# Liczby pierwsze

# Wprowadzenie do liczb pierwszych

Wiele liczb naturalnych daje się rozłożyć na czynniki mniejsze *np. 10=5*2 lub 111=3*37*. Jednak istnieją liczby, które nie mogą być rozłożone w taki sposób. Takie liczby nazywamy **liczbami pierwszymi**.

Liczba pierwsza to taka liczba całkowita p większa od jedności, której jedynymi dziennikami są 1 oraz p. Każdą liczbę naturalną większą od jedności, która nie jest liczbą pierwszą, nazywamy **liczbą złożoną.**

Liczba 0 z definicji nie jest ani liczbą pierwszą, ani liczbą złożoną.

Liczba 1 z definicji nie jest ani liczbą pierwszą, ani liczbą złożoną.

Pierwsze 34 liczby pierwsze to : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 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 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

Na czerwono zaznaczono liczby pierwsze mniejsze od 100

Liczb pierwszych jest nieskończenie wiele. Niech π(n) będzie określało ilość liczb pierwszych nie większych od n. Dla dużych wartości liczby n mamy wzór:

$$\frac{\pi(n)}{n} \simeq \frac{1}{ln(n)}$$

Oto kilka przykładów : liczb pierwszych mniejszych od 1000 jest 168. Wśród wszystkich liczb 100-cyfrowych w przybliżeniu jedna na każde 300 jest liczbą pierwszą.

Problem liczb pierwszych polega na ich rozmieszczeniu wśród liczb naturalnych. Nikt nie opracował dotąd żadnego wzoru pozwalającego na wyszukiwanie kolejnych liczb pierwszych. Istnieją wzory wyszukiwania liczb pierwszych o określonych właściwościach, nie ma jednak wzoru, który by dla każdego argumentu generował by liczbę pierwszą.

## Sito Eratostenesa

Najpopularniejszym algorytmem wyznaczania liczb pierwszych jest **Sito Eratostenesa**. Oto algorytm :

- Ze zbioru liczb naturalnych z przedziału [2,n] wybieramy najmniejszą liczbę 2 i wykreślamy wszystkie jej wielokrotności większe od niej samej.

- Z pozostałych liczb wybieramy najmniejszą niewykreśloną liczbę ( jest to liczba 3 ) i usuwamy wszystkie jej wielokrotności większe od niej samej.

- Wykreślanie powtarzamy do momentu gdy liczba i, której wielokrotność wykreślamy będzie większa niż pierwiastek z liczby n.

Wszystkie niewykreślone liczby z przedziału [2,n] są liczbami pierwszymi

## Gęstość liczb pierwszych

Teraz wprowadzamy nowe pojęcie **gęstości liczb pierwszych**. Niech $A_n$ oznacza ilość liczb pierwszych wśród liczb naturalnych 1,2,3,...,n. Zatem :

- $A_1 = 0$
- $A_2 = 1$
- $A_3 = 2$
- $A_4 = 2$
- $A_5 = 3$
- ...

Gęstość liczb pierwszych wśród n pierwszych liczb całkowitych jest dana przez stosunek : $\mathbf{A_n / n}$.

Poniżej przedstawiam tabelę zawierającą procent liczb pierwszych w danym przedziale **[a,b]** :

| a | b | procent |
|---|---|---|
| 2 | 2 | 100% |
| 2 | 4 | 66,67% |
| 2 | 8 | 57,14% |
| 2 | 16 | 40% |
| 2 | 32 | 35,48% |
| 2 | 64 | 28,57% |
| 2 | 128 | 24,41% |
| 2 | 256 | 21,18% |
| 2 | 512 | 18,98% |
| 2 | 1024 | 16,81% |
| 2 | 2048 | 15,1% |

| | | |
|---|---|---|
| 2 | 4096 | 13,77% |
| 2 | 8192 | 12,55% |
| 2 | 16384 | 11,60% |
| 2 | 32768 | 10,72% |
| 2 | 65536 | 9,98% |
| 2 | 131072 | 9,35% |
| 2 | 262144 | 8,77% |
| 2 | 524288 | 8,28% |
| 2 | 1048576 | 7,82% |

Procent liczb pierwszych z przedziału [a,..,b]

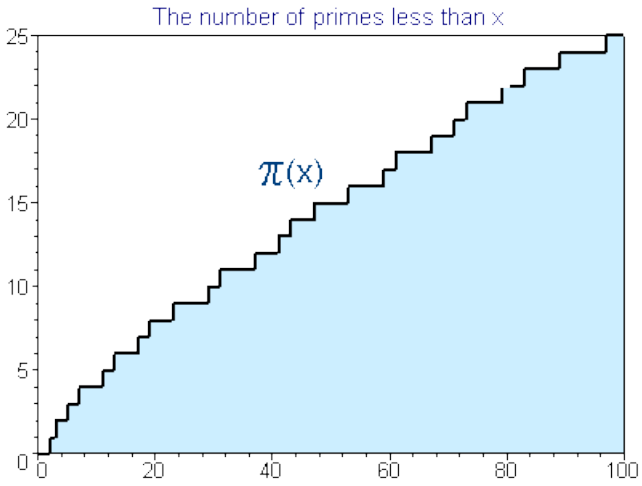
Niech π(n) będzie określało ilość liczb pierwszych nie większych od n. Jak już wspomniałem - dla dużych wartości liczby n mamy wzór:

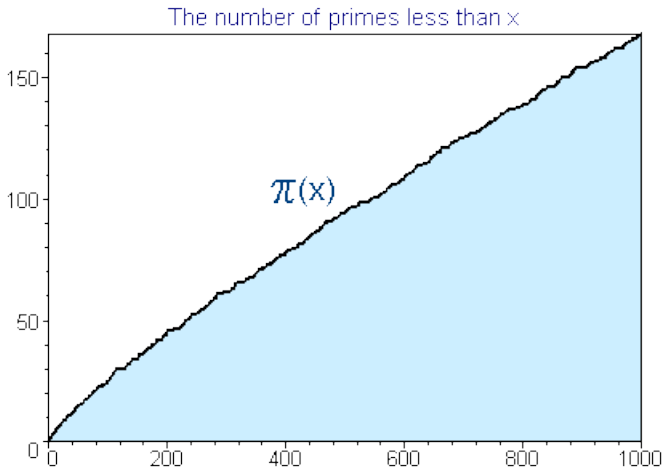
$$\frac{\pi(n)}{n} \simeq \frac{1}{ln(n)}$$

**Twierdzenie o liczbach pierwszych mówi nam, że :**

$$\frac{\frac{\pi(n)}{n}}{\frac{1}{ln(n)}}$$

dąży do 1 przy wzroście liczby n. Oto przybliżony wykres funkcji **π(n)** :




## Rodzaje liczb pierwszych

### Liczby Mersenne'a

- Niech liczba $M_q = 2^q - 1$
- Niech q będzie liczbą naturalną.

Wtedy $M_q$ jest liczbą Mersenne'a. Sprośród wszystkich wygenerowanych do tej pory liczb tego typu zaledwie 48 to liczby pierwsze.

### Liczby pierwsze bliźniacze.

Liczby bliźniacze to dwie liczby pierwsze różniące się o 2.
Na przykład:

- (3, 5)
- (5, 7)
- (59, 61)
- (1619, 1621)

### Liczby pierwsze czworacze

Liczby czworacze to takie liczby: p , p+2, p+6, p+8, że każda z nich jest liczbą pierwszą.
Na przykład:

- 5, 7, 11, 13
- 821, 823, 827, 829

**Liczby pierwsze izolowane**
Liczba pierwsza p jest izolowana, jeśli najbliższa liczba pierwsza różni się od niej co najmniej o 4.
Na przykład 89, 157, 173.

**Liczby Sophie Germain**
Liczba pierwsza p jest liczbą Sophie Germain, jeśli liczba 2p+1 także jest liczbą pierwszą.

**Liczby pierwsze lustrzane**
To pary liczb pierwszych, z których jedna powstaje przez zapisanie cyfr dziesiętnych drugiej w odwrotnej kolejności. Przykłady:

- 13 i 31
- 17 i 71

**Liczby pierwsze palindromiczne**
To liczby pierwsze, które nie zmieniają się, gdy ich cyfry dziesiętne zapiszemy w odwrotnej kolejności. Przykłady: 11, 101, 131, 191, 929.

## Wzory na liczby pierwsze

Próbowano znaleźć proste wzory arytmetyczne, które dawałyby tylko liczby pierwsze, chociaż niekoniecznie wszystkie liczby pierwsze. Fermat wysunął słynne przypuszczenie, że wszystkie liczby postaci :

$$\mathbf{F(n) = 2^{2^n} + 1}$$

są liczbami pierwszymi. Rzeczywiści dla n=1,2,3,4 otrzymujemy :

- F(1)=5
- F(2)=17

- F(3)=257
- F(4)=65537

Wszystkie powyższe liczby są pierwsze. Ale w roku 1723 Euler odkrył, że F(5)=641*6700417 nie jest liczbą pierwszą.

Innym ciekawym wyrażeniem, które daje wiele liczb pierwszych jest

**$F(n) = n^2 - n + 41$**

Dla n=1,2,3,...,40 wyrażenie f(n) jest liczbą pierwszą. Natomiast dla n=41 mamy f(n)=412 i jest to liczba złożona.

Wyrażenie

**$F(n) = n^2 - 79n + 1601$**

daje liczby pierwsze przy wszelkich wartościach n aż do 79. Zawodzi jednak dla n=80

## Testy pierwszości

Aby sprawdzić, czy liczba naturalna **n** jest liczbą pierwszą, należy dzielić ją kolejno przez wszystkie liczby większe od 1 i mniejsze równe od **floor(n/2)**. Jeśli przy każdym dzieleniu reszta z dzielenia jest różna od zera, to liczba jest liczbą pierwszą. Natomiast jeżeli choć jedno dzielenie daje resztę równą zero, to sprawdzana liczba naturalna jest liczbą złożoną.

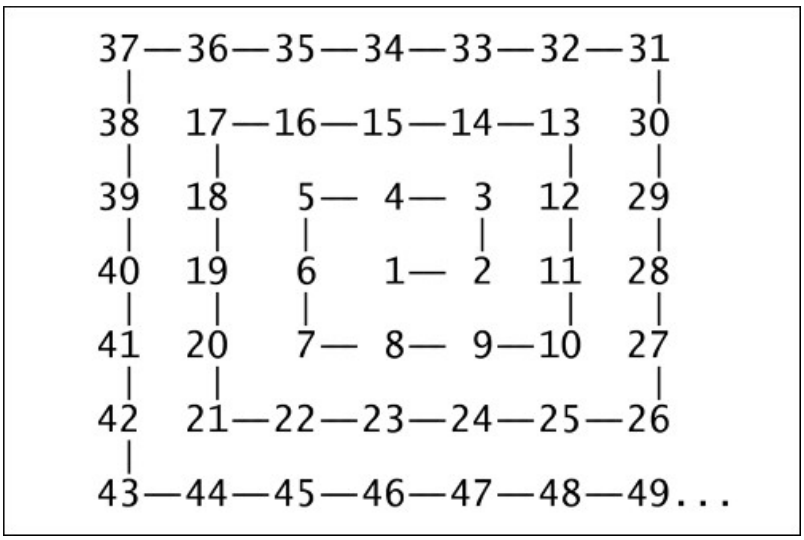
Oto przykład funkcji sprawdzającej czy dana liczba **n** jest liczbą pierwszą. Funkcja została napisana w języku **PHP**

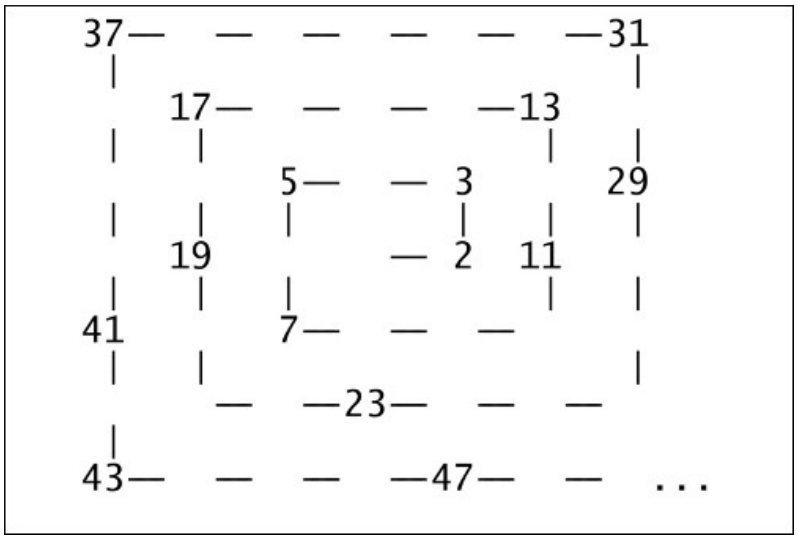
```
function is_prime($n)
{
$wynik=0;
$i=2;
$g=floor($n/2);
while (($wynik==0) & ($i<=$g))
{
if ($n%$i==0) ++$wynik;
++$i;
}
if ($wynik==0) return(0);
else return(1);
}
```

Jeżeli funkcja zwróci wartość 0 to liczba n jest liczbą pierwszą.

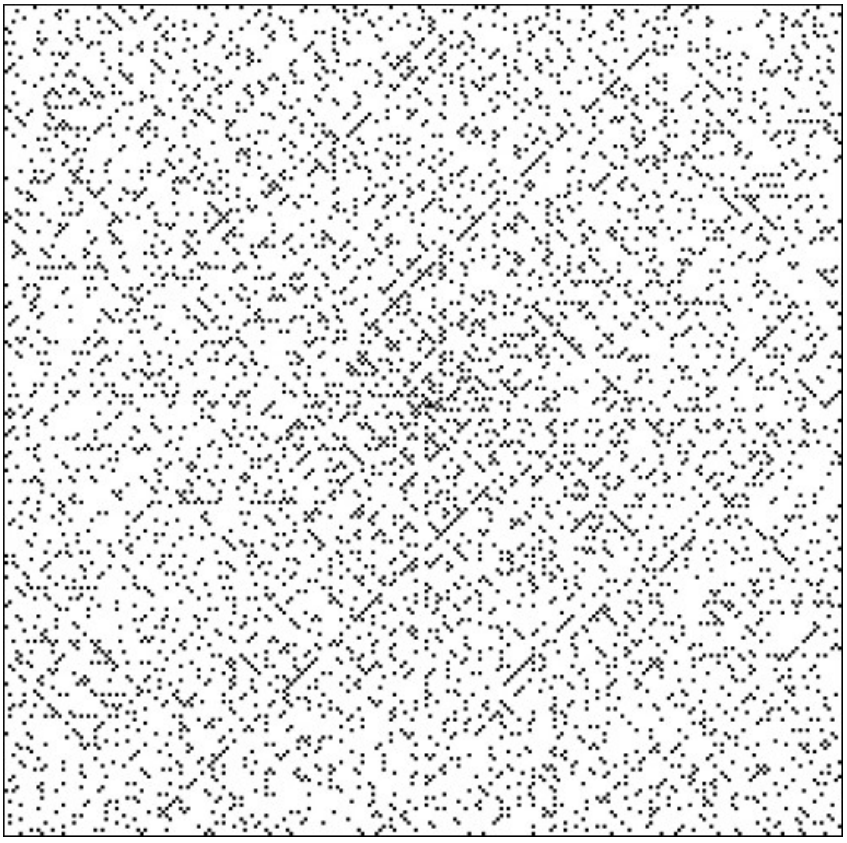
## Spirala Ulama

W matematyce spirala Ulama lub spirala liczb pierwszych to graficzna metoda pokazywania pewnych niewyjaśnionych do dziś różnic w rozkładzie liczb pierwszych, zaproponowana przez polskiego matematyka Stanisława Ulama w 1963 roku. Na kwadratowej tablicy zaczynając od 1 w środku spiralnie wypisuje się kolejne liczby naturalne. Na niektórych przekątnych liczby pierwsze częściej grupują się niż na innych. Fakt ten nie został do tej pory wyjaśniony.






Liczby pierwsze w układzie Spirali Ulama



Liczby pierwsze w Spirali Ulama w układzie 200x200

# Hipotezy

Czego nie wiadomo o liczbach pierwszych:

**Hipoteza 1**
Czy istnieje liczba pierwsza między $n^2$ a $(n+1)^2$ dla każdego $n>0$?

**Hipoteza 2**
Czy istnieje nieskończenie wiele liczb pierwszych postaci $n^2+1$ gdzie n jest liczbą całkowitą?

**Hipoteza 3**
Czy każda liczba parzysta jest sumą dwóch nieparzystych liczb pierwszych?

**Hipoteza 4**
Czy istnieje nieskończenie wiele par liczb pierwszych, takich jak 11,13 albo 17,19 różniących się o 2. Jest to problem **bliźniaczych** liczb pierwszych.

# Ciekawostki

**Ciekawostka 1**
W 1914 roku amerykański matematyk Derrick Norman Lehmer opublikował po raz pierwszy listę wszystkich 664579 liczb pierwszych mniejszych od 10 milionów. Stworzył on tę listę za pomocą sita Eratostenesa.

**Ciekawostka 2**
Liczba *11111111111111111111* złożona z 23 jedynek jest liczbą pierwszą.

**Ciekawostka 3**
Liczba *31415926535897932384626433832795028841* zestawiona z początkowych 38 cyfr rozwinięcia dziesiętnego liczby $\pi$ , jest liczbą pierwszą.

**Ciekawostka 4**
Liczba *73939133* nie tylko jest liczbą pierwszą, ale liczby otrzymane z niej przez kolejne obcinanie cyfr od prawej strony też są liczbami pierwszymi:

- 7393913 jest liczbą pierwszą
- 739391 jest liczbą pierwszą
- 73939 jest liczbą pierwszą

- 7393 jest liczbą pierwszą
- 739 jest liczbą pierwszą
- 73 jest liczbą pierwszą
- 7 jest liczbą pierwszą

## Największe liczby pierwsze

Największa odkryta dotąd liczba pierwsza to $\mathbf{2^{74207281}-1}$, która liczy sobie **22338618** cyfr w zapisie dziesiętnym. Została ona odkryta przez Curtisa Coopera 7 stycznia 2016 roku.

Oto lista innych wielkich liczb pierwszych :

| Liczba pierwsza | Liczba cyfr | Rok odkrycia |
|---|---|---|
| $2^{74207281}-1$ | 22338618 | 2016 |
| $2^{57885161}-1$ | 17425170 | 2013 |
| $2^{57885161}-1$ | 17425170 | 2013 |
| $2^{43112609}-1$ | 12978189 | 2008 |
| $2^{30402457}-1$ | 9152052 | 2005 |
| $2^{3021377}-1$ | 909526 | 1998 |
| $2^{2976221}-1$ | 895932 | 1997 |
| $2^{1398269}-1$ | 420921 | 1996 |
| $2^{1257787}-1$ | 378632 | 1996 |
| $2^{859433}-1$ | 258716 | 1994 |
| $2^{756839}-1$ | 227832 | 1992 |

| | | |
|---|---|---|
| $2^{216091}-1$ | 65050 | 1985 |
| $2^{132049}-1$ | 39751 | 1983 |
| $2^{110503}-1$ | 33265 | 1988 |
| $2^{86243}-1$ | 25962 | 1982 |

Największą liczbą pierwszą sprzed ery komputerów jest liczba, która nosi nazwę odkrywcy - **liczba Ferriera** i wynosi:

**20 988 936 657 440 586 486 151 264 256 610 222 593 863 921**

Jest to 44-cyfrowa liczba znaleziona za pomocą mechanicznego kalkulatora w 1951r.

## Kryptografia

Duże liczby pierwsze są często wykorzystywane w kryptografii ze względu na swe specyficzne właściwości. Dla przykładu opiszę kryptosystem RSA. Wykorzystujemy tutaj dwie pary kluczy : klucz publiczny i klucz prywatny.

**Algorytm RSA:**

- Najpierw generujemy klucz publiczny oraz klucz prywatny:
    - wybieramy losowo dwie liczby pierwsze p i q.
    - obliczamy iloczyn tych liczb n=pq
    - obliczamy wrtość funkcji Eulera dla n : $\varphi(n)=(p-1)(q-1)$
    - wybieramy liczbę e z przedziału [1,n] względnie pierwszą z $\varphi(n)$
    - znajdujemy liczbę d : $d=e^{-1} \bmod \varphi(n)$
    - klucz publiczny to para liczb (n,e)
    - klucz prywatny to para liczb (n,d)
- Szyfrowanie i deszyfrowanie

- Aby zaszyfrować wiadomość dzielimy ją na bloki mi o wartości nie większej niż n
- Teraz każdy z bloków szyfrujemy według wzoru : $c_i = m_i^e \bmod n$
- Natomiast aby odszyfrować wiadomość musimy każdy z bloków $c_i$ odszyfrować według wzoru : $m_i = c_i^d \bmod n$

## Algorytmy Probabilistyczne

Algorytmy probabilistyczne z bardzo dużym prawdopodobieństwem sprawdzają czy dana liczba jest liczbą pierwszą. Ale niestety istnieje niewielkie prawdopodobieństwo pomyłki.

**Algorytm:**

1. Wprowadź liczbę n
2. Wybierz losowo liczbę k z przedziału [1,n-1]
3. Sprawdź czy liczba k świadczy o złożoności liczby n
    1. Jeżeli tak to liczba n nie jest liczbą pierwszą
    2. Jeżeli nie to sprawdź czy sprawdzono już 200 różnych liczb k
        1. Jeżeli nie to wróć do punktu 2
        2. Jeżeli tak to n jest liczbą pierwszą.

W powyższym algorytmie prawdopodobieństwo pomyłki jest mniejsze niż **1/200**.

## Funkcja Eulera

Dla każdego n>=1 niech φ(n) będzie liczbą takich liczb całkowitych z przedziału 1<=a<=n, że NWD(a,n)=1. Wtedy funkcję φ nazywamy funkcją Eulera.

- **Własność 1**
  Nich p będzie liczbą pierwszą. Wtedy φ(p)=p-1
- **Własność 2**
  Niech m>=1 oraz n>=1 oraz NWD(m,n)=1. Wtedy φ(mn)=φ(m)φ(n).

- **Własność 3**
  Niech p będzie liczbą pierwszą. Wtedy $\varphi(p^k)=p^{k-1}(p-1)$
- **Małe twierdzenie Fermata**
  Jeżeli **p** jest liczbą pierwszą, nie będącą dzielnikiem liczby całkowitej **a** to:

$$a^{\varphi(p)} \equiv 1 \pmod{p}$$

Oto przykład algorytmu wyliczającego funkcję **Eulera** w języku PHP. Użyłem funkcji pomocniczej **nwd**, która oblicza największy wspólny dzielnik dla dwóch liczb naturalnych większych od 0.

```
function nwd($a,$b)
{
while($a*$b!=0)
{
if ($a>$b)
{
$a=$a%$b;
}
else
{
$b=$b%$a;
}
}
$wynik=$a+$b;
return($wynik);
}

function euler($n)
{
$wynik=0;
for ($i=1;$i<$n;++$i)
{
$sprawdz=nwd($i,$n);
if ($sprawdz==1) ++$wynik;
}
return($wynik);
}
```

W poniższej tabeli podałem wartości funkcji Eulera dla kolenych potęg liczby 10.

| n | φ(n) |
|---|---|
| 10 | 4 |
| 100 | 40 |
| 1000 | 400 |
| 1000 | 400 |
| 10000 | 4000 |
| 100000 | 40000 |

Wartość funkcji Eulera dla kolejnych potęg liczby 10

## Książki o liczbach pierwszych


- Paulo Ribenboim, Mała księga wielkich liczb pierwszych, Wydawnictwo Naukowo-Techniczne, Warszawa 1997.
- Andrzej Szepietowski, Matematyka Dyskretna, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2000.
- Wacław Marzantowicz, Piotr Zarzycki, Elementy Teorii Liczb, Wydawnictwo Naukowe UAM
- Piotr Zarzycki, Elementarna teoria liczb, PWN, Warszawa 2006.
- R. Courant, H. Robbins, Co to jest Matematyka, Państwowe Wydawnictwo Naukowe, Warszawa 1959
- Wacław Sierpiński, Arytmetyka Teoretyczna, Państwowe Wydawnictwo Naukowe, Warszawa 1968
- Philip J. Davis, Reuben Hersh, Świat Matematyki, Wydawnictwo Naukowe PWN, Warszawa 1994
- I.N. Bronsztejn, K.A. Siemiendiajew, G. Musiol, H. Muhlig, Nowoczesne Kompendium Matematyki, Wydawnictwo Naukowe PWN, Warszawa 2007

- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Wprowadzenie do algorytmów, Wydawnictwa Naukowo-Techniczne, Warszawa 1998
- Marcin Karbowski, Podstawy Kryptografii, Wydawnictwa Helion, Gliwice 2014
- David Harel, Yishai Feldman, Rzecz o istocie informatyki - Algorytmika, Wydawnictwa Naukowo-Techniczne, Warszawa 2008
- Jacek Wojdanowski, Kod liczb pierwszych, Wydawnictwo Poligraf, Brzezia Łąka 2016
- Lubina Jan, Zagadka wszechczasów - rozwiązana , Wydawnictwo Poligraf, Brzezia Łąka 2017
- Michał Zalewski, Cisza w sieci, Wydawnictwo Helion 2005