Gauss の和を計算してみよう配布資料

これは、アゴラと知の探究講座で営業した配布資料です。講義の画像を見るとき握っておくならこれがお勧めです。下の文は、営業案作成前に書いた受講者募集用の案内です。

Gauss の和を計算してみよう内容案内

1 の n 乗根に符号のようなものをうまいことつけて足したもの、例えば 1 の 5 乗根

$$\zeta_5 = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5},\ \zeta_5^2,\ \zeta_5^3,\ \zeta_5^4$$

に符号 ± 1 をうまくつけて足して出来る $G_5 = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$ などを Gauss の和と言います。「試しにこれを 2 乗してみよう」あたりから始めて、Gauss の和とそれに関連するものをいろいろ計算してうまくいったりいかなかったりな感じを楽しんでみるのも悪くないかも？という少し行き当たりばったりな気配のする企画です。

Gauss の和を計算してみよう

担当：鈴木浩志

2010.8.9-12.

1　複素平面と 1 の n 乗根

案内にも書いた通り、例えば 1 の 5 乗根で 1 以外のもの

$$\zeta_5 = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5},\ \zeta_5^2,\ \zeta_5^3,\ \zeta_5^4$$

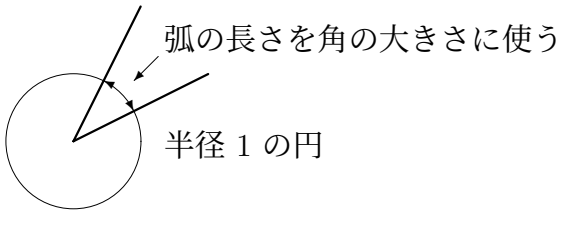
にうまいこと符号をつけて足してできる

$$G_5 = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$$

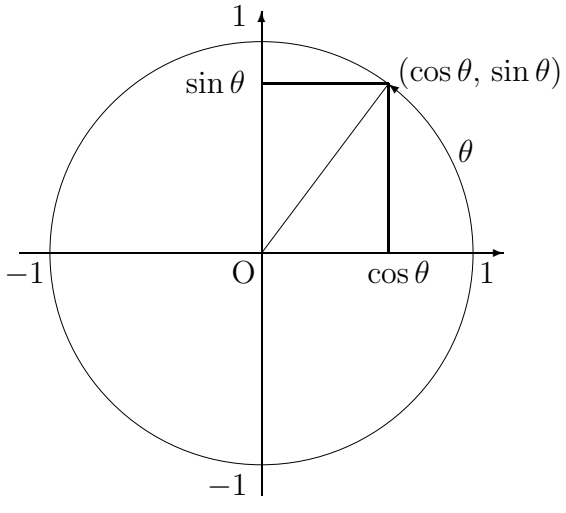
が Gauss の和の具体例で、第 1 話は、この G_5 を 2 乗してみるだけでおしまいの予定ですが、その前に、上に書いてあることを一通り説明するのが今回の主なお題です。安全のため、高校で習ったようなことまで、くどくど書いてあるかもです。

1.1　角の大きさと三角関数

角の大きさを、その角が切り取る半径 1 の円の弧の長さで表す。例えば、90° は $\frac{\pi}{2}$、180° は π と表す。



座標変面に原点を中心とする半径 1 の円を描き、$(1,0)$ から反時計回りに円周上を角の大きさつまり弧の長さで θ だけ回った点の座標を $(\cos\theta, \sin\theta)$ とする。



時計回りに回ったときは負の角と考えるとすべての実数 x に対し $\cos x$, $\sin x$ が定まる。これらと、

$$\tan x = \frac{\sin x}{\cos x},\ \sec x = \frac{1}{\cos x},\ \operatorname{cosec} x = \frac{1}{\sin x},\ \cot x = \frac{\cos x}{\sin x}$$

を三角関数という。(後ろの 4 つについては、分母が 0 になるところ以外で定義される。)

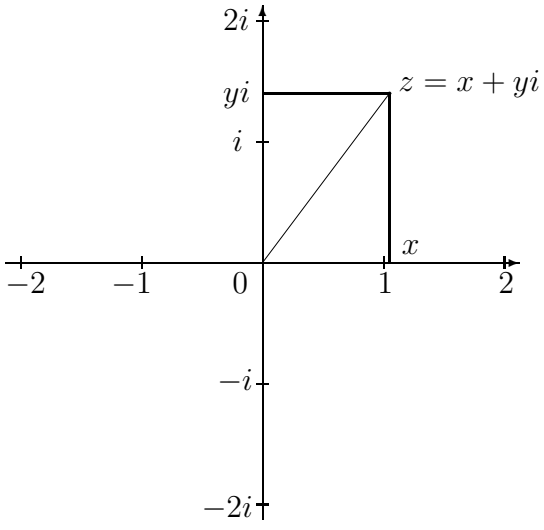
1.2 複素平面と複素数の積

$i^2 = -1$ となる数 i を使って

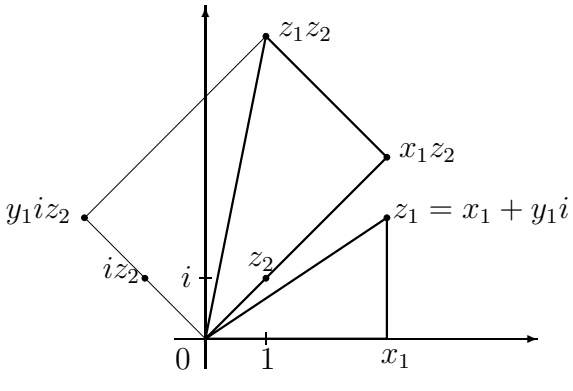
$$z = x + yi \quad (x, y \in \mathbb{R})$$

と表される数 z を複素数といい、複素数全体のなす集合を $\mathbb{C}$ で表す。複素数は、判別式が負の 2 次方程式を解いた時などに現れる。

複素数は、横軸に $1, 2, 3, \ldots$ と目盛りをとり、縦軸に $i, 2i, 3i, \ldots$ と目盛りをとった平面の点として表すことが多い。この平面を、複素平面とか Gauss 平面などと呼ぶ。(少し前の高校の教科書にはあって、複素数平面って書いてあったが、今も書いてあるのかどうかは不明。)



横軸を実軸、縦軸を虚軸といい、$\mathrm{Re}\, z = \Re z = x$ を z の実部、$\mathrm{Im}\, z = \Im z = y$ を z の虚部と呼ぶ。$z_1 = x_1 + y_1 i$, $z_2 = x_2 + y_2 i$ の和 $z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)i$ は、複素平面では、0, z_1, $z_1 + z_2$, z_2 が平行四辺形となる点である。$-z$ は 0 に関して z と対称な点である。$\overline{z} = x - yi$ を z の共役複素数という。これは実軸に関して z と対称な点である。$|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}$ を z の絶対値という。これは 0 からの距離に等しい。$z \neq 0$ について、$z = |z|(\cos\theta + i\sin\theta)$ となる θ を z の偏角といい、$\arg z$ などで表す。偏角は 2π の整数倍のずれを許す。$iz_2 = -y_2 + x_2 i$ は、0 を中心として z_2 を $\dfrac{\pi}{2}$ 回転したものなので、z_1, $z_2 \neq 0$ とすると、三角形 0, $x_1 z_2$, $z_1 z_2$ は、三角形 0, x_1, z_1 を、1 が z_2 に重なるように $|z_2|$ 倍して回転したものである。



よって、複素数を掛けると、絶対値が積に、偏角が和になる。つまり、

$$|z_1 z_2| = |z_1||z_2|, \quad \arg(z_1 z_2) = \arg z_1 + \arg z_2$$

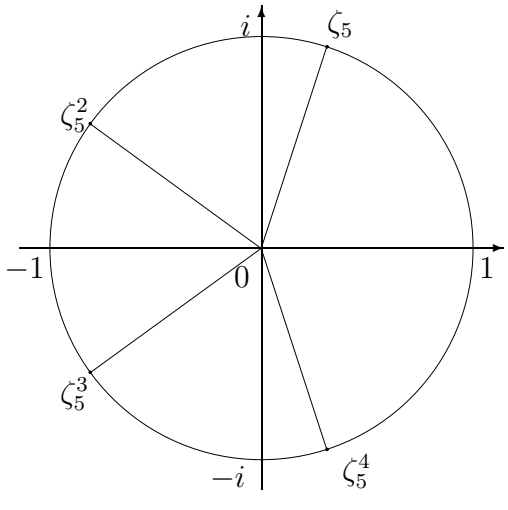
が成り立つ。

1.3 1 の n 乗根

以上で準備が終わったので、最初に戻る。

$$\zeta_5 = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$$

は、絶対値が 1 で、偏角が $\dfrac{2\pi}{5}$ の複素数であるから、$\zeta_5^2, \zeta_5^3, \zeta_5^4$ はどれも絶対値が 1 で、偏角は順に $\dfrac{4\pi}{5}, \dfrac{6\pi}{5}, \dfrac{8\pi}{5}$ である。5 乗すると、どれも絶対値が 1 で偏角が 2π の整数倍の複素数、つまり 1 になるので、これらは 1 の 5 乗根である。1 も入れると、全部で 5 個あるので、1 の 5 乗根、つまり $z^5 = 1$ の解はこれで全部である。



$$z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1)$$

であるから、ζ_5 は $z^4 + z^3 + z^2 + z + 1 = 0$ の解である。よって、

$$\zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = -1$$

が成り立つ。これと、$\zeta_5^5 = 1$ に注意して計算すると、$G_5^2 = 5$ であることがわかる。

ζ_5 と同様に、1 以上の整数 n に対し、

$$\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

とおくと、1 の n 乗根は、

$$1,\ \zeta_n,\ \zeta_n^2,\ \ldots,\ \zeta_n^{n-1}$$

であり、$n \geqq 2$ について、

$$\zeta_n + \zeta_n^2 + \cdots + \zeta_n^{n-1} = -1$$

が成り立つことがわかる。

2　コンパスと定規で正 17 角形を描こう (描かないけど)

前回最後の計算を実際にやってみると、

$$\begin{aligned}
G_5^2 &= (\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4)^2 \\
&= \zeta_5^2 + (-\zeta_5^2)^2 + (-\zeta_5^3)^2 + (\zeta_5^4)^2 \\
&\quad +2\zeta_5(-\zeta_5^2) + 2\zeta_5(-\zeta_5^3) + 2\zeta_5\zeta_5^4 \\
&\quad +2(-\zeta_5^2)(-\zeta_5^3) + 2(-\zeta_5^2)\zeta_5^4 + 2(-\zeta_5^3)\zeta_5^4 \\
&= \zeta_5^2 + \zeta_5^4 + \zeta_5^6 + \zeta_5^8 - 2\zeta_5^3 - 2\zeta_5^4 + 2\zeta_5^5 + 2\zeta_5^5 - 2\zeta_5^6 - 2\zeta_5^7 \\
&= \zeta_5^2 + \zeta_5^4 + \zeta_5 + \zeta_5^3 - 2\zeta_5^3 - 2\zeta_5^4 + 2 + 2 - 2\zeta_5 - 2\zeta_5^2 \\
&= 4 - (\zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4) \\
&= 4 - (-1) = 5
\end{aligned}$$

です。これから G_5 を求めて、正 5 角形を描いてみたり、G_{17} から始めて、正 17 角形を結局描いてみなかったりするのが本日のお題です。

2.1　正 5 角形の作図

$G_5^2 = 5$ であるから、G_5 は $\sqrt{5}$ または $-\sqrt{5}$ のどちらかであるが、複素平面で考えると、$2\cos\dfrac{2\pi}{5} = \zeta_5 + \zeta_5^4$ が正の実数、$2\cos\dfrac{4\pi}{5} = \zeta_5^2 + \zeta_5^3$ が負の実数であることが見て取れるので、$G_5 > 0$ であること、つまり、$G_5 = \sqrt{5}$ であることがわかる。

$$\begin{cases} \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = -1 \\ \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5} \end{cases}$$

を両辺足したり引いたりして 2 で割ると、

$$\begin{aligned}
2\cos\frac{2\pi}{5} &= \zeta_5 + \zeta_5^4 = \frac{\sqrt{5}-1}{2} \\
2\cos\frac{4\pi}{5} &= \zeta_5^2 + \zeta_5^3 = -\frac{\sqrt{5}+1}{2}
\end{aligned}$$

となって、$\cos\dfrac{2\pi}{5} = \dfrac{\sqrt{5}-1}{4}$ であることがわかる。

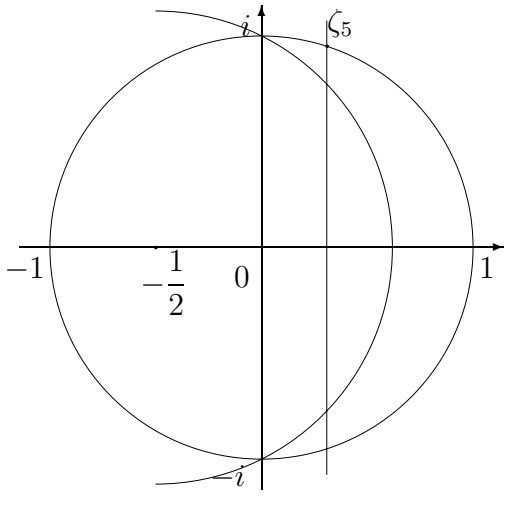
これを使って、コンパスと定規で正 5 角形を描くのであるが、コンパスと定規による作図でやってよいのは、

1. 与えられた (既に描かれた) 2 点を通る直線を引く

2. 与えられた点を中心とする与えられた半径の円を描く

の 2 つの作業である。数学的には、定規はどんなに長い直線でも引けて、コンパスはどんな半径の円もかけることになっているが、直線は延ばせばいくらでも描けはするものの、コンパスの開きの限界より大きな半径の円は描けないので、実際に描くときは若干の工夫が必要になることがある。

コンパスと定規による作図では平面を複素平面と思って計算しながら描くのが普通である。0 と 1 は、もしあれば与えられた点から選ぶのが普通であるが、白紙に正 5 角形を描く時は最初に何も描かれていないので平面上に適当に 0 と 1 を取った状態から始める。まず、0 を中心とする半径 1 の円と、0 と 1 を通る直線を描いて、-1 をとり、-1 と 1 を結ぶ線分の垂直二等分線を引いて、円の上部との交点 i を取る。-1 と 0 の中点 $-\dfrac{1}{2}$ を描く。$-\dfrac{1}{2}$ を中心として、i を通る円は、半径 $\dfrac{\sqrt{5}}{2}$ なので、実軸の正の部分と $\dfrac{\sqrt{5}-1}{2}$ で交わる。この点と 0 を結んだ線分の垂直二等分線は、円の上部と ζ_5 で交わる。残った角 $\dfrac{8\pi}{5}$ を 4 等分すると、$\zeta_5^2, \zeta_5^3, \zeta_5^4$ が描ける。先に描いた垂直二等分線は円の下部と ζ_5^4 で交わるので、4 等分で描いた点と一致すれば成功したことがわかる。



2.2 正 17 角形

奇素数 p について、正 p 角形がコンパスと定規で作図できるのは、$p = 2^{2^n} + 1$ と表されるときで、そのときに限るという定理が Gauss により示されているので正 17 角形や正 257 角形や正 65537 角形がコンパスと定規で作図できる。ここでは、正 17 角形について大まかに説明するので、一度実際に描いてみてほしい。$\bmod 17$ で 0 以外の 16 個を繰り返し 2 乗すると半分の個数に減り続けて 1 のみになる。各段階で消えたものを 1 つずつ覚えておいて、掛けたものを付け足していくと、もとの数が順に再現される。

$$1, 2, 3, 4, 5, 6, 7, 8, -8, -7, -6, -5, -4, -3, -2, -1$$

を 2 乗すると

$$1, 4, -8, -1, 8, 2, -2, -4$$

で 3 などが消えている。さらに 2 乗すると、

$$1, -1, -4, 4$$

で 2 などが消える。さらに 2 乗すると

$$1, -1$$

で 4 が消える。これに、4 を掛けたものを付け足すと、

$$1, -1, 4, -4$$

となり、さらに 2 を掛けたものを付け足すと、

$$1, -1, 4, -4, 2, -2, 8, -8$$

となり、3 を掛けたものを付け足すと、

$$1, -1, 4, -4, 2, -2, 8, -8, 3, -3, 5, -5, 6, -6, 7, -7$$

となる。この並び順を使うと、ζ_{17} のべきの後半の符号を $-$ にして足したものの 2 乗を計算して、半分の長さのものを求めることが繰り返せる。まず

$$G_{17} = \zeta_{17}+\zeta_{17}^{-1}+\zeta_{17}^{4}+\zeta_{17}^{-4}+\zeta_{17}^{2}+\zeta_{17}^{-2}+\zeta_{17}^{8}+\zeta_{17}^{-8}-\zeta_{17}^{3}-\zeta_{17}^{-3}-\zeta_{17}^{5}-\zeta_{17}^{-5}-\zeta_{17}^{6}-\zeta_{17}^{-6}-\zeta_{17}^{7}-\zeta_{17}^{-7}$$

とおくと、$G_{17}^2 = 17$ と $G_{17} > 0$ であることから、$G_{17} = \sqrt{17}$ が確かめられる。よって、

$$\zeta_{17}+\zeta_{17}^{-1}+\zeta_{17}^{4}+\zeta_{17}^{-4}+\zeta_{17}^{2}+\zeta_{17}^{-2}+\zeta_{17}^{8}+\zeta_{17}^{-8}+\zeta_{17}^{3}+\zeta_{17}^{-3}+\zeta_{17}^{5}+\zeta_{17}^{-5}+\zeta_{17}^{6}+\zeta_{17}^{-6}+\zeta_{17}^{7}+\zeta_{17}^{-7} = -1$$

であるから、

$$\zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^{4} + \zeta_{17}^{-4} + \zeta_{17}^{2} + \zeta_{17}^{-2} + \zeta_{17}^{8} + \zeta_{17}^{-8} = \frac{\sqrt{17}-1}{2}$$
$$\zeta_{17}^{3} + \zeta_{17}^{-3} + \zeta_{17}^{5} + \zeta_{17}^{-5} + \zeta_{17}^{6} + \zeta_{17}^{-6} + \zeta_{17}^{7} + \zeta_{17}^{-7} = -\frac{\sqrt{17}+1}{2}$$

である。次に、

$$\alpha = \zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^{4} + \zeta_{17}^{-4} - \zeta_{17}^{2} - \zeta_{17}^{-2} - \zeta_{17}^{8} - \zeta_{17}^{-8}$$
$$\beta = \zeta_{17}^{3} + \zeta_{17}^{-3} + \zeta_{17}^{5} + \zeta_{17}^{-5} - \zeta_{17}^{6} - \zeta_{17}^{-6} - \zeta_{17}^{7} - \zeta_{17}^{-7}$$

とおくと、

$$\begin{aligned}\alpha^2 &= 8 - (\zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^{4} + \zeta_{17}^{-4} + \zeta_{17}^{2} + \zeta_{17}^{-2} + \zeta_{17}^{8} + \zeta_{17}^{-8}) \\ &= 8 - \frac{\sqrt{17}-1}{2} = \frac{17-\sqrt{17}}{2}\end{aligned}$$

であり、β は α の ζ_{17} を ζ_{17}^{3} に取り替えたものなので、

$$\begin{aligned}\beta^2 &= 8 - (\zeta_{17}^{3} + \zeta_{17}^{-3} + \zeta_{17}^{5} + \zeta_{17}^{-5} + \zeta_{17}^{6} + \zeta_{17}^{-6} + \zeta_{17}^{7} + \zeta_{17}^{-7}) \\ &= 8 - \frac{-\sqrt{17}-1}{2} = \frac{17+\sqrt{17}}{2}\end{aligned}$$

である。複素平面で描いてみると、$\alpha > 0, \beta > 0$ が見て取れるので、

$$\alpha = \sqrt{\frac{17-\sqrt{17}}{2}},\ \beta = \sqrt{\frac{17+\sqrt{17}}{2}}$$

であることがわかる。よって、

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

$$\zeta_{17}^{2}+\zeta_{17}^{-2}+\zeta_{17}^{8}+\zeta_{17}^{-8}=\frac{1}{2}\left(\frac{\sqrt{17}-1}{2}-\sqrt{\frac{17-\sqrt{17}}{2}}\right)$$

$$\zeta_{17}^{3}+\zeta_{17}^{-3}+\zeta_{17}^{5}+\zeta_{17}^{-5}=\frac{1}{2}\left(-\frac{\sqrt{17}+1}{2}+\sqrt{\frac{17+\sqrt{17}}{2}}\right)$$

$$\zeta_{17}^{6}+\zeta_{17}^{-6}+\zeta_{17}^{7}+\zeta_{17}^{-7}=\frac{1}{2}\left(-\frac{\sqrt{17}+1}{2}-\sqrt{\frac{17+\sqrt{17}}{2}}\right)$$

である。最後に、$\gamma=\zeta_{17}+\zeta_{17}^{-1}-\zeta_{17}^{4}-\zeta_{17}^{-4}$ とおくと、

$$\begin{aligned}\gamma^2 &= 4+(\zeta_{17}^{2}+\zeta_{17}^{-2}+\zeta_{17}^{8}+\zeta_{17}^{-8})-2(\zeta_{17}^{3}+\zeta_{17}^{-3}+\zeta_{17}^{5}+\zeta_{17}^{-5})\\ &= \frac{17+3\sqrt{17}}{4}-\frac{1}{2}\sqrt{\frac{17-\sqrt{17}}{2}}-\sqrt{\frac{17+\sqrt{17}}{2}}\end{aligned}$$

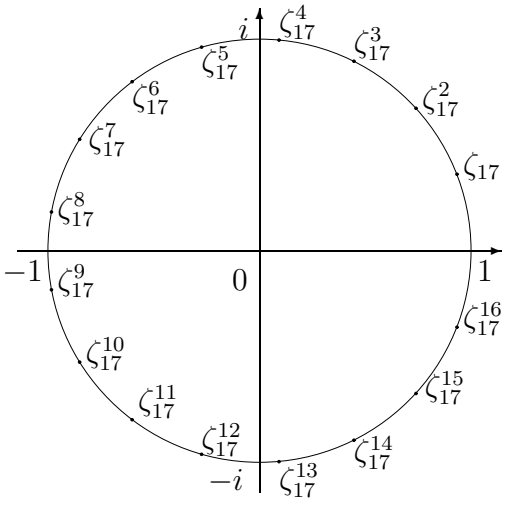
となり、複素平面で描いてみると、$\gamma>0$ が見て取れるので、

$$\gamma=\sqrt{\frac{17+3\sqrt{17}}{4}-\frac{1}{2}\sqrt{\frac{17-\sqrt{17}}{2}}-\sqrt{\frac{17+\sqrt{17}}{2}}}$$

であることがわかる。よって、

$$\begin{aligned}\cos\frac{2\pi}{17} &= \frac{1}{2}(\zeta_{17}+\zeta_{17}^{-1})\\ &= \frac{\sqrt{17}-1}{16}+\frac{1}{8}\sqrt{\frac{17-\sqrt{17}}{2}}+\frac{1}{4}\sqrt{\frac{17+3\sqrt{17}}{4}-\frac{1}{2}\sqrt{\frac{17-\sqrt{17}}{2}}-\sqrt{\frac{17+\sqrt{17}}{2}}}\end{aligned}$$

であることがわかる。以前に述べたように、平行四辺形を使って、複素数の和、相似な三角形を使って、複素数の積が描けるので、平方根さえ描ければ、正 17 角形がコンパスと定規で描けることになる。方法は述べないので、自分で工夫して正 17 角形を描いてみよう。



3　平方剰余と Gauss の和

2 回半つぶしていまだに Gauss の和の定義がでてきていないので、この辺で書いておきます。正 17 角形のとき、既に少し出てきましたが、整数 a, b, c について、$a-b$ が c の倍数のとき $a \equiv b \mod c$ と書き、a と b は $\mod c$ で合同といいます。ここで使うのは c が素数 p のときだけです。

3.1　Gauss の和の定義

奇素数 p が与えられたとき、$\mod p$ で異なる 0 と合同でないもの全体

$$1, 2, 3, \ldots, \frac{p-1}{2}, \frac{p+1}{2}(\equiv -\frac{p-1}{2}), \ldots, p-3(\equiv -3), p-2(\equiv -2), p-1(\equiv -1)$$

を 2 乗すると、$\mod p$ で半分に減る (証明は次節)。ζ_p の指数が $\mod p$ で 2 乗になっているものの係数を $+1$、そうでないものの係数を -1 として加えたものが Gauss の和 G_p である。

$p = 3$ の場合、$\mod 3$ で異なる 0 と合同でないものは、

$$1, 2(\equiv -1)$$

の 2 つで、2 乗すると、$\mod 3$ で 1 のみになる。ζ_3^1 の係数を $+1$、$\zeta_3^2 = \zeta_3^{-1}$ の係数を -1 にして足したものが、

$$G_3 = \zeta_3 - \zeta_3^2$$

である。

$p=5$ のとき、

$$1, 2, 3(\equiv -2), 4(\equiv -1)$$

の 2 乗は、$\bmod 5$ で 1 と 4 である。ζ_5^1 と ζ_5^4 の係数を $+1$、ζ_5^2 と ζ_5^3 の係数を -1 にして足すと、第 1 話に出てきた

$$G_5 = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$$

になる。

$p=7$ のとき、

$$1, 2, 3, 4(\equiv -3), 5(\equiv -2), 6(\equiv -1)$$

を 2 乗すると、$\bmod 7$ で 1, 4, 2 になるので、

$$G_7 = \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6$$

である。同様にして、

$$\begin{aligned} G_{11} &= \zeta_{11} - \zeta_{11}^2 + \zeta_{11}^3 + \zeta_{11}^4 + \zeta_{11}^5 - \zeta_{11}^6 - \zeta_{11}^7 - \zeta_{11}^8 + \zeta_{11}^9 - \zeta_{11}^{10} \\ G_{13} &= \zeta_{13} - \zeta_{13}^2 + \zeta_{13}^3 + \zeta_{13}^4 - \zeta_{13}^5 - \zeta_{13}^6 - \zeta_{13}^7 - \zeta_{13}^8 + \zeta_{13}^9 + \zeta_{13}^{10} - \zeta_{13}^{11} + \zeta_{13}^{12} \end{aligned}$$

である。

3.2 平方剰余

奇素数 p と互いに素な整数 m について、m がある整数の 2 乗と $\bmod p$ で合同なら $\bmod p$ で平方剰余、どんな整数の 2 乗とも $\bmod p$ で合同でないとき、$\bmod p$ で平方非剰余という。平方剰余のとき値が $+1$、平方非剰余のとき値が -1、m が p で割り切れるときは値が 0 という記号、$\left(\dfrac{m}{p}\right)_2$ が定義されていて、平方剰余記号とか Legendre 記号とか呼ばれている。これを使うと、Gauss の和は

$$G_p = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right)_2 \zeta_p^m$$

と表される。

$m_1^2 \equiv m_2^2 \mod p$ となるのは、$m_1^2 - m_2^2 = (m_1 - m_2)(m_1 + m_2)$ が p で割り切れるときで、p が素数なので、$m_1 - m_2$ または $m_1 + m_2$ が p で割り切れるとき、つまり、$m_1 \equiv \pm m_2 \mod p$ のときである。また、p が奇素数なので、$m_2 \equiv -m_2 \mod p$ となるのは m_2 が p で割り切れる場合である。よって、$\mathrm{mod}\, p$ で異なる 0 と合同でない $p-1$ 個の数

$$1, 2, 3, \ldots, p-1$$

は、2 乗すると、$\mathrm{mod}\, p$ で、ちょうど半分に減る。よって、平方剰余なものと平方非剰余なものはどちらも $\dfrac{p-1}{2}$ 個ある。よって、

$$\sum_{m=1}^{p-1} \left(\frac{m}{p}\right)_2 = 0$$

が成り立つ。

$a \not\equiv b \mod p$ つまり、$a-b$ が p で割れないとき、p と互いに素な数 m を掛けても $m(a-b)$ は p で割れない。よって、$ma \not\equiv mb \mod p$ であるから、$\mathrm{mod}\, p$ で異なる 0 と合同でない $p-1$ 個のもの全体に m を掛けると $\mathrm{mod}\, p$ で異なる 0 と合同でない $p-1$ 個のものになるはずである。つまり、m, $2m$, …, $(p-1)m$ の中には、1 から $p-1$ と合同なものが、それぞれひとつずつある。さらに、平方剰余なものに平方剰余なものを掛けると平方剰余なものになるので、平方非剰余なものに平方剰余なものを掛けると平方非剰余でなければならない。さらにこれから、平方非剰余なものに平方非剰余なものを掛けると平方剰余なものになることがわかる。以上はまとめて、整数 m_1, m_2 について、

$$\left(\frac{m_1 m_2}{p}\right)_2 = \left(\frac{m_1}{p}\right)_2 \left(\frac{m_2}{p}\right)_2$$

と表せる。

ここで、G_p の 2 乗を計算してみる。

$$G_p^2 = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right)_2 \zeta_p^m \sum_{\ell=1}^{p-1} \left(\frac{\ell}{p}\right)_2 \zeta_p^\ell$$

であるが、ℓ が $\mathrm{mod}\, p$ で 1 から $p-1$ まで動くとき、$m\ell$ も $\mathrm{mod}\, p$ で 1 から $p-1$ と合同な数を 1 回ずつ動くので、

$$\sum_{\ell=1}^{p-1} \left(\frac{\ell}{p}\right)_2 \zeta_p^\ell = \sum_{\ell=1}^{p-1} \left(\frac{m\ell}{p}\right)_2 \zeta_p^{m\ell}$$

が成り立つ。よって、$\left(\frac{m}{p}\right)_2^2 = 1$ であるから、

$$\begin{aligned} G_p^2 &= \sum_{m=1}^{p-1}\left(\frac{m}{p}\right)_2\zeta_p^m\sum_{\ell=1}^{p-1}\left(\frac{m\ell}{p}\right)_2\zeta_p^{m\ell} = \sum_{m=1}^{p-1}\sum_{\ell=1}^{p-1}\left(\frac{m}{p}\right)_2\left(\frac{m\ell}{p}\right)_2\zeta_p^m\zeta_p^{m\ell} \\ &= \sum_{m=1}^{p-1}\sum_{\ell=1}^{p-1}\left(\frac{m}{p}\right)_2^2\left(\frac{\ell}{p}\right)_2\zeta_p^{m(1+\ell)} = \sum_{m=1}^{p-1}\sum_{\ell=1}^{p-1}\left(\frac{\ell}{p}\right)_2\zeta_p^{m(1+\ell)} \\ &= \sum_{\ell=1}^{p-1}\left(\frac{\ell}{p}\right)_2\sum_{m=1}^{p-1}\zeta_p^{m(1+\ell)} \end{aligned}$$

である。ここで、$\sum_{m=1}^{p-1}\zeta_p^{m(1+\ell)}$ は $\ell = p-1$ なら 1 を $p-1$ 個足して $p-1$、それ以外のときは、$\zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = -1$ に等しいから、

$$G_p^2 = (p-1)\left(\frac{p-1}{p}\right)_2 - \sum_{\ell=1}^{p-2}\left(\frac{\ell}{p}\right)_2$$

ここで、$\sum_{\ell=1}^{p-1}\left(\frac{\ell}{p}\right)_2 = 0$ であったから、$\sum_{\ell=1}^{p-2}\left(\frac{\ell}{p}\right)_2 = -\left(\frac{p-1}{p}\right)_2$ である。よって、$G_p^2 = \left(\frac{p-1}{p}\right)_2 p = \left(\frac{-1}{p}\right)_2 p$ であることがわかる。ここで、$\left(\frac{-1}{p}\right)_2$ を知る必要がある。

3.3 Fermat の小定理と Euler の規準

a, b を整数、p を素数とする。$(a+b)^p$ を展開して出て来る 2 項係数 $\binom{p}{k}$ は、$k = 0, p$ を除き、p で割り切れる。よって、$(a+b)^p \equiv a^p + b^p \mod p$ である。これを使って、n に関する帰納法により、全ての整数 n について、$n^p \equiv n \mod p$ が示される。n が p で割れなければ、$n^{p-1} \equiv 1 \mod p$ がわかる。これらを、Fermat の小定理という。

$x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m \equiv 0 \mod p$ という $\bmod p$ の方程式に整数解 d があれば、$x - d$ で割って余りを計算してみることにより、$(x-d)(x^{m-1} + b_1x^{m-2} + \cdots + b_{m-1}) \equiv 0 \mod p$ と $\bmod p$ で因数分解できることがわかる。p は素数なので、$x \equiv d \mod p$ または、$x^{m-1} + b_1x^{m-2} + \cdots + b_{m-1} \equiv 0 \mod p$ となる。よって、$\bmod p$ での n 次方程式の $\bmod p$ で合同でない解は、n 個以下であることがわかる。

p を奇素数とする。$x^{\frac{p-1}{2}} \equiv 1 \mod p$ という方程式は、Fermat の小定理により、$\mod p$ で異なる平方剰余な $\dfrac{p-1}{2}$ 個の解を持つので、これで全部である。よって、x が平方非剰余の場合、$x^{\frac{p-1}{2}}$ は 1 と合同でない。が、Fermat の小定理により、$(x^{\frac{p-1}{2}})^2 \equiv 1 \mod p$ であるから、$x^{\frac{p-1}{2}} \equiv -1 \mod p$ でなければならない。どちらにしても、$\left(\dfrac{x}{p}\right)_2 \equiv x^{\frac{p-1}{2}} \mod p$ が成り立つ。これを、Euler の規準という。

特に $x = -1$ とおくと、$\left(\dfrac{-1}{p}\right)_2 \equiv (-1)^{\frac{p-1}{2}} \mod p$ であることがわかる。が、どちらも ± 1 なので、両辺は等しいことがわかる。つまり、$\left(\dfrac{-1}{p}\right)_2 = (-1)^{\frac{p-1}{2}}$ である。よって、$G_p^2 = (-1)^{\frac{p-1}{2}} p$ であることがわかる。

4 Gauss の和の値

ここで、高木貞治 著 代数的整数論 岩波書店 に書かれた証明に頼って、Gauss の和の値を求めます。

4.1 Gauss の和の別の表示

$$H = (\zeta_p - \zeta_p^{-1})(\zeta_p^3 - \zeta_p^{-3}) \cdots (\zeta_p^{p-2} - \zeta_p^{-(p-2)})$$

とおく。これが G_p と等しいのであるが、とりあえず、2 乗を求める。

$$\begin{aligned}(-1)^{\frac{p-1}{2}} H &= (\zeta_p^{-1} - \zeta_p)(\zeta_p^{-3} - \zeta_p^3) \cdots (\zeta_p^{-(p-2)} - \zeta_p^{p-2}) \\ &= (\zeta_p^{p-1} - \zeta_p^{-(p-1)})(\zeta_p^{p-3} - \zeta_p^{-(p-3)}) \cdots (\zeta_p^2 - \zeta_p^{-2})\end{aligned}$$

をかけて、

$$\begin{aligned}(-1)^{\frac{p-1}{2}} H^2 &= (\zeta_p - \zeta_p^{-1})(\zeta_p^2 - \zeta_p^{-2}) \cdots (\zeta_p^{p-1} - \zeta_p^{-(p-1)}) \\ &= \zeta_p^{1+2+\cdots+(p-1)}(1 - \zeta_p^{-2})(1 - \zeta_p^{-4}) \cdots (1 - \zeta_p^{-2(p-1)})\end{aligned}$$

である。既に注意した通り、$1, 2, \ldots, p-1$ に p で割れない数 -2 をかけると、$1 \mod p$ から $p-1 \mod p$ まで 1 回ずつ現れるので、

$$(-1)^{\frac{p-1}{2}} H^2 = \zeta_p^{\frac{p(p-1)}{2}}(1 - \zeta_p)(1 - \zeta_p^2) \cdots (1 - \zeta_p^{p-1})$$

である。ここで、$\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ は $x^{p-1} + x^{p-2} + \cdots + 1 = 0$ の解全体であったので、

$$x^{p-1} + x^{p-2} + \cdots + 1 = (x - \zeta_p)(x - \zeta_p^2) \cdots (x - \zeta_p^{p-1})$$

と因数分解できる。$x = 1$ を代入すると、$(-1)^{\frac{p-1}{2}} H^2 = p$ つまり、$H^2 = (-1)^{\frac{p-1}{2}} p = G_p^2$ であることがわかる。したがって、H は G_p または $-G_p$ のいずれかである。

整数係数の式で、ζ_p を代入すると H になるものと G_p になるものに、$t+1$ を代入してできる式の $\dfrac{p-1}{2}$ 次の項の係数を $\mod p$ で比較することにより、$H = G_p$ であることが確かめられる。(時間切れのため、この部分は 5 話以降に話すことにした。)

4.2 Gauss の和の値

$\zeta_p^m = \cos\dfrac{2m\pi}{p} + i\sin\dfrac{2m\pi}{p}$ であるから、

$$G_p = H = (2i)^{\frac{p-1}{2}} \sin\frac{2\pi}{p}\sin\frac{2\cdot 3\pi}{p}\sin\frac{2\cdot 5\pi}{p}\cdots\sin\frac{2(p-2)\pi}{p}$$

である。$p \equiv 1 \mod 4$ の場合、積に出て来る sin のうち、後半の $\dfrac{p-1}{4}$ 個が負の値なので、$G_p > 0$ であることがわかる。よって、この場合、$G_p = \sqrt{p}$ である。$p \equiv 3 \mod 4$ の場合、最初の $\dfrac{p+1}{4}$ 個の sin が正で、後ろの $\dfrac{p-3}{4}$ 個が負の値なので、$G_p = i\sqrt{p}$ であることがわかる。

4.3 関連書籍

高木貞治 著 初等整数論講義 共立出版 に Gauss の行った、複雑な恒等式による Gauss の和の値の決定が書かれている。また、正 17 角形の具体的な作図法も書かれている。

高木貞治 著 近世数学史談 数学雑談 共立出版 の冒頭に Gauss が正 17 角形の作図を発見した時の歴史的な経緯が書かれている。

ここまでが、2010. 8. 9–12. 営業分で、次頁以降が、2010. 10–11. 営業分です。次回が初回の方がいたため、復習が多めに編成されています。

5　前回までのお話 (その 1)

案内にも書いた通り、例えば 1 の 5 乗根で 1 以外のもの

$$\zeta_5 = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5},\ \zeta_5^2,\ \zeta_5^3,\ \zeta_5^4$$

にうまいこと符号をつけて足してできる

$$G_5 = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$$

が Gauss の和の具体例である。まず、ζ_p の説明を行う。

5.1　複素平面と 1 の p 乗根

$i^2 = -1$ となる数 i を使って

$$z = x + yi \quad (x, y \in \mathbb{R})$$

と表される数 z を複素数といい、複素数全体のなす集合を $\mathbb{C}$ で表す。複素数は、横軸に $1, 2, 3, \ldots$ と目盛りをとり、縦軸に $i, 2i, 3i, \ldots$ と目盛りをとった平面の点として表すことが多い。この平面を、複素平面とか Gauss 平面などと呼ぶ。横軸を実軸、縦軸を虚軸といい、$\mathrm{Re}\, z = \Re z = x$ を z の実部、$\mathrm{Im}\, z = \Im z = y$ を z の虚部と呼ぶ。$\overline{z} = x - yi$ を z の共役複素数という。これは実軸に関して z と対称な点である。$|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}$ を z の絶対値という。これは 0 からの距離に等しい。$z \neq 0$ について、$z = |z|(\cos\theta + i\sin\theta)$ となる θ を z の偏角といい、$\arg z$ などで表す。偏角は 2π の整数倍のずれを許す。$z_1 = |z_1|(\cos\theta_1 + i\sin\theta_1)$ と $z_2 = |z_2|(\cos\theta_2 + i\sin\theta_2)$ を掛けると

$$z_1 z_2 = |z_1||z_2|(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2))$$

であることが確かめられるので、複素数を掛けると、絶対値が積に、偏角が和になることがわかる。つまり、

$$|z_1 z_2| = |z_1||z_2|, \quad \arg(z_1 z_2) = \arg z_1 + \arg z_2$$

が成り立つ。

n を 1 以上の整数とする。1 の n 乗根、つまり n 乗すると 1 になる数は、絶対値が 1 で 偏角が $\dfrac{2\pi}{n}$ の整数倍である。よって、

$$\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

とおくと、1 の n 乗根は、

$$1,\ \zeta_n,\ \zeta_n^2,\ \ldots,\ \zeta_n^{n-1}$$

である。$z^n - 1 = (z-1)(z^{n-1} + z^{n-2} + \cdots + z + 1)$ であるから、$n \geqq 2$ の場合、ζ_n は、方程式 $z^{n-1} + z^{n-2} + \cdots + z + 1 = 0$ の解であり、

$$\zeta_n + \zeta_n^2 + \cdots + \zeta_n^{n-1} = -1$$

が成り立つことがわかる。n が素数の場合、この方程式は有理数の範囲でこれ以上因数分解できない。次節でこれを確かめておく。まだ計算してみていない場合、この式を踏まえて、G_5^2 を計算してみるとよい。(p. 6 に答えがある。)

5.2 Eisenstein の定理

有理数の範囲で因数分解できない式を、$\mathbb{Q}$ 上既約であるという。p を素数とする。整数係数の n 次式、

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

の係数 $a_1, \ldots, a_n$ が p の倍数で、a_n が p^2 の倍数でないとき、この式は $\mathbb{Q}$ 上既約である。この定理を Eisenstein の定理という。また、この形の式を Eisenstein 多項式という。

証明は、まず有理数の範囲で因数分解できたと仮定して、整数の範囲で因数分解できることを確かめる。有理数の範囲での因数分解の分母をまとめて、

$$\begin{aligned} & x^n + a_1 x^{n-1} + \cdots + a_n \\ = \ & \frac{1}{b_0 c_0}(b_0 x^m + b_1 x^{m-1} + \cdots + b_m)(c_0 x^{n-m} + c_1 x^{n-m-1} + \cdots + c_{n-m}) \end{aligned}$$

$(1 \leqq m \leqq n-1)$ とする。$b_0, \ldots, b_m, c_0, \ldots, c_{n-m}$ は整数であるが、$b_0 c_0$ の因数で、$b_0, \ldots, b_m$ をすべて割り切るものや、$c_0, \ldots, c_{n-m}$ をすべて割

り切るものがあれば約分しておく。分母をはらうと、

$$\begin{aligned} & b_0c_0(x^n + a_1x^{n-1} + \cdots + a_n) \\ = \ & (b_0x^m + b_1x^{m-1} + \cdots + b_m)(c_0x^{n-m} + c_1x^{n-m-1} + \cdots + c_{n-m}) \end{aligned}$$

は整数の範囲での因数分解である。b_0c_0 を割る素数 q が存在したと仮定する。約分してあるので、$b_0, \ldots, b_m$ の中に、q で割れないものがある。よって、$b_0x^m + b_1x^{m-1} + \cdots + b_m$ は $\bmod q$ で 0 と合同ではない。同様に $c_0x^{n-m} + c_1x^{n-m-1} + \cdots + c_{n-m}$ も $\bmod q$ で 0 と合同ではない。よって、その積は、$\bmod q$ で 0 と合同でない一番次数の小さい項どうしの積が残るので、やはり $\bmod q$ で 0 と合同でない。$b_0c_0(x^n + a_1x^{n-1} + \cdots + a_n)$ は $\bmod q$ で 0 と合同なので、これは矛盾である。よって、分母を割る素数は存在しない、つまり $b_0c_0 = \pm 1$ であることがわかる。必要なら -1 倍して、$b_0 = c_0 = 1$ としておく。
整数の範囲での因数分解であることがわかったので、$\bmod p$ で考える。$b_1, \ldots, b_m, c_1, \ldots, c_{n-m}$ の中に p で割り切れないものがあったとすると、$x^m + b_1x^{m-1} + \cdots + b_m$ と $x^{n-m} + c_1x^{n-m-1} + \cdots + c_{n-m}$ の積の $\bmod p$ で 0 でない一番次数の小さい項は、$x^m + b_1x^{m-1} + \cdots + b_m$ の $\bmod p$ で 0 でない一番次数の小さい項と、$x^{n-m} + c_1x^{n-m-1} + \cdots + c_{n-m}$ の $\bmod p$ で 0 でない一番次数の小さい項の積で、$x^m x^{n-m} = x^n$ より次数が小さくなるので、$a_1, \ldots, a_n$ が p で割り切れることと矛盾する。よって、$b_1, \ldots, b_m, c_1, \ldots, c_{n-m}$ は全て p で割り切れる。すると、$a_n = b_mc_{n-m}$ は p^2 で割り切れることになって矛盾する。よって、このような因数分解は存在せず、$x^n + a_1x^{n-1} + \cdots + a_n$ は $\mathbb{Q}$ 上既約である。

ここで、$g(x) = x^{p-1} + x^{p-2} + \cdots + 1$ について考える。$(t+1)^p \equiv t^p + 1 \mod p$ であるから、

$$g(t+1) = \frac{(t+1)^p - 1}{t} \equiv t^{p-1} \mod p$$

である。さらに $g(1) = p$ なので、$g(t+1)$ は $\mathbb{Q}$ 上既約で、$g(x)$ も $\mathbb{Q}$ 上既約であることがわかる。

有理数係数の式 $f(x)$ を、$f(\zeta_p) = 0$ となるものとする。このような 0 でない式のうちで、次数が最小のものを $h(x)$ とすると、$h(x)$ で $f(x)$ を割った余りは ζ_p を代入すると 0 になるので、$h(x)$ の次数の最小性により 0 となる。特に $f = g$ の場合を考えると、$g(x)$ の既約性により、$g(x)$ は 有理数係数の式で ζ_p を代入すると 0 になるもののうち、次数が最小

のものであることがわかる。さらに、今の議論から、$f(\zeta_p) = 0$ となる有理数係数の式 $f(x)$ は $g(x)$ で割り切れることがわかる。

台風で、順延のためここから後は、2010. 11. 13. に 2 回分続けて営業しました。

6　前々回までのお話 (その２)

整数 a, b, c について、$a-b$ が c の倍数のとき $a \equiv b \mod c$ と書き、a と b は $\mod c$ で合同という。整数係数の式の場合、$f_1(x)-g_1(x)$ の係数がすべて c の倍数のとき $f_1 \equiv f_2 \mod p$ とする。

p を素数とする。整数を $\mod p$ で考えると、異なるものは、$0 \bmod p$, ..., $(p-1) \bmod p$ の p 個である。m を p で割り切れない整数とすると、$m(a-b)$ が p で割り切れるのは $a-b$ が p で割り切れるときなので、$\mod p$ で異なる $0 \bmod p$, ..., $(p-1) \bmod p$ に m を掛けてできる $0 \bmod p$, ..., $m(p-1) \bmod p$ は $\mod p$ で異なる。よって、順序は入れ替わるかもしれないが $0 \bmod p$, ..., $(p-1) \bmod p$ が 1 回ずつ現れることがわかる。

6.1　コンパスと定規による正 17 角形の作図

コンパスと定規による作図でやってよいのは、

1. 与えられた (既に描かれた) 2 点を通る直線を引く
2. 与えられた点を中心とする与えられた半径の円を描く

の 2 つの作業である。複素平面の点 0 と 1 が与えられた状態から始めて、コンパスと定規を使って、作図を行うと考えると、円と直線や、円と円の交点の座標は 2 次方程式を解くことで求められるので、コンパスと定規で作図できるのは、四則演算と 2 次方程式を解くことを繰り返して表せる点だけである。そうなる複素数を根にもつ $\mathbb{Q}$ 上既約な式は、次数が 2 のべきでなければならない。前回の ζ_p を根にもつ式 $g(x)=x^{p-1}+x^{p-2}+\cdots+1$ は $\mathbb{Q}$ 上既約だったので、奇素数 p について、正 p 角形がコンパスと定規で作図できるなら、$p=2^m+1$ と表されるはずである。$m=m'q$ と m が奇素数 q の倍数の場合、$2^m+1=(2^{m'}+1)(2^{m'(q-1)}-2^{m'(q-2)}+\cdots-2^{m'}+1)$ と因数分解できるので p が素数にならない。よって、m は奇素数の因数を持たず、$p=2^{2^n}+1$ と表せる。さらに逆も成り立つ、つまり、奇素数 p について、正 p 角形が、コンパスと定規で作図できるのは、$p=2^{2^n}+1$ と表せるときで、そのときに限るという定理が Gauss により示されている。(この当時の歴史的な話は高木貞治 著 近世数学史談 数学雑談 共立出版 の冒頭に詳しく書かれている。) というわけで、正 17 角形や正 257 角形や正 65537 角形がコンパスと定規で作図できる。ここでは正 17 角形で説明する。

mod 17 で 0 以外の 16 個を並べた

$$1, 2, 3, 4, 5, 6, 7, 8, -8, -7, -6, -5, -4, -3, -2, -1$$

を 2 乗すると

$$1, 4, -8, -1, 8, 2, -2, -4$$

さらに 2 乗すると、

$$1, -1, -4, 4$$

さらに 2 乗すると

$$1, -1$$

である。各段階で消えた数を下から順に、1 つずつ 4, 2, 3 などと選んで、掛けたものを後ろに付け足していくと、もとの列を並べ替えたものが出来る。4 を掛けたものを付け足すと、

$$1, -1, 4, -4$$

さらに 2 を掛けたものを付け足すと、

$$1, -1, 4, -4, 2, -2, 8, -8$$

さらに、3 を掛けたものを付け足すと、

$$1, -1, 4, -4, 2, -2, 8, -8, 3, -3, 5, -5, 6, -6, 7, -7$$

となる。この並び順を ζ_{17} の指数に使って、後ろ半分符号を変えて足したものを

$$G_{17} = \zeta_{17}+\zeta_{17}^{-1}+\zeta_{17}^{4}+\zeta_{17}^{-4}+\zeta_{17}^{2}+\zeta_{17}^{-2}+\zeta_{17}^{8}+\zeta_{17}^{-8}-\zeta_{17}^{3}-\zeta_{17}^{-3}-\zeta_{17}^{5}-\zeta_{17}^{-5}-\zeta_{17}^{6}-\zeta_{17}^{-6}-\zeta_{17}^{7}-\zeta_{17}^{-7}$$

とおくと、$G_{17}^2 = 17$ と $G_{17} > 0$ であることから、$G_{17} = \sqrt{17}$ が確かめられる。これと、

$$\zeta_{17}+\zeta_{17}^{-1}+\zeta_{17}^{4}+\zeta_{17}^{-4}+\zeta_{17}^{2}+\zeta_{17}^{-2}+\zeta_{17}^{8}+\zeta_{17}^{-8}+\zeta_{17}^{3}+\zeta_{17}^{-3}+\zeta_{17}^{5}+\zeta_{17}^{-5}+\zeta_{17}^{6}+\zeta_{17}^{-6}+\zeta_{17}^{7}+\zeta_{17}^{-7} = -1$$

から、

$$\zeta_{17} + \zeta_{17}^{-1} + \zeta_{17}^{4} + \zeta_{17}^{-4} + \zeta_{17}^{2} + \zeta_{17}^{-2} + \zeta_{17}^{8} + \zeta_{17}^{-8},$$
$$\zeta_{17}^{3} + \zeta_{17}^{-3} + \zeta_{17}^{5} + \zeta_{17}^{-5} + \zeta_{17}^{6} + \zeta_{17}^{-6} + \zeta_{17}^{7} + \zeta_{17}^{-7}$$

が求められる。次に、

$$\zeta_{17}+\zeta_{17}^{-1}+\zeta_{17}^{4}+\zeta_{17}^{-4}-\zeta_{17}^{2}-\zeta_{17}^{-2}-\zeta_{17}^{8}-\zeta_{17}^{-8},$$
$$\zeta_{17}^{3}+\zeta_{17}^{-3}+\zeta_{17}^{5}+\zeta_{17}^{-5}-\zeta_{17}^{6}-\zeta_{17}^{-6}-\zeta_{17}^{7}-\zeta_{17}^{-7}$$

を 2 乗したものは、どちらも上の 2 つで表せて、複素平面で描いてみると、どちらも正の実数であることがわかるので、

$$\zeta_{17}+\zeta_{17}^{-1}+\zeta_{17}^{4}+\zeta_{17}^{-4},$$
$$\zeta_{17}^{2}+\zeta_{17}^{-2}+\zeta_{17}^{8}+\zeta_{17}^{-8},$$
$$\zeta_{17}^{3}+\zeta_{17}^{-3}+\zeta_{17}^{5}+\zeta_{17}^{-5},$$
$$\zeta_{17}^{6}+\zeta_{17}^{-6}+\zeta_{17}^{7}+\zeta_{17}^{-7}$$

が求められる。最後に、$\zeta_{17}+\zeta_{17}^{-1}-\zeta_{17}^{4}-\zeta_{17}^{-4}$ の 2 乗は、上の 4 つで表せて、複素平面で描いてみると、正の実数であることが見て取れるので、$2\cos\dfrac{2\pi}{17}=\zeta_{17}+\zeta_{17}^{-1}$ が求められる。実際には、

$$\begin{aligned}\cos\frac{2\pi}{17} &= \frac{1}{2}(\zeta_{17}+\zeta_{17}^{-1})\\ &= \frac{\sqrt{17}-1}{16}+\frac{1}{8}\sqrt{\frac{17-\sqrt{17}}{2}}+\frac{1}{4}\sqrt{\frac{17+3\sqrt{17}}{4}-\frac{1}{2}\sqrt{\frac{17-\sqrt{17}}{2}}-\sqrt{\frac{17+\sqrt{17}}{2}}}\end{aligned}$$

である。複素平面に 0 と 1 と 実数が与えられたとき、その実数の平方根さえコンパスと定規で描ければ、正 17 角形がコンパスと定規で描けることがわかる。方法は述べないので、自分で工夫して正 17 角形を描いてみてほしい。

6.2 Gauss の和と平方剰余記号

p を奇素数とする。$x^2\equiv a^2 \mod p$ となるのは、$(x-a)(x+a)$ が p で割り切れるとき、つまり $x-a$ または $x+a$ が p で割り切れるときなので、$x\equiv\pm a \mod p$ である。よって、$\bmod p$ で異なる 0 と合同でないもの全体

$$1,2,3,\ldots,\frac{p-1}{2},\frac{p+1}{2}(\equiv-\frac{p-1}{2}),\ldots,p-3(\equiv-3),p-2(\equiv-2),p-1(\equiv-1)$$

を 2 乗すると、$a \mod p$ と $-a \mod p$ が $a^2 \mod p$ になるので $\bmod p$ でちょうど半分に減る。ζ_p の指数が $\bmod p$ で 2 乗になっているものの係

数を $+1$、そうでないものの係数を -1 として加えたものが Gauss の和 G_p である。

例えば $p=7$ のとき、

$$1, 2, 3, 4(\equiv -3), 5(\equiv -2), 6(\equiv -1)$$

を 2 乗すると、$\bmod 7$ で 1, 4, 2 になるので、

$$G_7 = \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6$$

である。

この係数を表す記号がある。奇素数 p と互いに素な整数 m について、m がある整数の 2 乗と $\bmod p$ で合同なら $\bmod p$ で平方剰余、どんな整数の 2 乗とも $\bmod p$ で合同でないとき、$\bmod p$ で平方非剰余という。平方剰余のとき値が $+1$、平方非剰余のとき値が -1、m が p で割り切れるときは値が 0 という記号、$\left(\dfrac{m}{p}\right)_2$ を平方剰余記号とか Legendre 記号とか呼ぶ。(右下の 2 は、書いてないことの方が多いが、夏の営業で分数と見間違えた方がいたようなので、いちいち書くことにした。) 例えば、

$$\left(\frac{1}{7}\right)_2 = \left(\frac{2}{7}\right)_2 = \left(\frac{4}{7}\right)_2 = 1, \quad \left(\frac{3}{7}\right)_2 = \left(\frac{5}{7}\right)_2 = \left(\frac{6}{7}\right)_2 = -1, \quad \left(\frac{0}{7}\right)_2 = 0$$

である。これを使うと、Gauss の和は

$$G_p = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right)_2 \zeta_p^m$$

と表される。

6.3 Fermat の小定理と Euler の規準

a, b を整数、p を素数とする。$(a+b)^p$ を展開して出て来る 2 項係数 $\binom{p}{k}$ は、$k=0, p$ を除き、p で割り切れる。よって、$(a+b)^p \equiv a^p + b^p \bmod p$ である。これを使って、n に関する帰納法により、全ての整数 n について、$n^p \equiv n \mod p$ が示される。n が p で割れなければ、$n^{p-1} \equiv 1 \bmod p$ がわかる。これらを、Fermat の小定理という。

$x^m + a_1 x^{m-1} + \cdots + a_{m-1}x + a_m \equiv 0 \mod p$ という $\bmod p$ の方程式に整数解 d があれば、$x-d$ で割って余りを計算してみることにより、

$(x-d)(x^{m-1}+b_1x^{m-2}+\cdots+b_{m-1}) \equiv 0 \mod p$ と $\mod p$ で因数分解できることがわかる。p は素数なので、$x \equiv d \mod p$ または、$x^{m-1}+b_1x^{m-2}+\cdots+b_{m-1} \equiv 0 \mod p$ となる。よって、$\mod p$ での n 次方程式の $\mod p$ で合同でない解は、n 個以下であることがわかる。

p を奇素数とする。Fermat の小定理により、$x^{\frac{p-1}{2}} \equiv 1 \mod p$ という方程式と、$x^{\frac{p-1}{2}} \equiv -1 \mod p$ という方程式は、$\mod p$ で異なる解を $\dfrac{p-1}{2}$ 個ずつ持つ。平方剰余は、$x^{\frac{p-1}{2}} \equiv 1 \mod p$ の解であるが個数が等しいので解全体になる。平方非剰余は、$x^{\frac{p-1}{2}} \equiv -1 \mod p$ の解全体と一致するはずである。どちらにしても、$\left(\dfrac{x}{p}\right)_2 \equiv x^{\frac{p-1}{2}} \mod p$ が成り立つ。これを、Euler の規準という。これを使うと、

$$\left(\frac{m_1m_2}{p}\right)_2 \equiv \left(\frac{m_1}{p}\right)_2\left(\frac{m_2}{p}\right)_2 \mod p$$

であることがわかるが、p が奇素数で、値が ±1 なので

$$\left(\frac{m_1m_2}{p}\right)_2 = \left(\frac{m_1}{p}\right)_2\left(\frac{m_2}{p}\right)_2$$

である。また、$x=-1$ とおくと、$\left(\dfrac{-1}{p}\right)_2 \equiv (-1)^{\frac{p-1}{2}} \mod p$ であることがわかる。やはりどちらも ±1 なので、両辺は等しいことがわかる。つまり、$\left(\dfrac{-1}{p}\right)_2 = (-1)^{\frac{p-1}{2}}$ である。

また、1 と -1 が $\dfrac{p-1}{2}$ 個ずつであることから、全部足すと 0 つまり、

$$\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)_2 = 0$$

であることもわかる。

7 Gauss の和の値

ここで、高木貞治 著 代数的整数論 岩波書店 に書かれた証明に頼って、Gauss の和の値を求める。(難しい恒等式を使った Gauss のもとの証明は、高木貞治 著 初等整数論講義 共立出版に書かれている。)

$$H = (\zeta_p - \zeta_p^{-1})(\zeta_p^3 - \zeta_p^{-3}) \cdots (\zeta_p^{p-2} - \zeta_p^{-(p-2)})$$

とおく。これが G_p と等しいのであるが、とりあえず、2 乗を比べ、その後で符号を調べる。

7.1 G_p^2 と H^2

まず、G_p の 2 乗を計算してみる。

$$G_p^2 = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right)_2 \zeta_p^m \sum_{\ell=1}^{p-1} \left(\frac{\ell}{p}\right)_2 \zeta_p^\ell$$

であるが、ℓ が 1 から $p-1$ まで動くとき、p で割れない数 m を掛けた $m\ell$ も $\bmod p$ で 1 から $p-1$ と合同な数を 1 回ずつ動くので、

$$\sum_{\ell=1}^{p-1} \left(\frac{\ell}{p}\right)_2 \zeta_p^\ell = \sum_{\ell=1}^{p-1} \left(\frac{m\ell}{p}\right)_2 \zeta_p^{m\ell}$$

が成り立つ。よって、$\left(\frac{m}{p}\right)_2^2 = 1$ であるから、

$$\begin{aligned} G_p^2 &= \sum_{m=1}^{p-1} \left(\frac{m}{p}\right)_2 \zeta_p^m \sum_{\ell=1}^{p-1} \left(\frac{m\ell}{p}\right)_2 \zeta_p^{m\ell} = \sum_{m=1}^{p-1}\sum_{\ell=1}^{p-1} \left(\frac{m}{p}\right)_2 \left(\frac{m\ell}{p}\right)_2 \zeta_p^m \zeta_p^{m\ell} \\ &= \sum_{m=1}^{p-1}\sum_{\ell=1}^{p-1} \left(\frac{m}{p}\right)_2^2 \left(\frac{\ell}{p}\right)_2 \zeta_p^{m(1+\ell)} = \sum_{m=1}^{p-1}\sum_{\ell=1}^{p-1} \left(\frac{\ell}{p}\right)_2 \zeta_p^{m(1+\ell)} \\ &= \sum_{\ell=1}^{p-1} \left(\frac{\ell}{p}\right)_2 \sum_{m=1}^{p-1} \zeta_p^{m(1+\ell)} \end{aligned}$$

である。ここで、$\sum_{m=1}^{p-1}\zeta_p^{m(1+\ell)}$ は $\ell=p-1$ なら 1 を $p-1$ 個足して $p-1$、それ以外のときは、$\zeta_p+\zeta_p^2+\cdots+\zeta_p^{p-1}=-1$ に等しいから、

$$G_p^2=(p-1)\left(\frac{p-1}{p}\right)_2-\sum_{\ell=1}^{p-2}\left(\frac{\ell}{p}\right)_2$$

ここで、$\sum_{\ell=1}^{p-1}\left(\frac{\ell}{p}\right)_2=0$ であったから、$\sum_{\ell=1}^{p-2}\left(\frac{\ell}{p}\right)_2=-\left(\frac{p-1}{p}\right)_2$ である。よって、$G_p^2=\left(\frac{p-1}{p}\right)_2 p=\left(\frac{-1}{p}\right)_2 p=(-1)^{\frac{p-1}{2}}p$ であることがわかる。

次に、H の 2 乗を計算する。H に

$$\begin{aligned}(-1)^{\frac{p-1}{2}}H &= (\zeta_p^{-1}-\zeta_p)(\zeta_p^{-3}-\zeta_p^{3})\cdots(\zeta_p^{-(p-2)}-\zeta_p^{p-2})\\ &= (\zeta_p^{p-1}-\zeta_p^{-(p-1)})(\zeta_p^{p-3}-\zeta_p^{-(p-3)})\cdots(\zeta_p^{2}-\zeta_p^{-2})\end{aligned}$$

を掛けると、

$$\begin{aligned}(-1)^{\frac{p-1}{2}}H^2 &= (\zeta_p-\zeta_p^{-1})(\zeta_p^{2}-\zeta_p^{-2})\cdots(\zeta_p^{p-1}-\zeta_p^{-(p-1)})\\ &= \zeta_p^{1+2+\cdots+(p-1)}(1-\zeta_p^{-2})(1-\zeta_p^{-4})\cdots(1-\zeta_p^{-2(p-1)})\end{aligned}$$

である。既に注意したとおり、1, 2, …, $p-1$ に p で割れない数 -2 を掛けると、$1 \bmod p$ から $(p-1) \bmod p$ まで 1 回ずつ現れるので、

$$(-1)^{\frac{p-1}{2}}H^2=\zeta_p^{\frac{p(p-1)}{2}}(1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1})$$

である。ここで、ζ_p, ζ_p^2, …, ζ_p^{p-1} は $x^{p-1}+x^{p-2}+\cdots+1=0$ の解全体であったので、

$$x^{p-1}+x^{p-2}+\cdots+1=(x-\zeta_p)(x-\zeta_p^2)\cdots(x-\zeta_p^{p-1})$$

と因数分解できる。$x=1$ を代入すると、$(-1)^{\frac{p-1}{2}}H^2=p$ つまり、$H^2=(-1)^{\frac{p-1}{2}}p=G_p^2$ であることがわかる。したがって、H は G_p または $-G_p$ のいずれかである。

7.2 符号の比較

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

とおく。$(t+1)^p \equiv t^p + 1 \mod p$ であったので、

$$g(t+1) = \frac{(t+1)^p - 1}{t} \equiv t^{p-1} \mod p$$

である。このとき、整数係数の式 $f(x)$ に対し、$\varphi(f)$ を $f(t+1) \bmod p$ の $p-2$ 次以下の部分とする。整数係数の 2 つの式 $f_1(x)$ と $f_2(x)$ について、作り方から、$\varphi(f_1+f_2) = \varphi(f_1)+\varphi(f_2)$ が成り立つ。$\varphi(f_1 f_2)$ は $\varphi(f_1)\varphi(f_2)$ の $p-2$ 次以下の部分である。また、$f_1(x)$, $f_2(x)$ が $f_1(\zeta_p) = f_2(\zeta_p)$ をみたせば、$f_1(x) - f_2(x)$ は $g(x) = x^{p-1} + x^{p-2} + \cdots + 1$ で割り切れるので、$f_1(t+1) - f_2(t+1) \mod p$ は t^{p-1} で割り切れて、$p-2$ 次以下の部分は 0 である。つまり、$f_1(\zeta_p) = f_2(\zeta_p)$ なら、$\varphi(f_1) = \varphi(f_2)$ となることがわかる。

そこで、H を与える式と、G_p を与える式の φ での値を比べて $H = G_p$ であることを確かめる。

まず H の方を調べる。

$$f_1(x) = (x - x^{p-1})(x^3 - x^{p-3}) \cdots (x^{p-2} - x^2)$$

とおくと、$f_1(\zeta_p) = H$ である。

$$f_1(t+1) = ((t+1) - (t+1)^{p-1})((t+1)^3 - (t+1)^{p-3}) \cdots ((t+1)^{p-2} - (t+1)^2)$$

の 各因数は t で割れるので、$\dfrac{p-3}{2}$ 次以下の項は 0 である。$\dfrac{p-1}{2}$ 次の項の係数を a とおくと、a は因数の 1 次の項の係数を掛けたものになる。よって、

$$\begin{aligned}
(\frac{p-1}{2})! \cdot a &\equiv (\frac{p-1}{2})! \cdot 2 \cdot 6 \cdots (2p-4) \\
&\equiv (\frac{p-1}{2})! \cdot 2^{\frac{p-1}{2}} \cdot 1 \cdot 3 \cdots (p-2) \\
&\equiv 2 \cdot 4 \cdots (p-1) \cdot 1 \cdot 3 \cdots (p-2) \\
&\equiv (p-1)! \mod p
\end{aligned}$$

である。Fermat の小定理から、

$$x^{p-1} - 1 \equiv (x-1)(x-2) \cdots (x-(p-1)) \mod p$$

と $\bmod p$ で因数分解できることがわかる。$x = 0$ とおくと、$(p-1)! \equiv -1 \mod p$ がわかる。

次に G_p の方を調べる。

$$f_2(x) = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right)_2 x^m$$

とおくと、$f_2(\zeta_p) = G_p$ である。Euler の規準により、$\left(\frac{m}{p}\right)_2 \equiv m^{\frac{p-1}{2}} \mod p$ であったから、

$$f_3(x) = \sum_{m=1}^{p-1} m^{\frac{p-1}{2}} x^m$$

とおくと、$\varphi(f_2) = \varphi(f_3)$ である。$\varphi(f_3)$ の $\frac{p-1}{2}$ 次の項の係数を $b \bmod p$ とする。これは、$f_3(t+1) = \sum_{m=1}^{p-1} m^{\frac{p-1}{2}}(t+1)^m$ の $\frac{p-1}{2}$ 次の項の係数を $\bmod p$ で見たものなので、展開すれば、

$$(\frac{p-1}{2})! \cdot b \equiv \sum_{m=1}^{p-1} m^{\frac{p-1}{2}} m(m-1)\cdots(m-\frac{p-1}{2}+1) \mod p$$

である。(最初の $\frac{p-3}{2}$ 個は 0 であるが、計算を容易にするため加えられている。) これを展開して、m のべきの和で表して、$1 \leqq n \leqq p-2$ のとき、$\sum_{m=1}^{p-1} m^n \equiv 0 \mod p$ であること (次節で確かめる) と、$\sum_{m=1}^{p-1} m^{p-1} \equiv p-1 \equiv -1 \mod p$ であることに注意すると、$(\frac{p-1}{2})! \cdot b \equiv -1 \mod p$ であることがわかる。よって、$\varphi(f_1) = \varphi(-f_3)$ は起こりえないので、$H = G_p$ であることがわかる。

7.3 n 乗の和の $\bmod p$ での値

$1 \leqq n \leqq p-2$ とし、$\sum_{m=1}^{p-1} m^n \equiv 0 \mod p$ を示す。

$$a_m = (m+1)m(m-1)\cdots(m-n+1)$$

とおくと、

$$a_{m-1} = m(m-1)\cdots(m-n+1)(m-n)$$

なので、

$$a_m - a_{m-1} = (n+1)m(m-1)\cdots(m-n+1)$$

である。これを、$m = 1, \ldots, p-1$ で足すと

$$\begin{aligned} & (n+1)\sum_{m=1}^{p-1} m(m-1)\cdots(m-n+1) \\ = \;& a_{p-1} - a_0 \\ = \;& p(p-1)\cdots(p-n+1) - 1\cdot 0\cdots(-n+1) \equiv 0 \mod p \end{aligned}$$

となる。$n+1$ は p で割り切れないので、$\sum_{m=1}^{p-1} m(m-1)\cdots(m-n+1) \equiv 0 \mod p$ である。展開して、$n = 1$ から順に並べると、

$$\begin{aligned} &\sum_{m=1}^{p-1} m \equiv 0 \mod p \\ &\sum_{m=1}^{p-1} m^2 - \sum_{m=1}^{p-1} m \equiv 0 \mod p \\ &\cdots \\ &\sum_{m=1}^{p-1} m^{p-2} - \cdots \equiv 0 \mod p \end{aligned}$$

なので、n に関する帰納法により、$\sum_{m=1}^{p-1} m^n \equiv 0 \mod p$ がわかる。

7.4 Gauss の和の値

$\zeta_p^m = \cos\dfrac{2m\pi}{p} + i\sin\dfrac{2m\pi}{p}$ であるから、

$$G_p = H = (2i)^{\frac{p-1}{2}} \sin\frac{2\pi}{p}\sin\frac{2\cdot 3\pi}{p}\sin\frac{2\cdot 5\pi}{p}\cdots\sin\frac{2(p-2)\pi}{p}$$

である。$p \equiv 1 \mod 4$ の場合、積に出て来る sin のうち、後半の $\dfrac{p-1}{4}$ 個が負の値なので、$G_p > 0$ であることがわかる。よって、この場合、$G_p = \sqrt{p}$ である。$p \equiv 3 \mod 4$ の場合、最初の $\dfrac{p+1}{4}$ 個の sin が正で、後ろの $\dfrac{p-3}{4}$ 個が負の値なので、$G_p = i\sqrt{p}$ であることがわかる。

8　その他

8.1　その後の発展

平方剰余記号の代わりに、$\left(\frac{\text{-}}{n}\right)$ を使って作る一般の Gauss の和があって、$n = 3, 4$ の場合、sin の代わりに Weierstrass の $\wp$ 関数を使って表せ、$n = 4$ の場合は、Gauss の和の値がきれいに書けるという論文 (Matthews, C.R., Gauss sums and elliptic functions I. The Kummer sum, Invent. math. 52(1979), 163–185 と Matthews, C.R., Gauss sums and elliptic functions: II. The Quartic sum, Invent. math. 54(1979), 23–52) があります。

8.2　知の探究講座用課題

1.

1. 与えられた (既に描かれた) 2 点を通る直線を引く
2. 与えられた点を中心とする与えられた半径の円を描く

の 2 つの作業を繰り返し、コンパスと定規を使って、正 17 角形を描いてみよう。
2. 手順に沿って、自分で $\cos\dfrac{2\pi}{17}$ を計算し、この資料に書かれた値が正しいかどうか確かめてみよう。
3. 定規の届く距離より少し離れた 2 点間を通る直線や、与えられた点を中心としてコンパスの届く距離より少し離れた点を通る円とこの直線との交点を手持ちのコンパスと定規で描く方法を考えてから、実際に実行してみよう。(余り離れると誤差が大きくなるので「少し」は 3 倍くらいでやってみると良い。)
4. 平方剰余記号には平方剰余の相互法則と呼ばれる平方剰余記号をすばやく計算するのに便利な、奇素数 p, q について

$$\left(\frac{p}{q}\right)_2\left(\frac{q}{p}\right)_2 = \cdots$$

の形の公式と、2 つの補充法則 (第 1 補充法則は、前に出てきた $\left(\dfrac{-1}{p}\right)_2 = (-1)^{\frac{p-1}{2}}$) がある。証明や使い方を調べたり、試しに使ったりしてみよう。

8.3　謝辞

夏の営業にご参加の、広島市立美鈴が丘高校の才野瀬一郎 先生から、感想と作図に関する自作のまとめを書いた丁寧なお手紙をいただきました。ありがとうございます。