2024（令和 6）年度特別研究
有限アーベル群の指標と整数論
（指導教員　平野幹）

1320012Y　井上幸治
1320107C　只信伊織
1320143Z　沼田要
1320180K　満岡音羽
1320216Z　山本琳太郎

要旨

G を有限アーベル群とするとき、G から環 $\mathbb{C}$ の乗法群 $\mathbb{C}^\times$ への群準同型 $\chi : G \to \mathbb{C}^\times$ のことを G 上の指標という。有限アーベル群の指標は整数論において基本的であり、素数の研究において有用である。今回の卒業研究では，指標によって定義される概念として L 関数やガウス和，ヤコビ和，3 次剰余指標などについて学び，ディリクレの算術級数定理や 3 次剰余の相互法則といった非常に興味深い定理を証明した．この過程を通じて，有限アーベル群の指標と整数論の関わりについて解析的整数論と代数的整数論の二つの観点から理解を深めることができた。

第 1 章では，有限アーベル群の指標について述べる．まず，有限アーベル群 G 上の指標を定義し，群 G と G 上の指標全体のなす群の間の関係や直交性という性質を証明する．また，ディリクレ指標やルジャンドル記号などの重要な指標の例を導入する．

第 2 章では，有限アーベル群の指標と解析的整数論の関わりの一例について述べる．まず，$N \in \mathbb{N}$ とするとき，剰余環 $\mathbb{Z}/N\mathbb{Z}$ の乗法群 $(\mathbb{Z}/N\mathbb{Z})^\times$ 上の指標 χ に対して，ディリクレの L 関数 $L(s, \chi)$ を定義する．そこでは，類型であるリーマンのゼータ関数 $\zeta(s)$ の性質を踏まえて，L 関数の積表現や全複素平面への解析接続について述べる．そして，$s = 1$ での値 $L(1, \chi)$ を評価することによって，ある形の素数の無限性を示すディリクレの算術級数定理を証明する．

第 3 章では，有限アーベル群の指標と代数的整数論の関わりの一例について述べる．最初に，p を素数とするとき，剰余環 $\mathbb{Z}/p\mathbb{Z}$ の乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ 上の指標 χ, λ に対して，整数論で重要なガウス和 $g(\chi)$ やヤコビ和 $J(\chi, \lambda)$ を定義する．これを用いて，2 つの素数の間の関係を記述する平方剰余の相互法則を証明する．次に，環 $\mathbb{Z}[\omega]$ の素元 π に対して 3 次剰余指標 χ_π を定義し，これを使って 3 次合同方程式 $x^3 \equiv a \ (\pi),\ a \in \mathbb{Z}[\omega]$ が解を持つための必要十分条件を述べる．そして，この 3 次剰余指標によって $\mathbb{Z}[\omega]$ の素元の間の関係を記述する 3 次剰余の相互法則を先のガウス和とヤコビ和を用いて証明する．

目次

1. 有限アーベル群の指標

1.1 指標 [満岡 菅羽]

Def 1.1

有限アーベル群 G 上の指標 $\overset{\text{def}}{\Leftrightarrow}$ 準同型 $\chi : G \to \mathbb{C}^\times$ $(\mathbb{C}^\times = \mathbb{C} \setminus \{0\})$

$\widehat{G}$ を指標全体からなる集合とすると、$\forall \chi, \chi' \in \widehat{G}$ に対し、

積：$\chi\chi'(g) \overset{\text{def}}{=} \chi(g)\chi'(g)$ 、逆：$\chi^{-1}(g) \overset{\text{def}}{=} \chi(g)^{-1}$ $(\forall g \in G)$

が定義され、$\widehat{G}$ は群をなす。（$\widehat{G}$ を指標群という。）

また、e：G の単位元 とすると、$\chi(e) = 1$ である。

よって、$\#G = n$ のとき、

$$\chi(g)^n = \chi(g^n) = \chi(e) = 1 \qquad (\chi(g) \text{は} 1 \text{の} n \text{乗根})$$

であり、特に $|\chi(g)| = 1$ が成り立つ。

これより、$\chi \in \widehat{G}$ に対し、共役：$\overline{\chi}(g) \overset{\text{def}}{=} \overline{\chi(g)}$ $(\forall g \in G)$ を定義すると、

$$\chi(g)\overline{\chi}(g) = \chi(g)\overline{\chi(g)} = |\chi(g)|^2 = 1$$

より、$\overline{\chi}(g) = \chi^{-1}(g)$ である。

Th 1.2

G：有限アーベル群のとき、$G \simeq \widehat{G}$ とくに、$|G| = |\widehat{G}|$

proof

> 有限アーベル群の基本定理
>
> G：有限アーベル群 に対し、$\exists g_1, \cdots, g_k \in G$（$G$ の生成元）、$\exists n_1, \cdots, n_k \in \mathbb{Z}_{>0}$（$g_i (i = 1, \cdots, k)$ に対応する位数）s.t.
>
> $$G \simeq \langle g_1 \rangle \times \cdots \times \langle g_k \rangle \ , \ \langle g_i \rangle \simeq \mathbb{Z}/n_i\mathbb{Z} \quad (i = 1, \cdots, k)$$

$\chi \in \widehat{G}$ に対し、$\chi(g_i)^{n_i} = 1$

ここで、$H = \{(\alpha_1, \cdots, \alpha_k) \in \mathbb{C}^k \mid \alpha_i^{n_i} = 1\} = \{(\zeta_1^{r_1}, \cdots, \zeta_k^{r_k}) \mid 0 \le r_i \le n_i - 1, \zeta_i : 1 \text{の原始} n_i \text{乗根}\}$

とすると、このとき

$$\varphi : \widehat{G} \to H \ ; \ \chi \mapsto (\chi(g_1), \cdots, \chi(g_k))$$

$$\psi : H \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \ ; \ (\zeta_1^{r_1}, \cdots, \zeta_k^{r_k}) \mapsto (r_1, \cdots, r_k)$$

が定義され、これらは同型である。したがって、このことと有限アーベル群の基本定理より

$$\widehat{G} \simeq H \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \simeq G$$

□

Def 1.3

$\bmod N (\in \mathbb{N})$ の ディリクレ指標 $\overset{\text{def}}{\Leftrightarrow}$ 群 $(\mathbb{Z}/N\mathbb{Z})^\times = \{n \pmod N \mid (n, N) = 1\}$ 上の指標

このとき、関数 $\chi : \mathbb{Z} \to \mathbb{C}$（同じ χ に対して）を

$$\chi(n) = \begin{cases} \chi\ (n\ (\mathrm{mod}\ N)) & (n,N)=1 \\ 0 & (n,N)>1 \end{cases}$$

と定義する。この関数もまた、ディリクレ指標という。

ディリクレ指標は次の性質をもつ。

(1) $\chi(n)=0 \iff (n,N)>1$

(2) $\forall m,n \in \mathbb{Z}$ に対し、$\chi(mn)=\chi(m)\chi(n)$ （強い意味で乗法的）

(3) $m \equiv n\ (N) \Rightarrow \chi(m)=\chi(n)$ （$\chi(n)$ は $n\ (\mathrm{mod}\ N)$ にのみ依存）

Ex 1.4

$\forall \bar{n} \in (\mathbb{Z}/N\mathbb{Z})^\times$ に対し、

$$\chi_0(\bar{n}) = 1$$

は $(\mathbb{Z}/N\mathbb{Z})^\times$ 上の指標であり、主指標という。また、χ_0 は $\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$ 上の単位元である。

Ex 1.5

p：素数とし、$\forall \bar{n} \in (\mathbb{Z}/p\mathbb{Z})^\times$ に対し、

$$\chi_2(\bar{n}) := \left(\frac{n}{p}\right) := \begin{cases} 0 & p \mid n \\ 1 & p \nmid n \text{ かつ } \exists x \in \mathbb{Z} \text{ s.t. } x^2 \equiv n\ (p) \\ -1 & \text{その他} \end{cases}$$

は $(\mathbb{Z}/p\mathbb{Z})^\times$ 上の指標であり、ルジャンドル記号という。

Th 1.2 より $\varphi(N)$ 個のディリクレ指標が存在する。ここで、

$$\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times = \#\{n\ (\mathrm{mod}\ N) \mid (n,N)=1\} = N\prod_{p \mid N}(1-p^{-1})$$

はオイラー関数である。

Th 1.6 （直交性）

χ：mod N のディリクレ指標とする。このとき、

$$\sum_{n\ (\mathrm{mod}\ N)} \chi(n) = \begin{cases} \varphi(N) & \chi=\chi_0 \\ 0 & \chi \neq \chi_0 \end{cases}$$

（※ $\sum_{n\ (\mathrm{mod}\ N)}$ は $\mathbb{Z}/N\mathbb{Z}$ の任意の1つの代表系についての和を示す。）

proof

$\chi=\chi_0$ のとき、

$$\sum_{n\ (\mathrm{mod}\ N)} \chi(n) = \#\{\chi_0=1 \text{ をとる } n\} = \#(\mathbb{Z}/N\mathbb{Z})^\times = \varphi(N)$$

より成り立つ。

$\chi \neq \chi_0$ のとき、

$\exists m \in \mathbb{Z}$ s.t. $(m, N) = 1$ かつ $\chi(m) \neq 1$

2のとき、

$$(1 - \chi(m)) \sum_{n \pmod N} \chi(n) = \sum_{n \pmod N} \chi(n) - \sum_{n \pmod N} \chi(mn)$$
$$= \sum_{n \pmod N} \chi(n) - \sum_{n \pmod N} \chi(n)$$
$$= 0$$

(☺ mn は n とともに $\mathbb{Z} \pmod N$ の代表系を動く)

$\chi(m) \neq 1$ より $1 - \chi(m) \neq 0$ よって $\sum_{n \pmod N} \chi(n) = 0$ □

Cor 1.7

χ_1, χ_2 : 2つのディリクレ指標 $\pmod N$ とする。このとき、

$$\frac{1}{\varphi(N)} \sum_{n \pmod N} \chi_1(n) \overline{\chi_2}(n) = \begin{cases} 1 & \chi_1 = \chi_2 \\ 0 & \chi_1 \neq \chi_2 \end{cases}$$

proof Th 1.6 より χ を $\chi_1 \overline{\chi_2}$ とすると導かれる。 □

Th 1.8

$n \in \mathbb{Z}$ とする。このとき、

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(N) & n \equiv 1 \ (N) \\ 0 & n \not\equiv 1 \ (N) \end{cases}$$

(※ $\sum_{\chi}$ はすべてのディリクレ指標 $\pmod N$ をわたる。)

proof $G = \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$ とすると、

$\chi : G \to \mathbb{C}^\times ; \chi \mapsto \chi(x)$ (Th 1.8)

は、$G' = (\mathbb{Z}/N\mathbb{Z})^\times$ とした

$\chi : G' \to \mathbb{C}^\times ; x \mapsto \chi(x)$ (Th 1.6)

と同型であるため、Th 1.6 と同じものと考えられ、この定理は成り立つ。 □

Cor 1.9

$a, b \in \mathbb{Z}$, $(b, N) = 1$ とする。このとき、

$$\frac{1}{\varphi(N)} \sum_{\chi} \chi(a) \overline{\chi}(b) = \begin{cases} 1 & a \equiv b \ (N) \\ 0 & a \not\equiv b \ (N) \end{cases}$$

proof $nb \equiv a \ (N)$ となる $n \in \mathbb{Z}$ をとると、$\forall \chi : \bmod N$ のディリクレ指標に対し、

$$\chi(a) = \chi(nb) = \chi(n)\chi(b)$$

両辺 $\overline{\chi(b)}$ をかけると $|\chi(b)|^2 = 1$ より

$$\chi(a)\overline{\chi(b)} = \chi(n)$$

よって、Th1.8 より成り立つ。 □

2. 解析的整数論と指標

解析的整数論ではリーマンのゼータ関数、ディリクレ指標、L 関数について扱った。

2.1　L 関数　[山本琳太郎・井上幸治]

Def 2.1　リーマンのゼータ関数

リーマンのゼータ関数$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}(\sigma>1)$は$s=1$で 1 位の極をもち$\sigma>1$で成り立つオイラー積表示$\zeta(s)=\prod_p\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots\right)=\prod_p\frac{1}{1-p^{-s}}$　$\left(p\text{は素数}\right)$をもつ。

また、メリン変換により$\sigma>1$で成り立つ積分表示

$\Gamma(s)$をガンマ関数として、

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

をもつ

また、解析接続によって複素数全体に有理型関数として接続される。

リーマンのゼータ関数には有名な関数等式が知られている。

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

Def 2.2　χ をディリクレ指標（mod N）とする。χ に対応するディリクレの L 関数とは

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\tag{1}$$

と定義され、$|\chi(n)|\leq 1$であることからこの級数は$\sigma>1$に対してリーマンのゼータ関数で上から抑えられることより絶対収束する。

χ は乗法性を持つので、オイラー積表示

$$L(s,\chi)=\prod_p\left(1+\frac{\chi(p)}{p^s}+\frac{\chi(p^2)}{p^{2s}}+\cdots\right)$$

をもち、さらに χ は強い意味での乗法性$\chi(p^k)=\chi(p)^k$をもつので

$$L(s,\chi)=\prod_p(1-\chi(p)p^{-s})^{-1}\,(\sigma>1)\tag{2}$$

主指標χ_0に対しては(2)より、

$$L(s,\chi_0)=\prod_p(1-\chi_0(p)p^{-s})^{-s}$$

$\chi_0(p)$は p が N の約数のとき、つまり素因数のとき 0 なので

$$\prod_p (1-\chi_0(p)p^{-s})^{-s} = \prod_{p\nmid N}(1-p^{-s})^{-1}$$
$$= \prod_{p|N}(1-p^{-s})\prod_p (1-p^{-s})^{-1}$$
$$= \prod_{p|N}(1-p^{-s})\cdot\zeta(s)$$

$\prod_{p|N}(1-p^{-s})$は有限の値なのでこのときＬ関数は特定の因数を除いてリーマンのゼータ関数と一致し、そしてそれは解析接続により複素数全体に有理型に接続され唯一の特異点としてs=1において留数$\prod_{p|N}(1-p^{-1}) = \frac{\varphi(N)}{N}$の１位の極をもつ。

$\chi \neq \chi_0$に対して$x \to \infty$のとき、定理 2.1　ディリクレ指標の直交性より

$$\left|\sum_{n=1}^{x}\chi(n)\right| = \left|\sum_{n=1}^{N(x|N)}\chi(n) + \sum\nolimits_{*}\chi(n)\right| \left(\sum\nolimits_{*} \square : n = N\left[\frac{x}{N}\right]+1 \sim x\right)$$
$$= \left|\left[\frac{x}{N}\right]\sum_{n(modN)}\chi(n) + \sum\nolimits_{*}\chi(n)\right|$$
$$= \left|\sum\nolimits_{*}\chi(n)\right| \leq \left|x - N\left[\frac{x}{N}\right]\right|$$
$$\leq N = \mathrm{O}(1)$$

より$L(s,\chi)$の収束軸σ_0は$\sigma_0 = \limsup_{k\to\infty}\frac{\log\sum_{n=k}^{\infty}\chi(n)}{\log(k)} = \limsup_{k\to\infty}\frac{\log N}{\log k} = 0$より０であることがわかる。(1)は$\sigma > 0$において正則な関数を定義し、それはまた解析接続によって複素数全体に正則に接続され$\zeta(s)$のような関数等式をみたす。

以上より、Ｌ関数は$\chi = \chi_0$のとき、$L(s,\chi_0)$は$\sigma > 1$で収束し複素数全体に有理型関数として接続され$s = 1$で1位の極をもつ。$\chi \neq \chi_0$のとき、$L(s,\chi)$は$\sigma > 0$で収束し複素数全体に正則に接続される。

Ｌ関数の重要な定理として$L(1,\chi) \neq 0$であることを証明する。また、この結果から$(a,N) = 1$（$a \in \mathbb{Z}, N \in \mathbb{N}$)をみたすとき、$Nk + a(k \in \mathbb{Z}_{\geq 1})$の形の素数が無限に存在することを示すことができる。

Th 2.3 χをχ_0と異なるディリクレ指標（mod N）とする。このとき

$$L(1,\chi) \neq 0$$

proof

$$F(s) = \prod_{\chi} L(s,\chi)$$

とおく。ここでχはすべてのディリクレ指標にわたる。このとき$\sigma > 1$において
(2)のオイラー積表示と対数をとることにより

$$\log F(s) = \sum_{\chi}\sum_{p} \log(1-\chi(p)p^{-s})^{-1}$$

$$= \sum_{\chi}\sum_{p}\sum_{r=1}^{\infty} \frac{1}{r}\frac{\chi(p)^r}{p^{rs}} \qquad \left(\log \text{のテイラー展開により}\right)$$

$$= \varphi(N)\sum_{p}\sum_{\substack{r\geq 1 \\ p^r \equiv 1 (mod N)}} \frac{1}{rp^{rs}} \qquad \left(\text{ディリクレ指標の直交性より}\right)$$

このことから$s \in \mathbb{R}_{>1}$に対して$\log F(s) \geq 0$　よって

$$\lim_{s\to 1} F(s) \geq 1 \left(s\text{: 実数}\right)$$

F(s)は s=1 で 1 位の極をもつ唯一の因子$L(s,\chi_0)$を含むので、2 つ以上の指標$\chi \neq \chi_0$に対して$L(1,\chi) = 0$ならば$F(s)$は$s = 1$で正則で$\lim_{s\to 1} F(s) = 0$であるがそれはこの結果に矛盾する。
よって$L(1,\chi) = 0$となるような$\chi \neq \chi_0$が存在するならばそれは高々 1 つしかない。
そのような指標 χ は$L(1,\chi) = 0$より$L(1,\bar{\chi}) = \overline{L(1,\chi)} = 0$より存在するならば実指標でなければならないことがわかる。

Th 2.3　（再掲）

「χ を χ_0 と異なるディリクレ指標 $(\mathrm{mod}\ N)$ とする。そのとき

$$L(1,\chi) \neq 0$$

が成り立つ。」

proof

$L(1,\chi) = 0$ となる指標が存在するならば実指標であることが示された。しかし実際にはそうした実指標は存在しない。つまり、実指標 $\chi \neq \chi_0$ であれば $L(1,\chi) \neq 0$ である。この事実を背理法により示す。

証明に先立ち、L 関数 $L(s,\chi)$ の正則性について記しておく。

・$\chi = \chi_0$ のとき、$s = 1$ において留数 $\frac{\varphi(N)}{N}$ の 1 位の極をもち、それ以外では正則。したがって

$$\lim_{s\to 1} L(s,\chi_0) = \infty$$

・$\chi \neq \chi_0$ のとき、解析接続により $\sigma > 0$ で広義一様絶対収束する正則関数。

まず、実指標 $\chi \neq \chi_0$ が $L(1,\chi) = 0$ を満たしていると仮定して矛盾を導く。

$\sigma > 1$ に対して

$$\Phi(s) = \frac{L(s,\chi)L(s,\chi_0)}{L(2s,\chi_0)}$$

とおく。すると分子は、$s = 1$ における $L(s,\chi_0)$ の極は、そこにおける $L(s,\chi)$ の零点と打ち消しあって正則である。一方、分母 $L(2s,\chi_0)$ は $s = \frac{1}{2}$ で極を持つ以外は正則で 0 とは異なるから、結局 $\Phi(s)$ は $\sigma \geqq \frac{1}{2}$ に対して正則である。

$\sigma > 1$ に対して、オイラー積表示を使って変形すると、

$$\begin{aligned}
\Phi(s) &= \prod_p \frac{1-\chi_0(p)p^{-2s}}{(1-\chi(p)p^{-s})(1-\chi_0(p)p^{-s})} \\
&= \prod_{p\nmid N} \frac{1-p^{-2s}}{(1-\chi(p)p^{-s})(1-p^{-s})} \qquad (\because \text{ディリクレ指標の定義}) \\
&= \prod_{p\nmid N} \frac{1+p^{-s}}{1-\chi(p)p^{-s}} \\
&= \prod_{\chi(p)=1} \frac{1+p^{-s}}{1-p^{-s}} = \prod_{\chi(p)=1} (1+p^{-s})\cdot\frac{1}{1-p^{-s}} \\
&= \prod_{\chi(p)=1} (1+p^{-s})(1+p^{-s}+p^{-2s}+\cdots) \\
&= \prod_{\chi(p)=1} (1+2p^{-s}+2p^{-2s}+\cdots)
\end{aligned}$$

となる。なお 3 行目と 4 行目の等号は χ が実指標のため $\chi(p) = \pm 1$ であり、$\chi(p) = -1$ なら、$\frac{1+p^{-s}}{1+p^{-s}} = 1$ となることから $\chi(p) = 1$ を満たすものだけの和になることによる。

この結果より $\Phi(s)$ を非負実係数の通常のディレクレ級数と見ることができ、

$$\Phi(s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}\qquad(\sigma>1)\,,\ a_n\geq 0$$

と表すと、$\sigma>1$ で絶対収束する。
そこで $\Phi(s)$ を $s=2$ においてテーラー展開する。$\Phi(s)$ は $\sigma\geqq\frac{1}{2}$ で正則であるから、正則領域 $|s-2|<\frac{3}{2}$ に対してテイラー展開ができる。つまり

$$\Phi(s)=\sum_{k=0}^{\infty}\frac{(s-2)^k}{k!}\Phi^{(k)}(2)$$

ここで $\sigma>1$ ではディレク級数は絶対収束するため微分と和の交換ができるので

$$\begin{aligned}\Phi^{(k)}(2)&=\frac{d^{(k)}}{ds^{(k)}}\left(\sum_{n=1}^{\infty}\frac{a_n}{n^s}\right)\Bigg|_{s=2}\\&=\sum_{n=1}^{\infty}\left(\frac{d^{(k)}}{ds^{(k)}}\frac{a_n}{n^s}\right)\Bigg|_{s=2}\\&=\sum_{n=1}^{\infty}a_n(-\log n)^k n^{-s}\Bigg|_{s=2}=\sum_{n=1}^{\infty}a_n(-1)^k(\log n)^k n^{-2}\end{aligned}$$

よって、

$$\Phi(s)=\sum_{k=0}^{\infty}\frac{(s-2)^k}{k!}\sum_{n=1}^{\infty}a_n(-1)^k(\log n)^k n^{-2}=\sum_{k=0}^{\infty}\frac{(2-s)^k}{k!}\sum_{n=1}^{\infty}\frac{a_n\,(\log n)^k}{n^2}$$

すると、$a_n\geqq 0$ によって右辺に生じた二重和は、実数 s, $\frac{1}{2}<s<2$ に対して単調減少関数となっていることを示している。従って、

$$\Phi(s)\geqq\Phi(2)=\sum_{n=1}^{\infty}\frac{a_n}{n^2}\geqq 1\quad\therefore\Phi(s)\geqq 1\quad\left(s\in\mathbb{R},\ \frac{1}{2}<s<2\right)$$

しかし、一方で $\Phi(s)$ は、分子は $s=\frac{1}{2}$ で正則だから有界であり、分母 $L(2s,\chi_0)$ は $s=\frac{1}{2}$ で極を持つから、

$$\lim_{s\to\frac{1}{2}+0}\Phi(s)=\frac{L(\frac{1}{2},\chi)L(\frac{1}{2},\chi_0)}{\lim_{s\to\frac{1}{2}+0}L(2s,\chi_0)}=0$$

となり、これは $\frac{1}{2}<s<2$ に対して $\Phi(s)\geqq 1$ であることに矛盾している。
したがって、$L(1,\chi)=0$ となる実指標 $\chi\neq\chi_0$ は存在しない。つまり、$\chi\neq\chi_0$ であれば、$L(1,\chi)\neq 0$ である。 □

以上で準備が整ったので、ディリクレ指標 $\chi\pmod N$ に対応したディリクレの L 関数の解析的な性質を使ってディリクレの算術級数定理を証明する。

0.1　ディリクレの算術級数定理 [井上 幸治]

Th 2.4「$N \in \mathbb{N}$ とし、$a \in \mathbb{Z}$ が $(a, N) = 1$ を満たしているとする。
そのとき、等差数列（算術級数）$\{Nk + a\}_{k=1,2,3,\cdots}$ は無限個の素数を含む。」
この定理を証明するには

$$\sum_{\substack{p \\ p \equiv a \pmod N}} \frac{1}{p} = \infty \qquad (p : \text{素数})$$

を示せば十分である。なぜなら、$p = Nk + a \ \Leftrightarrow \ p \equiv a \pmod N$ を満たす素数 p が有限個しかなければ、その逆数の和は有限になり上式は成り立たない。よってこの十分条件が成り立つことを示していく。
proof
$\sigma > 1$ に対して

$$G(s) = \sum_{\substack{p \\ p^r \equiv a \pmod N}} \sum_{\substack{r \geqq 1}} \frac{1}{rp^{rs}}$$

とおく。すると、右辺は

$$\sum_{\substack{p \\ p^r \equiv a \pmod N}} \sum_{\substack{r \geqq 1}} \frac{1}{rp^{rs}} \leqq \sum_{\substack{p \\ p^r \equiv a \pmod N}} \sum_{\substack{r \geqq 1}} \frac{1}{(p^r)^s} = \zeta(s)$$

と $\zeta(s)$ で上から抑えられるため $\sigma > 1$ で絶対収束する。そこで右辺の二重和について 2 通りの変形をして $s \to 1$ の極限を考える。

(A) まず $G(s)$ をディリクレ指標 $\chi \pmod N$ の直交性を使い、$\chi = \chi_0$ の和 (A_1) と $\chi \neq \chi_0$ の和 (A_2) の 2 つに分ける。

$$\begin{aligned}
G(s) &= \sum_p \sum_{r \geqq 1} \frac{1}{\varphi(N)} \sum_\chi \overline{\chi}(a)\chi(p^r)\frac{1}{rp^{rs}} \qquad (\because ★★★★) \\
&= \frac{1}{\varphi(N)} \sum_\chi \overline{\chi}(a) \sum_p \sum_{r=1}^{\infty} \frac{\chi(p)^r}{rp^{rs}} \\
&= \frac{1}{\varphi(N)} \sum_\chi \overline{\chi}(a) \log L(s, \chi) \qquad (\because \text{L 関数のオイラー積表示}) \\
&= \underbrace{\frac{1}{\varphi(N)} \log L(s, \chi_0)}_{(A_1)} \quad + \quad \underbrace{\frac{1}{\varphi(N)} \sum_{\chi \neq \chi_0} \overline{\chi}(a) \log L(s, \chi)}_{(A_2)}
\end{aligned}$$

（★★★★）ディリクレ指標の直交性より、$p^r,\ a \in \mathbb{Z},\ (a, N) = 1$ のとき

$$\frac{1}{\varphi(N)} \sum_\chi \chi(p^r)\overline{\chi}(a) = \begin{cases} 1 & p^r \equiv a \pmod N \text{のとき} \\ 0 & p^r \not\equiv a \pmod N \text{のとき} \end{cases}$$

ここで絶対収束性により、和の順序交換は許される。
すると、$L(s, \chi_0)$ は $s = 1$ で 1 位の極を持つので $s \to 1$ のとき (A_1) は ∞ に発散する。

一方、$\log L(s,\chi)$ は $\chi \neq \chi_0$ に対し、$L(s,\chi) \neq 0$ かつ有界であるから、(A_2) は 0 以外の有限な値に収束する。つまり $s \to 1$ のとき (A_1) と (A_2) の和である $G(s)$ は発散しなければならない。

(B) 次に内側の r に関する和を $r=1$ の和 (B_1) と $r \geqq 2$ の和 (B_2) の 2 つに分ける。

$$G(s) = \underbrace{\sum_{\substack{p \\ p \equiv a \pmod N}} \frac{1}{p^s}}_{(\mathsf{B}_1)} + \underbrace{\sum_{p} \sum_{\substack{r \geq 2 \\ p^r \equiv a \pmod N}} \frac{1}{rp^{rs}}}_{(\mathsf{B}_2)}$$

この (B_2) で $s=1$ としたものを評価すると、

$$\begin{aligned}
(B_2)|_{s=1} &\leqq \sum_p \sum_{r=2}^{\infty} \frac{1}{rp^r} \\
&\leqq \sum_p \sum_{r=2}^{\infty} \frac{1}{2p^r} = \sum_p \frac{1}{2} \cdot \frac{p^{-2}}{1-p^{-1}} = \sum_p \frac{1}{2} \cdot \frac{1}{p(p-1)} \\
&\leqq \sum_{n=2}^{\infty} \frac{1}{2} \cdot \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \frac{1}{2} \left(\frac{1}{n-1} - \frac{1}{n} \right) = \frac{1}{2} \text{（有界）}
\end{aligned}$$

したがって、$s \to 1$ のとき、(B_2) は有界である。
ところで先ほどの (A) 式の評価結果により、$s \to 1$ のとき $G(s)$ は発散する。すると (B_2) は有界であるので $s \to 1$ のとき (B_1) は発散しなければならない。
よって (B_1) で $s \to 1$ として

$$\sum_{\substack{p \\ p \equiv a \pmod N}} \frac{1}{p} \quad \to \quad \infty$$

が成り立ち、定理の十分条件が示せた。 □

この定理を使えば様々な規則性を持った素数が無限に存在することがわかる。
例えば、$N=10, a=1$ とすると、$11, 31, 41, 61, 71, 101$ などの一の位が 1 の素数が無限個あることがわかるし、$a=3,7,9$ のときには同様に一の位が 3,7,9 の素数も無限にあることがわかる。
また　$N=1000, a=1$ のとき　　$3001,\ 4001,\ 7001,\ 9001,\ 13001, \cdots$
　$N=1000, a=-1$ のとき　　$1999,\ 2999,\ 4999,\ 8999,\ 13999, \cdots$
と、下 3 桁が 001 や 999 の素数が無限にあることもわかる。

3　代数的整数論と指標

3.1　ガウス和とヤコビ和 [只信伊織]

ここでは，整数論において重要なガウス和を定義し，その性質をいくつか述べる．以下では，p を素数とし，$F_p \coloneqq \mathbb{Z}/p\mathbb{Z}$ とおく．また，χ を $F_p^\times$ 上の指標とする．

定義 3.1. $a \in F_p$ とする．このとき，χ に対して，

$$g_a(\chi) \overset{\text{def}}{=} \sum_{t \in F_p^\times} \chi(t)\zeta^{at}$$

と定義する．ここで，ζ は 1 の原始 p 乗根である．$g_a(\chi)$ を χ に属する F_p 上の**ガウス和**という．

上の定義では，$a = n + p\mathbb{Z}$ に対して $\zeta^a \coloneqq \zeta^n$ と定めていることに注意する．このとき，$k \in \mathbb{Z}$ とすると $\zeta^{a+pk} = \zeta^a(\zeta^p)^k = \zeta^a$ となるので，ζ^a の値は代表元の取り方によらない．

命題 3.2. $a \in F_p$ とする．

(1) $a \neq 0$ かつ $\chi \neq \chi_0$ ならば，$g_a(\chi) = \chi(a^{-1})g_1(\chi)$.

(2) $a \neq 0$ かつ $\chi = \chi_0$ ならば，$g_a(\chi_0) = -1$.

(3) $a = 0$ かつ $\chi \neq \chi_0$ ならば，$g_0(\chi) = 0$.

(4) $a = 0$ かつ $\chi = \chi_0$ ならば，$g_0(\chi_0) = p - 1$.

証明. (1). $a \neq 0$ かつ $\chi \neq \chi_0$ とする．このとき，

$$\chi(a)g_a(\chi) = \chi(a)\sum_{t \in F_p^\times} \chi(t)\zeta^{at} = \sum_{t \in F_p^\times} \chi(at)\zeta^{at}.$$

ここで，t が $F_p^\times$ を亙るとき，$a \neq 0$ より at も $F_p^\times$ を亙る．よって，

$$\chi(a)g_a(\chi) = \sum_{t \in F_p^\times} \chi(t)\zeta^t = g_1(\chi).$$

したがって，$g_a(\chi) = \chi(a)^{-1}g_1(\chi) = \chi(a^{-1})g_1(\chi)$.

(2). $a \neq 0$ かつ $\chi = \chi_0$ のとき，

$$g_a(\chi_0) = \sum_{t \in F_p^\times} \zeta^{at} = \sum_{t=1}^{p-1} \zeta^{at} = -1 + \sum_{t=0}^{p-1} \zeta^{at} = -1 + \frac{\zeta^{ap} - 1}{\zeta^a - 1} = -1.$$

(3). $a = 0$ かつ $\chi \neq \chi_0$ のとき，指標の直交性より，

$$g_0(\chi) = \sum_{t \in F_p^\times} \chi(t) = 0.$$

(4). $a = 0$ かつ $\chi = \chi_0$ のとき，$\#F_p^\times = p - 1$ なので，

$$g_0(\chi_0) = \sum_{t \in F_p^\times} 1 = p - 1.$$

□

以降，$g_1(\chi)$ を単に $g(\chi)$ と書くことにする．

命題 3.3. $\chi \neq \chi_0$ とすると，$|g(\chi)| = \sqrt{p}$.

証明. $\sum_{a\in F_p} g_a(\chi)\overline{g_a(\chi)}$ を 2 通りの方法で計算する．

$a \neq 0$ とすると，命題 3.2 より $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$ かつ $g_a(\chi) = \chi(a^{-1})g(\chi)$. よって，$g_a(\chi)\overline{g_a(\chi)} = \chi(a)\chi(a^{-1})g(\chi)\overline{g(\chi)} = |g(\chi)|^2$. また，$g_0(\chi) = 0$ なので，

$$\sum_{a\in F_p} g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|^2.$$

一方で，ガウス和の定義より，

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in F_p^\times}\sum_{y\in F_p^\times} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}.$$

ここで，$x \neq y$ のとき $\sum_{a\in F_p}\zeta^{a(x-y)} = \frac{\zeta^{p(x-y)}-1}{\zeta^{x-y}-1} = 0$ であり，$x = y$ のとき $\sum_{a\in F_p}\zeta^{a(x-y)} = p$. よって，

$$\begin{aligned}\sum_{a\in F_p} g_a(\chi)\overline{g_a(\chi)} &= \sum_{x\in F_p^\times}\sum_{y\in F_p^\times}\chi(x)\overline{\chi(y)}\left(\sum_{a\in F_p}\zeta^{a(x-y)}\right)\\ &= p\sum_{x\in F_p^\times}\chi(x)\overline{\chi(x)} = p\sum_{x\in F_p^\times}1\\ &= p(p-1).\end{aligned}$$

ゆえに，$(p-1)|g(\chi)|^2 = p(p-1)$. $|g(\chi)| \geq 0$ なので，$|g(\chi)| = \sqrt{p}$ となる． □

系 3.4. $\chi \neq \chi_0$ とすると，$g(\chi)g(\overline{\chi}) = \chi(-1)p$.

証明. 命題 3.3 より，$g(\chi)\overline{g(\chi)} = p$. ここで，$\chi(-1) = \pm 1$ より $\overline{\chi(-1)} = \chi(-1)$ なので，

$$\overline{g(\chi)} = \sum_{t\in F_p^\times}\overline{\chi(t)}\cdot\overline{\zeta}^t = \overline{\chi(-1)}\sum_{t\in F_p^\times}\overline{\chi(-t)}\cdot\overline{\zeta}^t = \chi(-1)\sum_{t\in F_p^\times}\overline{\chi}(-t)\zeta^{-t}.$$

t が $F_p^\times$ 上を亙るとき，$-t$ も $F_p^\times$ を亙るので，

$$\overline{g(\chi)} = \chi(-1)\sum_{t\in F_p^\times}\overline{\chi}(t)\zeta^t = \chi(-1)g(\overline{\chi}).$$

よって，$\chi(-1)g(\chi)g(\overline{\chi}) = p$. $\chi(-1) = \pm 1$ なので，$g(\chi)g(\overline{\chi}) = \chi(-1)p$ である． □

次に，ガウス和と同様に重要なヤコビ和を定義し，ガウス和とヤコビ和の間に成り立つ関係について述べていく．以下では χ, λ を $F_p^\times$ 上の指標とする．

定義 3.5. χ, λ に対して，

$$J(\chi,\lambda) \overset{\text{def}}{=} \sum_{a+b=1}\chi(a)\lambda(b)$$

と定義する．ここで，a, b は $F_p^\times$ を動く．$J(\chi,\lambda)$ を**ヤコビ和**という．

ガウス和とヤコビ和には次のような関係が成り立つ．

定理 3.6. $\chi, \lambda \neq \chi_0$ とする．このとき，

(1) $J(\chi_0, \chi_0) = p - 2$.

(2) $J(\chi_0, \chi) = -1$.

(3) $J(\chi, \chi^{-1}) = -\chi(-1)$.

(4) $\chi\lambda \neq \chi_0$ のとき，

$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

証明. (1). $\{(a, b) \in (F_p^\times)^2 \mid a + b = 1\} = \{(a, 1 - a) \mid a \in F_p^\times,\ a \neq 1\}$ なので，

$$J(\chi_0, \chi_0) = \sum_{a \in F_p^\times \setminus \{1\}} \chi_0(a)\chi_0(1 - a) = \sum_{a \in F_p^\times \setminus \{1\}} 1 = p - 2.$$

(2). 指標の直交性より，

$$J(\chi_0, \chi) = \sum_{a \in F_p^\times \setminus \{1\}} \chi(a) = -\chi(1) + \sum_{a \in F_p^\times} \chi(a) = -1.$$

(3).

$$J(\chi, \chi^{-1}) = \sum_{a \in F_p^\times \setminus \{1\}} \chi(a)\chi^{-1}(1 - a) = \sum_{a \in F_p^\times \setminus \{1\}} \chi(a(1 - a)^{-1}).$$

$c = a(1 - a)^{-1}$ とおくと，$c \neq -1$ のとき $a = c(1 + c)^{-1}$. よって，a が $F_p^\times \setminus \{1\}$ を亙るとき，$a(1 - a)^{-1}$ は $F_p^\times \setminus \{-1\}$ を亙る．よって，指標の直交性より，

$$J(\chi, \chi^{-1}) = \sum_{c \in F_p^\times \setminus \{-1\}} \chi(c) = -\chi(-1) + \sum_{c \in F_p^\times} \chi(c) = -\chi(-1).$$

(4). ガウス和の定義より，

$$g(\chi)g(\lambda) = \sum_{x, y \in F_p^\times} \chi(x)\lambda(y)\zeta^{x+y} = \sum_{t \in F_p} \left(\sum_{x+y=t} \chi(x)\lambda(y) \right) \zeta^t.$$

$t = 0$ のとき，指標の直交性より，

$$\sum_{x+y=0} \chi(x)\lambda(y) = \sum_{x \in F_p^\times} \chi(x)\lambda(-x) = \lambda(-1) \sum_{x \in F_p^\times} \chi\lambda(x) = 0.$$

$t \neq 0$ のとき，各 $x, y \in F_p^\times$ に対して $x = tx'$, $y = ty'$ となる $x', y' \in F_p^\times$ がただ一つ存在する．このとき，$x + y = t$ とすると，$x' + y' = 1$. よって，

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi\lambda(t)J(\chi, \lambda).$$

したがって，

$$g(\chi)g(\lambda) = \sum_{t \in F_p} \chi\lambda(t)J(\chi, \lambda)\zeta^t = J(\chi, \lambda)g(\chi\lambda).$$

よって，$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$ となる． □

系 3.7. $\chi, \lambda \neq \chi_0$ とし，$\chi\lambda \neq \chi_0$ とする．このとき，

$$|J(\chi, \lambda)| = \sqrt{p}.$$

証明. 命題 3.3 と定理 3.6 の (4) より,

$$|J(\chi,\lambda)| = \frac{|g(\chi)||g(\lambda)|}{|g(\chi\lambda)|} = \frac{\sqrt{p}\sqrt{p}}{\sqrt{p}} = \sqrt{p}.$$

□

命題 3.8. $n \in \mathbb{Z}_{>2}$, $p \equiv 1\ (n)$ とし，χ を位数 n の指標とする．このとき,

$$g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}).$$

証明. χ の位数は $n > 2$ なので，定理 3.6 より，$g(\chi)^2 = J(\chi,\chi)g(\chi^2)$.

$n = 3$ のとき，$\chi^2 = \overline{\chi}$ なので，系 3.4 より,

$$g(\chi)^3 = g(\chi)g(\overline{\chi})J(\chi,\chi) = \chi(-1)pJ(\chi,\chi).$$

$n > 3$ のとき，定理 3.6 より,

$$g(\chi)^3 = J(\chi,\chi)g(\chi^2)g(\chi) = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3).$$

よって，帰納的に,

$$g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})g(\chi^{n-1}).$$

$\chi^{n-1} = \chi^{-1} = \overline{\chi}$ なので，系 3.4 より,

$$g(\chi)^n = g(\chi)g(\overline{\chi})J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}) = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}).$$

□

系 3.9. χ を位数 3 の指標とすると，$g(\chi)^3 = pJ(\chi,\chi)$.

証明. 命題 3.8 より，$g(\chi)^3 = \chi(-1)pJ(\chi,\chi)$. ここで，$\chi$ の位数は 3 なので,

$$\chi(-1) = \chi((-1)^3) = \chi(-1)^3 = \chi^3(-1) = 1.$$

よって，$g(\chi)^3 = pJ(\chi,\chi)$. □

また，χ を位数 3 の指標とすると，$J(\chi,\chi) \in \mathbb{Z}[\omega] \coloneqq \{a + b\omega \mid a, b \in \mathbb{Z}\}$ となる．ここで，ω は 1 でない 1 の原始 3 乗根である．このとき，次が成り立つ.

命題 3.10. $p \equiv 1\ (3)$ とし，χ を位数 3 の指標とする．また，$J(\chi,\chi) = a + b\omega$, $a, b \in \mathbb{Z}$ とおく．このとき,

(1) $b \equiv 0\ (3)$.

(2) $a \equiv -1\ (3)$.

証明. ガウス和の定義より,

$$g(\chi)^3 = \left(\sum_{t\in F_p^\times} \chi(t)\zeta^t\right)^3 \equiv \sum_{t\in F_p^\times} \chi(t)^3\zeta^{3t} \quad (3).$$

χ の位数は 3 なので，任意の $t \in F_p^\times$ に対して $\chi(t)^3 = 1$. ゆえに，$(3, p) = 1$ なので,

$$g(\chi)^3 \equiv \sum_{t=1}^{p-1} \zeta^{3t} = -1 + \sum_{t=0}^{p-1} \zeta^{3t} = -1 \quad (3).$$

よって，系 3.9 より $g(\chi)^3 = pJ(\chi,\chi)$ なので，

$$pJ(\chi,\chi) \equiv a + b\omega \equiv -1 \quad (3).$$

χ を $\overline{\chi}$ に置き換えて同様に考えると，$\overline{g(\chi)} = \chi(-1)g(\overline{\chi}) = g(\overline{\chi})$ なので，

$$g(\overline{\chi})^3 = pJ(\overline{\chi},\overline{\chi}) \equiv a + b\overline{\omega} \equiv -1 \quad (3).$$

二つの式の差をとると，$b(\omega - \overline{\omega}) \equiv 0\ (3)$. よって，$b\sqrt{-3} \equiv 0\ (3)$. 両辺を 2 乗すると，$-3b^2 \equiv 0\ (9)$. ゆえに，$9 \mid -3b^2$ なので，$3 \mid b$. また，$a + b\omega \equiv -1\ (3)$ なので，$a \equiv -1\ (3)$. □

3.2 平方剰余の相互法則 [只信伊織]

p を素数とするとき，$\left(\frac{-}{p}\right)$ をルジャンドル記号として $\chi_p(n + p\mathbb{Z}) \coloneqq \left(\frac{n}{p}\right)$ と定義すれば，χ_p は $F_p^\times$ 上の指標である．この χ_p のガウス和によって，素数の間の関係を記述する平方剰余の相互法則を示すことができる．まずは，ルジャンドル記号に対して成り立つ命題を証明する．以下では p を奇素数とする．

命題 3.11. $a \in \mathbb{Z}$ とすると，

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \quad (p).$$

証明. $p \mid a$ のとき，$\left(\frac{0}{p}\right) = 0$ なので上の式は成り立つ．

$p \nmid a$ とする．このとき，フェルマーの小定理より $a^{p-1} \equiv 1\ (p)$. よって，

$$(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) = a^{p-1} - 1 \equiv 0 \quad (p).$$

ゆえに，$a^{\frac{p-1}{2}} \equiv \pm 1\ (p)$.

一方で，$x^2 \equiv a\ (p)$ を満たす $x \in \mathbb{Z}$ が存在すれば，$p \nmid x$. よって，$A = a + p\mathbb{Z}$ とおくと，

$$\exists x \in \mathbb{Z} \text{ s.t. } x^2 \equiv a \quad (p) \iff \exists X \in F_p^\times \text{ s.t. } X^2 = A.$$

Γ を $F_p^\times$ の生成元とすると，上の条件は，ある $n \in \mathbb{Z}$ が存在して $\Gamma^{2n} = A$ を満たすことと同値．このとき，

$$A^{\frac{p-1}{2}} = \Gamma^{n(p-1)} = 1.$$

逆に，$A^{\frac{p-1}{2}} = 1$ が成り立つとするとき，$A = \Gamma^a$, $0 \le a \le p-2$ とすると，$\Gamma^{\frac{a(p-1)}{2}} = 1$. よって，$p-1 \mid \frac{a(p-1)}{2}$. $0 \le a \le p-2$ より $p-1 \nmid a$ なので，これは $2 \mid a$ と同値である．ゆえに，$\left(\frac{a}{p}\right) = 1$ と $a^{\frac{p-1}{2}} \equiv 1\ (p)$ は同値である．したがって，

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \quad (p).$$

□

先の命題で $a = -1$ とすると，$(-1)^{\frac{p-1}{2}}$ と $\left(\frac{-1}{p}\right)$ はともに ± 1 しか取り得ないので，次の系が成り立つ．

系 3.12.

$$(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right).$$

この系と $\chi_p = \left(\frac{-}{p}\right)$ のガウス和によって，次の平方剰余の相互法則を証明することができる．
ここで，一般の環 R において，$\alpha, \beta, \gamma \in R$ に対し，

$$\alpha \equiv \beta \quad (\gamma) \overset{\text{def}}{\iff} \gamma \mid (\alpha - \beta) \overset{\text{def}}{\iff} \exists \delta \in R \text{ s.t. } \alpha - \beta = \delta\gamma.$$

と定義する．これは同値関係である．

定理 3.13. p, q を相異なる奇素数とする．このとき，

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

証明. $p^* = (-1)^{\frac{p-1}{2}} p$ とおく．$g(\chi_p)^q$ を 2 通りの方法で計算することで証明する．
χ_p は実数値しか取り得ないので，$\overline{\chi_p} = \chi_p$. よって，系 3.4 と系 3.12 より，

$$g(\chi_p)^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p = p^*.$$

両辺を $\frac{q-1}{2}$ 乗すると，命題 3.11 より，

$$g(\chi_p)^{q-1} = (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \quad (q).$$

よって，

$$g(\chi_p)^q \equiv \left(\frac{p^*}{q}\right) g(\chi_p) \quad (q).$$

一方で，ガウス和の定義より，

$$\begin{aligned} g(\chi_p)^q &= \left(\sum_{t \in F_p^\times} \left(\frac{t}{p}\right) \zeta^t\right)^q \\ &\equiv \sum_{t \in F_p^\times} \left(\frac{t}{p}\right)^q \zeta^{qt} = \sum_{t \in F_p^\times} \left(\frac{t}{p}\right) \zeta^{qt} = g_q(\chi_p) \quad (q). \end{aligned}$$

命題 3.2 より，$g_q(\chi_p) = \left(\frac{q^{-1}}{p}\right) g(\chi_p) = \left(\frac{q}{p}\right) g(\chi_p)$ なので，

$$g(\chi_p)^q \equiv \left(\frac{q}{p}\right) g(\chi_p) \quad (q).$$

したがって，2 通りの方法で計算することができたので，

$$\left(\frac{q}{p}\right) g(\chi_p) \equiv \left(\frac{p^*}{q}\right) g(\chi_p) \quad (q).$$

両辺に $g(\chi_p)$ をかけると，$g(\chi_p)^2 = p^*$ なので，

$$\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \quad (q).$$

$(p^*, q) = 1$ なので，

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \quad (q).$$

両辺とも ± 1 しか取り得ないので,

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

ここで，$p^* = (-1)^{\frac{p-1}{2}}$ を戻せば,

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

したがって,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

3.3　3次剰余指標　[沼田要]

$D := \mathbb{Z}[\omega] := \{s+t\omega \mid s,t\in\mathbb{Z}\}$　$(\omega\in\mathbb{C},\ \omega^3=1,\ \omega\neq 1)$

とする。このとき、Dは環である。

また、$\alpha\in D$のノルム$N\alpha$を

$N\alpha := \alpha\bar{\alpha}$　($\bar{\alpha}$: αと共役な複素数)

で定める。

Prop 3.14

> $\alpha\in D$が単元$\Leftrightarrow N\alpha=1$
>
> また, D上の単元は$\pm 1, \pm\omega, \pm\omega^2$

(proof) ($\Rightarrow$) $\alpha\in D$：単元とする。

このとき、$\exists\beta\in D$ s.t. $\alpha\beta=1$

両辺のノルムを考えると,

$N(\alpha\beta)=N(1)$

$N(\alpha\beta)=\alpha\beta\cdot\overline{\alpha\beta}=\alpha\bar{\alpha}\cdot\beta\bar{\beta}=N\alpha\cdot N\beta$

$N(1)=1$

$\therefore N\alpha\cdot N\beta=1$

$N\alpha, N\beta\in\mathbb{N}$なので、$N\alpha=1$　//

($\Leftarrow$) $\alpha\in D$について、$N\alpha=1$とする。

このとき、$\alpha\bar{\alpha}=1$　$\therefore$ α：単元　//

さて、$\alpha=a+b\omega\in D$、$(a,b\in\mathbb{Z})$を単元とする。

$N\alpha=\alpha\bar{\alpha}=1$なので、

$a^2-ab+b^2=1$　$\therefore (2a-b)^2+3b^2=4$

このとき、$a,b\in\mathbb{Z}$の値の可能性として、

(i) $2a-b=\pm 1$, $b=\pm 1$

(ii) $2a-b=\pm 2$, $b=0$

(i)で$b=1\Rightarrow a=1$ or $0\Rightarrow\alpha=1+\omega(=-\omega^2)$ or ω

$b=-1\Rightarrow a=0$ or $-1\Rightarrow\alpha=-\omega$ or $-(1+\omega)(=\omega^2)$

(ii)で$b=0\Rightarrow a=1$ or $-1\Rightarrow\alpha=1$ or -1

さらに、これらの値は単元としての条件を満たす。

よって、D上の単元は ± 1、$\pm\omega$、$\pm\omega^2$ □

Prop 3.15

$\pi \in D$：素元とする。

このとき、$\exists p \in \mathbb{Z}$：素数 s.t. $N\pi = p$ or p^2

また、$N\pi = p \Rightarrow \forall q \in \mathbb{Z}$：素数 s.t. $\pi \nsim q$

$N\pi = p^2 \Rightarrow \pi \sim p$

(proof) $N\pi = n > 1$ とすると、$\pi\bar{\pi} = n$

このとき、$\exists p \in \mathbb{Z}$：素数 s.t. $\pi \mid p$

$p = \pi\gamma$ $(\gamma \in D)$ とすると、

$N\pi \cdot N\gamma = Np = p^2$

このとき、「$N\pi = p$ かつ $N\gamma = p$」——(i)

または「$N\pi = p^2$ かつ $N\gamma = 1$」——(ii)

(i) $\pi = u q$ (u：単元、$q \in \mathbb{Z}$：素数) とすると、

$p = N\pi = Nu \cdot Nq = q^2$ これは $p, q \in \mathbb{Z}$：素数 に矛盾

$\therefore \forall q \in \mathbb{Z}$：素数 s.t. $\pi \nsim q$

(ii) γ：単元なので、$\pi \sim p$ □

Prop 3.16

$\pi \in D$ s.t. $N\pi = p$ $(p \in \mathbb{Z}$：素数) とする。

このとき、πはD上素元となる。

(proof) $\pi \in D$を素元でないとする。

このとき、$\exists \rho, \gamma \in D$ s.t. $\pi = \rho\gamma$、$N\rho, N\gamma > 1$

そのとき、$p = N\pi = N\rho \cdot N\gamma$. これは $p \in \mathbb{Z}$：素数に矛盾 $\therefore \pi$：D上素元 □

Prop 3.17

$p \in \mathbb{Z}$：素数について、

(i) $p \equiv 1 \pmod 3 \Rightarrow \exists \pi \in D$：素元 s.t. $p = \pi\bar{\pi}$

(ii) $p \equiv 2 \pmod 3 \Rightarrow p$は$D$上素元

また、$3 = -\omega^2(1-\omega)^2$であり、$1-\omega$は$D$上素元

(proof) $p \in D$：素元でないとする。

このとき、$\exists \pi, \gamma \in D$ s.t. $p=\pi\gamma$　　$N\pi, N\gamma > 1$

$\therefore p^2 = N\pi \cdot N\gamma$　$\therefore N\pi = p$

$\pi = a+b\omega$ $(a,b\in\mathbb{Z})$ として、ノルムを考えると、

$p = a^2-ab+b^2$　　$\therefore 4p = (2a-b)^2 + 3b^2$

$\therefore p \equiv (2a-b)^2$ (3)

$3 \nmid p \Rightarrow p \equiv 1$ (3)

$k\in\mathbb{Z}$ に対し、

$(3k+1)^2 = 3(3k^2+3k)+1 \equiv 1$ (3)

$(3k+2)^2 = 3(3k^2+4k+1)+1 \equiv 1$ (3)

$\therefore$「$p\in D$:素元でない」かつ「$3\nmid p$」$\Rightarrow p \equiv 1$ (3)

これの対偶を考えると、

$p \not\equiv 1$ (3) $\Rightarrow$「$p\in D$:素元」または「$3 \mid p$」

さらに $p\equiv 2$ (3) $\Rightarrow p \not\equiv 1$ (3) を合わせて考えると、

$p \equiv 2$ (3) $\Rightarrow p \in D$:素元　　これより (ii) は OK //

$p \equiv 1$ (3) とする。このとき、平方剰余の相互法則より、

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}$$

$$= \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$\therefore \exists a\in\mathbb{Z}$ s.t. $a^2 \equiv -3$ (p)

$\therefore \exists b\in\mathbb{Z}$ s.t. $pb = a^2+3$

$\therefore p \mid (a^2+3) = (a+\sqrt{-3})(a-\sqrt{-3})$

$= (a+1+2\omega)(a-1-2\omega)$

p:素元とすると、$p \mid (a+1+2\omega)$ or $p \mid (a-1-2\omega)$

$p \mid (a+1+2\omega)$ とすると、

$\exists c+d\omega \in D$ s.t. $p(c+d\omega) = a+1+2\omega$

$\therefore pd = 2$　　しかし、$p\equiv 1$ (3) より $p \neq 2$、$d = \frac{2}{p} \notin \mathbb{Z}$

$p \mid (a-1-2\omega)$ としても同様の結論が得られる。

従って、p は D 上素元でない。

$\therefore \exists \pi, \gamma \in D$ s.t. $p=\pi\gamma$、$N\pi > 1$、$N\gamma > 1$

ノルムを考えると、$p^2 = Np = N\pi \cdot N\gamma$　　$\therefore p = N\pi = \pi\overline{\pi}$

また、Prop 3.16 より $\pi \in D$ は素元　　よって (i) は OK //

$x^3-1=(x-1)(x-\omega)(x-\omega^2)$であり、

$x^2+x+1=(x-\omega)(x-\omega^2)$である。

ここで$x=1$を代入すると、

$$3=(1-\omega)(1-\omega^2)=(1+\omega)(1-\omega)^2$$
$$=-\omega^2(1-\omega)^2$$

$\therefore q=N(1-\omega)^2$　　$\therefore 3=N(1-\omega)$　　Prop3.16より　$1-\omega$はD上素元　□

以上より、次の命題が得られる。

Prop3.18

$\pi\in D$が素元

$\Leftrightarrow$ (1) (2) (3) のいずれかを満たす

(1) $\exists p\in\mathbb{Z}$:素数、$p\equiv 1$ (3) s.t. $p=\pi\overline{\pi}$

(2) $\exists p\in\mathbb{Z}$:素数、$p\equiv 2$ (3) s.t. $\pi\sim p$

(3) $\pi\sim 1-\omega$

$\pi\in D$:素元とする。

ここで、剰余環 $D/\pi D:=\{\alpha+\pi D\mid\alpha\in D\}$ について考える。

Prop 3.19

$\pi\in D$:素元とする。

このとき $D/\pi D$ は位数 $N\pi$ の有限体である。

(proof) claim 1　$D/\pi D$は体

$\alpha\in D$ s.t. $\alpha\not\equiv 0\ (\pi)$とする。

このとき、$\exists\beta,\gamma\in D$ s.t. $\beta\alpha+\gamma\pi=1$

$\therefore\beta\alpha=1\ \ (\pi)$

$\therefore(\alpha+\pi D)(\beta+\pi D)=\alpha\beta+\pi D=1+\pi D$

$\therefore\alpha+\pi D$は$D/\pi D$上の単元

claim2　$D/\pi D$は位数$N\pi$

Prop3.18で場合分けをする。

subclaim1　$p\equiv 1$ (3):$\mathbb{Z}$上素数で、$\pi\overline{\pi}=N\pi=p$とする。このとき、$\{0,1,\cdots,p-1\}$が完全代表系となる。

要素は$N\pi=p$個となる。

$\pi=a+b\omega$ $(a,b\in\mathbb{Z})$とする。このとき、$p=a^2-ab+b^2$より$p\nmid b$

$(p \mid b$ とすると、$0 \equiv a^2 \ (p)$ $\therefore p \mid a^2$、p:素数より $p \mid a$ $\therefore p \mid \pi$ これは π:素元(既約元)に矛盾$)$

$\mu = m + n\omega \ (m, n \in \mathbb{Z})$ とすると、

$\exists c \in \mathbb{Z}$ s.t. $cb \equiv n \ (p)$ $(\because (b, p) = 1 \mid n)$

そのとき、$\mu - c\pi = m + n\omega - c(a + b\omega)$

$= m - ca + (n - cb)\omega$

$\equiv m - ca \ (p)$

$\therefore \mu \equiv m - ca \ (\pi)$ $(\because \pi \mid p)$ $\therefore \forall \mu \in D \ \exists l \in \mathbb{Z}$ s.t. $\mu \equiv l \ (\pi)$

$l = sp + r \ (s, r \in \mathbb{Z}, \ 0 \leq r < p)$ とする。

このとき、$l \equiv r \ (p)$ で、さらに $l \equiv r \ (\pi)$

よって、$\forall \mu \in D \ \exists v \in \{0, 1, \cdots, p-1\}$ s.t. $\mu \equiv v \ (\pi)$

また、$v \equiv v' \ (\pi)$ $(v, v' \in \mathbb{Z}, \ 0 \leq v, v' < p)$ のとき、

$\exists \gamma \in D$ s.t. $v - v' = \pi\gamma$ であり、 $(v - v')^2 = pN\gamma$

$\therefore p \mid v - v'$ $\therefore v = v'$ //

subclaim2 $\pi = q \equiv 2 \ (3)$、$q \in \mathbb{Z}$:素数とする。このとき、$\{a + b\omega \mid 0 \leq a, b < q\}$ が完全代表系となる。要素は $N\pi = q^2$ 個となる。

$\mu = m + n\omega \in D \ (m = qs + a, \ n = qt + b, \ s, t, a, b \in \mathbb{Z}, \ 0 \leq a, b < q)$ とする。

このとき、$\mu = (qs + a) + (qt + b)\omega$

$\equiv a + b\omega \ (q)$

次に $a + b\omega \equiv a' + b'\omega \ (q)$ $(0 \leq a, b, a', b' < q)$ とする。

そのとき $(a - a') + (b - b')\omega \equiv 0 \ (q)$

$\therefore \frac{a - a'}{q} + \frac{b - b'}{q}\omega \in D$ $\therefore \frac{a - a'}{q} \in \mathbb{Z}$、$\frac{b - b'}{q} \in \mathbb{Z}$

$0 \leq a, b < q$ より $\frac{a - a'}{q}, \frac{b - b'}{q} \in \mathbb{Z} \Leftrightarrow a = a', \ b = b'$ //

subclaim3 $\pi = 1 - \omega$ のとき、$\{-1, 0, 1\}$ が完全代表系とする。要素は $N\pi = 3$ 個となる。

$\mu = m + n\omega \ (m, n \in \mathbb{Z})$ とする。

このとき、$\mu + n(1 - \omega) = m + n\omega + n - n\omega = m + n$

よって、$\mu + n(1 - \omega) \equiv m + n \ (1 - \omega)$ $\therefore \mu \equiv m + n \ (1 - \omega)$

従って、$\forall \mu \in D \ \exists l \in \mathbb{Z}$ s.t. $\mu \equiv l \ (1 - \omega)$

$l = 3s + r \ (s, r \in \mathbb{Z}, \ 0 \leq r < 2)$ とする。

このとき、$l \equiv r \ (3)$ なので、$l \equiv r \ (1 - \omega)$ となる。 $(\because -\omega^2(1 - \omega)^2 = 3)$

$\therefore \forall \mu \in D \ \exists r \in \{-1, 0, 1\}$ s.t. $\mu \equiv r \ (1-\omega)$

次に $r \equiv r' \ (1-\omega)$ $(r, r' \in \mathbb{Z}, 0 \leq r, r' < 3)$ のとき、

$\exists \gamma \in D$ s.t. $r - r' = (1-\omega)\gamma$ であり、 $(r-r')^2 = 3N\gamma$

$\therefore 3 \mid (r-r') \quad \therefore r = r'$ □

このPropから $D/\pi D$ の乗法群 $(D/\pi D)^\times$ は位数 $N\pi - 1$ の巡回群になることがわかる。

これより、$\alpha \in D$ に対し、$\pi \nmid \alpha$ とすると、 $\alpha^{N\alpha - 1} \equiv 1 \ (\pi)$ となる。

以降、$F = D/\pi D$ 、 $F^\times = (D/\pi D)^\times$ $\pi \in D$:素元 s.t. $N\pi \neq 3$ とする。

このとき、$1 + \pi D$、$\omega + \pi D$、$\omega^2 + \pi D \in F$ は相異なる。

(∵) $1 + \pi D = \omega + \pi D$ を仮定すると、

$1 \equiv \omega \ (\pi)$ であり、$\pi \mid (1-\omega)$ また、$1-\omega$:素元なので、$\pi \sim 1-\omega$ よって $N\pi = N(1-\omega) = 3$ 矛盾,

$1 + \pi D = \omega + \pi D$ を仮定すると、$1 - \omega^2 \ (\pi)$ であり、$\pi \mid (1-\omega^2) = (1+\omega)(1-\omega)$

π:素元なので、$\pi \mid (1-\omega)$ or $\pi \mid (1+\omega)$

$\pi \mid (1-\omega) \Rightarrow N\pi = 3$ となり矛盾, $\pi \mid (1+\omega) \Rightarrow \pi$:単元となり矛盾,

$\omega + \pi D = \omega^2 + \pi D$ を仮定すると、$\omega \equiv \omega^2 \ (\pi)$ であり、$\pi \mid (\omega - \omega^2) = \omega(1-\omega)(1+\omega)$

π:素元なので、$\pi \mid \omega$ or $\pi \mid (1-\omega)$ or $\pi \mid (1+\omega)$

$\pi \mid (1-\omega) \Rightarrow N\pi = 3$ となり矛盾, $\pi \mid \omega$ or $\pi \mid (1+\omega) \Rightarrow \pi$:単元となり矛盾 //

よって、$\{1 + \pi D, \omega + \pi D, \omega^2 + \pi D\}$ は位数3で $F^\times$ の部分群なので、ラグランジュの定理より $3 \mid (N\pi - 1)$

Prop 3.20

$\alpha \in D$, $\pi \nmid \alpha$ とする。このとき、$\exists! m \in \{0, 1, 2\}$ s.t. $\alpha^{\frac{N\pi - 1}{3}} \equiv \omega^m \ (\pi)$

(proof) $\pi \mid (\alpha^{N\pi - 1} - 1) = (\alpha^{\frac{N\pi-1}{3}} - 1)(\alpha^{\frac{N\pi-1}{3}} - \omega)(\alpha^{\frac{N\pi-1}{3}} - \omega^2)$

π:素元なので、$\exists m \in \{0, 1, 2\}$ s.t. $\pi \mid (\alpha^{\frac{N\pi-1}{3}} - \omega^m)$, $\pi \mid (\alpha^{\frac{N\pi-1}{3}} - \omega^m)$

また、$m, n \in \{0, 1, 2\}$ s.t. $\pi \mid (\alpha^{\frac{N\pi-1}{3}} - \omega^m)$, $\pi \mid (\alpha^{\frac{N\pi-1}{3}} - \omega^n)$ とすると、$\pi \mid (\alpha^{\frac{N\pi-1}{3}} - \omega^m) - (\alpha^{\frac{N\pi-1}{3}} - \omega^n) = (\omega^n - \omega^m)$

$\therefore \omega^n \equiv \omega^m \ (\pi) \quad \therefore \omega^n = \omega^m$ □

これにより、3次剰余指標の定義ができる。

Def 3.21

$\chi_\pi : F^\times \to \{1, \omega, \omega^2\}$ において、$\alpha + \pi D \in F^\times$ に対し、

$\chi_\pi(\alpha + \pi D) = \alpha^{\frac{N\pi - 1}{3}} \ (\pi)$

となるものを π を法とする3次剰余指標という。

Rem $\alpha \in D$ に対し、

$$\chi_\pi(\alpha) = \begin{cases} \chi_\pi(\alpha + \pi D) & (\pi \nmid \alpha) \\ 0 & (\pi \mid \alpha) \end{cases}$$

に拡張可能である。以降、$\chi_\pi : D \to \{0, 1, \omega, \omega^2\}$ とする。

Prop3.22

$\alpha \in D$, $\pi \nmid \alpha$ とする。このとき、$\chi_\pi(\alpha) = 1 \Leftrightarrow x^3 \equiv \alpha \ (\pi)$ が D 上で解をもつ

(proof) $\pi \nmid \alpha$ より、$A := \alpha + \pi D \neq 0 + \pi D$

また、解をもつとき $x \not\equiv 0 \ (\pi)$ となるので、

$\exists x \in D$ s.t. $x^3 \equiv \alpha \ (\pi) \Leftrightarrow \exists x \in D,\ x \not\equiv 0 \ (\pi)$ s.t. $x^3 \equiv \alpha \ (\pi)$

$\Leftrightarrow \exists X \in F^\times$ s.t. $X^3 = A$ ——(*)

また、$F^\times$ は位数 $N\pi - 1$ の巡回群なので、$F^\times$ の生成元を $\Gamma \in F^\times$ とする。また $A = \Gamma^a$ $(a \in \mathbb{Z})$ とおくと、

$(*) \Leftrightarrow \exists n \in \mathbb{Z}$ s.t. $\Gamma^{3n} = \Gamma^a \Leftrightarrow \exists n \in \mathbb{Z}$ s.t. $A^{\frac{N\pi-1}{3}} = (\Gamma^a)^{\frac{N\pi-1}{3}} = (\Gamma^{3n})^{\frac{N\pi-1}{3}} = \Gamma^{n(N\pi-1)} = 1$

$\Leftrightarrow \alpha^{\frac{N\pi-1}{3}} \equiv 1 \ (\pi) \Leftrightarrow \chi_\pi(\alpha) = 1$ □

Prop3.23

$\alpha \in D$ とする。このとき $\overline{\chi_\pi(\alpha)} = \chi_{\bar\pi}(\bar\alpha) = \chi_\pi(\alpha)^2$

(proof) claim1 $\overline{\chi_\pi(\alpha)} = \chi_{\bar\pi}(\bar\alpha)$

$\alpha^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\alpha) \ (\pi)$ より、$\exists \beta \in D$ s.t. $\pi\beta = \alpha^{\frac{N\pi-1}{3}} - \chi_\pi(\alpha)$ よって $\bar\pi\bar\beta = \bar\alpha^{\frac{N\pi-1}{3}} - \overline{\chi_\pi(\alpha)}$

$\therefore \bar\alpha^{\frac{N\pi-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \ (\bar\pi)$ また、$N\pi = N\bar\pi$ なので、

$\chi_{\bar\pi}(\bar\alpha) = \bar\alpha^{\frac{N\bar\pi-1}{3}} = \bar\alpha^{\frac{N\pi-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \ (\bar\pi)$ //

claim2 $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2$

$\chi_\pi(\alpha) = 0$ or 1 or ω or ω^2 であり、$\bar 0 = 0^2$, $\bar 1 = 1^2$, $\bar\omega = \omega^2$, $\bar{\omega^2} = \omega = \omega^4 = (\omega^2)^2$ なので、

$\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2$ □

ex $q \equiv 2 \ (3)$: $\mathbb{Z}$ 上素数、$n \in \mathbb{Z}$ s.t. n と q は互いに素 とする。

このとき、$\bar n = n$, $\bar q = q$ なので、Prop3.23 より $\chi_q(n) = \chi_{\bar q}(\bar n) = \chi_q(n)^2$

$\therefore \chi_q(n)(1 - \chi_q(n)) = 0$

q と n は互いに素で $\chi_q(n) \neq 0$ なので $\chi_q(n) = 1$

よって、Prop3.22 より $x^3 \equiv n \ (q)$ は D 上で常に解をもつ。

3.4　3 次剰余の相互法則 [只信伊織]

まず，3 次剰余の相互法則を定式化するために必要な概念である primary を定義する．以下では $D = \mathbb{Z}[\omega]$ とおき，$\pi \in D$ は素元，$p, q \in \mathbb{Z}$ はそれぞれ $p \equiv 1\ (3)$, $q \equiv 2\ (3)$ となる素数とする．

定義 3.24. π が $\pi \equiv 2\ (3)$ を満たすとき，π は **primary** であるという．

$q \equiv 2\ (3)$ なので，q は D の primary な素元である．また，素元 $\pi = a + b\omega \in D$ が primary であることは，$a \equiv 2\ (3)$, $b \equiv 0\ (3)$ と同値である．さらに，$\pi = a + b\omega$ が primary であるとき，$\overline{\pi} = a + b\overline{\omega} = (a - b) - b\omega$. このとき，$a - b \equiv 2\ (3)$, $-b \equiv 0\ (3)$ なので，$\overline{\pi}$ も primary である．

命題 3.25. $N\pi = p$ とする．このとき，π と同伴な元の中で primary なものはただ一つである．

証明. $\pi = a + b\omega$, $a, b \in \mathbb{Z}$ とする．π と同伴な元は $\pi, \omega\pi, \omega^2\pi, -\pi, -\omega\pi, -\omega^2\pi$ である．よって，a, b でこれらの元を表すと，

(1) $a + b\omega$.
(2) $-b + (a - b)\omega$.
(3) $(b - a) - a\omega$.
(4) $-a - b\omega$.
(5) $b + (b - a)\omega$.
(6) $(a - b) + a\omega$.

$N\pi = p = a^2 - ab + b^2$ なので，$3 \mid a$ かつ $3 \mid b$ とすると $p \equiv 0\ (3)$ となり矛盾．よって，$3 \nmid a$ または $3 \nmid b$. 必要なら (1) と (2) を置き換えることによって $3 \nmid a$ としてよい．さらに，(1) と (4) を置き換えることによって $a \equiv 2\ (3)$ としてよい．このとき，$p = a^2 - ab + b^2$ より $1 \equiv 4 - 2b + b^2\ (3)$. よって，$b(b - 2) \equiv 0\ (3)$ なので，$b \equiv 0, 2\ (3)$. $b \equiv 0\ (3)$ であれば $a + b\omega$ が primary であり，$b \equiv 2\ (3)$ であれば $b + (b - a)\omega$ が primary なので，存在が示された．

一意性を示すために，$a + b\omega$ が primary であるとする．このとき，$a \equiv 2\ (3)$, $b \equiv 0\ (3)$ より $-b, b - a, -a, b \not\equiv 2\ (3)$ なので，(2)-(5) は primary でない．また，$a \not\equiv 0\ (3)$ なので，(6) も primary でない．よって，primary は一意的である．　□

これにより，primary な素元が次のように分類できる．

命題 3.26. $\pi \in D$ が primary な素元であることは，以下のどちらかが成り立つことと同値である．

(1) ある素数 $p \equiv 1\ (3)$ が存在して $N\pi = p$，かつ，$\pi \equiv 2\ (3)$.
(2) ある素数 $q \equiv 2\ (3)$ が存在して $\pi = q$.

$N\pi = p$ とすると，写像 $\varphi : \mathbb{Z}/p\mathbb{Z} \ni n + p\mathbb{Z} \mapsto n + \pi D \in D/\pi D$ によって $F_p \coloneqq \mathbb{Z}/p\mathbb{Z}$ と $F_\pi \coloneqq D/\pi D$ は同型になるので，3 次剰余指標 χ_π を位数 3 の $F_p^\times$ 上の指標とみなすことができる．よって，χ_π に対してガウス和やヤコビ和を考えることができ，同様の性質が成り立つ．

ここで，χ を位数 3 の $F_p^\times$ 上の指標とすると，系 3.7 より $J(\chi, \chi)\overline{J(\chi, \chi)} = p$. よって，命題 3.10 も踏まえると，$J(\chi, \chi)$ はノルムが p である D の primary な素元である．特に，3 次剰余指標 χ_π に対しては次が成り立つ．

補題 3.27. $N\pi = p$ かつ π は primary とする．このとき，

$$J(\chi_\pi, \chi_\pi) = \pi.$$

証明. ヤコビ和の定義より，

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &= \sum_{x \in F_\pi^\times \setminus \{1\}} \chi_\pi(x)\chi_\pi(1-x) \\ &\equiv \sum_{x \in F_\pi^\times \setminus \{1\}} x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} = \sum_{x \in F_\pi^\times} x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \quad (\pi). \end{aligned}$$

ここで $X^{\frac{p-1}{3}}(1-X)^{\frac{p-1}{3}} = \sum_{k=0}^{2(p-1)/3} a_k X^k$ とおくと，

$$J(\chi_\pi, \chi_\pi) \equiv \sum_{x \in F_\pi^\times} \sum_{k=0}^{2(p-1)/3} a_k x^k = \sum_{k=0}^{2(p-1)/3} a_k \left(\sum_{x \in F_\pi^\times} x^k \right) \quad (\pi).$$

このとき，$F_\pi^\times$ の生成元を Γ とすると，任意の $0 \leq k \leq \frac{2(p-1)}{3}$ に対して，

$$\sum_{x \in F_\pi^\times} x^k = \sum_{i=0}^{p-2} \Gamma^{ki} = \frac{\Gamma^{k(p-1)} - 1}{\Gamma^k - 1} = 0.$$

よって，$J(\chi_\pi, \chi_\pi) \equiv 0\ (\pi)$ なので，$\pi \mid J(\chi_\pi, \chi_\pi)$. 素元は既約元でもあるので，$J(\chi_\pi, \chi_\pi) \sim \pi$. primary の一意性より，$J(\chi_\pi, \chi_\pi) = \pi$. □

補題 3.27 と系 3.9 より次が成り立つ.

系 3.28. $N\pi = p$ かつ π は primary とする．このとき，

$$g(\chi_\pi)^3 = p\pi.$$

先に示した平方剰余の相互法則では，相異なる素数の間にある関係を記述することができた．これと同様に，先の 3 次剰余指標 χ_π によって D の相異なる素元の関係を記述することができる．これが次の 3 次剰余の相互法則である.

定理 3.29. $\pi_1, \pi_2 \in D$ を primary な素元とし，$N\pi_1, N\pi_2 \neq 3$ かつ $N\pi_1 \neq N\pi_2$ とする．このとき，

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

証明. 命題 3.26 に基づいて，

(1) ある素数 $q_1, q_2 \equiv 2\ (3)$ が存在して $\pi_1 = q_1,\ \pi_2 = q_2$.

(2) ある素数 $q \equiv 2\ (3),\ p \equiv 1\ (3)$ が存在して $\pi_1 = q,\ \pi_1 = \pi,\ N\pi = p$.

(3) ある素数 $p_1, p_2 \equiv 1\ (3)$ が存在して $N\pi_1 = p_1,\ N\pi_2 = p_2$.

に場合分けして考える.

(1). $\pi_1 = q_1,\ \pi_2 = q_2$ とすると，$(q_1, q_2) = 1$ なので，$\chi_{q_1}(q_2) = \chi_{q_2}(q_1) = 1$.

(2). $\pi_1 = q,\ \pi_1 = \pi,\ N\pi = p$ とする．$g(\chi_\pi)^{q^2}$ を 2 通りの方法で計算する.

まず，系 3.28 より，$g(\chi_\pi)^3 = p\pi$. 両辺を $\frac{q^2-1}{3}$ 乗すると，$g(\chi_\pi)^{q^2-1} = (p\pi)^{q^2-1}$. $Nq = q^2$ なので，3 次剰余指標の定義より，

$$g(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi) \quad (q).$$

よって，$(p,q)=1$ なので，

$$g(\chi_\pi)^{q^2} \equiv \chi_q(p)\chi_q(\pi)g(\chi_\pi) = \chi_q(\pi)g(\chi_\pi) \quad (q).$$

一方，ガウス和の定義より，

$$g(\chi_\pi)^{q^2} = \left(\sum_{t\in F_\pi^\times} \chi_\pi(t)\zeta^t\right)^{q^2} \equiv \sum_{t\in F_\pi^\times} \chi_\pi(t)^{q^2}\zeta^{q^2t} \quad (q)$$

ここで，$q^2 \equiv 1$ (3) かつ $\chi_\pi(t)$ は 1 の 3 乗根なので，

$$g(\chi_\pi)^{q^2} \equiv \sum_{t\in F_\pi^\times} \chi_\pi(t)\zeta^{q^2t} = g_{q^2}(\chi_\pi) \quad (q).$$

命題 3.2 より，$g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q)^{-2}g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$ なので，

$$g(\chi_\pi)^{q^2} \equiv \chi_\pi(q)g(\chi_\pi) \quad (q).$$

以上より，$g(\chi_\pi)^{q^2}$ を 2 通りの方法で計算できたので，

$$\chi_\pi(q)g(\chi_\pi) \equiv \chi_q(\pi)g(\chi_\pi) \quad (q).$$

両辺に $\overline{g(\chi_\pi)}$ をかけると，命題 3.3 より $g(\chi_\pi)\overline{g(\chi_\pi)} = p$ なので，

$$\chi_\pi(q)p \equiv \chi_q(\pi)p \quad (q).$$

$(p,q)=1$ なので，

$$\chi_\pi(q) \equiv \chi_q(\pi) \quad (q).$$

したがって，

$$\chi_\pi(q) = \chi_q(\pi).$$

(3). $N\pi_1 = p_1$, $N\pi_2 = p_2$ とする．このとき，$\gamma_1 = \overline{\pi_1}$, $\gamma_2 = \overline{\pi_2}$ とおくと，$p_1 = \pi_1\gamma_1$, $p_2 = \pi_2\gamma_2$ かつ γ_1, γ_2 も primary である．ここで，系 3.9 より，$g(\chi_{\gamma_1})^3 = p_1\gamma_1$. 両辺を $\frac{p_2-1}{3}$ 乗すると，

$$g(\chi_{\gamma_1})^{p_2-1} = (p_1\gamma_1)^{\frac{p_2-1}{3}} \equiv \chi_{\pi_2}(p_1\gamma_1) \quad (\pi_2).$$

よって，

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1}) \quad (\pi_2).$$

一方で，

$$\begin{aligned} g(\chi_{\gamma_1})^{p_2} &= \left(\sum_{t\in F_{\gamma_1}^\times} \chi_{\gamma_1}(t)\zeta^t\right)^{p_2} \\ &\equiv \sum_{t\in F_{\gamma_1}^\times} \chi_{\gamma_1}(t)^{p_2}\zeta^{p_2t} = \sum_{t\in F_{\gamma_1}^\times} \chi_{\gamma_1}(t)\zeta^{p_2t} = g_{p_2}(\chi_{\gamma_1}) \quad (\pi_2) \end{aligned}$$

命題 3.2 より，$g_{p_2}(\chi_{\gamma_1}) = \chi_{\gamma_1}(p_2^{-1})g(\chi_{\gamma_1}) = \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1})$ なので，

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \quad (\pi_2).$$

したがって，

$$\chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1}) \quad (\pi_2).$$

両辺に $\overline{g(\chi_{\gamma_1})}$ をかけると，命題 3.3 より，

$$\chi_{\gamma_1}(p_2^2)p_1 \equiv \chi_{\pi_2}(p_1\gamma_1)p_1 \quad (\pi_2).$$

$\pi_2 \nmid p_1$ なので，

$$\chi_{\gamma_1}(p_2^2) \equiv \chi_{\pi_2}(p_1\gamma_1) \quad (\pi_2).$$

よって，

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_2}(p_1\gamma_1). \tag{a}$$

同様に，$g(\chi_{\pi_2})^3 = p_2\pi_2$ を $\frac{p_1-1}{3}$ 乗して，mod π_1 をとると，

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2). \tag{b}$$

が得られる．また，$\gamma_1 = \overline{\pi_1}$, $\overline{p_2} = p_2$ なので，$\chi_{\gamma_1}(p_2^2) = \chi_{\overline{\pi_1}}(\overline{p_2})^2 = \chi_{\pi_1}(p_2)^4 = \chi_{\pi_1}(p_2)$. この式と (a),(b) より，

$$\begin{aligned}\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2)\\ &= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) = \chi_{\pi_1}(p_2\pi_2)\\ &= \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\gamma_1)\\ &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1).\end{aligned}$$

$\pi_2 \nmid p_1\gamma_1$ より $\chi_{\pi_2}(p_1\gamma_1) \neq 0$ なので，

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

以上より全ての場合で定理が示された． □

参考文献

[1] D.B. ザギヤー著　片山孝次訳. 数論入門. 岩波書店，1990.

[2] Kenneth Ireland, Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 1990.

[3] 藤崎源二郎，森田康夫，山本芳彦. 数論への出発. 日本評論社，2004.

[4] 雪江明彦. 整数論 3 解析的整数論への誘い. 日本評論社，2014.

[5] 杉浦光夫. 解析入門 I. 東京大学出版会，2021.