２次ガウス周期の基本定理に関するノート

2019 年夏
石動高校　片山　喜美

定規とコンパスを使って正 17 角形の作図が可能であることを、19 歳のガウスは、1 の 17 乗根のうち 1 を除く 16 個の虚数ををうまく並べて、それを 2 分割したものの和を計算し、次に 4 分割したものの和、さらに、8 分割したものの和を順次計算していくことで示した。いわゆる**ガウスの f 項周期**のアイディアである。

概略としては、以下に述べるようなことである。$\zeta = e^{\frac{2\pi}{17}}$ とすると、$1, \zeta, \zeta^2, \cdots\cdots, \zeta^{16}$ は複素数平面において正 17 角形の頂点を表す。それらのうち、1 を除く $\zeta, \zeta^2, \cdots\cdots, \zeta^{16}$ の 16 個を「ある規則」に基づいて $\zeta^1, \zeta^3, \zeta^9, \zeta^{10}, \zeta^{13}, \zeta^5, \zeta^{15}, \zeta^{11}, \zeta^{16}, \zeta^{14}, \zeta^8, \zeta^7, \zeta^4, \zeta^{12}, \zeta^2, \zeta^6$ と並べる。これを順次 2 分割、4 分割、8 分割して、その和を計算していくとうまくいくのである。

その第 1 段階で、「ある規則」で並べたものを 1 つ置きにとって和をとったものである**２次のガウス周期** $a_1 = \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2$ は、残りの項の和 $a_2 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$ とともに、2 次方程式 $x^2 + x - 4 = 0$ の解であり、$a_1 = \dfrac{-1 + \sqrt{17}}{2}$,　$a_2 = \dfrac{-1 - \sqrt{17}}{2}$ となるのである。

一般の奇素数 p についても、1 の p 乗根のうち、1 を除くものを「ある規則」に基づいて並べたものを 1 つ置きにとった和に関して、きれいな結果が導かれる。そのことについて、栗原将人著「ガウスの数論世界をゆく」に従って、自分なりに計算してみた。このノートは先に作成した「正 17 角形の作図とガウス周期について」に続くものである。

1　整数を奇素数 p で割った余りの集合について

整数を 17 で割った余りは、$0, 1, 2, \cdots\cdots, 16$ のいずれかである。$\mathbb{F}_{17} = \{0, 1, 2, \cdots\cdots, 16\}$ に普通の整数の和・差・積から導かれる計算を考える。すなわち、もし、この範囲からはずれたら、17 で割った余りになるように調整するのである。

例えば、$a = 2, b = 3$ なら、そのまま $a + b = 5$ でよいが、$a = 12, b = 13$ なら、普通に足すと 25 で範囲からはみ出るので、それを 17 で割った余りを考え、$a + b = 8$ とする。同様に、普通の整数の計算で $12 - 13 = -1$、$12 \times 13 = 156$ となるものを 17 で割った余りに直し、$a - b = 16$ 、$ab = 3$ とする。詳細は省略するが、この計算方法で和・差・積は全て $\mathbb{F}_{17}$ の範囲に収まり、結合法則や分配法則を満たす。すなわち、うまく計算が進むということである。

問題は、商（割り算）である。これについては、以下の補題から考えていく。

補題１．１　$a \in \mathbb{F}_{17}, a \neq 0$ ならば、$b \in \mathbb{F}_{17}$ で　$ab = 1$ を満たすものがただ一つ存在する。

証明１）乗積表による証明

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	$\underline{1}$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	4	6	8	10	12	14	16	$\underline{1}$	3	5	7	9	11	13	15
3	3	6	9	12	15	$\underline{1}$	4	7	10	31	16	2	5	8	11	14
4	4	8	12	16	3	7	11	15	2	6	10	14	$\underline{1}$	5	9	13
5	5	10	15	3	8	13	$\underline{1}$	6	11	16	4	9	14	2	7	12
6	6	12	$\underline{1}$	7	13	2	8	14	3	9	15	4	10	16	5	11
7	7	14	4	11	$\underline{1}$	8	15	5	12	2	9	16	6	13	3	10
8	8	16	7	15	6	14	5	13	4	12	3	11	2	10	$\underline{1}$	9
9	9	$\underline{1}$	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	10	3	13	6	16	9	2	12	5	15	8	$\underline{1}$	11	4	14	7
11	11	5	16	10	4	15	9	3	14	8	2	13	7	$\underline{1}$	12	6
12	12	7	2	14	9	4	16	11	6	$\underline{1}$	13	8	3	15	10	5
13	13	9	5	$\underline{1}$	14	10	6	2	15	11	7	3	16	12	8	4
14	14	11	8	5	2	16	13	10	7	4	$\underline{1}$	15	12	9	6	3
15	15	13	11	9	7	5	3	$\underline{1}$	16	14	12	10	8	6	4	2
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	$\underline{1}$

上の表より、補題が成り立つことがわかる。//

証明２）ユークリッドの互除法による証明

$1 \leqq a \leqq 16$ のとき、 a と素数 17 は互いに素であるから、ユークリッドの互除法を用いた計算により、$ax + 17y = 1$ を満たす整数 x, y を求めることができる。このとき $ax \equiv 1 \pmod{17}$ をみたす。x を 17 で割った余りを b とすれば、$\mathbb{F}_{17}$ における計算では、$ab = 1$ となる。

一意性については、２つの $1 \leqq b_1, b_2 \leqq 16$ に対して、$ab_1 = 1$, $ab_2 = 1$ が成り立ったとすると、差し引いて、$a(b_1 - b_2) = 0$ 。このとき、 $-15 \leqq b_1 - b_2 \leqq 15$ であるから、先の式を満たすためには,$b_1 - b_2 = 0$ とならなければいけない。従って、 $ab = 1, b \in \mathbb{F}_{17}$ を満たす b は唯一つである。//

定義１．２

$a \in \mathbb{F}_{17}, a \neq 0$ に対して、$b \in \mathbb{F}_{17}$ で　$ab = 1$ を満たすものを $\mathbb{F}_{17}$ の乗法に関する a の **逆元** とよび、a^{-1} と表す。

また、$a, b \in \mathbb{F}_{17}$,　$b \neq 0$ のとき、商 $a \div b$ は、積 ab^{-1} で計算される数を表すものとする。

例.　　$a = 4, b = 7$ のとき、 $a \div b = ab^{-1} = 4 \cdot 7^{-1} = 4 \cdot 5 = 3$

これらのことから、 $\mathbb{F}_{17}$ は四則演算に関して閉じており、和及び積に関する逆元を持ち、また、しかるべき計算法則を満たしている。すなわち、$\mathbb{F}_{17}$ **は体である。**

さて、$\mathbb{F}_{17}$ から 0 を除いたものは、乗法に関して群をなす。それを $\mathbb{F}_{17}^{\times}$ と表す。

$\mathbb{F}_{17}^{\times}$ において、

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^n	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

となり、3 のべき乗 $3^0, 3^1, \cdots, 3^{15}$ で、$1, 2, \cdots\cdots 16$ を全て表せることがわかる。
（なお、 $3^{16} = 1$ である。）

定義１．３
有限乗法群 G について、1 つの元 $g \in G$ があり、G の任意の元は g のべき乗で表されるとき、G は g によって生成される巡回群であるという。このとき、g を群 G の生成元という。

例　$\mathbb{F}_{17}^{\times}$ は、3 を生成元とする巡回群である。

定理１．４
任意の奇素数 p について、体 $\mathbb{F}_p$ の 0 以外の元がなす乗法群 $\mathbb{F}_p^{\times} = \{1, 2, \cdots\cdots, p-1\}$ は巡回群となる。

※　この定理は大変重要である。いくつかの証明方法があるが、ここでは省略する。

2　$\mathbb{F}_p^{\times}$ の２分割について

定理１．４により、$\mathbb{F}_p^{\times} = \{g^0, g^1, \cdots\cdots, g^{p-2}\}$　(g は生成元) と表すことができる。
この順に並べたものを 1 つ置きにとって
$H_2 = \{g^0, g^2, \cdots\cdots, g^{p-3}\}$,　$gH_2 = \{g^1, g^3, \cdots\cdots, g^{p-2}\}$
という風に $\mathbb{F}_p^{\times}$ を 2 つに分割する。

定理２．１
H_2 は、$\mathbb{F}_p^{\times}$ の平方数全体の集合である。

証明）H_2 の元が全て平方数であることは明らかである。
$a \in \mathbb{F}_p^{\times}$ が平方数であるとき、$\exists x \in \mathbb{F}_p^{\times}$　$s.t.$　$a = x^2$
このとき、 g が生成元であることから、 $x = g^k$ とおける。従って、$a = g^{2k}$ となる。
$2k, p-1$ とも偶数であるから、$2k$ を $p-1$ で割った余りは偶数であり、$2m$　$(0 \leqq 2m \leqq p-3)$ とできる。 $g^{p-1} = 1$ であるから、$a = x^k = g^{2k} = g^{(p-1)l+2m} = g^{2m} = (g^m)^2 \in H_2$
以上により、定理は示された。//

$\zeta = e^{\frac{2\pi}{p}}$ とおく。
正 17 角形の作図可能性について復習する。$\zeta = e^{\frac{2\pi}{17}}$ と置くと、$1, \zeta, \zeta^2, \cdots, \zeta^{16}$ は正 17 角形の頂点となる。前節で述べたように、整数を 17 で割った余りで考える数の世界で、0 を除いた $\mathbb{F}_{17}^{\times} = \{1, 2, \cdots\cdots, 16\}$ は 3 を生成元とする巡回乗法群である。生成元 3 の巾で表して、
$\mathbb{F}_{17}^{\times} = \{3^0, 3^1, \cdots\cdots, 3^{15}\} = \{1, 3, 9, 10, 13, 5, 15, 11.16.14, 8, 7, 4, 12, 2, 6\}$ となる。

１つおきにとって、
$H_2 = \{1, 9, 13, 15, 16.8, 4, 2\}$　　$3H_2 = \{3, 10, 5, 11.14, 7, 12, 6\}$
とする。
そして、$a_1 = \sum_{\alpha \in H_2} \zeta^{\alpha}$　　$a_2 = \sum_{\alpha \in H_2} \zeta^{3\alpha} = \sum_{\alpha \in 3H_2} \zeta^{\alpha}$
とすると、 $a_1 + a_2 = -1$,　$a_1 \cdot a_2 = -4$ となり、2 次方程式 $x^2 + x - 4 = 0$ に結びつくのであった。見通しのよい計算を行うためには、次の記号の定義と「ガウスの積公式」が役立つ。

定義２．２　$n \in \mathbb{Z}$ に対して、$[n]_2 = \sum_{\alpha \in H_2} \zeta^{n\alpha}$ と定義する。

この記号を用いると、 $a_1 = [1]_2$,　$a_2 = [3]_2$ となる。

次の定理が成り立つ。

定理２．１　（ガウスの積公式）

$$[m]_2 \cdot [n]_2 = \sum_{\alpha \in H_2} [m + n\alpha]_2 = \sum_{\alpha \in H_2} [m\alpha + n]_2$$

この定理の証明は、別のレポート「正 17 角形の作図とガウス周期について」に記載してあるので、ここでは省略する。この定理により、2 分割のときの積 $a_1 \cdot a_2$ は

$$a_1 \cdot a_2 = [1]_2 \cdot [3]_2 = \sum_{\alpha \in H_2} [1 + 3\alpha]_2 = \sum_{\alpha \in H_2} [1 \cdot \alpha + 3]_2$$

として計算を進めていくのである。

その他の奇素数 p についても、$p = 17$ のときと同様に a_1, a_2 の値を求めてみる。
g を $\mathbb{F}_p^{\times}$ の原始根として、$a_1 = [1]_2$, $a_2 = [g]_2$
$a_1 \cdot a_2 = [1]_2 \cdot [g]_2 = \sum_{\alpha \in H_2} [1 \cdot \alpha + g]_2$ により計算していく。

2.1　$p = 3$ の場合

$1, \zeta, \zeta^2$ が正三角形の頂点。$a_1 + a_2 = \zeta + \zeta^2 = -1$,　$a_1 \cdot a_2 = \zeta \cdot \zeta^2 = \zeta^3 = 1$

従って、2 次方程式 $x^2 + x + 1 = 0$ を満たす。これを解いて　$x = \dfrac{-1 \pm \sqrt{3}i}{2}$
a_1 の虚数部は正であるから、$a_1 = \dfrac{-1 + \sqrt{3}i}{2}$　$a_2 = \dfrac{-1 - \sqrt{3}i}{2}$

2.2　$p = 5$ の場合

n	0	1	2	3
$2^n \pmod 5$	1	2	4	3

左の表からわかるように、$\mathbb{F}_5^{\times}$ は 2 で生成される巡回群となる。従って、 $H_2 = \{1, 4\}$　$2H_2 = \{2, 3\}$

$\zeta, \zeta^2, \zeta^4, \zeta^3$ と並べ、$a_1 = \zeta + \zeta^4 \quad a_2 = \zeta^2 + \zeta^3$

- $a_1 + a_2 = [1]_1 = -1$
- $a_1 \cdot a_2 = \sum_{\alpha \in H_2} [1 \cdot \alpha + 2]_2 = [1+2]_2 + [4+2]_2 = [3]_2 + [1]_2 = a_2 + a_1 = -1$

従って、2 次方程式 $x^2 + x - 1 = 0$ を満たす。これを解いて　$x = \dfrac{-1 \pm \sqrt{5}}{2}$

$a_= \zeta + \zeta^4 = 2\cos\dfrac{2\pi}{5} > 0$ より、$a_1 = \dfrac{-1+\sqrt{5}}{2}$　　$\cos\dfrac{2\pi}{5} = \dfrac{-1+\sqrt{5}}{4}$

2.3　$p = 7$ の場合

n	0	1	2	3	4	5
$3^n \pmod 7$	1	3	2	6	4	5

左の表からわかるように、$\mathbb{F}_7^\times$ は 3 で生成される巡回群となる。

従って、 $H_2 = \{1, 2, 4\} \quad 2H_2 = \{3, 6, 5\}$

- $a_1 + a_2 = [1]_1 = -1$
- $a_1 \cdot a_2 = \sum_{\alpha \in H_2} [1 \cdot \alpha + 3]_2 = [1+3]_2 + [2+3]_2 + [4+3]_2 = [4]_2 + [5]_2 + [0]_2 = a_1 + a_2 + 3 = -1$

  ただし、$[0]_2 = \sum_{\alpha \in H_2} \zeta^0 = \sum_{\alpha \in H_2} 1 =^{\#} H_2 = 3$ を用いた。

従って、2 次方程式 $x^2 + x + 2 = 0$ を満たす。これを解いて　$x = \dfrac{-1 \pm \sqrt{7}i}{2}$

2.4　$p = 11$ の場合

n	0	1	2	3	4	5	6	7	8	9
$2^n \pmod{11}$	1	2	4	8	5	10	9	7	3	6

上の表からわかるように、$\mathbb{F}_{11}^\times$ は 2 で生成される巡回群となる。

従って、 $H_2 = \{1, 4, 5, 9, 3\} \quad 2H_2 = \{2, 8, 10, 7, 6\}$

- $a_1 + a_2 = [1]_1 = -1$
- $a_1 \cdot a_2 = \sum_{\alpha \in H_2} [1 \cdot \alpha + 2]_2 = [1+2]_2 + [4+2]_2 + [5+2]_2 + [9+2]_2 + [3+2]_2 \quad =$
  $[3]_2 + [6]_2 + [7]_2 + [0]_2 + [5]_2 = a_1 + a_2 + a_2 + 5 + a_1 = 2(a_1 + a_2) = -2 + 5 = 3$

  ただし、$[0]_2 = \sum_{\alpha \in H_2} \zeta^0 = \sum_{\alpha \in H_2} 1 =^{\#} H_2 = 5$ を用いた。

従って、2 次方程式 $x^2 + x + 3 = 0$ を満たす。これを解いて　$x = \dfrac{-1 \pm \sqrt{11}i}{2}$

2.5 $p = 13$ の場合

n	0	1	2	3	4	5	6	7	8	9	10	11
$2^n \pmod{13}$	1	2	4	8	3	6	12	11	9	5	10	7

上の表からわかるように、$\mathbb{F}_{13}^{\times}$ は 2 で生成される巡回群となる。

従って、 $H_2 = \{1, 4, 3, 12, 9, 10\}$ $2H_2 = \{2, 8, 6, 11, 5, 7\}$

- $a_1 + a_2 = [1]_1 = -1$
- $a_1 \cdot a_2 = \sum_{\alpha \in H_2} [1 \cdot \alpha + 2]_2$
  $= [1+2]_2 + [4+2]_2 + [3+2]_2 + [12+2]_2 + [9+2]_2 + [10+2]_2$
  $= [3]_2 + [6]_2 + [5]_2 + [1]_2 + [11]_2 + [12]_2 = a_1 + a_2 + a_2 + a_1 + a_2 + a_1$
  $= 3(a_1 + a_2) = -3$

従って、2 次方程式 $x^2 + x - 3 = 0$ を満たす。これを解いて $\quad x = \dfrac{-1 \pm \sqrt{13}}{2}$

2.6 $p = 19, 23$ の場合

$p = 19, 23$ について、ここまでの奇素数と同様に、以下のように求めていく。

- $2^n \pmod{p}$, $3^n \pmod{p}$ を順に調べて、 $\mathbb{F}_p^{\times} = \{1, 2, \cdots, p-1\}$ の乗法群としての生成元 g を見つける。
- $H_2 = \{g^0, g^2, \cdots\cdots, g^{p-3}\}$ $\quad gH_2 = \{g^1, g^3, \cdots\cdots, g^{p-2}\}$ とおく。
- $a_1 = \sum_{\alpha \in H_2} \zeta^{\alpha} = [1]_2$ $\quad a_1 = \sum_{\alpha \in gH_2} \zeta^{\alpha} = [g]_2$
- $a_1 + a_2 = [1]_2 = -1$
- ガウスの積公式により、$a_1 \cdot a_2 = [1]_2 \cdot [g]_2 = \sum_{\alpha \in H_2} [\alpha + g]_2$ とし、以降具体的に計算する。

結果として a_1 と a_2 を解とする 2 時方程式とその解は

- p = 19 のとき $\quad x^2 + x + 5 = 0 \quad x = \dfrac{-1 \pm \sqrt{19}i}{2}$
- p = 23 のとき $\quad x^2 + x + 6 = 0 \quad x = \dfrac{-1 \pm \sqrt{23}i}{2}$

実際の計算はここでは省略する。やってみると時間と手間がかかるだろうが、いい練習問題となることと思う。そして、一般の奇素数 p について成り立つことが予想されるものと思う。

3　２次ガウス周期の基本定理

前節までに計算した結果によると、奇素数 $p=3,5,7,11,13,17,19,23$ に対して $\zeta=e^{\frac{2\pi}{p}}$ とおき、$\zeta,\zeta^2,\cdots\cdots,\zeta^{p-1}$ をある規則で２つに分けてた和を a_1 と a_2 とすると、それらは $\dfrac{-1\pm\sqrt{p}}{2}$ となるか、$\dfrac{-1\pm\sqrt{p}i}{2}$ となるのであった。一般の奇素数についても同様な結果が得られることを示したい。また、実数となるのか虚数となるのか、素数 p に関する判定基準を求めたい。。

この節では、$\zeta=e^{\frac{2\pi}{p}}=\cos\dfrac{2\pi}{p}+i\sin\dfrac{2\pi}{p}$ とする。

前節で述べたように、奇素数 p について、整数を p で割った余りで０以外のものの集合は、$1\leqq g\leqq p-1$ を満たす整数 g を生成元とする巡回群となる。この g を **「素数 p についての原始根」** と呼ぶ。

前節までの具体的な奇素数に関する計算では、この定理を用いるのでは無く、天下り的ではあるが具体的に $g=2$ や $g=3$ が生成元となることを示して進めた。

定義３．１　奇素数 p に関する原始根を g とし、

$$H_2=\{g^0,g^2,\cdots\cdots,g^{p-3}\}\qquad gH_2=\{g^1,g^3,\cdots\cdots,g^{p-2}\}$$

と定義する。

さらに、 $p-1$ の任意の約数 d に対して、

$$H_d=\{g^0,g^d,g^{2d},\cdots\cdots,g^{p-d-1}\}$$

$$gH_d=\{g^1,g^{d+1}g^{2d+1},\cdots\cdots,g^{p-d}\}$$

$$\cdots\cdots$$

$$\cdots\cdots$$

$$g^{d-1}H_d=\{g^{d-1},g^{2d-11}g^{3d-1},\cdots\cdots,g^{p-2}\}$$

とおく。($d=2$ としたものは、前の定義と同じになっている)

定義３．２　d を $p-1$ の約数とする。 $n\in\mathbb{Z}$ に対して、 $[n]_d=\displaystyle\sum_{\alpha\in H_d}\zeta^{n\alpha}$ と定義する。

定義３．３　$a_1=\zeta+\zeta^{g^2}+\zeta^{g^3}+\cdots\cdots+\zeta^{g^{p-3}}=\displaystyle\sum_{\alpha\in H_2}\zeta^{\alpha}$

$$a_2=\zeta^{g}+\zeta^{g^3}+\zeta^{g^5}+\cdots\cdots+\zeta^{g^{p-2}}=\sum_{\alpha\in H_2}\zeta^{\alpha}$$

とおく。

＜注意＞

- $a_1=[1]_2$ である。これを**奇素数 p に関する２次ガウス周期**という。

  また、$p-1$ の約数 d に対して、$[1]_d=\sum_{\alpha\in H_d}\zeta^{\alpha}$ を **d 次ガウス周期**という。

- $a_2=[g]_2$ である。

補題３－１　　$a_1+a_2=-1$

証明）　$a_1+a_2=\zeta+\zeta^2+\cdots\cdots+\zeta^{p-1}=1+\zeta+\zeta^2+\cdots\cdots+\zeta^{p-1}-1=\dfrac{1-\zeta^p}{1-\zeta}-1=\dfrac{1-1}{1-\zeta}-1=0-1=-1$　//

これに加えて、積 $a_1\cdot a_2$ がわかればよいのだが、それぞれ ζ の巾の和であるものの積を展開して得られるものを、うまく整理するのは簡単ではない。

$p=3,5,7,11,13,17,19,23$ について、積 $a_1\cdot a_2$ の値から、さらに、a_1,a_2 を解とする２次方程式を作って解いてみると、$x=\dfrac{-1\pm\sqrt{p}}{2}$ もしくは、$x=\dfrac{-1\pm\sqrt{p}\,i}{2}$ という結果が得られた。解の方から積 $a_1\cdot a_2$ の値に逆戻りする。

$x^2+x+c=0$ の解は $x=\dfrac{-1\pm\sqrt{1-4c}}{2}$ であるから、$1-4c=p$ もしくは $1-4c=-p$ となる。従って、$c=\dfrac{1-p}{4}$ もしくは、$c=\dfrac{1+p}{4}$ となるのであろう。積 $a_1\cdot a_2$ がそれらの値になることを示す。

n を $g-1$ で割った余りを $\overline{n}$ で表すことにする。
$\overline{\alpha+g}$ が H_2 に属するなら $[\alpha+g]_2=[1]_2$、gH_2 に属するなら $[\alpha+g]_2=[g]_2$

まず、$p=17$ のときの計算を振り返ってみる。

$\alpha\in H_2$	1	9	13	15	16	8	4	2
$\alpha+3$	4	12	16	1	2	11	7	5
H_2に属する	○		○	○	○			
$3H_2$に属する		○				○	○	○

(1) $\alpha+3=\beta$　　$(\alpha,\beta\in H_2)$ を満たすもの
$(\alpha,\beta)=(1,4),(16,2),(13,16),(15,1)$

(2) $\alpha+3=3\beta$　　$(\alpha,\beta\in H_2)$ を満たすもの
必要に応じて $3^{-1}\equiv 6 \pmod{17}$ も用いて、$3^{-1}12=4$,　$3^{-1}11=15$,　$3^{-1}7=8$,　$3^{-1}5=13$ であるから、
$(\alpha,\beta)=(9,4),(8,15),(4,8),(2,13)$

(1),(2) とも 4 つずつなので、$a_1 \cdot a_2 = [1]_2 \cdot [3]_2 = \sum_{\alpha \in H_2} [\alpha + 3]_2 = 4[1]_2 + 4[3]_2 = -4$　と
なる。

一般の p 及び乗法群 $\mathbb{F}_p^{\times}$ の巡回群としての生成元 g について、(1)$\alpha + g = \beta$　$(\alpha, \beta \in H_2)$ の解の集合と、(2)$\alpha + g = g\beta$　$(\alpha, \beta \in H_2)$ の解の集合の間の対応を考える。
$A = \{(\alpha, \beta) \,|\, \alpha, \beta \in H_2, \quad \alpha + g = \beta\}$,　$B = \{(\alpha, \beta) \,|\, \alpha, \beta \in H_2, \quad \alpha + g = g\beta\}$ とする。
そして、$\phi : A \longrightarrow B$ で 1 対 1、上への写像を考えるのである。

まず、次の補題を準備しておく。

補題３－２　H_2 は乗法に関して群をなす。

証明）$H_2 = \{g^0, g^{3^2}, \cdots\cdots g^{3^{p-3}}\} = \{g^{2k} \,|\, 0 \leqq k \leqq \frac{p-3}{2}\}$ である。

- $1 = g^0 \in H_2$
- $a, b \in H_2$ のとき、$a = g^{2k}$,　$b = g^{2l}$　$(k.l \in \mathbb{Z})$ とできる。従って、 $ab = g^{2k} \cdot g^{2l} = g^{\overline{2(k+l)}} \in H_2$
- $a^{-1} = (g^{2k})^{-1} = g^{\overline{-2k}} \in H_2$　　（証明終）

命題３－３
$x \in H_2 \Longrightarrow [x]_2 = [1]_2$　　$x \in gH_2 \Longrightarrow [x]_2 = [g]_2$

証明）

- $x \in H_2$ のとき、$x = g^{2l}$,　$0 \leqq 2l \leqq p-3$ と表すことができる。
  $[x]_2 = \sum_{\alpha \in H_2} \zeta^{x\alpha} = \sum_{j=0}^{\frac{p-3}{2}} \zeta^{g^{2l} \cdot g^{2j}} = \sum_{j=0}^{\frac{p-3}{2}} \zeta^{g^{2l+2j}} = \sum_{k=l}^{\frac{p-3}{2}+l} \zeta^{g^{2k}} = \sum_{k=l}^{\frac{p-3}{2}} \zeta^{g^{2k}} + \sum_{k=\frac{p-3}{2}+1}^{\frac{p-3}{2}+l} \zeta^{g^{2k}}$
  最後の第 2 項$= \sum_{m=0}^{l-1} \zeta^{g^{2m+(p-1)}} = \sum_{m=0}^{l-1} (\zeta^{g^{p-1}})^{g^{2m}} = \sum_{m=0}^{l-1} \zeta^{g^{2m}}$
  従って、$[x]_2 = \sum_{k=l}^{\frac{p-3}{2}} \zeta^{g^{2k}} + \sum_{m=0}^{l-1} \zeta^{g^{2m}} = \sum_{k=0}^{\frac{p-3}{2}} \zeta^{g^{2k}} = [1]_2$
- $x \in gH_2$ のとき、$x = g^{2l+1}$,　$1 \leqq 2l+1 \leqq p-2$ と表すことができる。
  $[x]_2 = \sum_{\alpha \in H_2} \zeta^{x\alpha} = \sum_{j=0}^{\frac{p-3}{2}} \zeta^{g^{2l+1} \cdot g^{2j}} = \sum_{j=0}^{\frac{p-3}{2}} \zeta^{g^{2l+1+2j}} = \sum_{k=l}^{\frac{p-3}{2}+l} \zeta^{g^{2k+1}} = \sum_{k=l}^{\frac{p-3}{2}} \zeta^{g^{2k+1}} + \sum_{k=\frac{p-3}{2}+1}^{\frac{p-3}{2}+l} \zeta^{g^{2k+1}}$
  最後の第 2 項$= \sum_{m=0}^{l-1} \zeta^{g^{2m+1+(p-1)}} = \sum_{m=0}^{l-1} (\zeta^{g^{p-1}})^{g^{2m+1}} = \sum_{m=0}^{l-1} \zeta^{g^{2m+1}}$

従って、$[x]_2 = \sum_{k=l}^{\frac{p-3}{2}} \zeta^{g^{2k+1}} + \sum_{m=0}^{l-1} \zeta^{g^{2m+1}} = \sum_{k=0}^{\frac{p-3}{2}} \zeta^{g^{2k+1}} = \sum_{k=0}^{\frac{p-3}{2}} \zeta^{g \cdot g^{2k}} = [g]_2$

（証明終）

命題３－４

p を奇素数、$\mathbb{F}_p = \{0, 1, 2 \cdots, p-1\}$ 有限体、g を乗法群 $\mathbb{F}_p^{\times}$ の生成元（p の原始根）とする。また、$H_2 = \{g^0, g^2, \cdots\cdots, g^{p-3}\}$ とおく。

(1) $\alpha, \beta \in H_2, \quad \alpha \neq 0$ が $\alpha + g = \beta$ を満たすとき、$\alpha' = g^2\alpha^{-1}$, $\beta' = \alpha^{-1}\beta$ とおくと、α', $\beta' \in H_2$ かつ $\alpha' + g = g\beta'$ を満たす。

(2) $\alpha, \beta \in H_2$ が $\alpha + g = g\beta$ を満たすとき、$\alpha' = g^2\alpha^{-1}$, $\beta' = g^2\alpha^{-1}\beta$ とおくと、α', $\beta' \in H_2$ かつ $\alpha' + g = g\beta'$ を満たす。

証明）

(1) $\alpha + g = \beta \quad (\alpha \neq 0)$ が成り立つとき、その両辺に $g\alpha^{-1}$ をかけて、$g + g^2\alpha^{-1} = g\alpha^{-1}\beta$

従って、$\alpha' + g = g\beta' \quad //$

(2) $\alpha + g = g\beta \quad (\alpha \neq 0)$ が成り立つとき、その両辺に $g\alpha^{-1}$ をかけて、$g + g^2\alpha^{-1} = g^2\alpha^{-1}\beta$

従って、$\alpha' + g = \beta' \quad //$

この命題により、

・$\alpha + g = \beta$ を満たす (α, β) から $\alpha + g = g\beta$ を満たす (α, β) への写像
$\phi(\alpha, \beta) = (g^2\alpha^{-1}, \alpha^{-1}\beta)$

・$\alpha + g = 3\beta$ を満たす (α, β) から $\alpha + g = \beta$ を満たす (α, β) への写像
$\psi(\alpha, \beta) = (g^2\alpha^{-1}, g^2\alpha^{-1}\beta)$

が得られる。そして、計算して確かめられることであるが、ϕ と ψ は互いに逆写像となっている。

$p = 17$, $g = 3$ のときについて、先に求めた $\alpha + 3 = \beta \quad (\alpha, \beta \in H_2)$ の解 (α, β) の ϕ による像を計算すると

(α, β)	$(1, 4)$	$(13, 16)$	$(15, 1)$	$(16, 2)$
$\phi(\alpha, \beta)$	$(9, 4)$	$(2, 13)$	$(4, 8)$	$(8, 15)$

となる。また、ψ による写像は、上表の逆の対応となっている。

ϕ による 1 ： 1 対応により、次が成り立つ。

命題３－５　$\alpha \in H_2$ で $[\alpha + g]_2 = [1]_2$ となるものの個数と、$\alpha \in H_2$ で $[\alpha + g]_2 = [g]_2$ となるものの個数は等しい。

($A=\{\alpha\in H_2 \mid [\alpha+g]_2=[1]_2\}$、$B=\{\alpha\in H_2 \mid [\alpha+g]_2=[g]_2\}$ とおくと、$^{\#}A=^{\#}B$)

証明）　前述のことから、ϕ が $\alpha+g=\beta$ を満たす (α,β) 全体の集合 A から $\alpha+g=g\beta$ を満たす (α,β) 全体の集合 B への 1 : 1 写像である。従って、それら 2 つの集合 A,B の元の個数は等しい。

さらに、$\alpha\in A \Longleftrightarrow [\alpha]_2=[1]_2$,　$\alpha\in B \Longleftrightarrow [\alpha]_2=[g]_2$ である。

従って、命題が成り立つ。　//

$p=17$ のとき、H_2 の元の個数は $8=\dfrac{17-1}{2}$ であり、集合 A,B がその半分の 4 つずつになっている。

では、$p=7$ のときはどうか？ H_2 の元の個数は、$\dfrac{8-1}{2}=3$ なので、A,B がその半分ずつとはなれない。(1.5 個ずつにはなれない)

具体的に確かめると

$\alpha\in H_2$	1	2	4
$\alpha+3$	4	5	0
H_2に属する	○		
$3H_2$に属する		○	

H_2, $3H_2$ が 1 つずつと 0 が 1 つである。$[0]_2=^{\#}H_2=\dfrac{p-1}{2}$ であったから、

$[1]_2\cdot[3]_2=(a_1+a_2)+\dfrac{7-1}{2}=-1+3=2$

$P=17$ のときには、$\alpha+3=0$ を満たす $\alpha\in H_2$ は無かったが、$p=7$ のときにはあった。どんな p のときに $\alpha+3=0$ を満たす $\alpha\in H_2$ が存在するのだろうか？

命題３－６　$\alpha+g=0$ を満たす $\alpha\in H_2$ が存在する　$\Longleftrightarrow$　$p\equiv 3 \pmod 4$

証明）

$\alpha+g=0 \Longleftrightarrow \alpha=-1\cdot g$　である。

g が $\mathbb{F}_p^{\times}$ の生成元であるとき、$g^{p-1}=1$ である。従って、$(g^{\frac{p-1}{2}})^2=1$ から $g^{\frac{p-1}{2}}=\pm 1$ であるが、$g^{\frac{p-1}{2}}=1$ とすると g が生成元であることに矛盾するので、$g^{\frac{p-1}{2}}=-1$ となる。

- $p\equiv 1 \pmod 4$ のとき
  $p=4k+1$ とおけるから、$\alpha=-1\cdot g=g^{\frac{p-1}{2}}\cdot g=g^{2k}\cdot g=g^{2k+1}\in gH_2$
- $p\equiv 3 \pmod 4$ のとき
  $p=4k+3$ とおけるから、$\alpha=-1\cdot g=g^{\frac{p-1}{2}}\cdot g=g^{2k+1}\cdot g=g^{2k+2}\in H_2$

（証明終）

上の命題の証明から、$p\equiv 3 \pmod 4$ のとき、$\alpha\in H_2$ で $\alpha+g=0$ となるものは唯一つであることも言える。

従って、以下のような計算となる。

(1) $p \equiv 1 \pmod 1$ のとき

H_2 に含まれる $\dfrac{p-1}{2}$ 個の元 α のうち、半分の $\dfrac{p-1}{4}$ 個は $\alpha + g \in H_2$ を満たし、残りの半分は $\alpha + g \in gH_2$ を満たす。なお、$\alpha + g = 0$ を満たすものはない。

従って、$[1]_2 \cdot [g]_2 = \displaystyle\sum_{\alpha \in H_2} [\alpha + g]_2 = \frac{p-1}{4}([1]_2 + [g]_2) = -\frac{p-1}{4}$

(2) $p \equiv 1 \pmod 3$ のとき

H_2 に含まれる $\dfrac{p-1}{2}$ 個の元 α のうち、$\alpha + g = 0$ を満たすものが 1 つある。

残り $\dfrac{p-3}{2}$ 個の元 α のうち、半分の $\dfrac{p-3}{4}$ 個は $\alpha + g \in H_2$ を満たし、残りの半分は $\alpha + g \in gH_2$ を満たす。

従って、$[1]_2 \cdot [g]_2 = \displaystyle\sum_{\alpha \in H_2} [\alpha + g]_2 = [0]_2 + \frac{p-3}{4}([1]_2 + [g]_2) = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$

以上のことから、次の定理が成り立つ。

定理３－７　（２次ガウス周期の基本定理）

(1) $p \equiv 1 \pmod 4$ のとき

$$a_1 \cdot a_2 = -\frac{p-1}{4}$$

a_1, a_2 を解とする 2 次方程式は

$$x^2 + x - \frac{p-1}{4} = 0$$

その解は

$$x = \frac{-1 \pm \sqrt{p}}{2}$$

(2) $p \equiv 3 \pmod 4$ のとき

$$a_1 \cdot a_2 = \frac{p+1}{4}$$

a_1, a_2 を解とする 2 次方程式は

$$x^2 + x + \frac{p+1}{4} = 0$$

その解は

$$x = \frac{-1 \pm \sqrt{p}i}{2}$$

$\alpha+g=\beta,\quad \alpha+g=g\beta$ のところを、粟原先生の本では、体 $\mathbb{F}_p$ 上の 2 次曲線 $x^2+g=y^2,\quad x^2+g=gy^2$ の点の個数として数えている。併せて、$1+x^2=y^2,\quad 1+gx^2=gy^2$ の点の個数も計算している。この場合、$\pm x$ が $x^2=\alpha$ に対応し、$\pm y$ が $y^2=\beta$ に対応することから 4 倍の個数になることや、0 の場合にはどうするかなど、少し注意がいる。先のことを考えると 2 次曲線の方がよいのかもしれないが、この時点では、このレポートの数え方の方がシンプルだと思う。

なお、$[1]_2\cdot[g]_2=\sum_{\alpha\in H_2}[1+g\alpha]_2$ の形でガウスの積公式を使うと、$1+g\alpha=\beta$ もしくは、$1+g\alpha=g\beta$ となり、その個数の対応を考えることになる。それは、2 次曲線では $1+x^2=y^2,\quad 1+gx^2=gy^2$ の点の個数の計算になる。

ガウスの積公式の最初の形と 2 番目の形を結びつけることから、2 次ガウス周期の基本定理の別証明が得られる。さらに、別の証明もある。それらについては、別の機会にレポートできればと思う。