数理解析研究所講究録
1154巻 2000年 144-154

原始根に関する多項式型Artin予想について

竹内 良平 (Ryouhei Takeuchi)
(都立大理・博士課程)

1. Introduction

1.1 Main Theorems

Artinの原始根に関する予想とは,「整数aに対して,aが-1や平方数でなければ$a \bmod p$が原始根となるような素数pが無限に存在する」という命題が正しいというものである.この命題を次の同値関係に基づいて拡張する.

$$a \text{ が } \bmod p \text{ で原始根} \iff f(X) = X - a \text{ の根が } \bmod p \text{ で原始根}$$

であるから,$f(X)$としてmonicで既約な一般の整係数多項式全体を対象にすれば命題は拡張される.ここで扱う拡張された命題を正確に記述する為に必要な記号を定義し,Artin予想の次のような一般化について考える(R.Takeuchi[6]).

Notation 1. 素数pの集合を$\mathcal{P}$とし,その部分集合$\mathcal{S}$がnatural densityを持つとする.このとき,

$$\mathcal{S}(x) := \{ p \in \mathcal{S} \mid p \leq x \} \text{ (counting set)}, \quad \pi(x) := \sharp\mathcal{P}(x) \sim x/\log x \text{ (素数定理)},$$
$$\delta(\mathcal{S}) := \lim_{x \to \infty} (\sharp\mathcal{S}(x)/\pi(x)) \text{ (natural density)}$$

とする.また,$f(X) \in \mathbb{Z}[X]$はmonicで既約なもののみを考えて,

$$\mathrm{Spl}(f) := \{ p \in \mathcal{P} \mid f(X) \bmod p \text{が異なる一次因子の積に分解する} \},$$
$$N_f := \{ p \in \mathrm{Spl}(f) \mid \exists a \in \mathbb{F}_p^{\times},\ f(a) \equiv 0 \pmod{p} \ \wedge\ a \bmod p \text{は原始根} \}.$$

そして,次の命題についてこの論文では考えることにする.

多項式型 Artin 予想 いくつかのN_fが有限集合となる『例外多項式』を除いて,ほとんどのfに対しては,N_fは無限集合である.即ち,$f(X) \bmod p$の$\deg f$個の根の中で,原始根となるものが存在するような素数$p \in \mathrm{Spl}(f)$が無限に存在する.

H.W.Lenstra, Jr.も[2]の論文で類似の命題について考察している.特に上の命題

で, $\deg f = 1$ のときは original の Artin 予想であり, このときは C.Hooley[1] によって「一般化された Riemann 予想」(GRH と略記) の仮定の下で counting function $\sharp N_f(x)$ の大きさが評価され, 例外多項式は $X+1, X-a^2$ (-1, 平方数 に対応) のみである (即ち, Artin 予想は正しい) ことが知られている. 当然, $\deg f > 1$ のときの例外多項式も決定したい訳だが, 今回は, $f(X) = X^2 - m$, $X^3 - m$ の形の二項方程式に対して GRH 仮定の下で例外多項式を決定できた.

Theorem 1. GRH を仮定すると, $f(X) = X^2 - m$ の形の例外多項式は $X^2 + 1$, $X^2 + 4k^4$, $X^2 + 27k^6$ のみであり, $f(X) = X^3 - m$ の形の例外多項式は $X^3 - k^2$, $X^3 + 3k^2$ のみである. 但し, $k \in \mathbb{N}$ とする.

これは, $f(X) = X^2 - m$, $X^3 - m$ の形の二項方程式に対して GRH (もっと正確には, ある種の Kummer 拡大の Dedekind's zeta に対する Riemann 予想) を仮定して $N_f(x)$ の大きさが explicit に評価できたことの Corollary である. その評価の記述の為に記号を準備すると,

Notation 2. よく知られているように Artin's constant を

$$C := \sum_{n=1}^{\infty} \frac{\mu(n)}{n\varphi(n)} = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p(p-1)}\right) = 0.37395\cdots$$

とする (μ : Möbius 関数, φ : Euler 関数).

また, $m \in \mathbb{Z}$ に対して, m の square-free part を $[m]'$ で表すことにして,

$$h_m := \max\{\, k \in \mathbb{N} \mid \sqrt[k]{m} \in \mathbb{Z} \,\} \quad (\text{つまり } m \text{ は丁度 } h_m \text{ 乗数である}),$$

$$U_m := \prod_{p \mid h_m} \frac{p(p-2)}{p^2-p-1}, \quad V_m := \prod_{\substack{p \mid [m]' \\ p \mid h_m}} \frac{-1}{p-2} \prod_{\substack{p \mid [m]' \\ p \nmid h_m}} \frac{-1}{p^2-p-1}.$$

Theorem 2. $f(X) = X^2 - m$ に対して, GRH を仮定すると,

$$\sharp N_f(x) = \delta(N_f) \cdot \pi(x) + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

ここで $\delta(N_f)$ の値は,

(A) $[m]' \equiv 1 \pmod 4$ のとき, $\delta(N_f) = \frac{3}{4} U_m(1 + V_m) \times C$,
(B) $[m]' \equiv 2 \pmod 4$ のとき, $\delta(N_f) = \frac{3}{4} U_m \times C$,
(C) $[m]' \equiv 3 \pmod 4$ のとき, $k \in \mathbb{Z}$ として
(C-1) $m \neq -1$ & $m \neq -4k^4$ のとき, $\delta(N_f) = \frac{3}{4} U_m(1 - \frac{1}{3} V_m) \times C$,
(C-2) $m = -1$ or $m = -4k^4$ のとき, $\delta(N_f) = 0$.

Theorem 3. $f(X) = X^3 - m$ に対して, GRH を仮定すると,

$$\sharp N_f(x) = \delta(N_f) \cdot \pi(x) + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

ここで $\delta(N_f)$ の値は,

(A) $[m]' \equiv 1 \pmod 4$ のとき,
(A-1) $[m]' \neq -3$ のとき, $\delta(N_f) = \frac{8}{45} U_m(1 - V_m) \times C$,
(A-2) $[m]' = -3$ のとき, $\delta(N_f) = 0$,
(B) $[m]' \not\equiv 1 \pmod 4$ のとき, $\delta(N_f) = \frac{8}{45} U_m \times C$.

1.2 Hooley's method

ここでは, 今回の定理の証明の基になっている Hooley の original の Artin 予想に対する [1] の論文のアイデアを紹介する. ここでは, $a \in \mathbb{Z}$ を -1 でも平方数でもないものとする. このとき, 次の集合 W の density を計算することが目標である.

$$W := \{\, p \in \mathcal{P} \mid a \bmod p \text{ は原始根} \,\}.$$

この W は $f(X) = X - a$ のときの N_f であることに注意. ここで, index を表す記号

$$r(a,p) := \begin{cases} [\mathbb{F}_p^\times : \langle a \bmod p \rangle] & (\text{if } a \neq 0 \text{ in } \mathbb{F}_p) \\ \infty & (\text{if } a = 0 \text{ in } \mathbb{F}_p) \end{cases}$$

を定義しておくと, $r(a,p) = 1 \Leftrightarrow \mathbb{F}_p^\times = \langle a \rangle \Leftrightarrow a \bmod p$ は原始根, である. そして, $r(a,p) = \infty$ となる素数 p は高々有限個しかないので考えないことにする.

もし, $a \bmod p$ が原始根でないとすると, ある素数 l が存在して $r(a,p)$ を割るから, W_l を l が $r(a,p)$ を割らないような素数 p の集合とすると, $W = \bigcap_{l \in \mathcal{P}} W_l$ が成り立つ. また ζ_l を 1 の原始 l 乗根として, W_l の元は代数体 $F_l = \mathbb{Q}(\zeta_l, \sqrt[l]{a})$ で次のように特徴付けられる.

$$\begin{aligned} p \notin W_l &\iff p \equiv 1 \pmod l \ \ \& \ \ a^{(p-1)/l} \equiv 1 \pmod p \\ &\iff p \text{ は } F_l/\mathbb{Q} \text{ で完全分解.} \end{aligned} \tag{1}$$

Chebotarev's density theorem によると, $\delta(W_l) = 1 - [F_l : \mathbb{Q}]^{-1}$ であるので, $\forall n \in \mathbb{N}$ に対して

$$\delta(\bigcap_{\substack{l \in \mathcal{P} \\ l \mid n}} W_l) = \sum_{d \mid n} \frac{\mu(d)}{[F_d : \mathbb{Q}]}. \tag{2}$$

ここで, F_d は l が d の素因子を動くときの F_l たちの合成体とする. (2) の式において, $n \to \infty$ として考えたいのだが, Chebotarev's density theorem は無限の数体の集合には適応できない. しかしながら, W の density の上限には成り得る. 即ち,

$$\delta(W) \leq \sum_{d=1}^{\infty} \frac{\mu(d)}{[F_d : \mathbb{Q}]}. \tag{3}$$

ここまでが代数的な議論である. あとは (3) での等式を得る為に, 解析的な議論が必要になり, 使う道具は GRH を仮定して得られる Chebotarev's density theorem の effectine version である.

こうして, $\delta(W)$ を代数体の言葉で書いておき, explicit なものにする為に, $[F_d : \mathbb{Q}]$ の計算をし, (3) の右辺の Euler product expansion をする. これで, $\delta(W)$ が explicit に求まるのである.

1.3 Outline of proof

Hooley の方法を真似て, $\sharp N_f(x)$ の評価をするのだが, これには次の prime ideal の集合が活躍する.

Notation 3. K を代数体, $\mathcal{O}_K$ を K の整数環, $\gamma \in \mathcal{O}_K$ として $M \in \mathbb{N}$ とする.

$$B_\gamma(K, x, M) := \left\{ \mathfrak{p} \;\middle|\; \begin{array}{c} \mathfrak{p} \text{ は } K \text{ の prime ideal, } \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p \leq x, \\ p \equiv 1 \pmod{M} \text{ , } \gamma \text{ は mod } \mathfrak{p} \text{ で原始根} \end{array} \right\}.$$

そして, この $\sharp B_\gamma(K, x, M)$ の大きさは, L.Murata によって次の様に評価されている.

Theorem 4 (Murata[3]). $k \in \mathbb{N}$ を square-free なものとして,

$$G_{k,M} := K(\zeta_k, \zeta_M, \sqrt[k]{\gamma}).$$

この形の全ての代数体における GRH を仮定すると,

$$\sharp B_\gamma(K, x, M) = \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{[G_{k,M} : K]} \right) \cdot \pi(x) + O\left(\frac{x \log\log x}{\log^2 x} \right). \tag{4}$$

この Theorem 4 の証明は, 前の sub-section で説明した Hooley の方法を代数体に持ち上げて parallel に議論することによって得られる. さて, この Theorem 4 を使って, $\sharp N_f(x)$ の評価をする訳であるが, その計算は次の 3 つの Step から成る.

Step 1. $\sharp N_f(x)$ を $\sharp B_\gamma(K, x, M)$ の有限和で表す.

Step 2. $\sharp B_\gamma(K, x, M)$ と (4) 式によって対応する, $[G_{k,M} : K]$ を計算する.

Step 3. $\sum_{k=1}^{\infty}(\mu(k)/[G_{k,M} : K])$ の Euler product expansion を計算する.

具体的には, $f(X) = X^2 - m$ のときには, $K = \mathbb{Q}(\sqrt{m})$, $\gamma = \sqrt{m}$ を取り, $f(X) = X^3 - m$ のときには, $K = \mathbb{Q}(\sqrt[3]{m}, \zeta_3)$, $\gamma = \sqrt[3]{m}$ として計算をする.

2. Proof of theorems

2.1 Step 1

ここでの話は, 一般の既約二項方程式で成立するので, $f(X) = X^t - m$ として議論を進めることにする (但し, $m \neq -1$). また, 紙面の都合により各 Proposition の証明は省略する ([3] 参照のこと).

次数 t の素因数分解を $p_1^{a_1} \cdots p_r^{a_r}$ とし, $t_0 = p_1 \cdots p_r$ とする. 更に, $d \mid t$ に対して $K_d = \mathbb{Q}(\sqrt[d]{m}, \zeta_{t_0})$ とする. このとき, $N_f(x)$ と $B_{\sqrt[t]{m}}(K_t, x, t)$ を結びつける次の Proposition が成立する.

Proposition 1.

$$\mathfrak{P} \in B_{\sqrt[t]{m}}(K_t, x, t) \implies \mathcal{N}_{K_t/\mathbb{Q}}(\mathfrak{P}) = p \in N_f(x)$$

また, $N_f(x)$ に属する素数は K_t で完全分解することも簡単に示すことができるので, $B_{\sqrt[t]{m}}(K_t, x, t)$ の元はすべて $N_f(x)$ の元の完全分解によって得られることが分かった. 次に, $p \in N_f(x)$ としたとき, これが $K_t/\mathbb{Q}$ で完全分解して生ずる素 ideal のうち, いくつが $B_{\sqrt[t]{m}}(K_t, x, t)$ に属するかが問題になるが, この解答を与えるのが次の Proposition である.

Proposition 2. $p \in N_f(x)$ が $K_t/\mathbb{Q}$ で完全分解して生ずる素 ideal で, $B_{\sqrt[t]{m}}(K_t, x, t)$ に属するものの個数は,

$$\varphi(t_0) \cdot [K_t : K_1] \cdot \frac{\varphi(\tilde{p})}{\tilde{p}}$$

で与えられる. 但し, $\tilde{p} = p_1^{d_1} \cdots p_r^{d_r}$, $d_i = \begin{cases} 1 & (\text{if } (p-1)/t \not\equiv 0 \pmod{p_i}) \\ 0 & (\text{if } (p-1)/t \equiv 0 \pmod{p_i}) \end{cases}$ とする.

これによって, $\tilde{p}$ の値が同じである $N_f(x)$ の元は, 同じ個数の $B_{\sqrt[t]{m}}(K_t, x, t)$ の元を生じることが分かった. そこで, $\tilde{p}$ の値によって $N_f(x)$ を分割することを考える. t_0 の任意の約数 d に対して,

$$F_f(x, d) := \{ p \in N_f(x) \mid \tilde{p} = d \}$$

とすれば, $N_f(x) = \bigcup_{d \mid t_0} F_f(x, d)$ であり, これは disjoint union なので,

$$\sharp N_f(x) = \sum_{d \mid t_0} \sharp F_f(x, d). \tag{5}$$

この $N_f(x)$ の分割に対応して,

$$A_{\sqrt[t]{m}}(K_t, x, d) := \{ \mathfrak{P} \in B_{\sqrt[t]{m}}(K_t, x, t) \mid \mathcal{N}_{K_t/\mathbb{Q}}(\mathfrak{P}) = p,\ \tilde{p} = d \}$$

とすれば, Proposition 2 より,

$$\sharp A_{\sqrt[t]{m}}(K_t,x,d)=\varphi(t_0)\cdot[K_t:K_1]\cdot\frac{\varphi(d)}{d}\cdot\sharp F_f(x,d) \tag{6}$$

である. この $A_{\sqrt[t]{m}}(K_t,x,d)$ の元を $\mathfrak{P}$ とし $\mathcal{N}_{K_t/\mathbb{Q}}(\mathfrak{P})=p$ とすると $\tilde{p}=d$ で, Proposition 2 の記号で $p_i^{1-d_i}\,|\,(p-1)/t$ となり, $t_0/d=p_1^{1-d_1}\cdots p_r^{1-d_r}$ であるから, $t_0/d\,|\,(p-1)/t$, つまり $p\equiv 1 \pmod{t\cdot t_0/d}$ となる. よって, $\mathfrak{P}$ は $B_{\sqrt[t]{m}}(K_t,x,t)$ の部分集合 $B_{\sqrt[t]{m}}(K_t,x,t\cdot t_0/d)$ の元であることがわかる. 同様に, $\forall s\,|\,d$ について $B_{\sqrt[t]{m}}(K_t,x,t\cdot t_0/d)\supset B_{\sqrt[t]{m}}(K_t,x,t\cdot t_0/s)\supset A_{\sqrt[t]{m}}(K_t,x,s)$ である. 逆に, $B_{\sqrt[t]{m}}(K_t,x,t\cdot t_0/d)$ の元を $\mathfrak{P}$ とすると, $\mathcal{N}_{K_t/\mathbb{Q}}(\mathfrak{P})=p\equiv 1 \pmod{t\cdot t_0/d}$, つまり $t_0/d\,|\,(p-1)/t$ で $\tilde{p}\,|\,d$ となる. よって, $\exists s\,|\,d$ に対して, $\mathfrak{P}$ は $A_{\sqrt[t]{m}}(K_t,x,s)$ の元であることが分かる. 以上のことから,

$$B_{\sqrt[t]{m}}(K_t,x,t\cdot t_0/d)=\bigcup_{s|d}A_{\sqrt[t]{m}}(K_t,x,s)$$

であり, これも disjoint union なので,

$$\sharp B_{\sqrt[t]{m}}(K_t,x,t\cdot t_0/d)=\sum_{s|d}\sharp A_{\sqrt[t]{m}}(K_t,x,s).$$

左辺を d の関数, 右辺を s の関数とみて Möbius の反転公式を使えば,

$$\sharp A_{\sqrt[t]{m}}(K_t,x,d)=\sum_{s|d}\mu(s)\cdot\sharp B_{\sqrt[t]{m}}(K_t,x,t\cdot t_0 s/d) \tag{7}$$

を得る. (5),(6),(7) を合わせると, $\sharp N_f(x)$ を $\sharp B_{\sqrt[t]{m}}(K_t,x,t\cdot t_0 s/d)$ の有限和で表す次の Proposition を得る.

Proposition 3.

$$\sharp N_f(x)=\frac{1}{\varphi(t_0)\cdot[K_t:K_1]}\sum_{d|t_0}\frac{d}{\varphi(d)}\left\{\sum_{s|d}\mu(s)\cdot\sharp B_{\sqrt[t]{m}}\left(K_t,x,t\cdot\frac{t_0 s}{d}\right)\right\}$$

2.2 Step 2, 3 for $f(X)=X^2-m$

ここでは, $f(X)=X^2-m$ の場合の Step 2, 3 の議論を GRH 仮定の下に行う. $t=2$ なので, $t_0=2$, $K_t=\mathbb{Q}(\sqrt{m})$ であるから Proposition 3 より, $m\neq -1$ として,

$$\sharp N_f(x)=\sharp B_{\sqrt{m}}(\mathbb{Q}(\sqrt{m}),x,2)-\frac{1}{2}\sharp B_{\sqrt{m}}(\mathbb{Q}(\sqrt{m}),x,4). \tag{8}$$

また, Theorem 4 より, $M=2,4$ に対する $g(k,M):=[G_{k,M}:\mathbb{Q}(\sqrt{m})]$ の値と $\sum_{k=1}^{\infty}(\mu(k)/g(k,M))$ の Euler product expansion を計算することが目標である.

2.2.1 Computation of $g(k,2)$

体次数 $g(k,M)$ を計算する為には次の 2 つの Lemma が本質的である.

Lemma 1. $m \in \mathbb{Z}$ に対して,

$$\mathbb{Q}(\sqrt[n]{m}) \cap \mathbb{Q}(\zeta_k) = \begin{cases} \mathbb{Q}(\zeta_{(k,2n)}), & (\text{if } m = -1) \\ \mathbb{Q}(\sqrt{m}), & \left(\begin{array}{l} \text{if } m \neq -1 \ \& \ n : \text{even} \ \& \\ \begin{cases} [m]' \equiv 1 \pmod 4 \ \& \ [m]' \mid k, \\ [m]' \not\equiv 1 \pmod 4 \ \& \ 4[m]' \mid k. \end{cases} \end{array} \right) \\ \mathbb{Q}, & (\text{otherwise}). \end{cases}$$

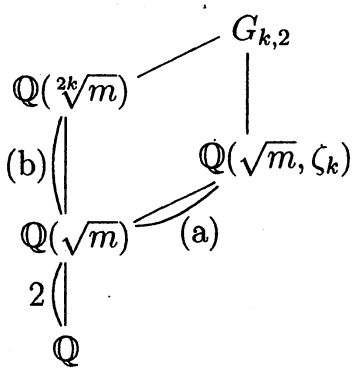
Proof. cf. P.D.T.A Elliot : Acta Arith., **13** (1967) pp.133 Lemma 2 □

Lemma 2. $m \neq -1$ のとき,

$$[\mathbb{Q}(\sqrt[n]{m}) : \mathbb{Q}] = \begin{cases} \dfrac{n}{2(h_m, n)}, & (\text{if } 4 \mid n \ \& \ m = -4k^4 \, (k \in \mathbb{N})) \\ \dfrac{n}{(h_m, n)}, & (\text{otherwise}) \end{cases}$$

Proof. cf. 藤崎 源二郎 : 体とガロア理論, pp.211 □

目標は $\sum_{k=1}^{\infty}(\mu(k)/g(k,2))$ であるから, k は square-free として考える. また, $f(X)$ は既約なので $2 \nmid h_m$ に注意.



定義から,

$$g(k,2) = [\mathbb{Q}(\sqrt[2k]{m}, \zeta_k) : \mathbb{Q}(\sqrt{m})]$$

である. また, Lemma 1 より,

$$(\text{a}) = \begin{cases} \dfrac{\varphi(k)}{2}, & (\text{if } [m]' \equiv 1 \pmod 4 \ \& \ [m]' \mid k) \\ \varphi(k), & (\text{otherwise}) \end{cases}$$

であり, $g(k,2) = (\text{a}) \times (\text{b})$ であることが分かる.

そして, Lemma 2 から,

$$(\text{b}) = \begin{cases} \dfrac{k}{2(h_m, k)}, & (\text{if } 2 \mid k \ \& \ m = -4k^4 \, (k \in \mathbb{N})) \\ \dfrac{k}{(h_m, k)}, & (\text{otherwise}) \end{cases}$$

であるから, これらをまとめると,

Proposition 4. $m \neq -1$ のとき,

$$g(k,2) = \begin{cases} \dfrac{k\varphi(k)}{2(h_m,k)}, & \left(\text{if } \begin{cases} 4 \mid n \ \&\ m = -4k^4\,(k \in \mathbb{N}), \\ [m]' \equiv 1 \pmod 4 \ \&\ [m]' \mid k. \end{cases}\right) \\ \dfrac{k\varphi(k)}{(h_m,k)}, & (\text{otherwise}) \end{cases}$$

2.2.2 Euler product expansion of $\sum(\mu(k)/g(k,2))$

Euler 積表示の為には, 次の Lemma が重要である.

Lemma 3. $h \in \mathbb{N}$ とする. このとき, 数論的関数 $w : \mathbb{N} \to \mathbb{Q}$ を

$$w(k) := \frac{\mu(k)(h,k)}{k\varphi(k)}$$

と定義すると, 無限和 $\sum w(k)$ は,

$$\sum_{k=1}^{\infty} w(k) = \prod_{p \mid h}\left(1 - \frac{1}{p-1}\right)\prod_{p \nmid h}\left(1 - \frac{1}{p(p-1)}\right)$$

なる Euler 積表示を持ち収束する. また, $J \in \mathbb{N}$ を square-free とするとき, 無限和 $\sum_{J \mid k} w(k)$ は,

$$\sum_{J \mid k} w(k) = \prod_{\substack{p \mid J \\ p \mid h}} \frac{-1}{p-2} \prod_{\substack{p \mid J \\ p \nmid h}} \frac{-1}{p^2-p-1} \sum_{k=1}^{\infty} w(k).$$

Proof. $w(k)$ は乗法的 (即ち, $(m,n) = 1 \Rightarrow w(mn) = w(m)w(n)$) であり, Möbius 関数により k が square-free のときが本質的であることに注意すると,

$$\begin{aligned} \sum_{k=1}^{\infty} w(k) &= \left\{\sum_{d \mid J} w(d)\right\}\left\{\sum_{(l,J)=1} w(l)\right\} \\ &= \prod_{p \mid J}\left(1 - \frac{(h,p)}{p(p-1)}\right) \sum_{(l,J)=1} w(l) \\ &= \prod_{\substack{p \mid J \\ p \mid h}}\left(1 - \frac{1}{p-1}\right) \prod_{\substack{p \mid J \\ p \nmid h}}\left(1 - \frac{1}{p(p-1)}\right) \sum_{(l,J)=1} w(l) \\ &= \prod_{p \mid h}\left(1 - \frac{1}{p-1}\right) \prod_{p \nmid h}\left(1 - \frac{1}{p(p-1)}\right) \quad \left[\because J = \prod_{p \in \mathcal{P}(x)} p,\ x \to \infty\right] \end{aligned}$$

となり, この値は Artin's constant C の有理数倍なので収束する. また,

$$\sum_{J \mid k} w(k) = \sum_{(l,J)=1} w(Jl) = \frac{\mu(J)(h,J)}{J\varphi(J)} \sum_{(l,J)=1} w(l)$$

$$= \prod_{\substack{p|J \\ p|h}} \frac{-1}{p-1} \prod_{\substack{p|J \\ p\nmid h}} \frac{-1}{p(p-1)} \sum_{(l,J)=1} w(l)$$

$$= \prod_{\substack{p|J \\ p|h}} \frac{-1}{p-2} \prod_{\substack{p|J \\ p\nmid h}} \frac{-1}{p^2-p-1} \sum_{k=1}^{\infty} w(k)$$

と計算できる. □

次にこの Lemma 3 と Proposition 4 を使って, $\sum_{k=1}^{\infty}(\mu(k)/g(k,2))$ を Euler 積に展開する.

- $m = -4k^4\ (k \in \mathbb{N})$ のとき,

$$\begin{aligned} \sum_{k=1}^{\infty} \frac{\mu(k)}{g(k,2)} &= \sum_{2\nmid k} w(k) + \sum_{2|k} 2w(k) \\ &= \sum_{2\nmid k} w(k) + \sum_{2\nmid k} 2w(2)w(k) \\ &= \sum_{2\nmid k} w(k) - \sum_{2\nmid k} w(k) \quad \left[\because w(2) = -\frac{1}{2}\right] \\ &= 0 \end{aligned} \tag{9}$$

- $[m]' \not\equiv 1 \pmod 4$ & $m \neq -1, -4k^4\ (k \in \mathbb{N})$ のとき,

$$\begin{aligned} \sum_{k=1}^{\infty} \frac{\mu(k)}{g(k,2)} &= \sum_{k=1}^{\infty} w(k) \\ &= \prod_{p|h_m} \left(1 - \frac{1}{p-1}\right) \prod_{p\nmid h_m} \left(1 - \frac{1}{p(p-1)}\right) \\ &= \prod_{p|h_m} \frac{p(p-2)}{p^2-p-1} \prod_{p} \left(1 - \frac{1}{p(p-1)}\right) \\ &= U_m \times C \end{aligned} \tag{10}$$

- $[m]' \equiv 1 \pmod 4$ のとき,

$$\begin{aligned} \sum_{k=1}^{\infty} \frac{\mu(k)}{g(k,2)} &= \sum_{[m]'\nmid k} w(k) + \sum_{[m]'|k} 2w(k) \\ &= \sum_{k=1}^{\infty} w(k) + \sum_{[m]'|k} w(k) \\ &= \left\{1 + \prod_{\substack{p|[m]' \\ p|h_m}} \frac{-1}{p-2} \prod_{\substack{p|[m]' \\ p\nmid h_m}} \frac{-1}{p^2-p-1}\right\} \sum_{k=1}^{\infty} w(k) \\ &= U_m(1+V_m) \times C \end{aligned} \tag{11}$$

同様にすれば, $g(k,4)$ を計算し $\sum(\mu(k)/g(k,4))$ の Euler 積表示も得ることができて, (8) から $\delta(N_f)$ の値を計算することができる.

2.2.3 Case $m=-1$

ここでは, 除外していた $m=-1$ の case について考える. $f(X)=X^2+1$ とすると, 明らかに $p\in N_f(x) \Leftrightarrow r(-1,p)=2$ であるから, $N_f=\{2\}$ (つまり, $\sharp N_f<\infty$, $\delta(N_f)=0$) で X^2+1 は例外多項式である.

Remark. $m=-1$ のとき, 形式的に $\sum_{k=1}^{\infty}(\mu(k)/g(k,2))$ を計算してみると, $g(k,2)=[\mathbb{Q}(\sqrt[2k]{-1},\zeta_k):\mathbb{Q}(\sqrt{-1})]=[\mathbb{Q}(\zeta_{4k}):\mathbb{Q}(\zeta_4)]=\varphi(4k)/2$ であるから,

$$\begin{aligned}\sum_{k=1}^{\infty}\frac{\mu(k)}{g(k,2)}=\sum_{k=1}^{\infty}\frac{2\mu(k)}{\varphi(4k)}&=\sum_{2\nmid k}\frac{2\mu(k)}{\varphi(4k)}+\sum_{2|k}\frac{2\mu(k)}{\varphi(4k)}\\&=\sum_{2\nmid k}\frac{2\mu(k)}{\varphi(4k)}-\sum_{2\nmid k}\frac{\mu(k)}{\varphi(4k)}\\&=\frac{1}{2}\sum_{2\nmid k}\frac{\mu(k)}{\varphi(k)}\\&=\frac{1}{2}\prod_{p\geq 3}\left(1-\frac{1}{p-1}\right)\end{aligned}$$

ここで Mertents's Theorem より, e を自然対数の底, E を Euler's constant として,

$$0<\frac{1}{2}\prod_{3\leq p\leq x}\left(1-\frac{1}{p-1}\right)<\prod_{p\leq x}\left(1-\frac{1}{p}\right)=\frac{e^{-E}}{\log x}+O\left(\frac{1}{\log^2 x}\right)$$

であるから, $x\to\infty$ として,

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{g(k,2)}=0$$

となる. このように factor が全て正で, Euler product が 0 に収束していく X^2-m の形の例外多項式は X^2+1 だけである. その他の例外多項式, 例えば X^2+4k^4 $(k\in\mathbb{N})$ のときは,

$$\begin{aligned}\sum_{k=1}^{\infty}\frac{\mu(k)}{g(k,2)}&=\sum_{2\nmid k}w(k)+\sum_{2|k}2w(k)\\&=\sum_{k=1}^{\infty}w(k)+\sum_{2|k}w(k)\\&=\left\{1+\prod_{\substack{p|2\\p|h_m}}\frac{-1}{p-2}\prod_{\substack{p|2\\p\nmid h_m}}\frac{-1}{p^2-p-1}\right\}\times U_m\times C\\&=0\times U_m\times C=0\quad\left[\because 2\nmid h_m\right]\end{aligned}$$

のように1つのfactorが0であるが為に例外性を持つのである.

これまでの議論をまとめれば, Theorem 2を得ることができる. また, Theorem 3も同様な議論で得られるし, 一般の既約二項方程式 $f(X) = X^t - m$ に対しても (複雑になると思われるが) $\delta(N_f)$ の値は計算可能である.

このTheorem 2, 3から $\delta(N_f) = 0$ であるものを絞り込むことができて, それらに対して直接例外性を示す (このことにGRHは仮定しない, [6] 参照) ことによって, 例外多項式を決定するTheorem 1を導くことができるのである.

参考文献

[1] C.Hooley : *On Artin's Conjecture.* J. reine angew. Math., **225** (1967), 209-220.

[2] H.W.Lenstra, Jr. : *On Artin's Conjecture and Euclid's Algorithm in Global Fields.* Invent. Math., **42** (1977), 201-224.

[3] Leo Murata : *A problem analogous to Artin's conjecture for primitive roots and its applications.* Arch. Math. (Basel) **57** (1991), no.6, 555–565.

[4] J.W.Sander : *On Fibonacci Primitive Roots.* Fibonacci Quarterly, **28** (1990), 79-80.

[5] D.Shanks. : *Fibonacci Primitive Roots.* Fibonacci Quarterly, **10** (1972), 163-168.

[6] R.Takeuchi : *On the polynomial type generalization of "Artin's Conjecture for primitive root"* (in Japanese). Tokyo Metropolitan University, Master thesis (1997/98).

[7] C.Batut, D.Bernardi, H.Cohen, M.Oliver. : PARI-GP 1.39. `ftp://megrez.math.u-bordeaux.fr/pub/pari/`

〒192-0397 東京都八王子市南大沢1－1
東京都立大学理学研究科数学教室
E-mail: `ryouhei@comp.metro-u.ac.jp`