数学の楽しみ方～フィボナッチ数列を題材にして

２０１９年1月１３日　数学工房駒込教室
諏訪紀幸　(中央大学理工学部)

数学工房会報はその配付を心待ちにしているのですが，とりわけ巻頭言では塾主の桑野耕一先生の社会批評や数学の学びへの提言が読み取れ，確かにそうだと思うこともありますし，図星を突かれて怒る人もいるだろうと思うこともあります．例えば，一昨年１月に配付された会報１２２号では

数学科出身者なら数学工房の初級の基礎教程程度のことは大学でやったと言う人が多いでしょう．ところが，ちょっと高度な数学をご自分で身に付けようとすると，ほとんどの方が挫折します．ということはできていないのです．たとえ大学，大学院で講義を受けたとしても，表面的な知識にとどまって，理論を通して身に付けるべき基本技術，方法を自分のものにしていないのです．

と，よく内情をご存知でいらっしゃる，これでは藩札学位横行のことも先刻お見通しに違いないと，大学にたつきを求めている者は考え込まざるを得ないことを書いておられます．

また，昨年９月に配付された会報１２７号では

数学工房では「数学の基本語彙と文法」から作用素環にいたるまで，基礎数学の学びと稽古の場を長年にわたって提供してきました．しかしながら，抽象の使いこなしの復仇は日暮れて道遠しです．表の知識は伝わるように見えても，その背後にあるセンスを教えることは実に難しいと感じています．抽象を使いこなすためにはセンスが必要です．

とぼやきで始めておられます．私にもこのようなぼやきは始終のことです．いつ頃からか覚えはありませんが，数学の技法は教えることはできるが，その背後にある感覚は教えることはできない，自分でその感覚に気付くように仕向けることが精一杯だと考えるようになりました．それには数学のここで楽しく感じた，その受け止め方を大切に扱うこと，そこから始めるのが一法であるように思います．数学の楽しみ方は人それぞれ，千差万別でしょう．

フィボナッチ数列を含むルーカス数列は，高校数学で扱われる階差数列の典型的な例です．ルーカス数列については膨大な研究結果の蓄積があり，専門誌 Fibonacci Quaterly が発刊されている程ですが，今回はルーカス数列を題材に数学の楽しみ方について，皆さんと対話をしながら考えて行きたいと思います．そこで，以下の場面を用意しました．

１．解法を楽しむ～二階線型差分方程式を例として
２．類似を楽しむ～二階線型差分方程式と二階線型微分方程式を並べて
３．日々の情景を楽しむ～Lucas 数列を例として
４．風景の広がりを感じる～lois de l'apparition et la répétition の証明に向けて
５．悠久の流れを感じる～温故知新の一例
６．日常の営為を楽しむ～時々の花々を愛でる

それでは，ダンテとヴェルギリウスの地獄巡りの後追いにならぬよう気を付けながら，順次巡って行きましょう．

１．解法を楽しむ～二階線型差分方程式を例として

高校数学では漸化式とよばれている二階線型差分方程式 $x_{k+2}+px_{k+1}+qx_k=0$ $(x_0=c_1,\, x_1=c_2)$ の幾つかの解法について説明します．

最初に高校数学での方法を復習し，次に行列の言葉でその方法を機能的に捉え直します．これは線型差分方程式を線型代数の枠組みで理解する出発点です．最後に母函数による方法を紹介します．それぞれの方法の n 階線型差分方程式への一般化について，その関連を見ながら考えを進めることは，数学を稽古するには格好の題材です．

解法 1．$\lambda^2+p\lambda+q=0=(\lambda-\alpha)(\lambda-\beta)$ とおくと，$p=-\alpha-\beta$, $q=\alpha\beta$．したがって，$x_{k+2}+px_{k+1}+qx_k=0$ は

$$x_{k+2}-\beta x_{k+1}=\alpha(x_{k+1}-\beta x_k)$$

と書き直せる．$y_k=x_{k+1}-\beta x_k$ とおくと，$y_{k+1}=\alpha y_k$, $y_0=c_2-\beta c_1$．したがって，各 $k\geq 0$ に対して

$$y_k=(c_2-\beta c_1)\alpha^k$$

が成立する．$C=c_2-\beta c_1$ とおくと，

$$\begin{aligned}
x_k-\beta x_{k-1}&=C\alpha^{k-1},\\
\beta(x_k-\beta x_{k-1})&=C\alpha^{k-2}\beta,\\
&\vdots\\
\beta^{k-2}(x_2-\beta x_1)&=C\alpha\beta^{k-2},\\
\beta^{k-1}(x_1-\beta x_0)&=C\beta^{k-1}
\end{aligned}$$

辺々加えて

$$x_k-\beta^k x_0=C(\alpha^{k-1}+\alpha^{k-2}\beta+\cdots+\alpha\beta^{k-2}+\beta^{k-1})$$

を得る．これから，

$$x_k=c_1\beta^k+(c_2-\beta c_1)(\alpha^{k-1}+\alpha^{k-2}\beta+\cdots+\alpha\beta^{k-2}+\beta^{k-1})$$

(a) $\alpha\neq\beta$ の場合．

$$x_k=c_1\beta^k+(c_2-\beta c_1)\frac{\alpha^k-\beta^k}{\alpha-\beta}=\frac{c_2-\beta c_1}{\alpha-\beta}\alpha^k+\frac{-c_2+\alpha c_1}{\alpha-\beta}\beta^k$$

(a) $\alpha=\beta$ の場合．

$$x_k=c_1\alpha^k+k(c_2-\alpha c_1)\alpha^{k-1}$$

解法 2．二階線型差分方程式

$$x_{k+2}+px_{k+1}+qx_k=0,\ x_0=c_1,\ x_1=c_2$$

は $y_k=x_{k+1}$ とおくことによって連立差分方程式

$$\begin{cases}x_{k+1}=\quad y_k\\ y_{k+1}=-qx_k-py_k,\quad x_0=c_1,\ y_0=c_2\end{cases}$$

と書き換えられる．

$$A=\begin{pmatrix}0&1\\-q&-p\end{pmatrix}$$

とおくと，

$$\begin{pmatrix}x_{k+1}\\y_{k+1}\end{pmatrix}=A\begin{pmatrix}x_k\\y_k\end{pmatrix}$$

したがって，各 $k\geq 0$ に対して

$$\begin{pmatrix}x_k\\y_k\end{pmatrix}=A^k\begin{pmatrix}x_0\\y_0\end{pmatrix}=A^k\begin{pmatrix}c_1\\c_2\end{pmatrix}$$

が成立する．ここで，α, β を A の固有値とする．このとき，α, β は $\lambda^2 + p\lambda + q = 0$ の根で，$\begin{pmatrix} 1 \\ \alpha \end{pmatrix}, \begin{pmatrix} 1 \\ \beta \end{pmatrix}$ はそれぞれ α, β を固有値とする A の固有ベクトル．

(I) $\alpha \neq \beta$ のとき，

$$A = \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}^{-1}$$

ここで，

$$\begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}^{-1} = \frac{1}{\beta - \alpha} \begin{pmatrix} \beta & -1 \\ -\alpha & 1 \end{pmatrix}$$

なので，

$$A^k = \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} \alpha^k & 0 \\ 0 & \beta^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}^{-1} = \frac{1}{\beta - \alpha} \begin{pmatrix} \alpha^k\beta - \alpha\beta^k & -\alpha^k + \beta^k \\ \alpha^{k+1}\beta - \alpha\beta^{k+1} & -\alpha^{k+1} + \beta^{k+1} \end{pmatrix}$$

したがって，二階線型差分方程式

$$x_{k+2} + px_{k+1} + qx_k = 0,\ x_0 = c_1,\ x_1 = c_2$$

の解は

$$x_k = \frac{1}{\beta - \alpha}\{c_1(\alpha^k\beta - \alpha\beta^k) + c_2(-\alpha^k + \beta^k)\} = \frac{1}{\beta - \alpha}\{(c_1\beta - c_2)\alpha^k + (-c_1\alpha + c_2)\beta^k\}$$

で与えられる．

(II) $\alpha = \beta$ のとき，

$$A = \begin{pmatrix} 0 & 1 \\ -\alpha^2 & 2\alpha \end{pmatrix}$$

ここで，

$$S = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix},\ N = A - S = \begin{pmatrix} -\alpha & 1 \\ -\alpha^2 & \alpha \end{pmatrix}$$

とおけば，$SN = NS$ で $N^2 = 0$．したがって，

$$A^k = (S + N)^k = S^k + kS^{k-1}N = \begin{pmatrix} (1-k)\alpha^k & k\alpha^{k-1} \\ -k\alpha^{k+1} & (1+k)\alpha^k \end{pmatrix}$$

したがって，二階線型差分方程式

$$x_{k+2} + px_{k+1} + qx_k = 0,\ x_0 = c_1,\ x_1 = c_2$$

の解は

$$x_k = c_1(1-k)\alpha^k + c_2k\alpha^{k-1} = c_1\alpha^k + (-c_1\alpha + c_2)k\alpha^{k-1}$$

で与えられる．

解法３．$\{a_k\}_{k\geq 0}$ を $a_{k+2} = -pa_{k+1} - qa_k$, $a_0 = c_1$, $a_1 = c_2$ によって帰納的に定義される数列とする．このとき，

$$f(t) = \sum_{k=0}^{\infty} a_k t^k$$

とおくと，

$$f(t)+ptf(t)+qt^2f(t)=a_0+(pa_0+a_1)t$$

したがって，

$$f(t)=\frac{a_0+(pa_0+a_1)t}{1+pt+qt^2}$$

さらに，

$$1+pt+qt^2=(1-\alpha t)(1-\beta t)$$

とおく．

(I) $\alpha\neq\beta$ のとき

$$f(t)=\frac{a_0\beta-a_1}{\beta-\alpha}\frac{1}{1-\alpha t}+\frac{-a_0\alpha+a_1}{\beta-\alpha}\frac{1}{1-\beta t}=\sum_{k=0}^{\infty}\frac{1}{\beta-\alpha}\big\{(a_0\beta-a_1)\alpha^k+(-a_0\alpha+a_1)\beta^k\big\}t^k$$

これから，

$$a_k=\frac{1}{\beta-\alpha}\big\{(a_0\beta-a_1)\alpha^k+(-a_0\alpha+a_1)\beta^k\big\}=\frac{1}{\beta-\alpha}\big\{(c_1\beta-c_2)\alpha^k+(-c_0\alpha+c_1)\beta^k\big\}$$

(II) $\alpha=\beta$ のとき

$$f(t)=\frac{a_0}{1-\alpha t}+\frac{(-\alpha a_0+a_1)t}{(1-\alpha t)^2}=\sum_{k=0}^{\infty}\big\{a_0\alpha^k+(-a_0\alpha+a_1)k\alpha^{k-1}\big\}t^k$$

これから，

$$a_k=a_0\alpha^k+(-a_0\alpha+a_1)k\alpha^{k-1}=c_1\alpha^k+(-c_1\alpha+c_2)k\alpha^{k-1}$$

補足４．$\dfrac{1}{1-t}=\displaystyle\sum_{k=0}^{\infty}t^k$ の両辺を微分して

$$\frac{1}{(1-t)^2}=\sum_{k=0}^{\infty}(k+1)t^k$$

を得る．一般に正の整数 n に対して

$$\frac{1}{(1-t)^n}=\sum_{k=0}^{\infty}\binom{n+k-1}{k}t^k$$

が成立する．

例５．(吸収壁のある酔歩問題) 一直線の上に座標が $0,1,\dots,N$ の点を考える．最初 k $(1\leq k\leq N-1)$ に存在した一つの粒子が 1 秒後には確率 p で $k+1$ に，確率 q で $k-1$ に移るものとする．また，この法則で運動を続けて 0 または N に達したとき，そこで運動を停止するものとする．このとき，最初に k に存在した一つの粒子が 0 に到達する確率 p_k について論ぜよ．ただし，$p+q=1$, $p\neq1$, $q\neq1$ とする．

解．$p_0=1$, $p_N=0$ とおけば，$1\leq k\leq N-1$ に対して $p_k=pp_{k+1}+qp_{k-1}$ が成立する．これから，差分方程式

$$p_{k+1}-\frac{1}{p}p_k+\frac{q}{p}p_{k-1}=0,\ p_0=1,\ p_N=0$$

を得る．特性方程式 $\lambda^2-\dfrac{1}{p}\lambda+\dfrac{q}{p}=0$ の根は $\lambda=1,\dfrac{1-p}{q}=\dfrac{q}{p}$ で与えられる．

(I) $p \neq q$ のとき，差分方程式 $p_{k+1} - \dfrac{1}{p}p_k + \dfrac{q}{p}p_{k-1} = 0$ の一般解は $A1^k + B\Big(\dfrac{q}{p}\Big)^k$ で与えられる．ここで，$p_0 = 1,\, p_N = 0$ なので，

$$A + B = 1,\ A + B\Big(\frac{q}{p}\Big)^N = 0$$

したがって，

$$A = -\frac{\Big(\dfrac{q}{p}\Big)^N}{1 - \Big(\dfrac{q}{p}\Big)^N},\ B = \frac{1}{1 - \Big(\dfrac{q}{p}\Big)^N}$$

これから，

$$p_k = -\frac{\Big(\dfrac{q}{p}\Big)^N}{1 - \Big(\dfrac{q}{p}\Big)^N}1^k + \frac{1}{1 - \Big(\dfrac{q}{p}\Big)^N}\Big(\frac{q}{p}\Big)^k = \frac{\Big(\dfrac{q}{p}\Big)^k - \Big(\dfrac{q}{p}\Big)^N}{1 - \Big(\dfrac{q}{p}\Big)^N}$$

(II) $p = q = \dfrac{1}{2}$ のとき，差分方程式 $p_{k+1} - \dfrac{1}{p}p_k + \dfrac{q}{p}p_{k-1} = 0$ の一般解は $p_k = 1^k(A + Bk)$ で与えられる．ここで，$p_0 = 1,\, p_N = 0$ なので，$A = 1,\, A + BN = 0$．したがって，$B = -\dfrac{1}{N}$．これから，

$$p_k = 1^k\Big(1 - \frac{1}{N}k\Big) = \frac{N - k}{N}$$

２．類似を楽しむ〜二階線型差分方程式と二階線型微分方程式を並べて

二階線型微分方程式 $\dfrac{d^2x}{dt^2} + p\dfrac{dx}{dt} + qx = 0,\, x(0) = c_1,\, \dfrac{dx}{dt}(0) = c_2$ の幾つかの解法について説明します．

二階線型差分方程式のそれぞれの解法に対比させて二階線型微分方程式の解法を紹介しますが，高校数学に収まっていない前提知識を補います．線型差分方程式と線型微分方程式の解法の類似の背後に何かがある，それを言葉にするには何が必要でしょうか．

準備１．微分方程式 $\dfrac{dx}{dt} = \alpha x + f(t),\, x(0) = c$ の解は

$$x = e^{\alpha x}\Big\{c + \int_0^t f(u)e^{-\alpha u}du\Big\}$$

によって与えられる．

解の導き方．$\dfrac{dx}{dt} = \alpha x + f(t)$ の両辺に $e^{-\alpha t}$ を掛けて

$$\frac{dx}{dt}e^{-\alpha t} = \alpha x e^{-\alpha t} + f(t)e^{-\alpha t}$$

を得る．ここで，$z = xe^{-\alpha t}$ とおけば，

$$\frac{dz}{dt} = \Big(\frac{dx}{dt} - \alpha x\Big)e^{-\alpha t} = f(t)e^{-\alpha t}$$

さらに，$z(0) = x(0) = c$ なので，

$$z = c + \int_0^t f(u)e^{-\alpha u}du$$

これから，

$$x = e^{-\alpha t}\Big\{c + \int_0^t f(u)e^{-\alpha u}du\Big\}$$

例２．微分方程式 $\dfrac{dx}{dt} = \alpha x + \gamma$, $x(0) = c$, $\alpha \neq 0$ の解は

$$x = e^{\alpha x}\Big\{c - \frac{\gamma}{\alpha}(e^{-\alpha t} - 1)\Big\} = \Big(c + \frac{\gamma}{\alpha}e^{-\alpha t}\Big) - \frac{\gamma}{\alpha}$$

によって与えられる．

解法３．$\lambda^2 + p\lambda + q = 0 = (\lambda - \alpha)(\lambda - \beta)$ とおくと，

$$p = -\alpha - \beta,\ q = \alpha\beta$$

したがって，$\dfrac{d^2x}{dt^2} + p\dfrac{dx}{dt} + qx = 0$ は

$$\frac{d}{dt}\Big(\frac{dx}{dt} - \beta x\Big) = \alpha\Big(\frac{dx}{dt} - \beta x\Big)$$

と書き直せる．$y = \dfrac{dx}{dt} - \beta x$ とおくと，

$$\frac{dy}{dt} = \alpha y,\ y(0) = c_2 - \beta c_1$$

したがって，

$$y = (c_2 - \beta c_1)e^{\alpha t}$$

これから，

$$\frac{dx}{dt} = \beta x + (c_2 - \beta c_1)e^{\alpha t}$$

したがって，

$$x = e^{\beta t}\Big\{c_1 + \int_0^t (c_2 - \beta c_1)e^{(\alpha-\beta)u}du\Big\}$$

(a) $\alpha \neq \beta$ の場合．

$$x = e^{\beta t}\Big\{c_1 + \frac{c_2 - \beta c_1}{\alpha - \beta}\big(e^{(\alpha-\beta)t} - 1\big)\Big\} = \frac{c_2 - \beta c_1}{\alpha - \beta}e^{\alpha t} + \frac{-c_2 + \alpha c_1}{\alpha - \beta}e^{\beta t}$$

(a) $\alpha = \beta$ の場合．

$$x = e^{\alpha t}\big\{c_1 + (c_2 - \beta c_1)t\big\}$$

補足４．微分方程式 $\dfrac{dx}{dt} = ax$ の一般解は $x = Ce^{at}$ によって与えられる．

解の導き方．$x \neq 0$ と仮定する．このとき，

$$\frac{dx}{dt} = adt$$

の両辺を積分して

$$\log|x| = at + C$$

を得る．これから，$x = \pm e^C e^{at}$．さらに，$\pm e^C$ を C で置き換えて $x = Ce^{at}$ を得る．

補足５．微分方程式 $\dfrac{d^2x}{dt^2} = -\omega^2 x$ $(\omega > 0)$ の一般解は $x = 0$ または

$$x = a\sin(\omega t + \varphi)\ (a > 0,\ 0 \leq \varphi < 2\pi)$$

によって与えられる．

解の導き方．$x \neq 0$ と仮定する．このとき，

$$2\frac{d^2x}{dt}\frac{dx}{dt} = -\omega^2\Big(2\frac{dx}{dt}x\Big)$$

の両辺を積分して

$$\Big(\frac{dx}{dt}\Big)^2 = \omega^2(a^2 - \omega^2)\ (a > 0)$$

を得る．したがって，

$$\frac{dx}{dt} = \pm\omega\sqrt{a^2 - \omega^2}$$

さらに，

$$\frac{dx}{\sqrt{a^2 - x^2}} = \pm\omega dt$$

の両辺を積分して

$$\sin^{-1}\frac{x}{a} = \pm\omega t + \varphi$$

を得る．$x = a\sin(-\omega t + \varphi) = -a\sin(\omega t - \varphi)$ の場合，$-\varphi$ を $-\varphi + \pi$ で置き換えて $x = a\sin(\omega t + \varphi)$ の形に書き直せる．さらに，$0 \leq \varphi < 2\pi$ としてよい．

補足 6．微分方程式 $\dfrac{d^2x}{dt^2} + 2\lambda\dfrac{dx}{dt} + (\lambda^2 + \omega^2)x\ (\omega > 0)$ の一般解は $x = 0$ または

$$x = ae^{-\lambda t}\sin(\omega t + \varphi)\ (a > 0,\ 0 \leq \varphi < 2\pi)$$

によって与えられる．

解の導き方．$z = xe^{\lambda t}$ とおくと，

$$\frac{dz}{dt} = \Big(\frac{dx}{dt} + \lambda\Big)e^{\lambda t},\ \frac{d^2z}{dt^2} = \Big(\frac{d^2x}{dt^2} + 2\lambda\frac{dx}{dt} + \lambda^2 x\Big)e^{\lambda t}$$

したがって，

$$\frac{d^2z}{dt^2} + \omega^2 z = \Big\{\frac{d^2x}{dt^2} + 2\lambda\frac{dx}{dt} + (\lambda^2 + \omega^2)x\Big\}e^{\lambda t} = 0$$

したがって，

$$z = 0 \text{ または } z = a\sin(\omega t + \varphi)\ (a > 0,\ 0 \leq \varphi < 2\pi)$$

これから

$$x = 0 \text{ または } x = ae^{-\lambda t}\sin(\omega t + \varphi)\ (a > 0,\ 0 \leq \varphi < 2\pi)$$

解法 7．二階線型微分方程式

$$\frac{d^2x}{dt^2} + p\frac{dx}{dt} + qx = 0,\ x(0) = c_1,\ \frac{dx}{dt}(0) = c_2$$

は $y = \dfrac{dx}{dt}$ とおくことによって連立微分方程式

$$\begin{cases} \dfrac{dx}{dt} = \quad y \\ \dfrac{dy}{dt} = -qx - py, \quad x(0) = c_1,\ y(0) = c_2 \end{cases}$$

と書き換えられる．

$$A = \begin{pmatrix} 0 & 1 \\ -q & -p \end{pmatrix}$$

とおくと，

$$\frac{d}{dt}\begin{pmatrix} x \\ y \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix}$$

したがって，

$$\begin{pmatrix} x \\ y \end{pmatrix} = \exp At \begin{pmatrix} x(0) \\ y(0) \end{pmatrix} = \exp At \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

が成立する．ここで，α, β を A の固有値とする．このとき，α, β は $\lambda^2 + p\lambda + q = 0$ の根で，$\begin{pmatrix} 1 \\ \alpha \end{pmatrix}, \begin{pmatrix} 1 \\ \beta \end{pmatrix}$ はそれぞれ α, β を固有値とする A の固有ベクトル．

(I) $\alpha \neq \beta$ のとき，

$$A = \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}\begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}^{-1}$$

ここで，

$$\begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}^{-1} = \frac{1}{\beta - \alpha}\begin{pmatrix} \beta & -1 \\ -\alpha & 1 \end{pmatrix}$$

なので，

$$\exp At = \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}\begin{pmatrix} e^{\alpha t} & 0 \\ 0 & e^{\beta t} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}^{-1} = \frac{1}{\beta - \alpha}\begin{pmatrix} \beta e^{\alpha t} - \alpha e^{\beta t} & -e^{\alpha t} + e^{\beta t} \\ \alpha\beta e^{\alpha t} - \alpha\beta e^{\beta t} & -\alpha e^{\alpha t} + \beta e^{\beta t} \end{pmatrix}$$

したがって，二階線型微分方程式

$$\frac{d^2x}{dt^2} + p\frac{dx}{dt} + qx = 0,\ x(0) = c_1,\ \frac{dx}{dt}(0) = c_2$$

の解は

$$x = \frac{1}{\beta - \alpha}\{c_1(\beta e^{\alpha t} - \alpha e^{\beta t}) + c_2(-e^{\alpha t} + e^{\beta t})\} = \frac{1}{\beta - \alpha}\{(c_1\beta - c_2)e^{\alpha t} + (-c_1\alpha + c_2)e^{\beta t}\}$$

で与えられる．

(II) $\alpha = \beta$ のとき，

$$A = \begin{pmatrix} 0 & 1 \\ -\alpha^2 & 2\alpha \end{pmatrix}$$

ここで，

$$S = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix},\ N = A - S = \begin{pmatrix} -\alpha & 1 \\ -\alpha^2 & \alpha \end{pmatrix}$$

とおけば，$SN = NS$ で $N^2 = 0$．したがって，

$$\exp At = (\exp St)(\exp Nt) = (\exp St)(1 + Nt) = \begin{pmatrix} (1 - \alpha t)e^{\alpha t} & te^{\alpha t} \\ -\alpha^2 e^{\alpha t} & (1 + \alpha t)e^{\alpha t} \end{pmatrix}$$

したがって，二階線型微分方程式

$$\frac{d^2x}{dt^2} + p\frac{dx}{dt} + qx = 0,\ x(0) = c_1,\ \frac{dx}{dt}(0) = c_2$$

の解は

$$x = c_1e^{\beta t} + c_2te^{\beta t} = \{c_1 + (-c_1\alpha + c_2)t\}e^{\beta t}$$

で与えられる．

解法８．$X(s) = L[x(t)]$ とおく．

$$\frac{d^2x}{dt^2} + p\frac{dx}{dt} + qx = 0,\ x(0) = c_1,\ \frac{dx}{dt}(0) = c_2$$

に Laplace 変換を施して

$$\{-x'(0) - sx(0) + s^2X(s)\} + p\{-x(0) + sX(s)\} + qX(s) = 0$$

を，したがって，

$$X(s) = \frac{c_1 s + (pc_1 + c_2)}{s^2 + ps + q}$$

を得る．

(I) $s^2 + ps + q = (s - \alpha)(s - \beta)$ $(\alpha, \beta \in \mathbb{R},\ \alpha \neq \beta)$ のとき，$\alpha + \beta = -p$ なので，

$$\frac{c_1 s + (pc_1 + c_2)}{s^2 + ps + q} = \frac{c_1\alpha + (pc_1 + c_2)}{\alpha - \beta}\frac{1}{s - \alpha} - \frac{c_1\beta + (pc_1 + c_2)}{\alpha - \beta}\frac{1}{s - \beta} = \frac{-c_1\beta + c_2}{\alpha - \beta}\frac{1}{s - \alpha} + \frac{c_1\alpha - c_2}{\alpha - \beta}\frac{1}{s - \beta}$$

これから，

$$x(t) = \frac{-c_1\beta + c_2}{\alpha - \beta}e^{\alpha t} + \frac{c_1\alpha - c_2}{\alpha - \beta}e^{\beta t}$$

(II) $s^2 + ps + q = (s - \alpha)^2$ $(\alpha \in \mathbb{R})$ のとき，$2\alpha = -p$ なので，

$$\frac{c_1 s + (pc_1 + c_2)}{s^2 + ps + q} = \frac{c_1(s - \alpha) + (-c_1\alpha + c_2)}{(s - \alpha)^2} = \frac{c_1}{s - \alpha} + \frac{-c_1\alpha + c_2}{(s - \beta)^2}$$

これから，

$$x(t) = c_1 e^{\alpha t} + (-c_1\alpha + c_2)te^{\alpha t}$$

(III) $s^2 + ps + q = (s + \lambda)^2 + \omega^2$ $(\lambda, \omega \in \mathbb{R},\ \omega > 0)$ のとき，$2\lambda = p$ なので，

$$\frac{c_1 s + (pc_1 + c_2)}{s^2 + ps + q} = \frac{c_1(s + \lambda) + (c_1\lambda + c_2)}{(s + \lambda)^2 + \omega^2}$$

これから，

$$x(t) = e^{-\lambda t}\Big(c_1 \cos\omega t + \frac{c_1\lambda + c_2}{\omega}\sin\omega t\Big)$$

補足９．$f(t)$ を $t \geq 0$ において定義された函数とする．広義積分

$$L[f(t)] = \int_0^\infty f(t)e^{-st}dt$$

が存在するとき，$F(s) = L[f(t)]$ を $f(t)$ の Laplace 変換とよぶ．例えば，

(1) $L[1] = \dfrac{1}{s}$

(2) $L[\cos\omega t] = \dfrac{s}{s^2 + \omega^2}$

(3) $L[\sin\omega t] = \dfrac{\omega}{s^2 + \omega^2}$

また，$F(s) = L[f(t)]$ とおけば，

(4) $L[e^{at}f(t)] = F(s - a)$ $(s > a)$

(5) $L[tf(t)] = -F'(s)$

(6) $L[f'(t)] = -f(0) + sF(s)$, $L[f''(t)] = -f'(0) - sf(0) + s^2F(s)$
が成立する．

例１０．(ばねの振動) 二つのばねで左右に引っ張られた振動子が水平面の上で摩擦を受けて一次元的に動くときの運動について論ぜよ．ただし，ばねの力は Hooke の法則に従い，また，摩擦力は運動の速度に比例するものとする．

解．時間を t で，振動子の座標を x で表わす．また，ばねの弾性係数をそれぞれ k_1, k_2，力が加わっていない状態でのばねの先端の座標をそれぞれ a_1, a_2 とおく．このとき，Hooke の法則から，

$$F_1 = k_1(x - a_1),\ F_2 = k_2(x - a_2)$$

を得る．座標の原点を二つのばねの釣り合う点にとると，$x = 0$ のとき，$F_1 = F_2$ となる．したがって，

$$k_1a_1 = k_2a_2$$

一方，摩擦力 R は運動の速度に比例し，運動の方向と反対向きになるので，

$$R = -\rho\frac{dx}{dt}\ (\rho > 0)$$

質点の質量を m とすると，Newton の運動法則から

$$m\frac{d^2}{dx^2} = -\rho\frac{dx}{dt} - k_1(x - a_1) + k_2(a_2 - x)$$

$k = k_1 + k_2$ とおけば，微分方程式

$$m\frac{d^2x}{dt^2} + \rho\frac{dx}{dt} + kx = 0$$

を得る．特性方程式 $m\lambda^2 + \rho\lambda + k = 0$ の根は $\lambda = \dfrac{-\rho \pm \sqrt{\rho^2 - 4mk}}{2m}$ で与えられる．

(I) $\rho^2 - 4mk > 0$ のとき，

$$x = A\exp\frac{-\rho - \sqrt{\rho^2 - 4mk}}{2m}t + B\exp\frac{-\rho + \sqrt{\rho^2 - 4mk}}{2m}t \quad \text{(過減衰)}$$

(II) $\rho^2 - 4mk = 0$ のとき，

$$x = (A + Bt)\exp\frac{-\rho}{2m}t \quad \text{(臨界減衰)}$$

(III) $\rho^2 - 4mk < 0$ のとき，

$$x = \exp\frac{-\rho}{2m}t\left(A\cos\frac{\sqrt{4mk - \rho^2}}{2m}t + B\sin\frac{\sqrt{4mk - \rho^2}}{2m}t\right) \quad \text{(減衰振動)}$$

３．日々の情景を楽しむ〜Lucas 数列を例として

二階線型差分方程式において係数と初項を整数とすれば一般項は整数となり，整数独特の問題，例えば整除の問題が立ち現れます．

この方面では，１８７８年に発表された Edouard Lucas の論文 Théorie des fonctions numériques simplement périodiques は大きな最初の一歩でした．論文を読むと，Mersenne 数が素数であるか否かを判定する方法の確立が Lucas の研究の目的の一つだったことが分かります．彼の結果は Lucas の判定法として素数についての論著ではしばしば引用されています．ここではその副産物であったかもしれない Lucas の lois de l'apparition et la répétition を紹介します．数値例を眺めることから始めます．

定義１．P, Q を整数 $\neq 0$ とする．初項 $L_0 = 0$, $L_1 = 1$ および線型漸化式 $L_{k+2} = PL_{k+1} - QL_k$ によって定義される数列 $(L_k)_{k\geq 0}$ を (P, Q) に伴う Lucas 数列という．

例２．$P = 1$, $Q = -1$ に伴う Lucas 数列は Fibonacci 数列 $(F_k)_{k\geq 0}$ に他ならない．例えば，

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ F_7 = 13,\ F_8 = 21,\ F_9 = 34,\ F_{10} = 55,$$
$$F_{11} = 89,\ F_{12} = 144,\ F_{13} = 233,\ F_{14} = 377,\ F_{15} = 610,\ F_{16} = 987,\ F_{17} = 1597,\ F_{18} = 2584,$$
$$F_{19} = 4181,\ F_{20} = 6765,\ F_{21} = 10946, \ldots$$

例３．$P = 2$, $Q = -1$ に伴う Lucas 数列は Pell 数列 $(P_k)_{k\geq 0}$ に他ならない．例えば，

$$P_0 = 0,\ P_1 = 1,\ P_2 = 2,\ P_3 = 5,\ P_4 = 12,\ P_5 = 29,\ P_6 = 70,\ P_7 = 169,\ P_8 = 408,\ P_9 = 985,$$
$$P_{10} = 2378,\ P_{11} = 5741,\ P_{12} = 13860,\ P_{13} = 33461,\ P_{14} = 80782,\ P_{15} = 195025,\ P_{16} = 470832,$$
$$P_{17} = 1136689,\ P_{18} = 2744210,\ P_{19} = 6625109,\ P_{20} = 15994428,\ P_{21} = 38613965, \ldots$$

命題４．(Binet の公式) α, β を二次方程式 $t^2 - Pt + Q = 0$ の根とする．$\alpha \neq \beta$ なら $L_k = \dfrac{\alpha^k - \beta^k}{\alpha - \beta}$ $(k \geq 0)$ が成立する．

例５．$F_k = \dfrac{1}{\sqrt{5}}\left\{\left(\dfrac{1+\sqrt{5}}{2}\right)^k - \left(\dfrac{1-\sqrt{5}}{2}\right)^k\right\}$

例６．$P_k = \dfrac{1}{2\sqrt{2}}\{(1+\sqrt{2})^k - (1-\sqrt{2})^k\}$

観察７．素数 p を法とする Fibonacci 数列

(1) $p = 2$

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 0,\ F_4 = 1,\ F_5 = 1,\ F_6 = 0, \ldots$$

(2) $p = 3$

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 0,\ F_5 = 2,\ F_6 = 2,\ F_7 = 1,\ F_8 = 0,\ F_9 = 1, \ldots$$

(3) $p = 5$

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 0,\ F_6 = 3,\ F_7 = 3,\ F_8 = 1,\ F_9 = 4,$$
$$F_{10} = 0,\ F_{11} = 4,\ F_{12} = 4,\ F_{13} = 3,\ F_{14} = 2,\ F_{15} = 0,\ F_{16} = 2,\ F_{17} = 2,\ F_{18} = 4,\ F_{19} = 1,$$
$$F_{20} = 0,\ F_{21} = 1, \ldots$$

(4) $p = 7$

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 1,\ F_7 = 6,$$
$$F_8 = 0,\ F_9 = 6,\ F_{10} = 6,\ F_{11} = 5,\ F_{12} = 4,\ F_{13} = 2,\ F_{14} = 6,\ F_{15} = 1,$$
$$F_{16} = 0,\ F_{17} = 1, \ldots$$

(5) $p = 11$

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ F_7 = 2,\ F_8 = 10,\ F_9 = 1,$$
$$F_{10} = 0,\ F_{11} = 1, \ldots$$

(6) $p = 13$

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,$$
$$F_7 = 0,\ F_8 = 8,\ F_9 = 8,\ F_{10} = 3,\ F_{11} = 11,\ F_{12} = 1,\ F_{13} = 12,$$
$$F_{14} = 0,\ F_{15} = 12,\ F_{16} = 12,\ F_{17} = 11,\ F_{18} = 10,\ F_{19} = 8,\ F_{20} = 5,$$
$$F_{21} = 0,\ F_{22} = 5,\ F_{23} = 5,\ F_{24} = 10,\ F_{25} = 2,\ F_{26} = 12,\ F_{27} = 1,$$
$$F_{28} = 0,\ F_{22} = 1, \ldots$$

(7) $p = 17$

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ F_7 = 13,\ F_8 = 4,$$
$$F_9 = 0,\ F_{10} = 4,\ F_{11} = 4,\ F_{12} = 8,\ F_{13} = 12,\ F_{14} = 3,\ F_{15} = 15,\ F_{16} = 1,\ F_{17} = 16,$$
$$F_{18} = 0,\ F_{19} = 16,\ F_{20} = 16,\ F_{21} = 15,\ F_{22} = 14,\ F_{23} = 12,\ F_{24} = 9,\ F_{25} = 4,\ F_{26} = 13,$$
$$F_{27} = 0,\ F_{28} = 13,\ F_{29} = 13,\ F_{30} = 9,\ F_{31} = 5,\ F_{32} = 14,\ F_{33} = 2,\ F_{34} = 16,\ F_{35} = 1,$$
$$F_{36} = 0,\ F_{37} = 1, \ldots$$

(8) $p = 19$

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ F_7 = 13,\ F_8 = 2,$$
$$F_9 = 15,\ F_{10} = 17,\ F_{11} = 13,\ F_{12} = 11,\ F_{13} = 5,\ F_{14} = 16,\ F_{15} = 2,\ F_{16} = 18,\ F_{17} = 1,$$
$$F_{18} = 0,\ F_{19} = 1, \ldots$$

観察８．素数 p を法とする Pell 数列

(1) $p = 2$

$$P_0 = 0,\ P_1 = 1,\ P_2 = 0,\ P_3 = 1,\ P_4 = 0,\ P_5 = 1, \ldots$$

(2) $p = 3$

$$P_0 = 0,\ P_1 = 1,\ P_2 = 2,\ P_3 = 2,\ P_4 = 0,\ P_5 = 2,\ P_6 = 1,\ P_7 = 1,\ P_8 = 0,\ P_9 = 1, \ldots$$

(3) $p = 5$

$$P_0 = 0,\ P_1 = 1,\ P_2 = 2,\ P_3 = 0,\ P_4 = 2,\ P_5 = 4,$$
$$P_6 = 0,\ P_7 = 4,\ P_8 = 3,\ P_9 = 0,\ P_{10} = 3,\ P_{11} = 1,$$
$$P_{12} = 0,\ P_{13} = 1, \ldots$$

(4) $p = 7$

$$P_0 = 0,\ P_1 = 1,\ P_2 = 2,\ P_3 = 5,\ P_4 = 5,\ P_5 = 1,$$
$$P_6 = 0,\ P_7 = 1, \ldots$$

(5) $p = 11$

$$P_0 = 0,\ P_1 = 1,\ P_2 = 2,\ P_3 = 5,\ P_4 = 1,\ P_5 = 7,$$
$$P_6 = 4,\ P_7 = 4,\ P_8 = 1,\ P_9 = 6,\ P_{10} = 2,\ P_{11} = 10,$$
$$P_{12} = 0,\ P_{13} = 10,\ P_{14} = 9,\ P_{15} = 6,\ P_{16} = 10,\ P_{17} = 4,$$
$$P_{18} = 7,\ P_{19} = 7,\ P_{20} = 10,\ P_{21} = 5,\ P_{22} = 9,\ P_{23} = 1,$$
$$P_{24} = 0,\ P_{25} = 1, \ldots$$

(6) $p = 13$

$$P_0 = 0,\ P_1 = 1,\ P_2 = 2,\ P_3 = 5,\ P_4 = 12,\ P_5 = 3,\ P_6 = 5,$$
$$P_7 = 0,\ P_8 = 5,\ P_9 = 10,\ P_{10} = 12,\ P_{11} = 8,\ P_{12} = 2,\ P_{13} = 12,$$
$$P_{14} = 0,\ P_{15} = 12,\ P_{16} = 11,\ P_{17} = 8,\ P_{18} = 1,\ P_{19} = 10,\ P_{20} = 8,$$
$$P_{21} = 0,\ P_{22} = 8,\ P_{23} = 3,\ P_{24} = 1,\ P_{25} = 5,\ P_{26} = 11,\ P_{27} = 1,$$
$$P_{28} = 0,\ P_{29} = 1, \ldots$$

(7) $p = 17$

$$P_0 = 0,\ P_1 = 1,\ P_2 = 2,\ P_3 = 5,\ P_4 = 12,\ P_5 = 12,\ P_6 = 2,\ P_7 = 16,$$
$$P_8 = 0,\ P_9 = 16,\ P_{10} = 15,\ P_{11} = 12,\ P_{12} = 5,\ P_{13} = 5,\ P_{14} = 15,\ P_{15} = 1,$$
$$P_{16} = 0,\ P_{17} = 1, \ldots$$

(8) $p = 19$

$$P_0 = 0,\ P_1 = 1,\ P_2 = 2,\ P_3 = 5,\ P_4 = 12,\ P_5 = 10,\ P_6 = 13,\ P_7 = 17,\ P_8 = 9,\ P_9 = 16,$$
$$P_{10} = 3,\ P_{11} = 3,\ P_{12} = 9,\ P_{13} = 2,\ P_{14} = 13,\ P_{15} = 9,\ P_{16} = 12,\ P_{17} = 14,\ P_{18} = 2,\ P_{19} = 18,$$
$$P_{20} = 0,\ P_{21} = 18,\ P_{22} = 17,\ P_{23} = 14,\ P_{24} = 7,\ P_{25} = 9,\ P_{26} = 6,\ P_{27} = 2,\ P_{28} = 10,\ P_{29} = 3,$$
$$P_{30} = 16,\ P_{31} = 16,\ P_{32} = 10,\ P_{33} = 17,\ P_{34} = 6,\ P_{35} = 10,\ P_{36} = 7,\ P_{37} = 5,\ P_{38} = 17,\ P_{39} = 1,$$
$$P_{40} = 0,\ P_{41} = 1, \ldots$$

定義 9．P, Q を整数 $\neq 0$，$(L_k)_{k\geq 0}$ を (P,Q) に伴う Lucas 数列とし，m を整数 ≥ 2 とする．$L_k \equiv 0 \mod m$ となるような最小の正の整数を，もし存在すれば，Lucas 数列 $(L_k)_{k\geq 0}$ の m を法とする rank といい，$r(m)$ で表わす．

定義 10．P, Q を整数 $\neq 0$，$(L_k)_{k\geq 0}$ を (P,Q) に伴う Lucas 数列とし，m を整数 ≥ 2 とする．$L_k \equiv 0 \mod m$, $L_{k+1} \equiv 1 \mod m$ となるような最小の正の整数を，もし存在すれば，Lucas 数列 $(L_k)_{k\geq 0}$ の m を法とする period といい，$k(m)$ で表わす．

定義 11．(Legendre 記号) p を素数 > 2 とする．p と互いに素な整数 a に対して

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & (a \text{ が } p \text{ を法として平方元}) \\ -1 & (a \text{ が } p \text{ を法として非平方元}) \end{cases}$$

と定義する．

定理 12．(Lucas の lois de l'apparition et la répétition I) P, Q を整数 $\neq 0$，$(L_k)_{k\geq 0}$ を (P,Q) に伴う Lucas 数列とし，p を素数 > 2 とする．このとき，$p \nmid Q$ なら $(L_k)_{k\geq 0}$ の p を法とする rank $r(p)$ が存在する．さらに，$L_k \equiv 0 \mod p \Leftrightarrow r(p)|k$．また，$D = P^2 - 4Q$ とおけば，

(1) $\left(\frac{D}{p}\right) = 1$ なら，$r(p)|(p-1)$.

(2) $\left(\frac{D}{p}\right) = -1$ なら，$r(p)|(p+1)$.

定義 13．P, Q を整数 $\neq 0$ とする．初項 $S_0 = 2$, $S_1 = P$ および線型漸化式 $S_{k+2} = PS_{k+1} - QS_k$ によって定義される数列 $(S_k)_{k\geq 0}$ を (P,Q) に伴う companion Lucas 数列という．

α, β を二次方程式 $t^2 - Pt + Q = 0$ の根とする．このとき，$S_k = \alpha^k + \beta^k$ $(k \geq 0)$ が成立する．

例 1 4．$P=1, Q=-1$

$$S_0=2,\ S_1=1,\ S_2=3,\ S_3=4,\ S_4=7,\ S_5=11,\ S_6=18,\ S_7=29,\ S_8=47,\ S_9=76,$$
$$S_{10}=123,\ S_{11}=199,\ S_{12}=322,\ S_{13}=521,\ S_{14}=843,\ S_{15}=1264,\ S_{16}=2207,$$
$$S_{17}=3571,\ S_{18}=5778,\ S_{19}=9349,\ S_{20}=15127,\ S_{21}=24476,\ldots$$

例 1 5．$P=2, Q=-1$

$$S_0=2,\ S_1=2,\ S_2=6,\ S_3=14,\ S_4=34,\ S_5=82,\ S_6=198,\ S_7=478,\ S_8=1154,\ S_9=2786,$$
$$S_{10}=6726,\ S_{11}=16238,\ S_{12}=39202,\ S_{13}=94642,\ S_{14}=228486,\ S_{15}=551614,\ S_{16}=1331714,$$
$$S_{17}=3215042,\ S_{18}=7761798,\ S_{19}=18738638,\ S_{20}=45239074,\ S_{21}=109216786,\ldots$$

観察 1 6．素数 p を法とする companion Lucas 数列，$P=1, Q=-1$

(1) $p=3$

$$S_0=2,\ S_1=1,\ S_2=0,\ S_3=1,\ S_4=1,\ S_5=2,\ S_6=0,\ S_7=2,\ S_8=2,\ S_9=1,\ldots$$

(2) $p=5$

$$S_0=2,\ S_1=1,\ S_2=3,\ S_3=4,\ S_4=2,\ S_5=1,\ S_6=3,\ S_7=4,\ S_8=2,\ S_9=1,$$
$$S_{10}=3,\ S_{11}=4,\ S_{12}=2,\ S_{13}=1,\ S_{14}=3,\ S_{15}=4,\ S_{16}=2,\ S_{17}=1,\ S_{18}=3,\ S_{19}=4,$$
$$S_{20}=2,\ S_{21}=1,\ldots$$

(3) $p=7$

$$S_0=2,\ S_1=1,\ S_2=3,\ S_3=4,\ S_4=0,\ S_5=4,\ S_6=4,\ S_7=1,$$
$$S_8=5,\ S_9=6,\ S_{10}=4,\ S_{11}=3,\ S_{12}=0,\ S_{13}=3,\ S_{14}=3,\ S_{15}=6,$$
$$S_{16}=2,\ S_{17}=1,\ldots$$

(4) $p=11$

$$S_0=2,\ S_1=1,\ S_2=3,\ S_3=4,\ S_4=7,\ S_5=0,\ S_6=7,\ S_7=7,\ S_8=3,\ S_9=10,$$
$$S_{10}=2,\ S_{11}=1,\ldots$$

(5) $p=13$

$$S_0=2,\ S_1=1,\ S_2=3,\ S_3=4,\ S_4=7,\ S_5=11,\ S_6=5,$$
$$S_7=3,\ S_8=8,\ S_9=11,\ S_{10}=6,\ S_{11}=4,\ S_{12}=10,\ S_{13}=1,$$
$$S_{14}=11,\ S_{15}=12,\ S_{16}=10,\ S_{17}=9,\ S_{18}=6,\ S_{19}=2,\ S_{20}=8,$$
$$S_{21}=10,\ S_{22}=5,\ S_{23}=2,\ S_{24}=7,\ S_{25}=9,\ S_{26}=3,\ S_{27}=12,$$
$$S_{28}=2,\ S_{22}=1,\ldots$$

(6) $p=17$

$$S_0=2,\ S_1=1,\ S_2=3,\ S_3=4,\ S_4=7,\ S_5=11,\ S_6=1,\ S_7=12,\ S_8=13,$$
$$S_9=8,\ S_{10}=4,\ S_{11}=12,\ S_{12}=16,\ S_{13}=11,\ S_{14}=10,\ S_{15}=4,\ S_{16}=14,\ S_{17}=1,$$
$$S_{18}=15,\ S_{19}=16,\ S_{20}=14,\ S_{21}=13,\ S_{22}=10,\ S_{23}=6,\ S_{24}=16,\ S_{25}=5,\ S_{26}=4,$$
$$S_{27}=9,\ S_{28}=13,\ S_{29}=5,\ S_{30}=1,\ S_{31}=6,\ S_{32}=7,\ S_{33}=13,\ S_{34}=3,\ S_{35}=16,$$
$$S_{36}=2,\ S_{37}=1,\ldots$$

(7) $p = 19$

$$S_0 = 2,\ S_1 = 1,\ S_2 = 3,\ S_3 = 4,\ S_4 = 7,\ S_5 = 11,\ S_6 = 18,\ S_7 = 10,\ S_8 = 9,$$
$$S_9 = 0,\ S_{10} = 9,\ S_{11} = 9,\ S_{12} = 18,\ S_{13} = 8,\ S_{14} = 7,\ S_{15} = 15,\ S_{16} = 3,\ S_{17} = 18,$$
$$S_{18} = 2,\ S_{19} = 1, \ldots$$

観察 1 7．素数 p を法とする companion Lucas 数列，$P = 2, Q = -1$

(1) $p = 3$

$$S_0 = 2,\ S_1 = 2,\ S_2 = 0,\ S_3 = 2,\ S_4 = 1,\ S_5 = 1,\ S_6 = 0,\ S_7 = 1,\ S_8 = 2,\ S_9 = 2, \ldots$$

(2) $p = 5$

$$S_0 = 2,\ S_1 = 2,\ S_2 = 1,\ S_3 = 4,\ S_4 = 4,\ S_5 = 2,$$
$$S_6 = 3,\ S_7 = 3,\ S_8 = 4,\ S_9 = 1,\ S_{10} = 1,\ S_{11} = 3,$$
$$S_{12} = 2,\ S_{13} = 2, \ldots$$

(3) $p = 7$

$$S_0 = 2,\ S_1 = 2,\ S_2 = 6,\ S_3 = 0,\ S_4 = 6,\ S_5 = 5,$$
$$S_6 = 2,\ S_7 = 1, \ldots$$

(4) $p = 11$

$$S_0 = 2,\ S_1 = 2,\ S_2 = 6,\ S_3 = 3,\ S_4 = 1,\ S_5 = 5,$$
$$S_6 = 0,\ S_7 = 5,\ S_8 = 10,\ S_9 = 3,\ S_{10} = 5,\ S_{11} = 2,$$
$$S_{12} = 9,\ S_{13} = 9,\ S_{14} = 5,\ S_{15} = 8,\ S_{16} = 10,\ S_{17} = 6,$$
$$S_{18} = 0,\ S_{19} = 6,\ S_{20} = 1,\ S_{21} = 8,\ S_{22} = 6,\ S_{23} = 9,$$
$$S_{24} = 2,\ S_{25} = 2, \ldots$$

(5) $p = 13$

$$S_0 = 2,\ S_1 = 2,\ S_2 = 6,\ S_3 = 1,\ S_4 = 8,\ S_5 = 4,\ S_6 = 3,$$
$$S_7 = 10,\ S_8 = 10,\ S_9 = 4,\ S_{10} = 5,\ S_{11} = 1,\ S_{12} = 7,\ S_{13} = 2,$$
$$S_{14} = 11,\ S_{15} = 11,\ S_{16} = 7,\ S_{17} = 12,\ S_{18} = 5,\ S_{19} = 9,\ S_{20} = 10,$$
$$S_{21} = 3,\ S_{22} = 3,\ S_{23} = 9,\ S_{24} = 8,\ S_{25} = 12,\ S_{26} = 6,\ S_{27} = 11,$$
$$S_{28} = 2,\ S_{29} = 2, \ldots$$

(6) $p = 17$

$$S_0 = 2,\ S_1 = 2,\ S_2 = 6,\ S_3 = 14,\ S_4 = 0,\ S_5 = 14,\ S_6 = 11,\ S_7 = 2,$$
$$S_8 = 15,\ S_9 = 15,\ S_{10} = 11,\ S_{11} = 3,\ S_{12} = 0,\ S_{13} = 3,\ S_{14} = 6,\ S_{15} = 15,$$
$$S_{16} = 2,\ S_{17} = 2, \ldots$$

(7) $p = 19$

$S_0 = 2,\ S_1 = 2,\ S_2 = 6,\ S_3 = 14,\ S_4 = 15,\ S_5 = 6,\ S_6 = 8,\ S_7 = 3,\ S_8 = 14,\ S_9 = 12,$
$S_{10} = 0,\ S_{11} = 12,\ S_{12} = 5,\ S_{13} = 3,\ S_{14} = 11,\ S_{15} = 6,\ S_{16} = 4,\ S_{17} = 14,\ S_{18} = 13,\ S_{19} = 2,$
$S_{20} = 17,\ S_{21} = 17,\ S_{22} = 13,\ S_{23} = 5,\ S_{24} = 4,\ S_{25} = 13,\ S_{26} = 11,\ S_{27} = 16,\ S_{28} = 5,\ S_{29} = 7,$
$S_{30} = 0,\ S_{31} = 7,\ S_{32} = 14,\ S_{33} = 16,\ S_{34} = 8,\ S_{35} = 13,\ S_{36} = 15,\ S_{37} = 5,\ S_{38} = 6,\ S_{39} = 17,$
$S_{40} = 2,\ S_{41} = 2, \ldots$

定理１８．(Lucas の lois de l'apparition et la répétition II) P, Q を整数 $\neq 0$，$(S_k)_{k\geq 0}$ を (P, Q) に伴う companion Lucas 数列，p を素数 > 2 とし，$p \nmid Q$ と仮定する．このとき，$S_k \equiv 0 \mod p$ となるような k が存在する $\Leftrightarrow 2|r(p)$.

４．風景の広がりを感じる〜lois de l'apparition et la répétition の証明に向けて

Edouard Lucas, Théorie des fonctions numériques simplement périodiques での lois de l'apparition et la répétition の証明は，さらに，１９１３年に発表された Robert Daniel Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$ での別証は，高校数学の範囲でも理解でき，また理論としてさらに発展させられる方法ですが，ここでは抽象化の効用という視点から証明に必要な概念を俯瞰することにします．特に，群論における位数の概念が鍵となります．

定義１．n を整数 ≥ 2 とする．$a, b \in \mathbb{Z}$ に対して $a - b$ が n で割り切れるとき a は b に n を法として合同であるといい，$a \equiv b \mod n$ と記す．

命題２．n を整数 ≥ 2 とする．このとき，
(1) $a \equiv a \mod n$.
(2) $a \equiv b \mod n$ なら，$b \equiv a \mod n$.
(3) $a \equiv b \mod n$, $b \equiv c \mod n$ なら，$a \equiv c \mod n$.
(4) $a \equiv b \mod n$, $c \equiv d \mod n$ なら，$a + c \equiv b + d \mod n$.
(5) $a \equiv b \mod n$, $c \equiv d \mod n$ なら，$ac \equiv bd \mod n$.

定義３．A を可換環，$\mathfrak{a}$ を A のイデアルとする．$a, b \in \mathbb{Z}$ に対して $a - b \in \mathfrak{a}$ のとき a は b に $\mathfrak{a}$ を法として合同であるといい，$a \equiv b \mod \mathfrak{a}$ と記す．

命題４．A を可換環，$\mathfrak{a}$ を A のイデアルとする．このとき，
(1) $a \equiv a \mod \mathfrak{a}$.
(2) $a \equiv b \mod \mathfrak{a}$ なら，$b \equiv a \mod \mathfrak{a}$.
(3) $a \equiv b \mod \mathfrak{a}$, $b \equiv c \mod \mathfrak{a}$ なら，$a \equiv c \mod \mathfrak{a}$.
(4) $a \equiv b \mod \mathfrak{a}$, $c \equiv d \mod \mathfrak{a}$ なら，$a + c \equiv b + d \mod \mathfrak{a}$.
(5) $a \equiv b \mod \mathfrak{a}$, $c \equiv d \mod \mathfrak{a}$ なら，$ac \equiv bd \mod \mathfrak{a}$.

命題５．n, m を互いに素な整数 ≥ 2 とする．このとき，任意の整数 a, b に対して連立合同方程式 $x \equiv a \mod n$, $x \equiv b \mod m$ は nm を法として唯一つ解を持つ．

命題６．A を可換環，$\mathfrak{a}$, $\mathfrak{b}$ を A のイデアルとし，$\mathfrak{a} + \mathfrak{b}$ と仮定する．このとき，$\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$．さらに，対応 $a \mapsto (a \mod \mathfrak{a}, a \mod \mathfrak{b})$ によって定義される環の準同型 $\varphi : A \to A/\mathfrak{a} \times A/\mathfrak{b}$ は環の同型 $A \xrightarrow{\sim} A/\mathfrak{a} \times A/\mathfrak{b}$ を誘導する．

命題７．(剰余定理) $f(t)$ を実係数多項式，a を実数とする．このとき，$f(t)$ を $t - a$ で割ったときの剰余は $f(a)$ に等しい．

定理８．(環の準同型定理) $\varphi : A \to B$ を環の準同型とし，剰余環 $A/\mathrm{Ker}\,\varphi$ における a の類を $[a]$ で表わす．このとき，$\tilde{\varphi}([a]) = \varphi(a)$ によって環の準同型 $\tilde{\varphi} : A/\mathrm{Ker}\,\varphi \to B$ が定義される．さらに，$\tilde{\varphi} : A/\mathrm{Ker}\,\varphi \to B$ は環の同型 $\tilde{\varphi} : A/\mathrm{Ker}\,\varphi \xrightarrow{\sim} \mathrm{Im}\,\varphi$ を誘導する．

例９．対応 $f(t) \mapsto f(i)$ によって定義される環の準同型 $\varphi : \mathbb{R}[t] \to \mathbb{C}$ は環の同型 $\tilde{\varphi} : \mathbb{R}[t]/(t^2+1) \xrightarrow{\sim} \mathbb{C}$ を誘導する．

記号/観察１０．P, Q を整数とし，$D = P^2 - 4Q$ とおく．このとき，$D \equiv 0, 1 \mod 4$．D は二次式 $t^2 - Pt + Q$ の判別式に他ならない．以下，D が平方数でないと仮定する．

$$R_D = \begin{cases} \mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D}\ ;\ a, b \in \mathbb{Z}\} & (D \equiv 0 \mod 4) \\ \mathbb{Z}\big[\dfrac{1+\sqrt{D}}{2}\big] = \Big\{\dfrac{a+b\sqrt{D}}{2}\ ;\ a, b \in \mathbb{Z},\ a \equiv b \mod 2\Big\} & (D \equiv 1 \mod 4) \end{cases}$$

と記すことにする．このとき，対応

$$t \mapsto \frac{P + \sqrt{D}}{2}$$

によって定義される環の準同型 $\varphi : \mathbb{Z}[t] \to \mathbb{C}$ は環の同型 $\tilde{\varphi} : \mathbb{Z}[t]/(t^2 - Pt + Q) \xrightarrow{\sim} R_D$ を誘導する．

さらに，$\eta = a + b\sqrt{D}$ $(a, b \in \mathbb{Q})$ に対して $\bar{\eta} = a - b\sqrt{D}$ と記すことにする．このとき，$\eta, \xi \in R_D$ に対して $\overline{\eta + \xi} = \bar{\eta} + \bar{\xi}$, $\overline{\eta\xi} = \bar{\eta}\,\bar{\xi}$ が成立する．

記号１１．p を素数とする．このとき，剰余環 $\mathbb{Z}/p\mathbb{Z}$ は体．$\mathbb{Z}/p\mathbb{Z}$ を $\mathbb{F}_p$ とも記す．

観察１２．P, Q を整数とし，$D = P^2 - 4Q$ とおく．D が平方数でないと仮定する．このとき，対応

$$t \mapsto \frac{P + \sqrt{D}}{2}$$

によって環の同型 $\tilde{\varphi} : \mathbb{Z}[t]/(t^2 - Pt + Q) \xrightarrow{\sim} R_D$ が定義される．さらに，p を素数とすれば，環の同型 $\tilde{\varphi} : \mathbb{Z}[t]/(t^2 - Pt + Q) \xrightarrow{\sim} R_D$ は p を法とする還元によって環の同型 $\tilde{\varphi} : \mathbb{F}_p[t]/(t^2 - Pt + Q) \xrightarrow{\sim} R_D/(p)$ を誘導する．また，可換図式

$$\begin{array}{ccc} \mathbb{Z}[t]/(t^2 - Pt + Q) & \xrightarrow{\tilde{\varphi}} & R_D \\ \downarrow & & \downarrow \\ \mathbb{F}_p[t]/(t^2 - Pt + Q) & \xrightarrow{\tilde{\varphi}} & R_D/(p) \end{array}$$

を得る．

定理１３．(Fermat の定理) p を素数，a を整数とする．このとき，$a^p \equiv a \mod p$ が成立する．さらに，a が p と素なら，$a^{p-1} \equiv 1 \mod p$ が成立する．

言換え１４．p を素数，$a \in \mathbb{F}_p$ とする．このとき，$a^p = a$ が成立する．さらに，$a \neq 0$ なら，$a^{p-1} = 1$ が成立する．

定理１５．(Euler の判定法) p を素数 > 2，a を p と素な整数とする．このとき，$\left(\dfrac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.

言換え１６．p を素数 > 2，$a \in \mathbb{F}_p$ $(a \neq 0)$ とする．このとき，$a^{(p-1)/2} = \pm 1$．さらに，a が $\mathbb{F}_p$ の平方元 $\Leftrightarrow a^{(p-1)/2} = 1$.

観察１７．p を素数 > 2，P, Q を整数とし，$D = P^2 - 4Q$ とおく．このとき，$t \mapsto (t + P)/2$ によって定義される環の同型 $\mathbb{F}_p[t] \xrightarrow{\sim} \mathbb{F}_p[t]$ は環の同型 $\mathbb{F}_p[t]/(t^2 - Pt + Q) \xrightarrow{\sim} \mathbb{F}_p[t]/(t^2 - D)$ を誘導する．また，$t^2 - Pt + Q$ が $\mathbb{F}_p[t]$ において可約 $\Leftrightarrow$ D が $\mathbb{F}_p$ の平方元.

(a) D が $\mathbb{F}_p$ の平方元 $\neq 0$ である場合．$r \in \mathbb{F}_p$ $(r \neq 0)$ が存在して $r^2 = D$ となる．さらに，対応

$$t \mapsto \Big(\frac{P+r}{2}, \frac{P-r}{2}\Big)$$

によって定義される環の準同型 $\psi : \mathbb{Z}[t] \to \mathbb{F}_p \times \mathbb{F}_p$ は環の同型 $\tilde{\psi} : \mathbb{F}_p[t]/(t^2 - Pt + Q) \xrightarrow{\sim} \mathbb{F}_p \times \mathbb{F}_p$ を誘導する．

(b) D が $\mathbb{F}_p$ の非平方元である場合．t の $\mathbb{F}_p[t]/(t^2 - Pt + Q)$ における類を $\sqrt{D}$ と記せば，

$$\mathbb{F}_p[t]/(t^2 - Pt + Q) = \mathbb{F}_p(\sqrt{D}) = \{a + b\sqrt{D}\,;\ a, b \in \mathbb{F}_p\}$$

と見なせる．さらに，$(a, b) \neq (0, 0)$ なら，$\dfrac{1}{a + b\sqrt{D}} = \dfrac{a - b\sqrt{D}}{a^2 - Db^2}$．したがって，$\mathbb{F}_p(\sqrt{D})$ は体．

また，Euler の判定法から $\sqrt{D}^p = -\sqrt{D}$ を，さらに Fermat の定理から $(a + b\sqrt{D})^p = a - b\sqrt{D}$ を得る．

観察 1 8．P, Q を整数とし，$D = P^2 - 4Q$ とおく．D が平方数でないと仮定とする．さらに，p を素数 > 2 とする．このとき，

(a) $\Big(\dfrac{D}{p}\Big) = 1$ なら，各 $\eta \in R_D$ に対して $\psi(\eta) = (a, b)$ とおけば $\psi(\bar{\eta}) = (b, a)$ が成立する．

(b) $\Big(\dfrac{D}{p}\Big) = -1$ なら，各 $\eta \in R_D$ に対して $\bar{\eta} \equiv \eta^p \mod p$ が成立する．

系 1 9．P, Q を整数 $\neq 0$，$(L_k)_{k\geq 0}$, $(S_k)_{k\geq 0}$ をそれぞれ (P, Q) に伴う Lucas 数列あるいは companion Lucas 数列とする．また，$D = P^2 - 4Q$ とおき，$D \neq 0$ と仮定する．さらに，p を素数 > 2 とする．このとき，

(a) $\Big(\dfrac{D}{p}\Big) = 1$ なら，$L_{pk} \equiv L_k \mod p$．特に，$L_p \equiv L_1 \mod p$.

(b) $\Big(\dfrac{D}{p}\Big) = -1$ なら，$L_{pk} \equiv -L_k \mod p$．特に，$L_p \equiv -L_1 \mod p$.

(c) $S_{pk} \equiv S_k \mod p$．特に，$S_p \equiv S_1 \mod p$.

証明．$\alpha = \dfrac{P + \sqrt{D}}{2}$, $\beta = \dfrac{P - \sqrt{D}}{2}$ とおく．D が平方数なら，$\mathbb{Z}$ において

$$S_{pk} = \alpha^{pk} + \beta^{pk} \equiv \alpha^k + \beta^k = S_k \mod p$$

さらに，$(p, D) = 1$ なら，$\mathbb{Z}$ において

$$L_{pk} = \frac{\alpha^{pk} - \beta^{pk}}{\sqrt{D}} \equiv \frac{\alpha^k - \beta^k}{\sqrt{D}} = L_k \mod p$$

以下，D が平方数でないと仮定する．このとき，R_D において $\alpha^{pk} + \beta^{pk} \equiv \alpha^k + \beta^k \mod p$．ここで，$pR_D \cap \mathbb{Z} = p\mathbb{Z}$ なので，$S_{pk} \equiv S_k \mod p$.

さらに，$\Big(\dfrac{D}{p}\Big) = 1$ なら，R_D において $\alpha^{pk} - \beta^{pk} \equiv \alpha^k - \beta^k \mod p$．ここで，$(D, p) = 1$ なので，

$$L_{pk} = \frac{(\alpha^{pk} - \beta^{pk})(\alpha - \beta)}{D} \equiv \frac{(\alpha^k - \beta^k)(\alpha - \beta)}{D} = L_k \mod p$$

一方，$\Big(\dfrac{D}{p}\Big) = -1$ なら，R_D において $\alpha^{pk} - \beta^{pk} \equiv -\alpha^k + \beta^k \mod p$．したがって，

$$L_{pk} = \frac{(\alpha^{pk} - \beta^{pk})(\alpha - \beta)}{D} \equiv \frac{(-\alpha^k + \beta^k)(\alpha - \beta)}{D} = -L_k \mod p$$

定義/定理２０．G を群，$g \in G$ とする．$g^r = 1$ となるような整数 $r \neq 0$ が存在するとき，g は有限位数であるという．g が有限位数であるとき，$g^r = 1$ となるような最小の正の整数 r を g の位数とよぶ．さらにこのとき，整数 n に対して，$g^n = 1 \Leftrightarrow n$ は r で割り切れる．

定理２１．(Lagrange の定理) G を有限群，$g \in G$ とする．このとき，g の位数は G の位数の約数．

観察２２．p を素数 > 2 とする．$S_k \equiv 0 \mod p \Leftrightarrow \alpha^k \equiv -\beta^k \mod p$．さらに，$p \nmid D$ と仮定する．このとき，$L_k \equiv 0 \mod p \Leftrightarrow \alpha^k \equiv \beta^k \mod p$.

観察２３．p を素数 > 2 とし，$p \nmid Q$ と仮定する．このとき．$S_k \equiv 0 \mod p \Leftrightarrow \mathbb{Z}/p\mathbb{Z}$ あるいは $R_D/(p)$ において $(\alpha/\beta)^k = -1$．さらに，$p \nmid D$ と仮定する．このとき，$L_k \equiv 0 \mod p \Leftrightarrow$ 剰余環 $\mathbb{Z}/p\mathbb{Z}$ あるいは $R_D/(p)$ において $(\alpha/\beta)^k = 1$.

Lucas の lois de l'apparition et la répétition I の証明.

観察２３から Lucas 数列 $(L_k)_{k\geq 0}$ の p を法とする rank $r(p)$ は乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ あるいは $(R_D/pR_D)^\times$ における α/β の位数に他ならない．D が平方数なら，$(\mathbb{Z}/p\mathbb{Z})^\times$ の位数が $p-1$ なので，Lagrange の定理から $r(p)$ は $p-1$ の約数．以下，D が平方数でないと仮定する．

(1) $\left(\dfrac{D}{p}\right) = 1$ の場合．観察１７から乗法群 $(R_D/pR_D)^\times$ は $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ に同型．したがって，$r(p)$ は $p-1$ の約数.

(2) $\left(\dfrac{D}{p}\right) = -1$ の場合．観察１８から剰余環 $R_D/pR_D = \mathbb{F}_p(\sqrt{D})$ において $\beta = \alpha^p$ なので，$\alpha/\beta = 1/\alpha^{p-1}$ が成立する．ここで，観察１７から乗法群 $(R_D/pR_D)^\times = \mathbb{F}_p(\sqrt{D})^\times$ の位数は p^2-1．したがって，Lagrange の定理から $(\alpha/\beta)^{p+1} = 1$．したがって，定理２０から $r(p)$ は $p+1$ の約数.

Lucas の lois de l'apparition et la répétition II の証明.

$S_k \equiv 0 \mod p$ となるような k が存在すると仮定する．さらに，$S_k \equiv 0 \mod p$ となるような最小の正の整数 k を取る．このとき，観察２３から剰余環 $\mathbb{Z}/p\mathbb{Z}$ あるいは R_D/pR_D において $(\alpha/\beta)^k = -1$ なので，乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ あるいは $(R_D/pR_D)^\times$ における α/β の位数は $2k$ に等しい．

逆に，$r(p)$ が偶数であると仮定し，$r(p) = 2k$ とおく．このとき，剰余環 $\mathbb{Z}/p\mathbb{Z}$ あるいは R_D/pR_D において $(\alpha/\beta)^{2k} = 1$ が成立する．D が平方数なら，剰余環 $\mathbb{Z}/p\mathbb{Z}$ が体なので，$\mathbb{Z}/p\mathbb{Z}$ において $(\alpha/\beta)^k = -1$. 以下，D が平方数でないと仮定する．

(1) $\left(\dfrac{D}{p}\right) = 1$ の場合．観察１８から，$\psi(\alpha/\beta) = (a, b)$ とおけば，$\psi(\beta/\alpha) = (b, a)$．さらに，$ab = 1$ が成立する．ここで，$(\alpha/\beta)^{2k} = 1$ なので，$a^{2k} = 1$，したがって，$a^k = -1$．したがって，$b^k = -1$，これから，$(\alpha/\beta)^k = -1$.

(2) $\left(\dfrac{D}{p}\right) = -1$ の場合．剰余環 $R/pR = \mathbb{F}_p(\sqrt{D})$ が体なので，R/pR において $(\alpha/\beta)^k = -1$.

５．悠久の流れを感じる～温故知新の一例

２０世紀半ばに Alexandre Grothendieck は Jean Deiudonné や若い俊英たちの協力を得て，代数幾何学で大変革を成し遂げ，数論幾何学に必要なインフラストラクチュアを整備しました．その成果の最たるものが Weil 予想の解決，Mordell 予想の解決，Fermat 予想の解決という驚異の三段跳びです.

さて，Lucas 数列を Grothendieck が構築した代数幾何学に結び付けることはつい最近まで考えたことはありませんでした．しかし，１９６９年に発表された論文 R. R. Laxton, On groups of linear recurrences の存在を知り，Grothendieck が構築した理論の一つである group scheme の理論の枠組みの中でその論文の内容を定式化できることに気付きました．今にしてみれば，Laxton の仕事は整数論の対象である Lucas

数列の可除性の問題を幾何的に捉えることを示唆した画期的なものだったと思います．しかし，残念ながらその仕事は見過ごされ忘れ去られたようです．Laxton は２０００年に亡くなったと伝え聞いています．半世紀後に彼の仕事を蘇らせることができたのは，数学に携わる仲間としてこれ以上ない喜びでした．

なお，ここで援用している group scheme の理論はその基礎事項だけであり，以下に述べることはすべて行列の言葉に翻訳することができます．ただ，group scheme 係数の cohomology 群の計算が決定的であるところが一ヶ所あり，ここを group scheme の理論を介さずに証明するのは相当に煩雑であろうと想像します．まだ評価の定まっていない仕事ですが，群作用の観点から Lucas 数列の可除性の問題を明晰に論述できたと考えています．ここでも群論における位数という概念が鍵になっています．

記号１．R を可換環，$P, Q \in R$ とし，$f(t) = t^2 - Pt + Q$ とおく．

$$\mathcal{L}(f, R) = \{(w_k)_{k\geq 0} \in R^{\mathbb{N}}\,;\, \text{各 } k \geq 0 \text{ に対して } w_{k+2} - Pw_{k+1} + Qw_k = 0 \text{ が成立する}\,\}$$

と記すことにする．このとき，対応 $(w_k)_{k\geq 0} \mapsto (w_0, w_1)$ は R 加群の同型 $\mathcal{L}(f, R) \xrightarrow{\sim} R^2$ を与える．また，$\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, R)$ に対して $\Delta(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2$ と定義する．

記号２．$\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, \mathbb{Z})$ とする．w_0 と w_1 が互いに素であるとき，$\boldsymbol{w}$ は reduced であるという．

$$\mathcal{R}(f, \mathbb{Z}) = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f, \mathbb{Z})\,;\, \boldsymbol{w} \text{ は reduced で，} w_0 > 0 \text{ または } w_0 = 0,\, w_1 = 1\}.$$

と記すことにする．

観察３．R を可換環，$P, Q \in R$ とし，$\tilde{R} = R[t]/(t^2 - Pt + Q)$ とおく．t の $\tilde{R}$ における類を θ で表わす．このとき，$\{1, \theta\}$ は $\tilde{R}$ の R 基底．したがって，R 加群の準同型 $\omega : \tilde{R} \to$ が $\omega(a + b\theta) = b$ $(a, b \in R)$ によって定義される．さらに，R 加群の準同型 $\omega : \tilde{R} \to R^{\mathbb{N}}$ を $\omega(\eta) = (\omega(\eta\theta^k))_{k\geq 0}$ によって定義すれば，ω は R 加群の同型 $\tilde{R} \xrightarrow{\sim} \mathcal{L}(f, R)$ を誘導する．実際，$\eta = a + b\theta \in \tilde{R}$ に対して $\omega(\eta) = (b, a + Pb, \dots)$ が成立する．

R 加群の同型 $\tilde{R} \xrightarrow{\sim} \mathcal{L}(f, R)$ を通して $\mathcal{L}(f, R)$ に乗法を定義する．このとき，$\boldsymbol{v}, \boldsymbol{w} \in \mathcal{L}(f, R)$ に対して

$$\boldsymbol{v}\boldsymbol{w} = (v_0w_1 + v_1w_0 - Pv_0w_0, v_1w_1 - Qv_0w_0, \dots)$$

が成立する．また，$\mathcal{L}(f, R)$ の単位元は Lucas 数列 $\boldsymbol{L} = (L_k)_{K\geq 0}$ によって与えられる．

さらに，$\eta \in \tilde{R}$, $\boldsymbol{w} = \omega(\eta) \in \mathcal{L}(f, R)$ とすれば，$\mathrm{Nr}_{\tilde{R}/R}\eta = \Delta(\boldsymbol{w})$ が成立する．したがって，$\boldsymbol{w}$ が $\omega(\eta) \in \mathcal{L}(f, R)$ において可逆 $\Leftrightarrow \Delta(\boldsymbol{w}) \in R^\times$．

観察４．対応 $(w_0, w_1) \mapsto (w_0 : w_1)$ は一対一対応 $\mathcal{R}(f, \mathbb{Z}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q})$ を与える．また，

$$\{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f, \mathbb{Z})\,;\, \Delta(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2 \neq 0\}$$

は $\mathcal{L}(f, \mathbb{Q})^\times/\mathbb{Q}^\times \subset \mathbb{P}^1(\mathbb{Q})$ の完全代表系．また，p を素数とすれば，

$$\{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{R}(f, \mathbb{Z})\,;\, \Delta(\boldsymbol{w}) = w_1^2 - Pw_0w_1 + Qw_0^2 \not\equiv 0 \mod p\}$$

は $\mathcal{L}(f, \mathbb{Z}_{(p)})^\times/\mathbb{Z}_{(p)}^\times \subset \mathbb{P}^1(\mathbb{Q})$ の完全代表系．

記号５．R を可換環，$P, Q \in R$ とし，$D = P^2 - 4Q$, $\tilde{R} = R[t]/(t^2 - Pt + Q)$ とおく．t の $\tilde{R}$ における類を θ で表わす．さらに，$\tilde{R}$ の乗法は

$$(a + b\theta)(a' + b'\theta) = (aa' - Qbb') + (ab' + a'b + Pbb')\ (a, b, a', b' \in R)$$

によって与えられる．したがって，Weil restriction $G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$ は Hopf 代数の言葉では

$$G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} = \mathrm{Spec}\, R\big[U, V, \frac{1}{U^2 + PUV + QV^2}\big]$$

(a) 乗法

$$U \mapsto U \otimes U - QV \otimes V,\ V \mapsto U \otimes V + V \otimes U + PV \otimes V;$$

(b) 単位元

$$U \mapsto 1,\ V \mapsto 0;$$

(c) 逆元

$$U \mapsto \frac{U + PV}{U^2 + PUV + QV^2},\ V \mapsto -\frac{V}{U^2 + PUV + QV^2}$$

と記述できる．さらに，埋め込み写像 $R^\times \to \tilde{R}^\times$ は

$$U \mapsto T,\ V \mapsto 0$$

によって定義される群スキームの準同型

$$i : \mathbb{G}_{m,R} = \operatorname{Spec} R\big[T, \frac{1}{T}\big] \to G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} R\big[U, V, \frac{1}{U^2 + rUV + sV^2}\big]$$

によって表現される．一方，norm 写像 $\mathrm{Nr} : \tilde{R}^\times \to R^\times$ は

$$T \mapsto U^2 + PUV + QV^2$$

によって定義される群スキームの準同型

$$\mathrm{Nr} : G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} R\big[U, V, \frac{1}{U^2 + PUV + QV^2}\big] \to \mathbb{G}_{m,R} = \operatorname{Spec} R\big[T, \frac{1}{T}\big]$$

によって表現される．

(1) $i : \mathbb{G}_{m,R} \to G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$ は closed immersion.

(2) $\mathrm{Nr} : G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}$ は faithfully flat.

(3) $\mathrm{Nr} \circ i : \mathbb{G}_{m,R} \to \mathbb{G}_{m,R}$ は二乗写像.

D が R において冪零でなければ，$G_{P,Q} \otimes_R R[1/D] = \big(\prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}\big) \otimes_R R[1/D]$ は $\tilde{R}[1/D]$ において分解する $R[1/D]$ の上の torus.

記号 6．$U_{P,Q} = \mathrm{Ker}[\mathrm{Nr} : \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}] = \mathrm{Ker}[\mathrm{Nr} : G_{P,Q} \to \mathbb{G}_{m,R}]$ とおく．このとき，

$$U_{P,Q} = \operatorname{Spec} R[U, V]/(U^2 + PUV + QV^2 - 1)$$

(a) 乗法

$$U \mapsto U \otimes U - QV \otimes V,\ V \mapsto U \otimes V + V \otimes U + PV \otimes V;$$

(b) 単位元

$$U \mapsto 1,\ V \mapsto 0;$$

(c) 逆元

$$U \mapsto U + PV,\ V \mapsto -V.$$

D が R において冪零でなければ，$U_{P,Q} \otimes_R R[1/D]$ は $\tilde{R}[1/D]$ において分解する $R[1/D]$ の上の torus.

記号７．$G_{(P,Q)} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}/\mathbb{G}_{m,R}$ とおく．具体的には

$$G_{(P,Q)} = \operatorname{Spec} R[X,Y]/(X^2 + PXY + QY^2 - Y)$$

(a) 乗法

$$X \mapsto X \otimes 1 + 1 \otimes X - PX \otimes X - 2QX \otimes Y - 2QY \otimes X - PQY \otimes Y,$$
$$Y \mapsto Y \otimes 1 + 1 \otimes Y + (P^2 - 2Q)Y \otimes Y + PX \otimes Y + PY \otimes X + 2X \otimes X;$$

(b) 単位元

$$X \mapsto 0,\ Y \mapsto 0$$

と記述できる．

さらに，群スキームの準同型

$$\beta : G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} R\big[U, V, \frac{1}{U^2 + PUV + QV^2}\big]$$
$$\to G_{(P,Q)} = \operatorname{Spec} R[X,Y]/(X^2 + PXY + QY^2 - Y)$$

が

$$X \mapsto \frac{UV}{U^2 + PUV + QV^2},\ Y \mapsto \frac{V^2}{U^2 + PUV + QV^2}$$

によって定義される．群スキームの列

$$0 \longrightarrow \mathbb{G}_{m,R} \xrightarrow{i} G_{P,Q} \xrightarrow{\beta} G_{(P,Q)} \to 0$$

は完全．

さらに，群スキームの準同型

$$\alpha : G_{(P,Q)} = \operatorname{Spec} R[X,Y]/(X^2 + PXY + QY^2 - Y) \to U_{P,Q} = \operatorname{Spec} R[U,V]/(U^2 + PUV + QV^2 - 1)$$

が

$$U \mapsto 1 - PX - 2QY,\ V \mapsto 2X + PY$$

によって定義される．D が R において冪零でなければ，α は $R[1/D]$ の上で同型．

また，群スキームの準同型

$$\gamma : G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} = \operatorname{Spec} R\big[U, V, \frac{1}{U^2 + PUV + QV^2}\big] \to U_{P,Q} = \operatorname{Spec} R[U,V]/(U^2 + PUV + QV^2 - 1)$$

を合成

$$G_{P,Q} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \xrightarrow{\beta} G_{(P,Q)} \xrightarrow{\alpha} U_{P,Q}$$

として定義する．したがって，γ は

$$U \mapsto \frac{U^2 - QV^2}{U^2 + PUV + QV^2},\ V \mapsto \frac{2UV + PV^2}{U^2 + PUV + QV^2}$$

によって与えられる．

定理８．P, Q を整数 $\neq 0$，$(L_k)_{k\geq 0}$ を (P,Q) に伴う Lucas 数列とし，m を正の整数とする．このとき，$(m,Q) = 1$ なら $(L_k)_{k\geq 0}$ の m を法とする rank $r(m)$ および period $k(m)$ が存在する．さらに，θ を $\mathbb{Z}[t]/(t^2 - Pt + Q)$ における t の像とすれば，

$$r(m) = [\theta \text{ の } G_{(P,Q)}(\mathbb{Z}/m\mathbb{Z}) \text{ における位数}],$$
$$k(m) = [\theta \text{ の } G_{P,Q}(\mathbb{Z}/m\mathbb{Z}) \text{ における位数}]$$

が成立する．

系９．P, Q を整数 $\neq 0$，m を整数 ≥ 2 とし，$(m,Q) = 1$ と仮定する．
(1) k を正の整数とする．このとき，$L_k \equiv 0 \mod m \Leftrightarrow r(m)|k$.
(2) k を正の整数とする．このとき，$L_k \equiv 0 \mod m$, $L_{k+1} \equiv 1 \mod m \Leftrightarrow k(m)|k$.
(3) $r(m)|k(m)$．さらに，$Q = 1$ なら

$$k(m) = \begin{cases} r(m) & k(m) \text{ が奇数} \\ 2r(m) & k(m) \text{ が偶数} \end{cases}$$

が成立する．

補題１０．P, Q を整数 $\neq 0$ とし，$D = P^2 - 4Q$ とおく．また，p を素数 > 2，n を正の整数とする．このとき，
(1) $\left(\dfrac{D}{p}\right) = 1$ なら，$G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ は位数 $(p-1)p^{n-1}$ の巡回群.
(2) $\left(\dfrac{D}{p}\right) = -1$ なら，$G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ は位数 $(p+1)p^{n-1}$ の巡回群.
(3) $p|D$ なら，$G_{(P,Q)}(\mathbb{Z}/p\mathbb{Z})$ は位数 p の巡回群．さらに，$p \neq 3$，または，$p = 3$, $D \not\equiv -3 \mod 9$ なら，$G_{(P,Q)}(\mathbb{Z}/p^n\mathbb{Z})$ は位数 p^n の巡回群.

命題１１．P, Q を整数 $\neq 0$，p を素数 > 2，n を正の整数とし，$(m,Q) = 1$ と仮定する．また，$\nu = \mathrm{ord}_p L_{r(p)}$ とおく．このとき，
(1) $\nu = \mathrm{ord}_p L_{k(p)}$
(2) $r(p^n) = \begin{cases} r(p) & (n \leq \nu) \\ p^{n-\nu} r(p) & (n > \nu) \end{cases}$
(3) $k(p^n) = \begin{cases} k(p) & (n \leq \nu) \\ p^{n-\nu} k(p) & (n > \nu) \end{cases}$

命題１２．P, Q を整数 $\neq 0$ とし，$D = P^2 - 4Q$ とおく．また，p を素数 > 2 とし，$(p,Q) = 1$ と仮定する．
(1) $\left(\dfrac{D}{p}\right) = 1$ なら，$k(p)|(p-1)$，また，$r(p)|(p-1)$.
(2) $\left(\dfrac{D}{p}\right) = -1$ なら，$k(p)|(p^2-1)$，また，$r(p)|(p+1)$.
(3) $p|D$ なら，$k(p)|p(p-1)$，また，$r(p) = p$．さらに，$p \neq 3$，または，$p = 3$, $D \not\equiv -3 \mod 9$ なら，$r(p^n) = p^n$，したがって，$\mathrm{ord}_p L_{r(p)} = 1$.

命題１３．P, Q を整数とする．$P \equiv 0 \mod 2$, $Q \equiv 1 \mod 2$, $P \neq 0$ と仮定し，$\nu = \mathrm{ord}_2 P$ とおく．このとき，
(1) $r(2^n) = \begin{cases} 2 & (n \leq \nu) \\ 2^{n-\nu+1} & (n \geq \nu + 1) \end{cases}$

(2) $\nu = 1$ なら，各 $n \geq 1$ に対して $k(2^n) = 2^n$.
(3) $\nu \geq 2$ と仮定する．$-Q$ の $G_{P,Q}(\mathbb{Z}/2^n\mathbb{Z})$ における位数を 2^μ とおけば，

$$k(2^n) = \begin{cases} 2^{n-\nu+1} & (n \geq \nu+1,\ \mu \leq n-\nu) \\ 2^{\mu+1} & (\text{それ以外}) \end{cases}$$

系 1 4．$\nu = \mathrm{ord}_2 P \geq 2$ と仮定する．このとき，
(1) $Q \equiv 1 \mod 2^\nu$ なら

$$k(2^n) = \begin{cases} 2 & (n=1) \\ 4 & (2 \leq n \leq \nu) \\ 2^{n-\nu+1} & (n \geq \nu+1) \end{cases}$$

(2) $Q \equiv -1 \mod 2^\nu$ なら

$$k(2^n) = \begin{cases} 2 & (1 \leq n \leq \nu) \\ 2^{n-\nu+1} & (n \geq \nu+1) \end{cases}$$

命題 1 5．P, Q を整数とし，$P \equiv 1 \mod 2$, $Q \equiv -1 \mod 4$, $P^2 - 3Q \neq 0$ と仮定する．また，$\nu = \mathrm{ord}_2(P^2-Q)(P^2-3Q)$ とおく．このとき，$\nu \geq 3$．さらに，

$$\text{(1) } r(2^n) = \begin{cases} 3 & (n=1) \\ 6 & (2 \leq n \leq \nu) \\ 6 \times 2^{n-\nu} & (n \geq \nu+1) \end{cases}$$

(2) 各 $n \geq 1$ に対して $k(2^n) = 3 \times 2^{n-1}$.

命題 1 6．P, Q を整数とし，$P \equiv 1 \mod 2, Q \equiv 1 \mod 4, P^2 - Q \neq 0$ と仮定する．また，$\nu = \mathrm{ord}_2(P^2-Q)$ とおく．このとき，$\nu \geq 2$．さらに，

$$\text{(1) } r(2^n) = \begin{cases} 3 & (n \leq \nu) \\ 3 \times 2^{n-\nu} & (n \geq \nu+1) \end{cases}$$

(2) $P \equiv 5 \mod 8, Q \equiv 1 \mod 4$ と仮定する．このとき，

$$k(2^n) = \begin{cases} 3 & (n=1) \\ 6 & (n=2) \\ 3 \times 2^{n-2} & (n \geq 3) \end{cases}$$

(3) $P \equiv -5 \mod 8, Q \equiv 1 \mod 4$ と仮定する．このとき，

$$k(2^n) = \begin{cases} 3 & (n=1,2) \\ 3 \times 2^{n-2} & (n \geq 3) \end{cases}$$

(4) $P \equiv 1 \mod 8, Q \equiv 1 \mod 4, P^2 - Q \neq 0$ と仮定する．また，$\mu = \min[\mathrm{ord}_2(P+r-2)-1, \mathrm{ord}_2(r-1)]$ とおく．このとき，$\mu \geq 2$．また，

$$k(2^n) = \begin{cases} 3 & (n=1) \\ 6 & (2 \leq n \leq \mu+1) \\ 6 \times 2^{n-\mu-1} & (n \geq \mu+2) \end{cases}$$

(5) $P \equiv -1 \mod 8, Q \equiv 1 \mod 4$ and $P^2 - Q \neq 0$ と仮定する．また，$\mu = \min[\mathrm{ord}_2(P+r), \mathrm{ord}_2(r-1)]$ とおく．このとき，$\mu \geq 2$．また，

$$k(2^n) = \begin{cases} 3 & (1 \leq n \leq \mu) \\ 3 \times 2^{n-\mu} & (n \geq \mu + 1) \end{cases}$$

観察１７．R を可換環とする．このとき，群 $G_{P,Q}(R) = \tilde{R}^{\times}$ は R 代数 $\tilde{R}$ の上に乗法によって R 線型に作用する．したがって，R 基底 $\{1, \theta\}$ に関する正則表現 $\rho_R : G_{P,Q}(R) \to GL(2,R)$ は

$$\rho_R : \eta = (u,v) \mapsto \begin{pmatrix} u & -Qv \\ v & u+Pv \end{pmatrix}$$

によって与えられる．準同型 $\rho_R : G_{P,Q}(R) \to GL(2,R)$ は群スキームの準同型 $\rho : G_{P,Q} \to GL_{2,R}$ によって表現される．$\rho : G_{P,Q} \to GL_{2,R}$ は closed immersion.

定義から完全列の可換図式

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & G_{P,Q} & \xrightarrow{\beta} & G_{(P,Q)} & \longrightarrow & 0 \\ & & \| & & \downarrow \rho & & \downarrow \rho & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & GL_{2,R} & \longrightarrow & PGL_{2,R} & \longrightarrow & 1 \end{array}$$

を得る．準同型 $\rho : G_{(P,Q)} \to PGL_{2,R}$ は closed immersion．また，$G_{(P,Q)}$ は $\rho : G_{(P,Q)} \to PGL_{2,R}$ を介して $\mathbb{P}^1_R$ の上に作用する．

記号１８．P, Q を整数 $\neq 0$ とし，θ を剰余環 $\mathbb{Z}[t]/(t^2 - Pt + Q)$ における t の像とする．θ によって生成される $G_{P,Q}(\mathbb{Z}[1/Q])$ の部分群，$\beta(\theta)$ によって生成される $G_{(P,Q)}(\mathbb{Z}[1/Q])$ の部分群，$\gamma(\theta)$ によって生成される $U_{P,Q}(\mathbb{Z}[1/Q])$ の部分群をすべて Θ と記す．

また，準同型 $\rho : G_{(P,Q)}(\mathbb{Z}[1/Q]) \to PGL(2, \mathbb{Z}[1/Q])$ による $\Theta \subset G_{(P,Q)}(\mathbb{Z}[1/Q])$ の像も Θ と記す．

定理１９．p を素数，n を正の整数，$\boldsymbol{w} = (w_k)_{k \geq 0} \in \mathcal{R}(f, \mathbb{Z})$ とし，$(p, Q) = 1$ と仮定する．このとき，$k \geq 0$ が存在して $w_k \equiv 0 \mod p^n$ となる $\Leftrightarrow (w_0 : w_1)$ が $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ における $(0:1)$ の Θ 軌道に属する．したがって，

$$\#\{(w_0 : w_1) \in \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) \,;\, (w_k)_{k \geq 0} \in \mathcal{L}(f, \mathbb{Z}/p^n\mathbb{Z}),\ \text{各 } k \text{ に対して } w_k \neq 0\} = (p+1)p^{n-1} - r(p^n).$$

を得る．さらに，$\mu = \mathrm{ord}_p \Delta(\boldsymbol{w})$ とおく．このとき，

$$\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z}) \text{ における軌道 } (w_0 : w_1)\Theta \text{ の長さ} = \begin{cases} 1 & (n \leq \mu) \\ r(p^{n-\mu}) & (n \geq \mu + 1) \end{cases}$$

が成立する．

系２０．P, Q を整数 $\neq 0$，$(S_k)_{k \geq 0}$ を (P, Q) に伴う companion Lucas 数列，p を素数 > 2，$p \nmid Q$ と仮定する．このとき，$S_k \equiv 0 \mod p$ となるような k が存在する $\Leftrightarrow 2 | r(p)$．さらにこのとき，正の整数 n に対して $S_{r(p^n)/2} \equiv 0 \mod p^n$ が成立する．

文献

[1] E. Lucas – Théorie des fonctions numériques simplement périodiques. Amer. J. Math. 1 (1878)
[2] R. D. Carmichael – On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. Ann. of Math. 15 (1913)

[3] D. H. Lehmer – An extended theory of Lucas' functions. Ann. of Math. 31 (1930)
[4] M. Hall – Divisors of second-order sequences. Bull. Amer. Math. Soc. 43 (1937)
[5] M. Ward – The linear p-adic recurrences of order two. Illinois J. Math. 6 (1962)
[6] R. R. Laxton – On groups of linear recurrences, I. Duke Math. J. 36 (1969)
[7] R. R. Laxton – On groups of linear recurrences, II. Elements of finite order. Pacific J. Math. 32 (1970)
[8] N. Suwa – Geometric aspects of Lucas sequences, I. Preprint series No.122, 中央大学 (2018), Tokyo J. Math. に掲載予定
[9] N. Suwa – Geometric aspects of Lucas sequences, II. Preprint series No.125, 中央大学 (2018)

６．日常の営為を楽しむ〜時々の花々を愛でる

数学工房会報第１２２号所収の入門桑野道場に掲載されている熊野充博さんの解答を観賞します．ここでも鍵になるのは群論における位数の概念です．

観察１．$5^m+11=2^n$ が成立するような正の整数 $m,\,n$ は $(m,n)=(1,4)$ に限る．

証明．$m,\,n$ を $2^n=5^m+11$ が成立するような正の整数とする．$2^n\geq 5^1+11=16$ なので，$n\geq 4$．以下，$n>4,\,m>1$ と仮定する．このとき，$2^n=5^m+11,\,2^4=5+11$ の辺々を差し引いて

$$2^4(2^{n-4}-1)=5(5^{m-1}-1)$$

を得る．ここで，$(2^4,2^{n-4}-1)=1,\,(5,5^{m-1}-1)=1$ なので，

$$\mathrm{ord}_5(2^{n-4}-1)=1,\ \mathrm{ord}_2(5^{m-1}-1)=4,\ \mathrm{ord}_p(2^{n-4}-1)=\mathrm{ord}_p(5^{m-1}-1)\ (p\text{ は素数}\neq 2,5)$$

さらに，乗法群 $(\mathbb{Z}/5\mathbb{Z})^\times$ における 2 の位数が 4，乗法群 $(\mathbb{Z}/5^2\mathbb{Z})^\times$ における 2 の位数が 20 なので，

$$4|(n-4),\ 20\nmid(n-1)$$

一方，乗法群 $(\mathbb{Z}/2^4\mathbb{Z})^\times$ における 5 の位数が 4 なので，

$$4|(m-1)$$

したがって，

$$(5^4-1)|(5^{m-1}-1)$$

ここで，$(5^2+1)|(5^4-1),\,5^2+1=2\cdot 13$ なので，$13|(2^{n-4}-1)$．さらに，乗法群 $(\mathbb{Z}/13\mathbb{Z})^\times$ における 2 の位数が 12 なので，

$$12|(n-4)$$

したがって，

$$(2^{12}-1)|(2^{n-4}-1)$$

ここで，$(2^3-1)|(2^{12}-1),\,2^3-1=7$ なので，$7|(5^{m-1}-1)$．さらに，乗法群 $(\mathbb{Z}/7\mathbb{Z})^\times$ における 5 の位数が 6 なので，

$$6|(m-1)$$

したがって，

$$(5^6-1)|(5^{m-1}-1)$$

ここで，$(5^2+5+1)|(5^6-1),\,5^2+5+1=31$ なので，$31|(2^{n-4}-1)$．さらに，乗法群 $(\mathbb{Z}/31\mathbb{Z})^\times$ における 2 の位数が 5 なので，$5|(n-4)$．これは，$4|(n-4),\,20\nmid(n-4)$ に反する．

以上のことから結論を得る．

観察２．$5^m+7=2^n$ が成立するような正の整数 $m,\,n$ は $(m,n)=(2,5)$ に限る．

証明．$m,\,n$ を $2^n=5^m+7$ が成立するような正の整数とする．$2^n\geq 5^2+7=32$ なので，$n\geq 5$．以下，$n>5,\,m>2$ と仮定する．このとき，$2^n=5^m+7,\,2^5=5^2+7$ の辺々を差し引いて

$$2^5(2^{n-5}-1)=5^2(5^{m-2}-1)$$

を得る．ここで，$(2^4,2^{n-5}-1)=1,\,(5^2,5^{m-2}-1)=1$ なので，

$$\mathrm{ord}_5(2^{n-5}-1)=2,\ \mathrm{ord}_2(5^{m-2}-1)=5,\ \mathrm{ord}_p(2^{n-5}-1)=\mathrm{ord}_p(5^{m-2}-1)\ (p\text{ は素数}\neq 2,5)$$

さらに，乗法群 $(\mathbb{Z}/5^2\mathbb{Z})^\times$ における 2 の位数が 20，乗法群 $(\mathbb{Z}/5^3\mathbb{Z})^\times$ における 2 の位数が 100 なので，

$$20|(n-5),\ 100\nmid(n-5)$$

一方，乗法群 $(\mathbb{Z}/2^5\mathbb{Z})^\times$ における 5 の位数が 8 なので，

$$8|(m-2)$$

したがって，

$$(5^8-1)|(5^{m-2}-1)$$

ここで，$(5^2+1)|(5^8-1),\,5^2+1=2\cdot 13$ なので，$13|(2^{n-5}-1)$．さらに，乗法群 $(\mathbb{Z}/13\mathbb{Z})^\times$ における 2 の位数が 12 なので，

$$12|(n-5)$$

したがって，

$$(2^{12}-1)|(2^{n-5}-1)$$

ここで，$(2^3-1)|(2^{12}-1),\,2^3-1=7$ なので，$7|(5^{m-2}-1)$．さらに，乗法群 $(\mathbb{Z}/7\mathbb{Z})^\times$ における 5 の位数が 6 なので，$6|(m-2)$．ここで，$8|(m-2)$ なので，

$$24|(m-2)$$

したがって，

$$(5^{24}-1)|(5^{m-2}-1)$$

ここで，$(5^4-5^2+1)|(5^{24}-1),\,5^4-5^2+1=601$ なので，$601|(2^{n-5}-1)$．さらに，乗法群 $(\mathbb{Z}/601\mathbb{Z})^\times$ における 2 の位数が 25 なので，$25|(n-5)$．これは，$20|(n-5),\,100\nmid(n-5)$ に反する．

以上のことから結論を得る．

補足３．観察 1 と観察 2 での議論では t^n-1 の因数分解を利用して計算を軽くしている．例えば，

$$\begin{aligned}
t^4-1&=(t-1)(t+1)(t^2+1)\\
&\Rightarrow\ 5^4-1=4\cdot 6\cdot 26=2^4\cdot 3\cdot 13,\\
t^6-1&=(t-1)(t+1)(t^2+t+1)(t^2-t+1)\\
&\Rightarrow\ 5^6-1=4\cdot 6\cdot 31\cdot 21=2^3\cdot 3\cdot 7\cdot 31,\\
t^{12}-1&=(t-1)(t+1)(t^2+t+1)(t^2+1)(t^2-t+1)(t^4-t^2+1)\\
&\Rightarrow\ 2^{12}-1=1\cdot 3\cdot 7\cdot 5\cdot 3\cdot 13=3^2\cdot 5\cdot 7\cdot 13\\
&\Rightarrow\ 5^{12}-1=4\cdot 6\cdot 31\cdot 13\cdot 21\cdot 601=2^4\cdot 3^2\cdot 7\cdot 13\cdot 31\cdot 601,\\
t^{24}-1&=(t-1)(t+1)(t^2+t+1)(t^2+1)(t^2-t+1)(t^4+1)(t^4-t^2+1)(t^8-t^4+1)\\
&\Rightarrow\ 5^{24}-1=4\cdot 6\cdot 31\cdot 13\cdot 21\cdot 626\cdot 601\cdot 390001=2^5\cdot 3^2\cdot 7\cdot 13\cdot 31\cdot 313\cdot 601\cdot 390001
\end{aligned}$$

補足４．p を素数，a を p と素な整数とする．Fermat の定理から乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ における a の位数は $p-1$ の約数．さらに，r を $p-1$ の正の約数とする．このとき，r が乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ における a の位数に等しい $\Leftrightarrow$ (1) $a^r \equiv 1 \mod p$，(2) r の各素因数 q に対して $a^{r/q} \not\equiv 1 \mod p$.

例えば，

$$\text{乗法群 } (\mathbb{Z}/13\mathbb{Z})^\times \text{ における 2 の位数} = 12 \Leftarrow 2^6 \equiv -1 \mod 13,\ 2^4 \equiv 3 \mod 13$$
$$\text{乗法群 } (\mathbb{Z}/7\mathbb{Z})^\times \text{ における 5 の位数} = 6 \Leftarrow 5^3 \equiv -1 \mod 7,\ 5^2 \equiv 4 \mod 7$$
$$\text{乗法群 } (\mathbb{Z}/31\mathbb{Z})^\times \text{ における 2 の位数} = 5 \Leftarrow 2^5 \equiv 1 \mod 31$$
$$\text{乗法群 } (\mathbb{Z}/601\mathbb{Z})^\times \text{ における 2 の位数} = 25 \Leftarrow 2^{25} \equiv 1 \mod 601,\ 2^5 \equiv 32 \mod 601$$

補足５．p を素数，a を p と素な整数，r を乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ における a の位数とする．このとき，$a^r \not\equiv 1 \mod p^2$ なら，任意の正の整数 n に対して乗法群 $(\mathbb{Z}/p^n\mathbb{Z})^\times$ における a の位数は rp^{n-1} に等しい．

例えば，$2^2 \equiv -1 \mod 5$ なので，乗法群 $(\mathbb{Z}/5\mathbb{Z})^\times$ における 2 の位数は 4．さらに，$2^4 \equiv 16 \mod 25$ なので，乗法群 $(\mathbb{Z}/25\mathbb{Z})^\times$ における 2 の位数は 20，乗法群 $(\mathbb{Z}/125\mathbb{Z})^\times$ における 2 の位数は 100.

観察 1 での議論から「$5^m+27=2^n$ が成立するような正の整数 m, n は $(m,n)=(1,5)$ に限る」「$5^m+59=2^n$ が成立するような正の整数 m, n は $(m,n)=(1,6)$ に限る」等々，観察 2 での議論から「$5^m+239=2^n$ が成立するような正の整数 m, n は $(m,n)=(2,6)$ に限る」「$5^m+103=2^n$ が成立するような正の整数 m, n は $(m,n)=(2,7)$ に限る」等々，金太郎飴のような結果が幾らでも導き出せます．また，「乗法群 $(\mathbb{Z}/390001\mathbb{Z})^\times$ における 2 の位数が $16250=2\cdot5^4\cdot13$ である」ことを利用して，「$5^m+3=2^n$ が成立するような正の整数 m, n は $(m,n)=(3,7)$ に限る」「$5^m+131=2^n$ が成立するような正の整数 m, n は $(m,n)=(3,8)$ に限る」等々，これまた金太郎飴本舗を営むことができます．しかしながら，その先はとなるとどうしたものやら．ただ，$p^m+a=q^n$ (p, q は相異なる素数，a, m, n は正の整数) という形の不定方程式を個々に扱うとその度ごとに多様でありながら何かしら調和にみちた整数の世界を感じることができるかもしれません．Lucas も具体的な例を多く計算することによって，そしてその例が示している調和の世界を感じることによって，彼の名が付された定理を発見したのだと想像します．

会報１２２号の巻頭言にある桑野先生のぼやきと励ましを引用してこの対話の場を閉めることにしましょう．

この世の中，いつの間にやら，世界中，根拠薄弱なことや嘘，憎悪の扇動を何の痛痒も感じずに広めるような人種がのさばるようになりました．そのようなものの対極にあるのが数学です．本当に学ぼうとすると楽ではありませんが，数学を友とし一生付き合えるということは，一個の人間として実に幸福なことだと思います．

参考書

[1] 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．講談社 (2017)
[2] 中島匠一，分数と小数から広がる整数の世界～フェルマーの小定理からアルチン予想まで．技術評論社 (2016)
[3] 中村滋，フィボナッチ数の小宇宙～フィボナッチ数，リュカ数，黄金分割．日本評論社 (2002)