą całkowitą, pierwszą względem m , to istnieją liczby naturalne x i y , obie $\leq \sqrt{m}$, takie, iż przy odpowiednim znaku $+$ lub $-$ liczba $ax \pm y$ jest podzielna przez m . Dowód. Twierdzenie jest oczywiście prawdziwe dla $m = 1$, gdyż wtedy możemy przyjąć $x = y = 1$. Przypuśćmy więc, że m jest liczbą naturalną > 1 i niech q oznacza największą liczbę naturalną $\leq \sqrt{m}$: będzie więc $q + 1 > \sqrt{m}$, zatem $(q+1)^2 > m$. Weźmy pod uwagę liczby całkowite $ax - y$, gdzie x i y przybierają wartość $0, 1, 2, \dots, q$. Liczb takich jest $(q+1)^2 > m$, a ponieważ różnych reszt z ich dzielenia przez m jest tylko m , więc przy dwóch różnych układach x_1, y_1 i x_2, y_2 gdzie na przykład $x_1 \geq x_2$, liczby $ax_1 - y_1$ i $ax_2 - y_2$ muszą przy dzieleniu przez m dawać tę samą resztę, zatem liczba $ax_1 - y_1 - (ax_2 - y_2) = a(x_1 - x_2) - (y_1 - y_2)$ musi być podzielna przez m . Nie może tu być $x_1 = x_2$, gdyż wtedy liczba $y_1 - y_2$ byłaby podzielna przez m , co wobec $0 \leq y_1 \leq q \leq \sqrt{m} < m$ (gdyż $m > 1$) i podobnie $0 \leq y_2 < m$, jest niemożliwe, skoro układy x_1, y_1 i x_2, y_2 są, jak zakładamy, różne. Nie może też tu być $y_1 = y_2$, gdyż wtedy liczba $a(x_1 - x_2)$ byłaby podzielna przez m ; a więc skoro liczba a jest pierwszą względem m , liczba $x_1 - x_2$ byłaby podzielną przez m , co wobec $0 \leq x_1 \leq q < m$ $0 \leq x_2 \leq q$

oraz $x_1 \neq x_2$ jest niemożliwe. Jest więc $x_1 \neq x_2$ oraz $y_1 \neq y_2$. Wobec $x_1 \geq x_2$ liczba $x = x_1 - x_2$ jest więc naturalną, zaś liczba $y_1 - y_2$ - całkowitą, różną od zera, zatem liczba $y = |y_1 - y_2|$ naturalną, przy czym $x = x_1 - x_2 \leq x_1 \leq q \leq \sqrt{m}$, oraz $y \leq q \leq \sqrt{m}$, zaś liczba $a(x_1 - x_2) - (y_1 - y_2) = ax \pm y$ przy odpowiednim znaku jest podzielna przez m . Twierdzenie Thue'go zostało więc udowodnione. Jako łatwy wniosek stąd wyprowadzimy następujące Twierdzenie Fermata. Każda liczba pierwsza postaci $4k + 1$ jest sumą dwóch kwadratów liczb naturalnych. Dowód. W myśl wniosku z twierdzenia Wilsona, jeżeli p jest liczbą pierwszą postaci $4k + 1$, to liczba $a^2 + 1$, gdzie $a = (p-1)/2!$ jest podzielna przez p , przy czym liczba a , jako iloczyn liczb naturalnych $\leq p-1/2 \leq p$ jest pierwszą względem p . W myśl twierdzenia Thue'go (dla $m = p$) istnieją więc liczby naturalne x, y , obie $\leq \sqrt{p}$, takie iż przy odpowiednim znaku $+$ lub $-$ liczba $ax \pm y$ jest podzielna przez p . Wynika stąd, że liczba $a^2x^2 - y^2 = (ax - y)(ax + y)$ jest podzielna przez p , a ponieważ liczba $a^2x^2 + x^2 = (a^2 + 1)x^2$ jest, jak wiemy, podzielna przez p , więc liczba $x^2 + y^2 = (a^2x^2 + x^2) - (a^2x^2 - y^2)$ jest podzielna przez p . Lecz ponieważ x i y są liczbami naturalnymi $\leq \sqrt{p}$, zatem $< \sqrt{p}$, gdyż p , jako liczba pierwsza, nie jest kwadratem liczby naturalnej, więc liczba $x^2 + y^2$ jest naturalną > 1 oraz $< 2p$, a ponieważ jest podzielna przez liczbę pierwszą p , więc musi być równą p . Jest więc $p = x^2 + y^2$, zatem p jest sumą dwóch kwadratów liczb naturalnych, c. b. d. o.

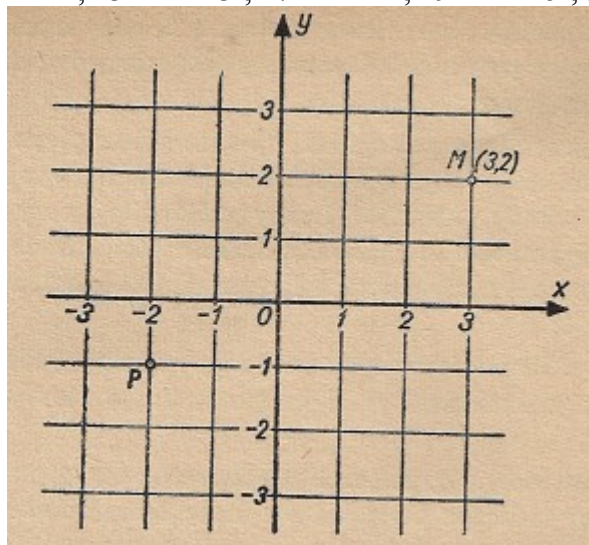
Co się tyczy liczb postaci $4k + 3$ (nie tylko pierwszych), to żadna z nich nie jest sumą dwóch kwadratów liczb całkowitych, gdyż, jak wiemy, kwadrat liczby całkowitej przy dzieleniu przez 4 daje resztę 0 lub 1, zatem suma dwóch kwadratów przy dzieleniu przez 4 może dawać tylko resztę 0, 1 lub 2, a nigdy nie daje reszty 3.

Tuk więc z liczb pierwszych na sumę dwóch kwadratów rozkładają się tylko liczba $2 = 1^2 + 1^2$ oraz liczby pierwsze postaci $4k+1$. Łatwo jest dowieść, że jeżeli nie zwracać uwagi na porządek składników, to liczba pierwsza nie może dawać dwóch różnych rozkładów na sumy kwadratów dwóch liczb naturalnych. Gdyby bowiem liczba pierwsza p dawała dwa takie rozkłady $p = a^2 + b^2 = a_1^2 + b_1^2$, to mielibyśmy

$$p^2 = (a^2 + b^2)(a_1^2 + b_1^2) = (aa_1 + bb_1)^2 + (ab_1 - ba_1)^2 = (aa_1 - bb_1)^2 + (ab_1 + ba_1)^2 \text{ oraz}$$

$(aa_1 + bb_1)(ab_1 + ba_1) = (a^2 + b^2)a_1b_1 + (a_1^2 + b_1^2)ab = p(a_1b_1 + ab)$. Iloczyn ten jest więc podzielny przez p . Jeżeli pierwszy z czynników jest podzielny przez p , to, ponieważ jest on liczbą naturalną, więc $aa_1 + bb_1 \geq p$, zatem $(aa_1 + bb_1)^2 \geq p^2$ i pierwszy z rozkładów liczby p^2 na sumę dwóch kwadratów daje $ab_1 - ba_1 = 0$, czyli $ab_1 = ba_1$, a ponieważ liczby a i b (i podobnie liczby a_1 i b_1) są względnie pierwsze (gdyż kwadrat każdego ich dzielnika wspólnego jest dzielnikiem liczby $p = a^2 + b^2$), więc byłoby $a = a_1$ i $b = b_1$, wbrew założeniu, że rozkłady są różne. Podobnie dochodzimy do sprzeczności, zakładając, że czynnik $ab_1 + ba_1$ jest podzielny przez p .

A oto jedyne rozkłady na sumę dwóch kwadratów (liczb rosnących) liczb pierwszych postaci $4k + 1$ mniejszych od stu $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, $37 =$



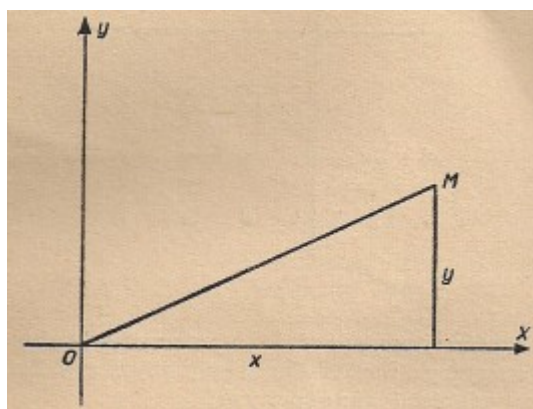
Rysunek 1

$$= 1^2 + 6^2, 41 = 4^2 + 5^2, 53 = 2^2 + 7^2, 61 = 5^2 + 6^2, 73 = 3^2 + 8^2, 89 = 5^2 + 8^2, 97 = 4^2 + 9^2.$$

Wiadomo też jakie liczby naturalne rozkładają się na sumy dwóch kwadratów. Na to żeby liczba naturalna n była sumą dwóch kwadratów liczb całkowitych, potrzeba i wystarcza, żeby iloraz z dzielenia jej przez największy kwadrat, przez który jest podzielna, nie miał żadnego dzielnika postaci $4k + 3$. Na to zaś żeby liczba naturalna była sumą kwadratów dwóch liczb naturalnych, potrzeba i wystarcza, żeby poza wspomnianym przed chwilą warunkiem albo liczba ta miała co najmniej jeden dzielnik pierwszy postaci $4k + 1$, albo też żeby największa potęga liczby 2 ją dzieląca miała wykładnik nieparzysty.

Rozkłady $n = x^2 + y^2$, gdzie x i y są liczbami całkowitymi, $0 \leq x \leq y$, dla wszystkich liczb naturalnych $n \leq 10000$ podał A. van Wijngarden, zaś rozkłady dla $n \leq 20000$ podał H. Gupta

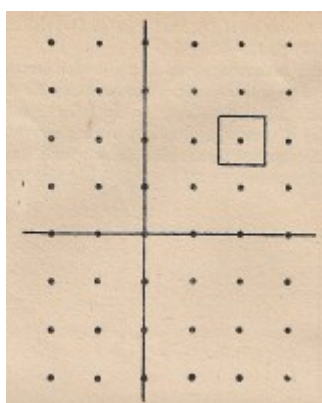
Rozkłady liczb całkowitych na sumy dwóch kwadratów możemy ilustrować geometrycznie. Poprowadźmy na płaszczyźnie proste względem siebie prostopadłe: Ox i Oy (powyższy rysunek). Po obu stronach każdej z nich poprowadźmy szereg równoległych kolejno odległych o jednostkę długości. Równoległe do prostej Ox opatrzymy kolejnymi numerami 1, 2, 3, ... idąc ku górze, zaś



Rysunek 2

numerami -1,-2, ... idąc ku dołowi; podobnie równoległe do osi Oy opatrzymy po prawej stronie kolejno numerami 1, 2, 3, po lewej zaś numerami -1, -2, Same zaś proste Ox i Oy opatrzymy numerami 0.

Obrazem rozkładu $x^2 + y^2$ będziemy nazywali punkt M płaszczyzny, który leży na przecięciu się prostokąta o numerze x do prostej Ox z prostokątem o numerze y do prostej Oy . Więc na przykład obrazem rozkładu $3^2 + 2^2$ będzie punkt M , oznaczony na rysunku 1; obrazem rozkładu $(-2)^2 + (-1)^2$ jest punkt P . Obrazem rozkładu $0^2 + 0^2$ jest punkt O .



Rysunek 3

Ogólnie możemy powiedzieć, że obrazem rozkładu $x^2 + y^2$ jest punkt płaszczyzny o współrzędnych całkowitych x , y . Punkty te nazywamy punktami sieciowymi. Jasną jest rzeczą, że każdemu rozkładowi $x^2 + y^2$ odpowiada pewien punkt sieciowy i że na odwrót, każdy punkt sieciowy jest obrazem pewnego rozkładu na sumę dwóch kwadratów.

Weźmy pod uwagę punkt sieciowy M , który jest obrazem rozkładu $x^2 + y^2$. Na podstawie twierdzenia Pitagorasa odległość OM równa jest $\sqrt{x^2 + y^2}$ (rysunek 2).

Wnosimy stąd, że rozkładom $n = x^2 + y^2$ odpowiadają punkty sieciowe, leżące na

obwodzie koła, zatoczonego promieniem \sqrt{n} dokoła punktu O. Oznaczmy, dla danej liczby n, przez $\tau(n)$ liczbę wszystkich jej rozkładów na sumę dwóch kwadratów $n = x^2 + y^2$. Będzie więc $\tau(n)$ liczbą punktów sieciowych znajdujących się na obwodzie koła, zatoczonego promieniem \sqrt{n} dokoła punktu O, czyli koła, którego równaniem (w geometrii analitycznej) jest $x^2 + y^2 = n$. Jasnym jest też, że liczba $\tau(0) + \tau(1) + \tau(2) + \dots + \tau(n)$ będzie liczbą wszystkich punktów sieciowych, znajdujących się wewnątrz lub na obwodzie koła K zatoczonego promieniem \sqrt{n} dokoła punktu O. Oznaczmy $\tau(1) + \tau(2) + \dots + \tau(n) = T(n)$. Przyporządkujemy każdemu punktowi sieciowemu kwadrat o jednostce pola, mający ów punkt jako środek, a boki równoległe do osi Ox i Oy (rysunek 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 określić stopień tego przybliżenia. Jeżeli mianowicie zakreślimy z punktu O koło o promieniu $\sqrt{n} + 1/\sqrt{2}$, to ponieważ $1/\sqrt{2}$ 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, zatem

$$P < \pi (\sqrt{n} + 1/\sqrt{2})^2$$

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

$$P > \pi (\sqrt{n} - 1/\sqrt{2})^2$$

Wobec $P = 1 + T(n)$ znajdujemy więc dla $T(n)$ nierówności

$$\pi (\sqrt{n} - 1/\sqrt{2})^2 - 1 < T(n) < \pi (\sqrt{n} + 1/\sqrt{2})^2 - 1$$

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

$$0 < \pi/2 - 1 < 1 \leq \sqrt{n}$$

możemy napisać nierówności

$$\begin{aligned} \pi \left(\sqrt{n + \frac{1}{2}} \right)^2 - 1 &= \pi n + \pi \sqrt{2} * \sqrt{n} + \frac{\pi}{2} - 1 < \pi n + 6\sqrt{n} \\ \pi \left(\sqrt{n - \frac{1}{2}} \right)^2 - 1 &= \pi n + \pi \sqrt{2} * \sqrt{n} + \frac{\pi}{2} - 1 > \pi n - 6\sqrt{n} \end{aligned}$$

wobec których ostatnie nierówności dla $T(n)$ dają

$$\pi n - 6\sqrt{n} < T(n) < \pi n + 6\sqrt{n}$$

zatem

$$|T(n) / n - \pi| < 6/\sqrt{n}$$

Niech ϵ będzie dowolną liczbą dodatnią. Dla dostatecznie wielkich n, mianowicie dla $n > 36/\epsilon^2$ będzie $6/\sqrt{n} < \epsilon$ zatem liczba

$T(n)/n - \pi$ jest mniejsza od ϵ . Możemy więc powiedzieć, że dla dostatecznie wielkich n średnia

arytmetyczna

$$T(n)/n = \tau(1) + \tau(2) + \dots + \tau(n) / n$$

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

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

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 dwóch liczb całkowitych. W myśl twierdzenia Gaussa, na to żeby liczba naturalna n była sumą trzech kwadratów liczb całkowitych, potrzeba i wystarcza, żeby n nie było postaci $4^h(8k + 7)$, gdzie h i k są to liczby całkowite ≥ 0 . Wynika stąd, że każda liczba naturalna postaci $8k + 3$ jest sumą trzech kwadratów liczb nieparzystych. Co do liczb naturalnych postaci $8k + 1$, istnieje przypuszczenie, że z wyjątkiem liczb 1 i 25 są one sumami trzech kwadratów liczb naturalnych (Stanisław Gołaszewski sprawdził to przypuszczenie dla liczb ≤ 5000). Łatwo jest natomiast dowieść, że każda liczba całkowita daje się nieskończenie wieloma sposobami przedstawić w postaci $x^2 + y^2 - z^2$, gdzie x , y i z są liczbami naturalnymi. Wynika to natychmiast z tożsamości

$$\begin{aligned} 2k - 1 &= (2t)^2 + (k - 2t^2)^2 - (k - 2t^2 - 1)^2 \\ 2k &= (2t + 1)^2 + (k - 2t^2 - 2t)^2 - (k - 2t^2 - 2t - 1)^2 \end{aligned}$$

dla całkowitych k i t .

Liczby $t_k = k(k+1) / 2$, gdzie $k = 1, 2, \dots$, nazywamy trójkątnymi. Można dowieść, że każda liczba naturalna jest sumą trzech lub mniej liczb trójkątnych (dowód nie jest jednak łatwy). Więc na przykład $1 = t_1$, $2 = t_1 + t_1$, $3 = t_2 = t_1 + t_1 + t_1$, $4 = t_1 + t_2$, $5 = t_1 + t_1 + t_2$, $6 = t_3 = t_2 + t_2$, $7 = t_1 + t_3 = t_1 + t_1 + t_2 + t_2$, $8 = t_1 + t_1 + t_3$, $9 = t_2 + t_2 + t_2 = t_2 + t_3$, $10 = t_4 = t_1 + t_2 + t_3$.

Można dowieść elementarnie, że każda liczba naturalna jest sumą czterech kwadratów liczb całkowitych. Z liczb nieparzystych tylko liczby 1, 3, 5, 9, 11, 17, 29 i 41 nie są sumami czterech kwadratów liczb naturalnych, a z liczb parzystych tylko liczby $4^h \cdot 2$, $4^h \cdot 6$ i $4^h \cdot 14$, gdzie $h = 0, 1, 2, \dots$. Jedynymi liczbami naturalnymi, które nie są sumami pięciu kwadratów liczb naturalnych są liczby 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18 i 33. Każda liczba naturalna > 188 jest sumą pięciu lub mniej kwadratów.

Najmniejszą liczbą, która jest kwadratem liczby naturalnej, a zarazem sumą dwóch kwadratów liczb naturalnych jak też sumą trzech kwadratów liczb naturalnych, jest liczba $169 = 13^2 = 5^2 + 12^2 = 3^2 + 4^2 + 12^2$. Liczba ta jest zarazem sumą czterech, pięciu . . . 155-ciu kwadratów liczb naturalnych, ale nie jest sumą 156-ciu kwadratów liczb naturalnych. Rozkład liczby 169 na sumę dziesięciu kwadratów liczb naturalnych otrzymujemy na przykład ze wzoru $169 = 11^2 + 5^2 + 4^2 + 7 \cdot 1^2$, rozkład zaś na sumę stu kwadratów liczb naturalnych ze wzoru $169 = 23 \cdot 2^2 + 77 \cdot 1^2$.

Rozkłady liczb całkowitych na sumy sześciątów. Łatwo dowieść, że istnieje nieskończenie wiele liczb całkowitych, które nie są sumami trzech (lub mniej) sześciątów liczb całkowitych. Takimi są na przykład wszystkie liczby postaci $9k \pm 4$, gdzie k jest liczbą całkowitą. Wacław Sierpiński wyraził przypuszczenie, że każda liczba całkowita daje się i to nieskończenie wieloma sposobami przedstawić w postaci $x^3 + y^3 - z^3 - t^3$, gdzie x , y , z i t są liczbami naturalnymi. Przypuszczenie to sprawdził dla wszystkich liczb całkowitych o wartości bezwzględnej ≤ 100 oraz dla nieskończenie wielu innych, na przykład dla wszystkich liczb podzielnych przez 3. Dla liczby 2 wynika to na przykład z tożsamości

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

zaś dla liczby 3 z tożsamości

$$3 = (6n^3 + 1)^3 + 1^3 - (6n^3 - 1)^3 - (6n^2)^3 \text{ dla } n = 1, 2, \dots$$

Łatwo jest dowieść, że każda liczba podzielna przez 3 jest sumą czterech sześciątów liczb całkowitych, co wynika bezpośrednio z tożsamości

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

Można stąd łatwo wyprowadzić wniosek, że każda liczba całkowita jest sumą pięciu sześciątów liczb całkowitych, i to na nieskończenie wiele różnych sposobów. Zajmowano się też przedstawieniem liczb całkowitych w postaci $x^3 + y^3 + 2z^3$, gdzie x , y i z są to liczby całkowite. Matematyk chiński Chao Ko dowiódł, że każda liczba naturalna ≤ 100 prócz, być może, liczb 76 i 99 daje się w ten sposób przedstawić. Mamy na przykład

$$13 = (-35)^3 + (-62)^3 + 2 \cdot 52^3, 31 = 52^3 + 31^3 + 2 \cdot (-44)^3.$$

Liczba 76 jest najmniejszą liczbą naturalną, o której nie wiemy, czy daje się przedstawić w postaci $x^3 + y^3 + 2z^3$, gdzie x , y i z są liczbami całkowitymi. Łatwo dowieść, że każda liczba całkowita $\neq 0$ daje skończoną liczbę rozkładów na sumę dwóch sześciątów liczb całkowitych. Natomiast nie każda liczba naturalna ma skończoną liczbę rozkładów na sumę trzech sześciątów liczb całkowitych, na przykład liczba 1 ma nieskończenie wiele takich rozkładów, $1 = 1 + n^3 + (-n)^3$ dla $n = 1, 2, \dots$, albo jeżeli nie chcemy, by dwa sześciany się znosiły: $1 = (9n^4)^3 + (1 - 9n^3)^3 + (3n - 9n^4)^3$ dla $n = 1, 2, \dots$. Można dowieść, że dla każdej liczby naturalnej s istnieje liczba naturalna mająca więcej niż s różnych rozkładów na liczbę dwóch sześciątów liczb naturalnych. Najmniejszą liczbą naturalną, rozkładającą się dwoma różnymi sposobami na sumę dwóch sześciątów liczb naturalnych (jeżeli nie zwracać uwagi im porządek składników), jest liczba $1729 = 10^3 + 9^3 = 12^3 + 1^3$. Najmniejszą liczbą naturalną, rozkładającą się dwoma sposobami na różnicę sześciątów dwóch liczb naturalnych, jest liczba

$$721 = 9^3 - 2^3 = 16^3 - 15^3.$$

Liczba 0 nie rozkłada się na sumę trzech sześciątów liczb całkowitych różnych od zera, ale dowód tego twierdzenia (będącego szczególnym przypadkiem tak zwanego wielkiego twierdzenia Fermata) nie jest łatwy. Natomiast 0 ma nieskończenie wiele rozkładów na sumę czterech sześciątów liczb całkowitych różnych od zera, bo na przykład

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

W inkii 1782 E. Waring wypowiedział bez dowodu twierdzenie, że każda liczba naturalna jest sumą dziewięciu lub mniej sześciątów liczb naturalnych, co udowodnił dopiero w 1909 Wieferich. W roku 1939 L. E. Dickson dowiódł, że każda liczba naturalna z wyjątkiem liczb 23 i 239 jest sumą ośmiu lub mniej sześciątów liczb naturalnych, zaś w 1942 r. J. W. Linnik dowiódł, że każda dostatecznie wielka liczba naturalna jest sumą siedmiu lub mniej sześciątów liczb naturalnych. Nie wiemy jednak, czy istnieje nieskończenie wiele liczb naturalnych, nie będących sumami czterech ani mniej sześciątów liczb naturalnych. Liczby postaci $(k^3 - k)/6$, gdzie k jest liczbą naturalną, zwane są liczbami piramidalnymi. Udowodniono, że każda liczba całkowita jest sumą dziewięciu liczb piramidalnych, zaś każda dostatecznie wielka liczba naturalna jest sumą ośmiu liczb piramidalnych. Istnieje przypuszczenie, że każdy kwadrat liczby naturalnej jest sumą czterech liczb

piramidalnych. Sumy bikwadratów. Waring twierdził, że każda liczba naturalna jest sumą 19-tu czwartych potęg liczb całkowitych. Sprawdzono to dla liczb $< 10^{26}$. Dowiedzono też, że każda liczba naturalna jest sumą 35-ciu czwartych potęg liczb całkowitych, a każda dostatecznie wielka liczba naturalna jest sumą 16-tu czwartych potęg liczb całkowitych. Jest to najlepszy wynik tego rodzaju, gdyż żadna liczba postaci $16^h \cdot 31$, gdzie $h = 0, 1, 2, \dots$, nie jest sumą mniej niż 16-tu bikwadratów. Nie znamy żadnej liczby naturalnej, która by więcej niż dwoma sposobami (jeżeli nie zwracać uwagi na porządek składników) rozkładała się na sumę dwóch czwartych potęg liczb naturalnych. Takie, które rozkładają się dwoma sposobami, są znane, na przykład $133^4 + 134^4 = 59^4 + 158^4$. Każda liczba naturalna jest sumą algebraiczną dwunastu bikwadratów, a każda dostatecznie wielka liczba naturalna jest sumą algebraiczną dziesięciu bikwadratów, i to na nieskończenie wiele sposobów. Nie wiemy natomiast, czy każda dostatecznie wielka liczba naturalna jest sumą algebraiczną dziewięciu bikwadratów. Żadna natomiast liczba postaci $16k + 8$ nie jest sumą algebraiczną mniej niż ośmiu bikwadratów. Zajmiemy się teraz rozkładami na sumy potęg liczb wymiernych. Udowodnimy, że liczba 3 nie jest sumą dwóch kwadratów liczb wymiernych. Przypuśćmy, że liczba 3 jest sumą dwóch kwadratów liczb wymiernych. Sprowadzając te ostatnie do wspólnego mianownika będziemy mieli równanie

$$3 = (x/z)^2 + (y/z)^2,$$

gdzie x i y są liczbami całkowitymi, zaś z jest liczbą naturalną. Stąd $3z^2 = x^2 + y^2$. Istnieją więc liczby naturalne z , dla których $3z^2$ jest sumą kwadratów dwóch liczb całkowitych. Niech z oznacza najmniejszą z takich liczb naturalnych. Wówczas żadna z liczb x i y nie jest podzielna przez 3. Gdyby bowiem jedna z liczb x , y była podzielna przez 3, to z równania $3z^2 = x^2 + y^2$ wynika, że i druga byłaby podzielna przez 3, a więc mielibyśmy $x = 3a$, $y = 3b$, gdzie a i b są liczbami całkowitymi, skąd, w myśl naszego równania, $3z^2 = 9(a^2 + b^2)$, zatem $z^2 = 3(a^2 + b^2)$, co dowodzi, że i liczba z jest podzielna przez 3, zatem $z = 3c$, gdzie c jest liczbą naturalną $< z$ i mamy $3c^2 = a^2 + b^2$, wbrew założeniu, że z jest najmniejszą liczbą naturalną, której potrojony kwadrat jest sumą dwóch kwadratów liczb całkowitych. Żadna z liczb x i y nie jest więc podzielna przez 3. Ale ponieważ liczba całkowita niepodzielna przez 3 przy dzieleniu przez 3 daje resztę 1 lub 2, a więc kwadrat jej przy dzieleniu przez 3 daje zawsze resztę 1, więc suma $x^2 + y^2$ przy dzieleniu przez 3 daje resztę 2, wbrew temu, że jest ona równa $3z^2$. Dowiedliśmy więc, że liczba 3 nie jest sumą kwadratów dwóch liczb wymiernych. Wynika stąd natychmiast, że przy naturalnym n liczba 3^{2n+1} nie jest sumą kwadratów dwóch liczb wymiernych gdyż wtedy i liczba 3 byłaby taką sumą). Zatem istnieje nieskończenie wiele liczb naturalnych, które nie są sumami dwóch kwadratów liczb wymiernych. Udowodnimy teraz, że jeżeli liczba wymierna dodatnia w jest sumą kwadratów dwóch liczb wymiernych to jest ona taką sumą na nieskończenie wiele różnych sposobów. Niech więc liczba wymierna dodatnia w będzie sumą dwóch kwadratów liczb wymiernych u i v , $w = u^2 + v^2$. Możemy tu oczywiście założyć, że $u \geq v \geq 0$. Jeżeli $v = 0$, to wobec $w > 0$ mamy $u > 0$ i $w = u^2$. Ponieważ dla naturalnych n mamy tożsamość

$$(n^2 + 1)^2 = (n^2 - 1)^2 + (2n)^2, \text{ więc } w = ((n^2 - 1)u/n^2 + 1)^2 + (2nu/n^2 + 1)^2$$

przy czym liczby $(n^2 - 1)u/n^2 + 1$ i $2nu/n^2 + 1$ wzrastają, gdy n wzrasta. Mamy tu więc nieskończenie wiele rozkładów liczby w na sumę dwóch kwadratów liczb wymiernych dodatnich. Przypuśćmy teraz, że $v > 0$. Wystarczy oczywiście dowieść, że dla każdego rozkładu $w = u^2 + v^2$, gdzie u i v są to liczby wymierne dodatnie, znajdziemy rozkład $w = u_1^2 + v_1^2$, gdzie u_1 i v_1 są liczbami wymiernymi, dodatnimi, przy czym $u_1 > u$. Z równości $w = u^2 + v^2$ wynika jak łatwo sprawdzić dla naturalnych n równość

$$w = \left(\frac{u(n^2 - 1) + 2vn}{n^2 + 1} \right)^2 + \left(\frac{v(n^2 - 1) - 2un}{n^2 + 1} \right)^2$$

Obierzmy jako n liczbę naturalną $n > 1 + 2u/v$ i połączmy

$$u_1 = \frac{u(n^2 - 1) + 2vn}{n^2 + 1}, v_1 = \frac{v(n^2 - 1) - 2un}{n^2 + 1}$$

Będzie tu $u_1 = u + (2/n^2 + 1)(vn - u) > u$, gdyż $vn > 2u > u$, przy czym, wobec $n - 1 > 2u/v$, będzie $v(n^2 - 1) = (n - 1)v(n + 1) > 2u(n + 1) > 2un$, zatem $v_1 > 0$. Żądany dowód został więc przeprowadzony. Zauważymy tu, że można też dowieść, chociaż jest to rzeczą już znacznie trudniejszą, że jeżeli liczba jest sumą dwóch sześciątów różnych liczb wymiernych dodatnich, to jest taką sumą na nieskończenie wiele sposobów. Ale liczba będąca sumą dwóch równych sześciątów liczb wymiernych dodatnich, jak tego można dowieść, w jeden tylko sposób rozkłada się na sumę dwóch sześciątów liczb wymiernych > 0 .

Łatwo dowieść, że twierdzenie to jest równoważne twierdzeniu, że liczba 2 tylko w jeden sposób $2 = 1^3 + 1^3$ rozkłada się na sumę dwóch sześciątów liczb wymiernych dodatnich, ale dowód tego ostatniego twierdzenia jest trudny. Łatwo jest dowieść, że suma dwóch różnych sześciątów liczb wymiernych dodatnich jest zarazem różnicą dwóch różnych sześciątów liczb wymiernych dodatnich. Wynika to natychmiast z tożsamości:

$$x^3 + y^3 = \left(\frac{x(x^2 + 2y^2)}{x^2 - y^2} \right)^3 - \left(\frac{y(2x^2 + y^2)}{x^2 - y^2} \right)^3$$

dla $x \neq y$, której sprawdzenie pozostawiamy czytelnikowi. Więc na przykład

$$2^3 + 1^3 = (20/7)^3 - (17/7)^3$$

Przyjmując w naszej tożsamości $x = 2, y = -1$, otrzymujemy

$$7 = 2^3 - 1^3 = (4/3)^3 + (5/3)^3$$

liczba 7 może więc być przedstawiona jako suma dwóch różnych sześciątów liczb wymiernych dodatnich. Natomiast, jak łatwo dowieść, liczba 7 nie jest sumą dwóch sześciątów liczb naturalnych.

/Dla liczby 6 mamy rozkład

$$6 = (17/21)^3 + (37/21)^3$$

Natomiast, liczba 8 nie jest sumą dwóch sześciątów liczb wymiernych dodatnich, ale dowód nie jest łatwy. Dla liczby 9 mamy $2^3 + 1^3$.

Można dowieść elementarnie (choć dowód nie jest łatwy), że każda liczba wymierna dodatnia daje się na nieskończenie wiele sposobów przedstawić jako suma trzech sześciątów liczb wymiernych dodatnich. Natomiast łatwo jest dowieść, że każda liczba wymierna w daje się przedstawić w postaci $w = x^3 + y^3 + z^3 - 3xyz$, gdzie x, y, z są liczbami wymiernymi. Wynika to natychmiast z tożsamości

$$w = w^3 + (w+1/3)^3 + (w-1/3)^3 - 3w(w^2 - 1/9)$$

której sprawdzenie pozostawiamy czytelnikowi. Powróćmy jeszcze do rozkładów liczb wymiernych na sumę dwóch kwadratów. Rozkłady liczby 1 na sumę dwóch kwadratów liczb wymiernych, $1 = u^2 + v^2$, można przedstawić geometrycznie jako punkty koła $x^2 + y^2 = 1$ o wymiernych współrzędnych u, v , które krócej nazywamy wymiernymi punktami uważanego koła. Udowodnimy, że te wymierne punkty są tak na naszym kole rozłożone, że na dowolnym jego łuku jest ich nieskończenie wiele.

Wobec symetrii koła, jak też symetrii punktów wymiernych płaszczyzny (względem osi współrzędnych) wystarczy to udowodnić dla jednej ćwiartki koła, na przykład tej, która zawiera punkty o obu współrzędnych nie ujemnych. Niech p i q będą dwoma punktami naszego koła, należącymi do rozpatrywanej ćwiartki i niech a i b będą odcięte tych punktów: będą to więc liczby rzeczywiste, takie iż $0 \leq a \leq 1$ i $0 \leq b \leq 1$, przy czym możemy założyć, że $a < b$. Dla dowodu naszego twierdzenia wystarczy dowieść, że na obwodzie naszego koła istnieje punkt wymierny o odciętej x , gdzie $a < x < b$.

Wobec $0 \leq a < b \leq 1$ mamy

$$\sqrt{\frac{2}{b+1}} - 1 < \sqrt{\frac{2}{a+1}} - 1$$

przeto istnieje liczba wymierna w , taka, iż

$$\sqrt{\frac{2}{b+1}} - 1 < w < \sqrt{\frac{2}{a+1}} - 1$$

Stąd $a < 1 - w^2 / 1 + w^2 < b$

Położmy $x = 1 - w^2 / 1 + w^2$, $y = 2w / 1 + w^2$ liczby x i y będą wymierne, $a < x < b$ i, jak łatwo sprawdzić, będzie $x^2 + y^2 = 1$, a więc punkt o odciętej x i rzędnej y będzie punktem wymiernym, leżącym na naszym kole, przy czym $a < x < b$, c.b.d.o.

Jeżeli P jest wymiernym punktem naszego koła o dodatnich współrzędnych, Q - rzutem punktu P na oś odciętych, zaś O - środkiem koła, to odcinki OP , OQ i PQ mają odpowiednio długości 1 , x i y , a więc OPQ jest trójkątem prostokątnym o wymiernych bokach. Stąd, że punkty wymierne leżą na naszym kole wszędzie gęsto, wynika z łatwością, że dla dowolnego kąta ostrego α istnieje trójkąt prostokątny o wymiernych bokach (a więc też, przy odpowiednim powiększeniu, trójkąt prostokątny o naturalnych bokach) mający kąt ostry dowolnie bliski kąta α .

Z dowiedzionej własności punktów wymiernych koła $x^2 + y^2 = 1$, że leżą na nim wszędzie gęsto, łatwo wyprowadzić, że punkty wymierne powierzchni kuli $x^2 + y^2 + z^2 = 1$ leżą na niej wszędzie gęsto. Wystarczy tu dowieść, że dla dowolnych liczb rzeczywistych a, b, c, d , gdzie $0 \leq a < b \leq 1$, $0 \leq c < d \leq 1$ istnieje na powierzchni naszej kuli punkt wymierny (x, y, z) taki, iż $a < x < b$, $c < y < d$.

Wobec $0 \leq a < b \leq 1$, jak dowiedliśmy wyżej, istnieją liczby wymierne u i v takie, iż $a < u < b$ oraz $u^2 + v^2 = 1$, zaś wobec $0 \leq c < d \leq 1$ istnieją liczby wymierne u_1 i v_1 takie iż $c/v < u_1 \leq d/v$ oraz $u_1^2 + v_1^2 = 1$. Niech $x = u$, $y = u_1 v$, $z = v_1 v$: będą to liczby wymierne i będzie $a < x < b$, $c < y < d$ oraz $x^2 + y^2 + z^2 = u^2 + u_1^2 v^2 + v_1^2 v^2 = u^2 + v^2 = 1$ c.b.d.o

CZEŚĆ DZIESIĄTA

KONGRUENCJE

Przystawanie liczb według danego modułu. Jeżeli m jest daną liczbą naturalną, to o liczbach całkowitych a i b mówimy, że przystają do siebie według modułu m , jeżeli ich różnica jest podzielna przez m , a więc jeżeli istnieje liczba całkowita k taka, iż $a - b = km$. Dla wyrażenia, że liczba a przystaje do liczby b według modułu m K. F. Gauss wprowadził znakowanie

$$(1) \quad a \equiv b \pmod{m}$$

co czytamy: a przystaje do b modulo m . Wzór (1) nazywamy kongruencją.

Jasną jest rzeczą, że dla liczb całkowitych a i b wzór (1) zachodzi wtedy i tylko wtedy, gdy liczby a i b przy dzieleniu przez m dają jednakowe reszty. Jasne jest też, że wzór (1) pociąga za sobą wzór $b \equiv a \pmod{m}$

i na odwrót. Stosunek \equiv jest więc symetryczny. Mamy też dla każdej liczby całkowitej a i każdej

liczby naturalnej m

$$a \equiv a \pmod{m}:$$

każda liczba całkowita przystaje więc sama do siebie według każdego modułu naturalnego. Jeżeli a , b i c są liczbami całkowitymi, przy czym $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to

$$a \equiv c \pmod{m}$$

(gdyż, jeżeli a i b dają przy dzieleniu przez m jednakowe reszty, a także b i c dają przy dzieleniu przez m jednakowe reszty, to a i c dają przy dzieleniu przez m jednakowe reszty). Stosunek \equiv jest więc przechodni. Wyprowadzone trzy własności stosunku \equiv wykazują, że ma on wiele podobieństwa ze stosunkiem równości $=$ (co też usprawiedliwia używanie tu symbolu \equiv przypominającego znak równości). Są też i inne podobieństwa między kongruencjami a równościami. Podobnie jak równości, kongruencje (o tym samym module) można stronami dodawać, odejmować i mnożyć. W samej rzeczy, jeżeli

$$a \equiv b \pmod{m} \text{ oraz } c \equiv d \pmod{m},$$

to liczby $a - b$ oraz $c - d$ są podzielne przez m , skąd wobec wzorów

$$\begin{aligned} (a \pm c) - (b \pm d) &= (a - b) \pm (c - d), \\ ac - bd &= (a - b)c + b(c - d) \end{aligned}$$

wynika, iż lewe ich strony są podzielne przez m , czyli

$$a \pm c \equiv b \pm d \pmod{m} \text{ oraz } ac \equiv bd \pmod{m}.$$

Twierdzenie o dodawaniu i mnożeniu dwu kongruencji uogólnijmy natychmiast na dowolną skończoną liczbę kongruencji. Z twierdzenia o dodawaniu kongruencji wynika natychmiast, że (podobnie jak dla równań) można przenosić wyrazy z jednej strony kongruencji na drugą, zmieniając ich znaki (jest to bowiem równoważne odejmowaniu przeniesionego wyrazu od obu stron kongruencji). Z twierdzenia o mnożeniu kongruencji wynika w szczególności, że obie strony kongruencji można mnożyć przez jedną i tą samą liczbę całkowitą oraz że obie strony kongruencji można podnosić do jednej i tej samej potęgi o naturalnym wykładniku. Więc na przykład z oczywistej kongruencji $6 \equiv -1 \pmod{7}$ wynika kongruencja $6^{100} \equiv (-1)^{100} \pmod{7}$, czyli $6^{100} \equiv 1 \pmod{7}$. A oto inny przykład. Mamy oczywiście $2^5 \equiv 2 \pmod{10}$ skąd, podnosząc obie strony kongruencji do potęgi piątej, znajdujemy $2^{25} \equiv 2^5 \pmod{10}$, skąd wobec przechodniości stosunku \equiv mamy $2^{25} \equiv 2 \pmod{10}$, i podnosząc obie strony do czwartej potęgi: $2^{100} = 2^4 \pmod{10}$, a ponieważ $2^4 \equiv 6 \pmod{10}$, więc $2^{100} \equiv 6 \pmod{10}$. Tak więc liczba 2^{100} przy dzieleniu przez 10 daje resztę 6. Zauważymy atoli, że kongruencji o tym samym module nie możemy na ogół dzielić stronami, ani też potęgować stronami, Na przykład z kongruencji $48 \equiv 18 \pmod{10}$ i $12 \equiv 2 \pmod{10}$ nie wynika kongruencja $4 \equiv 9 \pmod{10}$, a z kongruencji $7 \equiv 2 \pmod{5}$ i $1 \equiv 6 \pmod{5}$ nie wynika kongruencja $7^1 \equiv 2^6 \pmod{5}$.

Udowodniono, że jedynymi modułami m , dla których przy wszelkich całkowitych a i b oraz naturalnych c i d wzory $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$ pociągają za sobą wzór $a^c \equiv b^d \pmod{m}$, są $m = 1, 2, 6, 42$ i 1806 . Ponieważ dzielnik dzielnika danej liczby jest dzielnikiem tejże liczby, więc kongruencja, zachodząca według danego modułu, zachodzi też według każdego dzielnika tegoż modułu. Niektóre udowodnione przedtem twierdzenia dają się łatwo wyrazić przy pomocy kongruencji. Na przykład małe twierdzenie Fermata można tak wyrazić: Dla każdej liczby pierwszej p oraz każdej liczby całkowitej a zachodzi kongruencja

$$a^p \equiv a \pmod{p}.$$

Wniosek zaś z tego twierdzenia można tak wyrazić: Jeżeli p jest liczbą pierwszą, zaś a liczbą całkowitą niepodzielną przez p , to

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

Twierdzenie zaś Wilsona i jego odwrócenie można tak wyrazić: Na to, żeby liczba naturalna $p > 1$ była pierwszą, potrzeba i wystarcza, żeby było

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

Rozwiązywanie kongruencji. Weźmy teraz pod uwagę kongruencję

$$f(x) \equiv 0 \pmod{m},$$

gdzie m jest daną liczbą naturalną, zaś $f(x)$ wielomianem całkowitym względem x stopnia naturalnego n o całkowitych współczynnikach:

$$f(x) = A_0x^n + A_1x^{n-1} + A_2x^{n-2} + \dots + A_{n-1}x + A_n,$$

gdzie A_0, A_1, \dots, A_n są to liczby całkowite. Pierwiastkiem naszej kongruencji nazywamy każdą liczbę całkowitą x , dla której jest ona prawdziwa. Nasuwa się pytanie, jak można znaleźć wszystkie pierwiastki danej kongruencji albo stwierdzić, że ich nie ma. Przypuśćmy, że a i b są to jakiegokolwiek liczby przystające do siebie według modułu m ,

$$a \equiv b \pmod{m}.$$

W myśl twierdzeń o mnożeniu i potęgowaniu kongruencji otrzymujemy stąd ciąg kongruencji:

$$A_0a^n \equiv A_0b^n \pmod{m}$$

$$A_1a^{n-1} \equiv A_1b^{n-1} \pmod{m}$$

.....

$$A_{n-1}a \equiv A_{n-1}b \pmod{m}$$

$$A_n \equiv A_n \pmod{m}.$$

Dodając te kongruencje stronami, otrzymujemy

$$A_0a^n + A_1a^{n-1} + \dots + A_{n-1}a + A_n \equiv A_0b^n + A_1b^{n-1} + \dots + A_{n-1}b + A_n \pmod{m}$$

Dowiedliśmy więc, że jeżeli $f(x)$ jest wielomianem całkowitym względem x o współczynnikach całkowitych, to dla każdej liczby naturalnej m i liczb całkowitych a i b kongruencja

$$a \equiv b \pmod{m}$$

pociąga za sobą kongruencję $f(a) \equiv f(b) \pmod{m}$. Z twierdzenia tego wynika natychmiast, że jeżeli liczba a jest pierwiastkiem kongruencji $f(x) \equiv 0 \pmod{m}$, gdzie $f(x)$ jest wielomianem względem x o współczynnikach całkowitych, to każda liczba przystająca do a według modułu m również jest pierwiastkiem tej kongruencji. Całą taką klasę liczb do siebie przystających według modułu m i spełniających daną kongruencję będziemy uważali za jeden jej pierwiastek.

Każda liczba całkowita przystaje według modułu m do jednej i tylko jednej z liczb ciągu

$$(i) \quad 0, 1, 2, \dots, m-1$$

(gdyż przystaje do swej reszty z dzielenia przez m). Dla wyznaczenia wszystkich pierwiastków kongruencji $f(x) \equiv 0 \pmod{m}$ wystarczy więc wyznaczyć wszystkie liczby ciągu (i), które ją spełniają. Jeżeli liczbami tymi są r_1, r_2, \dots, r_s , to wszystkimi pierwiastkami naszej kongruencji będą liczby $r_i + mt$, gdzie $i = 1, 2, \dots, s$, zaś t jest dowolną liczbą całkowitą.

Jeżeli żadna z liczb (i) nie spełnia naszej kongruencji, to nie spełnia jej żadna liczba całkowita i mamy wtedy kongruencję niemożliwą. Jeżeli zaś co najmniej jedna z liczb ciągu (i) spełnia naszą kongruencję, to jest ona wtedy spełniona przez nieskończenie wiele liczb całkowitych. Ale jako liczbę pierwiastków naszej kongruencji umawiamy się nazywać liczbę liczb ciągu (i) spełniających tę kongruencję. Sprawdzenie, które z liczb ciągu (i) spełniają naszą kongruencję, jest teoretycznie rzeczą łatwą. Możemy więc powiedzieć, że teoretycznie potrafimy znaleźć wszystkie pierwiastki każdej danej kongruencji (której lewa strona jest wielomianem jednej zmiennej o współczynnikach całkowitych).

Przykłady. 1. Rozwiążemy kongruencję

$$x^2 + x \equiv 0 \pmod{2}.$$

Wobec $m = 2$, ciąg (i) składa się tu tylko z dwóch liczb 0 i 1, z których każda, jak łatwo sprawdzić, spełnia naszą kongruencję. Powiemy więc, że kongruencja nasza ma dwa pierwiastki. Jest ona oczywiście spełniona przez każdą liczbą całkowitą x , czyli jest spełniona tożsamościowo. Natomiast kongruencja

$$x^2 + x + 1 \equiv 0 \pmod{2}$$

nie jest spełniona przez żadną liczbą całkowitą i przeto jest kongruencją niemożliwą.

2. Z małego twierdzenia Fermata wynika, że jeżeli p jest liczbą pierwszą, to kongruencja

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

ma $p-1$ pierwiastków, którymi są liczby 1, 2, ..., $p-1$ oraz wszystkie liczby całkowite przystające do którejkolwiek z nich według modułu p (innymi słowy wszystkie liczby całkowite niepodzielne przez p). Żadna z liczb podzielnych przez p nie spełnia naszej kongruencji.

3. Rozwiążemy kongruencję

$$x^2 \equiv 1 \pmod{8}.$$

Wobec $m = 8$ ciąg (i) składa się tu z liczb 0, 1, 2, 3, 4, 5, 6, 7 i, jak łatwo sprawdzić, z nich tylko liczby 1, 3, 5, i 7 spełniają naszą kongruencję. Ma ona więc cztery pierwiastki; zatem, w danym razie ma więcej pierwiastków niż wynosi jej stopień, aczkolwiek nie jest spełniona tożsamościowo. Jest tu więc inaczej niż dłu równań.

4. Rozwiążmy kongruencję

$$x^7 - 3x + 2 \equiv 0 \pmod{5}.$$

Wobec $m = 5$ ciąg (i) składa się tu z liczb 0, 1, 2, 3 i 4. Liczba 0 oczywiście nie spełnia naszej kongruencji, zaś liczba 1 ją spełnia. Łatwo też sprawdzić, że liczba 2 nie spełnia naszej kongruencji. W myśl małego twierdzenia Fermata mamy $3^4 \equiv 1 \pmod{5}$, a ponieważ $3^3 \equiv 27 \equiv 2 \pmod{5}$, więc $3^7 \equiv 2 \pmod{5}$, skąd z łatwością sprawdzamy, że liczba 3 spełnia naszą kongruencję. Wobec $4 \equiv -1 \pmod{5}$ znajdujemy dalej $4^7 \equiv -1 \pmod{5}$ i z łatwością sprawdzamy, że liczba 4 nie jest pierwiastkiem naszej kongruencji. Kongruencja nasza ma więc dwa pierwiastki: 1 i 3. Wszystkimi liczbami całkowitymi spełniającymi naszą kongruencję są więc liczby $1 + 5t$ oraz $3 + 5t$, gdzie t jest dowolną liczbą całkowitą. Jeżeli p jest liczbą pierwszą i r_1, r_2, \dots, r_k są dowolnymi różnymi liczbami ciągu 0, 1, 2, ..., $p-1$, to łatwo można dać przykład kongruencji, której pierwiastkami (spośród liczb ciągu 0, 1, 2, ..., $p-1$) będą liczby r_1, r_2, \dots, r_k i tylko te liczby. Taką będzie na przykład kongruencja

$$(x - r_1)(x - r_2) \dots (x - r_k) \equiv 0 \pmod{p}.$$

Ale jeżeli m jest liczbą naturalną i r_1, r_2, \dots, r_k jest ciągiem różnych liczb spośród $0, 1, 2, \dots, m-1$, to nie zawsze istnieje kongruencja, której pierwiastkami (spośród liczb tego ciągu) są liczby r_1, r_2, \dots, r_k i tylko te liczby. Można na przykład dowiedzieć, że nie ma wielomianu $f(x)$ o współczynnikach całkowitych, takiego, żeby kongruencja $f(x) \equiv 0 \pmod{6}$ miała pierwiastki 2 i 3, lecz nie miała pierwiastka 0. Dla modułów pierwszych p zachodzi twierdzenie Lagrange'a że jeżeli $f(x)$ jest wielomianem całkowitym n -go stopnia względem x o współczynnikach całkowitych i jeżeli współczynnik przy x^n nie jest podzielny przez p , to kongruencja $f(x) \equiv 0 \pmod{p}$ ma co najwyżej n pierwiastków. Jak wynika z podanego wyżej przykładu 3, twierdzenie to może być fałszywe dla modułów złożonych. To, cośmy dotąd mówili o pierwiastkach kongruencji, dotyczy kongruencji, których lewa strona jest wielomianem o współczynnikach całkowitych. Inaczej ma się rzecz z kongruencjami, w których niewiadoma wchodzi do wykładnika. Jak na przykład znaleźć wszystkie liczby całkowite x , spełniające kongruencję

$$2^x \equiv 1 \pmod{7}?$$

Oczywiście w grę wchodzi tu tylko liczby całkowite $x \geq 0$. W myśl małego twierdzenia Fermata mamy $2^6 \equiv 1 \pmod{7}$, skąd wynika, że $2^{6k} \equiv 1 \pmod{7}$ dla $k = 0, 1, 2, \dots$. Zatem wszystkie liczby całkowite nieujemne podzielne przez 6 spełniają naszą kongruencję. Pozostają więc do zbadania inne liczby całkowite ≥ 0 , a więc liczby $6k + r$, gdzie $k = 0, 1, 2, \dots$, zaś $r = 1, 2, 3, 4$ lub 5 . Wobec $2^{6k} \equiv 1 \pmod{7}$ dla $k = 0, 1, 2, \dots$, mamy $2^{6k+r} \equiv 2^r \pmod{7}$ dla $r = 1, 2, 3, 4, 5$, a ponieważ według modułu 7 mamy $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4$, więc z łatwością wnosimy, że wszystkie rozwiązania naszej kongruencji w liczbach całkowitych nieujemnych x zawarte są we wzorach $x = 6k$ lub $x = 6k + 3$, gdzie $k = 0, 1, 2, \dots$. Wszystkimi pierwiastkami naszej kongruencji są więc liczby całkowite nieujemne i podzielne przez 3. Łatwo byłoby też dowiedzieć, że kongruencja $2^x \equiv 3 \pmod{7}$ nie ma żadnego rozwiązania w liczbach całkowitych x . Zajmiemy się jeszcze rozwiązaniem kongruencji

$$x^x \equiv 2 \pmod{5}.$$

Niech $f(x) = x^x$ i niech a i b będą liczbami naturalnymi, przy czym $a \equiv b \pmod{20}$, na przykład $b \equiv a + 20k$, gdzie k jest liczbą całkowitą ≥ 0 . Jeżeli a jest podzielne przez 5, to będzie oczywiście $a^a \equiv b^b \pmod{5}$ (gdyż obie strony będą wówczas podzielne przez 5). Jeżeli zaś a nie jest podzielne przez 5, to w myśl małego twierdzenia Fermata będzie $a^4 \equiv 1 \pmod{5}$, skąd $a^{20} \equiv 1 \pmod{5}$ oraz $b^b \equiv (a + 20k)^{a+20k} \equiv a^{a+20k} \equiv a^a \cdot a^{20k} \equiv a^a \pmod{5}$, zatem $a^a \equiv b^b \pmod{5}$. Dowiedliśmy więc, że jeżeli $a \equiv b \pmod{20}$, to $f(a) \equiv f(b) \pmod{5}$. Jeżeli więc wszystkimi liczbami spośród liczb ciągu $1, 2, 3, \dots, 20$, spełniającymi naszą kongruencję będą liczby r_1, r_2, \dots, r_k , to wszystkimi liczbami naturalnymi spełniającymi naszą kongruencję będą liczby $r_i + 20t$, gdzie $i = 1, 2, \dots, k$, zaś $t = 0, 1, 2, \dots$. Należy więc dokonać 20 prób podstawiając do naszej kongruencji za x liczby $1, 2, \dots, 20$. Doszliśmy w ten sposób do wniosku, że wszystkimi liczbami naturalnymi spełniającymi kongruencję $x^x \equiv 2 \pmod{5}$ są liczby $3 + 20t$ oraz $17 + 20t$, gdzie $t = 0, 1, 2$,

Niekiedy łatwo jest dowiedzieć, że dane równanie nie ma rozwiązań w liczbach całkowitych, dowodząc, że kongruencja przy odpowiednim module nie ma rozwiązań w liczbach całkowitych.

Na przykład dowód, że przy naturalnym n równanie $2x^3 + 1 = 7y^n$ nie ma rozwiązań w liczbach całkowitych x i y , można tak przeprowadzić. Gdyby liczby całkowite x i y spełniały to równanie, to oczywiście liczba x byłaby pierwiastkiem kongruencji

$$2x^3 + 1 \equiv 0 \pmod{7}.$$

Lecz kongruencja ta nie ma rozwiązań w liczbach całkowitych x , gdyż, jak łatwo sprawdzić, sześcián liczby całkowitej przy dzieleniu przez 7 daje resztę 0, 1 lub 6, zatem podwójny sześcián zwiększony o jedność - resztę 1, 3 lub 6.

CZEŚĆ JEDENASTA

FUNKCJE LICZBOWE $\varphi(N)$, $\sigma(N)$ I Ex

Przez $\varphi(n)$ oznaczamy (dla naturalnych n) liczbę liczb naturalnych $\leq n$ i pierwszych względem n . Funkcja liczbowa $\varphi(n)$ nazywana jest funkcją Gaussa, gdyż Gauss wprowadził to znakowanie, a przez wielu zachodnich matematyków funkcją Eulera, gdyż Euler wcześniej ją badał. Z definicji funkcji φ wynika natychmiast, że jeżeli p jest liczbą pierwszą, to $\varphi(p) = p - 1$ (gdyż wszystkimi liczbami naturalnymi $\leq p$ i pierwszymi względem liczby pierwszej p są liczby $1, 2, \dots, p-1$, których jest $p - 1$). Natomiast, jeżeli n jest liczbą złożoną, $n = ab$, gdzie a i b są liczbami naturalnymi > 1 oraz $< n$, to wśród liczb $1, 2, \dots, n$ znajdują się co najmniej dwie różne liczby, które nie są pierwsze względem n , mianowicie liczby a i $n = ab > a$. Wynika stąd, że dla n złożonych mamy $\varphi(n) \leq n-2$. Ponieważ wreszcie mamy oczywiście $\varphi(n) = 1$, więc widzimy, że równość $\varphi(n) = n-1$ zachodzi wtedy i tylko gdy n jest liczbą pierwszą. Łatwo jest obliczyć wartość $\varphi(n)$, gdy n jest potęgą liczby pierwszej $n = p^k$, gdzie p jest liczbą pierwszą, zaś k liczbą naturalną. Wśród liczb $1, 2, 3, \dots, p^k$ nie będą pierwszymi względem p^k te i tylko te liczby, które są podzielne przez p , a więc liczby postaci pt , gdzie t jest liczbą naturalną taką, iż $pt \leq p^k$ skąd $t \leq p^{k-1}$. Takich liczb naturalnych t jest oczywiście p^{k-1} . W ciągu $1, 2, \dots, p^k$ mamy więc p^{k-1} liczb, które są pierwsze względem p^k . Stąd wniosek, że w ciągu naszym mamy $p^k - p^{k-1}$ liczb pierwszych względem p^k i przeto, że $\varphi(p^k) = p^{k-1}(p-1)$.

Można dowieść, że jeżeli a i b są liczbami naturalnymi względnie pierwszymi, to $\varphi(ab) = \varphi(a)\varphi(b)$ i stąd z łatwością wyprowadzić wniosek, że jeżeli liczba naturalna n daje rozkład na czynniki pierwsze $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, to $\varphi(n) = p_1^{\alpha_1-1}(p_1-1) p_2^{\alpha_2-1}(p_2-1) \dots p_s^{\alpha_s-1}(p_s-1)$, co możemy też napisać w postaci

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right)$$

Oto wartości funkcji $\varphi(n)$ dla $n \leq 10$:

$\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = 4, \varphi(9) = 6, \varphi(10) = 4$.

Mamy $\varphi(n) = 1$ tylko dla $n = 1$ i dla $n = 2$, zaś dla $n > 2$ liczba $\varphi(n)$ jest zawsze parzysta. Można dowieść, że istnieje nieskończenie wiele liczb parzystych m , dla których równanie $\varphi(x) = m$ nie ma rozwiązań w liczbach naturalnych x . Takimi, jak dowiódł A. Schinzel, są na przykład liczby $m = 2 \cdot 7^k$, gdzie $k = 1, 2, 3, \dots$

R. D. Carmichael wypowiedział przypuszczenie, że nie ma liczby naturalnej m , dla której równanie $\varphi(x) = m$ miałyby jedno i tylko jedno rozwiązanie w liczbach naturalnych x . Przypuszczenie to zostało sprawdzone dla liczb $m \leq 10^{400}$. Przypuszczam, że dla każdej liczby naturalnej $s > 1$ istnieje nieskończenie wiele liczb naturalnych m , dla których równanie $\varphi(x) = m$ ma dokładnie s rozwiązań.

A. Schinzel zaś dowiódł w sposób całkiem elementarny (w komunikacie, przedstawionym na zjeździe matematyków czechosłowackich w Pradze w 1955 r.), że dla każdej liczby naturalnej s , istnieje liczba naturalna m , dla której równanie $\varphi(x) = m$ ma więcej niż s rozwiązań. Można dowieść, że dla każdej liczby naturalnej k równanie $\varphi(x+k) = \varphi(x)$ ma co najmniej jedno rozwiązanie (w liczbach naturalnych x), zaś A. Schinzel dowiódł, że dla każdej liczby naturalnej s istnieje liczba naturalna k , dla której równanie $\varphi(x+k) = \varphi(x)$ ma więcej niż s rozwiązań.

Słynne jest twierdzenie Eulera, że dla każdej liczby naturalnej m oraz każdej liczby całkowitej a pierwszej względem m liczba $a^{\varphi(m)} - 1$ jest podzielna przez m . Dla liczb m pierwszych daje to małe twierdzenie Fermata. Współczesny nam matematyk węgierski L. Rédei dowiódł, iż dla każdej liczby naturalnej $m > 1$ oraz każdej liczby całkowitej a liczba $a^m - a^{\varphi(m)}$ jest podzielna przez m . Stąd z łatwością wynika twierdzenie Eulera.

Łatwo dowieść, że $\varphi(n) > \sqrt{n} / 4$ dla $n = 1, 2, \dots$, skąd wynika, że funkcja $\varphi(n)$ wzrasta nieograniczenie, gdy n nieograniczenie wzrasta. Funkcja $\varphi(n)$ nie wzrasta jednak stale, a nawet

istnieje nieskończenie wiele liczb naturalnych n takich, iż $\varphi(n+1) < \varphi(n)$: takimi są na przykład wszystkie liczby pierwsze $n > 3$. Nie wiemy, czy istnieją liczby złożone n , dla których $n-1$ jest podzielne przez $\varphi(n)$. Jak dowiódł A. Schinzel, na to, żeby liczba naturalna n była podzielna przez $\varphi(n)$ potrzeba i wystarcza, żeby było $n = 2^\alpha$, gdzie $\alpha = 0, 1, 2, \dots$ lub $n = 2^\alpha 3^\beta$, gdzie α i β są liczbami naturalnymi. Nie wiadomo, czy istnieje nieskończenie wiele liczb naturalnych które nie są postaci $k - \varphi(k)$, gdzie k jest liczbą naturalną. Znamy dużo liczb naturalnych n , dla których $\varphi(n) = \varphi(n)(n+1)$, un przykład $n = 1, 3, 15, 104, 164, 194, 255, 495, 584, 975, 2204$, ale nie wiemy, czy jest ich nieskończenie wiele. Mamy też $\varphi(n) = \varphi(n+1) \varphi(n+2)$ dla $n = 5186$. Jeżeli d jest dzielnikiem naturalnym liczby naturalnej n , z definicji funkcji $\varphi(n)$ wynika z łatwością, że w ciągu $1, 2, \dots, n$ jest $\varphi(n/d)$ liczb mających z liczbą n największy wspólny dzielnik d . Stąd można łatwo wyprowadzić następującą własność funkcji φ : suma wszystkich liczb $\varphi(d)$, rozciągnięta na wszystkie dzielniki naturalne d liczby n , jest dla każdej liczby naturalnej n równa n . Więc na przykład liczba 6 ma dzielniki naturalne 1, 2, 3, 6 a więc $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6$. Suma dzielników liczby naturalnej. Sumę wszystkich dzielników liczby naturalnej n oznaczamy przez $\sigma(n)$. Łatwo obliczyć, że $\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 7, \sigma(5) = 6, \sigma(6) = 12, \sigma(7) = 8, \sigma(8) = 15, \sigma(9) = 10, \sigma(10) = 18$. Liczba pierwsza p ma tylko dwa dzielniki naturalne 1 i p , stąd $\sigma(p) = p + 1$ dla wszelkich liczb pierwszych p . Na odwrót, jeżeli dla liczby naturalnej n mamy $\sigma(n) = n + 1$, to n jest liczbą pierwszą. Jest bowiem wówczas $n \neq 1$ (gdyż $\sigma(1) = 1 < 1 + 1$), a gdyby liczba n była złożona, $n = ab$, gdzie a i b są liczbami naturalnymi > 1 i mniejszymi od n , to liczba n miałaby co najmniej trzy różne dzielniki: 1, a oraz n , skąd $\sigma(n) \geq 1 + a + n > n + 1$. Równanie $\sigma(x) = x + 1$ spełniają więc wszystkie liczby pierwsze, i tylko takie liczby. Jeżeli n jest potęgą liczby pierwszej, $n = p^k$, gdzie p jest liczbą pierwszą, zaś k liczbą naturalną, to jak łatwo sprawdzić, liczba n ma tylko dzielniki 1, p, p^2, \dots, p^k , których sumą jest

$$1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

Jest więc $\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$

W szczególności $\sigma(2^k) = 2^{k+1} - 1$ dla $k = 1, 2, \dots$

Łatwo dowieść, że jeżeli a i b są to liczby względnie pierwsze, d przebiega wszystkie dzielniki naturalne liczby a , zaś δ wszystkie dzielniki naturalne liczby b , to iloczyn $d\delta$ przebiega wszystkie dzielniki naturalne liczby ab . Stąd łatwo wynika, że jeżeli liczby a i b są względnie pierwsze, to $\sigma(ab) = \sigma(a)\sigma(b)$. Własność tę uogólniamy przez indukcję na iloczyn dowolnej skończonej liczby liczb naturalnych, z których każde dwie są względnie pierwsze. Jeżeli więc q_1, q_2, \dots, q_s są różnymi liczbami pierwszymi, zaś $\alpha_1, \alpha_2, \dots, \alpha_s$ liczbami naturalnymi, to

$$\sigma(q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}) = \sigma(q_1^{\alpha_1}) \sigma(q_2^{\alpha_2}) \dots \sigma(q_s^{\alpha_s})$$

co wobec znalezionej wyżej wzoru $\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$, daje

$$\sigma(q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}) = \frac{q_1^{\alpha_1+1} - 1}{q_1 - 1} * \frac{q_2^{\alpha_2+1} - 1}{q_2 - 1} \dots \frac{q_s^{\alpha_s+1} - 1}{q_s - 1}$$

Wzór ten pozwala obliczać sumę dzielników liczby naturalnej, której rozwinięcie na czynniki pierwsze jest znane. Więc na przykład

$$\sigma(100) = \sigma(2^2 \cdot 5^2) = (2^3 - 1) \cdot (5^3 - 1) / (2 - 1) = 7 \cdot 31 = 217.$$

Istnieją liczby naturalne n , dla których $\sigma(n) = \sigma(n+1)$, na przykład $n = 14$, ale nie wiemy, czy takich liczb jest nieskończenie wiele. Łatwo natomiast jest dowieść, że istnieje nieskończenie wiele liczb naturalnych n takich, iż $\sigma(n) > \sigma(n+1)$ (na przykład wszystkie liczby $n = p - 1$, gdzie p jest liczbą pierwszą > 3 , jak też, że istnieje nieskończenie wiele liczb naturalnych n takich, iż $\sigma(n) < \sigma(n+1)$ (na przykład wszystkie liczby n pierwsze). Można też dowieść, że istnieje nieskończenie wiele

liczb naturalnych m , dla których równanie $\sigma(x) = m$ nie ma rozwiązań.

Liczby doskonałe. Liczbę naturalną n , która jest sumą wszystkich swych mniejszych od niej samej dzielników naturalnych, nazywamy liczbą doskonałą. Ponieważ $\sigma(n) - n$ jest sumą wszystkich mniejszych od n dzielników naturalnych liczby n , więc liczby doskonałe są to liczby naturalnych, które spełniają równanie

$$\sigma(n) = 2n.$$

Łatwo sprawdzić, że żadna z liczb naturalnych < 6 nie jest doskonałą. Najmniejszą liczbą doskonałą jest liczba 6. Dzielnikami naturalnymi liczby 6, mniejszymi od 6 są 1, 2 i 3, przy czym $6 = 1 + 2 + 3$. Łatwo byłoby stwierdzić, że następną liczbą doskonałą jest $28 = 1 + 2 + 4 + 7 + 14$.

Cztery najmniejsze liczby doskonałe znane były już w starożytności a Euklides podał następujący sposób otrzymywania i liczb doskonałych parzystych:

"Obliczamy kolejne sumy składników szeregu : $1 + 2 + 4 + 8 + 16 + 32 + \dots$

Jeżeli suma taka okaże się liczbą pierwszą, to pomnożmy ją porzez ostatni składnik. Otrzymamy liczbę doskonałą".

Kolejnymi składnikami wypisanego szeregu geometrycznego są 1, $1 + 2 = 3$, $1 + 2 + 4 = 7$, $1 + 2 + 4 + 8 = 15$, $1 + 2 + 4 + 8 + 16 = 31$, ... Pierwszymi są tu 3, 7, 31. Mnożąc je odpowiednio przez ostatni składnik, otrzymujemy liczby doskonałe $3 \cdot 2 = 6$, $7 \cdot 4 = 28$, $31 \cdot 16 = 496$. Następną otrzymaną w ten sposób liczbą doskonałą byłaby liczba $64 \cdot 127 = 8128$. Udowodnimy, że metoda Euklidesa daje wszystkie liczby doskonałe parzyste. Przede wszystkim okażemy, że każda z liczb otrzymanych metodą Euklidesa jest liczbą doskonałą parzystą.

Sumy naszego szeregu geometrycznego mają postać

$$1 + 2 + 2^2 + \dots + 2^{k-1} = 2^k - 1 \text{ dla } k = 1, 2, \dots$$

Jeżeli metoda Euklidesa istotnie daje tylko liczby doskonałe, to znaczy, że jeżeli dla pewnej liczby naturalnej n liczba $2^k - 1$ jest pierwszą, to liczba $n = 2^{k-1}(2^k - 1)$ musi być doskonałą. Przypuśćmy więc, że $2^k - 1 = p$ jest liczbą pierwszą. Oczywiście musi być wtedy $k > 1$, i p jest liczbą pierwszą nieparzystą. Liczby $2^k - 1$ oraz p są więc względnie pierwsze i, jak wiemy, mamy

$$\sigma(2^{k-1}p) = \sigma(2^{k-1})\sigma(p) = (2^k - 1)(p + 1) = (2^k - 1) \cdot 2^k = 2^n.$$

Liczba n jest więc doskonałą i oczywiście parzystą. Okażemy teraz, że każda liczba doskonała parzysta może być otrzymana metodą Euklidesa. W tym celu potrzeba i wystarczy okazać, że jeżeli n jest liczbą doskonałą parzystą, to istnieje liczba naturalna k taka, iż $n = 2^{k-1}(2^k - 1)$ oraz, iż $2^k - 1$ jest liczbą pierwszą. Przypuśćmy więc, że n jest liczbą doskonałą parzystą i niech 2^{k-1} oznacza najwyższą potęgę liczby 2, dzielącą n . Będzie tu więc k liczbą naturalną > 1 i będzie $n = 2^{k-1}l$, gdzie l jest liczbą nieparzystą, a więc pierwszą względem 2^{k-1} . Stąd, jak wiemy, $\sigma(n) = \sigma(2^{k-1}l) = \sigma(2^{k-1})\sigma(l) = (2^k - 1)\sigma(l)$. Lecz skoro n jest liczbą doskonałą, to $\sigma(n) = 2n = 2^k l$. Mamy więc $(2^k - 1)\sigma(l) = 2^k l$. Ponieważ $2^k - 1$ jest liczbą nieparzystą, więc stąd wynika, że liczba $\sigma(l)$ musi być podzielna przez 2^k , $\sigma(l) = 2^k m$, gdzie m jest liczbą naturalną, co daje $(2^k - 1)m = l$, zatem $m + 1 = 2^k m = \sigma(l)$. Lecz m jest dzielnikiem liczby l , przy czym różnym od 1, gdyż w razie $m = 1$ byłoby $2^k - 1 = 1$, zatem $k = 1$, gdyż tymczasem $k > 1$. Z równości $\sigma(l) = l + m$ wynika więc, że l i m są wszystkimi różnymi dzielnikami naturalnymi liczby l . Dowodzi to, że l jest liczbą pierwszą oraz że $m = 1$. Jest więc $l = 2^k - 1$ i $2^k - 1$ jest liczbą pierwszą.

Dowiedliśmy więc, że na to, aby liczba parzysta n była doskonałą, potrzeba i wystarcza, żeby miała postać $n = 2^{k-1}(2^k - 1)$, gdzie k jest liczbą naturalną i gdzie $2^k - 1$ jest liczbą pierwszą.

Dowodzi to, że postępowanie podane przez Euklidesa daje wszystkie liczby doskonałe parzyste (i tylko takie liczby). Wynika stąd też, że tyle będziemy znali liczb doskonałych parzystych, ile będziemy znali liczb pierwszych postaci $2^k - 1$, gdzie k jest liczbą naturalną. Liczby tej postaci noszą nazwę liczb Mersenne'a.. Liczb pierwszych Mersenne'a znamy dotąd 17: tyleż więc znamy

dotąd liczb doskonałych, przy czym pięć największych z nich znaleziono dopiero w ostatnich latach. Największą znaną liczbą doskonałą jest liczba $2^{2280} (2^{2281} - 1)$ mająca 1373 cyfry. Nie wiemy, czy liczb doskonałych parzystych jest nieskończenie wiele i nie znamy żadnej liczby doskonałej nieparzystej. Udowodniono, że nie ma liczb doskonałych nieparzystych mniejszych od $2 \cdot 10^{12}$.

Szukano też dla różnych danych liczb naturalnych $k > 2$ liczb naturalnych n , spełniających równanie $\sigma(n) = kn$. Liczbami spełniającymi równanie $\sigma(n) = 3n$ są na przykład liczby $120 = 2^3 \cdot 3 \cdot 5$, $672 = 2^5 \cdot 3 \cdot 7$, $523776 = 2^9 \cdot 3 \cdot 11 \cdot 31$. Liczbami spełniającymi równanie $\sigma(n) = 4n$ są na przykład liczby $30240 = 2^5 \cdot 3^3 \cdot 5 \cdot 7$, $32760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$. Liczbą spełniającą równanie $\sigma(n) = 5n$ jest na przykład $14182439040 = 2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19$.

Nie wiemy, czy istnieje nieskończenie wiele liczb naturalnych, dla których liczba $\sigma(n)$ jest podzielna przez n . Łatwo dowieść, że istnieje nieskończenie wiele liczb naturalnych takich, iż $\sigma(n) = 2n - 1$: takimi są na przykład wszystkie liczby $n = 2^k$, gdzie $k = 0, 1, 2, \dots$. Nie wiadomo natomiast, czy istnieją liczby naturalne n , spełniające równanie $\sigma(n) = 2n + 1$, czyli tzw. liczby quasidokonałe, będące sumami wszystkich swych nietrywialnych (tj. różnych od 1 i od n) dzielników naturalnych.

Liczby zaprzyjaźnione. Liczby naturalne m i n nazywamy zaprzyjaźnionymi, jeżeli $\sigma(m) = \sigma(n) = m + n$ lub, co na jedno wychodzi, jeżeli suma mniejszych od m dzielników naturalnych liczby m jest równa liczbie n , zaś suma mniejszych od n dzielników naturalnych liczby n jest równa liczbie m .

Liczby doskonałe można by uważać za liczby zaprzyjaźnione same z sobą. Parą różnych najmniejszych liczb zaprzyjaźnionych jest 220 i 280, którą jakoby znalazł jeszcze Pitagoras. Inną taką parę tworzą liczby $1184 = 2^5 \cdot 37$ i $1210 = 2 \cdot 5 \cdot 11^2$. Znamy kilkaset takich par, ale nie wiemy, czy jest ich nieskończenie wiele ani też, czy istnieją takie, gdzie jedna z liczb jest nieparzysta, a druga parzysta. Oznaczmy $f(n) = \sigma(n) - n$: będzie to suma wszystkich dzielników liczby n mniejszych od n . Istnieje przypuszczenie Catalana, że dla naturalnych n ciąg

$$n, f(n), ff(n), fff(n), \dots$$

jest albo okresowy, albo urywa się na liczbie 1.

Jeżeli p jest liczbą pierwszą, to oczywiście $f(p) = 1$. Dla $n = 12$ ciągiem naszym jest 12, 16, 15, 9, 4, 3, 1.

Dla $n = 6$ ciąg nasz jest okresowy: 6, 6, 6, ...

Dla $n = 220$ ciąg też jest okresowy: 220, 280, 220, 280, ...

Wyrażono przypuszczenie, że istnieją liczby naturalne n , dla których ciąg nasz urywa się na liczbie 1 i składa się z dowolnej liczby wyrazów.

Funkcja $E(x)$. Jeżeli x jest liczbą rzeczywistą, to przez $E(x)$ oznaczmy największą liczbę całkowitą $\leq x$. Więc na przykład $E(7/2) = 3$, $E(1/3) = 0$, $E(-1/2) = -1$, $E(\sqrt{2}) = 1$, $E(-\sqrt{10}) = -4$, $E(\pi) = 3$.

Z definicji funkcji $E(x)$ wynika natychmiast, że dla każdej liczby rzeczywistej x mamy

$$E(x) \leq x, \text{ lecz } E(x) + 1 > x.$$

zatem też $x - 1 < E(x)$ oraz $0 \leq x - Ex < 1$. Jasną jest rzeczą, że $x = E(x)$ wtedy i tylko wtedy, gdy x jest liczbą całkowitą. Jasne jest też, że jeżeli a i b są to liczby rzeczywiste takie, iż $a \leq b$, to $E(a) \leq E(b)$. Stąd i z uwagi, że zawsze $E(x) \leq x$ i $E(y) \leq y$, wynika, że $E(x) + E(y) \leq E(x + y)$ dla rzeczywistych x i y . Mamy na przykład

$$0 = E(1/2) + E(1/2) < E(1/2 + 1/2) = 1, \quad E(3/4) + E(5/2) = E(4/3 + 5/2) = 3$$

Jeżeli k jest liczbą całkowitą, to $E(k + x) = k + E(x)$ dla rzeczywistych x . Można dowieść, że jeżeli n jest liczbą naturalną, zaś x liczbą rzeczywistą, to

$$E(x/n) = E(E(x)/n)$$

Jeżeli x jest liczbą rzeczywistą ≥ 1 , to $1, 2, \dots, E(x)$ są wszystkimi liczbami naturalnymi $\leq x$. Można dowieść, że jeżeli

$$x = c_0, c_1 c_2 c_3 \dots$$

jest rozwinięciem dziesiętnym liczby dodatniej x , to

$$c_n = E(10^n x) - 10E(10^{n-1} x) \text{ dla } n = 1, 2, \dots$$

jest to więc wzór na n -tą cyfrę rozwinięcia dziesiętnego liczby x . Więc na przykład tysięczną cyfrą rozwinięcia dziesiętnego liczby $\sqrt{2}$ jest $E(10^{1000} \sqrt{2}) - 10E(10^{999} \sqrt{2})$. Niełatwą jednak rzeczą byłoby tę cyfrę obliczyć, gdyż dla obliczenia liczby $E(10^{1000} \sqrt{2})$ trzeba by znać liczbę $\sqrt{2}$ z dokładnością do $1/10^{1000}$. Można dowieść, że istnieje liczba rzeczywista $a > 0$ taka, iż dla każdej liczby naturalnej n liczba

$$\left| E(10^{2^n} a) - 10^{2^{n-1}} E(10^{2^{n-1}} a) \right|$$

jest n -tą z kolei liczbą pierwszą.

CZEŚĆ DWUNASTA

ROZWIJANIE LICZB RZECZYWISTYCH NA UŁAKMKI ŁAŃCUHOWE

Niech x będzie daną liczbą rzeczywistą: będzie więc, jak wiemy, $0 \leq x - E(x) < 1$. Jeżeli x nie jest liczbą całkowitą, to będzie

$$x_1 = 1/x_1 - E(x_1)$$

Z liczbą x_1 możemy postąpić jak z liczbą x , tj. gdy x_1 nie jest liczbą naturalną, oznaczyć

$$x_2 = 1/x_1 - E(x_1)$$

będzie to liczba rzeczywista > 1 . Z liczbą x_2 możemy postąpić podobnie itd. Postępując w ten sposób albo przy pewnym naturalnym n dojdziemy do liczby naturalnej x_n i wówczas znajdziemy

$$x = E(x) + \frac{1}{x_1}, x_1 = E(x_1) + \frac{1}{x_2}, \dots, x_{n-1} = E(x_{n-1}) + \frac{1}{x_n}$$

skąd

$$x = E(x) + \frac{1}{E(x_1) + \frac{1}{E(x_2) + \frac{1}{E(x_3) \dots + \frac{1}{E(x_{n-1}) + \frac{1}{x_n}}}}}$$

co, dla oszczędności zapisujemy w postaci

$$x = E(x) + \frac{1}{|E(x_1)} + \frac{1}{|E(x_2)} + \dots + \frac{1}{|E(x_{n-1})} + \frac{1}{|x_n}$$

albo też otrzymamy ciąg nieskończony równości

$$x = E(x) + \frac{1}{x_1}, x_1 = E(x_1) + \frac{1}{x_2}, \dots, x_{n-1} = E(x_{n-1}) + \frac{1}{x_n}, \dots$$

gdzie liczby x_1, x_2, x_3, \dots są wszystkie > 1

Niech będzie na przykład $x = 355/113$. Będzie tu $E_x = 3, x - E_x = 16/113, x_1 = 113/16, E_{x_1} = 7, x_1 - E_{x_1} = 1/16, x_2 = 16$

zachodzi tu więc pierwszy przypadek i mamy rozwinięcie $355/113 = 3 + 1/|7 + 1/|16$.

Jako drugi przykład weźmy liczbę $x = 3, 14159$. Będzie tu $E_x = 3, x_1 = 1/0,14159 = 100000 / 14159, E_{x_1} = 7, x_2 = 14159/887, E_{x_2} = 15, x_3 = 887 / 854, E_{x_3} = 1, x_4 = 854/33, E_{x_4} = 25, x_5 = 33/29, E_{x_5} = 1, x_6 = 29/4, E_{x_6} = 7, x_7 = 4$ a więc i tu mamy pierwszy przypadek oraz otrzymujemy rozwinięcie

$$3,14159 = 3 + 1/|7 + 1/|15 + 1/|1 + 1/|25 + 1/|1 + 1/|7 + 1/|4$$

Jasną jest rzeczą, że jeżeli zachodzi pierwszy przypadek, to liczba x jest wymierna. Łatwo też dowieść, że jeżeli liczba x jest wymierna, to zachodzi pierwszy przypadek. Jeżeli bowiem $x = l/m$, gdzie l jest liczbą całkowitą, m - liczbą naturalną, i jeżeli $x - E(x) \neq 0$, to $l/m - E(l/m) = k/m$, gdzie k jest liczbą naturalną $< m$: zatem liczba $x_1 = m/k$ ma mianownik mniejszy od mianownika liczby $x = l/m$. Mianowniki liczb x_1, x_2, \dots maleją więc stale, a więc ciąg tych liczb nie może być nieskończony. Dla każdej więc liczby niewymiernej zachodzi drugi przypadek i na odwrót. Każda liczba niewymierna x wyznacza więc pewien ciąg nieskończony liczb naturalnych $E(x_1), E(x_2), E(x_3), \dots$, który otrzymujemy w wyżej podany sposób. Dla pewnych tylko liczb niewymiernych znane są własności tego ciągu. Wiemy na przykład dla jakich liczb niewymiernych x ciąg ten jest okresowy. Zachodzi to wtedy i tylko wtedy, gdy liczba niewymierna x spełnia równanie drugiego stopnia o współczynnikach całkowitych. W szczególności będzie tak dla pierwiastków drugiego stopnia z liczb naturalnych, o ile są liczbami niewymiernymi. Sprawdzimy to dla kilku z nich.

Niech więc będzie najpierw $x = \sqrt{2}$ (co jest liczbą niewymierną, spełniającą równanie $x^2 - 2 = 0$). Mamy tu $E(\sqrt{2}) = 1$, zatem $x_1 = 1/\sqrt{2}-1$, co po pomnożeniu licznika i mianownika przez $\sqrt{2}+1$ daje $x_1 = \sqrt{2}+1$, skąd $E(x_1) = E\sqrt{2} + 1 = 2$ zatem

$$x_2 = 1/\sqrt{2}+1-2 = 1/\sqrt{2}-1 = x_1$$

Jest więc $x_2 = x_1$, skąd przez indukcję wnosimy, że $x_n = x_1 = \sqrt{2}+1$ dla $n = 1, 2, \dots$, skąd $E(x_n) = 2$ dla $n = 1, 2, \dots$. Ciąg $E(x_1), E(x_2), \dots$ jest więc w naszym przypadku okresowy o okresie czystym składającym się z jednego tylko wyrazu 2.

Dla $x = \sqrt{3}$ znaleźlibyśmy $E(\sqrt{3}) = 1$, skąd $x_1 = 1/\sqrt{3}-1 = \sqrt{3}+1/2$, zatem $E(x_1) = 1$ skąd

$$x_2 = 1/\sqrt{3}+1/2 - 1 = 2/\sqrt{3}-1 = \sqrt{3}+1, \text{ Zatem } E(x_2) = 2$$

więc $x_3 = 1/\sqrt{3}-1 = x_1$ i przez indukcję wnosimy, że $x_{2k-1} = x_1$ zaś $x_{2k} = x_2$ dla $k = 1, 2, \dots$. Stąd $E(x_{2k-1}) = 1, E(x_{2k}) = 2$ dla $k = 1, 2, \dots$. Ciąg $E(x_1), E(x_2), \dots$ jest więc okresowy o okresie czystym dwuwyrzowym, utworzonym z liczb 1 i 2. W podobny sposób dla liczb 5, 6, 7, 8, 10 otrzymalibyśmy odpowiednio okresy (4), (2,4), (1,1,1,4), (1,4), (6). Ogólnie, dla znalezienia okresu dla liczby \sqrt{n} , gdzie n jest liczbą naturalną, nie będącą kwadratem liczby naturalnej, można podać następujące postępowanie, wymagające tylko wykonywania działań wymiernych na liczbach wymiernych: Przyjmując $a_0 = (E\sqrt{n}), b_1 = a_0, c_1 = n-a_0^2$ wyznaczamy kolejno liczby a_{k-1}, b_k i c_k dla k

= 2, 3, ... ze wzorów

$$a_{k-1} = E(a_0 + b_{k+1}/c_{k-1}), \quad b_k = a_{k-1}c_{k-1} - b_{k-1}, \quad c_k = n - b_k^2/c_{k-1}$$

Jeżeli s oznacza najmniejszą liczbę naturalną, taką iż $b_{s+1} = b_1$ i $c_{s+1} = c_1$ (a można dowieść, że liczbę taką zawsze znajdziemy), to okresem dla liczby \sqrt{n} będzie (a_1, a_2, \dots, a_s) . Nie znamy wzoru ogólnego na liczbę s wyrazów okresu dla liczby \sqrt{n} , gdy n jest dowolną liczbą naturalną, nie będącą kwadratem. W roku 1941 W. Patz ogłosił (na blisko trzystu stronach) tablice tych okresów dla $n \leq 10000$. Udowodniono, że dla każdej liczby naturalnej s istnieje nieskończenie wiele liczb naturalnych n takich, że okres dla liczby \sqrt{n} składa się z s wyrazów. Dla $n = 1000$ okres ma 19 wyrazów; dla $n = 991$ ma on 60 wyrazów dla $n = 9739$ ma on 210 wyrazów. Udowodniono, że okres (a_1, a_2, \dots, a_s) dla liczby \sqrt{n} ma zawsze tę własność, że $a_s = 2E(\sqrt{n})$, zaś w razie $s > 1$ ciąg $(a_1, a_2, \dots, a_{s-1})$ jest symetryczny, tj. $a_i = a_{s-i}$, dla $i = 1, 2, \dots, s-1$. Na przykład okresem dla $n = 46$ jest $(1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12)$ i mamy tu $s = 12$, $a_s = 12 = 2E(\sqrt{46})$, a ciąg $1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1$ jest symetryczny. Dla $n = 61$ mamy okres $(1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 1, 4)$: jest tu $s = 11$, $a_{11} = 14 = 2E(\sqrt{61})$ a ciąg $1, 4, 3, 1, 2, 2, 1, 3, 4, 1$ jest symetryczny. Wyznaczanie okresów dla liczb \sqrt{n} ma zastosowanie przy rozwiązywaniu równania $x^2 - ny^2 = 1$. Można mianowicie dowieść, że jeżeli okresem dla liczby \sqrt{n} jest (a_1, a_2, \dots, a_s) , zaś $a_0 = E(\sqrt{n})$, to w razie parzystości liczby s licznik x i mianownik y ułamka nieprzywiedlnego, będącego wartością liczby wymiernej

$$a_0 + 1 / |a_1 + 1| / |a_2 + \dots + 1| / |a_{s-1}$$

dają rozwiązanie równania $x^2 - ny^2 = 1$ w najmniejszych liczbach naturalnych. Jeżeli zaś s jest liczbą nieparzystą, to należy wziąć licznik i mianownik ułamka nieprzywiedlnego, będącego wartością liczby

$$a_0 + 1 / |a_1 + 1| / |a_2 + \dots + 1| / |a_s + 1| / |a_1 + 1| / |a_2 + \dots + 1| / |a_{s-1}$$

Zauważymy tu jeszcze, że z każdego rozwiązania równania $x^2 - ny^2 = 1$ w liczbach naturalnych x, y można otrzymać natychmiast rozwiązanie w większych liczbach naturalnych, gdyż z równości $x^2 - ny^2 = 1$, jak łatwo sprawdzić, wynika równość $(2x^2 - 1)^2 - n(2xy)^2 = 1$.

Z innych liczb niewymiernych znajdziemy tu jeszcze rozwinięcie na ułamek łańcuchowy arytmetyczny liczby $x_0 = \sqrt{5} + 1/2$

Ponieważ $Ex_0 = 1$, więc $x_1 = 1/x_0 - 1 = \sqrt{5} + 1/2 = x_0$ co daje rozwinięcie na ułamek łańcuchowy okresowy o okresie jednowyrazowym, utworzonym z jednej liczby 1:

$$\sqrt{5} + 1/2 = 1 + 1 / |1 + 1| / |1 + 1| / |1 + 1| / |1 + \dots$$

Biorąc kolejne redukty tego ułamka nieskończonego, czyli liczby

$$1, 1 + 1 / |1, 1 + 1| / |1 + 1| / |1, \dots$$

otrzymalibyśmy, jako ich wartości, ciąg nieskończony liczb wymiernych

$$1/1, 2/1, 3/2, 5/3, 8/5, 13/8, 21/13, \dots$$

o których łatwo byłoby dowieść, że jego n -tym wyrazem jest liczba wymierna v_{n+1}/v_n , gdzie v_n jest n -tym wyrazem ciągu Fibonacciego. Co się zaś tyczy rozwijania liczb wymiernych dodatnich na ułamek łańcuchowy arytmetyczny, to można tu stosować algorytm Euklidesa (kolejnych dzielen). Jeżeli mianowicie n_1 i n_2 są to dane liczby naturalne i dzielnik n_1 przez n_2 otrzymujemy iloraz całkowity q_1 , i resztę n_3 , a w razie $n_3 > 0$, dzielnik n_2 przez n_3 otrzymujemy iloraz naturalny q_2 i resztę n_4 itd., aż dojdziemy do reszty $n_{k+1} = 0$, czyli jeżeli mamy ciąg równości $n_1 = q_1 n_2 + n_3, n_2 =$

$q_2 n_3 + n_4, \dots, n_{k-2} = q_{k-2} n_{k-1} + n_k, n_{k-1} = q_{k-1} n_k$, to będzie

$$n_1/n_2 = q_1 + 1/q_2 + 1/q_3 + \dots + 1/q_{k-1}$$

Usprawiedliwia to dla algorytmu Euklidesa nazwę algorytmu, ułamka ciągłego.