

$$a^{\varphi(n)} \equiv 1 \pmod{a}$$

Collatzの予想と 数学的考察

$$P\left(\lim_{n \rightarrow \infty} \bar{X}_n = \mu\right) = 1$$

数学2班

片岡 悠斗 佐藤 優大 高橋 勇輝 山田 朔

指導 武埜 章太

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt$$

●はじめに

コラッツ(Collatz)の予想とは、次の主張である:

ある正の整数 n を決め、次の〈操作〉を行う。すべての n はこの〈操作〉を繰り返すと、1に到達する。

〈操作〉

$$f(n) = \begin{cases} n/2 & \text{if } n \equiv 0 \pmod{2} \\ 3n + 1 & \text{if } n \equiv 1 \pmod{2} \end{cases}$$

ex. $n = 3$ のとき,

$$3 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1$$

このとき、 $n = 3$ の試行回数は7回であるという(1に至るまでに操作した回数)。

また、Collatzの予想に関して

- 1937年に数学者Lothar Collatzによって提唱された、数論における未解決問題である。
- コンピュータにより 5×2^{60} まで反例がないことが示されている。
- 2011年大学入試センター試験数学IIB第6問に題材として取り上げられた。

●研究動機

操作は四則演算のみで内容に関しては小学生でも理解に難くないものの、一方で提唱以来80年以上も厳密な証明は与えられていないという二律背反的な特徴に興味を持った。

しかし、課題研究という比較的短時間の研究の中では、この予想の証明は困難であると考え、予想の証明ではなく性質の究明を目的として研究を始めた。

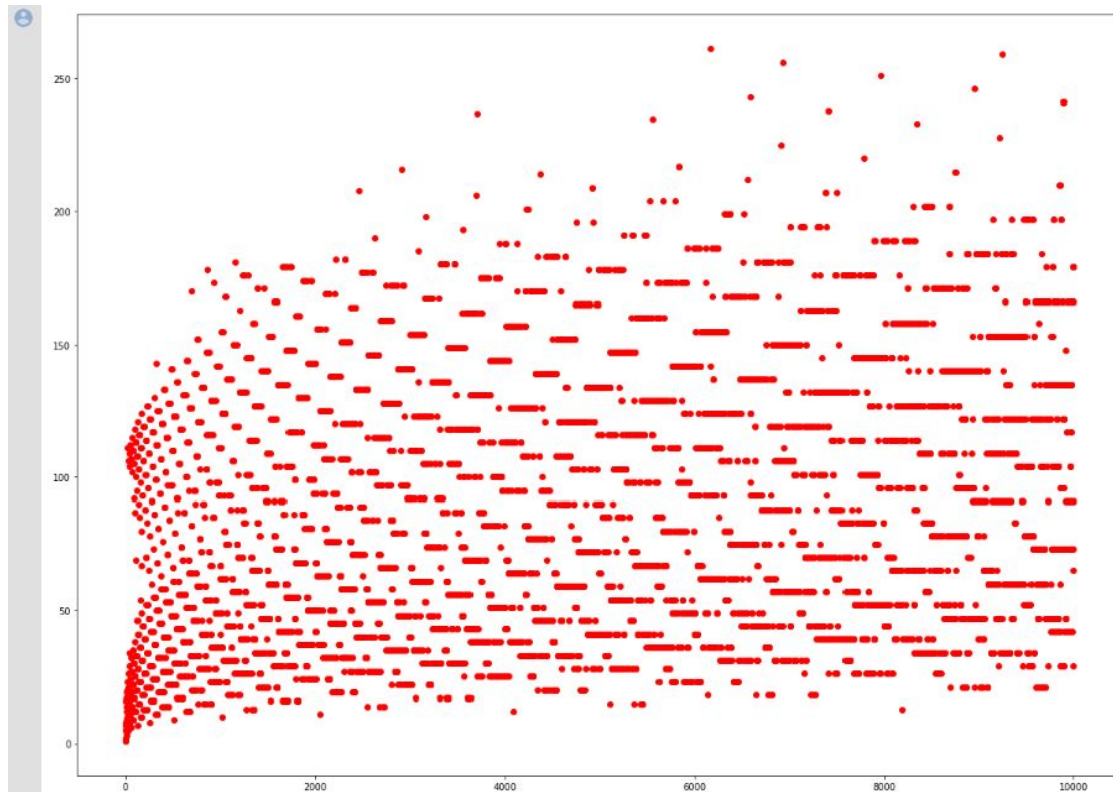
● 試行回数と散布図

我々は、プログラミング言語「Python」を用いて様々な散布図を作成し、性質の解明を図った。

I. 初期値と試行回数

横軸に初期値($1 \leq n \leq 10^4$), 縦軸にその数の試行回数をとった散布図.

〈Figure.1 散布図〉



→多数の曲線が集まっているように見える.

ex. 非負整数 k があって $n = 2^k$ と表される初期値 n の試行回数は, グラフ $y = \log_2 n$ 上に分布する.

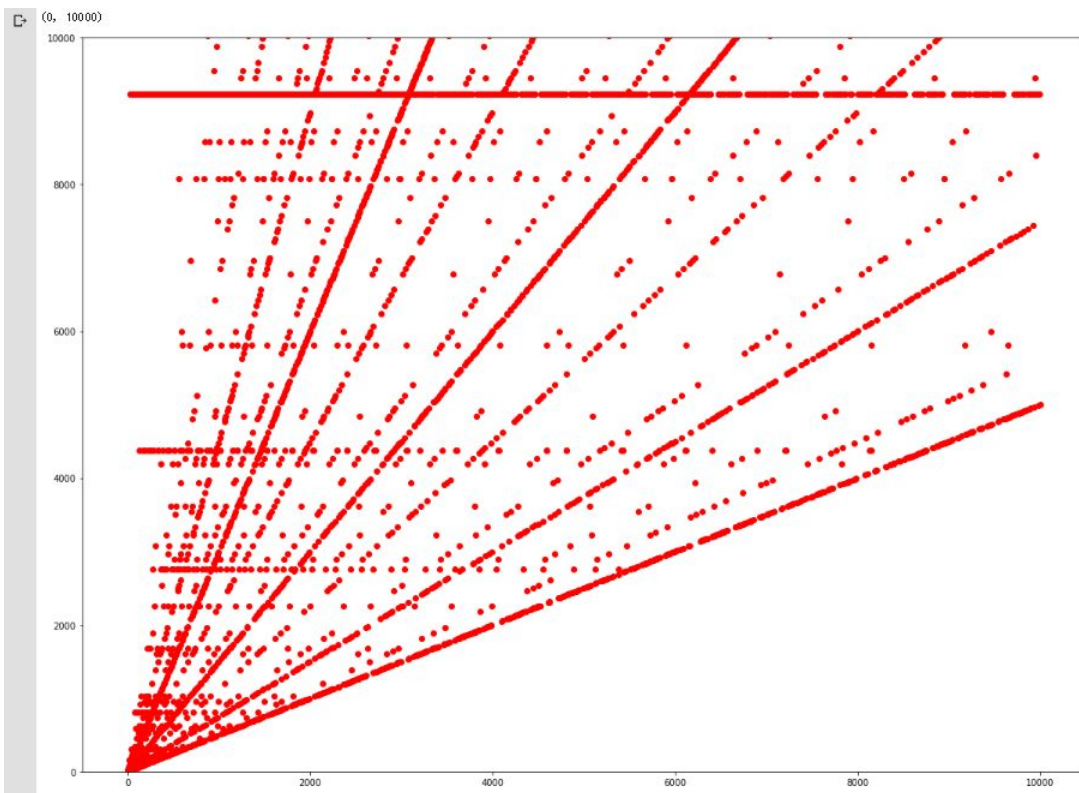
II. 初期値と最大値

横軸に初期値($1 \leq n \leq 10^4$), 縦軸に操作の間で生成される最大の数をとった散布図.
〈Figure.2 生成プログラム〉

```
[6] plt.figure(figsize=(20,15))
MAXIT = 10000
def collatz(x):
    lists = []
    while x != 1:
        x = x/2 if x%2 == 0 else x*3 + 1
        lists.append(x)
    return lists

max_cs = [max(collatz(i)) for i in range(2,MAXIT+1)]
plt.plot(range(2,MAXIT+1),max_cs,"ro")
plt.ylim(0,10000)
```

〈Figure.3 散布図〉

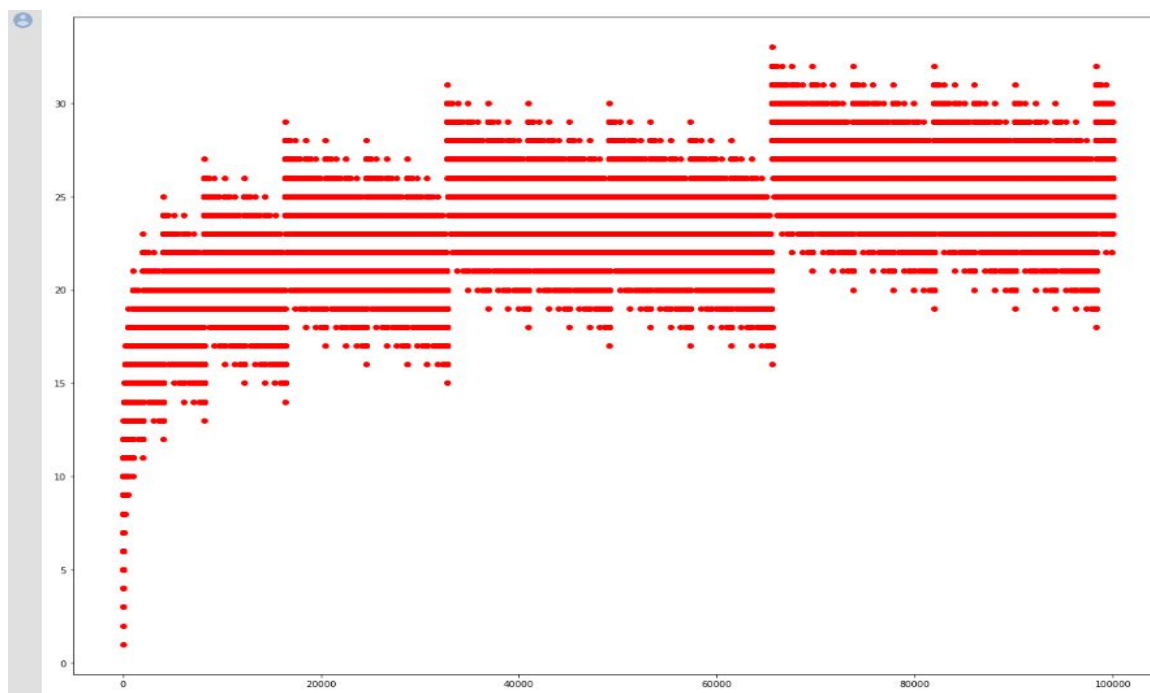


→右上がりや, 横軸に平行な直線が多数集まっているように見える.

III. 増加の操作を $n + 1$ としたときの初期値と試行回数

増加の操作をCollatzの予想から変えて $n + 1$ として、横軸に初期値($1 \leq n \leq 10^5$), 縦軸にその数の試行回数をとった散布図.

〈Figure.4 散布図〉



→周期的に横軸に平行な直線が多数集まっているように見える.

→また、点の集合のパターンが徐々に横長かつ上に出現しているように見える.

➤ 結果

グラフや試行回数からCollatzの予想に関する性質が存在しているようであった. 具体的な特徴を得るまでには至らなかったが, Collatzの予想への数学的な面白さや美しさへの興味が深まった.

●「俺らの予想」

Collatzの予想の性質について調べているうちに、予想で提示されたものと似たような形式の操作のなかに、すべての正の整数がある整数に辿り着くようなものがあるのではないかと考えた。そこで、Collatzの予想という名前に肖って、次のようにテーマを再設定した:

「俺らの予想」

すべての正の整数に対し、ある特定の整数に到達するような増加の操作が、 $3n + 1$ 以外にも存在する。ただし、減少の操作 $n/2$ は変更しない。

➤ 研究と考察

STEP 1 増加の操作を $n + 1$ に変える

STEP 1 → すべての正の整数は1に到達する。

[略証]

k を正の整数とする。正の偶数 $2k$ は1回の操作で $f(2k) = k$ 、正の奇数 $2k - 1$ は2回の操作で $f(f(2k - 1)) = k$ のように変化する。これは、いずれも操作の前後で減少している。ただし、 $k = 1$ の場合は変わらない。よって、すべての正の整数は操作の繰り返しによって1に到達する。□

STEP 2 p を奇数とし、増加の操作を $p(n + 1)$ とする。

STEP 2 → $n + 1$ はすべての正の整数 n が1に達する操作である。

STEP 2 非負整数 m について、増加の操作を $p \times 2^m(n + 1)$ としても、結局減少の操作

STEP 2で 2^m 部は割られるので、奇数のみ考えればよい。

➤ 仮説

「俺らの予想」は次のように言い換えられる:

ある正の整数 n を決め、次の〈操作〉を行う。すべての n はこの〈操作〉を繰り返すと、1に到達する。

〈操作〉

$$f(n) = \begin{cases} n/2 & \text{if } n \equiv 0 \pmod{2} \\ p(n + 1) & \text{if } n \equiv 1 \pmod{2} \end{cases}$$

➤ 実験

実際に $p = 3, 5, 7, \dots$ のときに成り立つか調べてみた。実験範囲を $1 \leq n \leq 10^7$ とする($p = 1$ の場合はSTEP 1で確かめられている)。

- $p = 3$ のとき、すべての n が3に到達した。
- $p = 5$ のとき、5に到達しない n が存在した。
- $p = 7, 9, \dots$ のときも、 p に到達しない n が存在した。

➤ 考察

すべての奇数 p について「俺らの予想」は成り立たないようである。では、「俺らの予想」の要望に沿うような p の条件が存在するのではないか。

実験を行った各奇数について、減少の操作に関わる2の累乗で評価してみる。

$$2^1 < \mathbf{3} < 2^2 < \mathbf{5, 7} < 2^3 < \mathbf{11} < \dots$$

つまり、試行回数が十分大きいとき、

- $p = 3$ のとき、1回の増加に対して最低平均1回減少する必要がある。
- $p = 5, 7$ のとき、1回の増加に対して最低平均2回減少する必要がある。

⇒一般に正の整数 k があつて、奇数 p が $2^k < p < 2^{k+1}$ と表されるとき、1回の増加に対して最低平均 k 回減少する必要がある。

また、2で k 回割り切ることのできる正の整数は 2^k 個に1つ現れるので、 $2^2 < p$ のときの p が「俺らの予想」に添いにくいことも十分考えられる。

➤ 結果

以上のことから、「俺らの予想」は次のようになった:

減少の操作を $n/2$ とする。ある特定の正の整数に到達するような増加の操作には、Collatzの予想の $3n + 1$ 以外に、 $n + 1$ と $3(n + 1)$ がある。

●数論的追究

さらに抽象的にCollatzの予想の性質を探るため、合同式という概念を用いた。

〈合同式の定義〉

n を2以上の整数とする。2整数 a, b について、 $a - b$ が n で割り切れるとき、 a と b は n を法として**合同**であるという。式では、次のように表す：

$$a \equiv b \pmod{n}$$

〈参考〉

定義は、「 n を2以上の整数とする。2整数 a, b のいずれも n で割った余りが等しければ、 a と b は n を法として合同である」という同値な言い換えができる。

また、 a, b, c, d を整数、 m, n を2以上の整数とすると、合同式について、次が成り立つ。

1. $a \equiv a \pmod{n}$
2. $a \equiv b \Leftrightarrow b \equiv a \pmod{n}$
3. $a \equiv b, b \equiv c \Rightarrow a \equiv c \pmod{n}$
4. $a \equiv b, c \equiv d \Leftrightarrow a + c \equiv b + d \pmod{n}$
5. $a \equiv b, c \equiv d \Rightarrow ac \equiv bd \pmod{n}$
6. $a \equiv b \pmod{m}, c \equiv d \pmod{n} \Leftrightarrow an + cm \equiv bn + dm \pmod{mn}$

さらに、 t を正の整数、 $1 \leq i \leq t$ について p_i を相異なる素数、 q_i を正の整数とする。任意の t について次が成り立つ。ただし、命題 P, Q について、その論理積「 P かつ Q 」は「 $P \wedge Q$ 」で表す：

7. $a \equiv 1 \pmod{p_1^{q_1}} \wedge \dots \wedge a \equiv 1 \pmod{p_t^{q_t}} \Leftrightarrow a \equiv 1 \pmod{p_1^{q_1} \dots p_t^{q_t}}$

また、 a, b, c はどの2つも互いに素な正の整数とし、扱う操作を次のように再定義した：

$$f(n) = \begin{cases} n/a & \text{if } n \equiv 0 \pmod{a} \\ bn + c & \text{otherwise} \end{cases}$$

結果として、すべての初期値 n が1に達しうるような操作の特徴を発見した。

➤ 特徴I

増加の操作の定数 c について、 $c = 1$ である。

[略証]

$c > 1$ であったとき、 $n \equiv 0 \pmod{c}$ が初期値となると $bn + c \equiv 0 \pmod{c}$ となり、 a と c が互いに素であることから、 $bn + c$ はたとえ可能な限り減少できても c までとなる。□

➤ 特徴II

増加の操作の係数 b について、 a が素数のとき $b \equiv 1 \pmod{a}$ である。

[略証]

a を法とし、 $f_2(n) = bn + 1$ とおく。また、 k 回 $f(n)$ を繰り返したものを $f^k(n)$ と表す。 k を、 $1 \leq k < a$ なる整数とする。操作の性質上、 $f_2(n)$ は、 $f_2(n) \equiv 1$ たりえない。

(i) $b \equiv 1$ のとき、 $b_2^k(n) \equiv 1 + k$ であるので、確かに1と合同たりえない。

(ii) $b \not\equiv 1$ のとき、 $f_2^k(n) \equiv b^k + \frac{b^k - 1}{b - 1}$ である。 b の条件より a は奇素数であって、 $\gcd(a, b - 1) = 1$ より、方程式 $f_2^k(n) \equiv 1$ は、両辺を $b - 1$ 倍して $b^{k+1} \equiv b$ 、さらに適当な変換を施して $b^k \equiv 1$ とできる。ここで、Fermatの小定理より $k = a - 1$ であって、これは k の範囲にある。よって、 $b \not\equiv 1$ は増加の操作に適さない。□

同様に、次の条件を発見した:

- a が4以上の2の累乗のとき、 $b \equiv 1 \pmod{4}$.
- a が奇素数 p の累乗のとき、 $b \equiv 1 \pmod{p}$.
- a が2種類以上の素数の累乗の積のとき、 $b \equiv 1 \pmod{a}$.

以上が、すべての初期値 n が1に達しうるような操作の必要条件であると考えた。

●謝辞

研究についてご指導ならびにご協力くださった武埜 章太先生, ありがとうございます.

●参考文献

愛知県立豊田西高等学校 2年 古川 陽一『ループという現象 ～コラッツ予想より～』
<https://toyotanishi-h.aichi-c.ed.jp/education/ssh/ss-bu/sska10.pdf> 最終閲覧:2020/01/21

以上.