三角立方数・四面立方数について

清水　一慶　　友澤　啓太　　最上　伸一

2011/08/27

1　はじめに

昨年小倉で開催された数学コンソーシアムで、我々は研究報告 “On Trianglar-Square Numbers” を発表した．これを、同年の 12 月 20 日、奈良先端科学技術大学（NAIST）でも発表した際、質疑応答の時間にある質問が呈された．それは、「今回三角数かつ平方数である数について研究していたが、例えば三角数かつ立方数である数を研究してみる予定はあるか.」といった内容である．我々はそれまで立方数についても考えようと思ったことはなく、この質問は我々にとって驚くべき質問だった．その場での応答では「今後の研究課題とします」とした．そして発表会が終わってから早速この問題に取り組み始めたが、かなりの困難を要した．しかし、この問題を考察し続けたところ、ある程度まで結果が得られたので、その内容をレポートにまとめることにした.

2　三角立方数

N が三角数かつ立方数である自然数とすると，ある自然数 m, k が存在し，

$$N = \frac{1}{2}m(m+1) = k^3$$

と表せる．ここで，m と $m+1$ は互いに素であるから，$m, m+1$ についての条件は

(i) m が立方数で，$m+1$ が立方数を 2 倍した自然数である．

(ii) $m+1$ が立方数で，m が立方数を 2 倍した自然数である．

(i) の場合，$m = x^3$，$m+1 = 2y^3$（$x, y \in \mathbb{Z}$）とおけて，

$$x^3 - 2y^3 = -1$$

(ii) の場合，$m = 2y^3$，$m+1 = x^3$（$x, y \in \mathbb{Z}$）とおけて，

$$x^3 - 2y^3 = 1$$

となる．ゆえに，三角立方数の一般項を求めるには,

$$x^3 - 2y^3 = \pm 1$$

を満たす自然数の組 (x, y) を求めることが必要かつ十分である．

3　四面立方数

ここで少し立ち返って，三角数，平方数の意味について考えよう．

三角数とは、その数の碁石を用意し，平面上に正三角形の形に並べられる数である．また，平方数とは，その数の碁石を，平面上に正方形を形作るように並べられる数である．

では立方数ではどうか．立方数の数の碁石を用意すると，その碁石を並べるという表現をすると少し変にはなるが，空間内で立方体を形成するように並べられる．ならば，碁石を空間内で正四面体を形成するように並べられる数を考えてみるのもいいかもしれない．よってこれからその数を四面数と呼ぶことにし，その一般項 T を求めてみる．

一辺が m 個の正四面体であれば，一辺が 1 から m までの正三角形を積み上げていけば正四面体ができあがる．ゆえに，

$$\begin{aligned} T &= \sum_{k=1}^{m} \frac{1}{2}k(k+1) \\ &= \frac{1}{6}m(m+1)(m+2) \end{aligned}$$

となる．これが四面数の一般項である．

ではここで，四面数かつ立方数である数を考えてみよう．N を四面立方数とすると，

$$N = \frac{1}{6}m(m+1)(m+2) = k^3$$

なる自然数 m, k が存在する．変形すると，

$$m(m+1)(m+2) = 6k^3$$

m，$m+1$，$m+2$ は連続 3 整数より，3 以上の因数を共有することはない．素因数 2 を共有するならば，m と $m+2$ が共有する．ゆえに，

(i) m，$m+2$ が偶数のとき．

(ii) $m+1$ が偶数のとき．

に場合分けすることができる．

(i) のとき，$m = 2t$ とおけて，上式に代入すると，

$$2t(t+1)(2t+1) = 3k^3$$

2 と 3 は互いに素より，k^3 は 2 を素因数にもつ．つまり，k は 2 の倍数である．ゆえに，$k = 2l$（$l \in \mathbb{N}$）と表せて，上式に代入すると，

$$t(t+1)(2t+1) = 12l^3$$

いま，t，$t+1$，$2t+1$ は対ごとに素であり，$2t+1$ は奇数である．ゆえに，自然数 x，y，z を用いて，

$$\begin{aligned} (t, t+1, 2t+1) &= (2^2 \cdot 3x^3, y^3, z^3),\ (2^2x^3, 3y^3, z^3),\ (2^2x^3, y^3, 3z^3) \\ &\quad (3x^3, 2^2y^3, z^3),\ (x^3, 2^2 \cdot 3y^3, z^3),\ (x^3, 2^2y^3, 3z^3) \end{aligned}$$

と表される．これらは，それぞれ，

$$\begin{aligned}(m, m+1, m+2) &= (3\cdot(2x)^3, z^3, 2y^3),\ ((2x)^3, z^3, 6y^3),\ ((2x)^3, 3z^3, 2y^3)\\ &\quad (6x^3, z^3, (2y)^3),\ (2x^3, z^3, 3\cdot(2y)^3),\ (2x^3, 3z^3, (2y)^3)\end{aligned}$$

となる．

(ii) のとき，m，$m+1$，$m+2$ は対ごとに素より，

$$(m, m+1, m+2) = (3x^3, 2y^3, z^3), (x^3, 6y^3, z^3), (x^3, 2y^3 3z^3)$$

(i)，(ii) を考えると，

$$x^3 - 2y^3 = \pm 1$$

$$x^3 - 3y^3 = \pm 1$$

$$x^3 - 6y^3 = \pm 1$$

の自然数解 (x, y, z) が求められるかどうかがとても重要な鍵になる．

私は，この解について Excel で地道に探してみた．しかし，$x^3 - 2y^3 = \pm 1$ における解 $(1, 1)$ が得られただけで，他の解は全く得ることができなかった．ゆえに，

$$x^3 - Ny^3 = \pm 1$$

について，$N = 2$ のときは解 $(1, 1)$ のみが，$N = 3, 6$ のときは自然数解が存在しないことを示すのを目標に議論していく．

4 準備

これから，次の議論に必要な準備をすることにする．

i を虚数単位とし，$\omega = \frac{-1+\sqrt{3}i}{2}$，つまり 1 の虚立方根とする（$\omega^2 + \omega + 1 = 0$ が成り立つ）．

α の共役複素数を $\overline{\alpha}$ と表すことにする．

また集合 R を $R = \mathbb{Z}[\omega]$ とする．$\omega^2 = -1 - \omega$ より，R の任意の元は $a + b\omega$（$a, b \in \mathbb{Z}$）で表される．R は整域である．(R の元は，一般に Eisenstein 整数と呼ばれる.)

R の単元のみからなる群（単数群）を R' とする．

また，$\lambda = 1 - \omega$ とする．

R の元 α と素元 π に対し，

$$\mathrm{ord}_\pi(\alpha) = \max\{k | \pi^k \text{ は } \alpha \text{ を割り切る }\}$$

と定義する．

補題 1 $\alpha = a + b\omega \in R$ に対し，$D(\alpha) = a^2 - ab + b^2$ とすると，R の元には，$D(\alpha)$ を大きさとする除法の定理が成り立つ．すなわち R の元 α と $\beta \neq 0$ に対し，

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

なる R の元 γ, δ が存在する．

証明　R の元 θ, ϕ に対し，$D(\theta) \geqq 0$，$D(\theta\phi) = D(\theta)D(\phi)$ が成り立つ．

いま，$\dfrac{\alpha}{\beta} = \gamma' = p+q\omega$ なる有理数 p, q に対し，それぞれに最も近い整数を c, d とする．$\gamma = c+d\omega$ とし，$\alpha - \beta\gamma = \delta$ とすれば，γ, δ は R の元であり，$|p-c| \leqq \dfrac{1}{2}$，$|q-d| \leqq \dfrac{1}{2}$ より，

$$\begin{aligned} D(\delta) &= D(\alpha - \beta\gamma) \\ &= D(\beta\gamma' - \beta\gamma) \\ &= D(\beta)D(\gamma' - \gamma) \\ &= D(\beta)\left\{(p-c)^2 + (q-d)^2\right\} \\ &\leqq D(\beta)\left\{\frac{1}{4} + \frac{1}{4}\right\} \\ &< D(\beta) \qquad \blacksquare \end{aligned}$$

補題 2 R は単項イデアル整域である．

証明　R の任意のイデアルを I とする．

I が零イデアルならば，$I = (0)$ より，I は単項イデアル．

I が 0 以外の元を含むとき，零元でない I の元のうち，大きさ D が最小のものを β とする．

I の任意の元 α には，補題 1 より，

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

なる $\gamma, \delta \in R$ が存在する．$\alpha, \beta \in I$ より，$\delta = \alpha - \beta\gamma \in I$ となるが，$D(\beta)$ の最小性より，$D(\delta) = 0$，すなわち $\delta = 0$ となる．ゆえに，$\alpha = \beta\gamma$ となり，$I = (\beta)$ であるため，I は単項イデアル．

以上より，R の任意のイデアルは単項イデアルであるため，示された．$\blacksquare$

補題 3 R の元には素元分解の一意性が成り立つ

今回はこの証明は省く．

補題 4 $\alpha = a + b\omega \in R$ とすると，$\overline{\alpha} = a - b - b\omega$

証明

$$\begin{aligned} \overline{\alpha} &= \overline{\alpha + b\omega} \\ &= a + b\overline{\omega} \\ &= a + b(-1-\omega) \\ &= a - b - b\omega \qquad \blacksquare \end{aligned}$$

補題 5 $\alpha \in R$ ならば，$\alpha\overline{\alpha}$ は非負整数．

証明　$\alpha = a + b\omega$（$a, b \in \mathbb{Z}$）とおくと，

$$\begin{aligned} \alpha\overline{\alpha} &= (a+b\omega)(a-b-b\omega) \\ &= a^2 - ab + b^2 \in \mathbb{Z} \qquad \blacksquare \end{aligned}$$

補題 6 $R' = \{\pm 1, \pm\omega, \pm\overline{\omega}\}$ である．

証明　α を R の単元とすると，ある $\beta \in R$ が存在し，$\alpha\beta = 1$ となる．
　$1 = D(\alpha\beta) = D(\alpha)D(\beta)$ となるが，$D(\alpha), D(\beta)$ はそれぞれ非負整数より，$D(\alpha) = 1$
　よって，$\alpha = a + b\omega$（$a, b \in \mathbb{Z}$）とおくと，

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

$$\Leftrightarrow \quad \left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2 = 1$$

　$|b| \geqq 2$ ならば,

$$\left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2 \geqq \frac{3}{4} \cdot 2^2 > 1$$

となるため，$|b| \leqq 1$ である．この下で a, b を探し α を求めると，

$$\alpha = \pm 1, \pm\omega, \pm\overline{\omega} \qquad \blacksquare$$

補題 7 x, y を 0 でない整数とするとき，

$$x \text{ と } y \text{ が } \mathbb{Z} \text{ 上で互いに素} \quad \Leftrightarrow \quad x \text{ と } y \text{ が } R \text{ 上で互いに素}$$

証明　（$\Leftarrow$）は明らか.（$\Rightarrow$）は背理法による．x と y が共通の素元 π を持つとすると，$x = \pi\alpha$，$y = \pi\beta$ と表せる．このとき，

$$x^2 = (\pi\alpha)^2 = \pi\alpha\overline{\pi\alpha} = (\pi\overline{\pi})(\alpha\overline{\alpha})$$

$$y^2 = (\pi\beta)^2 = \pi\beta\overline{\pi\beta} = (\pi\overline{\pi})(\beta\overline{\beta})$$

となる．ここで，x と y は $\mathbb{Z}$ 上で互いに素であるから，x^2 と y^2 も $\mathbb{Z}$ 上で互いに素．しかしながら，補題 5 より $\pi\overline{\pi}$ は整数であり，π は素元であるから $\pi\overline{\pi} \neq 1$．これは x^2 と y^2 が互いに素であることに矛盾する．以上より，示された．$\blacksquare$　（これは R，$\mathbb{Z}$ 双方の，互いに素の概念が一致することを表す.）

補題 8 λ は R の素元である．

証明　$\lambda(x + \omega y) = 1 \quad \Leftrightarrow \quad x = \dfrac{2}{3}, y = \dfrac{1}{3}$ より，λ は R の単元ではない．
　ここで π を，λ を割り切る R の素元とすると，$\lambda = \pi\alpha$（$\alpha \in R$）と表せる．

$$3 = \lambda\overline{\lambda} = (\pi\overline{\pi})(\alpha\overline{\alpha})$$

　補題 5 より，$\pi\overline{\pi}, \alpha\overline{\alpha}$ は非負整数で，π は素元より $\pi\overline{\pi} \neq 1$．ゆえに，$\pi\overline{\pi} = 3$，$\alpha\overline{\alpha} = 1$ である．
　よって，α は単元であるから，λ は素元 π と同伴である．ゆえに示された．$\blacksquare$

補題 9 3 と λ^2 は同伴である．

証明　$3 = -\overline{\omega}\lambda^2 \quad -\overline{\omega} \in R'$　$\blacksquare$

補題 10 λ と $\overline{\lambda}$ は同伴である．

証明　$\overline{\lambda} = -\overline{\omega}\lambda \quad -\overline{\omega} \in R'$　$\blacksquare$

補題 11 2 は R の素元である．

証明　2 は明らかに R の単元ではない．

π を，2 を割り切る R の素元とすると，$2 = \pi\alpha$（$\alpha \in R$）と表せる．

$$4 = (\pi\alpha)^2 = \pi\alpha \cdot \overline{\pi\alpha} = (\pi\overline{\pi})(\alpha\overline{\alpha})$$

補題 5 より，$\pi\overline{\pi}, \alpha\overline{\alpha}$ は非負整数で，π は素元より $\pi\overline{\pi} \neq 1$．また，$\alpha\overline{\alpha} = 2$ となる $\alpha \in R$ は存在しない．ゆえに，$\pi\overline{\pi} = 4$，$\alpha\overline{\alpha} = 1$ である．

よって，α は単元であるから，2 は素元 π と同伴である．よって示された．■

補題 12 x, y が $\mathbb{Z}$ 上で互いに素な整数のとき，R の素元 π が,

$$x - y, \qquad x - \omega y, \qquad x - \overline{\omega} y$$

のいずれか 2 つを割り切れば，π と λ は同伴である．

証明　まず，補題 7 より，x, y は R 上で互いに素である．

(i) π が $x - y$ と $x - \omega y$ を割り切るとき，$\lambda y = (x - \omega y) - (x - y)$ は，π で割り切れる．仮に π が λ と同伴でないとすると，π は y を割り切らなければならない．このとき $x = (x - y) + y$ より，x は π で割り切れる．これは x, y が R 上で互いに素であることに矛盾する．

(ii) π が $x - \omega y$ と $x - \overline{\omega} y$ を割り切るとき，$\omega\lambda y = (x - \omega y) - (x - \overline{\omega} y)$ より,（　）と同様に議論でき，π と λ は同伴.

(iii) π が $x - \overline{\omega} y$ と $x - y$ を割り切るとき，$\overline{\omega}\lambda = (x - \overline{\omega} y) - (x - y)$ より,（　）と同様に議論でき，π と λ は同伴.

以上より，示された．■

補題 13 剰余環 $R/2R$ は四つの類からなり，その完全剰余系は

$$0, \qquad 1, \qquad \omega, \qquad 1 + \omega$$

である．

証明　R の二元 $a + b\omega$、$c + d\omega$ に対し，

$$a + b\omega \equiv c + d\omega \pmod{2R}$$

$$(a + b\omega) - (c + d\omega) \in 2R$$

$$(a - c) + (b - d)\omega \in 2R$$

よって，ある R の元 $p + q\omega$ が存在し，

$$(a - c) + (b - d)\omega = 2(p + q\omega)$$

と表せる．ゆえに,

$$(a - c - 2p) + (b - d - 2q)\omega = 0$$

$$\therefore \begin{cases} a - c = 2p \\ b - d = 2q \end{cases}$$

よって，$a + b\omega \equiv c + d\omega (\mathrm{mod}\ 2R)$ ならば,

$$a \equiv c \pmod{2\mathbb{Z}}, \qquad b \equiv d \pmod{2\mathbb{Z}}$$

逆にこのとき，$a + b\omega \equiv c + d\omega (\mathrm{mod}\ 2R)$　ゆえに，完全剰余系は上に表されるものである．■

なお，このとき，

$$\pm 1 \equiv 1, \qquad \pm\omega \equiv \omega, \qquad \pm\omega^2 \equiv 1 + \omega \pmod{2R},$$

$$1^3 \equiv \omega^3 \equiv (1+\omega)^3 \equiv 1 \pmod{2R}$$

が成り立つ．

5　$x^3 - 3y^3 = \pm 1$ について

$N = 3$ のとき，自然数解 (x, y) が存在しないことを示すのが目標だったのだが，これをもっと一般化して，

$$x^3 - 3y^3 = z^3$$

を満たす $xyz \neq 0$ なる整数解 (x, y, z) が存在しないことを示す．

背理法によって示す．この方程式が $xyz \neq 0$ なる整数解をもつと仮定すると，$\max\{|x|, |y|, |z|\}$ が最小となる解が存在し，それを改めて (x, y, z) とおく．

x, y, z のうちいずれか二つが共通因数を持てば y もその因数をもち，$\max\{|x|, |y|, |z|\}$ の最小性に反する解が得られるため，x, y, z は対ごとに素である．

方程式を変形すると

$$3y^3 = (x - z)(x - \omega z)(x - \overline{\omega} z)$$

補題 9 よりこの左辺は λ^2 で割り切れる．また，

$$x - z \equiv x - \omega z \equiv x - \overline{\omega} z \pmod{\lambda R}$$

より，$x - z, x - \omega z, x - \overline{\omega} z$ はすべて λ で割り切れる．

ゆえに，$\mathrm{ord}_\lambda(y^3) \geqq 3 - 2 = 1$ より，素元 λ は y^3 を割り切るため，y を割り切る．ゆえに，y^3 は λ^2 で割り切れ，すなわち 3 で割り切れる．3 は $\mathbb{Z}$ における素数であるため，y は 3 で割り切れる．そのため，y^3 は 27 の倍数である

ここで，$x - \omega z$ が λ^2 で割り切れるとき，

$$x - \omega z \in \lambda^2 R \quad \Leftrightarrow \quad x - \omega z \in 3R \quad \Leftrightarrow \quad x \equiv z \equiv 0 \pmod{3\mathbb{Z}}$$

より，x, z は互いに素でなくなるから，$\mathrm{ord}_\lambda(x - \omega z) = 1$ である．$x - \overline{\omega} z$ についても同様にいえて，$\mathrm{ord}_\lambda(x - \overline{\omega} z) = 1$ である．ゆえに，$\mathrm{ord}_\lambda(x - z) \geqq 8 - 2 = 6$ であり，$x - z$ は 27 で割り切れる．

以上から，

$$x - z = 27r, \quad x - \omega z = \lambda\epsilon, \quad x - \overline{\omega} z = \overline{\lambda}\overline{\epsilon} \quad (r \in \mathbb{Z}, \epsilon \in R)$$

とおける．これを代入して，

$$3y^3 = 27r \cdot \lambda\epsilon \cdot \overline{\lambda}\overline{\epsilon} \quad \Leftrightarrow \quad \left(\frac{y}{3}\right)^3 = r\epsilon\overline{\epsilon}$$

ここで，$r, \epsilon, \overline{\epsilon}$ がどの 2 つも互いに素であることを示す．もし，$r, \epsilon, \overline{\epsilon}$ のうちどれか 2 つが素元 π で割り切れれば，$x-z, x-\omega z, x-\overline{\omega}z$ のうちどれか 2 つが π で割り切れる．よって補題 12 より，π と λ は同伴である．ところが，$r, \epsilon, \overline{\epsilon}$ のうちどれか 2 つを選ぶとき，必ず ϵ または $\overline{\epsilon}$ を含むので，$\epsilon, \overline{\epsilon}$ のうち少なくとも 1 つは λ で割り切れる．これは，

$$\mathrm{ord}_\lambda(x-\omega z) = \mathrm{ord}_\lambda(x-\overline{\omega}z) = 1$$

に反する．よって，$r, \epsilon, \overline{\epsilon}$ はどの 2 つも互いに素である．

ゆえに，

$$r = u\beta^3, \quad \epsilon = v\alpha^3, \quad \overline{\epsilon} = \overline{v}\overline{\alpha}^3 \quad (u, v \in R', \alpha, \beta \in R)$$

と表せる．

r について，

$$r^2 = u\beta^3 \cdot \overline{u}\overline{\beta}^3 = \left(\beta\overline{\beta}\right)^3$$

より，r^2 は整数の三乗で表されるため，r は立方数である．ゆえに，$r = c^3$ と表せる．$(c \in \mathbb{Z})$

ここで，x, y, z の奇偶により，次のように場合分けする．

(I) x が偶数で，y, z が奇数である．

(II) y が偶数で，z, x が奇数である．

今，x, y, z は互いに素であり，z が偶数のとき，

$$x^3 - 3y^3 = z^3 \quad \Leftrightarrow \quad z^3 - 3(-y)^3 = x^3$$

とできるので，(I) と同等である．ゆえに，この場合分けは十分である．

(I) のとき，

$$v\lambda\alpha^3 = x - \omega z \equiv -\omega \pmod{2R}$$

補題 13 より，$\alpha^3 \equiv 1 \pmod{2R}$ であるから，

$$v(1-\omega) \equiv -\omega \quad \Leftrightarrow \quad v \equiv 1 + \omega \pmod{2R} \quad \therefore\ v = \pm\overline{\omega}$$

ゆえに，

$$x - z = 27c^3, \tag{1}$$

$$x - \omega z = \overline{\omega}\lambda\alpha^3, \tag{2}$$

$$x - \overline{\omega}z = \omega\overline{\lambda}\overline{\alpha}^3 \tag{3}$$

と表せる．$\alpha = a + b\omega \quad (a, b \in \mathbb{Z})$ とおくと，(2)，(3) より，

$$\begin{cases} x = -2a^3 + 3a^2b + 3ab^2 - 2b^3 \\ z = a^3 + 3a^2b - 6ab^2 + b^3 \end{cases} \tag{4}$$

ゆえに，

$$x - z = -3a^3 + 9ab^2 - 3b^3$$

(1) より，

$$-9c^3 = a^3 - 3ab^2 + b^3$$

$$\Longrightarrow \quad a^3 + b^3 \equiv 0 \pmod{3\mathbb{Z}}$$

ところが，(4) より $x \equiv z \equiv 0 (\bmod 3)$ となり，x と z が互いに素であることに矛盾する．

(II) のとき，

$$v\lambda\alpha^3 = x - \omega z \equiv \lambda \pmod{2R}$$

よって補題 13 より，$\lambda^3 \equiv \alpha^3 \equiv 1$ であるから，$v \equiv 1 \quad \therefore v = \pm 1$

ゆえに，

$$x - z = 27c^3, \tag{5}$$

$$x - \omega z = \lambda\alpha^3, \tag{6}$$

$$x - \overline{\omega} z = \overline{\lambda}\overline{\alpha}^3 \tag{7}$$

と表せる．$\alpha = a + b\omega \quad (a, b \in \mathbb{Z})$ とおくと，(6)，(7) より，

$$\begin{cases} x = a^3 + 3a^2b - 6ab^2 + b^3 \\ z = a^3 - 6a^2b + 3ab^2 + b^3 \end{cases}$$

よって，

$$x - z = 9ab(a - b)$$

(5) より，

$$3c^3 = ab(a - b)$$

仮に $a, b, a - b$ のうち 2 つを割り切る素数 l が存在すれば，l は a, b を割り切るため，x, z は素因数に l をもつ．これは，x と z が互いに素であることに反する．ゆえに，$a, b, a - b$ は対ごとに素であり，3 は素数であるから，

$$(a, b, a - b) = (x'^3, 3y'^3, z'^3),\ (3y'^3, -z'^3, x'^3),\ (z'^3, x'^3, -3y'^3)$$

とおける (x', y', z' は 0 でない整数)．上のどの場合においても，

$$x'^3 - 3y'^3 = z'^3$$

を満たすため，(x', y', z') は方程式の解である．

ところが，

$$y^3 = 9x'^3y'^3z'^3(x - \omega z)(x - \overline{\omega} z)$$

より，

$$\max\left\{|x'|^3, |y'|^3, |z'|^3\right\} < |y|^3 \leqq \max\left\{|x|^3, |y|^3, |z|^3\right\}$$

$$\text{よって，} \quad \max\{|x'|, |y'|, |z'|\} < \max\{|x|, |y|, |z|\}$$

これは，$\max\{|x|,|y|,|z|\}$ の最小性に矛盾する．

以上より，仮定は誤りで，

$$x^3-3y^3=z^3$$

は，$xyz\neq 0$ なる整数解を持たない．■

よって，演繹的に，$z=\pm 1$ のときも解をもたないので

$$x^3-3y^3=\pm 1$$

は，自然数解 (x,y) をもたない．

6 $x^3-2y^3=\pm 1$ について

$N=2$ のとき，自然数解が $(x,y)=(1,1)$ 以外にもたないことを示すことが目標であったが，ここでも一般化して

$$x^3-2y^3=z^3$$

を満たす自然数解はすべて $(x,y,z)=(n,n,-n)\quad(n\in\mathbb{Z})$ で与えられることを示す．

$(x,y,z)=(n,n,-n)$ は方程式の解であるから，$(x,y,z)\neq(n,n,-n)$ なる解が存在しないことを示せばよい．これを背理法によって示す．このような解が存在すると仮定して，そのうち $\max\{|x|,|y|,|z|\}$ が最小のものを改めて (x,y,z) とおく．

$x=z=n$ ならば $y=n$ となり仮定に反するので，$x\neq z$ である．また，x,y,z は対ごとに素でなければならない．両辺 2 を法とする整数における剰余類をとると，$x^3\equiv z^3$ より，$x\equiv z$ である．x,z は互いに素であるから，x,z は奇数である．式を変形して，

$$2y^3=(x-z)(x-\omega z)(x-\overline{\omega}z) \tag{8}$$

ここで，y について以下の 2 つに場合分けをする．

(I) y が 3 で割り切れないとき．

(II) y が 3 で割り切れるとき．

(I) のとき，

$$x-z,\quad x-\omega z,\quad x-\overline{\omega}z$$

のうち，いずれか 2 つを割り切る素元 π が存在すれば，補題 12 から，π と λ は同伴である．しかし，(8) の左辺は λ^2 で割り切れるため，補題 9 より 3 で割り切れる．これは右辺が 3 で割り切れないことに反する．よって，これらは対ごとに素である．

また $x-z$ は 2 で割り切れるので，$x-z=2r\quad(r\in\mathbb{Z})$ とおいて (8) に代入すると，

$$y^3=r(x-\omega z)(x-\overline{\omega}z)$$

$r,x-\omega z,x-\overline{\omega}z$ はどの 2 つも互いに素より，

$$r = u\beta^3, \qquad x - \omega z = v\alpha^3, \qquad x - \overline{\omega} z = \overline{v\alpha}^3 \quad (u, v \in R', \alpha, \beta \in R)$$

と表せる．

r については，第 5 章と同様の議論より，r は立方数となるから，$r = c^3$ とおきなおせる．

また，x, z は奇数より，

$$v\alpha^3 = x - \omega z \equiv 1 + \omega \pmod{2R}$$

$\alpha^3 \equiv 1$ より，$v \equiv 1 + \omega (\mathrm{mod}\ 2R)$．よって，$v = \pm\overline{\omega}$ である．

ゆえに，

$$x - z = 2c^3, \tag{9}$$

$$x - \omega z = \overline{\omega}\alpha^3, \tag{10}$$

$$x - \overline{\omega} z = \omega\overline{\alpha}^3 \tag{11}$$

となる．$\alpha = a + b\omega \quad (a, b \in \mathbb{Z})$ とおくと，(10)，(11) より，

$$\begin{cases} x = -a^3 + 3a^2 b - b^3 \\ z = a^3 - 3ab^2 + b^3 \end{cases} \tag{12}$$

よって，

$$x - z = (a + b)(2a - b)(2b - a)$$

(9) より，

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

仮に，$a + b, 2a - b, 2b - a$ のうち，どれか 2 つを割り切る素数 l が存在すれば，l は

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

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

を割り切る．l は $x - z$ を割り切るので，$2y^3$ の素因数であるから，l は 3 ではない．よって，a, b は l で割り切れる．ところが (12) より，x, z は共に l で割り切れ，互いに素であることに反する．ゆえに，$a + b, 2a - b, 2b - a$ はどの 2 つも互いに素であり，2 は素数であるから，

$$(a + b, 2a - b, 2b - a) = (x'^3, 2y'^3, z'^3),\ (2y'^3, -z'^3, x'^3),\ (z'^3, x'^3, -2y'^3)$$

とおける（x', y', z' は 0 でない整数）．これらのどの場合においても，

$$x'^3 - 2y'^3 = z'^3$$

を満たすため，(x', y', z') は方程式の解である．

この (x', y', z') について，

$$y^3 = x'^3 y'^3 z'^3 (x - \omega z)(x - \overline{\omega} z)$$

より，

$$\max\left\{|x'|^3, |y'|^3, |z'|^3\right\} \leqq |y|^3 \leqq \max\left\{|x|^3, |y|^3, |z|^3\right\}$$

$\max\left\{|x'|^3, |y'|^3, |z'|^3\right\} \leqq |y|^3$ の等号が成立するための必要条件は，

$$|(x - \omega z)(x - \overline{\omega} z)| = 1$$

(10)，(11) より，$|\alpha\overline{\alpha}|^3 = 1$．ゆえに，$|\alpha\overline{\alpha}| = 1$．よって，

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

これを満たす整数 a, b は，$(a,b) = (1,1)$ または $(1,0)$ である．ところが，このとき，$(x,z) = (1,-1), (-1,1)$ より，$x \neq -z$ に反する．

ゆえに，等号は成立せず，

$$\max\{|x'|, |y'|, |z'|\} < \max\{|x|, |y|, |z|\}$$

である．これは，$\max\{|x|, |y|, |z|\}$ の最小性に矛盾する．

(II) のとき，第 5 章と同様の議論により，$x-z, x-\omega z, x-\overline{\omega}z$ はすべて λ で割り切れ，

$$\mathrm{ord}_\lambda(x-\omega z) = \mathrm{ord}_\lambda(x-\overline{\omega}z) = 1$$

である．また，$o_\lambda(x-z) \geqq 6-2 = 4$ より，$x-z$ が偶数であることもふまえて，

$$x-z = 18r, \quad x-\omega z = \lambda\epsilon, \quad x-\overline{\omega}z = \overline{\lambda}\overline{\epsilon} \quad (r \in \mathbb{Z}, \epsilon \in R)$$

と表せる．このとき，

$$2y^3 = 18r \cdot \lambda\epsilon \cdot \overline{\lambda}\overline{\epsilon} \quad \Leftrightarrow \quad \left(\frac{y}{3}\right)^3 = r\epsilon\overline{\epsilon}$$

$r, \epsilon, \overline{\epsilon}$ は対ごとに素であるから，

$$r = c^3, \quad \epsilon = v\alpha^3, \quad \overline{\epsilon} = \overline{v\alpha}^3 \quad (v \in R', \alpha \in R)$$

と表せる．x, z は奇数であるから，

$$v\lambda\alpha^3 = x - \omega z \equiv 1 + \omega \pmod{2R} \text{ より，} v = \pm 1$$

となるため，

$$x - z = 18c^3 \tag{13}$$

$$x - \omega z = \lambda\alpha^3 \tag{14}$$

$$x - \overline{\omega}z = \overline{\lambda}\overline{\alpha}^3 \tag{15}$$

と表せる．$\alpha = a + b\omega \quad (a, b \in \mathbb{Z})$ とおくと，(14)，(15) より，

$$\begin{cases} x = a^3 + 3a^2b - 6ab^2 + b^3 \\ z = a^3 - 6a^2b + 3ab^2 + b^3 \end{cases}$$

したがって，(13) より，

$$2c^3 = ab(a-b)$$

第 5 章と同様の議論により，$a, b, a-b$ は互いに素であるから，

$$(a, b, a-b) = (x'^3, 2y'^3, z'^3), \ (2y'^3, -z'^3, x'^3), \ (z'^3, x'^3, -2y'^3)$$

とおける（x', y', z' は 0 でない整数）．これらのどの場合でも

$$x'^3 - 2y'^3 = z'^3$$

を満たすため，(x', y', z') は方程式の解である．ところが，

$$y^3 = 9x'^3 y'^3 z'^3 (x - \omega z)(x - \overline{\omega} z)$$

より，

$$\max\left\{|x'|^3, |y'|^3, |z'|^3\right\} < |y|^3 \leqq \max\left\{|x|^3, |y|^3, |z|^3\right\}$$

$$\therefore \quad \max\{|x'|, |y'|, |z'|\} < \max\{|x|, |y|, |z|\}$$

これは，$\max\{|x|, |y|, |z|\}$ の最小性に矛盾する．

以上より，仮定は誤りで，

$$x^3 - 2y^3 = z^3$$

の整数解は，すべて $(x, y, z) = (n, n, -n)$ で与えられる．■

ゆえに，$z = \pm 1$ なる整数解は $(x, y, z) = (-1, -1, 1), (1, 1, -1)$ のみであるから，

$$x^3 - 2y^3 = \pm 1$$

の自然数解は $(x, y) = (1, 1)$ のみである．

7　$x^3 - 6y^3 = \pm 1$ について

$N = 6$ のとき，自然数解 (x, y) をもたないことを示すのが目標だったのだが，これについては証明することがまだできていない．これまでの論法をそのまま適用すると，

$$x - z = 54c^3, \tag{16}$$

$$x - \omega z = \lambda \alpha^3, \tag{17}$$

$$x - \overline{\omega} z = \overline{\lambda} \overline{\alpha}^3 \tag{18}$$

と表せるのだが，$\alpha = a + b\omega$ とおいて，これを a, b, c の関係式で表すと，

$$6c^3 = ab(a - b)$$

となる．$a, b, a - b$ は対ごとに素なのだが，6 は合成数であるので，$\max\{|x|, |y|, |z|\}$ がさらに小さい解をうまく導き出せない．また，剰余類の点でも矛盾が生じない．よって，新たな方法を模索することが必要となる．

8　結果

以上の議論から，三角立方数は，

$$N = \frac{1}{2} \cdot 1 \cdot 2 = 1^3 = 1$$

のみであることがわかった．

四面立方数について，(i) のとき，条件を満たす m が存在する必要条件が，

$$x^3 - y^3 = \pm 1,$$

$$x^3 - 3y^3 = \pm 1$$

をみたす自然数の組 (x, y) が存在することであるが，Fermat の最終定理 $(n = 3)$ と，第 5 章の結果より，(i) を満たす $(m, m+1, m+2)$ の組が存在しないことがわかる．

(ii) について，

(A) $(m, m+1, m+2) = (3x^3, 2y^3, z^3)$ のとき，

$$z^3 - 2y^3 = 1$$

より，このような自然数解は存在しないため，不適である．

(B) $(m, m+1, m+2) = (x^3, 2y^3, 3z^3)$ のとき，

$$x^3 - 2y^3 = -1$$

より，これをみたす自然数の組 $(x.y)$ は $(1, 1)$ のみであるから，$m = 1$ が必要である．このとき，

$$N = \frac{1}{6} \cdot 1 \cdot 2 \cdot 3 = 1^3 = 1$$

より，1 は四面立方数である．

(C) $(m, m+1, m+2) = (x^3, 6y^3, z^3)$ のとき，

$$x^3 - 6y^3 = -1,$$

$$z^3 - 6y^3 = 1$$

の解についてはまだ解っていないが，x^3 と z^3 について比べると，

$$z^3 - x^3 = 2$$

であり，これを変形すると

$$z^3 - 2 \cdot 1^3 = x^3$$

となる．第 6 章の結果から，これを満たす自然数の組 (x, z) は存在しない．

以上より，四面立方数は 1 のみであることがわかる．

9　一般的な N について

これまでの議論から，$N = 3$ のときは解をもたず，$N = 2$ のときは解 $(1, 1)$ のみをもった．この時点で，すでに Pell 方程式とは大きく様相が異なっている．一般的な N については，今までのような具体的な数についての議論より，さらに難しい議論を要するだろう．

ちなみに，$N = p^3 \pm 1$ のときは明らかに解 $(p, 1)$ をもつ．N が立方数のときは，Fermat の最終定理により解をもたない．これら以外の N では，$N = 19$ のとき $(8, 3)$，$N = 43$ のとき $(7, 2)$，$N = 182$ のとき $(17, 3)$ をもつ（これらがすべてかどうかはわからない）．

10　まとめ

$N = 2, 3$ のときの証明にあたり，非常に助けとなった参考文献が，松坂和夫著の『代数系入門』と MATHEMATICS.PDF(http://mathematics.web.infoseek.co.jp/) 掲載の『$n = 3$ における Fermat の定理』である．3 次の Pell 方程式の議論を目標に環論の勉強を進めた結果，$n = 3$ における Fermat の最終定理のを理解することができ，さらにその証明を参考に $N = 2, 3$ のときの証明ができてとても有意義な結果となった．これからの目標は，$N = 6$ について，また一般的な N についての 3 次の Pell 方程式の考察であるが、受験生の身であるがゆえ，その時間はこの一年には残されていないだろう．ある意味，このレポートの完成をけじめとして，この一年を全力で受験勉強に注ごうと思う．その後で，この問題に取り組みたい．

それと，レポートを読んだ方で，この問題についておもしろい結果が得られた方がいれば是非教えてください．