ガウス周期に関するノート　その2

- 4次ガウス周期 -

2020年4月～5月まとめ
富山県立石動高校　片山　喜美

栗原将人著「ガウスの数論世界をゆく」（数学書房）でガウス周期を勉強したノートである。自分なりの解釈や計算等を書き留めてみる。

その1では、2次ガウス周期の基本定理、さらにそれを利用した平方剰余の相互法則の証明を扱った。その2では4次ガウス周期について扱う。

1　ガウスの d 次周期とガウスの積公式

1.1　ガウスの d 次周期

正十七角形が定規とコンパスで作図可能であることの証明では、$\mathbb{F}_p^{\times}=\{1,2,\cdots\cdots,16\}$ を $H_2=\{g^0,g^2,\cdots\cdots,g^{14}\}$ と gH_2 （g は $\mathbb{F}_p^{\times}$ の生成元で、例えば3）の2つに分けた。

続いて、それらをさらに2分割ずつして、$H_4=\{g^{4m}\,|\,m=0,1,2,3\}$, gH_4, g^2H_4, g^3H_4 という4分割を考えていった。

もちろん、$p-1=16$ が4の倍数であるから4分割ができるわけで、$p=7$ のときは、$p-1=6$ となり、4分割はできない。2分割に続いてできるのは、それを3分割ずつにした6分割である。（この3分割が3次方程式に対応し、正七角形は定規とコンパスでは作図できなことにつながる。）

$p-1$ の約数を d とするとき、$\mathbb{F}_p^{\times}$ の d 分割を以下のように定義する。

定義 1.1.1　$\mathbb{F}_p^{\times}$ の生成元の1つを g、d を $p-1$ の約数とするとき、
$H_d=\left\{g^{dm}\,|\,0\leqq m\leqq\frac{p-1-d}{d}\right\}$ と定義する。

注意；この H_d の定義は、生成元 g のと取り方によらない。（別の生成元 g' があったとしたら、g を g' で表すこと、およびその逆について考えると、g' で定義したものが g で定義したものと同じであることがわかる。）

定義 1.1.2　（ガウス d 次周期）
p は奇素数、$\zeta=e^{\frac{2\pi i}{p}}$ とする。
$a\in\mathbb{Z}$ に対して、$[a]_d=\displaystyle\sum_{k\in H_d}\zeta^{ak}$ と定義する。

これを「ガウス d 次周期」と呼ぶ。

1.2　ガウスの積公式

命題 1.2.1

(1) $a \equiv b \pmod{p} \Longrightarrow [a]_d = [b]_d$

(2) $a \in g^j H_d \Longrightarrow [a]_d = [g^j]_d \quad (j = 0, 1, \cdots, d-1)$

(3) $[0]_d = \dfrac{p-1}{d}$

証明）2 次ガウス周期で証明したのと同じ方法で証明できる。

(1) $a \equiv b \pmod{p}$ のとき、$\zeta^a = \zeta^b$ より従う。

(2) $a \in g^j H_d$ のとき、$a = g^j \cdot g^{dm} = g^{j+dm}$

$$[a]_d = \sum_{k \in H_d} \zeta^{ak} = \sum_{l=0}^{\frac{p-1-d}{d}} \zeta^{g^{j+dm} g^{dl}} = \sum_{l=0}^{\frac{p-1-d}{d}} \zeta^{g^{j+d(m+l)}} = \sum_{n=m}^{\frac{p-1-d}{d}+m} \zeta^{g^{j+dn}}$$

$$= \sum_{n=m}^{\frac{p-1-d}{d}} \zeta^{g^{j+dn}} + \sum_{n=\frac{p-1}{d}}^{\frac{p-1-d}{d}+m} \zeta^{g^{j+dn}} \qquad \cdots\cdots ①$$

ここで、① の第 2 の和は、$\zeta^{g^{j+(p-1)}} + \zeta^{g^{j+(p-1)+d}} + \cdots\cdots + \zeta^{g^{j+(p-1)+(m-1)d}}$ で、$g^{p-1} = 1$ であるから、$\zeta^{g^{j+0}} + \zeta^{g^{j+d}} + \cdots\cdots + \zeta^{g^{j+(m-1)d}}$ となる。

従って、$① = \displaystyle\sum_{n=m}^{\frac{p-1-d}{d}} \zeta^{g^{j+dn}} + \sum_{n=0}^{m-1} \zeta^{g^{j+dn}} = \sum_{n=0}^{\frac{p-1-d}{d}} \zeta^{g^{j+dn}} = \sum_{k \in H_d} \zeta^{g^j k} = [g^j]_d$ //

定理 1.2.2　（ガウスの積公式）

$$[a]_d [b]_d = \sum_{k \in H_d} [a + bk]_d = \sum_{k \in H_d} [ak + b]_d$$

証明）2 次ガウス周期でガウスの積公式を証明したのと同じ方法で証明できる。

$$[a]_d [b]_d = \sum_{l \in H_d} \zeta^{al} \sum_{m \in H_d} \zeta^{bm} = \sum_{l \in H_d} \sum_{m \in H_d} \zeta^{al+bm} = \sum_{l \in H_d} \sum_{m \in H_d} \zeta^{(a+bl^{-1}m)l} \qquad \cdots ②$$

② 式の二重和において、外側の和の l を固定して、内側の和のところで m を H_d の元全体を動かすとき、$l^{-1}m$ も H_d の元全体を動く。

従って、

$$② = \sum_{l \in H_d} \sum_{k \in H_d} \zeta^{(a+bk)l} = \sum_{k \in H_d} \sum_{l \in H_d} \zeta^{(a+bk)l} = \sum_{k \in H_d} [a + bk]_d$$

また、$[a]_d [b]_d = [b]_d [a]_d = \displaystyle\sum_{k \in H_d} [b + ak]_d$ であり、第 2 の形に等しいこともいえる。

以上により、定理は示された。 //

2　ガウスの4次周期

4次周期を作れるのは、 $\mathbb{F}_p^\times = p-1$ が4の倍数であるときである。従って、 $p \equiv 1 \pmod 4$ のときである。

2.1　計算例

- $p = 17$ のとき

  $g = 3$, $H_4 = \{1, 13, 16, 4\}$ として、前の計算 $[1]_4[g^2]_4$ をガウスの積公式で実施してみる。

  $[1]_4[9]_4 = \sum_{k \in H_4} [1+9k]_4$

k	1	13	16	4
$1+9k$	10	118	145	37
$1+9k \pmod{17}$	10	16	9	3

H_4		○		
gH				○
g^2H_4			○	
g^3H_4	○			

  上の表より、$[1]_4[g^2]_4 = [1]_4 + [g]_4 + [g^2]]_4 + [g^3]_4 = \zeta + \zeta^2 + \cdots\cdots + \zeta^{16} = -1$

- $p = 13$ のとき

  $g = 2, \quad H_4 = \{1, , 3, 9\}$, $gH_4 = \{2, 6, 5\}$, $g^2H_4 = \{4, 12, 10\}$, $g^3H_4 = \{8, 11, 17\}$ として、前の計算 $[1]_4[g^2]_4$ をガウスの積公式で実施してみる。

  $[1]_4[4]_4 = \sum_{k \in H_4} [1+4k]_4$

k	1	3	9
$1+4k$	5	13	37
$1+4k \pmod{13}$	10	0	11

H_4			
gH	○		
g^2H_4			
g^3H_4			○

  上の表より、$[1]_4[g^2]_4 = [g]_4 + [g^3]_4 + [0]_4 = [g]_2 + \dfrac{13-1}{4} = \dfrac{-1-\sqrt{13}}{2} + 3 = \dfrac{5-\sqrt{13}}{2}$

  ただし、2次ガウス周期の値に公式を用いた。

  $[1]_4 + [g^2]_4 = [1]_2 = [1]_2\ \dfrac{-1+\sqrt{13}}{2}$ となるから、$[1]_4, [g^2]_4$ は次の2次方程式の2つの解となる。

$$x^2 - \frac{-1+\sqrt{13}}{2}x + \frac{5-\sqrt{13}}{2} = 0$$

解は $x = \dfrac{\frac{-1+\sqrt{13}}{2} \pm \sqrt{\frac{14-2\sqrt{13}}{4} - (10-2\sqrt{13})}}{2}$

$= \dfrac{1}{4}\left(-1+\sqrt{13} \pm \sqrt{-26+6\sqrt{13}}\right)$

2.2　4 次ガウス周期の値の計算に向けて

$[1]_4$ と $[g^2]_4$ を解に持つ 2 次方程式を考える。

まず、 $[1]_4 + [g^2]_4 = [1]_2 = \dfrac{-1+\sqrt{(-1)^{\frac{p-1}{2}}p}}{2}$

（最後の値は、ガウス 2 次周期の基本定理による。）

次に、ガウスの積公式によって、

$$[1]_4[g^2]_4 = \sum_{k\in H_4}[1+g^2k]_4 = N_0[1]_4 + N_1[g]_4 + N_2[g^2]_4 + N_3[g^3]_4 + M[0]$$

ただし、 $N_j =^{\#} \{k \in H_4 \,|\, 1+g^2k \in g^jH_4\}$　$(j=0,1,2,3)$　$M =^{\#} \{k \in H_4 \,|\, 1+g^2k = 0\}$

これらは、$1+g^2X = g^jY$　$X, Y \in H_4$,　$j=0,1,2,3)$ の解の個数を考えることに結びつく。

2 次ガウス周期の基本公、, 第 2 補充則を証明するときには、 $1+X=Y$ や $1+X = gY, 1+gX = Y, 1+gX = gY$　$(X, Y^{\in}H_2)$ の解の個数を考えた。

4 次ガウス周期の場合は、上の形に限らず、 $1+g^iX = g^jY$　$(X, Y \in H_4)$

の形の方程式を並べて、それらの解の個数の関係を調べていく。

2.3　-1 がどの分割に含まれるか

$1+g^iX = g^jY$ の解の個数を考えるとき、$1+g^iX = 0$ が解を持つかどうかが重要になる。 このとき、 $-1 = g^iX$ であるから、まずは、-1 が $H_4, gH_4, g^2H_4, g^3H_4$ のいずれに属するかについて調べる。

生成元 g について、$-1 = g^{\frac{p-1}{2}}$ であった。 これが g^jH_4 に含まれるとすると、

$\dfrac{p-1}{2} = 4m+j$ となる。このとき、 $p \equiv 1 \pmod 4$ であったから、 $p = 4k+1$ として、 $2k = 4m+j$ 。よって、 $j = 0, 2$ のいずれかになる。

- $j=0$ のとき

  $2k = 4m$ であるから、$p = 4k+1 = 8m+1$

  逆に、$p = 8m+1$ のとき、$g^{\frac{p-1}{2}} = g^{4m} \in H_4$

- $j=2$ のとき

  $2k = 4m+2$ であるから、$p = 4k+1 = 8m+5$

  逆に、$p = 8m+5$ のとき、$g^{\frac{p-1}{2}=g^{4m+2}} \in g^2H_4$

補題 2.3.1　$p \equiv 1 \pmod 8 \Longrightarrow -1 \in H_4$,　$p \equiv 5 \pmod 8 \Longrightarrow -1 \in g^2H_4$

2.4　個数の計算

$N(i,j) =^{\#} \{X \in H_4 \,|\, 1+g^iX \in g^jH_4\}$ とおく。求めたいのは、$N(2,j)\quad (j=0,1,2,3)$ であるが、それだけを単独で求めるのは難しく、他のものと絡み合わせることによって求められる。

補題 2.4.1　$i' \equiv i,\, j' \equiv j \pmod 4 \Longrightarrow N(i',\, j') = N(i,\, j)$

証明）$1+g^{i'}X' = g^{j'}Y' \quad i' \equiv i,\, j' \equiv j \pmod 4$ とする。
$i' = i+4k,\, j' = j+4l \quad (k,\, l \in \mathbb{Z})$ とおくと、$1+g^i(g^{4k}X') = g^j(g^{4l}Y)$
$X = g^{4k}X',\, Y = g^{4l}Y'$ とおくと、$1+g^iX = g^jY \quad (X,\, Y \in H_4)$ を満たす。また、この逆の対応も得られる。従って、解の個数について、$N(i',\, j') = N(i,\, j)$ が成り立つ。//

$1+g^iX = g^jY$ のとき、$1+g^j(-Y) = g^i(-X)$ と変形できる。このとき、-1 が H_4 に属するのか、それとも g^2H_4 に属するのかで違いが出てくる。

補題 2.4.2

(1) $p \equiv 1 \pmod 8$ のとき、$N(i,\, j) = N(j+2,\, i+2) \quad \cdots\cdots ①$

(2) $p \equiv 5 \pmod 8$ のとき、$N(i,\, j) = N(j+2,\, i+2) \quad \cdots\cdots ①'$

証明）

(1) $p \equiv 1 \pmod 8$ のとき

補題 2.3.1 より $-1 \in H_4$ であるから、$X' = -X,\, Y' = -Y \quad$ とおいて、$1+g^jX' = g^iY' \quad (X',\, Y' \quad \in H_4)$ となる。

この写像 $(X,Y) \to (X',Y')$ は逆に戻ることができるので 1 対 1 対応となる。

従って、解の個数について、$N(j,\, i) = N(i,\, j)$//

(2) $p \equiv 5 \pmod 8$ のとき

補題 2.3.1 より $-1 \in g^2H_4$ であるから、$-1 = g^2k \quad (k \in H_4)$ とおける。

$X' = X,\, Y' = kY \quad$ とおいて、$1+g^{j+2}X' = g^{i+2}Y' \quad (X',\, Y' \in H_4)$ となる。

この写像 $(X,Y) \to (X',Y')$ は逆に戻ることができるので 1 対 1 対応となる。

従って、解の個数について、$N(i,\, j) = N(j+2,\, i+2)$//

注意.　補題 2.4.1 により、$j+2,\, i+2$ を 4 で割った余りで考えて、常に 0 から 3 の間にとって計算を進めることになる。

補題 2.4.3　$N(i,j) = N(-i,j-i) = N(4-i,j-i) \quad \cdots\cdots ②$

証明）$1+g^iX = g^jY$ が成り立っているとき、両辺に $g^{-i}X^{-1}$ を掛けて
$g^{-i}X^{-1} + 1 = g^{j-i}X^{-1}Y$

$X' = X^{-1}, Y = X^{-1}Y$ とおくと、 $1 + g^{-i}X' = g^{j-i}Y \quad (X', Y' \in H_4)$ となる。
この写像は逆に戻ることが出切るので 1 対 1 対応となる。
従って、$N(i,j) = N(-i, j-i) = N(4-i, j-i)//$

注意. ①, ①′, ② はいずれも 2 回繰り返すと元に戻る。

2.5 $p \equiv 1 \pmod 8$ のときの計算

- まず、$N(0,0) = A$, $N(0,1) = B$, $N(0,2) = C$, $N(0,3) = D$ とおく。

  以下では、① を適用したものを右矢印、② を適用したものを下矢印で表す。

- $N(1,0) \to N(0,1)$
  $\downarrow$
  $N(3,3)$ であるから、 $N(1,0) = N(3,3) = B$

- $N(1,1) \to N(1,1)$
  $\downarrow$
  $N(3,0) \to N(0,3)$ であるから、 $N(1,1) = N(3,0) = D$

- $N(1,2) \to N(2,1)$
  $\downarrow \qquad \downarrow$
  $\downarrow \qquad N(2,3)$
  $\downarrow$
  $N(3,1) \to N(1,3)$
  $\downarrow$
  $N(3,2) \to N(2,3)$

  これらは $N(0,j)$ に結びつかないので、新たに変数を用意して
  $N(1,2) = N(1,3) = N(2,1) = N(2,3) = N(3,1) = N(3,2) = E$ とおく。

- $N(2,0) \to N(0,2)$
  $\downarrow$
  $N(2,2)$ であるから、 $N(2,0) = N(2,2) = C$

以上から、

$$\begin{pmatrix} N(0,0) & N(0,1) & N(0,2) & N(0,3) \\ N(1,0) & N(1,1) & N(1,2) & N(1,3) \\ N(2,0) & N(2,1) & N(2,2) & N(2,3) \\ N(3,0) & N(3,1) & N(3,2) & N(3,3) \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{pmatrix}$$

ここで、各行ごとに、$N(i,0)$, $N(i,1)$, $N(i,2)$, $N(i,3)$ および $1+g^iX=0 \quad (X \in H_4)$ を満たす X の個数を合わせると ${}^{\#}H_4 = \dfrac{p-1}{4}$ になる。

$p \equiv 1 \pmod 8$ のときは、第1行だけ $1+g^iX=0$ の解を1つ持ち、他の行は持たない。

第1行　$A+B+C+D+1 = \dfrac{p-1}{4}$　　$\therefore A+B+C+D = \dfrac{p-5}{4}$　$\cdots\cdots$③

第2行　$B+D+2E = \dfrac{p-1}{4}$　$\cdots\cdots$④

第4行　$2C+2E = \dfrac{p-1}{4}$　$\cdots\cdots$⑤

第4行は第2行と同じ。

ここで求めたいのは、第3行である。この第3行を用いて計算すると、

$$[1]_4[g^2]_4 = \sum_{k \in H_4} [1+gk]_4 = C[1]_4 + E[g]_4 + C[g^2]_4 + E[g^3]_4 = C([1]_4+[g^2]_4) + E([g]_4+[g^3]_4)$$

$$= C[1]_2 + E[g]_2 = C\frac{-1+\sqrt{p}}{2} + E\frac{-1-\sqrt{p}}{2} = \underline{-\frac{1}{2}(C+E) + \frac{1}{2}(C-E)\sqrt{p}}$$

よって、C と E を求めればよい。あるいは、$C+E$ 及び $C-E$ がわかればよい。

まず、⑤ より、$C+E = \dfrac{p-1}{8}$ である。

後に、$C-E$ の値を求める。そのために、しばらく計算を続ける。

③ − ④　　$A+C-2E=-1,$　　$\therefore A = -C+2E-1$　$\cdots\cdots$⑥

④ − ⑤　　$B-2C+D=0,$　　$\therefore D = 2C-B$　　$\cdots\cdots$⑦

ところで、A から E まで5つの未知数に対して、関係式は ③, ④, ⑤ の3つしか立てておらず、このままでは C と E を求めることができない。そこで、ガウスは次のような方程式について考察したそうである。

$$1+X+gY+g^2Z=0 \quad (X, Y, Z, \in H_4) \qquad \cdots\cdots Ⓐ$$

1. まず、$1+X$ をまとめて考えてみる。

   $1+X=0$ となるか、H_4, gH_4, g^2H_4, g^3H_4 のいずれかに属する。場合分けして考える。

   (1) $1+X=0$ のとき
   Ⓐ は、$gY+g^2Z=0$ となる。よって、$Y=-gZ$。
   ここでは、$p \equiv 1 \pmod 8$ の場合について調べているのであったから、$-1 \in H_4$ となる。従って、この式の左辺は H_4 の元で、右辺は gH_4 の元となり、成り立たない。故に $1+X=0$ となる Ⓐ の解は無い。

   (2) $1+X \in H_4$ のとき
   $1+X=W \quad (W \in H_4)$ とおくと、Ⓐ は、$W+gY+g^2Z=0$ となる。

$1+gW^{-1}Y=g^2(-W^{-1}Z)$ として、 $X'=W^{-1}Y,\ Y'=-W^{-1}Z$ とおけば、
$1+gX'=g^2Y'\quad (X',\,Y'\in H_4)$ となる。
$1+X=W$ の解の個数は、 $N(0,0)=A$ で、 $1+gX'=g^2Y$ の解の個数は、
$N(1,2)=E$ であるから、この場合の Ⓐ の解の個数は AE となる。

(3) $1+X\in gH_4$ のとき
$1+X=gW\quad (W\in H_4)$ とおくと、 Ⓐ は、 $gW+gY+g^2Z=0$ となる。
$1+W^{-1}Y=g(-W^{-1}Z)$ として、 $X'=W^{-1}Y,\ Y'=-W^{-1}Z$ とおけば、
$1+X'=gY'\quad (X',\,Y'\in H_4)$ となる。
$1+X=gW$ の解の個数は、 $N(0,1)=B$ で、 $1+X'=gY$ の解の個数は、
$N(0,1)=B$ であるから、この場合の Ⓐ の解の個数は B^2 となる。

(4) $1+X\in g^2H_4$ のとき
$1+X=g^2W\quad (W\in H_4)$ とおくと、 Ⓐ は、 $g^2W+gY+g^2Z=0$ となる。
$gWY^{-1}+1=g(-Y^{-1}Z)$ として、 $X'=WY^{-1}Y,\ Y'=-Y^{-1}Z$ とおけば、
$1+gX'=gY'\quad (X',\,Y'\in H_4)$ となる。
$1+X=g^2W$ の解の個数は、 $N(0,2)=C$ で 、$1+X'=gY$ の解の個数は、
$N(1,1)=D$ であるから、この場合の Ⓐ の解の個数は CD となる。

(5) $1+X\in g^3H_4$ のとき
$1+X=g^3W\quad (W\in H_4)$ とおくと、 Ⓐ は、 $g^3W+gY+g^2Z=0$ となる。
$g^2WY^{-1}+1=g(-Y^{-1}Z)$ として、 $X'=WY^{-1}Y,\ Y'=-Y^{-1}Z$ とおけば、
$1+g^2X'=gY'\quad (X',\,Y'\in H_4)$ となる。
$1+X=g^3W$ の解の個数は、 $N(0,3)=D$ で、 $1+g^2X'=gY$ の解の個数は、 $N(2,1)=E$ であるから、この場合の Ⓐ の解の個数は DE となる。

以上により、、Ⓐ の解の総数は、 $AE+B^2+CD+DE\qquad\cdots\cdots$Ⓑ

2. 次に、$1+$ g Y をまとめて考えてみる。

$1+gY=0$ となるか、$H_4,\ gH_4,\ g^2H_4,\ g^3H_4$ のいずれかに属するかである。場合分けして考える。

(1) $1+gY=0$ のとき、
$-1=gY\in gH_4$ となるが、$p\equiv 1\pmod 8$ のときは、 $-1\in H_4$ であるからあり得ない。

(2) $1+gY\in g^jH_4\quad (j=0,1,2,3)$ のとき
$1+g^jY=W\quad (W\in H_4)$ とおくと、 Ⓐ は、 $X+g^jW+g^2Z=0$ となる。
$1+g^jX^{-1}W=g^2(-X^{-1}Z)$ として、 $X'=X^{-1}W,\ Y'=-X^{-1}Z$ とおけば、
$1+g^jX'=g^2Y'\quad (X',\,Y'\in H_4)$ となる。
$1+gY=g^jW$ の解の個数は、 $N(1,j)$ で、 $1+g^jX'=g^2Y$ の解の個数は、
$N(j,2)$ であるから、この場合の Ⓐ の解の個数は $N(1,j)N(j,2)\quad (j=0,1,2,3)$ となる。

従って、Ⓐ の解の総数は、

$N(1,0)N(0,2)+N(1,1)N(1,2)+N(1,2)N(2,2)+N(1,3)N(3,2)$

$= BC + DE + EC + E^2$ $\cdots\cdots$ Ⓒ

3. 上記の 2 通りの数え方から Ⓑ = Ⓒ として

$$AE + B^2 + CD + DE = BC + DE + EC + E^2$$

⑥, ⑦ を代入して

$$(-C + 2E - 1)E + B^2 + C(2C - B) = BC + EC + E^2$$

$$B^2 + 2C^2 + E^2 - 2BC - 2EC - E = 0 \quad \cdots\cdots ⑧$$

$$(B - C)^2 + (C - E)^2 = E$$

ここで、$C - E = V$ とおいて考える。⑤ より、$C + E = \frac{1}{8}(p-1)$ である。

差し引いて、

$$2E = \frac{1}{8}(p-1) - V, \qquad E = \frac{1}{16}(p-1) - \frac{1}{2}V$$

⑧ に代入して、

$$(B - C)^2 + V^2 = \frac{1}{16}(p-1) - \frac{1}{2}V$$

$$(B - C)^2 + V^2 + \frac{1}{2}x + \frac{1}{16} = \frac{1}{16}p$$

$$\{4(B - C)\}^2 + (4V + 1)^2 = p \quad \cdots\cdots ⑩$$

$W = B - C$ とおくと

$$\underline{(4V + 1)^2 + (4W)^2 = p}$$

これは、素数 p を 2 つの整数の平方の和で表す式になっている。

そして、前に計算したことと合わせると

$$[1]_4[g^2]_4 = -\frac{p-1}{16} + \frac{V}{2}\sqrt{p}$$

以上をまとめて、次の定理となる。

定理 2.5

$p \equiv 1 \pmod 8$ のとき、$(4V + 1)^2 + (4W)^2 = p$ を満たす整数 V, W $(y > 0)$ がある。

さらに、4 次ガウス周期について、 $[1]_4[g^2]_4 = -\frac{p-1}{16} + \frac{V}{2}\sqrt{p}$ が成り立つ。

□ $p \equiv 1 \pmod 8$ を満たす素数 p に関する計算例

- $P = 17$ のとき
  $1^2 + 4^2 = 17$ であるから、$4V + 1 = 1, \quad V = 0, \quad W = 1$

  従って、$[1]_4[g^2]_4 = -\dfrac{17-1}{16} + \dfrac{0}{2}\sqrt{17} = -1$

- $P = 41$ のとき
  $5^2 + 4^2 = 41$ であるから、$4V + 1 = 5, \quad V = 1, \quad y = 1$

  従って、$[1]_4[g^2]_4 = -\dfrac{41-1}{16} + \dfrac{1}{2}\sqrt{41} = -\dfrac{5}{2} + \dfrac{1}{2}\sqrt{41}$

- $P = 73$ のとき
  $3^2 + 8^2 = 73$ である。$4V + 1 = 3$, とすると、$V = \dfrac{1}{2}$ となり、不都合である。
  $(-3)^2 + 8^2 = 73$ として、$4V + 1 = -3, \quad V = -1$ とする。また、$W = 2$
  従って、$[1]_4[g^2]_4 = -\dfrac{73-1}{16} + \dfrac{-1}{2}\sqrt{73} = -\dfrac{9}{2} - \dfrac{1}{2}\sqrt{73}$

$[g]_4[g^3]_4$ についても計算する。ガウスの積公式より、

$$[g]_4[g^3]_4 = \sum_{\alpha \in H_4} [g + g^3\alpha]_4$$

$g + g^3X = g^jY \quad (X, Y \in H_4)$ は $1 + g^2X = g^{j-1}Y$ と同値であるから、$a + g^2X = 0$ の解が無いことも含めて、上の式より

$$[g]_4[g^3]_4 = \sum_{j=0}^{3} N(2, j-1)[g^j]_4 = N(2,3)[1]_4 + N(2,0)[g]_4 + N(2,1)[g^2]_4 + N(2,2)[g^3]_4$$

$$= E([1]_4 + [g^2]_4) + C([g]_4 + [g^3]_4) = E[1]_2 + C[g]_2$$

$$= E \cdot \frac{-1 + \sqrt{p}}{2} + C \cdot \frac{-1 - \sqrt{p}}{2} = -\frac{C+E}{2} - \frac{C-E}{2}\sqrt{p} = -\frac{p-1}{8} - \frac{V}{2}\sqrt{p}$$

2.6 $p \equiv 5 \pmod 8$ のときの計算

$p \equiv 5 \pmod 8$ のとき、
$N(i, j) = N(j + 2, i + 2) \quad \cdots\cdots ①'$
$N(i, j) = N(-i, j - i) = N(4 - i, j - i) \quad \cdots\cdots ②$
を用いて計算する。

- まず、$N(0, 0) = A$, $N(0, 1) = B$, $N(0, 2) = C$, $N(0, 3) = D$ とおく。

  以下では、①' を適用したものを右矢印、② を適用したものを下矢印で表す。

- $N(1,0) \to N(2,3)$
  $\downarrow$ $\quad$ $\downarrow$
  $\downarrow$ $\quad$ $N(2,1) \to N(3,0)$
  $\downarrow$ $\quad$ $\downarrow$
  $N(3,3) \to N(1,1) \quad N(1,1)$
  $\downarrow$
  $N(3,0)$

  これらは $N(0,j)$ に結びつかないので、新たに変数を用意して
  $N(1,0) = N(1,1) = N(2,1) = N(2,3) = N(3,0) = N(3,3) = E$ とおく。

- $N(1,2) \to N(0,3)$
  $\downarrow$
  $N(3,1) \to N(3,1)$ $\quad$ であるから、 $N(1,2) = N(3,1) = D$

- $N(1,3) \to N(1,3)$
  $\downarrow$
  $N(3,2) \to N(0,1)$ $\quad$ であるから、 $N(1,3) = N(3,2) = B$

- $N(2,0) \to N(2,0)$
  $\downarrow$
  $N(2,2) \to N(0,0)$ $\quad$ であるから、 $N(2,0) = N(2,2) = A$

- $N(3,1) = D, \quad N3,2) = B$ は既出

以上から、

$$\begin{pmatrix} N(0,0) & N(0,1) & N(0,2) & N(0,3) \\ N(1,0) & N(1,1) & N(1,2) & N(1,3) \\ N(2,0) & N(2,1) & N(2,2) & N(2,3) \\ N(3,0) & N(3,1) & N(3,2) & N(3,3) \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ E & E & D & B \\ A & E & A & E \\ E & D & B & E \end{pmatrix}$$

ここで、各行ごとに、$N(i,0)$, $N(i,1)$, $N(i,2)$, $N(i,3)$ および $1 + g^i X = 0 \quad (X \in H_4)$ を満たす X の個数を合わせると ${}^{\#}H_4 = \dfrac{p-1}{4}$ になる。

$p \equiv 5 \pmod 8$ のときは、第 3 行だけ $1 + g^i X = 0$ の解を 1 つ持ち、他の行は持たない。

第 1 行 $\quad A + B + C + D = \dfrac{p-1}{4} \quad \cdots\cdots ⑪$

第 2 行 $\quad B + D + 2E = \dfrac{p-1}{4} \quad \cdots\cdots ⑫$

第 4 行 $\quad 2A + 2E + 1 = \dfrac{p-1}{4}, \qquad \therefore 2A + 2E = \dfrac{p-5}{4} \quad \cdots\cdots ⑬$

第 4 行は第 2 行と同じ。

ここで求めたいのは、第3行である。$p \equiv 5 \pmod 8$ のときは、$1+g^2X=0$ を満たす $X \in H_4$ が1つあることに注意して、この第3行を用いて計算すると、

$$[1]_4[g^2]_4 = \sum_{k \in H_4} [1+gk]_4 = A[1]_4 + E[g]_4 + A[g^2]_4 + E[g^3]_4 + [0]_4$$

$$= A([1]_4 + [g^2]_4) + E([g]_4 + [g^3]_4) + [0]_4 + \frac{p-1}{4}$$

$$= A[1]_2 + E[g]_2 = A\frac{-1+\sqrt{p}}{2} + E\frac{-1-\sqrt{p}}{2} + \frac{p-1}{4}$$

$$= \underline{-\frac{1}{2}(A+E) + \frac{p-1}{4} + \frac{1}{2}(A-E)\sqrt{p}}$$

よって、A と E を求めればよい。あるいは、$A+E$ 及び $A-E$ がわかればよい。

まず、⑬ より、$A+E = \dfrac{p-5}{8}$ であるから、

$$[1]_4[g^2]_4 = -\frac{1}{2}\cdot\frac{p-5}{8} + \frac{p-1}{4} + \frac{1}{2}(A-E)\sqrt{p} = \frac{3p+1}{16} + \frac{1}{2}(A-E)\sqrt{p}$$

後に、$A-E$ の値を求める。そのために、しばらく計算を続ける。

⑪ − ⑫　　$A+C-2E=0,$　　$\therefore C=-A+2E$　$\cdots\cdots$⑭

⑫ − ⑬　　$-2A+B+D=1,$　　$\therefore D=2A-B$　　$\cdots\cdots$⑮

$p \equiv 1 \pmod 8$ のときと同様に、次の方程式について考察する。

$$1+X+gY+g^2Z=0 \quad (X,\, Y,\, Z, \in H_4)$$

変形すると、

$$1+X+gY=-g^2Z$$

$p \equiv 5 \pmod 8$ のときは、$-1 \in g^2H_4$ となるから、$-g^2 \in H_4$ である。従って、上の方程式の解の個数を考えることは、

$$1+X+gY=Z \quad (X,Y,Z \in H_4) \qquad \cdots\cdots Ⓐ'$$

の解の個数を考えることと同じである。

1. まず、$1+X$ をまとめて考えてみる。

   $1+X=0$ となるか、$H_4,\, gH_4,\, g^2H_4,\, g^3H_4$ のいずれかに属する。場合分けして考える。

   (1) $1+X=0$ のとき
   $-1=X \in \quad H_4$ となるが、$p \equiv 5 \pmod 8$ のときは $-1 \in g^2H_4$ であるから、あり得ない。

(2) $1+X \in g^j H_4$ のとき

$1+X=g^jW \quad (W \in H_4, \quad j=0,1,2,3)$ とおくと、 Ⓐ' は、 $g^jW+gY=Z$ となる。

$1+g^{j-1}X^{-1}W=g^{-1}X^{-1}Z$ として、 $X'=X^{-1}Y,\ Y'=-X^{-1}Z$ とおけば、

$1+g^{j-1}X'=g^{-1}Y' \quad (X', Y' \in H_4)$ となる。

$1+X=g^jW$ の解の個数は、 $N(0,j)$ で、 $1+g^{j-1}X'=g^{-1}Y$ の解の個数は、$N(j-1,-1)$ であるから、 Ⓐ' の解の個数は

$N(0,0)N(-1,-1)+N(0,1)N(0,-1)+N(0,2)N(1,-1)+N(0,3)N(2,-1)$

$=N(0,0)N(3,3)+N(0,1)N(0,3)+N(0,2)N(1,3)+N(0,3)N(2,3)$

$=AE+BD+CB+DE \qquad \cdots\cdots$ Ⓑ'

2. 次に、$1+$ g Y をまとめて考えてみる。

$1+gY=0$ となるか、$H_4,\ gH_4,\ g^2H_4,\ g^3H_4$ のいずれかに属するかである。場合分けして考える。

(1) $1+gY=0$ のとき

$-1=gY \in gH_4$ となるが、$p \equiv 5 \pmod 8$ のときは、 $-1 \in g^2H_4$ であるからあり得ない。

(2) $1+gY \in g^jH_4 \quad (j=0,1,2,3)$ のとき

$1+g^jY=W \quad (W \in H_4)$ とおくと、 Ⓑ は、 $X+g^jW=Z$ となる。

$1+g^jX^{-1}W=X^{-1}Z$ として、 $X'=X^{-1}W,\ Y'=X^{-1}Z$ とおけば、

$1+g^jX'=Y' \quad (X', Y' \in H_4)$ となる。

$1+gY=g^jW$ の解の個数は、 $N(1,j)$ で、 $1+g^jX'=Y$ の解の個数は、$N(j,0)$ であるから、 Ⓐ' の解の個数は $N(1,j)N(j,2) \quad (j=0,1,2,3)$ となる。

従って、Ⓐ' の解の総数は、

$N(1,0)N(0,0)+N(1,1)N(1,0)+N(1,2)N(2,0)+N(1,3)N(3,0)$

$=EA+E^2+DA+BE \qquad \cdots\cdots$ Ⓒ'

3. 上記の 2 通りの数え方より Ⓑ' $=$ Ⓒ' として

$$EA+BD+CB+DE=EA+E^2+AD+BE$$

⑭, ⑮ を代入して

$$B(2A-B+1)E+(-A+2E)B+(2A-B+1)E=E^2+A(2A-B+1)+BE$$

$$2AB-B^2+B-AB+2BE+2AE-BE+E=E^2+2A^2-AB+A+BE$$

$$2A^2+B^2+E^2-2AB-2AE+A-B-E=0$$

$$(A-B)^2+(A-B)+(A-E)^2=E$$

$$\left\{(A-B)+\frac{1}{2}\right\}^2+(A-E)^2=E+\frac{1}{2} \qquad \cdots\cdots ⑯$$

ここで、$A-E=V$ とおいて考える。⑬ より、$A+E=\dfrac{1}{8}(p-5)$ である。

差し引いて、

$$2E=\frac{1}{8}(p-5)-V, \qquad E=\frac{1}{16}(p-5)-\frac{1}{2}V$$

⑯ に代入して、

$$\left\{(A-B)+\frac{1}{2}\right\}^2+V^2=\frac{1}{16}(p-5)-\frac{1}{2}V+\frac{1}{4}$$

$$\left\{(A-B)+\frac{1}{2}\right\}^2+\left(V+\frac{1}{4}\right)^2=\frac{1}{16}p$$

$$\{4(A-B)+2\}^2+(4x+1)^2=p \qquad \cdots\cdots ⑰$$

$W=A-B$ とおくと

$$\underline{(4V+1)^2+(4W+2)^2=p}$$

これは、素数 p を 2 つの整数の平方の和で表す式になっている。

そして、前に計算したことと併せると

$$[1]_4[g^2]_4=\frac{3p+1}{16}+\frac{V}{2}\sqrt{p}$$

以上をまとめて、次の定理となる。

定理 2.6

$p\equiv 1 \pmod 8$ のとき、$(4V+1)^2+(4W+2)^2=p$ を満たす整数 V, W $(W>0)$ がある。

さらに、4 次ガウス周期について、$[1]_4[g^2]_4=-\dfrac{3p+1}{16}+\dfrac{V}{2}\sqrt{p}$ が成り立つ。

□ $p\equiv 5 \pmod 8$ を満たす素数 p に関する計算例

- $P=5$ のとき
  $1^2+2^2=17$ であるから、$4V+1=1, \quad x=0, \quad W=0$

  従って、$[1]_4[g^2]_4=-\dfrac{3\cdot 5+1}{16}+\dfrac{0}{2}\sqrt{5}=1$

- $P=13$ のとき
  $3^2+2^2=13$ であるから、$4V+1=-3, \quad V=-1, \quad W=0$

  従って、$[1]_4[g^2]_4=-\dfrac{3\cdot 13+1}{16}+\dfrac{-1}{2}\sqrt{13}=-\dfrac{5}{2}-\dfrac{1}{2}\sqrt{13}$

- $P = 29$ のとき
  $5^2 + 2^2 = 29$ である。$4V + 1 = 5$, であるから、$V = 1, \quad W = 0$

  従って、$[1]_4[g^2]_4 = -\dfrac{3 \cdot 29 + 1}{16} + \dfrac{1}{2}\sqrt{29} = -\dfrac{11}{2} - \dfrac{1}{2}\sqrt{29}$

$[g]_4[g^3]_4$ についても計算する。ガウスの積公式より、

$$[g]_4[g^3]_4 = \sum_{\alpha \in H_4} [g + g^3\alpha]_4$$

$g + g^3X = g^jY \quad (X, y \in H_4)$ は $1 + g^2X = g^{j-1}Y$ と同値であるから、$a + g^2X = 0$ の解が 1 つあることも含めて、上の式より

$$[g]_4[g^3]_4 = \sum_{j=0}^{3} N(2, j-1)[g^j]_4 + [0]_4$$

$$= N(2,3)[1]_4 + N(2,0)[g]_4 + N(2,1)[g^2]_4 + N(2,2)[g^3]_4 + \frac{p-1}{4}$$

$$= E([1]_4 + [g^2]_4) + A([g]_4 + [g^3]_4) + \frac{p-1}{4} = E[1]_2 + A[g]_2 + \frac{p-1}{4}$$

$$= E \cdot \frac{-1 + \sqrt{p}}{2} + A \cdot \frac{-1 - \sqrt{p}}{2} + \frac{p-1}{4} = -\frac{A+E}{2} - \frac{A-E}{2}\sqrt{p} + \frac{p-1}{4}$$

$$= -\frac{p-5}{16} - \frac{V}{2}\sqrt{p} + \frac{p-1}{4} \quad = \frac{3p+1}{16} - \frac{V}{2}\sqrt{p}$$

ここまでのところで、不十分なのは、「$p \equiv 1 \pmod 8$ のとき $(4V+1)^2 + (4W)^2 = p$ 、$p \equiv 5 \pmod 8$ のとき $(4V+1)^2 + (4W+2)^2 = p$ と、表すときの V の取り方は 1 通りとなのか？」である。2 通り以上あると、どの V を使えばよいのかを判断しなければいけないことになってしまう。そのことについては、$a^2 + b^2 = p \quad (a, b \in \mathbb{Z})$ の解についての考察を行う。である。なお、結論は「1 通り」である。

3 $a^2 + b^2 = p \quad (a, b \in \mathbb{Z})$ の解について

奇素数 p を $a^2 + b^2 = p$ というふうに、2 つの整数の平方の和で表すことについて考える。奇素数 p は、$p \equiv 1 \pmod 4$ もしくは、$p \equiv 3 \pmod 4$ のいずれかである。

$a^2, b^2 \equiv 0, 1 \pmod 4$ のいずれかであるから、$a^2 + b^2 \equiv 0, 1, 2 \pmod 4$ である。従って、$p \equiv 3 \pmod 4$ である p について、$a^2 + b^2 = p$ を満たす整数 a, b は存在しない。

$p \equiv 1 \pmod 4$ のときは、前のところで示したことから

$$p \equiv 1 \pmod 8 \Longrightarrow (4V+1)^2 + (4W)^2 = p$$
$$p \equiv 5 \pmod 8 \Longrightarrow (4V+1)^2 + (4W+2)^2 = p$$

というふうに、$a^2+b^2=p$ を満たす整数 a, b が少なくとも 1 組存在する。

§ 2.5 及び§ 2.6 の最後のところで、具体的な素数 $P=5,13,17,29,41,73$ の場合について調べてみたら、 $a=4V+1$ を満たすような整数 a が 1 通りだけとれることがわかった。この章では、一般の素数 p についても、$a=4V+1$ となるような a は 1 通りになることを示す。(b については、たとえば、 $b>0$ となる偶数であると条件をつけると 1 通りになる。)

3.1 $\mathbb{Z}[i]$ から $\mathbb{F}_p$ への写像 $\epsilon_p : a+bi \to \bar{a}+\bar{b}\bar{\mu}$ について

まず、整数全体 $\mathbb{Z}$ から $\mathbb{F}_p=\{0,1,2,\cdots\cdots,p-1\}$ への写像については、
$a\in\mathbb{Z}$ に対して、それを a で割った余り $\bar{a}$ $(0\leqq\bar{a}<p)$ を対応させるのであった。
この $\mathbb{Z}$ から $\mathbb{F}_p$ への写像を $\epsilon_p(a)=\bar{a}$ と表すことにする。

$a^2+b^2=p$ は、実数の範囲ではこれ以上因数分解できないが、虚数単位 i $(i^2=-1$ を満たす数) を導入すると、$(a+bi)(a-bi)$ と因数分解できる。例えば、$5=(1+2i)(1-2i)$ と分解できてしまう。整数に虚数単位 i を加えて、$a+bi$ $(a,b\in\mathbb{Z})$ の形で表される数全体を考え、それを $\mathbb{Z}[i]$ で表し、「ガウス整数」と呼ぶ。$\mathbb{Z}[i]$ の 2 つの数の和、差が $\mathbb{Z}[i]$ の元であることは明らかであるし、積は、計算の途中に i^2 が生じたら -1 に換えることとすると、形を整えて、やはり $\mathbb{Z}[i]$ の数となる。

残念ながら商は必ずしも $\mathbb{Z}[i]$ の元とはならない。例えば、$\dfrac{1+i}{2-i}=\dfrac{(1+i)(2+i)}{(2-i)(2+i)}=\dfrac{2+i+2i-1}{4+1}=\dfrac{1}{5}+\dfrac{3}{5}i$ となり、 $\mathbb{Z}[i]$ の元ではなくなる。これは、$\mathbb{Z}$ のときも、2 つの元の和、差、積はやはり、$\mathbb{Z}$ の元であるが、商は、$\mathbb{Z}$ の範囲からはずれてしまうものがあるのと同じである。

※このように、和、差、積はその数の範囲に入るが、商の中にはその数の範囲からはずれてしまうことがあるような状況を「その数の集合は環 (ring) になる」という。$\mathbb{Z}$ や $\mathbb{Z}[i]$ は環である。

さらに、商もその数の範囲に入るときは「その数の集合は体 (field) になる」という。$\mathbb{Q}$, $\mathbb{R}$ や $\mathbb{Q}[i]$, $\mathbb{C}=\mathbb{R}[i]$ は体である。

$p\equiv 1 \pmod 4$ のときは、 $\mu^2\equiv -1 \pmod p$ を満たす整数 μ が存在するのであった。このとき、$\bar{\mu}=\epsilon_P(\mu)$ は、 $\mathbb{F}_p$ における虚数単位ともいえる。(この場合、$\mathbb{F}_p$ において、$p-1$ を -1 とみなすような柔軟な考えで行くことにする。)

従って、虚数単位 i を $\bar{\mu}$ に対応させるようにして、 $\epsilon_p:\mathbb{Z}[i]\to\mathbb{F}_p$ を $\epsilon_p(a+bi)=\bar{a}+\bar{b}\bar{\mu}$ として定義するのが自然である。この対応により、$\mathbb{Z}[i]$ における様々な計算がうまく $\mathbb{F}_p$ における計算に対応する。(詳細については書かないが、ϵ_p が $\mathbb{Z}[i]\to\mathbb{F}_p$ の環準同型となるのである。)

3.2 $I=\{sp+t(i-\mu)\,|\,s,\,t,\in\mathbb{Z}[i]$ について

前節で定義した写像 ϵ_p について、$\epsilon_p(p)=0$, $\epsilon_P(i-\mu)=\bar{\mu}-\bar{\mu}=0$ となる。従って、$sp+t(i-\mu)$ $(s,t,\in\mathbb{Z}[i])$ の形で表される $\mathbb{Z}[i]$ の元はすべて ϵ_p で写して 0 になる。その

ような数全体の集合を $I = \{sp + t(i-\mu) \,|\, s, t \in \mathbb{Z}[i]\}$ とおく。

では、ϵ_p で $\mathbb{F}_p$ に写して 0 になる $\mathbb{Z}[i]$ の元全体の集合は、どのような数の集合になるのか、それを $K = \{a + bi \in \mathbb{Z}[i] \,|\, \epsilon_p(a+bi) = 0\}$ とおいて考える。。

まず、$I \subset K$ である。

次に、$a + bi \in K$ を考える。

$\epsilon_p(a+bi) = \bar{a} + \bar{b}\bar{\mu}$ で、$a = \bar{a} + kp,\ b = \bar{b} + lp,\ \mu = \bar{\mu} + mp \quad (k, l, m \in \mathbb{Z})$ と表せる。

$$\epsilon_p(a+bi) = 0 \quad \Longleftrightarrow \quad \bar{a} + \bar{b}\bar{\mu} = np \quad (n \in \mathbb{Z})$$

従って、$\bar{a} = -\bar{b}\bar{\mu} + np = -\bar{b}(\mu - mp) + np = -\bar{b}\mu + Np \quad (N \in \mathbb{Z})$

よって、$a + bi = (\bar{a} + kp) + (\bar{b} + lp)i = (-\bar{b}\mu + Np + kp) + (\bar{b} + lp)i$

$= (N + k + li)p + \bar{b}(i - \mu)$　　これは集合 I に含まれる数である。

ゆえに、$\epsilon_p(a+bi) = 0 \quad \Longrightarrow \quad a + bi \in I$　　すなわち、$K \subset I$

以上により、ϵ_p で写して $\mathbb{F}_p$ の 0 となる $\mathbb{Z}[i]$ の元の集合は I に等しいことがわかった。

このとき、Ker $\epsilon_p = I$ などと書く。

注意.

I の定義では、$sp + t(i-\mu)$ における $(i-\mu)$ の係数 t は $\mathbb{Z}[i]$ の元であるのに対して、$\epsilon_p(a+bi) = 0$ から計算して最後に出てきた式では、$(i-\mu)$ の係数が $\bar{b}$ という整数になっているので、どうしてなのかとしばらく疑問に思っていた。そのため、少し考えてみた。

$t = c + di \quad (c, d \in \mathbb{Z})$ とおいて、$t(i-\mu) = (c+di)(i-\mu)$ を考えてみる。

$(c+di)(i-\mu) = \{(c - d\mu) + d(i+\mu)\}(i-\mu) = (c-d\mu)(i-\mu) + d(-1-\mu^2)$ と変形し、

$\mu^2 + 1 = Mp \quad (M \in \mathbb{Z})$ とおけることから、$t(i-\mu) = -dMp + (c-d\mu)(i-\mu)$ となる。従って、

$sp + t(i-\mu) = (s - dM)p + (c - d\mu)(i-\mu)$

と $(i-\mu)$ の係数を整数にすることができる。

整数の範囲で、1 次式 $ax + by \quad (a, b \in \mathbb{Z})$ により a, b の最小公倍数 d を表すことができるが、そのとき、a, b の取り方は一通りではなかった。

同様に、$sp + t(i-\mu) \quad (s, t \in \mathbb{Z}[i])$ によって、p と $i - \mu$ の $\mathbb{Z}[i]$ における最大公約数というべき数 (p と $i-\mu$ の両方を $\mathbb{Z}[i]$ の中で割り切りる数の中で絶対値が最大の数) を表すことができる。そのときの s, t の取り方は 1 通りでは無く、その中に t が整数となるものをとることができる。

注意 2.

栗原先生の本で $a^2 + b^2 = p$ について取り扱っているところでは、天下り的に $I = \{sp + t(\mu + i) \,|\, s, t \in \mathbb{Z}[i]\}$ を考えていた。説明に従って証明を追っていけば、確かに結論にたどり着くのであるが、どうしてこの集合を考えるのか、わかりにくかった。そこで自分で少し考えてみたところ、$a + bi$ を $\bar{a} + \bar{b}\bar{\mu}$ に結び付ける写像の核（Kernel）として $I = \{sp + t(i-\mu) \,|\, s, t \in \mathbb{Z}[i]\}$ と定義するのが自然だと思えた。

環の間の準同型写像について、その核（Kernel) はイデアルになる。そして、$\mathbb{Z}$ や $\mathbb{Z}[i]$ のようなユークリッド環においては、すべてのイデアルが単項生成イデアルになる。 イデアル I の生成元を考えると、それは、 I に含まれる元の中で絶対値が最小となる。 I

には p が含まれているから、生成元の絶対値 2 乗は、 p の絶対値の 2 乗の p^2 を割り切る。そのことから結論に至るのである。

$p \equiv 1 \pmod 4$ のとき、 g を $\mathbb{F}_p$ の生成元として、$a = g^{\frac{p-1}{4}}$ と置くと、 $a^2 = g^{\frac{p-1}{2}} = -1$ となる。$a + np \quad (n \in \mathbb{Z})$ についても、$(a+np)^2 \equiv -1 \pmod p$ となる。 $a + np$ の中で絶対値が最も小さいものを μ とする。このとき、 $-\dfrac{p}{2} < \mu < \dfrac{p}{2}$ が成り立つ。（負になることもあり得る。）

いくつかの奇素数 p について $I = \{sp + t(i-\mu) \,|\, s, t, \in \mathbb{Z}[i]\}$ を考えてみる。$\mathbb{Z}[i]$ において、整数における互除法と同様な計算を p と $i - \mu$ に適用して、 p と $i - \mu$ の最大公約数を具体的に求めていく。それが I の生成元となる。

- $p = 5$ のとき

  $\mu = 2$ とできる。

  $\dfrac{5}{-2+i} = \dfrac{5(-2-i)}{4+1} = -2 - i \in \mathbb{Z}[i]$ より、$5 = (-2-i)(-2+i)$ 。

  $s \cdot 5 + t(i-2) = s(-2-i)(-2+i) + t(-2+i) = \{s(-2-i) + t\}(-2+i)$

  従って、 $I = \{u(-2+i) \,|\, u \in \mathbb{Z}[i]\}$ であり、$(-2)^2 + 1^2 = 5$

- $p = 13$ のとき

  $g = 2, \quad 2^3 = 8, \quad \mu = -5$ とできる。

  $\dfrac{13}{5+i} = \dfrac{13(5-i)}{25+1} = -\dfrac{5}{2} - \dfrac{1}{2}i$ 。これに最も近い $\mathbb{Z}[i]$ の元の 1 つは、 2 （3 や $2-i, 3-i$ としてもよい） 。

  $13 = 2(5+i) + (3-2i)$

  $\dfrac{5+i}{3-2i} = \dfrac{(5+i)(3+2i)}{9+4} = \dfrac{13+13i}{13} = 1 + i \in \mathbb{Z}[i]$

  $\dfrac{13}{3-2i} = \dfrac{13(3+2i)}{9+4} = 3 + 2i$ より、$13 = (3+2i)(3-2i)$ 。

  $\dfrac{5+i}{3-2i} = \dfrac{(5+i)(3+2i)}{9+4} = 1 + i$ より、$i + 5 = (1+i)(3-2i)$ 。

  $s \cdot 13 + t(i+5) = s(3+2i)(3-2i) + t(1+i)(3-2i) = \{s(3+2i) + t(1+i)\}(3-2i)$

  従って、 $I \subset \{u(3-2i) \,|\, u \in \mathbb{Z}[i]\}$ である。

  一方、 $3 - 2i = 1 \cdot 13 + (-2)(i+5) \in I$ より、 $\{u(3-2i) \,|\, u \in \mathbb{Z}[i]\} \subset I$ である。

  従って、$I = \{u(3-2i) \,|\, u \in \mathbb{Z}[i]\}$ であり、$3^2 + (-2)^2 = 13$

- $p = 17$ のとき

  $g = 3, \quad 3^4 \equiv 13 \pmod{17}, \quad \mu = -4$ とできる。

  $\dfrac{17}{4+i} = \dfrac{17(4-i)}{16+1} = 4 - i$ 。$17 = (4-i)(4+i)$

  $17 = (4-i)(4+i)$ 。

  $s \cdot 17 + t(i+4) = s(4-i)(4+i) + t(4+i) = \{s(4-i)(i+4) + t\}(4+i)$

  従って、 $I = \{u(4+i) \,|\, u \in \mathbb{Z}[i]\}$ であり、$4^2 + 1^2 = 17$

次の定理が成り立つ。

定理 3.2.1　$p \equiv 1 \pmod 4$ を満たす素数 p について、 $-\dfrac{p}{2} < \mu < \dfrac{p}{2}$, $\mu^2 \equiv -1 \pmod p$ を満たす整数 μ をとる。

$\mathbb{Z}[i]$ から $\mathbb{F}_p$ への写像 ϵ_p を $\epsilon_p(a+bi) = \bar{a} + \bar{b}\bar{\mu}$ と定義する。

さらに $\mathrm{Ker}\ \epsilon_p = \{z \in \mathbb{Z}[i] \,|\, \epsilon_p(z) = 0\}$ 、$I = \{sp + t(i-\mu) \,|\, s, t \in \mathbb{Z}[i]\}$ とおくと、

- $\mathrm{Ker}\ \epsilon_p = I$ である。
- $\exists \alpha_0 \in I$　s.t.　$I = \{u \cdot \alpha_0 \,|\, u \in \mathbb{Z}[i]\}$

この定理の証明には、次の補題を使う。

補題 3.2.2　$\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$ のとき、$\exists q, r \in \mathbb{Z}[i]$　s.t.　$\alpha = q\beta + r$　$(0 \leqq |r| < |\beta|)$

証明）$\dfrac{\alpha}{\beta}$ に最も近い $\mathbb{Z}[i]$ の元（の 1 つ）を q とする。このとき、$\left|\dfrac{\alpha}{\beta} - q\right| \leqq \sqrt{(\frac{1}{2})^2 + (\frac{1}{2})^2} = \dfrac{1}{\sqrt{2}}$

$r = \alpha - q\beta$ とおくと、$|r| = |\alpha - q\beta| = \left|\dfrac{\alpha}{\beta} - q\right| |\beta| \leqq \dfrac{1}{\sqrt{2}}|\beta| < |\beta|$

このように定めた q, r は条件を満たす。//

定理 3.2.1 の証明）

- $\mathrm{Ker}\ (\epsilon_p) = I$ であることについては、前に示した。
- 　$\alpha = a + bi \in I$ について、 $|\alpha|^2 = a^2 + b^2$ は 0 以上の整数であるから、それが正の最小値となるもの α_0 をとることができる。

  任意の $\alpha \in I$ について、 補題 3.2.2 より、$\alpha = q\alpha_0 + r$　$(0 \leqq |r| < |\alpha_0|)$ とできる。$\alpha, \alpha_0 \in I$ のとき $r = \alpha - q\alpha_0$ も、やはり I に属する数であることは簡単に示すことができる。もし、 $0 < |r| < |\alpha_0|$ であれば、$|\alpha_0|^2$ の最小性に反する。よって、$r = 0$ である。従って、任意の $\alpha \in I$ について、 $\alpha = q\alpha_0$ と表すことができる。

  すなわち、$I = \{u \cdot \alpha_0 \,|\, u \in \mathbb{Z}[i]\}$ だといえる。

以上で定理が示された。

定理 3.2.3

$I = \{u \cdot \alpha_0 \,|\, u \in \mathbb{Z}[i]\}$　$\alpha_0 = a + bi$　$(a, b \in \mathbb{Z})$ とするとき、 $a^2 + b^2 = p$ が成り立つ。

証明）　$p \in I$ であるから、 $\exists u \in \mathbb{Z}[i]$　s.t.　$p = u\alpha_0$

絶対値の 2 乗を考えて、 $p^2 = |u|^2|\alpha_0|^2$。このとき、 $|u|^2, |\alpha_0|^2$ は自然数で p^2 の約数であるから、$|\alpha_0|^2 = 1, p, p^2$ のいずれかである。

- $|\alpha_0| = p^2$ とすると

  $\mu \in I$ であり、$|\mu|^2 < \left(\frac{p}{2}\right)^2 < p^2 = |\alpha_0|^2$ となる。これは、$|\alpha_0|^2$ の最小性に反する。したがって、$|\alpha_0| = p^2$ となることはない。

- $|\alpha_0| = 1$ とすると

  $sp + (c+di)(i-\mu)\} = 1$ となる、$s,\, t = c+di \in \mathbb{Z}[i]$ が存在する。両辺の実部、虚部を p による法で考えて、$-c\mu - d \equiv 1, \quad c - d\mu \equiv 0 \pmod{p}$

  第2式から $c \equiv d\mu$ として第1式に代入すると、左辺 $\equiv -d\mu \cdot \mu - d \equiv -d(\mu^2+1) \equiv -d(-1+1) \equiv 0$。　右辺　$\equiv 1$ 。これから $0 \equiv 1 \pmod{p}$ となり、矛盾。したがって、$|\alpha_0| = 1$ となることはない。

以上から、$|\alpha_0|^2 = p$ が成り立つ。　　（証明終わり）

定理 3.2.4　$\pm\alpha_0,\, \pm i\alpha_0.\, \pm\overline{\alpha_0},\, \pm i\overline{\alpha_0}$ の絶対値の2乗は、いずれも p に等しい。また、$\alpha = c+di$ が $c^2+d^2 = p$ をみたすとすれば、α は $\pm\alpha_0,\, \pm i\alpha_0,\, \pm\overline{\alpha_0},\, \pm i\overline{\alpha_0}$ のいずれかに等しい。

証明）　前半は自明である。

$c^2+d^2 = p$ が成り立つとする。$c+di = (c+d\mu) + d(i-\mu)$ と変形し、$(c+d\mu)$ の部分を考える。

$(c+d\mu)(c-d\mu) = c^2 - d^2\mu^2 \equiv c^2 - d^2(-1) \equiv c^2+d^2 \equiv 0 \pmod{p}$

従って、整数 $c+d\mu,\, c-d\mu$ のいずれか一方、もしくは両方が p で割り切れなければいけない。

- $c + d\mu = kp \quad (k \in \mathbb{Z})$ のとき

  $c+di = kp + d(i-\mu) \in I$ となるから、$c+di = u\alpha_0 \quad (u \in \mathbb{Z}[i])$ となる。

  $(\because I = \{u \cdot \alpha_0 \,|\, u \in \mathbb{Z}[i]\})$

  $|c+di|^2 = |u|^2|\alpha_0|^2 \qquad p = |u|^2 p \qquad |u|^2 = 1 \qquad u = \pm 1,\, \pm i \qquad \therefore \alpha = \pm\alpha_0,\, \pm i\alpha_0$

- $c - d\mu = kp \quad (k \in \mathbb{Z})$ のとき

  $c-di = (c-d\mu) - d(i-\mu) = kp + (-d)(i-\mu) \in I$ となるから、$c-di = u\alpha_0 \quad (u \in \mathbb{Z}[i])$ となる。

  $(\because I = \{u \cdot \alpha_0 \,|\, u \in \mathbb{Z}[i]\})$

  $|c-di|^2 = |u|^2|\alpha_0|^2 \qquad p = |u|^2 p \qquad |u|^2 = 1 \qquad u = \pm 1,\, \pm i$

  $\therefore \overline{\alpha} = \pm\alpha_0,\, \pm i\alpha_0 \qquad \alpha = \pm\overline{\alpha_0},\, \pm i\overline{\alpha_0}$

（証明終わり）

$\alpha = \pm\alpha_0,\, \pm i\alpha_0,\, \pm\overline{\alpha_0},\, \pm i\overline{\alpha_0} = \pm(a+bi),\, \pm(-b+ai),\, \pm(a-bi),\, \pm(b+ai)$

であるから、$a^2+b^2 = p$ を満たす整数の組は、$\pm(a,b),\, \pm(a,-b),\, \pm(b,a),\, \pm(b,-a)$ の8通りである。これらは、本質的に同じようなもので、例えば、$a, b > 0$ で a は奇数、b は偶数であるという条件をつけると1通りしかない。

あるいは、$[1]_4[g^2]_4$ の計算では

$$\begin{cases} (4V+1)^2+(4W)^2=p & (p\equiv 1 \pmod 8) \\ (4V+1)^2+(4W+2)^2=p & (p\equiv 5 \pmod 8) \end{cases}$$

の形が出てきたので、$a=4V+1\equiv 1 \pmod 4$, $b>0$ (偶数) という条件とすれば、やはり 1 通りになる。なぜならば、a を奇数とするとき、$a\equiv 1$ もしくは、$a\equiv 3 \pmod 4$ のいずれかになるが、もし、$a\equiv 3 \pmod 4$ ならば、a の代わりに $-a$ を a とすれば $a\equiv 1 \pmod 4$ とできる。

このとき、$b^2=p-a^2=p-(4V+1)^2=p-8V(2V+1)-1$ であるから、

$p\equiv 1 \pmod 8$ のとき $b^2\equiv 0 \pmod 8$ 、$p\equiv 5 \pmod 8$ のとき $b^2\equiv 4 \pmod 8$

従って、$p\equiv 1 \pmod 8$ のとき $b=4W$ 、$p\equiv 5 \pmod 8$ のとき $b=4W+2$ となる。そして、$Y\geqq 0$ とすれば、b の取り方は 1 通りに限られる。

以上により、

$(4V+1)^2+b^2=p$ を満たす整数 V がただ 1 つあり、

$$[1]_4[g^2]_4=\begin{cases} -\dfrac{p-1}{16}+\dfrac{V}{2}\sqrt{p} & (p\equiv 1 \pmod 8) \\ \dfrac{3p+1}{16}+\dfrac{V}{2}\sqrt{p} & (p\equiv 5 \pmod 8) \end{cases}$$

とできる。

※　第 2 章で扱ったときは、V がただ 1 つ定まることは言えなかった。

4　ガウスの 4 次周期を解に持つ 2 次方程式について

4.1　$[1]_4$ と $[g^2]_4$ を解に持つ 2 次方程式について

$[1]_4+[g^2]_4=[1]_2=\dfrac{-1+\sqrt{p}}{2}$ および、第 2 章における $[1]_4[g^2]_4$ に関する結果から、$[1]_4$, $[g^2]_4$ を 2 つの解にもつ x の 2 次方程式は、以下のとおりになる。

(i) $p\equiv 1 \pmod 8$ のとき

$$x^2-\frac{-1+\sqrt{p}}{2}x-\frac{p-1}{16}+\frac{V}{2}\sqrt{p}=0$$

このとき、判別式は

$$D=\left(\frac{-1+\sqrt{p}}{2}\right)^2-4\left(-\frac{p-1}{16}+\frac{V}{2}\sqrt{p}\right)=\frac{1}{4}\left\{(1+p-2\sqrt{p})+(p-1)-8V\sqrt{p})\right\}$$

$$=\frac{1}{2}\left\{p-(4V+1)\sqrt{p}\right\}=\frac{1}{2}\left(p-a\sqrt{p}\right)$$

(ii) $p \equiv 5 \pmod 8$ のとき

$$x^2 - \frac{-1+\sqrt{p}}{2}x + \frac{3p+1}{16} + \frac{V}{2}\sqrt{p} = 0$$

このとき、判別式は

$$D = \left(\frac{-1+\sqrt{p}}{2}\right)^2 - 4\left(\frac{3p+1}{16} + \frac{V}{2}\sqrt{p}\right) = \frac{1}{4}\left\{(1+p-2\sqrt{p}) + (-3p-1) - 8V\sqrt{p})\right\}$$

$$= \frac{1}{2}\left\{-p - (4V+1)\sqrt{p}\right\} = \frac{1}{2}\left(-p - a\sqrt{p}\right)$$

なお、2 次方程式の解は $x = \frac{1}{2}\left\{\frac{-1+\sqrt{p}}{2} \pm \sqrt{D}\right\}$ である。

4.2 $[g]_4$と $[g^3]_4$ を解に持つ 2 次方程式について

$[g]_4 + [g^3]_4 = g1]_2 = \frac{-1-\sqrt{p}}{2}$ および、第 2 章における $[g]_4[g^3]_4$ に関する結果から、$[g]_4$, $[g^3]_4$ を 2 つの解にもつ x の 2 次方程式は、以下のとおりになる。

(i) $p \equiv 1 \pmod 8$ のとき

$$x^2 - \frac{-1-\sqrt{p}}{2}x - \frac{p-1}{16} - \frac{V}{2}\sqrt{p} = 0$$

このとき、判別式は

$$D' = \left(\frac{-1-\sqrt{p}}{2}\right)^2 - 4\left(-\frac{p-1}{16} - \frac{V}{2}\sqrt{p}\right) = \frac{1}{4}\left\{(1+p+2\sqrt{p}) + (p-1) + 8V\sqrt{p})\right\}$$

$$= \frac{1}{2}\left\{p + (4X+1)\sqrt{p}\right\} = \frac{1}{2}\left(p + a\sqrt{p}\right)$$

(ii) $p \equiv 5 \pmod 8$ のとき

$$x^2 - \frac{-1-\sqrt{p}}{2}x + \frac{3p+1}{16} - \frac{V}{2}\sqrt{p} = 0$$

このとき、判別式は

$$D' = \left(\frac{-1-\sqrt{p}}{2}\right)^2 - 4\left(\frac{3p+1}{16} - \frac{V}{2}\sqrt{p}\right) = \frac{1}{4}\left\{(1+p+2\sqrt{p}) + (-3p-1) + 8V\sqrt{p})\right\}$$

$$= \frac{1}{2}\left\{-p + (4X+1)\sqrt{p}\right\} = \frac{1}{2}\left(-p + a\sqrt{p}\right)$$

なお、２次方程式の解は $x = \dfrac{1}{2}\left\{\dfrac{-1+\sqrt{p}}{2} \pm \sqrt{D}\right\}$ である。

※　上記では、$a = 4V+1 \equiv 1 \pmod 4$ で考えているが、栗原先生の本では、$p \equiv 5 \pmod 8$ のときは、$a = -(4V+1)$ としている。ガウスがこのようにしているとのことである。すると、そのときの判別式は

$$D = \frac{1}{2}\left(-p + a\sqrt{p}\right) = -\frac{1}{2}\left(p - a\sqrt{p}\right)$$

となる。

こうすると、

$$D = (-1)^{\frac{p-1}{4}} \cdot \frac{\left(p - a\sqrt{p}\right)}{2}$$

といった、きれいな書き方にまとめることができる。

同様に、

$$D' = (-1)^{\frac{p-1}{4}} \cdot \frac{\left(p + a\sqrt{p}\right)}{2}$$

となる。

４次剰余の相互法則を考えるときに、D を $\mathbb{F}_q$　(q は p とは相異なる素数) に写したものが、$\mathbb{F}_q$ の中で平方数になっているのかどうかが鍵となる。そのことについては、ノートその３で扱う予定である。