

Mnich i liczby pierwsze

Bartłomiej Pawlik

Dla owocnej pracy naukowej kluczowe są regularne śledzenie najnowszych wyników w danej dziedzinie oraz współpraca między naukowcami. Nie zawsze tak było – na przykład Kartezjusz i Pierre de Fermat unikali czytania prac innych uczonych, gdyż uważali że takie postępowanie może za bardzo wpłynąć na ich własną twórczość.

Jednym z pionierów współczesnego „społecznościowego” podejścia do pracy naukowej był Marin Mersenne (1588–1648), francuski mnich ze zgromadzenia minimitów (braci najmniejszych). W klasztornej celi Mersenne'a znaleziono po jego śmierci ślady korespondencji naukowej z prawie osiemdziesięcioma (!) przedstawicielami różnych dziedzin nauki¹. Przez pewien czas uczoney organizował również regularne, cotygodniowe spotkania, które niektórzy historycy uważają za pierwowzór działalności towarzystw matematycznych.

Mersenne był przede wszystkim doskonałym organizatorem i mentorem dla młodych naukowców, choć sam nie wykazywał wybitnych zdolności matematycznych. Mimo to z jego nazwiskiem nierozzerwalnie związane są konkretne pojęcia matematyczne. Najbardziej znane spośród nich są tak zwane *liczby pierwsze Mersenne'a*.

Liczbą Mersenne'a M_n nazywamy liczbę o jeden mniejszą od n -tej potęgi dwójki, czyli

$$M_n = 2^n - 1.$$

Zatem początkowe liczby Mersenne'a to

n	1	2	3	4	5	6	7	8	9	10	11	12
M_n	1	3	7	15	31	63	127	255	511	1023	2047	4095

Zauważmy, że M_2, M_3, M_5 i M_7 są liczbami pierwszymi – ten fakt może nasunąć pochopne przypuszczenie, że jeśli n jest liczbą pierwszą, to M_n również jest liczbą pierwszą. Jednak już przykład liczby M_{11} pokazuje, że nie jest ono poprawne:

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89.$$

Można jednak w prosty sposób uzasadnić analogiczną implikację dla liczb złożonych:

Jeżeli n jest liczbą złożoną, to M_n również jest liczbą złożoną.

¹ Poza wspomnianą wcześniej dwójką usilnie niezależnych (Fermat, Kartezjusz), Mersenne korespondował również m.in. z Galileuszem, Bernardem de Bessym, Thomasem Hobbsem, czy obydwoma Pascalami.

W uzasadnieniu posłużymy się następującym wzorem skróconego mnożenia², który jest prawdziwy dla każdej pary dodatnich liczb całkowitych a i b :

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

Zauważmy, że jeżeli n jest liczbą złożoną, to istnieją liczby całkowite k i b ($k, b > 1$) o tej własności, że $n = k \cdot b$. Wówczas dla złożonej liczby n mamy

$$M_n = 2^n - 1 = 2^{k \cdot b} - 1 = (2^k)^b - 1.$$

Z przywołanego wyżej wzoru skróconego mnożenia wynika zatem, że liczba M_n jest podzielna przez liczbę $(2^k - 1)$.

Mimo że liczby pierwsze postaci $(2^n - 1)$ były rozważane już przez Euklidesa, nazwisko francuskiego mnicha przyłgnęło do nich ze względu na przypuszczenie, które wyraził on zaledwie kilka lat przed śmiercią. W jednym z listów do Bernarda de Besy'ego stwierdził, że dla

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

liczby M_n są liczbami pierwszymi, natomiast dla wszystkich pozostałych $n < 258$ są one złożone³. Pełne sprawdzenie hipotezy Mersenne'a zakończyło się dopiero po trzystu latach od jej sformułowania i wyszło na jaw, że pomylił się on w pięciu przypadkach: M_{67} i M_{257} okazały się liczbami złożonymi, natomiast na jego liście zabrakło liczb pierwszych M_{61} , M_{89} i M_{107} .

Ostatecznie przypuszczenie Mersenne'a zostało sprawdzone z wykorzystaniem obliczeń komputerowych, jednak imponujące częściowe wyniki otrzymano dużo wcześniej. W roku 1750 Leonhard Euler dowiódł, że M_{31} jest liczbą pierwszą, natomiast w 1876 Édouard Lucas⁴ potwierdził pierwszość liczby M_{127} .

Liczba M_{31} jest stosunkowo niewielka – wynosi trochę więcej niż 2 miliardy – i sprawdzenie jej pierwszości można przeprowadzić ręcznie (oczywiście należałoby temu przedsięwzięciu poświęcić sporo czasu) – wystarczy wykazać, że nie jest podzielna przez żadną z 4792 liczb pierwszych⁵ mniejszych od pierwiastka kwadratowego z M_{31} .

² Poprawność wzoru można sprawdzić poprzez wymnożenie nawiasów po prawej stronie równości i – otrzymamy sumę wyrazów, wśród których jest $(b-1)$ par liczb przeciwnych, co oznacza, że suma redukuje się do różnicy, która jest zapisana po lewej stronie wzoru.

³ Liczb pierwszych mniejszych od 258 jest 55.

⁴ Édouardowi Lucasowi zawdzięczamy posługiwanie się terminem *liczby Fibonacciego* - matematyk rozpowszechnił nazwę honorującą Leonarda z Pizy (XII-XIII wiek) nie mając pojęcia o tym, że te liczby były znane już w starożytnych Indiach. Lucas jest również autorem znanej gry o wieżach z Hanoi.

⁵ Euler wykazał się niemałym kunsztem ograniczając zbiór potencjalnych dzielników pierwszych, które należy sprawdzić. Zauważył, że wystarczy przeanalizować tylko te liczby pierwsze, które przy dzieleniu przez 248 dają resztę 1 lub 63 – w rozważanym zakresie są tylko 84 takie liczby.

Analogiczne podejście do badania pierwszości M_{127} byłoby całkowicie beznadziejne⁶ – w zapisie dziesiętnym ma ona 39 cyfr.

Lucas wykazał się niebywałą pomysłowością. Udało mu się opracować szybki algorytm, który można zastosować do badania pierwszości liczb Mersenne'a, gdy n przy dzieleniu przez 4 daje resztę 3.

Rozważmy następujący ciąg, którego pierwszy wyraz jest równy 4, a każdy kolejny to kwadrat poprzedniego elementu pomniejszony o 2. Początkowe wyrazy tego ciągu to:

$$\begin{aligned}a_1 &= 3 \\a_2 &= 3^2 - 2 = 7 \\a_3 &= 7^2 - 2 = 47 \\a_4 &= 47^2 - 2 = 2207 \\&\dots\end{aligned}$$

Lucas wykazał, że

dla liczby pierwszej p , która przy dzieleniu przez 4 daje resztę 3, liczba M_p jest liczbą pierwszą wtedy i tylko wtedy, gdy jest ona dzielnikiem wyrazu a_{p-1} ciągu.

Jak widać, elementy przedstawionego ciągu rosną całkiem szybko, ale i z tym można sobie poradzić – wystarczy wspomóc się arytmetyką modularną. Chcąc zbadać pierwszość ustalonej liczby M_p , możemy każdy interesujący nas element ciągu a_n zastąpić resztą z dzielenia tego elementu przez M_p .

W tym kontekście często korzysta się z zapisu

$$a \equiv_k b,$$

który czytamy „ a przystaje do b modulo k ”, a rozumiemy w następujący sposób: „reszty z dzielenia liczb a i b przez k są takie same”.

Zilustrujmy działanie powyższego testu na przykładzie liczby $M_7 = 127$. Rozważmy reszty z dzielenia elementów ciągu a_n przez M_7 :

$$\begin{aligned}a_1 &= 3 \equiv_{127} 3 \\a_2 &= 3^2 - 2 = 7 \equiv_{127} 7 \\a_3 &= 7^2 - 2 = 47 \equiv_{127} 47 \\a_4 &\equiv_{127} 47^2 - 2 = 2207 \equiv_{127} 48 \\a_5 &\equiv_{127} 48^2 - 2 = 2302 \equiv_{127} 16 \\a_6 &\equiv_{127} 16^2 - 2 = 254 \equiv_{127} 0\end{aligned}$$

Wyraz a_6 przystaje do 0 modulo M_7 , co oznacza, że liczba M_7 jest dzielnikiem liczby a_6 , więc z twierdzenia Lucasa wynika, że M_7 jest liczbą pierwszą!

⁶ Dla porównania, liczb pierwszych mniejszych od $\sqrt{M_{127}}$ jest około 300 miliardów. Zatem ręczne sprawdzanie pierwszości liczby M_{127} poprzez dzielenie jej przez liczby pierwsze nie większe niż jej pierwiastek byłoby zajęciem naprawdę czasochłonnym: przyjmijmy że zaczniemy dzisiaj wieczorem i będziemy sprawdzać po jednej liczbie pierwszej na sekundę bez żadnych przerw. Skończymy pracę za 10 miliardów lat, czyli mniej więcej wtedy kiedy, zgodnie z aktualnymi przewidywaniami, umrze Słońce.

Metoda Lucasa została uogólniona (dla dowolnego nieparzystego n) pół wieku później (w 1930 r.) przez Derricka Lehmera i znana jest jako test Lucasa-Lehmera.

Do dziś nie wiadomo, czy liczb pierwszych Mersenne'a jest nieskończenie wiele. Mimo to między innymi właśnie prostota testu Lucasa-Lehmera sprawiła, że od wielu dekad poszukiwania kolejnych liczb pierwszych Mersenne'a są ściśle powiązane z odpowiedzią na następujące pytanie:

Jaka jest największa znana obecnie liczba pierwsza?

W 1996 roku John H. Conway i Richard K. Guy w popularnonaukowej *Księżde liczb* napisali, że w momencie, gdy ktoś czyta ich książkę, największa znana liczba pierwsza jest najpewniej liczbą Mersenne'a. Przypuszczenie okazało się wyjątkowo trafne – w ciągu 25 lat od publikacji wspomnianej książki lider rankingu największych znanych liczb pierwszych zmienił się kilkanaście razy, ale za każdym razem była nim liczba Mersenne'a⁷. Największą znaną obecnie⁸ liczbą pierwszą jest odkryta 12 października 2024 roku liczba

$$M_{136\,279\,841} = 2^{136\,279\,841} - 1,$$

która w zapisie dziesiętnym ma ponad 41 milionów cyfr. Nowa liczba pierwsza Mersenne'a – tak jak piętnaście poprzednich – została odkryta dzięki projektowi *GIMPS* (*Great Internet Mersenne Prime Search*), czyli darmowemu ogólnodostępnemu oprogramowaniu służącemu do wyszukiwania liczb pierwszych Mersenne'a w wyniku obliczeń rozproszonych, w których wykorzystuje się możliwość współdzielenia zasobów obliczeniowych (procesora i pamięci operacyjnej komputerów). Odkrywcą liczby pierwszej $M_{136\,279\,841}$ jest Luke Durant – matematyk-amator z Kalifornii.

Motywacje do szukania ogromnych liczb pierwszych mogą być różne. Praktycznym elementem tych badań jest fakt, że duże liczby pierwsze znajdują konkretne zastosowania, np. w kryptografii. Podchodząc do takiej zabawy pragmatycznie – można na niej też zarobić. Obecnie za odkrycie nowej największej liczby pierwszej *GIMPS* oferuje 3 tysiące dolarów (jeżeli zostanie ona odkryta przy użyciu tego oprogramowania). Amerykańska organizacja pozarządowa *Electronic Frontier Foundation* oferuje 150 tysięcy dolarów za odkrycie liczby pierwszej mającej co najmniej 100 milionów cyfr w zapisie dziesiętnym⁹ i 250 tysięcy dolarów za liczbę pierwszą mającą co najmniej miliard cyfr.

⁷ Ostatni okres, w którym największa znana liczba pierwsza nie była liczbą Mersenne'a przypada na lata 1989-1992. Prym wiodła wtedy liczba $391\,581 \cdot 2^{216\,193} - 1$.

⁸ Jest to informacja, która prawdopodobnie szybko się zestarzeje. Odstępy między nowymi rekordzistami ostatnimi laty nie są większe niż kilka lat.

⁹ Jeżeli odkrywca znajdzie taką liczbę korzystając z *GIMPS*, to otrzyma tylko jedną trzecią tej kwoty.