2 平方和の定理，オイラーの 2 次式

中川仁

上越教育大学

2022 年 7 月 30 日

2 つの平方数の和

素数 $2, 5, 13, 17, 29$ などは

$$2 = 1^2+1^2, \quad 5 = 1^2+2^2, \quad 13 = 2^2+3^2, \quad 17 = 1^2+4^2, \quad 29 = 2^2+5^2$$

のように 2 つの平方数の和として表される.

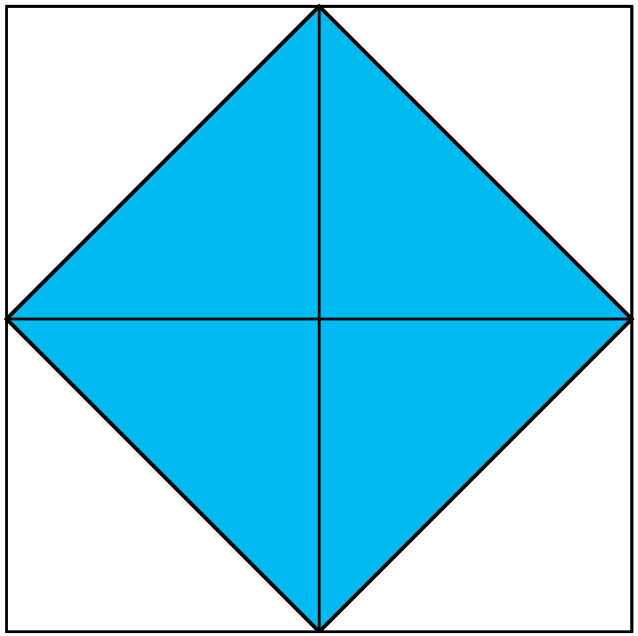
このような素数 p は

方眼紙を使って面積 p の正方形がかけるようなもの

である.

方眼紙を使って面積 p の正方形を描く

面積 2 の正方形は次のようにしてかける．



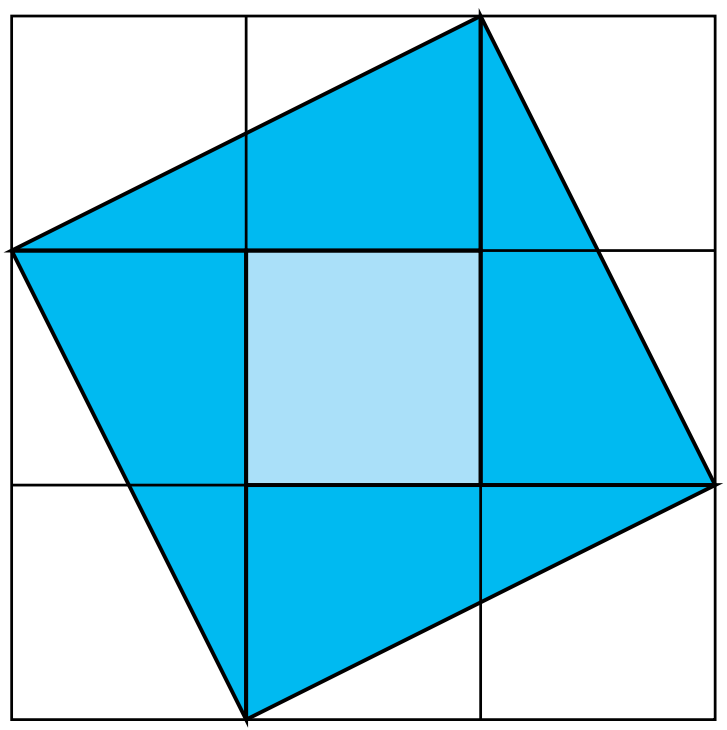
直角三角形の面積 $1/2$

$$(1/2) \times 4 = 2$$

$$1^2 + 1^2 = 2$$

方眼紙を使って面積 p の正方形を描く

面積 5 の正方形は次のようにしてかける.



水色正方形の面積 1

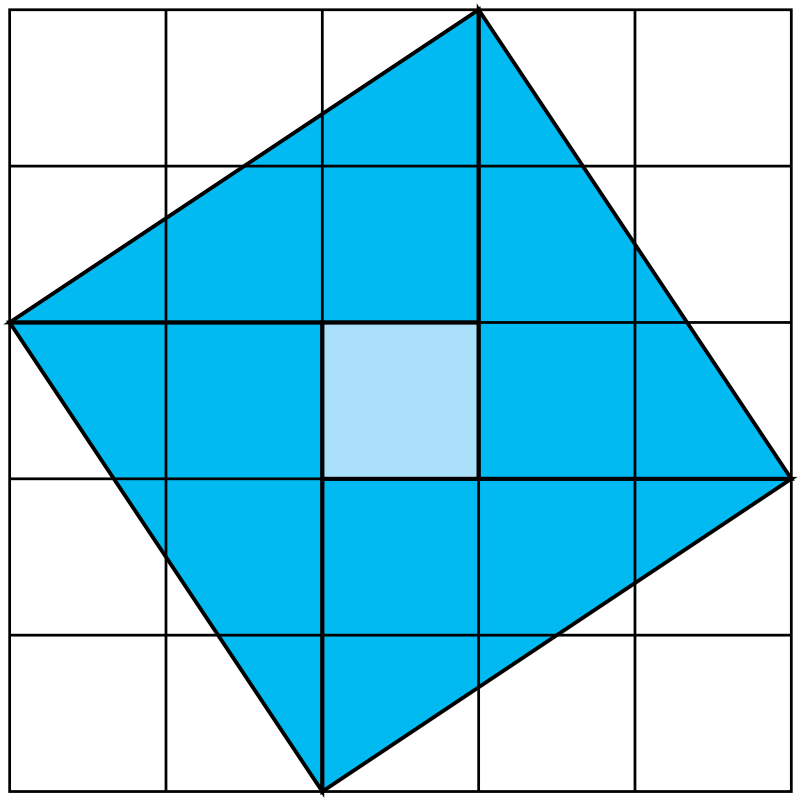
直角三角形の面積 1

$1 + 1 \times 4 = 5$

$2^2 + 1^2 = 5$

方眼紙を使って面積 p の正方形を描く

面積 13 の正方形は次のようにしてかける.



水色正方形の面積 1

直角三角形の面積 3

$1 + 3 \times 4 = 13$

$3^2 + 2^2 = 13$

2 つの平方数の和

これについて次の定理が知られている．

定理 1.1 (2 平方和の定理)

素数 p が 2 つの平方数の和として表せるためには，$p = 2$ であるかまたは $p = 4q + 1$ の形であることが必要十分である．

これはフェルマーによって提起され，オイラーによって証明された．

素数値をたくさんとる 2 次式

素数 q に対して変数 x の 2 次式

$$f_q(x) = x^2 + x + q$$

を考える．

例えば $q = 11$ とすると

$$f_{11}(x) = x^2 + x + 11$$

である．x に連続する 10 個の整数 $n = 0, 1, \ldots, 9$ を代入するとき，$f_{11}(n)$ の値は次の表のようになる．

$f_{11}(n)$, $n = 0, 1, \ldots, 9$ の値

n	0	1	2	3	4	5	6	7	8	9
$f_{11}(n)$	11	13	17	23	31	41	53	67	83	101

この表の下段に現れる 10 個の $f_{11}(n)$ の値はすべて素数である.

素数値をたくさんとる 2 次式

今度は $q = 41$ とすると

$$f_{41}(x) = x^2 + x + 41$$

である．x に連続する 40 個の整数 $n = 0, 1, \ldots, 39$ を代入するとき，$f_{41}(n)$ の値は次の表のようになる．

$f_{41}(n)$, $n = 0, 1, \ldots, 39$ の値

n	0	1	2	3	4	5	6	7	8	9
$f_{41}(n)$	41	43	47	53	61	71	83	97	113	131
x	10	11	12	13	14	15	16	17	18	19
$f_{41}(n)$	151	173	197	223	251	281	313	347	383	421
n	20	21	22	23	24	25	26	27	28	29
$f_{41}(n)$	461	503	547	593	641	691	743	797	853	911
n	30	31	32	33	34	35	36	37	38	39
$f_{41}(n)$	971	1033	1097	1163	1231	1301	1373	1447	1523	1601

この表の下段に現れる 40 個の $f_{41}(n)$ の値 $41, 43, 47, \ldots, 1601$ もすべて素数である．これは 1772 年にオイラーによって発見された事実である．

これから話すこと

以下，2 元 2 次形式の整数論を用いて

- 2 平方和の定理の証明
- $f_{41}(n)$, $n = 0, 1, \ldots, 39$ の値が素数となる理由

を述べる．

まず初等整数論における基本的な事実をいくつか準備する．

整数 $m > 1$ と整数 a, b について，$a - b$ が m で割り切れるとき

$$a \equiv b \pmod{m}$$

とかいて，a と b は法 m で**合同**であるという．

1 次不定方程式 $ax - ny = 1$

命題 2.1

$n > 1$ を自然数，a を n と互いに素な整数とする．このとき n と互いに素な整数 x, $1 \leq x < n$ で $ax \equiv 1 \pmod{n}$ を満たすものが一意的に存在する．よって $ax - ny = 1$ を満たす $x, y \in \mathbb{Z}$ が存在する．

[証明] $G = \{x \in \mathbb{Z} : 1 \leq x \leq n-1,\ x \text{ は } n \text{ と互いに素 }\}$.

写像 $f : G \to G$ を　$f(x) = ax$ を n で割った余り と定義．

f は単射．$\because x, y \in G,\ f(x) = f(y) = r$

$\Longrightarrow ax = nq + r,\ ay = ns + r,\ q, s \in \mathbb{Z}.$

$\Longrightarrow a(x-y) = n(q-s) \Longrightarrow x - y$ は n で割り切れる．

$x, y \in G$ より $|x - y| < n,\ x - y = 0,\ x = y$.

f は有限集合 G から G 自身への単射 $\Longrightarrow$ f は全単射．

よって $f(a') = 1$ となる $a' \in G$ が一意的に存在する． □

法 p の逆数

上の命題で $n = p$ を素数とすれば次の系を得る．

系 2.2

p を素数とし，a を p で割り切れない整数とする．このとき整数 a', $1 \leq a' < p$ で $aa' \equiv 1 \pmod{p}$ を満たすものが一意的に存在する．

Wilson の定理

命題 2.3 (Wilson の定理)

素数 p に対して $(p-1)! \equiv -1 \pmod{p}$ が成り立つ．

[証明] 例えば，$p = 11$ のときは

$$2 \cdot 6 \equiv 3 \cdot 4 \equiv 5 \cdot 9 \equiv 7 \cdot 8 \equiv 1 \pmod{11},$$
$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 = (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \equiv 1 \pmod{11}.$$

一般の場合も $aa' \equiv 1 \pmod{p}$ となるものをペアにすれば

$$(p-2)! \equiv 1 \pmod{p}$$

となる．この両辺に $(p-1)$ をかければ $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$ を得る．

系 2.4

p が $4q+1$ の形の素数ならば，$m^2 \equiv -1 \pmod{p}$ となる整数 m が存在する．

[証明] 例えば $p = 13 = 4 \times 3 + 1$ のとき，1 から 12 までの整数を 1 と 12，2 と 11, のように，たすと 13 になるような 6 組のペアにしてかければ

$$\begin{aligned} 12! &= (1 \cdot 12)(2 \cdot 11)(3 \cdot 10)(4 \cdot 9)(5 \cdot 8)(6 \cdot 7) \\ &\equiv (-1^2)(-2^2)(-3^2)(-4^2)(-5^2)(-6^2) = (-1)^6(6!)^2 \pmod{13} \\ &\equiv (6!)^2 \pmod{13}. \end{aligned}$$

命題 2.3 (Wilson の定理) により $12! \equiv -1 \pmod{13}$ だから
$(6!)^2 \equiv 12! \equiv -1 \pmod{13}$.

一般の場合も同様．

□

2 元 2 次形式の判別式

a, b, c を実数として，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 $f(x, y)$ の**判別式**とよぶ．

$a, b, c \in \mathbb{Z}$ のとき，$f(x, y)$ を $\mathbb{Z}$ **係数 2 元 2 次形式**という．この場合，判別式 $D(f)$ は整数である．

2 元 2 次形式の同値

整数を成分とする行列式 1 をもつ 2 次行列全体のなす (行列の積に関する) 群を $\mathrm{SL}_2(\mathbb{Z})$ で表す．$\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ によって，2 元 2 次形式 $f(x, y)$ は

$$f((x, y)\gamma) = f(rx + ty, sx + uy)$$

に変換される．

2 つの $\mathbb{Z}$ 係数 2 元 2 次形式 $f(x, y)$ と $g(x, y)$ について，
$\gamma \in \mathrm{SL}_2(\mathbb{Z})$ で $g(x, y) = f((x, y)\gamma)$ となるものが存在するとき，
$f(x, y)$ と $g(x, y)$ は**同値**であるといい，$f(x, y) \sim g(x, y)$ とかく．

行列による 2 元 2 次形式の表示

$f(x,y) = ax^2 + bxy + cy^2$ は行列とベクトルの積として次のように表せる.

$$f(x,y) = (x,y) \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

このとき

$$D(f) = b^2 - 4ac = -4\left(ac - \frac{b^2}{4}\right) = -4 \begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix}. \tag{3.1}$$

同値な 2 元 2 次形式の判別式は等しい

命題 3.1

$f(x,y) \sim g(x,y)$ ならば $D(f) = D(g)$ である.

[証明] $f(x,y) = ax^2 + bxy + cy^2$ とする.

$\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ があり $g(x,y) = f((x,y)\gamma)$ となる.

$$g(x,y) = (x,y)\,\gamma \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} {}^{\mathrm{t}}\gamma \begin{pmatrix} x \\ y \end{pmatrix}.$$

これに (3.1) を適用する. $|{}^{\mathrm{t}}\gamma| = |\gamma| = ru - st = 1$ より

$$D(g) = -4|\gamma| \begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix} |{}^{\mathrm{t}}\gamma| = -4 \begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix} = D(f).$$

正定値 2 元 2 次形式

定義 3.2

2 元 2 次形式 $f(x,y) = ax^2 + bxy + cy^2$ が，任意の $(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\}$ に対して $f(x,y) > 0$ となるとき，$f(x,y)$ は**正定値**であるという．

$f(x,y)$ が正定値 $\iff a > 0,\ D(f) < 0$.

[証明] $\Rightarrow$) $f(x,y)$ が正定値ならば $a = f(1,0) > 0$,
$f(x,1) = ax^2 + bx + c > 0\ (\forall x \in \mathbb{R}) \Longrightarrow D(f) = b^2 - 4ac < 0$.

$\Leftarrow$) $a > 0$ かつ $D(f) < 0$ ならば

$$f(x,y) = a\left(x + \frac{b}{2a}y\right)^2 + \frac{4ac - b^2}{4a}y^2 \geq 0$$

であり，等号が成り立つのは $y = 0,\ x = 0$ のときに限る．

同値類

命題 3.1 により同値な 2 元 2 次形式は同じ判別式をもつ．そこで与えられた判別式の値をもつような $\mathbb{Z}$ 係数 2 元 2 次形式の集合を考えたとき，それを同値なもの同士に分けるといくつに分かれるか，すなわち同値類の数が問題になる．
例えば，判別式が -23 の $\mathbb{Z}$ 係数正定値 2 元 2 次形式の集合は次の 3 つの同値類に分かれる．

- $x^2 + xy + 6y^2$ と同値なもの．
- $2x^2 + xy + 3y^2$ と同値なもの．
- $2x^2 - xy + 3y^2$ と同値なもの．

簡約形式

この問題には，次のような特別な 2 元 2 次形式が重要になる．

定義 3.3

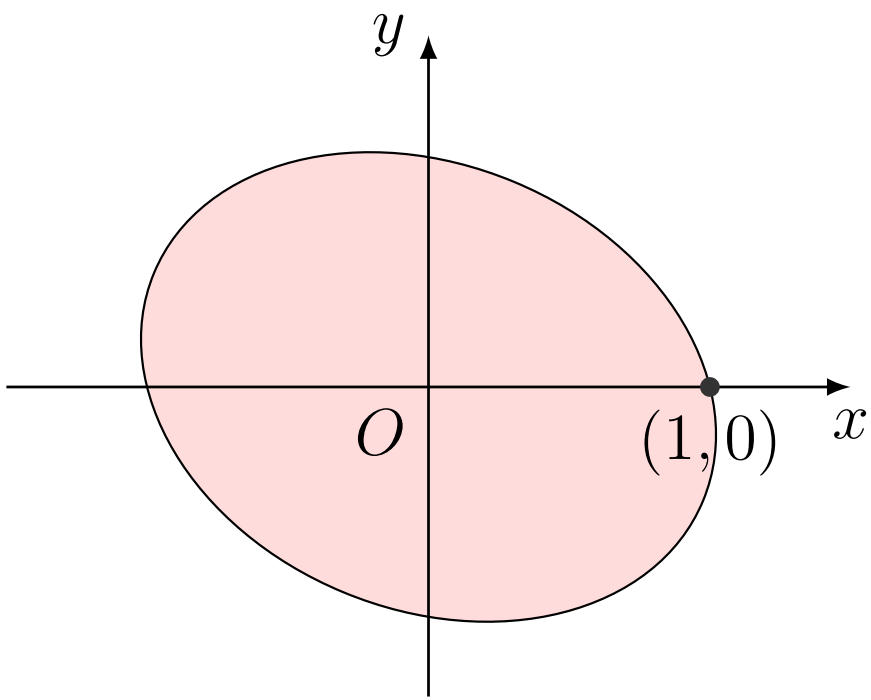
$f(x,y) = ax^2 + bxy + cy^2$ を正定値 2 元 2 次形式とする．$f(x,y)$ の係数 a, b, c が条件

$$-a < b \leq a < c \text{ または } 0 \leq b \leq a = c \tag{3.2}$$

を満たすとき，$f(x,y)$ は**簡約形式**であるという．

正定値 2 元 2 次形式の $\mathbb{Z}^2 \setminus \{(0,0)\}$ 上の最小値

$f(x,y) = ax^2 + bxy + cy^2$ を正定値 2 元 2 次形式とすれば，不等式 $f(x,y) \leq a$ を満たす点 (x,y) の集合は楕円の内側である．
この楕円の内側にある点 $(x,y) \in \mathbb{Z}^2$, $(x,y) \neq (0,0)$，は明らかに有限個．そこでの最小値 m がある．m は $\mathbb{Z}^2 \setminus \{(0,0)\}$ 上の $f(x,y)$ の最小値になる．明らかに $m \leq f(1,0) = a$ である．



与えられた 2 元 2 次形式と同値な簡約形式 1

命題 3.4

任意の正定値 2 元 2 次形式 $f(x,y)$ はある簡約形式と同値である.

[証明] $m = \min\{f(x,y) \,|\, (x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}\}$.
$m = f(r,s)$, $(r,s) \in \mathbb{Z}^2$, $(r,s) \neq (0,0) \Longrightarrow r$ と s は互いに素.
命題 2.1 より $ru - st = 1$ となる $u, t \in \mathbb{Z}$ がある.

$\gamma_1 = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. $f_1(x,y) = f(rx+ty, sx+uy)$ とおく.

$f_1(x,y)$ における x^2 の係数は $f_1(1,0) = f(r,s) = m$.

$f_1(x,y) = mx^2 + kxy + ly^2$ とかき，$k/2m$ に一番近い整数を q とする：

$$-\frac{1}{2} < \frac{k}{2m} - q \leq \frac{1}{2}, \quad -m < k - 2mq \leq m.$$

与えられた 2 元 2 次形式と同値な簡約形式 2

$\gamma_2 = \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. $f_2(x,y) = f_1(x-qy, y)$ とおく.

$f_2(x,y) = a'x^2 + b'xy + c'y^2$ とかく.

$$f_2(x,y) = mx^2 + (k-2mq)xy + (mq^2 - kq + l)y^2.$$

よって $a' = m$, $b' = k - 2mq$, $c' = mq^2 - kq + l$.

q のとり方から, $-m < b' \leq m$. また

$$c' = f_2(0,1) = f_1(-q,1) = f(-rq+t, -sq+u) \geq m = a'.$$

よって $a' > 0$, $-a' < b' \leq a' \leq c'$.

$a' < c'$ または $a' = c'$, $0 \leq b' \leq a' \Longrightarrow f_2(x,y)$ は簡約.

もし $a' = c'$ かつ $-a' < b' < 0 \Longrightarrow f_3(x,y) = f_2(y,-x)$ とおけば
$f_3(x,y) = a'x^2 - b'xy + a'y^2$ となり, $f_3(x,y)$ は簡約.

$f_1(x,y), f_2(x,y), f_3(x,y)$ は $f(x,y)$ と同値である. □

簡約形式の最小値

補題 3.5

$f(x,y) = ax^2 + bxy + cy^2$ を簡約な正定値 2 元 2 次形式とする．
このとき

$$a = \min\{f(x,y) \,|\, (x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}\}.$$

また $f(r,s) = a$, $(r,s) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ とすれば

(i) $a < c$ のとき．$(r,s) = \pm(1,0)$.

(ii) $0 \leq b < a = c$ のとき．$(r,s) = \pm(1,0), \pm(0,1)$.

(iii) $a = b = c$ のとき．$(r,s) = \pm(1,0), \pm(0,1), \pm(1,-1)$.

[証明] 平方完成により容易に示される． □

簡約形式の有限性

命題 3.6

与えられた負の判別式 $D < 0$ をもつ $\mathbb{Z}$ 係数正定値 2 元 2 次形式 $f(x, y) = ax^2 + bxy + cy^2$ で簡約なものは有限個である．

[証明] $a, b, c \in \mathbb{Z}$ が $a > 0$, $b^2 - 4ac = D$ で (3.2) を満たせば

$$4a^2 \leq 4ac = b^2 - D \leq a^2 + |D|, \quad 3a^2 \leq |D|, \quad 1 \leq a \leq \sqrt{\frac{|D|}{3}}.$$

よって a の値は有限個．各 a について $-a < b \leq a$ より b の値も有限個．a, b に対して $4ac = b^2 + |D|$ を満たす c は高々 1 つ． □

2 元 2 次形式の類別

命題 3.7

$f(x,y)$ と $g(x,y)$ を判別式 $D<0$ をもつ $\mathbb{Z}$ 係数正定値 2 元 2 次形式でともに簡約であるとする．このとき $f(x,y)$ と $g(x,y)$ が同値ならば $f(x,y)=g(x,y)$ である．

[証明] 補題 3.5 からただちにしたがう． □

命題 3.6 から与えられた負の整数 D を判別式にもつ $\mathbb{Z}$ 係数正定値 2 元 2 次形式で簡約なものは有限個である．それらを $g_1(x,y),\ldots,g_h(x,y)$ とすれば，命題 3.4 により D を判別式にもつ任意の $\mathbb{Z}$ 係数正定値 2 元 2 次形式は，ある $g_i(x,y)$ $(1\leq i\leq h)$ と同値である．さらに命題 3.7 により $1\leq i<j\leq h$ に対して $g_i(x,y)$ と $g_j(x,y)$ は同値ではない．したがって次の系を得る．

類数の有限性

系 3.8

与えられた負の整数 D に対して，D を判別式にもつ有限個の $\mathbb{Z}$ 係数正定値 2 元 2 次形式 $g_1(x,y),\ldots,g_h(x,y)$ が存在して，D を判別式にもつ任意の $\mathbb{Z}$ 係数正定値 2 元 2 次形式 $f(x,y)$ は $g_1(x,y),\ldots,g_h(x,y)$ のどれか 1 つだけと同値になる．

定義 3.9

系 3.8 における 2 元 2 次形式 $g_1(x,y),\ldots,g_h(x,y)$ の個数 h を判別式 D の 2 元 2 次形式の**類数**とよび，$h(D)$ で表す．

類数の計算例 1

例 3.10 ($D = -4$)

$ax^2 + bxy + cy^2$ が判別式 -4 で簡約とすれば

$$b^2 - 4ac = -4, \quad -a < b \leq a < c \text{ または } 0 \leq b \leq a = c.$$

$1 \leq a \leq \sqrt{4/3} \Longrightarrow a = 1$. $-1 < b \leq 1 < c$ または $0 \leq b \leq 1 = c$.

$b^2 - 4c = -4$ より b は偶数．よって $b = 0$，したがって $c = 1$．ゆえに判別式 -4 の簡約形式は $x^2 + y^2$ だけであり，$h(-4) = 1$ を得る．

類数の計算例 2

例 3.11 ($D = -163$)

$ax^2 + bxy + cy^2$ が判別式 -163 で簡約とすれば

$$b^2 - 4ac = -163, \qquad -a < b \leq a < c \text{ または } 0 \leq b \leq a = c.$$

したがって $|b| \leq a$ である．$1 \leq a \leq \sqrt{163/3}$ より $1 \leq a \leq 7$．
$b^2 - 4ac = -163$ より b は奇数．
$a = 1 \Longrightarrow b = 1,\ c = 41$．
$a = 2, 3, 4, 5, 6, 7$ のとき，$|b| \leq a$ となる奇数 b について
$4ac = b^2 + 163$ となる c がないことが確かめられる．
ゆえに判別式 -163 の簡約形式は $x^2 + xy + 41y^2$ だけであり
$h(-163) = 1$ を得る．

2 平方和の定理の必要性の証明

奇素数 p が 2 つの平方数の和として $p = a^2 + b^2$ と表せるとする.

a, b がともに偶数 $\Longrightarrow p = a^2 + b^2$ は偶数となって矛盾.

a, b がともに奇数 $\Longrightarrow a^2, b^2$ ともに奇数
$\Longrightarrow p = a^2 + b^2$ は偶数となって矛盾.

したがって a, b のうち一方が偶数で他方は奇数である.
$a = 2m$, $b = 2n + 1$ としてよい. このとき

$$p = a^2 + b^2 = 4m^2 + 4n^2 + 4n + 1 = 4(m^2 + n^2 + n) + 1.$$

2 平方和定理のラグランジュによる十分性の証明

逆に $p = 4q + 1$ とする．系 2.4 により $m^2 \equiv -1 \pmod{p}$ となる $m \in \mathbb{Z}$ が存在する．$m^2 + 1 = pc$, $c \in \mathbb{Z}$ とかいて $\mathbb{Z}$ 係数 2 元 2 次形式 $f(x, y) = px^2 + 2mxy + cy^2$ を考える．この判別式は

$$D(f) = (2m)^2 - 4pc = 4(m^2 - pc) = -4.$$

例 3.10 で見たように判別式 -4 の $\mathbb{Z}$ 係数 2 元 2 次形式はすべて $g(x, y) = x^2 + y^2$ と同値である．したがって $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ が存在して

$$\begin{aligned} f(x, y) = g((x, y)\gamma) = g(rx + ty, sx + uy) &= (rx + ty)^2 + (sx + uy)^2 \\ &= (r^2 + s^2)x^2 + 2(rt + su)xy + (t^2 + u^2)y^2 \end{aligned}$$

となる．x^2 の係数を比較して $p = r^2 + s^2$ を得る． □

Frobenius-Rabinovitch の定理

連続した整数 x における 2 次多項式 $f_q(x)$ の値が素数になるという現象は次の定理によって説明される.

定理 5.1 (Frobenius-Rabinovitch)

q を素数とする. 次の 2 条件は互いに同値である.

(1) $h(1-4q)=1$.

(2) $f_q(n)=n^2+n+q$, $0 \le n \le q-2$ はすべて素数である.

[証明]

$$f_q(x,y)=x^2+xy+qy^2, \quad f_q(x)=f_q(x,1)$$

とおく. $D(f_q)=1-4q$ である.

(1) ⇒ (2) の証明

$h(1-4q)=1$ とする．ある整数 $0 \leq n \leq q-2$ に対して $f_q(n)$ が合成数であると仮定して矛盾を導く．$f_q(n)$ の最小の素因数を p として

$$f_q(n) = pm, \qquad (m \text{ は自然数})$$

とかく．このとき $p \leq m$ である．ここで $\mathbb{Z}$ 係数 2 元 2 次形式

$$g(x,y) = px^2 + (1+2n)xy + my^2$$

を考える．$g(x,y)$ の判別式は

$$\begin{aligned} D(g) &= (1+2n)^2 - 4pm = 1 + 4(n^2+n-pm) \\ &= 1 + 4(n^2+n-n^2-n-q) = 1-4q. \end{aligned}$$

$h(1-4q)=1$ より $g(x,y)$ は $f_q(x,y)$ と同値である．したがって $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ が存在して

(1) ⇒ (2) の証明 つづき

$$\begin{aligned} g(x,y) &= f_q(rx+ty, sx+uy) \\ &= (rx+ty)^2 + (rx+ty)(sx+uy) + q(sx+uy)^2 \\ &= (r^2+rs+qs^2)x^2 + (2rt+ru+ts+asu)xy + (t^2+tu+qu^2)y^2. \end{aligned}$$

x^2 の係数を比較して，$p = r^2+rs+qs^2 = f_q(r,s)$ を得る．

もし $s=0 \Longrightarrow p = r^2$ となって矛盾．ゆえに $s \neq 0$, $s^2 \geq 1$ であり

$$p = r^2+rs+qs^2 = \left(r+\frac{s}{2}\right)^2 + \left(q-\frac{1}{4}\right)s^2 \geq q-\frac{1}{4}.$$

これから $p \geq q$ を得る．一方，$0 \leq n \leq q-2$ より

$$f_q(n) = n^2+n+q \leq (q-2)^2+(q-2)+q = q^2-2q+2 < q^2.$$

これと $q \leq p$ および $p \leq m$ より，$q^2 \leq p^2 \leq pm = f_q(n) < q^2$ となって矛盾．ゆえに (2) が成り立つ．

(2) ⇒ (1) の証明

逆に $0 \leq n \leq q-2$ 対して $f_q(n) = n^2 + n + q$ が素数であるとする．
ここで $q^2 \geq 2q > (4q-1)/2 > (4q-1)/3$ に注意する．
$f(x,y) = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$, $a > 0$, $D(f) = 1 - 4q$，簡約とする．このとき $1 \leq a \leq \sqrt{(4q-1)/3} < q$ かつ $|b| \leq a$．よって $1 \leq a \leq q-1$．$b^2 - 4ac = 1 - 4q$ より b は奇数．
$n = (|b|-1)/2$ とおく．$1 \leq |b| \leq a \leq q-1$ より
$0 \leq n = \frac{1}{2}(|b|-1) \leq \frac{1}{2}(q-2) \leq q-2.$

$$f_q(n) = n(n+1) + q = \frac{1}{4}(b^2 - 4ac + 4ac - 1 + 4q) = ac.$$

仮定より $f_q(n)$ は素数，$1 \leq a \leq c \Longrightarrow a = 1,\ c = f_q(n)$．
このとき $|b| = 1,\ 1 - 4q = b^2 - 4ac = 1 - 4c,\ c = q$ である．
$c = q \geq 2 > 1 = a$ より $b = 1$ である．以上により
$f(x,y) = x^2 + xy + qy^2 = f_q(x,y)$．ゆえに $h(1-4q) = 1$． □

類数が 1 の判別式

$h(D) = 1$ となるような負の整数 D は 1967 年に Baker と Stark によって独立に証明された次の定理によって決定されている.

定理 5.2

類数 $h(D)$ が 1 となる負の整数 D は次の 9 個に限る.

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

したがって $h(1-4q) = 1$ となる素数 q は次の 6 個に限る.

$$q = 2,\ 3,\ 5,\ 11,\ 17,\ 41.$$

正の判別式についての Gauss 予想

正の整数 D を判別式にもつ $\mathbb{Z}$ 係数 2 元 2 次形式の類数 $h(D)$ も同様に定義される.

これについて Gauss は

Gauss 予想

$h(D) = 1$ となる正の整数 D は無数に存在するであろう

と予想したが，これは現在でも未解決である.

Frobenius-Rabinovitch の定理の拡張

自然数 ν の素因数の数を重複も許して $\deg \nu$ で表すことにする．例えば，$\deg 10 = 2$, $\deg 8 = 3$, $\deg 15 = 2$ である．$\deg p = 1 \iff p$ は素数．素数 q に対して $f_q(x) = x^2 + x + q$ とし

$$m(1-4q) = \max\{\deg(f_q(n)) \,:\, 0 \leq n \leq q-2\}$$

とおく．このとき Frobenius-Rabinovitch の定理は

$$m(1-4q) = 1 \iff h(1-4q) = 1$$

を主張している．佐々木隆二氏は

$$m(1-4q) = 2 \iff h(1-4q) = 2$$

を証明した．しかし $m(-84) = 3$ であるが $h(-84) = 4$ である．また佐々木氏は常に

$$m(1-4q) \leq h(1-4q)$$

が成り立つことも証明している．

参考文献

[1] 青木昇，素数と 2 次体の整数論，共立出版，2012.