数理解析研究所講究録
第1625巻2009年56-66

ガウスの4次剰余の理論について(1)

九州大学大学院・数理学府博士課程院生　伊波 靖 (Yasushi Iha)
Graduate School of Mathematics
Kyushu University

1. はじめに

この論文では,ガウスの数論の核心部分である冪剰余理論の論文の中でも,特に,1828年発表の「4次剰余の理論・第1論文 (Theoria residuorum biquadraticorum Commentatio prima , Werke , volume : bd. 2 pp.67-91)」と1832年発表の「4次剰余の理論・第2論文」(Theoria residuorum biquadraticorum Commentatio secunda,Werke, volume : bd. 2 pp.95-148) の内容を紹介し,所見を述べることを目的としています.

2. 4次剰余理論の成立過程

1805年

この年,3次及び4次剰余の理論の研究を始める.(「4次剰余の理論・第1論文より」)

1807年

2月15日,3次及び4次剰余に関する理論の研究を始める.(「ガウスの数学日記」より)特に,ガウスによるとこのとき既に3次と4次に関する何らかの相互法則を発見している.証明はこの時点では未完である.

1813年

10月23日.この日,ガウスによると4次剰余相互法則が完成したと述べている.

1814年

7月9日.ガウスは帰納的に行われる極めて重要な観察を通じて,4次剰余の理論はレムニスケート関数と極めて優美に結びついていることを発見した.

1825年

4月5日.「4次剰余の理論・第1論文」の概容である「4次剰余の理論・要約I」(Theoria residuorum biquadraticorum Comm I ,Werke, volume : bd. 2 pp.165-168) をゲッチンゲン王立協会の雑誌で発表.

1828年

「4次剰余の理論・第1論文」を発表.この論文の中でガウスは自らが発見した4次剰余

の第１及び第２補充法則の証明を行った.

1831 年

4月 15 日,「4次剰余の理論・第2論文」の要約である「4次剰余の理論・要約Ⅱ」(Theoria residuorum biquadraticorum Comm Ⅱ,Werke, volume : bd. 2 pp.169-178) をゲッチンゲン王立協会の雑誌で発表.

1832 年

「4次剰余の理論・第2論文」を発表. この論文の中でガウスは4次剰余相互法則を帰納的に定式化 (第 67 条) したが, 証明は与えなかった. この論文では4次剰余の第2補充法則Ⅲの定式化 (第 63 条) と証明 (第 68〜76 条) を行った. 又, この論文でガウス整数が導入され, 数論の領域が広がった. (ガウス整数に関する記述は, 第 30 条〜57 条参照)

3. 第1論文 (第1条〜第 23 条) の内容について

先ず, ガウスは第5条において次のようなあつまり A,B,C,D を考えた. あつまり A は1と $p-1$ の間にある $4k+1$ 型の素数 p の全ての4次剰余のあつまりとし, その上 e は無作為に抽出された $4k+1$ 型の素数 p の平方非剰余とする. つまり, e は1と $p-1$ の間にある p の平方非剰余ならば何でも良い. さらに, あつまり B は法 p に関して積 eA から生じる正の最小剰余のあつまりとする. 同様に, あつまり C は法 p に関して積 e^2A から生じる正の最小剰余のあつまりとし, あつまり D は法 p に関して積 e^3A から生じる正の最小剰余のあつまりとする.

したがって, 二つの4次剰余の積は明らかに4次剰余である. 言い換えると, あつまり A の二つの数の積から常にその正の最小剰余が同じあつまり A に所属するような積が生じる. 同様に B の数と D の数の積, あるいは C の数同士の積はその積の最小剰余を A の中に持つ. さらに, 積 AB と積 CD の最小剰余はあつまり B の中の数になる. 同様に積 AC, 積 BB, 積 CD の最小剰余はあつまり C の中の数になる. 積 AC, 積 BB, 積 DD の最小剰余はあつまり C の中の数になる. 最後に, 積 AD と積 BC の最小剰余はあつまり D の中の数になることを第7条で示した. 以上をまとめると次の表 3.1 のようになる.

	A	B	C	D
A	A	B	C	D
B	★	C	D	A
C	★	★	A	B
D	★	★	★	C

(表 3.1)

そしてこのときガウスは, 第8条においてあつまり A,B,C,D の要素を p の原始根 g を用いて, 次の表 3.2 のように表した.

	最小剰余数
A	$1 , g^4 , g^8 , g^{12} , \cdots\cdots , g^{p-5}$
B	$g , g^5 , g^9 , g^{13} , \cdots\cdots , g^{p-4}$
C	$g^2 , g^6 , g^{10} , g^{14} , \cdots\cdots , g^{p-3}$
D	$g^3 , g^7 , g^{11} , g^{15} , \cdots\cdots , g^{p-2}$

(表 3.2)

このとき,

$$1 \ , \ g \ , \ g^2 \ , \ g^3 \ , \ \cdots\cdots \ , \ g^{p-4} \ , \ g^{p-3} \ , \ g^{p-2}$$

の正の最小剰余は, 順序を別にして

$$1 \ , \ 2 \ , \ 3 \ , \ 4 \ , \ \cdots\cdots \ , \ p-3 \ , \ p-2 \ , \ p-1$$

のどれかと一致する. したがって, 逆に考えると

$$1 \ , \ 2 \ , \ 3 \ , \ 4 \ , \ \cdots\cdots \ , \ p-3 \ , \ p-2 \ , \ p-1$$

は全て上の表 3.2 のように, あつまり A,B,C,D という 4 つの類のいずれかに配分される. したがって,p で割り切れない任意の整数を, 法 p に関する最小剰余の「物差し」を基準として考えると, これらのあつまり A,B,C,D という 4 つの類のいずれかに確実に配分できる.

そして, ガウスは次の記念碑的な「**ガウスの 4 次剰余の第 1 補充法則**」を導き, 第 9 条において証明した.

定理 3.1　ガウスの 4 次剰余の第 1 補充法則

p が $8n+1$ 型の素数ならば常に -1 はあつまり A に所属する. つまり -1 は 4 次剰余になり,p が $8n+5$ 型の素数ならば常に -1 はあつまり C に所属する.

ガウスは更に, 次の著しく優雅でかつ単純な定理（4 次の第 2 補充法則 I）を発見し, 第 12 条で示し, 第 13 条でその証明を行った.

定理 3.2　ガウスの 4 次剰余の第 2 補充法則 I

p は $4k+1$ 型の素数で

$$p = a^2 + b^2$$

と分解され,a が奇数で,b が偶数のとき, 次が成立する.

a が $8m+1$ 型又は $8m+7$ 型になるたびに, 数 2 はあつまり A に含まれ, 反対に,a が $8m+3$ 型 又は $8m+5$ 型になるたびに, 数 2 はあつまり C に含まれる.

最後に, 第 14 条〜第 21 条においてガウスは次の定理 3.3 を得た.

定理 3.3　ガウスの 4 次剰余の第 2 補充法則 II

p は $4k+1$ 型の素数で $p = a^2 + b^2$ と分解され,a が奇数で,b が偶数のとき, 次が成立する.

$\frac{1}{2}b$ が $4m$ 型,$4m+1$ 型,$4m+2$ 型,$4m+3$ 型になるのかに応じて,2 はそれぞれ, あつまり A,B,C,D に所属する.

以上のことより, ガウスが「4 次剰余の理論・第 1 論文」において, 強調したかったのは, 合同式

$$x^4 \equiv -1 \pmod p \quad , \quad x^4 \equiv 2 \pmod p$$

の解の存在の判定や解そのものを求めることではないことが分かる. ガウスがこの論文で問題としたことは, 実は

−1 や 2 があつまり A,B,C,D にどのように配分されるのか?

ということである. つまり,

非 4 次剰余の世界を更に B,C,D に細分したこと

が最大のアイディアであり発見であった.

4.　第 2 論文 (第 24 条〜第 76 条) の内容について

ガウスは第 36 条において,primary に関して次のように述べている.

4 つの随伴奇複素数の内, 法 $2+2i$ に関して 1 と合同であるもの

つまり, ガウスは次のように primary を定義した.

定義 4.1　ガウスの 4 次剰余の primary

α を複素数とすると,α が primary とは, 次の合同式を満たすことである.

$$\alpha \equiv 1 \pmod{2+2i}$$

上のことから次が出てくる. つまり,$\alpha = a + bi$ が primary ならば

$$a \equiv 1 \pmod 4 \quad かつ \quad b \equiv 0 \pmod 4$$

あるいは

$$a \equiv 3 \pmod 4 \quad \text{かつ} \quad b \equiv 2 \pmod 4$$

つまり,α を $1+i$ 以外の素数とすると, その随伴数のうちに, ただ一つだけ primary が存在する.

又, ガウスは第 37 条で, ガウス整数域における素元分解の一意性定理が成り立つことを示し, 第 51 条で次のような, フェルマーの小定理のガウス整数への拡張を行った.

定理 4.1　フェルマーの小定理のガウス整数への拡張

k はそのノルムが p に等しい法 $m=a+bi$ で割れないガウス整数を表すとすると,

$$k^{p-1} \equiv 1 \pmod m$$

となる. ここで,$p=a^2+b^2$ である.

そして, ガウスは素元分解の一意性定理により, 次のような因数分解が成立することと,

$$k^{p-1}-1=\left(k^{\frac{1}{4}(p-1)}-1\right)\left(k^{\frac{1}{4}(p-1)}-i\right)\left(k^{\frac{1}{4}(p-1)}+1\right)\left(k^{\frac{1}{4}(p-1)}+i\right)$$

定理 4.1 を用いて, 第 61 条において, 次のように 4 次指標を定義した. 数 k の法 m に関する指標 λ を,

数 $k^{\frac{1}{4}(p-1)}$ が合同な i の冪の指数であるように定義する

つまり, 現代的な表記で分かりやすく書くと次のように定義される.

定義 4.2　4 次指標 (characteres biquadraticos)

$m=a+bi$ は $\mathbb{Z}[i]$ の素元,$(m)\neq(1+i)$,　$m \nmid k$ となる $k\in\mathbb{Z}[i]$ に対し

$$k^{\frac{1}{4}(p-1)} \equiv i^{\lambda} \pmod m$$

となる $\lambda=0,1,2,3$ が一意に決まる. ここで,$p=a^2+b^2$

そして, ガウスは「ある原始根を底に取ると,4 次剰余は,4 で割れる. 或いは,$4n$ 形の指数 (index) を持つ. 平方剰余であるような 4 次非剰余は $4n+2$ 型の指数を持つ. 最後に, 平方非剰余の指数は, 一部は $4n+1$ 型であり, 一部は $4n+3$ 型である. このようにして, 確かに,4 つの類が生じる.」ことに注目した. しかし, 後者の 2 つの類の区別は絶対的ではなく, 採用された原始根の選択に依存している. 何故ならば, 原始根の半分に対しては, 与えられた平方非剰余は $4n+1$ 型の指数を持つが, 他の半分に対しては,$4n+3$ 型の指数を持つことが容易に分かるからである. そのため, ガウスはこのような 2 意性を除くために, 原始根 g は, その法 m に対して指数

$$\frac{1}{4}(p-1)$$

が $+i$ になるものを採用した. つまり,

$$g^{\frac{1}{4}(p-1)} \equiv i \pmod m$$

この条件により, ガウスは指標の族の定義を, 原始根に依拠せずに, 法 m で次のように定義することができた.

定義 4.3　4 次指標 (characteres biquadraticos) の族 (Classis) の定義
第 1 族は,$k^{\frac{1}{4}(p-1)} \equiv 1$ となるような数を含む. つまり, 4 次指標 $\lambda = 0$.
第 2 族は,$k^{\frac{1}{4}(p-1)} \equiv i$ となるような数を含む. つまり, 4 次指標 $\lambda = 1$.
第 3 族は,$k^{\frac{1}{4}(p-1)} \equiv -1$ となるような数を含む. つまり, 4 次指標 $\lambda = 2$.
第 4 族は,$k^{\frac{1}{4}(p-1)} \equiv -i$ となるような数を含む. つまり, 4 次指標 $\lambda = 3$.

この定義 4.3 はオイラーの規準のガウス整数への拡張になっている. そして, あつまり A,B,C,D という分け方から, **族 1,2,3,4 という分け方に変える**ことにより, フェルマーの小定理の拡張 (定理 4.1) とこのオイラーの規準の拡張を結びつけたことはガウスの発見である.

そして, 指標に関して数多くの計算をし, 帰納法により, ついにガウスは第 63 条において次のような, 補充法則を示し, 第 68 条〜76 条で証明した.

定理 4.2　ガウスの 4 次剰余の第 2 補充法則 III
全ての素な随伴数のうちで primary な法 $m = a + bi$ に関する数 $1 + i$ の指標 λ は

$$\lambda \equiv \frac{1}{4}(a - b - 1 - b^2) \pmod 4$$

となる. つまり, 次が成立する.

$$(1+i)^{\frac{1}{4}(p-1)} \equiv i^{\frac{1}{4}(a-b-1-b^2)} \pmod m$$

ここで,$p = a^2 + b^2$ である.

そして, 第 67 条において, 次の 4 次剰余の基本定理（4 次剰余相互法則）を示した. しかし, 証明は行っていない

定理 4.3　4 次剰余の基本定理 (Theorema fundamentale theoriae residuorum biquadaticorum)
$a + bi$, $a' + b'i$ は, それらの随伴数の内で primary であるような, すなわち, 法 $2 + 2i$ に関して 1 と合同であるような素数を表すとしよう. このとき,2 つの数 $a + bi$, $a' + b'i$ の両方とも, 或いは少なくとも一方が第 1 種の法 ($a \equiv 1$, $b \equiv 0 \pmod{4}$) に属するならば, すなわち法 4 に関して

$$\equiv 1$$

ならば,数 $a+bi$ の法 $a'+b'i$ に関する４次剰余指標は,数 $a'+b'i$ の法 $a+bi$ に関する指標と一致する．それに対して,2つの数 $a+bi$, $a'+b'i$ がいずれも第１種の法 ($a \equiv 1, b \equiv 0 \pmod{4}$) に属さないならば,すなわち,両方とも法４に関して

$$\equiv 3+2i$$

とすれば,これらの指標は２だけ相異なる[注1]．

(注１)

「指標は２だけ相異なる」とは，４次指標 λ は

$$\lambda = 0, 1, 2, 3$$

なので,このとき, i^{λ} において２異なるのは,例えば,一方が $\lambda = 1$ ならば,他方は $\lambda = 3$ になり,もし一方が $\lambda = 0$ ならば,他方は $\lambda = 2$ になるということである．

４次剰余の基本定理を式で説明すると次のようになる．ここで, λ, λ' はそれぞれ, $a+bi$ の法 $a'+b'i$ に関する指標と $a'+b'i$ の法 $a+bi$ に関する指標とする．

$$(a+bi)^{\frac{1}{4}(p-1)} \equiv i^{\lambda} \pmod{a'+b'i} \quad \cdots\cdots ①式$$

$$(a'+b'i)^{\frac{1}{4}(p'-1)} \equiv i^{\lambda'} \pmod{a+bi} \quad \cdots\cdots ②式$$

つまり,少なくとも一方が第１種の法の場合は,①式の λ と②式の λ' が等しくなり,例えば, $\lambda = 2$ の場合は, $\lambda' = 2$ になる．両方とも第１種の法に属さない場合は,①式の λ と②式の λ' が２異なるので,例えば, $\lambda = 1$ の場合は, $\lambda' = 3$ になる．

以上より分かることは，４次剰余の場合も平方剰余の場合と同じ道筋を歩いているということである．つまり,フェルマーの小定理を一般化して４次指標に着目するところである．この段階では,まだ４次剰余の基本定理とは関係は薄い．しかし,ガウスは最初から平方剰余の基本定理と同じ理論展開で４次剰余の基本定理を構築できることを予想していたと考えられる．しかし,平方剰余の基本定理と異なり,４次剰余の基本定理の平方剰余の基本定理と同様な単純な構造を構築するプロセスは困難を極めた．４次剰余相互法則構築にガウスが時間が掛かった理由は様々考えられる．例えば,ガウスが「非ユークリッド幾何学の構築」に打ち込んでいたことや,当時ガウスは測量を実施するために多くの時間を取られていたことなどが挙げられる．しかし,最大の理由は「数域の拡張が困難」だったからだと考えられる．

又,ここで,どの部分に「**４次剰余の相互性**」があるのかを説明する．今,

$$m = a+bi \quad , \quad n = a'+b'i$$

とする. このとき, もし2つの数 $a+bi$, $a'+b'i$ の両方とも, 或いは少なくとも一方が第1種の法 ($a \equiv 1$, $b \equiv 0 \pmod{4}$) に属するならば, すなわち法4に関して

$$\equiv 1$$

ならば, 数 $a+bi$ の法 $a'+b'i$ に関する4次剰余指標は, 数 $a'+b'i$ の法 $a+bi$ に関する指標と一致する. 従って, 例えば, m が第1族ならば, n の第1族が決定する. もし, m が第2族ならば, もちろん n も第2族になる.

又, 2つの数 $a+bi$, $a'+b'i$ がいずれも第1種の法 ($a \equiv 1$, $b \equiv 0 \pmod{4}$) に属さないならば, すなわち, 両方とも法4に関して

$$\equiv 3+2i$$

とすれば, これらの指標は2だけ相異なる. 従って, 例えば, m が第1族ならば, n の第3族が決定する. もし, m が第2族ならば, もちろん n は第4族になる. つまり, 第1族, 第2族, 第3族, 第4族のいずれに属するのかは, 一方が決まれば, 他方も決まるところに「**4次剰余の相互性**」がある. ガウスの関心は4次の合同式を解くことよりも, 4次剰余の相互性そのものに関心があったと考えられる.

5. ガウスの4次剰余相互法則と現代的な表記法との関係について

結論からいえば, ガウスの4次剰余相互法則は, 次の現代的な表記法による4次剰余相互法則そのものである.

定理 5.1　現代的な表記法による4次剰余相互法則

m, n を $\mathbb{Z}[i]$ の primary な素数とし,

$$(m) \neq (1+i) \quad , \quad (n) \neq (1+i) \quad , \quad (m) \neq (n)$$

のとき次が成立する.

$$\left(\frac{m}{n}\right)_4 = (-1)^{\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1)} \left(\frac{n}{m}\right)_4$$

以下でその理由を説明する. 先ず, 現代的な primary は次のように表される.

定義 5.1　現代的な表記による4次の primary

単元でない $k = a+bi \in \mathbb{Z}[i]$ が

$$k \equiv 1 \pmod{(1+i)^3}$$

を満たすとき primary という.

上の定義から結局次の条件が得られる. つまり, $k = a+bi$ が primary ならば

$$a \equiv 1 \pmod{4} \quad \text{かつ} \quad b \equiv 0 \pmod{4}$$

あるいは

$$a \equiv 3 \pmod 4 \quad かつ \quad b \equiv 2 \pmod 4$$

したがって,ガウスの primary の定義と現代的な表記による primary の定義は同等であることが分かる.そして,次のようにルジャンドル記号のアイデアを使って4次剰余記号を定義すればよい.

$$\left(\frac{k}{m}\right)_4 :\equiv k^{\frac{1}{4}(p-1)} \pmod m$$

ここで,$m = a + bi$, $p = a^2 + b^2$ より,p は m のノルム Nm になっている.従って,次のようになる.

$$\left(\frac{k}{m}\right)_4 :\equiv k^{\frac{1}{4}(Nm-1)} \pmod m$$

したがって,ガウスの4次剰余の基本定理(4次剰余相互法則)は先ず,次のように定式化される.

ガウスの4次剰余の基本定理(4次剰余相互法則)

m , n が同時に $3+2i$ に合同 (mod 4) でないならば ,
つまり,法4に関して $\equiv 1$ ならば,

$$\left(\frac{n}{m}\right)_4 = \left(\frac{m}{n}\right)_4$$

m , n が同時に $3+2i$ に合同 (mod 4) ならば

$$\left(\frac{n}{m}\right)_4 = -\left(\frac{m}{n}\right)_4$$

(m , $n \in \mathbb{Z}[i]$ は primary な素数)

ここで,m , $n \in \mathbb{Z}[i]$ の primary な素元は mod 4 では次の二つの可能性しかない.

$$\equiv 1 \pmod 4 \qquad , \qquad \equiv 3 + 2i \pmod 4$$

つまり,$\pi = a + bi$ とすると

$$a \equiv 1 \ , \ b \equiv 0 \pmod 4 \quad 又は \quad a \equiv 3 \ , \ b \equiv 2 \pmod 4$$

ということである.$a \equiv 1$, $b \equiv 0 \pmod 4$ ならば

$$N\pi - 1 = a^2 + b^2 - 1 \equiv 0 \pmod 8$$

$a \equiv 3$, $b \equiv 2 \pmod 4$ ならば

$$N\pi - 1 = a^2 + b^2 - 1 \equiv 4 \pmod 8$$

になる. したがって

$$(-1)^{\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1)}$$

の値を考えたとき,m , n の両方が $a \equiv 3$, $b \equiv 2 \pmod 4$ ならば

$$\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1) = \text{奇数}$$

それ以外ならば

$$\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1) = \text{偶数}$$

になる. したがって,

$$m \equiv 3 + 2i \pmod 4 \quad , \quad n \equiv 3 + 2i \pmod 4$$

のときは,

$$(-1)^{\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1)} = -1$$

になり, それ以外のときは

$$(-1)^{\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1)} = 1$$

になる. したがって, 以上より, 次のように定式化される.

ガウスの4次剰余の基本定理（4次剰余相互法則）

$$\left(\frac{n}{m}\right)_4 = (-1)^{\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1)}\left(\frac{m}{n}\right)_4$$

m , $n \in \mathbb{Z}[i]$ の primary な素元

又,m , n は互いに素な primary prime なので必然的に次が成立する.

$$(m) \neq (1+i) \quad , \quad (n) \neq (1+i) \quad , \quad (m) \neq (n)$$

つまり, ガウスの4次剰余相互法則は, 現代的な表記法による4次剰余相互法則そのものであることが示された. ガウスの4次剰余相互法則は一見すると現代的な4次剰余相互法則とほとんど関係が無いように見えるが, 実は, 関係が無いどころか, 現代的な表記法による4次剰余相互法則そのものなのである.

参考・引用文献

[1] Gauss 「Theoria residuorum biquadraticorum. Commentatio prima」 Werke , volume : bd. 2 , pp.67-91

[2] Gauss 「Theoria residuorum biquadraticorum. Commentatio secunda」 Werke , volume : bd. 2 , pp.95-148

[3] Gauss 「Theoria residuorum biquadraticorum. Comm. Ⅰ」 Werke , volume : bd. 2 , pp.165-168

[4] Gauss 「Theoria residuorum biquadraticorum. Comm. Ⅱ」 Werke , volume : bd. 2 , pp.169-178

[5] Gauss 「Kubische und biquadratische Reste」 Werke , volume : bd. 10 Abt 1 , pp.37-77

[6] Gauss 高瀬正仁訳『ガウス整数論 (Disquisitiones arithmeticae) 第5版』(朝倉書店) 2003年

[7] 高瀬正仁 「ガウスの数学日記について」, 第14回 数学史シンポジウム会報 pp.13-28 津田塾大学数学・計算機科学研究所 2003年

[8] 高瀬正仁 「ガウスの数学日記について (続)」, 第15回 数学史シンポジウム会報 pp.30-43 津田塾大学数学・計算機科学研究所 2004年

[9] Dunnington 『CARL FRIEDRICH GAUSS — Titan of Science)』

[10] 倉田令二郎 『平方剰余の相互法則』(日本評論社) 1992年

[11] 高瀬正仁 『ガウスの遺産と継承者たち』(海鳴社) 1990年

[12] 山本芳彦 『数論入門1』『数論入門2』(岩波書店) 1996年

[13] 加藤和也 『解決！フェルマーの最終定理』(日本評論社) 1996年

[14] 加藤和也, 黒川信重, 斉藤毅 『数論Ⅰ』(岩波書店) 2005年

[15] 平松豊一 『相互法則入門』(牧野書店) 1998年

[16] 河田敬義 『19世紀の数学 -整数論-』(共立出版) 1992年

[17] 久保田富雄 『数論論説』(牧野書店) 1999年

[18] 足立恒雄 『フェルマーの大定理』(日本評論社) 1996年

[19] 三宅克哉 「類体論の歴史と概要」(数理科学『特集 類体論の１００年』P5～P12) (サイエンス社) 1998年

[20] 伊波靖 「４次剰余相互法則の関数論的考察」(筑波大学大学院教育研究科修士論文) 2000年