代数的整数を用いた$n = 3, 4$の場合のフェルマーの最終定理の証明

明治大学理工学部数学科
2012 年度藏野研究室卒業論文
越前谷 彩香
菅野 翔
小林 彰大
三石 知生

2013 年 2 月 25 日

1　はじめに

フランスの数学者であるフェルマー[1]は、ディオファントス[2]の著書「算術」を研究し、「算術」のページの余白に 48 の書き込みをしていた。その中の一つに次のようなものがある。

＜ある三乗数を二つの三乗数の和で表すこと、あるいはある四乗数を二つの四乗数の和で表すこと、および一般に、二乗よりも大きい冪の数を同じ冪の二つの和で表すことは不可能である＞

すなわち、

方程式 $x^n + y^n = z^n$ $(n \geq 3)$ を満たす三つの自然数は存在しない

ということである。さらにフェルマーの書き込みはこう続く。

＜私はこの命題の真に驚くべき証明を持っているが、余白が狭すぎるのでここに記すことはできない＞

その後フェルマーがこの証明の詳細を述べることはなく、わずかなヒントを記したメモを残すのみであった。フェルマーが正しい証明を得ていたかは定かではない。のちにフェルマーの息子がこれを含む 48 の書き込みをまとめ、「算術」の付録

[1]Pierre de Fermart (1601-1665) 職業は弁護士でありながら、数論だけでなく、幾何学や積分学など様々な分野で業績を残した。

[2]Diophantus (250 年頃) 古代ギリシアの数学者。著書の「算術」は 13 巻に及ぶ。

として 1670 年に刊行した。この刊行によりこの問題は有名になり、のちに「フェルマーの最終定理」と呼ばれ、数世紀にわたって世界中に知られることとなった。

フェルマーはこの他にも様々な所見を残しており、それらは何世紀という時の流れのなかで証明されていった。その中で最後に残ったのが、フェルマーの最終定理である。それが最終定理と呼ばれる所以である。フェルマーの最終定理を証明するために多くの方法が考え出され、多くの理論が生まれた。そしてついに、3 世紀以上の時を経て、1994 年にワイルズ[3]により証明された。

フェルマーの最終定理は、$n = 4$ と n が奇素数の場合に証明すればよいということは、簡単にわかる。$n = 4$ と n がいくつかの奇素数の場合については、1800 年代までに様々な人物により証明が得られていた。$n = 4$ の場合は、「算術」の書き込みの中でフェルマーが無限降下法を用いて証明をしていた。後に 18 世紀になって、オイラー[4]が Gauss 整数上に拡張して別証明を与えている。$n = 3$ の場合も、オイラーが無限降下法を利用して証明を得た。その後ガウス[5]が $\mathbb{Z}[\omega]$ を用いて別証明を行った。$n = 5$ の場合は、ルジャンドル[6]とディリクレ[7]によって証明された。x, y, z のどれかが偶数であり、かつ 5 の倍数である場合とそうでない場合の 2 つの場合に分け、その第一の場合をディリクレが、第二の場合をルジャンドルが証明を完成させた。$n = 7$ の場合は 1839 年にラメ[8]が証明を与えた。しかしこの辺りで初等的な手法による証明は限界とされた。その後、クンマー[9]は円分体の整数論を適用して素数を正則素数と非正則素数に分け、正則素数に対してフェルマーの最終定理が正しいことを証明した。素数全体の集合の中で、約半数が正則素数であろうという予想がある。100 以下の非正則素数は、37, 59, 67 のみであることが知られている。

個々の証明の中でも、$n = 3, 4$ の場合の代数的整数を用いた証明は明確であり、かつ代数的整数の性質を含め興味深いものであるので、これを卒業論文のテーマにした。

第 2 章、第 3 章では Gauss 整数と呼ばれる代数的整数 $\mathbb{Z}[i]$ に関する基本的な性質をまとめた。第 4 章では、$n = 4$ におけるオイラーが与えた証明を行う。第 5 章では代数的整数 $\mathbb{Z}[\omega]$ の定義や性質をまとめる。第 5 章では $n = 3$ における $\mathbb{Z}[\omega]$ を

[3]Andrew John Wiles (1953-) オックスフォード大学教授。1993 年にフェルマーの最終定理の証明を発表したが、後に誤りがあることが判明。1994 年に正しい証明を発表した。

[4]Leonhard Euler (1707-1783) 天文学や力学、流体力学などの自然科学を含め、数学のあらゆる分野の研究を行った。

[5]Karl Friedrich Gauss (1777-1855) 合同式や原子根の概念を確立させ、平方剰余の相互法則や円分方程式などの理論を与えた。

[6]Adrien Marie Legendre (1752-1833) フランスパリの数学者。整数論や楕円積分について研究を行った。

[7]Peter Gustav Lejeune Dirichlet (1805-1859) ドイツの数学者。整数論だけでなく、解析の分野でも多くの業績を残した。

[8]Gabriel Lame (1795-1871) フランスの数学者。$n = 7$ の証明の後、最終定理の完全な証明を試みるが、ラメの証明では不可能だとクンマーにより明らかにされた。

[9]Ernst Eduard Kummer (1810-1893) ドイツの数学者。フェルマーの最終定理に対する貢献で 1857 年に (フェルマーの最終定理の証明に対して与えられることになっていた) 賞を受賞した。

用いたガウスの証明方法を扱う。

2 Gauss整数 $a+bi$

定義 2.1

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

を Gauss（の複素) 整数の集合とする。

一般の整数の集合 $\mathbb{Z}$ を有理整数の集合と呼ぶことにする。

注意 2.2 $a+bi$ の書き方は一意的である。つまり、$a,b,c,d\in\mathbb{R}$ について、

$$a+bi=c+di \iff \begin{cases} a=c \\ b=d \end{cases}$$

が成立する。

事実 2.3 (1) Gauss 整数の和、差、積は Gauss 整数である。実際、

$$(a+bi)\pm(c+di)=(a\pm c)+(b\pm d)i$$

$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$$

となり、実部、虚部ともに有理整数となっているので、これらは Gauss 整数である。

(2) Gauss 整数の商は必ずしも Gauss 整数ではない。$c+di\neq 0$ とする。

$$\frac{a+bi}{c+di}=\frac{a+bi}{c+di}\frac{c-di}{c-di}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i$$

ここで、$(c,d)\neq(0,0)$ なので、$c-di\neq 0, c^2+d^2\neq 0$ に注意する。実部、虚部ともに有理数ではあるが、必ずしも有理整数ではない。すなわち、必ずしも Gauss 整数ではない。

定義 2.4 $\beta\neq 0, \alpha,\beta\in\mathbb{Z}[i]$ とする。$\dfrac{\alpha}{\beta}\in\mathbb{Z}[i]$ であるとき、β は α を割り切るといい、$\beta\mid\alpha$ とかく。このとき、α を β の倍数、β を α の約数という。

注意 2.5 $\alpha,\beta\in\mathbb{Z}[i]$ とし、β は α を割り切るとする。このとき、ある $\gamma\in\mathbb{Z}[i]$ が存在し、$\alpha=\beta\gamma$ とかける。

また、$a,b,c\in\mathbb{Z}$ に対し、Gauss 整数の範囲内で c が $a+bi$ を割り切ることは、有理整数の範囲内で c が a を割り切りかつ c は b も割り切ることと同値である。特に、Gauss 整数の範囲内で c が a を割り切ることは、有理整数の範囲内で c が a を割り切ることと同値である。

系 2.6 $\alpha_1, \alpha_2, \beta, \mu_1, \mu_2 \in \mathbb{Z}[i]$ とし、β が α_1, α_2 を割り切るとするならば、β は $\alpha_1 \pm \alpha_2$ を割り切る。または一般に β は $\mu_1\alpha_1 + \mu_2\alpha_2$ を割り切る。

証明 後半を示す。 $\alpha_1 = \gamma_1\beta, \alpha_2 = \gamma_2\beta$ とおく。

$$\mu_1\alpha_1 + \mu_2\alpha_2 = (\mu_1\gamma_1 + \mu_2\gamma_2)\beta$$

であるので、β は $\mu_1\alpha_1 + \mu_2\alpha_2$ を割り切る。 **証明終**

定義 2.7 $\mu = a + bi \in \mathbb{Z}[i]$ の共役複素数は $\overline{\mu} = a - bi \in \mathbb{Z}[i]$ である。

$$N(\mu) = \mu\overline{\mu} = |\mu|^2 = a^2 + b^2$$

を μ のノルムという。これは、μ の倍数である。

注意 2.8 $\mathbb{N}_0 = \{0, 1, 2, \cdots\}$ とおく。$\mu \in \mathbb{Z}[i]$ のとき、$N(\mu) \in \mathbb{N}_0$ である。特に、$N(\mu) = 0$ であることは、$\mu = 0$ であることと同値である。

注意 2.9 次の等式が成り立っている。

$$\overline{\beta + \gamma} = \overline{\beta} + \overline{\gamma}$$
$$\overline{\beta\gamma} = \overline{\beta}\,\overline{\gamma}$$

系 2.10 $\alpha, \beta \in \mathbb{Z}[i]$ とし、 β は α を割り切るとするならば、$N(\beta)$ は $N(\alpha)$ を割り切る。

証明 $\alpha = \beta\gamma, \gamma \in \mathbb{Z}[i]$ とおく。

$$N(\alpha) = \alpha\overline{\alpha} = \beta\gamma\overline{(\beta\gamma)} = \beta\gamma\overline{\beta}\,\overline{\gamma} = \beta\overline{\beta}\gamma\overline{\gamma} = N(\beta)N(\gamma)$$

よって、 $N(\beta)$ は $N(\alpha)$ を割り切る。 **証明終**

定義 2.11 1 の約数を Gauss 整数の単数という。また、$\mathbb{Z}[i]$ の単数全体を $\mathbb{Z}[i]^\times$ で表す。

命題 2.12 $\alpha \in \mathbb{Z}[i]$ とする。このとき、α が単数であることは、$N(\alpha) = 1$ であることと同値である。また、$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ である。

証明 $(\Rightarrow)$ $\alpha = a + bi$ $(a, b \in \mathbb{Z})$ を単数とする。α は 1 の約数なので、系 2.10 より、$N(\alpha)$ は $N(1) = 1$ の約数である。注意 2.5 より、$N(\alpha) = 1$ となる。

$(\Leftarrow)$ $N(\alpha) = 1$ とする。 $N(\alpha) = \alpha\overline{\alpha} = 1$ より、α は 1 の約数であり、 α は単数となる。 **証明終**

Gauss 整数のすべての単数を求める。$\epsilon = a + bi \in \mathbb{Z}[i]^\times$ $(a, b \in \mathbb{Z})$ とする。ϵ は単数なので、$N(\epsilon) = a^2 + b^2 = 1$ となる。このとき、

$$\begin{cases} a = \pm 1 \\ b = 0 \end{cases} \quad \text{または} \quad \begin{cases} a = 0 \\ b = \pm 1 \end{cases} \quad \text{である。}$$

従って、単数は、$\pm 1, \pm i$ の四つである。

定義 2.13 $\beta \neq 0, \alpha, \beta \in \mathbb{Z}[i]$ とする。$\dfrac{\alpha}{\beta}$ が単数に等しいとき、α, β を互いに同伴 (α は β の同伴数) という。

$\alpha = a + bi$ の同伴数は、$\pm\alpha, \pm i\alpha$ の四つである。すなわち、$a + bi, -a - bi, -b + ai, b - ai$ である。

定義 2.14 $\alpha \in \mathbb{Z}[i], N(\alpha) \geq 2$ とする。α の約数が単数または、α と同伴な元のみであるとき、α は Gauss 整数の素数という。

注意 2.15 $\alpha \in \mathbb{Z}[i]$, α を素数とする。$\alpha = \beta\gamma$ $(\beta, \gamma \in \mathbb{Z}[i])$ とすると、β または γ は単数である。また、「$\alpha = \beta\gamma$ を満たす $\beta, \gamma \in \mathbb{Z}[i]$ があれば、β と γ のどちらかは単数である」が成立するとき、α は素数である。

補題 2.16 $\alpha \in \mathbb{Z}[i]$ に対して、$N(\alpha)$ が有理素数ならば、α は素数である。

証明 $\alpha = \beta\gamma$ $(\beta, \gamma \in \mathbb{Z}[i])$ とすれば、$N(\alpha) = N(\beta)N(\gamma)$ である。$N(\alpha)$ は有理素数なので、$N(\beta) = 1$ または $N(\gamma) = 1$ となる。よって、命題 2.12 より、β または γ が単数となる。よって、注意 2.15 より、α は素数である。 **証明終**

定理 2.17 $\alpha \in \mathbb{Z}[i], N(\alpha) \geq 2$ とすると、α は有限個の素数の積で表せる。

証明 $N(\alpha)$ に関する帰納法で示す。

(i) $N(\alpha) = 2$ のとき。$N(\alpha)$ は有理素数なので、補題 2.16 より、α は素数である。

(ii) $N(\alpha) > 2$ のとき。$2 \leq N(\beta) < N(\alpha)$ を満たす Gauss 整数 β に対しては、定理 2.17 が正しいと仮定する。α は素数とすると、定理 2.17 は正しい。α は素数でないとすると、$\alpha = \beta\gamma$ $(\beta, \gamma \in \mathbb{Z}[i]$ であり、β, γ は単数でない) と書ける。よって、$N(\alpha) = N(\beta)N(\gamma)$ と書け、このとき、$2 \leq N(\beta), N(\gamma) < N(\alpha)$ である。帰納法の仮定より、β, γ は有限個の素数の積である。従って、α は有限個の素数の積である。

よって、$N(\alpha) \geq 2$ ならば α は有限個の素数の積で表せる。 **証明終**

定理 2.18 任意の $\alpha, \beta \in \mathbb{Z}[i]$ $(\beta \neq 0)$ について、

$$\alpha = \kappa\beta + \rho \ , \ |\rho| < |\beta|$$

を満たす $\kappa, \rho \in \mathbb{Z}[i]$ が存在する。

証明 $x+yi \in \mathbb{Z}[i]$ $(x,y \in \mathbb{Z})$ は、Gauss 平面上において、正方格子点で表される。任意の $\xi \in \mathbb{C}$ に対して、ξ はこの格子のある正方格子内にあり、その正方形の四つの頂点のうち少なくとも一つから ξ までの距離は 1 よりも小 (正確には $\frac{\sqrt{2}}{2}$ 以下) である。

$\xi = \frac{\alpha}{\beta}$ のとき、ξ との距離が最小の頂点を κ とすれば、$\kappa \in \mathbb{Z}[i]$ で、

$$\left| \frac{\alpha}{\beta} - \kappa \right| < 1$$

である。$\rho = \alpha - \kappa\beta$ とおけば、$\rho \in \mathbb{Z}[i]$ で、

$$\left| \frac{\rho}{\beta} \right| < 1 \text{ すなわち、} |\rho| < |\beta|$$

が成立する。 **証明終**

この定理 2.18 に基づいて、$0 \neq \alpha, \beta \in \mathbb{Z}[i]$ について、Euclid 互除法を行うことができる。

$$\alpha = \kappa\beta + \beta_1 \ , \ |\beta_1| < |\beta|$$

$\beta_1 = 0$ なら終わり。$\beta_1 \neq 0$ ならば、

$$\beta = \kappa_1\beta_1 + \beta_2 \ , \ |\beta_2| < |\beta_1|$$

これを続けていくと、

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$|\beta| > |\beta_1| > |\beta_2| > \cdots\cdots$$

であり、$|\beta|^2 = N(\beta)$ より、

$$N(\beta) > N(\beta_1) > N(\beta_2) > \cdots\cdots$$

となる。これは、正の有理整数なので、真減少列は無限には続かない。つまり、剰余は終に 0 にならなければならない。

$\beta_{n-1} = \kappa_n\beta_n$ とする。

定理 2.19 $0 \neq \alpha, \beta, \gamma \in \mathbb{Z}[i]$ とする。γ が α, β の公約数であることと、γ が β_n の約数であることは同値である。

証明 $(\Rightarrow)$ $\gamma \in \mathbb{Z}[i]$, γ を α, β の公約数とする。

$\alpha = \kappa\beta + \beta_1$ より γ は β_1 の約数である。
$\beta = \kappa_1\beta_1 + \beta_2$ より γ は β_2 の約数である。
$\cdots\cdots\cdots\cdots$
$\beta_{n-3} = \kappa_{n-2}\beta_{n-2} + \beta_{n-1}$ より γ は β_{n-1} の約数である。
$\beta_{n-2} = \kappa_{n-1}\beta_{n-1} + \beta_n$ より γ は β_n の約数である。

($\Leftarrow$) $\gamma \in \mathbb{Z}[i], \gamma$ を β_n の約数とする。

$\beta_{n-1} = \kappa_n\beta_n$ より γ は β_{n-1} の約数である。
$\beta_{n-2} = \kappa_{n-1}\beta_{n-1} + \beta_n$ より γ は β_{n-2} の約数である。
$\cdots\cdots\cdots\cdots\cdots$
$\beta = \kappa_1\beta_1 + \beta_2$ より γ は β の約数である。
$\alpha = \kappa\beta + \beta_1$ より γ は α の約数である。
よって、γ は α, β の公約数である。

証明終

定理 2.19 を満たす β_n を α, β の最大公約数といい、(α, β) とかく。[10]

定理 2.20 $0 \neq \alpha, \beta \in \mathbb{Z}[i], (\alpha, \beta) = \delta$ とするならば、

$$\alpha\xi + \beta\eta = \delta$$

となる $\xi, \eta \in \mathbb{Z}[i]$ が存在する。

証明

$$\begin{aligned}
&\alpha = \kappa\beta + \beta_1 \\
&\beta = \kappa_1\beta_1 + \beta_2 \\
&\cdots\cdots\cdots
\end{aligned}$$

$$\beta_{n-3} = \kappa_{n-2}\beta_{n-2} + \beta_{n-1} \tag{1}$$
$$\beta_{n-2} = \kappa_{n-1}\beta_{n-1} + \delta \tag{2}$$
$$\beta_{n-1} = \kappa_n\delta$$

とする。式 (2) を用いると、

$$\delta = \beta_{n-2} - \kappa_{n-1}\beta_{n-1}$$

β_{n-1} に式 (1) を代入すると、

$$\begin{aligned}
\delta &= \beta_{n-2} - \kappa_{n-1}(\beta_{n-3} - \kappa_{n-2}\beta_{n-2}) \\
&= -\kappa_{n-1}\beta_{n-3} + (1 + \kappa_{n-1}\kappa_{n-2})\beta_{n-2} \\
&\cdots\cdots\cdots
\end{aligned}$$

よって、$\alpha\xi + \beta\eta = \delta$ となる $\xi, \eta \in \mathbb{Z}[i]$ が存在する。 証明終

系 2.21 $\pi \in \mathbb{Z}[i]$ を素数とし、π は $\alpha\beta$ $(\alpha, \beta \in \mathbb{Z}[i])$ を割り切るとするならば、π は α を割り切るか、π は β を割り切る。

[10]定理 2.19 より、最大公約数は、単元倍の違いを除いて一意的に定まる。すなわち、(α, β) は単元倍の違いだけとり方があり、一意的には定まらない。

証明 π は素数なので、 $(\pi, \alpha) = \pi$ または 1 である。

(i) $(\pi, \alpha) = \pi$ のときは、 π は α を割り切る。

(ii) $(\pi, \alpha) = 1$ のときは、定理 2.20 より、

$$\pi\xi + \alpha\eta = 1$$

を充たす $\xi, \eta \in \mathbb{Z}[i]$ が存在する。両辺に β を掛けると、

$$\beta\pi\xi + \beta\alpha\eta = \beta$$

となる。仮定より、π は $\alpha\beta$ を割り切るので、π は β を割り切る。

証明終

系 2.22 $\alpha \in \mathbb{Z}[i]$ とする。 α は単元倍と順序の違いを除いて、有限個の素数の積に一意的に表せる。

証明 $\alpha = \pi_1 \cdots \pi_n = \kappa_1 \cdots \kappa_m$ (各 π_i, κ_i は素数) とする。このとき、 $n = m$ であり、$\kappa_1 \cdots \kappa_m$ を並べ替えれば、任意の i に対して、 π_i と κ_i が同伴であることを n に関する帰納法で示す。

(i) $n = 1$ のとき、
$\pi_1 = \kappa_1 \cdots \kappa_m$ である。 π_1 は素数なので、 $m = 1$ となり、 $\pi_1 = \kappa_1$ となる。

(ii) $n \geq 2$ のとき、
π_1 は $\kappa_1 \cdots \kappa_m$ を割り切るので、系 2.21 より、ある κ_i があって、π_1 は κ_i を割り切る。$\kappa_1, \ldots, \kappa_m$ を並べ替えて、π_1 は κ_1 を割り切るとしてよい。$\kappa_1 = \epsilon\pi_1$ とおくことができ、κ_1 素数なので、ϵ は単数である。よって、

$$\pi_1\pi_2 \cdots \pi_n = \kappa_1\kappa_2 \cdots \kappa_m$$
$$\pi_1\pi_2 \cdots \pi_n = \epsilon\pi_1\kappa_2 \cdots \kappa_m$$
$$\pi_2 \cdots \pi_n = \epsilon\kappa_2 \cdots \kappa_m$$

帰納法の仮定より、 $n-1 = m-1$ であることがわかる。よって、 $n = m$ である。$\kappa_2 \cdots \kappa_n$ を並べ替えると、π_i と κ_i は同伴とすることができる。$(2 \leq i \leq n)$

よって、 $n = m$ で、並べ替えると、π_i と κ_i は同伴となった。$(1 \leq i \leq n)$ **証明終**

3　$x^2 + y^2 = a$の解

3.1　Gauss素数と有理素数

Gauss整数$a + bi$の中で、いかなるものが素数であるか。Gauss素数と有理素数にいかなる関係性があるのか。また、それらの基本的な性質について考察する。

補題 3.1 πを$\mathbb{Z}[i]$における素数、pをπで割り切れる最小の自然数とする。このとき、pは有理素数である。

証明 まず、

$$N(\pi) = \pi\overline{\pi} \in \mathbb{N}$$

であるので、πで割れる最小の自然数pは存在する。

πは単数ではないので、1はπで割り切れない。よって、$p \neq 1$である。

このとき、もし

$$p = ab \ \ (a, b \in \mathbb{Z}, p > a > 1, p > b > 1)$$

と表わせたとすると、aあるいはbが、πで割り切れることになる。これは、pの最小性に反する。

ゆえに、$a = 1$または$b = 1$となり、pは有理素数であることがわかる。　**証明終**

定理 3.2 $p \in \mathbb{Z}$を有理奇素数とする。

このときpは、

(1) $\mathbb{Z}[i]$においても素数である。

(2) $\mathbb{Z}[i]$のある素数πのノルムに等しい。すなわち、$p = \pi\overline{\pi}$と素因数分解できる。さらに、πと$\overline{\pi}$は同伴ではない。

のどちらかが成り立つ。[11]

証明 $p = \epsilon\pi_1\pi_2 \cdots \pi_k$を素因数分解とする（$\epsilon$は$\mathbb{Z}[i]$の単数, $\pi_1, \pi_2, \cdots, \pi_k$は$\mathbb{Z}[i]$の素数）。両辺のノルムをとると

$$\begin{aligned} p^2 &= N(\epsilon\pi_1\pi_2 \cdots \pi_k) \\ &= N(\pi_1)N(\pi_2) \cdots N(\pi_k) \end{aligned}$$

である。pは有理素数であるので、$k = 1$又は2であることが従う。

[11]有理奇素数pを割り切る素数πをとる。(1)のケースでは$N(\pi) = p^2$, (2)のケースでは$N(\pi) = p$に注意する。

(i) $k = 1$ のとき。

$p = \epsilon\pi_1$ より、p は素数である。

(ii) $k = 2$ のとき。

$p = N(\pi_1) = \pi_1\overline{\pi}_1$ となり、これがすなわち p の素因数分解で、p は二つの互いに共役な素数の積に等しい。(ここで、π が素数であることと $\overline{\pi}$ が素数であることは、同値であることに注意する。)

また、π_1 と $\overline{\pi}_1$ が同伴数ならば、$\overline{\pi}_1$ は $\pm\pi_1, \pm i\pi_1$ のいずれかと一致するはずである。$\pi_1 = x + yi$ とすれば、

(a) $\overline{\pi}_1 = \pi_1$ の場合、$x - yi = x + yi$ である。従って $y = 0$ となり $N(\pi_1) = x^2 = p$ より p が有理素数であることに反する。

(b) $\overline{\pi}_1 = -\pi_1$ の場合、$x - yi = -x - yi$ である。従って $x = 0$ となり $N(\pi_1) = y^2 = p$ より p が有理素数であることに反する。

(c) $\overline{\pi}_1 = i\pi_1$ の場合、$x - yi = -y + xi$ である。従って $y = -x$ となり $N(\pi) = x^2 + y^2 = 2x^2 = p$ より、p が奇素数であることに反する。

(d) $\overline{\pi}_1 = -i\pi_1$ の場合、$x - yi = y - xi$ である。従って $x = y$ となり $N(\pi) = 2x^2 = p$ より、p が奇素数であることに反する。

ゆえに π_1 と $\overline{\pi}_1$ は同伴数になり得ない。

証明終

注意 3.3 $p = 2$ に関しては、$2 = N(1 + i) = (1 + i)(1 - i)$ と素因数分解できる。以後、

$$\lambda = 1 - i$$

とする。$N(\lambda) = 2$ より、補題 2.16 によって、λ は素数である。$\overline{\lambda} = 1 + i = i\lambda$ より。λ と $\overline{\lambda}$ は互いに同伴である。$2 = \lambda\overline{\lambda} = i\lambda^2$ から、有理素数 2 はこの素数 λ の平方と同伴数である。

補題 3.4 $a + bi \in \mathbb{Z}[i]$ について、

$$\lambda \mid a + bi \Leftrightarrow a \equiv b \pmod 2$$

が成り立つ。

証明 ($\Leftarrow$) 次の二つの場合が考えられる。

(i) a, b がともに偶数のとき、$a + bi$ は 2 で割り切れ、λ は 2 の約数であるので $\lambda \mid a + bi$ が成り立つ。

(ii) a, b がともに奇数のとき、$a + bi - \lambda$ が 2 で割り切れるので $\lambda \mid a + bi$ が成り立つ。

($\Rightarrow$) a, b の一方が奇数、もう一方が偶数ならば $a - 1 \equiv b \pmod 2$
よって、$a+bi-1$ が λ で割り切れ、1 が λ で割れることになり矛盾する。 証明終

注意 3.5 $\lambda \nmid \xi$ なら、$\xi = 1+2\eta$ または $\xi = i+2\eta$ と書ける。よって、$\xi^2 \equiv \pm 1 \mod 4$, $\xi^4 \equiv 1 \mod 8$ となることに注意する。

定理 3.6 $p \in \mathbb{Z}$ を有理奇素数とする。このとき、

$$p \equiv 1 \pmod 4 \Leftrightarrow p = \pi\overline{\pi}\ （\pi, \overline{\pi} \text{は } \mathbb{Z}[i] \text{ の素数}）$$

が成立する。

証明 ($\Leftarrow$) $\pi = x + yi$ とおくと、

$$p = x^2 + y^2$$

ここで p が奇素数であることより、x, y のうち、一方が偶数、もう一方が奇数である。そのとき、4 を法として偶数の平方は 0 に合同であり、奇数の平方は 1 に合同であることから、$p \equiv 1 \pmod 4$ であることが従う。

($\Rightarrow$) $p \equiv 1 \pmod 4$ ならば平方剰余の第一補充法則より、$\left(\dfrac{-1}{p}\right) = 1$ が成り立つ。すなわち、-1 は p を法とする平方剰余であり、$r^2 + 1$ が p の倍数であるような有理整数 r が存在する。$r^2 + 1 = (r + i)(r - i)$ であるから、もし p が $\mathbb{Z}[i]$ の素数であれば、注意 2.5 によって、p は $r + i$ または $r + i$ を割り切る。明らかにそれは不可能なので、定理 3.2 より、

$$p = \pi\overline{\pi}$$

と表せる。 証明終

定理 3.2、注意 3.3 と定理 3.6 より、次がすぐにわかる。

系 3.7 $p \in \mathbb{Z}$ を有理奇素数とするとき、

$$p \equiv 3 \pmod 4 \Leftrightarrow p \text{ は } \mathbb{Z}[i] \text{ の素数}$$

3.2 $x^2 + y^2 = a$ の解

上記の結果を応用して有理整数に関する不定方程式

$$x^2 + y^2 = a \quad (a > 0) \tag{3}$$

の解を求めることができる。

注意 3.8 x, y が公約数 m を持つとき、$x = x'm, y = y'm$ とすれば、a は m^2 で割り切れることになり、また $a = a'm^2$ とすれば (3) は

$$x'^2 + y'^2 = a'$$

となるから、初めから (3) において

$$(x, y) = 1 \tag{4}$$

なる解のみを求めることとする。

定理 3.9 正の有理整数 a が互いに素なる二つの平方数に分解できるための必要十分条件は

$$a = 2^h p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k} \tag{5}$$

と書けることである。ただし、$h = 0$ または 1、$p_1 \equiv p_2 \equiv \cdots \equiv p_k \equiv 1 \pmod 4$ である。

また、このときの分解の表わし方は 2^{k-1} 通りである。つまり、

$$^{\#}\left\{(x^2, y^2) \,\middle|\, x, y \in \mathbb{Z}, x^2 + y^2 = a, x^2 \le y^2, (x, y) = 1\right\} = 2^{k-1} \tag{6}$$

が成り立つ。

証明 $a = x^2 + y^2$ と分解できたとすると、

$$a = (x + yi)(x - yi)$$

であるから、いま a が $4n + 3$ の形の有理素因数 q を持つとすれば、系 3.7 より q は $\mathbb{Z}[i]$ の素数であり、注意 2.5 より x かつ y を割り切る。これは (4) の条件に矛盾する。

また、a が有理素数 2 を h 個含むとすれば、$2 = i\lambda^2$ $(\lambda = 1 - i)$ であるから、λ^{2h} が $x + yi$ と $x - yi$ との間に分配されるが、$\overline{\lambda} = i\lambda$ であるので、$x + yi, x - yi$ はそれぞれ λ^h で割り切れる。もし $h > 1$ ならば、$x + yi$ は λ^2 従って 2 で割り切れ、x, y がともに 2 で割り切れることになって (4) に矛盾する。

ゆえに、方程式 (3) が (4) の条件のもとで解を持つためには、a が $4n + 3$ の形の素因数を含まないこと、また a が素因数 2 を含むなら 1 個に限ることが、必要な条件である。

逆に、a が (5) と表されるとする。定理 3.6 より、各 p_i は $\mathbb{Z}[i]$ の素数を用いて、

$$p_1 = \pi_1\overline{\pi}_1,\ p_2 = \pi_2\overline{\pi}_2,\ \cdots,\ p_k = \pi_k\overline{\pi}_k$$

と表せる。また、p_i はこの $\pi_i, \overline{\pi}_i$ とその同伴数以外の素数で割れない。

a が $4n + 1$ の形の有理素数 p をちょうど g 個含むとする。定理 3.6 より $\mathbb{Z}[i]$ の素数 $\pi, \overline{\pi}$ を用いて、$p = \pi\overline{\pi}$ と表せる。素数冪 $\pi^g, \overline{\pi}^g$ が $x + yi$ と $x - yi$ の間に分配されることになるが、もし $x + yi$ または $x - yi$ が $\pi\overline{\pi}$ で割り切れるならば、x と y がともに p で割り切れることになり、(4) に矛盾する。ゆえに $x + yi$ は π^g または $\overline{\pi}^g$ で割り切れなければならない。

(i) $h = 0$ のとき

$$\begin{aligned} a &= p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k} \\ &= (\pi_1\overline{\pi}_1)^{h_1}(\pi_2\overline{\pi}_2)^{h_2} \cdots (\pi_k\overline{\pi}_k)^{h_k} \end{aligned}$$

となるので、

$$x + yi = \pi_1^{h_1}\pi_2^{h_2} \cdots \pi_k^{h_k}$$

とすれば $a = x^2 + y^2$ を満たす。$a = x^2 + y^2$ を満たす $x + yi$ としては、因数のいくつかをそれらの共役数または同伴数でおき換えたものだけが考えられる。

同伴数でおき換えた場合、$x + yi$ も同伴数になるだけであり、(6) の左辺は本質的に増えることはない。異なる (x^2, y^2) が得られるのは、因数 $\pi_i (1 \leqq i \leqq k)$ のいくつかを $\overline{\pi}_i$ でおき換えたものだけである。しかし、すべての因数を共役数でおき換えれば、

$$\begin{aligned} \overline{\pi}_1^{h_1}\overline{\pi}_2^{h_2} \cdots \overline{\pi}_k^{h_k} &= \overline{\pi_1^{h_1}\pi_2^{h_2} \cdots \pi_k^{h_k}} \\ &= \overline{x + yi} \\ &= x - yi \end{aligned}$$

となり、元の数の共役数となる。従って、異なる $x^2 + y^2$ は 2^{k-1} 通りである。$x + iy$ の同伴数とその共役として、$\pm x \pm iy, \pm y \pm ix$ の 8 つの数が出てくる。よって、(6) の左辺の個数を計算するときは、同伴と共役を同一視する必要がある。

(ii) $h = 1$ のとき

$$\begin{aligned} a &= 2p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k} \\ &= \lambda\overline{\lambda}(\pi_1\overline{\pi}_1)^{h_1}(\pi_2\overline{\pi}_2)^{h_2} \cdots (\pi_k\overline{\pi}_k)^{h_k} \end{aligned}$$

となるので、

$$x + yi = \lambda\pi_1^{h_1}\pi_2^{h_2} \cdots \pi_k^{h_k}$$

とすればよい。$\overline{\lambda} = i\lambda$ より、λ を $\overline{\lambda}$ に変えても $x + yi$ は同伴数に変わるだけだから、異なる $x^2 + y^2$ はやはり 2^{k-1} 通りである。

証明終

例 **3.10**

$$F(a) := \left\{ (x^2, y^2) \,\middle|\, x, y \in \mathbb{Z}, x^2 + y^2 = a, x^2 \leq y^2, (x, y) = 1 \right\}$$

$$G(a) := \left\{ (x^2, y^2) \,\middle|\, x, y \in \mathbb{Z}, x^2 + y^2 = a, x^2 \leq y^2 \right\}$$

とおき、例えば $a = 3^2 \cdot 5^3$ とすれば

$$G(3^2 \cdot 5^3) = F(3^2 \cdot 5^3) \coprod F(5^3) \coprod F(3^2 \cdot 5) \coprod F(5)$$

が成り立ち、$F(3^2\cdot 5^3) = F(3^2\cdot 5) = \phi, {}^{\#}F(5^3) = {}^{\#}F(5) = 1$ となる。よって ${}^{\#}G(3^2\cdot 5^3) = 2$ である。

実際、$5^3 = 2^2 + 11^2, 5 = 1^2 + 2^2$ と分解できるので、

$$3^2 \cdot 5^3 = 2^2 \cdot 3^2 + 3^2 \cdot 11^2 = 3^2 \cdot 5^2 + 2^2 \cdot 3^2 \cdot 5^2$$

と 2 通りの平方数の和に分解できる。

4 Fermat の最終定理 ($n = 4$ の場合)

Fermat の最終定理とは、$x^n + y^n = z^n$ $(n > 2)$ が正の整数解を持たないという主張である。この章では、$n = 4$ の時に上記の式が正の整数解を持たないことを確かめてみる。

より一般に方程式、

$$\alpha^4 + \beta^4 = \gamma^2, (\alpha, \beta, \gamma \neq 0) \tag{7}$$

が $\mathbb{Z}[i]$ において解を持たないことを証明する。

証明 (7) が解を持つとして、背理法で矛盾を導く。$\mathbb{Z}[i]$ では、素因数分解の一意性が成り立つので

$$(\alpha, \beta) = 1,\ (\alpha, \gamma) = 1,\ (\beta, \gamma) = 1 \tag{8}$$

であると仮定してよい。

$\lambda \nmid \xi$ を満たせば、注意 3.5 によって、

$$\xi^2 \equiv \pm 1 \pmod 4 \tag{9}$$

$$\xi^4 \equiv 1 \pmod 8 \tag{10}$$

が成立することに注意する。次の 2 つの場合に分けて考える。

(i) $\lambda \nmid \alpha$ かつ $\lambda \nmid \beta$ の場合。

(10) より

$$\alpha^4 + \beta^4 \equiv 2 \pmod 8$$

である。故に

$$\gamma^2 \equiv 2 \pmod 8 \tag{11}$$

である。よって、$i\lambda^2 = 2$ より $\lambda \mid \gamma$ である。$\gamma = \lambda\nu$ とおく。(11) より

$$2 \equiv \gamma^2 = \lambda^2\nu^2 = -2i\nu^2 \pmod 8$$

であるが、2 で割ると

$$1 \equiv -i\nu^2 \pmod 4$$

となり、i をかけて

$$\nu^2 \equiv i \pmod 4 \tag{12}$$

である。

このとき、$(\lambda, \nu) = 1$ である。そうでないと仮定して、$\nu = \lambda\nu$ とおくと

$$i \equiv \nu^2 = \lambda^2\nu'^2 = -2i\nu'^2 \pmod 4$$

であるが、両辺に $-i$ をかけると

$$1 \equiv -2\nu'^2 \pmod 4$$

となる。よって

$$1 \equiv 0 \pmod 2$$

となり矛盾する。故に、$(\lambda, \nu) = 1$ である。

しかし、(9) と (12) より

$$i \equiv \pm 1 \pmod 4$$

であり、これに矛盾である。

よって、(i) は起こらない。

(ii) $\lambda \mid \alpha$ かつ $\lambda \nmid \beta$ の場合。ここで、$(\alpha, \beta) = 1$ より、α, β の両方が λ で割れることはないことに注意する。($\lambda \nmid \alpha$ かつ $\lambda \mid \beta$ なら、α と β を交換する。)

$$\alpha = \lambda^m\alpha_0\ , (\alpha_0, \lambda) = 1,\ (\beta, \lambda) = 1,\ (\gamma, \lambda) = 1,\ m > 0$$

とおく。すると (7) は

$$\lambda^{4m}\alpha_0^4 + \beta^4 = \gamma^2$$

である。ここで ϵ を単数、つまり $\epsilon = \pm 1, \pm i$ とし、$m \in \mathbb{N}$ として

$$\epsilon\lambda^{4m}\alpha_0^4 + \beta^4 = \gamma^2 \tag{13}$$

が α_0, β, γ の 2 つずつが互いに素かつ、$\lambda \nmid \alpha_0,\ \lambda \nmid \beta,\ \lambda \nmid \gamma$ を満たす解を持たないことを示す。

(13) が解を持つとして、背理法で示す。

(13) が成り立つならば、

$$(\gamma - \beta^2)(\gamma + \beta^2) = \epsilon\lambda^{4m}\alpha_0^4 \tag{14}$$

である。ここで、$\gamma - \beta^2,\ \gamma + \beta^2$ の公約数は $2\gamma,\ 2\beta^2$ の公約数でなければならない。それは、

$$\begin{aligned} 2\gamma &= (\gamma - \beta^2) + (\gamma + \beta^2) \\ 2\beta^2 &= -(\gamma - \beta^2) + (\gamma + \beta^2) \end{aligned}$$

より明らかであろう。

また、$(\beta, \gamma) = 1$ であるから、公約数は 2 の約数でなければならない。$\mathbb{Z}[i]$ では 2 を割り切る素数は λ のみである。$2 = i\lambda^2$ に注意すれば $GCD(\gamma+\beta^2, \gamma-\beta^2)$ は、$1,\ \lambda,\ \lambda^2$ のどれかである。(14) より $\gamma-\beta^2,\ \gamma+\beta^2$ の片方は λ^2 で割れる。しかし、$\gamma+\beta^2 = (\gamma-\beta^2)+2\beta^2$ より、片方が λ^2 で割れれば、もう一方も λ^2 で割れる。よって、$(\gamma-\beta^2, \gamma+\beta^2) = \lambda^2$ である。このとき、

$$\begin{aligned} \gamma+\beta^2 &= \epsilon_1\lambda^2\beta'^4 \\ \gamma-\beta^2 &= \epsilon_2\lambda^{4m-2}\alpha'^4 \end{aligned}$$

とおく。($\lambda^2 \parallel \gamma+\beta^2$ または $\lambda^2 \parallel \gamma-\beta^2$ なので、必要なら β を $i\beta$ にとりかえ、$\lambda^2 \parallel \gamma+\beta^2$ としてよい。ただし、ϵ_1, ϵ_2 は単数で、$(\alpha', \beta') = 1, (\alpha', \lambda) = 1, (\beta', \lambda) = 1$ であり、$(\alpha', \beta) = 1, (\beta', \beta) = 1$ に注意する。)

従って、

$$2\beta^2 = \epsilon_1\lambda^2\beta'^4 - \epsilon_2\lambda^{4m-2}\alpha'^4$$

である。両辺を 2 で割って

$$\beta^2 = \vartheta\beta'^4 + \eta\lambda^{4(m-1)}\alpha'^4 \tag{15}$$

である。ただし、$\vartheta = \frac{\epsilon_1\lambda^2}{2} = -i\epsilon_1,\ \ \eta = -\frac{\epsilon_2\lambda^2}{2} = i\epsilon_2$ は単数である。

m に関する数学的帰納法で証明する。

$m = 1$ のときは、$\beta^2 = \vartheta\beta'^4 + \eta\alpha'^4$ である。$(\lambda, \beta') = 1, (\lambda, \alpha') = 1$ より $\lambda \nmid \vartheta\beta'^4$, $\lambda \nmid \eta\alpha'^4$ であり、従って $\lambda \mid \vartheta\beta'^4 + \eta\alpha'^4$ となる。すると、補題 3.4 により、$\lambda \mid \beta$ となり矛盾する。故に、$m = 1$ のときは解を持たない。

次に $m > 1$ と仮定する。(15) が成り立つので、$\lambda^{4(m-1)}$ は 4 で割れる。mod 4 で考えると、

$$\beta^2 \equiv \vartheta\beta'^4 \pmod 4$$

であり、故に (9), (10) によって

$$\pm 1 \equiv \vartheta \pmod 4$$

となる。ϑ は単数 ($\pm 1,\ \ \pm i$ のどれか) であるから、

$$\vartheta = \pm 1$$

である。故に (15) は

$$\pm\beta^2 = \beta'^4 + \eta'\lambda^{4(m-1)}\alpha'^4 \ \ (\eta' = \pm\eta)$$

になる。$\pm\beta^2$ は β^2 または $(i\beta)^2$ に等しいから、β または $i\beta$ を γ' と書けば、

$$\gamma'^2 = \beta'^4 + \eta'\lambda^{4(m-1)}\alpha'^4$$

となる。η' は単数であり、α', β', γ' は二つずつ互いに素で、どれも λ で割れない。故に (13) が指数 m のときに解を持つならば、指数 $m-1$ のときにも解を持たなければならない。 証明終

5 整数環 $\mathbb{Z}[\omega]$ の性質

フェルマーの最終定理の $n=3$ の場合を証明するために、まずは $\mathbb{Z}[\omega]$ の性質をまとめておく。この章では 1 の原始 3 乗根を ω で表す。つまり、

$$\omega = \frac{-1+\sqrt{-3}}{2}$$

とおく。このとき、

$$\overline{\omega} = \omega^2 = \frac{-1-\sqrt{-3}}{2}$$

である。

$$\mathbb{Q}(\sqrt{-3}) = \{x+y\omega | x, y \in \mathbb{Q}\}$$

とおくと、$\mathbb{Q}(\sqrt{-3})$ は四則で閉じている。実際、$x, x', y, y' \in \mathbb{Q}$ とすると、

$$\begin{aligned}
(x+y\omega) \pm (x'+y'\omega) &= (x \pm x') + (y \pm y')\omega \\
(x+y\omega)(x'+y'\omega) &= xx' + (xy'+x'y)\omega + yy'\omega^2 \\
&= xx' + (xy'+x'y)\omega + yy'(-\omega-1) \\
&= (xx'-yy') + (xy'+x'y-yy')\omega \\
\frac{x'+y'\omega}{x+y\omega} &= \frac{(x'+y'\omega)(x+y\overline{\omega})}{(x+y\omega)(x+y\overline{\omega})} \\
&= \frac{(x'+y'\omega)\{x+y(-\omega-1)\}}{x^2+xy(\omega+\overline{\omega})+y^2\omega\overline{\omega}} \\
&= \frac{(x'+y'\omega)(x-1-y\omega)}{x^2-xy+y^2}
\end{aligned}$$

である。有理数は四則で閉じているので、これらも $\mathbb{Q}(\sqrt{-3})$ の元となる。[12]

この章において、

$$\mathbb{Z}[\omega] = \{x+y\omega | x, y \in \mathbb{Z}\}$$

を $\mathbb{Q}(\sqrt{-3})$ の整数環と言うことにする。以下 $\mathbb{Z}[\omega]$ の元を整数、$\mathbb{Z}$ の元を有理整数と表すことにする。

[12] ここで $x, y \in \mathbb{Q}$ のときに、$x=y=0$ であることと $x+y\omega=0$ であることは同値である。$x+y\omega \neq 0$ のとき、$x+y\overline{\omega} \neq 0$ である。また、$x+y\omega \neq 0$ であるとき

$$x^2-xy+y^2 = (x+\frac{y}{2})^2 + \frac{3}{4}y^2 > 0$$

である。

注意 5.1 $\overline{\omega} = -\omega - 1$ なので、$\overline{\omega}$ は整数である。

定義 5.2 α, β を整数、$\beta \neq 0$ とする。α/β が整数のとき、α は β で割り切れるという。このとき、α を β の倍数、β を α の約数といい、$\beta|\alpha$ と書く。

注意 5.3 a, b, c を有理整数とするとき、$\mathbb{Z}[\omega]$ において $a + b\omega$ が c で割り切れることと、$\mathbb{Z}$ において a と b が c で割り切れることは同値である。

証明 $a + b\omega$ が c で割り切れるとすると、$d, e \in \mathbb{Z}$ として、

$$a + b\omega = c(d + e\omega) = cd + ce\omega$$

となる。よって、$a = cd, b = ce$ であるので、a と b は c で割り切れる。

逆に、$a = cd, b = ce$ と表せたとき、$a + b\omega = c(d + e\omega)$ となるので、$a + b\omega$ は c で割り切れる。 **証明終**

このことから、$a, b, c \in \mathbb{Z}$ であるとき、$\mathbb{Z}[\omega]$ において $a \equiv b \pmod{c}$ であることと、$\mathbb{Z}$ において $a \equiv b \pmod{c}$ であることは同値である。また、$\mathbb{Z}[\omega]$ において b が a で割り切れることと、$\mathbb{Z}$ において b が a で割り切れることも同値である。

定義 5.4 $\alpha = x + y\omega$ とするとき、$|\alpha|^2 = \alpha\overline{\alpha}$ を α のノルムといい、$N(\alpha)$ と表す。このとき、$N(\alpha) = \alpha\overline{\alpha} = (x + y\omega)(x + y\overline{\omega}) = x^2 - xy + y^2$ であるので、$N(\alpha)$ は非負整数である。

注意 5.5 $\alpha = 0$ であることと、$N(\alpha) = 0$ であることは同値である。

注意 5.6 $\alpha = \beta\gamma$ であるとき、$N(\alpha) = N(\beta)N(\gamma)$ である。
実際、

$$N(\alpha) = \alpha\overline{\alpha} = \beta\gamma\overline{\beta\gamma} = \beta\overline{\beta}\gamma\overline{\gamma} = N(\beta)N(\gamma)$$

である。

定義 5.7 α を整数とする。α が 1 を割り切るとき、α を $\mathbb{Z}[\omega]$ の単数という。$\mathbb{Z}[\omega]$ の単数全体の集合を $\mathbb{Z}[\omega]^\times$ で表す。

定理 5.8 α を整数とするとき、次の 3 つは同値である。

(i) $\alpha \in \mathbb{Z}[\omega]^\times$

(ii) $\alpha = \pm 1, \pm\omega, \pm\omega^2$

(iii) $N(\alpha) = 1$

証明 (i)⇒(ii) $\epsilon = x + y\omega \in \mathbb{Z}[\omega]^\times$ とする。すると ϵ が 1 を割り切るので、ある整数 ϵ' が存在して、$\epsilon\epsilon' = 1$ を満たす。よって $N(\epsilon\epsilon') = N(1)$ より、$N(\epsilon)N(\epsilon') = 1$ である。$N(\epsilon), N(\epsilon')$ は非負整数なので、$N(\epsilon) = 1$ である。よって、

$$\begin{aligned} 1 = N(\epsilon) &= \epsilon\overline{\epsilon} \\ &= (x + y\omega)(x + y\overline{\omega}) \\ &= x^2 - xy + y^2 \end{aligned}$$

となり、両辺に 4 をかけると

$$4x^2 - 4xy + 4y^2 = 4$$

なので、

$$(2x - y)^2 + 3y^2 = 4$$

となる。$2x - y, y$ は有理整数なので、この式を満たす x, y は、

$$\begin{cases} 2x - y &= \pm 2 \\ y &= 0 \end{cases}$$

または、

$$\begin{cases} 2x - y &= \pm 1 \\ y &= \pm 1 \end{cases}$$

を満たす。これを解くと、

$$(x, y) = (1, 0), (-1, 0), (1, 1), (0, -1), (0, 1), (-1, -1)$$

なので、

$$\begin{aligned} \epsilon &= x + y\omega \\ &= \pm 1, \pm\omega, \pm(1 + \omega) \\ &= \pm 1, \pm\omega, \mp\omega^2 \end{aligned}$$

となる。
(ii)⇒(iii) $\alpha = \pm 1$ のとき $N(\alpha) = (\pm 1)\cdot(\pm 1) = 1$、$\alpha = \pm\omega$ のとき $N(\alpha) = (\pm\omega)\cdot(\pm\overline{\omega}) = (\pm\omega)\cdot(\pm\omega^2) = 1$、$\alpha = \pm\omega^2$ のとき $N(\alpha) = (\pm\omega^2)\cdot(\pm\overline{\omega^2}) = (\pm\omega^2)\cdot(\pm\omega) = 1$ である。
(iii)⇒(i) $N(\alpha) = 1$ とすると、$\alpha\overline{\alpha} = 1$ なので、α は 1 を割り切る。よって α は単数である。 **証明終**

定義 5.9 α, β を整数とする。α と β の公約数が単数のみのとき、α と β は互いに素という。

定義 5.10 α,β を整数とする。α/β が単数のとき、α と β を互いに同伴 *(α は β の同伴数)* という。

定義 5.11 α を整数、$N(\alpha) \geq 2$ とする。α の約数が単数または α の同伴数のみのとき、α を $\mathbb{Z}[\omega]$ の素数という。

以下 $\mathbb{Z}$ の素数を有理素数、$\mathbb{Z}[\omega]$ の素数を単に素数と表すことにする。

補題 5.12 $N(\alpha)$ が有理素数ならば、α は素数である。

証明 β, γ を整数、$\alpha = \beta\gamma$ とすると、$N(\alpha) = N(\beta)N(\gamma)$ である。$N(\alpha)$ は有理素数なので、$N(\beta) = 1$ または $N(\beta) = 1$ となるので、β または γ は単数である。よって α は素数である。 **証明終**

定理 5.13 α を整数とする。$N(\alpha) \geq 2$ ならば、α は有限個の素数の積で表せる。

証明 $N(\alpha)$ に関する帰納法で示す。
$N(\alpha) = 2$ のとき、補題 5.12 より従う。
$N(\alpha) > 2$ のとき、α が素数でないとしてよい。すると、$\alpha = \beta\gamma,\ N(\beta) \geq 2,\ N(\gamma) \geq 2$ と書ける。$N(\alpha) = N(\beta)N(\gamma)$ なので、$N(\beta) < N(\alpha),\ N(\gamma) < N(\alpha)$ である。帰納法の仮定より、β, γ は有限個の素数の積で表せる。従って $\alpha = \beta\gamma$ も有限個の素数の積で表せる。 **証明終**

定理 5.14 α,β を整数、$\beta \neq 0$ とする。すると、$\alpha = \beta\kappa + \rho$ かつ $|\rho| < |\beta|$ を満たす整数 κ, ρ が存在する。

証明 複素平面上において、$\mathbb{Z}[\omega]$ の元は 120° の角をもつひし形を基本とする格子点で表される。$\frac{\alpha}{\beta}$ はこの格子の、あるひし形に属する。このひし形の左上と右下の頂点を中心とする半径 1 の円をかくと、右上と左下の頂点以外のひし形の円周上の点、および内部の点は円内に含まれる。よって $\frac{\alpha}{\beta}$ は、ある頂点から 1 より小さい距離にある。その頂点を κ とおくと、

$$\left|\frac{\alpha}{\beta} - \kappa\right| < 1$$

である。$\rho = \alpha - \beta\kappa$ とおくと ρ は整数で、$\alpha = \beta\kappa + \rho$ かつ

$$\left|\frac{\rho}{\beta}\right| = \left|\frac{\alpha - \beta\kappa}{\beta}\right| = \left|\frac{\alpha}{\beta} - \kappa\right| < 1$$

なので、$|\rho| < |\beta|$ を満たす。 **証明終**

定理 5.14 を用いて、整数 α,β の最大公約数を求めることができる。

$$\alpha = \kappa\beta + \beta_1,\ |\beta_1| < |\beta|$$

とする。$|\beta_1| < |\beta|$ より、$N(\beta_1) < N(\beta)$ である。$N(\beta_1) \neq 0$ なら

$$\beta = \kappa_1\beta_1 + \beta_2,\ N(\beta_2) < N(\beta_1)$$

を充たす κ_1, β_2 が存在する。これを続けると、真の減少列

$$N(\beta) > N(\beta_1) > N(\beta_2) > \cdots$$

を得る。ノルムは非負整数なので、この減少列は止まる。つまり、$\beta_{n+1} = 0$ を充たす自然数 n がある。すなわち

$$\begin{aligned}
\alpha &= \kappa\beta + \beta_1 \\
\beta &= \kappa_1\beta_1 + \beta_2 \\
\beta_1 &= \kappa_2\beta_2 + \beta_3 \\
&\vdots \\
\beta_{n-2} &= \kappa_{n-1}\beta_{n-1} + \beta_n \\
\beta_{n-1} &= \kappa_n\beta_n
\end{aligned}$$

となる。このとき $\beta_{n-1} = \kappa_n\beta_n$ より、β_n は β_{n-1} の約数である。$\beta_{n-2} = \kappa_{n-1}\beta_{n-1} + \beta_n$ より、β_n は β_{n-2} の約数である。これを繰り返すと、β_n は β と α の約数であるので、β_n は β と α の公約数である。
また、α と β の任意の公約数を δ とすると、$\alpha = \kappa\beta + \beta_1$ より $\beta_1 = \alpha - \kappa\beta$ なので、δ は β_1 の約数である。$\beta = \kappa_1\beta_1 + \beta_2$ より $\beta_2 = \beta - \kappa_1\beta_1$ なので、δ は β_2 の約数である。これを繰り返すと、δ は β_n の約数である。

従って、β_n は α と β の最大公約数である。このとき $\beta_n = \gcd(\alpha, \beta)$ と表す。$\gcd(\alpha, \beta) = 1$ のとき、単に $(\alpha, \beta) = 1$ と書く。

定理 5.15 α, β を整数とする。すると整数 ξ, η が存在して、$\alpha\xi + \beta\eta = \gcd(\alpha, \beta)$ を満たす。

証明 上記の最大公約数を求める過程において、$\beta_{-1} = \alpha, \beta_0 = \beta$ とおく。このとき、任意の $i(-1 \leq i \leq n-2)$ において、

$$\beta_i\xi + \beta_{i+1}\eta = \beta_n \tag{16}$$

を満たす整数 ξ, η が存在することを i に関する上からの帰納法で示す。
$i = n-2$ のとき、$\beta_{n-2} = \kappa_{n-1}\beta_{n-1} + \beta_n$ より $\beta_{n-2} - \kappa_{n-1}\beta_{n-1} = \beta_n$ なので (16) を満たす。
$i < n-2$ のとき、$i+1$ 以上では (16) が成り立つと仮定する。すると、

$$\beta_{i+1}\xi + \beta_{i+2}\eta = \beta_n$$

を満たす整数ξ,ηが存在する。$\beta_i = \kappa_{i+1}\beta_{i+1} + \beta_{i+2}$より$\beta_{i+2} = \beta_i - \kappa_{i+1}\beta_{i+1}$なので、これを代入すると

$$\beta_{i+1}\xi + (\beta_i - \kappa_{i+1}\beta_{i+1})\eta = \beta_n$$

より

$$\beta_i\eta + \beta_{i+1}(\xi - \kappa_{i+1}\eta) = \beta_n$$

となり、iのときも(16)を満たす。従って$i = -1$とすると定理5.15を満たす。

証明終

定理 5.16 α,β,γを整数、$(\alpha,\beta) = 1$とする。$\alpha\gamma$がβで割り切れるならば、γがβで割り切れる。

証明 定理5.15より、

$$\alpha\xi + \beta\eta = 1$$

を満たす整数ξ,ηが存在する。両辺にγをかけると

$$\alpha\gamma\xi + \beta\gamma\eta = \gamma$$

である。$\alpha\gamma$はβで割り切れるので、$\alpha\gamma\xi + \beta\gamma\eta$は$\beta$で割り切れる。よって$\gamma$が$\beta$で割り切れる。

証明終

定理 5.17 α,β,γを整数、γを素数とする。$\alpha\beta$がγで割り切れるならば、αかβのどちらかはγで割り切れる。

証明 $(\alpha,\gamma) = 1$のとき、定理5.16よりβがγで割り切れる。
$(\alpha,\gamma) \neq 1$のとき、単数以外のαとγの公約数が存在する。γは素数なので、公約数は$\epsilon\gamma$(ただしϵは単数)である。よってαは$\epsilon\gamma$で割り切れるので、αはγで割り切れる。

証明終

定理 5.18 αを整数とする。$N(\alpha) \geq 2$ならば、αは有限個の素数の積に順序と単数の積の違いを除いて一意的に表せる。

証明 $\alpha = \pi_1 \cdots \pi_n = \kappa_1 \cdots \kappa_m(\pi_1,\ldots,\pi_n,\kappa_1,\ldots,\kappa_m$は素数)とするとき、$n = m$で、順序を入れかえれば、任意の$i(1 \leq i \leq n)$に対し$\pi_i$と$\kappa_i$は同伴となることを、$n$に関する帰納法で示す。
$n = 1$のとき、$\pi_1 = \kappa_1 \cdots \kappa_m$で、$\pi_1$は素数なので$m = 1$で$\pi_1 = \kappa_1$である。
$n > 1$のとき、$\pi_1 \cdots \pi_n = \kappa_1 \cdots \kappa_m$とする。$\kappa_1 \cdots \kappa_m$は$\pi_1$で割り切れるので、定理5.17より、ある$i(1 \leq i \leq m)$があって$\kappa_i$が$\pi_1$で割り切れる。並べかえて$\kappa_1$が$\pi_1$で割り切れるとする。$\kappa_1$は素数なので、$\kappa_1 = \epsilon\pi_1$(ただし$\epsilon$は単数)と書ける。よって

$$\pi_1 \cdots \pi_n = (\epsilon\pi_1)\kappa_2 \cdots \kappa_m$$

であるので、両辺を π_1 で割ると

$$\pi_2 \cdots \pi_n = \epsilon\kappa_2 \cdots \kappa_m$$

となる。すると帰納法の仮定より、$n-1=m-1$ であり、順番を入れかえると任意の $i(2 \le i \le n)$ に対し π_i と κ_i は同伴となる。従って $n=m$ で、任意の $i(1 \le i \le n)$ に対し π_i と κ_i は同伴となる。 証明終

命題 5.19 p を有理素数とする。すると p は $\mathbb{Z}[\omega]$ においても素数であるかまたは、$p=\pi\overline{\pi}$（π は素数）である。

証明 $p=\pi\pi_1\cdots\pi_n$ を $\mathbb{Z}[\omega]$ における素因数分解とする。すると $N(\pi)N(\pi_1\cdots\pi_n)=N(p)=p^2$ より、p^2 は $N(\pi)$ で割り切れる。π は素数なので $N(\pi)\neq 1$ であり、p は有理素数なので $N(\pi)=p^2$ または $N(\pi)=p$ である。
$N(\pi)=p^2$ のときは、$p=\pi\kappa$ とおくと、$N(\pi)N(\kappa)=N(p)=p^2$ なので $N(\kappa)=1$ である。よって κ は単数である。ゆえにこのとき p は $\mathbb{Z}[\omega]$ でも素数である。
$N(\pi)=p$ のとき、$N(\pi)=\pi\overline{\pi}=p$ である。 証明終

定理 5.20 (1) 3 は素数 $\lambda=1-\omega$ の平方と同伴である。

(2) p を有理素数、$p\neq 3$ とする。

(i) $p\equiv 1 \pmod 3$ であることと、p が 2 つの素数の積で表せることは同値である。また、このとき、p を分解する 2 つの素数は同伴でない。

(ii) $p\equiv 2 \pmod 3$ であることと、p が $\mathbb{Z}[\omega]$ においても素数であることは同値である。

証明

(1)

$$\begin{aligned} N(\lambda) &= \lambda\overline{\lambda} \\ &= (1-\omega)(1-\overline{\omega}) \\ &= 1-(\omega+\overline{\omega})+\omega\overline{\omega} \\ &= 1+1+1 \\ &= 3 \end{aligned}$$

であるので、補題 5.12 より λ は素数である。
また、

$$\begin{aligned} 1-\overline{\omega} &= 1-\omega^2 \\ &= (1+\omega)(1-\omega) \\ &= -\omega^2(1-\omega) \end{aligned}$$

であるので

$$\begin{aligned} 3 &= (1-\omega)(1-\overline{\omega}) \\ &= -\omega^2(1-\omega)^2 \\ &= -\omega^2\lambda^2 \end{aligned}$$

となり、$-\omega^2$ は単数なので、3 は λ^2 と同伴である。

(2) (i) p を有理素数、$p \neq 3$ とする。

主張 5.21 $p \equiv 1 \pmod 3$ であることと、$p = \pi\overline{\pi}$（π は素数）であることは同値である。

証明 $p = \pi\overline{\pi}$（π は素数）、$\pi = a - b\omega$（$a, b \in \mathbb{Z}$）と書けたとする。すると

$$\begin{aligned} p &= \pi\overline{\pi} \\ &= (a-b\omega)(a-b\overline{\omega}) \\ &= a^2 - (\omega+\overline{\omega})ab + b^2\omega\overline{\omega} \\ &= a^2 + ab + b^2 \end{aligned}$$

両辺を 4 倍すると

$$\begin{aligned} 4p &= 4(a^2+ab+b^2) \\ &= (2a+b)^2 + 3b^2 \end{aligned}$$

であるので

$$(2a+b)^2 \equiv 4p \pmod 3$$

となる。よって

$$p \equiv 4p \equiv (2a+b)^2 \equiv 1 \pmod 3$$

となる。
逆に、$p \equiv 1 \pmod 3$ とするとき、

$$\left(\frac{p}{3}\right) = 1$$

である。一方、平方剰余の相互法則より

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}},$$

よって

$$(-1)^{\frac{p-1}{2}} = \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right)$$

である。また第一補充法則より、$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ なので、

$$\begin{aligned}\left(\frac{-3}{p}\right) &= \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right)\\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\\ &= (-1)^{p-1}\\ &= 1\end{aligned}$$

である。よって、ある有理整数 r が存在して、$r^2 \equiv -3 \pmod{p}$ を満たす。このとき、$\delta = \gcd(p, r - \sqrt{-3})$ とおく。ここで、命題 5.19 より p は $\mathbb{Z}[\omega]$ における素数であるか、$p = \pi\overline{\pi}$（π は素数）と表せるかのどちらかであることに注意する。δ は p を割り切るので、p が $\mathbb{Z}[\omega]$ の素数であるときは、$\delta = 1$ または $\delta = p$ である。$p = \pi\overline{\pi}$（π は素数）であるときは、$\delta = 1, \delta = \pi, \delta = \overline{\pi}$ または $\delta = p$ である。従って、

$$\delta = \pi\text{（ただし } p = \pi\overline{\pi}\text{、}\pi\text{は素数）}, \ \delta = 1, \text{ または } \delta = p$$

となる。

$\delta = 1$ とする。$\delta' = \gcd(p, r + \sqrt{-3})$ とおくと、共役をとることにより $\overline{\delta'}$ は p と $r - \sqrt{-3}$ を割り切る。今 $\delta = 1 = \gcd(p, r - \sqrt{-3})$ より、$\overline{\delta'}$ は単数である。よって δ' は単数なので、$\gcd(p, r + \sqrt{-3}) = 1$ である。従って、

$$\gcd(p, (r + \sqrt{-3})(r - \sqrt{-3})) = \gcd(p, r^2 + 3) = 1$$

であるが、$r^2 \equiv -3 \pmod{p}$ なので $r^2 + 3$ が p で割り切れることに矛盾する。よって $\delta = 1$ とはならない。

$\delta = p$ とするとき、$\sqrt{-3} = 1 + 2\omega$ なので、$r - \sqrt{-3} = (r - 1) - 2\omega$ が p で割り切れる。よって $r - 1$ と 2 が p で割り切れる。2 が有理素数 p で割り切れることから $p = 2$ であるが、これは $p \equiv 1 \pmod{3}$ であることに矛盾する。よって $\delta = p$ とはならない。

故に、$\delta = \pi$、ただし π は素数で $p = \pi\overline{\pi}$ となる。　　証明終

さらにこのとき、π と $\overline{\pi}$ が同伴でないことを示す。

$\delta = \pi = \gcd(p, r - \sqrt{-3})$ の共役をとると、$\overline{\pi} = \gcd(p, r + \sqrt{-3})$ であるので、

$$\gcd(\pi, \overline{\pi}) = \gcd(p, r - \sqrt{-3}, r + \sqrt{-3})$$

となる。π は素数なので、

$$\gcd(\pi, \overline{\pi}) = 1 \text{ または } \pi$$

である。$\gcd(\pi,\overline{\pi}) = \pi$ とするとき、$\gcd(p, r-\sqrt{-3}, r+\sqrt{-3}) = \pi$ なので、$r+\sqrt{-3}$ が π で割り切れる。よって $(r+\sqrt{-3})+(r-\sqrt{-3}) = 2r$ が π で割り切れるので、$N(2r) = (2r)^2$ が $N(\pi) = \pi\overline{\pi} = p$ で割り切れる。よって $2r$ が p で割り切れるが、$p \equiv 1 \pmod 3$ より 2 は p で割り切れないので、r が p で割り切れる。しかしこれは $r^2 \equiv -3 \pmod p$ であることに矛盾する。従って $\gcd(\pi,\overline{\pi}) = \pi$ は正しくない。よって $\gcd(\pi,\overline{\pi}) = 1$ であるので、π と $\overline{\pi}$ は同伴でない。

(ii) 命題 5.19 と主張 5.21 より従う。 証明終

命題 5.22 x, y を有理整数とする。このとき、$x \equiv y \pmod 3$ であるならば、$x - y\omega$ が $\lambda = 1-\omega$ で割り切れる。

証明 $x \equiv y \pmod 3$ とすると、$x-y$ が 3 で割り切れる。$3 = -\omega^2\lambda^2$ なので $x-y$ が λ で割り切れる。また $\lambda = 1-\omega$ より $\omega = 1-\lambda$ なので、

$$x - y\omega = x - y(1-\lambda) = (x-y) + y\lambda$$

である。$x-y$ と $y\lambda$ は λ で割り切れるので、$(x-y)+y\lambda = x-y\omega$ は λ で割り切れる。 証明終

注意 5.23 $\xi = x - y\omega$（x, y は有理整数）とおくと、命題 *5.22* の対偶より、ξ が λ で割り切れないならば $x \not\equiv y \pmod 3$ である。このとき、$x - y \equiv \pm 1 \pmod 3$ なので $x - y = \pm 1 + 3\eta$（η は整数）とおくと、

$$\begin{aligned}\xi &= x - y\omega \\ &= (x-y) + y\lambda \\ &= \pm 1 + 3\eta + y\lambda \\ &= \pm 1 + \lambda\zeta \quad （ただし \zeta = -\omega^2\lambda\eta + y）\end{aligned}$$

と書ける。

定理 5.24 p を有理素数とする。このとき、$p = x^2 + 3y^2$ が有理整数解をもつことと、$p = 3$ または $p \equiv 1 \pmod 3$ であることは同値である。さらに、このとき正の整数解は唯一つである。

証明 $p = 3$ のとき、$x = 0, y = 1$ が有理整数解である。
$p \equiv 1 \pmod 3$ とする。すると定理 5.20 より $p = \pi\overline{\pi}$（π は素数）と書ける。$\pi = a - b\omega$（a, b は有理整数）とおくとき、$p = \pi\overline{\pi}$ において π を同伴数

$$\pm\pi, \pm\omega\pi = \pm\{b + (a+b)\omega\}, \pm\omega^2\pi = \mp\{(a+b) + a\omega\}$$

でおき換えることができる。

a と b の両方が 2 で割り切れるとすると、$\pi = a - b\omega$ も 2 で割り切れる。よって $\pi\overline{\pi} = p$ が 2 で割り切れるが、これは $p \equiv 1 \pmod 3$ であることに矛盾する。よって a と b の少なくとも 1 つは 2 で割り切れない、すなわち奇数である。両方が奇数とすると、$a + b$ が偶数となるので、$a, b, a + b$ のうち 1 つだけが偶数である。よって、同伴数におき換えることにより、初めから $\pi = a - b\omega$ において b を偶数としてよい。m を有理整数として $b = 2m$ とおくと、

$$\begin{aligned} p &= \pi\overline{\pi} \\ &= (a - 2m\omega)(a - 2m\overline{\omega}) \\ &= a^2 - 2am(\omega + \overline{\omega}) + 4m^2\omega\overline{\omega} \\ &= a^2 + 2am + 4m^2 \\ &= (a + m)^2 + 3m^2 \end{aligned}$$

となるので、有理整数解 $x = a + m, y = m$ をもつ。

一意性を示す。$p = \pi\overline{\pi} = (a - 2m\omega)(a - 2m\overline{\omega})$ とする。有理整数解をもつとして、解を $x = c, y = d$ とする。すると p は有理素数なので、$(c, d) = 1$ である。このとき $e = c - d$ とおくと、

$$\begin{aligned} \pi\overline{\pi} = p = c^2 + 3d^2 &= (e + d)^2 + 3d^2 \\ &= e^2 + 2ed + 4d^2 \\ &= e^2 - 2ed(\omega + \overline{\omega}) + 4d^2\omega\overline{\omega} \\ &= (e - 2d\omega)(e - 2d\overline{\omega}) \end{aligned}$$

である。$(e - 2d\omega)(e - 2d\overline{\omega})$ が素数 π で割り切れるので、$e - 2d\omega$ が π で割り切れるとしてよい。もし $e - 2d\omega$ が $\pi\overline{\pi}$ で割り切れるとすると、$e - 2d\omega$ が p で割り切れるので、e と $2d$ が p で割りきれる。$p = 3$ または $p \equiv 1 \pmod 3$ より、2 は p で割り切れないので、d が p で割り切れる。従って、$e + d$ が p で割り切れるので、c が p で割り切れるが、これは $(c, d) = 1$ に矛盾する。よって、$e - 2d\omega$ は π で割り切れ、かつ $\overline{\pi}$ では割り切れない。よって $\pi\overline{\pi} = (e - 2d\omega)(e - 2d\overline{\omega})$ より、素因数分解の一意性から $e - 2d\omega$ は素数、すなわち $e - 2d\omega$ と π は同伴である。π の同伴数で ω の係数が偶数のものは符号の違いを除いて唯一つで、それを $a - b\omega = a - 2m\omega$ とおいたので、$e - 2d\omega = a - 2m\omega$ である。よって $c = a + m, d = m$ なので、解は唯一つである。

逆は対偶を示す。すなわち、$p \equiv -1 \pmod 3$ ならば有理整数解をもたないことを示す。 $p \equiv -1 \pmod 3$ のとき、有理整数解をもつとする。$p = a^2 + 3b^2$ とすると $p \equiv a^2 \pmod 3$ であるので、$a^2 \equiv -1 \pmod 3$ であるが、これは不可能である。よって解をもたない。 **証明終**

6　Fermat の最終定理 ($n = 3$ の場合)

この章では、$x^n + y^n = z^n$ が、$n = 3$ の時に正の整数解を持たないことを確かめてみる。

より一般に方程式、

$$\alpha^3 + \beta^3 + \gamma^3 = 0, \ \ (\alpha, \beta, \gamma \neq 0) \tag{17}$$

が $\mathbb{Z}[\omega]$ において解を持たないことを証明する。

証明 $(\alpha, \beta) = \delta$ とすると

$$\gamma^3 = -(\alpha^3 + \beta^3)$$

であるので、$\delta \mid \gamma$ となり

$$\left(\frac{\alpha}{\delta}\right)^3 + \left(\frac{\beta}{\delta}\right)^3 + \left(\frac{\gamma}{\delta}\right)^3 = 0$$

となるので、$(\alpha, \beta) = 1, \ (\alpha, \gamma) = 1, \ (\beta, \gamma) = 1$ としてよい。$\lambda = 1 - \omega$ とおき、$\xi \in \mathbb{Z}[\omega]$ が $\lambda \nmid \xi$ を満たすとすると

$$\xi^3 \equiv \pm 1 \pmod 9 \tag{18}$$

である。それを、以下、確かめてみよう。まず、命題 5.22 と注意 5.23 によって、$\lambda \nmid \xi$ なら

$$\xi = \pm 1 + \lambda\eta, \tag{19}$$

と書ける。ただし、η は整数である。また、$\lambda = -\sqrt{-3}(1 + \omega)$ より λ と $\sqrt{-3}$ は同伴であるので、$\xi = \pm 1 + \eta\sqrt{-3}$ とも書ける。よって、

$$\pm\xi = 1 + \eta\sqrt{-3}$$

とする。両辺を 3 乗すると

$$\pm\xi^3 = 1 - 9\eta^2 + 3\sqrt{-3}\eta(1 - \eta^2)$$

となる。ここで、(19) により、$\eta(1 - \eta^2) = -(\eta - 1)\eta(\eta + 1)$ は、λ で割り切れることに注意する。よって、$3\sqrt{-3}\eta(1 - \eta^2)$ は、9 で割れる。この式から直ちに、(18) が従う。

さて、(17) に解があるとして、$\lambda \nmid \alpha, \ \lambda \nmid \beta, \ \lambda \nmid \gamma,$ とすると、(18) より

$$\pm 1 \pm 1 \pm 1 \equiv 0 \pmod 9$$

となる。これはどのように符合 $\pm$ を組み合わせてみても不可能である。よって、$\alpha, \beta, \gamma,$ のうちどれか 1 つだけが λ で割り切れる。α が λ で割り切れるとしてよい。すると

$$\alpha = \lambda^m \alpha_0, \ m \geqq 1, \ (\alpha_0, \lambda) = 1, \ (\beta, \lambda) = 1, \ (\gamma, \lambda) = 1$$

とおくことができる。(17) より

$$\beta^3 + \gamma^3 = -\lambda^{3m}\alpha_0^3$$

を得る。

ここで、m を自然数、ϵ を単数とし、

$$\beta^3 + \gamma^3 = \epsilon\lambda^{3m}\alpha_0^3 \tag{20}$$

が $\alpha_0,\ \beta,\ \gamma \in \mathbb{Z}[\omega]$ であり、2 つずつ互いに素で、かつ $\lambda \nmid \alpha_0,\ \lambda \nmid \beta,\ \lambda \nmid \gamma$ を満たす解を持たないことを m についての帰納法で示す。

(18) より、

$$\pm 1 \pm 1 \equiv \epsilon\lambda^{3m}\alpha_0^3 \pmod{\lambda^4}$$

となる。この左辺が λ で割れることから左辺は 0 であり

$$0 \equiv \epsilon\lambda^{3m}\alpha_0^3 \pmod{\lambda^4}$$

である。

ここで、$m = 1$ とすると

$$0 \equiv \epsilon\lambda^3\alpha_0^3 \pmod{\lambda^4}$$

となるが、$\lambda \nmid \alpha_0$ より矛盾するので、$m = 1$ のときは不可能である。

よって、$m \geqq 2$ のときに (20) に解があるならば、指数を $m - 1$ としても、(20) に解があることを示せばよい。

$m \geqq 2$ で成り立つと仮定する。

$$\beta^3 + \gamma^3 = (\beta + \gamma)(\beta + \omega\gamma)(\beta + \omega^2\gamma)$$

であり、また

$$\begin{aligned} \beta + \omega\gamma &= (\beta + \gamma) - (1 - \omega)\gamma \\ &= (\beta + \gamma) - \lambda\gamma \\ \beta + \omega^2\gamma &= (\beta + \gamma) + (\omega^2 - 1)\gamma \\ &= (\beta + \gamma) + \omega^2\lambda\gamma \end{aligned}$$

に注意する。よって、

$$\begin{cases} \beta + \omega\gamma &= (\beta + \gamma) - \lambda\gamma \\ \beta + \omega^2\gamma &= (\beta + \gamma) + \omega^2\lambda\gamma \end{cases}$$

となる。(20) によって、λ^{3m} が $\beta^3 + \gamma^3$ の三つの因数 $\beta + \gamma,\ \beta + \omega\gamma,\ \beta + \omega^2\gamma$ の間に分配されねばならないから、これらの因数のどれかは λ で割れるが、どれか一つが λ

で割れるならば、(6) から見えるように三つともに λ で割れなければならない。しかし三つとも λ の一乗だけで割れるのでは足りないから、どれかは λ^2 で割れなければならないが、一つが λ^2 で割れるならば、(4) によって他の二つは λ の一乗でしか割れない。故に $\beta+\gamma,\ \beta+\omega\gamma,\ \beta+\omega^2\gamma$ の中で λ^2 で割れるのは一つだけである。

必要なら γ を $\omega\gamma$ または $\omega^2\gamma$ でおき換えて $\beta+\gamma$ が λ^{3m-2} で割れるとしてよい。

よって

$$\begin{cases} \beta+\gamma &= \lambda^{3m-2}\kappa \\ \beta+\omega\gamma &= \lambda\mu \\ \beta+\omega^2\gamma &= \lambda\nu \end{cases} \tag{21}$$

と書ける。ここで、$\kappa,\ \mu,\ \nu \in \mathbb{Z}[\omega],\ \lambda \nmid \kappa,\ \mu,\ \nu$ である。また、これら三つのうちどの二つにも λ 以外の公約数はない。何故なら例えば、κ と μ が λ 以外の公約数をもつならば

$$\begin{aligned} (\beta+\gamma)-(\beta+\omega\gamma) &= \lambda\gamma \\ \omega(\beta+\gamma)-(\beta+\omega\gamma) &= -\lambda\beta \end{aligned}$$

となる。これは $(\beta,\gamma)=1$ に矛盾する。故に、$\kappa,\ \mu,\ \nu$ は二つずつ互いに素である。(20), (21) から

$$\kappa\mu\nu = \epsilon\alpha_0^3$$

である。故に、$\kappa,\ \mu,\ \nu$ は 2 つずつが互いに素な立法数の同伴数になるので、

$$\begin{aligned} \beta+\gamma &= \epsilon_1\lambda^{3m-2}\alpha'^3 \\ \beta+\omega\gamma &= \epsilon_2\lambda\beta'^3 \\ \beta+\omega^2\gamma &= \epsilon_3\lambda\gamma'^3 \end{aligned}$$

と書ける。ただし、$\alpha',\ \beta',\ \gamma'$ は二つずつ互いに素で、かつ λ とも素である整数である。また、$\epsilon_1,\ \epsilon_2,\ \epsilon_3$ は単数である。よって

$$\begin{vmatrix} 1 & 1 & \epsilon_1\lambda^{3(m-1)}\alpha'^3 \\ 1 & \omega & \epsilon_2\beta'^3 \\ 1 & \omega^2 & \epsilon_3\gamma'^3 \end{vmatrix} = 0$$

となるはずである。何故ならば、上の行列を A とすると、

$$A\begin{pmatrix} \beta \\ \gamma \\ -\lambda \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

となり、故に、$\det A = 0$ となるからである。この行列式を第三列に関して展開すれば余因子 $\omega^2-\omega, 1-\omega^2, \omega-1$ はいずれも λ の同伴数であるから、展開の各項を λ で割って

$$\beta'^3 + \vartheta\gamma'^3 = \vartheta'\lambda^{3(m-1)}\alpha'^3 \tag{22}$$

を得る。ただし ϑ および ϑ' は単数である。ここで (18) と $m > 1$ であることから

$$\pm 1 \pm \vartheta \equiv 0 \pmod{\lambda^3}$$

を得る。ϑ は $\pm 1,\ \pm\omega,\ \pm\omega^2$ のどれかに等しいので

$$\vartheta = \pm 1$$

を得る。$\vartheta = -1$ のときは γ' の代わりに $-\gamma'$ と書けば、(22) は

$$\beta'^3 + \gamma'^3 = \epsilon' \lambda^{3(m-1)} \alpha'^3$$

となる。よって、α', β', γ' は二つずつ互いに素で、どれも λ で割れない。故に (20) が指数 m のときに解を持つならば、指数 $m - 1$ のときにも解を持たなければならない。 **証明終**

参考文献

[1] 「フェルマーの最終定理 ピュタゴラスに始まり、ワイルズが証明するまで」 サイモン・シン著 青木薫訳 （新潮社）

[2] 「フェルマーの最終定理～証明への道具立てと発見的推理～」山口周（東宛社）

[3] 「フェルマーの大定理 第２版 整数論の源流」 足立恒雄 （日本評論社）

[4] 「初等整数論講義 第２版」 高木貞治 （共立出版）