Power residueに対するdifference set について

八木　勇磨

2007年1月31日

目 次

第 1 章 Introduction **2**
1.1 序文 2
1.2 Difference set の定義 4

第 2 章 基本定理と k が 3 以上の奇数である時の k-th power residue に対する difference set **8**
2.1 基本定理 8
2.2 k が 3 以上の奇数である時の k-th power residue に対する difference set は存在しないことの証明 12

第 3 章 4th power residue に対する difference set **16**
3.1 証明の準備 1 17
3.2 証明の準備 2 20
3.3 Chowla の定理の証明 22

第 4 章 6th power residue に対する difference set **24**
4.1 証明の準備 1 24
4.2 証明の準備 2 28
4.3 Lehmer の定理の証明 35

第 5 章 8th power residue に対する difference set **37**
5.1 証明の準備 1 37
5.2 証明の準備 2 40
5.3 Lehmer の定理の証明 42

第 6 章 12th power residue に対する difference set **44**
6.1 証明の準備 1 44
6.2 証明の準備 2 48
6.3 Whiteman の定理の証明 50

第1章　Introduction

この章では、最初にこの論文の概要を説明する. 次に、difference set の定義をし、定義で使う合同方程式の解の集合の位数に対する補題を証明する. そして最後に、次の章から使う記号を定義する.

1.1　序文

この節では、この論文の概要を説明する. この論文の目的は、k が 3 以上の奇数、または 4、6、8、12 であり、a と b は位数が奇素数 p の有限体 $\mathbb{F}_p$ の元である時、$\mathbb{F}_p$ の 0 でない任意の元 g に対して、$g = a^k - b^k$ という方程式の解 (a, b) が存在して、その解 (a, b) の個数が g によらず一定であることの必要十分条件に対して、別証明を与えるということである. まず、証明したい定理を紹介する. k が 4 または、8 でない時は、否定的な結果であるので、k が 4 と 8 である時だけを紹介する. なお、記号の定義は後で行う. ちなみに、後で説明するが、$g = a^k - b^k$ という方程式の解 (a, b) が存在して、その解 (a, b) 個数が g によらず一定であることは、後で定義する H_k が difference set であることと同値である.

定理 1.1.1 (Chowla 1944). $5 < p \equiv 1\ (4)$ とする. その時、次の同値性が成り立つ.

(1) H_4 : difference set $\Leftrightarrow p = 1 + 4a^2$ $(1 < \exists a$: 奇数$)$.
(2) $H_4 \cup \{0\}$: difference set $\Leftrightarrow p = 9 + 4b^2$ $(\exists b$: 奇数$)$.

定理 1.1.2 (Lehmer 1953). $p \equiv 1\ (8)$ とする. その時、次の同値性が成り立つ.

(1) H_8 : difference set $\Leftrightarrow p = 1 + 8c^2 = 9 + 64d^2$ $(\exists c, d \in \mathbb{Z})$.
(2) $H_8 \cup \{0\}$: difference set $\Leftrightarrow p = 49 + 8e^2 = 441 + 64f^2$ $(\exists e, f \in \mathbb{Z})$.

例えば Chowla の定理の (1) で、$a = 3$ とすると、$p = 37$ となる. よって、$\mathbb{F}_{37}$ の 0 でない任意の元 g に対して、$g = a^4 - b^4$ となる方程式の解 (a, b) が存在して、その解 (a, b) の個数が g によらず一定であるということを表している. (2) で、例えば $b = 1$ とすると、$p = 13$ となる. よって、$\mathbb{F}_{13}$ の 0 でない任意の元に対して、同様のことが言える.

この論文で行うこれらの定理の証明を概説する. まず、証明するための基本となる定理を紹介する. その定理は、後で定義する高次のガウス和を用いてその必要十分条件を与えた定理である. 2 章でその定理を証明する. なお、記号の定義は後で行う.

定理 1.1.3 (Berndt, Evans 1979　基本定理). $k+1 < p \equiv 1\ (k)$ とする. その時、次の同値性が成り立つ.

(1) H_k: difference set $\Leftrightarrow \mid G_k - 1 \mid^2 = p(k-1)+1$.
(2) $H_k \cup \{0\}$: difference set $\Leftrightarrow \mid G_k + k - 1 \mid^2 = (p+k-1)(k-1)$.

この定理の G_k は高次のガウス和とよばれるものである. 後で説明するが、高次のガウス和を用いて、後で定義する S_k を表すことが出来る. $\mid S_k \mid^2$ は $\sum_{g_i, g_j \in H_k} \mathbb{e}(g_i - g_j)$ になるのだが、$g_i - g_j$ という部分が、difference set に関係する. その結果、基本定理のように高次のガウス和が difference set と関係を持つことになる. この定理の証明を概説すると、円分多項式の各項の係数が 1 であることにより、$g = a^k - b^k$ という式の解 (a, b) が存在して、その解 (a, b) の個数が g によらず一定であることを証明する. この定理より、k が 3 以上の奇数である時の k-th power residue に対する difference set が存在しないことを証明出来る. しかし、4、6、8、12 である k については、基本定理だけでは証明出来ない. k が 6、8、12 である時は、k が 4 である時と同様に証明出来るので、k が 4 である時だけを解説する. 3 章の 2 節で G_4 を計算する. その際、指標の性質を用いて、G_4 をガウス和で表すことが重要である. G_4 をガウス和で表せると、ガウス和の性質を用いることによって G_4 が計算出来る. ちなみに、高次のガウス和が difference set と関係を持つので、ガウス和も difference set と関係を持つことがわかる. そして、3 章の 3 節でその計算した G_4 と基本定理を使って、Chowla の定理を証明する. なお、この論文は主に、k が 4、6、8、12 である時の解説である. 以上がこの論文の概要である.

次に、k-th power residue に対する difference set の歴史を解説する. それを下の表にまとめた.

年	著者	k	$H_k\ (\subset \mathbb{F}_p)$	論文
1944	Chowla	2 , 4	○	[3]
1953	Lehmer	3 以上の奇数 , 6	×	[7]
1953	Lehmer	8	○	[7]
1957	Whiteman	16	×	[12]
1960	Whiteman	10	×	[13]
1960	Whiteman	12	×	[11]
1966	Muskat	14 , 22	×	[8]
1967	Baumert, Fredricksen	18	×	[1]
1970	Muskat, Whiteman	20	×	[9]
1979	Berndt, Evans	4 , 8	○	[2]
1979	Berndt, Evans	3 以上の奇数 , 6 , 12	×	[2]
1980	Evans	16	×	[4]
1983	Evans	24	×	[5]

年	著者	摘要	論文
2004	Ott	H_k がある p に対して difference set $\Rightarrow$ k が 2 のべき乗	[10]
2005	Yuan, Yahui	Ott の証明に間違いを発見	[14]

ただし、$p \equiv 1\ (k)$ であり、H_k が○とは、H_k がある p に対して $\mathbb{F}_p$ の difference set であることを表し、H_k が $\times$ とは、H_k がどの p に対しても $\mathbb{F}_p$ の difference set でないことを表している. また、次の場合は除いている.

$k = 20,\ p \equiv 21\ (40),\ 5$ が p を法として nonquartic

$k = 22,\ p \equiv 23\ (88),\ 2$ が p を法として eleventh power nonresidue

$k = 24,\ p \equiv 25\ (48),\ 2$ が p を法として noncubic, 3 が p を法として nonquartic

筆者がまとめる論文 [2] の内容は、その論文より前に証明されていた k が 3 以上の奇数、または 4、6、8、12 である時の k-th power residue に対する difference set が存在するための必要十分条件についての別証明である. ちなみに、最初の証明は円分体の理論から証明された. この別証明は、その円分体による最初の証明より短い証明である. [2] の論文の翌年には [2] と同様に、16th power residue に対する difference set は存在しないことについても別証明を与えた. そして、この別証明により、その 3 年後には、初めて 24th power residue に対する difference set は存在しないことが証明された. よって、[2] の内容は、k-th power residue に対する difference set の研究において価値がある.

さらに最近では、Ott の 2004 年の論文 [10] で、k-th power residue に対する difference set が存在するのは、k が 2 のべき乗である時であるという主張が発表された. しかし、残念ながら、Yuan と Yahui の 2005 年の論文 [14] で、Ott の証明は間違っていることが指摘された. なお、Ott の主張自体が否定されたわけではない. 以上が、k-th power residue に対する difference set の歴史の概説である.

この論文はガウス和、ヤコビ和、power residue character に関する基礎的事項の証明は省略した. それらは全て [6] を参考にした.

末筆になりましたが、この 3 年間、セミナー等で御指導して頂きました雪江明彦教授には心から感謝します. また、幾つかの助言を頂きました早坂紀彦先輩、TEX に関することで大変お世話になりました森本聡先輩にとても感謝します. そして、良き相談相手であったセミナー仲間の酒井祐貴子さん、曽根浩圭君、樋口勇気君、福井邦彦君、渡邉崇君にも感謝します.

1.2 Difference set の定義

この節では、最初に $\mathbb{F}_p$ の difference set を定義し、定義で使う合同方程式の解の集合の位数に対する補題を証明する. そして最後に、次の章から使う記号を定義する.

それでは、$\mathbb{F}_p$ の difference set を定義する.

定義 1.2.1. p を奇素数とし、$H \subseteq \mathbb{F}_p$ とする. このとき 0 でない $\mathbb{F}_p$ の任意の元 g に対して、

$$g = g_i - g_j \quad (g_i, g_j \in H) \tag{1.2.2}$$

の解が存在して、解の集合 $\{(g_i, g_j) \mid g_i, g_j \in H\}$ の位数が g によらず一定であるならば、H を $\mathbb{F}_p$ の difference set と言う.

以後、この論文では p を奇素数とする. 次に、(1.2.2) の解の集合の位数に対する補題を証明する.

補題 1.2.3. H を $\mathbb{F}_p$ の difference set とする. また、$1 < \ l \in \mathbb{N}$、$\lambda \in \mathbb{N}$ に対して、$\mid H \mid = l$ とし、(1.2.2) の解の集合の位数を λ とする. すると、次の式が成り立つ.

$$\lambda(p-1) = l(l-1).$$

証明. $p-1$ は $\mathbb{F}_p$ の 0 でない元の数である. そして、$g \neq 0$ なので、$g \equiv g_i - g_j$ と表した時、$i \neq j$ である. よって、g の表し方は、$l(l-1)$ 通りになる. ゆえに、$l(l-1)$ 通りに取ってきた $g_i - g_j$ で 0 以外の全ての g がそれぞれ λ 通りに表せるのだから、g の数 $p-1$ と λ の積が $l(l-1)$ になることがわかる. □

以後、この論文では l を H の位数とし、λ を (1.2.2) の解の集合の位数とする. また、l を 1 より大きい整数と仮定し、λ を 1 以上の整数と仮定する. この l と λ に対する仮定の理由は、この論文では空集合である difference set と 1 つの元からなる difference set を考えないからである.

次に、p を法とする k-th power residue の集合を定義する.

定義 1.2.4. $2 < k \in \mathbb{N}$ とする. その時、

$$H_k = \left\{ n^k \in \mathbb{F}_p^{\times} \mid n \in \mathbb{F}_p^{\times} \right\}$$

と定義し、この H_k を p を法とする k-th power residue の集合と言う.

以後、この論文では k を 2 より大きい整数と仮定する. この k に対する仮定の理由は、後で説明する. また、H を H_k または $H_k \cup \{0\}$ とし、H_k は空集合でないとする. なお、(1.2.2) を考える時は、H_k を $\mathbb{F}_p$ の部分集合とみなして差を考える.

ここで、H_k と difference set を理解するために、例を考える.

例 1.2.5 (difference set の例). $k = 2$, $p = 7$ とする. すると、$\mathbb{F}_7^{\times}$ の任意の元 n に対して n^2 は、$\mathbb{F}_7^{\times}$ の元で

$$1^2 = 1,\ 2^2 = 4,\ 3^2 = 2,\ 4^2 = 2,\ 5^2 = 4,\ 6^2 = 1$$

になる. よって、$H_2 = \{1, 2, 4\}$ となる. このとき、$\mathbb{F}_7$ の 0 でない任意の元 g は、H_2 の 2 つの元による差で

$$1 = 2 - 1,\ 2 = 4 - 2,\ 3 = 4 - 1,\ 4 = 1 - 4,\ 5 = 2 - 4,\ 6 = 1 - 2$$

になる. よって、g_i と g_j を H_2 の元とした時、$\mathbb{F}_7$ の 0 でない任意の元 g に対して、$g = g_i - g_j$ という式の解が存在し、解の個数が g によらず 1 個になる. その結果、H_2 は difference set である.

例 1.2.6 (difference set にならない例). $k = 2, p = 5$ とする. すると、$\mathbb{F}_5^\times$ の任意の元 n に対して n^2 は、$\mathbb{F}_5^\times$ の元で

$$1^2 = 1,\ 2^2 = 4,\ 3^2 = 4,\ 4^2 = 1$$

になる. よって、$H_2 = \{1, 4\}$ となる. このとき、$\mathbb{F}_5$ の 0 でない元 g は、H_2 の 2 つの元による差で

$$2 = 1 - 4,\ 3 = 4 - 1$$

しか表せない. よって、H_2 は difference set ではない.

ところで、H を H_k または $H_k \cup \{0\}$ とすると、(1.2.2) はそれぞれ

$$g = a^k - b^k \quad (a, b \in \mathbb{F}_p^\times)$$
$$g = a^k - b^k \quad (a, b \in \mathbb{F}_p)$$

という式に書き換えることが出来る. よって、H_k または $H_k \cup \{0\}$ が difference set であることの必要十分条件を調べることは、$\mathbb{F}_p$ の 0 でない元 g 対して、$g = a^k - b^k$ の解が存在して、解の集合 $\{(a, b)\}$ の位数が g によらず一定であることの必要十分条件を調べることと同値になる. ちなみに、e を自然対数とした時に、以後

$$\sum_{g_i, g_j \in H} e^{\frac{2\pi\sqrt{-1}(g_i - g_j)}{p}}$$

というものを考えることによって、H_k または $H_k \cup \{0\}$ が difference set であることの必要十分条件を調べる.

次に、今後使う記号を定義する.

定義 1.2.7. (1) $x \in \mathbb{Z}$ に対して、$\mathbb{e}(x)$ を次のように定義する.

$$\mathbb{e}(x) = e^{\frac{2\pi\sqrt{-1}x}{p}}.$$

(2) $\mathbb{F}_p$ 上の自明でない指標 χ に対してガウス和 $g(\chi)$ を次のように定義する.

$$g(\chi) = \sum_{n=0}^{p-1} \chi(n)\mathbb{e}(n).$$

(3) $\mathbb{F}_p$ 上の自明でない指標 χ と ψ に対してヤコビ和 $J(\chi,\psi)$ を次のように定義する.

$$J(\chi,\psi)=\sum_{n=0}^{p-1}\chi(n)\psi(1-n).$$

(4) 奇素数 p に対して i^* を次のように定義する.

$$i^*=\begin{cases} 1 & p\equiv 1\ (4),\\ \sqrt{-1} & p\equiv 3\ (4).\end{cases}$$

また、以後次の補題を使う.

補題 1.2.8. χ と ψ と $\chi\psi$ を $\mathbb{F}_p$ 上の自明でない指標とし、φ を $\mathbb{F}_p$ 上の 2 次指標とする. その時、次が成り立つ.

(1) $\mid g(\chi)\mid=\sqrt{p}$.
(2) $g(\chi)g(\bar{\chi})=\chi(-1)p$.
(3) $J(\chi,\psi)=\dfrac{g(\chi)g(\psi)}{g(\chi\psi)}$.
(4) $\mid J(\chi,\psi)\mid=\sqrt{p}$.
(5) $g(\varphi)=i^*p^{\frac{1}{2}}$.

これらの証明については、(1) が [6, Proposition 8.2.2.] で、(2) が [6, p.92] で、(3) が [6, Chapter 8 Theorem 1.(d)] で、(4) が [6, Chapter 8 Corollary.] で、(5) が [6, Chapter 6 Theorem 1.] でそれぞれ証明されている. 以後、この論文では χ を $\mathbb{F}_p$ 上の自明でない指標とする.

最後に、以後この論文では様々な記号を定義するので、様々な記号を以下の表にまとめた.

p	p.5	l、λ	p.5	k	p.5
H_k	p.5	$\mathrm{e}(x)$	p.6	i^*	p.6
χ	p.6	$g(\chi)$	p.6	$J(\chi,\psi)$	p.6
G_k	p.8	S_k	p.8	$K(\chi)$	p.17
a_4、b_4	p.17	r_4、s_4	p.20	R_i	p.20
a_3、b_3	p.24	r_3、s_3	p.28	ϵ_3	p.28
ϵ_6	p.29	ν	p.30	α	p.32
a_8、b_8	p.37	a_{12}、b_{12}	p.44		

第2章　基本定理とkが3以上の奇数である時のk-th power residueに対するdifference set

この章では、この論文の基本定理と、基本定理から導くことが出来る命題と、kが3以上の奇数である時のk-th power residueに対するdifference setは存在しないことを証明する.

2.1　基本定理

この節では、基本定理を証明する. まず、高次のガウス和G_kを定義する.

定義 2.1.1. $2 < k \in \mathbb{N}$とする. その時、

$$G_k = \sum_{n=0}^{p-1} \mathfrak{e}(n^k)$$

と定義し、このG_kをk次のガウス和と言う.

すると、次の定理が成り立つ.

定理 2.1.2 (Berndt, Evans 1979　基本定理). $2 < k \in \mathbb{N}$に対して、$k+1 < p \equiv 1\ (k)$とする. その時、次の同値性が成り立つ.

(1) H_k: difference set $\Leftrightarrow \mid G_k - 1 \mid^2 = p(k-1)+1$.
(2) $H_k \cup \{0\}$: difference set $\Leftrightarrow \mid G_k + k - 1 \mid^2 = (p+k-1)(k-1)$.

この定理ではpが$k+1$より大きいという条件があるが、それについては後で説明する. それでは、この定理を証明するための準備をする.

定義 2.1.3. $2 < k \in \mathbb{N}$とする. その時、

$$S_k = \sum_{t \in H_k} \mathfrak{e}(t)$$

と定義する.

後で説明するが、G_k をこの S_k で表すことが出来る. それを示すには次の補題を使う.

補題 2.1.4. $(t,p)=1$ とし、ある t に対して $n^k \equiv t\ (p)$ となる n が存在するとする. その時、n の個数は t によらず $(k,p-1)$ になる.

この補題は、${\mathbb{F}_p}^\times$ が巡回群になることより証明出来るのだが、ここでは詳細を省略する. なお、定理 2.1.2 では $p \equiv 1\ (k)$ であるとしていたので、k は $p-1$ を割り切り、

$$(k,p-1)=k$$

となる. この結果 G_k は、n が 0 である時に $\mathbb{e}(n^k)=1$ であることと、n が 0 でない時に S_k の定義より、

$$G_k = kS_k + 1$$

となる. この式は、

$$S_k = \frac{G_k - 1}{k} \tag{2.1.5}$$

と書き換えることが出来る. ゆえに、$|\ G_k - 1\ |^2$ の代わりに $|\ S_k\ |^2$ を、$|\ G_k + k - 1\ |^2$ の代わりに $|\ S_k + 1\ |^2$ を考えることによって定理 2.1.2 を証明する.

また、$|\ S_k\ |^2$ と $|\ S_k + 1\ |^2$ は定義より

$$|\ S_k\ |^2 = S_k\bar{S}_k = \sum_{g_i,g_j \in H_k} \mathbb{e}(g_i - g_j)$$

$$|\ S_k + 1\ |^2 = (S_k+1)(\bar{S}_k+1) = \sum_{g_i,g_j \in H_k \cup \{0\}} \mathbb{e}(g_i - g_j)$$

になる. よって、H_k と $H_k \cup \{0\}$ が difference set になることの必要十分条件を調べる時に、$|\ S_k\ |^2$ と $|\ S_k + 1\ |^2$ をそれぞれ考える理由は、(1.2.2) を

$$\mathbb{e}(g) = \mathbb{e}(g_i - g_j)\ (g_i, g_j \in H)$$

という式に書き換えることが出来るからである. それでは、定理 2.1.2 の証明をする.

定理 2.1.2 の証明. まず (1) を証明する. ここで、difference set の定義と補題 2.1.4 より、$p-1=kl$ となることがわかる. よって、

$$l = \frac{p-1}{k} \tag{2.1.6}$$

となる.

($\Rightarrow$) 仮定より、補題 1.2.3 が成り立つ. よって、補題 1.2.3 と (2.1.6) より、

$$\lambda = \frac{p-1-k}{k^2} \tag{2.1.7}$$

となる. 次に、$|\ S_k\ |^2$ を考える. g_i と g_j が等しければ $\mathbb{e}(g_i - g_j) = 1$ となり、g_i と g_j が等しくなる個数は l である. また、g_i と g_j が等しくない時は $n \equiv g_i - g_j$ となる (g_i, g_j) の個数が λ である. よって、$|\ S_k\ |^2$ は

$$|\ S_k\ |^2 = l + \lambda \sum_{n=1}^{p-1} \mathbb{e}(n)$$

になることがわかる. この式の右辺は、$\sum_{n=1}^{p-1} \mathbb{e}(n) = -1$ になることと、(2.1.6) と (2.1.7) より、

$$l - \lambda = \frac{p(k-1)+1}{k^2}$$

になる. その結果、(2.1.5) より求めたい式が得られる.

($\Leftarrow$) まず $|\ S_k\ |^2$ を考えると、S_k の定義と (2.1.5) と仮定より、

$$|\ S_k\ |^2 = \sum_{g_i, g_j \in H_k} \mathbb{e}(g_i - g_j) = \frac{p(k-1)+1}{k^2}$$

となる. この式の右辺を左辺に移項すると、

$$\sum_{g_i, g_j \in H_k} \mathbb{e}(g_i - g_j) - \frac{p(k-1)+1}{k^2} = 0 \tag{2.1.8}$$

となることがわかる. ここで、この式の有理数部分の値を a_0 であるとすると、$0 = g_i - g_j$ となる (g_i, g_j) の個数は l であるので、$a_0 = l - \dfrac{p(k-1)+1}{k^2}$ となる. また、1 以上 $p-1$ 以下の整数 n に対して a_n を $n \equiv t - t'\ (p)$ となる解の集合 $\{(g_i, g_j) \mid g_i, g_j \in H_k\}$ の位数とする. すると、(2.1.8) は、今のところ $a_1 = a_2 = \cdots = a_{p-1}$ であると限らないが、

$$\sum_{n=0}^{p-1} a_n \mathbb{e}(n) = 0$$

という式に書き換えることが出来る.

ここで今、$2 \leq l$ より、H_k の元である g_i と g_j に対して、$g_i - g_j \not\equiv 0\ (p)$ となる (g_i, g_j) が存在する. よって、1 以上 $p-1$ 以下の整数 n に対して、$a_n \neq 0$ である n が存在する. また、

$$f(x) = a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}$$
$$g(x) = 1 + x + \cdots + x^{p-1}$$

とすると、$\mathbb{e}(1)$ は $f(x) = 0$ の解になり、$g(x)$ は $\mathbb{e}(1)$ の $\mathbb{Q}$ 上の最小多項式になる. よって、0 以上 $p-1$ 以下の整数 n に対して a_n は $\mathbb{Q}$ の元であることから、$g(x)$ は $f(x)$ を割り切る. ゆえに、

$$0 < a_0 = a_1 = \cdots = a_{p-1}$$

となる. その結果、a_n は $n \equiv g_i - g_j\ (p)$ となる解の集合 $\{(g_i, g_j) \mid g_i, g_j \in H_k\}$ の位数であるから、1 以上 $p-1$ 以下の全ての整数 n に対して、$n \equiv g_i - g_j\ (p)$ となる解が存在し、解の集合 $\{(g_i, g_j) \mid g_i, g_j \in H_k\}$ の位数は n によらず一定であるということが言えた.

次に、(2) を証明する. ($\Leftarrow$) の証明は (1) と同様に出来るので、($\Rightarrow$) だけの証明をする. まず、H に対する l と λ を $H = H_k$ である時と、$H = H_k \cup \{0\}$ である時の区別をする. l と λ を $H = H_k$ である時にそれぞれ l と λ とし、$H = H_k \cup \{0\}$ である時にそれぞれ l' と λ' とする. すると、l' は l に 1 を足したものであるから、(2.1.6) より、

$$l' = l + 1 = \frac{p+k-1}{k} \tag{2.1.9}$$

になることがわかる. また、仮定より補題 1.2.3 が成り立つ. よって、補題 1.2.3 と (2.1.9) より、

$$\lambda' = \frac{p+k-1}{k^2} \tag{2.1.10}$$

となる. ゆえに、$|\ S_k + 1\ |^2$ を (1) と同様に考えると、(2.1.9) と (2.1.10) より、

$$|\ S_k + 1\ |^2 = l' + \lambda' \sum_{n=1}^{p-1} \mathbb{e}(n) = l' - \lambda' = \frac{(p+k-1)(k-1)}{k^2}$$

となる. その結果、この式と (2.1.5) から求めたい式が得られ、証明が出来た. □

注 2.1.11. この定理の ($\Leftarrow$) の証明のポイントは、$f(x)$ が $\mathbb{Q}$ 上の多項式であれば、$g(x)$ の各項の係数が 1 であることを用いて ($\Leftarrow$) の証明が出来ることより、$|\ S_k\ |^2$ の値が有理数でありさえすれば ($\Leftarrow$) の証明が出来るということである. しかし、$|\ S_k\ |^2$ が $\mathbb{Q}$ の元になることの証明は、$|\ S_k\ |^2 = \dfrac{3p+1}{16}$ となることの証明より容易であるわけではない.

また、$|\ S_k\ |^2$ が $\mathbb{Q}$ の元であるならば、H_k が difference set であることより、

$$|\ S_k\ |^2 \in \mathbb{Q} \Leftrightarrow |\ S_k\ |^2 = \frac{p(k-1)+1}{k^2}$$

となることがわかる. 同様に、

$$|\ S_k + 1\ |^2 \in \mathbb{Q} \Leftrightarrow |\ S_k + 1\ |^2 = \frac{(p+k-1)(k-1)}{k^2}$$

となる.

ところで、この定理での p が $k+1$ である時だが、(1) に関しては (2.1.6) より、$l = 1$ となるので、H_k は 1 つの元からなる difference set になる. この論文ではその difference set を考えない. 次に (2) に関しては、(2.1.10) より $\lambda' = \dfrac{2}{k}$ となり、k が 2 より大きい整数であると仮定しているので、λ' は整数にならない. よって、(2) は成り立たない. ゆえに、この定理の p に $k+1$ より大きいという条件がある.

2.2 kが3以上の奇数である時のk-th power residueに対するdifference setは存在しないことの証明

この節では、基本定理から導くことが出来る命題と、kが3以上の奇数である時のk-th power residueに対するdifference setは存在しないことを証明する. まず、次の命題を証明する.

命題 2.2.1. $2 < k$に対して$p \equiv 1\ (2k)$とする. その時、H_kと$H_k \cup \{0\}$はdifference setではない.

証明. まず、$[\mathbb{Q}(S_k) : \mathbb{Q}]$を求める. そのために、$S_k$が$\mathbb{Q}$上で異なる共役を何個持つかを考える. つまり、

$$\left\{\sigma_g(S_k) \mid \sigma_g : \mathbb{e}(1) \mapsto \mathbb{e}(g), \forall g \in {\mathbb{F}_p}^{\times}\right\}$$

の位数を考える. すると、S_kの定義より、この集合の位数は$\{gH_k \mid g \in {\mathbb{F}_p}^{\times}\}$の位数と等しくなる. ここで、ラグランジュの定理より、$|\ {\mathbb{F}_p}^{\times}\ | = [\,{\mathbb{F}_p}^{\times} : H_k\,]\ |\ H_k\ |$である. また、補題2.1.4より$p-1 = kl$である. よって、$[\,{\mathbb{F}_p}^{\times} : H_k\,] = k$となり、$[\,\mathbb{Q}(S_k) : \mathbb{Q}\,] = k$であることがわかる. また、$2 < k$と仮定しているので、$2 < [\,\mathbb{Q}(S_k) : \mathbb{Q}\,]$となり、$S_k \notin \mathbb{Q}$となる.

次に、[6, Proposition 4.2.1.] で証明されている

$$r \in H_k \Leftrightarrow r^{\frac{p-1}{k}} \equiv 1\ (p)$$

であることを使う. すると、$r \in H_k$であるとした時、$(p-r)^{\frac{p-1}{k}}$は

$$(p-r)^{\frac{p-1}{k}} \equiv (-r)^{\frac{p-1}{k}} = (-1)^{\frac{p-1}{k}} \cdot r^{\frac{p-1}{k}} \equiv (-1)^{\frac{p-1}{k}}\ \ (p)$$

になる. 今、$p \equiv 1\ (2k)$としているので、$\dfrac{p-1}{k}$は偶数である. よって、$(p-r)^{\frac{p-1}{k}} \equiv 1\ (p)$となり、$p-r \in H_k$となることがわかる. その結果、$S_k$の項に$\mathbb{e}(r)$が存在すると、$S_k$の項に$\mathbb{e}(p-r)$も存在する. ここで、$\mathbb{e}(r)$と$\mathbb{e}(p-r)$の和を考えると、その和は虚部が打ち消されて実部だけになる. 同様に、S_kの全ての項について考えると、$S_k \in \mathbb{R}$となることがわかる.

ここで、H_kと$H_k \cup \{0\}$がそれぞれdifference setになると仮定すると、定理2.1.2よりそれぞれ$|\ S_k\ |^2 \in \mathbb{Q}$と$|\ S_k + 1\ |^2 \in \mathbb{Q}$になる. よって、$S_k \in \mathbb{R}$であるのでそれぞれ${S_k}^2 \in \mathbb{Q}$と$(S_k+1)^2 \in \mathbb{Q}$になることがわかる. ゆえに、$S_k \notin \mathbb{Q}$より、どちらの場合も$[\,\mathbb{Q}(S_k) : \mathbb{Q}\,] = 2$となる. これは、$2 < [\,\mathbb{Q}(S_k) : \mathbb{Q}\,]$に矛盾する. よって、$H_k$と$H_k \cup \{0\}$はdifference setではない. □

この証明方法は、kが2より大きい整数でなければ証明出来ない. しかし、後で証明するが、kが2であってもこの命題の主張自体は成り立つ. ただし、その証明方法は違うことと、H_2とdifference setの関係をまとめて書きたかったことより、ここではkは2より大きい整数であると仮定した.

次に、k が 3 以上の奇数であるとした時の k-th power residue に対する difference set は存在しないことを証明する．なお、その定理は、命題 2.2.1 の 2 より大きい k に対する $2k$ を 3 以上の奇数 k にしたものである．

定理 2.2.2 (Lehmer 1953). 3 以上の奇数 k に対して、$p \equiv 1\ (k)$ とする．その時、H_k と $H_k \cup \{0\}$ は difference set ではない．

証明. 整数 m に対して $p = 1 + km$ とし、m を奇数と仮定する．すると、k が奇数であることより、p は偶数になる．これは、p が奇数であることに矛盾する．よって、m は偶数になることがわかる．このことを使うと、命題 2.2.1 の証明と同様に証明が出来る． □

ここで、この論文は主に k が 4、6、8、12 である時の k-th power residue に対する difference set が存在するための必要十分条件の証明について書いているが、quadratic residue に対する difference set の定理である次の定理を証明する．

定理 2.2.3 (Chowla 1944). H_2 が difference set であることと、$H_2 \cup \{0\}$ が difference set であることは、どちらも $p \equiv 3\ (4)$ となることと同値である．

この定理を証明するための準備として、次の命題を証明する．

命題 2.2.4. $p \equiv 1\ (k)$ とし、χ を $\mathbb{F}_p$ 上の位数 k の指標とする．その時、$\mathbb{F}_p$ の任意の元 t に対して、$n^k \equiv t\ (p)$ となる n の個数は $\sum_{i=0}^{k-1} \chi^i(t)$ になる．

証明. まず、0 ではない t に対して、$n^k \equiv t\ (p)$ となる n が存在する時を考える．すると、その合同方程式の t に対して $\chi(t) = 1$ となることがわかる．よって、

$$\sum_{i=0}^{k-1} \chi^i(t) = k$$

となる．また、補題 2.1.4 より、$n^k \equiv t\ (p)$ となる n の個数は k であるということがわかる．よって、0 ではない t に対して、$n^k \equiv t\ (p)$ となる n が存在する時に命題は成り立つ．

次に、$n^k \equiv 0\ (p)$ となる時を考える．すると、$\mathbb{F}_p$ が体であるので、$n^k \equiv 0$ であるならば $n = 0$ となる．よって、$n^k \equiv 0\ (p)$ となる n の個数は 1 であることがわかる．また、自明でない指標 χ は $\chi(0) = 0$ であることと、自明な指標 χ^0 は $\chi^0(0) = 1$ であると定義していることより、

$$\sum_{i=0}^{k-1} \chi^i(0) = 1$$

となる．よって、$n^k \equiv 0\ (p)$ となる時にも命題が成り立つ．

最後に、$n^k \equiv t\ (p)$ となる n が存在しない時を考える．χ は ${\mathbb{F}_p}^\times$ から絶対値 1 の複素数の集合への乗法的準同型写像である．また、χ は位数が k であるので、$\mathrm{Im}(\chi) \simeq \mathbb{Z}/k\mathbb{Z}$

である. よって、準同型定理を使うと、$\mathrm{Ker}(\chi) \simeq \mathbb{Z}/\frac{p-1}{k}\mathbb{Z}$ となる. ところで、巡回群の部分群は巡回群である. よって、巡回群 $\mathbb{Z}/(p-1)\mathbb{Z}$ の部分群である $\mathbb{Z}/\frac{p-1}{k}\mathbb{Z}$ は巡回群になる. ゆえに、$\chi(t) = 1$ となる t に対して、$t^{\frac{p-1}{k}} \equiv 1\ (p)$ となることがわかる. その結果、[6, Proposition 4.2.1.] より、$\chi(t) = 1$ であるならば、$n^k \equiv t\ (p)$ となる n が存在することが言える.

今、$n^k \equiv t\ (p)$ となる n が存在しないとしているので、$\chi(t) \neq 1$ となる. また、χ は位数 k の指標であるから $\chi^k(t) - 1 = 0$ となることより、

$$\sum_{i=0}^{k-1} \chi^i(t) = 0$$

となることがわかる. ゆえに、$n^k \equiv t\ (p)$ となる n が存在しない時にも命題は成り立つ.

これで $n^k \equiv t\ (p)$ となるという合同方程式に対しての全ての状況を調べたことになり、その全ての状況で n の個数が $\sum_{i=0}^{k-1} \chi^i(t)$ になることが言えた. □

これで、定理 2.2.3 の証明が出来る.

定理 2.2.3 の証明. 基本定理の証明は k が 2 である時にも成り立つ. よって、$k = 2$ であるとして基本定理を使うと、p が 3 より大きく $p \equiv 1\ (2)$ である時に、H_2 と $H_2 \cup \{0\}$ が difference set になることの必要十分条件は、それぞれ

$$\mid G_2 - 1 \mid^2 = p + 1$$
$$\mid G_2 + 1 \mid^2 = p + 1$$

であることがわかる. この必要十分条件に、計算した G_2 を代入する. χ を $\mathbb{F}_p$ 上の 2 次指標とすると、G_2 は命題 2.2.4 より、

$$G_2 = \sum_{n=0}^{p-1} \mathbb{e}(n^2) = \sum_{n=0}^{p-1} \mathbb{e}(n)(1 + \chi(n)) = g(\chi)$$

になる. その結果、$\mid G_2 \pm 1 \mid^2$ は

$$\mid G_2 \pm 1 \mid^2 = \mid g(\chi) \pm 1 \mid^2 = \mid g(\chi) \mid^2 \pm \left(g(\chi) + \overline{g(\chi)}\right) + 1$$

になることがわかる.

ここで、$p \equiv 1\ (4)$ とする. すると、補題 1.2.8 の (1) と (5) と、定義 1.2.7 の (4) より、

$$\mid g(\chi) \mid^2 \pm \left(g(\chi) + \overline{g(\chi)}\right) + 1 = p \pm 2p^{\frac{1}{2}} + 1$$

となる. よって、$\mid G_2 \pm 1 \mid^2$ は $p+1$ にならないことと、基本定理より、H_2 と $H_2 \cup \{0\}$ は difference set ではないことがわかる. その結果、H_2 が difference set である時と、$H_2 \cup \{0\}$ が difference set である時は、どちらも $p \equiv 3\ (4)$ となる.

次に、$p \equiv 3\ (4)$ とする. すると、補題 1.2.8 の (1) と (5) と、定義 1.2.7 の (4) より、

$$| g(\chi) |^2 \pm \left(g(\chi) + \overline{g(\chi)} \right) + 1 = p + 1$$

となることがわかる. よって、$| G_2 \pm 1 |^2 = p + 1$ となることと、基本定理より、H_2 と $H_2 \cup \{0\}$ は difference set になることがわかる. □

第3章　4th power residueに対するdifference set

この章では、4th power residue に対する difference set が存在することの必要十分条件についての定理を証明する. 次の定理がその定理である.

定理 3.0.1 (Chowla 1944). $5 < p \equiv 1\ (4)$ とする. その時、次の同値性が成り立つ.

(1) H_4 : difference set $\Leftrightarrow p = 1 + 4a^2$ $(1 < \exists a$: 奇数).
(2) $H_4 \cup \{0\}$: difference set $\Leftrightarrow p = 9 + 4b^2$ $(\exists b$: 奇数).

注 3.0.2. この定理には、$p \equiv 1\ (4)$ という条件があるが、これからの証明ではこの条件が必要になる. 証明では計算した G_4 を用いるのだが、その G_4 を計算する際、χ が $\mathbb{F}_p$ 上の位数 4 の指標であるとした時の $g(\chi)$ で G_4 を表す. ところで、$\mathbb{F}_p^\times$ は $\mathbb{Z}/(p-1)\mathbb{Z}$ と同型であり、$\mathbb{Z}/(p-1)\mathbb{Z}$ の指標群は $\mathbb{Z}/(p-1)\mathbb{Z}$ と同型である. また、χ の指標群は $\mathbb{Z}/(p-1)\mathbb{Z}$ の指標群の部分群であるので、4 が $p-1$ を割り切る. よって、$g(\chi)$ と G_4 を $p \equiv 1\ (4)$ という条件付きでそれぞれ考えなければならないので、この定理にも $p \equiv 1\ (4)$ という条件が必要になる.

この定理の証明の概要を説明する. この定理の証明は、基本定理を用いる. しかし、基本定理だけでは証明出来ないので、G_4 を計算する. その際、G_4 を $\mathbb{F}_p$ 上の位数 4 の指標である χ に対しての $g(\chi)$ で表すことが重要である. G_4 を $g(\chi)$ で表すには、ある t に対して $n^4 \equiv t\ (p)$ となる n の個数が $\sum_{i=0}^{k-1} \chi^i(t)$ であるという命題 2.2.4 を用いるのだが、その個数が $\chi(t)$ で表せることが重要になる. ちなみに、命題 2.2.4 では、$n^k \equiv t\ (p)$ となる n が存在することの必要十分条件は、$\mathbb{F}_p$ 上の位数 k の指標である χ に対して、$\chi(t) = 1$ であるということが重要であった. G_4 を $g(\chi)$ で表せると、ガウス和の性質を用いることによって G_4 が計算出来る. その計算した G_4 と基本定理を用いると、ほとんど Chowla の定理が証明出来るのだが、最後に G_4 を表す記号の条件が重要になる. その条件は、ヤコビ和を少し変形した $K(\chi)$ を表す $\mathbb{Z}$ の元の条件と同値である. よって、その $\mathbb{Z}$ の元を用いて $K(\chi)$ を表す定理を証明する必要がある. その際、$K(\chi)$ をあるヤコビ和で表せることが重要になる. この定理が証明出来ると、Chowla の定理の証明が完成する. まとめると、この定理の証明はガウス和からの証明である. 以上が、この定理の証明の概要である.

なお、この章は 3 つの節にし、$\mathbb{Z}$ の元を用いて $K(\chi)$ を表す定理の証明、G_4 の計算、定理 3.0.1 の証明という構成である.

3.1 証明の準備１

この節では、ヤコビ和を少し変形した $K(\chi)$ を定義し、$\mathbb{Z}$ の元を用いてその $K(\chi)$ を表す定理を証明する. まず、その $K(\chi)$ の定義をする.

定義 3.1.1. χ を $\mathbb{F}_p$ 上の自明でない指標とする. その時、

$$K(\chi) = \chi(4)J(\chi, \chi)$$

と定義する.

この $K(\chi)$ について、次の定理が成り立つ.

定理 3.1.2. $p \equiv 1\ (4)$ とし、χ を位数 4 の指標とする. その時、

$$p = {a_4}^2 + {b_4}^2, a_4 \equiv -\left(\frac{2}{p}\right)\ \ (4)$$

である $\mathbb{Z}$ の元 a_4 と b_4 に対して、

$$K(\chi) = a_4 + b_4\sqrt{-1}$$

となる. ただし、$\left(\frac{2}{p}\right)$ はルジャンドル記号である.

この定理を証明することがこの節での目標である. ちなみに、この定理の a_4 と b_4 の 4 は、χ の位数に合わせて定義した. それでは、この定理の証明の準備として次の命題を証明する.

命題 3.1.3. χ を $\mathbb{F}_p$ 上の自明でない指標とし、φ を $\mathbb{F}_p$ 上の 2 次指標とする. その時、

$$K(\chi) = J(\chi, \varphi)$$

となる.

証明. まず、$J(\chi, \chi)$ を考えると、定義より、

$$J(\chi, \chi) = \sum_{n=0}^{p-1} \chi(n(1-n))$$

となる. ここで、t を $n(1-n) \equiv t\ (p)$ となる 0 以上 $p-1$ 以下の整数とする. すると、$n(1-n) \equiv t\ (p)$ は

$$(2n-1)^2 \equiv 1 - 4t\ (p)$$

と式変形出来る. よって、命題2.2.4 より、$n(1-n) \equiv t\ (p)$ となる n の個数は $\sum_{i=0}^{1} \varphi^i(1-4t)$ になる. ゆえに、

$$\sum_{n=0}^{p-1} \chi(n(1-n)) = \sum_{t=0}^{p-1} \chi(t)(1 + \varphi(1-4t))$$

となることがわかる. この式の右辺に自明でない指標の和があるが、それは 0 である. よって、右辺に 1 である $\bar{\chi}(4)\chi(4)$ をかけると、右辺は

$$\bar{\chi}(4)\sum_{t=0}^{p-1}\chi(4t)\varphi(1-4t) \tag{3.1.4}$$

になる. なお、$\mathbb{F}_p^{\times}$ が巡回群であるので、$\{4t \mid t \in \mathbb{F}_p\} = \{t \mid t \in \mathbb{F}_p\}$ となる. よって、(3.1.4) は $4t$ を t に書き直せて、

$$\bar{\chi}(4)\sum_{t=0}^{p-1}\chi(t)\varphi(1-t)$$

になることがわかる. ゆえに、$\sum_{t=0}^{p-1}\chi(t)\varphi(1-t) = J(\chi,\varphi)$ であることと、$K(\chi)$ の定義より、求めたい式が得られる. □

これで、定理 3.1.2 の証明が出来る.

定理 3.1.2 の証明. まず、$\mathbb{Z}$ の元 a_4 と b_4 に対して、$K(\chi) = a_4 + b_4\sqrt{-1}$ となることを証明する. χ の位数が 4 であるので、0 以上 $p-1$ 以下の整数 n に対して、$\chi(n) \in \mathbb{Z}[\sqrt{-1}]$ となる. また、$K(\chi)$ は $\chi(n)$ の和と積で表せるので、$K(\chi) \in \mathbb{Z}[\sqrt{-1}]$ になる. よって、$\mathbb{Z}$ の元 a_4 と b_4 に対して、$K(\chi) = a_4 + b_4\sqrt{-1}$ となることがわかる.

次に、$p = {a_4}^2 + {b_4}^2$ となることだが、$K(\chi) = a_4 + b_4\sqrt{-1}$ であることと、命題 3.1.3 と、補題 1.2.8 の (4) より、$p = {a_4}^2 + {b_4}^2$ となることがわかる.

最後に、$a_4 \equiv -\left(\dfrac{2}{p}\right)$ (4) となることを証明する. n が 0 または 1 である時に、$\chi(1-n)\chi^2(n) = 0$ である. よって、2 次指標である χ^2 をルジャンドル記号で表すと、$K(\chi)$ は、

$$a_4 + b_4\sqrt{-1} = J(\chi,\chi^2) = \sum_{n=0}^{p-1}\chi(1-n)\chi^2(n) = \sum_{n=2}^{p-1}\chi(1-n)\left(\frac{n}{p}\right) \tag{3.1.5}$$

になる. ところで、自明でない指標の和は 0 であるので $\sum_{n=0}^{p-1}\chi(1-n) = 0$ となる. また、$n = 0$、1 である時、それぞれ $\chi(1-n) = 1$、0 となる. よって、(3.1.5) は

$$\sum_{n=2}^{p-1}\chi(1-n)\left(\frac{n}{p}\right) - \sum_{n=0}^{p-1}\chi(1-n) = \sum_{n=2}^{p-1}\chi(1-n)\left\{\left(\frac{n}{p}\right) - 1\right\} - 1 \tag{3.1.6}$$

になることがわかる.

ここで、実際に計算すると、

$$\begin{aligned} 1 &= 1 + (1-\sqrt{-1}\,)\cdot 0 \\ \sqrt{-1} &= 1 + (1-\sqrt{-1}\,)(-1) \\ -1 &= 1 + (1-\sqrt{-1}\,)(-1-\sqrt{-1}\,) \\ -\sqrt{-1} &= 1 + (1-\sqrt{-1}\,)(-\sqrt{-1}\,) \end{aligned}$$

となることがわかる. よって、2以上$p-1$以下のnに対して、$\chi(1-n)$は1の4乗根であることより、

$$\chi(1-n) \equiv 1 \quad \left((1-\sqrt{-1})\,\mathbb{Z}[\sqrt{-1}\,] \right) \tag{3.1.7}$$

になる. また、2以上$p-1$以下のnに対して、$\left(\frac{n}{p}\right) = \pm 1$であることより、

$$\left(\frac{n}{p}\right) - 1 \equiv 0 \ \ (2) \tag{3.1.8}$$

となることがわかる. ところで、自明でない指標の和は0であるので$\sum_{n=0}^{p-1}\left(\frac{n}{p}\right) = 0$である. よって、$\sum_{n=2}^{p-1}\left(\frac{n}{p}\right) = -1$ となることと、(3.1.7) と (3.1.8) より、(3.1.6) は

$$\begin{aligned}\sum_{n=2}^{p-1}\chi(1-n)\left\{\left(\frac{n}{p}\right)-1\right\}-1 &\equiv \sum_{n=2}^{p-1}\left\{\left(\frac{n}{p}\right)-1\right\}-1 \\ &= -p\ \left(2\,(1-\sqrt{-1}\,)\mathbb{Z}[\,\sqrt{-1}\,]\right)\end{aligned}$$

になる. ゆえに、$(a_4+p)+b_4\sqrt{-1} \equiv 0\ \left(2\,(1-\sqrt{-1}\,)\mathbb{Z}[\,\sqrt{-1}\,]\right)$ という式が得られる. この両辺の絶対値の2乗を考えると、$p = {a_4}^2 + {b_4}^2$であることより、

$$8 \mid {a_4}^2 + {b_4}^2 + p^2 + 2a_4p = p(p+1+2a_4)$$

となる. さらに、pが素数であることより、8が$p+1+2a_4$を割り切るので、

$$a_4 \equiv -\frac{p+1}{2} \ \ (4)$$

となることがわかる.

今、$p \equiv 1\ (4)$という条件があるが、0以上の整数mに対して、$p = 8m+1$である時と、$p = 8m+5$である時に場合分けする. まず、$p = 8m+1$である時を考える. すると、

$$-\frac{p+1}{2} = -\frac{8m+2}{2} = -(4m+1) \equiv -1\ (4)$$

となる. 次に、$p = 8m+5$である時を考える. すると、

$$-\frac{p+1}{2} = -\frac{8m+6}{2} = -(4m+3) \equiv 1\ (4)$$

となる. ここで、[6, Proposition 5.1.3.] で証明されている$p = 8m+1$である時に$\left(\frac{2}{p}\right) = 1$であり、$p = 8m+5$である時に$\left(\frac{2}{p}\right) = -1$であることを使う. すると、$-\frac{p+1}{2} \equiv -\left(\frac{2}{p}\right)\ (4)$であることがわかる. よって、

$$a_4 \equiv -\frac{p+1}{2} \equiv -\left(\frac{2}{p}\right) \ \ (4)$$

となることがわかる. □

定理 3.1.2 と同様に、次の系が証明出来る.

系 3.1.9. $p \equiv 1\ (4)$ とし、χ を位数 4 の指標とする. その時、

$$p = {r_4}^2 + {s_4}^2, r_4 \equiv 1\ (2)$$

となる $\mathbb{Z}$ の元 r_4 と s_4 に対して、

$$J(\chi, \chi) = r_4 + s_4\sqrt{-1}$$

となる.

後で説明するが、この系を用いて G_4 を表すことは出来るのだが、それでは定理 3.0.1 の証明が完全に出来ない. そこが、ヤコビ和を少し変形した $K(\chi)$ を考える理由である.

ちなみに、この系の r_4 と s_4 の 4 は、χ の位数に合わせて定義した.

3.2 証明の準備２

この節では、G_4 を計算する. まず、以後見やすいように次のように定義する.

定義 3.2.1. χ を位数 24 の指標とし、i を 2 以上 10 以下の整数とする. その時、

$$R_i = g(\chi^i) + g(\bar{\chi}^i)$$

と定義する.

i を 2 以上 10 以下の整数としたのは、その時しか R_i を使わないので i をそのように制限した. また、見やすくするために R_i を定義しただけなので、R_i の定義にそれ以上の深い意味はない. それでは、G_4 を計算した次の定理を証明する.

定理 3.2.2. 定理 3.1.2 の記号を用いる. その時、

$$G_4 = p^{\frac{1}{2}} \pm \left\{ 2\left(\frac{2}{p}\right)(p + a_4 p^{\frac{1}{2}}) \right\}^{\frac{1}{2}}$$

となる.

証明. まず、G_4 を定義から考える. すると、命題 2.2.4 より、

$$G_4 = \sum_{n=0}^{p-1} \mathbb{e}(n^4) = \sum_{t=0}^{p-1} \mathbb{e}(t)\left(1 + \chi(t) + \chi^2(t) + \chi^3(t)\right) \tag{3.2.3}$$

となる. すると、$\sum_{t=0}^{p-1} \mathbb{e}(t) = 0$ であることと、$\chi^3 = \bar{\chi}$ であることと、補題 1.2.8 の (5) より、(3.2.3) は

$$g(\chi) + g(\bar{\chi}) + p^{\frac{1}{2}}$$

になることがわかる. よって、R_6 である $g(\chi)+g(\bar{\chi})$ を求めればよい. そのために ${R_6}^2$ を考えると、

$$ {R_6}^2 = g^2(\chi) + g^2(\bar{\chi}) + 2g(\chi)g(\bar{\chi}) $$

となる.

まず、$g^2(\chi) + g^2(\bar{\chi})$ を求める. 補題 1.2.8 の (3) と (5) と、$K(\chi)$ の定義と、$\bar{\chi}(4) = \bar{\chi}^2(2) = \left(\dfrac{2}{p}\right)$ であることより、

$$ g^2(\chi) = g(\chi^2)J(\chi,\chi) = p^{\frac{1}{2}}\bar{\chi}(4)K(\chi) = \left(\frac{2}{p}\right)p^{\frac{1}{2}}K(\chi) $$

となることがわかる. また、$g^2(\chi)$ の χ を $\bar{\chi}$ にすれば $g^2(\bar{\chi})$ を求めることが出来て、

$$ g^2(\bar{\chi}) = \left(\frac{2}{p}\right)p^{\frac{1}{2}}K(\bar{\chi}) $$

となる. その結果、$K(\bar{\chi}) = \overline{K(\chi)}$ であることと、定理 3.1.2 より、

$$ g^2(\chi) + g^2(\bar{\chi}) = 2\left(\frac{2}{p}\right)a_4 p^{\frac{1}{2}} \tag{3.2.4} $$

となることがわかる.

次に、$2g(\chi)g(\bar{\chi})$ を求める. 補題 1.2.8 の (2) より、

$$ 2g(\chi)g(\bar{\chi}) = 2\chi(-1)p \tag{3.2.5} $$

となる. また、補題 1.2.8 の (2) と (3) と (5) より、次の 2 つの式が成り立つ.

$$ {J}^2(\chi,\chi) = \left(\frac{g^2(\chi)}{g(\chi^2)}\right)^2 = \frac{g^4(\chi)}{p}. $$
$$ g^4(\chi) = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2). $$

この 2 つの式をまとめると、

$$ {J}^2(\chi,\chi) = \chi(-1)J(\chi,\chi)J(\chi,\chi^2) $$

となる. 両辺を $J(\chi,\chi)$ で割り、命題 3.1.3 と $K(\chi)$ の定義より、

$$ J(\chi,\chi) = \chi(-1)K(\chi) = \chi(-1)\chi(4)J(\chi,\chi) $$

となることがわかる. さらに、両辺を $J(\chi,\chi)$ で割ると、$1 = \chi(-1)\chi(4)$ となる. ところで、

$$ \chi^2(-1) = \chi(1) = 1 $$
$$ \chi^2(4) = \chi^4(2) = \left(\frac{2}{p}\right)^2 = 1 $$

である. よって、$\chi(-1)$ と $\chi(4)$ は ± 1 になる. ゆえに、$1 = \chi(-1)\chi(4)$ であることから $\chi(-1) = \chi(4)$ となることがわかる. その結果、$\chi(4) = \chi^2(2) = \left(\frac{2}{p}\right)$ であることより、(3.2.5) は

$$2\chi(-1)p = 2\chi(4)p = 2\left(\frac{2}{p}\right)p \tag{3.2.6}$$

になる.

これで、${R_6}^2$ を求めることが出来て、(3.2.4) と (3.2.6) より、

$${R_6}^2 = 2\left(\frac{2}{p}\right)(p + a_4 p^{\frac{1}{2}})$$

となる. よって、

$$R_6 = \pm\left\{2\left(\frac{2}{p}\right)(p + a_4 p^{\frac{1}{2}})\right\}^{\frac{1}{2}} \tag{3.2.7}$$

となることがわかる. これで、求めたい式が得られた. □

3.3 Chowlaの定理の証明

この節では、Chowla の定理を証明する.

定理 3.0.1 の証明. (2) は (1) と同様に証明出来るので、(1) だけの証明をやる.

まず、命題 2.2.1 を使う. すると、$k = 4$ であることより、$p \equiv 1\ (8)$ となる時、H_4 は difference set ではないということがわかる. よって、$p \equiv 5\ (8)$ である時を考える. すると、[6, Proposition 5.1.3.] より、$\left(\frac{2}{p}\right) = -1$ である. ゆえに、定理 3.2.2 の G_4 の式は

$$G_4 = p^{\frac{1}{2}} \pm i(2p + 2a_4 p^{\frac{1}{2}})^{\frac{1}{2}} \tag{3.3.1}$$

になる.

($\Leftarrow$) $p \equiv 1\ (4)$ である時、p は一意的に正の奇数の 2 乗足す、正の偶数の 2 乗の形に表せる. また、仮定と定理 3.2.2 の条件より $p = 1 + 4a^2 = {a_4}^2 + {b_4}^2$ である. よって、$a_4 \equiv 1\ (4)$ という条件より、${a_4}^2 = 1$ となり、さらに $a_4 = 1$ となることがわかる. ゆえに、(3.3.1) より

$$|\ G_4 - 1\ |^2 = (p - 2p^{\frac{1}{2}} + 1) + (2p + 2p^{\frac{1}{2}}) = 3p + 1$$

となる. その結果、基本定理の (1) より、H_4 は difference set になる.

($\Rightarrow$) 仮定と基本定理の (1) より、

$$|\ G_4 - 1\ |^2 = 3p + 1$$

となる. また、(3.3.1) より、

$$| G_4 - 1 |^2 = (p - 2p^{\frac{1}{2}} + 1) + (2p + 2a_4 p^{\frac{1}{2}}) = 3p + 1 + 2p^{\frac{1}{2}}(a_4 - 1)$$

となることがわかる. ゆえに、$| G_4 - 1 |^2$ に対する 2 つの式より、$a_4 = 1$ となる. よって、$p = {a_4}^2 + {b_4}^2$ であることより、

$$p = 1 + {b_4}^2$$

となる. また、この定理の $5 < p$ という条件と、$p \equiv 5\ (8)$ である時を考えていることより、0 より大きい整数 m に対して、$p = 1 + 4(2m + 1)$ となる. よって、

$${b_4}^2 = 4(2m + 1)$$

となる. その結果、${b_4}^2$ は 1 より大きい奇数 a に対して $4a^2$ となることがわかる. □

ここで、定理 3.1.2 ではなく系 3.1.9 を用いて G_4 を表した時を考える. すると、G_4 は

$$G_4 = p^{\frac{1}{2}} \pm i(2p - 2r_4 p^{\frac{1}{2}})^{\frac{1}{2}}$$

となる. ちなみに、$p = {r_4}^2 + {s_4}^2$ であるので、$2p - 2r_4 p^{\frac{1}{2}} > 0$ となる. 問題となるのが、この定理の $(\Leftarrow)$ の証明だが、同様に $r_4 \equiv 1\ (2)$ であることと、$p = 1 + 4a^2 = {r_4}^2 + {s_4}^2$ であることより、$r_4 = \pm 1$ となることがわかる. すると、$r_4 = -1$ となる時に、$| G_4 - 1 |^2 = 3p + 1$ となる. また、$r_4 = 1$ となる時に、$| G_4 - 1 |^2 = 3p + 1 - 2p^{\frac{1}{2}}$ となり、$| G_4 - 1 |^2 \neq 3p + 1$ となる. よって、系 3.1.9 を用いて G_4 を表した時では、この定理の証明は不完全である. ゆえに、この定理の $(\Leftarrow)$ の証明で、$a_4 \equiv 1\ (4)$ という条件が重要となる. なお、$a_4 \equiv 1\ (4)$ または $r_4 \equiv -1\ (4)$ という条件を導くには、命題 3.1.3 が重要である. この章では $\chi(4)J(\chi, \chi)$ の性質のうち、その命題 3.1.3 しか用いていないが、次の章からは違う. よって、この章だけ見れば $\chi(4)J(\chi, \chi)$ を $K(\chi)$ と定義する必要はないのだが、次の章以降で見やすくするために、最初から $\chi(4)J(\chi, \chi)$ を $K(\chi)$ と定義したのである. 以上が、$K(\chi)$ をわざわざ定義した理由である. ちなみに、次の章から用いる $\chi(4)J(\chi, \chi)$ の性質も、重要な所は命題 3.1.3 を用いることである.

ところで、$p = 5$ である時だが、その時 $H_4 = \{1\}$ となり $H_4 \cup \{0\} = \{0, 1\}$ となる. よって、H_4 は difference set であるが、この論文では 1 つの元からなる difference set を考えていない. また、$H_4 \cup \{0\}$ は difference set ではない.

第4章　6th power residueに対するdifference set

この章では、6th power residue に対する difference set は存在しないことを証明する. 次の定理がその定理である.

定理 4.0.1 (Lehmer 1953). $7 < p \equiv 1\ (6)$ とする. その時、H_6 と $H_6 \cup \{0\}$ は difference set ではない.

この定理には $p \equiv 1\ (6)$ という条件があるが、注 3.0.2 と同様に、この条件が必要になる.

4.1　証明の準備１

この節では、位数 3 の指標である χ に対し、$\mathbb{Z}$ の元を用いて $K(\chi)$ を表す定理を証明し、その定理を用いてヤコビ和に対する同様の定理を証明する. 次の定理がその $\mathbb{Z}$ の元を用いて $K(\chi)$ を表す定理である.

定理 4.1.1. $p \equiv 1\ (6)$ とし、χ を位数 6 の指標とする. その時、

$$p = {a_3}^2 + 3{b_3}^2, a_3 \equiv -1\ (3)$$

である $\mathbb{Z}$ の元 a_3 と b_3 に対して、

$$K(\chi^2) = a_3 + b_3\sqrt{-3} = \left(\frac{-1}{p}\right) K(\chi)$$

となる.

この定理を証明するために、最初に次の命題を証明する.

命題 4.1.2. χ を位数 $2k$ の指標とする. その時、次の式が成り立つ.

(1) $K(\chi) = \left(\frac{-1}{p}\right) K(\chi^{k-1})$.
(2) $K(\chi) = \chi(-1)J(\chi, \chi^{k-1})$.

証明. まず、(1) から証明する. $\chi^{k-1} = \bar{\chi}\chi^k$ であることと、命題 3.1.3 より、

$$\frac{K(\chi^{k-1})}{K(\chi)} = \frac{K(\bar{\chi}\chi^k)}{K(\chi)} = \frac{J(\bar{\chi}\chi^k, \chi^k)}{J(\chi, \chi^k)} \tag{4.1.3}$$

となる. さらに、補題 1.2.8 の (2) と (3) と、2 次指標である χ^k がルジャンドル記号で表せることより、(4.1.3) は

$$\frac{g(\bar{\chi}\chi^k)g(\chi^k)}{g(\bar{\chi})}\frac{g(\chi\chi^k)}{g(\chi)g(\chi^k)} = \chi^k(-1) = \left(\frac{-1}{p}\right)$$

になることがわかる.

次に、(2) の証明をする. $\dfrac{J(\chi, \chi^{k-1})}{K(\chi)}$ を考えると、(1) より

$$\frac{J(\chi, \chi^{k-1})}{K(\chi)} = \frac{J(\chi, \bar{\chi}\chi^k)}{K(\chi)} = \frac{J(\chi, \bar{\chi}\chi^k)}{\chi^k(-1)K(\bar{\chi}\chi^k)} \tag{4.1.4}$$

となる. さらに、命題 3.1.3 と補題 1.2.8 の (2) と (3) より、(4.1.4) は

$$\frac{J(\chi, \bar{\chi}\chi^k)}{\chi^k(-1)J(\bar{\chi}\chi^k, \chi^k)} = \frac{g(\chi)g(\bar{\chi}\chi^k)}{g(\chi^k)\chi^k(-1)}\frac{g(\bar{\chi})}{g(\bar{\chi}\chi^k)g(\chi^k)} = \chi(-1)$$

になることがわかる. □

ちなみに、この章ではこの命題の (2) を使わない. しかし、(1) と (2) は似ていることより、2 つをまとめて書いた. 次に、次の補題を証明する.

補題 4.1.5. $p \equiv 1\ (6)$ とし、χ を位数 6 の指標とし、Ω を代数的整数環とする. その時、

$$J(\chi^2, \chi^2) \equiv -1 \quad (3\Omega)$$

となる.

証明. 補題 1.2.8 の (2) と (3) より、

$$g(\chi^2)g(\bar{\chi}^2) = \chi^2(-1)p,$$
$$\frac{g^2(\chi^2)}{g(\chi^4)} = J(\chi^2, \chi^2)$$

となる. この 2 つの式の両辺をそれぞれかけると、$\chi^4 = \bar{\chi}^2$ であることと、$\chi^2(-1) = 1$ であることより、

$$g^3(\chi^2) = pJ(\chi^2, \chi^2) \tag{4.1.6}$$

となることがわかる.

次に、$\omega = \dfrac{-1+\sqrt{-3}}{2}$ として、ω と ω^2 を考える. すると、

$$\omega = 1 + \sqrt{3}\,\frac{-\sqrt{3}+\sqrt{-1}}{2}$$
$$\omega^2 = 1 + \sqrt{3}\,\frac{-\sqrt{3}-\sqrt{-1}}{2}$$

となる. よって、

$$\omega \equiv 1 \ \ (\sqrt{3}\Omega),\ \omega^2 \equiv 1 \ \ (\sqrt{3}\Omega)$$

となることがわかる. また、$n = 0$ である時に $\chi^2(n) = 0$ であることと、χ^2 が 3 次指標であるので 1 以上 $p-1$ 以下の n に対して $\chi^2(n)$ は 1 または、ω または、ω^2 になることより、$g(\chi^2)$ は

$$g(\chi^2) = \sum_{n=0}^{p-1} \chi^2(n)\mathfrak{e}(n) \equiv \sum_{n=1}^{p-1} \mathfrak{e}(n) = -1 \ \ (\sqrt{3}\Omega)$$

になる. この式の両辺を 3 乗すると、

$$g^3(\chi^2) \equiv -1 \ \ (3\Omega)$$

となることがわかる. この式は (4.1.6) と、$p \equiv 1\ (6)$ であることと、$J(\chi^2, \chi^2)$ は Ω の元であることより、

$$J(\chi^2, \chi^2) \equiv -1 \ \ (3\Omega)$$

になる. □

これで、定理 4.1.1 の証明が出来る.

定理 4.1.1 の証明. まず、$K(\chi^2) = \left(\dfrac{-1}{p}\right) K(\chi)$ となることを証明する. $k = 3$ として命題 4.1.2 の (1) を用いる. 両辺に $\left(\dfrac{-1}{p}\right)$ をかけると、

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

となることがわかる.

次に、$\mathbb{Z}$ の元 a_3 と b_3 に対して $K(\chi) = a_3 + b_3\sqrt{-3}$ となることを証明する. 定義より、

$$K(\chi^2) = \chi^2(4)J(\chi^2) = \chi^2(4)\sum_{n=0}^{p-1} \chi^2\left(n(1-n)\right) = \sum_{n=0}^{p-1} \chi^2\left(4n(1-n)\right) \tag{4.1.7}$$

となる. ここで、m を 2 以上 $\dfrac{p-1}{2}$ 以下の整数であるとすると、$n = p-m+1$ は $\dfrac{p+3}{2}$ 以上 $p-1$ 以下の整数になる. その $n = p-m+1$ に対して $4n(1-n)$ を考えると、

$$4(p-m+1)(m-p) = 4\left\{pm - m^2 + m - p(p-m+1)\right\} \equiv 4m(1-m)\ (p)$$

となる. よって、整数 m' と m'' に対して $m' \equiv m''\ (p)$ であるならば、$\chi(m') = \chi(m'')$ であることより、

$$\chi^2\left(4(p-m+1)(m-p)\right) = \chi^2\left(4m(1-m)\right)$$

となることがわかる. ゆえに、(4.1.7) は n が 0 と 1 である時に $\chi^2\left(4n(1-n)\right) = 0$ であることと、$n = \dfrac{p+1}{2}$ である時に $\chi^2\left(4n(1-n)\right) = 1$ であることより、

$$1 + 2\sum_{n=2}^{\frac{p-1}{2}} \chi^2\left(4n(1-n)\right)$$

になる. この式は、χ^2 が位数 3 の指標であることから $\chi^2\left(4n(1-n)\right) = 1$ または $\dfrac{-1 \pm \sqrt{-3}}{2}$ になることより、$\mathbb{Z}$ の元 a_3 と b_3 に対して、

$$a_3 + b_3\sqrt{-3}$$

になることがわかる.

次に、$p = {a_3}^2 + 3{b_3}^2$ となることだが、$K(\chi^2) = a_3 + b_3\sqrt{-3}$ であることと、命題 3.1.3 と、補題 1.2.8 の (4) より、$p = {a_3}^2 + 3{b_3}^2$ となる.

最後に、$a_3 \equiv -1\ (3)$ となることを証明する. まず、Ω を代数的整数環であるとする. すると、$K(\chi^2) = a_3 + b_3\sqrt{-3}$ であることより、$K^3(\chi^2) \equiv {a_3}^3\ \ (3\Omega)$ となる. また、$a_3 \equiv 0$ または $\pm 1\ \ (3)$ であるので、

$${a_3}^3 - a_3 = a_3(a_3-1)(a_3+1) \equiv 0\ \ (3)$$

となる. よって、${a_3}^3 \equiv a_3\ \ (3)$ となり、

$$K^3(\chi^2) \equiv a_3\ \ (3\Omega) \tag{4.1.8}$$

となることがわかる.

ところで、$K(\chi^2)$ は定義と補題 4.1.5 より、

$$K(\chi^2) \equiv -\chi^2(4)\ \ (3\Omega)$$

になることがわかる. この式の両辺を 3 乗すると、

$$K^3(\chi^2) \equiv -\chi^6(4) = -1\ \ (3\Omega)$$

となる. よって、(4.1.8) より、

$$a_3 \equiv -1\ \ (3)$$

となることがわかる. □

最後に、定理 4.1.1 の系を証明する.

系 4.1.9. $p \equiv 1\ (6)$ とし、χ を位数 6 の指標であるとする. その時、

$$4p = {r_3}^2 + 3{s_3}^2, r_3 \equiv 1\ (3), s_3 \equiv 0\ (3)$$

である $\mathbb{Z}$ の元 r_3 と s_3 に対して、

$$2J(\chi^2, \chi^2) = r_3 + s_3\sqrt{-3}$$

となる.

証明. まず、Z の元 r_3 と s_3 に対して $2J(\chi^2, \chi^2) = r_3 + s_3\sqrt{-3}$ となることを証明する. $x^2 \equiv 4\ (p)$ の解 x には 2 が存在するので、$\chi^3(4) = 1$ となる. よって、$K(\chi)$ の定義と、$\overline{\chi^2} = \chi^4$ であることと、定理 4.1.1 より、

$$2J(\chi^2, \chi^2) = 2\chi^4(4)K(\chi^2) = 2\chi(4)K(\chi^2) = 2\chi(4)(a_3 + b_3\sqrt{-3}) \tag{4.1.10}$$

となる. よって、$\chi(4) = \chi^2(2) = 1$ または $\dfrac{-1 \pm \sqrt{-3}}{2}$ であるので、$\mathbb{Z}$ の元 r_3 と s_3 に対して、$2J(\chi^2, \chi^2) = r_3 + s_3\sqrt{-3}$ となることがわかる.

次に、${r_3}^2 + 3s_3^2 = 4p$ となることだが、$2J(\chi^2, \chi^2) = r_3 + s_3\sqrt{-3}$ であることと、補題 1.2.8 の (4) より、${r_3}^2 + 3s_3^2 = 4p$ となる.

最後に、$r_3 \equiv 1\ (3), s_3 \equiv 0\ (3)$ となることを証明する. $2J(\chi^2, \chi^2) = r_3 + s_3\sqrt{-3}$ であることと、補題 4.1.5 より、

$$2J(\chi^2, \chi^2) - 1 = (r_3 - 1) + s_3\sqrt{-3} \equiv 0\ \ (3\Omega)$$

となる. よって、$r_3 \equiv 1\ (3), s_3 \equiv 0\ (3)$ となることがわかる. □

4.2 証明の準備２

この節では、G_6 を計算する. まず、定義をする.

定義 4.2.1. 2 が p を法として cubic nonresidue である時、

$$\epsilon_3 = \pm 1, \epsilon_3 \equiv |\ b_3\ |\ \ (3)$$

と定義する.

この ϵ_3 は、$b_3 \equiv 0\ (p)$ となる時は定義出来ないのだが、2 が p を法として cubic nonresidue である時は $b_3 \not\equiv 0\ (p)$ となる. このことは後で説明する. さて、この ϵ_3 を用いると、次の定理が成り立つ.

定理 4.2.2. $\epsilon_6 = \mathrm{sgn}\left\{(a_3 + \epsilon_3 \mid b_3 \mid)({G_3}^2 - p)\right\}$ とし、$p \equiv 1\ (6)$ とし、χ を位数 6 の指標とする. その時、次のことが成り立つ. 2 が p を法として cubic residue である時、

$$G_6 = G_3 + i^* p^{-\frac{1}{2}}({G_3}^2 - p).$$

2 が p を法として cubic nonresidue である時、

$$G_6 = G_3 + \frac{1}{2} i^* p^{-\frac{1}{2}} \left\{(4p - {G_3}^2) + \epsilon_6 G_3 (12p - 3{G_3}^2)^{\frac{1}{2}}\right\}.$$

この定理を証明することがこの節の目標である. この定理を証明するために、最初に次の定理を証明する.

定理 4.2.3. $p \equiv 1\ (6)$ とし、χ を位数 6 の指標とする. その時、G_3 は

$$x^3 - 3px - pr_3 = 0$$

の実根である.

証明. まず、G_3 を定義から考える. すると、命題 2.2.4 より、

$$G_3 = \sum_{n=0}^{p-1} \mathbb{e}(n^3) = \sum_{t=0}^{p-1} \mathbb{e}(t)\left(1 + \chi^2(t) + \chi^4(t)\right)$$

となる. この式は、$\sum_{t=0}^{p-1} \mathbb{e}(t) = 0$ であることと、$\chi^4 = \bar{\chi}^2$ であることより、

$$g(\chi^2) + g(\bar{\chi}^2)$$

になることがわかる. さらにこの式は、$\overline{g(\chi^2)} = \chi^2(-1) g(\bar{\chi}^2)$ であることと、$\chi^2(-1) = 1$ であることより、

$$g(\chi^2) + \overline{g(\chi^2)}$$

になる. よって、$G_3 \in \mathbb{R}$ となることがわかる.

次に、${G_3}^3$ を考えると、補題 1.2.8 の (1) より、

$${G_3}^3 = g^3(\chi^2) + \overline{g^3(\chi^2)} + 3pG_3$$

となる. この式は、(4.1.6) と系 4.1.9 より、

$$pJ(\chi^2, \chi^2) + pJ(\bar{\chi}^2, \bar{\chi}^2) + 3pG_3 = pr_3 + 3pG_3$$

になる. よって、G_3 は $x^3 - 3px - pr_3 = 0$ の解になることがわかる. □

次に、次の補題を証明する.

補題 4.2.4. 定理 4.2.3 の $x^3 - 3px - pr_3$ は $\mathbb{Q}$ 上で既約である.

証明. $x^3 - 3px - pr_3$ の最後の項である $-pr_3$ が p^2 で割り切れないことが証明出来ると、アイゼンシュタインの既約性判定定理を用いてこの補題が証明出来る. そのために、$p \mid r_3$ であると仮定して、矛盾を導く. 仮定と系 4.1.9 の $4p = {r_3}^2 + 3{s_3}^2$ であることより、$p \mid 3{s_3}^2$ となることがわかる. ここで、$p = 3$ とすると、$4p = {r_3}^2 + 3{s_3}^2$ であることより、$3 \mid {r_3}^2$ となり、$3 \mid r_3$ となる. しかし、系 4.1.9 により $r_3 \equiv 1\ (3)$ であるので、矛盾する. よって $p \neq 3$ となることより、$p \mid {s_3}^2$ となり、$p \mid s_3$ となる. ゆえに、$4p = {r_3}^2 + 3{s_3}^2$ と、仮定より $p^2 \mid 4p$ であるので、$p \mid 4$ となる. これは矛盾である.

したがって、$p \nmid r_3$ であることがわかり、$p^2 \nmid -pr_3$ となることが証明出来た. □

次に、次の命題を証明する.

命題 4.2.5. $p \equiv 1\ (6)$ とし、χ を位数 6 の指標とし、$\nu = \operatorname{sgn}\left\{s_3({G_3}^2 - p)\right\}$ とする. その時、

$$g(\chi) = \frac{1}{2} i^* \bar{\chi}(4) p^{-\frac{1}{2}} \left\{ {G_3}^2 - 2p + \nu G_3 (4p - {G_3}^2)^{\frac{1}{2}} \sqrt{-1} \right\}$$

となる.

証明. $K(\chi)$ の定義と命題 3.1.3 より、

$$\chi^2(4) J(\chi^2, \chi^2) = J(\chi^2, \chi^3)$$

となる. この式の両辺に $\chi^4(4)$ をかけると、$\chi^6(4) = 1$ であることより、

$$J(\chi^2, \chi^2) = \chi^3(4)\chi(4) J(\chi^2, \chi^3) \tag{4.2.6}$$

となることがわかる. ところで、$x^2 \equiv 4\ (p)$ の解 x には 2 が存在する. よって、$\chi^3(4) = 1$ となるので、(4.2.6) は

$$J(\chi^2, \chi^2) = \chi(4) J(\chi^2, \chi^3) \tag{4.2.7}$$

になる. この式の左辺は (4.1.6) より、右辺は補題 1.2.8 の (3) と $\chi^5 = \bar{\chi}$ であることより式変形出来る. そして、その式の両辺を $g(\chi^2)$ で割ると、(4.2.7) は

$$\frac{g^2(\chi^2)}{p} = \frac{\chi(4) g(\chi^3)}{g(\bar{\chi})} \tag{4.2.8}$$

になることがわかる.

ところで、補題 1.2.8 の (2) と $\chi^3(-1) = \chi(-1)$ であることより、

$$g(\chi^3) g(\bar{\chi}^3) = \chi^3(-1) p = \chi(-1) p = g(\chi) g(\bar{\chi})$$

となる. よって、$\dfrac{g(\chi^3)}{g(\bar{\chi})} = \dfrac{g(\chi)}{g(\bar{\chi}^3)}$ となる. ゆえに、$\bar{\chi}^3 = \chi^3$ であることと、補題 1.2.8 の (5) より、(4.2.8) は

$$\frac{\chi(4)g(\chi)}{g(\chi^3)} = \frac{\chi(4)g(\chi)}{i^* p^{\frac{1}{2}}}$$

になることがわかる. その結果、両辺に $\bar{\chi}(4)i^* p^{\frac{1}{2}}$ をかけると、

$$g(\chi) = \bar{\chi}(4)p^{-\frac{1}{2}} i^* g^2(\chi^2) \tag{4.2.9}$$

となる.

さて、定理 4.2.3 の証明より、$G_3 = g(\chi^2) + \overline{g(\chi^2)}$ であるので、

$$\mathrm{Re}\{g(\chi^2)\} = \frac{1}{2}G_3$$

となる. また、補題 1.2.8 の (1) より、

$$\mathrm{Im}\{g(\chi^2)\} = \pm\frac{1}{2}(4p - {G_3}^2)^{\frac{1}{2}}$$

となることがわかる. よって、$g(\chi^2)$ の虚部の符号を ν とすると、

$$g(\chi^2) = \frac{1}{2}\left\{G_3 + \nu(4p - {G_3}^2)^{\frac{1}{2}}\sqrt{-1}\right\} \tag{4.2.10}$$

となる. この式の両辺を 2 乗すると、

$$g^2(\chi^2) = \frac{1}{2}\left\{{G_3}^2 - 2p + \nu G_3(4p - {G_3}^2)^{\frac{1}{2}}\sqrt{-1}\right\}$$

となることがわかる. その結果、(4.2.9) より、求めたい式が得られる.

次に、ν を考える. $g^3(\chi^2)$ の虚部は (4.2.10) より、

$$\begin{aligned}\mathrm{Im}\{g^3(\chi^2)\} &= 3\frac{1}{4}{G_3}^2\left\{\frac{1}{2}\nu(4p - {G_3}^2)^{\frac{1}{2}}\right\} - \left\{\frac{1}{8}\nu(4p - {G_3}^2)^{\frac{2}{3}}\right\} \\ &= \frac{1}{2}\nu({G_3}^2 - p)(4p - {G_3}^2)^{\frac{1}{2}}\end{aligned}$$

になる. また、(4.1.6) と系 4.1.9 より、

$$\mathrm{Im}\{g^3(\chi^2)\} = \frac{1}{2}ps_3\sqrt{3}$$

となることがわかる. この $\mathrm{Im}\{g^3(\chi^2)\}$ についての 2 つの式より、

$$\frac{1}{2}\nu({G_3}^2 - p)(4p - {G_3}^2)^{\frac{1}{2}} = \frac{1}{2}ps_3\sqrt{3}$$

となる. この式は $g^3(\chi^2)$ の虚部であるので、$4p - {G_3}^2$ は 0 以上である. また、p は奇素数であることより、符号 ν は ${G_3}^2 - p$ の符号と s_3 の符号に依ることがわかる. よって、

$$\nu = \mathrm{sgn}\left\{s_3({G_3}^2 - p)\right\}$$

となることがわかる. □

最後に、定義と補題の証明をする.

定義 4.2.11. $\omega = \dfrac{-1+\sqrt{-3}}{2}$ とし、χ を位数 6 の指標とし、2 は p を法として cubic nonresidue であるとする. その時、

$$\alpha = \pm 1,\ \chi(4) = \omega^{\alpha}$$

と定義する.

ちなみに、$\chi(4) = \chi^2(2)$ であることと、χ^2 は 3 次指標であることより、2 が p を法として cubic nonresidue である時、$\chi(4)$ は ω または ω^{-1} になることがわかる. よって、α を定義することが出来る. さて、この α を用いると、次の補題が成り立つ.

補題 4.2.12. 定理 4.1.1 と系 4.1.9 の記号を用いる. また、2 は p を法として cubic nonresidue であるとする. その時、

$$s_3 = \alpha(a_3 + \epsilon_3 \mid b_3 \mid)$$

となる.

証明. (4.1.10) より、2 が p を法として cubic nonresidue である時に、

$$s_3 = \alpha a_3 - b_3 \tag{4.2.13}$$

となる. この式は、$a_3 \equiv -1\ (3)$ であることと、$s_3 \equiv 0\ (3)$ であることより、

$$b_3 \equiv -\alpha\ (3) \tag{4.2.14}$$

になることがわかる. この式の両辺に $\operatorname{sgn} b_3$ をかけると、$b_3 \operatorname{sgn} b_3 = \mid b_3 \mid$ であることより、

$$\mid b_3 \mid \equiv -\alpha \operatorname{sgn} b_3\ \ (3)$$

となる. よって、ϵ_3 の定義と、ϵ_3 と $-\alpha \operatorname{sgn} b_3$ は ± 1 であることより、

$$-\alpha \operatorname{sgn} b_3 = \epsilon_3$$

となることがわかる. この式の両辺に $\mid b_3 \mid$ をかけると、

$$-\alpha b_3 = \epsilon_3 \mid b_3 \mid$$

となる. その結果、$\alpha = \pm 1$ であることより、(4.2.13) は

$$\alpha(a_3 - \alpha b_3) = \alpha(a_3 + \epsilon_3 \mid b_3 \mid)$$

になることがわかる. □

なお、2がpを法としてcubic nonresidueである時に$\alpha = \pm 1$であることと、(4.2.14)より、2がpを法としてcubic nonresidueである時に$b_3 \not\equiv 0\ (p)$となることがわかる. よって、ϵ_3を定義することが出来る.

これで、定理4.2.2の証明の証明が出来る.

定理4.2.2の証明. まず、G_6を定義から考える. すると、命題2.2.4と、$\sum_{t=0}^{p-1} \mathbb{e}(t) = 0$であることより、

$$G_6 = \sum_{n=0}^{p-1} \mathbb{e}(n^6) = \sum_{t=0}^{p-1} \mathbb{e}(t) \left(\sum_{i=1}^{5} \chi^i(t) \right)$$

となる. この式は、$\chi^4 = \bar{\chi}^2$であることより、

$$g(\chi) + g(\chi^2) + g(\chi^3) + g(\bar{\chi}^2) + g(\bar{\chi})$$

になることがわかる. さらにこの式は、$g(\chi)+g(\bar{\chi}) = R_4$であることと、$g(\chi^2)+g(\bar{\chi}^2) = G_3$であることと、補題1.2.8の(5)より、

$$R_4 + G_3 + i^* p^{\frac{1}{2}}$$

になる. よって、R_4を求めればよい. そのために、命題4.2.5を用いる. そして、$g(\chi)$のχを$\bar{\chi}$に置き換えるとする. すると、系4.1.9より$2J(\chi^2, \chi^2) = r_3 + is_3\sqrt{3}$であるので、$s_3$が$-s_3$になる. また、$G_3 = g(\chi^2) + g(\bar{\chi}^2)$であることと、$p$は奇素数であることより、$G_3$と$p$はそれぞれ変わらず$G_3$と$p$になる. よって、$g(\chi)$の$\chi$を$\bar{\chi}$に置き換えた時に、$\mathrm{sgn}\left\{s_3({G_3}^2 - p)\right\}$である$\nu$は$-\nu$になる. その結果、2が$p$を法としてcubic residueである時に、$\chi(4) = 1$となることより、

$$R_4 = i^* p^{\frac{1}{2}} ({G_3}^2 - 2p)$$

となることがわかる.

次に、2がpを法としてcubic nonresidueである時を考える. すると、定義4.2.11より、

$$\bar{\chi}(4) = -\frac{1 + \alpha\sqrt{-3}}{2}$$

となる. その結果、命題4.2.5にある$g(\chi)$のχを$\bar{\chi}$に置き換えた時に、$\bar{\chi}(4)$が$\chi(4)$になることと、νが$-\nu$になることより、

$$R_4 = -\frac{1}{2} i^* p^{-\frac{1}{2}} \left\{ {G_3}^2 - 2p - \nu\alpha G_3 (12p - 3{G_3}^2)^{\frac{1}{2}} \right\}$$

となることがわかる. この式の$\nu\alpha$をϵ_6であるとすると、命題4.2.5と補題4.2.12より、

$$\epsilon_6 = \mathrm{sgn}\left\{ (a_3 + \epsilon_3 \mid b_3 \mid)({G_3}^2 - p) \right\}$$

となることがわかる. □

この節の最後に、次の定理 4.2.3 の系を証明する.

系 4.2.15. $x^3 - 3pr - pr_3 = 0$ という式の G_3 以外の解も実数である.

証明. m を p を法とする原始根とした時に、$\sum_{n=0}^{p-1} \mathbb{e}(n^3 m)$ を考える. すると、命題 2.2.4 と、χ は位数 6 の指標であることと、m が p を法とする原始根であることより、

$$\begin{aligned}\sum_{n=0}^{p-1} \mathbb{e}(n^3 m) &= \sum_{t=0}^{p-1} \mathbb{e}(tm)\left(1 + \chi^2(t) + \chi^4(t)\right) \\ &= \sum_{tm=0}^{p-1} \mathbb{e}(tm)\left(\overline{\chi^2(m)}\chi^2(tm) + \overline{\chi^4(m)}\chi^4(tm)\right) \\ &= \overline{\chi^2(m)}g(\chi^2) + \chi^2(m)g(\bar{\chi}^2) \\ &= \overline{\chi^2(m)}g(\chi^2) + \chi^2(m)\overline{g(\chi^2)}\end{aligned} \tag{4.2.16}$$

となる. よって、$\sum_{n=0}^{p-1} \mathbb{e}(n^3 m) \in \mathbb{R}$ となることがわかる. ところで、m が p を法とする原始根であるので、$m^{\frac{p-1}{3}} \not\equiv 1\ (p)$ となる. すると、[6, Proposition 4.2.1.] より、$x^3 \equiv m\ (p)$ となる x が存在しない. よって、命題 2.2.4 の証明と同様に

$$\chi^2(m) \neq 1 \tag{4.2.17}$$

となる. ゆえに、(4.2.16) と $G_3 = g(\chi^2) + \overline{g(\chi^2)}$ であることより、$G_3 \neq \sum_{n=0}^{p-1} \mathbb{e}(n^3 m)$ となることがわかる.

さて、$\sum_{n=0}^{p-1} \mathbb{e}(n^3 m)$ の 3 乗を考えると、(4.2.16) と、$\left(\overline{\chi^2(m)}\right)^3$ と $\left(\chi^2(m)\right)^3$ は 1 であることと、補題 1.2.8 の (1) より、

$$\left(\sum_{n=0}^{p-1} \mathbb{e}(n^3 m)\right)^3 = g^3(\chi^2) + \overline{g^3(\chi^2)} + 3p\sum_{n=0}^{p-1} \mathbb{e}(n^3 m)$$

となる. よって、定理 4.2.3 の証明と同様に、$\sum_{n=0}^{p-1} \mathbb{e}(n^3 m)$ は $x^3 - 3px - pr_3 = 0$ の解になることがわかる.

次に、$\sum_{n=0}^{p-1} \mathbb{e}(n^3 m^2)$ を考える. すると、$\sum_{n=0}^{p-1} \mathbb{e}(n^3 m)$ と同様に、

$$\sum_{n=0}^{p-1} \mathbb{e}(n^3 m^2) = \overline{\chi^2(m^2)}g(\chi^2) + \chi^2(m^2)\overline{g(\chi^2)} \tag{4.2.18}$$

$$\left(\sum_{n=0}^{p-1} \mathbb{e}(n^3 m^2)\right)^3 = g^3(\chi^2) + \overline{g^3(\chi^2)} + 3p\sum_{n=0}^{p-1} \mathbb{e}(n^3 m^2)$$

となる. よって、$\sum_{n=0}^{p-1} \mathbb{e}(n^3m^2) \in \mathbb{R}$ であることと、$\sum_{n=0}^{p-1} \mathbb{e}(n^3m^2)$ は $x^3 - 3px - pr_3 = 0$ の解になることがわかる. ところで、(4.2.17) より、$\chi^2(m) = \frac{-1\pm\sqrt{-3}}{2}$ となる. よって、$\chi^2(m^2) = (\chi^2(m))^2 \neq 1$ となるので、(4.2.18) と $G_3 = g(\chi^2) + \overline{g(\chi^2)}$ であることより、$G_3 \neq \sum_{n=0}^{p-1} \mathbb{e}(n^3m^2)$ となる. また、$\chi^2(m^2) = \chi^4(m) = \overline{\chi^2(m)}$ であることより $\chi^2(m) \neq \chi^2(m^2)$ であるので、$\sum_{n=0}^{p-1} \mathbb{e}(n^3m) \neq \sum_{n=0}^{p-1} \mathbb{e}(n^3m^2)$ となることがわかる. □

4.3 Lehmer の定理の証明

この節では、Lehmer の定理を証明する.

定理 4.0.1 の証明. $H_6 \cup \{0\}$ は H_6 と同様に証明出来るので、H_6 だけの証明をやる.

まず、命題 2.2.1 を使う. すると、$k = 6$ であることより、$p \equiv 1\ (12)$ となる時、H_6 は difference set ではないということがわかる. よって、$p \equiv 7\ (12)$ である時を考える. すると、定義 1.2.7 の (4) と定理 4.2.2 より、次の式が成り立つ. 2 が p を法として cubic residue である時、

$$G_6 = G_3 + p^{-\frac{1}{2}}({G_3}^2 - p)\sqrt{-1}.$$

2 が p を法として cubic nonresidue である時、

$$G_6 = G_3 + \frac{1}{2}p^{-\frac{1}{2}}\left\{(4p - {G_3}^2) + \epsilon_6 G_3(12p - 3{G_3}^2)^{\frac{1}{2}}\right\}\sqrt{-1}.$$

最初に、2 が p を法として cubic residue である時を考える. 定理 4.2.3 の $G_3 \in \mathbb{R}$ であることと ${G_3}^4 = 3p{G_3}^2 + pr_3G_3$ であることより、$|\, G_6 - 1\,|^2$ を計算し、${G_3}^4$ を消すと、

$$\begin{aligned} |\, G_6 - 1\,|^2 &= |\, (G_3 - 1) + p^{-\frac{1}{2}}({G_3}^2 - p)\sqrt{-1}\,|^2 \\ &= 2{G_3}^2 + (r_3 - 2)G_3 + p + 1 \end{aligned}$$

となる. また、H_6 が difference set であると仮定して基本定理を用いると、

$$|\, G_6 - 1\,|^2 = 5p + 1 \tag{4.3.1}$$

となる. よって、$|\, G_6 - 1\,|^2$ に対する 2 つの式より、

$$2{G_3}^2 + (r_3 - 2)G_3 - 4p = 0$$

となる. この式は、補題 4.2.4 に矛盾する. よって、2 が p を法として cubic residue である時に、H_6 は difference set ではない.

次に 2 が p を法として cubic nonresidue である時を考える. $|\ G_6 - 1\ |^2$ を計算し、2 が p を法として cubic residue である時の証明と同様に ${G_3}^4$ と ${G_3}^3$ を消すと、

$$|\ G_6 - 1\ |^2 = \frac{1}{2}{G_3}^2 - \frac{1}{2}(4 + r_3)G_3 + 4p + 1 + \frac{1}{2}\epsilon_6(G_3 - r)(12p - 3{G_3}^2)^{\frac{1}{2}}$$

となる. よって、この式と (4.3.1) より、

$${G_3}^2 - (4 + r_3)G_3 - 2p = \epsilon_6(r_3 - G_3)(12p - 3{G_3}^2)^{\frac{1}{2}}$$

となる. この式の両辺を 2 乗して、同様に ${G_3}^4$、${G_3}^3$ を消すと、

$$(4{r_3}^2 + 8r_3 - 4p + 16){G_3}^2 + 8p(r_3 - 1)G_3 + 4p(p - 5{r_3}^2 - 2r_3) = 0$$

となる. ゆえに、この式の項が全て 0 でないと補題 4.2.4 に矛盾してしまう. よって、$p - 5{r_3}^2 - 2r_3 = 0$ となるので、$p = r_3(5r_3 + 2)$ となる. p は奇素数であることより $r_3 = 1$ となるので、$p = 7$ となる. これは、$7 < p$ であることに矛盾する. よって、2 が p を法として cubic nonresidue である時に、H_6 は difference set ではない. □

ちなみに、$p = 7$ である時に $H_6 = \{1\}$ となり $H_6 \cup \{0\} = \{0, 1\}$ となる. よって、H_6 は difference set であるが、この論文では 1 つの元からなる difference set を考えていない. また、$H_6 \cup \{0\}$ は difference set ではない.

第5章　8th power residueに対するdifference set

この章では、8th power residue に対する difference set が存在することの必要十分条件についての定理を証明する. 次の定理がその定理である.

定理 5.0.1 (Lehmer 1953). $p \equiv 1\ (8)$ とする. その時、次の同値性が成り立つ.

(1) H_8 : difference set $\Leftrightarrow p = 1 + 8c^2 = 9 + 64d^2 \quad (\exists\, c, d \in \mathbb{Z})$.
(2) $H_8 \cup \{0\}$: difference set $\Leftrightarrow p = 49 + 8e^2 = 441 + 64f^2 \quad (\exists\, e, f \in \mathbb{Z})$.

この定理には $p \equiv 1\ (8)$ という条件があるが、注 3.0.2 と同様に、この条件が必要になる.

5.1　証明の準備１

この節では、位数 8 の指標である χ に対し、$\mathbb{Z}$ の元を用いて $K(\chi)$ を表す定理を証明をする. 次の定理がその $\mathbb{Z}$ の元を用いて $K(\chi)$ を表す定理である.

定理 5.1.1. $p \equiv 1\ (8)$ とし、χ を位数 8 の指標とする. その時、

$$p = {a_8}^2 + 2{b_8}^2, a_8 \equiv -1\ (4)$$

である $\mathbb{Z}$ の元 a_8 と b_8 に対して、

$$K(\chi) = a_8 + b_8\sqrt{-2}$$

となる.

証明. まず、$\mathbb{Z}$ の元 a_8 と b_8 に対して、$K(\chi) = a_8 + b_8\sqrt{-2}$ となることを証明する. [6, Proposition 4.2.1.] より、$x^2 \equiv -1\ (p)$ になる x が存在することと、$(-1)^{\frac{p-1}{2}} = 1$ になることは同値である. 今、$p \equiv 1\ (8)$ であることより、$(-1)^{\frac{p-1}{2}} = 1$ となるので、$\left(\dfrac{-1}{p}\right) = 1$ となることがわかる. よって、命題 4.1.2 の (1) より、

$$K(\chi) = K(\chi^3) \tag{5.1.2}$$

となる.

ところで、$K(\chi)$ は χ の値の和と積になる. よって、整数 x に対して $e^{\frac{2\pi\sqrt{-1}x}{8}} = \mathbb{e}_8(x)$ とし、1 以上 8 以下の整数 i に対して $c_i \in \mathbb{Z}$ とした時に、$K(\chi)$ は

$$\begin{aligned} K(\chi) = c_1\mathbb{e}_8(1) + c_2\mathbb{e}_8(2) + c_3\mathbb{e}_8(3) + c_4\mathbb{e}_8(4) \\ + c_5\mathbb{e}_8(5) + c_6\mathbb{e}_8(6) + c_7\mathbb{e}_8(7) + c_8\mathbb{e}_8(8) \end{aligned}$$

になる. この式より、

$$\begin{aligned} K(\chi^3) = c_1\mathbb{e}_8(3) + c_2\mathbb{e}_8(6) + c_3\mathbb{e}_8(1) + c_4\mathbb{e}_8(4) \\ + c_5\mathbb{e}_8(7) + c_6\mathbb{e}_8(2) + c_7\mathbb{e}_8(5) + c_8\mathbb{e}_8(8) \end{aligned}$$

となることがわかる. よって、

$$\begin{aligned} K(\chi^3) - K(\chi) &= c_1\left(\mathbb{e}_8(3) - \mathbb{e}_8(1)\right) + c_2\left(\mathbb{e}_8(6) - \mathbb{e}_8(2)\right) + c_3\left(\mathbb{e}_8(1) - \mathbb{e}_8(3)\right) \\ &\quad + c_5\left(\mathbb{e}_8(7) - \mathbb{e}_8(5)\right) + c_6\left(\mathbb{e}_8(2) - \mathbb{e}_8(6)\right) + c_7\left(\mathbb{e}_8(5) - \mathbb{e}_8(7)\right) \\ &= (-c_1 + c_3 + c_5 - c_7)\sqrt{2} + (-c_2 + c_6)2 \\ &= 0 \end{aligned}$$

となる. この式と $c_i \in \mathbb{Z}$ であることより、

$$c_1 - c_3 - c_5 + c_7 = 0\,,\ c_2 - c_6 = 0$$

となることがわかる. よって、$c_2\mathbb{e}_8(2) + c_6\mathbb{e}_8(6)$ は

$$c_2\mathbb{e}_8(2) + c_6\mathbb{e}_8(6) = (c_2 - c_6)\mathbb{e}_8(2) = 0 \tag{5.1.3}$$

になる. また、$c_1\mathbb{e}_8(1) + c_3\mathbb{e}_8(3) + c_5\mathbb{e}_8(5) + c_7\mathbb{e}_8(7)$ は

$$\begin{aligned} &c_1\mathbb{e}_8(1) + c_3\mathbb{e}_8(3) + c_5\mathbb{e}_8(5) + c_7\mathbb{e}_8(7) \\ &= (c_1 - c_3 - c_5 + c_7)\frac{1}{\sqrt{2}} + (c_1 + c_3 - c_5 - c_7)\frac{\sqrt{-1}}{\sqrt{2}} \\ &= (c_1 - c_5)\sqrt{-2} \end{aligned} \tag{5.1.4}$$

になることがわかる.

よって (5.1.3) と、(5.1.4) と、$\mathbb{e}_8(4) = -1$ であること、$\mathbb{e}_8(8) = 1$ であることより、

$$K(\chi) = -c_4 + c_8 + (c_1 - c_5)\sqrt{-2}$$

となる. ゆえに、$c_i \in \mathbb{Z}$ であることより、$\mathbb{Z}$ の元 a_8 と b_8 に対して、

$$K(\chi) = a_8 + b_8\sqrt{-2}$$

となることがわかる.

次に、$p = {a_8}^2 + 2{b_8}^2$ となることだが、$K(\chi) = a_8 + b_8\sqrt{-2}$ であることと、命題 3.1.3 と、補題 1.2.8 の (4) より、$p = {a_8}^2 + 2{b_8}^2$ となる.

最後に、$a_8 \equiv -1$ (4) となることを証明する. 定理 3.1.2 の証明と同様に、ルジャンドル記号を使って、$K(\chi)$ を計算すると、

$$\begin{aligned} a_8 + b_8\sqrt{-2} &= \sum_{n=2}^{p-1} \chi(1-n) \left(\frac{n}{p}\right) \\ &= \sum_{n=2}^{p-1} \chi(1-n) \left\{ \left(\frac{n}{p}\right) - 1 \right\} - 1 \end{aligned} \tag{5.1.5}$$

となることがわかる. ところで、1 以上 7 以下の整数 m に対して、

$$\mathfrak{e}_8(m) = 1 + (1 - \mathfrak{e}_8(1)\,)\,(-\mathfrak{e}_8(m-1) - \mathfrak{e}_8(m-2) - \cdots - \mathfrak{e}_8(1) - 1\,)$$

となる. よって、$\chi(1-n)$ は 1 の 8 乗根であることより、

$$\chi(1-n) \equiv 1 \quad (\,(1 - \mathfrak{e}_8(1)\,)\,\mathbb{Z}[\mathfrak{e}_8(1)]\,) \tag{5.1.6}$$

となる. また、2 以上 $p-1$ 以下の n に対して、

$$\left(\frac{n}{p}\right) - 1 \equiv 0 \ (2) \tag{5.1.7}$$

となることがわかる.

よって、(5.1.6) と (5.1.7) より、(5.1.5) は

$$\begin{aligned} \sum_{n=2}^{p-1} \chi(1-n) \left\{ \left(\frac{n}{p}\right) - 1 \right\} - 1 &\equiv \sum_{n=2}^{p-1} \left\{ \left(\frac{n}{p}\right) - 1 \right\} - 1 \\ &= p \quad (\,2(1 - \mathfrak{e}_8(1)\,)\mathbb{Z}[\mathfrak{e}_8(1)]\,) \end{aligned}$$

になる. よって、$(a_8 - p) + b_8\sqrt{-2} \equiv 0 \quad (\,2(1 - \mathfrak{e}_8(1)\,)\mathbb{Z}[\mathfrak{e}_8(1)]\,)$ という式が得られ、この式の両辺の絶対値の 2 乗を考えると、$p = {a_8}^2 + 2{b_8}^2$ であることより、

$$8 \mid (a_8 + p)^2 + 2{b_8}^2 = p^2 + p + 2pa_8 = p(p + 1 + 2a_8)$$

となることがわかる. さらに、p が素数であることより、8 が $p + 1 + 2a_8$ を割り切ることがわかる. よって、$p \equiv 1$ (8) であるので、a_8 は

$$a_8 \equiv -\frac{p+1}{2} = -1 \ (4)$$

になる. □

5.2 証明の準備２

この節では、G_8 を計算する. 次の定理が G_8 を計算した定理である.

定理 5.2.1. $p = 1+8k$ とし、χ を位数 8 の指標とする. その時、$R_6 = \pm\left\{2(p + a_4 p^{\frac{1}{2}})\right\}^{\frac{1}{2}}$ となり、

$$G_8 = p^{\frac{1}{2}} + R_6 \pm \left\{(a_8 + p^{\frac{1}{2}})\left(2\chi^2(2)R_6 + 4(-1)^k p^{\frac{1}{2}}\right)\right\}^{\frac{1}{2}}$$

となる.

証明. 最初に、R_6 を考える. すると、(3.2.7) より、

$$R_6 = \pm\left\{2\left(\frac{2}{p}\right)(p + a_4 p^{\frac{1}{2}})\right\}^{\frac{1}{2}}$$

である. ここで、[6, Proposition 5.1.3.] で証明されているいる $p \equiv 1\ (8)$ である時に、$\left(\frac{2}{p}\right) = 1$ であることを使うと、求めたい式が得られる.

次に、G_8 を考える. 命題 2.2.4 と、$\sum_{t=0}^{p-1} \mathbb{e}(t) = 0$ であることを使う. すると、$\chi^7 = \bar{\chi}$, $\chi^6 = \bar{\chi}^2$, $\chi^5 = \bar{\chi}^3$ となることと、R_i の定義より、

$$\begin{aligned} G_8 &= \sum_{t=0}^{p-1} \mathbb{e}(t)\left(\sum_{i=1}^{7} \chi^i(t)\right) \\ &= g(\chi^4) + \left(g(\chi^2) + g(\bar{\chi}^2)\right) + \left(g(\chi) + g(\bar{\chi})\right) + \left(g(\chi^3) + g(\bar{\chi}^3)\right) \\ &= p^{\frac{1}{2}} + R_6 + R_3 + R_9 \end{aligned}$$

となる. よって、$R_3 + R_9$ を求めればよい. そのために、$(R_3 + R_9)^2$ を求める.

まず、${R_3}^2$ を求める. 補題 1.2.8 の (2) と (3) と、$K(\chi)$ の定義より、

$$\begin{aligned} {R_3}^2 &= g^2(\chi) + g^2(\bar{\chi}) + 2g(\chi)g(\bar{\chi}) \\ &= g(\chi^2)\bar{\chi}^2(2)K(\chi) + g(\bar{\chi}^2)\chi^2(2)K(\bar{\chi}) + 2\chi(-1)p \end{aligned}$$

となることがわかる. また、R_3 の χ を χ^3 にすれば R_9 を求めることが出来て、$\left(\chi^3\right)^2 = \bar{\chi}^2$, $\left(\bar{\chi}^3\right)^2 = \chi^2$ であることと、$\chi^3(-1) = \chi^2(-1)\chi(-1) = \chi(-1)$ であることより、

$${R_9}^2 = g(\bar{\chi}^2)\chi^2(2)K(\chi^3) + g(\chi^2)\bar{\chi}^2(2)K(\bar{\chi}^3) + 2\chi(-1)p$$

になる. ところで、[6, Proposition 5.1.3.] で証明されている $p \equiv 1\ (8)$ である時に、$\left(\frac{2}{p}\right) = 1$ であることを使うと、$\chi^2(2) = \pm 1$ となるので、$\chi^2(2) = \bar{\chi}^2(2)$ となる. よって、(5.1.2) と、(5.1.2) からわかる $K(\bar{\chi}) = K(\bar{\chi}^3)$ であることと、定理 5.1.1 より、

$$\begin{aligned} {R_3}^2 + {R_9}^2 &= \chi^2(2)\left\{g(\chi^2) + g(\bar{\chi}^2)\right\}\left\{K(\chi) + K(\bar{\chi})\right\} + 4\chi(-1)p \\ &= 2\chi^2(2)a_8 R_6 + 4\chi(-1)p \end{aligned} \tag{5.2.2}$$

となることがわかる.

次に、$2R_3R_9$ を求める. $2R_3R_9$ は

$$\begin{aligned} 2R_3R_9 &= 2\left(g(\chi)+g(\bar{\chi})\right)\left(g(\chi^3)+g(\bar{\chi}^3)\right) \\ &= 2\left(g(\chi)g(\chi^3)+g(\chi)g(\bar{\chi}^3)+g(\bar{\chi})g(\chi^3)+g(\bar{\chi})g(\bar{\chi}^3)\right) \end{aligned}$$

になるので、この 4 つの項を求める.

まず、$g(\chi)g(\chi^3)$ を求める. 命題 4.1.2 の (2) の両辺に $\chi(-1)$ をかけると、$\chi^2(-1)=\chi(1)=1$ であることより $J(\chi,\chi^3)=\chi(-1)K(\chi)$ となることと、補題 1.2.8 の (3) より、$g(\chi)g(\chi^3)$ は、

$$g(\chi)g(\chi^3)=g(\chi^4)J(\chi,\chi^3)=p^{\frac{1}{2}}\chi(-1)K(\chi) \tag{5.2.3}$$

になる. また、$g(\chi)g(\chi^3)$ の χ を $\bar{\chi}$ にすれば $g(\bar{\chi})g(\bar{\chi}^3)$ を求めることが出来て、$\chi(-1)=\pm1$ であることより $\bar{\chi}(-1)=\chi(-1)$ となるので、

$$g(\bar{\chi})g(\bar{\chi}^3)=p^{\frac{1}{2}}\chi(-1)K(\bar{\chi})$$

となることがわかる.

次に、$g(\bar{\chi})g(\chi^3)$ を求める. (5.2.3) の両辺に $\dfrac{g(\bar{\chi})}{g(\chi)}$ をかけて、$K(\chi)$ の定義と、補題 1.2.8 の (2) と (3) より、

$$\begin{aligned} g(\bar{\chi})g(\chi^3) &= p^{\frac{1}{2}}\chi(-1)\chi(4)\frac{g^2(\chi)}{g(\chi^2)}\frac{g(\bar{\chi})}{g(\chi)} \\ &= p^{\frac{1}{2}}\chi^2(2)\frac{\chi^2(-1)p}{g(\chi^2)} \\ &= p^{\frac{1}{2}}\chi^2(2)g(\bar{\chi}^2) \end{aligned}$$

となる. また、$g(\bar{\chi})g(\chi^3)$ の χ を $\bar{\chi}$ にすれば $g(\chi)g(\bar{\chi}^3)$ を求めることが出来て、(5.2.2) を導く時と同様に $\chi^2(2)=\bar{\chi}^2(2)$ となるので、

$$g(\chi)g(\bar{\chi}^3)=p^{\frac{1}{2}}\chi^2(2)g(\chi^2)$$

となることがわかる.

よって、$2R_3R_9$ を求めることが出来て、定理 5.1.1 より、

$$\begin{aligned} 2R_3R_9 &= 2p^{\frac{1}{2}}\left(\chi(-1)K(\chi)+\chi^2(2)g(\chi^2)+\chi^2(2)g(\bar{\chi}^2)+\chi(-1)K(\bar{\chi})\right) \\ &= 2p^{\frac{1}{2}}\left(2\chi(-1)a_8+\chi^2(2)R_6\right) \end{aligned} \tag{5.2.4}$$

となる.

その結果、$(R_3+R_9)^2$ を求めることが出来て、(5.2.2) と (5.2.4) より、

$$\begin{aligned} (R_3+R_9)^2 &= \left(2\chi^2(2)a_8R_6+4\chi(-1)p\right)+\left\{2p^{\frac{1}{2}}\left(2\chi(-1)a_8+\chi^2(2)R_6\right)\right\} \\ &= (a_8+p^{\frac{1}{2}})(2\chi^2(2)R_6+4\chi(-1)p^{\frac{1}{2}}) \end{aligned}$$

となることがわかる.

最後に、$\chi(-1) = (-1)^k$ であることを証明する. $\chi^2(-1) = 1$ であることより、$\chi(-1) = \pm 1$ である. また、[6, Proposition 4.2.1.] より、$x^8 \equiv -1\ (p)$ になる x が存在することと、$(-1)^{\frac{p-1}{8}} = 1$ になることは同値である. よって、今 $p = 1 + 8k$ であるので $(-1)^{\frac{p-1}{8}} = (-1)^k$ となることより、$\chi(-1) = (-1)^k$ となる. □

5.3 Lehmer の定理の証明

この節では、Lehmer の定理を証明する.

定理 5.0.1 の証明. (2) は (1) と同様に証明出来るので、(1) だけの証明をやる.

まず、命題 2.2.1 を使う. すると、$k = 8$ であることより、$p \equiv 1\ (16)$ となる時、H_8 は difference set ではないということがわかる. よって、$p \equiv 9\ (16)$ である時を考える. すると、G_8 は定理 5.2.1 の k が $2k + 1$ になり $(-1)^{2k+1} = -1$ であることより、$R_6 = \pm\left\{2(p + a_4 p^{\frac{1}{2}})\right\}^{\frac{1}{2}}$ に対して、

$$G_8 = p^{\frac{1}{2}} + R_6 \pm \left\{(a_8 + p^{\frac{1}{2}})\left(4p^{\frac{1}{2}} - 2\chi^2(2)R_6\right)\right\}^{\frac{1}{2}}\sqrt{-1} \tag{5.3.1}$$

になる. また、[6, Proposition 5.1.3.] で証明されている $p \equiv 1\ (8)$ である時に、$\left(\frac{2}{p}\right) = 1$ であることと、定理 3.1.2 と、定理 5.1.1 より、

$$p = {a_4}^2 + {b_4}^2 = {a_8}^2 + 2{b_8}^2,\ a_4 \equiv -1\ (p),\ a_8 \equiv -1\ (p)$$

である.

(⇐) 仮定より、$p = 1 + 8c^2 = 9 + 64d^2$ である. よって、[6, p.64] より、$\chi^2(2) = 1$ となる. また、$1 + 8c^2 = {a_8}^2 + 2{b_8}^2$ となることと、$a_8 \equiv -1\ (p)$ であることより、$a_8 = -1$ となる. 同じく、$9 + 64d^2 = {a_4}^2 + {b_4}^2$ となることと、$a_4 \equiv -1\ (p)$ であることより、$a_4 = 3$ となることがわかる. その結果、$R_6 = \pm\left\{2(p + 3p^{\frac{1}{2}})\right\}^{\frac{1}{2}}$ となることと、(5.3.1) より、$|\ G_8 - 1\ |^2$ を計算すると、

$$|\ G_8 - 1\ |^2 = (p^{\frac{1}{2}} + R_6 - 1)^2 + (1 - p^{\frac{1}{2}})(2R_6 - 4p^{\frac{1}{2}}) = 7p + 1$$

となる. よって、基本定理の (1) より、H_8 は difference set になる.

(⇒) 仮定と基本定理の (1) より、

$$|\ G_8 - 1\ |^2 = 7p + 1$$

となる. また、(5.3.1) より、

$$\begin{aligned}|\ G_8 - 1\ |^2 &= (p^{\frac{1}{2}} + R_6 - 1)^2 + (a_8 + p^{\frac{1}{2}})\left(4p^{\frac{1}{2}} - 2\chi^2(2)R_6\right) \\ &= 7p + 1 + 2p^{\frac{1}{2}}(2a_8 + a_4 - 1) \\ &\quad + 2R_6\left(p^{\frac{1}{2}} - 1 - \chi^2(2)a_8 - \chi^2(2)p^{\frac{1}{2}}\right)\end{aligned}$$

となることがわかる. $|\, G_8 - 1 \,|^2$ に対する 2 つの式と、$R_6 \notin \mathbb{Z}[\, p^{\frac{1}{2}} \,]$ であることより、R_6 の係数と、$p^{\frac{1}{2}}$ の係数は 0 になる. よって、$\chi^2(2) = 1$, $a_8 = -1$, $a_4 = 3$ となるので、$p = 1 + 2{b_8}^2 = 9 + {b_4}^2$ になる. また、$\chi^2(2) = 1$ であることと、[6, p.64] より、$8 \mid b_4$ となる. □

第6章　12th power residueに対するdifference set

この章では、12th power residue に対する difference set は存在しないことを証明する. 次の定理がその定理である.

定理 6.0.1 (Whiteman 1960). $13 < p \equiv 1\ (12)$ とする. その時、H_{12} と $H_{12} \cup \{0\}$ は difference set ではない.

この定理には $p \equiv 1\ (12)$ という条件があるが、注 3.0.2 と同様に、この条件が必要になる.

6.1　証明の準備１

この節では、位数 12 の指標である χ に対し、$\mathbb{Z}$ の元を用いて $K(\chi)$ を表す定理を証明をする. 次の定理がその $\mathbb{Z}$ の元を用いて $K(\chi)$ を表す定理である.

定理 6.1.1. $p \equiv 1\ (12)$ とし、χ を位数 12 の指標とする. その時、次のことが成り立つ.

$$K(\chi) = \begin{cases} -K(\chi^3) & 3 \mid a_4, \\ K(\chi^3) & 3 \nmid a_4. \end{cases}$$

また、

$$(a_{12}, b_{12}) = \begin{cases} (-a_4, -b_4) & 3 \mid a_4, \\ (a_4, b_4) & 3 \nmid a_4. \end{cases}$$

である $\mathbb{Z}$ の元 a_{12} と b_{12} に対して、

$$K(\chi) = a_{12} + b_{12}\sqrt{-1}$$

となる.

証明. まず、$\mathbb{Z}$ の元 a_{12} と b_{12} に対して、$K(\chi) = a_{12} + b_{12}\sqrt{-1}$ となることを証明する. (5.1.2) を導く時と同様に、

$$K(\chi) = K(\chi^5) \tag{6.1.2}$$

となることがわかる. ところで、$K(\chi)$ は χ の値の和と積になる. よって、整数 x に対して $e^{\frac{2\pi\sqrt{-1}x}{12}} = \mathfrak{e}_{12}(x)$ とし、1 以上 12 以下の整数 i に対して $c_i \in \mathbb{Z}$ とした時に、$K(\chi)$ は

$$\begin{aligned} K(\chi) = {} & c_1\mathfrak{e}_{12}(1) + c_2\mathfrak{e}_{12}(2) + c_3\mathfrak{e}_{12}(3) + c_4\mathfrak{e}_{12}(4) \\ & + c_5\mathfrak{e}_{12}(5) + c_6\mathfrak{e}_{12}(6) + c_7\mathfrak{e}_{12}(7) + c_8\mathfrak{e}_{12}(8) \\ & + c_9\mathfrak{e}_{12}(9) + c_{10}\mathfrak{e}_{12}(10) + c_{11}\mathfrak{e}_{12}(11) + c_{12}\mathfrak{e}_{12}(12) \end{aligned}$$

になる. また、この式より、

$$\begin{aligned} K(\chi^5) = {} & c_1\mathfrak{e}_{12}(5) + c_2\mathfrak{e}_{12}(10) + c_3\mathfrak{e}_{12}(3) + c_4\mathfrak{e}_{12}(8) \\ & + c_5\mathfrak{e}_{12}(1) + c_6\mathfrak{e}_{12}(6) + c_7\mathfrak{e}_{12}(11) + c_8\mathfrak{e}_{12}(4) \\ & + c_9\mathfrak{e}_{12}(9) + c_{10}\mathfrak{e}_{12}(2) + c_{11}\mathfrak{e}_{12}(7) + c_{12}\mathfrak{e}_{12}(12) \end{aligned}$$

となることがわかる. よって、

$$\begin{aligned} & K(\chi^5) - K(\chi) \\ & = c_1(\mathfrak{e}_{12}(5) - \mathfrak{e}_{12}(1)) + c_2(\mathfrak{e}_{12}(10) - \mathfrak{e}_{12}(2)) + c_4(\mathfrak{e}_{12}(8) - \mathfrak{e}_{12}(4)) \\ & \quad + c_5(\mathfrak{e}_{12}(1) - \mathfrak{e}_{12}(5)) + c_7(\mathfrak{e}_{12}(11) - \mathfrak{e}_{12}(7)) + c_8(\mathfrak{e}_{12}(4) - \mathfrak{e}_{12}(8)) \\ & \quad + c_{10}(\mathfrak{e}_{12}(2) - \mathfrak{e}_{12}(10)) + c_{11}(\mathfrak{e}_{12}(7) - \mathfrak{e}_{12}(11)) \\ & = (-c_1 + c_5 + c_7 - c_{11})\sqrt{3} + (-c_2 - c_4 + c_8 + c_{10})\sqrt{-3} \\ & = 0 \end{aligned}$$

となる. この式と $c_i \in \mathbb{Z}$ であることより、

$$c_1 - c_5 - c_7 + c_{11} = 0\,,\ c_2 + c_4 - c_8 - c_{10} = 0$$

となることがわかる. よって、$c_1\mathfrak{e}_{12}(1) + c_5\mathfrak{e}_{12}(5) + c_7\mathfrak{e}_{12}(7) + c_{11}\mathfrak{e}_{12}(11)$ は

$$\begin{aligned} & c_1\mathfrak{e}_{12}(1) + c_5\mathfrak{e}_{12}(5) + c_7\mathfrak{e}_{12}(7) + c_{11}\mathfrak{e}_{12}(11) \\ & \quad = (c_1 - c_5 - c_7 + c_{11})\frac{\sqrt{3}}{2} + (c_1 + c_5 - c_7 - c_{11})\frac{\sqrt{-1}}{2} \\ & \quad = (c_1 - c_7)\sqrt{-1} \end{aligned} \tag{6.1.3}$$

になる. また、$c_2\mathfrak{e}_{12}(2) + c_4\mathfrak{e}_{12}(4) + c_8\mathfrak{e}_{12}(8) + c_{10}\mathfrak{e}_{12}(10)$ は

$$\begin{aligned} & c_2\mathfrak{e}_{12}(2) + c_4\mathfrak{e}_{12}(4) + c_8\mathfrak{e}_{12}(8) + c_{10}\mathfrak{e}_{12}(10) \\ & \quad = (c_2 - c_4 - c_8 + c_{10})\frac{1}{2} + (c_2 + c_4 - c_8 - c_{10})\frac{\sqrt{-3}}{2} \\ & \quad = c_2 - c_8 \end{aligned} \tag{6.1.4}$$

になることがわかる.

その結果、(6.1.3) と、(6.1.4) と、$\mathfrak{e}_{12}(3) = \sqrt{-1}$, $\mathfrak{e}_{12}(6) = -1$, $\mathfrak{e}_{12}(9) = -\sqrt{-1}$, $\mathfrak{e}_{12}(12) = 1$ であることより、

$$K(\chi) = (c_2 - c_8) + (-c_6 + c_{12}) + \{(c_1 - c_7) + (c_3 - c_9)\}\sqrt{-1}$$

となる. ゆえに、$c_i \in \mathbb{Z}$ であることより、$\mathbb{Z}$ の元 a_{12} と b_{12} に対して、

$$K(\chi) = a_{12} + b_{12}\sqrt{-1}$$

となることがわかる.

次に、$K(\chi) = \pm K(\chi^3)$ となることを証明する. $K(\chi) = a_{12} + b_{12}\sqrt{-1}$ であること、命題 3.1.3 と、補題 1.2.8 の (4) より、$p = {a_{12}}^2 + {b_{12}}^2$ となる. また、$p \equiv 1\ (12)$ であることより $p \equiv 1\ (4)$ となり、その時、定理 3.1.2 より、$p = {a_4}^2 + {b_4}^2$, $a_4 \equiv -\left(\dfrac{2}{p}\right)\ (4)$ である a_4 と b_4 に対して、$K(\chi^3) = a_4 + b_4\sqrt{-1}$ となる. よって、a_{12} が奇数であることが証明できると、p の表現の一意性から、$a_{12} = \pm a_4$、$b_{12} = \pm b_4$ となる. ゆえに、a_{12} が奇数であることを証明する. $K(\chi) = a_{12} + b_{12}\sqrt{-1}$ であることと、$K(\chi)$ の定義より、

$$(a_{12} - 1) + b_{12}\sqrt{-1} = K(\chi) - 1 = \chi(4)\sum_{n=0}^{p-1}\chi\left(n(1-n)\right) - 1 \tag{6.1.5}$$

となる. また、$\chi(4)\chi\left(n(1-n)\right)$ の n が $\dfrac{p+1}{2}$ である時、

$$\chi(4)\chi\left(\left(\frac{p+1}{2}\right)\left(1 - \frac{p+1}{2}\right)\right) = \chi\left(\,(p+1)(1-p)\,\right) = \chi(1) = 1$$

となることがわかる. よって、(6.1.5) は

$$\chi(4)\sum_{n=0}^{p-1}\chi\left(n(1-n)\right) - 1 = \sum_{n \neq \frac{p+1}{2}}\chi\left(4n(1-n)\right) \tag{6.1.6}$$

になる.

ところで、$\chi\left(4n(1-n)\,\right)$ の n を $1-n$ にすると、$\chi\left(4n(1-n)\,\right)$ となる. よって、$\dfrac{p+1}{2}$ 以外の 0 以上 $p-1$ 以下のある n に対して $\chi\left(n(1-n)\,\right)$ の値は、n が $1-n+p$ である時の値と一緒になる. ゆえに、1 以上 6 以下の整数 i に対して $m_i \in \mathbb{Z}$ であるとすると、(6.1.6) は

$$\begin{aligned}
&2m_1 + m_2(\sqrt{3} + \sqrt{-1}) + m_3(1 + \sqrt{-3}) \\
&\quad + 2m_4\sqrt{-1} + m_5(-1 + \sqrt{-3}) + m_6(-\sqrt{3} + \sqrt{-1}) \\
&\qquad = (2m_1 + m_3 - m_5) + (m_2 + 2m_4 + m_6)\sqrt{-1} \\
&\qquad\quad + (m_2 - m_6)\sqrt{3} + (m_3 + m_5)\sqrt{-3}
\end{aligned}$$

になる. その結果、この式が $(a_{12}-1)+b_{12}\sqrt{-1}$ であることより、$\sqrt{-3}$ の係数である m_3+m_5 は 0 になるので、$m_3=-m_5$ となることがわかる. よって、

$$a_{12}-1=(2m_1+m_3-m_5)=2(m_1-m_5)$$

となり、a_{12} は奇数であることがわかる. ゆえに、$(a_{12},b_{12})=(\pm a_4,\pm b_4)$ または、$(a_{12},b_{12})=(\pm a_4,\mp b_4)$ であることがわかる. なお、$(a_{12},b_{12})=(\pm a_4,\pm b_4)$ である時、$K(\chi)=\pm K(\chi^3)$ となり、$(a_{12},b_{12})=(\pm a_4,\mp b_4)$ である時、$K(\bar{\chi})=\pm K(\chi^3)$ となる.

まず、$K(\bar{\chi})=\pm K(\chi^3)$ となると仮定する. すると、この式は、左辺を $K(\chi)$ の定義と補題 1.2.8 の (3) より、右辺を命題 3.1.3 と補題 1.2.8 の (3) より式変形すると、

$$\bar{\chi}(4)\frac{g^2(\bar{\chi})}{g(\bar{\chi}^2)}=\pm\frac{g^2(\chi^3)}{g(\chi^6)}$$

になる. この式の $g(\chi^6)$ は、補題 1.2.8 の (5) より $p^{\frac{1}{2}}$ になることから、この式の両辺に $p^{\frac{1}{2}}$ をかけると、

$$g^2(\chi^3)=\pm p^{\frac{1}{2}}\bar{\chi}(4)\frac{g^2(\bar{\chi})}{g(\bar{\chi}^2)}$$

となることがわかる. よって、$J^2(\chi,\chi^3)$ は、補題 1.2.8 の (2) と (3) より、

$$J^2(\chi,\chi^3)=\pm\frac{g^2(\chi)g^2(\chi^3)}{g^2(\chi^4)}=\pm\frac{p^{\frac{1}{2}}\bar{\chi}(4)g^2(\bar{\chi})g^2(\chi)}{g^2(\chi^4)g(\bar{\chi}^2)}=\pm\frac{p^{\frac{5}{2}}\bar{\chi}(4)}{g^2(\chi^4)g(\bar{\chi}^2)}$$

になる. この式は、χ の位数の違いに気を付けて (4.2.9) を用いると $g^2(\chi^4)$ を変形出来ることと、$\chi(4)\bar{\chi}(4)=1$ であることと、$\chi^3(4)=\chi^6(2)=\pm1$ であることより、

$$\pm\frac{p^{\frac{5}{2}}\bar{\chi}(4)}{\chi^2(4)p^{\frac{1}{2}}g(\chi^2)g(\bar{\chi}^2)}=\pm p\frac{\bar{\chi}(4)}{\chi^2(4)}=\pm p\frac{1}{\chi^3(4)}=\pm p$$

になることがわかる. よって、$J(\chi,\chi^3)=\pm\sqrt{p}$ または、$\pm\sqrt{-p}$ となる. しかし、$J(\chi,\chi^3)$ と $\sqrt{-1}$ は $\mathbb{Q}(\mathfrak{e}_{12}(1))$ の元であるが、$\sqrt{p}\notin\mathbb{Q}(\mathfrak{e}_{12}(1))$ であることより、矛盾する. その結果、$K(\bar{\chi})=\pm K(\chi^3)$ ではないことがわかる. ゆえに、$K(\chi)=\pm K(\chi^3)$ となる.

最後に、$3\mid a_4$ である時に $K(\chi)=-K(\chi^3)$ となることと、$3\nmid a_4$ である時に $K(\chi)=K(\chi^3)$ となることを証明する. そのために、$\epsilon=\pm1, K(\chi)=\epsilon K(\chi^3)$ であるとして、$3\mid a_4$ である時に $\epsilon=-1$ となることと、$3\nmid a_4$ である時に $\epsilon=1$ となることを証明する. $K(\chi)=\epsilon K(\chi^3)$ の両辺を 3 乗すると、左辺は、

$$K^3(\chi)\equiv K(\chi^3)\quad(\,3\mathbb{Q}(\mathfrak{e}_{12}(1))\,)$$

になる. 同様に、右辺は $\epsilon K^3(\chi^3)\equiv\epsilon K(\chi^9)\quad(\,3\mathbb{Q}(\mathfrak{e}_{12}(1))\,)$ になる. よって、$\chi^9=\bar{\chi}^3$ であることより、

$$K(\chi^3)\equiv\epsilon K(\bar{\chi}^3)\quad(\,3\mathbb{Q}(\mathfrak{e}_{12}(1))\,)$$

となることがわかる. ゆえに、$K(\chi^3) = a_4 + b_4\sqrt{-1}$ であることより、

$$(1-\epsilon)a_4 + (1+\epsilon)b_4\sqrt{-1} \equiv 0 \quad (\,3\mathbb{Q}\,(\mathbb{e}_{12}(1))\,)$$

となる. その結果、$(1-\epsilon)a_4$ と $(1+\epsilon)b_4$ の両方が 3 で割り切れなければならない. また、$p = {a_4}^2 + {b_4}^2$ であることより、a_4 と b_4 の両方が 3 で割り切れることはない. よって、

$$3 \mid a_4 \Rightarrow 3 \nmid b_4 \Rightarrow \epsilon = -1$$

となる. また、

$$3 \nmid a_4 \Rightarrow \epsilon = 1$$

となることがわかる. □

6.2 証明の準備２

この節では、G_{12} を計算する. 次の定理が G_{12} を計算した定理である.

定理 6.2.1. 次の式が成り立つ.

$$G_{12} = G_6 + R_6 \pm p^{-\frac{1}{2}} G_3 \left\{ 2\left(\frac{2}{p}\right)(p + a_{12}p^{\frac{1}{2}}) \right\}^{\frac{1}{2}}.$$

証明. まず、G_{12} を定義から考える. すると、命題 2.2.4 と、$\sum_{t=0}^{p-1} \mathbb{e}(t) = 0$ であることを使う. すると、$\chi^{11} = \bar{\chi}\,, \chi^9 = \bar{\chi}^3\,, \chi^7 = \bar{\chi}^5$ となることと、R_i の定義より、

$$\begin{aligned} G_{12} &= \sum_{t=0}^{p-1} \mathbb{e}(t) \left(\sum_{i=1}^{11} \chi^i(t) \right) \\ &= \big(g(\chi^2) + g(\chi^4) + g(\chi^6) + g(\chi^8) + g(\chi^{10}) \big) + \big(g(\chi^3) + g(\bar{\chi}^3) \big) \\ &\quad + \big(g(\chi) + g(\bar{\chi}) \big) + \big(g(\chi^5) + g(\bar{\chi}^5) \big) \\ &= G_6 + R_6 + R_2 + R_{10} \end{aligned}$$

となる. よって、$R_2 + R_{10}$ を求めればよい. そのために、$(R_2 + R_{10})^2$ を求める.

まず、${R_2}^2$ 求める. 補題 1.2.8 の (2) と (3) と、$K(\chi)$ の定義より、

$$\begin{aligned} {R_2}^2 &= g^2(\chi) + g^2(\bar{\chi}) + 2g(\chi)g(\bar{\chi}) \\ &= g(\chi^2)\bar{\chi}^2(2)K(\chi) + g(\bar{\chi}^2)\chi^2(2)K(\bar{\chi}) + 2\chi(-1)p \end{aligned}$$

となることがわかる. また、R_2 の χ を χ^5 にすれば R_{10} を求めることが出来て、$(\chi^5)^2 = \bar{\chi}^2\,, (\bar{\chi}^5)^2 = \chi^2$ であることと、$\chi^5(-1) = \chi^4(-1)\chi(-1) = \chi(-1)$ であることより、

$${R_{10}}^2 = g(\bar{\chi}^2)\chi^2(2)K(\chi^5) + g(\chi^2)\bar{\chi}^2(2)K(\bar{\chi}^5) + 2\chi(-1)p$$

となる．ところで、(5.1.2) と同様に、$K(\chi) = K(\chi^5)$ となる．また、この式の χ を $\bar{\chi}$ にすると、$K(\bar{\chi}) = K(\bar{\chi}^5)$ となることがわかる．よって、定理 6.1.1 と、$\overline{g(\chi^2)} = \chi^2(-1)g(\bar{\chi}^2) = g(\bar{\chi}^2)$ であることより、

$$\begin{aligned} {R_2}^2 + {R_{10}}^2 &= \left\{g(\chi^2)\bar{\chi}^2(2) + g(\bar{\chi}^2)\chi^2(2)\right\}\left\{K(\chi) + K(\bar{\chi})\right\} + 4\chi(-1)p \\ &= 4a_{12}\mathrm{Re}\left\{\bar{\chi}^2(2)g(\chi^2)\right\} + 4\chi(-1)p \end{aligned} \tag{6.2.2}$$

となることがわかる．

次に、$2R_2R_{10}$ を求める．$2R_2R_{10}$ は

$$\begin{aligned} 2R_2R_{10} &= 2\left(g(\chi) + g(\bar{\chi})\right)\left(g(\chi^5) + g(\bar{\chi}^5)\right) \\ &= 2\left(g(\chi)g(\chi^5) + g(\chi)g(\bar{\chi}^5) + g(\bar{\chi})g(\chi^5) + g(\bar{\chi})g(\bar{\chi}^5)\right) \end{aligned}$$

になるので、この 4 つの項を求める．

まず、$g(\chi)g(\chi^5)$ を求める．命題 4.1.2 の (2) の両辺に $\chi(-1)$ をかけると、$\chi^2(-1) = \chi(1) = 1$ であることより $J(\chi, \chi^5) = \chi(-1)K(\chi)$ となることと、補題 1.2.8 の (3) より、$g(\chi)g(\chi^5)$ は

$$g(\chi)g(\chi^5) = g(\chi^6)J(\chi, \chi^5) = p^{\frac{1}{2}}\chi(-1)K(\chi) \tag{6.2.3}$$

になる．また、$g(\chi)g(\chi^5)$ の χ を $\bar{\chi}$ にすれば $g(\bar{\chi})g(\bar{\chi}^5)$ を求めることが出来て、$\chi(-1) = \pm 1$ であることより、$\bar{\chi}(-1) = \chi(-1)$ となるので、

$$g(\bar{\chi})g(\bar{\chi}^5) = p^{\frac{1}{2}}\chi(-1)K(\bar{\chi})$$

となることがわかる．

次に、$g(\bar{\chi})g(\chi^5)$ を求める．(6.2.3) の両辺に $\dfrac{g(\bar{\chi})}{g(\chi)}$ をかけて、$K(\chi)$ の定義と、補題 1.2.8 の (2) と (3) より、

$$\begin{aligned} g(\bar{\chi})g(\chi^5) &= p^{\frac{1}{2}}\chi(-1)\chi(4)\frac{g^2(\chi)}{g(\chi^2)}\frac{g(\bar{\chi})}{g(\chi)} \\ &= p^{\frac{1}{2}}\chi^2(2)\frac{\chi^2(-1)p}{g(\chi^2)} \\ &= p^{\frac{1}{2}}\chi^2(2)g(\bar{\chi}^2) \end{aligned}$$

となる．また、$g(\bar{\chi})g(\chi^5)$ の χ を $\bar{\chi}$ にすれば $g(\chi)g(\bar{\chi}^5)$ を求めることが出来て、

$$g(\chi)g(\bar{\chi}^5) = p^{\frac{1}{2}}\bar{\chi}^2(2)g(\chi^2)$$

となることがわかる．

よって、$2R_2R_{10}$ を求めることが出来て、定理 6.1.1 と、$g(\bar{\chi}^2) = \overline{g(\chi^2)}$ であることより、

$$\begin{aligned} 2R_2R_{10} &= 2p^{\frac{1}{2}}\left(\chi(-1)K(\chi) + \bar{\chi}^2(2)g(\chi^2) + \chi^2(2)g(\bar{\chi}^2) + \chi(-1)K(\bar{\chi})\right) \\ &= 2p^{\frac{1}{2}}\left(2\chi(-1)a_{12} + 2\mathrm{Re}\left\{\bar{\chi}^2(2)g(\chi^2)\right\}\right) \end{aligned} \tag{6.2.4}$$

となる.

その結果、$(R_2+R_{10})^2$ を求めることが出来て、(6.2.2) と (6.2.4) より、

$$\begin{aligned}(R_2+R_{10})^2 &= \left(4a_{12}\mathrm{Re}\left\{\bar{\chi}^2(2)g(\chi^2)\right\}+4\chi(-1)p\right)\\ &\quad+\left\{2p^{\frac{1}{2}}\left(2\chi(-1)a_{12}+2\mathrm{Re}\left\{\bar{\chi}^2(2)g(\chi^2)\right\}\right)\right\}\\ &=(2a_{12}+2p^{\frac{1}{2}})\left(2\mathrm{Re}\left\{\bar{\chi}^2(2)g(\chi^2)\right\}+2\chi(-1)p^{\frac{1}{2}}\right)\end{aligned} \tag{6.2.5}$$

となることがわかる. この式の $2\mathrm{Re}\{\bar{\chi}^2(2)g(\chi^2)\}$ は、χ の位数の違いに気を付けて命題 4.2.5 を用いると式変形出来ることと、$\bar{\chi}^6(2)=\left(\frac{2}{p}\right)$ であることと定義 1.2.7 の (4) より、

$$2\mathrm{Re}\left\{\bar{\chi}^2(2)g(\chi^2)\right\}=p^{-\frac{1}{2}}\left(\frac{2}{p}\right)({G_3}^2-2p) \tag{6.2.6}$$

になる.

最後に、$\chi(-1)=\left(\frac{2}{p}\right)$ であることを証明する. 定理 5.2.1 の証明で、$p=1+8k$ である時に $\chi(-1)=(-1)^k$ となることを証明したことと同様に、$p=1+12k$ である時に $\chi(-1)=(-1)^k$ となる. ところで、[6, Proposition 5.1.3.] より、$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ である. よって、$p=1+12k$ である時に $(-1)^{\frac{p^2-1}{8}}=(-1)^k$ となる. ゆえに、

$$\chi(-1)=\left(\frac{2}{p}\right) \tag{6.2.7}$$

となる. その結果、(6.2.5) と、(6.2.6) と、(6.2.7) より、

$$\begin{aligned}(R_2+R_{10})^2&=(2a_{12}+2p^{\frac{1}{2}})\left\{p^{-\frac{1}{2}}\left(\frac{2}{p}\right)({G_3}^2-2p)+2\left(\frac{2}{p}\right)p^{\frac{1}{2}}\right\}\\ &=2(a_{12}+p^{\frac{1}{2}})\,p^{-\frac{1}{2}}\left(\frac{2}{p}\right){G_3}^2\\ &=2p^{-\frac{1}{4}}{G_3}^2\left(\frac{2}{p}\right)(p+a_{12}p^{\frac{1}{2}})\end{aligned}$$

となる. □

6.3 Whiteman の定理の証明

この節では、Whiteman の定理を証明する.

定理 6.0.1 の証明. $H_{12}\cup\{0\}$ は H_{12} と同様に証明出来るので、H_{12} だけの証明をやる.

まず、命題 2.2.1 を使う. すると、$k=12$ であることより、$p\equiv 1\ (24)$ となる時、H_{12} は difference set ではないということがわかる. よって、$p\equiv 13\ (24)$ である時を考え

る. すると、定理 4.2.2 と定義 1.2.7 の (4) より、次の式が成り立つ. 2 が p を法として cubic residue である時、

$$G_6 = G_3 + p^{-\frac{1}{2}}({G_3}^2 - p).$$

2 が p を法として cubic nonresidue である時、

$$G_6 = G_3 + \frac{1}{2}p^{-\frac{1}{2}}\left\{(4p - {G_3}^2) + \epsilon_6 G_3(12p - 3{G_3}^2)^{\frac{1}{2}}\right\}.$$

また、[6, Proposition 5.1.3.] で証明されている $p \equiv 5\ (8)$ である時に、$\left(\dfrac{2}{p}\right) = -1$ であることと、(3.2.7) と、定理 6.2.1 より、

$$G_{12} = G_6 \pm \left\{(2p + 2a_4 p^{\frac{1}{2}})^{\frac{1}{2}} \pm p^{-\frac{1}{2}} G_3(2p + 2a_{12}p^{\frac{1}{2}})^{\frac{1}{2}}\right\}\sqrt{-1}$$

となる. a_{12} は定理 6.1.1 より、$3 \nmid a_4$ である時に $a_{12} = a_4$ であり、$3 \mid a_4$ である時に $a_{12} = -a_4$ である. よって、$3 \nmid a_4$ である時に、

$$G_{12} = G_6 \pm (2p + 2a_4\, p^{\frac{1}{2}})^{\frac{1}{2}}(1 \pm p^{-\frac{1}{2}} G_3)\sqrt{-1}$$

となり、$3 \mid a_4$ である時に、$p = {a_4}^2 + {b_4}^2$ であることより、

$$\begin{aligned} G_{12} &= G_6 \pm (2p + 2a_4\, p^{\frac{1}{2}})^{\frac{1}{2}}\left\{1 \pm p^{-\frac{1}{2}} G_3(p - a_4\, p^{\frac{1}{2}})^{\frac{1}{2}}(p + a_4\, p^{\frac{1}{2}})^{-\frac{1}{2}}\right\}\sqrt{-1} \\ &= G_6 \pm (2p + 2a_4\, p^{\frac{1}{2}})^{\frac{1}{2}}\left\{1 \pm (pb_4)^{-1} G_3(p - a_4\, p^{\frac{1}{2}})\right\}\sqrt{-1} \end{aligned}$$

となる. ここで、G_{12} をまとめるために、V を次のように定義する.

$$V = \begin{cases} 1 \pm p^{-\frac{1}{2}} G_3 & 3 \nmid a_4, \\ 1 \pm (pb_4)^{-1} G_3(p - a_4 p^{\frac{1}{2}}) & 3 \mid a_4. \end{cases}$$

すると、G_{12} は、

$$G_{12} = G_6 \pm V(2p + 2a_4 p^{\frac{1}{2}})^{\frac{1}{2}}\sqrt{-1} \tag{6.3.1}$$

になる. ちなみに、定理 4.2.3 より $G_3 \in \mathbb{R}$ であるので、$V \in \mathbb{R}$ である. この式を使って、$|\, G_{12} - 1\,|^2$ を求める.

2 が p を法として cubic nonresidue である時は、2 が p を法として cubic residue である時と同様に証明出来るので、2 が p を法として cubic residue である時だけの証明をする. $p \equiv 13\ (24)$ である時に $G_6 \in \mathbb{R}$ であることと、定理 4.2.3 より ${G_3}^3 = 3pG_3 + pr_3$ であることを用いて、$|\, G_{12} - 1\,|^2$ を計算し、${G_3}^4$ と ${G_3}^3$ を消すと、

$$\begin{aligned} |\, G_{12} - 1\,|^2 &= |\, (G_6 - 1) \pm V(2p + 2a_4 p^{\frac{1}{2}})^{\frac{1}{2}}\sqrt{-1}\,|^2 \\ &= (2 - 2p^{-\frac{1}{2}}){G_3}^2 + (4p^{\frac{1}{2}} + r_3 - 2)G_3 \\ &\quad + p + 2p^{\frac{1}{2}} + 2r_3 p^{\frac{1}{2}} + 1 + V^2(2p + 2a_4 p^{\frac{1}{2}}) \end{aligned}$$

となる. この式の V^2 は $3 \mid a_4$ である時も $3 \nmid a_4$ である時も、G_3 の 2 次式になる. よって、$\mid G_{12} - 1 \mid^2$ は $\mathbb{Z}[\, p^{\frac{1}{2}} \,]$ 上の G_3 の 2 次式になることがわかる.

ところで、H_{12} が difference set であると仮定して基本定理の (1) を用いると、

$$\mid G_{12} - 1 \mid^2 = 11p + 1$$

となる. また、補題 4.2.4 にある $x^3 - 3px - pr_3$ は $\mathbb{Z}[\, p^{\frac{1}{2}} \,]$ 上でも既約であることがわかる. よって、$\mid G_{12} - 1 \mid^2$ に対する 2 つの式をまとめた式は、${G_3}^2$ の係数も、G_3 の係数も、定数項も 0 でないと矛盾してしまう. 定数項を見ると、

$$\begin{aligned}(p + 2p^{\frac{1}{2}} + 2r_3p^{\frac{1}{2}} + 1) + (2p + 2a_4p^{\frac{1}{2}}) - (11p + 1)& \\ = -8p + 2p^{\frac{1}{2}}(a_4 + r_3 + 1)&\end{aligned}$$

となる. この式は $a_4 + r_3 + 1 \in \mathbb{Z}$ であることより、0 になることはない. よって、仮定が矛盾する. □

ちなみに、$p = 13$ である時に、$H_{12} = \{1\}$ となり $H_{12} \cup \{0\} = \{0, 1\}$ となる. よって、H_{12} は difference set であるが、この論文では 1 つの元からなる difference set を考えていない. また、$H_{12} \cup \{0\}$ は difference set ではない.

関連図書

[1] L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets,* Math. Comp. **21**(1967), 204–219.

[2] Bruce C. Berndt and Ronald J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal,* J. Number Theory **11** (1979), 349–398.

[3] S. A. Chowla, *A property of biquadratic residues,* Proc. Nat. Acad. Sci. India. Sect. A. **14** (1944), 45–46.

[4] Ronald J. Evans, *Bioctic Gauss sums and sixteenth power residue difference sets,* Acta Arith. **38** (1980), 37–46.

[5] Ronald J. Evans *Twenty-fourth power residue difference sets,* Math. Comp. **40** (1983), 677–683.

[6] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, second edition, 1990.

[7] Emma Lehmer, *On residue difference sets,* Canadian J. Math. **5** (1953), 425–432.

[8] J. B. Muskat, *The cyclotomic numbers of order fourteen,* Acta Arith. **11** (1966), 263–279.

[9] Joseph B. Muskat and Albert L. Whiteman, *The cyclotomic numbers of order twenty,* Acta Arith. **17** (1970), 185–216.

[10] Udo Ott, *Sharply flag-transitive projective planes and power residue difference sets,* J. Algebra **276** (2004), 663–673.

[11] A. L. Whiteman, *The cyclotomic numbers of order twelve,* Acta Arith. **6** (1960), 53–76.

[12] Albert Leon Whiteman, *The cyclotomic numbers of order sixteen* Trans. Amer. Math. Soc. **86** (1957), 401–413.

[13] Albert Leon Whiteman, *The cyclotomic numbers of order ten,* American Mathematical Society, Providence, R.I., 1960.

[14] Pingzhi Yuan and Hu Yahui, *A note on power residue difference sets,* J. Algebra **291** (2005), 269–273.