Liczby Pierwsze

Marek Wójcik i Kamil Gawor

Krótki Kurs Historii Matematyki, semestr 2024Z

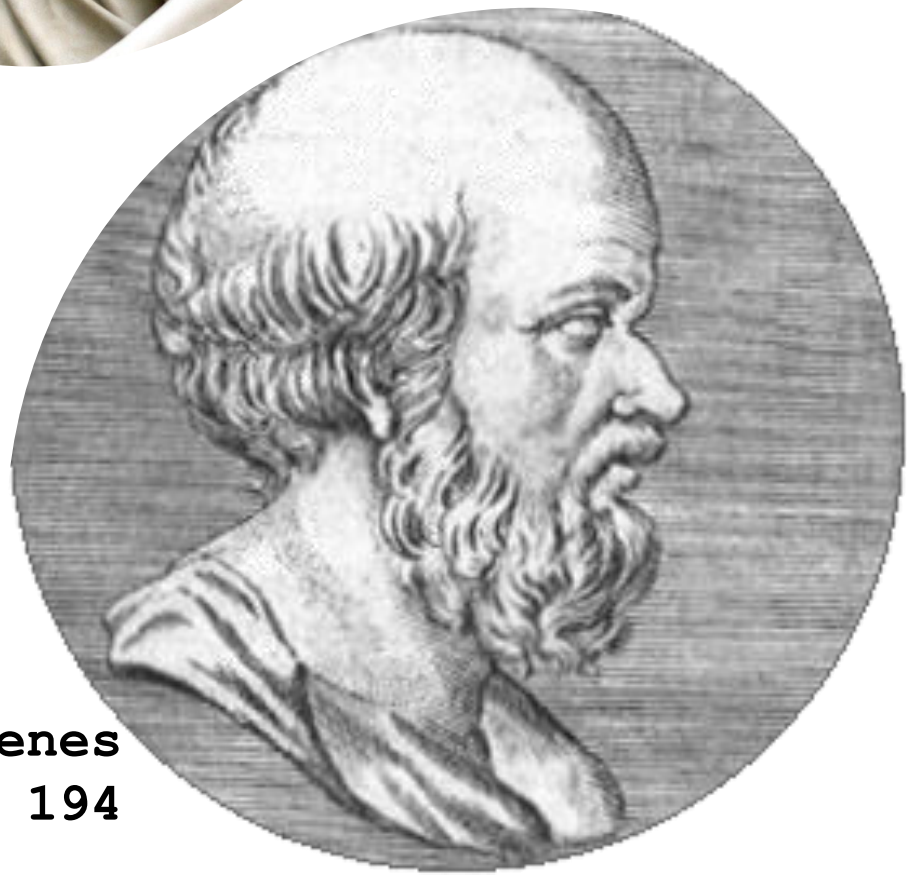
Wydział MiNI, Politechnika Warszawska

Odkrycie liczb pierwszych

Euklides
~365 - ~270

W "Elementach" Euklidesa pojawiły się takie zagadnienia, jak:

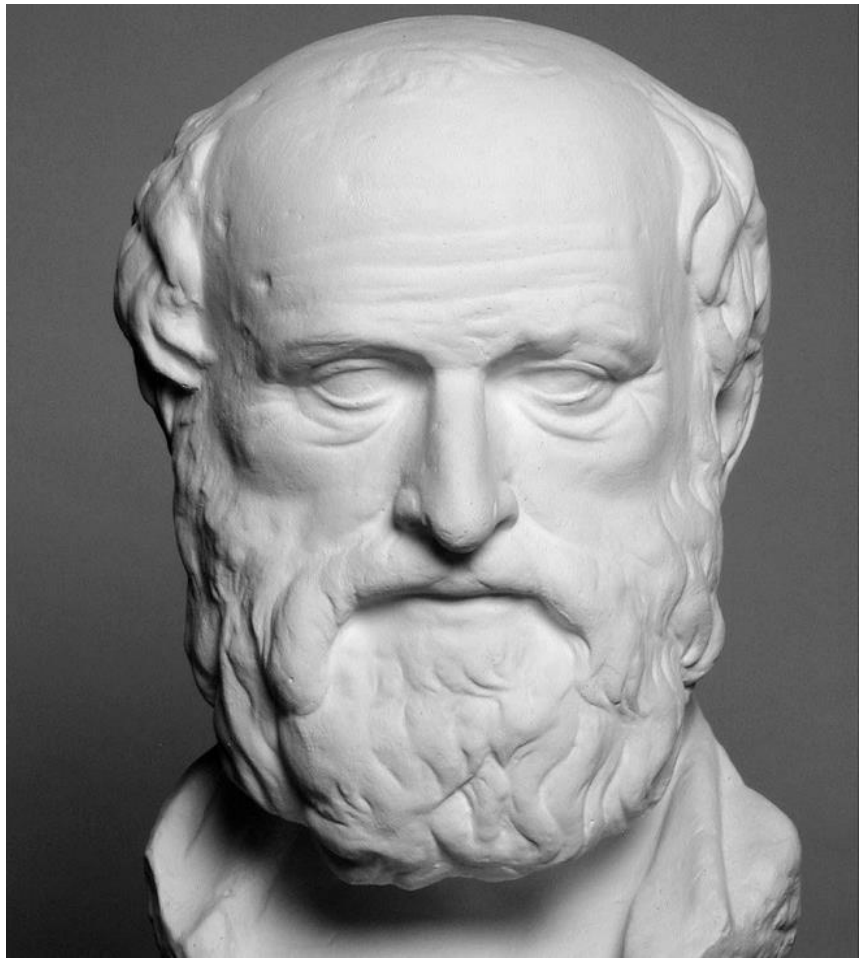
- Definicja l. pierwszej
- Dowód nieskończoności zbioru liczb pierwszych
- Podstawowe twierdzenie arytmetyki
- Algorytm Euklidesa



Eratostenes
276 - 194

Później Eratostenes stworzył prosty algorytm znajdowania l. pierwszych, zwany Sitem

Sito Eratosten



Eratostenes
276 - 194

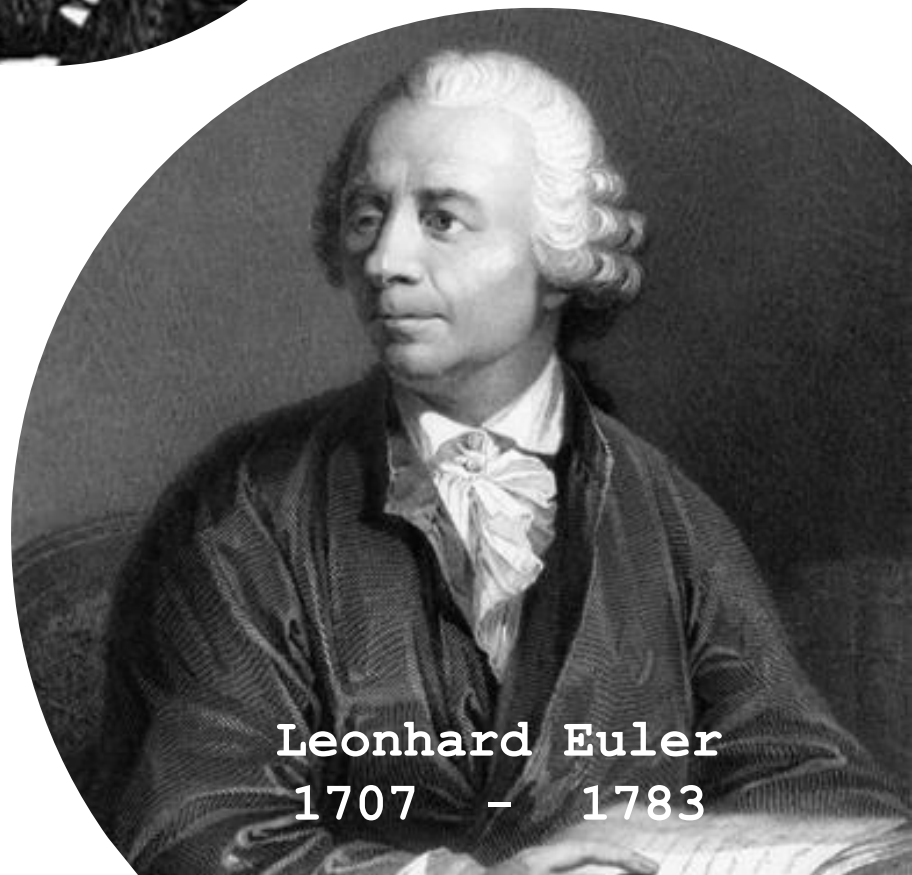
	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

Dlaczego 1 nie jest liczbą pierwszą?

- Sito Eratostenesa
- Podstawowe twierdzenie arytmetyki
- Funkcja Eulera (tocjent)

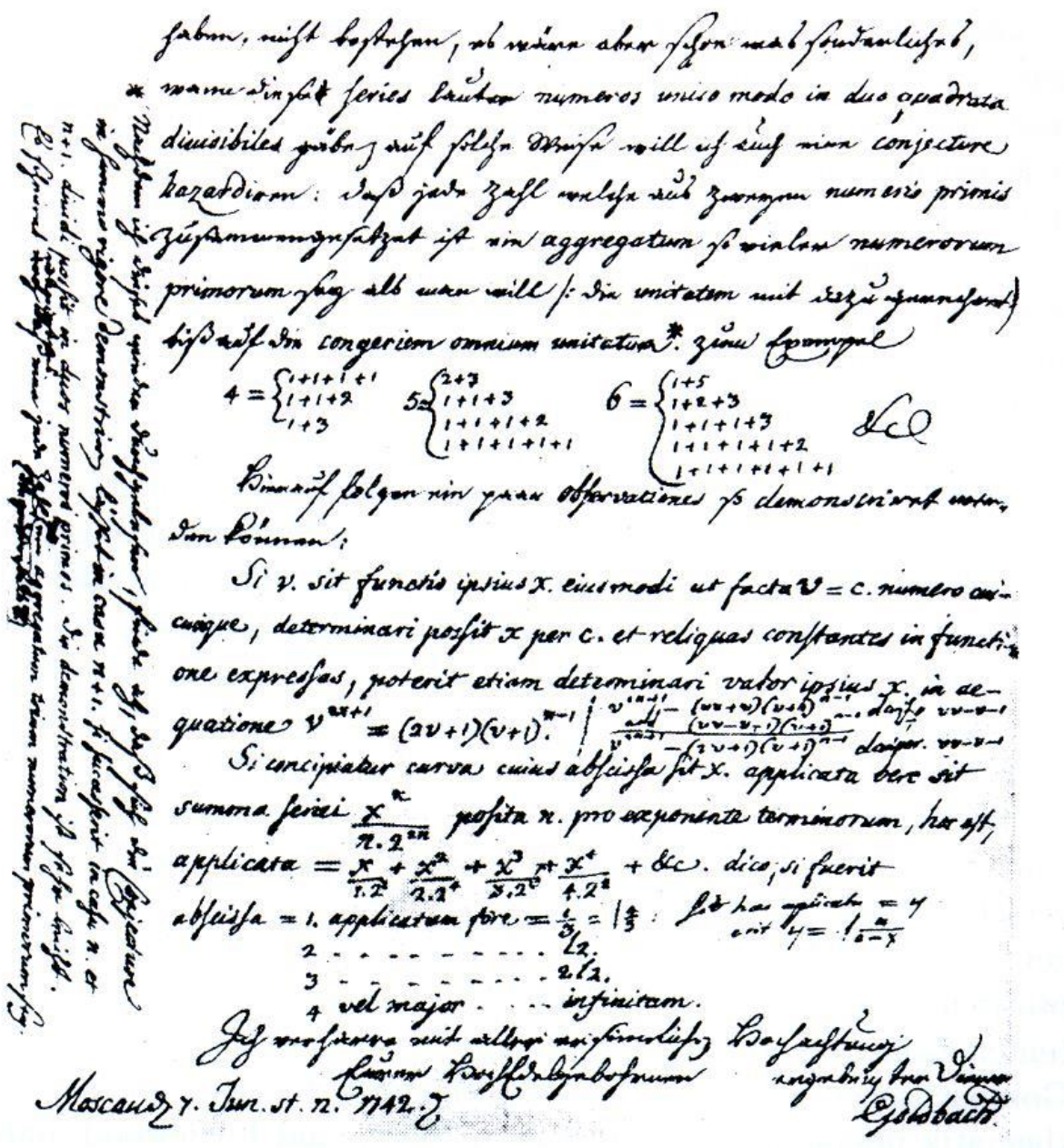
Christian Goldbach
1690 - 1764

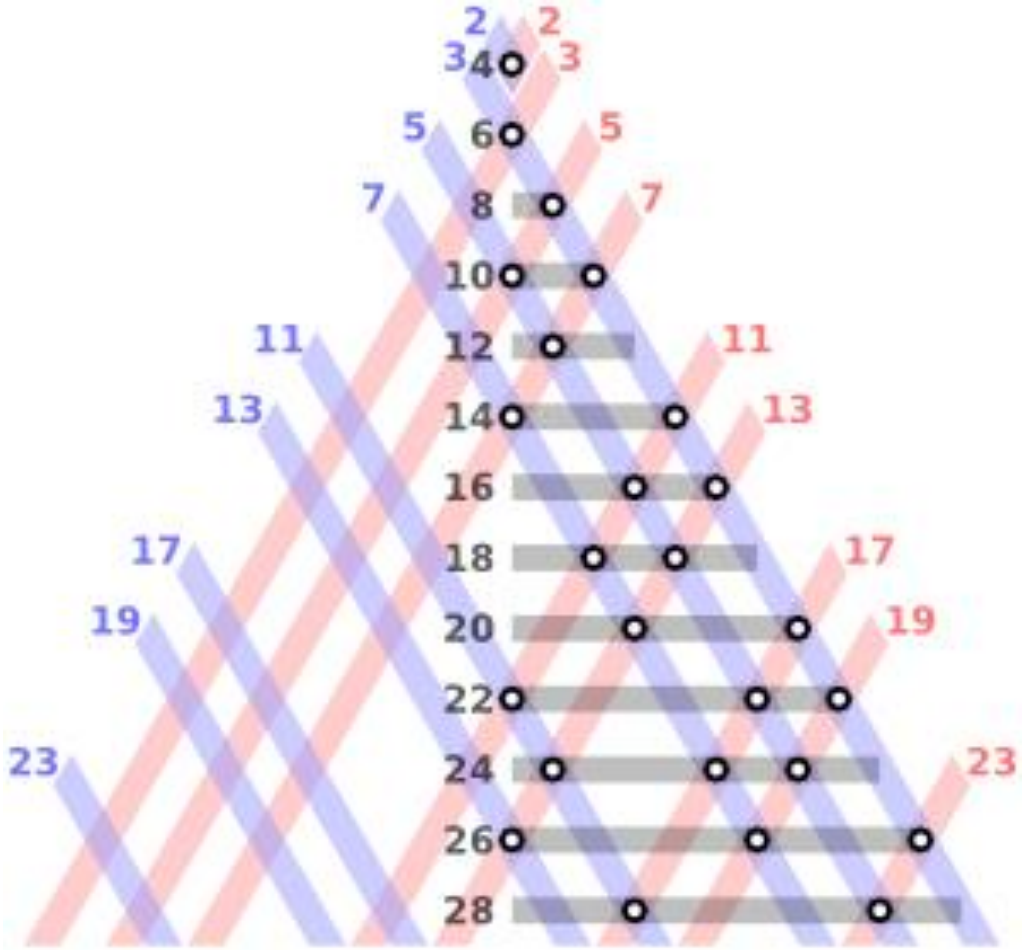


Leonhard Euler
1707 - 1783

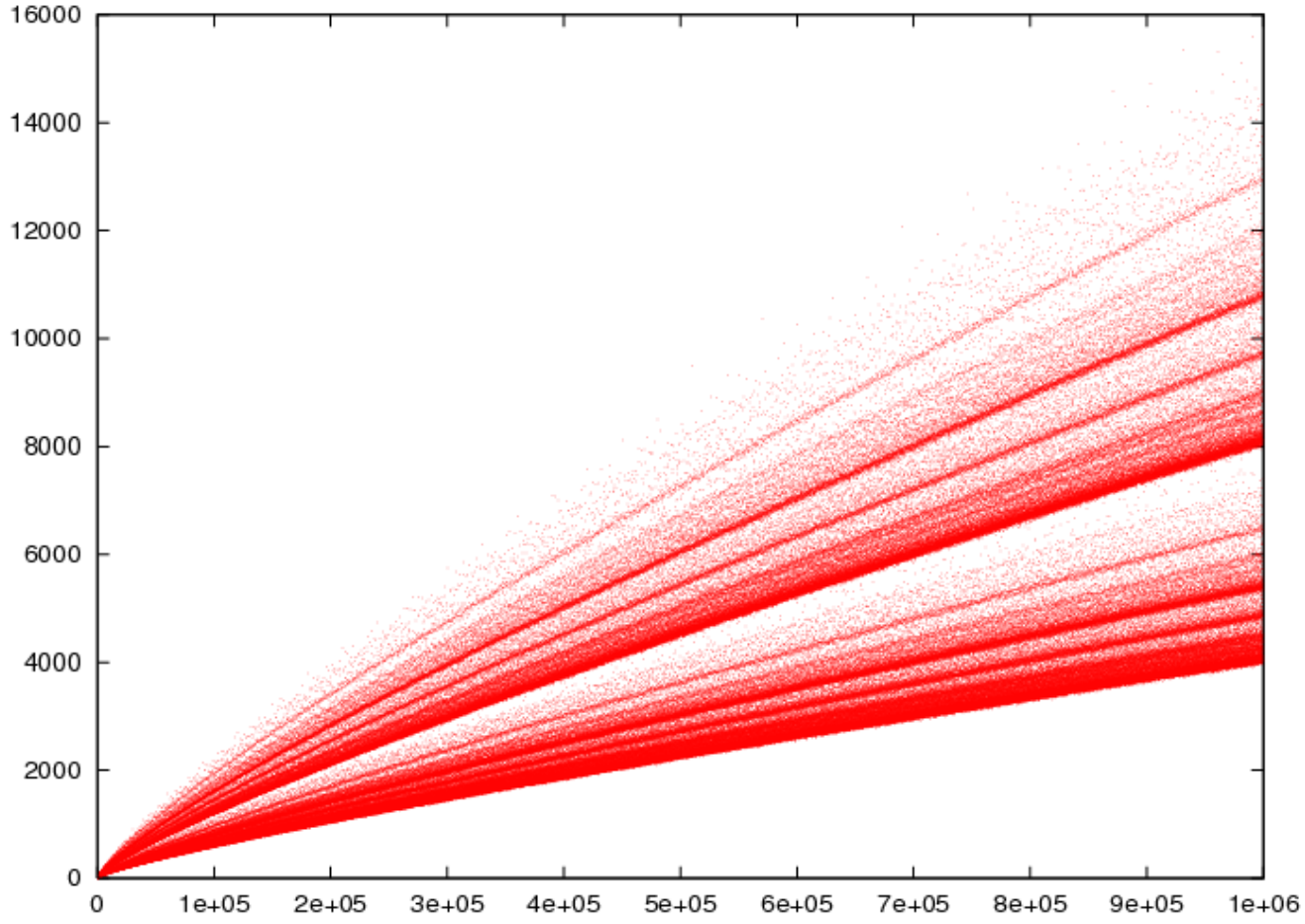
Hipoteza Goldbacha

Czy dowolną parzystą liczbę naturalną można przedstawić za pomocą sumy dwóch liczb pierwszych?



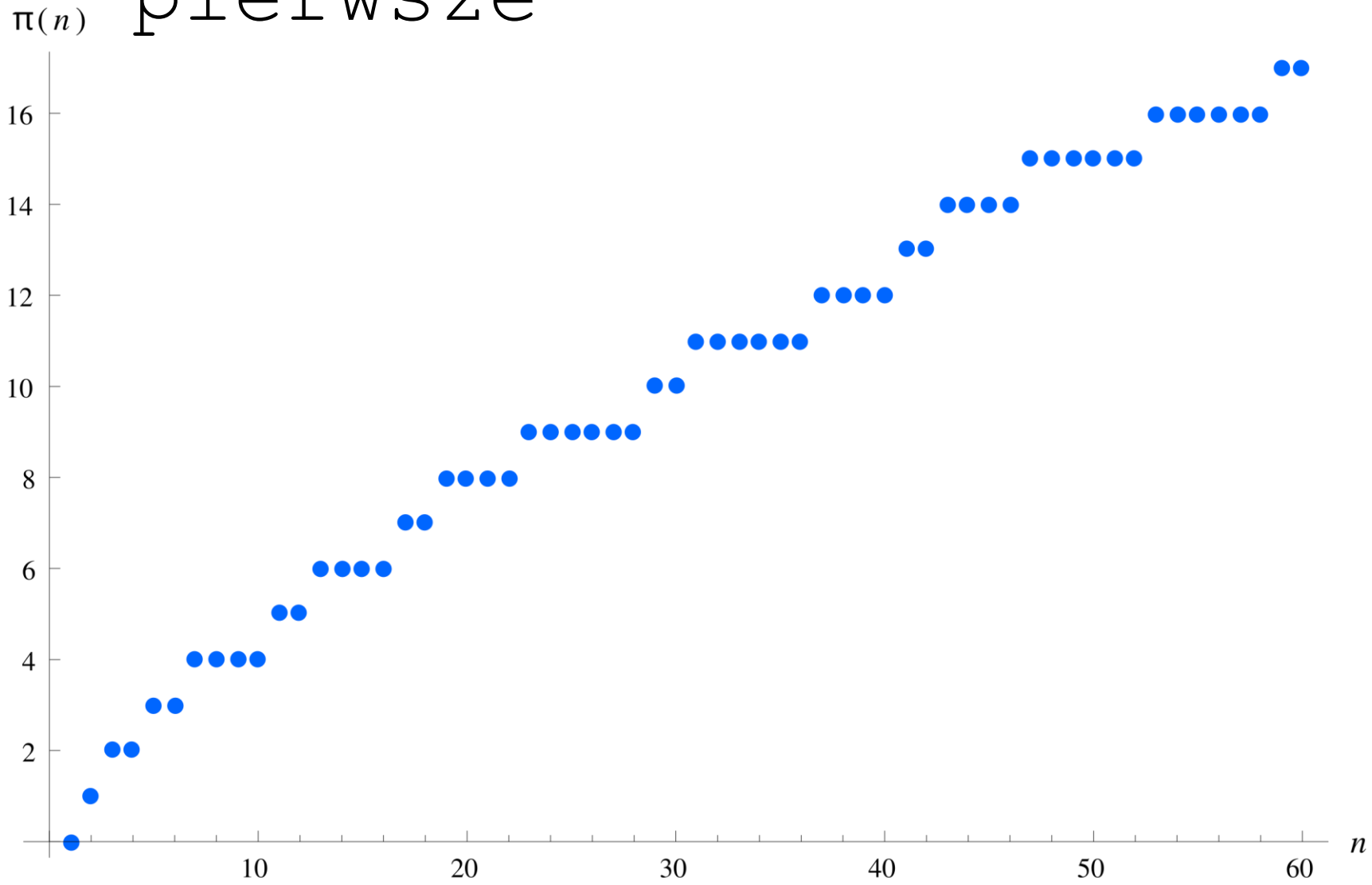


Na powyższym diagramie kropki symbolizują przedstawienie liczby



Na tyle sposobów można przedstawić liczbę za pomocą sumy dwóch liczb pierwszych

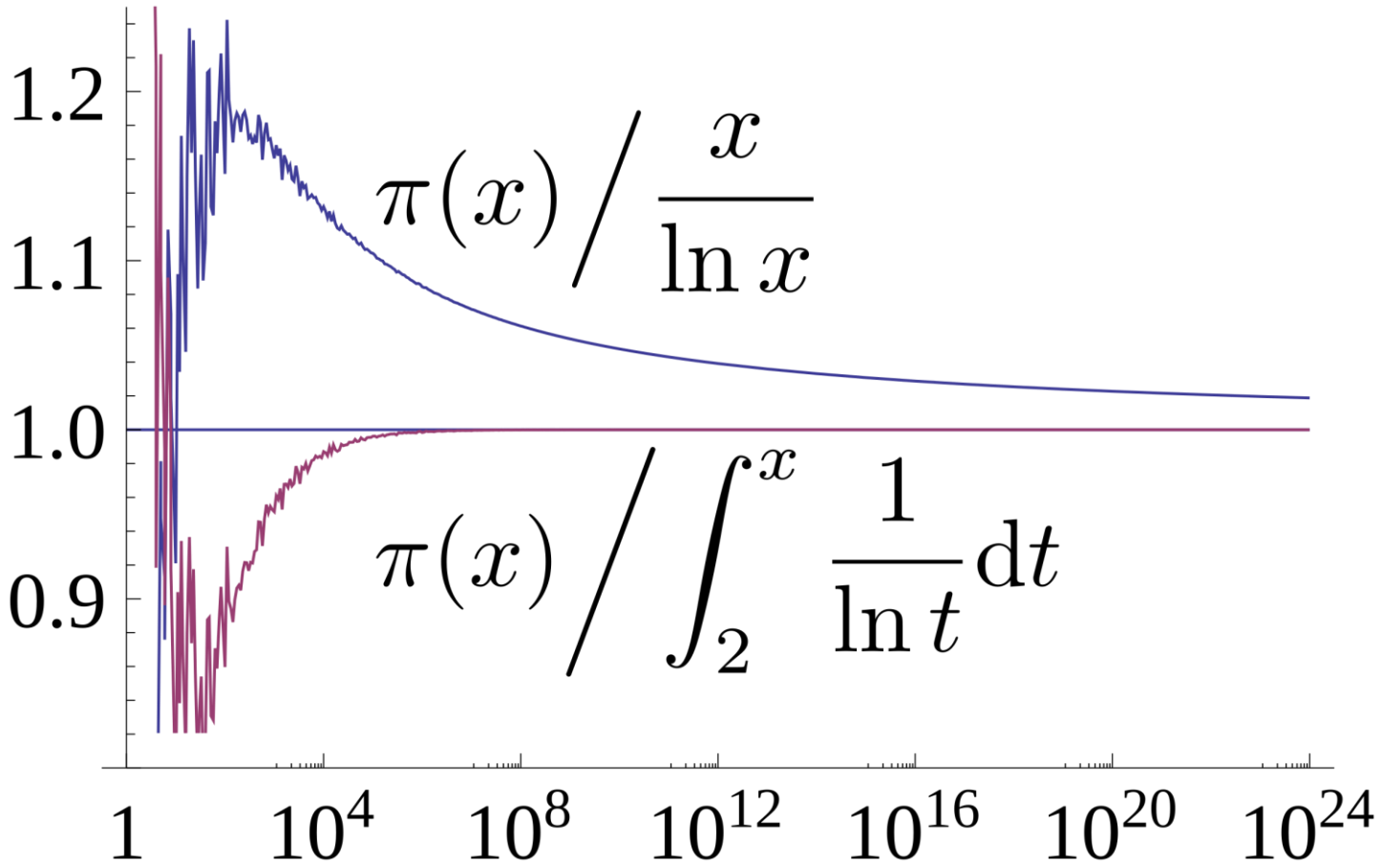
Funkcja licząca liczby pierwsze



Twierdzenie o liczbach pierwszych

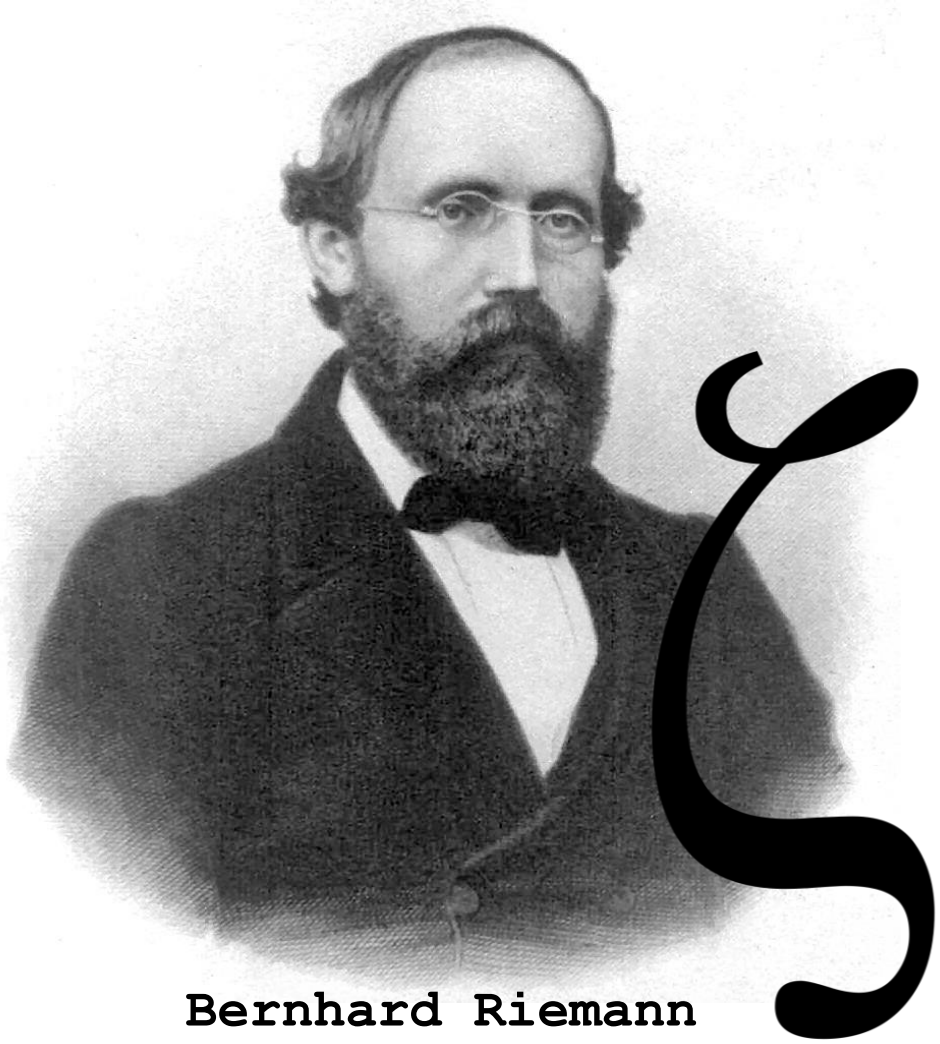
- Udowodnione niezależnie przez Jackquesa Hadamarda oraz Charlesa Poussina w 1896 r.

$$\pi(x) \sim \frac{x}{\log x}$$



O liczbie liczb pierwszych mniejszych od zadanej wielkości

- "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse"
- 9 stronnicowy artykuł autorstwa Bernharda Riemanna wydany w listopadzie 1859 r.
- rozszerzył definicję funkcji dzeta Eulera na liczby zespolone
- dowód meromorficzność funkcji
- **zależność między rozmieszczeniem jej miejsc zerowych a liczbą liczb pierwszych**
- **sformułowanie hipotezy Riemanna**



Bernhard Riemann
1826-1866

VII.

Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.

(Monatsberichte der Berliner Akademie, November 1859.)

Meinen Dank für die Auszeichnung, welche mir die Akademie durch die Aufnahme unter ihre Correspondenten hat zu Theil werden lassen, glaube ich am besten dadurch zu erkennen zu geben, dass ich von der hierdurch erhaltenen Erlaubniss baldigst Gebrauch mache durch Mittheilung einer Untersuchung über die Häufigkeit der Primzahlen; ein Gegenstand, welcher durch das Interesse, welches Gauss und Dirichlet demselben längere Zeit geschenkt haben, einer solchen Mittheilung vielleicht nicht ganz unwerth erscheint.

Bei dieser Untersuchung diente mir als Ausgangspunkt die von Euler gemachte Bemerkung, dass das Product

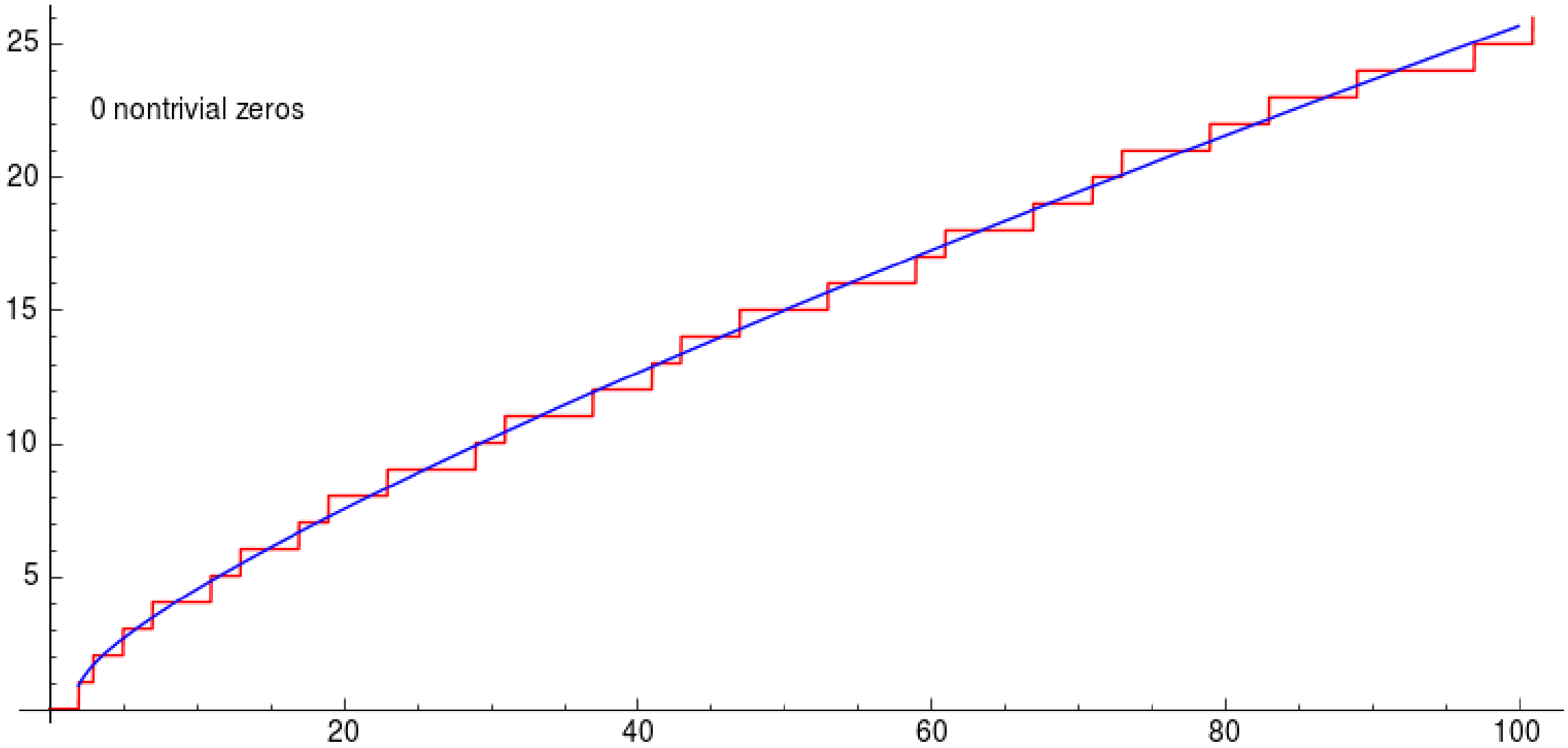
$$\Pi \frac{1}{1-\frac{1}{p^s}} = \Sigma \frac{1}{n^s},$$

wenn für p alle Primzahlen, für n alle ganzen Zahlen gesetzt werden. Die Function der complexen Veränderlichen s, welche durch diese beiden Ausdrücke, so lange sie convergiren, dargestellt wird, bezeichne ich durch $\zeta(s)$. Beide convergiren nur, so lange der reelle Theil von s grösser als 1 ist; es lässt sich indess leicht ein immer gültig bleibender Ausdruck der Function finden. Durch Anwendung der Gleichung

$$\int_0^\infty e^{-nx} x^{s-1}\, dx = \frac{\Pi(s-1)}{n^s}$$

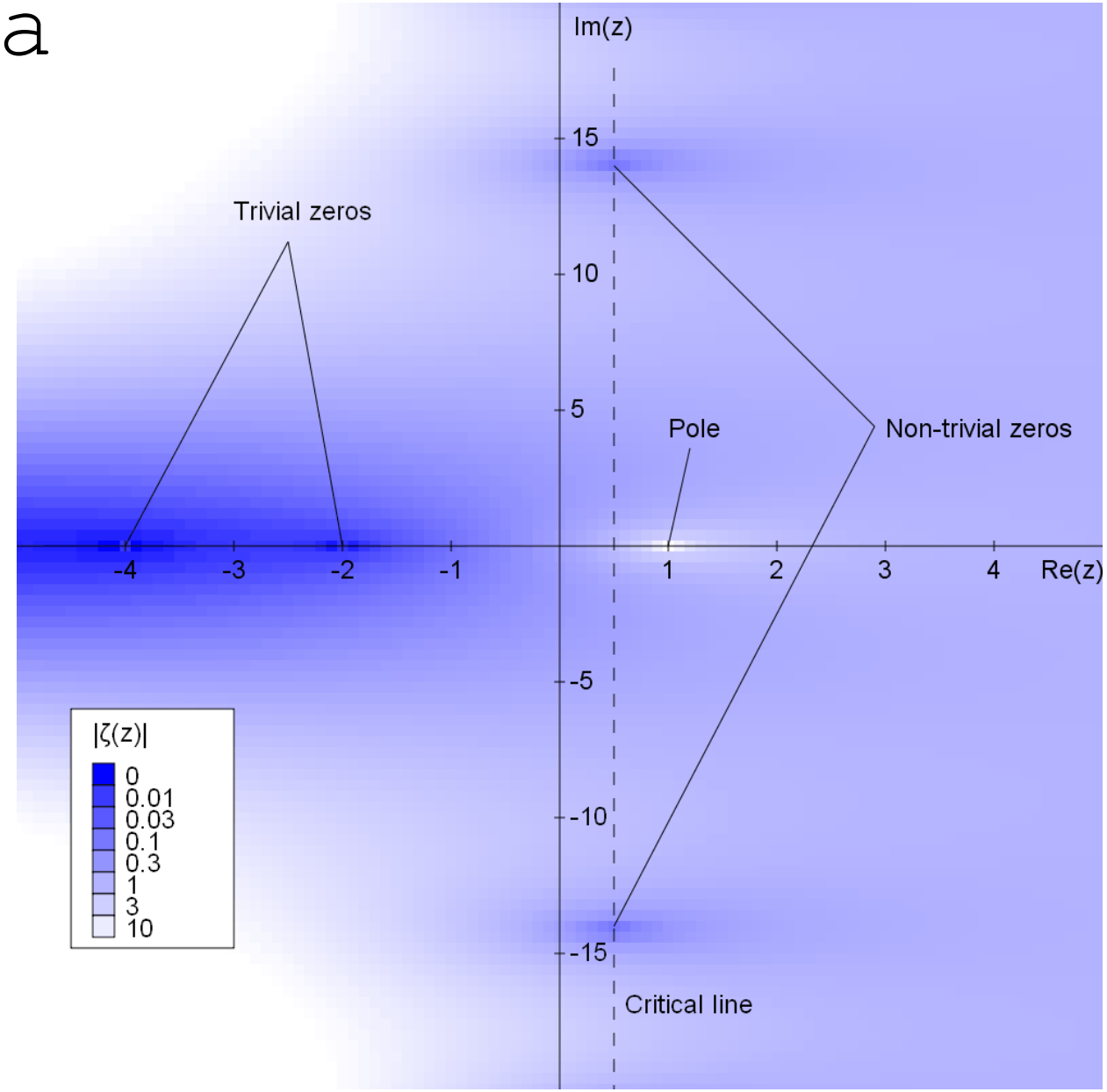
erhält man zunächst

$$\Pi(s-1)\, \zeta(s) = \int_0^\infty \frac{x^{s-1}\, dx}{e^x - 1}.$$


0 nontrivial zeros
25
20
15
10
5
20
40
60
80
100

Hipoteza Riemanna

Wszystkie nietrywialne zera funkcji dzeta leżą na prostej Re(z)=1/2



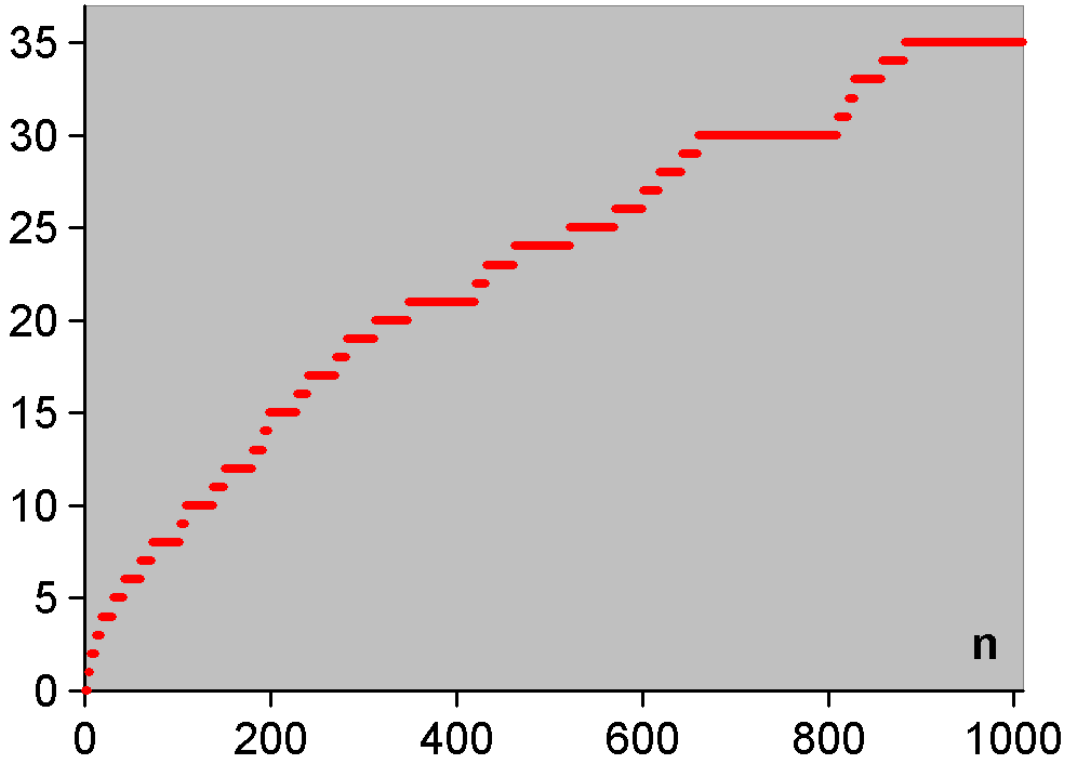
Jeśli hipoteza Riemanna zachodzi...

$$\pi(x) - \operatorname{li}(x) = O\left(x^{\beta} \log x\right)$$

$$|\pi(x) - \operatorname{li}(x)| < \frac{1}{8\pi}\sqrt{x}\log(x) \qquad x \geq 2657$$

Liczby bliźniacze

- Para liczb pierwszych, których różnica wynosi 2
- Liczba 5 jest bliźniacza z 3 oraz 7
- $2996863034895 \cdot 2^{1290000} \pm 1$ (388,342 znaków)



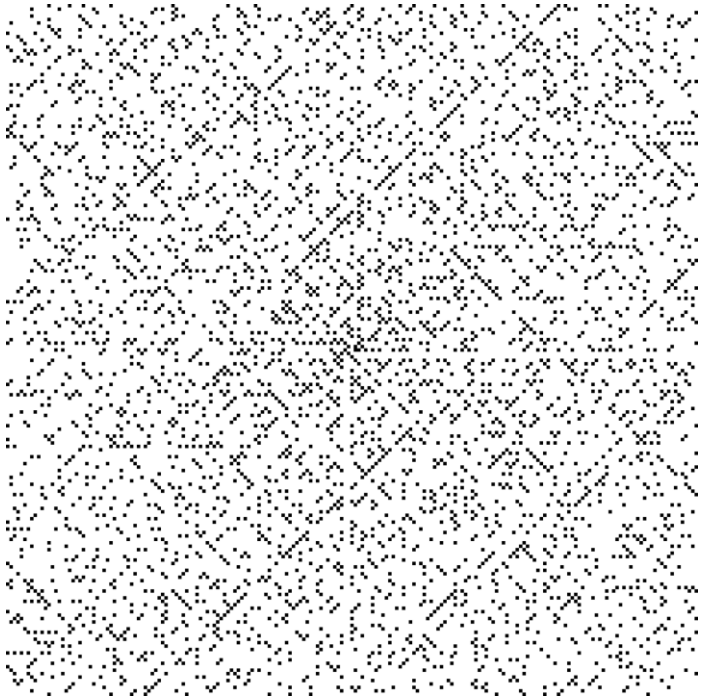
Hipoteza o liczbach pierwszych bliźniaczych

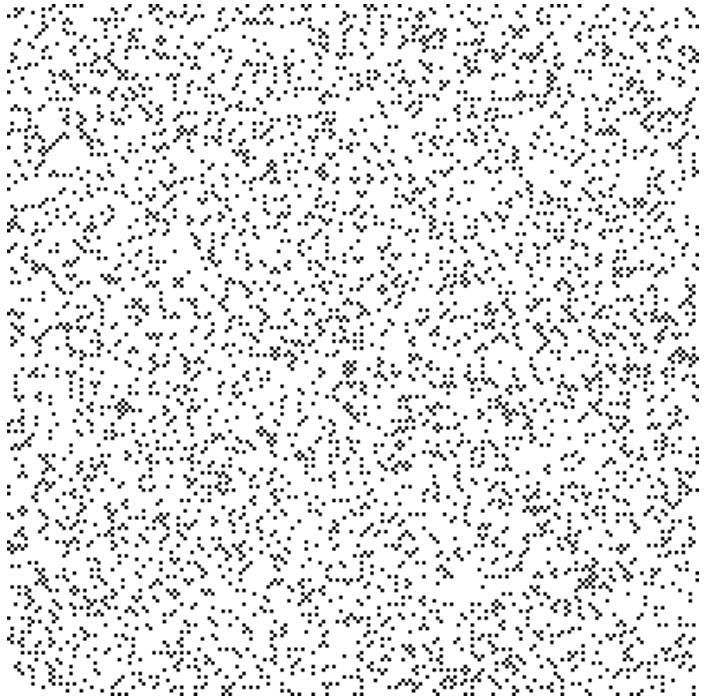
- Czy istnieje nieskończenie wiele liczb pierwszych bliźniaczych?
- W 1919 r. Viggo Brun wykazał, że szereg odwrotności liczb pierwszych bliźniaczych jest zbieżny
- Stała Bruna $B_2 \approx 1.902160583104$

1882 -

Spirala Ulama

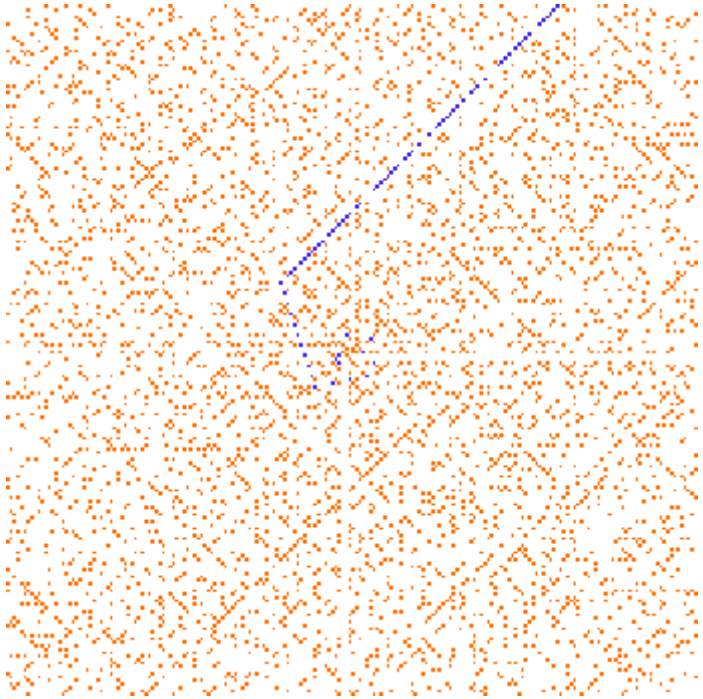
- Stanisław Ulam – polski matematyk, przedstawiciel Lwowskiej Szkoły Matematyki

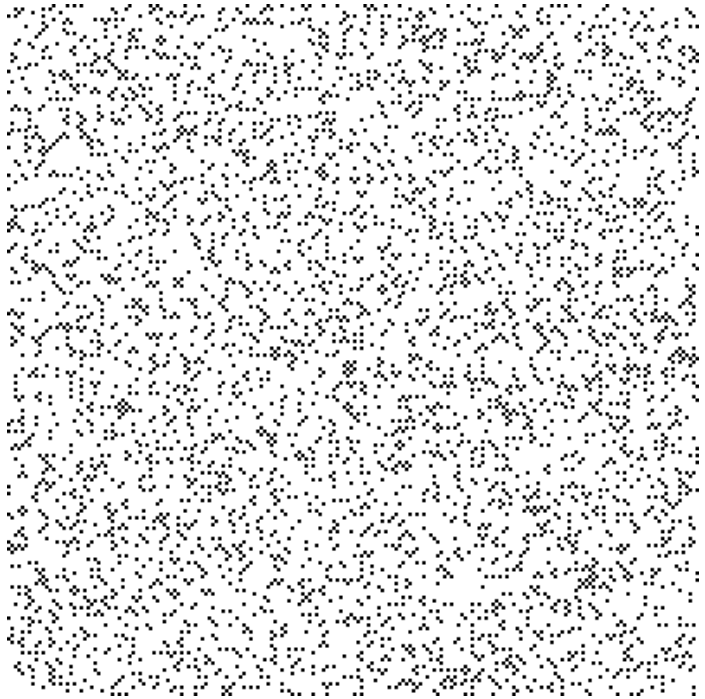


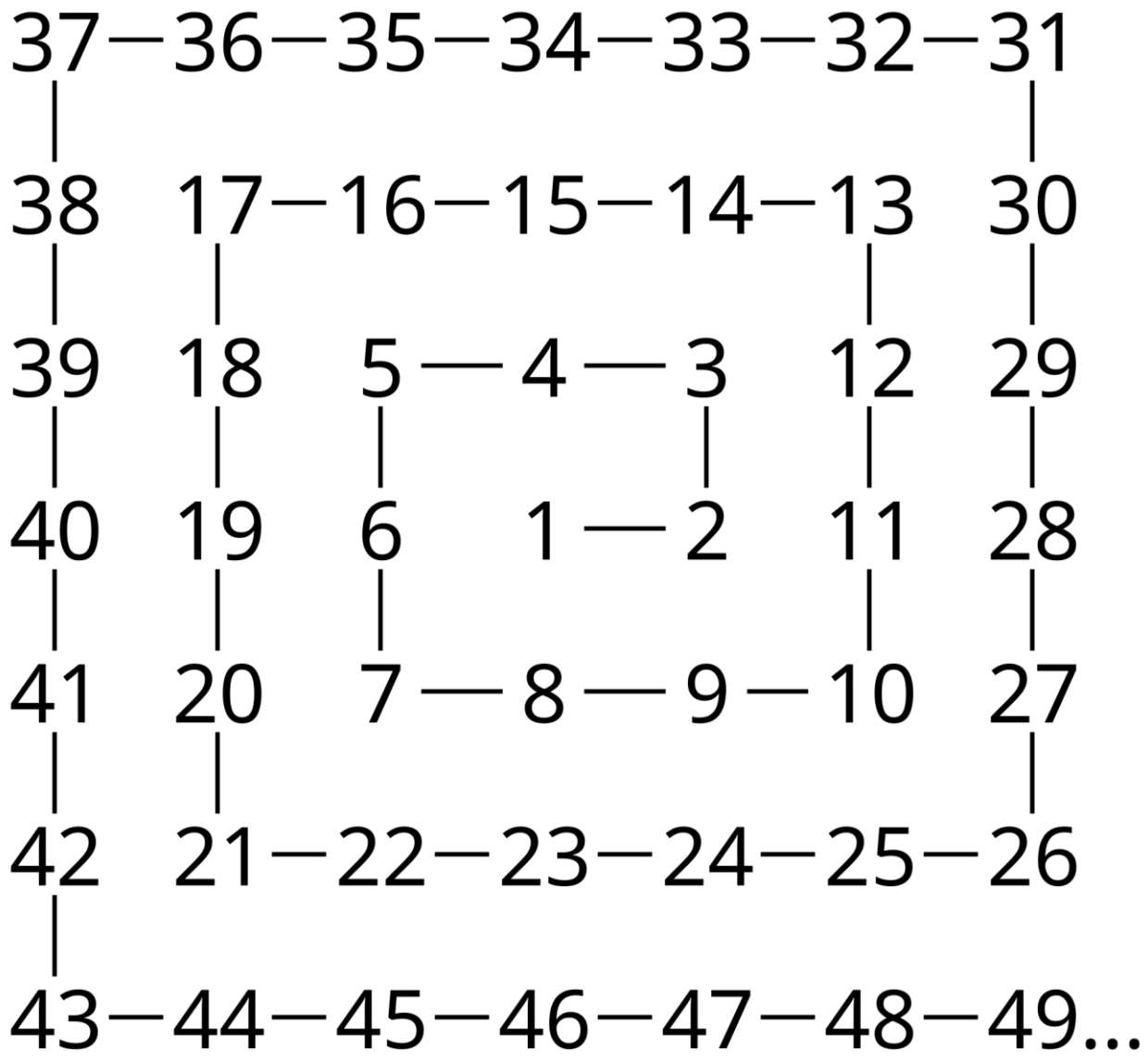


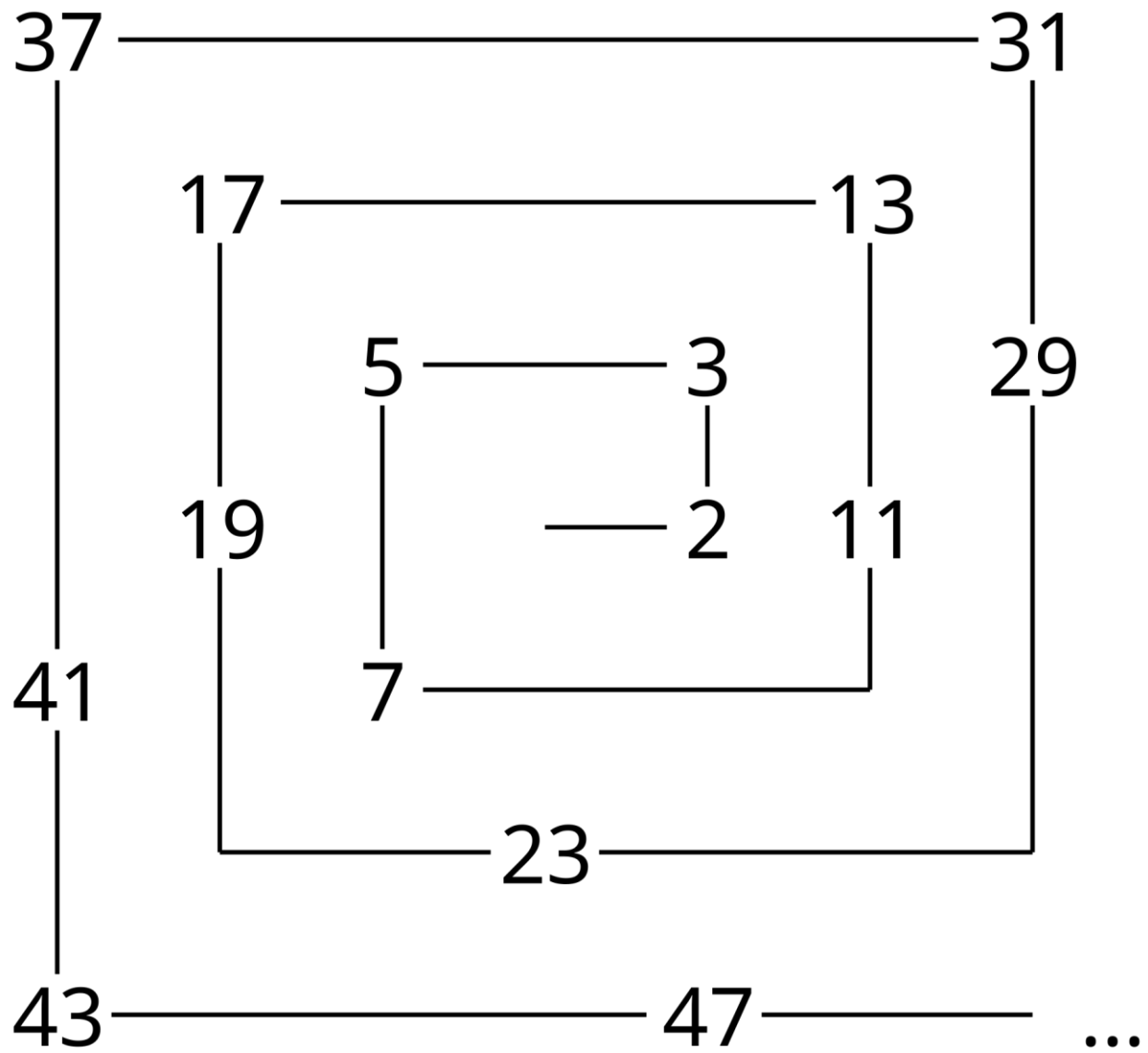
Spirala Ulama

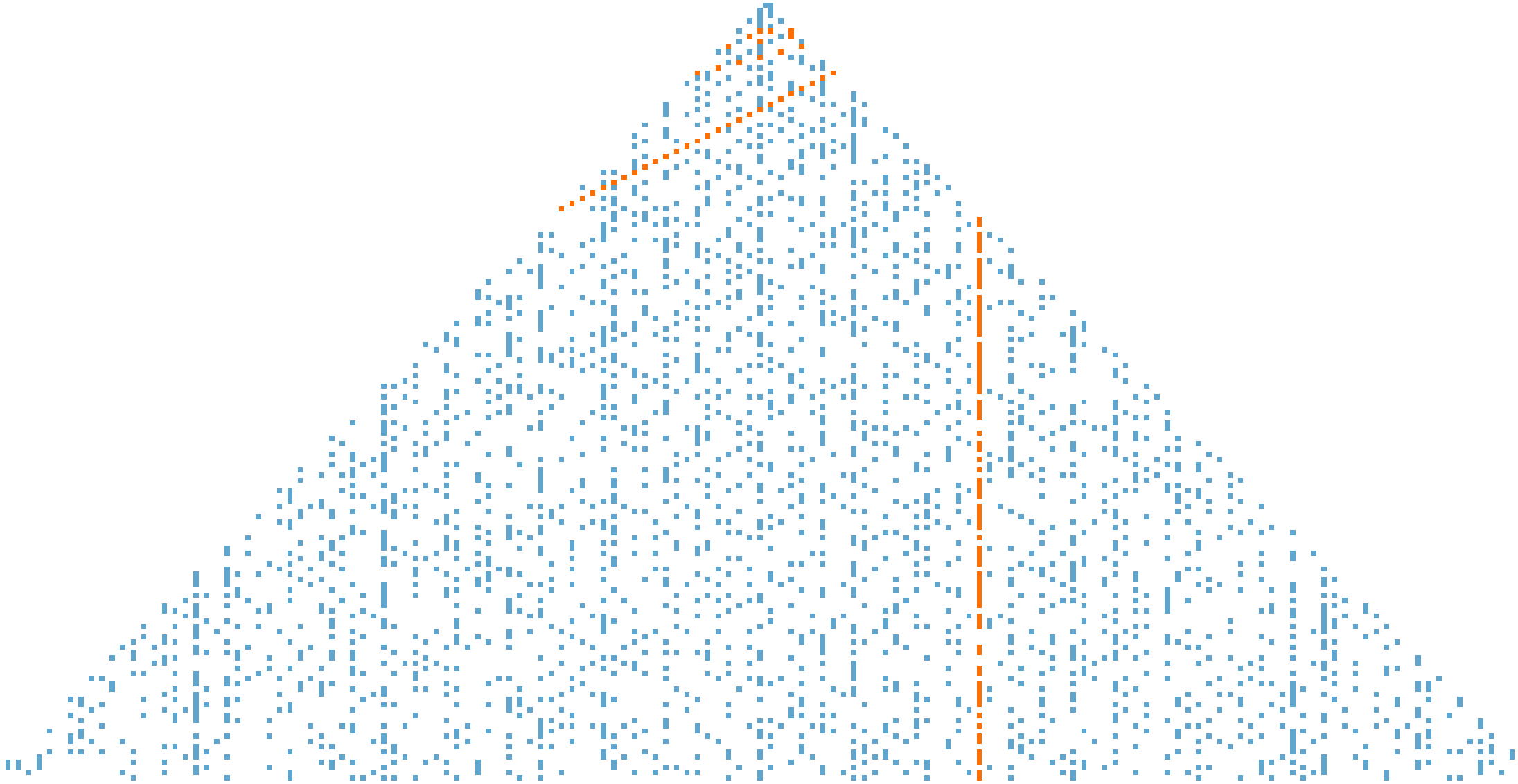
- Stanisław Ulam – polski matematyk, przedstawiciel Lwowskiej Szkoły Matematyki

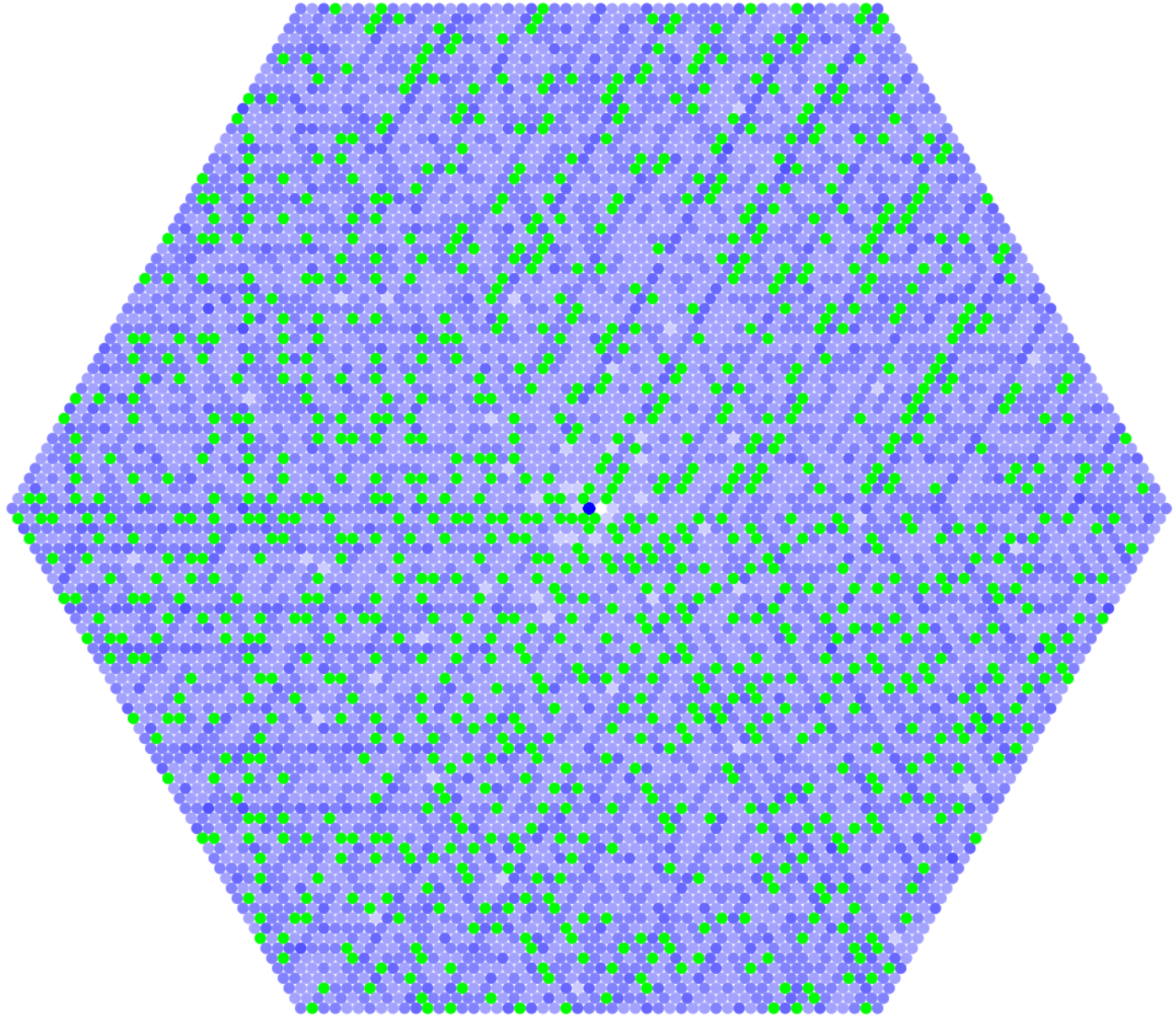





37 36 35 34 33 32 31
38 17 16 15 14 13 30
39 18 5 4 3 12 29
40 19 6 1 2 11 28
41 20 7 8 9 10 27
42 21 22 23 24 25 26
43 44 45 46 47 48 49...


37
31
17
13
5
3
29
19
2
11
41
7
23
43
47
...





Liczby Mersenne'a

$$M_p=2^p-1$$

Znane są 52 l. pierwsze Mersenne'a

Największa z nich jest największą znaną dotychczas liczbą pierwszą:

1588 - 1648

Great Internet Mersenne Prime Search
GIMPS
Finding World Record Primes Since 1996

Username Password Log In Register Forgot password?

Home | Get Started | Current Progress | Create Account | Reports | Manual Testing | More Information / Help | Donate — Make a donation

Welcome to GIMPS
the Great Internet Mersenne Prime Search

Join GIMPS | Downloads | Known Primes | Progress Overview | Milestones | History

What is GIMPS?

GIMPS is a collaborative project of volunteers who search for Mersenne prime numbers.

Find out how it works, create an account, download software, start searching!

Ask questions on the Mersenne Forum.

All exponents below 71 184 691 have been tested and verified.
All exponents below 128 455 189 have been tested at least once.

Previous Day Stats		Today's Numbers	
Newly Factored	88	GFLOP/s	49 027 743
First Prime Tests	186	GHz-Days	24 513 872
Verified Prime Tests	454	CPUs & GPUs	2 872 048

$2^{136279841}-1$ is the New Largest Known Prime Number

October 21, 2024 — The Great Internet Mersenne Prime Search (GIMPS) has discovered a new Mersenne prime number, $2^{136279841}-1$. At 41,024,320 digits, it eclipses by more than 16 million digits the previous largest known prime number found by GIMPS nearly 6 years ago.

Luke Durant, GIMPS most prolific contributor using free GIMPS software, proved the number prime on October 12. After notifying the GIMPS server, GIMPS began a rigorous process of independently confirming the prime number on several different hardware platforms using several different programs. This process concluded on October 19th.

This prime ends the 28 year reign of ordinary PCs finding the largest known prime. In 2017, Mihai Preda authored Mersenne prime search software that runs on GPUs. GPUs were primarily used in PCs as video cards or for mining cryptocurrency. Nowadays, video cards are also used to power the AI revolution. Durant's idea was to use these powerful GPUs that are now available in the cloud and heavily discounted when they are being under-utilized. Luke organized these cloud GPUs creating a kind of "cloud supercomputer" spanning 17 countries. After nearly a year of testing, Luke finally struck paydirt. On October 11, an NVIDIA A100 GPU in Dublin, Ireland, reported that M136279841 is probably prime. On October 12, an NVIDIA H100 in San Antonio, Texas, USA, confirmed primality with a Lucas-Lehmer test.

Luke, a 36 year-old researcher from San Jose, CA, and former NVIDIA employee, is one of thousands of GIMPS volunteers contributing spare CPU and GPU time in hopes of making a little bit of history. Mihai Preda, and later George Woltman, wrote the GPU software. Aaron Blosser keeps the GIMPS server running smoothly. This discovery is also made possible by the combined effort of each and every GIMPS volunteer testing Mersenne numbers that did not turn out to be prime. In recognition of all the above, official credit for this discovery goes to "L. Durant, M. Preda, G. Woltman, A. Blosser, et al."

The new prime is only the 52nd known Mersenne prime ever discovered. Mersenne primes were named for the French monk Marin Mersenne, who studied these numbers more than 350 years ago. GIMPS, founded by George Woltman in 1996, has discovered the last 18 Mersenne primes. Volunteers download a free program to search for these primes, with a $3000 award offered to anyone lucky enough to find a new prime. Prof. Chris Caldwell maintained an authoritative web site on the largest known primes, and wrote an excellent history of Mersenne primes.

Prime95

Test Edit Advanced Options Window Help

Communication thread - Inactive

```
[Main thread Jan 13 00:32] Mersenne number primality test program version 30.19 build 20
[Main thread Jan 13 00:32] Optimizing for CPU architecture: AMD Zen, L2 cache size: 6x512 KB, L3 cache size: 2x16 MB
[Main thread Jan 13 00:34] Starting worker.
[Comm thread Jan 13 00:34] Updating computer information on the server
[Comm thread Jan 13 00:34] Exchanging program options with server
[Comm thread Jan 13 00:34] Getting assignment from server
[Comm thread Jan 13 00:34] PrimeNet success code with additional info:
[Comm thread Jan 13 00:34] Server assigned PRP work.
[Comm thread Jan 13 00:34] Got assignment 0FCF2E9778CF01B92F6CB407238B3C63: PRP M139743557
[Comm thread Jan 13 00:34] Sending expected completion date for M139743557: Jan 26 2025
[Comm thread Jan 13 00:34] Done communicating with server.
```

Worker #1 - 0.03% of PRP M139743557

```
[Jan 13 00:34] Worker starting
[Jan 13 00:34] Setting affinity to run worker on CPU core #1
[Jan 13 00:34] No work to do at the present time.  Waiting.
[Jan 13 00:34] Resuming.
[Jan 13 00:34] Setting affinity to run helper thread 1 on CPU core #2
[Jan 13 00:34] Setting affinity to run helper thread 2 on CPU core #3
[Jan 13 00:34] Setting affinity to run helper thread 4 on CPU core #5
[Jan 13 00:34] Setting affinity to run helper thread 5 on CPU core #6
[Jan 13 00:34] Setting affinity to run helper thread 3 on CPU core #4
[Jan 13 00:34] Starting Gerbicz error-checking PRP test of M139743557 using FMA3 FFT length 7680K, Pass1=768, Pass2=10K, clm=4, 6 threads
[Jan 13 00:34] Preallocating disk space for the proof interim residues file p139743557.residues
[Jan 13 00:34] PRP proof using power=10 and 64-bit hash size.
[Jan 13 00:34] Proof requires 17.9GB of temporary disk space and uploading a 192MB proof file.
[Jan 13 00:36] Iteration: 10000 / 139743557 [0.00%], ms/iter: 11.849, ETA: 19d 03:55
[Jan 13 00:38] Iteration: 20000 / 139743557 [0.01%], ms/iter: 11.220, ETA: 18d 03:28
[Jan 13 00:40] Iteration: 30000 / 139743557 [0.02%], ms/iter: 11.095, ETA: 17d 22:35
[Jan 13 00:41] Iteration: 40000 / 139743557 [0.02%], ms/iter: 11.285, ETA: 18d 05:56
[Jan 13 00:43] Iteration: 50000 / 139743557 [0.03%], ms/iter: 11.691, ETA: 18d 21:39
```

For Help, press F1 NUM

Liczby Mersenne'a a liczby doskonałe

Euklides: $2^p - 1$ jest pierwsza => $2^{p-1}(2^p - 1)$ jest doskonała.

Euler: Każda parzysta liczba doskonała jest postaci $2^{p-1}(2^p - 1)$.

Zależność ta znana jest dzisiaj jako Twierdzenie Euklidesa-Eulera.

Liczba doskonała – liczba naturalna, która jest sumą wszystkich swych naturalnych dzielników właściwych

Liczby Fermata

$$F_n = 2^{2^n} + 1$$

$F_0 = 2^1 + 1 = 3$
$F_1 = 2^2 + 1 = 5$
$F_2 = 2^4 + 1 = 17$
$F_3 = 2^8 + 1 = 257$
$F_4 = 2^{16} + 1 = 65537$
$F_5 = 2^{32} + 1 = 4294967297$

1601 - 1665

Źródła:

https://pl.wikipedia.org/wiki/Historia_liczb
https://en.wikipedia.org/wiki/Prime_number
https://pl.wikipedia.org/wiki/Liczby_pierwsze
https://cs.uwaterloo.ca/journals/JIS/VOL15/Caldwell1/cald5.pdf
https://en.wikipedia.org/wiki/Goldbach%27s_conjecture
https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes
https://en.wikipedia.org/wiki/Ulam_spiral
https://en.wikipedia.org/wiki/Twin_prime
https://pl.wikipedia.org/wiki/Liczby_bliźniacze
https://en.wikipedia.org/wiki/Riemann_hypothesis
https://en.wikipedia.org/wiki/Prime-counting_function
https://en.wikipedia.org/wiki/Prime_number_theorem
https://en.wikipedia.org/wiki/On_the_Number_of_Primes_Less_Than_a_Given_Magnitude
https://mathworld.wolfram.com/ChebyshevFunctions.html
https://mathworld.wolfram.com/PrimeCountingFunction.html