原始ピタゴラス数

賣間優太

1　はじめに

こんにちは．この記事では，高校数学の整数及び複素数についての知識のみを前提として書きました．高校生の方々でも十分に理解できるように書いたので，是非読んでいただけたら嬉しいです．

みなさんは**ピタゴラス数**というものをご存知ですか？ピタゴラス数とは，直角三角形の三辺を成す三つの正の整数の組 (a,b,c) のことです．これは三平方の定理より，

$$a^2+b^2=c^2$$

を満たす正の整数の組 (a,b,c) のことであると言い換えることができます．ピタゴラス数 (a,b,c) のうち，3 数の最大公約数が 1 であるもののことを**原始ピタゴラス数**といいます．この記事では，c の値 (いわゆる斜辺の長さ) を特殊な値に設定したときそれに対応する (a,b) の組の個数がどうなるかについて考察します．結論から先に述べると，本記事の最後には次の定理を証明します；

定理． p を $4n+1$ 型素数とするとき，

$$a^2+b^2=p^2$$

を満たす正整数の組 $(a,b)(a<b)$ がただ一つ存在する．

本記事では，この定理を**ガウス整数**を導入して示します．あまり聞き慣れない用語かもしれませんが，高校で習う整数，複素数の知識があれば十分に理解できるように第二章でこれについて補足します．もしわからないところがあってもあまり気にせず気軽に読み進めて下さい．

2　ガウス整数 $\mathbb{Z}[i]$

第二章では，第三章で目標の定理を証明するための準備をします．ざっくり言うと，ガウス整数の素因数分解の一意性まで証明します．

以下, 有理整数 (通常の整数) 全体の集合を $\mathbb{Z}$ とし，正整数全体の集合を $\mathbb{N}$ とする．

$a, b \in \mathbb{Z}$ を用いて $a + bi(i$ は虚数単位$)$ とかける複素数を**ガウス整数**と呼び，ガウス整数全体の集合を $\mathbb{Z}[i]$ のように表す．

例 1. $2, 1+i, -2+3i \in \mathbb{Z}[i]$ である．

定義 1. $\alpha, \beta \in \mathbb{Z}[i]$ とする．ある $\gamma \in \mathbb{Z}[i]$ が存在して

$$\beta = \alpha\gamma$$

となるとき，α は β の**約数**，β は α の**倍数**，β は α で**割り切れる**などといい，$\alpha|\beta$ と書く．

例 2. $(1+2i)(1+i) = -1+3i$ より，$-1+3i$ は $1+2i, 1+i$ で割り切れる．

定義 2. $\alpha \in \mathbb{Z}[i]$ が**単元（可逆元）**であるとは，α が 1 の約数であることをいう．すなわち，ある $\beta \in \mathbb{Z}[i]$ が存在して，

$$\alpha\beta = 1$$

となることである．

$\mathbb{Z}$ における単元は ± 1 である．$\mathbb{Z}[i]$ における単元は $\pm 1, \pm i$ であることが知られているが，これは定理 1 で証明する．

定義 3. （ノルム）$\alpha \in \mathbb{Z}[i]$ とする．$\alpha = a + bi(a, b \in \mathbb{Z})$ の**ノルム**を

$$N(\alpha) = a^2 + b^2$$

で定める．

この定義から，$\alpha \in \mathbb{Z}[i]$ のノルム $N(\alpha)$ は非負整数値をとることがわかる．

命題 1. （ノルムの積法則）

$\alpha, \beta \in \mathbb{Z}[i]$ に対して

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

が成り立つ．

証明.

$$\alpha = a + bi, \beta = c + di \qquad (a, b, c, d \in \mathbb{Z})$$

とおくと，

$$\alpha\beta = (ac - bd) + (ad + bc)i$$

であるから

$$\begin{aligned} N(\alpha\beta) &= (ac-bd)^2+(ad+bc)^2 \\ &= a^2c^2-2acbd+b^2d^2+a^2d^2+2adbc+b^2c^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= N(\alpha)N(\beta) \end{aligned}$$

□

定理 1. $\mathbb{Z}[i]$ における単元は $\pm1, \pm i$ のみである．

証明. $\pm1, \pm i$ が $\mathbb{Z}[i]$ における単元であることは明らかである．

$\varepsilon \in \mathbb{Z}[i]$ を $\mathbb{Z}[i]$ における単元とすると，ある $\varepsilon' \in \mathbb{Z}[i]$ が存在して

$$\varepsilon\varepsilon' = 1$$

となる．両辺のノルムを考えると，命題 1 より

$$N(\varepsilon)N(\varepsilon') = 1$$

ガウス整数のノルムは非負整数値をとることに気をつけると，

$$(N(\varepsilon), N(\varepsilon')) = (1,1)$$

となることがわかる．いま，$\varepsilon = a+bi(a,b\in\mathbb{Z})$ とおくと，

$$a^2+b^2 = 1$$

となる．$a,b\in\mathbb{Z}$ より，

$$(a,b) = (\pm1,0),(0,\pm1)$$

であるから，$\varepsilon = \pm1, \pm i$ となる． □

定理 2. （ガウス整数の余りつき割り算）

$\alpha, \beta \in \mathbb{Z}[i]$ とし，$\beta \neq 0$ とする．このとき，

$$\alpha = \beta\gamma+\delta, \quad N(\delta) < N(\beta)$$

となるような $\gamma, \delta \in \mathbb{Z}[i]$ が存在する．

証明. $\gamma \in \mathbb{Z}[i]$ を，$\left|\dfrac{\alpha}{\beta}-\gamma\right|$ の値が最小となるようにとる．ガウス整数は複素数全体において稠密でない（飛び飛びの値をとる）ことからこれを満たす γ は確かに存在する．複素数平面上で考えると，

$$\left|\frac{\alpha}{\beta}-\gamma\right| \leq \frac{1}{\sqrt{2}}$$

が成り立つことがわかる．特に，$\left|\dfrac{\alpha}{\beta}-\gamma\right| < 1$ であるから，この両辺に $|\beta|(>0)$ をかけたあと辺々二乗して整理することで

$$|\alpha-\beta\gamma|^2 < |\beta|^2$$

を得る．$\delta = \alpha - \beta\gamma$ とおくと，$\delta \in \mathbb{Z}[i]$ であり，ガウス整数の絶対値の二乗はノルムに等しいことに気をつけると，

$$\alpha = \beta\gamma + \delta, \quad N(\delta) < N(\beta)$$

となるから，所望の $\gamma, \delta \in \mathbb{Z}[i]$ を得る． □

定理 3.（単項イデアル整域）

$\alpha, \beta \in \mathbb{Z}[i]$ とする．集合 I を次のように定める；

$$I = \{s\alpha + t\beta | s, t \in \mathbb{Z}[i]\}$$

このとき，ある $\gamma \in \mathbb{Z}[i]$ が存在して，集合 J を

$$J = \{s\gamma | s \in \mathbb{Z}[i]\}$$

と定めると，$I = J$ となる．

証明. $I = \{0\}$ のとき，$\gamma = 0$ とすれば題意を満たす．

$I \neq \{0\}$ のとき，I の元であってノルムが 0 でないものが存在する．それらのノルムは正整数値をとることから，その中でノルムが最小となるようなものが存在するので，それを $\gamma(\in I)$ とおき，$J = \{s\gamma | s \in \mathbb{Z}[i]\}$ とおく．この γ が題意を満たすことを示す．

まず，$I \subset J$ を示す．$\delta \in I$ とする．δ を γ で割り算すると，定理 2 より

$$\delta = \gamma p + q, \quad N(\gamma) > N(q)$$

となるような $p, q \in \mathbb{Z}[i]$ が存在する．$\gamma \in I$ より，$-\gamma p \in I$．また，$\delta \in I$ であるから，$q = \delta - \gamma p \in I$．$N(\gamma) > N(q)$ であることと，$\gamma \in I$ はノルムが 0 でない I の元のうち最小のものであることを考慮すると，$N(q) = 0$ となるしかなく，このとき $q = 0$ である．したがって，$\delta = \gamma p \in J$ となるから $I \subset J$.

次に，$J \subset I$ を示す．$\varepsilon \in J$ とする．このとき，ある $s \in \mathbb{Z}[i]$ が存在して $\varepsilon = s\gamma$ とかける．$\gamma \in I$ より，$s\gamma = \varepsilon \in I$ となるから $J \subset I$．以上より，$I = J$ が示された． □

なお，代数学の用語を用いると，定理 3 における I のことを α, β で生成された**イデアル**，J のことを γ で生成されたイデアルといい，$I = (\alpha, \beta), J = (\gamma)$ と書く．(γ) のようにただ一つの元で生成されるイデアルを**単項イデアル**という．以下，I, J のような集合を考えるときは，単に $(\alpha, \beta), (\gamma)$ のように記すことにする．

定義 4.（素元と既約元）

$\alpha, \beta, \gamma \in \mathbb{Z}[i]$ とし，$\alpha \neq 0$ で単元でないとする．

(1) $\alpha | \beta\gamma$ ならば $\alpha | \beta$ または $\alpha | \gamma$ となるとき，α を **素元**という．

(2) $\alpha = \beta\gamma$ ならば β, γ のいずれか一方が単元になるとき，α を**既約元**という．

命題 2. $\alpha \in \mathbb{Z}[i]$ は，$\alpha \neq 0$ で単元でないとする．

α が素元であることと，α が既約元であることは同値である．

証明.（既約元ならば素元であることの証明）

α が既約元であるとする．$\alpha | \beta\gamma \quad (\beta, \gamma \in \mathbb{Z}[i])$ とし，$\beta\gamma = k\alpha (k \in \mathbb{Z}[i])$ とする．定理 3 より，ある $\delta \in \mathbb{Z}[i]$ が存在して $(\alpha, \beta) = (\delta)$ となる．$\alpha \in (\alpha, \beta) = (\delta)$ であるから，$s \in \mathbb{Z}[i]$ を用いて $\alpha = \delta s$ と書ける．α は既約元であるから，δ, s のうち一方が単元になる．

δ が単元のとき，$(\delta) = (1)(= \mathbb{Z}[i])$ となる．実際，δ は単元であるから $\delta\varepsilon = 1$ なる $\varepsilon \in \mathbb{Z}[i]$ が存在し，$x \in \mathbb{Z}[i]$ を任意に取ったとき，$x = x \cdot 1 = x\delta\varepsilon \in (\delta)$ となるから $(1) \subset (\delta)$. $(\delta) \subset (1)$ は明らかである．このとき，$(\alpha, \beta) = (1)$ となるから，$1 = t\alpha + u\beta$ を満たす $t, u \in \mathbb{Z}[i]$ が存在する．このとき，

$$\gamma = t\alpha\gamma + u\beta\gamma = t\alpha\gamma + uk\alpha = \alpha(t\gamma + uk)$$

となるから $\alpha|\gamma$ である．よって α は素元である．

s が単元のとき，$sy = 1$ なる $y \in \mathbb{Z}[i]$ が存在する．このとき，$y\alpha = y\delta s = \delta sy = \delta$ となる．$\beta \in (\alpha, \beta) = (\delta)$ より，ある $z \in \mathbb{Z}[i]$ が存在して $\beta = \delta z$ となる．$\beta = \delta z = y\alpha z$ より $\alpha|\beta$ である．よって α は素元である．

（素元ならば既約元であることの証明）

α を素元とする．$\alpha = \beta\gamma(\beta, \gamma \in \mathbb{Z}[i])$ とおく．明らかに $\alpha|\beta\gamma$ であるから，$\alpha|\beta$ または $\alpha|\gamma$ である．$\alpha|\beta$ とする．このとき $\beta = k\alpha(k \in \mathbb{Z}[i])$ とおけるから，$\alpha = k\alpha\gamma$．$\alpha \neq 0$ より $1 = k\gamma$ となるから γ は単元となり，α は既約元である．$\alpha|\gamma$ の場合も同様． □

定義 5. $\alpha, \beta \in \mathbb{Z}[i]$ とする．単元 ε を用いて $\alpha = \varepsilon\beta$ とかけるとき，α, β は**同伴**であるという．

定理 4.（ガウス整数の素因数分解の一意性）任意の 0 でない $\alpha \in \mathbb{Z}[i]$ は，

$$\alpha = \varepsilon\pi_1^{e_1} \cdots \pi_r^{e_r}$$

の形に分解できる．ただし，ε は単元，$\pi_i \in \mathbb{Z}[i]$ はどの二つも互いに同伴でない素元，$e_i \in \mathbb{N}(i = 1, \ldots, r)$ である．

さらに，同伴な素元や積の順序交換によって互いに移り合うものを同じとみなすと，分解は一意に定まる．

証明.（分解が存在することの証明）

$N(\alpha) = n$ とし，n についての数学的帰納法で示す．$\alpha \neq 0$ より，$n \geq 1$ である．

$n = 1$ のとき，α は単元である．（便宜的に）$r = 0$ として分解される．

$n \leq k$ を満たすすべての n で分解が存在したと仮定する．α が素元のときは α 自身が題意を満たす分解となる．α が素元でないとき，単元でない $\beta, \gamma \in \mathbb{Z}[i]$ を用いて $\alpha = \beta\gamma$ と書けて，このとき $N(\alpha) = N(\alpha\beta) = N(\beta)N(\gamma)$ となる．β, γ は単元でないから $N(\beta), N(\gamma) > 1$．よって $N(\beta), N(\gamma) \leq k$. 帰納法の仮定より β, γ は題意を満たす分解を持つので，これらを掛け合わせて，β, γ に共通する素元（同伴なものは同じと見なす）同士で整理することで α の分解を得る．

（分解が一意的であることの証明）

存在性の証明と同様に，$N(\alpha) = n$ についての数学的帰納法で示す．

$n = 1$ のとき，α は単元であるから（便宜的に）$r = 0$ とすると一意性は明らか．

$n \leq k$ を満たすすべての n で分解が一意（ただし，同伴な素元や積の順序交換によって互いに移り合うものを同じとみなす）であると仮定する．α が二通りの素因数分解を持つと仮定し，単元 δ, ε，素元 π_i, π'_j（それぞれどの二つも互いに同伴でない），$e_i, f_j \in \mathbb{N}(i = 1, \ldots r, j = 1, \ldots s)$ を用いて

$$(\alpha =)\varepsilon\pi_1^{e_1} \cdots \pi_r^{e_r} = \delta\pi_1'^{f_1} \cdots \pi_s'^{f_s} \qquad (\star)$$

とかけたとする．左辺は π_1 の倍数であるから，$\delta, \pi'_1, \ldots \pi'_s$ のうちいずれかは π_1 で割り切れる．$\pi_1|\delta$ は明らかに不適．$\pi_1|\pi'_1$ とすると，ある $x \in \mathbb{Z}[i]$ が存在して $\pi'_1 = \pi_1 x$．π'_1 は素元であるから既約元でもあり，π_1 は

単元でないから x が単元となる．よって π_1 と π_1' は同伴．このことから，$(\star)$ の両辺を π_1 で割ると

$$\varepsilon\pi_1^{e_1-1}\cdots\pi_r^{e_r}=\delta y\pi_1'^{f_1-1}\cdots\pi_s'^{f_s}$$

このとき δy は単元である．$\beta=\varepsilon\pi_1^{e_1-1}\cdots\pi_r^{e_r}=\delta y\pi_1'^{f_1-1}\cdots\pi_s'^{f_s}$ とおくと，明らかに $N(\beta)<N(\alpha)=k+1$ であり，$\beta\in\mathbb{Z}[i]$ であるから $N(\beta)\leq k$．帰納法の仮定より，同伴な素元や積の順序交換によって互いに移り合うものを同じと見なすことで β の分解は一意であることが従う．この条件下で，$\alpha=\pi_1\beta$ の分解も一意である． □

3　原始ピタゴラス数

まず，補題を 1 つ示す．ここで，$4n+1$ 型素数とは，$p\equiv 1 \pmod 4$ を満たす素数 p のことである．

補題. 奇素数 p に対して，以下の *1,2* は同値

1. ある $a,b\in\mathbb{N}$ が存在して $a^2+b^2=p$
2. p は $4n+1$ 型素数

また，p が $4n+1$ 型素数のとき，組 (a,b) は順序を除いて一意に定まる．

証明. $((1)\Longrightarrow(2)$ の証明$)$ $a^2+b^2=p$ なる $a,b\in\mathbb{N}$ が存在したとする．p は奇数なので a^2,b^2 の偶奇は異なるから，a,b の偶奇は異なる．$s,t\in\mathbb{Z}_{\geq 0}$ を用いて $a=2s,b=2t+1$ としてよい．このとき，$a^2+b^2=(2s)^2+(2t+1)^2=4(s^2+t^2+t)+1$ となるから p は $4n+1$ 型素数.

$((2)\Longrightarrow(1)$ の証明$)$ $p\equiv 1 \pmod 4$ なら，p は $\mathbb{Z}[i]$ において素元ではないため，単元でない $a+bi,c+di\in\mathbb{Z}[i]$ があり $p=(a+bi)(c+di)$ となる．ノルムをとると，$p^2=(a^2+b^2)(c^2+d^2)$ である．$a+bi,c+di$ は単元でないから，$a^2+b^2,c^2+d^2>1$ である．よって，$p=a^2+b^2=c^2+d^2$ となるしかないため，示された．

(一意性の証明) $a^2+b^2=p$ より，$(a+bi)(a-bi)=p$．$\alpha=a+bi$ と置き，α が素元であることを示す．$\beta,\gamma\in\mathbb{Z}[i](N(\beta)\leq N(\gamma))$ を用いて $\alpha=\beta\gamma$ とおくと，両辺のノルムをとって $p=N(\alpha)=N(\beta\gamma)=N(\beta)N(\gamma)$．$N(\beta),N(\gamma)\in\mathbb{Z}_{\geq 0},N(\beta)\leq N(\gamma)$ と，p は素数であることより，$(N(\beta),N(\gamma))=(1,p)$．よって β は単元であるから，α は既約元．命題 2 より α は素元．よって，定理 4 より，同伴な素元や積の順序交換によって互いに移り合うものを同じと見なすことで p の $\mathbb{Z}[i]$ における分解は一意に定まる．このとき，組 (a,b) は順序を除いて一意に定まるから示された． □

定理. p を $4n+1$ 型素数とするとき，

$$a^2+b^2=p^2$$

を満たす正整数の組 (a,b) が順序を除いて一意に存在する．

証明. 補題と，$x,y,z,w\in\mathbb{Z}$ に対して成り立つ有名な恒等式

$$(x^2+y^2)(z^2+w^2)=(xz-yw)^2+(xw+yz)^2$$

より，存在性が従う．$a^2+b^2=p^2$ より，$(a+bi)(a-bi)=p^2$．$\alpha=a+bi$ とおき，$\beta_1,\gamma_1\in\mathbb{Z}[i](N(\beta_1)\leq N(\gamma_1))$ を用いて $\alpha=\beta_1\gamma_1$ とする．両辺のノルムをとって $p^2=N(\alpha)=N(\beta_1\gamma_1)=N(\beta_1)N(\gamma_1)$.

$N(\beta_1), N(\gamma_1) \in \mathbb{Z}_{\geq 0}, N(\beta_1) \leq N(\gamma_1)$ と，p は素数であることより，$(N(\beta_1), N(\gamma_1)) = (1, p^2), (p, p)$. $\alpha^* = a - bi$ とおき，$\beta_2, \gamma_2 \in \mathbb{Z}[i] (N(\beta_2) \leq N(\gamma_2))$ を用いて $\alpha^* = \beta_2\gamma_2$ とすると，先と同様の議論により $(N(\beta_2), N(\gamma_2)) = (1, p^2), (p, p)$.

ここで，$\beta, \gamma \in \mathbb{Z}[i]$ であって，$N(\beta) = N(\gamma) = p$ となるときを考える．$s, t, u, v \in \mathbb{Z}$ を用いて，$\beta = s + ti, \gamma = u + vi$ とおくと，$s^2 + t^2 = u^2 + v^2 = p$ である．補題より，これを満たす正整数の組は順序を除いて一意的であるから，$(s, t) = (\pm u, \pm v), (\pm v, \pm u)$（複号任意）となる．よって，$\beta$ と γ は同伴である．よって，$\alpha' = \beta\gamma$ は，β^2 と同伴である．

(i)　$(N(\beta_1), N(\gamma_1)) = (N(\beta_2), N(\gamma_2)) = (1, p^2)$ のとき

β_1, β_2 は単元であるから α, α^* は既約元．よって，α, α^* は素元．このとき定理 4 より，組 (a, b) は順序を除いて一意に定まる．

(ii)　$(N(\beta_1), N(\gamma_1)) = (1, p^2), (N(\beta_2), N(\gamma_2)) = (p, p)$ のとき

先と同様の議論により α は素元．また，前半の議論により $\alpha^* = \varepsilon\beta_2^2$ とかける．$p^2 = \alpha\alpha^* = \alpha\varepsilon\beta_2^2$ より，$\varepsilon\alpha = \left(\dfrac{p}{\beta_2}\right)^2$．ここで，$\beta_2$ の複素共役を β_2^* とおくと，

$$\frac{p}{\beta_2} = \frac{N(\beta_2)}{\beta_2} = \frac{|\beta_2|^2}{\beta_2} = \frac{\beta_2\beta_2^*}{\beta_2} = \beta_2^*$$

であるから $\varepsilon\alpha = (\beta_2^*)^2$ となるが，これは α が素元であることに矛盾．よって，$(N(\beta_1), N(\gamma_1)) = (1, p^2), (N(\beta_2), N(\gamma_2)) = (p, p)$ となるような分解は存在しない．$(N(\beta_1), N(\gamma_1)) = (p, p), (N(\beta_2), N(\gamma_2)) = (1, p^2)$ のときも同様.

(iii)　$(N(\beta_1), N(\gamma_1)) = (N(\beta_2), N(\gamma_2)) = (p, p)$ のとき

α, α^* はそれぞれ β_1^2, β_2^2 と同伴であるから，単元 ε を用いて $p^2 = \alpha\alpha^* = \varepsilon\beta_1^2\beta_2^2$ と書ける．従って，$\varepsilon = \left(\dfrac{p}{\beta_1\beta_2}\right)^2$．$\varepsilon = \pm 1, \pm i$ であるから，以下個々の場合を調べる．

(甲) $\varepsilon = \pm 1$ のとき.

$\dfrac{p}{\beta_1\beta_2} = \pm 1, \pm i$ より単元 δ を用いて $p = \delta\beta_1\beta_2$ となる．補題より，p の分解は同伴な素元と積の順序を無視して一意に定まり，$\beta_2 = \beta_1^*$（β_1 の複素共役）としてよい．このときある $x, y \in \mathbb{N}$ を用いて $p = x^2 + y^2$ と書けて，組 (x, y) は順序を除いて一意である．$i = 1, 2$ に対して，β_i, γ_i は互いに同伴なので，組 (x, y) と (a, b) は順序を除いて一対一に対応する．よって，組 (a, b) は順序を除いて一意的である.

(乙) $\varepsilon = \pm i$ のとき.

$z \in \mathbb{C}$ の方程式 $z^2 = \pm i$ を解くと $z = \dfrac{\pm 1 \pm i}{\sqrt{2}}$（複号任意）．よって $\dfrac{p}{\beta_1\beta_2} = \dfrac{\pm 1 \pm i}{\sqrt{2}}$．となるが，これは $p \in \mathbb{Z}, \beta_1, \beta_2 \in \mathbb{Z}[i]$ に矛盾．よって $\varepsilon = \pm i$ となる分解は存在しない.

以上より，分解が存在するすべての場合において組 (a, b) が一意に定まることが示された．$z \in \mathbb{C}$ の方程式 $z^2 = \pm i$ を解くと $z = \dfrac{\pm 1 \pm i}{\sqrt{2}}$（複号任意）．よって $\dfrac{p}{\beta_1\beta_2} = \dfrac{\pm 1 \pm i}{\sqrt{2}}$．となるが，これは $p \in \mathbb{Z}, \beta_1, \beta_2 \in \mathbb{Z}[i]$ に矛盾．よって $\varepsilon = \pm i$ となる分解は存在しない.

以上より，分解が存在するすべての場合において組 (a, b) が一意に定まることが示された．　□

4　おわりに

いかがでしたか？実は，本記事で証明した内容よりも強い定理が成り立つことが示されています．気が向いたら証明してみてください；

定理. $n \in \mathbb{N}$ とする．$i = 1, \ldots, n$ として，p_i をどの二つも相異なる $4n+1$ 型素数，$f_i \in \mathbb{N}$ とする．このとき，

$$a^2 + b^2 = p_1^{f_1} \cdots p_n^{f_n}$$

を満たす正整数の組 (a, b) は，順序を無視して少なくとも 2^{n-1} 個存在する．

本記事では，この定理の $n = 1, f_1 = 2$ における場合を証明したことになります．こちらの証明は，『ぺるせんたげの学習帳　斜辺を共有するピタゴラス数たち (https://percentage011.hatenablog.com/entry/2022/02/06/130054)』という記事で証明されているので興味がある方は是非ご覧になってください．

ここまで読んでいただきありがとうございました．

参考文献

[1] J.H.Silverman　著，鈴木治郎　訳，『はじめての数論』丸善出版，2022

[2] 雪江明彦　著，整数論 1　『初等整数論から p 進数へ』日本評論社，2021

[3]【連続講義】代数的整数論への招待～ガウス整数～，Masaki Koga[数学解説](https://youtube.com/playlist?list=PL5Pahvi5ekKeCDWgbVTV-WgONOqaDcc_g&si=iY7JpBMXgU3KcrpL)