フェルマーの 2 平方数定理の Zagier による証明について

2024 年 3 月
片山　喜美

定理　$p = 4k + 1$（k は自然数）のタイプの素数 p は

$p = a^2 + b^2$　$(a, b$ は自然数)

と表される。

この定理の証明については、ガウス整数 $\mathbb{Z}[i]$ で考えるなど（例えば、参考文献 [1] で述べたように)、ある程度の代数学の知識が必要なものだと思っていた。ところが、D.Zagier による”One-sentence Proof”’(「一文の証明」　参考文献 [2]) があることを教えてもらった。その方法について、さすがに一文を見ただけではわからないので、少し書き留めておく。

1　素数 $p = 4k + 1$ に対応する風車ブロックについて

$p = 4k + 1$（k は自然数）のタイプの素数 p について、集合

$$S = \{(x, y, z) \quad | \quad x, y, z \in \mathbb{N}, \quad p = x^2 + 4yz \}$$

を考える。

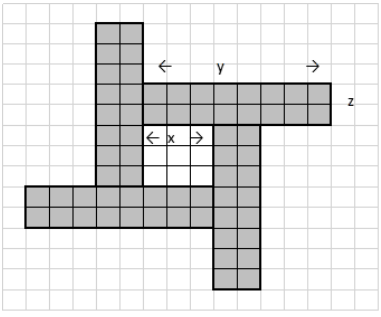
補題 1.1 S は空集合ではない。また、有限集合である。

$\because)$ $p = 1^2 + 4 \cdot 1 \cdot k$ より、 $(1, 1, k) \in S$

また、$p > x^2, p > 4yz$ であるから、それを満たす自然数 x, y, z の個数は有限であり、S は有限集合である。//

次に、S の元 (x, y, z) に対応した「風車ブロック」を以下のように定義する。

- 一辺 x 個のブロックの正方形を作る。
- 次に、正方形の上辺の上に、横 y 個、縦 z 個のブロックを左端を揃えておく。
- 正方形の右辺の右には、横 z 個、縦 y 個のブロックを上端を揃えておく。
- 正方形の下辺の下、左辺の左にもブロックをおいて、風車のような形を作る。



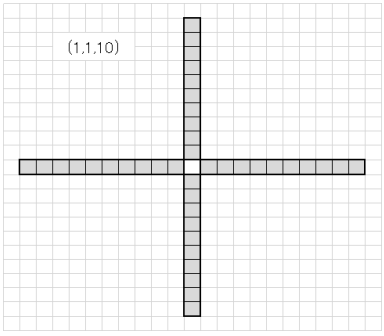
(x, y, z) に対応した風車ブロック

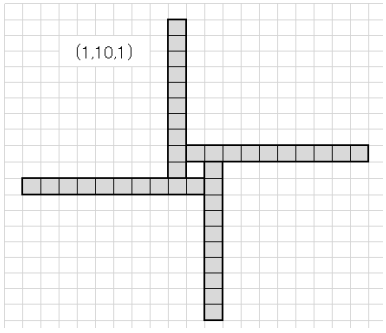
このとき、ブロックの個数は x^2+4yz となる。

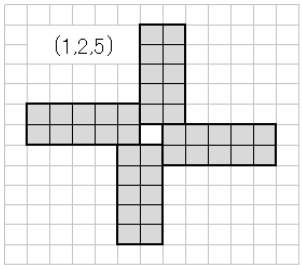
例　$p=41$ のとき

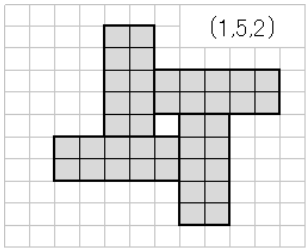
$yz=\dfrac{41-x^2}{4}$ となることから、x は奇数である。従って、 $x=1,3,5$

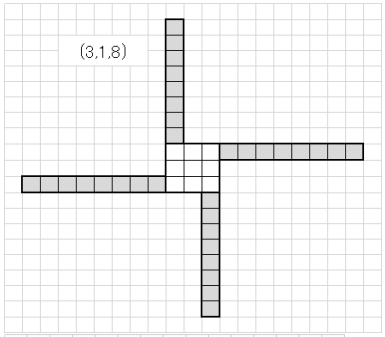
$(x,\,y,\,z)=(1,1,10),\,(1,10,1),\,(1,2,5),\,(1,5,2),\,(3,1,8),\,(3,8,1),$
$(3,2,4),\,(3,4,2),\,(5,1,4),\,(5,4,1),\,(5,2,2)$

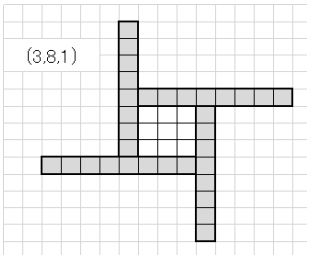


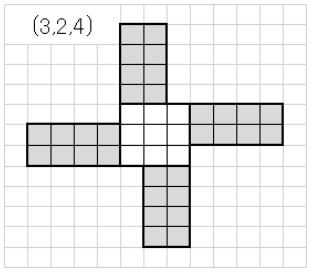


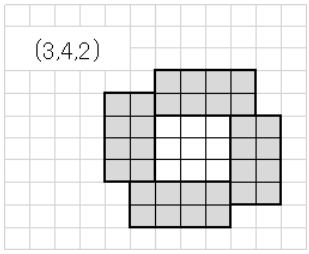


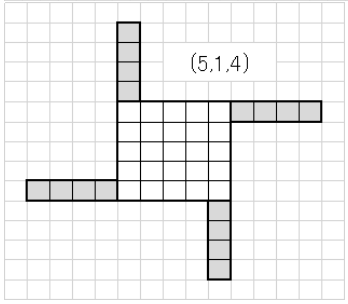


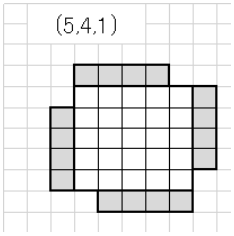


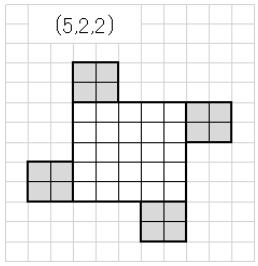












さて、 p を固定したとき、 $p=x^2+4yz$ は、y と z について対称な式である。よって、$(x,\,y,\,z)\in S \quad \Longrightarrow (x,\,z,\,y)\in S$ である。

S の元 $(x,\,y,\,z)$ に対して、 $\phi((x,\,y,\,z))=(x,\,z,\,y)$ と定めると、

- $\phi((x,\,y,\,z))\in S$
- $\phi(\phi((x,\,y,\,z)))=(x,\,y,\,z)$ すなわち $\phi\circ\phi$ は恒等写像である。

（上記の性質を持つ写像を「*involution*」と呼ぶ。）

S の元のうち、 $y \neq z$ のものは、 ϕ による対応でペアをなす。

$p = 41$ の例では、$(1,1,10)$ と $(1,10,1)$、$(1,2,5)$ と $(1,5,2)$、$(3,1,8)$ と $(3,8,1)$、$(3,2,4)$ と $(3,4,2)$、$(5,1,4)$ と $(5,4,1)$ がペアをなしている。

$(5,2,2)$ だけ、 $y = z$ を満たしており、ペアを作らない。言い換えると、ϕ の不動元となっている。そして、

$$41 = 5^2 + 4 \cdot 2 \cdot 2 = 5^2 + 4^2$$

により、 $41 = a^2 + b^2$ の解を与えているのである。

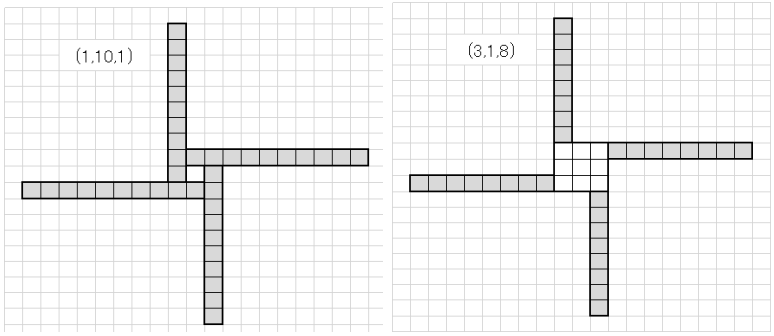
$p = 41$ の場合、*5*組のペアと不動元が *1* つの計 *11* 個の元がある。従って、S の元の個数は奇数である。以下の命題が成り立つ。

命題 *1.2* S の元の個数が奇数ならば、$p = a^2 + b^2$ を満たす自然数 a, b が存在する。

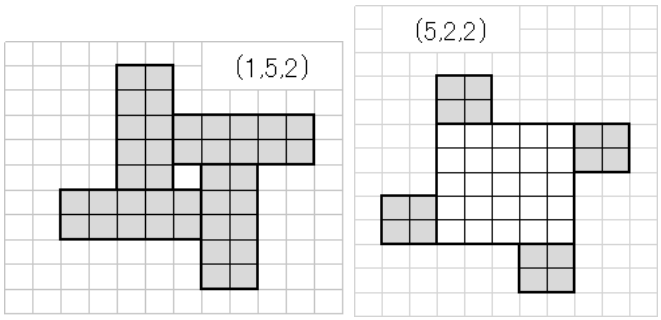
∴) もし、 ϕ により不動なものが無ければ、S の元は、ϕ で結ばれるものをペアにしていける。よって、S の元の個数は偶数になる。従って、S の元の個数が奇数であれば、ϕ により不動なもの、すなわち $y = z$ を満たすものがある。このとき、$p = x^2 + 4y^2$ であるから、 $a = x, b = 2y$ とおけばよい。*//*

2 Zagier Map（あるいは、シルエット写像）

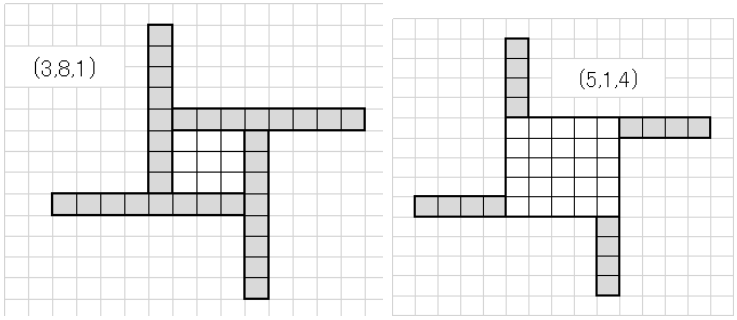
上では、 (x, y, z) と (x, z, y) でペアを作ることを考えた。ここでは、風車ブロックのシルエットが同じもの、あるいはちょうど裏返しになっているものをペアにすることを考える。



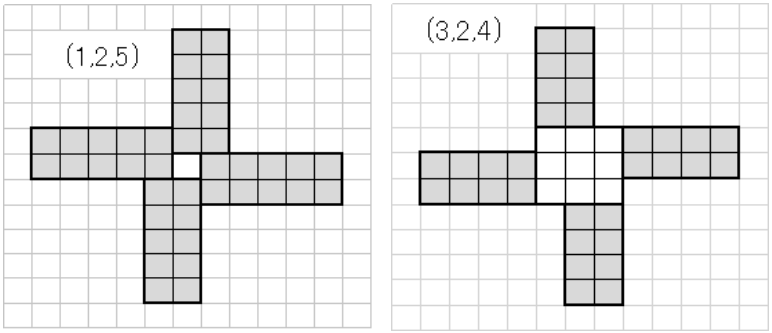
(1, 10, 1) と (3, 1, 8) はシルエットにすると同じになる。



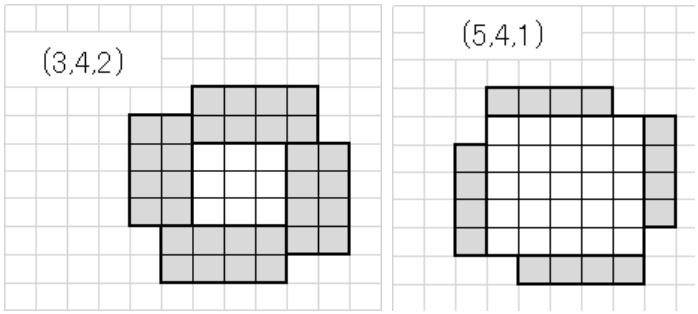
(1, 10, 1) と (3, 1, 8) は同じシルエット



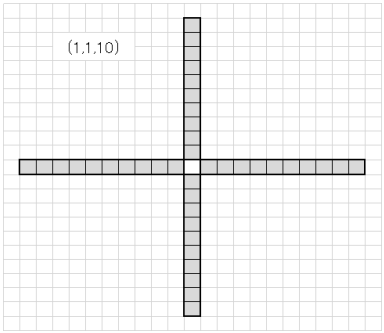
(3, 8, 1) と (5, 1, 4) は同じシルエット。



(1, 2, 5) と (3, 2, 4) は裏返しのシルエット。



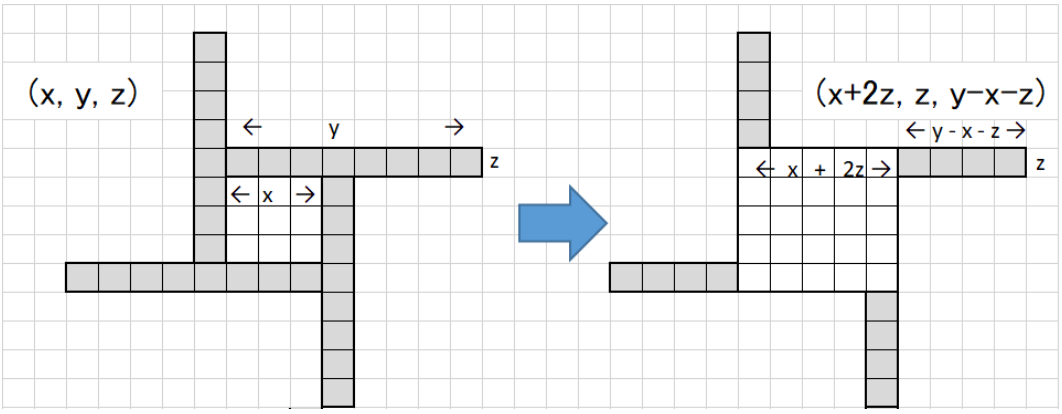
(3, 4, 2) と (5, 4, 1) は裏返しのシルエット。



(1, 1, 10) は同じシルエットも裏返しのシルエットも無い。
この x, y, z は、 $41 = 1 + 4 \cdot 10$ に結びついている。

同じシルエット、もしくは、裏返しのシルエットへの対応を考える。

[1] $x + z < y$ のとき



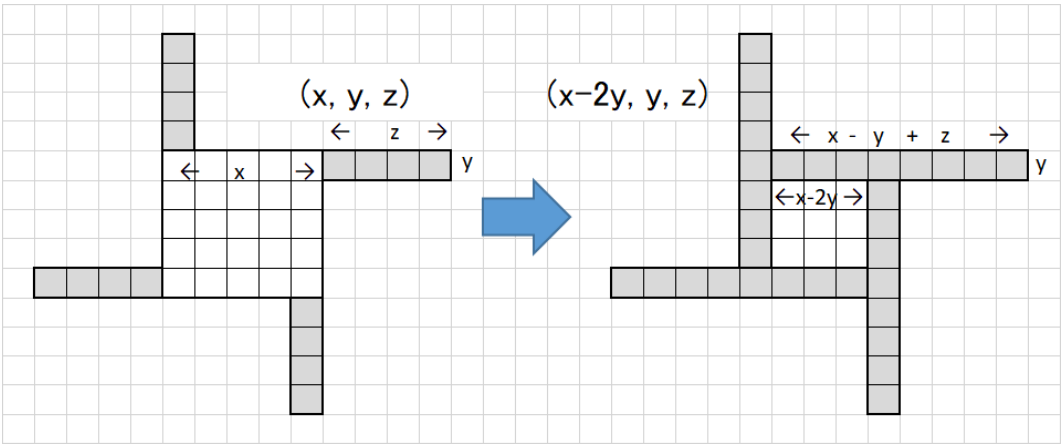
一辺 x の正方形を上下、前後に z ずつ増やしたものにする。
$x' = x + 2z,\ y' = z,\ z' = y - x - z$ となり

$$x'^2 + 4y'z' = (x+2z)^2 + 4z(y-x-z) = (x^2+4xz+4z^2) + 4(yz-xy-z^2) = x^2+4yz = p$$

従って、$(x', y', z') \in S$ である。また、新たな風車ブロックは、$x' = x + 2z = x + 2y' > 2y'$ を満たしている。

上の対応の逆を考える。今度は、正方形を上下、左右に y ずつ小さくする。そのためには、$x > 2y$ を満たす風車ブロックに限る。

[2] $x > 2y$ のとき



対応は、 $x' = x - 2y,\ y' = x - y + z,\ z' = y$ となり

$$x'^2 + 4y'z' = (x-2y)^2 + 4(x-y+z)y = (x^2-4xy+4y^2) + 4(xy-y^2+yz) = x^2+4yz = p$$

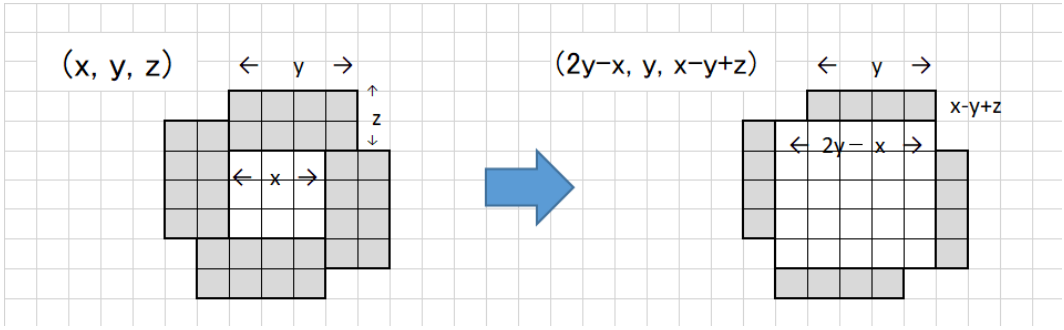
従って、 $(x', y', z') \in S$ である。また、新たな風車ブロックは、$x' + z' = (x - 2y) + y = x - y < x - y + z = y'$ であるから、 $x' + z' < y'$ を満たしている。すなわち、[1] の条件を満たしている。

[1] と [2] の写像を合成すると、恒等写像になっていることは、以下の計算で確かめられる。
$x'' = x' - 2y' = (x + 2z) - 2z = x, \quad y'' = x' - y' + z' = (x + 2z) - z + (y - x - z) = y, \quad z'' = y' = z$

[3] $x+z=y$ のとき

$p=x^2+4(x+z)z=x^2+4xz+4z^2=(x+2z)^2$
これを満たす素数 p は存在しない。

[4] $x<y<x+z$ のとき



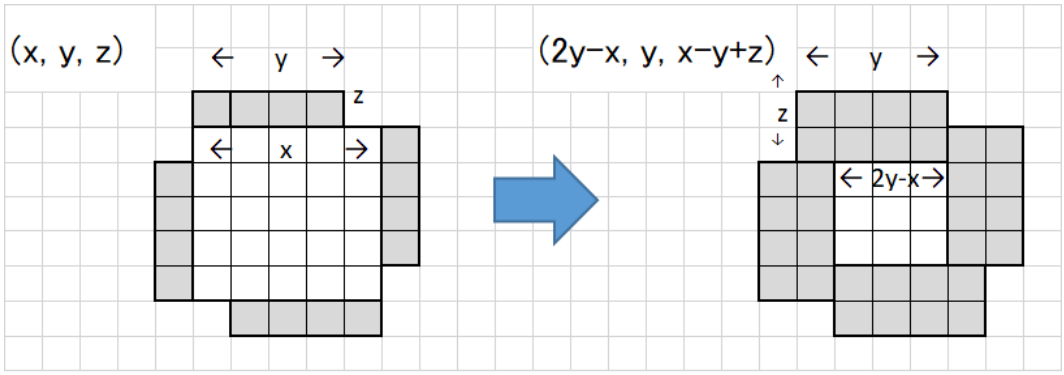
一辺 x の正方形を上下、前後に $y-x$ ずつ増やしたものにする。
$x'=x+2(y-x)=2y-x,\ y'=y,\ z'=z-(y-x)=x-y+z$ となり

$$x'^2+4y'z'=(2y-x)^2+4y(x-y+z)=(x^2-4xy+4y^2)+4(xy-y^2+yz)=x^2+4yz=p$$

従って、$(x',\ y',\ z')\in S$ である。また、新たな風車ブロックは、$x'=y+(y-x)=y'+(y-x)>y',\quad y'=y>y-\frac{1}{2}x=\frac{1}{2}(2y-x)=\frac{1}{2}x'$ であるから、
$\frac{1}{2}x'<y'<x'$、すなわち $y'<x'<2y'$ を満たしている。このとき 正方形の一辺を x から x' へ増やしたブロック数は、 $y-x=y'-(2y'-x')=x'-y'$ である。

上の対応の逆を考える。今度は、一辺 x の正方形を上下、左右に $x-y$ ブロックずつ小さくする。そのためには、 $y<x<2y$ を満たす風車ブロックに限る。

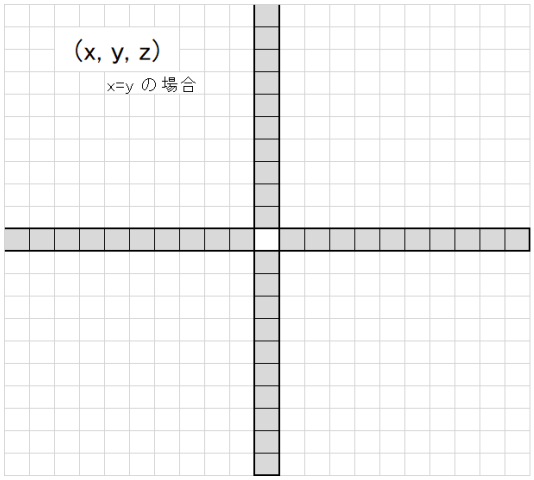
[5] $y<x<2y$ のとき



$x'=x-2(x-y)=2y-x,\ y'=y,\ z'=z+(x-y)=x-y+z$ となり、前の変換と全く同じである。従って、$x^2+4y'z'=p$ が成り立つのは上と同じである。

[4] と [5] の写像を合成すると、恒等写像になっていることは、計算で確かめられる。

[6] $x=y$ のとき



このとき、正方形のブロックを増やすことも減らすこともできない。

この場合、上の [4],[5] の変換で $x = y$ の時、変換したものが元のものと同じである、すなわち変換 $x' = 2y - x,\ y' = y,\ z' = x - y + z$ の不動元になっているとみなすことができる。

[7] $x = 2y$ のとき
$p \equiv 1 \pmod 4$ を満たす素数 p について、$p = x^2 + 4yz$ が成り立つとき x は奇数であるから、このような風車ブロックはありえない。

以上の場合分けを x の大きさで分類し直して整理すると、

- [1] $x < y - z$ のとき、変換は　$x' = x + 2z,\ y' = z,\ z' = y - x - z$
- [3] $x = y - z$ を満たす風車ブロックはできない。
- [4] $y - z < x < y$ のとき、[6] $x = y$ のとき、[5] $y < x < 2y$ のとき、
変換は $x' = 2y - x,\ y' = y,\ z' = x - y + z$
- [7] $x = 2y$ を満たす風車ブロックはできない。
- [2] $2y < x$ のとき、変換は　$x' = x - 2y,\ y' = x - y + 2zz,\ z' = y$

S の元は、x と y, z の関係で整理して、上記のいずれかに当てはまる。従って、 $S \to S$　の写像 ψ を以下のように定めることができる。

Zagier Map (あるいは、シルエット写像)

$$\psi((x,\ y,\ z)) = \begin{cases} (x + 2z,\ z, y - x - z) & (x < y - z \text{ のとき}) \\ (2y - x,\ y,\ x - y + z) & (y - z < x < 2y \text{ のとき}) \\ (x - 2y,\ x - y + z,\ y) & (2y < x \text{ のとき}) \end{cases}$$

先に示したように、この写像は *involution*（ $\psi \circ \psi$ が恒等写像）である。

3　定理の証明

補題 *3.1*　有限集合 $S = \{(x,\ y,\ z) \quad | \quad p = x^2 + 4yz, \quad x,\ y,\ z \in \mathbb{N}\}$ の個数は奇数である。

∵) 写像 ψ による S の不動元は、 $x = y$ を満たすものに限る。このとき、 $p = x^2 + 4xz = x(x + 4z)$ が成り立つ。

p は素数であり、 $x + 4yz > 1$ であるから、 $x = 1, \quad x + 4z = p$ とならなければいけない。$p = 4k + 1$ であるから、 $z = k$ である。

以上により、 ψ はただ *1* つの不動元 $(1, 1, k)$ を持つ。

その他の S の元は、 ψ により、2 つの元で 1 組のペアをつくる。従って、S の元の個数は奇数である。*//*

定理 *3.2* $p \equiv 1 \pmod 4$ であるすべての素数 p は、 $p = a^2 + b^2 \quad (a, b \in \mathbb{N})$ と表すことができる。

∵) 補題 *3.1* および命題 *1.2* により、定理は成り立つ。*//*

4 Zagier の One-Sentence Proof

D. Zagier "A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ *Is a Sum of Two Squares"* は以下のようなものである。

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 \quad ; \quad x^2 + 4yz = p \}$ *defined by*

$$(x, y, z) \quad \mapsto \begin{cases} (x + 2z, z, y - x - z) & if \quad x < y - z \\ (2y - x, y, x - y + z) & if \quad y - z < x < 2y \\ (x - 2y, x - y + z, y) & if \quad 2y < x \end{cases}$$

has exactly one fixed point, so $|S|$ *is odd and the involution defined by* $(x, y, z) \quad \mapsto \quad (x, z, y)$ *also has a fixed point.*

これでは僕にはわからないので、「*4* で割って *1* 余る素数が *2* つの平方数で表されることの“一文証明”」https://wakara.co.jp/mathlog/20210224 [3] を見て少し考えてみたのであった。

なお、ネット上には 「*Why was this visual proof missed for 400 years?*（*Fermat's two square theorem*)」（なぜ、フェルマーの *2* 平方和定理に関するこの視覚的な証明が *400* 年見過ごされてきたのか？） という動画もある。

参考文献

[1] 片山　喜美「$x^2 + y^2 = p \quad (p$ は素数$)$ について」
（http://ja9nfo.web.fc2.com/math/202203FactorizationOfp.pdf 参照）

[2] D. Zagier "A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ *Is a Sum of Two Squares"*

The American Mathematical Monthly, Vol. 97, No. 2 (Feb., 1990), p. 144

[3] 「*4* で割って *1* 余る素数が *2* つの平方数で表されることの“一文証明”」
https://wakara.co.jp/mathlog/20210224