

二次方程式の先にあるもの

中川仁

上越教育大学 自然系数学

2016 年 5 月 2 日

① イン트로ダクション

② 2 元 2 次形式

③ 2 元 3 次形式

整数論とは

私の専門は整数論.

整数論にはだれでも問題の意味がわかるが未解決の問題がたくさんある. 例えば

予想 1.1 (ゴールドバッハ予想)

4 以上のすべての偶数は 2 つの素数の和でかける.

$$12 = 5 + 7, 16 = 5 + 11, 36 = 7 + 29, \dots\dots$$

予想 1.2 (双子素数の予想)

p と $p + 2$ がともに素数であるようなものは無数に存在する.

$$3 \text{ と } 5, 5 \text{ と } 7, 11 \text{ と } 13, 17 \text{ と } 19, 29 \text{ と } 31, 41 \text{ と } 43, \dots\dots$$

このように誰にでも意味がわかることで、未解決のことがたくさんあるのが整数論という分野の魅力である.

今日は皆さんがよく知っている 2 次方程式の話から始めて、私自身の研究結果の中で一番よいと思っているものについて説明する.

2 次方程式

定義 2.1

3 つの数 a, b, c ($a \neq 0$) が与えられたとき, x を未知数とする方程式

$$ax^2 + bx + c = 0$$

を **2 次方程式** という. $D = b^2 - 4ac$ をその**判別式** という.

2 つの 2 次方程式

$$2x^2 - 2x - 3 = 0,$$

$$x^2 - 4x - 3 = 0$$

を考える. これらの判別式を計算すると, それぞれ

$$(-2)^2 - 4 \times 2 \times (-3) = 4 + 24 = 28,$$

$$4^2 - 4 \times 1 \times (-3) = 16 + 12 = 28.$$

解の公式

2 次方程式の解の公式

$$x = \frac{-b \pm \sqrt{D}}{2a} \quad (D = b^2 - 4ac)$$

を用いてこれらの 2 次方程式を解けば

$$2x^2 - 2x - 3 = 0,$$

$$x = \frac{2 \pm \sqrt{28}}{4} = \frac{1 \pm \sqrt{7}}{2}, \quad \alpha = \frac{1 + \sqrt{7}}{2} \text{ とおく.}$$

$$x^2 - 4x - 3 = 0,$$

$$x = \frac{4 \pm \sqrt{28}}{2} = 2 \pm \sqrt{7}, \quad \beta = 2 + \sqrt{7} \text{ とおく.}$$

$$\frac{2\beta + 1}{\beta + 1} = \frac{5 + 2\sqrt{7}}{3 + \sqrt{7}} = \frac{(5 + 2\sqrt{7})(3 - \sqrt{7})}{(3 + \sqrt{7})(3 - \sqrt{7})} = \frac{1 + \sqrt{7}}{2} = \alpha.$$

2 次方程式の変数変換

そこで 1 番目の方程式で $x = \frac{2X + 1}{X + 1}$ とおけば

$$2 \left(\frac{2X + 1}{X + 1} \right)^2 - 2 \frac{2X + 1}{X + 1} - 3 = 0,$$

$$2(2X + 1)^2 - 2(2X + 1)(X + 1) - (X + 1)^2 = 0,$$

$$8X^2 + 8X + 2 - 4X^2 - 6X - 2 - X^2 - 2X - 1 = 0,$$

$$X^2 - 4X - 3 = 0. \quad (2 \text{ 番目の方程式})$$

すなわち上の**変数変換によって 1 番目の方程式から 2 番目の方程式がでる！**

もう少しこの変換を見やすくするために x のほかに別の変数 y を導入して次のように考える.

2 元 2 次形式

定義 2.2

3 つの数 a, b, c が与えられたとき, x, y を変数とする 2 次式

$$f(x, y) = ax^2 + bxy + cy^2$$

を **2 元 2 次形式** という. $D(f) = b^2 - 4ac$ をその**判別式** という.

ただし, $D(f) < 0$ のときは $a > 0$ のものだけ考える.

2 元 2 次形式の変数変換

判別式 28 をもつ 2 つの 2 元 2 次形式

$$\begin{aligned}f(x, y) &= 2x^2 - 2xy - 3y^2, \\g(x, y) &= x^2 - 4xy - 3y^2\end{aligned}$$

を考える. $f(x, y)$ の x に $2x + y$, y に $x + y$ を代入すると

$$\begin{aligned}f(2x + y, x + y) &= 2(2x + y)^2 - 2(2x + y)(x + y) - 3(x + y)^2 \\&= 2(4x^2 + 4xy + y^2) - 2(2x^2 + 3xy + y^2) \\&\quad - 3(x^2 + 2xy + y^2) \\&= x^2 - 4xy - 3y^2 = g(x, y).\end{aligned}$$

2 元 2 次形式の同値

これまで係数 a, b, c は単に数としていたが、以下 a, b, c は整数とする.

上の例のように 2 つの整数係数 2 元 2 次形式

$$f(x, y) = ax^2 + bxy + cy^2, \quad g(x, y) = a'x^2 + b'xy + c'y^2$$

に対して、整数 p, q, r, s で $ps - qr = 1$ となるようなある変数変換 $(x, y) \mapsto (px + ry, qx + sy)$ によって

$$g(x, y) = f(px + ry, qx + sy)$$

と移り合うとき、 $f(x, y)$ と $g(x, y)$ は同値であるといい、

$$f(x, y) \sim g(x, y)$$

と表す.

判別式は変わらない

命題 2.3

2つの2元2次形式 $f(x, y)$, $g(x, y)$ が同値ならば

$$D(f) = D(g)$$

が成り立つ.

2 元 2 次形式の同値の例

2 元 2 次形式

$$f(x, y) = 34x^2 - 42xy + 13y^2$$

の判別式は $D(f) = 42^2 - 4 \times 34 \times 13 = -4$ である.

$$g_1(x, y) = f(y, -x) = 13x^2 + 42xy + 34y^2$$

$$\begin{aligned} g_2(x, y) &= g_1(x - 2y, y) = 13(x - 2y)^2 + 42(x - 2y)y + 34y^2 \\ &= 13x^2 - 10xy + 2y^2, \end{aligned}$$

$$g_3(x, y) = g_2(y, -x) = 2x^2 + 10xy + 13y^2,$$

$$\begin{aligned} g_4(x, y) &= g_3(x - 2y, y) = 2(x - 2y)^2 + 10(x - 2y)y + 13y^2 \\ &= 2x^2 + 2xy + y^2, \end{aligned}$$

$$g_5(x, y) = g_4(y, -x) = x^2 - 2xy + 2y^2,$$

$$\begin{aligned} g_6(x, y) &= g_5(x + y, y) = (x + y)^2 - 2(x + y)y + 2y^2 \\ &= x^2 + y^2. \end{aligned}$$

したがって

$$34x^2 - 42xy + 13y^2 \sim x^2 + y^2.$$

実は判別式が -4 である整数係数の 2 元 2 次形式はすべて

$$x^2 + y^2$$

と同値であることがわかる.

2 元 2 次形式の類別

一般に整数 $m \neq 0$ が与えられたとき, 判別式の値が m であるような整数係数の 2 元 2 次形式は有限個の類に類別される.

すなわち h 個の $f_1(x, y), \dots, f_h(x, y)$ が存在して, 判別式 m の 2 元 2 次形式はこれらの $f_i(x, y)$ のどれか 1 つだけと同値になる.

この類別の個数 h のことを, $h = h(m)$ とかき, 判別式 m の 2 元 2 次形式の**類数**とよぶ.

判別式 -4 の 2 元 2 次形式はすべて $x^2 + y^2$ と同値だから, $h(-4) = 1$ となる.

自分自身にうつす変換

$f(x, y) = x^2 - 2y^2$ とする. $D(f) = 8$ である.

$p = 3, q = 2, r = 4, s = 3$ は

$$ps - qr = 3 \times 3 - 2 \times 4 = 9 - 8 = 1$$

を満たし

$$\begin{aligned} f(3x + 4y, 2x + 3y) &= (3x + 4y)^2 - 2(2x + 3y)^2 \\ &= 9x^2 + 24xy + 16y^2 \\ &\quad - 2(4x^2 + 12xy + 9y^2) \\ &= x^2 - 2y^2 = f(x, y). \end{aligned}$$

$f(x, y)$ を自分自身にうつすような変換の個数は

- $D(f) > 0$ ならば無数にある.
- $D(f) < 0$ ならばちょうど 2 個か, 4 個か, 6 個のいずれか.

類数についての問題

2元2次形式の類数については、ガウス (1777–1855) をはじめ多くの数学者によって研究されている。判別式が負の場合は、判別式が正の場合よりもあつかいやすい。

定理 2.4 (Baker, Stark 1966)

$h(m) = 1$ となる負の整数 m は次の 9 個に限る。

$$-3, -4, -7, -8, -11, -19, -43, -67, -163.$$

次はガウスによって提出された予想であり、現在でも未解決である。

予想 2.5

$h(m) = 1$ となる正の整数 m は無数に存在する。

2 元 3 次形式とその判別式

定義 3.1

4 つの数 a, b, c, d が与えられたとき, x, y を変数とする 3 次式

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$$

を **2 元 3 次形式** という.

$$D(f) = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2$$

をその **判別式** という.

2 元 3 次形式の同値

2 つの整数係数 2 元 3 次形式

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3, \quad g(x, y) = a'x^3 + b'x^2y + c'xy^2 + d'y^3$$

に対して, p, q, r, s は整数で $ps - qr = 1$ となるようなある変数変換 $(x, y) \mapsto (px + ry, qx + sy)$ によって

$$g(x, y) = f(px + ry, qx + sy)$$

と移り合うとき, $f(x, y)$ と $g(x, y)$ は同値であるといい,

$$f(x, y) \sim g(x, y)$$

と表す.

2 元 3 次形式の類数

2 元 2 次形式のときと同様に, 2 つの整数係数 2 元 3 次形式 $f(x, y)$ と $g(x, y)$ が同値ならば

$$D(f) = D(g)$$

が成り立つ.

一般に整数 $m \neq 0$ が与えられたとき, 判別式の値が m であるような整数係数の 2 元 3 次形式は有限個の類に類別される.

すなわち h 個の $f_1(x, y), \dots, f_h(x, y)$ が存在して, 判別式 m の 2 元 3 次形式はこれらの $f_i(x, y)$ のどれか 1 つだけと同値になる.

この類別の個数 h のことを, $h = h(m)$ とかき, 判別式 m の 2 元 3 次形式の類数とよぶ.

整数係数 2 元 3 次形式 $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ のなかで b, c が 3 の倍数であるものだけを考える. そのようなもので判別式が m であるものも有限個の類に類別される. その類の数を $\hat{h}(m)$ で表す.

判別式が正の場合には, 同値を考えたときの変数変換が 2 元 3 次形式 $f(x, y)$ を自分自身にうつすようなものが 1 つの場合と 3 つの場合がある. そのような 2 元 3 次形式で判別式が m の類の数をそれぞれ $h_1(m), h_2(m)$ で表す. 同様に $\hat{h}_1(m), \hat{h}_2(m)$ を定義する.

2 元 3 次形式の例

$$f(x, y) = x^3 + 3x^2y - y^3$$

とおく.

$$D(f) = -4 \times 3^3 \times (-1) - 27(-1)^2 = 4 \times 27 - 27 = 81.$$

$$\begin{aligned} f(-x - y, x) &= (-x - y)^3 + 3(-x - y)^2x - x^3 \\ &= -x^3 - 3x^2y - 3xy^2 - y^3 \\ &\quad + 3x^3 + 6x^2y + 3xy^2 - x^3 \\ &= x^3 + 3x^2y - y^3 = f(x, y). \end{aligned}$$

定理 3.2 (Nakagawa 1998)

任意の正整数 m に対して次の等式が成り立つ.

$$\begin{aligned}\hat{h}_1(27m) + \frac{1}{3}\hat{h}_2(27m) &= h(-m), \\ 3h_1(m) + h_2(m) &= \hat{h}(-27m).\end{aligned}$$

1995 年に当時大阪大学の博士課程の大学院生だった大野泰生さんが修士論文の中で上の等式が成立するだろうという述べていて、数学会の講演で予想として発表したものである。その講演を聞いた瞬間に m がある条件を満たす場合の証明が頭に浮かんでいたことをよく覚えてる。一般の場合の証明を完成させるのにはそれから 2 年かかった。

これまで自分が研究してきてよく知っていることがすべて使えて、この予想を解くためには必要ないことは余り知らなかったという幸運に恵まれ、そういう予想を日本人の大野さんが見つけたという偶然が重なったおかげで、私が証明することができたと思う。

大野さんについて

大野さんは、近畿大学を経て、現在東北大学理学部の教授.
大野さんのホームページ [3] には次のようにかかれています.

- 興味をもっていること
数列や関数などの引き起こす素朴で調和のとれた現象とその背後にある原理を、なるべく簡素平明に解き明かすこと.
- 学生に望むこと
自分で触れて、自分で感じ、自分で考える. そうして独自のセンスを磨くこと.

参考文献

- [1] 青木昇, 素数と2次体の整数論, 共立出版, 2012.
- [2] J. Nakagawa, On the relations among the class numbers of binary cubic forms, Invent. math. 134, 101-138 (1998)
- [3] <http://www.math.tohoku.ac.jp/people/ohno.html>
- [4] 大野泰生・谷口 隆, 「数学者的思考回路」,
<http://www.shokabo.co.jp/column-math/list.html>
- [5] ジョセフ・F・シルバーマン, はじめての数論 原著第3版, 丸善出版, 2014.