オイラーと $x^3+y^3=2z^3$

大塚美紀生

定理 整数 $x,\ y,\ z$ が

$$x^3+y^3=2z^3 \tag{1}$$

を満たすならば，$z=0$ または $x=y=z$ である。

この定理は，オイラー (Leonhard Euler) によって 1770 年に示された(→[1])。これと同時に発表され，同じ手法で示された 3 次のフェルマー問題[注1]の陰に隠れてしまった感もあるが，定理の証明で用いられた

補助定理 $a,\ b$ が互いに素な自然数で，a^2+3b^2 が立方数ならば，

$$a=t(t^2-9u^2),\quad b=3u(t^2-u^2) \tag{2}$$

となるような整数 $t,\ u$ が存在する。

にギャップがある(証明されてない)と長い間信じられてきたために，最初に証明したのはオイラーではなく，ルジャンドル (A.M.Legendre) が 1808 年に証明したなどとする書物もある。

ところが，補助定理の内容はオイラー自身により 1760 年に厳密に証明されていたことが，1966 年バーグマン (G.Bergmann) により発見(→[2], [3])されたため，どちらの定理も 1770 年の時点でオイラーが厳密に証明していたことがわかる。

本稿では，上述の主定理について，オイラーがとったであろう証明を辿ってみようと思う。とは言うものの，原典すべてを入手して目を通すことは不可能なので，補助定理の証明は [3] を引用してまとめ直すことにし，主定理の証明は [1] を参考にしながら筆者自らが考えることにした。

その他の初等的証明としては [6] などが，代数的整数論の知識を活かした証明としては [4] (*Theorem 122*) などが知られている。

いくつかの補題

補題 1 a と b がともに奇数であるとき，

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

を満たすような整数 $u,\ v$ が存在する。[注2] さらに，a と b が互いに素ならば，u と v も互いに素である。

(**証明**) $(a+b)+(a-b)=2a$ は 4 で割れない偶数であるから，$a+b$ と $a-b$ の一方は 4 の倍数である。

$a+b$ が 4 の倍数のとき，$a-3b$ も 4 の倍数であり，

$$4(a^2+3b^2)=(1^2+3\cdot1^2)(a^2+3b^2)=(a-3b)^2+3(a+b)^2$$

となることを参考にして

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

とおくと，$u,\ v$ は整数であり，

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

よって，

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

$a-b$ が 4 の倍数のとき，$a+3b$ も 4 の倍数であり，

$$4(a^2+3b^2)=(1^2+3\cdot1^2)(a^2+3b^2)=(a+3b)^2+3(a-b)^2$$

となることを参考にして

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

とおくと，$u,\ v$ は整数であり，

$$a+b\sqrt{3}\,i=(1+\sqrt{3}\,i)(u-v\sqrt{3}\,i)\tag{4}$$

となる。

$$u+3v=a,\quad u-v=\pm b$$

より u と v の最大公約数は a と b の公約数となるから，a と b が互いに素ならば，u と v も互いに素である。　（証明おわり）

補題 2　$a^2+3b^2\,(a,\ b\in\boldsymbol{Z})$ の素因数 p が $p=q^2+3r^2\,(q,\ r\in\boldsymbol{Z})$ の形をしているならば，

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

を満たすような整数 $u,\ v$ が存在する。[注2] さらに，a と b が互いに素ならば，u と v も互いに素である。

（**証明**）$p=q^2+3r^2$ より

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

は素数 p で割り切れるから，$qb+ar$ または $qb-ar$ は p で割り切れる。

$qb+ar$ が p で割り切れるとき

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

は p^2 で割り切れるから，$qa-3rb$ は p で割り切れることになり，

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

とおくと $u,\ v$ は整数であり，

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

よって，

$$a+b\sqrt{3}\,i=\frac{q^2+3r^2}{q+r\sqrt{3}\,i}(u+v\sqrt{3}\,i)=(q-r\sqrt{3}\,i)(u+v\sqrt{3}\,i) \tag{5}$$

$qb-ar$ が p で割り切れるときは

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

とみることにより，

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

はともに整数であり，

$$a+b\sqrt{3}\,i=(q+r\sqrt{3}\,i)(u+v\sqrt{3}\,i) \tag{6}$$

と表される。

$$a=qu\pm 3rv,\quad b=qv\mp ru$$

より u と v の最大公約数は a と b の公約数となるから，a と b が互いに素ならば，u と v も互いに素である。　（証明おわり）

補題 3　a と b が互いに素な整数であるとき，a^2+3b^2 の素因数は 2 または q^2+3r^2 $(q,\ r\in \boldsymbol{Z})$ の形をした素数だけで尽くされ，a^2+3b^2 の素因数分解は

$$a^2+3b^2=2^{2m}({q_1}^2+3{r_1}^2)({q_2}^2+3{r_2}^2)\cdots({q_n}^2+3{r_n}^2)$$

の形$(m,\ n$ は非負整数$)$となる。

（**証明**）　a^2+3b^2 が偶数のときは，$gcd(a,\ b)=1$ より $a,\ b$ はともに奇数であるから，補題 1 より a^2+3b^2 は 4 で割り切れ，$\dfrac{a^2+3b^2}{4}$ も $\alpha^2+3\beta^2$ $(\alpha,\ \beta\in \boldsymbol{Z})$ の形となる。$\dfrac{a^2+3b^2}{4}$ に対してこの操作を繰り返すことにより，補題の証明は

a^2+3b^2 が奇数

である場合に帰着される。

さらに，a^2+3b^2 が q^2+3r^2 $(q,\ r\in \boldsymbol{Z})$ の形の素因数 $p=q^2+3r^2$ をもつとすれば，補題 2 より $\dfrac{a^2+3b^2}{p}$ も $\alpha^2+3\beta^2$ $(\alpha,\ \beta\in \boldsymbol{Z})$ の形となり，この操作を繰り返せば，

a^2+3b^2 が q^2+3r^2 の形の素数を因数にもたない奇数

である場合に補題を証明すれば十分である。このとき $a^2+3b^2=1$ なら証明は完了するので，$a^2+3b^2>1$ として矛盾を導く。

a^2+3b^2 の素因数の一つを s として，

$$a=ms+c,\quad |c|<\frac{1}{2}s\quad (m,\ c\in \boldsymbol{Z})$$

$$b=ns+d,\quad |d|<\frac{1}{2}s\quad (n,\ d\in \boldsymbol{Z})$$

とする。

$$a^2+3b^2=s(m^2s+3n^2s+2mc+6nd)+c^2+3d^2$$

より c^2+3d^2 は s で割り切れ，

$$c^2+3d^2=st \quad (t\in \boldsymbol{N})$$

と表されるが，$c^2+3d^2<\dfrac{s^2}{4}+3\cdot\dfrac{s^2}{4}=s^2$ より

$$s>t$$

である。

ここで，$t=1$ または $t=\dfrac{c^2+3d^2}{s}$ の素因数がすべて $q^2+3r^2\,(q,\ r\in \boldsymbol{Z})$ の形であるとすれば，補題 2 の操作を繰り返すことにより s も $\alpha^2+3\beta^2\,(\alpha,\ \beta\in \boldsymbol{Z})$ の形となって s の仮定に反するから，t の素因数の中に q^2+3r^2 の形でない素数 s_1 が存在し，

$$s>t\geqq s_1$$

次に，素数 s_1 から始めて同じ操作を繰り返すと $q^2+3r^2\,(q,\ r\in \boldsymbol{Z})$ の形でない素数の列

$$s=s_0>s_1>s_2>\cdots$$

が無限に続くことになり，矛盾である。

したがって，a^2+3b^2 は 4 と $q^2+3r^2\,(q,\ r\in \boldsymbol{Z})$ の形の素数で割っていくと最終的には 1 となるので，補題 3 の主張が成り立つ。　　（証明おわり）

補題 4　a と b が互いに素な正の整数であるとき，

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

$(q_i,\ r_i$ は正の整数，${q_i}^2+3{r_i}^2$ は 4 または奇素数$)$

の形に，符号と積の順序を除いて一意的に分解される。また，$q+r\sqrt{3}\,i$ と $q-r\sqrt{3}\,i$ が同時に因数にはなり得ない。

(**証明**) このように分解できることについては補題 1 の(3), (4)，補題 2 の(5), (6)により明らかである。補題 3 により(有理整数の範囲で)

$$a^2+3b^2=2^{2m}({q_1}^2+3{r_1}^2)({q_2}^2+3{r_2}^2)\cdots({q_n}^2+3{r_n}^2)$$

と素因数分解できるから，一意性については各素因数ごとに示せばよい。

$$4=q^2+3r^2 \quad (q,\ r\in \boldsymbol{N})$$

については，直接考察により $q=r=1$ に定まる。

奇素数 $p=q^2+3r^2\,(q,\ r\in \boldsymbol{N})$ について，もう一つの表現を $p=s^2+3t^2\,(s,\ t\in \boldsymbol{Z})$ とすると，補題 2 より

$$s+t\sqrt{3}\,i=(q\pm r\sqrt{3}\,i)(u+v\sqrt{3}\,i)$$

と満たす整数 $u,\ v$ が存在し，

$$p=p(u^2+3v^2) \qquad \therefore\ \ u^2+3v^2=1$$

これより $u=\pm1,\ v=0$ に限られるから

$$s+t\sqrt{3}\,i=\pm(q+r\sqrt{3}\,i) \text{ または } \pm(q-r\sqrt{3}\,i)$$

となって，分解の一意性が成り立つ。

$q+r\sqrt{3}\,i$ と $q-r\sqrt{3}\,i$ がともに $a+b\sqrt{3}\,i$ の因数であるとすれば，$a+b\sqrt{3}\,i$ の分解の中に q^2+3r^2 が含まれる。実部および虚部を比較することにより，$a,\ b$ はともに q^2+3r^2 で割り切れることになり，a と b が互いに素であることに反する。よって，$q+r\sqrt{3}\,i$ と $q-r\sqrt{3}\,i$ が同時に因数にはなり得ない。　（証明おわり）

補助定理の証明

a と b が互いに素な自然数であるとき，補題 3 より

$$a^2+3b^2=2^{2m}({q_1}^2+3{r_1}^2)({q_2}^2+3{r_2}^2)\cdots({q_n}^2+3{r_n}^2)$$

と素因数分解できる。$({q_1}^2+3{r_1}^2)({q_2}^2+3{r_2}^2)\cdots({q_n}^2+3{r_n}^2)$ の部分は奇素数の積であるから，a^2+3b^2 が立方数ならば，

$$3\,|\,2m \text{ かつ } ({q_1}^2+3{r_1}^2)({q_2}^2+3{r_2}^2)\cdots({q_n}^2+3{r_n}^2) \text{ は立方数}$$

である。3 と 2 は互いに素であるから

$$m=3k \quad (k \text{ は非負整数})$$

と表され，

$$2^{2m}=4^{3k}=\{(1^2+3\cdot 1^2)^k\}^3$$

の形となることと各 ${q_j}^2+3{r_j}^2$ は素数であることに注意して，恒等式

$$(x^2+3y^2)(z^2+3w^2)=(xz+3yw)^2+3(xw-yz)^2$$

を用いると，ある整数 $t,\ u$ を用いて[注3]

$$a^2+3b^2=(t^2+3u^2)^3$$

と表される。$-1=(-1)^3$ であることにも注意して，t と u の符号を適当に調節すると，補題 4 より

$$\begin{aligned}a+b\sqrt{3}\,i&=(t+u\sqrt{3}\,i)^3\\&=t^3+3t^2u\sqrt{3}\,i+3t(u\sqrt{3}\,i)^2+(u\sqrt{3}\,i)^3\\&=t^3-9tu^2+(3t^2u-3u^3)\sqrt{3}\,i\end{aligned}$$

となる[注4]から，実部および虚部をそれぞれ比べると

$$a=t(t^2-9u^2),\quad b=3u(t^2-u^2)\quad (t,\ u\in \boldsymbol{Z}) \tag{2}$$

が得られる。　（証明おわり）

主定理の証明

整数 $x,\ y$ が(1)を満たすものとする。

$d = gcd(x,\ y) > 1$ であるとすれば，$x \mapsto \dfrac{x}{d},\ y \mapsto \dfrac{y}{d},\ z \mapsto \dfrac{z}{d}$ と置き換えて考えることができるので，はじめから

$$gcd(x,\ y) = 1$$

としてよい。すると，$x^3 + y^3\ (= 2z^3)$ は偶数であるから，x と y はともに奇数であり，

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

とおくと $p,\ q$ は整数であり，

$$x = a + b,\quad y = a - b \tag{7}$$

(1)に代入して

$$(a+b)^3 + (a-b)^3 = 2z^3$$
$$a(a^2 + 3b^2) = z^3 \tag{8}$$

ここで，a と b が共通の素因数 p をもつとすれば，(7)より x と y が公約数 p をもつことになって x と y が互いに素であることに反するから

$$gcd(a,\ b) = 1$$

であり，

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

1° $gcd(a,\ a^2 + 3b^2) = gcd(a,\ 3) = 1$ のとき

(8)より $a,\ a^2 + 3b^2$ はともに立方数であるから，補助定理より

$$a = t(t+3u)(t-3u) = v^3 \tag{9}$$
$$b = 3u(t^2 - u^2)$$

を満たす整数 $t,\ u,\ v$ が存在する。$t \mid a,\ u \mid b$ より t と u も互いに素であり，a が 3 で割れないことより t も 3 で割れないから

$$gcd(t,\ t \pm 3u) = gcd(t,\ 3u) = 1 \tag{10}$$

t と u がともに奇数であるとすれば，a と b はともに偶数となって互いに素であることに反するから

$$t \not\equiv u \pmod 2$$

したがって，$t + 3u$ と $t - 3u$ はともに奇数であるから，

$$\begin{aligned} gcd(t+3u,\ t-3u) &= gcd\big(t+3u,\ 2t-(t+3u)\big) \\ &= gcd(t+3u,\ 2t) \\ &= gcd(t+3u,\ t) \\ &= gcd(3u,\ t) \\ &= 1 \end{aligned} \tag{11}$$

(9), (10), (11) より

$$t + 3u = f^3,\quad t - 3u = g^3,\quad t = h^3 \tag{12}$$

を満たす整数 $f,\ g,\ h$ が存在して

$$f^3+g^3=2h^3 \tag{13}$$

が得られる。

$ab\neq 0$であるとすれば，(8)より$z\neq 0$であり，方程式(1)は$|z|\,(\geqq 1)$が最小である最小解をもつ。ところが，(8), (9), (12)より

$$|z|>|a|\geqq|t|=|h|^3\geqq|h|$$

であるから，(13)の成立は$|z|$の最小性に反する。よって，

$$a=0 \text{ または } b=0$$

であり，(7), (8)より

$$z=0 \text{ または } x=y=z$$

2° $gcd(a,\ a^2+3b^2)=gcd(a,\ 3)=3$のとき

$a=3c$とおいて(8)を書き直すと

$$9c(3c^2+b^2)=z^3$$

$a=3c$とbは互いに素であり，特にbは3で割れないから

$$\begin{aligned} gcd(9c,\ 3c^2+b^2)&=gcd(c,\ 3c^2+b^2)\\ &=gcd(c,\ b^2)\\ &=1 \end{aligned}$$

であり，$9c$と$3c^2+b^2$はともに立方数である。よって，補助定理より

$$b=t(t^2-9u^2),\quad c=3u(t^2-u^2) \tag{14}$$

を満たす整数$t,\ u$が存在するが，$9c=27u(t^2-u^2)$は立方数であるから

$$u(t+u)(t-u)=(-v)^3=-v^3 \tag{15}$$

を満たす整数vが存在する。$t\,|\,b,\ u\,|\,c\,|\,a$よりtとuも互いに素であるから

$$gcd(u,\ t\pm u)=gcd(u,\ t)=1 \tag{16}$$

tとuがともに奇数であるとすれば，(14)よりaとbはともに偶数となって，互いに素であることに反するから

$$t\not\equiv u \pmod 2$$

したがって，$t+u$と$t-u$はともに奇数であるから，

$$\begin{aligned} gcd(t+u,\ t-u)&=gcd\big(t+u,\ 2t-(t+u)\big)\\ &=gcd(t+u,\ 2t)\\ &=gcd(t+u,\ t)\\ &=gcd(u,\ t)\\ &=1 \end{aligned} \tag{17}$$

となるから，(15)より

$$u+t=f^3,\quad u-t=g^3,\quad u=h^3$$

を満たす整数$f,\ g,\ h$が存在する。

以下，**1°**と同様にして

$$z=0 \text{ または } x=y=z$$

が導かれる。 (証明おわり)

注 1 フェルマー問題(フェルマー予想)とは，n が 3 以上の自然数であるとき

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

を満たす整数 $x,\ y,\ z$ は存在しないという予想のことであり，長年未解決の問題であったが，1994 年ワイルズ(Andrew Wiles)により肯定的に解決された。フェルマー(Pierre de Fermat)自身は $n = 4$ のときを証明しており，冒頭で述べたように，オイラーが $n = 3$ のときを証明した。

注 2 補題 3 を証明するまでであれば，

$$a^2 + 3b^2 = 4(u^2 + 3v^2), \quad a^2 + 3b^2 = (q^2 + 3r^2)(u^2 + 3v^2)$$

を満たす整数 $u,\ v$ の存在を示すだけで十分であるが，補助定理の証明のことを考えて，この段階で $\boldsymbol{Z}[\sqrt{3}\,i\,]$ の議論を済ませ，二度手間を避けている。

注 3 前の補題からの流れを考えれば，

$$a^2 + 3b^2 = (u^2 + 3v^2)^3$$

とした方が見やすいのだが，補助定理の表記にあわせることにした。なお，補助定理の文字の使い方は，オイラーの原典[1]にあわせたものである。

注 4 補題 4 は，単に分解可能というだけでなく，$q + r\sqrt{3}\,i$ と $q - r\sqrt{3}\,i$ が同時には因数にならないことをも意味するので，$(q^2 + 3r^2)^3$ が $a^2 + 3b^2$ の因数であることが $\boldsymbol{Z}[\sqrt{3}\,i\,]$ において $(q + r\sqrt{3}\,i)^3$ と $(q - r\sqrt{3}\,i)^3$ のいずれか一方のみが $a + b\sqrt{3}\,i$ の因数になることを示している。

参考文献

[1] L.Euler, *Auflösung solcher Fragen, worzu Cubi erfordert werden*, Opera Omnia, (1), I, Capital 15, 484-498

[2] 足立恒雄，フェルマーの大定理，筑摩書房 (2006)

[3] 平松豊一・宇津木博，フェルマ予想入門，槙書店 (1988)

[4] T.Nagell, *Introduction to number theory*, Chelsea (1981)

[5] W.Sierpiński, *Elementary Theory of Numbers*, North - Holland (1988).

[6] A.Wakulicz, *On the equation* $x^3 + y^3 = 2z^3$, Colloq. Math. 5, 11 - 15 (1957)

2009.2.15