有理数ベクトルの行列進展開

学習院大学理学部数学科
07-043-063
矢作 浩樹

◊目的◊

素数pを法とした一般フィボナッチ数列を$\{a_n\}$とする。
単純に一般フィボナッチ数列と言えば
その一般項は漸化式$a_n = a_{n-2} + a_{n-1}$を満たすが、
ここでは$a_n \equiv a_{n-2} + a_{n-1} \pmod{p}$となる。
ゆえに$0 \leq a_n < p$である。

そしてベクトル$[a_n, a_{n+1}]$をb_nとしてベクトル列$\{b_n\}$を定義する。
$\{b_n\}$には必ず$b_1 = b_k$を満たす$k > 1$が存在する。
この時<u>最小の$k-1$を周期</u>、<u>$[b_1, b_2, \cdots, b_{k-1}]$を軌道</u>と呼ぶ。

有理数ベクトル$\dfrac{\begin{pmatrix} \mathrm{a}_n \\ \mathrm{a}_{n+1} \end{pmatrix}}{p}$を$G=\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$によって展開する

<u>行列進展開</u>について研究した。

$$\frac{G\begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}}{p} = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix} + \frac{\begin{pmatrix} v_n \\ v_{n+1} \end{pmatrix}}{p} \quad (v_n < p)$$

◊方法◊

$$\frac{t\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}a_n\\ a_{n+1}\end{pmatrix}}{p} = \begin{pmatrix}u_n\\ u_{n+1}\end{pmatrix} + \frac{\begin{pmatrix}v_n\\ v_{n+1}\end{pmatrix}}{p} \quad \cdots (1)$$

$r_n = [v_n, v_{n+1}]$としてベクトル列$\{r_n\}$を定義する。
$b_{n+1} = r_n$だから、$[b_1, b_2, \cdots, b_{k-1}] = [b_1, r_1, r_2, \cdots, r_{k-2}]$より軌道を求めることができる。
各々のpについて類方程式、軌道の数、最大周期を求める。

尚、(1)のように$\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$に自然数$t$を掛けたものを改めて$G$として用いる。
以後、$\underline{t = 10}$として観察した。

Table 1. 例：**p=11のときの軌道**

周期	軌道
1	[[0,0]]
5	[[3, 2],[9, 6],[5, 7],[4, 10],[1, 8]] [[6, 4],[7, 1],[10, 3],[8, 9],[2, 5]]
10	[[10, 10],[1, 2],[9, 8],[3, 5],[6, 3],[8, 2],[9, 1],[10, 1],[10, 0],[0, 1]] [[9, 9],[2, 4],[7, 5],[6, 10],[1, 6],[5, 4],[7, 2],[9, 2],[9, 0],[0, 2]] [[8, 8],[3, 6],[5, 2],[9, 4],[7, 9],[2, 6],[5, 3],[8, 3],[8, 0],[0, 3]] · · · [[3, 3],[8, 5],[6, 9],[2, 7],[4, 2],[9, 5],[6, 8],[3, 8],[3, 0],[0, 8]] [[2, 2],[9, 7],[4, 6],[5, 1],[10, 5],[6, 7],[4, 9],[2, 9],[2, 0],[0, 9]] [[1, 1],[10, 9],[2, 3],[8, 6],[5, 8],[3, 9],[2, 10],[1, 10],[1, 0],[0, 10]] [[7, 6],[5, 9],[2, 8],[3, 1],[10, 7],[4, 5],[6, 2],[9, 3],[8, 10],[1, 4]]

Table 2. **p=11のときのまとめ**

周期	1	5	10
軌道の数	1	2	11

最大周期：10
軌道の数：$11 + 2 + 1 = 14$
類方程式：$11^2 = 10 \times 11 + 5 \times 2 + 1 \times 1$

ほぼ全てのpについて周期1の軌道は[[0,0]]のみであるが、周期1の軌道が複数存在する事例があるので後にそれについて考察する。

◊結果◊

$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$の固有多項式$x^2 - x - 1 \equiv 0 \pmod{p}$について、その解の有無で分類される。
軌道の数をM、最大周期をNとする。

(解が0個のとき)	(解が2個のとき)
$M < N$	$M > N$
$p - 1 \not\equiv 0 \pmod{N}$	$p - 1 \equiv 0 \pmod{N}$
$p^2 - 1 \equiv 0 \pmod{N}$	$p^2 - 1 \equiv 0 \pmod{N}$
$M = \frac{p^2-1}{N} + 1$	

◊考察◊

$p = 109$のとき、周期1の軌道が109個存在する。

$10\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$より、すべての$p$について軌道$[[0,0]]$が存在するのは明らかである。
そしてほとんどのpについて、周期1の軌道は$[[0,0]]$のみ存在する。
しかし、$p = 109$のときのみ周期1の軌道が109個存在する。

TABLE 3. P=109 のときの周期 1 の軌道

[[0,0]],[[1,11]],[[2,22]],[[3,33]],[[4,44]],[[5,55]],[[6,66]],[[7,77]],[[8,88]],[[9,99]]
[[10,1]],[[11,12]],[[12,23]],[[13,34]],[[14,45]],[[15,56]],[[16,67]],[[17,78]],[[18,89]],[[19,100]]
[[20,2]],[[21,13]],[[22,24]],[[23,35]],[[24,46]],[[25,57]],[[26,68]],[[27,79]],[[28,90]],[[29,101]]
[[30,3]],[[31,14]],[[32,25]],[[33,36]],[[34,47]],[[35,58]],[[36,69]],[[37,80]],[[38,91]],[[39,102]]
[[40,4]],[[41,15]],[[42,26]],[[43,37]],[[44,48]],[[45,59]],[[46,70]],[[47,81]],[[48,92]],[[49,103]]
[[50,5]],[[51,16]],[[52,27]],[[53,38]],[[54,49]],[[55,60]],[[56,71]],[[57,82]],[[58,93]],[[59,104]]
[[60,6]],[[61,17]],[[62,28]],[[63,39]],[[64,50]],[[65,61]],[[66,72]],[[67,83]],[[68,94]],[[69,105]]
[[70,7]],[[71,18]],[[72,29]],[[73,40]],[[74,51]],[[75,62]],[[76,73]],[[77,84]],[[78,95]],[[79,106]]
[[80,8]],[[81,19]],[[82,30]],[[83,41]],[[84,52]],[[85,63]],[[86,74]],[[87,85]],[[88,96]],[[89,107]]
[[90,9]],[[91,20]],[[92,31]],[[93,42]],[[94,53]],[[95,64]],[[96,75]],[[97,86]],[[98,97]],[[99,108]]
[[100,10]],[[101,21]],[[102,32]],[[103,43]],[[104,54]],[[105,65]],[[106,76]],[[107,87]],[[108,98]]

『証明』

$$10\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}a_1\\ a_2\end{pmatrix}=\begin{pmatrix}u_1\\ u_2\end{pmatrix}p+\begin{pmatrix}v_1\\ v_2\end{pmatrix}$$

$$\begin{cases}10\mathrm{a}_2 \equiv v_1 \pmod{p}\\ 10(\mathrm{a}_1+a_2)\equiv v_2 \pmod{p}\end{cases}$$

ここで周期1とすると、$\underline{v_1=a_1, v_2=a_2}$だから、

$$\begin{cases}10\mathrm{a}_2 \equiv a_1 \pmod{p} \quad \cdots(2)\\ 10(\mathrm{a}_1+a_2)\equiv a_2 \pmod{p} \quad \cdots(3)\end{cases}$$

$$\therefore 10(10\mathrm{a}_2+a_2)\equiv a_2 \pmod{p}$$

$$\therefore 109\mathrm{a}_2 \equiv 0 \pmod{p} \quad \cdots(3)'$$

　109とpは素数で、$0 \leq a_2 < p = 109$だから、$p \neq 109$とすると(3)'が成立するのは$a_2 = 0$のときのみである。
そして$p = 109$のときは(3)'は常に成立し、a_2は$0 \leq a_2 < p = 109$の範囲で自由にとれる。
その各々のa_2に対してa_1は(2)によって唯一つに定まるため、(2)と(3)を満たす$[a_1, a_2]$は109個存在する。
よって$p = 109$のときのみ、周期1の軌道は109個存在する。

（証明終）

$p = 109$のときのみ周期1の軌道が複数存在するのは、観察前に$t = 10$としたためである。
tをそのまま変数として考えると、(3)'は

$$\underline{(t^2 + t - 1)}a_2 \equiv 0 \pmod{p}$$

となる。
よって以下のことが言える。

$t^2 + t - 1$を素因数分解する。
その素因数がpのとき、周期1の軌道はp個存在する。

Figure 1. t^2+t-1が素数or素数でないtの個数