# 円周上の格子点

高校 2 年 4 組 54 番　吉田 雄紀

## 1　はじめに

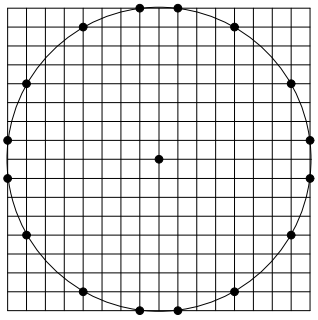
こんにちは。本日は、はるばる新校舎 3 階の数学研究部までお越しくださいまして、ありがとうございます。

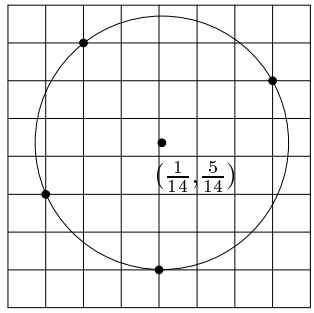
いきなりですが、$x$-$y$ 平面上の原点を中心とする、半径 $\sqrt{65}$ の円を描くと、下の左図のようになります。

この時、この円上にある格子点 ($x$ 座標も $y$ 座標も整数であるような点) は、図のように 16 個あります。

また、原点ではなく、中途半端な位置、例えば点 $(\frac{1}{14}, \frac{5}{14})$ を中心とする半径 $\sqrt{\frac{1105}{98}}$ の円を描くと、下の右図のようになり、円周上にある格子点の数は 4 つです。

この記事では、半径と中心の位置が与えられた時、その円周上にいくつの格子点があるか、ということを (一部の場合についてのみ) 考えてみます。





## 2　準備とか

この記事では、集合

$$\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$$

に注目します。この集合は、$\mathbf{Z}$(整数全体の集合) と似た性質を多く持っています。

$\mathbf{Z}[i]$ における言葉の定義をいくつかしておきます。

- $a, b \in \mathbf{Z}[i]$ とする。$a = bx$ となる元 $x \in \mathbf{Z}[i]$ が存在するとき、$a$ は $b$ で**割り切れる**と言い、$b \mid a$ と書く。
- $u \mid 1$ であるような $u \in \mathbf{Z}[i]$、すなわち $\pm 1, \pm i$ を**単元**という。これは $\mathbf{Z}$ での $\pm 1$ にあたる。
- ある単元 $u$ が存在し、$a = bu$ となるとき、$a$ と $b$ は**同伴する**と言い、$a \sim b$ と書く。例えば、$3 + 2i \sim -2 + 3i \sim -3 - 2i \sim 2 - 3i$ である。$a \sim \overline{a}$ となるのは $a \sim 1$ または $a \sim 1 + i$ の時のみ (偏角を見ると明らか)。
- $p \mid ab \Rightarrow p \mid a$ または $p \mid b$　が成立する、0 でも単元でもない $p \in \mathbf{Z}[i]$ を**素元**という。これは $\mathbf{Z}$ での素数の考え方にあたる。
- 数 $\alpha = a + bi \in \mathbf{Z}[i]$ の**ノルム**を、$N\alpha = \alpha\overline{\alpha} = a^2 + b^2 (= |\alpha|^2)$ で定義する。

素元を定義しましたが、この記事では、あまり定義にとらわれることなく、「素数的な存在」と考えておけば十分です。

以下、$\mathbf{Z}[i]$ に関する性質です。証明は省略しています。

(1) $\mathbf{Z}[i]$ は素元一意分解環である。

簡単に言えば、これは、

「集合 $\mathbf{Z}[i]$ の単元、0 以外の全ての数を、(整数の時の素因数分解と同じような感じで) 素元の積に 1 通りに分解することが出来る」

ということです。具体的には、$8 + i = (2 - i)(3 + 2i)$ などです ($2 - i, 3 + 2i$ は素元)。

$(8 + i = (1 + 2i)(2 - 3i)$ とも分解できますが、この時 $1 + 2i \sim 2 - i$、$2 - 3i \sim 3 + 2i$ となっています。このように、同伴する数で置き換えた分解は、合わせて 1 通りと考えることにします。)

素元には次のような性質があります。

(2) $p \in \mathbf{Z}[i]$ が素元である
$\Longleftrightarrow$ $p$ は 0 でも単元でもなく、かつ、$a \mid p$ の時 $a \sim 1$ または $a \sim p$ が成り立つ (既約元としての性質)

今後、$\mathbf{Z}$ での通常の素数 (ただし符号を変えた-2 や-3 なども含むことにします) のことを「有理素数」と呼ぶことにします。
ある数 $\pi \in \mathbf{Z}[i]$ が素元であるかどうかは、次の命題から調べられます。

(3) $\pi \in \mathbf{Z}[i]$ が素元である
$\Longleftrightarrow$ 「$\pi$は $|\pi| \equiv 3 \pmod 4$ を満たす有理素数」または「$N\pi$ は有理素数」

これより、3 や 7 は素元ですが、2 や 5 は素元ではありません。また、$N(7+2i) = 53$ は有理素数なので、$7+2i$ は素元です。さらに、

(4) $p$:正の有理素数、$p \equiv 1 \pmod 4$ のとき、$a^2 + b^2 = p$ $(a, b \in \mathbf{Z})$ は解を持つ。

これより、4 で割って 1 余る正の有理素数 $p$ について、ある $a, b$ が存在し、$p = (a+bi)(a-bi)$ のように素元の積に分解されることが分かります ($N(a+bi) = p$:有理素数 より $a+bi$ は素元)。

## 3 中心が原点の場合

ここから、最初に挙げた問題を考えていきます。この節では、円の中心が中途半端な位置ではなく、格子点 (原点としてよい) にある場合を考えます。すなわち、原点を中心とする半径 $\sqrt{N}(N \in \mathbf{Z})$ の円を描いた時、その円の通る格子点の数を考えることにします ($N \notin \mathbf{Z}$ の時、明らかに円周上に格子点はありません)。
この問題は、

$$a^2 + b^2 = N, \quad a, b \in \mathbf{Z}$$

の解 $(a, b)$ の個数を求めることにほかなりません。
ここで、上の式は、

$$(a+bi)(a-bi) = N, \quad a, b \in \mathbf{Z}$$

$$\alpha\overline{\alpha} = N, \quad \alpha \in \mathbf{Z}[i] \tag{1}$$

と変形できます。したがって、$\mathbf{Z}[i]$ に注目すべきなのです。以下、(1) の式で考えていきます。

まず、次の補題を示します。

**補題 1**

(1) が解を持つ時、4 で割って 3 余る任意の正の有理素数 $q$ について、$\mathrm{ord}_q(N)$ は偶数。

($n \in \mathbf{Z}$(あるいは $\mathbf{Z}[i]$) を有理素数 (あるいは素元)$p$ で何度も割る時、割り切れる最大回数を $\mathrm{ord}_p(n)$ と書く。)

**証明**

明らかに $a \mid \alpha \Leftrightarrow \overline{a} \mid \overline{\alpha}$ であるので、
4 で割って 3 余る任意の正の有理素数 $q$ について、$\mathrm{ord}_q(\alpha) = \mathrm{ord}_q(\overline{\alpha})$ 。$q$ は素元なので、$\mathrm{ord}_q(N) = \mathrm{ord}_q(\alpha\overline{\alpha}) = \mathrm{ord}_q(\alpha) + \mathrm{ord}_q(\overline{\alpha}) = 2\mathrm{ord}_q(\alpha)$ 。よって示された。

■

これより、$N$ を素因数分解したとき、4 で割って 3 余る有理素数の次数のなかに 1 つでも奇数がある場合、(1) の解は 0 個です。以後、

$$N = 2^e p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j} \cdot Q^2 \tag{2}$$

($N$ の素因数分解; $p_k$:4 で割って 1 余る有理素数、$Q^2$:4 で割って 3 余る素因数の積)
とおいて考えます。さらに、第 2 節の (4) より、各 $p_k (1 \leq k \leq j)$ について、$p_k = \pi_k\overline{\pi_k}$ となる素元 $\pi_k$ をとることができます (素元分解が 1 通りであることより、$\pi_k$ は同伴、共役を同一視すれば 1 通りに定まる)。
これらの記号を使って、(1) の右辺を変形してみると、

$$\alpha\overline{\alpha} = (1+i)^e(1-i)^e \ \pi_1^{e_1}\overline{\pi_1}^{e_1} \ \pi_2^{e_2}\overline{\pi_2}^{e_2} \cdots \pi_j^{e_j}\overline{\pi_j}^{e_j} \cdot Q^2 \tag{3}$$

$$\sim (1+i)^{2e}\pi_1^{e_1}\overline{\pi_1}^{e_1} \ \pi_2^{e_2}\overline{\pi_2}^{e_2} \cdots \pi_j^{e_j}\overline{\pi_j}^{e_j} \cdot Q^2 \tag{4}$$

右辺は $Q^2$ の部分を除き素元分解になっています。あとは、$\alpha$ の素元分解を考えて、以下のように解の個数が求まります。

**定理 1**

(3) の解の個数、すなわち (1) の解の個数は、$4(e_1+1)(e_2+1)\cdots(e_j+1)$ 個。

**証明**

補題 1 の証明中の $\mathrm{ord}_q(N) = 2\mathrm{ord}_q(\alpha)$ より、$Q \mid \alpha, Q \mid \overline{\alpha}$ である。
また、$a \mid \alpha \Leftrightarrow \overline{a} \mid \overline{\alpha}$ なので、

- (4) より $\mathrm{ord}_{1+i}(\alpha) = \mathrm{ord}_{1+i}(\overline{\alpha})$ $(\because 1+i \sim 1-i)$ であり、$\mathrm{ord}_{1+i}(\alpha) + \mathrm{ord}_{1+i}(\overline{\alpha}) = 2e$ なので $\mathrm{ord}_{1+i}(\alpha) = e$ 。
- (4) より $\mathrm{ord}_{\pi_k}(\overline{\alpha}) = \mathrm{ord}_{\overline{\pi_k}}(\alpha)$ であり、$\mathrm{ord}_{\pi_k}(\alpha) + \mathrm{ord}_{\pi_k}(\overline{\alpha}) = e_k$ なので $\mathrm{ord}_{\pi_k}(\alpha) + \mathrm{ord}_{\overline{\pi_k}}(\alpha) = e_k$ 。

これらより、

$$(3) \Longleftrightarrow \text{ある } u_1, u_2, \cdots, u_j \in \mathbf{Z}, 0 \leq u_k \leq e_k \text{が存在し、} \\ \alpha \sim (1+i)^e \pi_1^{u_1} \overline{\pi_1}^{(e_1-u_1)} \cdots \pi_j^{u_j} \overline{\pi_j}^{(e_j-u_j)} \cdot Q \tag{5}$$

となる ($\Rightarrow$:ここまでの議論より , $\Leftarrow$:計算すれば示される)。
ここで、$u_1, \cdots, u_j$ を $0 \leq u_k \leq e_k$ の範囲で自由に動かすと、右辺は $(e_1+1)(e_2+1)\cdots(e_j+1)$ 通り考えられるが、これらは全て互いに同伴しない (同伴するとすると、その同伴する 2 数の素元分解が一致せず、素元分解が 1 通りであることに反する)。
それぞれの右辺の値に対し、それに同伴する数は 4 つずつ存在するが、上のことより、それらは全て異なる。それらが $\alpha$ の解なので、解の個数は $4(e_1+1)(e_2+1)\cdots(e_j+1)$ 個。

■

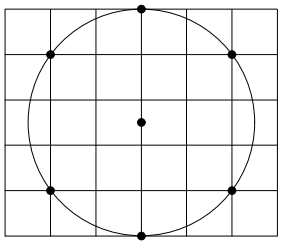
## 4　中心が中途半端な位置の場合

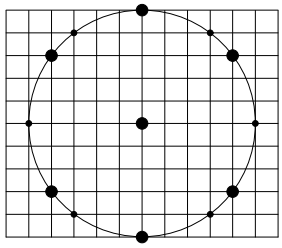
この記事では、円の中心の位置が $(\frac{-r_1}{p}, \frac{-r_2}{p})$ ($p$:正の有理素数,$r_1, r_2 \in \mathbf{Z}$) と表せる場合のみについて考えてみます。
ここで、$(\frac{-r_1}{p}, \frac{-r_2}{p})$ を中心とする半径 $\sqrt{r}$ の円周上の格子点を考える代わりに、原点を中心とする半径 $p\sqrt{r}$ の円周上の格子点 $(a, b)$ で、
$a + bi \equiv r_1 + r_2 i \pmod{p}$ となるものを考えても同じことなので、
「原点を中心とする半径 $\sqrt{N}(N \in \mathbf{Z})$ の円周が通る格子点 $(a, b)$ のうち $a + bi \equiv r_1 + r_2 i \pmod{p}$ を満たすものの数」を考えることにします ($\mathbf{Z}[i]$ においても $a \equiv b \pmod{p} \iff p \mid a - b$ という定義です)。つまり、

$$a^2 + b^2 = N, \quad a + bi \equiv r_1 + r_2 i \pmod{p}, \quad a, b \in \mathbf{Z} \tag{6}$$

これの解の個数を考えることになります。

( 下の左図では $(\frac{-0}{2}, \frac{-1}{2})$ を中心とする半径 $\sqrt{6.25}$ の円周上の格子点を考え、右の図では、原点を中心とする半径 $2\sqrt{6.25}$ の円周上の格子点 $(a,b)$(12 個の黒丸) のうち $a+bi \equiv i \pmod 2$ となるもの (6 個の大きな黒丸) を考えています。)





## 4.1 $p = 2$ の場合

非常に簡単です。一般に

- $a+bi \equiv 0 \pmod 2 \Rightarrow a^2+b^2 \equiv 0^2+0^2 \equiv 0 \pmod 4$
- $a+bi \equiv 1 \Rightarrow a^2+b^2 \equiv 1^2+0^2 \equiv 1$
- $a+bi \equiv i \Rightarrow a^2+b^2 \equiv 0^2+1^2 \equiv 1$
- $a+bi \equiv 1+i \Rightarrow a^2+b^2 \equiv 1^2+1^2 \equiv 2$

なので、$N \equiv 0 \pmod 4$ の場合、円周上の格子点 $(a,b)$ が全て $a+bi \equiv 0$ を満たし、

- $r_1+r_2i \equiv 0$ の時、解は $4(e_1+1)(e_2+1)\cdots(e_j+1)$ 個
- その他の時、解は 0 個

となります。同様にして、$N \equiv 2 \pmod 4$ の場合は

- $r_1+r_2i \equiv 1+i$ の時、解は $4(e_1+1)(e_2+1)\cdots(e_j+1)$ 個
- その他の時、解は 0 個

となります。
$N \equiv 1 \pmod 4$ の場合、円周上の格子点は $\equiv 1$ なものと $\equiv i$ なものの 2 種類ありますが、明らかに

$(a,b)$ が円周上の格子点で $a+bi \equiv 1 \pmod 2$
$\Longleftrightarrow (b,a)$ が円周上の格子点で $b+ai \equiv i \pmod 2$
なので、2 種類の点は一対一対応し、同数ずつあります。よって

- $r_1 + r_2 i \equiv 1$ or $i$ の時、解は $2(e_1+1)(e_2+1)\cdots(e_j+1)$ 個
- その他の時、解は 0 個

となります。$N \equiv 3 \pmod 4$ の時、解はありません。

## 4.2 $p \equiv 3 \pmod 4$ の場合

ここから群や写像の知識が少し必要になります。
まず、$\mathbf{Z}[i]/p\mathbf{Z}[i]$ におけるノルムの写像

$$\begin{aligned} N : \mathbf{Z}[i]/p\mathbf{Z}[i] &\longrightarrow \mathbf{Z}/p\mathbf{Z} \\ \alpha = a+bi &\longmapsto N(\alpha) = a^2+b^2 \bmod p \end{aligned}$$

を考えます (以下、$N(\cdots)$ とある場合は、この写像を指します)。
以下のように、$N^{-1}(0), N^{-1}(1), \cdots, N^{-1}(p-1)$ の元の数が綺麗に求まります。

**定理 2** $\left|N^{-1}(0)\right| = 1\ ,\ \left|N^{-1}(1)\right| = \left|N^{-1}(2)\right| = \cdots = \left|N^{-1}(p-1)\right| = p+1$

いくつかの補題を先に示します:

**補題 2** $\left|N^{-1}(0)\right|, \left|N^{-1}(1)\right|, \cdots, \left|N^{-1}(p-1)\right| > 0$
すなわち、任意の $a \in \mathbf{Z}/p\mathbf{Z}$ について、$N(\alpha) = a$ となる $\alpha$ が存在。

**証明**

$\bmod p$ の平方剰余は $\frac{p+1}{2}$ 個あるので、それらを $b_1, b_2, \cdots, b_{\frac{p+1}{2}}$ とおく。この時 $a-b_1, a-b_2, \cdots, a-b_{\frac{p+1}{2}}$ は全て互いに $\bmod p$ で合同でなく、また $\bmod p$ の平方非剰余は $\frac{p-1}{2}$ 個なので、これらの内、少なくとも 1 つは平方剰余。よって $a$ は 2 つの平方剰余の和で必ず表せるので、示された。

■

**補題 3** $\mathbf{Z}[i]/p\mathbf{Z}[i]$ は体である。

**証明**

乗法の逆元の存在のみ示す。後は明らか。
($\mathbf{Z}[i]/p\mathbf{Z}[i]$ から 0 を除いた集合を $(\mathbf{Z}[i]/p\mathbf{Z}[i])^*$ と表す)
$a \in (\mathbf{Z}[i]/p\mathbf{Z}[i])^* = \{b_1, b_2, \cdots, b_{p^2-1}\}$ とおく。
$\Big((\mathbf{Z}[i]/p\mathbf{Z}[i])^*$ の元数は $p^2-1\Big)$
任意の $1 \leq j, k \leq p^2-1$ について、$ab_j \neq ab_k$($\because ab_j = ab_k$ とすると、ある「$a', b'_j, b'_k \in \mathbf{Z}[i]$, いずれも $p$ で割れず、さらに $b'_j \not\equiv b'_k$」が存在し、
$a'b'_j \equiv a'b'_k$ となるが、$p$ は素元なので不可能)。これより $ab_1, ab_2, \cdots, ab_{p^2-1}$ は全て異なる $(\mathbf{Z}[i]/p\mathbf{Z}[i])^*$ の元なので、1 になるものが存在。よって、$a$ の逆元が存在。

■

**補題 4** $\left|N^{-1}(1)\right| = \left|N^{-1}(2)\right| = \cdots = \left|N^{-1}(p-1)\right|$ 。

**証明**

$1 \leq a \leq p-1$ のとき、$\beta \in N^{-1}(1), \gamma \in N^{-1}(a)$ とおける (補題 2 より)。
このとき、写像 $N^{-1}(1) \longrightarrow N^{-1}(a), \alpha \longmapsto \alpha \cdot \gamma\beta^{-1}$ が全単射なので、示された。

■

**定理 2 の証明:**

$p \equiv 3 \pmod 4$ より $-1$ は $p$ の平方非剰余なので、$0 \leq a, b \leq p-1$ の時、$p \mid a^2 + b^2$ ならば $a = b = 0$($\because a \neq 0$ とすると $b \neq 0$ となり、この時 $a^2, b^2$:平方剰余、$a^2/b^2 \equiv -1$:平方非剰余 となり矛盾)。よって
$\left|N^{-1}(0)\right| = |\{0\}| = 1$ 。
$\mathbf{Z}[i]/p\mathbf{Z}[i]$ の元数は $p^2$ なので、
$\left|N^{-1}(0)\right| + \left|N^{-1}(1)\right| + \left|N^{-1}(2)\right| + \cdots + \left|N^{-1}(p-1)\right| = p^2$ 。これと補題 4 より、示された。

■

これで、円周上の格子点を $\mathrm{mod}\, p$ で見た時に何種類の可能性があるかは求まりました。そこで、それぞれの可能性にいくつずつ円周上の格子点が分布しているかを調べます。

明らかに $N \equiv 0 \pmod{p}$ の時は $N^{-1}(0) = \{0\}$ より全ての点が $a + bi \equiv 0 \pmod{p}$ となります。よって、$N \not\equiv 0 \pmod{p}$ とします。
$(\mathbf{Z}[i]/p\mathbf{Z}[i])^*$ の構造を調べます。

**補題 5** 任意の自然数 $n$ について、$\sum_{d:n \text{ の約数}} \phi(d) = n$ 。

**証明**

$d \mid n$ のとき、

$$\begin{aligned} \phi(d) &= |\{k \mid 1 \leq k \leq n \ , \ \gcd(d,k) = 1\}| \\ &= \left|\{k \mid 1 \leq k \leq n \ , \ \gcd(n,k) = \frac{n}{d}\}\right| \end{aligned}$$

$d$ が $n$ の約数全体を動く時、$\frac{n}{d}$ も $n$ の約数全体を動く。このときの右辺の和は当然 $n$。

■

**定理 3** 群 $(\mathbf{Z}[i]/p\mathbf{Z}[i])^*$ は位数 $p^2 - 1$ の巡回群。

**証明**

$d$ を $p^2 - 1$ の約数とする。
$\mathbf{Z}[i]/p\mathbf{Z}[i]$ は体なので、任意の $d$ について、$x^d = 1$ の解は高々 $d$ 個。したがって、位数が $d$ の約数であるような元は $d$ 個以下。
乗法群 $(\mathbf{Z}[i]/p\mathbf{Z}[i])^*$ の元のうち位数 $d$ の元の個数を $c(d)$ とおくと、$c(d) = 0$ または $c(d) = \phi(d)$ である (位数 $d$ の元がある場合、その元で生成される位数 $d$ の巡回群中に位数 $d$ の元が $\phi(d)$ 個あるが、位数 $d$ の巡回群はそれしか存在しえない)。しかし $\sum_{d:p^2-1 \text{ の約数}} c(d) = \sum_{d:p^2-1 \text{ の約数}} \phi(d) = p^2 - 1$ なので、任意の $d$ について $c(d) = \phi(d)$。よって位数 $p^2 - 1$ の元が存在。よって示された。

■

(5) より、(6) は

$$\begin{aligned} &\text{ある } u_1, u_2, \cdots, u_j \in \mathbf{Z}, 0 \leq u_k \leq e_k \text{が存在し、} \\ \alpha \quad &\sim (1+i)^e \pi_1^{u_1} \overline{\pi_1}^{(e_1 - u_1)} \cdots \pi_j^{u_j} \overline{\pi_j}^{(e_j - u_j)} \cdot Q, \quad \text{かつ} \alpha \equiv r_1 + r_2 i \pmod{p} \end{aligned}$$

と同値です。

ここで、一般に、$a+bi \in \mathbf{Z}[i]$ とするとき、

$$\begin{aligned}(a+bi)^p-(a-bi) &= (a^p -_p C_2 a^{p-2}b^2 + \cdots -_p C_{p-1}ab^{p-1} - a)\\ &+ ({}_pC_1 a^{p-1}b -_p C_3 a^{p-3}b^3 + \cdots - b^p + b)i\\ &\equiv (a^p-a)-(b^p-b)i \equiv 0 \pmod p \text{(Fermat の小定理より)}\end{aligned}$$

なので、$\pi_k \equiv \overline{\pi_k}^p \pmod p$ となります。
巡回群である $(\mathbf{Z}[i]/p\mathbf{Z}[i])^*$ の位数 $p^2-1$ の元 (すなわち生成元) の 1 つを $\gamma$ とし、$\overline{\pi_k} \equiv \gamma^{t_k} \pmod p (1 \le k \le j)$ とおくと ($p \not| N$ としているので $p \not| \pi_k$)、

$$\begin{aligned}\alpha &\sim (1+i)^e \pi_1^{u_1}\overline{\pi_1}^{(e_1-u_1)}\cdots\pi_j^{u_j}\overline{\pi_j}^{(e_j-u_j)}\cdot Q\\ &\equiv (1+i)^e Q\cdot \overline{\pi_1}^{pu_1+(e_1-u_1)}\cdots\overline{\pi_j}^{pu_j+(e_j-u_j)}\\ &\equiv (1+i)^e Q\cdot \gamma^{e_1t_1+\cdots+e_jt_j+(p-1)(u_1t_1+u_2t_2+\cdots+u_jt_j)} \qquad (7)\end{aligned}$$

となり、$4(e_1+1)\cdots(e_j+1)$ 個の円周上の格子点の mod$p$ での分布、すなわち右辺の mod$p$ での分布は、
$(\gamma^k \sim \gamma^{k+\frac{p^2-1}{4}}$ より$)(p-1)(u_1t_1+u_2t_2+\cdots+u_jt_j) \bmod \frac{p^2-1}{4}$ の $(e_1+1)\cdots(e_j+1)$ 個の値の分布に帰着され、したがって $u_1t_1+u_2t_2+\cdots+u_jt_j$ の $(e_1+1)\cdots(e_j+1)$ 個の値の $\bmod \frac{p+1}{4}$ での分布に帰着されます。
しかし、残念なことに、これの分布は難解で、いまだによく分かりません。比較的均等に分布するような気がしますが、そうとは限りません。例を挙げると、$p=43$ の時、$j=10, e_1=\cdots=e_{10}=1, t_1 \equiv \cdots \equiv t_{10} \equiv 1 \pmod{11}$(このような素元 $\pi_k$ はおそらく実在します) の時、$2^{10}$ 個の値のうち $\equiv 5 \pmod{11}$ なものは 252 個ありますが、$\equiv 10 \pmod{11}$ なものは 1 個しかありません。

## 4.3 $p \equiv 1 \pmod 4$ の場合の概略

筆者が疲れてきたので、概略のみにします。
$p \equiv 3$ の時と同様に、$\mathbf{Z}[i]/p\mathbf{Z}[i]$ におけるノルムの写像を考えます。補題 2 と 4 が同様にして成立し、$\left|N^{-1}(a)\right|$ が綺麗に求まります。また、$(\mathbf{Z}[i]/p\mathbf{Z}[i])^*\Big(\mathbf{Z}[i]/p\mathbf{Z}[i]$ から $N(\alpha)=0$ な元を除いて出来る群 $\Big)$ の構造も分かります。しかし、格子点の分布を調べてみると、やはり難解なものになります。

## 5　おわりに

結局、あまり面白いことが示されませんでした。これは、残念なことです。

それはさておき。

このようなことを研究しようと思ったきっかけは、あるゲームにあります。それは、「共円」という名前のボードゲームです。このゲームは、面白いことはさることながら、数学的な研究も複数人によって行われており、その一環として、このような研究を行ってみました。この「共円」に関する数学的な研究は、まだ始まったばかりです。今後、「共円」がさらに研究され、素晴らしい発展を遂げることを期待します。

今年初めて、手書きではなく LaTeX を使って部誌を書きました。まだ慣れておらず、非常に時間がかかりました。

また、今年は部誌関連の研究を始めたのが、これまでの年で一番遅かったです。来年はもっと早めにテーマを決めて、十分な研究を行おうと思います。

さらに、今年初めて、自分の記事のテーマに幾何でないものを選びました(「円」は出てきますが)。そのためかどうか分かりませんが、数論とか現代数学とかの勉強不足を、随所で痛感することになりました。もっと勉強して、来年はさらに良い部誌を書きたいと思います。

これでこの記事を終えたいのですが、奇数ページで終わってはいけないということだそうなので、少し余談を。

ある図形を、いくつか (但し 2 個以上) の有限個の合同な小図形 (元の図形と相似形である必要はない) に分割することを「合同分割」といいます。例えば、正方形は、2 つの合同な直角二等辺三角形に合同分割できます。
私は去年、合同分割に関することを部誌に書きました。そこで予想として、次のようなものを挙げました。

「合同分割できない多角形が存在する。」

これについては、去年からほとんど考えていないのですが、例えば、

$$\angle A = \pi^\circ, \angle B = (180 + \sqrt{2})^\circ, \angle C = e^\circ, AB = 1, BC = e^\pi$$

の凹四角形 $ABCD$ がいくつかの合同図形に分割されるとは、あまり思えません。暇な方は、合同分割できない図形が存在するかどうかを是非考えてみてください。

これで本当にこの記事を終えようと思います。最後までこの記事を読んでくださり、ありがとうございました。

質問や感想は、yoshyoshyosh@hotmail.com までどうぞ。

## 6　参考文献・参考にしたもの


1. 国吉秀夫「群論入門 [新訂版]」サイエンス社
2. 木田祐司「初等整数論」朝倉書店
3. 共円研究板