$x^2 + y^2 = z^2$の拡張

01—諸言

$x^2 + y^2 = z^2$の非負整数解(x, y, z)は無限に存在することが知られている。しかし、

$x^2 + 5y^2 + 2z^2$の非負整数解は$(0, 0, 0)$(以下:自明解)のみである。

そこで、$x^2 + y^2 = z^2$に自然数の係数(a, b, c)をつけた$ax^2 + by^2 = cz^2$の非整数解(x, y, z)が無限に存在する条件、及び有限に存在する場合、自明解のみである条件と自明解以外の解(以下:非自明解)が存在する(a, b, c)の条件について考えた。

なお、非負整数解(x, y, z)のうち共通な約数を持たない組のみを考える。

02—方法

1. a, b, cが1でない平方数のときを考えた。
2. $b = c = 1$と固定して、aの値のみを変えて考えた。
3. $a = b = 1$と固定して、cの値のみを変えて考えた。
4. 文字の値を2種類以上変えたときについて考えた。

03—結果

1. まず、aが平方数のときについて考える。

   $a = {a_0}^2$(aは自然数)のとき

   $ax^2 + by^2 = cz^2$に代入して、$(a_0 x)^2 + by^2 = cz^2$

   $(a_0 x)^2$を平方数と考えることで、$x^2 + by^2 = cz^2$の形に帰着することができる。

   例えば、$4x^2 + y^2 = z^2$について、$(2x)^2 + y^2 = z^2$と変形でき、$x^2 + y^2 = z^2$の形に帰着するので、$4x^2 + y^2 = z^2$の非負整数解は無限に存在する。

   また、b, cが平方数の場合も同様に、文字が少ない形に帰着できる。

2. まず、$a = 2$のときについて考える。

   このとき、$x = 2mn, y = |2m^2 - n^2|, z = 2m^2 + n^2$と非負整数$m, n$を用いて表せることを示す。

   (証明)

   $2x^2 + y^2 = z^2$を変形して、$2x^2 = (z - y)(z + y)$

   $p = z - y$, $q = z + y$とすると、$2x^2 = pq$…(1)で、y, zはp, qを用いて、$y = \frac{q+p}{2}$,

   $z = \frac{q+p}{2}$ …(∗)と表せる。

   ここで、y, zは非負整数なので、$q + p$, $q - p$は偶数で、これはp, qの偶奇が一致することと同値である。

   また、(1)の左辺が偶数なので、pqも偶数である。

   よって、p, qは偶数なので、$p = 2p_0, q = 2q_0$(p_0, q_0は非負整数)と表せる。

(1)に代入して、$x^2 = 2p_0q_0$ …(2)

右辺が偶数なので、x^2も偶数である。

x^2が偶数であることとxが偶数であることは同値なので、$x = 2x_0$ (x_0は非負整数)と表せる。

(2)に代入して、${x_0}^2 = \frac{p_0q_0}{2}$…(3)

よって、p_0, q_0のうち、一方は平方数、もう一方は(平方数)× 2

(ⅰ) $p_0 = 2m^2, q = n^2$と表すとき(m, nは非負整数)

(3)に代入して、${x_0}^2 = m^2n^2$

$x_0 > 0$より、$x_0 = mn$

よって、$x = 2x_0 = 2mn$

また、(∗)より、$y = n^2 - 2m^2, z = 2m^2 + n^2$

(ⅱ) $p_0 = n^2, q = 2m^2$と表すとき(m, nは非負整数)

(a)と同様にして、$x = 2mn$

(∗)より、$y = 2m^2 - n^2, z = 2m^2 + n^2$

(ⅰ),(ⅱ)より、$x = 2mn, y = |2m^2 - n^2|, z = 2m^2 + n^2$ **(証明終)**

ここで、一般のaについても同様に$x = 2mn, y = |am^2 - n^2|, z = am^2 + n^2$と
表されると考えた。

実際、代入すると

$$
\begin{aligned}
&ax^2 + y^2 \\
&= a(2mn)^2 + (am^2 - n^2)^2 \\
&= 4am^2n^2 + a^2m^4 - 2am^2n^2 + n^2 \\
&= a^2m^4 + 2am^2n^2 + n^4 \\
&= (am^2 + n^2)^2 \\
&= z^2
\end{aligned}
$$

となるので、$x = 2mn, y = |am^2 - n^2|, z = am^2 + n^2$は、$ax^2 + y^2 = z^2$の非負整数解である。

3.導入:フェルマーの二平方和定理

2つの整数x, yを用いて$n = x^2 + y^2$と表せる

⇔nを素因数分解したとき、$4k + 3$型の素因数の指数は全て偶数

ここでnをcz^2とすると、z^2の素因数の指数は全て偶数なので、cz^2の素因数の指数の偶奇はcによって決まる。
よって、上の定理の対偶から、cの素因数で$4k+3$型かつその指数が奇数のものが1つでも存在するとき、cz^2は2つの平方数の和で表せないので、解は自明解のみである。
続いてそれ以外のcについて考える。

(ⅰ)cが平方数のとき
1. の通り解は無数に存在する

(ⅱ)cが平方数でないとき
ペル方程式を用いて考える。

導入:ペル方程式
cが平方数でないとき、方程式
$x^2-cy^2=1$
を満たす自然数の組(x,y)は無限に存在する。

ここで、s,tを$s^2-ct^2=1$を満たす自然数、(x_0,y_0,z_0)を$x^2+y^2=cz^2$の非自明解の一つとする。
式$(x_0s+cz_0t)^2-c(x_0t+z_0s)^2$を変形すると
$(x_0s+cz_0t)^2-c(x_0t+z_0s)^2$
$=(x_0^2-c_0^2)(s^2-ct^2)$
$=-y_0$ $(\because x_0^2-cz^2=-y^2, s^2-ct^2=1)$
このことから、$x_1=x_0s+cz_0t, z_1=x_0t-z_0s$とすると、上の式は$x_1^2-cz_1^2=-y_0$となり、数の組$(x_1,y_0,z_1)$は$x^2+y^2=cz^2$の$(x_0,y_0,z_0)$とは異なる新たな非自明解である。
非自明解の一つ(x_0,y_0,z_0)はフェルマーの二平方和定理を用いて見つけられるため、非自明解が1つでも存在すれば解は無限に存在することがわかった。

4.文字の値を2つ以上動かしたときについて考える。
$3x^2+3y^2=z^2$を例に取る。
この式の両辺を3倍して変形すると、$(3x)^2+(3y)^2=3z^2$
よって、$x^2+y^2=3z^2$の形に帰着するので、3)より、$3x^2+3y^2=z^2$の非負整数解は自明解のみである。

(1)$c=1$のとき、すなわち、$ax^2+by^2=z^2$のとき
(1-a)$a=b$のとき

$ax^2 + ay^2 = z^2$

$(ax)^2 + (ay)^2 = az^2$

これは、$x^2 + y^2 = cz^2$の形に帰着するので、3)より、aが$4k + 3$型かつその指数が奇数の素因数を1つでももつとき、解は自明解のみ。そうでない場合、解は無限に存在する。

(1-b)$a \neq b$のとき

$ax^2 + by^2 = z^2$

$abx^2 + (by)^2 = bz^2$

これは、$ax^2 + y^2 = cz^2$の形に帰着するが、一般的な自然数a,cについて、この形での解の規則性は見つけることができなかった。

(2)$c \neq 1$のとき

$ax^2 + by^2 = cz^2$

$abx^2 + (by)^2 = bcz^2$

これも$ax^2 + y^2 = cz^2$の形に帰着する。

よって、$ax^2 + y^2 = cz^2$の形を調べれば、すべての(a, b, c)について、解の規則性を調べることができることがわかった。

04—考察

2.および3.について、必要 十分性のある議論まで至れず、非負整数解をすべて数え上げているかまではわからなかった。

$ax^2 + y^2 = cz^2$のときに、(a, c)の値によって、非負整数解が無限に存在するのか、有限だとしたら、自明解のみか、非自明解も存在するのか規則性を掴むことができなかった。

05—結論

- 文字一つのみを動かした際に、解が無限に存在するか、あるいは自明解(0,0,0)のみになるのかという条件がわかった。
- 文字2つ以上を動かして考えるときに関して、変形を施すことでより簡単なパターンに帰着して考えることができた。
- しかし、上2つの結論において必要十分性のある議論ができず、非負整数解をすべて数え上げることはできなかった。

06—参考文献

「はじめての数論」ジョセフ・H・シルヴァーマン著 / 鈴木治郎訳

高校数学の美しい物語 https://manabitimes.jp/math

07—謝辞

本研究および発表にご指導を賜りました、深井先生、伊藤先生、石橋先生に感謝を申し上げます。

$\frac{1}{p^n}$の循環節の長さについての考察

1. 緒言

循環節の長さとは, ある分数を10進数表記したときの, 小数の循環の桁数を指す. この循環節の長さについて考察した. なお, ある既約分数が循環小数であるための必要十分条件は, 分母の素因数に2, 5以外の素数を含むことである. また, 今回扱うのは$\frac{k}{p^n}$型の既約分数であるから, pは2, 5以外の素数, kはpと互いに素な正整数, nは自然数とする.

2. 実験手順

以下, $\frac{1}{k}$の循環節の長さを$l(k)$と表記することにする.

$\frac{1}{p}, \frac{2}{p}, \frac{3}{p}, \ldots\ldots, \frac{p-1}{p}$の10進数表記において, 循環節の数字の並びが同じものを1つのグループとし, 異なるグループの数をpのグループ数と呼ぶことにする. 例えば, $p = 13$のとき, 循環節は$076923, 153846$の2種類がある. このとき$p(= 13)$のグループ数は 2である.

$l(p)$と$l(p^n)$にまつわる以下の4つの補題を証明することで$l(p^n) = l(p) \times p^{n-1}$を示した.

補題1. $a \equiv b(mod\ p) \Rightarrow a^{p^{n-1}} \equiv b^{p^{n-1}} (mod\ p^n)$

補題2. $l(p) \times A = (p - 1), l(p^n) \times B = (p - 1)p^{n-1}$となる自然数$A, B$が存在する.

補題3. AとBはそれぞれpとp^nのグループ数に一致する.

補題4. pとp^nのグループ数は一致する.

3. 実験結果

補題1. $a \equiv b(mod\ p) \Rightarrow a^{p^{n-1}} \equiv b^{p^{n-1}} (mod\ p^n)$

$a \equiv b(mod\ p)$の時, $a = pk + b$ (kは整数)とする. そのとき,

$a^{p^{n-1}} - b^{p^{n-1}} = (pk + b)^{p^{n-1}} - b^{p^{n-1}}$

二項定理によって展開すると

$(pk + b)^{p^{n-1}} - b^{p^{n-1}}$

$= \{(pk)^{p^{n-1}} + {}_{p^{n-1}}C_1 (pk)^{p^{n-1}} \cdot b + \cdots + {}_{p^{n-1}}C_{p^{n-1}-1} (pk) \cdot b^{p^{n-1}} + b^{p^n - 1}\} - b^{p^{n-1}}$

$= (pk)^{p^{n-1}} + {}_{p^{n-1}}C_1 (pk)^{p^{n-1}} \cdot b + \cdots + {}_{p^{n-1}}C_{p^{n-1}-1} (pk) \cdot b^{p^{n-1}}$

右辺の全ての項にp^nが含まれるため

$a^{p^{n-1}} - b^{p^{n-1}} \equiv 0(mod\ p^n)$

補題2. $l(p) \times A = (p-1), l(p^n) \times B = (p-1)p^{n-1}$となる自然数$A, B$が存在する.

[Ⅰ] $l(p) \times A = (p-1)$となる自然数Aが存在することを示す.

$\frac{1}{p} = 0.a_1a_2a_3a_4\cdots\cdots a_{l(p)}a_1a_2a_3a_4\cdots\cdots a_{l(p)}\cdots$ ・・・①

(a_1,a_2,a_3,a_4,……,a_p,……,$a_{l(p)}$は0以上9以下の整数) となる. 両辺$10^{l(p)}$倍して,

$\frac{10^{l(p)}}{p} = a_1a_2a_3a_4\cdots\cdots a_{l(p)}.a_1a_2a_3a_4\cdots\cdots a_{l(p)}\cdots$ ・・・②

①,②より,

$\frac{10^{l(p)}-1}{p} = a_1a_2a_3a_4\cdots\cdots a_{l(p)} \in \mathbb{N}$

右辺は自然数であるから, 左辺も自然数となる.

したがって, $10^{l(p)} - 1 \equiv 0(mod\ p) \Leftrightarrow 10^{l(p)} \equiv 1(mod\ p)$ ・・・③

フェルマーの小定理より,

$10^{p-1} \equiv 1(mod\ p)$ ・・・④

③,④より, $10^{l(p)} \equiv 10^{p-1} \equiv 1(mod\ p)$

ここで$l(p)$が$p-1$の約数でないとすると

$p - 1 = l(p) \times A + r(1 \le r \le l(p) - 1)$ と表せるので,

$10^{l(p)} \equiv 10^{l(p)\times A+r} \equiv 1(mod\ p)$

③より$10^{l(p)} \equiv 1\ (mod\ p)$ であるため, $10^{l(p)\times A} \equiv 1^A \equiv 1\ (mod\ p)$

つまり, $10^{l(p)\times A} \equiv 10^{l(p)\times A+r}(mod\ p)$

ここでpと10は互いに素なので$10^{l(p)\times A}$で割ることができ, $1 \equiv 10^r\ (mod\ p)$が得られる.

rは$1 \le r \le l(p) - 1$ を満たしているため, これは$\frac{1}{p}$の循環節の長さである$l(p)$より小さいrで循環することになり矛盾する.

よって, $l(p)$は$p-1$の約数である.

ゆえに, $l(p) \times A = (p-1)$となる自然数Aが存在する.

[Ⅱ] $l(p^n) \times B = (p-1)p^{n-1}$となる自然数$B$が存在することを示す.

$\frac{1}{p^n} = 0.a_1a_2a_3a_4\cdots\cdots a_{l(p^n)}a_1a_2a_3a_4\cdots\cdots a_{l(p^n)}\cdots$ ・・・①

(a_1,a_2,a_3,a_4,……,$a_{l(p^n)}$は0以上9以下の整数) となる.

両辺$10^{l(p^n)}$倍して,

$\frac{10^{l(p^n)}}{p^n} = a_1a_2a_3a_4\cdots\cdots a_{l(p^n)}.a_1a_2a_3a_4\cdots\cdots a_{l(p^n)}\ldots$ ・・・②

①,②より,

$\frac{10^{l(p^n)}-1}{p^n} = a_1a_2a_3a_4\cdots\cdots a_{l(p^n)}$

右辺は自然数であるから, 左辺も自然数となる.

したがって,

$10^{l(p^n)} - 1 \equiv 0(mod\ p^n) \Leftrightarrow 10^{l(p^n)} \equiv 1(mod\ p^n)$ ・・・③

一方フェルマーの小定理から

$10^{p-1} \equiv 1 (mod\ p)$ ・・・④
④と補題1より,
$1^{p^{n-1}} \equiv (10^{(p-1)})^{p^{n-1}} \ (mod\ p^n)$
$1 \equiv 10^{(p-1)\times p^{n-1}} \ (mod\ p^n)$ ・・・⑤
③⑤から
$10^{l(p^n)} \equiv 10^{(p-1)\times p^{n-1}} \ (mod\ p^n)$
ここで$l(p^n)$が$(p-1)\times p^{n-1}$の約数でないとすると
$(p-1)\times p^{n-1} = B \times l(p^n) + R (1 \le R \le l(p^n) - 1)$と表せるので
$10^{l(p^n)} \equiv 10^{B\times l(p^n)+R} \ (mod\ p^n)$
ここで③より$10^{l(p^n)} \equiv 1 (mod\ p^n)$なので
$10^{l(p^n)\times B} \equiv 1^B \equiv 1 \ (mod\ p^n)$
よって
$10^{l(p^n)\times B} \equiv 10^{B\times l(p^n)+R} \ (mod\ p^n)$
10とpは互いに素だから両辺$10^{l(p^n)\times B}$で割ることができ, $1 \equiv 10^R (mod\ p^n)$が得られる.
Rは$1 \le R \le l(p^n) - 1$を満たしているため, これは$\frac{1}{p^n}$の循環節の長さである$l(p^n)$より小さいRで循環することになり矛盾する.
よって, $l(p^n)$は$(p-1)\times p^{n-1}$の約数である.
ゆえに, $l(p^n) \times B = (p-1)\times p^{n-1}$となる自然数$B$が存在する.

補題3. AとBはそれぞれpとp^nのグループ数に一致する.

$\frac{1}{p}, \frac{2}{p}, \frac{3}{p}, \ldots, \frac{p-1}{p}$の循環の中身が数珠状になっていることを説明する.
$\frac{1}{p}$の筆算の余りの部分に注目すると, 一定の周期で循環していることがわかる.(補題4参照)
次に, $\frac{k}{p}$(kはpと互いに素な1以上$p-1$以下の整数)の筆算を思い浮かべる.
その筆算の小数第一位の余りが$\frac{1}{p}$の筆算のどれかの余りと等しくなっていることがある. 等しくなっているとき, 余りの羅列が同じになっている.
そして, それは$\frac{1}{p}$と$\frac{k}{p}$の循環の中身の羅列が等しくなっている.
仮に, その筆算の小数第一位の余りが$\frac{1}{p}$の筆算のどれかの余りと等しくなっていないならば, それは別のグループ(下に定義が書かれている)に属しているということである.
これからはこの事実を既知のものとする.

グループ数というものを定義する.
$\frac{1}{p}, \frac{2}{p}, \frac{3}{p}, \ldots, \frac{p-1}{p}$を10進数表記の小数に直す.
循環の中身が同じものを1グループとしたときのグループの数を**pのグループ数**と呼ぶ.

例として，$p = 13$のときを考え，小数の循環部分を抜き出すと次のようになる．

$\frac{1}{13}: 076923$ $\frac{2}{13}: 153846$ $\frac{3}{13}: 230769$ $\frac{4}{13}: 307692$ $\frac{5}{13}: 384615$ $\frac{6}{13}: 461538$ $\frac{7}{13}: 538461$

$\frac{8}{13}: 615384$ $\frac{9}{13}: 692307$ $\frac{10}{13}: 769230$ $\frac{11}{13}: 846153$ $\frac{12}{13}: 923076$

これらをグループに分ける．

$\frac{1}{13}: 076923$ $\frac{3}{13}: 230769$ $\frac{4}{13}: 307692$ $\frac{9}{13}: 692307$ $\frac{10}{13}: 769230$ $\frac{12}{13}: 923076$ …グループ①

$\frac{2}{13}: 153846$ $\frac{5}{13}: 384615$ $\frac{6}{13}: 461538$ $\frac{7}{13}: 538461$ $\frac{8}{13}: 615384$ $\frac{11}{13}: 846153$ …グループ②

以上より，13のグループ数は2である．

補題2より導かれた$l(p) \times A = (p - 1)$のAに意味づけをする．

例えば，$p = 13$のとき，$l(p) = 6$である．よって，$A = 2$とわかる．

また，上の例から，13のグループ数は2である．

これを一般の素数pについて考えると$\frac{1}{p}, \frac{2}{p}, \frac{3}{p}, \ldots, \frac{p-1}{p}$の循環節の長さは等しく$l(p)$であり，同じグループの循環の中身は順序が同じであるから，ひとつのグループに属する要素数は$l(p)$である．

また，$\frac{1}{p}, \frac{2}{p}, \frac{3}{p}, \ldots, \frac{p-1}{p}$の分数の個数は$p - 1$個だから，$\frac{p-1}{l(p)}$は$p$のグループ数であり，それは$A$に一致する．

次に，補題2より導かれた$l(p^n) \times B = (p - 1)p^{n-1}$の$B$に意味づけをする．$\frac{1}{p^n}, \frac{2}{p^n}, \frac{3}{p^n}, \ldots, \frac{p^n-1}{p^n}$の分数の個数は分子は$p$と互いに素であるため，$(p - 1)p^{n-1}$個となる．

また，$\frac{1}{p^n}, \frac{2}{p^n}, \frac{3}{p^n}, \ldots, \frac{p^n-1}{p^n}$のうち，分子が$p$と互いに素である循環節の長さは等しく$l(p^n)$であるから（補足参照），$\frac{(p-1)p^{n-1}}{l(p^n)}$は$p^n$のグループ数であり，それは$B$に一致する．

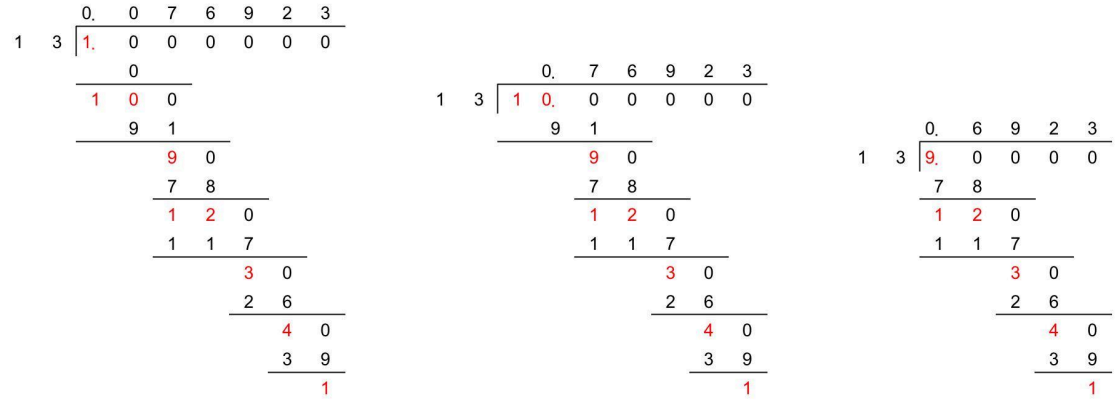
補題4．pとp^nのグループ数は一致する．

例として$p = 13$で考える．

$\frac{1}{13} = 0.076923, \frac{10}{13} = 0.769230, \frac{9}{13} = 0.692307$となることから，$\frac{1}{13}, \frac{10}{13}, \frac{9}{13}$は同じグループに属することがわかる．

これは$1 \div 13$を筆算で表したときに余りの部分に10が出てくることに由来する．（下図参照）

図. 1÷13の筆算について
赤色で示した数が1÷13の余り. 確かに余りを辿ることで同じグループにある分数を見つけられる.



$1 \div 13$の余りを辿っていけば, $\frac{1}{13}$と同じグループに属する, 分母が13の分数が一意的に得られる.

$\frac{1}{13^2} = \frac{1}{169}$でも同様に考えると, $\frac{1}{169}$と同じグループに属する, 分母が169の分数が一意的に得られる.

ここで, ある分数$\frac{q}{p}$を筆算で計算したときに一意的に得られる, 同じグループに属する分数列($\frac{1}{13}, \frac{10}{13}, \frac{9}{13}$のようなもの)をまとめて$\frac{q}{p}$から始まるグループと呼び, $\left\{\frac{q}{p}\right\}$と表記することにする.

また, この余りは$1 \times 10^0 \equiv 1(mod\ 13)$, $1 \times 10^1 \equiv 10(mod\ 13)$, $1 \times 10^2 \equiv 9(mod\ 13)$と計算できることが筆算の性質からわかる.

$k \times 10^x \equiv y(mod\ p)$, $k \times 10^x \equiv y'(mod\ p^n)$とする.

$k \times 10^x \equiv y'(mod\ p)$でもあるため, $y \equiv y'(mod\ p)$が示された. ･･･①

分母は同じ素数の累乗であり, かつ等しい分子を持つ分数($\frac{1}{13}$と$\frac{1}{169}$のようなもの)を考える.

①は, これらの分数から始まるそれぞれのグループにおいて, 第k項の分子同士が分母の素数を法として合同であることを示している.

13を例に考えると$\left\{\frac{1}{13}\right\}$の第3項である$\frac{9}{13}$と$\left\{\frac{1}{169}\right\}$の第3項である$\frac{100}{169}$について確かにそれぞれの分子同士が13を法にして合同になっている. $\because 9 \equiv 100(mod\ 13)$

このことから$\left\{\frac{1}{13}\right\}$と$\left\{\frac{1}{169}\right\}$, $\left\{\frac{2}{13}\right\}$と$\left\{\frac{2}{169}\right\}$といった, 分母は同じ素数の累乗であり, かつ等しい分子をもつ分数から始まるそれぞれのグループ同士が1対1に対応することがわかる.

また, $\left\{\frac{14}{13}\right\}$と$\left\{\frac{14}{169}\right\}$は対応しており, $\frac{14}{13} = 1\frac{1}{13}$であるため, $\left\{\frac{14}{169}\right\}$は$\left\{\frac{1}{13}\right\}$に対応する.

よって, pのグループ数とp^nのグループ数は一致することが示された.

まとめ

補題2より$l(p) \times A = (p-1), l(p^n) \times B = (p-1)p^{n-1}$が示され, 補題3, 4より$A = B$が示された.

$A = \frac{p-1}{l(p)}$, $B = \frac{(p-1)p^{n-1}}{l(p^n)}$より$\frac{p-1}{l(p)} = \frac{(p-1)p^{n-1}}{l(p^n)} \Leftrightarrow l(p^n) = (p-1)p^{n-1}$.

よって, 示された.

補足. $\frac{1}{p}$と$\frac{k}{p}$(kはpと互いに素な1以上$p-1$以下の整数)の循環節の長さは等しい

kがpの倍数のときpで約分することで, 分母の次数が下がってしまうため, kはpと互いに素であるとして考える.

$$\frac{1}{p} = 0.a_1a_2a_3\cdots\cdots a_sa_1a_2a_3\cdots\cdots a_s\cdots\cdots$$

$$\frac{k}{p} = 0.b_1b_2b_3\cdots\cdots b_tb_1b_2b_3\cdots\cdots b_t\cdots\cdots$$

とおくと, $\frac{1}{p}$の循環節の長さはs, $\frac{k}{p}$の循環節の長さはtである.

また, $\frac{k}{p}$を10進法で筆算したときの小数第x位の余りをyとおくと,

$$k \times 10^x \equiv y(mod\ p)$$

が成り立つ.（補題4参照）

これを用いると, 筆算の余りの部分を数式で記述できる. pを法として,

$1 \times 10^1 \equiv y_1$, $1 \times 10^2 \equiv y_2$, $1 \times 10^3 \equiv y_3$, …… , $1 \times 10^s \equiv y_s$…①

$k \times 10^1 \equiv y'_1$, $k \times 10^2 \equiv y'_2$, $k \times 10^3 \equiv y'_3$, …… , $k \times 10^t \equiv y'_t$…②

とおけば, a_mとy_m, b_mとy'_m(mは1以上s, t以下の整数)はそれぞれ1対1に対応している.

①の式の両辺をk倍すると,

$k \times 10^1 \equiv ky_1$, $k \times 10^2 \equiv ky_2$, $k \times 10^3 \equiv ky_3$, …… , $k \times 10^s \equiv ky_s$となる.

ここで, pを法として,

$ky_1 \equiv z_1$, $ky_2 \equiv z_2$, $ky_3 \equiv z_3$, …… , $ky_s \equiv z_s$

とおけば, y_mとz_m(mは1以上s, t以下の整数)はそれぞれ1対1に対応している.

ところで, $y'_1 = z_1$, $y'_2 = z_2$, $y'_3 = z_3$, ……であるから, 対応関係を考えると, $s = t$でないと矛盾が生じる. 以上から, $\frac{1}{p}$と$\frac{k}{p}$(kはpの倍数でない)の循環節の長さが等しい.

$\frac{1}{p^n}$と$\frac{k}{p^n}$(nは2以上の正整数, kはpと互いに素な1以上$p^n - 1$以下の整数)についても同様にして循環節の長さが同じになることが証明できる.

4. 考察

$l(p^n) = l(p) \times p^{n-1}$と表せることが示された.

しかし, $p = 3,487$のとき成り立たないことが計算によって明らかになった.

$p = 3,487$ はどちらも$10^{3-1} \equiv 1(mod\ 3^2)$, $10^{487-1} \equiv 1(mod\ 487^2)$を満たしているため

$10^{p-1} \equiv 1(mod p^2)$を満たす$p$が反例だと予想できた.

この反例が生まれた原因は補題4にあると考えている.

$\left\{\frac{kp+k'}{p}\right\}$と$\left\{\frac{kp+k'}{p^n}\right\}$は確かに対応しているため, $\left\{\frac{k'}{p}\right\}$と$\left\{\frac{kp+k'}{p^n}\right\}$も対応しているが, $\left\{\frac{k'}{p^n}\right\}$と$\left\{\frac{kp+k'}{p^n}\right\}$ は同じグループにあるとは言い切れないのではないかと予想している.

$p = 13$を例に考えると, $\left\{\frac{14}{13}\right\}$と$\left\{\frac{14}{169}\right\}$は確かに対応しているため, $\left\{\frac{1}{13}\right\}$と$\left\{\frac{14}{169}\right\}$も対応しているが, $\left\{\frac{1}{169}\right\}$と$\left\{\frac{14}{169}\right\}$は同じグループにあるとは言い切れないのではないかということだ.

また, $10^{p-1} \equiv 1(mod p^2)$を満たす$p$については$\left\{\frac{k'}{p^n}\right\}$と$\left\{\frac{kp+k'}{p^n}\right\}$ が同じグループにないことは示せたが, 逆は示せていない.

また, $l(p^n) = l(p) \times p^{n-1}$とオイラー関数についての式$\varphi(p^n) = (p-1) \times p^{n-1}$が酷似していることから, これらの関連性が推測された.

5. 結論

素数p, 自然数nについて$l(p^n) = l(p) \times p^{n-1}$が成り立つことが示されたが, すべての素数について成り立つわけではなく, 反例が存在することが分かった.

6. 参考文献

西来路文朗, 清水 健一　素数はめぐる 循環小数で語る数論の世界 ブルーバックス 2017年2月25日 240ページ

7. 謝辞

ご指導を賜りました町頭教授, 深井先生, 伊藤先生, 石橋先生, 心より感謝申し上げます.

縮小盤オセロの必勝法と必敗法

大阪府立大手前高等学校　オセロ班

概要：オセロは終局まで厳密な先読みが可能なゲームである．先行研究［1］［2］はいくつかの縮小盤オセロについて，探索アルゴリズムを用いて必勝法が先手後手どちらにあるのかを明らかにした．本稿では，３つの縮小盤（4×4，4×6，4×8 盤）について完全解析を行った．また，必勝法と必敗法の両方をデータとして保存した．それらのデータを比較し，必勝法よりも，必敗法の手順の方が複雑であると結論づけた．

1. はじめに

オセロは数学的に厳密な先読みが可能である二人零和有限確定完全情報ゲームに分類される．先行研究［1］［2］によって，以下表１の６種類のオセロについて「先手必勝」「後手必勝」「引き分け（必勝法なし）」のどれに属するかが示された．これは完全解析と呼ばれる．しかし一般的に，完全解析は必勝法の存在を確認するものであり，必勝法の具体的な手順全体は調べない．そこで本稿では，必勝法の手順全体を題材とし，実際に探索アルゴリズムを用いて必勝法の手順を木構造としてデータ化した．考察では，得られたデータから特徴や必勝法と必敗法の差異について言及する．

盤	4×4	4×6	4×8
必勝	後手	先手	先手
盤	4×10	6×6	8×8
必勝	先手	後手	なし

表１　先行研究の知見

2. オセロのルール

2. 1 通常ルール

以下に今回採用したオセロのルールを示す．ただし，7 番のルールは 2014 年のルール改定を反映している．そのため，先行研究［1］で採用されているルールとは異なる．

1. 黒が先手で，パスを除き黒と白が交互に一つずつ石を置く
2. 自分の石で相手の石を挟める場所に石を置け，挟んだ石をすべて自分の石の色に変える
3. 石を置ける場所がない場合はパスとなり，相手の手番となる
4. 石を置ける場所がある時は必ず打たなければならない
5. 双方が打てなくなると終局となる（空きマスが存在しても両者ともにパスとなれば終局となる）
6. 終局の際に石数の多かった方が勝ち
7. 空きマスが存在する盤面で終局した場合，石数が多い方に空きマスの数を加える

オセロは本来 8×8 マスのボードゲームであるが，研究を行う上で 4×4，4×6，4×8 盤などの小規模な盤面を考え，それを「縮小盤オセロ」と呼ぶ．なお，縮小盤オセロにおいて初期配置は中央の 4 マスの右上，左下が黒石，左上，右下が白石である．

2．2 「負けが勝ち」ルール

終局時の石数が少ない方が勝ちとする．2．1 の 6 番のルールのみ通常のルールと入れ替えたものである．

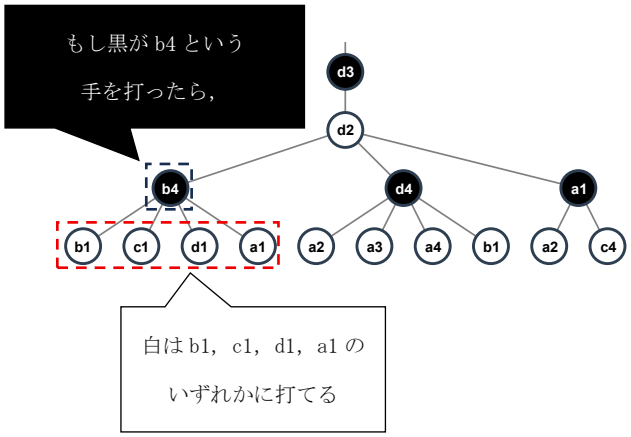
2．3 必勝法と必敗法の定義

必勝法は通常ルールにおいてその通りに手を打っていけば必ず勝てる手順のことを指す．その特性上，一種類のみとは限らない．また，その通りに手を打っていけば必ず負ける手順のことを必敗法と呼ぶことにする．必敗法は「負けが勝ち」ルールにおける必勝法ともいえる．

3． 完全解析

3．1 ゲーム木

ゲーム木とは，ゲームの中であり得るすべての進行のパターンを表したものである．下の図の例を用いて説明すると，



黒丸：黒が打つ手，白丸：白が打つ手

図 1　ゲーム木のイメージ

このように，ゲーム進行の条件分岐がすべて分かるものになっている．

3．2 必勝法の存在

すべての手順をアルゴリズムにしたがって終局まで先読みすることにより，各場面の最善手がわかる．初期盤面から両プレイヤーがつねに最善手を打ち続ける手順をパーフェクトプレイという．その勝敗によって，ゲームが先手必勝，後手必勝，引き分けのいずれかがわかる．

3．3 探索アルゴリズム

3．3．1 Mini-Max 法

ゲーム木探索アルゴリズムの一種である．このアルゴリズムにしたがえば，すべての手順を調べ，それぞれの場面における最善手がわかる．

本稿では，研究の初期段階で 4×4 盤オセロの完全解析をし，パーフェクトプレイを調べる際に用いた．

3．3．2 αβ 法

Mini-Max 法を改善したゲーム木探索アルゴリズムである．すべての手順を調べるのではなく，探索しなくても良い，明らかに最善手でない手を厳密に求め，その手を探索しないことで，より効率的に完全探索が出来るようにした手法である．ただし本稿ではこの手法は用いていない．

3. 3. 3 Negascout 法

αβ法よりも効率のいいゲーム木探索アルゴリズムのひとつである．最初に最も良いと思われる手順を探索し，その他の手を省きやすくするという手法である．

本稿では，4×6，4×8 盤に盤面を拡張するにあたって，最善手を探索する時間が大幅に増えると予想し，もう一度 4×4 盤をこのアルゴリズムで再検証し，その他の盤面もこのアルゴリズムで探索した．

3. 3. 4 Move Ordering

Negascout 法において、最初に最も良いと思われる手順を探索する順序を並べ変える手法である．

本稿ではマスごとの性質の違い（例えば隅は一度石を置くと返すことが出来ない）に着目し，探索の優先度を決めた．

3. 4 必勝の完全解析

解析の結果，以下が得られた．

盤	4×4	4×6	4×8
必勝	後手	先手	先手

表 2　必勝完全解析の結果

	a	b	c	d
1	2	3	6	9
2	1	W	B	8
3	4	B	W	10
4	7			5

図 2 4×4 盤の必勝パーフェクトプレイ

	a	b	c	d	e	f
1	10	13	14	4		
2	17	7	W	B	15	22
3	16	11	B	W	5	21
4	9	6	8	1	2	3

図 3　4×6 盤の必勝パーフェクトプレイ

	a	b	c	d	e	f	g	h
1	19	12	16	15	4	21		
2	20	17	7	W	B	22	27	11
3	25	18	13	B	W	5	10	
4	23	9	6	8	1	2	3	24

図 4 4×8 盤の必勝パーフェクトプレイ

3. 5 必敗の完全解析

解析の結果，以下が得られた．

盤	4×4	4×6	4×8
必敗	後手	なし	先手

表 3　必敗完全解析の結果

	a	b	c	d
1	2	3	10	11
2	1	W	B	8
3	4	B	W	12
4	5	7	6	9

図 5　4×4 盤の必敗パーフェクトプレイ

	a	b	c	d	e	f
1	21	8	7	10	11	12
2	19	13	W	B	17	15
3	9	11	B	W	14	16
4	18	3	2	1	4	5

図 6　4×6 盤の必敗パーフェクトプレイ

	a	b	c	d	e	f	g	h
1	10	17	6	13	12	19	15	26
2	9	7	5	W	B	14	20	25
3	8	21	4	B	W	11	23	24
4	27	22	18	16	1	2	3	28

図 7　4×8 盤の必敗パーフェクトプレイ

4 必勝法のデータ化手法の提案

4. 1 必勝木と必敗木

必勝木の構造の一部を図 2 に示す．必勝木は，初期盤面から必勝法を持たない手番の打てるすべての手に対して，必勝法を持つ手番の最善手を保存したデータである．つまり，ゲーム木の一部を取り出したものといえる．

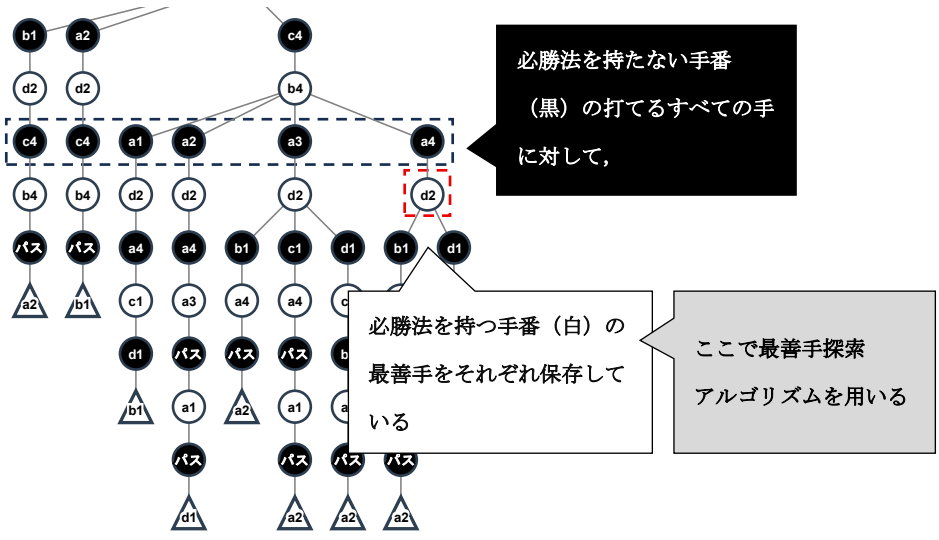


図 8　必勝木の構造イメージ

4.2 データ化

以下の結果が得られた．表 4 と表 5 ではそれぞれの盤における必勝木と必敗木の終端ノード数を示した．また図 9 で 4×4 盤の必敗木を例として紹介する．初手における盤の回転対称は考慮した．

盤	4×4	4×6	4×8
終端ノード数	9	86	213

表 4　必勝木の終端ノード数

盤	4×4	4×6	4×8
終端ノード数	95		5881

表 5　必敗木の終端ノード数

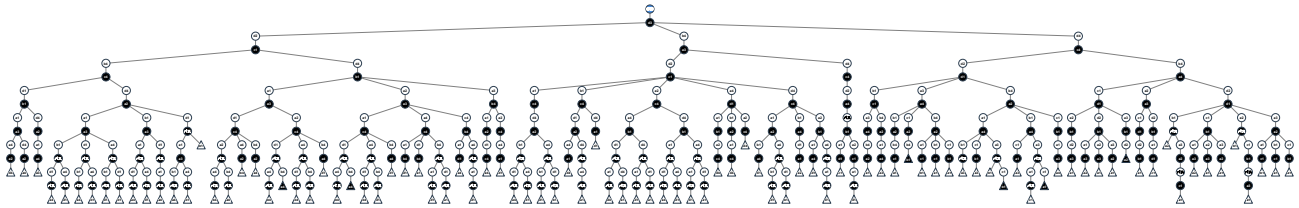


図 9　4×4 盤における必敗木

5 考察

結果のデータより，必勝法よりも必敗法の方が終端ノード数が多くなることがわかった．よって人間が実際に手順を覚えて，対局するなら必勝法の方が簡単だとわかる．

6. 結論

本稿では，4×4，4×6，4×8 盤の縮小盤オセロにおいて，必勝法，必敗法のデータ化に成功した．

なお，4×4 盤の必勝法を体験できるものとして，必勝プログラムは以下のリンクで誰でもプレイできるようにした．https://otanin495.github.io/44_onigiri/

7　参考文献

[1]竹下拓輝，池田諭，坂本眞人，伊藤隆夫:縮小盤オセロにおける完全解析，情報処理学会九州支部火の国情報シンポジウム，No.1A-2，pp.1-6（2015）
〈https://ipsj-kyushu.jp/page/ronbun/hinokuni/1004/1A/1A-2.pdf〉　（参照 2025-10-27）
[2] Hiroki Takizawa：Othello is Solved，arXiv:2310.19387,(2023)
[3] Seal Software，リバーシのアルゴリズム，工学社，2003-06-10，207 ページ

8　謝辞

本研究においてご指導いただいた教職員の方々，ならびに我々の研究発表を何度もお聞きいただき，そのたびに貴重な助言をくださった教授の方々に深く感謝申し上げます.