mała delta

Złożony problem liczb pierwszych

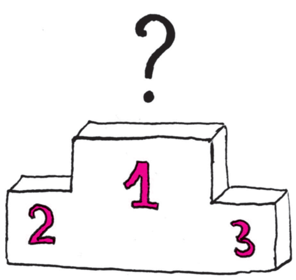
Wspaniałym i przystępnym źródłem informacji o liczbach pierwszych jest książeczka Wacława Sierpińskiego *Co wiemy i czego nie wiemy o liczbach pierwszych*, PZWS 1961, którą można znaleźć w wielu bibliotekach publicznych.

Co to jest liczba pierwsza? Najkrótsza definicja mówi, że to taka liczba naturalna, która ma dokładnie dwa dzielniki. Każda liczba naturalna ma przynajmniej dwa dzielniki: 1 i samą siebie. Wyjątkiem jest jedynka, dla której te dwa dzielniki okazują się tym samym. Nie chcemy też rozpatrywać w tym kontekście zera (pomijając dyskusyjną kwestię, czy należy ono do zbioru liczb naturalnych). Wobec tego można powiedzieć, że liczby pierwsze to takie, które oprócz dwóch oczywistych dzielników nie mają żadnych nieoczywistych – nie rozkładają się na iloczyn liczb większych od 1 i mniejszych od nich samych. Pozostałe liczby naturalne (oprócz jedynki, która tworzy swoją własną klasę) nazywamy liczbami złożonymi, ponieważ można je rozłożyć na iloczyn mniejszych czynników. Te czynniki nie muszą być różne – na przykład najmniejsza liczba złożona to $4 = 2 \cdot 2 = 2^2$. Natomiast ciekawą rzeczą jest to, że zestaw liczb pierwszych, których iloczyn jest daną liczbą, istnieje tylko jeden – takie rozkłady mogą się różnić tylko kolejnością czynników.

Więcej o rozkładzie na czynniki pierwsze można przeczytać na stronie 12.

Liczby pierwsze są w pewnym sensie ciekawsze niż liczby złożone. Po pierwsze, występują rzadziej. Po drugie, bardzo trudno przewidzieć ich wystąpienia – może być tak, że dwie kolejne liczby pierwsze są oddzielone tylko przez jedną liczbę złożoną, a może być tak, że między nimi jest bardzo duża przerwa. Pary liczb pierwszych oddzielonych tylko jedną liczbą złożoną to liczby pierwsze bliźniacze. Nie wiadomo, jak dużo ich jest – znamy wiele przykładów, także wśród dużych liczb, ale nikt dotąd nie udowodnił, że jest ich nieskończenie wiele. Jak zwykle w takich przypadkach, trwają poszukiwania coraz większych takich par. Największa znana obecnie para liczb bliźniaczych, znaleziona w 2009 roku, to

$$65516468355 \cdot 2^{333333} - 1 \quad \text{i} \quad 65516468355 \cdot 2^{333333} + 1.$$



A czy istnieją trójki liczb pierwszych, takie że pierwsza jest oddzielona od drugiej przez jedną liczbę złożoną i druga od trzeciej tak samo? Czytelnik Spostrzegawczy wymieni od razu liczby 3, 5 i 7. Okazuje się jednak, że jest to jedyny przykład „trojaczków". Żeby się o tym przekonać, wystarczy zauważyć, że liczby p, $p+2$ i $p+4$ dają różne reszty z dzielenia przez 3. Ponieważ mamy tylko trzy możliwe reszty do dyspozycji, to jedna z nich musi być zerem, czyli jedna z liczb p, $p+2$, $p+4$ jest podzielna przez 3. Wobec tego, jeśli żądamy, żeby te liczby były pierwsze, to wśród nich musi wystąpić 3. To oznacza, że nie ma innych możliwości poza układem 3, 5 i 7.

O liczbach pierwszych oddzielonych równymi odstępami – czyli o ciągach arytmetycznych złożonych z liczb pierwszych – piszemy na stronie 8.

Nie umiemy na razie rozstrzygnąć, ile jest par liczb pierwszych leżących możliwie blisko, ale wiadomo, że przerwy między kolejnymi liczbami pierwszymi mogą być dowolnie długie. Żeby się o tym przekonać, wystarczy podać metodę konstrukcji ciągu n kolejnych liczb złożonych dla n będącego dowolną liczbą naturalną. A ten ciąg wygląda tak:

$$(n+1)!+2,\ (n+1)!+3,\ (n+1)!+4,\ \ldots,\ (n+1)!+n+1$$

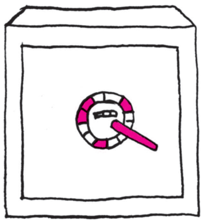
– kolejne liczby dzielą się przez $2, 3, 4, \ldots, n+1$.

$$C = 2^{2^{2^{1001}}} = 2^{2^{2^{1000}+2^{1000}}} = 2^{2^{2^{1000}}\cdot 2^{2^{1000}}} = \left(2^{2^{2^{1000}}}\right)^{2^{2^{1000}}}$$

$$D = (1000)^{2^{2^{1000}}}$$

Zatem $C > D$.

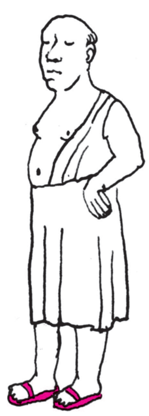
δ



Wreszcie, liczby pierwsze mają zastosowanie praktyczne. Na nich opierają się algorytmy szyfrujące, używane obecnie do zabezpieczania naprawdę ważnych rzeczy. Taki jest algorytm RSA, który jest przykładem szyfru z kluczem publicznym: powszechnie dostępne są dane pozwalające zaszyfrować wiadomość, ale odszyfrować ją można tylko znając drugą, prywatną część klucza. Żeby stworzyć taką parę złożoną z klucza publicznego i prywatnego, trzeba zacząć od dwóch odpowiednio dużych liczb pierwszych p i q. Bierzemy ich iloczyn $n = p \cdot q$. Liczba n wraz z innymi informacjami stanowi klucz publiczny. Natomiast liczby p i q zostają utajnione – będą częścią klucza prywatnego, bez nich nie uda się odczytać zaszyfrowanej wiadomości. Okazuje się, iż bezpieczeństwo tego szyfru wynika z faktu, że rozkładanie liczb na czynniki pierwsze ogólnie jest trudnym problemem. Dokładniej, jeśli znamy p i q, to łatwo obliczamy ich iloczyn n, ale jeśli znamy tylko n, to możemy mieć problem z odtworzeniem wartości p i q. Oczywiście, nie w takich przypadkach, gdy liczby są niezbyt wielkie, jak na przykład $n = 1517$. Tutaj komputer w ułamku sekundy, a Czytelnik w kilka minut sprawdzi, że $p = 37$ i $q = 41$. Ale jeśli liczby p i q mają ponad 200 cyfr długości...

Trzeba jednak wziąć pod uwagę ciągły rozwój algorytmów i sprzętu komputerowego. Te problemy obliczeniowe, których obecne komputery nie rozwiążą w sensownym czasie, za kilka lat mogą okazać się łatwiejsze – być może powstanie nowy algorytm rozwiązujący problem istotnie szybciej, a być może nowe parametry komputerów wystarczą do wykonania pewnych obliczeń. Wobec tego ciągle potrzebne są nowe liczby pierwsze, za każdym razem trochę większe niż wcześniej. Chcielibyśmy więc wiedzieć, jak szukać liczb pierwszych i jak sprawdzić, czy dana liczba jest pierwsza. Algorytmy używane obecnie do znajdowania liczb pierwszych i testowania pierwszości to temat na inną, dłuższą opowieść. Spróbujemy więc przyjrzeć się temu, jak dawniej szukano liczb pierwszych.

O najstarszej metodzie poszukiwania liczb pierwszych – sicie Eratostenesa – piszemy na stronie 10.



Przypomnijmy najpierw dowód, że liczb pierwszych jest nieskończenie wiele. Załóżmy przeciwnie, że jest ich skończenie wiele, a dokładnie k, i ponumerujmy je: $p_1, p_2, p_3, \ldots, p_k$. Popatrzmy teraz na iloczyn tych liczb i dodajmy do niego jedynkę: $q = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$. Czy liczba q jest pierwsza, czy złożona?

Okazuje się, że żadna z tych możliwości nie może mieć miejsca: q nie jest pierwsza, bo jest różna od każdej z liczb p_i, nie jest też złożona, bo nie dzieli się przez żadną z liczb pierwszych $p_1, \ldots, p_k$. Nie może więc istnieć, a skoro istnieje, oznacza to, że zbudowaliśmy ją, korzystając z błędnego założenia – jedynym założeniem było zaś istnienie tylko skończonej liczby liczb pierwszych. Trzeba więc z niego zrezygnować.

Mogłoby się wydawać, że ten dowód podsuwa nam pomysł, jak wyznaczać coraz większe liczby pierwsze: wystarczy wziąć wszystkie liczby pierwsze mniejsze od danej liczby, wymnożyć je, dodać jeden i... Zaraz, czy na pewno ta liczba nie jest złożona? Patrząc na przykłady małych liczb, wydaje się, że ten pomysł działa dobrze:

$$2 + 1 = 3, \quad 2 \cdot 3 + 1 = 7, \quad 2 \cdot 3 \cdot 5 + 1 = 31,$$
$$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211, \quad 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

– wszystkie wyniki są liczbami pierwszymi.

Ale już dla sześciu początkowych liczb pierwszych dostajemy

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509.$$

Czyli w naszym rozumowaniu musi być coś niepoprawnego. Zwróćmy uwagę na to, że w podanym dowodzie wszystko robiliśmy przy założeniu, że liczb pierwszych

?

Która liczba jest większa?

$$E = \sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{3}}}}}}}}}}}}}}}} \qquad \text{czy} \quad F = 10^{10^{10}}$$

δ

jest skończenie wiele. W szczególności obserwację, że liczba $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$ nie może być złożona, otrzymaliśmy, zakładając, że wymnożyliśmy wszystkie istniejące liczby pierwsze. Tymczasem mogą istnieć liczby pierwsze większe od każdej z wymnażanych, ale mniejsze od ich iloczynu – tutaj takimi liczbami są, na przykład, 17, 29, czy właśnie 59.

Istnieją inne wzory, których matematycy używali do znajdowania dobrych kandydatów na liczby pierwsze. Na przykład Marin Mersenne badał liczby postaci $2^n - 1$ i znajdował wśród nich liczby pierwsze, wiedząc, że taka liczba może być pierwsza tylko wtedy, gdy wykładnik n jest liczbą pierwszą. Na liczbach tej postaci bardzo dobrze działają niektóre testy pierwszości, więc znane są obecnie bardzo duże liczby pierwsze Mersenne'a. Aktualny rekord (prawie 13 milionów cyfr) to $2^{43112609} - 1$. Wyniki testów pierwszości dla tej liczby otrzymano w sierpniu 2008 roku i od tego czasu nie udało się trafić na żadną większą liczbę pierwszą Mersenne'a. Nie wiadomo nawet, czy jest ich nieskończenie wiele. Wiemy natomiast, że wśród liczb postaci $2^p - 1$, gdzie p to liczba pierwsza, istnieje nieskończenie wiele liczb złożonych.

Dziwna, „piętrowa" postać liczb pierwszych Fermata bierze się stąd, że jeśli liczba k ma w swoim rozkładzie choćby jeden czynnik nieparzysty (oznaczmy go q), to liczba $2^k + 1$ dzieli się przez $2^q + 1$; mam nadzieję, że Czytelnik Sprytny potrafi to udowodnić.

Pierre Fermat z kolei zajmował się liczbami postaci $2^{2^n} + 1$. Po sprawdzeniu pierwszości pięciu początkowych wyrazów tego ciągu (liczymy od $n = 0$) postawił nawet hipotezę, że wszystkie liczby opisane tym wzorem są pierwsze. Jednak szósta z tych liczb, $2^{2^5} + 1$, jest już złożona, ale Fermatowi nie udało się rozłożyć jej na czynniki pierwsze. Co ciekawe, pewien rozkład szóstej liczby Fermata można znaleźć za pomocą łatwych przekształceń arytmetycznych – trzeba tylko umieć dobrze zgadywać.

$$2^{2^5} + 1 = 2^{32} + 1 = 2^{32} + 2^{28} \cdot 5^4 - 2^{28} \cdot 5^4 + 1 =$$
$$= 2^{28}(2^4 + 5^4) - (2^{14} \cdot 5^2 + 1)(2^7 \cdot 5 + 1)(2^7 \cdot 5 - 1)$$

Widać, że to już koniec? Wystarczy zauważyć, że

$$2^4 + 5^4 = 16 + 625 = 641 = 640 + 1 = 2^7 \cdot 5 + 1.$$

Zatem

$$2^{2^5} + 1 = 641(2^{28} - (2^{14} \cdot 5^2 + 1)(2^7 \cdot 5 - 1)).$$

Liczby pierwsze Fermata okazały się ważne w geometrii: Carl Gauss udowodnił, że jeśli p jest taką liczbą, to można cyrklem i linijką skonstruować p-kąt foremny, a Pierre Wanzel – że dla żadnej innej liczby pierwszej taka konstrukcja nie jest możliwa.

Jak widać, rozstrzygnięcie tej hipotezy z pewnością leżało w zasięgu możliwości Fermata. Natomiast w zasięgu naszych możliwości do tej chwili nie leży rozstrzygnięcie, czy istnieją jeszcze inne liczby pierwsze Fermata, poza wymienionymi przez niego, czyli 3, 5, 17, 257 i 65537.

Później Leonard Euler poszukiwał liczb pierwszych wśród wartości pewnych wielomianów. Znalazł funkcję $f(x) = x^2 + x + 41$, która po podstawieniu liczb z zakresu od 0 do 39 daje w wyniku liczby pierwsze. Jak łatwo sprawdzić, dla $x = 40$ otrzymujemy już liczbę złożoną. A czy istnieją inne wielomiany postaci $x^2 + x + p$, gdzie p jest pierwsza, o tej własności, że dla liczb od 0 do $p - 2$ dają w wyniku liczbę pierwszą?

Odpowiedź w numerze.

W czasach Eulera powstała także piękna hipoteza, nierozstrzygnięta do dzisiaj. Christian Goldbach zauważył, że wiele liczb parzystych można przedstawić w postaci sumy dwóch liczb pierwszych (niekoniecznie różnych). Co więcej, nie znalazł przykładu liczby parzystej, której nie dałoby się zapisać w ten sposób (oprócz 2, która po prostu jest za mała). Postawił więc hipotezę, że każda liczba parzysta większa od 2 jest sumą dwóch liczb pierwszych. Prostota sformułowania jest, niestety, złudna.

!

Dla $2 < x \leqslant 3$ mamy $2 = \sqrt{2}^2 < \sqrt{2}^x \leqslant \sqrt{2}^3 = 2\sqrt{2} < 3$,
czyli $2 < \sqrt{2}^x < 3$ i dalej $2 < \sqrt{2}^{\sqrt{2}^x} < 3$,
skąd dochodzimy do $2 < E < 3$.

Zatem $E < F$.

δ

Przez ponad 250 lat, używając zarówno „tradycyjnych” metod matematycznych, jak i programów komputerowych, matematycy nie zdołali udowodnić ani obalić tej hipotezy. Sprawdzono ją jednak, oczywiście za pomocą metod komputerowych, dla liczb parzystych mniejszych od 10^{18} – umiemy przedstawić te liczby jako sumy dwóch liczb pierwszych. Te wyniki obliczeniowe skłaniają matematyków do wiary w prawdziwość hipotezy Goldbacha, ale dopóki nie będzie dowodu, nigdy nie wiadomo, co może się zdarzyć.

A co z liczbami nieparzystymi? Tak zwana słaba hipoteza Goldbacha mówi, że każdą liczbę nieparzystą większą niż 5 można przedstawić jako sumę trzech liczb pierwszych. Czytelnik Wnikliwy sprawdzi, że słaba hipoteza faktycznie wynika z tej dla liczb parzystych. Niestety, słabszej wersji także, jak dotąd, nie udało się rozstrzygnąć.

Na koniec – wracając do problemów, które powinny przynieść Czytelnikom więcej radości niż frustracji – zagadka. 30 jest największą liczbą, dla której wszystkie mniejsze od niej i względnie pierwsze z nią są liczbami pierwszymi. Jakie są inne takie liczby i dlaczego nie ma większych?

Odpowiedź w numerze.

Małą Deltę przygotowała Maria DONTEN-BURY

Prosto z nieba: Przyszłość Cyg X-1

Jeszcze zanim pierwsze teleskopy satelitarne umożliwiły zajrzenie w przestrzeń kosmiczną w czasach, gdy technologie kosmiczne wykorzystywane były przeważnie na potrzeby zimnej wojny, energetyczne promieniowanie pochodzące z gwiazd badano licznikami Geigera wynoszonymi w wyższe warstwy atmosfery przez suborbitalne rakiety, które, obracając się wokół własnej osi, skanowały niebo. Jednym z pierwszych odkrytych tą metodą obiektów (1964 r.) był Cyg X-1, znajdujący się w gwiazdozbiorze Łabędzia w okolicy η Cygni, w dolnej części „krzyża” tworzonego przez najjaśniejsze gwiazdy tej konstelacji. W kwietniu Łabędź widoczny jest na północnym wschodzie, w drugiej połowie nocy. Szybko ustalono, że w miejscu, z którego pochodzi promieniowanie rentgenowskie, znajduje się niebieski nadolbrzym typu widmowego O, nazwany HDE 226868. Z teorii budowy i ewolucji wynika jednak, że gwiazdy tego typu nie są w stanie emitować tak znacznych ilości fotonów X. Sprzeczność jest na szczęście pozorna i łatwa do wytłumaczenia – analizując zachowanie się linii widmowych w zależności od energii, astronomowie ujawnili istnienie świecącego słabo w świetle widzialnym towarzysza związanego z nadolbrzymem grawitacyjnie i powodującego zmiany widma z okresem orbitalnym (efekt Dopplera). Ów drugi, jasny rentgenowsko składnik układu, otoczony jest dyskiem akrecyjnym powstającym z materii „ściąganej” z HDE 226868, ma niewielkie rozmiary, ok. 50 km, oszacowane na podstawie zmienności czasowej promieniowania rentgenowskiego, oraz znaczną masę, rzędu 15 mas Słońca – parametry te jednoznacznie kwalifikują go jako czarną dziurę.

Mimo że rychło Cyg X-1 stał się powszechnie uznawanym „empirycznym dowodem” potwierdzającym teorię Einsteina, w 1975 roku klasycy teorii grawitacji, Kip Thorne i Stephen Hawking, zawarli głośny zakład o „istnienie (bądź nie) astrofizycznych czarnych dziur”. Hawking, który większość swojej kariery poświęcił studiowaniu czarnych dziur, przekornie przyjął rolę sceptyka, kwestionując jakość obserwacji Cyg X-1: wygrywając zakład, miał *na pocieszenie* otrzymać od Thorne'a 4 lata prenumeraty magazynu satyrycznego *Private Eye*; jednak zaledwie kilkanaście lat później, mając już do dyspozycji o wiele więcej doskonałych obserwacji, przyznał się (z pewnością bez cienia żalu) do przegranej.

Dorośli Czytelnicy zechcą sami sprawdzić, co w nagrodę otrzymał Thorne.

Niedawne pomiary odległości przy użyciu sieci teleskopów radiowych VLBA umożliwiają dokładne oszacowanie parametrów obu składników – zwłaszcza jasności, która jest w astronomii ściśle związana z pomiarem odległości – a także, co jeszcze ciekawsze, analizę ich przyszłych losów. Według przeprowadzonych symulacji Cyg X-1 przekształci się w ciągu następnych 3 milionów lat w ciasny, relatywistyczny układ czarna dziura–gwiazda neutronowa [1]. W odróżnieniu od układów podwójnych *dwu gwiazd neutronowych*, których radioastronomowie odkryli już kilka, nie znamy ani jednego układu „mieszanego” z czarną dziurą. Może to np. oznaczać, że z jakiegoś powodu występują one w przyrodzie bardzo rzadko. Byłaby to niewesoła wiadomość dla poszukiwaczy fal grawitacyjnych, gdyż właśnie relatywistyczne układy podwójne złożone z obiektów różnych typów stanowią główne źródło takich fal o możliwych do zaobserwowania częstościach. Czy naprawdę jest się czym martwić, zobaczymy za kilka lat – następna generacja detektorów (Advanced Virgo i LIGO) zacznie obserwacje w 2015 r.

Michał BEJGER

[1] `http://news.sciencemag.org/sciencenow/2011/08/the-fate-of-the-first-black-hole.html`

?

Która liczba jest większa?

$$G = (\log_2 2011)^{\log_2 2011} \quad \text{czy} \quad H = 2011^{\log_2 \log_2 2011}$$