数列の整除性について

渡邊百合佳*

奈良女子大学大学院人間文化研究科

今年も城崎新人セミナーに参加させていただき，様々な分野の方とお話をすることができ大変貴重な時間を過ごすことができました．ありがとうございました．

1 はじめに

まず，数列 $\{u_n\}$ を次のように定める．ただし，a と b は整数とする．

$$u_0 = 0,\ u_1 = 1,\ u_n = a\,u_{n-1} + b\,u_{n-2} \quad (n \geq 2).$$

この線形循環数列 $\{u_n\}$ は，古くから扱われてきた数列であり，さまざまなことが知られている．講演ではこの数列に関するある整除性について修士論文でまとめたことを発表した．この講演を行った後にいくつか既知のこととしてわかったこととして以下の定理 A，定理 B などがある．これらは [1, 第 2 章 IV] に述べられている．

定理 A. p を奇素数，$d = a^2 + 4b$ とする．$p \nmid abd$ ならば，$p \mid u_{\psi(p)}$．ただし $\psi(p) = p - \left(\frac{d}{p}\right)$，$\left(\frac{d}{p}\right)$ はルジャンドル記号．

定理 B.

$$a : \text{奇数},\ b : \text{奇数} \quad \Longrightarrow \begin{cases} 3 \mid n & \Rightarrow u_n \text{は偶数} \\ \text{その他} & \Rightarrow u_n \text{は奇数} \end{cases}$$

$$a : \text{奇数},\ b : \text{偶数} \quad \Longrightarrow n \geq 1 \text{ で } u_n \text{は奇数}$$

$$a : \text{偶数},\ b : \text{奇数} \quad \Longrightarrow u_n \equiv n \pmod 2$$

$$a : \text{偶数},\ b : \text{偶数} \quad \Longrightarrow n \geq 2 \text{ で } u_n \text{は偶数}$$

以上の定理は修士論文の内容の一部と重複している．たとえば定理 A については次章の定理 2.1 と同様である．しかし [1] で述べられている証明方法と違い，数列 $\{u_n\}$ を 2 次体 $\mathbb{Q}(\sqrt{d})$ 上で扱っていることが特徴である．次節で詳しく述べていくこととする．

* eay.watanabe@cc.nara-wu.ac.jp

2 $p \mid u_{p-1},\ p \mid u_{p+1}$

次の定理は定理 A と同様である．ここでは $\mathbb{Q}(\sqrt{d})$ の判別式 Δ が p の非剰余である場合には素数 p の条件として $p \nmid b$ をつけなくてもよい．

定理 2.1. p を素数とし，$d = a^2 + 4b$ とおく．d を正の整数 f と $\mathbb{Q}(\sqrt{d})$ の判別式 Δ を用いて $d = f^2\Delta$ と表わす．このとき，$p \nmid 4d$ ならば

$$\begin{cases} \left(\dfrac{\Delta}{p}\right) = 1,\ p \nmid b & \Longrightarrow p \mid u_{p-1} \quad (2.1) \\ \left(\dfrac{\Delta}{p}\right) = -1 & \Longrightarrow p \mid u_{p+1} \quad (2.2) \end{cases}$$

ただし，記号 $\left(\frac{\Delta}{p}\right)$ はルジャンドル記号である．

以下に定理 2.1 の証明の概略を述べる．特徴としては 2 次体 $\mathbb{Q}(\sqrt{d})$ 上で数列 $\{u_n\}$ を扱い，フェルマーの小定理の拡張やフロベニウス写像がキーワードである．

証明の概略

$\alpha = (a + \sqrt{d})/2$，$\beta = (a - \sqrt{d})/2$ として $\{u_n\}$ の一般項の公式 $u_n = (\alpha^n - \beta^n)/\sqrt{d}$ を用い，2 次拡大した $\mathbb{Q}(\sqrt{d})$ 上で考えていく．

まず，式 (2.1) については $\left(\frac{\Delta}{p}\right) = 1$ なので，素数 p は 2 次体 $\mathbb{Q}(\sqrt{d})$ の整数環 $\mathfrak{o}$ において二つの異なる素イデアル $\mathfrak{p}$, $\mathfrak{p}'$ に分解される．α と β はともに $\mathfrak{o}$ の元であるから，α^{p-1}，β^{p-1} の $\mathfrak{p}$, $\mathfrak{p}'$ 上における値を考えてみる．このとき，仮定 $p \nmid b$ より $(\alpha, p) = 1$，$(\beta, p) = 1$ が成り立つのでフェルマーの小定理の拡張を用いると，$\alpha^{p-1} \equiv 1 \equiv \beta^{p-1} \pmod{\mathfrak{p}}$ がわかる．よって，$(\sqrt{d}, \mathfrak{p}) = 1$ に注意すると $u_{p-1} \equiv 0 \pmod{\mathfrak{p}}$ となる．$\mathfrak{p}'$ 上においても全く同様にして $u_{p-1} \equiv 0 \pmod{\mathfrak{p}'}$ がわかる．ここで $\mathfrak{p} \cap \mathfrak{p}' = (p)$ に注意して $p \mid u_{p-1}$ が導かれる．ただし (p) は単項イデアルを表わす．

次に，式 (2.2) について述べる．$\left(\frac{\Delta}{p}\right) = -1$ の場合は，素数 p が整数環 $\mathfrak{o}$ においても素イデアルであることから，2 次体の共役写像が p に関するフロベニウス写像を導く．また，α と β はガロア群の元で共役であるので，フロベニウス写像などを用いると $\alpha^p \equiv \beta,\ \beta^p \equiv \alpha \pmod{(p)}$ がわかる．よって，$\alpha^{p+1} \equiv \alpha\beta \equiv \beta^{p+1} \pmod{(p)}$ となり，$(\sqrt{d}, p) = 1$ に注意すれば $u_{p+1} \equiv 0 \pmod{(p)}$ である．

3 そのほか

ここでは定理 2.1 で扱わなかった $p = 2,\ p \mid d,\ p \mid b$ の場合について述べる．$p = 2$ については定理 B と違い a, b の偶奇によって u_n が偶数であるための必要十分条件を与えている．

定理 3.1. $n \geq 0$ に対して次が成立する．

$$2 \mid u_n \Longleftrightarrow \begin{cases} n = 3k, k \text{ は } 0 \text{ 以上の整数}, & (a : \text{奇数},\ b : \text{奇数}) \\ n = 0, & (a : \text{奇数},\ b : \text{偶数}) \\ n = 2k, k \text{ は } 0 \text{ 以上の整数}, & (a : \text{偶数},\ b : \text{奇数}) \\ n \neq 1. & (a : \text{偶数},\ b : \text{偶数}) \end{cases}$$

次に $p \mid d$ の場合についてであるが，素数に限らず d の正の約数すべてにおいて次のことが成り立つ．

定理 3.2. c を正の整数で $c \mid d$ なるものとする．すると，　$c \mid u_c$.

系 3.3. $p \mid d$ なる任意の素数 p に対して　$p \mid u_p$.

また $p \mid b$ の場合は p が a を割り切るかかそうでないかによって次のように場合わけされる．

定理 3.4. p を素数とし，$p \mid b$ なるものとする．このとき，$n \geq 1$ で

$$\begin{cases} p \mid a & \Longrightarrow p \mid u_n, \\ p \nmid a & \Longrightarrow p \nmid u_n. \end{cases}$$

4　$p \mid u_n$ となる n の決定

ここでは，素数 p を固定し，$p \mid u_n$ なる n がどのようなものであるかを見る．ただし，$\alpha = (a + \sqrt{d})/2$ で $\overline{\alpha} = \alpha \mod (p)$，$(p)$ は単項イデアル，である．また，$\mathfrak{o}$ を整数環，$\sigma \in Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{1, \sigma\}$ とし，$\alpha^{\sigma-1}$ で $\alpha^{\sigma} \cdot \alpha^{-1}$ を表わすこととする．

定理 4.1. p は素数で $p \nmid b$，$p \nmid d$ とする．p が u_n を割り切るならば巡回群 $\langle \overline{\alpha^{\sigma-1}} \rangle$ の位数は n を割り切る．逆に，巡回群 $\langle \overline{\alpha^{\sigma-1}} \rangle$ の位数がある正の整数 m を割り切るならば p は u_m を割り切る．

証明. $p \mid u_n$ ならば $\overline{u_n} = \overline{0}$．よって $\overline{\sqrt{d} u_n} = \overline{\alpha}^{\,n} - (\overline{\alpha^{\sigma}})^n$．したがって

$$\overline{\alpha}^{\,n} = (\overline{\alpha^{\sigma}})^n.$$

今，$p \nmid b$ より $(\alpha, p) = 1$ なので

$$\overline{\alpha^{\sigma-1}}^{\,n} = \overline{1}.$$

これより $\langle \overline{\alpha^{\sigma-1}} \rangle$ の位数は n を割り切ることがわかる．

逆に，$\langle \overline{\alpha^{\sigma-1}} \rangle$ の位数を t として $t \mid m$ となる正の整数 m を取り，$m = tt'(t' \in \mathbb{Z})$ と表す．t の定義から $\overline{\alpha^{\sigma-1}}^{\,t} = \overline{1}$ が成り立つので

$$\overline{\alpha^{\sigma}}^{\,t} = \overline{\alpha}^{\,t}.$$

これより，

$$\overline{\sqrt{d} u_m} = \overline{\alpha}^{\,m} - (\overline{\alpha^{\sigma}})^{\,m} = \overline{\alpha}^{\,tt'} - (\overline{\alpha^{\sigma}})^{\,tt'} = (\overline{\alpha}^{\,t})^{\,t'} - (\overline{\alpha^{\sigma}}^{\,t})^{\,t'} = \overline{0}.$$

$(\sqrt{d}, p) = 1$ より $\overline{u_m} = \overline{0}$.　□

定理 4.1 において，素数 p が 2 次体 $\mathbb{Q}(\sqrt{d})$ で素イデアルを生成する場合に条件を強めることによって以下のように，より詳細に述べることができる．

定理 4.2. p を素数とし $p\nmid b, p\nmid d$ を満たす素イデアルとする．$\left|\left(\mathfrak{o}/(p)\right)^{\times} : \langle\overline{\alpha}\rangle\right| = g$ とおく．今，$g_1 = \gcd(g, p+1)$ とおけば $\overline{u_n} = \overline{0}$ となる n は $\dfrac{p+1}{g_1}$ で割り切れる．逆に n が $\dfrac{p+1}{g_1}$ で割り切れるならば $\overline{u_n} = \overline{0}$ が成り立つ．

証明. 先ほどの定理 4.1 と同様に，$p \mid u_m$ ならば $\overline{\alpha}^{\,m} = (\,\alpha^{\sigma}\,)^{\,m}$ である．今，p が素イデアルであることより，$\overline{\alpha^{\sigma}} = \overline{\alpha}^{\,p}$ が成り立つので $\overline{\alpha}^{\,m} = \overline{\alpha}^{\,pm}$．$p\nmid b$ より $(\alpha, p) = 1$ なので

$$\overline{\alpha}^{\,m(p-1)} = \overline{1}.$$

今，巡回群 $\langle\overline{\alpha}\rangle$ の位数を $\operatorname{ord}\overline{\alpha}$ で表せば，$\operatorname{ord}\overline{\alpha} = \left|\left(\mathfrak{o}/(p)\right)^{\times}\right| / \left|\left(\mathfrak{o}/(p)\right)^{\times} : \langle\overline{\alpha}\rangle\right| = \dfrac{p^2-1}{g}$ であるから，$m(p-1) = \dfrac{p^2-1}{g}k$ となる k が存在する．よって

$$m = \frac{p+1}{g}k.$$

ここで $g_2 = \dfrac{g}{g_1}$ とおくと，$g_2 m = \dfrac{p+1}{g_1}k$ となる．また，$g_1 = \gcd(g, p+1)$ より

$$\gcd\Big(g_2, \frac{p+1}{g_1}\Big) = 1.$$

よって

$$\frac{p+1}{g_1} \Big| m.$$

逆に，ある正の整数 m, l で $m = \dfrac{p+1}{g_1}l$ が成り立つとすると，$m(p-1) = \dfrac{p^2-1}{g}g_2 l$ である．今，$\operatorname{ord}\overline{\alpha} = \dfrac{p^2-1}{g}$ より $\overline{\alpha}^{\frac{p^2-1}{g}} = \overline{1}$．よって

$$\overline{\alpha}^{\,m(p-1)} = \overline{\alpha}^{\frac{p^2-1}{g}g_2 l} = \overline{1}.$$

これより $\overline{\alpha}^{\,pm} = \overline{\alpha}^{\,m}$ がわかる．ここで $\bar{\sigma}$ がフロベニウス写像であることから $\overline{\alpha^{\sigma}} = \overline{\alpha}^{p}$ なので $\overline{\alpha^{\sigma}}^{\,m} = \overline{\alpha}^{\,m}$ が成り立つ．ゆえに

$$\overline{\alpha}^{\,m} - \overline{\alpha^{\sigma}}^{\,m} = \overline{0}.$$

$(\sqrt{d}, p) = 1$ より $\overline{u_m} = \overline{0}$. □

定理 4.2 を言い換えると次がいえる．

系 4.3. p を素数とし $p\nmid b, p\nmid d$ を満たす素イデアルとする．$\left|\left(\mathfrak{o}/(p)\right)^{\times} : \langle\overline{\alpha}\rangle\right| = g$，$g_1 = \gcd(g, p+1)$ とおく．このとき，m を 0 でない $p \mid u_m$ なる最小の整数とすると $m = \dfrac{p+1}{g_1}$ である．さらに，p が u_n を割り切るならば m は n を割り切り，逆に m が n を割り切るならば p は u_n を割り切る．

また，以下の例は定理 4.2 において $g = 1$ とした場合である．

例 4.4. $\left(\mathfrak{o}/(p)\right)^{\times} = \langle\overline{\alpha}\rangle$ であるとき $\overline{u_n} = \overline{0}$ となる n は $p+1$ で割り切れ，逆に $p+1 \mid n$ なる正の整数 n に対して $\overline{u_n} = \overline{0}$ が成り立つ．

付録

定理 4.2 の例をいくつか載せる．記号は定理で用いたものをそのまま使っている．

系 4.3 より $(p+1)/g_1$ は p が u_n を割り切るような n の中で最小の n であること，$p \mid u_m$ となる m に対して $\frac{p+1}{g_1} \mid m$ であることがわかる．

例 **4.5** ($a=1, b=1$ の場合)**.**

p	2	3	7	13	17	23	37	43	47	53	67	73	83	$\cdots$
$(p+1)/g_1$	3	4	8	7	9	24	19	44	16	27	68	37	84	$\cdots$

例 **4.6** ($a=3, b=2$ の場合)**.**

p	3	5	7	11	23	29	31	37	41	61	71	73	79	$\cdots$
$(p+1)/g_1$	2	6	8	3	8	30	32	38	7	62	72	37	80	$\cdots$

例 **4.7** ($a=2, b=-7$ の場合)**.**

p	13	17	19	23	37	41	43	47	61	67	71	89	109	$\cdots$
$(p+1)/g_1$	14	6	5	24	19	42	44	12	62	68	72	90	55	$\cdots$

参考文献

[1] Paulo Ribenboim 著，吾郷孝視 訳編, 素数の世界 その探索と発見 第 2 版, 共立出版, (2001).