フェルマーの大定理の$n = 3, 4$の場合

岡本　崇志

2004年2月10日

1　研究内容について

今回研究するのは、フェルマーの大定理の $n = 3, 4$ の場合についてである。これを卒業研究の題材に選んだ理由は、初等整数論で証明することができるからである。また、この大定理の内容は、中高生にも理解可能な範囲で、今後教員になる私にとって意義深いものになると思ったからである。

2　フェルマーの大定理について

大定理の内容は次のことである。
『自然数 $n \geq 3$ に対して、次の方程式

$$x^n + y^n = z^n$$

を満たす自然数 x, y, z は存在しない。』
これは、１７世紀半ばにフランスのピエール・ド・フェルマーが、彼の愛読書であるバシェ版の「算術」の余白に書き残したものである。彼自身、そのメモに、「そのことの驚くべき証明を私は見つけたが、これを記すには余白が小さすぎる。」と、記している。それから３００年あまり経った１９９５年、イギリスのアンドリュー・ワイルズによってこの大定理は証明された。

3　記号と用語について

定義
整数 a, b に対して、$b = aq$ となる整数 q があるとき、a は b を割る、a は b の約数である、b は a で割り切れる、b は a の倍数である、などといい、このとき記号で、$a \mid b$ と表す。

定義
整数 a, b に対して、$a \neq 0$ または $b \neq 0$ のとき、それらの共通の約数のうちで最大のものを最大公約数といい、(a, b) と書き表す。

定義

整数 a, b の最大公約数が 1 であるとき、すなわち $(a, b) = 1$ のとき、a と b は互いに素であるという。

4　ピタゴラス数について

補題 1

$$x^2 + y^2 = z^2, \quad (x, y) = 1, \quad x \equiv 0 \pmod 2 \tag{1.1}$$

を満たす正の整数解は

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2 \tag{1.2}$$

で与えられる。また、a, b は以下の条件を満たす整数である。

$$(a, b) = 1, \quad a > b > 0, \quad a + b \equiv 1 \pmod 2 \tag{1.3}$$

(証明)

(1.1) が満たされているとすると、$(x, y) = 1, \quad x \equiv 0 \pmod 2$ より y は奇数である。x が偶数、y が奇数より z は奇数である。また、y と z は互いに素である。よって、$\frac{z-y}{2}, \quad \frac{z+y}{2}$ は共に整数で、互いに素である。(1.1) より $(\frac{x}{2})^2 = (\frac{z+y}{2})(\frac{z-y}{2})$ となり、右辺の 2 つの因数は互いに素だから、共に平方数でなければならない。従って、

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2, \quad a > b > 0, \quad (a, b) = 1$$

なる整数 a, b がある。また、

$$a + b \equiv a^2 + b^2 = z \equiv 1 \pmod 2.$$

逆に、(1.3) を満たす a, b に対し、x, y, z を (1.2) で与えると、

$$x^2 + y^2 = (2ab)^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2,$$

$$x > 0, \quad y > 0, \quad z > 0, \quad x \equiv 0 \pmod 2.$$

また、$(x, y) = d$ ならば、$d \equiv z$ であり、

$$d \equiv y = a^2 - b^2, \quad d \equiv z = a^2 + b^2,$$

即ち、$d \equiv 2a^2, \quad d \equiv 2b^2$ となる。$(a, b) = 1$ だから d は 1 か 2 でなければならない。y は奇数だから $d \neq 2$ なので $d = 1$. ゆえに、$(x, y) = 1$.

5　$x^4+y^4=z^4$ について

定理 1

$x^4+y^4=z^4, \quad x>0, \quad y>0, \quad z>0$ を満たす整数解は存在しない。

この定理が、フェルマーの大定理の $n=4$ の場合である。これからこの定理を証明する。

（証明）

$$x^4+y^4=u^2, \quad (x,y)=1 \tag{2.1}$$

が正の整数解を持たないことを示せば十分である。そこで、(2.1) を満たす解があるとし、u をそのような最小の数とする。そのとき $(x,y)=1$ なので x,y の少なくとも一方は奇数である。
また、$u^2=x^4+y^4\equiv 1$ または $2 \pmod 4$ であるが、$u^2\equiv 2 \pmod 4$ は起こり得ない。従って、

$$u^2=x^4+y^4\equiv 1 \pmod 4.$$

よって、u は奇数、即ち、x,y は一方が奇数で他方は偶数である。
今、x が偶数であるとする。（y を偶数としても、以下の議論は同様である。）そのとき、補題 1 より、次のような整数 a,b が存在する。

$$x^2=2ab, \quad y^2=a^2-b^2, \quad u=a^2+b^2,$$

$$a>0, \quad b>0, \quad (a,b)=1, \quad a+b\equiv 1 \pmod 2.$$

a が偶数、b が奇数なら、$y^2\equiv -1 \pmod 4$ となり、これは起こり得ない。よって、a が奇数で、b が偶数である。そこで、$b=2c$ とおくと、$(\frac{1}{2}x)^2=ac, \quad (a,c)=1$. よって、

$$a=d^2, \quad c=f^2, \quad d>0, \quad f>0, \quad (d,f)=1, \quad d\text{：奇数}$$

とおける。ゆえに、

$$y^2=a^2-b^2=d^4-4f^4$$

移項して、

$$4f^4+y^2=d^4$$

即ち、

$$(2f^2)^2+y^2=(d^2)^2, \quad (2f^2,y)=1.$$

ここで再び、補題１より次のような整数 l, m が存在する。

$$2f^2 = 2lm, \quad d^2 = l^2 + m^2, \quad l > 0, \quad m > 0, \quad (l, m) = 1.$$

$f^2 = lm$ で $(l, m) = 1$ より、

$$l = r^2, \quad m = s^2, \quad r > 0, \quad s > 0$$

とおけ、明らかに $(r, s) = 1$ で、

$$d^2 = r^4 + s^4, \quad d \leq d^2 = a \leq a^2 < a^2 + b^2 = u. \tag{2.2}$$

従って、(2.1) が正の整数解を持ったとすれば、それと同形な (2.2) を得る。しかも、d は u よりも小さな値である。これは u の最小性に反する。よって、定理は証明された。

6　$n = 3$ の場合の証明の準備

$n = 3$ の場合を証明するために次の定理を証明しておく。

定理２

a, b が互いに素で、$a^2 + 3b^2 = s^3$ ならば、

$$a = u(u^2 - 9v^2), \quad b = 3v(u^2 - v^2)$$

となるような整数 u, v が存在する。

この定理を証明するために、次の補題２～６が必要である。

補題２

$(a, b) = 1 \quad (a^2 + 3b^2 : \text{偶数})$ とする。そのとき、次のような整数 u, v が存在する。

$$a + b\sqrt{-3} = (1 \pm \sqrt{-3})(u + v\sqrt{-3}).$$

(証明)

$(a, b) = 1$ で $a^2 + 3b^2$ が偶数になるのは、a, b が共に奇数のときである。このとき、$a + b$ または $a - b$ は４の倍数である。

(1) $a + b$ が４の倍数とすると、$a - 3b$ も４の倍数で、

$$4(a^2 + 3b^2) = (1^2 + 3 \cdot 1^2)(a^2 + 3b^2)$$

$$= (a-3b)^2 + 3(a+b)^2$$

となり、$4(a^2+3b^2)$ は 4^2 で割り切れる。よって、

$$\frac{a^2+3b^2}{4} = \left(\frac{a-3b}{4}\right)^2 + 3\left(\frac{a+b}{4}\right)^2.$$

ここで、$u = \frac{a-3b}{4}, \quad v = \frac{a+b}{4}$ とおくと、u, v は整数で、$\frac{a^2+3b^2}{4} = u^2+3v^2$ となる。このとき、

$$u + v\sqrt{-3} = \frac{a-3b}{4} + \frac{a+b}{4}\sqrt{-3}$$

$$= \frac{(a+b\sqrt{-3})(1+\sqrt{-3})}{4}.$$

よって、

$$a + b\sqrt{-3} = \frac{4(u+v\sqrt{-3})}{1+\sqrt{-3}} = (1-\sqrt{-3})(u+v\sqrt{-3}), \quad (u,v) = 1.$$

(2) $a-b$ が 4 の倍数とすると、$a+3b$ も 4 の倍数で、

$$4(a^2+3b^2) = (1^2+3\cdot 1^2)(a^2+3b^2)$$
$$= (a+3b)^2 + 3(a-b)^2$$

となり、$4(a^2+3b^2)$ は 4^2 で割り切れる。よって、

$$\frac{a^2+3b^2}{4} = \left(\frac{a+3b}{4}\right)^2 + 3\left(\frac{a-b}{4}\right)^2.$$

ここで、$u = \frac{a+3b}{4}, \quad v = \frac{a-b}{4}$ とおくと、u, v は整数で、$\frac{a^2+3b^2}{4} = u^2+3v^2$ となる。このとき、

$$u + v\sqrt{-3} = \frac{a+3b}{4} + \frac{a-b}{4}\sqrt{-3}$$

$$= \frac{(a+b\sqrt{-3})(1-\sqrt{-3})}{4}.$$

よって、

$$a + b\sqrt{-3} = \frac{4(u+v\sqrt{-3})}{1-\sqrt{-3}} = (1+\sqrt{-3})(u+v\sqrt{-3}), \quad (u,v) = 1.$$

補題３

$(a,b)=1,\quad a^2+3b^2$ は奇素数 p で割り切れるとする。そのとき、正の整数 q,r で

$$p=q^2+3r^2$$

と表せる。更に、整数 u,v で

$$a+b\sqrt{-3}=(q\pm r\sqrt{-3})(u+v\sqrt{-3})$$

と表せる。

(証明)

まず、前半を仮定して後半を証明する。

$p=q^2+3r^2$ のとき、

$$(qb+ar)(qb-ar)=b^2(q^2+3r^2)-r^2(a^2+3b^2).$$

よって、p は $qb+ar$ または $qb-ar$ を割り切る。

(1) p が $qb+ar$ を割り切るとする。そのとき、

$$p(a^2+3b^2)=(q^2+3r^2)(a^2+3b^2)$$

$$=(qa-3rb)^2+3(qb+ar)^2$$

は p^2 で割り切れるので、

$$\frac{a^2+3b^2}{p}=\left(\frac{qa-3rb}{p}\right)^2+3\left(\frac{qb+ar}{p}\right)^2.$$

ここで、$u=\frac{qa-3rb}{p},\quad v=\frac{qb+ar}{p}$ とおくと、u,v は整数で、$\frac{a^2+3b^2}{p}=u^2+3v^2$ となる。このとき、

$$u+v\sqrt{-3}=\frac{qa-3rb}{p}+\frac{qb+ar}{p}\sqrt{-3}$$

$$=\frac{(q+r\sqrt{-3})(a+b\sqrt{-3})}{p}$$

よって、

$$a+b\sqrt{-3}=\frac{p(u+v\sqrt{-3})}{q+r\sqrt{-3}}=(q-r\sqrt{-3})(u+r\sqrt{-3}),\quad (u,v)=1.$$

(2) p が $qb-ar$ を割り切るとする。そのとき、

$$p(a^2+3b^2)=(q^2+3r^2)(a^2+3b^2)$$
$$=(qa+3rb)^2+3(qb-ar)^2$$

は p^2 で割り切れるので、

$$\frac{a^2+3b^2}{p}=\left(\frac{qa+3rb}{p}\right)^2+3\left(\frac{qb-ar}{p}\right)^2.$$

ここで、$u=\frac{qa+3rb}{p},\quad v=\frac{qb-ar}{p}$ とおくと、u,v は整数で、$\frac{a^2+3b^2}{p}=u^2+3v^2$ となる。このとき、

$$u+v\sqrt{-3}=\frac{qa+3rb}{p}+\frac{qb-ar}{p}\sqrt{-3}$$
$$=\frac{(q-r\sqrt{-3})(a+b\sqrt{-3})}{p}$$

よって、

$$a+b\sqrt{-3}=\frac{p(u+v\sqrt{-3})}{q-r\sqrt{-3}}=(q+r\sqrt{-3})(u+r\sqrt{-3}),\quad (u,v)=1.$$

補題４

x を a^2+3b^2 の奇数の約数で、$\alpha^2+3\beta^2\quad(\alpha,\beta\in Z)$ のような形をしていないものとする。そのとき、$\frac{a^2+3b^2}{x}$ も $\gamma^2+3\delta^2\quad(\gamma,\delta\in Z)$ のような形をしていない奇数の約数を持つ。

(証明)

$a^2+3b^2=xy\quad(x:$奇数$)$ とする。もしも y が偶数ならば、$2\mid a^2+3b^2$ なので、補題２の証明でみたように、$4\mid a^2+3b^2$ で、

$$x\left(\frac{y}{4}\right)=c^2+3d^2\quad(c,d\in Z).$$

この操作を $\frac{y}{4^k}$ が奇数となるまで続けると、

$$y=p_1p_2\cdots p_n\quad(\text{各 }p_i\text{ は４または奇素数})$$

と書ける。y のすべての奇素数因数が $\gamma^2+3\delta^2\quad(\gamma,\delta\in Z)$ という形をしているならば、補題２の証明と補題３の後半の証明でみたように、

$$a^2+3b^2=p_1(u^2+3v^2)\quad\text{より}\quad\frac{a^2+3b^2}{p_1}=u^2+3v^2$$

これを順次繰り返すことにより、

$$\frac{u^2+3v^2}{p_2}=m^2+3n^2,\cdots,\frac{k^2+3l^2}{p_n}=\alpha^2+3\beta^2$$

となり、x 自身が $\alpha^2+3\beta^2 \quad (\alpha,\beta\in Z)$ のような形になり、仮定に反する。

ここで補題３の前半の証明をする。

(補題３の前半の証明)
x を a^2+3b^2 の任意な奇数因数として、正の整数 q,r で

$$x=q^2+3r^2$$

と表されることを示す。

$$a=mx\pm c,\quad \mid c\mid<\frac{1}{2}x$$

$$b=nx\pm d,\quad \mid d\mid<\frac{1}{2}x$$

とする。すると、

$$c^2+3d^2=(a-mx)^2+3(b-nx)^2$$

$$=(a^2+3b^2)-2(am+3bn)x+(m^2+3n^2)x^2$$

となり、$x\mid a^2+3b^2$ なので、整数 y を使って、$c^2+3d^2=xy$ とおける。
ここで、

$$\mid xy\mid=\mid c\mid^2+3\mid d\mid^2\leq\left(\frac{1}{2}x\right)^2+3\left(\frac{1}{2}x\right)^2=x^2,$$

$x>0$ より $\mid y\mid\leq\mid x\mid$ となる。ここで、もし $x=y$ とすると、$c^2+3d^2=x^2$ となる。
x は奇数なので $x^2\equiv 1 \pmod 4$ である。
$x^2=c^2+3d^2$ で c^2+3d^2 は奇数なので c は偶数、d は奇数である。よって、

$$c^2\equiv 0,\quad d^2\equiv 1 \pmod 4.$$

従って、

$$c^2+3d^2\equiv 3 \pmod 4$$

となり、

$$x^2 \not\equiv c^2 + 3d^2 \quad (mod\, 4)$$

となる。ゆえに、$x^2 \neq c^2 + 3d^2$ となり矛盾する。よって、$x \neq y$ である。ゆえに、$y < x$ となる。
$(c, d) = e$ とする。$e \neq 1$ のとき、もし $e \mid x$ とすると、$e \mid a, \quad e \mid b$ より $(a, b) = 1$ に反する。よって、e は x を割らないので y のほうを割り、

$$f^2 + 3g^2 = xz, \quad (f, g) = 1, \quad z < y$$

とできる。$e = 1$ のときは $y = z$ である。
x が $\alpha^2 + 3\beta^2 \quad (\alpha, \beta \in Z)$ の形をしていないとすると、補題４より、z の奇数因数で $\gamma^2 + 3\delta^2 \quad (\gamma, \delta \in Z)$ のような形をしていないもの w がある。そこで、$a^2 + 3b^2$ の奇数因数で $q^2 + 3r^2 \quad (q, r \in Z)$ のような形をしていないもの x があったとすれば、上のことより、$(f, g) = 1$ な $f^2 + 3g^2$ の奇数因数で、$\gamma^2 + 3\delta^2 \quad (\gamma, \delta \in Z)$ のような形をしていないもの w がある。しかも、$w \leq z \leq y < x$ である。従って、無限降下法により矛盾する。よって結論を得る。

補題５

$(a, b) = 1$ のとき、

$$a + b\sqrt{-3} = \pm(q_1 \pm r_1\sqrt{-3})(q_2 \pm r_2\sqrt{-3}) \cdots (q_n \pm r_n\sqrt{-3})$$

なる分解が得られる。ここに、q_i, r_i は正の整数、$q_i^2 + 3r_i^2$ は４または奇素数を表す $(i = 1, 2, \cdots, n)$.

(証明)
前みたように $2 \mid a^2 + 3b^2$ なら、$4 \mid a^2 + 3b^2$ であった。従って、$a^2 + 3b^2 \neq 1$ なら $a^2 + 3b^2$ は４または奇素数をその因数にもつ。従って、補題２または補題３より、

$$a + \sqrt{-3} = (q \pm r\sqrt{-3})(u + v\sqrt{-3})$$

で、$a^2 + 3b^2$ が奇素数因数 p をもてば、$p = q^2 + 3r^2 \quad (q, r \in Z)$ と表せる。$(u, v) = 1$ なので、$u + v\sqrt{-3}$ に同じ操作をする。以下この操作を繰り返し行い、

$$a + b\sqrt{-3} = (q_1 \pm r_1\sqrt{-3}) \cdots (q_n \pm r_n\sqrt{-3})(u + v\sqrt{-3}),$$

$$u^2+3v^2=1$$

を得る。$u^2+3v^2=1$ より $v=0,\quad u=\pm1$ となり,

$$a+b\sqrt{-3}=\pm(q_1\pm r_1\sqrt{-3})(q_2\pm r_2\sqrt{-3})\cdots(q_n\pm r_n\sqrt{-3})$$

となる。

補題６

$(a,b)=1$ とする。

$$a^2+3b^2=(q_1^2+3r_1^2)\cdots(q_n^2+3r_n^2)$$

を、a^2+3b^2 の奇素数と４による因数分解とする。そのとき、$a+b\sqrt{-3}$ の補題５のような分解は、a^2+3b^2 の上のような分解で符号を除いて完全に決定する。また、$q+r\sqrt{-3}$ と $q-r\sqrt{-3}$ は同時に因数にはなり得ない。

(証明)
p を４または奇素数とするとき、$p=q^2+3r^2$ となるような q,r が符合を除いて一意に決まることをいえばよい。$p=4$ のときは明らかである。
p が奇素数のとき、$p=q\prime^2+3r\prime^2$ をもう１通りの表現とすると、補題３より、

$$q\prime+r\prime\sqrt{-3}=(q\pm r\sqrt{-3})(u+v\sqrt{-3}).$$

よって、

$$p=p(u^2+3v^2)$$

$$u^2+3v^2=1$$

これより、$u=\pm1,\quad v=0.$ 従って、

$$q\prime+r\prime\sqrt{-3}=\pm(q+r\sqrt{-3}).$$

後半は、もし $q+r\sqrt{-3}$ と $q-r\sqrt{-3}$ を共に因数にもてば、整数 q^2+3r^2 を因数にもつことになるが、a,b が互いに素であるので、これはあり得ない。

以上の補題２～６により定理２の証明が可能になる。

(定理２の証明)

$$(a+b\sqrt{-3}) = (u+v\sqrt{-3})^3$$

となるような整数 u, v が存在することをいえばよい。そこで、

$$a^2+3b^2 = p_1 \cdot \cdots \cdot p_n$$

を補題６における因数分解とする。この分解に含まれる２の最高冪を 2^{2k} とする。a^2+3b^2 は立方数なので、$3 \mid k$ である。また、同じ p_i が３の倍数個ずつあらわれるので、$3 \mid n$ である。従って、補題５，６より

$$a+b\sqrt{-3} = \pm(u+v\sqrt{-3})^3 \quad (u, v \in Z).$$

また、$-(u+v\sqrt{-3})^3 = \pm(-u-v\sqrt{-3})^3$ である。よって、

$$a+b\sqrt{-3} = (u+v\sqrt{-3})^3$$

$$= u^3+3u^2v\sqrt{-3}-9uv^2-3v^3\sqrt{-3}$$

$$= (u^3-9uv^2)+(3u^2v-3v^3)\sqrt{-3}$$

より、

$$a = u(u^2-9v^2), \quad b = 3v(u^2-v^2).$$

以上により結論を得る。

7　$x^3+y^3=z^3$ について

定理３

$$x^3+y^3 = z^3, \quad xyz \neq 0$$

を満足する整数解は存在しない。

(証明)
$x^3+y^3 = z^3$ が整数解をもてば、$x^3+y^3+(-z)^3 = 0$ なので、改めて、$x^3+y^3+z^3 = 0, \quad xyz \neq 0$ が整数解をもつとして矛盾を導く。まず、x, y, z は２つずつ互いに素としてよい。このとき、x, y, z のうち２つは奇

数で、残りの１つは偶数になる。そこで、x, y が奇数で z が偶数とする。このもとで、z は $|\, z\, |$ が最小なものとしておく。（他の場合でも以下の議論は同じである。）このとき、

$$x + y = 2a, \quad x - y = 2b$$

とかける。従って、

$$(-z)^3 = x^3 + y^3 = (a+b)^3 + (a-b)^3 = 2a(a^2 + 3b^2) \tag{3.1}$$

となる。そして、a, b は一方が偶数で他方が奇数であり、互いに素でもある。このとき、$a^2 + 3b^2$ は奇数で、８は $2a$ を割り切り、b は奇数である。また、$2a$ と $a^2 + 3b^2$ の公約数は、a と $a^2 + 3b^2$ の公約数である。$(a, b) = 1$ なので、この公約数は３の約数でなければならない。従って、

$$(2a, a^2 + 3b^2) = 1 \quad \text{または} \quad 3$$

となる。
(1)
$(2a, a^2 + 3b^2) = 1$ のとき (3.1) より、$2a$ と $a^2 + 3b^2$ は立法数で、整数 r, s により、

$$2a = r^3, \quad a^2 + 3b^2 = s^3.$$

このとき、定理２より、

$$a = u(u^2 - 9v^2), \quad b = 3v(u^2 - v^2)$$

となる整数 u, v を用いて $s = u^2 + 3v^2$ とかくことができる。このとき、v は奇数、$u \neq 0$、 u は偶数で３で割れない、$(u, v) = 1$ となる。また、

$$r^3 = 2a = 2u(u - 3v)(u + 3v)$$

となる。この各因数 $2u, u - 3v, u + 3v$ を考える。u は偶数、v は奇数より $u - 3v, u + 3v$ は共に奇数である。よって、$2u$ と $u \pm 3v$ の公約数は、u と $u \pm 3v$ の公約数であり、u と $\pm 3v$ の公約数でもある。$(u, v) = 1$、u は偶数より、$(2u, u \pm 3v) = 1$ となる。同様に、$(u - 3v, u + 3v) = 1$ である。従って、$2u, u - 3v, u + 3v$ は２つずつ互いに素である。よって、

$$2u = -l^3, \quad u - 3v = m^3, \quad u + 3v = n^3$$

と０でない整数 l, m, n を使って表せる。このとき、

$$l^3 + m^3 + n^3 = 0$$

である。ここで、u は３で割れないということと、$b \neq 0$ なことから、

$$| z^3 | = | 2a(a^2 + 3b^2) | = | l^3(u^2 - 9v^2)(a^2 + 3b^2) |$$

$$\geq 3 | l^3 | > | l^3 | .$$

これは、$| z |$ の最小性に反する。
(2)
$(2a, a^2 + 3b^2) = 3$ のとき、$a = 3c$ とすると、b は３で割れない。また、

$$(-z)^3 = 2a(a^2 + 3b^2) = 18c(3c^2 + b^2).$$

ここで、$18c$ と $3c^2 + b^2$ は互いに素なので、整数 r, s を使って、

$$18c = r^3, \quad 3c^2 + b^2 = s^3.$$

このとき、(1) と同様に、定理２より、

$$b = u(u^2 - 9v^2), \quad c = 3v(u^2 - v^2)$$

となる整数 u, v を用いて、$s = u^2 + 3v^2$ とかくことができる。そして、

$$\left(\frac{r}{3}\right)^3 = \frac{2}{3}c = 2v(u + v)(u - v).$$

ゆえに、(1) のときと同様にして、$2v, u + v, u - v$ は２つずつ互いに素である。よって、

$$2v = -l^3, \quad u + v = m^3, \quad u - v = -n^3$$

と０でない整数 l, m, n を使って表せる。このとき、

$$l^3 + m^3 + n^3 = 0$$

である。そして、

$$| z^3 | = 18 | c | (3c^2 + b^2) = 54 | v(u^2 - v^2) | (3c^2 + b^2)$$

$$= 27 | l |^3 | u^2 - v^2 | (3c^2 + b^2) \geq 27 | l^3 | > | l |^3 .$$

これは、$| z |$ の最小性に反する。
以上 (1)、(2) により結論を得る。