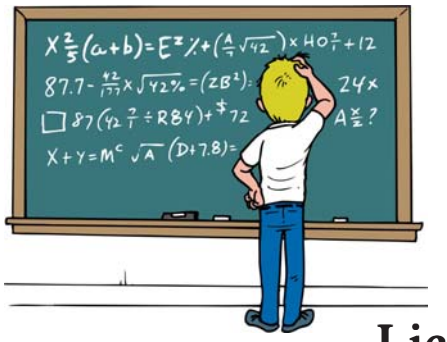

Kącik matematyczny

Stwierdzenie Pitagorasa, że liczby rządzą światem, jest ciągle aktualne. Świadczy o tym chociażby zastosowanie liczb pierwszych. Informacja podana w ubiegłym roku o znalezieniu największej liczby pierwszej, to nie tylko ciekawostka matematyczna, ale również fakt potwierdzający, że wzrosły potrzeby szyfrowania.

Liczby pierwsze cenniejsze niż inne

Poszukiwanie liczb pierwszych, to nie tylko zabawa dla matematyków. Wykorzystane do szyfrowania pozwalają na udoskonalenie systemów ochrony danych. Naukowiec, który znalazł ostatnią największą liczbę pierwszą, wzbogacił się o 100 tysięcy dolarów.

R. Gaik

Patrząc na te liczby, doznaje się uczucia obcowania z jedną z niewytłumaczalnych tajemnic stworzenia.

D. Zagier

Wiele odkryć w dziedzinie matematyki znajduje niespodziewane zastosowanie w „rzeczywistym świecie".

S. K. Stein „Potęga liczb"

Na wstępie chciałabym zaznaczyć, że nie jestem specjalistą z teorii liczb. Natomiast osiągnięcia z różnych działów matematyki, a w tym i z teorii liczb, ciągle mnie zdumiewają i zachwycają. Dlatego też, gdy w ubiegłym roku przeczytałam, że znaleziono największą liczbę pierwszą postanowiłam poszukać czegoś na ten temat. A oto wyniki moich poszukiwań.

Jesienią 2008 roku została podana kolejna liczba pierwsza, większa niż wszystkie do tej pory znane. Ma ona dokładnie 12978189 cyfr w zapisie dziesiętnym (czyli ok. 13 milionów). Odkrył ją Edison Smith, matematyk z Uniwersytetu Kalifornijskiego. Osiągnięcie to przyniosło mu nie tylko prestiż w świecie naukowym, ale i 100 tysięcy dolarów. Tak duże pieniądze zapłaciła założona w 1990 roku fundacja amerykańska – Electronic Frontier Foundation. Celem jej działalności jest między innymi zapewnienie prawa do prywatności i anonimowości w obecnym świecie informatycznym. Bezpieczeństwo obiegu informacji w Internecie zapewniają różne systemy szyfrujące. Podstawę ich stanowią właśnie liczby pierwsze. Oczywiście im większa jest liczba pierwsza, tym trudniej jest złamać klucz szyfrujący, czyli tym samym skuteczniejsze są systemy ochrony danych.

Połączenie liczb pierwszych z kryptografią (nauką o tworzeniu systemów kodujących informacje) nabrało szczególnego znaczenia w 1978 roku, za sprawą trzech profesorów prestiżowej uczelni amerykańskiej Massachusetts Institute of Technology: R. Rivesta, A. Shamera i L. Adelmana. Stworzony przez nich system szyfrowania danych, określany jest skrótem R.S.A. (od nazwisk autorów). Szyfr ten ma za zadanie umożliwić np. bankom czy przedsiębiorstwom transmisję informacji w sposób bezpieczny. Problem ten jest na tyle ważny, że rząd Stanów Zjednoczonych uznał publikowanie szyfru i technik jego łamania za naruszenie ustawy o kontroli broni.

W podstawach wspomnianego szyfru są takie proste pojęcia, jak podzielność liczb, wielokrotność i potęga liczb oraz oczywiście liczby pierwsze. Z pojęciami tymi spotykamy się już w szkole na lekcjach matematyki. Chciałabym może tylko przypomnieć, że dowolna liczba całkowita dodatnia większa od 1 jest liczbą pierwszą wtedy i tylko wtedy, gdy jest podzielna tylko przez 1 i samą siebie. Kolejne liczby pierwsze, to: 2, 3, 5, 7, 11, 13, 17, 19, ... itd. Istnieje wiele katalogów liczb pierwszych, ale niestety brak w nich jednoznacznej zasady, czy regularności tworzenia. Dlatego też znajdowanie częściowych rozwiązań trwa już od tysięcy lat, a nierozwiązanych problemów jest dziś więcej niż kiedykolwiek.

W XVIII wieku wybitny matematyk L. Euler odkrył pewną interesującą właściwość liczb, a mianowicie, gdy weźmiemy dwie różne liczby pierwsze i utworzymy liczbę

$$N^{(p-1)(q-1)+1} - N,$$

gdzie N jest dowolną liczbą naturalną, to okazuje się, że jest ona podzielna przez iloczyn $p \cdot q$. Krótko mówiąc, Euler udowodnił, że liczba taka jest zawsze wielokrotnością iloczynu $p \cdot q$. Dla przykładu weźmy $p=2$, $q=3$, wówczas otrzymamy liczbę postaci $N^3 - N$. Twierdzenie Eulera mówi, że dla dowolnej liczby naturalnej N liczba $N^3 - N$ jest podzielna przez $2 \cdot 3 = 6$. Rzeczywiście, biorąc $N=2$ czy $N=3$, mamy $2^3 - 2 = 6 = 1 \cdot 6$, $3^3 - 2 = 24 = 4 \cdot 6$ itd. Oczywiście dla pozostałych N własności te trzeba udowodnić, ale matematycy wiedzą, jak to zrobić.

Chcąc ułożyć bezpieczny szyfr, wybiera się dwie dostatecznie duże liczby pierwsze p i q. Następnie oblicza się iloczyn $p \cdot q$, który nazywa się kluczem publicznym. Klucz ten np. bank podaje do wiadomości swoim klientom, nie ujawniając, jakie liczby pierwsze zostały użyte. Aby złamać szyfr, szpieg musiałby znaleźć te dwie liczby pierwsze. Uwzględniając jednak fakt, że iloczyn dwóch liczb bardzo dużych daje gigantyczną liczbę, zadanie to staje się bardzo trudne. Szukanie bowiem podzielników liczb o ogromnej ilości cyfr (nawet przy użyciu komputera) jest niezwykle długą i mozolną pracą.

To szczególne zastosowanie liczb pierwszych sprawia, że są one dzisiaj tak bardzo cenione. Dlatego też znajdowanie ich jest nie tylko niezwykłym wyzwaniem naukowym, ale i intratnym zajęciem (patrz nagroda). Wymaga to jednak sporej wiedzy z teorii liczb i informatyki.

Teoria liczb jest jedną z najbardziej elementarnych gałęzi matematyki, a jednocześnie jedną z najtrudniejszych gałęzi obfitujących w niełatwe problemy. Wśród liczb całkowitych liczby pierwsze odgrywają ogromną rolę, podobną może do pier-

wiastków w chemii. Wystarczy przypomnieć sobie rozkład liczby na tzw. czynniki pierwsze. Jednak w tablicy liczb pierwszych brak jest jakiejkolwiek jednoznacznej zasady, czy regularności występowania. No, może jedynie to, że wszystkie liczby pierwsze z wyjątkiem dwójki są nieparzyste.

Co wiadomo o liczbach pierwszych, a czego nie wiadomo lub co się przypuszcza – to wszystko wypełniałoby niejedną książkę. Istotny jest tu fakt, że liczb pierwszych jest nieskończenie wiele. Piękny dowód tego podał Euklides już ponad 2000 lat temu.

Przy odkrywaniu kolejnych liczb pierwszych korzysta się niekiedy z bardzo wymyślnych metod. Jednak prostym sposobem jest metoda, jaką podał Eratostanes (276–194 p.n.e.) nazywana „sitem Erastotenesa". Polega ona na tym, że piszemy po kolei liczby naturalne (bez jedynki), a potem wykreślamy wszystkie podzielne przez 2 (ale zostawiamy początkową dwójkę), potem podzielne przez 3 (ale zostawiamy trójkę) itd. To znaczy, że za każdym razem zostawiamy najmniejszą kolejną liczbę pierwszą i wykreślamy wszystkie jej dalsze wielokrotności. Ale, tak jak to już było wspomniane, nie ma wzoru, który pozwoliłby wyliczyć dowolną liczbę pierwszą. Dlatego poszukiwane są różnorodne własności tych liczb, które pozwoliłyby je odnajdywać.

Odkryta ostatnio liczba jest tzw. liczbą Mersenne'a, tj. liczbą postaci 2^n – 1. Co więcej, odkrycie to przypada w 420. rocznicę urodzin i 360. rocznicę śmierci autora tych liczb – zakonnika franciszkanina Marina Mersenne'a (1588–1648). Wśród liczb postaci $M_p = 2^p - 1$, gdzie p jest liczbą pierwszą, znaleziono wiele liczb pierwszych (ale nie wszystkie one są liczbami pierwszymi). Co więcej, liczby tej postaci nie są „prawie wszystkie" pierwsze, jak przypuszczał Mersenne. Z drugiej strony nie wszystkie znane liczby pierwsze, to liczby Mersenne'a. Przed erą komputerów największą znaną liczbą pierwszą była znaleziona przez Eduarda Lucasa (1841–1891) liczba $M_{127} = 2^{127} - 1 = 170141183460469231731687303715884105727$.

Postać ta wskazuje, że innym ważnym problemem staje się potwierdzenie, że jest to liczba pierwsza. Sposób na rozwiązanie tego zadania podał E. Lucas. Udoskonalił go potem Amerykanin D. H. Lehmere (1905–1991). Obecnie zaś nazywany jest testem Lucasa-Lehmera (w skrócie *L-L*). A oto jego treść: „Liczba Mersenne'a $M_p = 2^p - 1$, gdzie p jest liczbą pierwszą, wtedy i tylko wtedy, gdy M_p jest dzielnikiem wyrazu $L_{p-1} = L^2_{p-2} - 2$ ciągu Lucasa (ciąg Lucasa określony jest rekurencyjnie: $L_1 = 4$, $L_n = L^2_{(n-1)} - 2$ dla $n \geq 2$)".

Oczywiście dzielenie można uprościć, bowiem stwierdzenie podzielności można zredukować do określania reszty z dzielenia. A tu bardzo pomocne stają się komputery.

Matematycy zarzucili już próby znalezienia wzoru, dającego wszystkie liczby pierwsze. Natomiast jest pewien postęp w poszukiwaniu rozmieszczenia liczb pierwszych wśród liczb naturalnych. Pewien ład zaczął się wynurzać z tego chaosu, kiedy nie są one rozważane w pojedynczych przypadkach, ale jako mnogość. Definiuje się wiele funkcji określających ich rozmieszczenie, jak np. funkcję $\Pi(n)$ jako liczbę liczb pierwszych mniejszych lub równych n.

Krótko mówiąc, aby poszukiwać liczb pierwszych, trzeba nabyć sporej wiedzy z teorii liczb.

A tak nawiasem mówiąc, Euler by się zdumiał, gdyby dowiedział się, że jego twierdzenia, iż pewna liczba jest wielokrotnością iloczynu dwóch liczb pierwszych, stanie się po dwóch wiekach podstawą do zbudowania tajnego szyfru. Fakt ten potwierdza, że badania matematyczne przeprowadzone dla ciekawych, czy intrygujących zagadnień nie zawsze muszą mieć natychmiastowe zastosowanie.

Aha, mogłoby się wydawać, że gdy dysponuje się komputerem o bardzo dużej mocy obliczeniowej, to nie powinno być problemów. Nic bardziej mylącego, ponieważ nie istnieje żaden uniwersalny wzór umożliwiający rozbijanie dużych liczb na czynniki pierwsze, to wiedza i pomysłowość ludzka są niezwykle cenne. Stąd też amerykańska fundacja w poszukiwaniu liczb pierwszych jest ważnym sponsorem projektu badawczego znanego jako GIMPS. Każdy może pomóc w tym przedsięwzięciu. Wystarczy ściągnąć specjalny program z oficjalnej strony projektu GIMPS. W taki to oto sposób tysiące ochotników na całym świecie za darmo użyczają na potrzeby programu badawczego niewielkiej mocy obliczeniowej swych osobistych komputerów. „Okruchy mocy" są sumowane i powstają ogromne możliwości obliczeniowe. Jest to metoda coraz częściej stosowana w ważnych projektach badawczych. Właśnie dzięki tej metodzie swoją wielką liczbę pierwszą znalazł E. Smith.

Krystyna Nowicka
Studium Nauczania Matematyki

P.S. Fundacja Electronic Frontier Foundation zapowiedziała, że uhonoruje pierwszego badacza, który znajdzie liczbę pierwszą mającą ponad 100 milionów cyfr dziesiętnych. Dostanie on 150 tysięcy dolarów. No to cóż, jak to mówią, do roboty.

Fot. Krzysztof Krzempek