2017 年度桂田研究室卒業レポート

定規とコンパスによって作図可能な正多角形の条件と

正１７角形の作図

明治大学 総合数理学部 現象数理学科
松本夏樹
指導教員：桂田祐史　准教授

目次

第０章　はじめに

第１章　正ｎ角形の作図
　１．円のｎ等分と正ｎ角形
　２．複素平面と１のｎ乗根

第２章　作図可能な図形
　１．基本的な作図
　２．ｎ次の無理数
　３．円分体

第３章　有限体
　１．有限体 $\mathbb{F}_p$
　２．有限体の乗法群
　３．$\mathbb{F}_p^{\times}$上の方程式
　４．原始根
　５．平方剰余
　６．$\overline{-1}$が平方剰余になるための条件
　７．４乗剰余
　８．d乗剰余

第４章　ガウス周期
　１．d次のガウス周期
　２．積公式
　３．$p = 17$のときの２次のガウス周期

第５章　２次のガウス周期
　１．有限体上の２次曲線の点の数
　２．２次のガウス周期の基本定理の証明

6. 正 17 角形の作図

1．$p = 17$についての２次のガウス周期

2．$p = 17$についての４次のガウス周期

3．$p = 17$についての８次のガウス周期

参考文献

第１章　はじめに

私の卒論の目的は，「正１７角形が定規とコンパスで作図可能であること」の証明を行うことである.この事実は，数学者の王とも呼ばれたガウスが若干１８歳（1976 年３月 30 日）の時に証明されたものである．

この論文では，初等整数論から始め，ガウス周期というものを導入する．２次のガウス周期の基本定理の証明を与えることで，積の公式と三角関数をうまく使いながら，正１７角形の作図が可能であることを示していく.４次のガウス周期の基本定理の証明は間に合わなかったため，扱っていない．

この論文で，計算量は少々多いが，積の公式のみで様々な素数に対してのガウス周期を求めることが可能だとわかるだろう．

また，作図の基本的な条件として、定規とコンパスのみで作図をし，１という長さのみを与える．

第１章　正ｎ角形の作図

ここでは、正n角形の作図をするためには何を求めなければいけないのかということについて考えていく．円周をn等分に作図するという問題から出発し，１のn乗根（という複素数）を調べるのが重要であるということを説明する．そこには、三角関数やド・モアブルの定理など高等学校教育で学習する数学を扱って説明をしていき，正５角形が作図可能であることなど具体的な値についても触れていく．

ここでの作図可能とは，すべて定規とコンパスのみで作図ができることを指す．

1.1 円のn等分と正n角形

まずは，円のn等分について考える．円をn等分するということは，円Cとその円上にP_0が与えられた時，P_0からP_0P_1, P_1P_2，$P_{n-1}P_0$の元が全て等しくなる$P_1, P_2, \cdots, P_{n-1}$を作図することが可能であれば，正多角形を作図することができることと同値である．

そこでもしこのような点が作図できたなら，$\frac{360^\circ}{n}$という角度が作図できる．

またその逆も成り立ち，$\frac{360^\circ}{n}$が作図可能であれば，円の弧をn等分することが可能である.したがって，正n角形が作図できるとは，$\frac{360^\circ}{n}$が作図できるかという問題に言い換えられる．

また,n等分が可能な時に，（中学時代に習ったであろう）角の二等分線の作図方法を用いれば$2n$等分が可能なことがわかる．これを繰り返すことにより，2^mn 等分が可能である．

ここからは，上のことについて座標を使って考える．また，弧度法を取り入れ，180°をπで表す．与えられた円Cに対してその中心を 0 とし，半径を 1 とするよう座標を入れ，

$$P_0 = (\,1\,,0\,)$$

$$P_1 = (\,\cos\frac{2\pi}{n}\,,sin\frac{2\pi}{n})$$

$$P_2 = (\,\cos 2\frac{2\pi}{n}\,,sin2\frac{2\pi}{n})\,,\cdots$$

$$P_{n-1} = (\,\cos(n-1)\frac{2\pi}{n}\,,sin(n-1)\frac{2\pi}{n}\,)$$

となる． $\cos\frac{2\pi}{n}$という長さが作図可能ならば，$P_1{}' = (\,\cos\frac{2\pi}{n}\,,0)$として，$P_1{}'$を通り，$x$ 軸と垂直な線を作図することで，P_1を作図することができる．つまり，$\cos\frac{2\pi}{n}$という長さが作図可能であるならば，円を n 等分することが可能である．もちろん$\cos\frac{2\pi}{n}$という長さがわかっても問題ない．

1.2 複素平面と 1 の n 乗根

ガウスが最初に気づいたアイディアは，三角関数$sin\frac{2\pi}{n}$や$cos\frac{2\pi}{n}$を考えるのではなく，複素数

$$\cos\frac{2\pi}{n} + isin\frac{2\pi}{n}$$

を考える，ということであった．この複素数を$\zeta = \cos\frac{2\pi}{n} + isin\frac{2\pi}{n}$とおく．$\zeta$が満たす方程式は，ド・モアブルの公式により

$$\zeta^n = 1$$

である．

$1\,,\zeta\,,\zeta^2\,,\cdots,\zeta^{n-1}$は複素平面上で正 n 角形をなすことがわかる．

$x^n = 1$をみたす数を 1 の n 乗根と呼ぶが，$1\,,\zeta\,,\zeta^2\,,\cdots,\zeta^{n-1}$が方程式$x^n = 1$の n 個の解であり，1 の n 乗根である．

第２章　作図可能な図形

この章では，1という長さが与えられた時に具体的に作図できる長さを求め，また具体的な正多角形について触れる．また，円分体の世界にも少し触れ，作図可能な正多角形の数を増やしておく．

2.1 基本的な作図

1という長さが与えられたとき，正の実数aが作図できるとは，点$(a,0)$が作図できることと定義しよう．このとき，次のことが言える．

(ⅰ) a,bが作図できるとき，$a\pm b$, abは作図できる．

(ⅱ) a,bが作図でき，$b\neq 0$のとき，$\frac{a}{b}$ は作図できる．

(ⅲ) a が作図でき，$a>0$のとき，$\sqrt{a}$は作図できる．

(ⅰ), (ⅱ)については，図による確認だけにとどめておく．

(ⅲ)については，中心が$\left(\frac{a-1}{2},0\right)$で半径が$\frac{a+1}{2}$である円Cについて考える．円Cの方程式は次のようになる．

$$\left(x-\frac{a-1}{2}\right)^2+y^2=\left(\frac{a+1}{2}\right)^2$$

であり，この図形のy軸との交点を考える．つまり上の方程式に$x=0$を代入すると

$$\left(\frac{a-1}{2}\right)^2+y^2=\left(\frac{a+1}{2}\right)^2$$

$$y^2=\left(\frac{a+1}{2}\right)^2-\left(\frac{a-1}{2}\right)^2=a$$

を得られるので，$(0\ ,\pm\sqrt{a})$であることがわかる．

以上により，任意の整数，有理数，$\sqrt{m}$ $\left(m\text{は正の有理数}\right)$が作図可能である．また，$b\neq 0$のとき，(ⅰ), (ⅱ)を使って，$\frac{a\pm\sqrt{m}}{b}$も作図可能である．

2.2　n次の無理数

αが有理数係数の代数方程式の解になるような無理数であるとする．αを解にもつ有理数方程式のうち，次数が最小のものを考え，その次数がnであるとき，

αはn次の無理数であるという．

ここで，定規と作図によって作図できる点の座標は，円が２次の曲線であることから，全て２次方程式を何度か繰り返して解くことによって得られる．xが作図可能であるとすると，２次方程式を何度か繰り返して解くことによってxが得られるので，xは(適当な負でない整数mに対して)2^m次の無理数となることがわかる．

2.3　円分数の世界

m_1, m_2は互いに素な３以上の整数で，nが$n = m_1 m_2$とかけているとする．ここで，正m_1角形とm_2角形が作図可能であるとき，正$n = m_1 m_2$角形も作図可能である．なぜなら，

$$m_1 x + m_2 y = 1$$

というx, yの不定方程式は，m_1とm_2が互いに素なので，整数解をもつ．(これは高校でも扱う内容であるため証明は省く)．両辺をnで割ると，

$$\frac{x}{m_2} + \frac{y}{m_1} = \frac{1}{n}$$

である．よって，

$$\cos\frac{2\pi}{n} = \cos\left(\frac{2\pi x}{m_2} + \frac{2\pi y}{m_1}\right)$$

であり，加法定理によって，$\cos\frac{2\pi x}{m_2}$，$sin\frac{2\pi x}{m_2}$，$\cos\frac{2\pi x}{m_1}$，$sin\frac{2\pi x}{m_1}$と整数の$\pm, \times, \div, \sqrt{*}$によって，$\cos\frac{2\pi}{n}$を表すことができる．これらの値は仮定示されているので，$\cos\frac{2\pi}{n}$は作図可能である．

第３章　有限体

この章では，合同式を使わずに，素数pに対してp個の有限体$\mathbb{F}_p$を導入して説明していく．ここは第４章以降の準備であり，後々扱う大事な性質や単語として，正多角形を書く上で必須となる原始根という言葉や$p-1$個の$\bar{1}, \bar{2}, \bar{3}, \cdots, \overline{p-1}$を剰余類というものに分けて，長方形に並べることがある．

また，この章の前半に関しては，高校の延長の内容が多い為，いくつか証明を省く．

3.有限体$\mathbb{F}_p$

pを素数として，前の章と同様に

$$\zeta = \cos\left(\frac{2\pi}{p}\right) + isin\left(\frac{2\pi}{p}\right)$$

とおく．ζに対して,その冪ζ^nを考える．$1,\zeta,\zeta^2,\cdots$は，複素平面上の単位円上で，正多角形の頂点をなすが，$\zeta^p = 1$であるから，$n \geq p$に対しても，ζ^nを考えていくと，$\zeta^{p+1} = \zeta$ $\zeta^{p+2} = \zeta^2,\cdots$と進むことになる．負の n についても同様に考えられる．よって，n は無限個あるが，現れる値は$\zeta,\zeta^2,\cdots,\zeta^{p-1},\zeta^p$の$p$個しかない。合同式を用いて表すと次のようになる．

$$a \equiv b\ (mod\ p)\ であれば\quad \zeta^a = \zeta^b$$

が成り立つ．この証明を次に示す．$a \equiv b\ (mod\ p)$というのは，$a - b = pk$となるような整数kがあることだから，

$$(\Rightarrow)\qquad \zeta^a = \zeta^{b+pk} = \zeta^b\zeta^{pk} = \zeta^{b(\zeta^p)^k} = \zeta^b$$

$(\Leftarrow)$　$1 = \zeta^{pk}$ *であることに注意して*

$$\zeta^a = \zeta^b$$

両辺にζ^{-b}をかけると

$$\zeta^{a-b} = 1 = \zeta^{pk}$$

$$\therefore\ a - b = pk$$

さらに，$a \equiv b\ (modp)$のとき，次のように書くとする。

$$\overline{a} = \overline{b}\ \Leftrightarrow\ a \equiv b\ (mod\ p)$$

すると，任意の$\overline{n}$ について，$\overline{0},\overline{1},\overline{2},\cdots,\overline{p-1}$の$p$個のどれかに一致することがわかる．そこで ,この$p$個の記号全体を

$$\mathbb{F}_p = \left\{\overline{0},\overline{1},\overline{2},\cdots,\overline{p-1}\right\}$$

と書くことにする．また，$\mathbb{F}_p$から$\overline{0}$を除いた集合を$\mathbb{F}_p^{\times}$と書く．つまり以下のようになる．

$$\mathbb{F}_p^{\times} = \left\{\overline{1},\overline{2},\cdots,\overline{p-1}\right\}$$

また上記のことにより，

$$\overline{a} = \overline{b}\ \Leftrightarrow\ \zeta^a = \zeta^b$$

$\mathbb{F}_p$の世界では，次のことが定義できる． 証明に関しては明快であるためここでは省く．

(3.1.1.)$\mathbb{F}_p$の元$\overline{a}$, $\overline{b}$ に対して， $\overline{a} \pm \overline{b} = \overline{a \pm b}$, $\overline{a} \times \overline{b} = \overline{ab}$と定義することにより，加法と減法と乗法が定義される．

割り算については，次の定理がある．この定理の証明にはpが素数であることが本質的

に使われる．

(定理 3.1.2) $\mathbb{F}_p$の世界で，$\overline{b} \neq \overline{0}$とすると，ある$\overline{x} \in \mathbb{F}_p$で

$$\overline{b} \times \overline{x} = \overline{a}$$

となるものがただ一つ存在する．

証明 条件の$\overline{b} \times \overline{x} = \overline{a}$は普通の整数の言葉に直すと「$bx - a = pk$となる整数$k$が存在する」という意味になる．つまり，

$$bx - pk = a$$

となるような整数x, kが存在することを証明すればよい．$\overline{b} \neq \overline{0}$であるから，$b$と$p$は互いに素である．この方程式が整数解を持つことは，高校の内容であるためここでは省く．ここでは，$\mathbb{F}_p$の世界では，$\overline{x}$の一意性を示す．

$$\overline{a} = \overline{b} \times \overline{x} = \overline{b} \times \overline{x'}$$

とかけたとする．$\overline{x} = \overline{x'}$を示す．$bx = a + pk,\ bx' = a + pk'$となるような整数$k, k'$が存在する，ということである．最初の式から次の式を引くと，$bx - bx' = pk - pk'$となる．したがって，$b(x - x') = p(k - k')$となる．左辺がpで割れるわけだが，bとpが互いに素であるから，$x - x'$はpで割れなければならない．これは，$\overline{x} = \overline{x'}$を意味している．

特に，$\overline{b} \neq \overline{0}$のとき，$\overline{b}\,\overline{x} = \overline{1}$となる$\overline{x} \in \mathbb{F}_p$を$b^{-1}$と書く．
つまり，$\mathbb{F}_p$は加減乗除で閉じた有限体であることがわかる．

3.2 有限体の乗法群

$\mathbb{F}_p$の$\overline{0}$でない元は何乗かすると，必ず$\overline{1}$になる．つまり，
命題 3.2.1
pを素数として，$\overline{a}$ を $\overline{0}$ ではない$\mathbb{F}_p$の元とするとき，

$$\overline{a}^n = \overline{1}$$

を満たす整数 n が存在する．
$\overline{0}$ ではない$\mathbb{F}_p$の元 $\overline{a}$ に対して，$\overline{a}^n$を満たす最小の正整数 n を $\overline{a}$ の位数という．さらに，位数について，次の定理を証明できる．

定理 3.2.2　$\mathbb{F}_p^{\times}$の任意の元 $\overline{a}$ に対して，$\overline{a}$ の位数は$p - 1$の位数である．

証明

H $= \{\overline{1}, \overline{a}, \overline{a}^2, \cdots, \overline{a}^{n-1}\}$とおく．上に書いた$\overline{1}, \overline{a}, \overline{a^2}, \cdots, \overline{a^{n-1}}$はすべてことなることに注意する．もし，$H = \mathbb{F}_p^{\times}$であるとすると$p = n - 1$であり，定理は証明される．もし，H の方が$\mathbb{F}_p^{\times}$より真に小さければ H に属さない$\overline{b}_2 \in \mathbb{F}_p^{\times}$をとる．

$$b_2 H = \{\overline{b}_2\overline{1}, \overline{b}_2\overline{a}, \overline{b}_2\overline{a}^2, \cdots, \overline{b}_2\overline{a}^{n-1}\}$$

とおく．$b_2 H$は H と同様に n この元からなる．$b_2 H$は$\overline{b}_2$で決まるので$\overline{b}_2 H$と書くべきだが，見やすいよう上記のように書くことにする．もし，$0 \le s \le t \le n-1$の範囲での整数s, tに対して，$\overline{b}_2\overline{a}^s = \overline{b}_2\overline{a}^t$があると仮定すると，$\overline{b}_2\overline{a}^s$で割ると，$\overline{a}^{t-s} = \overline{1}$が導かれ，これは n の最小性に矛盾する．また，

$$H \cap b_2 H = \emptyset$$

である．これは，$x \in H \cap b_2 H$とすると，$x = b_2\overline{a}^s = \overline{a}^t$を x が満たすことであるが，$b_2 = \overline{a}^{t-s}$となり，$b_2 \in H$であることがわかるが，これは$b_2$の取り方に矛盾する．
もし，$\mathbb{F}_p^{\times} = H \cup b_2 H$とすると，$n = \frac{p-1}{2}$であり定理が証明できる．そこで，$H \cup b_2 H$が$\mathbb{F}_p^{\times}$より真に小さいとする．同様に$H \cup b_2 H$に属さない$b_3 \in \mathbb{F}_p^{\times}$をとる．

$$b_3 H = \{\overline{b}_3\overline{1}, \overline{b}_3\overline{a}, \overline{b}_3\overline{a}^2, \cdots, \overline{b}_3\overline{a}^{n-1}\}$$

とおく．$b_3 H$は H と同様に n この元からなる．$b_2 H$のときと全く同じように証明することで，$b_3 H \cap (H \cup b_2 H) = \emptyset$が示せる．$\mathbb{F}_p^{\times} = b_3 H \cap (H \cup b_2 H)$ とすると，$n = \frac{p-1}{3}$となり証明することができる．これを繰り返し，$b_2, b_3, \cdots, b_m$をうまくとることで$\mathbb{F}_p^{\times}$を次のような長方形に並べられることがわかる．

$\overline{1}$	$\overline{a}$	$\overline{a}^2$	$\cdots$	$\overline{a}^{n-1}$
$\overline{b}_2$	$\overline{b}_2\overline{a}$	$\overline{b}_2\overline{a}^2$	$\cdots$	$\overline{b}_2\overline{a}^{n-1}$
$\overline{b}_3$	$\overline{b}_3\overline{a}$	$\overline{b}_3\overline{a}^2$	$\cdots$	$\overline{b}_3\overline{a}^{n-1}$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$\overline{b}_m$	$\overline{b}_m\overline{a}$	$\overline{b}_m\overline{a}^2$	$\cdots$	$\overline{b}_m\overline{a}^{n-1}$

$\mathbb{F}_p^{\times}$は$p-1$個の元からなるので，上の長方形の中の元の数を数えると

$$mn = p - 1$$

を得る．したがって，は$p-1$の約数となり，定理 3.2.2 が証明された．

命題　3.2.3
$\overline{a} \in \mathbb{F}_p^{\times}$の位数を$n$とする． 正の整数$m$にたいして$\overline{a}^m = \overline{1}$が成り立つとすると，$n$は$m$の約数である．

証明 まず位数の定義から，$n \leq m$である．nがmの約数でないとすると，mをnで割ったときの余りkは 0 ではなく，$0 < k < n$を満たす正の整数である．$m = nq +$ k(q*は正の整数*)と書けるので，

$$\overline{a}^{k} = \overline{a}^{m-nq} = \overline{a}^{m}\left(\overline{a}^{n}\right)^{-q} = \overline{1}$$

となり，このときはnの最小性に矛盾する．

3.3 $\mathbb{F}_p^{\times}$上の方程式

ここでは，$\mathbb{F}_p$を係数にもつ方程式について軽く触れる．$\mathbb{F}_p$が加減乗除のできる世界であることから，$\mathbb{F}_p$を係数にもつ方程式は実数の世界で方程式を考えた時と同じように話を進められる． まず，$\mathbb{F}_p$上の多項式とは，

$$f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n \qquad (\alpha_0, \cdots, \alpha_n \in \mathbb{F}_p)$$

の形の式のことである．$\alpha_0 \neq \overline{0}$のとき，この式は$n$次式であるという．$\mathbb{F}_p$上の$x$を変数とする多項式全体を$\mathbb{F}_p[x]$と表す．

命題 3.3.1
$f(x)$が$\mathbb{F}_p$上の多項式であり，$f(x) = g(x)h(x)$（$g(x), h(x) \in \mathbb{F}_p[x]$）と二つの多項式の積に因数分解されているとする．$\alpha \in \mathbb{F}_p$が$f(x)$の解であるとする，つまり，$f(\alpha) = \overline{0}$であるとすると$g(\alpha) = \overline{0}$か$h(\alpha) = \overline{0}$のどちらかが成り立つ．

証明 $g(\alpha) \neq \overline{0}$であるとする．定理 3.1.2 から$g(\alpha)g(\alpha)^{-1} = \overline{1}$となる，$g(\alpha)^{-1} \in \mathbb{F}_p^{\times}$が存在する．$f(\alpha) = g(\alpha)h(\alpha) = \overline{0}$であるから，$g(\alpha)^{-1}$を両辺にかけると，$h(\alpha) = \overline{0}$を得る．つまり，$g(\alpha) = \overline{0}$か$h(\alpha) = \overline{0}$のどちらかが成り立つ．

命題 3.3.2 (因数定理)
$\alpha \in \mathbb{F}_p$が$\mathbb{F}_p$上のn次の多項式$f(x)$の解であるとする．このとき，$f(x) = (x - \alpha)\, g(x)$となるような$n - 1$次の多項式$g(x) \in \mathbb{F}_p[x]$が存在する．

この証明は，高校で扱う因数定理と同じように証明できるので，ここでは省略する．
次の命題は，原始根の存在を証明するのに大切な証明になる．

命題 3.3.3 $\mathbb{F}_p$を係数とするn次方程式

$$x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n = \overline{0} \qquad (\alpha_1, \cdots, \alpha_n \in \mathbb{F}_p)$$

は$\mathbb{F}_p$に解を n 個以下しか持たない.

証明 nについての帰納法で示す. $n = 1$のとき, $x + \alpha_1 = \overline{0}$ の解は, $x = -\alpha_1$のみである.

$n = k$で成立すると仮定するとして, $n = k + 1$で成立することを示す. $k + 1$次式, $f(x) = x^{k+1} + \alpha_1 x^k + \cdots + \alpha_{k+1}$を考える. $f(x)$が$\mathbb{F}_p$に解を持たないとすると, 0 個の解を持つので, 題意をみたしている. そこで, $\mathbb{F}_p$に解を持つとする. βを解とする. このとき, 因数定理により, $f(x) = (x - \beta)g(x)$, $g(x) \in \mathbb{F}_p[x]$と因数分解される. 命題 3.3.1 により, $f(x) = \overline{0}$の解は, βと$g(x) = \overline{0}$の解であり, $g(x)$はk 次式であるので, $g(x)$の解は帰納法の仮定により, k 個以下の解を持つ. よって, $f(x)$は$k + 1$個以下の解を持つ. 以上により, 任意の次数の多項式にたいして, 上の命題は成立する.

3.4 原始根

次の条件を満たす整数のことを原始根と呼ぶ.

定義 $\overline{g}$が$\mathbb{F}_p^{\times}$の位数$p - 1$の元のとき, 整数 g を p の原始根と呼ぶ. また, 正の整数の原始根の中で最小のものを, 最小原始根と呼ぶ.

$p < 50$を満たす全ての素数に対して, 最小原始根を求めると次の表のようになる.

素数	2	3	4	7	11	13	17	19	23	29
原始根	1	2	2	3	2	2	3	2	5	2

また, 任意の素数pに対して, 原始根が存在する. それは, 次の定理によって示すことができる.

定理 3.4.1　任意の素数pに対して, $\mathbb{F}_p^{\times}$には位数$p - 1$の元が存在する.

証明 $p - 1$を

$$p - 1 = l_1^{e_1} \cdots l_r^{e_r}$$

と素因数分解する(ここで $l_1, \cdots, l_r$は相異なる素数, $e_1, \cdots, e_r$は正の整数). i を 1 以上r

以下の整数として，方程式

$$x^{\frac{p-1}{l_i}} = \overline{1}$$

を考える．この方程式の次数は$\frac{p-1}{l_i}$ だから，$\frac{p-1}{l_i} < p-1$ と命題 2.3.3 により，$\mathbb{F}_p^{\times}$の元が全て解になることはできない．そこで，上の方程式の解でない，$\mathbb{F}_p^{\times}$の元 αを取ることができる．

$$\beta_i = \alpha_i^{\frac{p-1}{l_i^{e_i}}}$$

とおく．仮定により

$$\beta_i^{l_i^{e_i-1}} = \alpha_i^{\frac{p-1}{l_i}} \neq \overline{1}$$

である．また，フェルマの小定理により$\beta_i^{l_i^{e_i}} = \alpha_i^{p-1} = \overline{1}$である．したがって，$\beta_i$は位数$l_i^{e_i}$を持つことが次のようにしてわかる．

まず，β_iの位数をn とすると，命題 3.2.3 から n は $l_i^{e_i}$の約数である．次に，$n \neq l_i^{e_i}$と仮定すると，l_iは素数だから，n は$l_i^{e_i-1}$の約数で

$$\beta_i^{l_i^{e_i-1}} = (\beta_i^n)^{\frac{l_i^{e_i-1}}{n}} = \overline{1}^{\frac{l_i^{e_i-1}}{n}} = \overline{1}$$

となり矛盾する．したがって，$n = l_i^{e_i}$ ，つまり$\beta_i^{e_i}$ である．

以上から，各 $i = 1, \cdots, r$ にたいして，位数 $l_i^{e_i}$ をもつ元β_i の存在がわかった．

そこで，

$$\beta = \beta_1 \cdots \beta_r$$

とおく．βの位数が$p-1$であることを証明する．

βの位数をmとすると，定理 3.2.2 により．mは$p-1$の約数である．したがって，$p-1 = mt$となる整数t がある．$t > 1$と仮定する．t を割る素数は，$p-1$を割る素数なので，$l_1^{e_1} \cdots l_r^{e_r}$のどれかである．$l_1$ がt を割るとしても一般性は失わないので，l_1 がt の約数であるとする．$t = l_1 t' \left(t' \text{は整数}\right)$と書くと，$\beta^{mt'} = (\beta^m)^{t'} = \overline{1}$となるが，一方

$$mt' = \frac{mt}{l_1} = \frac{p-1}{l_1} = l_1^{e_1-1} l_2^{e_2} \cdots l_r^{e_r}$$

を考えると，$r \geq 2$のとき，$i = 2, \cdots, r$に対して，mt'は倍数であるので，$\beta^{mt'} = \beta_2^{mt'}$となる．$\beta_1^{mt'} = \beta^{mt'} = \overline{1}$である．$\beta_1$の位数が$l_1^{e_1}$だったので，命題 3.2.3 から$l_1^{e_1}$は$mt' =$

$\frac{p-1}{l_1}$の約数となるが，これは矛盾である．

以上により，$t>1$という仮定に誤りがあることがわかり，$t=1$である．つまり，$m=p-1$ であり，β の位数は$p-1$である．

3.5 平方剰余

これ以降では,pは奇素数とする．gをpの原始根とする．定義により，$\overline{g}$の位数は$p-1$である．$\overline{g}^2$の位数は$\frac{p-1}{2}$である．すると，上で書いたような長方形を書くと

$\overline{1}$	$\overline{g}^2$	$\overline{g}^4$	$\cdots$	$\overline{g}^{p-3}$
$\overline{g}$	$\overline{g}^3$	$\overline{g}^5$	$\cdots$	$\overline{g}^{p-2}$

となる．$\overline{g}^{p-1}=\overline{1}$に注意しておく．上の行に並ぶ集合を$H_2$とする．下の行を$gH_2$とする．

$$\mathbb{F}_p^{\times}=H_2\cup gH_2$$

である．

ここで，$p=17$の平方剰余を求める．

p=17, g=3 とする.$\overline{1}=\overline{1},\overline{3}=\overline{3}$ ，$\overline{3}^2=\overline{9}$ ，$\overline{3}^3=\overline{27}=\overline{10}$ ，$\overline{3}^4=\overline{81}=\overline{13}$，$\cdots,\overline{3}^{16}=\overline{6}$ となるので，以下の表が書ける．

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

となる.よって，

$$H_2=\{\overline{1},\overline{9},\overline{13},\overline{15},\overline{16},\overline{8},\overline{4},\overline{2}\}$$
$$gH_2=\{\overline{3},\overline{10},\overline{5},\overline{11},\overline{14},\overline{7},\overline{12},\overline{6}\}$$

ということである．

H_2に含まれる元について，

$$H_2=\{\overline{g}^{2k}\mid k\text{は整数}\}$$

と書くことができ，次のことが成り立つことがわかる．

$\overline{a}\in\mathbb{F}_p$に対して，

$$\overline{a}\in H_2\Leftrightarrow\overline{a}=\overline{b}^2\text{を満たす}\overline{b}\in\mathbb{F}_p^{\times}\text{が存在する}$$

この同値関係を証明する．

(→) $\overline{a} \in H_2$であれば，$\overline{a} = \overline{g}^{2k}$とかけているので，$\overline{a} = \left(\overline{g}^{k}\right)^2$であり，$b = \overline{g}^{k}$ととれば，

$\overline{a} = \overline{b}^2$とかける．

(←) $\overline{a} = \overline{b}^2, \overline{b} \in \mathbb{F}_p^{\times}$であるとすると，$H_2$の元はすべて$\overline{g}$を使って書けるので，$b = \overline{g}^{j}$(j は整数)と書けるわけだが，このとき，$\overline{a} = \left(\overline{g}^{j}\right)^2 = \overline{g}^{2j}$となり，$H_2$にはいる．■

つまり，

$$H_2 = \left\{\overline{b}^2 \middle| \overline{b} \in \mathbb{F}_p^{\times}\right\}$$

と書けるのである．この表示から，H_2はgの取り方によらないことがわかる．またgH_2もgの取り方によらない．

ここで，整数aが$\overline{a} \in H_2$を満たすとき，aはpの平方剰余であるという．

また，整数aが$\overline{a} \in gH_2$を満たすとき，aはpの非平方剰余であるという．

3.6　$\overline{-1}$が平方剰余になるための条件

定理 3.6.1 pが$p \equiv 1\ (mod\ 4)$を満たすとき，-1はpの平方剰余であり，$p \equiv 3\ (mod\ 4)$を満たすとき，-1はpの非平方剰余である．

証明　gを原始根として，$\overline{g}^{\frac{p-1}{2}}$を考えると，$g$の定義から$\overline{g}^{\frac{p-1}{2}} \neq \overline{1}$である．また，$\left(\overline{g}^{\frac{p-1}{2}}\right)^2 = \overline{g}^{p-1} = \overline{1}$となる．$\mathbb{F}_p$のなかで，$x^2 = \overline{1}$をみたすのは，$\overline{1}$と$\overline{-1}$しかないので，

$$\overline{g}^{\frac{p-1}{2}} = -1$$

が得られる．

この等式を使って，定理 3.6.1 を証明する．$p \equiv 1\ (mod\ 4)$とする．このとき，

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

であり，$\overline{-1} = \overline{g}^{\frac{p-1}{2}} \in H_2$である．したがって，$-1$は$p$の平方剰余である．次に，$p \equiv 3\ (mod\ 4)$とする．このとき，

$$\overline{g}^{\frac{p-1}{2}} = \overline{g} \cdot \overline{g}^{\frac{p-3}{2}} = \overline{g}\left(\overline{g}^{\frac{p-3}{4}}\right)^2 \in gH_2$$

となり，-1はpの非平方剰余となる．

3.7 4 乗剰余

nを正の整数，aをpと素な整数とする．xについての合同式

$$x\text{^}n \equiv a \pmod{p}$$

が整数解を持つとき，aをpのn乗剰余であるという． $n = 2$のときが平方剰余となる．ここからは,$n = 4$のときについて考える． gを p の原始根とする．平方剰余のときと同様に，以下のような長方形を書く．

$\overline{1}$	$\overline{g}^4$	$\overline{g}^8$	$\cdots$	$\overline{g}^{p-5}$
$\overline{g}$	$\overline{g}^5$	$\overline{g}^9$	$\cdots$	$\overline{g}^{p-4}$
$\overline{g}^2$	$\overline{g}^6$	$\overline{g}^{10}$	$\cdots$	$\overline{g}^{p-3}$
$\overline{g}^3$	$\overline{g}^7$	$\overline{g}^{11}$	$\cdots$	$\overline{g}^{p-2}$

第一行全体の集合をH_4と書くことにする．平方剰余のときと同様な証明を行うことで,

$$H_4 = \{\alpha^2 | \alpha \in \mathbb{F}_p^{\times}\}$$

となることがわかる.よってH_4は原始根の取り方によらないことがわかる．

ここで，$p = 17$の 4 乗剰余を求めてみる．

p=17, g=3 とする.$\overline{1} = \overline{1}, \overline{3} = \overline{3}$, $\overline{3}^2 = \overline{9}$, $\overline{3}^3 = \overline{27} = \overline{10}$, $\overline{3}^4 = \overline{81} = \overline{13}$, $\cdots, \overline{3}^{16} = \overline{6}$ となるので，以下の表が書ける．

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

3.7 d乗剰余

dを$p-1$の約数とする．gをpの原始根として，

$$H_d = \{\overline{1}, \overline{g}^d, \overline{g}^{2d}, \cdots, \overline{g}^{(\frac{p-1}{d}-1)d}\}$$

とおく．H_dは$\frac{p-1}{d}$個の元からできている集合である．平方剰余のときと同様な証明を与

えることで,

補題　3.7.1　dを$p-1$の約数とする．gをpの原始根として,

$$H_d = \{\alpha^d \mid \alpha \in \mathbb{F}_p^{\times}\}$$

が成り立つ.

また，右辺にgが出てきていないことからH_dは原始根の取り方によらないことがわかる.

４．ガウス周期

この章では，ζの話にもどる．pを素数として

$$\zeta = \cos\left(\frac{2\pi}{p}\right) + isin\left(\frac{2\pi}{p}\right)$$

とおく．第１章で述べたように，$1, \zeta, \zeta^2, \cdots$と複素数平面上に並べていくと，単位円上に正$p$角形ができる．

4.1　d次のガウス周期

αを$\mathbb{F}_p$の元とする．$\alpha = \overline{a}$ のとき，

$$\zeta^{\alpha} = \zeta^{a}$$

と定義すると， この定義は a の取り方によらない．また次のことがわかる．

$$\sum_{\alpha \in \mathbb{F}_p} \zeta^{\alpha} = 0$$

証明　$x^p = 1$から$x^p - 1 = 0$であり，ζはこのxの解であるから，

$$\zeta^p - 1 = (\zeta - 1)(\zeta^{p-1} + \zeta^{p-2} + \cdots + 1) = 0$$

$\zeta - 1 \neq 0$より

$$\zeta^{p-1} + \zeta^{p-2} + \cdots + 1 = 0$$

を得る．

また，$\zeta^{p-1} + \zeta^{p-2} + \cdots + 1 = 0$より

$$\zeta^{p-1} + \zeta^{p-2} + \cdots \zeta = -1$$

$$\sum_{\alpha \in \mathbb{F}_p^{\times}} \zeta^{\alpha} = -1$$

が得られる．

定義 3.1.1

整数 a と$\mathbb{F}_p$の元βに対して，$a\beta = \overline{a}\beta$と定義する．任意の整数 a と$p-1$の約数$d$に対して，$[a]_d$を

$$[a]_d = \sum_{\beta \in H_d} \zeta^{a\beta}$$

で定義する．この形の数をd次のガウス周期と呼ぶことにする．H_dは前章で示した，

$H_d = \{\overline{1}, \overline{g}^d, \overline{g}^{2d}, \cdots, \overline{g}^{(\frac{p-1}{d}-1)d}\}$である．

この定義から成り立つ性質を紹介しておく．

命題 4.1.2

(1) aがpの倍数のとき，$[a]_d = \frac{p-1}{d}$である．

(2) aがpと互いに素なとき，$\mathbb{F}_p^\times$の中の$\overline{a}$が属するH_dの剰余類をaH_dと書くことにする．

このとき，

$$[a]_d = \sum_{\beta \in aH_d} \zeta^\beta$$

(3) $a \equiv b \ (mod\ p)$であれば，$[a]_d = [b]_d$である．

(4)aがpと互いに素で，整数bが$\overline{b} \in aH_d$を満たせば，$[a]_d = [b]_d$である．

証明

(1)aがpの倍数のとき，$\zeta^{a\beta} = \zeta^0 = 1$となるので，$H_d$が$\frac{p-1}{d}$個の元の集合であることから，

$$[a]_d = \sum_{\beta \in H_d} 1 = \frac{p-1}{d}$$

となる．

(2)は定義からすぐにわかる．

(3) $[a]_d$が

$$[a]_d = \sum_{\beta \in H_d} \zeta^{a\beta} = \sum_{\beta \in H_d} \zeta^{\overline{a}\beta}$$

と書けることから，

$$[a]_d = \sum_{\beta \in H_d} \zeta^{\overline{a}\beta} = \sum_{\beta \in H_d} \zeta^{\overline{b}\beta} = [b]_d$$

(4) $\overline{b} \in aH_d$が成り立つとき，$aH_d = bH_d$である．(2)より

$$[a]_d = \sum_{\beta \in aH_d} \zeta^\beta = \sum_{\beta \in bH_d} \zeta^\beta = [b]_d$$

が得られる．

$p = 17$の２次のガウス周期について求める．17 の最小原始根は３である．

$H_2 = \{\overline{1}, \overline{9}, \overline{13}, \overline{15}, \overline{16}, \overline{8}, \overline{4}, \overline{2}\}$，$3H_2 = \{\overline{3}, \overline{10}, \overline{5}, \overline{11}, \overline{14}, \overline{7}, \overline{12}, \overline{6}\}$ であることに注意し，

$$[1]_2 = \sum_{\beta \in H_2} \zeta^{1\cdot\beta}$$

$$= \zeta^1 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2$$

$$[3]_2 = \sum_{\beta \in H_2} \zeta^{3\cdot\beta}$$

$$= \sum_{\alpha \in 3H_2} \zeta^{\alpha}$$

$$= \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$$

となる．ここで，$[1]_2 + [3]_2$について

$$[1]_2 + [3]_2 = \zeta^1 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2 + \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$$

$$= \sum_{\alpha \in \mathbb{F}_p^{\times}} \zeta^{\alpha} = -1$$

となることがわかる．

同様に，$p = 17$の４次のガウス周期について求める．

$H_4 = \{\overline{1}, \overline{13}, \overline{16}, \overline{4}\}$ ，$3^2 H_4 = \{\overline{9}, \overline{15}, \overline{8}, \overline{2}\}$であることに注意すると，

$$[1]_4 = \sum_{\beta \in H_4} \zeta^{1\cdot\beta} = \zeta^1 + \zeta^{13} + \zeta^{16} + \zeta^4$$

$$[9]_4 = \sum_{\beta \in H_4} \zeta^{9\cdot\beta} = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2$$

となる．また，$[1]_4 + [9]_4 = [1]_2$であることがわかる．

4.2 積公式

定理 4.2.1　a, bを整数とする．このとき

$$[a]_d \cdot [b]_d = \sum_{\alpha \in H_d} \left[\overline{a} + \overline{b}\alpha\right]_d$$

$$= \sum_{\alpha \in H_d} \left[\overline{a}\alpha + \overline{b}\right]_d$$

が成り立つ．

証明

gを原始根として，$h = g^d$，$k = \frac{p-1}{d}$ とおくと，

$$H_d = \left\{\overline{1}, \overline{h}, \overline{h}^2, \cdots, \overline{h}^{k-1}\right\}$$

である．したがって，

$$[a]_d = \zeta^a + \zeta^{ah} + \zeta^{ah^2} + \cdots + \zeta^{ah^{k-1}}$$
$$[b]_d = \zeta^b + \zeta^{bh} + \zeta^{bh^2} + \cdots + \zeta^{bh^{k-1}}$$

となる．よって，

$$\begin{aligned}[a]_d \cdot [b]_d = {} & \zeta^{a+b} + \zeta^{a+bh} + \zeta^{a+bh^2} + \quad \cdots \quad + \zeta^{a+bh^{k-1}} \\ & \zeta^{ah+b} + \zeta^{(a+b)h} + \zeta^{ah+bh^2} + \quad \cdots \quad + \zeta^{ah+bh^{k-1}} \\ & \zeta^{ah^2+b} + \zeta^{ah^2+bh} + \zeta^{ah^2+bh^2} + \quad \cdots + \zeta^{ah+bh^{k-1}} \\ & \cdots \qquad\qquad\qquad\qquad \cdots \\ & \zeta^{ah^{k-1}+b} + \zeta^{ah^{k-1}+bh} + \zeta^{ah^{k-1}+bh^2} + \cdots + \zeta^{(a+b)h^{k-1}}\end{aligned}$$

を得る．上で，まず対角線上の和をとると

$$\zeta^{a+b} + \zeta^{(a+b)h} + \zeta^{(a+b)h^2} + \cdots + \zeta^{(a+b)h^{k-1}} = [a+b]_d$$

次に，その一つ斜め上の対角線の

$$\zeta^{a+bh}, \zeta^{ah+bh^2}, \cdots, \zeta^{ah^{k-2}+bh^{k-1}}$$

を加え，最後の行の第 1 項にある$\zeta^{ah^{k-1}+b} = \zeta^{(a+bh)h^{k-1}}$であることに注意して加えると，

$$\zeta^{a+bh} + \zeta^{ah+bh^2} + \cdots + \zeta^{ah^{k-2}+bh^{k-1}} + \zeta^{ah^{k-1}+b} = [a+bh]_d$$

同様に次の斜め上の値と$k-1$行目の第 1 項の値とk行目の第 2 項を加えると

$$\zeta^{a+bh^2} + \zeta^{ah+bh^3} + \cdots + \zeta^{ah^{k-3}+bh^{k-1}} + \zeta^{ah^{k-2}+bh} + \zeta^{ah^{k-1}+bh} = [a+bh^2]_d$$

これを同様に続けていくと

$$[a]_d \cdot [b]_d = [a+b]_d + [a+bh^2]_d + \cdots + [a+bh^{k-1}]_d = \sum_{\alpha \in H_d} \left[\overline{a} + \overline{b}\alpha\right]_d$$

と，証明できる．

p=17 のときの，$[1]_2 \cdot [3]_2$と$[1]_4 \cdot [9]_4$の値を求めてみる．

$[1]_2 \cdot [3]_2$について，$H_2 = \{\overline{1}, \overline{9}, \overline{13}, \overline{15}, \overline{16}, \overline{8}, \overline{4}, \overline{2}\}$であることに注意して，

$$[1]_2 \cdot [3]_2 = \sum_{\alpha \in H_2} \left[\overline{1}\alpha + \overline{3}\right]_2$$
$$\begin{aligned}= {} & \left[\overline{1}\cdot\overline{1} + \overline{3}\right]_2 + \left[\overline{1}\cdot\overline{9} + \overline{3}\right]_2 + \left[\overline{1}\cdot\overline{13} + \overline{3}\right]_2 + \left[\overline{1}\cdot\overline{15} + \overline{3}\right]_2 + \left[\overline{1}\cdot\overline{16} + \overline{3}\right]_2 \\ & + \left[\overline{1}\cdot\overline{8} + \overline{3}\right]_2 + \left[\overline{1}\cdot\overline{4} + \overline{3}\right]_2 + \left[\overline{1}\cdot\overline{2} + \overline{3}\right]_2 \\ = {} & [\overline{4}]_2 + [\overline{12}]_2 + [\overline{16}]_2 + [\overline{18}]_2 + [\overline{19}]_2 + [\overline{11}]_2 + [\overline{7}]_2 + \left[\overline{5}\right]_2 \\ = {} & \left[\overline{1}\right]_2 + \left[\overline{3}\right]_2 + \left[\overline{1}\right]_2 + \left[\overline{1}\right]_2 + \left[\overline{1}\right]_2 + \left[\overline{3}\right]_2 + \left[\overline{3}\right]_2 + \left[\overline{3}\right]_2 \\ = {} & 4([1]_2 + [3]_2) = -4 \qquad \left([1]_2 + [3]_2 = -1 \text{ を使った}\right)\end{aligned}$$

同様に計算を行うと，$H_4 = \{\overline{1}, \overline{13}, \overline{16}, \overline{4}\}$であることに注意して

$$[1]_4 \cdot [9]_4 = \sum_{\alpha \in H_4} \left[\overline{1}\alpha + \overline{9}\right]_4$$

$$= \left[\overline{1} \cdot \overline{1} + \overline{9}\right]_4 + \left[\overline{1} \cdot \overline{13} + \overline{9}\right]_4 + \left[\overline{1} \cdot \overline{16} + \overline{9}\right]_4 + \left[\overline{1} \cdot \overline{4} + \overline{9}\right]_4$$

$$= \left[\overline{10}\right]_4 + \left[\overline{21}\right]_4 + \left[\overline{25}\right]_4 + \left[\overline{13}\right]_4$$

$$= \left[\overline{10}\right]_4 + [\overline{4}]_4 + \left[\overline{8}\right]_4 + \left[\overline{13}\right]_4$$

ここで，$gH_4 = \{\overline{3}, \overline{5}, \overline{14}, \overline{12}\}$，$g^2H_4 = \{\overline{9}, \overline{15}, \overline{8}, \overline{2}\}$，$g^3H_4 = \{\overline{10}, \overline{11}, \overline{7}, \overline{6}\}$であることから，

$$[1]_4 \cdot [9]_4 = \left[\overline{10}\right]_4 + [\overline{4}]_4 + \left[\overline{8}\right]_4 + \left[\overline{13}\right]_4 = -1$$

となる．

4.3 $p = 17$のときの２次のガウス周期

$p = 17$のときの２つの２次のガウス周期の和と積が次のように計算できることがわかった．

$$[1]_2 + [3]_2 = -1 \ , \ [1]_4 \cdot [9]_4 = -4$$

そこで，解と係数の関係から，$[1]_2$と$[3]_2$は

$$x^2 + x - 4 = 0$$

の解であることがわかる．よって，

$$x = \frac{-1 \pm \sqrt{17}}{2}$$

$[1]_2$と$[3]_2$の符号の判定であるが，どちらの解にも虚数が含まれていないので，$[1]_2$は

$$[1]_2 = \zeta^1 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2$$

$$= \cos\frac{2\pi}{17} + \cos\frac{18\pi}{17} + \cos\frac{26\pi}{17} + \cos\frac{30\pi}{17} + \cos\frac{32\pi}{17} + \cos\frac{16\pi}{17} + \cos\frac{8\pi}{17} + \cos\frac{4\pi}{17}$$

$$= 2\cos\frac{2\pi}{17} + 2\cos\frac{16\pi}{17} + 2\cos\frac{8\pi}{17} + 2\cos\frac{4\pi}{17}$$

同様に$[3]_2$は

$$[3]_2 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$$

$$= \cos\frac{6\pi}{17} + \cos\frac{20\pi}{17} + \cos\frac{10\pi}{17} + \cos\frac{22\pi}{17} + \cos\frac{28\pi}{17} + \cos\frac{14\pi}{17} + \cos\frac{24\pi}{17} + \cos\frac{12\pi}{17}$$

$$= 2\cos\frac{6\pi}{17} + 2\cos\frac{14\pi}{17} + 2\cos\frac{10\pi}{17} + 2\cos\frac{12\pi}{17}$$

となることがわかる．和積の公式から

$$\cos\frac{2\pi}{17}+\cos\frac{16\pi}{17}=2\cos\frac{9\pi}{17}\cos\frac{7\pi}{17}$$

$$\cos\frac{14\pi}{17}+\cos\frac{12\pi}{17}=2\cos\frac{13\pi}{17}\cos\frac{\pi}{17}$$

となり，

$$\cos\frac{13\pi}{17}<\cos\frac{9\pi}{17}<0\,,0<\cos\frac{7\pi}{17}<\cos\frac{\pi}{17}$$

であるから，

$$\cos\frac{13\pi}{17}\cos\frac{\pi}{17}<\cos\frac{9\pi}{17}\cos\frac{7\pi}{17}$$

となる．さらに，

$$\cos\frac{10\pi}{17}<\cos\frac{8\pi}{17}\,,\cos\frac{6\pi}{17}<\cos\frac{4\pi}{17}$$

であるから，

$$[3]_2<[1]_2$$

がしめせた．よって，

$$[3]_2=\frac{-1-\sqrt{17}}{2}$$

$$[1]_2=\frac{-1+\sqrt{17}}{2}$$

となる．次の章では一般の２次のガウス周期ついて求めていく．

5. 2次のガウス周期

ここでは，pを奇素数とし，gをpの原始根としたとき，前章で求めた$[1]_2$，$[g]_2$の値を一般のpについて求める．その定理は次のようになる．

5.0 2次のガウス周期の基本定理 1

(1) $p \equiv 1\ (mod\ 4)$のとき，

$$[1]_2 \cdot [g]_2 = -\frac{p-1}{4}$$

が成り立ち，$[1]_2 \cdot [g]_2 = -1$であることを使うことで，$[1]_2$，$[g]_2$は

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

の2解になる．

(2) $p \equiv 3\ (mod\ 4)$のとき，

$$[1]_2 \cdot [g]_2 = \frac{p+1}{4}$$

が成り立ち，$[1]_2 \cdot [g]_2 = -1$であることを使うことで，$[1]_2$，$[g]_2$は

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

5.1 有限体上の2次曲線の点の数

gをpの原始根として4つの方程式

$$1 + x^2 = y^2, \quad 1 + x^2 = gy^2$$
$$1 + gx^2 = y^2, \quad 1 + gx^2 = gy^2$$

を考える．それぞれの式を「$1 = \cdots$」の形にすると，4つの式は(x, y)平面の双曲線になることがわかる．ここでは,これらの曲線を$\mathbb{F}_p$の世界で見ることにする．つまり，

$$\overline{1} + x^2 = y^2, \quad \overline{1} + x^2 = \overline{g}y^2$$
$$\overline{1} + \overline{g}x^2 = y^2, \quad \overline{1} + \overline{g}x^2 = \overline{g}y^2$$

とし，x, yも$\mathbb{F}_p$の元であるとする．$\mathbb{F}_p$にはp個しか元がないので，これらの方程式も有限個しか解を持たない．有限体$\mathbb{F}_p$上でも，これらの方程式を曲線の方程式と考え，方程

式の解(x,y)を$\mathbb{F}_p-$ *有理点*と呼ぶ.

この節では， 上の 4 つの曲線の$\mathbb{F}_p-$ *有理点*の数を数える．この章の最終目標が,$p\equiv 1\,(mod\,4)$と$p\equiv 1\,(mod\,4)$のpについて考えることから,この二つのpの$\mathbb{F}_p-$ *有理点*の数を数えていく．

(I)最初に，$p\equiv 1\,(mod\,4)$とする．まず，$x=\overline{0}$または$y=\overline{0}$となる$\mathbb{F}_p-$ *有理点*を数える．$p\equiv 1\,(mod\,4)$という仮定から，定理 3.6.1 により，-1は平方剰余である．実際に定理の証明の中で,$-\overline{1}=\overline{g}^{\frac{p-1}{2}}=(\overline{g}^{\frac{p-1}{4}})^2$ である．

(i) $\overline{1}+x^2=y^2$に対して，

$$x=\overline{0}\text{のとき，}\ \overline{1}=y^2\text{となるので，}\ y=\pm\overline{1}$$

$$y=\overline{0}\text{のとき，}\ -\overline{1}=x^2\text{となるので，}\ x=\pm\overline{g}^{\frac{p-1}{4}}$$

よって$\overline{1}+x^2=y^2$に対して,$x=\overline{0}$または$y=\overline{0}$となる$\mathbb{F}_p-$ *有理点*は，以下の 4 つになる．

$$(\overline{0}\,,\pm\overline{1}),\ \ (\pm\overline{g}^{\frac{p-1}{4}},\overline{0})$$

(ii) $\overline{1}+x^2=\overline{g}y^2$に対して，

$x=\overline{0}$のとき， $\overline{1}=\overline{g}y^2$という式になる．両辺に$\overline{g}^{-1}$をかけると，

$$\overline{g}^{-1}=y^2$$

と変形できる．

ここで,H_2は乗法で閉じた集合であり，H_2の要素aに対して，逆元a^{-1}もH_2の要素となる．

よって，

$$\overline{g}\in gH_2\Leftrightarrow\overline{g}^{-1}\in gH_2\text{であるから，}$$

$\overline{g}^{-1}$は平方非剰余となるので，$\overline{g}^{-1}=y^2$を満たすyは存在しない．

$y=\overline{0}$のとき,$y=\overline{0}$のとき，$-\overline{1}=x^2$となるので，$x=\pm\overline{g}^{\frac{p-1}{4}}$.

よって,$\overline{1}+x^2=\overline{g}y^2$に対して,$x=\overline{0}$または$y=\overline{0}$となる$\mathbb{F}_p-$ *有理点*は，

$$\left(\pm\overline{g}^{\frac{p-1}{4}},\overline{0}\right)$$

の二つだけとなる．

(iii) $\overline{1}+\overline{g}x^2=y^2$に対して，

$x=\overline{0}$のとき，$\overline{1}=y^2$となるので，$y=\pm\overline{1}$

$y=\overline{0}$のとき，$\overline{1}+\overline{g}x^2=\overline{0}$つまり，$\overline{g}x^2=-\overline{1}$となるので，両辺に$\overline{g}^{-1}$をかけると，

$$x^2=-\overline{1}\cdot\overline{g}^{-1}=\overline{g}^{\frac{p-1}{2}}\cdot\overline{g}^{-1}=\overline{g}^{\frac{p-1}{2}-1}=\overline{g}^{\frac{p-3}{2}}$$

と変形できる．ここで，$\frac{p-3}{2}$は$p=4k+1$であることを考えると奇数であることがわかる．

よって，$\overline{g}^{\frac{p-3}{2}}$は平方非剰余であるので，有理点を持たない．

したがって，$\overline{1}+\overline{g}x^2=y^2$に対して，$x=\overline{0}$または$y=\overline{0}$となる$\mathbb{F}_p-$*有理点*は，

$$(\overline{0},\pm\overline{1})$$

の２つだけである．

(iv) $\overline{1}+\overline{g}x^2=\overline{g}y^2$に対して，(ⅱ)と(ⅲ)より

$x=\overline{0}$のとき，$\overline{1}=\overline{g}y^2$という式になるので，有理点を持たない．

$y=\overline{0}$のとき，$\overline{g}x^2=-\overline{1}$となるので，有理点を持たないことがわかる．

この４つの曲線

$$\overline{1}+x^2=y^2,\qquad \overline{1}+x^2=\overline{g}y^2$$
$$\overline{1}+\overline{g}x^2=y^2,\qquad \overline{1}+\overline{g}x^2=\overline{g}y^2$$

上の，$x\neq\overline{0}$，$y\neq\overline{0}$となる$\mathbb{F}_p-$*有理点*の個数をそれぞれ，

$$\alpha,\qquad \beta,$$
$$\gamma,\qquad \delta$$

とする．上の計算結果から，それぞれの曲線のすべての$\mathbb{F}_p-$*有理点*の個数は

$$\alpha+4,\qquad \beta+2,$$
$$\gamma+2,\qquad \delta$$

となる．

ここからは，$\alpha,\beta,\gamma,\delta$の値を求める．

まずは，$\overline{1}+x^2$を考える．xの解の個数は有限体$\mathbb{F}_p$上であるから，p個であることに注意し，xに$\overline{0}$，$\pm\overline{g}^{\frac{p-1}{4}}$と異なる$p-3$個の元を代入すると，$\overline{1}+x^2$は$\overline{0}$にならないから，$\mathbb{F}_p^{\times}=H_2\cup gH_2$より，$\overline{1}+x^2$は$\overline{1}+x^2\in H_2$か$\overline{1}+x^2\in gH_2$のどちらかである．また，$y^2\in H_2$であり，$\overline{g}y^2\in gH_2$であることから，各$x$に対して，

$$\overline{1}+x^2=y^2\text{と}\overline{1}+x^2=\overline{g}y^2$$

のどちらか一つに解をもち，もう一つの式は解を持たない．よって，

$$\alpha+\beta=2(p-3)$$

が得られる．

同様に，$\overline{1}+\overline{g}x^2$に対しても行う．こちらは，$\overline{1}+\overline{g}x^2=\overline{0}$を満たす$x$は存在しないので，$x$に$\overline{0}$ 以外の$p-1$個の元を代入すると，$\overline{1}+\overline{g}x^2\in H_2$か$\overline{1}+\overline{g}x^2\in gH_2$のどちらかである．また，

$y^2\in H_2$であり，$\overline{g}y^2\in gH_2$であることから，各xに対して，

$$\overline{1}+x^2=y^2 \text{ と } \overline{1}+x^2=\overline{g}y^2$$

のどちらか一つに解をもち，もう一つの式は解を持たない．したがって，

$$\gamma+\ \delta=2(p-1)$$

次に，

$$\overline{1}+x^2=y^2\ \Leftrightarrow\ x^2=y^2-\overline{1}$$

$$\overline{1}+\overline{g}x^2=y^2\Leftrightarrow\ \overline{g}x^2=y^2-\overline{1}$$

と変形し，$y^2-\overline{1}$に対して，同様の手順を踏む．yに$\overline{0}$，$\pm\overline{1}$と異なる$p-3$個の元を代入すると，$y^2-\overline{1}\neq\overline{0}$であるから，$y^2-\overline{1}\in H_2$,$y^2-\overline{1}\in\overline{g}H_2$のどちらかは成り立つ．

したがって，

$$\alpha+\ \gamma=2(p-3)$$

が成り立つ．

また，γ , δについて

$$\gamma=\ \delta$$

が成り立つ．その証明は次のようになる．

まず，$\overline{1}+\overline{g}x^2=\overline{g}y^2$ ，$\overline{1}+\overline{g}x^2=y^2$の$\mathbb{F}_p-$ *有理点*(x,y)で$x\neq\overline{0}$，$y\neq\overline{0}$となる集合をそれぞれS_δ ,S_γとする．S_δ ,S_γの要素の個数がそれぞれ，γ , δとなる．S_δとS_γの要素を，$(x,y)\in S_\delta$，$(x,y)\in S_\gamma$とそれぞれ書くことにする．

$\overline{1}+\overline{g}x^2=\overline{g}y^2$の両辺にそれぞれ，$\overline{g}^{-1}(x^{-1})^2$をかけると，

$$\overline{g}^{-1}(x^{-1})^2+\overline{1}=(x^{-1}y)^2$$

となる．よって，$\overline{g}^{-1}(x^{-1})^2=\overline{g}(\overline{g}^{-1}x^{-1})^2$より，

$$\overline{1}+\overline{g}(\overline{g}^{-1}x^{-1})^2=(x^{-1}y)^2$$

となり，$\left(\overline{g}^{-1}x^{-1},x^{-1}y\right)\in S_\gamma$である．このように，$S_\delta$の元$(x,y)$に対して

$$\phi((x,y))=\ \left(\overline{g}^{-1}x^{-1},x^{-1}y\right)$$

と定義することによって，写像$\phi\colon S_\delta\ \rightarrow\ S_\gamma$ができる．

同様に，$\overline{1}+\overline{g}x^2=y^2$の両辺に$\overline{g}^{-1}(x^{-1})^2$をかけると

$$\overline{g}^{-1}(x^{-1})^2+\overline{1}=\overline{g}^{-1}(x^{-1}y)^2$$

よって，$\overline{g}^{-1}(x^{-1})^2 = \overline{g}(\overline{g}^{-1}x^{-1})^2$より，

$$\overline{1} + \overline{g}(\overline{g}^{-1}x^{-1})^2 = \overline{g}(\overline{g}^{-1}x^{-1}y)^2$$

となり，$\left(\overline{g}^{-1}x^{-1}, \overline{g}^{-1}x^{-1}y\right) \in S_\gamma$である．

$$\psi((x,y)) = \left(\overline{g}^{-1}x^{-1}, \overline{g}^{-1}x^{-1}y\right)$$

と定義すると，ψ： $S_\gamma \to S_\delta$なる写像が得られる． 定義から，

$$\psi(\phi((x,y))) = (x,y)$$

$$\phi(\psi((x,y))) = (x,y)$$

が成り立つので，ψはϕの逆写像であり，ϕは$1:1$は全単射であることがわかる．

よって，

$$\gamma = \delta$$

が得られる．

$$\alpha + \beta = 2(p-3)\ ,\ \gamma + \delta = 2(p-1)$$

$$\alpha + \gamma = 2(p-3)\ ,\quad \gamma = \delta$$

の４つの関係から，

$$\alpha = p-5\ ,\ \beta = \gamma = \delta = p-1$$

が得られる．よって，

$$\overline{1} + x^2 = y^2\ ,\quad \overline{1} + x^2 = \overline{g}y^2$$

$$\overline{1} + \overline{g}x^2 = y^2\ ,\quad \overline{1} + \overline{g}x^2 = \overline{g}y^2$$

の$\mathbb{F}_p -$ *有理点*の個数は，$x = \overline{0}$または$y = \overline{0}$となる$\mathbb{F}_p -$ *有理点*の個数も考慮すると

$$p-1, \qquad p+1,$$

$$p+1, \qquad p-1$$

となる．

(II) $p \equiv 3\ (mod\ 4)$のときでも，同様な証明を与えると，

$$\overline{1} + x^2 = y^2\ ,\quad \overline{1} + x^2 = \overline{g}y^2$$

$$\overline{1} + \overline{g}x^2 = y^2\ ,\quad \overline{1} + \overline{g}x^2 = \overline{g}y^2$$

の$\mathbb{F}_p -$ *有理点*の個数は，

$$p-1, \qquad p+1,$$

$$p+1, \qquad p-1$$

となる．

この結果は，$p \equiv 1\ (mod\ 4)$のときの結果と同じである．

よって，次の定理が得られる．

定理　5.1.1 pを奇素数とする．このとき

$$\overline{1}+x^2=y^2,\qquad \overline{1}+x^2=\overline{g}y^2$$
$$\overline{1}+\overline{g}x^2=y^2,\qquad \overline{1}+\overline{g}x^2=\overline{g}y^2$$

の$\mathbb{F}_p-$ *有理点*の個数は，

$$p-1,\qquad p+1,$$
$$p+1,\qquad p-1$$

である．

5.2　2 次のガウスの基本定理の証明

$[1]_2\cdot[g]_2=-1$であることがわかっていることから，$[1]_2$と$[g]_2$を求めるために必要な値は，$[1]_2\cdot[g]_2$の値である.ここで，積公式により，

$$[1]_2\cdot[g]_2=\sum_{\alpha\in H_2}\left[\overline{1}+\overline{g}\alpha\right]_2$$

となることはすでにわかっている．この値を前節の値を使って証明していく．

$\overline{1}+\overline{g}\alpha\in H_2$となる$\alpha\in H_2$の数を$A$個，$\overline{1}+\overline{g}\alpha\in gH_2$となる$\alpha\in H_2$の数を$B$個，

$\overline{1}+\overline{g}\alpha=\overline{0}$となる$\alpha\in H_2$の数を$C$個とすると，命題 4.1.2 を使うことで，上の式の右辺を$[1]_2,[g]_2,[0]_2$を使って次のように表すことができる．

$$[1]_2\cdot[g]_2=A[1]_2+\boldsymbol{B}[g]_2+C[0]_2 \qquad (5.1)$$

まず，Cの値は，$\overline{1}+\overline{g}\alpha=\overline{0}$は$\overline{g}\alpha=-\overline{1}$と同値である．これは，$-\overline{1}\in gH_2$を意味し，$-\overline{1}$が平方非剰余であることを示している．定理 3.6.1 により，$p\equiv 1\,(mod\,4)$のとき$C=0$であり，$p\equiv 3\,(mod\,4)$のとき$C=1$である．

また，$[0]_2$ は命題 4.1.2 により

$$[0]_2=\frac{p-1}{2}$$

次にAについて考える．A は

$$\{\alpha\in H_2\mid \beta\in H_2\ で\overline{1}+\overline{g}\alpha=\beta\ となるものが存在する\}$$

という集合の元の個数である．補題 3.7.1 によりH_2は$\mathbb{F}_p$の$\overline{0}$でない元の２乗全体だから，上の集合は，

$$\{x^2\mid x\in\mathbb{F}_p^{\times}\ で\overline{1}+\overline{g}x^2=y^2\ となるy\in\mathbb{F}_p^{\times}\ ものが存在する\}$$

と言い換えられる．$\overline{1}+\overline{g}x^2=y^2$の$\mathbb{F}_p-$ *有理点*(x,y)で$x\neq\overline{0},\ y\neq\overline{0}$なるものがあれば，$(\pm x,\ \pm y)$という４つの点もまた$\mathbb{F}_p-$ *有理点*であり，この４つの点のx座標の２乗は同じ

値を与える．つまり，上の式を満たす有理点一つにつき 4 つの有理点を得られるということである.よって，前節の定理 5.1.1 の記号を使えば，

$$\gamma = 4A \quad \therefore\ A = \frac{\gamma}{4}$$

となる．

同様に B は

$$\{x^2 \mid x \in \mathbb{F}_p^{\times} \text{で} \overline{1} + \overline{g}x^2 = \overline{g}y^2 \text{となる} y \in \mathbb{F}_p^{\times} \text{ものが存在する}\}$$

の元の数が B である．$\overline{1} + \overline{g}x^2 = \overline{g}y^2$の$x \neq \overline{0},\ y \neq \overline{0}$なる$\mathbb{F}_p -$ *有理点*(x, y)の数は，上の集合の元の 4 倍なので，前節の定理 5.1.1 の記号を使って，

$$B = \frac{\delta}{4}$$

が得られる．

定理 5.2.1 の結果から，それぞれ以下のことがわかる．

$p \equiv 1\ (mod\ 4)$のとき，$\gamma = \delta = p - 1$であるから，

$$A = B = \frac{p-1}{4}$$

$p \equiv 3\ (mod\ 4)$のとき，$\gamma = \delta = p - 3$であるから

$$A = B = \frac{p-3}{4}$$

よって，これらを式(5.1)に代入すると

$p \equiv 1\ (mod\ 4)$のとき，

$$[1]_2 \cdot [g]_2 = A[1]_2 + \boldsymbol{B}[g]_2 + C[0]_2$$

$$= \frac{p-1}{4}([1]_2 + [g]_2)$$

$$= -\frac{p-1}{4}$$

$p \equiv 3\ (mod\ 4)$のとき，

$$[1]_2 \cdot [g]_2 = A[1]_2 + \boldsymbol{B}[g]_2 + C[0]_2$$

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

$$= \frac{p+1}{4}$$

以上より，この章の初めに書いた以下の定理が示せた．

5.0 2 次のガウス周期の基本定理 1

(1) $p \equiv 1\ (mod\ 4)$のとき，

$$[1]_2 \cdot [g]_2 = -\frac{p-1}{4}$$

が成り立ち，$[1]_2 \cdot [g]_2 = -1$であることを使うことで，$[1]_2$，$[g]_2$は

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

の 2 解になる．

(2) $p \equiv 3\ (mod\ 4)$のとき，

$$[1]_2 \cdot [g]_2 = \frac{p+1}{4}$$

が成り立ち，$[1]_2 \cdot [g]_2 = -1$であることを使うことで，$[1]_2$，$[g]_2$は

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

また，ここで上の定理について一つ注意を述べておく．

(1) $p \equiv 1\ (mod\ 4)$のとき，$[1]_2$，$[g]_2$は$\frac{-1\pm\sqrt{p}}{2}$のどちらかであり，

(2) $p \equiv 1\ (mod\ 4)$のとき，$[1]_2$，$[g]_2$は$\frac{-1\pm i\sqrt{p}}{2}$のどちらかである．

ここで一般のpについて，正確にどちらになるかを決める問題のことを，ガウス和の符号決定問題といい，ここでは結論だけを述べ証明は省くことにする．

(1) $p \equiv 1\ (mod\ 4)$のとき

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

(2) $p \equiv 1\ (mod\ 4)$のとき

$$[1]_2 = \frac{-1+i\sqrt{p}}{2}\ ,[g]_2 = \frac{-1-i\sqrt{p}}{2}$$

である．

実際に，$p = 17$で試してみる．$17 \equiv 1\ (mod\ 4)$であるから，

$$[1]_2 = \frac{-1+\sqrt{17}}{2}, [g]_2 = \frac{-1-\sqrt{17}}{2}$$

となる.

この値は, 4.3 の最後の答えと一致していることがわかる.

6. 正 17 角形の作図

今までの知識を使いながら正 17 角形の作図が可能であることを示していく.
順序として, $p = 17$についての 2 次のガウス周期, 4 次のガウス周期, 8 次のガウス周期という順で求めていく.

6.1 $p = 17$についての 2 次のガウス周期

この値については, 前節でも前々節でも求めているので, 結果だけ確認しておく.

$$[1]_2 = \frac{-1+\sqrt{17}}{2}, [g]_2 = \frac{-1-\sqrt{17}}{2}$$

となる.

6.2 $p = 17$についての 4 次のガウス周期

まず, $p = 17$のときの 4 乗剰余は以下のようになる.

$H_4 = \{\overline{1}, \overline{13}, \overline{16}, \overline{4}\}, 3H_4 = \{\overline{3}, \overline{5}, \overline{14}, \overline{12}\}, 3^2H_4 = \{\overline{9}, \overline{15}, \overline{8}, \overline{2}\}, 3^3H_4 = \{\overline{10}, \overline{11}, \overline{7}, \overline{6}\}$

4 次のガウス周期については 4 章で求めたものを使いながら求めていく.

4.1 の最後の計算結果から

$$[1]_4 + [9]_4 = [1]_2 = [1]_2 = \frac{-1+\sqrt{17}}{2}$$

また, 4.2 の最後の計算結果から

$$[1]_4 \cdot [9]_4 = -1$$

よって, $[1]_4$と$[9]_4$の解は以下の方程式の解であることがわかる.

$$x^2 + \frac{1-\sqrt{17}}{2}x + 1 = 0$$

したがって,

$$x = \frac{-1+\sqrt{17} \pm \sqrt{34-2\sqrt{17}}}{4}$$

となる. 解に虚数部分がないので,

$$[1]_4 = \zeta^1 + \zeta^{13} + \zeta^{16} + \zeta^4$$

$$= \cos\frac{2\pi}{17} + \cos\frac{26\pi}{17} + \cos\frac{32\pi}{17} + \cos\frac{8\pi}{17}$$

$$= 2(\cos\frac{2\pi}{17} + \cos\frac{8\pi}{17})$$

$$[9]_4 = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2$$

$$= \cos\frac{18\pi}{17} + \cos\frac{30\pi}{17} + \cos\frac{16\pi}{17} + \cos\frac{4\pi}{17}$$

$$= 2(\cos\frac{16\pi}{17} + \cos\frac{4\pi}{17})$$

とそれぞれ表せる．ここで，$\cos\frac{4\pi}{17} < cos\frac{2\pi}{17}$ ，$\cos\frac{16\pi}{17} < cos\frac{8\pi}{17}$ であることから，

$$[1]_4 < [9]_4$$

が得られる．よって，

$$[1]_4 = \frac{-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}}}{4}, [9]_4 = \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}}{4}$$

となり，4 次のガウス周期を求めることができた．

また，8 次のガウス周期を求める際に$[3]_4$の値が必要となるので求めておく．

前節と同様に$[3]_4$と$3^2[3]_4$から$[3]_4$を求める．

$$[3]_4 = \sum_{\beta \in H_4} \zeta^{a\beta} = \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12}$$

$$[3^3]_4 = \sum_{\beta \in H_4} \zeta^{a\beta} = \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6$$

となる．$[3]_4 + [10]_4 = [3]_2$であることから，

$$[3]_4 + [10]_4 = \frac{-1 - \sqrt{17}}{2}$$

さらに，積の公式から

$$[3]_4 \cdot [10]_4 = \sum_{\alpha \in H_4} \left[\overline{3}\alpha + \overline{10}\right]_4$$

$$= \left[\overline{13}\right]_4 + \left[\overline{49}\right]_4 + \left[\overline{58}\right]_4 + \left[\overline{22}\right]_4$$

$$= \left[\overline{13}\right]_4 + \left[\overline{15}\right]_4 + \left[\overline{7}\right]_4 + \left[\overline{5}\right]_4$$

$$= \left[\overline{1}\right]_4 + \left[\overline{9}\right]_4 + \left[\overline{10}\right]_4 + \left[\overline{2}\right]_4$$

$$= -1$$

となる．よって，$[3]_4$と$[10]_4$は次の方程式の解になる．

$$x^2+\frac{1+\sqrt{17}}{2}x+1=0$$

よって，その解は

$$x=\frac{-1-\sqrt{17}\pm\sqrt{34+2\sqrt{17}}}{4}$$

となる．$[1]_4$を求めた時と同様に，虚数解がないことから，

$$[3]_4=\zeta^3+\zeta^5+\zeta^{14}+\zeta^{12}$$

$$=\cos\frac{6\pi}{17}+\cos\frac{10\pi}{17}+\cos\frac{28\pi}{17}+\cos\frac{24\pi}{17}$$

$$=2(\cos\frac{6\pi}{17}+\cos\frac{10\pi}{17})$$

$$[3^3]_4=\zeta^{10}+\zeta^{11}+\zeta^7+\zeta^6$$

$$=\cos\frac{20\pi}{17}+\cos\frac{22\pi}{17}+\cos\frac{14\pi}{17}+\cos\frac{12\pi}{17}$$

$$=2(\cos\frac{12\pi}{17}+\cos\frac{14\pi}{17})$$

であることがわかる．よって，

$$[3^3]_4<[3]_4$$

より，

$$[3]_4=\frac{-1-\sqrt{17}+\sqrt{34+2\sqrt{17}}}{4}$$

である．

6.3 $p=17$についての 8 次のガウス周期

8 次のガウス周期を求めていく．$H_8=\{\overline{1},\overline{16}\}$，$3^4H_8=\{\overline{4},\overline{13}\}$より$H_8\cup 3^4H_8=H_4$である．また，$3H_8=\{\overline{3},\overline{14}\}$，$3^5H_8=\{\overline{5},\overline{12}\}$となり，$3H_8\cup 3^5H_8=3H_4$であることに注意して，

$$[\overline{1}]_8+[\overline{4}]_8=[\overline{1}]_4=\frac{-1+\sqrt{17}-\sqrt{34-2\sqrt{17}}}{4}$$

である． 積の公式より

$$[\overline{1}]_8\cdot[\overline{4}]_8=\sum_{\alpha\in H_8}[\overline{1}+\overline{4}\alpha]_8$$

$$= \left[\overline{5}\right]_8 + \left[\overline{65}\right]_8$$
$$= \left[\overline{5}\right]_8 + \left[\overline{14}\right]_8$$
$$= [3]_4$$
$$= \frac{-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}}{4}$$

よって，$[\overline{1}]_8$，$[\overline{4}]_8$は次の方程式の解となる．

$$x^2 - \frac{-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}}}{4}x + \frac{-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}}{4} = 0$$

参考文献

栗原　将人 (2017)「ガウスの数論世界をゆく」，数学書房