Najsłynniejsza funkcja świata

Zanim oddalimy się od tytułu tego opracowania ,żeby potem do niego wrócić, kilka słów wstępu. Funkcja dzeta Riemanna jest bohaterką najsławniejszego i największego obecnie, nierozwiązanego problemu matematyki, tzw. hipotezy Riemanna. Funkcja ta opisana jest poniższym równaniem,

$$\zeta(z) = \sum_{n=1}^{\infty} \left(\frac{1}{n}\right)^z$$

Hipoteza mówi, że wszystkie miejsca zerowe tej funkcji (oprócz tzw. przypadków trywialnych o których nieco później) są położone na jednej prostej. No a gdzież miałyby być położone? – ktoś może spytać – Przecież wszystkie liczby leżą na jednej osi liczbowej. I w tym właśnie miejscu musimy odejść od głównej tematyki i zapoznać się z pełnym zbiorem liczb czyli płaszczyzną liczbową.

Płaszczyzna liczbowa (czyli ciało dwuwymiarowe) gromadzi w sposób uporządkowany wszystkie liczby. Dla lepszego skojarzenia możemy powiedzieć, że ta płaszczyzna wygląda jak płaski układ współrzędnych gdzie oś X to oś liczb rzeczywistych, a oś Y to oś liczb urojonych (ta nazwa historycznie pozostała w matematyce z okresu gdy liczby urojone przebijały się do ludzkiej świadomości chociaż matematyczna rzeczywistość liczb urojonych jest dokładnie taka sama jak rzeczywistość liczb rzeczywistych). Mamy więc dwie osie liczbowe położone prostopadle względem siebie. Całą resztę płaszczyzny wypełniają liczby, które są sumami liczb rzeczywistych i urojonych. Oczywiście każda suma jest liczbą (np.: $\sqrt{2}+\sqrt{5}$) – nie musimy tej sumy zapisywać w postaci ułamka dziesiętnego, ta suma jest już liczbą, która ma swoje konkretne położenie na osi. Analogicznie suma ***1+2i*** też jest liczbą. I to w dodatku bardzo ciekawą liczbą bo „***i***” użyte w jej zapisie jest równe $\sqrt{-1}$. W dalszym ciągu tego artykułu sukcesywnie będziemy burzyć szkolny stereotyp, że nie można wyciągać pierwiastków kwadratowych z liczb ujemnych.

Przyjęcie do wiadomości istnienia liczby, która jest pierwiastkiem z minus jeden miało o wiele dłuższą historię niż pogodzenie się z istnieniem $\sqrt{2}$. Otóż pitagorejczycy byli zaskoczeni własnym odkryciem, że przekątna kwadratu o boku jeden ma właśnie taką długość niedającą się wyrazić w postaci żadnego ułamka liczb całkowitych. Na szczęście dla $\sqrt{2}$ wystarczy spojrzeć na kwadrat z zaznaczoną przekątną aby uświadomić sobie że ten pierwiastek istnieje i nasz opór wewnętrzny nic tu nie wskóra. Jest to jedno z pierwszych potwierdzeń dla platońskiego punktu widzenia matematyki jako obiektu absolutnego który odkrywamy a nie tworzymy. Ze względu między innymi na fakty zawarte w dalszej części tej pracy autor uważa podobnie. Liczba „***i***" pojawiła się w matematyce z powodu rozważań nad równaniami trzeciego stopnia czyli tylko o stopień wyższymi od równań kwadratowych znanych ze szkoły.

równanie trzeciego stopnia:

$$ax^3 + bx^2 + cx + d = 0$$

W XVI wieku Cardano próbował podać ogólne rozwiązanie równania trzeciego stopnia. Czytelnik zapewne pamięta, że równanie stopnia drugiego ma swoją deltę i na jej podstawie wyznacza się rozwiązania. Cardano skupił się na równaniu prostszym od podanego wyżej mianowicie na:

$$x^3 + bx = c$$

i wyznaczył dla tego równania deltę. Za pomocą delty mógł obliczyć rozwiązania. Okazało się jednak, że dla pewnych wartości ***a*** i ***b*** delta daje się łatwo obliczyć, a dla innych otrzymujemy pierwiastek kwadratowy z liczby ujemnej. W sumie nie jest to nic zaskakującego biorąc pod uwagę znany ze szkoły fakt, że obliczając pierwiastek z delty dla równania kwadratowego też natykaliśmy się na pierwiastki z wielkości ujemnych. Różnica jest jednak fundamentalna ponieważ dla równania kwadratowego taki przypadek oznaczał brak rozwiązań a dla równania trzeciego stopnia nie. Cardano podał przykłady równań, w których musiał przerwać obliczenia po napotkaniu pierwiastka z liczby ujemnej, a następnie zgadywał rozwiązanie podstawiając za x konkretną wartość i okazywało się, że lewa=prawej (!?). Dla matematyka metoda „zgaduj-zgaduli" jest cokolwiek deprymująca dlatego Bombelli zaproponował, aby nie przejmować się liczbą ujemną pod pierwiastkiem i kontynuować przekształcanie równania. Na skutek tych przekształceń każdy taki przypadek dało się sprowadzić do wyglądającego „normalnie" równania, w którym plątała się tylko jedna dziwna rzecz – tzn. $\sqrt{-1}$. Tenże pierwiastek na końcu szczęśliwie ulegał wyredukowaniu pozostawiając czyste rozwiązanie. Czyli sprawa załatwiona – ale czy do końca? W swoich przekształceniach Bombelli posługiwał się np. wyłączeniem liczby przed pierwiastek korzystając z tożsamości:

$$\sqrt{a*b} = \sqrt{a} * \sqrt{b}$$

dla pierwiastka z minus 4 wyglądało to następująco:

$$\sqrt{-4} = \sqrt{4*(-1)} = \sqrt{4} * \sqrt{-1} = 2\sqrt{-1}$$

Po prawej stronie mamy iloczyn 2 i pierwiastka z ujemnej jedności. Pamiętając, że mnożenie to wielokrotne (w tym przypadku dwukrotne) dodawanie możemy napisać:

$$\sqrt{-4} = \sqrt{-1} + \sqrt{-1} \quad (!?)$$

Suma dwóch nieistniejących liczb daje inną nieistniejącą liczbę!

Cały ten galimatias nie był dla matematyków zbyt wygodny. $\sqrt{-1}$ był traktowany jako niechciany gość, którego mimo wszystko wpuszcza się do domu, a potem wyrzuca z wielkim hukiem i zadowoleniem, że pozmywał gary i w dodatku mówi się o nim, że go nie ma i nigdy nie było. Ten kłopotliwy (i trochę wstydliwy) problem skłonił część matematyków do zastanowienia się o co tu właściwie chodzi. Nowa rzeczywistość z platońskiego świata powoli zaczęła się przebijać do ludzkiej świadomości.

Euler jako pierwszy założył, że istnieje pewna liczba ***i*** (od łacińskiego imaginarius – wymyślona, wyobrażona), która jest wynikiem pierwiastkowania jedności ujemnej czyli:

$$i = \sqrt{-1}$$

Samo jednak wprowadzenie symbolu niczego jeszcze nie zmienia. Dalej niewiele wiadomo o tej dziwnej liczbie. Być może dowiedzielibyśmy się czegoś więcej sprawdzając jak daleko od zera jest ta liczba położona. Można to sprawdzić wyznaczając moduł (czyli wartość bezwzględną tej liczby). W ujęcie geometrycznym moduł daje nam informację właśnie o odległości danej liczby od zera (np. liczby:-2 oraz 2 mają moduł równy 2 i obydwie są oddalone od zera o 2).

Zauważmy, że skoro ***i*** jest wynikiem pierwiastkowania minus jedynki to automatycznie:

$$i^2 = -1$$

Wstawmy teraz obie strony równania pod moduł:

$$\left|i^2\right| = |-1|$$

Jeśli twierdzimy, że ***i*** jest liczbą to musi spełniać tożsamość, którą spełnia każda przyzwoita liczba:

$$|a * b| = |a| * |b|$$

Dla naszych rozważań oznacza to, że:

$$|i * i| = |-1|$$

$$|i| * |i| = |-1|$$

$$|i| * |i| = 1$$

Dzieląc obustronnie przez moduł z ***i***:

$$|i| = \frac{1}{|i|}$$

Powyższe równanie jest prawdziwe tylko dla $|i| = 1$. Łatwo to sprawdzić podstawiając za $|i|$ inne wartości.

Wniosek: Liczba ***i*** jest położona w jednostkowej odległości od zera podobnie jak liczby 1 oraz -1, ale nie jest żadną z nich. Gdzie więc jej szukać?

Z pomocą przychodzi nam równanie udowodnione przez Eulera. Dowód niestety wymaga znajomości matematyki wyższej a w szczególności rozwijania funkcji w szeregi nieskończone.

$e^{ix} = \cos x + i * \sin x$, dla dowolnego x.

Przytoczone równanie zawiera oprócz liczby ***i*** także liczbę ***e***, które należy się parę słów wyjaśnienia. Liczba ***e*** jest podstawą logarytmów naturalnych. Po prostu znany szeroko logarytm dziesiętny ($\log_{10} x$)staje się logarytmem naturalnym (oznaczanym przez ln) gdy w podstawę wstawimy mu ***e***:

$$\log_e x = \ln x$$

Sama liczba ***e*** jest natomiast liczbą niewymierną o nieskończonym i nieokresowym rozwinięciu dziesiętnym (jest dodatkowo liczbą przestępną podobnie jak π, ale nie będziemy się tym tutaj zajmować).

W przybliżeniu $e \approx 2.718281828459.....$

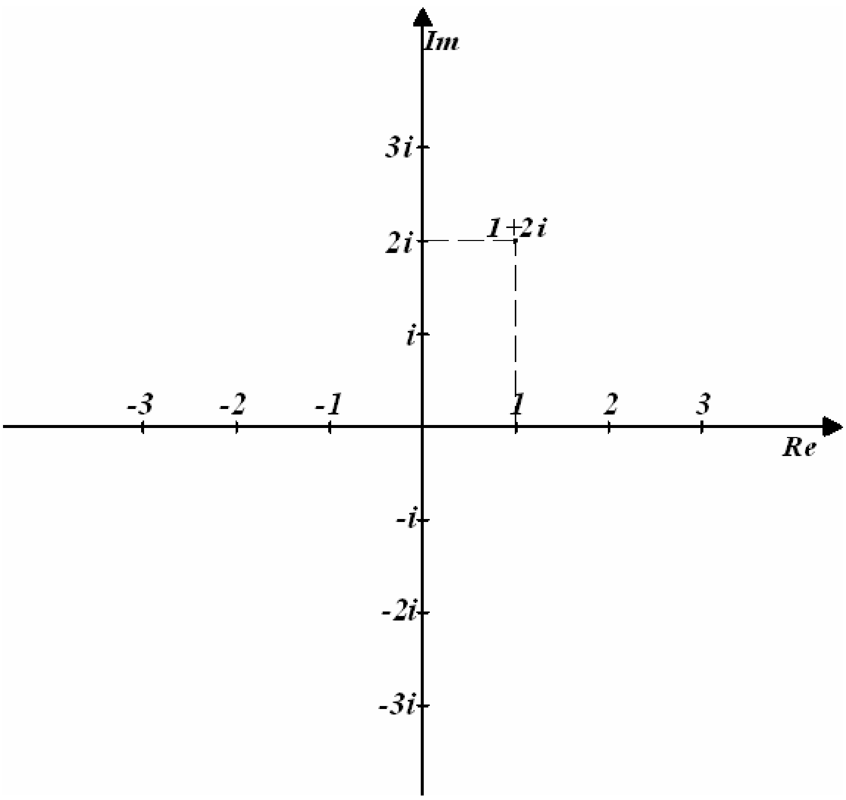
A dokładnie e jest granicą podanego poniżej ciągu:

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$$

Nieprzypadkowo logarytmy oparte na liczbie ***e*** nazywane są naturalnymi. Ich obecność w naturze świata (i wszechświata) jest powszechna. Tym samym powszechna jest obecność liczby ***e*** w matematycznych opisach zjawisk fizycznych i to praktycznie bez względu na ich rodzaj. Jest to bardzo ważna liczba w matematyce którą ,nie wiedzieć czemu, natura bardzo sobie ulubiła. Po tej dygresji na temat liczby ***e*** wróćmy do wcześniejszego równania Eulera.

$e^{ix} = \cos x + i * \sin x$

Pokazane w tym równaniu silne związki trygonometryczne doprowadziły Gauss'a do odnalezienia geometrycznej natury pełnego zbioru liczb. Dla utrwalenia napiszmy jeszcze raz, że jest to płaszczyzna z dwiema prostopadłymi osiami, gdzie pozostałe punkty płaszczyzny wypełniają liczby, które są sumami liczb rzeczywistych i urojonych (tzw. liczby zespolone).



Dodatkowo równanie Eulera było bazą do wykazania, że wszystkie liczby na płaszczyźnie można pierwiastkować, potęgować, logarytmować itd. Zachodzą wśród nich wszystkie relacje charakterystyczne dla liczb np. przemienność dodawania i mnożenia (dla ciekawych dodam, że Gauss wykazał również że płaszczyzna jest pełnym zbiorem liczb i nie można już tego zbioru poszerzyć na przestrzeń 3-wymiarową lub o większej liczbie wymiarów ze względu na niezachowanie przemienności mnożenia).

Jakby tego było mało równanie Eulera dla $x = \pi$ przybiera postać:

$e^{i\pi} = -1$

Tak silnego związku pomiędzy tymi trzema liczbami po lewej stronie nie spodziewałby się żaden matematyk przed przystąpieniem do rozpatrywania fenomenu $\sqrt{-1}$.
Związek ten jest naprawdę niespodziewany biorąc pod uwagę pochodzenie tych liczb z całkowicie odrębnych matematycznych zakątków:

e - zagadnienia związane z logarytmowaniem (pierwotnie w celu obliczania orbit planet)
i - zagadnienie rozwiązania ogólnego dla równań 3-go stopnia
π - zagadnienie obwodu i pola koła
-1 -jedność ujemna, której też na początku odmawiano prawa do matematycznego bytu, a jednak…

Kiedy w matematyce dochodzi się do takich wniosków nie może to być przypadek.
I rzeczywiście liczby zespolone a w konsekwencji funkcje zespolone zaczęły stopniowo ujawniać swoje fenomenalne właściwości. Bez nich nie poznalibyśmy tak intrygujących zagadnień jak np. uogólnione twierdzenie Newtona-Leibniza, fraktal Mandelbrota czy transformacja Laplace'a. Nic więc dziwnego, że to właśnie funkcje zespolone skrywają tajemnicę związaną z liczbami pierwszymi. To zdanie otwiera nowy przedział w naszych rozważaniach.

Liczba pierwsza to taka, którą można podzielić bez reszty wyłącznie przez nią samą lub przez jeden. Tak więc 21 nie jest liczbą pierwszą, bo dzieli się przez 3 i 7, ale już 3 i 7 są liczbami pierwszymi, ponieważ nie mają innych dzielników oprócz jedynki i siebie samych. Można powiedzieć, że liczby pierwsze są podstawowym budulcem dla liczb w ogóle, numerycznym odpowiednikiem atomów. Tak jak cząsteczkę wody można rozbić na dwa atomy wodoru i jeden tlenu, tak też liczby naturalne, np. 90, da się rozbić na elementarne cegiełki: 2, 3, 3 i 5, ponieważ 2 × 3 × 3 × 5 = 90. Dogłębne zrozumienie liczb pierwszych prowadzi do lepszego zrozumienia wszystkich liczb.

Jednym z pierwszych badaczy tych liczb był Euklides, żyjący ok. 300 lat p.n.e. w Aleksandrii. Zauważył on, że im większe wartości na osi liczbowej, tym rzadziej występują liczby pierwsze. Na przykład, między 10 a 20 są cztery liczby pierwsze (11, 13, 17, 19), natomiast między 110 a 120 jest już tylko jedna (113). Zastanawiał się, czy w pewnym momencie liczby te się wyczerpują, czy też ciągną się do nieskończoności. Euklides dokonał w końcu jednego z najbardziej genialnych i doniosłych odkryć w nauce: jako pierwszy udowodnił, że liczb pierwszych jest nieskończenie wiele. Skoro jest ich tak dużo a ich definicja jest elementarnie zrozumiała to automatycznie nasuwa się pytanie o równanie generujące kolejne liczby pierwsze (podobnie jak równanie, które generuje np. kolejne liczby parzyste lub nieparzyste). Mechanizm byłby prosty – jeśli bylibyśmy zainteresowani np. 789-tą liczbą pierwszą z kolei to podstawiamy do równania 789 a równanie zwraca nam liczbę pierwszą. Tym zagadnieniem zajmowano się już w starożytności za czasów Euklidesa, a jednak nie znaleziono nie tylko konstruktywnego równania tego typu, ale nawet wzoru, który generowałby wyłącznie liczby pierwsze, niekoniecznie wszystkie i tak pozostało do dziś!

Dobrze znane jest twierdzenie mówiące, że jeśli ***a*** i ***b*** są względnie pierwsze, czyli jedynym ich wspólnym dzielnikiem jest jedynka, to w ciągu $\{an+b\}$ istnieje nieskończenie wiele liczb pierwszych. Jest to twierdzenie Dirichleta; nic jednak nie można powiedzieć o tym, który z wyrazów tego ciągu jest liczbą pierwszą, a który nie. Są ponadto wzory, które skrywają nieskończenie wiele liczb pierwszych, chociaż wiadomo, że opisują one także liczby złożone (czyli takie, które można rozłożyć na liczby pierwsze). Liczby pierwsze świetnie generuje $2^n - 1$, gdzie n jest liczbą pierwszą. Cóż z tego skoro ciąg liczb pierwszych uzyskanych w ten sposób jest „dziurawy” tzn. pomiędzy dowolnymi dwiema liczbami ciągu mogą znajdować się liczby pierwsze „przegapione” przez ten wzór. Gdy natomiast skoncentrujemy uwagę na rozmieszczeniu liczb pierwszych, dość szybko odniesiemy wrażenie, że jest ono nadzwyczaj przypadkowe.

Istotnie, można dostrzec zjawiska zaskakujące. Jedyną liczbą pierwszą parzystą jest 2. Stąd wynika, że oprócz pary 2 i 3, liczby pierwsze nie mogą być odległe o mniej niż 2. Pary odległe o 2 występują na początku tablicy liczb pierwszych często: 5 i 7, 11 i 13, 17 i 19... Takie liczby pierwsze nazwano bliźniaczymi. Otóż liczby bliźniacze pojawiają się nawet bardzo daleko! Kolejna dziwna rzecz - nie ma w tym żadnego porządku! Zdarza się nawet, że istnieją całe serie liczb pierwszych: p, p+2, p+6 i p+8.
Takie są na przykład: 1871, 1873, 1877 i 1879.

Bywają także sytuacje całkiem odmienne - liczby pierwsze rozmieszczone są rzadko, odstęp między sąsiadami jest duży. Łatwo można wskazać ciąg kolejnych liczb naturalnych o zadanej z góry długości, wśród których nie ma liczby pierwszej. Ciąg trójwyrazowy to na przykład: 8, 9, 10, czterowyrazowy - 24, 25, 26, 27. Dla zadanego z góry ***n*** taki ciąg można wskazać następująco:

$(n+1)!-2, (n+1)!-3, ..., (n+1)!-(n+1)$.

Liczba ***n*** może być niewyobrażalnie wielka, na przykład 10^{1010} lub $(10!)^{100!}$. Wtedy wyrazy tego ciągu są jeszcze dalej, co więcej, takich ciągów jest nieskończenie wiele. Na temat samotnych liczb pierwszych uzyskano ciekawe rezultaty. Na przykład okazuje się, że istnieją liczby pierwsze odległe od innych tak bardzo, jak tylko chcemy! Formalnie - dla dowolnego ***k*** istnieje liczba pierwsza ***p*** o tej własności, że w przedziale $(p-k, p+k)$ jest ona jedyną liczbą pierwszą. W przypadku odległości 10 taką liczbą może być na przykład 211; poprzednia liczba pierwsza to 199, następna to 223. Twierdzenie nie podaje jednak sposobu na znajdowanie takich liczb pierwszych, mówi jedynie o ich istnieniu. Największe znane obecnie dla konkretnych liczb odstępy nie przekraczają tysiąca. Ale wiadomo, że istnieją liczby pierwsze takie, że w promieniu na przykład stu bilionów nie ma żadnej innej liczby pierwszej, co więcej, takich liczb jest nieskończenie wiele (!), choć może nigdy nie dowiemy się, jak wygląda przynajmniej jedna z nich. Z drugiej strony może się też zdarzyć, że wśród stu kolejnych liczb naturalnych odnajdziemy nawet dziesięć liczb pierwszych. Czy rządzą tym jakieś prawa? Ciekawe, że odpowiedzi na te i inne, podobne, elementarne wręcz pytania nie są znane. Pewne częściowe rozwiązania niektórych problemów są nadspodziewanie zawiłe i wykorzystują zaawansowane rezultaty z różnych działów matematyki. Udowodniono wiele zadziwiających twierdzeń opisujących własności liczb pierwszych. W miarę upływu czasu coraz bardziej utwierdzano się w przekonaniu, że w ich rozmieszczeniu nie ma żadnej regularności. I oto nagle, pod koniec XVIII wieku, został odkryty pewien zaskakujący związek.

Kluczem do sukcesu jest pytanie: ile liczb pierwszych znajduje się pomiędzy zerem a x, gdzie x może być dowolną liczbą naturalną? Żeby podać odpowiedź na to pytanie zdefiniowano funkcję $\pi(x)$ zliczającą liczby pierwsze (π jest tu użyte jako nazwa funkcji). Poniżej podano kilka wartości tej funkcji dla pewnych x

$\pi(2)=1$,
$\pi(3)=2$
$\pi(p)=2$

$\pi(10)=4$

$\pi(100)=25$

$\pi(1000)=168$

$\pi(10000)=1229$

$\pi(1000000)= 78498$

Dla lepszego zrozumienia: $\pi(1000)=168$ oznacza, że pomiędzy zerem a tysiącem jest 168 liczb pierwszych.

Czy można tu dopatrzyć się jakiejkolwiek regularności? Mimo to Carl Friedrich Gauss (w wieku 14 lat!!!) i Adrien Marie Legendre zauważyli niezależnie, że istnieje związek pomiędzy funkcją $\pi(x)$ a... logarytmem naturalnym. Związek ten jest następujący. Stosunek wartości x do jego logarytmu naturalnego przy wzrastającym x jest coraz bliższy wartości funkcji $\pi(x)$. W ścisłym matematycznym sformułowaniu wygląda to następująco:

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

A więc rozkład liczb pierwszych wśród liczb naturalnych choć jest chaotyczny to jednak podlega silnej prawidłowości. To już coś! Ważne jest by dodać, że podana równość jest asymptotyczna czyli dla każdego skończonego x możemy z dużym przybliżeniem określić wartość $\pi(x)$. Im większe x tym nasze przybliżenie staje się bliższe prawdzie, ale dokładną równość osiągamy dopiero dla nieskończenie dużego x. Konkludując możemy stwierdzić, że rozkład liczb pierwszych podlega prawom, ale dokładny rozkład tych liczb wśród liczb naturalnych wymyka się nam i możemy go określić tylko z pewnym prawdopodobieństwem (czy nie brzmi to podobnie do zasady nieoznaczoności Heisenberg'a z mechaniki kwantowej – czyżby nieoznaczoność była również wpisana w taki absolut jakim są liczby???).

Pojęcie liczby jest w matematyce czymś pierwotnym. Od niej wszystko się zaczęło. Zapewne początkowo służyła do celów praktycznych i była ściśle związana ze światem fizycznym. Za jej pomocą można było policzyć np. ilość upolowanych mamutów. Potem okazało się, że liczbę można traktować jako odrębny niefizyczny byt – np. jeszcze przed polowaniem można było obliczyć jak podzielić upolowane mamuty między członków plemienia zakładając z doświadczenia jak obfite będą łowy. W ten sposób liczba oderwała się od ziemskiego padołu i dała początek niesłychanej ewolucji abstrakcji matematycznych. Od czasów Newtona obserwujemy jednak zjawisko odwrotne. Matematyka wraz z całym swoim aparatem tryumfalnie powraca do opisu zjawisk otaczającego nas świata i wszechświata. Znajduje zastosowania we wszystkich dziedzinach ludzkiego rozwoju. Co ciekawe, nawet liczb pierwszych nie ominął ten los.

„Zarówno Gauss jak i inni matematycy mają rację twierdząc, że istnieje tylko jedna dyscyplina -teoria liczb, która jest tak daleko od zwyczajnej ludzkiej działalności, że pozostanie czysta i nieskażona."
G. H. Hardy, *A Mathematician's Apology,* 1940 .

Ten cytat został przekornie zamieszczony jako wstęp do kolejnego rozdziału. Cytat pochodzi z roku 1940 czyli z okresu kiedy obserwowany był rozwój technik kryptograficznych związanych z takim zaszyfrowaniem wiadomości, aby przeciwnik nie mógł jej odczytać.

Proces przesłania zaszyfrowanej wiadomości jest następujący. Nadawca (N) w pewien tylko sobie znany sposób zamienia informację jawną na zakodowaną. Następnie informacja w postaci zaszyfrowanej zostaje wysłana do odbiorcy (O), który wie (i tylko on wie) jak ją odkodować. W momencie przesyłania wiadomości jest ona oczywiście narażona na przechwycenie przez osoby niepożądane (OP). Gdy takie przechwycenie nastąpi można rozpocząć prace nad deszyfrowaniem ważnej informacji. Zauważmy, że gdyby OP przechwycił wiadomość od N wraz z informacją o sposobie jej kodowania miałby wszystkie instrumenty potrzebne żeby odczytać informację zaszyfrowaną jako jawną.

Trudność pierwsza:
N musi jednak przekazać O w jaki sposób zaszyfrował wiadomość, bo inaczej O nie będzie miał z niej żadnego użytku. W rzeczywistości wystarczy zdobyć informację o sposobie szyfrowania (tzw. klucz szyfrujący) i cała wymiana wiadomości pomiędzy N a O będzie dla nas jako OP całkowicie jasna.

Trudność druga:
Innym sposobem jest przejęcie zaszyfrowanej wiadomości i „popracowanie" nad nią przy użyciu technik kryptograficznych. Zwykle po upływie pewnego rozsądnego czasu taką

informację daje się odkodować i tym samym poznajemy klucz szyfrujący (tak na przykład rozszyfrowano Enigmę w czasie drugiej wojny światowej). Jeśli tylko N nie zdążył w tym czasie w jakiś inny potajemny sposób przekazać O nowego klucza szyfrującego cel jest osiągnięty. Dlatego skoro już nadajemy zaszyfrowaną informację to w taki sposób, aby jej przejęcie, nawet w takiej zakodowanej formie, było jak najmniej prawdopodobne.

Sposoby szyfrowania informacji mogą być oczywiście rozmaite od banalnych (zastąp A kolejną literą z alfabetu itd.) do bardzo wysublimowanych, ale wszystkie one wymagają utajnienia klucz szyfrującego. Czy można tego uniknąć? Zdrowy rozsądek podpowiada, że nie. Po co szyfrować informację, którą każdy będzie mógł odkodować i odczytać? A jednak…

Współczesna kryptografia opiera się na ciekawej właściwości liczb pierwszych: stosunkowo łatwo jest je pomnożyć ($7 \times 13 = 91$), ale znaleźć odpowiedź na pytanie, jakie dwie liczby pierwsze pomnożone przez siebie dadzą konkretny wynik, jest o wiele trudniej (? x ? = 323 , spróbujcie sami). W przypadku bardzo dużych liczb to zadanie staje się praktycznie niemożliwe.

Przykład:
Wyobraźmy sobie, że mamy superszybki komputer, który jedno dzielenie dowolnie dużych liczb wykonuje w trakcie jednego taktu zegara, a szybkość procesora wynosi $10GHz= 10^{10}\ Hz$. Załóżmy, ponadto, że ma w pamięci wszystkie liczby pierwsze mające w zapisie do 33 cyfr. Jego zadanie polega na sprawdzeniu, czy dana liczba n (65-cyfrowa) jest liczbą pierwszą. Komputer dzieli daną liczbę przez wszystkie liczby pierwsze mniejsze od $\sqrt{n}$ (na mocy sita Eratostenesa), czyli liczby pierwsze co najwyżej 33-cyfrowe (które ma już w pamięci !!!). Obliczając przybliżoną wartość $\pi(x)$ dla $x=10^{33}$ otrzymujemy, że takich liczb jest około

$$\frac{10^{33}}{\ln(10^{33})} \approx \frac{10^{33}}{76} \approx 10^{31}$$

Mamy więc do wykonania około 10^{31} operacji. Biorąc pod uwagę częstotliwość zegara komputera otrzymujemy około 10^{21} sekund, co daje około 10^{13} lat czyli jakieś 700 razy dłużej niż szacowany wiek istniejącego wszechświata !!!

Podany przykład mówi o sprawdzeniu czy dana liczba jest liczbą pierwszą, ale zadanie rozłożenia danej liczby złożonej na iloczyn dwóch liczb pierwszych (np. 65-cyfrowych) jest zadaniem, które również wymaga podobnie długiego czasu.
Dzięki temu możemy przesyłać zakodowane informacje w sposób jawny (!!), ponieważ ich przejęcie wiąże się z koniecznością rozkładu pewnej liczby złożonej na czynniki pierwsze. Inaczej mówiąc możemy włożyć do koperty zaszyfrowany list a klucz szyfrujący nakleić zamiast znaczka. Następnie możemy go wręczyć dowolnemu kurierowi (nie musi być zaufany) a adresat (który zna rozkład klucza na czynniki pierwsze) bez trudu odczyta zakodowaną wiadomość. Jak widzimy trudność pierwsza i trudność druga znikają.

W ten sposób dziś dzięki matematyce liczb pierwszych możemy przesyłać dane o kartach kredytowych przez internet. Również dzięki liczbom pierwszym możliwe jest kodowanie emaili i ochrona ich zawartości. A w skali globalnej, kody zbudowane z liczb pierwszych służą do szyfrowania rządowych i wojskowych połączeń telefonicznych i pozwalają na zabezpieczenie się przed podsłuchem. Jak wspomniano wcześniej można generować (proces ten nazywa się faktoryzacją) liczby pierwsze, ale ogólne równania, które do tego służą są „dziurawe". Dlatego z wyżej wymienionych powodów uzyskiwane obliczeniowo liczby pierwsze pochodzące z „przegapionych" niszy są ,z całą powagą tego słowa, ściśle tajne i chronione identycznie jak każda tajemnica militarna. Nie bez powodu Amerykańska Agencja Bezpieczeństwa zatrudnia najwięcej matematyków na świecie.
Firma RSA, która jest właścicielem patentu kodowania opartego na liczbach pierwszych podała do publicznej wiadomości, że transakcje dokonywane w oparciu o szyfr RSA są tak samo pewne jak to, że nikomu nie uda się (w rozsądnym czasie) rozłożyć podanej niżej liczby na iloczyn dwóch czynników pierwszych.

3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609

Gdyby komuś się to udało zapewne RSA zbankrutowałaby w ciągu jednego dnia, a kursy akcji firm dokonujących internetowych operacji bankowych sięgnęłyby dna.

Nie oznacza to, że nie znamy liczb pierwszych o większej liczbie cyfr niż podana tu, ale liczby tego rozmiaru są wystarczające do efektywnego kodowania. Dla zaspokojenia ciekawości dodam, że największą obecnie znaną liczbą pierwszą jest uzyskana w grudniu 2005 roku w projekcie cywilnym liczba, która ma w zapisie dziesiętnym 9.152.052 cyfry a mimo to dzieli się tylko przez 1 i przez samą siebie!!!

Nadszedł wreszcie czas, aby wrócić do tytułu tego opracowania czyli do funkcji dzeta Riemanna i hipotezy z nią związanej.

Nazwisko Riemanna pojawia się w wielu dziedzinach matematyki, chociaż jego dorobek naukowy mieści się w niewielu opublikowanych pracach - dzisiaj zapewne mógłby on mieć kłopoty z uzyskaniem profesury z powodu małej liczby publikacji. Prace Riemanna były jednak rewolucyjne i do dziś są źródłem natchnienia dla matematyków i fizyków; z jego nie zawsze sprecyzowanych pomysłów rozwinęły się całe teorie. Prywatnie Riemann był bardzo skromny i nieśmiały, przez całe, niezbyt długie życie (1826-1866) dane mu było borykać się z biedą i chorobami. Nieśmiałość w sposobie bycia nie przeszkodziła śmiałości myśli, która dała mu nieśmiertelność.

W 1859 roku Riemann opublikował liczącą zaledwie osiem stron pracę dotyczącą znanej już nam funkcji $\pi(x)$. Na początku podał pewne nowatorskie (lepsze niż logarytm naturalny) przybliżenie tej funkcji, ale tu już kończą się żarty - owa przybliżona funkcja o nazwie R(x) ma postać:

$$R(x) = Li(x) - \sum_{i=2}^{\infty} \frac{1}{i} Li(\sqrt[i]{x})$$

gdzie - jakby tego było mało funkcja Li(x) jest nieelementarną funkcją nazywaną logarytmem całkowym.

$$Li(x) = \int_2^x \frac{dt}{\ln t}$$

Ta przerażająca dla niespecjalisty zależność jest tylko próbką środków wykorzystywanych w teorii liczb. Następnie w oparciu o pokazaną wcześniej funkcję R(x) Riemann zaproponował – i teraz UWAGA !!! - **dokładną** zależność opisującą funkcję $\pi(x)$, w której wykorzystywał podaną przed chwilą funkcję R(x) oraz miejsca zerowe pewnej funkcji zespolonej. Czytelnik zapewne domyśla się już, że ta funkcja zespolona to właśnie funkcja dzeta Riemanna.

David Hilbert, zaliczany do najwybitniejszych umysłów przełomu XIX i XX wieku, orientujący się w niemal całej współczesnej mu matematyce, powiedział kiedyś podczas wykładu:
„Gdybym w efekcie dotknięcia czarodziejskiej różdżki zasnął i obudził się dopiero po 500 latach, to nie pytałbym o to, jakie były przemiany dziejowe, polityczne, społeczne, ale spytałbym, co wiadomo w tych czasach o miejscach zerowych funkcji dzeta Riemanna, bo to jest najważniejsze zagadnienie w ogóle”.

Tak się składa, że duża ilość zjawisk, którymi jak się wydaje rządzą ogromnie skomplikowane mechanizmy daje się w istocie opisać matematycznymi zależnościami w prostej formie. Przykładem niech będzie opis rozchodzenia się pola elektromagnetycznego. Zjawisko to można ująć w układ dwóch wektorowych równań różniczkowych, których forma jest tak prosta, że właściwie prostszych równań nie da się wymyślić. Natura jest prosta – można tak powiedzieć. I dlatego właśnie funkcja dzeta Riemanna jest tak intrygująca zarówno dla matematyków i fizyków (okazuje się, z grubsza mówiąc, że ze statystycznego punktu widzenia rozkład kilku milionów znanych ciekawych miejsc zerowych funkcji dzeta jest właściwie taki sam, jak pewne rozkłady prawdopodobieństwa, badane z zupełnie innych przyczyn w mechanice kwantowej układów bardzo wielu cząstek elementarnych).
Funkcja dzeta posiada właśnie ten atrybut – prostotę formy. Postać funkcji podana na początku artykułu może budzić wprost przeciwne skojarzenia ale to samo wyrażenie zapisane w innej formie nie powinno stanowić większego problemu dla kogoś kto dotarł do tego miejsca i nie odłożył tego opracowania na półkę.

$$\zeta(z) = \sum_{n=1}^{\infty} \left(\frac{1}{n}\right)^{z} = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \frac{1}{4^z} + \ldots$$

Jest to po prostu suma z-tych potęg odwrotności wszystkich liczb naturalnych, gdzie z jest oczywiście argumentem funkcji pochodzącym z całej płaszczyzny liczb. Funkcja dzeta ma faktycznie prostą formę, charakterystyczną dla prawideł rządzących naturą, ale jej własności nie są już takie proste. Chciałoby się powiedzieć – prostota formy nie oznacza prostoty treści.

Funkcja dzeta była znana matematykom długo przed sformułowaniem hipotezy Riemanna i wykryciem jej związków z liczbami pierwszymi, ale była wtedy rozpatrywana jako funkcja rzeczywista zmiennej rzeczywistej:

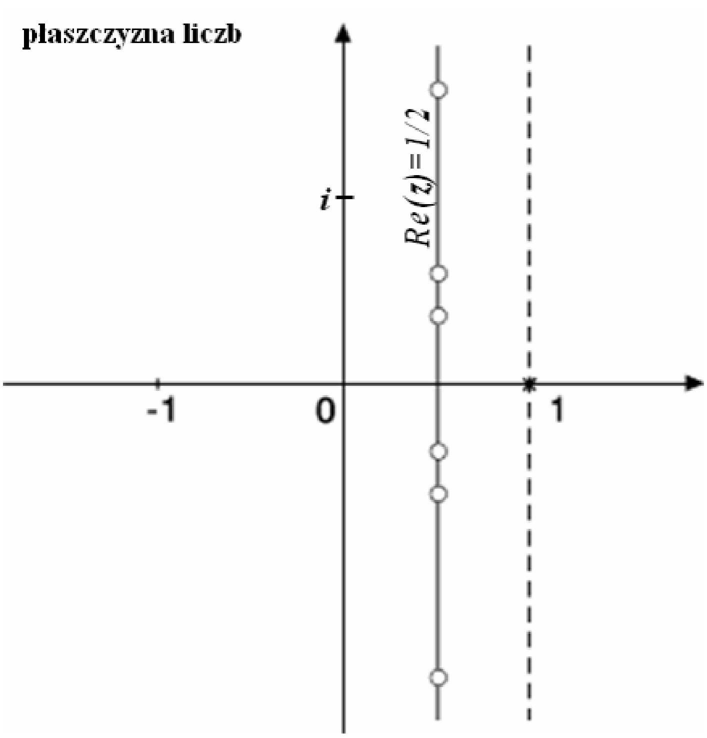
$$\zeta(x) = \sum_{n=1}^{\infty} \left(\frac{1}{n}\right)^{x} = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \dots$$

gdzie x jest zmienną funkcji przyjmującą wartości z przedziału liczb rzeczywistych (czyli z rzeczywistej osi liczbowej a nie z całej płaszczyzny). Rzecz jasna wartościami funkcji dla konkretnych x były również liczby rzeczywiste a nie zespolone. Już wtedy dzeta nastręczała sporo trudności przy próbach obliczania jej wartości. Wartości w punktach 2, 4, 6, 8, 10, 12 itd. umiano obliczać już w XVIII w. Na przykład wartość $\zeta(2)$, czyli suma kwadratów odwrotności wszystkich liczb naturalnych, jest równa $\frac{\pi^2}{6}$.

$$\zeta(2) = \sum_{n=1}^{\infty} \left(\frac{1}{n}\right)^{2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = \frac{\pi^2}{6}$$

Zupełnie inaczej wygląda sprawa wartości $\zeta(x)$ dla argumentów nieparzystych. Wiadomo o nich bardzo niewiele (do niedawna właściwsze byłoby stwierdzenie: nie wiadomo o nich prawie nic). Wszelkie metody stosowane do obliczania wartości $\zeta(2), \zeta(4), \zeta(6)$, itd. zawodzą na całej linii. W 1979 r. francuski matematyk Apéry wykazał, że $\zeta(3)$ jest liczbą niewymierną. Zrobił to w sposób pomysłowy, niebywale zręczny i zasadniczo całkowicie niezrozumiały: prześledzenie kolejnych kroków dowodu nie pozwala zrozumieć co trzeba byłoby w nim zmienić, żeby móc zastosować go do uzyskania jakichkolwiek informacji o wartościach $\zeta(5), \zeta(7), \zeta(9)$ ... Do niedawna twierdzenie Apéry'ego było właściwie jedyną informacją na temat wartości dzety w punktach nieparzystych.

Wiosną tego roku inny francuski matematyk, T. Rivoal , udowodnił, że wśród wartości $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ ..itd. jest nieskończenie wiele liczb niewymiernych. Jego dowód nie pozwala jednak wyliczyć żadnej z tych liczb. Prawdziwą swoją potęgę funkcja dzeta objawia jednak dopiero przy potraktowaniu jej jako funkcji zespolonej. Jak pokazał Riemann – w tej postaci jej miejsca zerowe skrywają odpowiedź na temat rozmieszczenia liczb pierwszych wśród liczb naturalnych. Od tej pory badanie miejsc zerowych funkcji dzeta stało się kamieniem filozoficznym matematyki. Miejsca zerowe, czyli takie dla których $\zeta(z) = 0$, stosunkowo łatwo odnaleźć wśród parzystych liczb ujemnych. Są to tzw. trywialnie miejsca zerowe uzyskiwane dla z=-2 , -4 , -6 itd. Jednak dzeta Riemanna jest funkcją zespoloną więc może zerować się również dla z nie należących do liczb rzeczywistych. I te właśnie miejsca zerowe są ujęte w hipotezę Riemanna. Hipoteza mówi, że są one położone na jednej prostej $\mathrm{Re}(z) = \frac{1}{2}$ (patrz rysunek poniżej), która nazywana jest prostą krytyczną. Czyli innymi słowy zerowanie następuje tylko dla takich liczb zespolonych, które są sumą $\frac{1}{2}$ oraz pewnych liczb urojonych. Odkrycia w matematyce są rzeczywiście zaskakujące – oto okazuje się, że odpowiedź na temat rozmieszczenia liczb pierwszych należy szukać (o ironio!!!) wśród tak niechcianych liczb urojonych.



Hipoteza Riemanna czeka już 150 lat na udowodnienie. Jak na razie nikomu się to nie udało chociaż udowodniono kilka innych twierdzeń związanych z miejscami zerowymi $\zeta(z)$. Mianowicie wiemy z całą pewnością, że wszystkie miejsca zerowe są położone w pasie pomiędzy osią liczb urojonych a prostą $\mathrm{Re}(z) = 1$ oznaczoną na rysunku linią przerywaną. Wiemy również, że na prostej krytycznej jest nieskończenie wiele miejsc zerowych (ale nie wiemy czy wszystkie). Ponadto udowodniono, że co najmniej $\frac{2}{5}$ czyli 40% miejsc zerowych leży na prostej krytycznej. To jednak za mało żeby stwierdzić, że hipoteza Riemanna jest prawdziwa. Gdyby się tak okazało może wreszcie poznalibyśmy tajemnicę liczb, które rzekomo sami sobie wymyśliliśmy. To odkrycie będzie miało zapewne bezpośredni wpływ na postęp w mechanice kwantowej zajmującej się podstawowymi „cegiełkami" wszechświata. Algorytmy rozkładu liczb złożonych na liczby pierwsze, które teraz nazywane są probabilistycznymi (bo dają odpowiedź mówiącą jak dalece prawdopodobne jest, że dwie wyliczone za ich pomocą liczby dają w efekcie rozpatrywaną liczbę złożoną) przeszłyby od wyników prawdopodobnych do stu procentowo pewnych, a to miałoby ze względów kryptograficznych bezpośredni wpływ na globalną ekonomię i szeroko pojęte bezpieczeństwo.

Czy kiedykolwiek dowiemy się czy Riemann miał rację stawiając swoją hipotezę? W tej kwestii zdania są podzielone. Z jednej strony uważa się, że jeżeli hipoteza Riemanna jest prawdziwa to zostanie kiedyś udowodniona podobnie jak wielkie twierdzenia Fermata, które na dowód czekało kilkaset lat. Z drugiej strony nie brakuje opinii, że hipoteza Riemanna może być przykładem twierdzenia, które mimo że jest prawdziwe (w sensie absolutnym) to nie będzie go można nigdy udowodnić. Dla poparcia takiej tezy przywoływane jest twierdzenie Gödla (koncepcyjnie oparte na liczbach pierwszych) , które mówi o istnieniu twierdzeń dla których nie można przeprowadzić dowodu rozstrzygającego o ich prawdziwości lub fałszu – dla niewtajemniczonego czytelnika może się do wydawać zaskakujące i rzeczywiście swojego czasu twierdzenie Gödla zatrzęsło fundamentami matematyki do tego stopnia, że niektórzy woleli nie rozumieć tego twierdzenia, bądź udawać że go nie rozumiejącą lub też zachowywali się tak jakby twierdzenie zawierało błędy, które na pewno ktoś odnajdzie, a więc można je zignorować. Na tym gruncie, w odniesieniu do liczb pierwszych, wyrosły całe koncepcje filozoficzne. Mówią one, że liczby pierwsze są swoistym bożym „odciskiem palca" odciśniętym u podstaw stworzenia. Jasnym sygnałem dla wszystkich istot rozumnych we wszechświecie. Sygnałem zawierającym przesłanie o barierach, których nasz rozum nie może przekroczyć. Kto wie, może rzeczywiście nigdy nie poznamy tajemnicy rozmieszczenia liczb pierwszych chociaż wiemy że jest ono ściśle zdeterminowane (takiego zdania był między innymi Euler) i na zawsze będziemy musieli posługiwać się jedynie prawdopodobieństwami. A być może ktoś dowiedzie prawdziwości hipotezy Riemanna lub też poznamy dowód o niemożliwości dowiedzenia tej hipotezy. Póki co możemy tylko czekać co pokaże czas…