

素数と数学の歴史

コスキヴィルタ ジャンステファン

埼玉大学

2022 年 6 月 18 日

埼玉大学連続市民講座

定義

素数とは、2以上の自然数で、1と自分自身以外に正の約数を持たないもののことをいう。

- 6の正の約数は1, 2, 3, 6の四つである。ゆえに6は素数でない。
- 素数のリスト:

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

素因数分解



定理 (ユークリッド, 紀元前 300)

2 以上の任意の整数は、ただ 1 通りに素数の積で書くことができる.

$$60 = 2 \times 2 \times 3 \times 5$$

疑問 1

問題

素数はどれぐらいたくさんあるのだろうか？



定理 (ユークリッド, 紀元前 300)

素数が無数に存在する.

$\pi(x) = x$ 以下の素数の個数

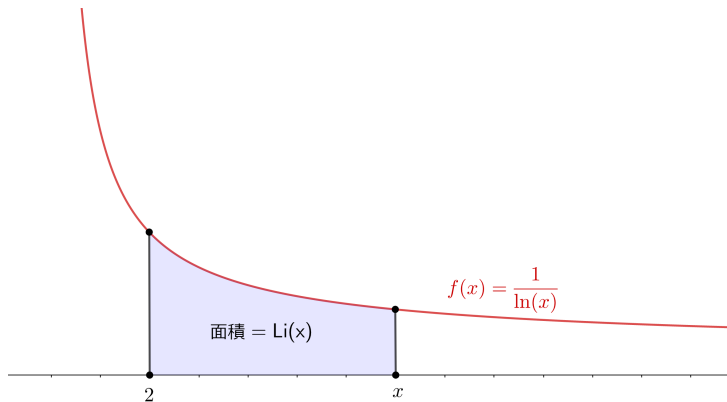


定理 (Hadamard–De la Vallée Poussin, 1896)

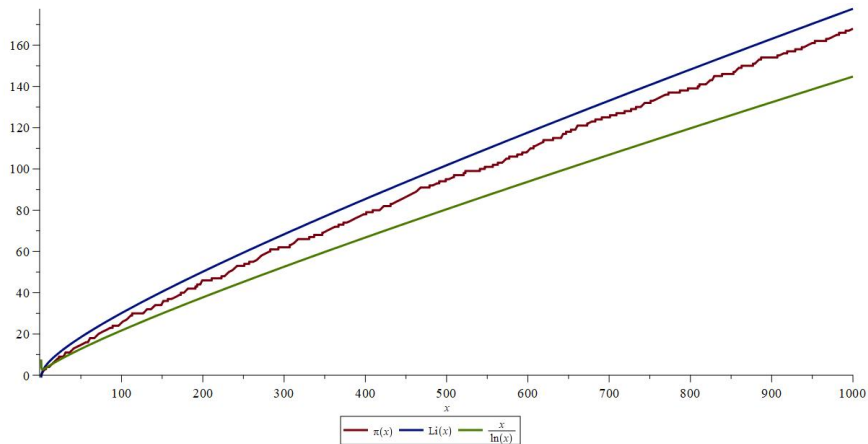
$$\pi(x) \sim \frac{x}{\ln(x)}.$$

対数積分

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



素数関数



x	$\pi(x)$	$\pi(x) - \frac{x}{\ln(x)}$	$\text{Li}(x) - \pi(x)$	$\pi(x) / \frac{x}{\ln(x)}$
1000	168	23	10	1.161
10^8	5761455	332774	754	1.061
10^{12}	37607912018	1416705193	38263	1.039
10^{16}	279238341033925	7804289844393	3214632	1.029
10^{20}	2220819602560918840	49347193044659701	222744644	1.023
10^{24}	18435599767349200867866	339996354713708049069	17146907278	1.019

予想

$$|\mathrm{Li}(x) - \pi(x)| < \frac{\sqrt{x} \ln(x)}{8\pi}$$

Schoenfeld (1976)

定理 (Skewes, 1955)

$\pi(x) > \text{Li}(x)$ をみたす x が無数に存在する.

定理 (Bays–Hudson, 2000)

1.398201×10^{316} と 1.398244×10^{316} の間に $\pi(x) > \text{Li}(x)$ をみたす x が存在する.

疑問 2

問題

素数の下一桁は何？

素数の下一桁

5 以降の素数の下一桁は 1,3,7,9 のいずれかである.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, ...

最初の 100000 個の素数の下一桁



Dirichlet の定理



定理 (算術級数定理, Dirichlet, 1837)

互いに素である二つの自然数 a, b に対して,

$$ax + b, \quad x : \text{自然数}$$

と書ける素数が無限に存在する.

Chebotarev の定理

素数 p について, p を a で割った余りを調べる. a と素である自然数全体を

$$x_1, x_2, \dots, x_n$$

とおく.

定理 (Chebotarev の密度定理, 1926)

素数 p をランダムに選ぶと, p を a で割った余りが x_i になる確率は $\frac{1}{n}$ である.

疑問 3

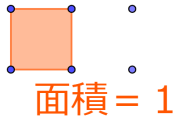
問題

素数 p に対して, p を二個の平方数の和で表せるか? つまり,

$$p = x^2 + y^2$$

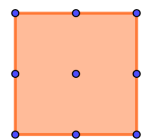
をみたす x, y が存在するか?

二個の平方数の和



面積 = 1

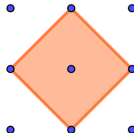
A diagram showing a 1x1 square on a grid of blue dots. The square is outlined in orange and is located in the lower-left quadrant of the grid. The text '面積 = 1' is written in orange below the square.



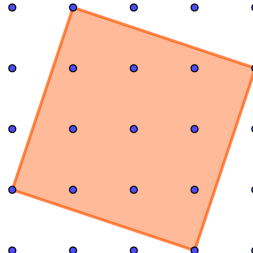
面積 = 4

A diagram showing a 2x2 square on a grid of blue dots. The square is outlined in orange and is located in the upper-right quadrant of the grid. The text '面積 = 4' is written in orange below the square.

二個の平方数の和

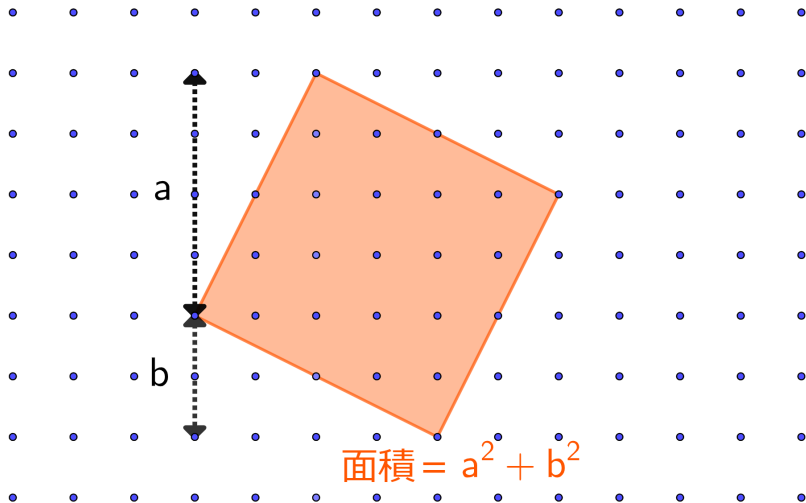


面積 = 2



面積 = 10

二個の平方数の和



チェック

```
test := proc(m)
local a, b, x, y, v;
a := floor(sqrt(m));
b := floor(sqrt(m));
v := 0;
for x from 0 to a do for y from 0 to b do
if  $x^2 + y^2 = m$  then v := 1; break;
end if; end do; end do; v; end proc;

test_prime := proc(N)
local L, P, i;
P := [seq(ithprime(i), i = 1 .. N)]; L := [];
for i to N do if test(P[i]) = 1 then
L := [op(L), P[i]]; end if; end do; L; end proc;
```

チェック

素数	$p = x^2 + y^2$?
3	×
5	$5 = 1^2 + 2^2$
7	×
11	×
13	$13 = 2^2 + 3^2$
17	$17 = 1^2 + 4^2$
19	×
23	×
29	$29 = 2^2 + 5^2$
31	×
37	$37 = 1^2 + 6^2$
41	$41 = 4^2 + 5^2$
43	×

Fermat の定理

定理 (Fermat, 1640)

$4k + 1$ 型の素数は二個の平方数の和で表すことができる。また逆に、ある奇素数が二個の平方数の和であるならば、 $4k + 1$ 型の素数である。



素数	$p = x^2 + y^2$?	$4k + 1$ 型?
3	×	×
5	$5 = 1^2 + 2^2$	○
7	×	×
11	×	×
13	$13 = 2^2 + 3^2$	○
17	$17 = 1^2 + 4^2$	○
19	×	×
23	×	×
29	$29 = 2^2 + 5^2$	○
31	×	×
37	$37 = 1^2 + 6^2$	○
41	$41 = 4^2 + 5^2$	○
43	×	×

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod{4}$ Is a Sum of Two Squares

D. ZAGIER

Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point. $\square$

2 次形式

一般に, 2 次形式とは,

$$f(x, y) = ax^2 + bxy + cy^2$$

の形のものという. ここで, a, b, c は整数である. 例えば,

$$x^2 + y^2, \quad x^2 + 5xy - 2y^2, \quad 2x^2 - xy + 3y^2, \quad \dots$$

は 2 次形式である.

定理

定理 (Fermat)

奇素数 p に対して, 以下が成り立つ.

$$p = x^2 + 2y^2 \iff p \text{ は } 8k + 1 \text{ 型, または } 8k + 3 \text{ 型.}$$

定理 (Fermat)

素数 $p > 3$ に対して, 以下が成り立つ.

$$p = x^2 + 3y^2 \iff p \text{ は } 3k + 1 \text{ 型.}$$

定理 (Gauss, 1801)

素数 $p \neq 5$ に対して, 以下が成り立つ.

$$p = x^2 + 5y^2 \iff p \text{ は } 20k + 1 \text{ 型, または } 20k + 9 \text{ 型.}$$

$$p = 2x^2 + 2xy + 3y^2 \iff p \text{ は } 20k + 3 \text{ 型, または } 20k + 7 \text{ 型.}$$



疑問 4

問題

連続する 2 つの素数の差はどれぐらい大きくなるか？どれぐらい小さくなるか？

n 番目の素数を p_n とおく.

$$p_{n+1} - p_n$$

はどのように変化するか？

未解決問題

双子素数とは、差が2の素数のペアのことをいう。例えば、 $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$ は双子素数である。

予想 (双子素数予想)

双子素数は無数に存在する。

予想 (de Polignac の予想)

正の偶数 k に対して、差が k である素数のペアは無数に存在する。

$$2996863034895 \times 2^{1290000} \pm 1$$

定理

$$\liminf(p_{n+1} - p_n) < 70000000$$

定理 (Polymath, Maynard, 2014)

$$\liminf(p_{n+1} - p_n) < 246$$

数列

$$n! + 2, n! + 3, n! + 4, \dots, n! + n$$

の全ての整数は素数でない.

予想 (Cramer)

定数 $C > 0$ が存在し, 以下の不等式が成立する.

$$p_{n+1} - p_n \leq C \ln(p_n)^2$$