ガウス周期に関するノート　その1

－　正十七角形の作図、2次ガウス周期、平方剰余の相互法則　－

2020年4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）を勉強したノートである。自分の数学の理解度に合わせた解釈や計算等を書き留めてみた。

ノートその1として、正十七角形の作図、2次ガウス周期の定義、ガウスの積公式による計算、ガウス2次周期の基本定理、そして、それを用いた平方剰余の相互法則および第2補充則の証明までとした。その2で4次ガウス周期について扱う。

1　正十七角形の作図

ガウスは、正十七角形が定規とコンパスで作図可能であることを示すために、以下のように考えていった。

(1) 正十七角形を複素平面上で考え、中心が原点とする。$\zeta = e^{\frac{2\pi i}{17}}$ とおき、頂点が $1, \zeta, \zeta^2, \cdots\cdots, \zeta^{16}$ で表されるものとする。

(2) 1を除く $\zeta, \zeta^2, \cdots\cdots, \zeta^{16}$ をうまく2つのグループに分ける。それは、単純に巾の順に並べるものではない。次のように考えていく。

- 整数を17で割った余りを $\mathbb{F}_{17} = \{0, 1, 2, \cdots, 16\}$ とし、それから0を除いたものを $\mathbb{F}_{17}^{\times} = \{1, 2, \cdots, 16\}$ とする。
  このとき、$\mathbb{F}_{17}^{\times}$ の元はすべて、3の巾で表されることが、下の表からわかる。

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$3^k \pmod{17}$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

  ※このような状況から、「$\mathbb{F}_{17}^{\times}$ は3を生成元とする乗法巡回群となる。」と言える。

- $\mathbb{F}_{17}^{\times}$ を $H_2 = \{3^{2m} \,|\, m = 0, 1, 2, \cdots, 7\}$ と $3H_2 = \{3^{2m+1} \,|\, m = 0, 1, 2, \cdots, 7\}$ の2つのグループに分ける。
  具体的には $H_2 = \{1, 9, 13, 15, 16, 8, 4, 2\}$,　$3H_2 = \{3, 10, 5, 11, 14, 7, 12, 6\}$ となる。

- ζ について、巾を上の2つのグループに属するもので和を取って、
  $\alpha = \sum_{k \in H_2} \zeta^k$,　$\beta = \sum_{k \in 3H_2} \zeta^k$　とする。

(3) α と β を求める。

- $\alpha+\beta$ は巾の小さい順に並び替えると
  $=\zeta+\zeta^2+\cdots\cdots+\zeta^{16}=(1+\zeta+\zeta^2+\cdots\cdots+\zeta^{16})-1=\dfrac{1-\zeta^{17}}{1-\zeta}-1=-1$
- $\alpha\cdot\beta$ は積を展開して 64 個の項となるが、$\zeta^{17}=1$ を用いて整理すると、
  $=4(\zeta+\zeta^2+\cdots\cdots+\zeta^{16})=-4$ となる。

  ※　このような積の計算について、具体的なものを 1 つ 1 つ確認してその結果が上記のようになるとするのは大変である。また、一般の場合にどうなるか考えることも必要である。そこで、うまく計算を進めるようにするのが**「ガウスの積公式」** であり、後に提示する。
- 上記より、α,β は x の 2 次方程式 $x^2+x-4=0$ の 2 つの解となる。
  方程式を解いて、$x=\dfrac{-1\pm\sqrt{17}}{2}$ となる。
- α,β の偏角をもとに、図形的に調べてみると、
  $\alpha=\dfrac{-1+\sqrt{17}}{2},\quad \beta=\dfrac{-1-\sqrt{17}}{2}$ であることがわかる。

(4) 次に、2 分割をさらに半分ずつにして、4 分割にする。

- $\mathbb{F}_{17}^{\times}$ の 16 個の元を以下のように 4 分割する。
  $H_4=\{3^{4m}\,|\,m=0,1,2,3\}$,　　$3H_4=\{3^{4m+1}\,|\,m=0,1,2,3\}$
  $3^2H_4=\{3^{4m+2}\,|\,m=0,1,2,3\}$,　$3^3H_4=\{3^{4m}\,|\,m=0,1,2,3\}$

  具体的には、
  $H_4=\{1,13,16,4\}$,　$3H_4=\{3,5,14,12\}$
  $3^2H_4=\{9,15,8,2\}$,　$3^3H_4=\{10,11,7,6\}$　となる。
- $\alpha_4=\displaystyle\sum_{k\in H_4}\zeta^k$,　$\beta_4=\sum_{k\in 3^2H_4}\zeta^k$,　とおく。

  $H_4\cup 3^2H_4=H_2$ であるから、$\alpha_4+\beta_4=\alpha=\dfrac{-1+\sqrt{17}}{2}$

$$\begin{aligned}\alpha_4\cdot\beta_4&=(\zeta+\zeta^{13}+\zeta^{16}+\zeta^4)(\zeta^9+\zeta^{15}+\zeta^8+\zeta^2)\\&=\ \zeta^{10}+\zeta^{16}+\zeta^9+\zeta^3\\&\quad\ \zeta^5+\zeta^{11}+\zeta^4+\zeta^{15}\\&\quad\ \zeta^8+\zeta^{14}+\zeta^7+\zeta^1\\&\quad\ \zeta^{13}+\zeta^2+\zeta^{12}+\zeta^6\\&=\zeta+\zeta^2+\cdots\cdots+\zeta^{16}=-1\end{aligned}$$

  従って、α_4,β_4 は x の 2 次方程式 $x^2-\dfrac{-1+\sqrt{17}}{2}x-1=0$ の解となる。
  方程式を解いて、

$$x=\frac{1}{2}\left\{\frac{-1+\sqrt{17}}{2}\pm\sqrt{\left(\frac{-1+\sqrt{17}}{2}\right)^2+4}\right\}$$
$$=\frac{1}{4}\left(-1+\sqrt{17}\pm\sqrt{34-2\sqrt{17}}\right)$$

偏角を考えて、
$\alpha_4 = \dfrac{1}{4}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right), \quad \beta_4 = \dfrac{1}{4}\left(-1+\sqrt{17}-\sqrt{34-2\sqrt{17}}\right)$
とわかる。

- $\alpha'_4 = \sum_{k\in H_4} \zeta^k, \quad \beta'_4 = \sum_{k\in 3^2H_4} \zeta^k, \quad$ とおく。

  $3H_4 \cup 3^3H_4 = 3H_2$ であるから、$\alpha'_4 + \beta'_4 = \beta = \dfrac{-1-\sqrt{17}}{2}$
  $\alpha_4 \cdot \beta_4$ の計算と同様にして、$\alpha'_4 \cdot \beta'_4 = -1$ がわかる。従って、α'_4, β'_4 は x の 2 次方程式 $x^2 - \dfrac{-1-\sqrt{17}}{2}x - 1 = 0$ の解となる。
  方程式を解いて、
  $x = \dfrac{1}{2}\left\{\dfrac{-1-\sqrt{17}}{2} \pm \sqrt{\left(\dfrac{-1-\sqrt{17}}{2}\right)^2 + 4}\right\}$
  $= \dfrac{1}{4}\left(-1-\sqrt{17} \pm \sqrt{34+2\sqrt{17}}\right)$

  偏角を考えて、
  $\alpha'_4 = \dfrac{1}{4}\left(-1-\sqrt{17}+\sqrt{34+2\sqrt{17}}\right), \quad \beta'_4 = \dfrac{1}{4}\left(-1-\sqrt{17}-\sqrt{34+2\sqrt{17}}\right)$
  とわかる。

(5) 8 分割にする。

- 巾のグループ分けは

$H_8 = \{3^0, 3^8\} = \{1, 16\},$	$3^4H_8 = \{3^4, 3^{12}\} = \{13, 4\}$
$3H_8 = \{3^1, 3^9\} = \{3, 14\},$	$3^5H_8 = \{3^5, 3^{13}\} = \{5, 12\}$
$3^2H_8 = \{3^2, 3^10\} = \{9, 8\},$	$3^6H_8 = \{3^6, 3^{14}\} = \{15, 2\}$
$3^3H_8 = \{3^3, 3^11\} = \{10, 7\},$	$3^7H_8 = \{3^7, 3^{15}\} = \{11, 6\}$

- $\alpha_8 = \zeta^1 + \zeta^{16}, \quad \beta_8 = \zeta^{13} + \zeta^4$ とおく。
  $\alpha_8 + \beta_8 = \alpha_4 = \dfrac{1}{4}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right)$
  $\alpha_8 \cdot \beta_8 = \zeta^{14} + \zeta^5 + \zeta^{12} + \zeta^3 = \beta'_4 = \dfrac{1}{4}\left(-1-\sqrt{17}-\sqrt{34+2\sqrt{17}}\right)$

- α_8, β_8 は x の 2 次方程式

  $x^2 - \dfrac{1}{4}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right)x + \dfrac{1}{4}\left(-1-\sqrt{17}-\sqrt{34+2\sqrt{17}}\right) = 0$

  の解となる。

- この方程式を解く。
  $x = \dfrac{1}{2}\left[\dfrac{1}{4}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right)\right.$

$$\pm\sqrt{\left\{\frac{1}{4}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right)\right\}^2-4\cdot\frac{1}{4}\left(-1-\sqrt{17}-\sqrt{34+2\sqrt{17}}\right)}\Bigg]$$

$$=\frac{1}{8}\Big\{\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right)$$
$$\pm\sqrt{68+12\sqrt{17}+2(-1+\sqrt{17})\sqrt{34-2\sqrt{17}}-16\sqrt{34+2\sqrt{17}}}\Big\}$$

- $\alpha_8=\zeta^1+\zeta^{16}=2\cos\dfrac{2\pi}{17}$, $\beta_8=\zeta^4+\zeta^{13}=2\cos\dfrac{8\pi}{17}$ であるから大小を考えて、
$$\cos\frac{2\pi}{17}=\frac{1}{16}\Big\{\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right)$$
$$+\sqrt{68+12\sqrt{17}+2(-1+\sqrt{17})\sqrt{34-2\sqrt{17}}-16\sqrt{34+2\sqrt{17}}}\Big\}$$

(6) 結論

上記で得られた $\cos\dfrac{2\pi}{17}$ は整数から始めて、加減乗除と平方根を繰り返して計算できることから、定規とコンパスで作図できると結論できる。

2 2次ガウス周期について

2.1 任意の奇素数 p に対する 体 $\mathbb{F}_p=\{0,1,2,\cdots\cdots,p-1\}$ とその乗法群 $\mathbb{F}_p^\times=\{1,2,\cdots\cdots,p-1\}$ について

- 任意の奇素数 p に対して、整数を p で割った余りの集合 $\mathbb{F}_p=\{0,1,2,\cdots\cdots,p-1\}$ に対して、 $p=17$ のときと同様に和、差、積、および 0 以外での商を定義することができて、$\mathbb{F}_p$ は体であると言える。商が問題となるのであるが、a,p が互いに素であるとき、 $ax+py=1$ を満たす整数 x,y が得られることから、$a^{-1}=x$ と考え、$b\div a=b\cdot x$ と考えればよいのである。

- $\mathbb{F}_p^\times=\{1,2,\cdots\cdots,p-1\}$ について、 $p=17$ のときと同様に、ある $g\in\mathbb{F}_p^\times$ が存在して、$\mathbb{F}_p^\times$ のすべての元は g の巾で表される。このとき、「g は $\mathbb{F}_p^\times$ の生成元である」 と言う。なお、 $g^{p-1}=1$ であることに注意しなければならない。

  この事実については、ある程度の証明が必要である。幾通りかの証明方法があり、並べてみると興味深いのであるが、ここでは省略する。

  例

  - $p=3$ のとき、 $g=2$ とできる。 $\mathbb{F}_3^\times=\{2^0,2^1\}$
  - $p=5$ のとき、 $g=2$ とできる。 $\mathbb{F}_5^\times=\{2^0,2^1,2^3,2^4\}=\{1,2,4,3\}$
    $\{3^0,3^1,3^2,3^3\}=\{1,3,4,2\}$ となるので、 $g=3$ としてもかまわない。
  - $p=7$ のとき、 $g=3$ とできる。 $\mathbb{F}_7^\times=\{3^03^1,3^3,3^4,3^5,3^6\}=\{1,3,2,6,4,5\}$
    ($2^3=1$ となってしまい、 $g=2$ とすることはできない。)

– $p=11$ のときは、 $g=2$、$p=13$ のとき、$g=2$ とできることがわかる。

2.2 2次ガウス周期

- $\mathbb{F}_p^{\times}$ を2分割する。($p-1$ は偶数なので2分割できる。)
  $H_2=\left\{g^{2m}\,|\,m=0,1,\cdots\cdots,\dfrac{p-3}{2}\right\},\quad gH_2=\left\{g^{2m+1}\,|\,m=0,1,\cdots\cdots,\dfrac{p-3}{2}\right\}$
  そして、 $\zeta=e^{\frac{2\pi i}{p}}$ として、次の2つの和を考える。

  $$\alpha=\sum_{k\in H_2}\zeta^k,\quad \beta=\sum_{k\in gH_2}\zeta^k$$

- $\alpha+\beta$ は、和の項の順序を並び替えると
  $=\zeta+\zeta^2+\cdots\cdots+\zeta^{p-1}=(1+\zeta+\zeta^2+\cdots\cdots+\zeta^{p-1})-1=\dfrac{1-\zeta^p}{1-\zeta}-1=-1$

- 積 $\alpha\beta$ について、$P=17$ のときは、64個の項をすべて確認して計算することが可能であるが、一般の場合を扱うには工夫が必要である。そこで、記号を導入していく。ガウスが導入した記号があるそうだが、栗原先生の著書では以下のような記号を用いている。

定義 2.2.1　$a\in\mathbb{Z}$ に対して、 $[a]_2=\displaystyle\sum_{k\in H_2}\zeta^{ak}$ と定義する。

これを「a についての2次ガウス周期」と呼ぶ。

命題 2.2.2　次が成り立つ。

(1) $a\equiv b\pmod p\Longrightarrow [a]_2=[b]_2$

(2) $a\in H_2\Longrightarrow [a]_2=[1]_2,\quad a\in gH_2\Longrightarrow [a]_2=[g]_2$

証明)

(1) $a\equiv b\pmod p$ のとき、 $b=a+p\quad(\in\mathbb{Z})$ とできるので、

$$[b]_2=\sum_{k\in H_2}\zeta^{(a+lp)k}=\sum_{k\in H_2}\zeta^{ak}\cdot(\zeta^p)^{lk}=\sum_{k\in H_2}\zeta^{ak}=[a]_2\ //$$

(2) $a\in H_2$ のとき、 $a=g^{2l}$ とできる。

$$[a]_2=\sum_{k\in H_2}\zeta^{g^{2l}k}=\sum_{m=0}^{\frac{p-3}{2}}\zeta^{g^{2l+2m}}=\sum_{n=l}^{\frac{p-3}{2}+l}\zeta^{g^{2n}}=\sum_{n=l}^{\frac{p-3}{2}}\zeta^{g^{2n}}+\sum_{n=\frac{p-3}{2}+1}^{\frac{p-3}{2}+l}\zeta^{g^{2n}}$$

最後の部分の第2の和において、 $g^{p-1}=1$ であるから、$n-\frac{p-1}{2}=\mu$ としても和が

変わらないから

$$\text{上式} = \sum_{n=l}^{\frac{p-3}{2}} \zeta^{g^{2n}} + \sum_{\mu=0}^{l-1} \zeta^{g^{2n}} = \sum_{n=0}^{\frac{p-3}{2}} \zeta^{g^{2n}} = \sum_{k\in H_2} \zeta^{1\cdot k} = [1]_2 //$$

$a \in gH_2 \Longrightarrow [a]_2 = [g]_2$ については、上とほぼ同様の計算変形で証明できる。//
（証明終わり）

定理 2.2.3　（ガウスの積公式）

$$[a]_2[b]_2 = \sum_{k\in H_2} [a+bk]_2 = \sum_{k\in H_2} [ak+b]_2$$

証明）$[a]_2[b]_2 = \sum_{m\in H_2} \zeta^{am} \sum_{l\in H_2} \zeta^{bl} = \sum_{m\in H_2} \sum_{l\in H_2} \zeta^{am+bl} = \sum_{m\in H_2} \sum_{l\in H_2} \zeta^{(a+blm^{-1})m}$
最後の部分の内側の l に関する和について、 m が固定されている中、l が H_2 の元をすべて動くとき、lm^{-1} は、p を法として H_2 のすべての元と合同な元を動くことがわかるから、

$$\text{上式} = \sum_{m\in H_2} \sum_{k\in H_2} \zeta^{(a+bk)m} = \sum_{k\in H_2} \sum_{m\in H_2} \zeta^{(a+bk)m} = \sum_{k\in H_2} [a+bk]_2$$

$[1]_2[g]_2 = [g]_2[1]_2$ であることから、定理の第 2 の式に等しいことも言える。

(証明終わり)

ガウスの積公式による計算例

(1) $p = 17$ のとき
ガウスによる正十七角形の作図を考察したときの α, β は、$p = 17, g = 3$ として、2 次ガウス記号で $\alpha = [1]_2, \beta = [3]_2$ と表される。ガウスの積公式で積 $\alpha\beta = [1]_2[3]_2$ を計算してみる。

$[1]_2[3]_2 = \sum_{k\in H_2} [1+3k]_2$　ただし、$H_2 = \{1, 9, 13, 15, 16, 8, 4, 2\}$ である。計算の様子を以下の表に表す。

k	1	9	13	15	16	8	4	2
$1+3k$	4	28	40	46	49	25	13	7
(mod 17)	4	11	6	12	15	8	13	7
H_2の元	○				○	○	○	
$3H_2$の元		○	○	○				○

従って、 $[1]_2[3]_2 = 4([1]_2 + [3]_2) = -4$

P.2 では、$\alpha\beta$ の計算を行うとき、展開して出てきた 64 個の項をすべて確かめることとしたが、ガウスの積公式を用いると、その作業をずいぶん軽減することができる。

(2) $p = 11$ のとき

$p = 11, g = 2$ として、ガウスの積公式で積 $\alpha\beta = [1]_2[2]_2$ を計算してみる。

$[1]_2[2]_2 = \sum_{k \in H_2} [1 + 2k]_2$　ただし、$H_2 = \{1, 4, 5, 9, 3\}$ である。計算の様子を以下の表に表す。

k	1	4	5	9	3
$1 + 2k$	3	9	11	8	7
(mod 11)	3	9	0	7	4
H_2の元	○	○			
$3H_2$の元				○	○

今度は、$H_2, 2H_2$ のいずれにも属しない 0 が出てきた。これについては、一般の奇素数 p について、次が成り立つ。

補題 2.2.4　$[0]_2 = \dfrac{p-1}{2}$

証明）$[0]_2 = \sum_{k \in H_2} \zeta^{0 \cdot k} = \sum_{k \in H_2} 1 =^{\#} H_2 = \dfrac{p-1}{2}$ //

従って、 $[1]_2[2]_2 = 2([1]_2 + [2]_2) + 0_2 = -2 + 5 = 3$

$[1]_2, [g]_2$ を 2 つの解とする 2 次方程式は、$x^2 + x + 3 = 0$ で、

その解は $x = \dfrac{-1 + \sqrt{11}i}{2}$ となる。

さらに、偏角を調べると、 $[1]_2 = \dfrac{-1 + \sqrt{11}i}{2}$,　$[g]_2 = \dfrac{-1 - \sqrt{11}i}{2}$ であることがわかる。

予想　これらの計算結果に加えて、いくつかの奇素数 p で計算してみると、

$$([1]_2, [g]_2) = \left(\frac{-1 + \sqrt{p}}{2}, \frac{-1 - \sqrt{p}}{2} \right) \quad \text{もしくは} \quad \left(\frac{-1 + \sqrt{p}i}{2}, \frac{-1 - \sqrt{p}i}{2} \right)$$

となっていることがわかる。そのことについて調べてみる。

2.3　-1 が $\mathbb{F}_p^{\times}$ の中で平方数になるか否かについて（第 1 補充則）

上記の予想で虚数解が現れるのは、$[0]_2$ が $[1+gk]_2 \quad (k \in H_2)$ の中に現れるときで、それは、 $p \equiv 3 \pmod 4$ のときであることが判明する。$[0]_2$ が現れると、2 次方程式の定数項が判別式を負にする大きさの正の数になってしまうので、虚数解になってしまう。。

このことについては、「-1 が $\mathbb{F}_p^{\times}$ の中で平方数になるか否か」が決め手になるので、少し整理しておく。

補題 2.3.1　p を奇素数、g を $\mathbb{F}_p^{\times}$ の生成元とする。

このとき、 $g^{p-1}=1$ を満たす。また、$1 \leqq m < p-1$ なる m について $g^m = 1$ となることはない。

証明）

- $1{\cdot}g,\ 2{\cdot}g,\ \cdots\cdots,\ (p-1){\cdot}g$ は $\pmod p$ で考えてすべて異なるので、$1,\ 2,\ \cdots\cdots,\ p-1$ を並び替えたものになっている。従って、すべての積を考えると、

  $(1\cdot g)\cdot(2\cdot g)\cdot\cdots\cdots\cdot\{(p-1)\cdot g\} = 1\cdot 2\cdot\cdots\cdots\cdot(p-1)$

  $\{1\cdot 2\cdot\cdots\cdots\cdot(p-1)\}\cdot g^{p-1} = 1\cdot 2\cdot\cdots\cdots\cdot(p-1)$

  $1\cdot 2\cdot\cdots\cdots\cdot(p-1) \neq 0$ なので、 $g^{p-1}=1$ となる。//

- もし、$1 \leqq m < p-1$ なる m について $g^m = 1$ となったら、$g^{m+1} = g$ になり、$g^0, g^1, g^2, \cdots\cdots, g^{p-1}$ の中に重複するものが出てくることとなる。これは、g の巾で $\mathbb{F}_p^{\times}$ の $p-1$ 個の元すべてを表すことに反する。従って、そのような m は存在しない。//

補題 2.3.2　$g^{\frac{p-1}{2}} = -1$ が成り立つ。（※ $g^{\frac{p-1}{2}} = p-1$ と同じことである。）

証明）$(g^{\frac{p-1}{2}})^2 = g^{p-1} = 1$ より、 $g^{\frac{p-1}{2}} = \pm 1$ である。

前の補題から $g^{\frac{p-1}{2}} \neq 1$ であるから、$g^{\frac{p-1}{2}} = -1$ //

補題 2.3.3　$\mathbb{F}_p^{\times}$ の元で平方数となっている元全体の集合は、 H_2 である。

証明）

- $a \in \mathbb{F}_p^{\times}$ が平方数であるとき、$a = b^2, \quad b \in \mathbb{F}_p^{\times}$ となる $b \in \mathbb{F}_p^{\times}$ が存在する。このとき、 生成元 g により $b = g^m$ と表されるから、$a = b^2 = g^{2m} \in H_2$ //

- $a \in H_2$ のとき、$a = g^{2m}$ と表される。 $b = g^m$ とおくと、$a = b^2$ となり、 a は平方数であると言える。//

命題 2.3.4　-1 が $\mathbb{F}_p^\times$ で平方数になる　$\Longleftrightarrow$　$p \equiv 1 \pmod 4$

証明）前の補題より、-1 が $\mathbb{F}_p^\times$ で平方数になる　$\Longleftrightarrow$　$-1 \in H_2$

$-1 = g^{\frac{p-1}{2}}$ であったから、$g^{\frac{p-1}{2}} = g^{2m}$ となる m が存在する。(2 m の取り方には、$p-1$ の整数倍の違いがあり得るが、$p-1$ は偶数であるから、いずれ $2m$ の形で表すことができる。)

従って、$\dfrac{p-1}{2} = 2m, \qquad p = 4m+1$。従って、$p \equiv 1 \pmod 4$ //

注意　$p \equiv 3 \pmod 4$ のとき、$p = 4m+3$ とおいて、$-1 = g^{\frac{p-1}{2}} = g^{2m+1} \in gH_2$

このことから、$p \equiv 1 \pmod 4 \Longrightarrow -1 \in H_2, \qquad p \equiv 3 \pmod 4 \Longrightarrow -1 \in gH_2$

ルジャンドル記号

$\mathbb{F}_p^\times$ において、a が平方数、すなわち $a \in H_2$ のとき、$\left(\dfrac{a}{p}\right) = 1$ 、a が非平方数、すなわち $a \in gH_2$ のとき、$\left(\dfrac{a}{p}\right) = -1$ と表す。これを**「ルジャンドル記号」**と言う。

命題 2.3.5　$\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$

証明）a, b をそれぞれ g の巾で表して、指数が偶数か奇数かで考えれば証明できる。//

命題 2.4.4 をルジャンドル記号で次のように表す。

命題 2.3.6　（第 1 補充則）

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & (p \equiv 1 \pmod 4 \text{ のとき}) \\ -1 & (p \equiv 3 \pmod 4 \text{ のとき}) \end{cases}$$

これを $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ と書くと便利なこともある。

3　ガウス 2 次周期の基本定理

目標は次の定理である。

定理 3.1　**（ガウス 2 次周期の基本定理）**

$$[1]_2[g]_2 = \begin{cases} \dfrac{1-p}{4} & (p \equiv 1 \pmod 4 \text{ のとき}) \\ \dfrac{1+p}{4} & (p \equiv 3 \pmod 4 \text{ のとき}) \end{cases}$$

証明）$[1]_2[g]_2 = \sum_{k\in H_2}[1+gk]_2 = A[1]_2 + B[g]_2 + C[0]_2$

$A =^{\#} \{k \in H_2 \,|\, 1+gk \in H_2\}, \quad B =^{\#} \{H_2 \,|\, 1+gk \in gH_2\}, \quad C =^{\#} \{H_2 \,|\, 1+gk = 0\}$

- まず、和を取る k の個数から　$A+B+C =^{\#} H_2 = \dfrac{p-1}{2}$　$\cdots\cdots$①
- 次に C について考える。

  $1+gk = 0$ のとき、$-1 = gk \in gH_2$ であるから、$p \equiv 3 \pmod 4$ である。（命題 2.4.6）

  従って、

$$C = \begin{cases} 0 & (p \equiv 1 \pmod 4 \text{ のとき}) \\ 1 & (p \equiv 3 \pmod 4 \text{ のとき}) \end{cases} \quad \cdots\cdots ②$$

- 最後に $A = B$ を示す。

  $1+gk \in H_2$ が成り立っていることは、$1+gX = Y$ を満たす $X, Y \in H_2$ が存在することであると解釈し、それがいくつあるか考える。

  両辺に $g^{-1}X^{-1}$ をかけて、 $g^{-1}X^{-1} + 1 = g^{-1}X^{-1}Y$

  さらに変形して、 $1 + g(g^{-2}X^{-1}) = g(g^{-2}X^{-1}Y)$

  ここで、 $X' = g^{-2}X^{-1}, \quad Y' = g^{-2}X^{-1}Y$ とおくと、$1+gX' = gY'$ を満たし、$X', Y' \in H_2$ であることは、X, Y を生成元 g の巾で表現することで確かめられる。

  従って、$1+gk' \in gH_2$ を満たす $k' \in H_2$ が存在することに結びつく。実際には、$k' = g^{-2}k^{-1}$ となる。

  逆に、$1+gk' \in gH_2$ が成り立っていることを $1+gX' = fY'$ を満たす $X', Y' \in H_2$ が存在することであると解釈し、上と同様の考察を行うと、 先ほどの逆対応である $k = g^{-2}k'^{-1}$ により、 $1+gk \in H_2$ となる。

  以上により、2 つの集合 $\{k \in H_2 \,|\, 1+gk \in H_2\}, \quad \{H_2 \,|\, 1+gk \in gH_2\}$ の間に $1:1$ の対応が得られる。

  よって、$A = B$　$\cdots\cdots$③ が成り立つ。

①, ②, ③ より、

(1) $p \equiv 1 \pmod 4$ のとき

$2A = \dfrac{p-1}{2}, \quad A = \dfrac{p-1}{4} = B, \, C = 0$

$\therefore \quad [1]_2[g]_2 = \dfrac{p-1}{4}([1]_2 + [g]_2) + 0 \cdot [0]_2 = -\dfrac{p-1}{4}//$

(2) $p \equiv 3 \pmod 4$ のとき

$$2A+1=\frac{p-1}{2},\quad A=\frac{p-3}{4}=B,\ C=1$$

$$\therefore\quad [1]_2[g]_2=\frac{p-3}{4}([1]_2+[g]_2)+1\cdot[0]_2=-\frac{p-3}{4}+\frac{p-1}{2}=\frac{1+p}{4}//$$

以上で、**定理 3.1　（ガウス 2 次周期の基本公式）** の証明が終わった。

さらに、2 次方程式を解いていく。

定理 3.2

(1) $p \equiv 1 \pmod 4$ のとき

$[1]_2, [g]_2$ を 2 つの解とする　x の 2 次方程式は、$x^2+x+\dfrac{1-p}{4}=0$ である。

その判別式は、$D=(-1)^2-4\cdot\dfrac{1-p}{4}=p$ となる。

解は、 $x=\dfrac{-1\pm\sqrt{p}}{2}$ となる。

(2) $p \equiv 3 \pmod 4$ のとき

$[1]_2, [g]_2$ を 2 つの解とする　x の 2 次方程式は、$x^2+x+\dfrac{1+p}{4}=0$ である。

その判別式は、$D=(-1)^2-4\cdot\dfrac{1+p}{4}=-p$ となる。

解は、 $x=\dfrac{-1\pm\sqrt{p}i}{2}$ となる。

2 つの解のどちらがどちらに対応するのかについては、次の定理のようになる。

定理 3.3　（ガウス 2 次周期の値）

(1) $p \equiv 1 \pmod 4$ のとき

$[1]_2=\dfrac{-1+\sqrt{p}}{2},\quad [g]_2=\dfrac{-1-\sqrt{p}}{2}$ となる。

(2) $p \equiv 3 \pmod 4$ のとき

$[1]_2=\dfrac{-1+\sqrt{p}i}{2},\quad [g]_2=\dfrac{-1-\sqrt{p}i}{2}$ となる。

栗原先生の著書では、「この証明は本書のレベルを超えている」と記載されているので、この学習ノートでは触れない。（いつか勉強できればよいのだが。）

4　平方剰余の相互法則　…　２次ガウス周期を用いた証明

１つの奇素数 p について、整数 a が $\mathbb{F}_p^{\times}$ で平方数であるかどうかを考えることに加え、p と異なる奇素数 q についても考え、q が $\mathbb{F}_p^{\times}$ で平方数であるかどうかおよび、p が $\mathbb{F}_q^{\times}$ で平方数であるかどうかについて考えると、実はきれいな関係式が成り立つというのである。具体的には次の定理となる。

定理４　平方剰余の相互定理

p, q を相異なる奇素数とすると、

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

が成り立つ。

栗原先生の著書によると、「この定理に対してガウスが６つの証明を出版しており、さらに、遺稿から２つの証明が見つかっている。遺稿の２つの証明は本質的には同じで１つの証明とも考えられることから、ガウスは７つの証明を与えた、と通常は言われている。」とのことである。

ガウス周期を用いた証明は、遺稿にあったもので、ガウスの「数論研究」入れるには長すぎたので断念し、別の証明を採用したのではと推測されている。

この証明について、自分なりに道筋を整理して追ってみた。

4.1　p について計算した２次ガウス周期を解に持つ２次方程式を $\mathbb{F}_q[x]$ へ写したものの考察

(1) p で考えた２次ガウス周期 $[1]_2, [g]_2$ については、

$$\phi_2(x) = x^2 + x + \frac{1}{4}\left\{1 - (-1)^{\frac{p-1}{2}}p\right\} \quad \in \mathbb{Q}[x]$$

とおくと、$\phi_2(x) = 0$ の２つの解となる。

(2) p, q について、$\mathbb{Z} \longrightarrow \mathbb{F}_p$ を $a \longrightarrow \bar{a}$、$\mathbb{Z} \longrightarrow \mathbb{F}_q$ を $a \longrightarrow \bar{\bar{a}}$　で表すこととする。

この対応は、$\mathbb{Q}$ の元のうち、分母にそれぞれ p を因数として含まないもの、q を因数として含まないものに対する写像に拡張することができる。それは、$\dfrac{a}{b} \to \bar{a}\cdot\bar{b}^{-1}$,　$\dfrac{a}{b} \to \bar{\bar{a}}\cdot\bar{\bar{b}}^{-1}$ というふうに、像において、分母に対する $\mathbb{F}_p, \mathbb{F}_q$ における逆元をかける対応をとればよい。）

そして、$\mathbb{Q}[x]$ の多項式 $f(X)$ が係数の分母に q を因数として含まないとき、その係数に対して $\mathbb{Q} \longrightarrow \mathbb{F}_q$ を適用したものを $\overline{\overline{f(x)}}$ で表すことにする。すると

$$\overline{\overline{\phi_2(x)}} = x^2 + x + \bar{\bar{4}}^{-1}\left\{1 - (-1)^{\frac{p-1}{2}}\bar{\bar{p}}\right\} \quad \in \mathbb{F}_q[x]$$

となる。

この 2 次方程式の解は、$x = \overline{\overline{2}}^{-1}\left\{-1 \pm \sqrt{(-1)^{\frac{p-1}{2}}\overline{p}}\right\}$ と表される。ただし、この数は $\mathbb{F}_q$ の数ではなく、それを拡大した数の世界（$\mathbb{F}_q$ の拡大体）に属するかもしれない。

※　整数を係数とする 2 次方程式の解は、整数になるとは限らず、有理数、無理数あるいは虚数となる場合があるのと同様である。

(3) (2) の解 x が $\mathbb{F}_q$ に属するのかどうか考える。

$x = \overline{\overline{2}}^{-1}\left\{-1 \pm \sqrt{(-1)^{\frac{p-1}{2}}\overline{p}}\right\}$ が $\mathbb{F}_q$ の数である。

$$\iff \quad \sqrt{(-1)^{\frac{p-1}{2}}\overline{p}} \in \mathbb{F}_q^{\times} \quad \iff \quad (-1)^{\frac{p-1}{2}}\overline{p} \text{ が } \mathbb{F}_q^{\times} \text{ の平方数である。}$$

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

最後の式は

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

となり、平方剰余の相互法則の形に迫ってきた。

4.2　$\overline{\overline{\phi_2(x)}} = 0$ の解が $\mathbb{F}_q$ に属するかどうかの $\left(\frac{q}{p}\right)$ の値による判定

別の観点から、$\overline{\overline{\phi_2(x)}} = 0$ の解が $\mathbb{F}_q$ に属するかどうか考える。すると、それは $\left(\frac{q}{p}\right)$ が 1 に等しいか -1 に等しいかで決まることがわかる。以下、それについて見ていく。

(1) $\mathbb{Z}[x]$ の q 次式 $f(x)$ で、$f([1]_2) = 0$ を満たすものを作りたい。$\mathbb{F}_q^{\times}$ の生成元を h とすると、$h^{q-1} = 1$ が成り立つ（命題 2.4.1）から、$\mathbb{F}_q^{\times}$ のすべての元は $x^{q-1} = 1$ を満たす。0 を含めると、$\mathbb{F}_q$ のすべての元は $x^q - x = 0$ を満たすと言える。
体 $\mathbb{F}_q$ を係数とする q 次方程式の解の個数は次数 q を超えないということから、$\mathbb{F}_q = \{a \,|\, x^q - x = 0\}$　であると言える。従って、**a という数が $\mathbb{F}_q$ の数であるかどうかは、$x^q - x = 0$ を満たすかどうかで判断できる。**

この考察によると、$\mathbb{F}_q[x]$ に写したときに $\overline{\overline{f(x)}} = x^q - x$ となる $f(x) \in \mathbb{Z}[x]$ を考えればよいということになる。従って、$[1]_2^q - [1]_2$ について調べようとうことになる。

(2) まず、$[1]_2^q$ の部分であるが、ガウスの積公式により、$[1]_2^n$ を以下のように計算していく。

- $n = 1$ のとき $[1]_2 = a_1 + b_1[1]_2 \quad (a_1 = 0,\, b_1 = 1)$
- $n = 2$ のとき

$$[1]_2[1]_2 = \sum_{k \in H_2}[1+k]_2 = A[1]_2 + B[g]_2 + C[0]_2$$

（A, B, C は 、それぞれ $1+k \in H_2$, $\in gH_2$, $=0$ となる $k \in H_2$ の個数である。）

$$= A[1]_2 + B(-1-[1]_2) + C \cdot \frac{p-1}{2} = \left(-B + \frac{p-1}{2}C\right) + (A-B)[1]_2$$

$$= a_2 + b_2[1]_2 \quad (a_2,\, b_2 \in \mathbb{Z})$$

とできる。

- $[1]_2^n = a_n + b_n[1]_2 \quad (a_n,\, b_n \in \mathbb{Z})$ が成り立っているとき、

$$[1]_2^{n+1} = [1]_2^n[1]_2 = (a_n + b_n[1]_2)[1]_2 = a_n[1]_2 + b_n[1]_2^2 = a_n[1] + b_n(a_2 + b_2[1]_2)$$

$$= a_2 b_n + (a_n + b_n b_2)[1]_2 = a_{n+1} + b_{n+1}[1]_2 \quad (a_{n+1},\, b_{n+1} \in \mathbb{Z})$$

とできる。

数学的帰納法により、次の補題が成り立つ。

補題 4.2.1 任意の自然数 n について、 $[1]_2^n = a_n + b_n[1]_2 \quad (a_n,\, b_n \in \mathbb{Z})$ と表すことができる。

(3) $\left(\dfrac{q}{p}\right) = 1$ のとき

前の補題を $n = q$ に適用して、 $[1]_2$ を差し引けば、$[1]_2^q - [1]_2 = a + b[1]_2$ と表せる。このとき、a, b が q で割り切れる整数であることを示していく。

$\left(\dfrac{q}{p}\right) = 1$ のとき $[q]_2 = [1]_2$ となるから、 $[1]_2^q - [q]_2$ を考えることになる。

ガウス周期の定義より、

$$[1]_2^q - [q]_2 = \left(\sum_{k \in H_2} \zeta^k\right)^q - \sum_{k \in H_2} (\zeta^k)^q$$

となる。

これは、 $(x_1 + x_2 + \cdots\cdots + x_l)^q - (x_1^q + x_2^q + \cdots\cdots + x_l^q)$ に

$x_j = \zeta^{g^{2(j-1)}} \quad (j = 1, 2, \cdots, \frac{p-1}{2})$ として代入したものである。

補題 4.2.2 $\quad (x_1 + x_2 + \cdots\cdots + x_l)^q - (x_1^q + x_2^q + \cdots\cdots + x_l^q) = qG(x_1, x_2, \cdots\cdots, x_l)$

$$G(x_1, x_2, \cdots\cdots, x_i) \in \mathbb{Z}[x_1, x_2, \cdots\cdots, x_l]$$

とできる。

証明）$(x_1 + x_2 + \cdots\cdots + x_l)^q$ の展開の一般項は $\quad \dfrac{q!}{r_1! r_2! \cdots\cdots r_l!} x_1^{r_1} x_2^{r_2} \cdots\cdots x_l^{r_l}$

である。

$0 < r_1, r_2 \cdots\cdots, r_k < q$ であるとき、係数の分母には素数 q が全く含まれず、分子には含まれることから、この係数は q の倍数であると言える。一方、いずれかの j

について、$r_j = q$ となっているとき、その他の r_m は 0 に等しいので、該当する項は x_j^q である。これらは、補題の式の第 2 番目の括弧でくくられた和を作る。以上により、補題が示された。(証明終わり)

$a+b[1]_2 = a(-[1]_2-[g]_2)+b[1]_2 = (-a+b)[1]_2-a[g]_2 = c_1\zeta+c_2\zeta^2+\cdots\cdots+c_{p-1}\zeta^{p-1}$
ただし、2次ガウス周期の定義から、$j \in H_2 \Longrightarrow c_j = -a+b, \quad j \in gH_2 \Longrightarrow c_j = -a$

もし、この表し方が 1 通りであるとすると、 前の補題から、 $-a+b, -a$ がともに q の倍数であると言える。従って、 a, b ともに q の倍数であると結論でき、証明が終わる。

問題は、「1 通りに表される」の部分である。それについて、以下に示す。

補題 4.2.3　$\zeta, \zeta^2, \cdots\cdots, \zeta^{p-1}$ は $\mathbb{Z}$ 上一次独立である。

証明）まず、 $P(x) = x^{p-1} + x^{p-2} + \cdots\cdots + x + 1$ が $\mathbb{Z}[x]$ の既約多項式（それ以上小さな次数の多項式の積に分解できない多項式）であることを示す。
$P(x) = \dfrac{x^p - 1}{x - 1}$ より、

$$P(y+1) = \frac{(y+1)^p - 1}{(y+1) - 1} = \frac{y^p +_p C_1 y^{p-1} + \cdots\cdots +_p C_{p-1} y + 1 - 1}{y}$$
$$= y^{p-1} +_p C_1 y^{p-2} + \cdots\cdots +_p C_{p-2} y +_p C_{p-1}$$

y のこの式が既約であることを示せば、$P(x)$ が既約であると言える。それには、次のアイゼンシュタインの既約判定定理を用いる。

定理 4.2.4　（アイゼンシュタインの既約判定定理）
$a_0 x^n + a_1 x^{n-1} + \cdots\cdots + a_{n-1} x + a_n \quad (a_0, a_1, \cdots, a_n \in \mathbb{Z})$ は、ある素数 p が存在して、

- a_0 は p で割り切れない
- $a_1, a_2, \cdots, a_n$ は p で割り切れる。
- a_n は p^2 で割り切れない

という条件を満たすとき既約である。

上記の $P(y+1)$ はアイゼンシュタインの既約判定定理の条件を満たしているので、$P(y+1)$ が y の式として既約である。従って、$P(x)$ も既約であると言える。//

$P(\zeta) = \dfrac{\zeta^p - 1}{\zeta - 1} = 0$ であるから、 ζ は $P(x) = 0$ の解である。

ζ を解に持つ次数最小の整数係数の方程式を $S(x)=0$ とする。その次数は、 $p-1$ 以下である。なぜなら、$p-1$ 次の $P(x)$ が ζ を解に持つからである。

係数を有理数まで許して割り算をして、$P(x)=S(x)Q(x)+R(x)$ $(R(x)$ の次数は $S(x)$ の次数より小$)$ と表すことにする。このとき、 $R(\zeta)=0$ となるが、$S(x)$ の次数の最小性から、 $R(x)$ は恒等的に 0 である。

従って、$P(x)=S(x)Q(x)$ となるが、 $P(x)$ が既約であることから、定数倍を除いて $P(x)=S(x)$ となる。すなわち、 ζ は、$p-1$ 次よりも小さい次数の $\mathbb{Z}$ 係数の方程式を満たすことはできない。

もし、$a_1\zeta^{p-1}+a_2\zeta^{p-2}+\cdots\cdots+a_{p-2}\zeta^2+a_{p-1}\zeta=0$ を満たす整数 $a_1,a_2,\cdots\cdots,a_{p-1}$ が存在したとすると、両辺を ζ で割って、

$a_1\zeta^{p-2}+a_2\zeta^{p-3}+\cdots\cdots+a_{p-2}\zeta+a_{p-1}=0$ を満たす。

これは、次数 $p-2$ 以下の多項式、$S(x)=a_1x^{p-2}+a_2x^{p-3}+\cdots\cdots+a_{p-1}$ が $S(\zeta)=0$ を満たすことを意味するので、上に示したことに反する。よって、補題 4.1.3 の一次独立性が示された。 （証明終わり）

整理すると、次の命題が成り立つことになる。

命題 4.2.5 $[1]_2^q-[1]_2=a+b[1]_2$ $(a,\,b\in\mathbb{Z},\,a,\,b\equiv 0\pmod q)$ と表すことができる。

この命題から、 $f(x)=x^q-x-(a+bx)$ とおくと、$f([1]_2)=0$ である。

$\mathbb{Z}[x]$ において $f(x)$ を $\phi_2(x)$ (2 次式で最高次の係数は 1) で割った式を考えると、その余りは整数係数の 1 次式である。さらに、 $[1]_2$ を解に持つことがわかる。

ところで、 $[1]_2=\dfrac{-1+\sqrt{(-1)^{\frac{p-1}{2}}p}}{2}$ であったから、整数係数の 1 次方程式の解となることはあり得ず、その余りは恒等的に 0 になることがわかる。

以上のことから $f(x)=Q(x)\phi_2(x)$ $(Q(x)\in\mathbb{Z}[x])$ と表すことができる。

$\mathbb{F}_q[x]$ へ写して $\overline{\overline{f(x)}}=\overline{\overline{Q(x)\phi_2(x)}}$。　　命題 4.1.4 より、 $x^q-x=\overline{\overline{Q(x)\phi_2(x)}}$

これにより、$\overline{\overline{\phi_2(x)}}=0$ の解、$\bar{\bar{2}}^{-1}\left\{-1\pm\sqrt{(-1)^{\frac{p-1}{2}}\bar{\bar{p}}}\right\}$ が $x^q-x=0$ を満たすことが言える。すなわち、 $\mathbb{F}_q$ の元であることがわかる。 $p,\,q$ が相異なる奇素数であることから、0 でないことも言える。

前節で考察したことを併せて、 $\left(\dfrac{q}{p}\right)=1\Longrightarrow(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\dfrac{p}{q}\right)=1$

が成り立つ。すなわち、 $\left(\dfrac{q}{p}\right)=1\Longrightarrow\left(\dfrac{q}{p}\right)\left(\dfrac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

が成り立つ。

(4) $\left(\dfrac{q}{p}\right)=-1$ のとき

$\left(\frac{q}{p}\right) = 1$ のときと同様に考えていくが、このときは、$[q]_2 = [g]_2 = -1 - [1]_2$ となることに注意する。

従って、 $[1]_2^q - (-1 - [1]_2) = a + b[1]_2 \quad (a, b \in \mathbb{Z} \quad a, b \equiv 0 \pmod q)$ とできる。

このため、この場合は $f(x) = x^q + x + 1 - (a + bx)$ とおく。

前と同様に、$\mathbb{F}_q[x]$ へ写して考えると、$\overline{\overline{\phi_2(x)}} = 0$ の解

$$\bar{\bar{2}}^{-1}\left\{-1 \pm \sqrt{(-1)^{\frac{p-1}{2}}\bar{\bar{p}}}\right\} \quad \cdots\cdots ①$$

が $x^q + x + 1 = 0$ の解であることがわかる。

2 つの解うちの 1 つを α で表すとき、もしそれが $\mathbb{F}_q$ に含まれる数であるならば、$\alpha^q = \alpha$ が成り立つ。

$x^q + x + 1 = 0$ に代入すると、$\alpha + \alpha + 1 = 0$ 。すなわち、$\alpha = -\bar{\bar{2}}^{-1} \quad \cdots\cdots ②$

① と ② を比べると、$(-1)^{\frac{p-1}{2}}\bar{\bar{p}} = 0$。しかし、 p, q は相異なる奇素数であるから、これはあり得ない。従って、 α が $\mathbb{F}_q$ の元であるとしたことが間違いであると言える。

前節で考察したことを併せて、 $\left(\frac{q}{p}\right) = -1 \Longrightarrow (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = -1$

が成り立つ。すなわち、

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

が成り立つ。

以上により、ガウス 2 次周期を用いた平方剰余の相互法則の証明が完成した。

5 第 2 補充則

2 が $\mathbb{F}_p$ で平方数になるかどうかについて考えるのが、第 2 補充則である。
次が成り立つ。

定理 5 （第 2 補充則）

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & (p \equiv \pm 1 \pmod 8 \text{ のとき}) \\ -1 & (p \equiv \pm 3 \pmod 8 \text{ のとき}) \end{cases}$$

この定理に対して、ここまでの考察に関連する 2 通りの証明を考える。

5.1　第 2 補充則の証明　その 1

2 が $\mathbb{F}_p^\times$ で平方数である。 $\Longleftrightarrow \sqrt{2} \in \mathbb{F}_p^\times \Longleftrightarrow \sqrt{2}$ が方程式 $x^p - x = 0$ を満たす。

従って、 $\sqrt{2}^p - \sqrt{2}$ について考える。これは、平方剰余の相互法則を証明したときと類似の考察である。

$\zeta = e^{\frac{\pi i}{4}} = \dfrac{\sqrt{2}}{2}(1+i)$ とおくと、$\zeta + \zeta^{-1} = \sqrt{2}$ となることから、これを利用する。

補題 5.1.1　$(\zeta + \zeta^{-1})^p - (\zeta^p + \zeta^{-p}) = pG(\zeta, \zeta^{-1})$　$(G(x,y) \in \mathbb{Z}[x,y])$ が成り立つ。

これは、既に示し補題 5.1.1 の変数を 2 個にしたものである。

ここで、 $G(\zeta, \zeta^{-1})$ に現れる項たちは、$\sum a_{l,m}\zeta^l(\zeta^{-1})^m = \sum a_{l,m}\zeta^{l-m}$に現れるような項であるから、整数を ζ^k にかけたものの集まりである。

ζ^k の取り得る値は、 $0, \pm 1, \pm\dfrac{\sqrt{2}}{2}(1+i), \pm\dfrac{\sqrt{2}}{2}(1-i)$ のいずれかである。

従って、上式の右辺 $= p\left\{a + b\dfrac{\sqrt{2}}{2}(1+i) + c\dfrac{\sqrt{2}}{2}(1-i)\right\}$　$(a,\, b,\, c \in \mathbb{Z})$ とできる。

整理して、上式の右辺 $= p\left\{a + \dfrac{\sqrt{2}}{2}(b+c) + \dfrac{\sqrt{2}}{2}(b-c)i\right\}$

一方、上式の左辺は、 $\zeta^p + \zeta^{-p}$ が　$p \equiv \pm 1 \pmod 8$ のとき $\sqrt{p}$ で、$p \equiv \pm 3 \pmod 8$ のとき $-\sqrt{p}$ となることに注意する。

(1) $p \equiv \pm 1 \pmod 8$ のとき

$$\sqrt{2}^p - \sqrt{2} = p\left\{a + \frac{\sqrt{2}}{2}(b+c) + \frac{\sqrt{2}}{2}(b-c)i\right\}$$

まず、左辺は実数であるから、右辺において i の係数が 0 とならなければならない。

$\therefore b = c$

従って、 $(\sqrt{2}^{p-1} - 1)\sqrt{2} = p(a + b\sqrt{2})$

この式で、$p-1$ は偶数であるから、 $\sqrt{2}^{p-1} - 1$ は整数になる。

$\sqrt{2}$ が無理数であることから、 $a = 0$ としなければならない。

従って、　$\sqrt{2}^{p-1} - 1 = pb$　となる。

以上より、 $\sqrt{2}$ は $\mathbb{F}_p$ において、$x^{p-1} - 1 = 0$　を満たすことが言えた。すなわち、$\sqrt{2}$ は $\mathbb{F}_p^\times$ の元となる。

よって、前の考察により、 $\left(\dfrac{2}{p}\right) = 1$ となる。

(2) $p \equiv \pm 3 \pmod 8$ のとき

$$\sqrt{2}^p + \sqrt{2} = p\left\{a + \frac{\sqrt{2}}{2}(b+c) + \frac{\sqrt{2}}{2}(b-c)i\right\}$$

まず、左辺は実数であるから、右辺において i の係数が 0 とならなければならない。

$\therefore b = c$

従って、 $(\sqrt{2}^{p-1}+1)\sqrt{2}=p(a+b\sqrt{2})$

この式で、$p-1$ は偶数であるから、 $\sqrt{2}^{p-1}+1$ は整数になる。

$\sqrt{2}$ が無理数であることから、 $a=0$ としなければならない。

従って、 $\sqrt{2}^{p-1}+1=pb$ となる。

以上より、 $\sqrt{2}$ は $\mathbb{F}_p$ において、$x^{p-1}+1=0$ を満たし、 $x^{p-1}-1=0$ は満たさないことが言えた。すなわち、 $\sqrt{2}$ は $\mathbb{F}_p^{\times}$ の元とならない。

よって、前の考察により、 $\left(\dfrac{2}{p}\right)=-1$ となる。

以上により、第 2 補充則が証明された。

5.2 第 2 補充則の証明 その 2

$1+X=Y$ $(X,Y\in H_2)$ や $1+gX=Y$ $(X,Y\in H_2)$ といった方程式の解の個数を数え、それが偶数か奇数かということに結びつける方法である。

$1+X=Y$ が成り立っているとき、 $1+(-Y)=-X$ となる。$X'=-Y,\ Y'=-X$ として、$1+X'=Y'$ となる。 従って、対応 $(X,Y)\to(X',Y')$ は方程式の解の対応になっている。それを考えるとき、$-1\in H_2$ なのか、それとも $-1\in gH_2$ なのかがポイントになる。

(1) $-1\in H_2$ のとき

これは、 $p\equiv 1 \pmod 4$ のときである。

- $1+X=Y$ $(X,Y\in H_2)$ の解に対して、 $1+(-Y)=-X$ となる。 $X'=-Y,\ Y'=-X$ とおくと、

  $1+X'=Y'$ $(X',Y'\in H_2)$ となる。対応 $(X,Y)\to(X',Y')$ は解の 1 対 1 対応となる。

- 具体的な素数で様子を見てみると、

  - $p=13$ のとき、

    $g=2,\quad H_2=\{1,4,3,12,9,19\}$ として、

(X,Y)	$(3,4)$	$(9,10)$
(X',Y')	$(9,10)$	$(3,4)$

  - $p=17$ のとき、

    $g=3,\quad H_2=\{1,9,13,15,16,8,4,2\}$ として、

(X,Y)	$(1,2)$	$(8,9)$	$(15,16)$
(X',Y')	$(15,16)$	$(8,9)$	$(1,2)$

  上の例で、 $P=13$ のとき解の個数は偶数で、 $p=17$ のときは」奇数である。$p=17$ のときには、 $(X,Y)\to(X',Y')$ の対応で不変なもの $(8,9)$ が存在しているのが奇数になる原因である。

- $(X,Y) \to (X',Y')$ の対応で不変なものは、 $X = p-(1+X)$ より、$X = \dfrac{p-1}{2}$ 。それ以外のものは別のものと対応していることになる。
  従って、 $\left(\dfrac{p-1}{2}, \dfrac{p+1}{2}\right)$ が $1+X=Y$ の解になるか否かによって、方程式の個数全体が奇数か偶数かに分かれると言える。
  その不変な (X,Y) が方程式の解になるかどうか調べる。

  $$X = \frac{p-1}{2} \in H_2 \Longleftrightarrow 2^2 \cdot \frac{p-1}{2} \in H_2 \Longleftrightarrow -2 \in H_2 \Longleftrightarrow 2 \in H_2 \Longleftrightarrow \left(\frac{2}{p}\right) = 1$$

  また、$2 \in H_2$ とすると、$Y = \dfrac{p+1}{2} = 2^{-1} \in H_2$ である。
  従って、$\left(\dfrac{2}{p}\right) = 1$ のとき、$\left(\dfrac{p-1}{2}, \dfrac{P+1}{2}\right)$ が方程式 $1+X=Y \quad (X,\, Y \in H_2)$ の解となり、方程式の解全体の個数は、奇数となる。

- 次に求めるべきものは、 $1+X=Y \quad (X,\, Y \in H_2)$ の解の個数である。
  2 次ガウス周期の基本公式を示したとき、
  $A =^{\#} \{X \in H_2 \,|\, 1+gX = Y \quad (Y \in H_2)\}$,
  $B =^{\#} \{X, \in H_2 \,|\, 1+gX = gY \quad (Y \in H_2)\}$
  $C =^{\#} \{(X \in H_2 \,|\, 1+gX = 0\}$
  について調べ、 $p \equiv 1 \pmod 4$ のときは、
  $\quad A = B = \dfrac{p-1}{4}, \quad C = 0$ となったのであった。
  ここでは、
  $D =^{\#} \{X \in H_2 \,|\, 1+X = Y \quad (Y \in H_2)\}$,
  $E =^{\#} \{X, \in H_2 \,|\, 1+X = gY \quad (Y \in H_2)\}$
  $F =^{\#} \{(X \in H_2 \,|\, 1+X = 0\}$
  とおいて、これらの個数を調べる.
  まず、 $\quad D+E+F = \dfrac{p-1}{2}, \quad F = 1 \quad$ である。
  X, Y の立場を逆にして、 $Y-1 \quad (Y \in H_2)$ を考えると、H_2, gH_2 の元か 0 に等しくなる。
  $^{\#}\{Y \in H_2 \,|\, Y-1 = X \quad (X \in H_2)\} = D$
  $^{\#}\{Y \in H_2 \,|\, Y-1 = gX \quad (X \in H_2)\} = A = \dfrac{p-1}{4}$
  $^{\#}\{Y \in H_2 \,|\, Y-1 = 0 = 1$
  これら 3 つの個数の和を考えて、 $D + \dfrac{p-1}{4} + 1 =^{\#} H_2 = \dfrac{p-1}{2}$
  従って、 $D = \dfrac{p-5}{4}$ となる。

- $\left(\dfrac{2}{p}\right) = 1$ のとき、この $\dfrac{p-5}{4}$ が奇数になるのであった。
  $P = 4m+1$, $\dfrac{p-5}{4} = 2k-1$ とおいて、$m-1 = 2k-1, \quad m = 2k$

従って、 $p = 8k+1 \equiv 1 \pmod 8$ となる。

- $\left(\dfrac{2}{p}\right) = -1$ のとき、この $\dfrac{p-5}{4}$ が偶数になるのであった。
  $P = 4m+1$, $\dfrac{p-5}{4} = 2k$ とおいて、$m-1 = 2k, \quad m = 2k+1$
  従って、 $p = 8k+5 \equiv 5 \pmod 8$ となる。

(2) $-1 \in gH_2$ のとき

これは、 $p \equiv 3 \pmod 4$ のときである。

- $1+X = Y \quad (X, \in gH_2, Y \in H_2)$ の解に対して、 $1+(-Y) = -X$ となる。
  $X' = -Y, Y' = -X$ とおくと、
  $1+X' = Y' \quad (X' \in gH_2, Y' \in H_2)$ となる。対応 $(X,Y) \to (X',Y')$ は解の 1 対 1 対応となる。
  この対応で不変なものは、 $X = p-(1+X)$ より、$X = \dfrac{p-1}{2}$ 。それ以外のものは別のものと対応していることになる。
  従って、 $\left(\dfrac{p-1}{2}, \dfrac{p+1}{2}\right)$ が $1+X = Y$ の解になるか否かによって、方程式の個数全体が奇数か偶数かに分かれると言える。
  その不変な (X,Y) が方程式の解になるかどうか調べる。

$$X = \frac{p-1}{2} \in gH_2 \Longleftrightarrow 2^2 \cdot \frac{p-1}{2} \in gH_2 \Longleftrightarrow -2 \in gH_2 \Longleftrightarrow 2 \in H_2 \Longleftrightarrow \left(\frac{2}{p}\right) = 1$$

  また、$2 \in H_2$ とすると、$Y = \dfrac{p+1}{2} = 2^{-1} \in H_2$ である。
  従って、 $\left(\dfrac{2}{p}\right) = 1$ のとき、$\left(\dfrac{p-1}{2}, \dfrac{P+1}{2}\right)$ が方程式 $1+X = Y \quad (X \in gH2, Y \in H_2)$ の解となり、方程式の解全体の個数は、奇数となる。

- $1+X = Y \quad (X \in gH_2, Y \in H_2)$ の解の個数であるが、それは、表現を変えて、$1+gX = Y \quad (X, Y \in H_2)$ の解の個数であると言える。
  前に調べたことから、 $p \equiv \pmod 4$ のとき、その個数は $\dfrac{p-3}{4}$ である。
- $\left(\dfrac{2}{p}\right) = 1$ のとき、この $\dfrac{p-5}{4}$ が奇数になるのであった。
  $P = 4m-1$, $\dfrac{p-3}{4} = 2k-1$ とおいて、$m-1 = 2k-1, \quad m = 2k$
  従って、 $p = 8k-1 \equiv -1 \pmod 8$ となる。

- $\left(\dfrac{2}{p}\right) = -1$ のとき、この $\dfrac{p-3}{4}$ が偶数になるのであった。
  $P = 4m-1$, $\dfrac{p-5}{4} = 2k$ とおいて、$m-1 = 2k, \quad m = 2k+1$
  従って、 $p = 8k-5 \equiv -5 \pmod 8$ となる。

以上により、第 2 補充則の 2 つ目の証明が完成した。