

Małgorzata Sobolewska

Studentka I roku II^o matematyki
Studenckie Koło Naukowe „Rozmaitości”
Uniwersytet Humanistyczno-Przyrodniczy
Jana Kochanowskiego w Kielcach

Recenzent: dr Michał Stachura

Jak liczby pierwsze wpłynęły na rozwój cywilizacji

Streszczenie:

Referat dotyczy zagadnienia liczb pierwszych ze szczególnym uwzględnieniem ich wpływu na rozwój cywilizacji. W pierwszej części pracy zawartych jest kilka faktów z dziejów liczb pierwszych tj. poszukiwanie wzoru na n -tą liczbę pierwszą i poszukiwanie coraz to większych liczb pierwszych. Praca porusza również temat projektu GIMPS, tzn. internetowego projektu mającego na celu odnajdywanie wielkich liczb pierwszych Mersenne’a. W kolejnej części pracy przedstawione jest zagadnienie dotyczące zastosowania liczb pierwszych w kryptografii, a ściślej mówiąc w algorytmie szyfrującym o nazwie RSA. Praca zawiera także przykład prezentujący przebieg procesu szyfrowania informacji przy pomocy RSA. W końcowej części referatu wyszczególnione zostały konkretne przykłady wykorzystania RSA oraz liczb pierwszych we współczesnym świecie.

Słowa kluczowe: liczby pierwsze, projekt GIMPS, algorytm RSA, zastosowanie liczb pierwszych.

Tekst pracy:

2, 3, 5, 7, 11, 13, 17... – liczby pierwsze. Wydawać by się mogło, że są to tylko zwykłe liczby, nieciekawe, kompletnie nam w życiu nieprzydatne, niepotrzebnie wymyślone przez matematyków. Są to jednak złudne wyobrażenia, co zostanie ukazane w niniejszym referacie.

Liczby pierwsze zdecydowanie wyróżniają się wśród innych liczb i od wieków stanowią zagadkę dla ludzkości. Liczbami pierwszymi uczeni interesowali się od dawna. Już około IV w. p.n.e. Euklides udowodnił, że jest ich nieskończenie wiele.

Eratostenes podał metodę pozwalającą na odnajdywanie kolejnych liczb pierwszych mniejszych od zadanej liczby, zwaną obecnie „Sitem Eratostenesa”. Jednakże jest to metoda dość pracochłonna i wymagająca sporej ilości „wolnego miejsca”. Metoda ta polega bowiem na usuwaniu (skreślaniu) z ciągu wypisanych uprzednio liczb naturalnych (większych od 2) wielokrotności odpowiednich liczb. Czyni się to według następującej zasady. Najpierw skreślamy wielokrotności liczby dwa oprócz niej samej, następnie wybieramy pierwszą nieskreśloną liczbę i skreślamy wszystkie większe liczby przez nią podzielne itd. Postępując według opisanego schematu, otrzymamy następującą, przykładową tablicę liczb pierwszych.

Tablica 1. Liczby pierwsze mniejsze od 60

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Uczeni i miłośnicy matematyki poszukiwali przez długie lata wzoru na liczby pierwsze. Okazało się jednak, że liczby te nie chcą się poddać ani uczonym, ani hobbystom i nikomu jak dotąd nie udało się znaleźć takiej zależności, która generowałaby wszystkie liczby pierwsze, w sposób bardziej efektywny niż „Sito Eratostenesa”.

Pomimo iż znany jest np. wzór na n -tą liczbę pierwszą postaci:

$$f(n) = \sum_{k=2}^{2^n} \left(k \cdot \left[\frac{1}{1 + \left| k - 2 + \sum_{i=1}^{k-1} \left[-\left(\frac{k}{i} \right) \right] \right]} \right] \cdot \left[\frac{1}{1 + \left| n - \sum_{j=2}^k \left[\frac{1}{1 + \left| j - 2 + \sum_{i=1}^{j-1} \left[-\left(\frac{j}{i} \right) \right] \right]} \right]} \right] \right),$$

gdzie: $[x]$ i $\{x\}$ oznaczają część całkowitą i część ułamkową liczby x , to wzór ten jest jednak mało użyteczny, ze względu na fakt, iż algorytmy przez niego generowane mają ogromną złożoność obliczeniową. Z tego powodu, wzór ten nie jest wykorzystywany.

Gdy poszukiwania ogólnego wzoru na liczby pierwsze nie przynosiły oczekiwanego rezultatu, rozpoczęto poszukiwania coraz to większych liczb pierwszych. Działania te przerodziły się w niemałe zawody. Zarówno matematycy jak i zwykli amatorzy prześcigali się w odnajdywaniu kolejnych liczb pierwszych. Należy przy tym wspomnieć, że zabawa ta wcale nie jest prosta. Choć istnieje nieskończenie wiele liczb pierwszych, to jednak trudno jest znaleźć nowe, większe od dotychczas znanych, liczby pierwsze. Dzieje się tak, bowiem wśród coraz to większych liczb naturalnych liczby pierwsze pojawiają się coraz rzadziej. Ponadto sprawdzenie czy pewna duża liczba naturalna jest pierwsza jest niebywale pracochłonne, nawet w dzisiejszych czasach – w erze komputerów.

Mówiąc o poszukiwaniach ogromnych liczb pierwszych, nie można nie wspomnieć o projekcie GIMPS (**G**reat **I**nternet **M**ersenne **P**ri me **S**earch), czyli projekcie obliczeń rozproszonych (obliczeń dokonują wspólnie użytkownicy komputerów z dostępem do Internetu), w którym biorą udział ochotnicy poszukujący wielkich liczb pierwszych Mersenne’a (są to liczby pierwsze postaci $2^p - 1$, gdzie p jest liczbą pierwszą).

W projekcie tym może wziąć udział każdy. Wystarczy w tym celu wejść na stronę <http://www.mersenne.org> i pobrać z niej odpowiednie oprogramowanie, które działa automatycznie w wolnym czasie komputera. Taka działalność przy odrobinie szczęścia może okazać się niezwykle dochodowa, gdyż Electronic Frontier Foundation (organizacja pozarządowa mająca na celu walkę o wolności obywatelskie w elektronicznym świecie) oferuje 150 000 dolarów za odkrycie liczby pierwszej zapisywanej przy pomocy 100 mln cyfr oraz 250 000 dolarów za odkrycie liczby pierwszej zapisywanej przy pomocy miliarda cyfr. Największą odnanioną dotąd 45 liczba Mersenne’a jest $2^{43\,112\,609} - 1$ i ma ona 12 978 189 cyfr. Odkrył ją 23 sierpnia 2008 roku Edson Smith w ramach projektu GIMPS. Jako ciekawostkę można dodać, że do zapisania tej liczby potrzeba około 7211 kartek formatu A4.

Po tych kilku zwięzłych informacjach na temat poszukiwań i ogólnego zainteresowania liczbami pierwszymi nasuwają się pytania: *Dlaczego liczby pierwsze cieszą się tak ogromnym zainteresowaniem? Dlaczego poszukiwania liczb pierwszych są wspierane przez fundacje*

i oferuje się za ich odnalezienie tak wielkie nagrody? Co wynika ze znajomości wielkich liczb pierwszych?

Otóż odpowiedź jest prosta. Poszukiwanie wielkich liczb pierwszych, które kiedyś wydawało się tylko zabawą, dziś okazało się niezwykle pożyteczne. Pewnego dnia ktoś zauważył, jak wykorzystać pewne bardzo proste fakty:

- po pierwsze łatwiej jest wymnożyć dwie, nawet bardzo duże liczby, niż daną liczbę przedstawić jako iloczyn dwóch innych liczb,
- po drugie poziom trudności diametralnie wzrasta jeśli jest tylko jedna możliwość takiego rozkładu, czyli w przypadku gdy liczba jest iloczynem dwóch liczb pierwszych.

Powyższe fakty znalazły zastosowanie w kryptografii, tj. teorii kodowania informacji. W ten właśnie sposób powstał RSA, czyli najbardziej znany, niesymetryczny i wyjątkowo bezpieczny algorytm szyfrujący, wykorzystujący liczby pierwsze, którego twórcami są Ronald Rivest, Adi Shamir i Leonard Adleman z MIT (Massachusetts Institute of Technology). Idea RSA opiera się na tym, iż można ogłosić publicznie sposób szyfrowania i podać liczby zastosowane do szyfrowania, tzw. klucz publiczny, ale zaszyfrowanej informacji nikt nie potrafi odczytać. Do odszyfrowania potrzebny jest bowiem klucz prywatny, który każdy legalny użytkownik systemu otrzymuje tylko dla siebie i oczywiście nie powinien go nikomu udostępniać. Fundamentem RSA jest algorytm służący do generowania unikalnych i bezpiecznych (odpornych na próby odgadnięcia) par kluczy. Algorytm ten mnoży dwie duże liczby pierwsze i z otrzymanego wyniku poprzez kilka innych dodatkowych operacji ustala klucz publiczny oraz zależny od niego klucz prywatny. Jeżeli do szyfrowania zostaną użyte odpowiednio duże liczby pierwsze, to szyfr będzie odporny na złamanie, ponieważ odczytanie zakodowanej wiadomości wymagałoby rozłożenia bardzo dużej liczby na czynniki pierwsze, co nawet przy dzisiejszym stopniu zaawansowania technik obliczeniowych jest niezwykle trudne i czasochłonne. Jedną z podstawowych zalet RSA (oprócz idei pary kluczy) jest jego siła – teoretycznie możliwe jest wykorzystywanie kluczy dowolnej długości (na przykład 512 lub 1024 bity). W dzisiejszych czasach wysoki poziom bezpieczeństwa zapewniają klucze o długości 1024 bitów (128 cyfr), natomiast w najbliższym czasie długość ta ma wzrosnąć do 2048 bitów.

Zaprezentujemy na prostym przykładzie, jak przebiega szyfrowanie informacji przy pomocy RSA.

Założmy, że celem jest zaszyfrowanie następującego komunikatu „I hope you like it”.

I. KONSTRUKCJA KLUCZA

- 1) Wybieramy dwie duże liczby pierwsze p i q (w naszym przypadku niezbyt duże, aby uprościć obliczenia):

$$p = 23, q = 31$$

- 2) Obliczamy ich iloczyn $n = p \cdot q$

$$n = 23 \cdot 31 = 713$$

- 3) Obliczamy liczbę $\varphi = (p - 1) \cdot (q - 1)$

$$\varphi = (p - 1) \cdot (q - 1) = 22 \cdot 30 = 660$$

- 4) Wybieramy losowo (zazwyczaj wykorzystując generator liczb losowych) liczbę e , taką, że $0 < e < n$ oraz $\text{NWD}(e, \varphi) = 1$. Niech:

$$e = 101$$

- 5) Znajdujemy liczbę d , taką że $e \cdot d \pmod{\varphi} = 1$ (tzn. reszta z dzielenia $e \cdot d$ przez φ jest równa 1):

$$d = 281$$

$$\text{Sprawdźmy: } e \cdot d \pmod{\varphi} = 28381 \pmod{660} = 1$$

- 6) Podajemy do ogólnej wiadomości klucz publiczny, który jest parą $K_{\text{publiczny}} = (n, e)$, czyli w naszym przypadku $K_{\text{publiczny}} = (713, 101)$.
- 7) Dla siebie zachowujemy w tajemnicy klucz prywatny, który jest parą $K_{\text{prywatny}} = (n, d)$, czyli w naszym przypadku $K_{\text{prywatny}} = (713, 281)$

II. SZYFROWANIE INFORMACJI

- 1) Dokonujemy przekształcenia szyfrowanej wiadomości tak, aby można było zastosować RSA tzn. przypisujemy poszczególnym literom alfabetu odpowiednie znaki. Możemy zrobić to w przykładowy sposób wskazany w tablicy poniżej.

Tablica 2. Przyporządkowanie literom alfabetu odpowiednich znaków

Litera	A	B	C	D	E	F	G	H	I	J	K	L	M
Znak	01	02	03	04	05	06	07	08	09	10	11	12	13
Litera	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Znak	14	15	16	17	18	19	20	21	22	23	24	25	26

Spację zaś szyfrujemy przy pomocy znaku 00.

Według podanego schematu szyfrowany komunikat sprowadzamy do następującej postaci:

090 008 151 606 002 515 210 012 091 105 000 920

- 2) Następnie szyfrujemy wiadomość. Do zaszyfrowania stosujemy wzór $c = m^e \pmod{n}$, tzn. kodem liczby m jest reszta z dzielenia potęgi m^e przez n , gdzie m jest liczbą odpowiadająca fragmentowi tekstu do zaszyfrowania (w naszym przypadku są to bloki liczbowe złożone z trzech cyfr, co wynika z ilości cyfr wybranej liczby n).

Według wzoru $c = m^{101} \pmod{713}$ mamy:

Wiadomość	090	008	151	605	002	515	210	012	091	105	000	920
Szyfr	111	541	399	388	188	196	538	052	091	238	000	322

W ten oto sposób otrzymaliśmy kod, przy pomocy którego utajniłmy nasz komunikat.

Kod ten jest postaci:

111 541 399 388 188 196 538 052 091 238 000 322

III. DESZYFROWANIE INFORMACJI

- 1) Do odszyfrowania wiadomości stosuje się analogiczny wzór, jak w przypadku szyfrowania, a mianowicie $m = c^d \pmod n$, tzn. liczymy resztę z dzielenia potęgi c^d przez n , gdzie c jest liczbą naturalną (w naszym przypadku są to 3-cyfrowe bloki wyodrębnione w zaszyfrowanym komunikacie).

Według wzoru $m = c^{281} \pmod{713}$ mamy:

Szyfr	111	541	399	388	188	196	538	052	091	238	000	322
Wiadomość	090	008	151	605	002	515	210	012	091	105	000	920

- 2) Zamiana danych liczbowych na wiadomość.

Powracamy do komunikatu słownego wykorzystując w tym celu Tablicę 2.

09 – I, 00 – SPACJA, 08 – H, 15 – O, 16 – P, 05 – E, 00 – SPACJA, 25 – Y, 15 – O, 21 – U, 00 – SPACJA, 12 – L, 09 – I, 11 – K, 05 – E, 00 – SPACJA, 09 – I, 20 – T.

W efekcie otrzymujemy nasz wyjściowy komunikat: „I hope you like it”.

Choć RSA został opracowany już w 1977 r., to jest wciąż powszechnie stosowany samodzielnie lub w połączeniu z innymi szybszymi algorytmami szyfrującymi takimi jak DES i nic nie wskazuje na to, aby sytuacja ta w najbliższym czasie miała ulec zmianie. Bez RSA, a zatem tym samym bez liczb pierwszych, na których jest on oparty, wiele zdobyć cywilizacyjnych takich jak: bankomaty, telefony komórkowe, telewizja cyfrowa, czy Internet nie mogłoby się obyć. To dzięki RSA i liczbom pierwszym bez obaw o własną prywatność i o poufność przekazywanych informacji możemy m.in. wysyłać e-maile, czy realizować wszelkie transakcje internetowe takie jak przelewy, sprawdzanie stanu konta, zakładanie lokaty, zakupy itp. Na RSA bazuje również coraz bardziej powszechny podpis elektroniczny. Wielkie liczby pierwsze znalazły także zastosowanie w testowaniu mocy obliczeniowej superkomputerów oraz przy konstruowaniu kodów korekcyjnych do wyszukiwania błędów w przekazie obrazów i danych (m.in. satelity, sondy kosmiczne).

Aż trudno uwierzyć, że liczby pierwsze – pojęcie wydawać by się mogło tak banalne – okazało się generować tak skomplikowane i zarazem tak użyteczne zagadnienia z nimi związane. Liczby pierwsze przez wieki skrywały w sobie tak ogromne możliwości, które tylko wystarczyło zauważyć i odpowiednio wykorzystać.

Lecz przecież nie poznaliśmy jeszcze całej tajemnicy liczb pierwszych. Być może skrywają one w sobie coś więcej, co tylko czeka na to, by ktoś to spostrzegł i co kolejny raz okaże się kluczowe w rozwoju naszej cywilizacji.

Literatura:

1. Derbyshire J., *Obsesja liczb pierwszych*, NAKOM, Poznań 2008
2. Mikołajczyk M., Śliwiński M., *Rekordowe pierwszaki*, <http://www.matematyka.wroc.pl/doniesienia/rekordowy-pierwszak>
3. Miś B., *W pogoni za rekordem*, "Wiedzy i Życia", nr 2 1998
4. Mochnacki W., *Kody korekcyjne i kryptografia*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2000
5. Omiljanowski K., *Czy istnieje wzór na n-tą liczbę pierwszą?*, <http://www.matematyka.wroc.pl/ciekawieomatematyce2/czy-istnieje-wzor-na-n-ta-liczbe-pierwsza>