初等整数論、初等幾何学、離散数学における未解決問題

山田智宏 (Tomohiro Yamada)

Introduction

未解決問題とは？

双子素数予想

$p, p+2$ が同時に素数となるものが無限に多く存在する

3, 5, 11, 17, 29, 41, . . . https://oeis.org/A001359

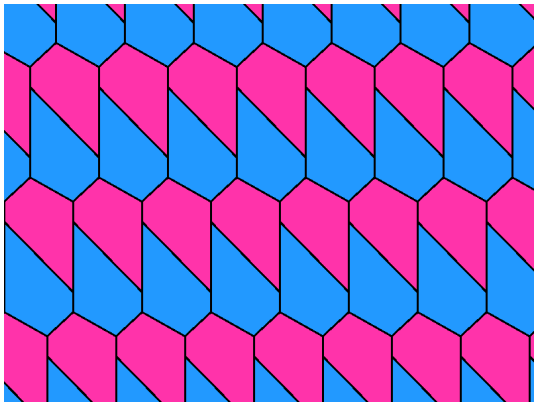
Goldbach 予想

4 以上のすべての偶数は 2 つの素数の和であらわされる

$4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 3 + 7 = 5 + 5, \ldots$

五角形による敷き詰め

一種類の五角形による平面の敷き詰め方をすべて求めよ



最近、解決された例

Fermatの最終定理（Wiles, 1994）

$n \geq 3$ のとき

$$x^n + y^n = z^n$$

となる整数 $xyz \neq 0$ は存在しない

Kepler予想（Hales, 1998-2015）

3次元空間に一種類の球を詰め込んだときの
球の体積の占める平均密度の最大値は$\pi/3\sqrt{2} =$
0.740480489$\cdots$ である

等弦点予想（Rychlik, 1996）

等弦点（その点を通る弦の長さが等しい点）を
複数持つ凸な平面図形は存在しない

素数の等差数列（Green and Tao, 2004）

素数のみからなる任意の長さの等差数列が存在する

$(3, 5, 7), (5, 11, 17, 23, 29), \ldots$

abc予想（Mochizuki, 2012-）

a, b, c を

$$a + b = c$$

となる自然数とし、abc を割り切る素数を1回ずつ掛けた積を r とする。このとき

$$\frac{\log r}{\log c} \to 1 (c \to \infty)$$

が成り立つ。

部分的解決

双子素数予想

PolyMath により急速に解決に近づく

$q - p \leq 246$ となる素数 p, q の組は無限にある（2014-2015）

五角形敷き詰め問題

Rao（2017）が凸五角形による敷き詰めを
すべて分類

Fermat予想は解かれたが…

$$x^a + y^b = z^c$$

についてはどうなるか？

（$a = b = c = 2$ のときはPythagoras triple）

$(2,3,6), (4,4,2)$ が不可能であることは古くから知られている

$(4,2,4)$ はFermat自身が証明、$(4,4,2)$ はEulerが証明、 $(2,3,6)$ は $(3,3,3)$ （Eulerが不完全ながら証明し、その後修正された）と同値

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}<1$$

となる (a,b,c) を決めれば、$\gcd(x,y,z)=1$ となる解は有限個（Darmon and Granville, 1995）

ただし、解の大きさの限界は不明

（なお $\gcd(x,y,z)=1$ に限定しないときは $2^n+2^n=2^{n+1}$, $3^{6n}+(2\times 3^{2n})^3=3^{2(3n+1)}$ などの解がある）

$(n, n, 2)(n \geq 4), (n, n, 3)(n \geq 3)$ については $\gcd(x, y, z) = 1$ となる解はない (Darmon and Merel, 1995)

$$
\begin{aligned}
1^7 + 2^3 &= 3^2, \\
2^7 + 17^3 &= 71^2, \\
17^7 + 76271^3 &= 21063928^2, \\
1414^3 + 2213459^2 &= 65^7, \\
9262^3 + 15312283^2 &= 113^7
\end{aligned}
$$

$(7, 3, 2)$ についてはこの5つしか解がない（Poonen, Schaefer and Stoll, 2005）

Beal予想

$a, b, c \geq 3$ のとき $\gcd(x, y, z) = 1$ となる
解は存在しない

Eulerは

$$x_1^n + x_2^n + \cdots + x_{n-1}^n = y^n$$

は0でない解を持たないと予想した。

しかし

Lander and Parkin 1966:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5,$$

Elkies, 1987-1988:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

一方、 $n \geq 6$ に対してEulerの予想が正しいかは不明！

Fermat予想は解かれたが、
多くの未解決問題が派生

約数の和と完全数

- 6 の約数 $1, 2, 3, 6$

- $1+2+3=6$

- $1+2+3+6=12$

- 28 の約数 $1, 2, 4, 7, 14, 28$
- $1+2+4+7+14=28$
- $1+2+4+7+14+28=56$

完全数

N の約数（N を除く）の和 $= N$

N の約数（N を含む）の和 $= 2N$

$$1 + 2 + 4 = 7$$
$$7 + 14 + 28 = 49$$
$$\sigma(28) = 56$$

$$N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

と分解すると

$$\sigma(p_1^{e_1}) = (p_1^{e_1} + p_1^{e_1-1} + \cdots + p_1 + 1)$$

などから

$$\sigma(N) = \prod_{i=1}^{k} (p_1^{e_1} + p_1^{e_1-1} + \cdots + p_1 + 1)$$

となる。

ここから、次のことが示される

- N が偶数で 2^e でちょうど割り切れるとき $2^{e+1}-1$ で $\sigma(N)$ は割り切れる

- $\sigma(N)$ が奇数ならば N は平方数か平方数の２倍

「神は６日で世界を創造した」（創世記）

偶数の完全数

$$\begin{aligned} N &= 2^{p-1} \quad (2^p - 1) \ , \\ \sigma(N) &= (2^p - 1) \ 2^p \quad = 2N. \end{aligned}$$

約数の和と完全数

$$N = p^e q_1^{2f_1} q_2^{2f_2} \cdots q_k^{2f_k},$$

$$p \equiv e \equiv 1 \pmod 4,$$

- $N > 10^{1500}$ (Ochem and Rao, 2012),
- $k \geq 10$ (Nielsen, 2015),
- P が N の最大の素因数ならば $10^{12}P^2N < 2^{4^{k+1}}$ (Nielsen, 2015)

k倍完全数

$\sigma(N) = kN$

$\sigma(120) = 360 = 3 \times 120$

k倍完全数に関する問題

- $k > 1$ に対し、奇数の k 倍完全数は存在しない？

- 各 $k \geq 3$ に対して k 倍完全数は偶数のものも有限個しか存在しないと予想されている

予想 3倍完全数は120, 672, 523776, 459818240, 1476304896, 51001180160 の6つのみ

4, 5, 6 倍完全数はそれぞれ 36, 65, 245 個知られており、1994年以降新しい例が発見されておらず、すべて発見されたと予想されている

基準約数（1 項約数）

$d \mid_1 N \Leftrightarrow \mathsf{gcd}(d, N/d) = 1$

N が p^e でちょうど割り切れるとき、 d も p^e で割り切れるか、または p で全く割り切れない

$N = \prod_{i=1}^{k} p_i^{e_i}$ の基準約数は

$\prod_{i \in S} p_i^{e_i}, S \subset \{1, 2, \ldots, k\}$ の形のもの

２項約数

$d \mid_2 N \Leftrightarrow \mathsf{gcd}_1(d, N/d) = 1$

これを繰り返すと…無限項約数

$$d \mid_\infty N \Leftrightarrow \mathsf{gcd}_\infty(d, N/d) = 1$$

具体的には

$e = l_s 2^s + l_{s-1} 2^{s-1} + \cdots + l_0, l_i \in \{0, 1\}$
と２進展開すると

$p^f \mid_\infty p^e \Leftrightarrow$
$f = m_s 2^s + m_{s-1} 2^{s-1} + \cdots + m_0,$
$m_i \leq l_i$

基準約数の和

$$\sigma^*(N) = \prod_{i=1}^{k} (p_i^{e_i} + 1)$$

２項約数の和

$$\sigma^*(p^{2f}) = \frac{(p^f - 1)(p^{f+1} + 1)}{p - 1},$$

$$\sigma^*(p^{2f-1}) = \frac{p^{2f} - 1}{p - 1}$$

無限項約数の和

$$\sigma^{(\infty)}(p^e) = \prod_{l_s=1} (p^{2^s} + 1),$$

$$\sigma^{(\infty)}(N) = \prod \sigma^{(\infty)}(p_i^{e_i})$$

基準完全数 $\sigma^*(N) = 2N$

２項完全数 $\sigma^{**}(N) = 2N$

無限項完全数 $\sigma^{(\infty)}(N) = 2N$

奇数の基準完全数、２項完全数、無限項完全数は存在しない！

偶数の基準完全数は $6, 60, 90, 87360, 146361946186458562560000$ が知られている。他に存在するか？

$k \geq 3$ について k 倍基準完全数は一つも知られていない

偶数の２項完全数は $6, 60, 90$ のみ！ (Wall, 1972)

無限項完全数 $6, 60, 90, 36720, 12646368, \ldots$

k 倍2項完全数

$k = 3 : 120, 672, 2160, 10080, \ldots$
$k = 4 : 30240, 1028160, 6168960$

https://oeis.org/A189000

超完全数 $\sigma(\sigma(N)) = 2N$

偶数 $\sigma(2^{p-1}) = 2^p - 1, \sigma(2^p - 1) = 2^p.$
（なお N が偶数ならば必ず $\sigma(\sigma(N)) \geq 2N$
となる）

奇数 平方数でなければならない

k倍超完全数 $\sigma(\sigma(N)) = kN$

（Cohen and te Riele 1996, https://oeis.org/A019278）

$k = 3 : 8, 21, 512$

知られているのは3つのみ、奇数のものが存在する！

https://oeis.org/A019281

$k = 4$: 15, 1023, 29127,
355744082763

2012年に4つ目が発見、奇数のものしか知られていない！

https://oeis.org/A019282

$k = 6 : 42, 84, 160, \ldots$

https://oeis.org/A019283

5倍超完全数は知られていない！

問題 σ を３回以上反復したとき

$$\sigma(\sigma(\ldots\sigma(N)\ldots)) = 2N$$

となる N は存在するか?（N は奇数の平方数でなければならない）

$\sigma(\sigma(\sigma(N))) < 2N$ となる例 $81 \to 121 \to 133 \to 160$

基準超完全数 $\sigma^*(\sigma^*(N)) = 2N$

- 奇数 $9,165$ のみ！ (Yamada, 2008)
- 偶数 $2, 238, 1640, 4320, \ldots$

基準k倍超完全数 $\sigma^*(\sigma^*(N)) = kN$

$k =$ 3 : 10, 30, 288, 660, 720, 2146560
$k =$ 4 : 18

のみ知られている

2項超完全数 $\sigma^{**}(\sigma^{**}(N)) = 2N$

2, 9 のみ！ (Yamada, 2018)

https://oeis.org/hA318175

無限項超完全数 $\sigma^{(\infty)}(\sigma^{(\infty)}(N)) = 2N$

奇数 9 のみ！ (Yamada, 2017) 偶数 2 以外に存在するか？

https://oeis.org/A318182

他にも約数に関する未解決問題は多数！

問題

各整数 $k > 0$ に対して

$$\sigma(n) = \sigma(n+k)$$

となる整数 n は無限に多く存在するか？

$\sigma(14) = \sigma(15) = 24,$
$\sigma(206) = \sigma(207) = 312,$
$\ldots$

10^{13} までに 10135 個存在する

https://oeis.org/A002961

$\sigma(33) = \sigma(35) = 48,$
$\sigma(54) = \sigma(56) = 120,$
$\ldots$

406521768760 までに 10000 個存在する

https://oeis.org/A007373

$\sigma(382) = \sigma(385) = 576,$
$\sigma(8922) = \sigma(8925) = 17856,$
$\ldots$

15902251782 までに 300 個存在する

https://oeis.org/A015861

無限個の解をもつものはあるか？

$k > 1$ で $3k-1, 14k-1$ がともに素数ならば
$n = 28(3k-1), n+22 = 6(14k-1)$ かつ
$\sigma(28(3k-1)) = \sigma(6(14k-1)) = 168k$

このような $k \leq x$ は $cx/\log^2 x$ 個存在する
と予想されている

一方 $k = 15$ のとき

$\sigma(26) = \sigma(41) = 42,$
$\sigma(62) = \sigma(77) = 96,$

の次の例は

$\sigma(20840574) = \sigma(20840589)$
$= 41783040.$

2^{28} までに解は$26, 62, 20840574,$
$25741470, 60765690, 102435795$ の6つ
だけ

格子点配置問題

$n \times n$ の盤上に、どの３つのコマも同一直線状に並ばないように何個までコマを配置できるか？

明らかに$2n$ 個以下。 $2n+1$ 個以上あれば、一列に３個並ぶ列が存在する。

$2n$個配置できる例は？

https://oeis.org/A000769

- $n \leq 46, 48, 50, 52$ について知られている

- $2n$個配置不可能なnは知られていない

配置の個数（回転・鏡像によって移り合うものは一つとして数える）

Hall, 1975: 少なくとも (3/2-o(1))n 個配置できる。p が素数のとき $\mathbb{Z}/p\mathbb{Z}$ 上の双曲線 $xy \equiv k \pmod{p}$ を変形することで $2p \times 2p$ の盤上に $3(p-1)$ 個配置できる。

しかし、充分大きな n については $n \times n$ の盤上に、$2n$ 個配置不可能と予想されている！

予想 (Pegg, Jr. 2005): 最大 $n(\pi/\sqrt{3} + o(1))$ 個なお $\pi/\sqrt{3} = 1.81379...$

問題

トーラス $(\mathbb{Z}/n\mathbb{Z})^2$ 上で考えるとどうなるか？

トーラスでは２直線が平行である場合と平行でない場合がある

そこで、トーラスに点を付け加えて、すべての直線が１点で交わるようにする

- $q = p^e$: 素数冪
- $\mathbb{F}_q$: 位数 q の有限体
- $q = p$ のときは $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

PG(r, q) $\mathbb{F}_q$ 上の r 次元射影空間

- $(x_0 : x_1 : \ldots : x_r), x_i \in \mathbb{F}_q$,
- $(x_0 : x_1 : \ldots : x_r)$ と $(kx_0 : kx_1 : \ldots : kx_r)$ を同一視する

PG$(2, q)$ 上では、

- 任意の２直線はちょうど１点で交わる
- 任意の直線は $q + 1$ 個の点をもつ
- ある点を通る直線は、どの点であっても
  ちょうど $q + 1$ 本ある

なお、このような性質をもつ空間が q が素数冪である場合以外に存在するかどうかも未解決！

（q が素数冪で、このような性質を持つ空間で $\mathrm{PG}(2,q)$ とは異なる構造をもつものは存在する）

PG(2,3) は
(1 : 0 : 0),
(0 : 1 : 0), (1 : 1 : 0), (1 : 2 : 0),
(0 : 0 : 1), (1 : 0 : 1); (2 : 0 : 1),
(0 : 1 : 1), (1 : 1 : 1), (2 : 1 : 1),
(0 : 2 : 1), (1 : 2 : 1), (2 : 2 : 1)
の13点からなる。

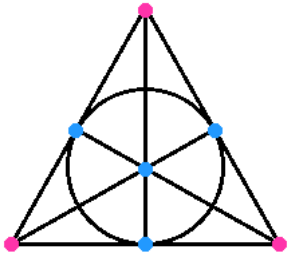
有限射影平面の点の個数

$$|\mathrm{PG}(2,q)| = \frac{q^3-1}{q-1} = q^2+q+1$$

実際 $(1:x_1:x_2)(x_1,x_2 \in \mathbb{F}_q)$,
$(0:1:x_3)(x_3 \in \mathbb{F}_q)$ および $(0:0:1)$
の q^2+q+1 点からなる。

問題

S を PG$(2,q)$ の部分集合で、どの３点も同一直線上に属さないとする。このとき $|S|$ の最大値は？



S 上の点 P を一つ取ると、この点 P を通る直線は $q+1$ 個ある。これらの各直線について、P 以外の S 上の点は高々1個しか通らない。

よって $|S| \leq q+2$

Bose, 1947: q が偶数のとき $q+2$ 個、 q が奇数のとき $q+1$ 個

$q+1$ 個のものを oval、$q+2$ 個のものを hyperoval という。

Segre, 1955a: q が奇数のとき、S が oval である必要十分条件は S が既約二次曲線であること。

q が偶数のとき既約二次曲線に１点を付け加えたものはhyperovalとなる。

Segre, 1957: $q = 2, 4, 8$ のときhyperovalはこの構造のもののみ。

$q = 2^e, e \geq 4$ のときこれとは別構造の hyperoval が存在するが、完全にはわかっていない。

高次元への一般化

k-arc: $\mathrm{PG}(r,q)$ 上の k 個の点集合で、どの $r+1$ 点をとっても、一つの $r-1$ 次元超平面に属さない

言い換えると… $r+1$ 個の点 $P_1, P_2, \ldots, P_{r+1}$ をとったときベクトル $\overrightarrow{P_k P_{r+1}} (k = 1, 2, \ldots, r)$ が線型独立

$k(r,q)$ を PG(r,q) 上の k-arc の存在する最大の k とする。

予想（Hirschfeld and Storme, 2001 より）

a) $N \geq q-1$ のとき $k(r,q) = N+2$,
b) q が偶数のとき $k(2,q) = k(q-2,q) = q+2$,
c) それ以外のとき $k(2,q) = k(q-2,q) = q+1$

Segre 1955b:

a) $q > r + 1$ のとき $k(r, q) \geq q + 1$: 実際、有理曲線 $(1 : t : t^2 : \ldots : t^r)(t \in PG(1, q))$ は $(q + 1)$-arc

b) $q \geq 5$ が奇数のとき $k(3, q) = q + 1$, $q \geq 7$ が奇数のとき $k(4, q) = q + 1$

c) $q > r + 1$ が奇数で $r \geq 4$ のとき $k(r, q) \leq q + r - 3 (r \geq 4)$

Casse 1969: $q = 2^e, e \geq 2$ のとき $k(3, q) = q+1$, $q = 2^e, e \geq 3$ のとき $k(4, q) = q+1$

Kaneta and Maruta 1989:

- $q > (4r - 5)^2$ が奇数のとき $k(r, q) = q + 1$

- PG(N, q) における $q + 1$-arc がすべて有理曲線ならば $k(N + 1, q) = q + 1$

後者の結果と Voloch 1990 から p が奇素数で $p > 45r - 140$ ならば $m(r, p) = p + 1$

m-cap: PG(r, q) 上のm 個の点集合で、どの3点も同一直線に属さない。

$m(r, q)$: PG(r, q) 上の m-cap が存在する最大の m

Bose 1947, Qvist 1952: $m(3,q) \leq q^2+1$

PG$(3,q)(q>2)$ における q^2+1-cap を ovoid という。

Barlotti 1955, Panella 1955: q が奇数のとき ovoid は 2次曲面

Hirschfeld 1983: $q > 11^2$ が奇数で $n \geq 4$ のとき

$$m(n,q) < q^{n-1} - (1/4)q^{n-3/2} + 3q^{n-2}.$$

Chao 1999: $q = 2^e$ のとき $m(4,q) \leq q^3 - q^2 + 6q - 3$, $q = 2^e, e \geq 3, n \geq 5$ のとき

$$\begin{aligned} m(n,q) \leq & q^{n-1} - q^{n-2} + 6q^{n-3} - 4q^{n-4} \\ & - 2(q^{n-5} + \cdots + q + 1) + 1. \end{aligned}$$

別の一般化

直線や超平面から、２次曲線などに拡張できないか？

- PG(2, $\overline{\mathbb{F}}_p$) において２つの２次曲線は必ず（重複も含めて）４点で交わる

- ある５点が、どの３点も同一直線上になければ、それらの５点を通る２次曲線がちょうど１つ存在する

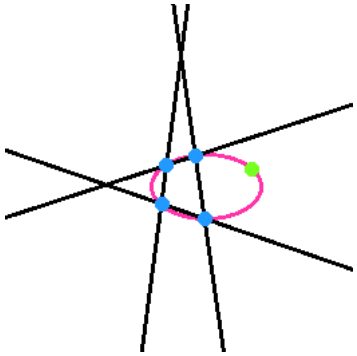
問題

PG$(2,q)$ において、どの６点も同じ２次曲線上にない点の集合 S の中で、点の個数 $|S|$ が最大となるものを求めよ。

既約な２次曲線に限定するか、可約な２次曲線（２つの直線の和集合になっている）も含めるか？

既約な２次曲線に限定した場合（最大の個数を $k^{+}(2,2,q)$ とおく）

２直線上の点全体と、その２直線の外にある点１つからなる集合をとれば、$|S| = 2q+2$ となるものがとれる



$2q + 2 \leq k^{+}(2, 2, q) \leq 2q + 24$ (Y., 2018).

可約な２次曲線を含めた場合は？（最大の個数を $k^{-}(2,2,q)$ とおく）

強欲算法で $cq^{1/5}(c>0)$ 個の点からなる、どの６点も同じ２次曲線（可約なものも含む）上にない点の集合が構成できる。

$cq^{1/5} < k^{-}(2,2,q) \leq q + 5$ (Y., 2018).

$k^{-}(2,2,q) > cq$ となる定数 $c > 0$ が存在するかも不明

MANY THANKS
FOR YOUR ATTENTION

Tomohiro Yamada
CJLC,
Osaka University, Japan
e-mail: tyamada1093@gmail.com