研究報告

ガウス整数環の素元の分布

学習院大学理学部　中　島　匠　一
学習院大学理学部　中　野　　伸

1　イントロダクション

自分自身と 1 以外に約数を持たない自然数を素数と呼ぶ。すべての自然数が素数の積として表されることからわかるように、整数について数学的考察を加える上で、素数は基本的な対象である。「素数は無限個存在する」というユークリッドの定理に始まって、ギリシャ時代から現代まで、素数の分布は非常に深く研究されている。

考察の対象を複素数まで広げようとするとき、ガウス整数が最初の考察対象となる。ガウス整数とは、整数 a,b と虚数単位 i によって $a+bi$ と表される複素数のことで、幾何学的には、複素数平面上の格子点に対応している。(数学者ガウスが初めて導入し、深く研究したことから、ガウス整数という名前で呼ばれている。) ガウス整数についても「素数」(ただし、本稿では「素元(そげん)」とか「ガウス素数」と呼ぶ) が存在して、素因数分解の一意性に当たる性質も成り立つ (2 節参照)。ガウス素数について考察すべき問題は数多いが、本稿では、複素数平面上でのガウス素数の分布に関する研究を報告する。取り上げる問題は、(通常の) 素数の分布の問題に準じているものが多い。しかし、ガウス素数の場合には分布の「土俵」が 2 次元 (＝平面) であるので、通常の素数の場合の 1 次元 (＝直線上) の分布では生じない複雑さが発生する点が興味深い。

本報告では、2 節で基本概念の復習と記号の説明を行ったあと、3 節で一様分布に関するワイルの定理を提示する。最後の 4 節で、我々の行った数値実験の結果を報告して、今後の方向を検討する。

2　ガウス整数環

最初に、数学で一般的に使われる記号を確認する。記号 $\mathbf{Z},\mathbf{R},\mathbf{C}$ は、それぞれ、整数環、実数体、複素数体を表す。虚数単位を i で表し、複素数 α に対して、

$$\mathrm{Re}\,\alpha \text{ (実部)}, \quad \mathrm{Im}\,\alpha \text{ (虚部)}$$

$\overline{\alpha} = \mathrm{Re}\,\alpha - (\mathrm{Im}\,\alpha)i$　(複素共役)
$N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} = (\mathrm{Re}\,\alpha)^2 + (\mathrm{Im}\,\alpha)^2$　(ノルム＝絶対値の 2 乗)
$\arg\alpha$　(偏角; $-\pi < \arg\alpha \leq \pi$)

という記号を使う。

我々の研究対象であるガウス整数の集合は

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

と表せる。この $\mathbf{Z}[i]$ は和・差・積に関して閉じていることが簡単に確かめられて、$\mathbf{Z}[i]$ が環（用語は、たとえば、[N] の第 2 章参照）をなすことがわかる。したがって、$\mathbf{Z}[i]$ はガウス整数環と呼ばれる。ガウス整数環は次のような性質を持つことが知られている。(以下、「ガウス整数環 $\mathbf{Z}[i]$ の素元」のことを「ガウス素数」と呼ぶ。)

(i) $\mathbf{Z}[i]$ の単数（＝（積に関する）可逆元）は $\pm 1, \pm i$ の 4 つである。

(ii) $\mathbf{Z}[i]$ は単項イデアル整域である。したがって、$\mathbf{Z}[i]$ の元は、単数といくつかのガウス素数の積に一意的に分解される。

(iii) 素数 2 は、$\mathbf{Z}[i]$ で $2 = -i(1+i)^2$ と分解される。したがって、2 を割り切るガウス素数は $1+i$（の単数倍）だけである。

(iv) 素数 p が $p \equiv 3 \pmod 4$ をみたすとする。このとき、p 自身がガウス素数であり、$N(p) = p^2$ である。

(v) 素数 p が $p \equiv 1 \pmod 4$ をみたすとする。このとき、ガウス素数 π とその複素共役 $\overline{\pi}$ があり、p は $\mathbf{Z}[i]$ において $p = \pi\overline{\pi}$ と分解する。また、$N(\pi) = N(\overline{\pi}) = p$ である。(注：ここに登場した記号 π は円周率ではなく、一般的な文字として使われている。)

少し注釈を与えておこう。性質 (i) は簡単な計算で確かめられ、(ii) は代数学の一般論から従う（たとえば、[N] の第 2 章参照)。性質 (iii)(iv)(v) の証明には数論的議論が必要であるが、それは省略する。用語としては、性質のことを、ガウス整数環で、(iii) 2 は分岐する、(iv) $p \equiv 3 \pmod 4$ をみたす p は惰性する、(v) $p \equiv 1 \pmod 4$ をみたす p は分解する、と表現することも多い。$N(p) = p^2$ であることから、(iv) の p は「2 次のガウス素数」と呼ばれ、$N(\pi) = N(\overline{\pi}) = p$ であることかから、(v) の $\pi, \overline{\pi}$ は「1 次のガウス素数」と呼ばれる。

理由を詳しく説明することは省略するが、整数論では一般的に「1 次の素数（または、素イデアル)」が重要であり、その事情はガウス整数環でも同じである。また、特にガウス整数環では「1 次のガウス素数の複素数平面上の分布」に面白い現象が起きていることが確かめられる。したがって、以下では上の (v) に対応するガウス素数の分布を考察してゆく。

ガウス素数が1つあれば、それの単数倍もガウス素数である。上の (i) に述べたように、ガウス整数環には単数が4つあるので、ガウス素数も4つずつ組になって現れる。そのようなガウス素数は「同伴」と呼ばれていて、同伴なガウス素数は同じノルムを持つことがすぐにわかる。同じノルムを持つガウス素数から1つ代表をとり出すために、次の定義をする。まず、初等整数論での議論により、$p \equiv 1 \pmod 4$ をみたす素数 p が無限個存在することはわかっている。それで、$p \equiv 1 \pmod 4$ をみたす素数 p で（大きさが小さい順に）n 番目のものを q_n と表す（$n \geq 1$）。具体的に書いておくと、

$$q_1 = 5, \quad q_2 = 13, \quad q_3 = 17, \quad q_4 = 29, \quad q_5 = 37, \cdots$$

である。上記 (v) により q_n はガウス整数環で2つのガウス素数の積に分解するが、さらに条件を付けて、

$$q_n = \pi_n \overline{\pi_n}, \quad \pi_n \equiv 1 \pmod{2(1+i)}, \quad \operatorname{Im} \pi_n > 0$$

をみたすガウス素数 π_n が唯1つ定まることが確かめられる。（注：条件 $\pi_n \equiv 1 \pmod{2(1+i)}$ をみたす π_n は primary と呼ばれる。これは整数論で意味のある条件であるが、説明は省略する。）簡単な計算によって、最初のほうの π_n が

$$\pi_1 = -1+2i, \quad \pi_2 = 3+2i, \quad \pi_3 = 1+4i, \quad \pi_4 = -5+2i, \quad \pi_5 = -1+6i$$

であることが確かめられる。

上記の最後の条件 $\operatorname{Im} \pi_n > 0$ により、π_n は複素数平面の上半分（＝上半平面）に分布していることになる。この分布を調べるのが我々の目的である。具体的に述べるために、さらに記号を導入しておく。上記の (v) によって π_n の絶対値はわかっている（$|\pi_n| = \sqrt{N(\pi_n)} = \sqrt{q_n}$）。よって、$\pi_n$ の偏角が問題となるが、その偏角を π で割ったものを θ_n とおく。つまり、

$$\theta_n = \frac{\arg \pi_n}{\pi}, \quad (0 < \theta_n < 1)$$

である。（注：上の式で、分母の π は円周率を表している；ガウス素数を表す π_n と記号がややこしいようだが、慣れると特に問題は起きないので、この記号を使う。これ以後も「単独の」π は円周率を表す。）

n が自然数全体を動くときの θ_n の分布が研究の主題だが、興味深いバリエーションもある。そのために、

$$\begin{aligned} d(\pi_n) &= \frac{\min\{N(\pi_k - \pi_n) \mid k \neq n\}}{8} \\ T(\pi_n) &= \{\pi_k - \pi_n \mid N(\pi_k - \pi_n) = 8d(\pi_n)\} \\ t(\pi_n) &= |T(\pi_n)| \end{aligned}$$

とおく（k, n は自然数を表している）。言葉で表せば、$d(\pi_n)$ は π_n からもっとも近いガウス素数（＝「お隣さん」）への距離（を8で割ったもの）であり、

$T(\pi_n)$ は π_n の「お隣さん」の配置で、$t(\pi_n)$ は π_n の「お隣さん」の数である。(注：上記の primary という条件により、$N(\pi_k - \pi_n)$ は必ず $8 = N(2(1+i))$ で割り切れる。よって、$N(\pi_k - \pi_n)$ を 8 で割ったものを $d(\pi_n)$ とおいた。) 通常の素数の場合には、「隣り合う素数の距離」が 2 に等しい場合が「双子素数」と呼ばれている。ガウス素数については $d(\pi_n) = 1$ となることが、「双子素数」の類似、と考えられる。その意味で、$d(\pi_n)$ は興味深い数である。通常の素数の場合には「隣の素数」の配置は、前か後ろのどちらかしかなく、面白いことは（あまり）ない。しかし、ガウス素数の場合には「2 次元の配置」ということから、$T(\pi_n)$ や $t(\pi_n)$ には、通常の素数では登場しない問題がいくつも現れてきて、興味深い。ただ、我々の研究は θ_n の分布を主眼としていて、$T(\pi_n)$ や $t(\pi_n)$ については、研究はまだ十分には進展していない。現時点での「推測」について 4 節で簡単に触れたので、参照していただきたい。

3　一様分布

我々の研究の主要なテーマは

偏角 θ_n の分布は、一様分布か？

という問題である。さて、「一様 (uniform)」という言葉は、数学では頻繁に使われる用語だが、通常の会話ではあまり登場しないかもしれない。一般的な言葉遣いだと、分布が均一である、というのが「一様分布」のイメージを表していそうである。いずれにしても、正確な定義を与えれば、曖昧さはなくなる。

数列 $\{a_n\}$ の各元 a_n は、実数の区間 $[0,1) = \{x \in \mathbf{R} \mid 0 \leq x < 1\}$ に属しているとする。このとき、数列 $\{a_n\}$ が（区間 $[0,1)$ 内で）一様分布している、とは、$b < c$ をみたす任意の $b, c \in [0,1)$ について

$$\lim_{N\to\infty} \frac{|\{n \leq N \mid b \leq a_n < c\}|}{N} = c - b$$

が成り立つこと、と定義される。この式の左辺の極限は a_n が（$[0,1)$ の部分区間である）$[b,c)$ に属する割合を表し、右辺の値は $\dfrac{\text{区間 } [b,c) \text{ の長さ}}{\text{区間 } [0,1) \text{ の長さ}}$ に等しい。このことから、上の等式が「分布が一様（＝均一）であること」を表している、ということが納得されるだろう。

一様分布の定義は上記の通りだが、実際に数列が与えられたときに定義の条件を直接確かめるのは困難なことが多い。この困難の解決のために、数学者ワイル (H. Weyl) がフーリエ展開を応用する手法を考案して、下記の定理を得た。ワイルの定理は一様分布の研究に非常に有効で、この分野の「基本定理」となっている。定理の主張を述べるために、1 つ記号を導入する。まず、区間 $[0,1)$ 内の数列 $\{a_n\}$ が与えられているとする。このとき、自然数 ν, N

について

$$S_\nu(N) = \sum_{n=1}^{N} \exp(2\pi i \nu a_n) \ \in \mathbf{C}$$

とおく（ワイルの和；ここで、$\exp(x) = e^x$（指数関数）である)。数列 $\{a_n\}$ の分布の一様性を（N に関する）複素数列 $S_\nu(N)$ の性質に言い換えるのが、ワイルの定理である。（ワイルの定理の証明を含む一様分布の一般論については、[KN] 参照。）

ワイルの定理　数列 $\{a_n\}$ が一様分布であるための必要十分条件は、任意の自然数 ν に対して

$$\lim_{N\to\infty} \frac{1}{N} S_\nu(N) = 0$$

が成り立つことである。

我々の研究では、このワイルの定理を通じて、偏角 θ_n の分布の一様性を調べた。

4　実験結果

ガウス素数（と、その偏角）の分布については、あまり多くの結果は知られていない。したがって、我々の研究では、まず具体的な数値実験を行うことからはじめた。実験に当たっては、学習院にサイトライセンスが導入されている数式処理ソフト Maple を利用した。Maple はグラフィックス機能も充実しており、我々も多くの「絵」を描いて研究を進めた。しかし、本報告では図の掲載は省略して、実験の結果として得られた予測とその証明の公算について述べることにする。

実験においては、ガウス素数 π_n を計算し、さらにその偏角 θ_n を求めるのが基本となる。このとき、素数 q_n は簡単に計算できるが、それを $q_n = \pi_n\overline{\pi_n}$ と分解するのは、難しい（素朴な手法では、時間がかかりすぎる)。この問題の解決のために文献の調査を行い、「コルナッキアのアルゴリズム」というものがあり、π_n の計算にはそれが有効であることをみつけた。これを受けて、我々はまずコルナッキアのアルゴリズムを Maple 上でプログラムして、π_n と θ_n のデータを集めた。そして、プロジェクトの予算で購入したＰＣを「計算専用マシン」としてデータの収集を進めた。その結果、現時点で、1.5×10^8（1 億 5 千万）以下の q_n についてガウス素数 π_n のデータが得られた（データ数は $4,222,500$ 個)。また、「お隣さん」を求めるプログラムを作成して、上記の範囲で $d(\pi_n), T(\pi_n), t(\pi_n)$ も計算した。

本報告の最後に、偏角 θ_n について、我々の膨大なデータから得られた「予測」を紹介しておく。ここで、記号 $S_\nu(N)$ は、$a_n = \theta_n$ に対するワイルの和である（3 節参照)。また、偏角の差を調べるために

$$\delta_n = \frac{\theta_{n+1} - \theta_n + 1}{2} \ \in (0,1) \quad (n \geq 1)$$

とおいた。(注：偏角の差 $\theta_{n+1}-\theta_n$ は区間 $(-1,1)$ に属している。これを区間 $(0,1)$ の分布に直すために、1 を足して 2 で割る、という変換をおこなっている。) 以上の記号のもとで、「予測」は次のようになる。

(I) すべての ν について、

$$N \to \infty \text{ のとき } \frac{1}{\sqrt{N}} S_\nu(N) \text{ は有界}$$

であろう。

(II) 偏角 θ_n は、区間 $(0,1)$ で一様分布であろう。

(III) $d(\pi_n)$ や $t(\pi_n)$ の値を指定して $\{\theta_n\}$ の部分数列をとっても、その部分数列は一様分布であろう。

(IV) 偏角の差から定まる数列 $\{\delta_n\}$ は、一様分布をして**いない**であろう。

我々のデータを処理してみると、「予測」(I)(III)(IV) はかなり確からしい、と見える。もちろん、有限個のデータからこれらの主張を確認することはできないが、かなり有力な傍証だ、とは言えそうである。ただし、(III) については、データの個数が十分に大きくて「推測」が有効だといえるのは、$d(\pi_n)=1$ の場合に限られている。($d(\pi_n)\geq 2$ となる頻度はかなり低くて、現在の計算範囲では、十分な個数のデータが得られていない。)

3 節で説明したワイルの定理により、(I) が成り立てば (II) が成り立っていることになる。しかし、その逆はいえない。つまり、「推測」(I) は「推測」(II) の定量的精密化である、といえる。今回の数値実験によって、$\sqrt{N}$ という「$S_\nu(N)$ の増大度」が予測できたことは、非常に興味深い。ガウス整数環の L-関数を応用すると (I)（または、それより少し弱い (II)）が証明できる可能性がある。今後は「予測」の証明に向けて研究を進めてゆく計画である。

5　参考文献

[KN] L.Kuipers, H.Niederreiter、「Uniform Distribution of Sequences」、Dover Publications、2002 年。

[N] 中島匠一「代数と数論の基礎」、共立出版、2000 年。