Liczby pierwsze

Mgr Andrzej MĄKOWSKI

Niewiele zwrotów, które stworzyli matematycy, by opisywać fakty matematyczne, zadomowiło się w języku potocznym. Jednym z nich jest „rozłożyć na czynniki pierwsze". Popularność swoją zawdzięcza on być może temu, że stykamy się z nim wszyscy, bowiem występuje w programie nauczania w klasie piątej. Fakt ten ma również pewne ujemne (kolejny zwrot matematyczny!) strony, np. tę, że nie poznajemy żadnych dowodów twierdzeń mówiących o liczbach pierwszych. W tym artykule postaramy się wykazać kilka elementarnych twierdzeń o liczbach pierwszych. Najpierw sformułujemy definicję liczby pierwszej — musimy wszak wiedzieć, czym będziemy się zajmować.

Definicja. Liczbę naturalną p nazywamy pierwszą wtedy i tylko wtedy, gdy jest ona większa od 1 i jedynymi jej dzielnikami są liczby 1 i p.

(Niektórzy Czytelnicy mogą się dziwić, po co żądamy, by liczba pierwsza była większa od 1; czasami w szkole nie zwracano na to uwagi. Gdyby zaliczyć liczbę 1 do liczb pierwszych, wtedy twierdzenie 4 tego artykułu byłoby fałszywe, bowiem nawet liczba czynników w rozkładzie na czynniki pierwsze liczby np. 6 nie byłaby określona: $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 2 \cdot 1 \cdot 3 = \ldots$.)

Zachodzi pozornie oczywiste

Twierdzenie 1. Każda liczba naturalna większa od 1 ma co najmniej jeden dzielnik będący liczbą pierwszą.

Dowód. Niech A_n będzie zbiorem wszystkich większych od 1 dzielników liczby n. Niech n będzie liczbą większą od 1. Wówczas A_n jest zbiorem niepustym, gdyż $n \in A_n$. Na mocy zasady minimum wnioskujemy, że w A_n istnieje liczba najmniejsza, nazwijmy ją d_n. Wykażemy, że d_n jest liczbą pierwszą. Z definicji zbioru A_n mamy, że $d_n | n$ i $d_n > 1$.

Jeżeli $k | d_n$, to także $k | n$ (dlaczego?) oraz $k \leqslant d_n$, czyli liczba k byłaby dzielnikiem liczby n nie większym od d_n, a więc, jeżeli $k \in A_n$, to $k = d_n$ (bo w A_n nie ma liczb mniejszych od d_n); jeżeli zaś $k \notin A_n$, to $k = 1$ (bo jedynym dzielnikiem liczby n nie należącym do A_n jest 1).

Wykazaliśmy więc, że $d_n > 1$ i jedynymi dzielnikami liczby d_n są 1 i d_n, czyli d_n jest liczbą pierwszą, a ponieważ $d_n | n$, więc zakończyliśmy dowód twierdzenia 1. Zauważmy, że wykazaliśmy także

Twierdzenie 2. Najmniejszy większy od 1 dzielnik liczby naturalnej większej od 1 jest liczbą pierwszą.

Fakt opisany twierdzeniem 2 wykorzystywaliśmy wielokrotnie w szkole, gdy trzeba było rozłożyć liczbę naturalną na czynniki pierwsze: dzieliliśmy ją przez najmniejszą (większą od 1) liczbę, przez którą dała się podzielić.

Teraz udowodnimy, że sprawdzona na wielu przykładach (choćby przez nas samych) możliwość rozłożenia liczby naturalnej na czynniki pierwsze, tzn. możliwość przedstawienia jej w postaci $p_1 p_2 \ldots p_r$, gdzie wszystkie liczby p_i są pierwsze, jest faktem ogólnie prawdziwym.

Twierdzenie 3. Każda liczba naturalna większa od 1 jest iloczynem skończonej liczby r (być może jednej) liczb pierwszych.

Dowód. Zastosujemy tutaj pewną wersję zasady indukcji matematycznej.

Liczba 2 jest, oczywiście, takim iloczynem ($r = 1$). Załóżmy, że każda liczba naturalna większa od 1 i mniejsza od n jest iloczynem liczb pierwszych. Rozróżnimy teraz dwa przypadki:

a) n jest liczbą pierwszą. Wówczas n jest iloczynem liczb pierwszych ($r = 1$).

b) n nie jest liczbą pierwszą, ma więc dzielnik a spełniający warunki $1 < a < n$. Istnieje więc liczba b, spełniająca nierówność $1 < b < n$ oraz równość $n = ab$.

Liczby a i b, na mocy założenia, są iloczynami liczb pierwszych, a więc i n jest takim iloczynem.

Wyłania się teraz pytanie: czy jest możliwe, by dwie osoby, nie popełniając błędu w obliczeniach, znalazły różne rozkłady tej samej liczby naturalnej na czynniki pierwsze?

Aby odpowiedzieć na to pytanie należy sprecyzować, co to są *różne* rozkłady. Sprawę tę rozstrzyga następujące twierdzenie:

Twierdzenie 4. Jeżeli n jest dowolną liczbą naturalną większą od 1 i $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ oraz wszystkie liczby p_i, q_j są pierwsze, to $r = s$ i można tak przestawić czynniki drugiego rozkładu (q_j), że $p_i = q_i$ dla $i = 1, 2, \ldots, r$.

Dowód. Przypuśćmy, że istnieją liczby naturalne większe od 1, mające dwa różne rozkłady na czynniki pierwsze, tzn. takie, że $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ (p_i, q_j — liczby pierwsze) i ciąg $q_1, q_2, \ldots, q_s$ nie jest permutacją ciągu $p_1, p_2, \ldots, p_r$. Niech N będzie najmniejszą spośród tych liczb (znowu stosujemy zasadę minimum).

Jest więc

$$N = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s.$$

Zauważmy, że każda liczba p_i jest różna od każdej liczby q_j, gdyby bowiem dla jakichś liczb k i l było $q_k = p_i$, to liczba $\frac{N}{p_i}$ byłaby liczbą mającą dwa różne rozkłady i przy tym mniejszą od N, co przeczy definicji liczby N.

Zasada minimum brzmi następująco: W każdym niepustym zbiorze złożonym z liczb naturalnych istnieje liczba najmniejsza. Analogiczne zdanie dla zbiorów liczb całkowitych, wymiernych lub rzeczywistych jest fałszywe.

Zapis $a|b$ czytamy „a jest dzielnikiem b", „a dzieli b", „b jest podzielne przez a". Oznacza on, że istnieje taka liczba całkowita c, że $b = ac$.

Rozwiązanie zadania M 107.

Mamy tożsamości:

$(a+b+c)^2 = a^2+b^2+c^2+2(ab+bc+ca)$,

$(ab+bc+ca)^2 = a^2b^2+b^2c^2+c^2a^2+$
$+2(ab^2c+bc^2a+ca^2b) = a^2b^2+b^2c^2+c^2a^2+$
$+2abc(a+b+c)$.

Jeżeli $a+b+c = 0$, to z tożsamości tych wynika, że

(1) $a^2+b^2+c^2 = -2(ab+bc+ca)$,

(2) $(ab+bc+ca)^2 = a^2b^2+b^2c^2+c^2a^2$.

Podnosząc obie strony równości (1) do kwadratu i uwzględniając równość (2) otrzymujemy

(3) $(a^2+b^2+c^2)^2 = 4(ab+bc+ca)^2 =$
$= 4(a^2b^2+b^2c^2+c^2a^2)$.

Z drugiej strony

(4) $(a^2+b^2+c^2)^2 = a^4+b^4+c^4+$
$+2(a^2b^2+b^2c^2+c^2a^2)$.

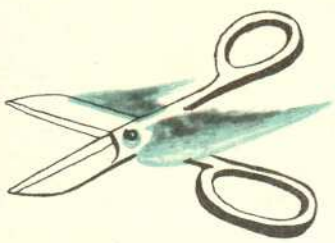
Z (3) i (4) otrzymujemy

$a^4+b^4+c^4+2(a^2b^2+b^2c^2+c^2a^2) =$
$= 4(a^2b^2+b^2c^2+c^2a^2)$,

stąd

(5) $a^4+b^4+c^4 = 2(a^2b^2+b^2c^2+c^2a^2)$.

Z równości (3) i (5) natychmiast wynika teza.



Największą znaną obecnie liczbą pierwszą jest liczba $2^{19937}-1$.

Rozwiązanie zadania M 108.

Wiadomo, że każdą liczbę naturalną m możemy zapisać w jeden tylko sposób w układzie dwójkowym:
$m = 2^a + 2^b + 2^c + \ldots$
$(0 \leqslant a < b < c < \ldots)$.
Każdą liczbę naturalną k można też w jeden tylko sposób zapisać w postaci $k = 2^p \cdot m$, gdzie m jest liczbą nieparzystą.
Zauważmy teraz, że każdemu rozkładowi liczby n na sumę składników nieparzystych
$n = m_1 \cdot 1 + m_2 \cdot 3 + m_3 \cdot 5 + \ldots =$
$= (2^{a_1} + 2^{b_1} + \ldots) \cdot 1 + (2^{a_2} + 2^{b_2} + \ldots) \cdot 3 +$
$+ (2^{a_3} + 2^{b_3} + \ldots) \cdot 5 + \ldots$
(tzn. rozkładowi, w którym m_1 składników jest równych 1, m_2 równych 3 itd., $m_i = 2^{a_i} + 2^{b_i} + \ldots$, $0 \leqslant a_i < b_i < \ldots$) można przyporządkować rozkład liczby n na różne składniki:
$n = 2^{a_1} \cdot 1 + 2^{b_1} \cdot 1 + \ldots + 2^{a_2} \cdot 3 +$
$+ 2^{b_2} \cdot 3 + \ldots + 2^{a_3} \cdot 5 + 2^{b_3} \cdot 5 + \ldots$
Przyporządkowanie to jest wzajemnie jednoznaczne.
Liczba n ma więc jednakową liczbę rozkładów każdego z omawianych typów.
Zadanie to jest, przynajmniej pozornie, podobne do zadania M 66 (Delta 10/1975).

Możemy więc założyć, że $p_1 < q_1$. Rozpatrzmy liczbę

$$A = N - p_1 q_2 \ldots q_s.$$

Z jednej strony mamy

(1) $$A = p_1 p_2 \ldots p_r - p_1 q_2 \ldots q_s = p_1 (p_2 \ldots p_r - q_2 \ldots q_s),$$

a więc $p_1 | A$, z drugiej zaś

(2) $$A = q_1 q_2 \ldots q_s - p_1 q_2 \ldots q_s = (q_1 - p_1) q_2 \ldots q_s.$$

A jest zatem liczbą naturalną mniejszą od N i większą od 1 (bo podzielną przez p_1), nie ma więc ona dwóch różnych rozkładów. W jednym jej rozkładzie, który otrzymalibyśmy rozłożywszy liczbę w nawiasie we wzorze (1), wystąpi liczba p_1, musiałaby więc ona wystąpić i w rozkładzie, który otrzymałoby się rozłożywszy we wzorze (2) liczbę $q_1 - p_1$. Liczby $q_2, \ldots, q_s$ są pierwsze i, jak stwierdziliśmy, są różne od p_1, a więc liczba p_1 musiałaby być dzielnikiem liczby $q_1 - p_1$, a więc i liczby pierwszej q_1, co jest sprzeczne z tym, że q_1 jest liczbą pierwszą większą od p_1.

Założenie, że istnieją liczby naturalne większe od 1, mające dwa rozkłady na czynniki pierwsze, doprowadziło nas do sprzeczności, udowodniliśmy więc twierdzenie 4.

Każdemu chyba nasuwało się pytanie, ile jest liczb pierwszych. Odpowiedź, że nieskończenie wiele, wynika z następującego twierdzenia:

Twierdzenie 5. Dla każdej liczby naturalnej n istnieje liczba pierwsza większa od n.

Dowód. Na podstawie twierdzenia 2 najmniejszy, większy od 1 dzielnik liczby $n!+1$ jest liczbą pierwszą.
Oznaczamy ją literą p. Gdyby było $p \leqslant n$, to $p | n!$, a ponieważ $p | n!+1$, więc także $p | 1$, co jest niemożliwe. Musi więc być $p > n$.

Twierdzenie 5 można udowodnić wieloma innymi sposobami. Oto dwa z nich.

I. Niech $F_n = 2^{2^n} + 1$ (jest to tzw. n-ta liczba Fermata). Zachodzi łatwa do udowodnienia przez indukcję tożsamość

$$F_0 F_1 \ldots F_{n-1} + 2 = F_n.$$

Wynika z niej, że jeżeli $k < n$, to F_k i F_n są względnie pierwsze, czyli nie mają wspólnego dzielnika większego od 1:
Niech bowiem d będzie wspólnym dzielnikiem liczb F_k i F_n. Z podanej tożsamości wynika, że wówczas $d | F_n - F_0 F_1 \ldots F_{n-1} = 2$, a ponieważ d, jako dzielnik liczby nieparzystej F_n, jest liczbą nieparzystą i jedynym dzielnikiem nieparzystym liczby 2 jest 1, więc $d = 1$.
Każda z liczb $F_0, F_1, \ldots$ ma, na mocy twierdzenia 1, czynnik pierwszy, żadne dwie nie mają, jak wykazaliśmy, wspólnego czynnika pierwszego, a więc czynników pierwszych liczb Fermata jest nieskończenie wiele (można wykazać, że liczb pierwszych nie będących dzielnikami liczb Fermata też jest nieskończenie wiele, takimi są np. liczby pierwsze postaci $4k+3$).

II. Przypuśćmy, że liczb pierwszych jest tylko skończona ilość: $p_1, p_2, \ldots, p_r$. Rozpatrzmy iloczyn

$$\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)^{-1} = \prod_{i=1}^{r} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \ldots\right).$$

Lewa strona tej równości jest oczywiście liczbą wymierną. Po prawej stronie mamy iloczyn skończonej liczby czynników, z których każdy jest szeregiem nieskończonym. Czytelnicy, którzy nie znają teorii szeregów, niech uwierzą, że wolno w tym przypadku mnożyć te szeregi „wyraz po wyrazie" i ustawić otrzymane iloczyny w dowolnym porządku. Iloczyn ten będzie więc równy sumie wszystkich (nieskończenie wielu) iloczynów

$$\frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}}$$

($\alpha_i \geqslant 0$). Każda liczba naturalna będąc iloczynem liczb pierwszych (twierdzenie 3) jest mianownikiem jakiegoś składnika. Wśród składników wystąpią więc wszystkie wyrazy tzw. szeregu harmonicznego $\left(\text{tj. } \sum_{n=1}^{\infty} \frac{1}{n}\right)$, o którym wiadomo, że jest rozbieżny.

Otrzymujemy więc sprzeczność: liczba wymierna równa jest ∞. Założenie, że liczb pierwszych jest ilość skończona, doprowadziło nas do sprzeczności.