Porządek w chaosie

O liczbach pierwszych

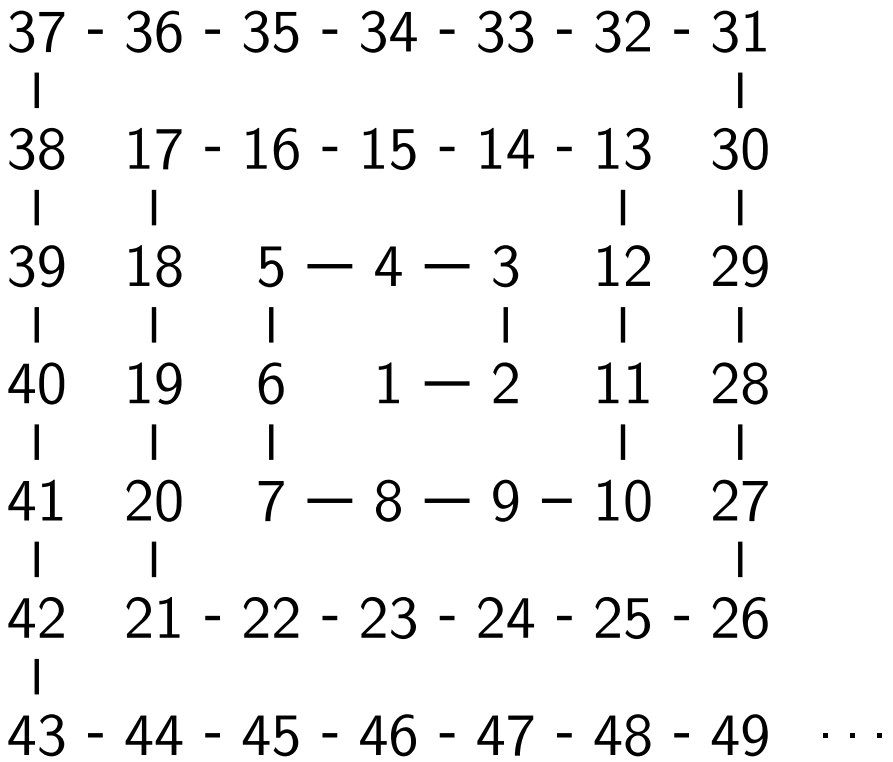
Magdalena Kwiatkowska

Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

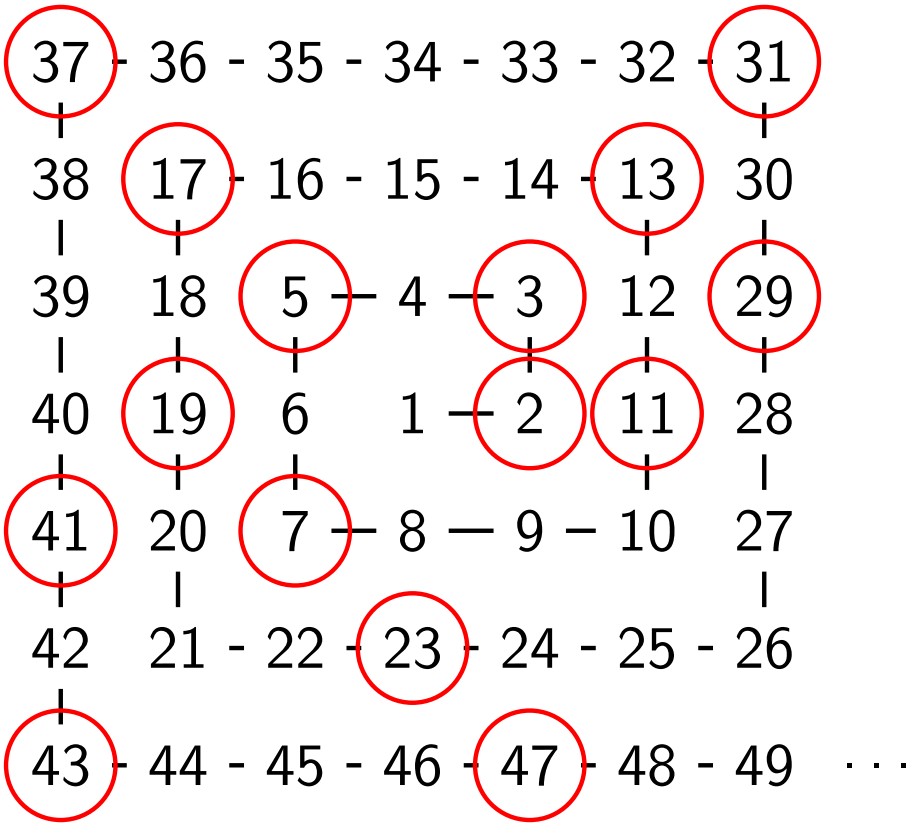
Wrocław 2025

Spis treści

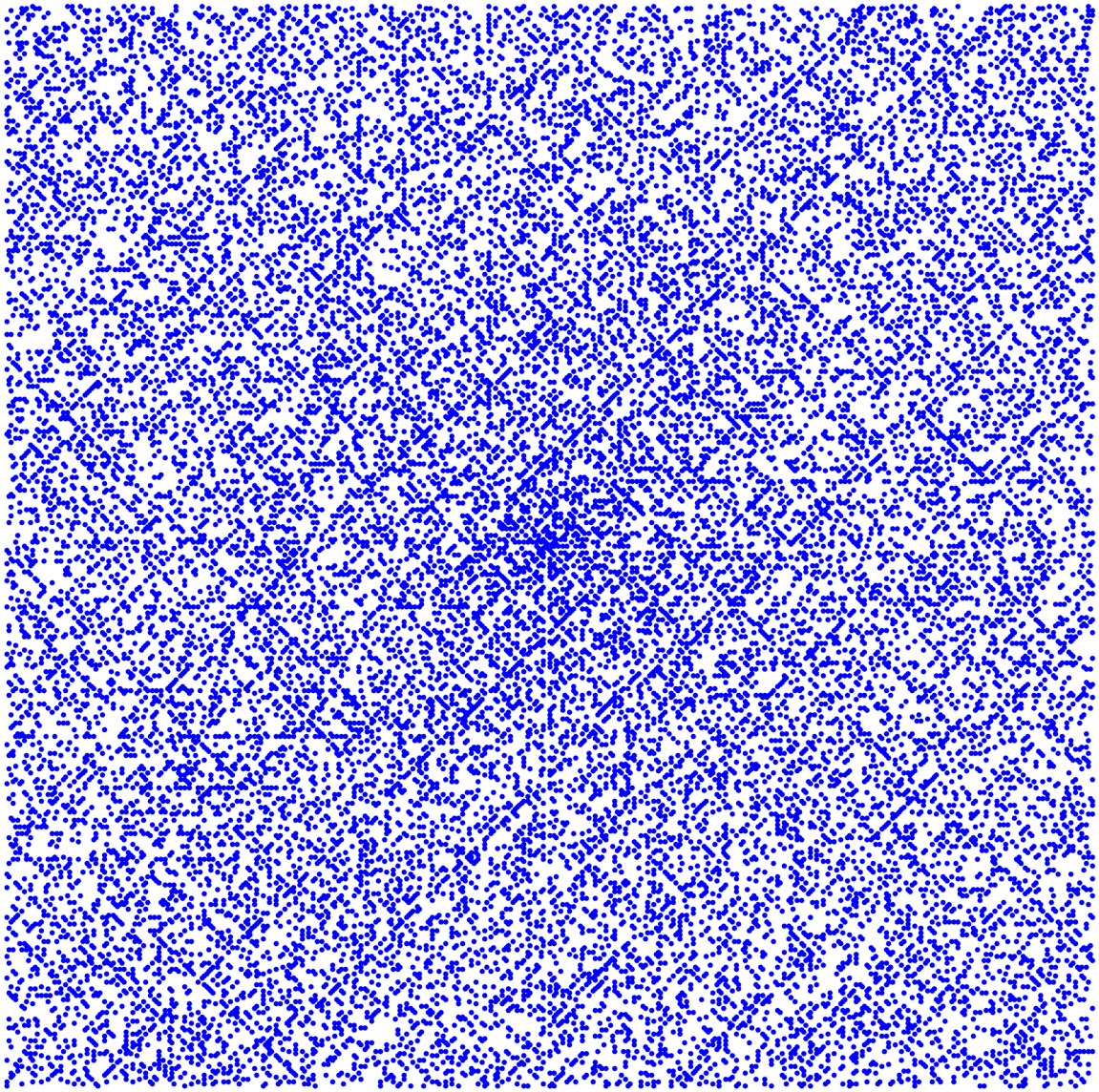
Spirala Ulama



Spirala Ulama



Spirala Ulama



Wzór Eulera

Już Euler zauważył pewną zależność liczb pierwszych, którą opisał wzorem $n^2 + n + 41$ dla $n = 0, 1, 2, \ldots, 39$.
Jak można zauważyć w podanej poniżej tabeli, a później Spirali Ulama, ten wzór genreuje dużo liczb pierwszych w charakterystyczny dla siebie sposób.

Tabela wartości dla $n^2 + n + 41$ dla $n \leq 39$

n	0	1	2	3	4	5	6	7	8	9	10
$p(n)$	**41**	**43**	**47**	**53**	**61**	**71**	**83**	**97**	**113**	**131**	**151**

n	11	12	13	14	15	16	17	18	19	20
$p(n)$	**173**	**197**	**223**	**251**	**281**	**313**	**347**	**383**	**421**	**461**

n	22	23	24	25	26	27	28	29	30
$p(n)$	**547**	**593**	**641**	**691**	**743**	**797**	**853**	**911**	**971**

n	31	32	33	34	35	36	37	38
$p(n)$	**1033**	**1097**	**1163**	**1231**	**1301**	**1373**	**1447**	**1523**

n	39
$p(n)$	**1601**

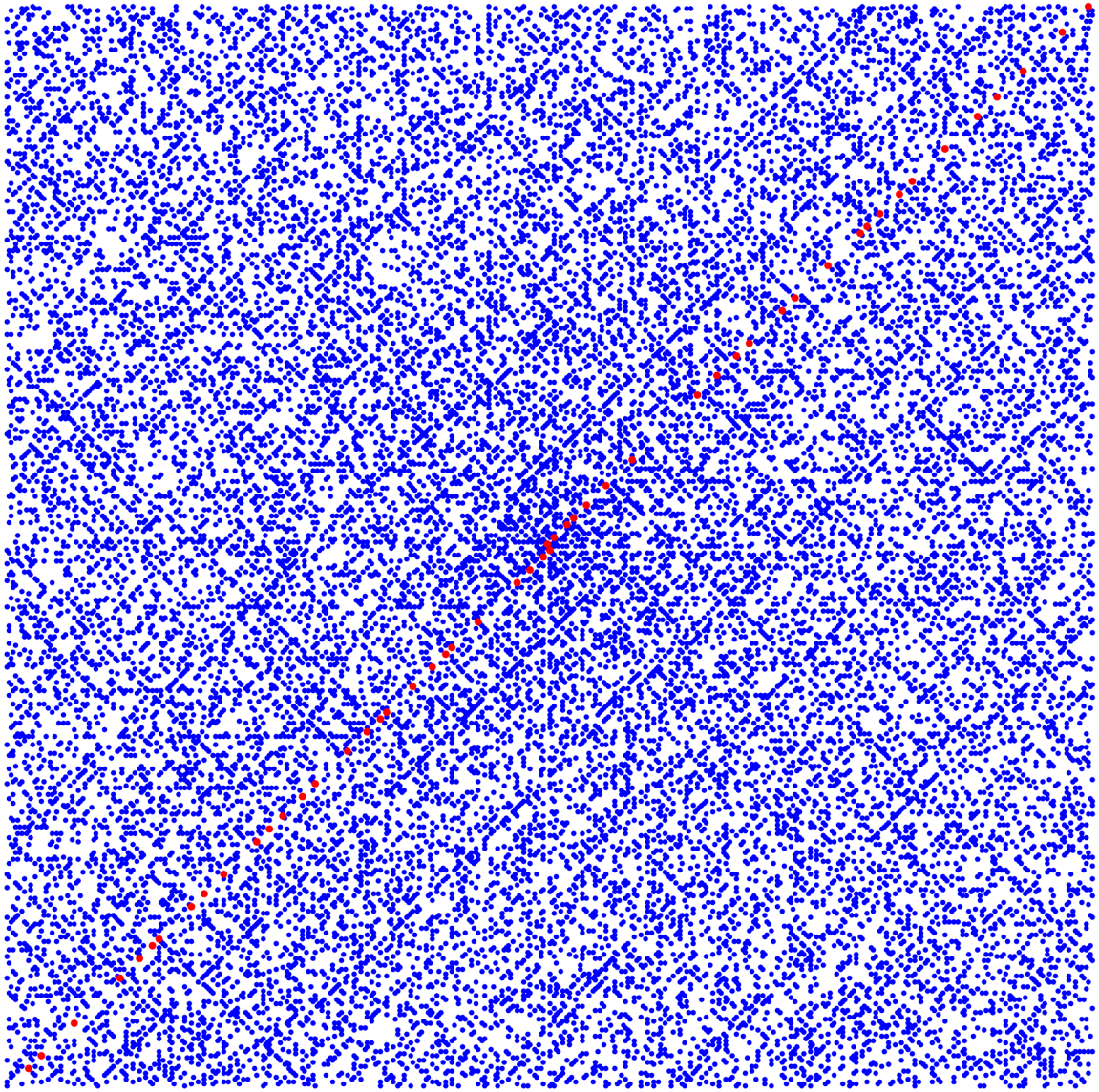
Przykładowa tabela wartości dla $n^2 + n + 41$ dla $n \geq 40$

n	40	41	43	50	60	100	205
$p(n)$	1681	1763	**1933**	**2591**	**3701**	**10141**	42271

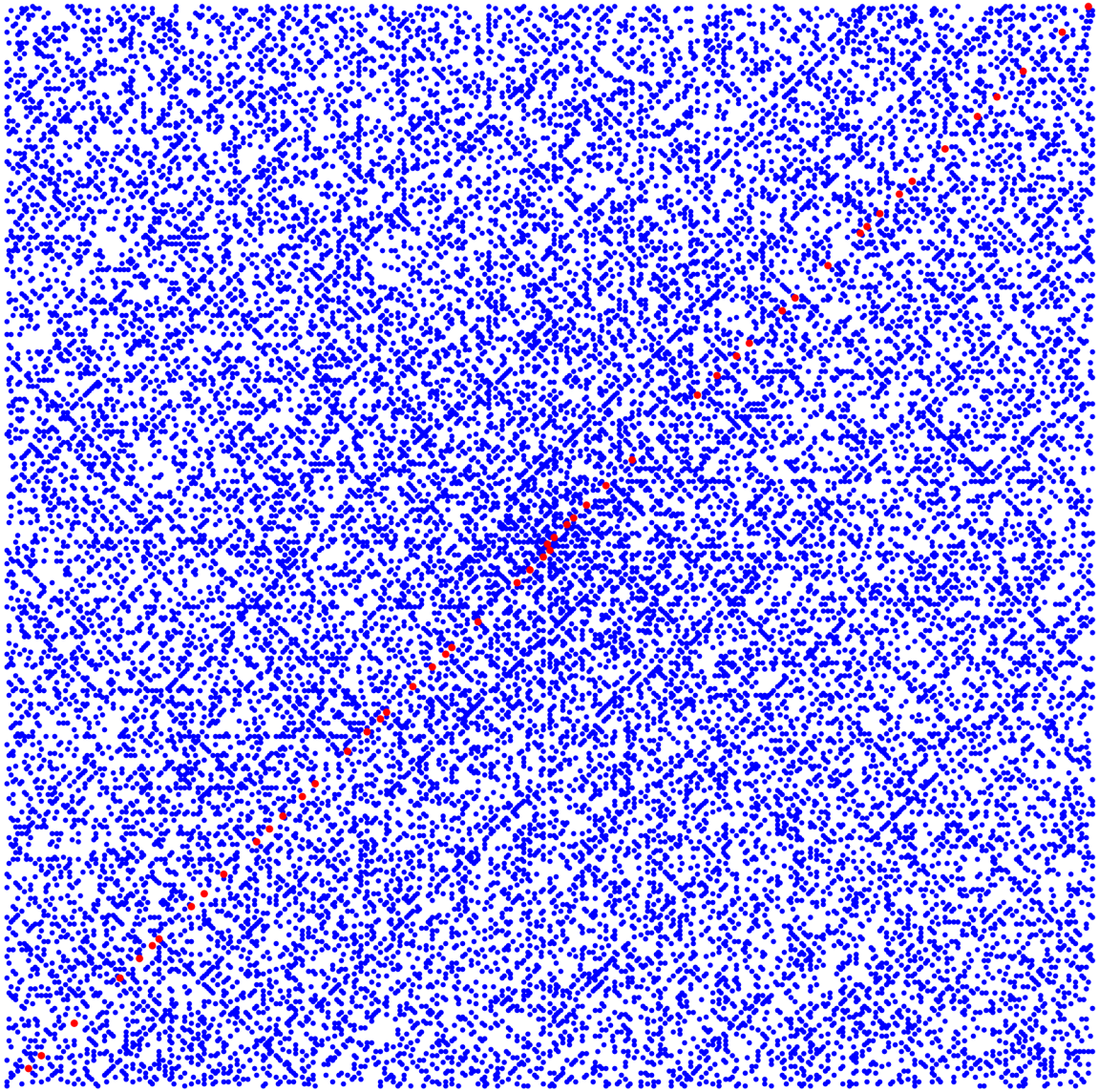
Wielomian Eulera

Spróbujmy rozważyć wielomian $P(n) = n^2 + n + p$, gdzie $p \in \{1, 3, 5, 11, 17, 41\}$, a $n \in \mathbb{N}$. Co można zauważyć każda liczba należąca do p generuje sporo liczb pierwszych, ale żadna z nich nie generuje ich wszystkich.
Liczby złożone otrzymamy zawsze, jeśli n jest podzielne przez p oraz $(n + 1)$ jest podzielne przez p. Zatem można rzec, że liczby $p \in \{1, 3, 5, 11, 17, 41\}$, to tak zwane ***szczęśliwe liczby Eulera***.

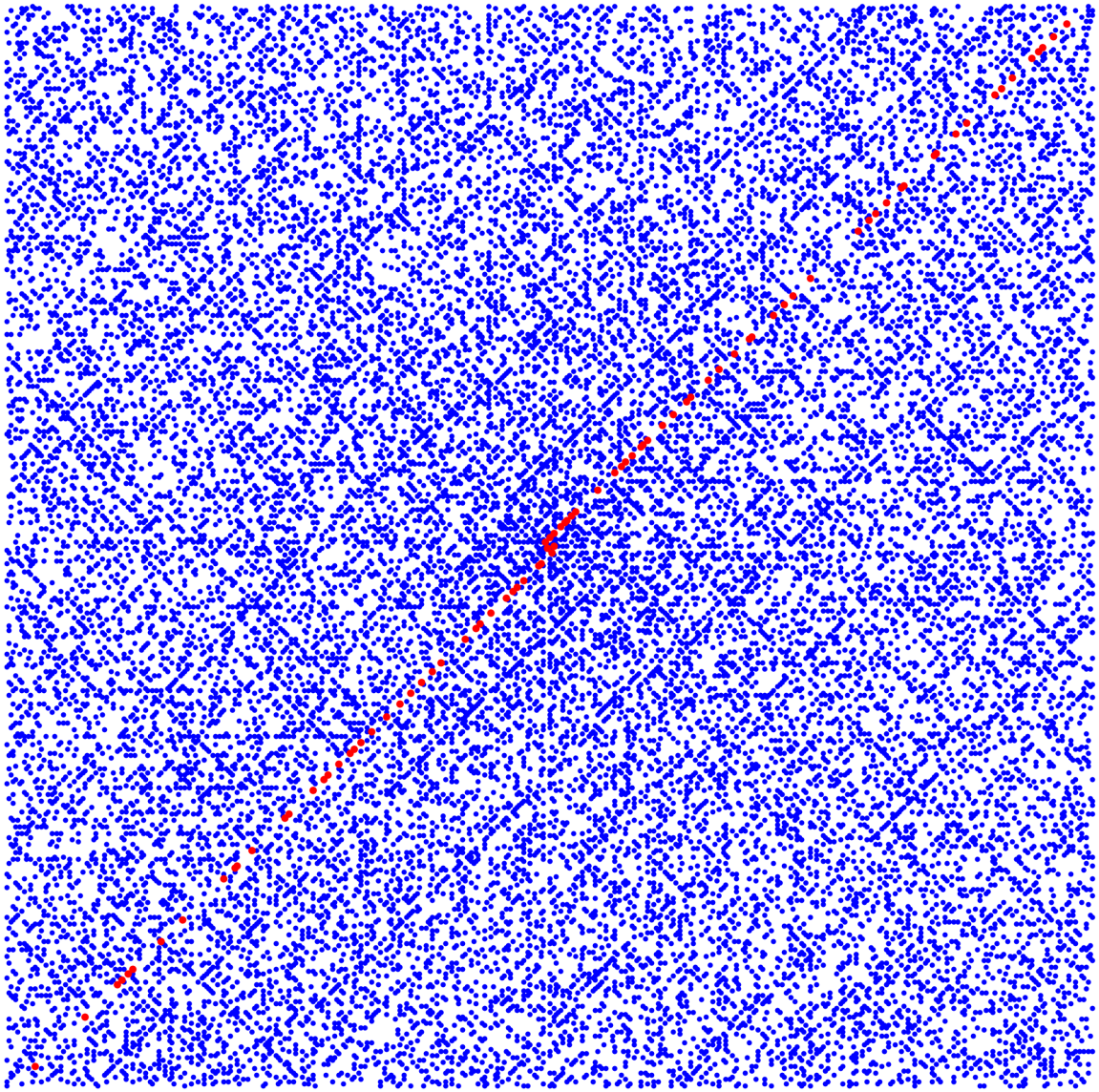
$P(n) = n^2 + n + 1$



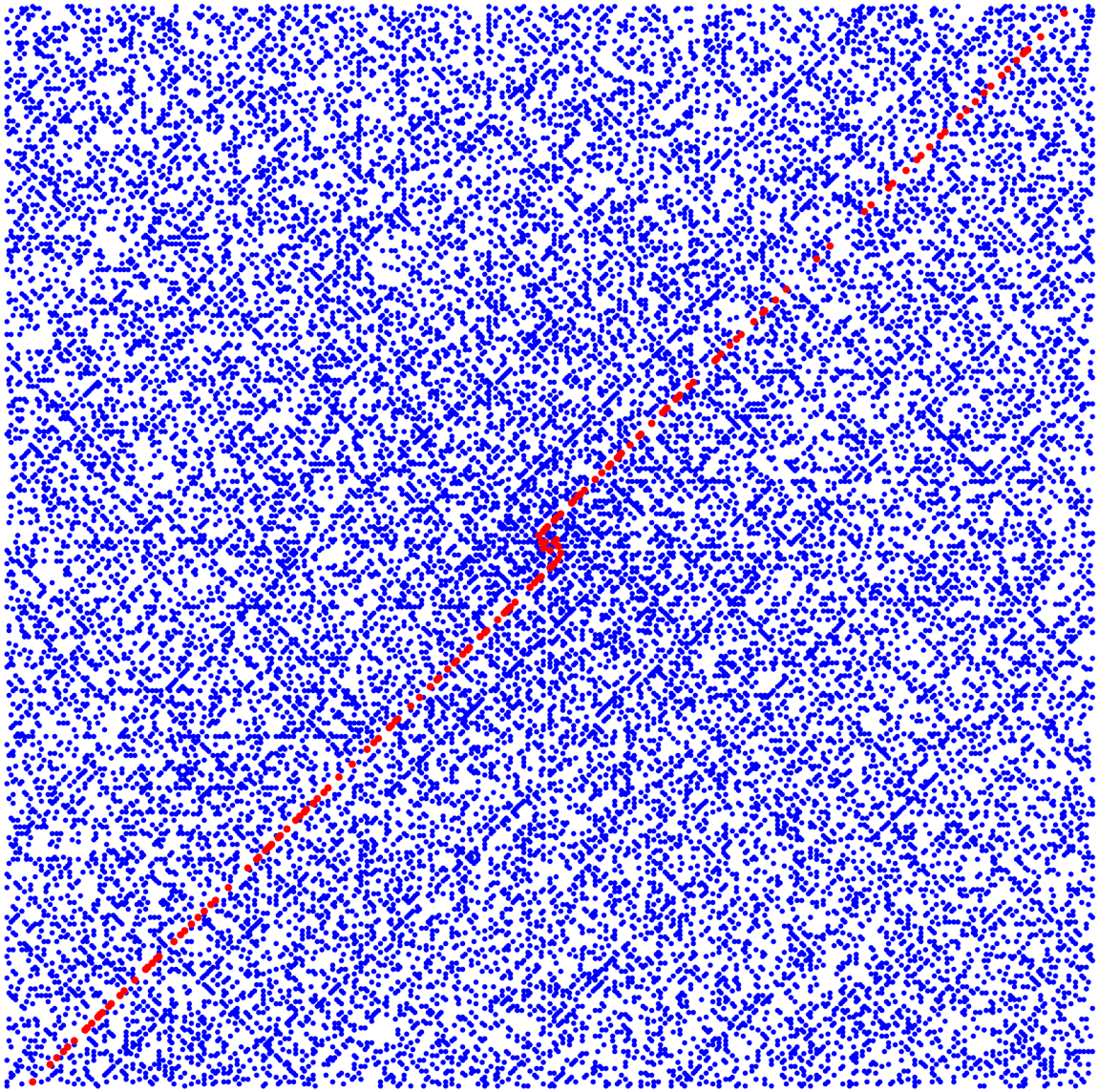
$P(n) = n^2 + n + 3$



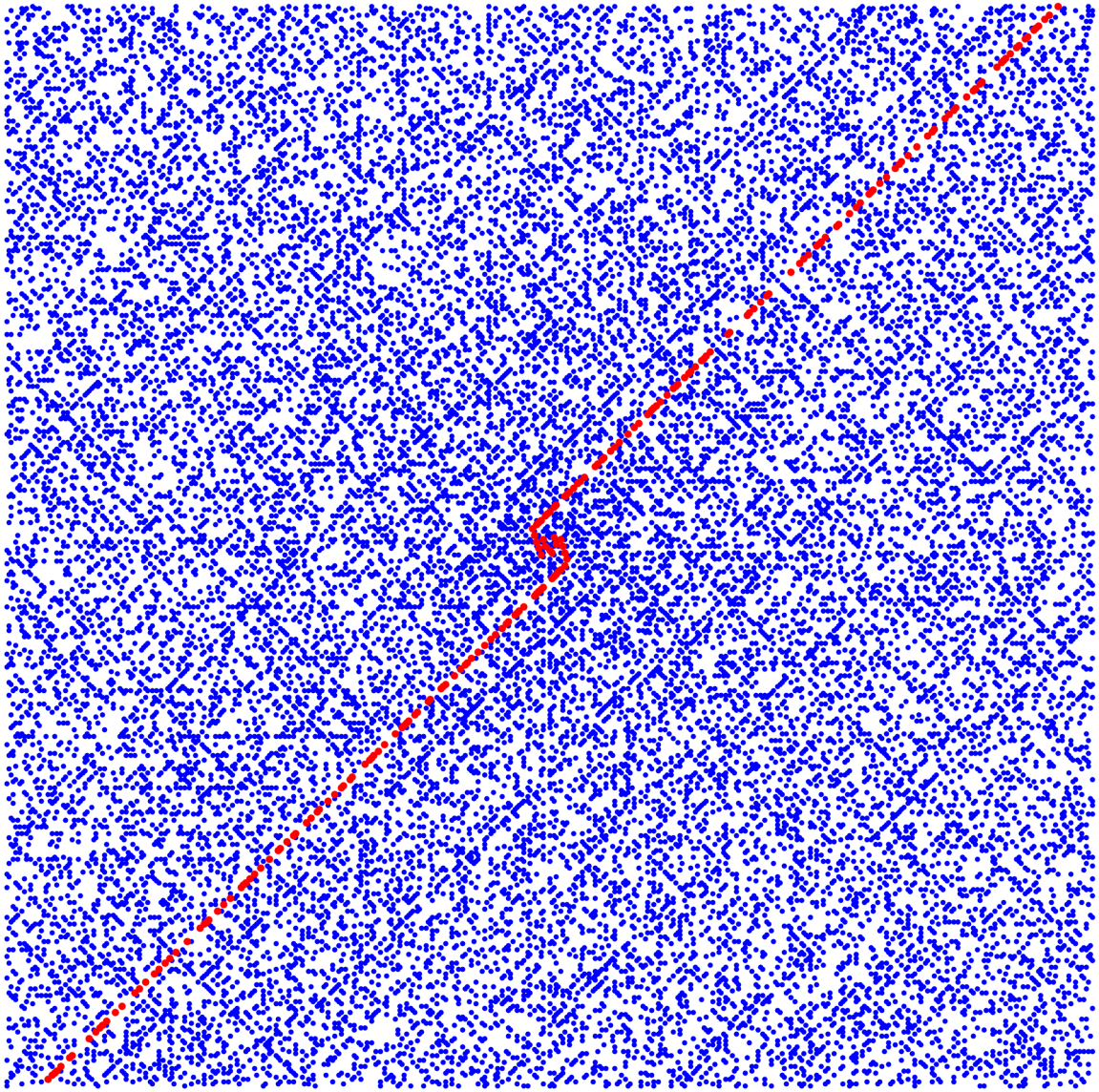
$P(n) = n^2 + n + 5$



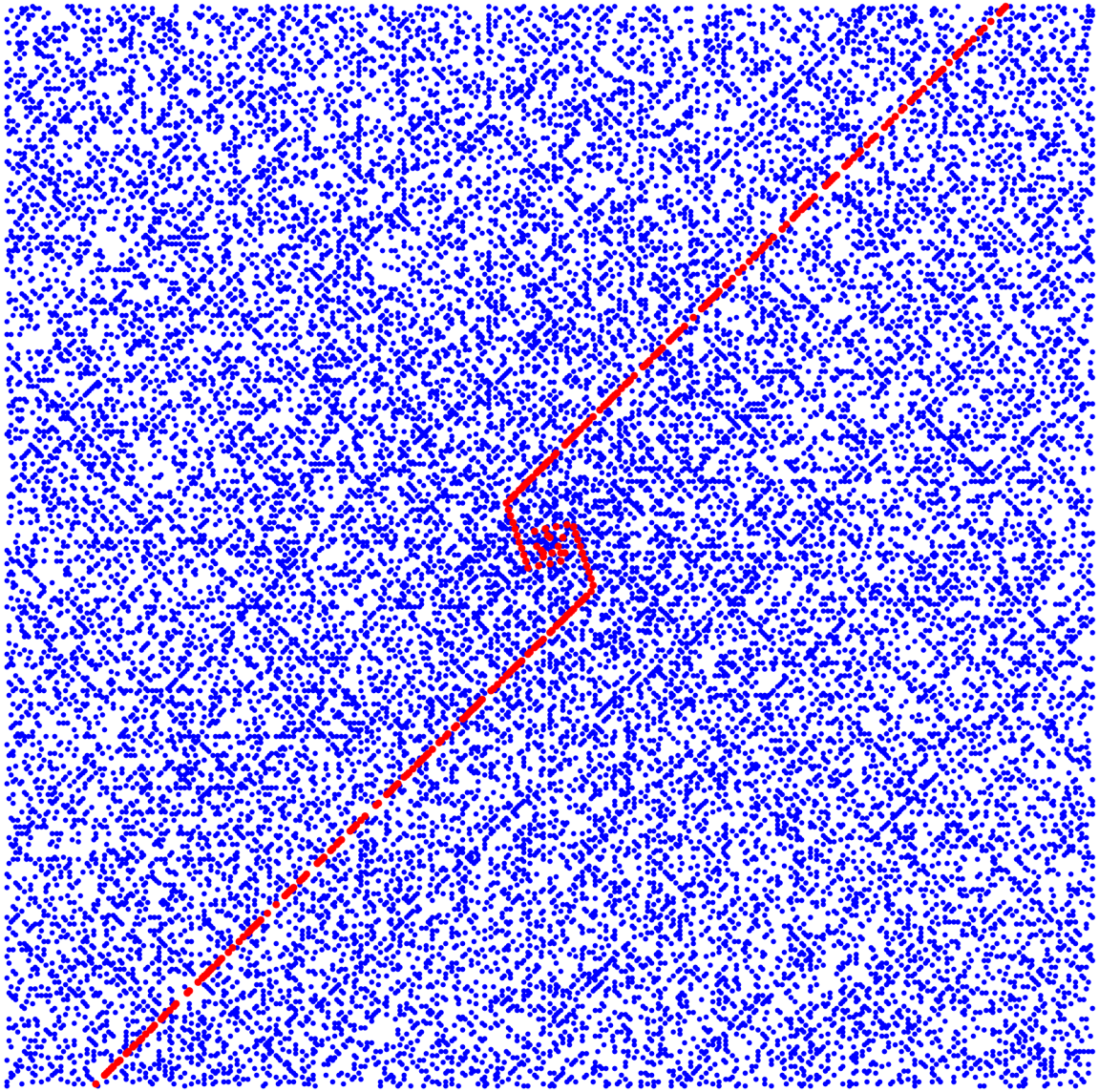
$P(n) = n^2 + n + 11$



$P(n) = n^2 + n + 17$



$P(n) = n^2 + n + 41$



Inne dość proste wzory

Istnieje dużo więcej ciekawych i prostych wzorów, które generują sporo liczb pierwszych.
Oto krótka ich lista.

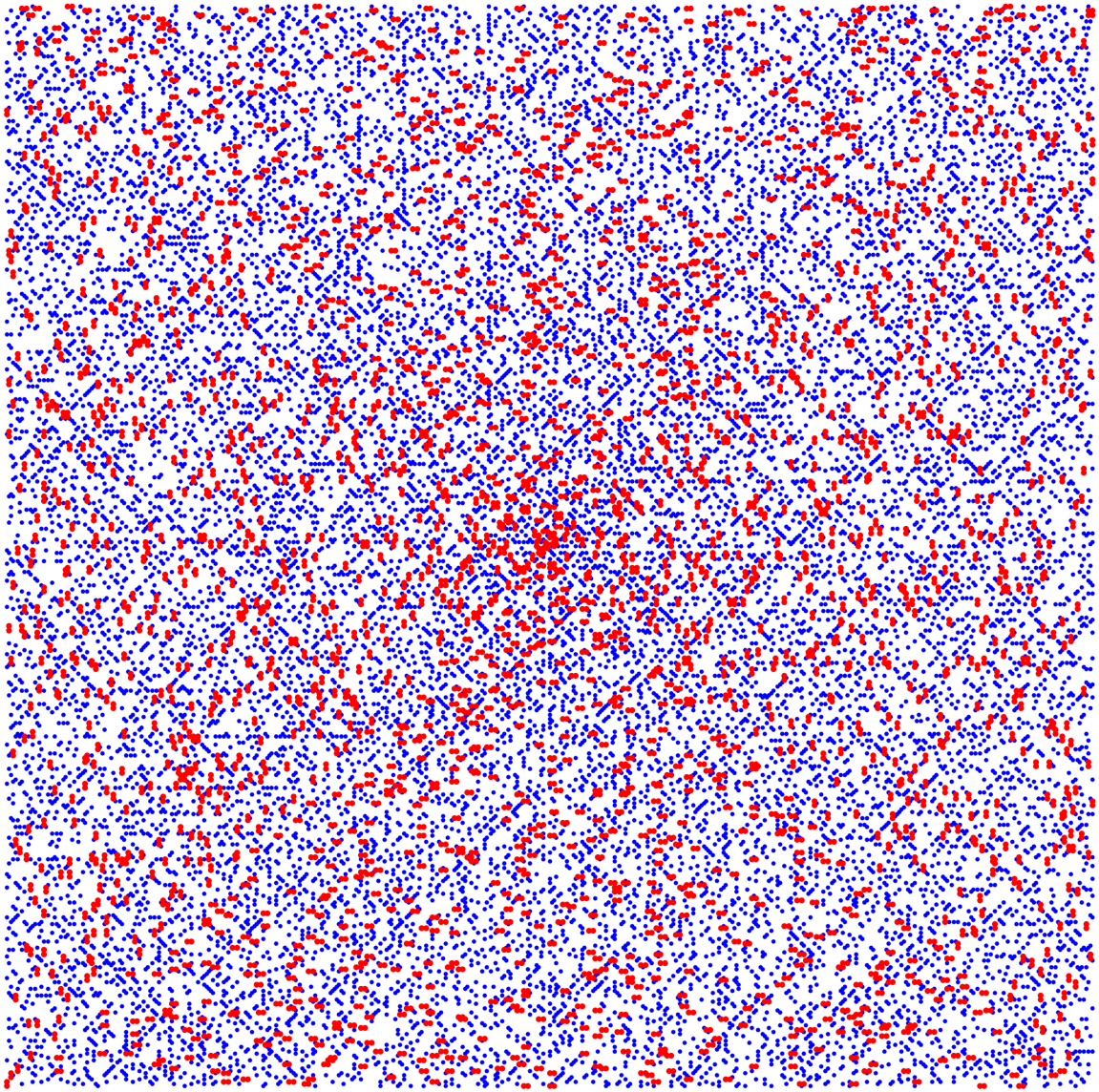
1. $2n^2 + 29$, tzw. *wzór Legendre'a*;
2. $4n^2 - 2n + 5$;
3. $n(4n - 1) + 41$;
4. $n^2 - n + 41$;
5. $n^2 - 3n + 43$.

Dalsze, być może i nowe odkrywanie takich wzorów, pozostawiam do samodzielnej eksploracji.

Szczególne liczby pierwsze

Liczby pierwsze bliźniacze to dwie liczby pierwsze, których różnica wynosi 2.
Przykłady: 3 i 5, 5 i 7, 11 i 13, 191 i 193, 1871 i 1873.
Czy istnieje nieskończenie wiele par liczb pierwszych bliźniaczych?

Liczby pierwsze bliźniacze

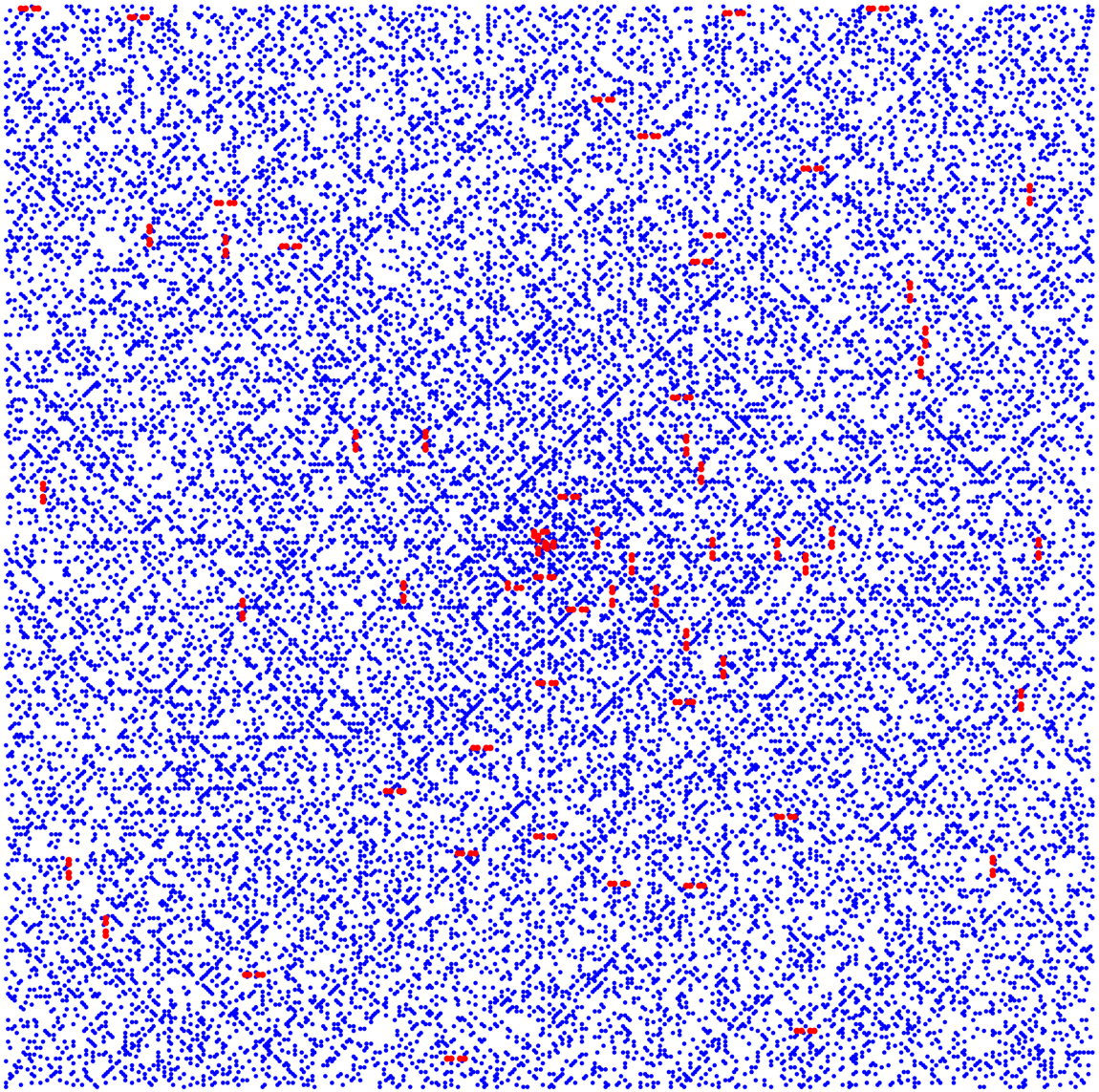


liczby czworacze

Liczby czworacze są to liczby pierwsze postaci:
$p, p+2, p+6, p+8$.
Z wyjątkiem czwórki: 5,7,11,13 liczby czworacze mają postać:
$30n+11, 30n+13, 30n+17, 30n+19$, gdzie
$n \in \{0, 3, 6, 27, 49, 62, 69, 108, 115, \ldots\}$. [1]
Przykłady: 3 i 5, 5 i 7, 11 i 13, 191 i 193, 1871 i 1873.

[1] `https://mathworld.wolfram.com/PrimeQuadruplet.html`

Liczby czworacze



Liczby Mersenne'a

Liczby Mersenne'a to szczególne liczby pierwsze postaci: $\mathcal{M}_n = 2^n - 1$, czyli liczba Mersenne'a to suma ciągu geometrycznego:

$$2^0 + 2^1 + 2^2 + \ldots + 2^{n-2} + 2^{n-1}$$

Warunkiem koniecznym, by $\mathcal{M}$ było liczbą pierwszą jest, by liczba n była pierwsza.
Pierwszość liczby n nie jest warunkiem wystarczającym, przykład:

$$\mathcal{M}_{11} = 2^{11} - 1 = 2047 = 23 * 89$$

Jeśli $\mathcal{M} = 2^n - 1$ jest liczbą pierwszą Mersenne'a, to $\mathcal{M}$-ta liczba trójkątna, tzn: $\Delta_{\mathcal{M}} = \frac{1}{2}\mathcal{M}(\mathcal{M}+1)$ jest doskonała. [2]

[2] J.H. Conway, R.K. Guy *Księga liczb*, Wydawnictwa Naukowo-Techniczne

Liczby Fermata

Liczba Fermata wyraża się w postaci: $\mathcal{F}_n = 2^{2^n} + 1$, $n \in \mathbb{N}$.
Znane do dziś liczby $\mathcal{F}$, które są pierwsze, to:

- $\mathcal{F}_0 = 2^{2^0} + 1 = 2^1 + 1 = 2 + 1 = 3$
- $\mathcal{F}_1 = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5$
- $\mathcal{F}_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$
- $\mathcal{F}_3 = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257$
- $\mathcal{F}_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65536 + 1 = 65537$

Liczby pierwsze Garmin

Liczba Garmin to dowolna liczba pierwsza p, która dla $2p+1$ zachowuje pierwszość.

Przykłady: $p = 23 \Rightarrow 2p+1 = 2*23+1 = 46+1 = 47 \in \mathbb{P}$

$p = 5 \Rightarrow 2p+1 = 2*5+1 = 10+1 = 11 \in \mathbb{P}$

$p = 131 \Rightarrow 2p+1 = 2*131+1 = 262+1 = 263 \in \mathbb{P}$

Szereg odwortności liczb pierwszych

Jak wiemy istnieje nieskończenie wiele liczb pierwszych. Jednak jak gęsto są one rozłożone?
Rozważmy nieskończony szereg odwrotności liczb pierwszych

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \dots.$$

Rozbieżność odwrotności liczb pierwszych

Twierdzenie:

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots = \infty$$

Dowód:[3] Dla $0 < u < 1$ mamy

$$\ln\left(\frac{1}{1-u}\right) = u + \frac{u^2}{2} + \frac{u^3}{3} + \ldots < u + \frac{1}{2}(u^2 + u^3 + \ldots) = u + \frac{u^2}{2(1-u)}.$$

Przyjmijmy, że $u = \frac{1}{p}$, wtedy otrzymujemy:

$$\frac{1}{p} > -\ln\left(1 - \frac{1}{p}\right) - \frac{1}{2p(p-1)}.$$

[3] W. Marzantowicz, P. Zarzycki *Elementarna teoria liczb* Wydanie 2, PWN

Rozbieżnosć odwrotności liczb pierwszych

Sumując tę nierówność po wszystkich p, uzyskujemy:

$$\sum_{p\in\mathbb{P}} \frac{1}{p} > \ln\left(\prod_{p\in\mathbb{P}} \left(1-\frac{1}{p}\right)^{-1}\right) - \frac{1}{2}\sum_{p\in\mathbb{P}} \frac{1}{p(p-1)}$$

Zauważmy, że

$$\sum_{p\in\mathbb{P}} \frac{1}{p(p-1)} < \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1.$$

Zatem:

$$\sum_{p\in\mathbb{P}} \frac{1}{p} > \ln\left(\prod_{p\in\mathbb{P}} \left(1-\frac{1}{p}\right)^{-1}\right) - \frac{1}{2}$$

Rozbieżność odwrotności liczb pierwszych

Rozpatrzmy

$$S(x) = \sum_{\substack{p \leq x \\ p \in \mathbb{P}}} \frac{1}{p}$$

Stąd

$$S(x) > \ln(\ln(x)) - \frac{1}{2}$$

Ostatecznie otrzymujemy:

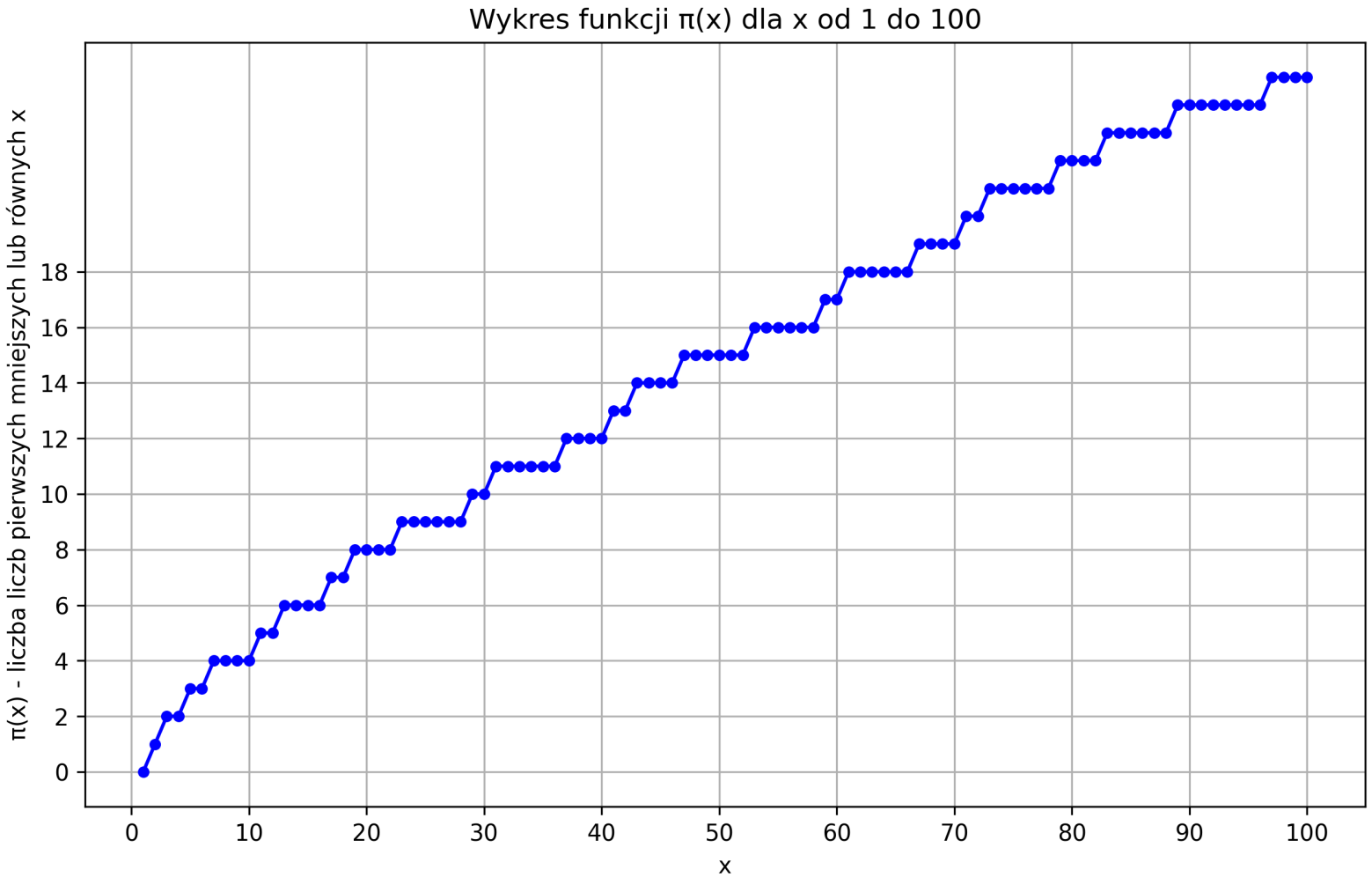
$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \lim_{x \to \infty} S(x) = \infty$$

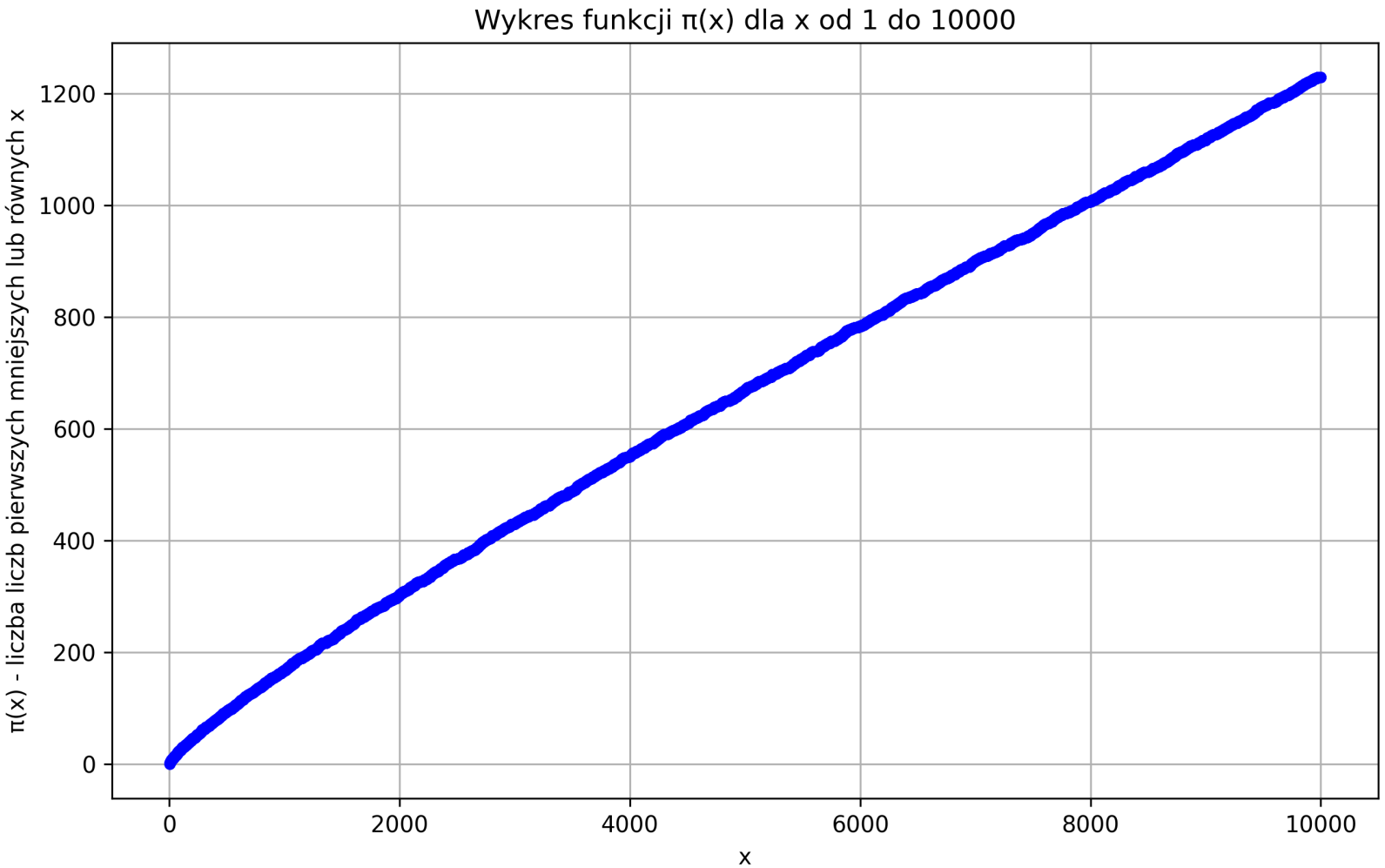
□

Funkcja $\pi(x)$

Najpierw zdefiniujmy funkcję $\pi(x)$, która danej liczbie rzeczywistej x przyporządkowuje liczbę liczb pierwszych nie większych od x. Funkcja zachowuje własności dla liczb rzeczywistych, jednak częściej odnosi się do liczb naturalnych.
Przykłady:

- Dla $x = 10$ otrzymujemy $\pi(10) = 4$. Czyli mamy 4 liczby pierwsze wśród pierwszych 10 liczb naturalnych $p \in \{2, 3, 5, 7\}$
- Dla $x = 1000$ mamy $\pi(1000) = 168$
- Dla $x = 10000$ otrzymujemy $\pi(10000) = 1229$.


Wykres funkcji π(x) dla x od 1 do 100
π(x) - liczba liczb pierwszych mniejszych lub równych x
0
2
4
6
8
10
12
14
16
18
0
10
20
30
40
50
60
70
80
90
100
x


Wykres funkcji π(x) dla x od 1 do 10000
π(x) - liczba liczb pierwszych mniejszych lub równych x
0
200
400
600
800
1000
1200
0
2000
4000
6000
8000
10000
x

Przybliżenie funkcji $\pi(x)$

Spróbujmy oszacować wartości funkcji zliczającej liczby pierwsze. Weźmy

$$\pi(x) \approx \frac{x}{\ln(x)}.$$

Otrzymujemy wtedy:

x	$\pi(x)$	$\frac{x}{\ln(x)}$	różnica [%]
10	4	4,3429	-8,56%
10^3	168	144,7649	16,05%
10^5	9 592	8 685,8896	10,44%
10^7	664 579	620 420,6873	7,12%
10^9	50 847 534	48 254 942,433	5,37%
10^{11}	4 118 054 813	3 948 728 953,5	4,28%
10^{13}	346 065 536 839	334 082 752 757,2	3,59%
10^{15}	29 844 570 422 669	28 952 965 460 216,8	3,08%

Oszacowanie $\frac{x}{\ln(x)}$

Jak można dostrzec, gdy x nam rosną, to różnica między $\pi(x)$ oraz $\frac{x}{\ln(x)}$ maleje, dzieje się tak, ponieważ zachodzi między nimi równość asymptotyczna, czyli

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

Można jeszcze dokładniej przybliżyć to oszacowanie za pomocą rozwinięcia logarytmu całkowego w szereg

$$\pi(x) \approx \frac{x}{\ln(x)} + \frac{x}{\ln^2(x)} + \frac{2x}{\ln^3(x)} + \ldots = \sum_{i=1}^{\infty} \frac{(i-1)!x}{\ln^i(x)}$$

Oszacowanie Gaussa

Gauss zasugerował, że liczba $\pi(x)$ liczb pierwszych w przedziale $[1, n]$ opisana jest zależnością:

$$\pi(x) \sim Li(x),$$

gdzie zachodzi między nimi równość asymptotyczna, tzn:

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

a

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

Twierdzenie Bertranda-Czebyszewa

Twierdzenie: Dla dowlonej liczby naturalnej $n \geq 2$ między liczbami n i $2n$ znajduje się co najmniej jedna liczba pierwsza.

Twierdzenie Dirichleta

Twierdzenie: W dowolnym ciągu arytmetrycznym liczb naturalnych $a, a+q, a+2q, a+3q, \ldots$, gdzie a i q są względnie pierwsze, istnieje nieskończenie wiele liczb pierwszych.

Przykład

Rozważmy ciąg $1, 5, 9, 13, \ldots$. Wówczas ciąg ma postać $n \equiv 1 \pmod 4$, więc ciąg liczb pierwszych w tym ciagu to: $5, 13, 17, 19, \ldots$.
Załóżmy przeciwnie, czyli ciąg liczb pierwszych tej postaci jest skończony. Niech

$$P = \{p_1, p_2, p_3, \ldots, p_m\},$$

gdzie $p_i \equiv 1 \pmod 4$. Euler udowodnił, że *każdy nieparzysty dzielnik pierwszy p liczby naturalnej postaci* $a^2 + 1$ *dla pewnego a musi dawać resztę 1 przy dzieleniu przez 4*.
Innymi słowy: *Jeśli p jest liczbą pierwszą i* $p \mid (a^2 + 1)$, *to* $p \equiv 1 \ (mod\ 4)$.

Przykład

Niech A będzie niepustym, skończonym podzbiorem wszystkich liczb pierwszych postaci $n \equiv 1 \pmod 4$. Niech X będzie iloczynem wszystkich elementów tego podzbioru A. Weźmy $A = P$, zatem $X = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m$. Rozważmy $N \geq 0$, N - liczba nautralna, taka że $N = (2X)^2 + 1$. Ponieważ X jest iloczynem liczb naturalnych, a N jest liczbą większą od 1, to musi posiadać co najmniej jeden dzielnik pierwszy. Dzielnik ten jest nieparzysty (X jako iloczyn liczb pierwszych p_i postaci $n \equiv 1 \pmod 4$, z których każda jest nieparzysta, więc całe X jest niepatrzyste $\Rightarrow$ $2X$ - parzyste $\Rightarrow$ $(2X)^2$ - parzyste $\Rightarrow$ $(2X)^2 + 1$ - nieparzyste).

Przykład

Niech q będzie dowolnym dzielnikiem pierwszym liczby N. Na mocy twierdzenia Eulera dzielnik ten musi spełniać

$$q \equiv 1 \pmod 4,$$

zatem q jest liczbą pierwszą tej postaci. **SPRZECZNOŚĆ.** Każda liczba pierwsza $p_i \in P$ jest dzielnikiem X. Gdyby tak było, to q dzieliłoby X, więc dzieliłoby również $(2X)^2$. Skoro q jest dzielnikiem $N = (2X)^2 + 1$ oraz q miałoby dzielić $(2X)^2$, to q musiałoby dzielić różnicę tych liczb, czyli 1. Oznacza to, że q musiałoby dzielić 1. Ale q jest liczbą pierwszą, więc $q > 1$. Zatem $q \notin P$. Czyli zbiór wszystkich liczb pierwszych postaci $n \equiv 1 \pmod 4$ jest nieskończony.

Oszacowania n-tej liczby pierwszej

Twierdzenie: Niech p_n będzie n-tą liczbą pierwszą, wtedy $p_n \leq 2^{2^{n-2}} + 1$. [4]

Dowód: Dla $n = 1$ otrzymujemy $p_1 = 2 \leq \sqrt{2} + 1$, dla $n = 2$ mamy $p_2 = 3 \leq 3$. Załóżmy, że $n \geq 3$. Łatwo zauważyć, że dla $i \neq j$ otrzymujemy $(\mathcal{F}_i, \mathcal{F}_j) = 1$. Zatem każda z liczb Fermata $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_{n-2}$ jest podzielna przez liczbę pierwszą nieparzystą, która nie dzieli pozostałych liczb Fermata. A stąd wynika, że $2 \nmid \mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_{n-2}$, a także $3 \nmid \mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_{n-2}$. Otrzymujemy $p_n \leq \mathcal{F}_{n-2} = 2^{2^{n-2}} + 1$. □

[4] W. Marzantowicz, P. Zarzycki *Elementarna teoria liczb* Wydanie 2, PWN

Oszacowanie Dirichleta

Czebyszew oszacował, że istnieją liczby dodatnie A, B, C takie, że dla wszystkich $x \geq 2$ mamy:

$$Ax \leq \upsilon(x) \leq 2\ln(4)x$$

oraz

$$B\frac{x}{\ln(x)} \leq \pi(x) \leq C\frac{x}{\ln(x)},$$

gdzie

$$\upsilon(x) = \sum_{p \leq x} \ln(p) = \ln\left(\prod_{p \leq x} p\right)$$

Na dodatek wartości B i C w przybliżeniu to $B = 0,92129$ oraz $C = 1,1055$.

Wnioski

- Jeśli liczba pierwsza Germain p przystaje do 3 (mod 4), to odpowiadająca jej liczba pierwsza $2p+1$ jest dzielnikiem liczby Mersenne'a $\mathcal{M}_p = 2^p - 1$.
- W każdym przedziale liczb naturalnych $(n, 2n)$ jest $\frac{\sqrt{2n}}{2}$ liczb pierwszych.
- Istnieje nieskończenie wiele liczb pierwszych postaci $4k-1$ oraz $4k+1$ - twierdzenie Dirichleta i przykład.
- Liczby pierwsze stają się coraz rzadsze, a ich gęstość można opisać jako $\approx \frac{1}{\ln(x)}$.
- Średni odstęp między kolejnymi liczbami pierwszymi to $\approx \ln(x)$.
- N-ta liczba pierwsza dla dużych n jest w przybliżeniu równa $n\ln(n)$, tzn. $p_n \approx n\ln(n)$. [5]

[5] P. Ribenboim *Mała księga wielkich liczb pierwszych*, Wydawnictwo Naukowo-Techniczne

Dziękuję za uwagę! :)