

2次形式による整数の表示に関する考察

北海道千歳北陽高等学校 教諭 高 倉 亘

(Keywords: 2次形式、判別式、原始解、類数、平方剰余)

1 緒 言

2次形式 $f(x, y) = ax^2 + bxy + cy^2$ と整数 n に対して、 $f(x, y) = n$ を満たす整数 x, y が存在するとき、 n は f によって表示されることになる。本稿では、与えられた2次形式が自然数 n を表示するか、あるいは、与えられた判別式を有する2次形式の中に自然数 n を表示するものが存在するかといった問題について考察する。

2次形式 f が0を表示することは明らかであり、2次形式 f が負の数 $-n$ を表示することは2次形式 $-f$ が自然数 n を表示することと同値である。これより、2次形式による整数の表示問題は自然数の表示問題に帰着される。^{1) - 10)}

2 2次形式による自然数を表示するための条件

$f(x, y) = ax^2 + bxy + cy^2$ を判別式 D の2次形式、 n を自然数とする。整数の組 (r, t) が $f(x, y) = n$ の原始解であるとは、 $f(r, t) = n$ かつ r, t が互いに素であるときにいう。また、このとき、 n は f により原始的に表示されるという。 n が f により表示されても、原始的に表示されるとは限らない。例えば、 $f(x, y) = x^2 + y^2$ のとき、 $2^2 + 2^2 = 8$ より、8は f により表示されるが原始的には表示されない。 (α, β) が $f(x, y) = n$ の非原始解であり、その最大公約数が d であるとき、明らかに d^2 は n を割り切る。ここで、 $\alpha = \alpha'd, \beta = \beta'd, n = n'd^2$ とおけば、 (α', β') は $f(x, y) = n'$ の原始解である。これより、2次形式による整数の表示問題は原始解の存在問題に帰着される。特に、 n が素数である場合等、1以外の平方数で割り切れないときには、 $f(x, y) = n$ の解は常に原始解である。

補題 1

$m^2 \equiv D \pmod{4n}$ 、 $0 \leq m < 2n$ を満たす整数 m が存在するとき、 n は判別式 D のある2次形式により原始的に表示される。

proof

仮定より、

$$\ell = \frac{m^2 - D}{4n}$$

が整数であることから、2次形式 $g(x, y) = nx^2 + mxy + \ell y^2$ が定まる。 g の判別式は $m^2 - 4n\ell = D$ であり、 $g(1, 0) = n$ であることから、 n は判別式 D の2次形

式 g により原始的に表示される。

q.e.d.

定理 1

自然数 n が、判別式 D のある 2 次形式で原始的に表示されるための必要十分条件は、 $m^2 \equiv D \pmod{4n}$ 、 $0 \leq m < 2n$ を満たす整数 m が存在することである。

proof

十分性は補題 1 で示されているので必要性を示す。自然数 n が判別式 D のある 2 次形式 $f(x, y) = ax^2 + bxy + cy^2$ で原始的に表示されたと仮定する。 $f(x, y) = n$ の 1 つの原始解を (r, t) とする。 r 、 t は互いに素であるから、1 次不定方程式

$$ry - tx = 1 \quad \dots$$

に整数解 $(x, y) = (s, u)$ が存在する。 $T = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ とおくと、 T は正の特殊 1 次変換

である。このとき、

$$\begin{pmatrix} n & \frac{m}{2} \\ \frac{m}{2} & \ell \end{pmatrix} = {}^t T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} T, \quad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

により、 $f(x, y)$ に正に対等な 2 次形式

$$g(x', y') = nx'^2 + mx'y' + \ell y'^2$$

が定まる。ここで、

$$\begin{cases} n = ar^2 + brt + ct^2 \\ m = 2ars + b(ru + st) + 2ctu \\ \ell = as^2 + bsu + cu^2 \end{cases}$$

が成立する。

ここで、 (s_0, u_0) の 1 つの解を (s_0, u_0) とすると、一般解は、

$$s = s_0 + rk, \quad u = u_0 + tk \quad (k \in \mathbb{Z})$$

と表される。これを、 $m = 2ars + b(ru + st) + 2ctu$ に代入すると、

$$\begin{aligned} m &= 2ar(s_0 + rk) + b(ru_0 + rtk + s_0t + rtk) + 2ct(u_0 + tk) \\ &= 2ars_0 + b(ru_0 + s_0t) + 2ctu_0 + 2nk \end{aligned}$$

となることから、

$$m \equiv 2ars_0 + b(ru_0 + s_0t) + 2ctu_0 \pmod{2n}$$

が成立する。したがって、 k を適当に選んで m が $0 \leq m < 2n$ を満たすようにできる。

一方、 g は f に正に対等であるから判別式が一致するので、

$$D = b^2 - 4ac = m^2 - 4n\ell$$

が成立する。ゆえに、

$$m^2 \equiv D \pmod{4n}, \quad 0 \leq m < 2n$$

を満たす整数 m が存在する。

q.e.d.

3 2次形式による整数の表示可能性に関する判定方法

前章の結果のみでは、 $m^2 \equiv D \pmod{4n}$ かつ $0 \leq m < 2n$ を満たす整数 m が存在しても、特定の2次形式 $f(x, y) = ax^2 + bxy + cy^2$ が n を表示するかどうかは判断できない。しかしながら、定理1の証明より、2次形式 f が n を表示すれば $f(x, y)$ に正に対等な2次形式

$$g(x', y') = nx'^2 + mx'y' + \ell y'^2$$

であって、

$$D = b^2 - 4ac = m^2 - 4n\ell \text{ かつ } m^2 \equiv D \pmod{4n}, \quad 0 \leq m < 2n \quad \dots$$

を満たすものが存在する。

) を満たす m, ℓ は有限個であるから、それぞれに対して、

$$\begin{pmatrix} n & \frac{m}{2} \\ \frac{m}{2} & \ell \end{pmatrix} = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

を満たす正の特殊1次変換 $T = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ が存在するかどうか判定する。

)ある m, ℓ に対して上のような T が存在すれば、 n は f で原始的に表示される。このとき、 (r, t) が $f(x, y) = n$ の原始解である。

特に、判別式 D の狭義の類数 $h^+(D)$ が1の場合、 f と g は必ず正に対等となり、 $m^2 \equiv D \pmod{4n}, 0 \leq m < 2n$ を満たす m が存在するとき、 n は f で原始的に表示される。

原理的には上述の手順で、 n が f によって表示されるかどうか判定し、表示される場合は、すべての原始解を求めることができる。判別式が負の場合は上のような T は常に有限個であるから、 $f(x, y) = n$ の原始解も有限個である。しかしながら、判別式が正の場合には $f(x, y) = n$ の原始解は無限個となる場合があり、原始解を求める計算も容易ではない。

4 2次形式による素数の表示例

本章では、与えられた2次形式がどのような奇素数を表示し得るかを考察する。なお、奇素数 p が2次形式で表示されるときは原始的な表示に限ることとする。また、以下の計算では平方剰余に関する次の結果を利用する。

$$\begin{aligned} \left(\frac{-1}{p}\right) &= \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases} \\ \left(\frac{-2}{p}\right) &= \begin{cases} 1 & p \equiv 1, 3 \pmod{8} \\ -1 & p \equiv 5, 7 \pmod{8} \end{cases} \\ \left(\frac{3}{p}\right) &= \begin{cases} 1 & p \equiv 1, 11 \pmod{12} \\ -1 & p \equiv 5, 7 \pmod{12} \end{cases} \\ \left(\frac{-3}{p}\right) &= \begin{cases} 1 & p \equiv 1 \pmod{3} \\ -1 & p \equiv 2 \pmod{3} \end{cases} \\ \left(\frac{5}{p}\right) &= \begin{cases} 1 & p \equiv 1, 4 \pmod{5} \\ -1 & p \equiv 2, 3 \pmod{5} \end{cases} \\ \left(\frac{-5}{p}\right) &= \begin{cases} 1 & p \equiv 1, 3, 7, 9 \pmod{20} \\ -1 & p \equiv 11, 13, 17, 19 \pmod{20} \end{cases} \end{aligned}$$

(1) $D = -3$ の場合

補遺1より、 $h^+(-3) = 1$ であり、判別式 -3 の簡約2次形式は、

$$f(x, y) = x^2 + xy + y^2$$

である。奇素数 p が判別式 -3 を有する2次形式で表示されるための必要十分条件は定理1より、

$$m^2 \equiv -3 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである。このとき、 $x^2 \equiv -3 \pmod{p}$ が解をもつ。逆に、 $x^2 \equiv -3 \pmod{p}$ が解 $\alpha (0 \leq \alpha < p)$ をもつときは、 m を α または $\alpha + p$ の奇数の方とおけば、

$$m^2 \equiv -3 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす。したがって、求める素数のうち100以下のものは、

$$3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97$$

である。これらを簡約2次形式 $f(x, y) = x^2 + xy + y^2$ により表示すると次のようになる。

$$\begin{aligned} &) f(x, y) = x^2 + xy + y^2 \text{ で表示できる } 100 \text{ 以下の奇素数} \\ & \quad 3 = 1^2 + 1 \cdot 1 + 1^2 = f(1, 1) \\ & \quad 7 = 2^2 + 2 \cdot 1 + 1^2 = f(2, 1) \\ & \quad 13 = 3^2 + 3 \cdot 1 + 1^2 = f(3, 1) \end{aligned}$$

$$19 = 3^2 + 3 \cdot 2 + 2^2 = f(3, 2)$$

$$31 = 5^2 + 5 \cdot 1 + 1^2 = f(5, 1)$$

$$37 = 4^2 + 4 \cdot 3 + 3^2 = f(4, 3)$$

$$43 = 6^2 + 6 \cdot 1 + 1^2 = f(6, 1)$$

$$61 = 5^2 + 5 \cdot 4 + 4^2 = f(5, 4)$$

$$67 = 7^2 + 7 \cdot 2 + 2^2 = f(7, 2)$$

$$73 = 8^2 + 8 \cdot 1 + 1^2 = f(8, 1)$$

$$79 = 7^2 + 7 \cdot 3 + 3^2 = f(7, 3)$$

$$97 = 8^2 + 8 \cdot 3 + 3^2 = f(8, 3)$$

(2) $D = -4$ の場合

補遺 1 より、 $\tilde{h}(-4) = 1$ であり、判別式 -4 の簡約 2 次形式は、

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

である。奇素数 p が判別式 -4 を有する 2 次形式で表示されるための必要十分条件は定理 1 より、

$$m^2 \equiv -4 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである。このような m が存在すれば偶数でなければならないから、 $m = 2m_0$ とおくことができる。このとき、

$$m_0^2 \equiv -1 \pmod{p}, \quad 0 \leq m_0 < p$$

が成立する。逆に上式を満たす m_0 が存在すれば $m = 2m_0$ は、

$$m^2 \equiv -4 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす。以上より、判別式 -4 の 2 次形式で表示される奇素数 p は、

$$x^2 \equiv -1 \pmod{p}$$

が解をもつ奇素数、すなわち、 $\left(\frac{-1}{p}\right) = 1$ となるものである。

これらは、 $p \equiv 1 \pmod{4}$ を満たすものである。したがって、求める素数のうち 100 以下のものは、

$$5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97$$

である。これらを簡約 2 次形式 $f(x, y) = x^2 + y^2$ により表示すると次のようになる。

) $f(x, y) = x^2 + y^2$ で表示できる 100 以下の奇素数

$$5 = 1^2 + 2^2 = f(1, 2)$$

$$13 = 2^2 + 3^2 = f(2, 3)$$

$$17 = 1^2 + 4^2 = f(1, 4)$$

$$29 = 2^2 + 5^2 = f(2, 5)$$

$$\begin{aligned}
37 &= 1^2 + 6^2 = f(1, 6) \\
41 &= 4^2 + 5^2 = f(4, 5) \\
53 &= 2^2 + 7^2 = f(2, 7) \\
61 &= 5^2 + 6^2 = f(5, 6) \\
73 &= 3^2 + 8^2 = f(3, 8) \\
89 &= 5^2 + 8^2 = f(5, 8) \\
97 &= 4^2 + 9^2 = f(4, 9)
\end{aligned}$$

(3) $D = -20$ の場合

補遺 1 より、 $\tilde{h}(-20) = 2$ であり、判別式 -20 の簡約 2 次形式は、

$$f_1(x, y) = x^2 + 5y^2, \quad f_2(x, y) = 2x^2 + 2xy + 3y^2$$

であるが、1 は f_1 で表示されるが、 f_2 では表示されない。したがって、 f_1 と f_2 は対等でない。奇素数 p が判別式 -20 を有する 2 次形式で表示されるための必要十分条件は定理 1 より、

$$m^2 \equiv -20 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである。このような m が存在すれば、偶数でなければならぬから、 $m = 2m_0$ とおくことができる。このとき、

$$m_0^2 \equiv -5 \pmod{p}, \quad 0 \leq m_0 < p$$

が成立する。逆に上式を満たす m_0 が存在すれば、 $m = 2m_0$ は、

$$m^2 \equiv -20 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす。以上から判別式 -20 の 2 次形式で表示される奇素数 p は、

$$p = 5 \text{ または } p \equiv 1, 3, 7, 9 \pmod{20}$$

を満たす。このような素数で 100 以下のものは、

$$3, 5, 7, 23, 29, 41, 43, 47, 61, 67, 83, 89$$

である。 f_1 、 f_2 のどちらで表示されるかは次のようにして判定できる。

$$f_1(x, y) = x^2 + 5y^2 = p \text{ とすると、 } x^2 \equiv p \pmod{5} \text{ となり、 } p = 5 \text{ または } \left(\frac{p}{5}\right) = 1$$

となることから、 $p = 5$ または $p \equiv 1, 9 \pmod{20}$ を得る。

$$f_2(x, y) = 2x^2 + 2xy + 3y^2 = p \text{ とする。 } f_2(x, y) \text{ は } 5 \text{ を表示できないので、 } p \neq 5$$

である。 $4x^2 + 4xy + 6y^2 = 2p$ より、 $(2x + y)^2 + 5y^2 = 2p$ 、したがって、

$$(2x + y)^2 \equiv 2p \pmod{5} \text{ となる。これより、 } \left(\frac{2p}{5}\right) = 1 \text{ となる。 } \left(\frac{2}{5}\right) = -1 \text{ であるから、}$$

$\left(\frac{p}{5}\right) = -1$ となる。ゆえに、 $p \equiv 3, 7 \pmod{20}$ を得る。

上に挙げた100以下の素数を $f_1(x, y)$ または $f_2(x, y)$ で表示すると次のようになる。

) $f_1(x, y) = x^2 + 5y^2$ で表示できる100以下の奇素数

$$5 = 0^2 + 5 \cdot 1^2 = f_1(0, 1)$$

$$29 = 3^2 + 5 \cdot 2^2 = f_1(3, 2)$$

$$41 = 6^2 + 5 \cdot 1^2 = f_1(6, 1)$$

$$61 = 4^2 + 5 \cdot 3^2 = f_1(4, 3)$$

$$89 = 3^2 + 5 \cdot 4^2 = f_1(3, 4)$$

) $f_2(x, y) = 2x^2 + 2xy + 3y^2$ で表示できる100以下の奇素数

$$3 = 2 \cdot 1^2 + 2 \cdot 1 \cdot (-1) + 3 \cdot (-1)^2 = f_2(1, -1)$$

$$7 = 2 \cdot 1^2 + 2 \cdot 1 \cdot 1 + 3 \cdot 1^2 = f_2(1, 1)$$

$$23 = 2 \cdot 2^2 + 2 \cdot 2 \cdot (-3) + 3 \cdot (-3)^2 = f_2(2, -3)$$

$$43 = 2 \cdot 5^2 + 2 \cdot 5 \cdot (-1) + 3 \cdot (-1)^2 = f_2(5, -1)$$

$$47 = 2 \cdot 5^2 + 2 \cdot 5 \cdot (-3) + 3 \cdot (-3)^2 = f_2(5, -3)$$

$$67 = 2 \cdot 1^2 + 2 \cdot 1 \cdot (-5) + 3 \cdot (-5)^2 = f_2(1, -5)$$

$$83 = 2 \cdot 7^2 + 2 \cdot 7 \cdot (-3) + 3 \cdot (-3)^2 = f_2(7, -3)$$

(4) $D = -24$ の場合

補遺1より、 $\tilde{h}^+(-24) = 2$ であり、判別式 -24 の簡約2次形式は、

$$f_1(x, y) = x^2 + 6y^2, \quad f_2(x, y) = 2x^2 + 3y^2$$

であるが、1は f_1 で表示されるが、 f_2 では表示されない。したがって、 f_1 と f_2 は対等でない。奇素数 p が判別式 -24 を有する2次形式で表示されるための必要十分条件は定理1より、

$$m^2 \equiv -24 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである。このような m が存在すれば、偶数でなければならぬから、 $m = 2m_0$ とおくことができる。このとき、

$$m_0^2 \equiv -6 \pmod{p}, \quad 0 \leq m_0 < p$$

が成立する。逆に上式を満たす m_0 が存在すれば、 $m = 2m_0$ は、

$$m^2 \equiv -24 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす。以上から判別式 -24 の2次形式で表示される奇素数 p は、

$$p = 3 \text{ または、 } \left(\frac{-6}{p} \right) = 1$$

となるもの、すなわち、

$$p = 3 \text{ または、 } p \equiv 1, 5, 7, 11 \pmod{24}$$

を満たすものである。したがって、判別式 -24 を有する2次形式で表示される100以下の奇素数は、

$$3, 5, 7, 11, 29, 31, 53, 59, 73, 79, 83, 97$$

である。 f_1 、 f_2 のどちらで表示されるかは次のようにして判定できる。

$f_1(x, y) = x^2 + 6y^2 = p$ とする。明らかに、 $p \neq 3$ であるので、 $x^2 \equiv p \pmod{3}$ となり、 $\left(\frac{p}{3} \right) = 1$ を得る。したがって、 $p \equiv 1, 7 \pmod{24}$ を得る。

$f_2(x, y) = 2x^2 + 3y^2 = p$ とすると、 $2x^2 \equiv p \pmod{3}$ となる。これより、 $p = 3$ または、

$$\left(\frac{p}{3} \right) = \left(\frac{2x^2}{3} \right) = \left(\frac{2}{3} \right) = -1$$

が成立する。したがって、 $p = 3$ または、 $p \equiv 5, 11 \pmod{24}$ を得る。

上に挙げた100以下の素数を $f_1(x, y)$ または $f_2(x, y)$ で表示すると次のようになる。

) $f_1(x, y) = x^2 + 6y^2$ で表示できる100以下の奇素数

$$7 = 1^2 + 6 \cdot 1^2 = f_1(1,1)$$

$$31 = 5^2 + 6 \cdot 1^2 = f_1(5,1)$$

$$73 = 7^2 + 6 \cdot 2^2 = f_1(7,2)$$

$$79 = 5^2 + 6 \cdot 3^2 = f_1(5,3)$$

$$97 = 1^2 + 6 \cdot 4^2 = f_1(1,4)$$

) $f_2(x, y) = 2x^2 + 3y^2$ で表示できる 100 以下の奇素数

$$3 = 2 \cdot 0^2 + 3 \cdot 1^2 = f_2(0,1)$$

$$5 = 2 \cdot 1^2 + 3 \cdot 1^2 = f_2(1,1)$$

$$11 = 2 \cdot 2^2 + 3 \cdot 1^2 = f_2(2,1)$$

$$29 = 2 \cdot 1^2 + 3 \cdot 3^2 = f_2(1,3)$$

$$53 = 2 \cdot 5^2 + 3 \cdot 1^2 = f_2(5,1)$$

$$59 = 2 \cdot 4^2 + 3 \cdot 3^2 = f_2(4,3)$$

$$83 = 2 \cdot 2^2 + 3 \cdot 5^2 = f_2(2,5)$$

(5) $D = 5$ の場合

補遺 2 より、 $h(5) = h^+(5) = 1$ であり、判別式 5 の簡約 2 次形式は、

$$f(x, y) = x^2 - xy - y^2$$

である。奇素数 p が判別式 5 を有する 2 次形式で表示されるための必要十分条件は定理 1 より、

$$m^2 \equiv 5 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである。このとき、

$$x^2 \equiv 5 \pmod{p}, \quad 0 \leq x < p$$

を満たす解をもつ。逆に、 $\alpha^2 \equiv 5 \pmod{p}, 0 \leq \alpha < p$ を満たす α が存在するときは、

α または $\alpha + p$ の奇数の方を m とおけば、

$$m^2 \equiv 5 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす。以上から、判別式 5 の 2 次形式で表示できる奇素数は、

$$p = 5 \text{ または } p \equiv 1, 4 \pmod{5}$$

を満たす。これらのうち 100 以下のものは、

$$5, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89$$

である。これらを簡約 2 次形式 $f(x, y) = x^2 - xy - y^2$ により表示すると次のようになる。

) $f(x, y) = x^2 - xy - y^2$ で表示できる 100 以下の奇素数

$$5 = 2^2 - 2 \cdot (-1) - (-1)^2 = f(2, -1)$$

$$11 = 3^2 - 3 \cdot (-1) - (-1)^2 = f(3, -1)$$

$$19 = 5^2 - 5 \cdot 1 - 1^2 = f(5, 1)$$

$$29 = 5^2 - 5 \cdot (-1) - (-1)^2 = f(5, -1)$$

$$31 = 5^2 - 5 \cdot (-2) - (-2)^2 = f(5, -2)$$

$$41 = 6^2 - 6 \cdot (-1) - (-1)^2 = f(6, -1)$$

$$59 = 7^2 - 7 \cdot (-2) - (-2)^2 = f(7, -2)$$

$$61 = 7^2 - 7 \cdot (-3) - (-3)^2 = f(7, -3)$$

$$71 = 9^2 - 9 \cdot 1 - 1^2 = f(9, 1)$$

$$79 = 8^2 - 8 \cdot (-3) - (-3)^2 = f(8, -3)$$

$$89 = 10^2 - 10 \cdot 1 - 1^2 = f(10, 1)$$

(6) $D = 12$ の場合

補遺 2 より、 $h(12) = 1$ 、 $h^+(12) = 2$ であり、判別式 12 の簡約 2 次形式は、

$$f_1(x, y) = 2x^2 - 2xy - y^2, \quad f_2(x, y) = x^2 - xy - 2y^2$$

である。奇素数 p が判別式 12 を有する 2 次形式で表示されるための必要十分条件は定理 1 より、

$$m^2 \equiv 12 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである。このとき、 m は偶数で $m = 2m_0$ とおけば m_0 は、

$$m_0^2 \equiv 3 \pmod{p}, \quad 0 \leq m_0 < p$$

を満たす。逆に上式を満たす m_0 が存在すれば、 $m = 2m_0$ は、

$$m^2 \equiv 12 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす。以上から判別式 12 を有する 2 次形式で表示される奇素数 p は、

$$x^2 \equiv 3 \pmod{p}$$

が解をもつもの、すなわち、

$p = 3$ または、 $p \equiv 1, 11 \pmod{12}$

を満たすものである。これらのうち100以下の奇素数は、

3、11、13、23、37、47、59、61、71、73、83、97

である。これらが、 f_1 、 f_2 のどちらで表示されるかは次のようにして判定できる。

$f_1(x, y) = 2x^2 - 2xy - y^2 = p$ とすると、 $4x^2 - 4xy - 2y^2 = 2p$ となるから、

$(2x - y)^2 - 3y^2 = 2p$ である。したがって、 $(2x - y)^2 \equiv 2p \pmod{3}$ となることから、

$p = 3$ または、 $\left(\frac{2p}{3}\right) = 1$ が成立する。 $\left(\frac{2p}{3}\right) = 1$ において、 $\left(\frac{2}{3}\right) = -1$ であることよ

り、 $\left(\frac{p}{3}\right) = -1$ である。以上から、 $p = 3$ または $p \equiv 2 \pmod{3}$ である。

$f_2(x, y) = x^2 - 2xy - 2y^2 = p$ とする。3は f_2 によって表示されない。したがっ

て、 $p \neq 3$ である。 $(x - y)^2 - 3y^2 = p$ となるから、 $(x - y)^2 \equiv p \pmod{3}$ が成立する。これより、 $p \equiv 1 \pmod{3}$ が得られる。

上に挙げた100以下の素数を $f_1(x, y)$ または $f_2(x, y)$ で表示すると次のようになる。

) $f_1(x, y) = 2x^2 - 2xy - y^2$ で表示できる100以下の奇素数

$$3 = 2 \cdot 2^2 - 2 \cdot 2 \cdot 1 - 1^2 = f_1(2, 1)$$

$$11 = 2 \cdot 2^2 - 2 \cdot 2 \cdot (-1) - (-1)^2 = f_1(2, -1)$$

$$23 = 2 \cdot 3^2 - 2 \cdot 3 \cdot (-1) - (-1)^2 = f_1(3, -1)$$

$$47 = 2 \cdot 4^2 - 2 \cdot 4 \cdot (-3) - (-3)^2 = f_1(4, -3)$$

$$59 = 2 \cdot 5^2 - 2 \cdot 5 \cdot (-1) - (-1)^2 = f_1(5, -1)$$

$$71 = 2 \cdot 5^2 - 2 \cdot 5 \cdot (-3) - (-3)^2 = f_1(5, -3)$$

$$83 = 2 \cdot 7^2 - 2 \cdot 7 \cdot 1 - 1^2 = f_1(7, 1)$$

) $f_2(x, y) = x^2 - 2xy - 2y^2$ で表示できる100以下の奇素数

$$13 = 5^2 - 2 \cdot 5 \cdot 1 - 2 \cdot 1^2 = f_2(5, 1)$$

$$37 = 5^2 - 2 \cdot 5 \cdot (-3) - 2 \cdot (-3)^2 = f_2(5, -3)$$

$$61 = 7^2 - 2 \cdot 7 \cdot (-1) - 2 \cdot (-1)^2 = f_2(7, -1)$$

$$73 = 7^2 - 2 \cdot 7 \cdot (-3) - 2 \cdot (-3)^2 = f_2(7, -3)$$

$$97 = 9^2 - 2 \cdot 9 \cdot (-1) - 2 \cdot (-1)^2 = f_2(9, -1)$$

(7) $D = 20$ の場合

補遺 2 より、 $h(20) = h^+(20) = 2$ であり、判別式 20 の簡約 2 次形式は、

$$f_1(x, y) = 2x^2 - 2xy - 2y^2, \quad f_2(x, y) = x^2 - 4xy - y^2$$

である。奇素数 p が判別式 20 を有する 2 次形式で表示されるための必要十分条件は定理 1 より、

$$m^2 \equiv 20 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである。このとき、 m は偶数で $m = 2m_0$ とおけば m_0 は、

$$m_0^2 \equiv 5 \pmod{p}, \quad 0 \leq m_0 < p$$

を満たす。逆に上式を満たす m_0 が存在すれば、 $m = 2m_0$ は、

$$m^2 \equiv 20 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす。以上から判別式 20 を有する 2 次形式で表示される奇素数 p は、

$$x^2 \equiv 5 \pmod{p}$$

が解をもつもの、すなわち、

$$p = 5 \text{ または } p \equiv 1, 4 \pmod{5}$$

を満たすものである。これらのうち 100 以下の奇素数は、

$$5, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89$$

である。ここで、 $f_1(x, y) = 2x^2 - 2xy - 2y^2$ は奇素数を表示することができないの

で、上の条件を満たす奇素数はすべて $f_2(x, y) = x^2 - 4xy - y^2$ で表示される。

上に挙げた 100 以下の素数を $f_2(x, y)$ で表示すると次のようになる。

) $f_2(x, y) = x^2 - 4xy - y^2$ で表示できる 100 以下の奇素数

$$5 = 9^2 - 4 \cdot 9 \cdot 2 - 2^2 = f_2(9, 2)$$

$$11 = 6^2 - 4 \cdot 6 \cdot 1 - 1^2 = f_2(6, 1)$$

$$19 = 2^2 - 4 \cdot 2 \cdot (-3) - (-3)^2 = f_2(2, -3)$$

$$29 = 3^2 - 4 \cdot 3 \cdot (-2) - (-2)^2 = f_2(3, -2)$$

$$31 = 4^2 - 4 \cdot 4 \cdot (-1) - (-1)^2 = f_2(4, -1)$$

$$41 = 3^2 - 4 \cdot 3 \cdot (-4) - (-4)^2 = f_2(3, -4)$$

$$59 = 6^2 - 4 \cdot 6 \cdot (-1) - (-1)^2 = f_2(6, -1)$$

$$61 = 5^2 - 4 \cdot 5 \cdot (-2) - (-2)^2 = f_2(5, -2)$$

$$71 = 4^2 - 4 \cdot 4 \cdot (-5) - (-5)^2 = f_2(4, -5)$$

$$79 = 4^2 - 4 \cdot 4 \cdot (-7) - (-7)^2 = f_2(4, -7)$$

$$89 = 5^2 - 4 \cdot 5 \cdot (-4) - (-4)^2 = f_2(5, -4)$$

5 結 言

本稿が数学に興味を持つ高校生への議論の題材提供となり、新たな問題提起がなされることを期待したい。

参 考 文 献

- 1) 高木貞治「初等整数論講義」共立出版.
- 2) 河田敬義「数論」岩波書店.
- 3) ディリクレ・デデキント「整数論講義」(酒井孝一 訳)共立出版.
- 4) C. F. ガウス「ガウス整数論」(高瀬正仁 訳)朝倉書店.
- 5) W.J. Leveque「Topics in number theory」Dover.
- 6) D.B. Zagier「Zetafunktionen und quadratische korper」Springer-Verlag.
- 7) 高倉 亘「 \sqrt{n} の連分数展開に関する考察」数学のいずみHP.
- 8) 高倉 亘「2次形式と2次代数的数に関する考察」数学のいずみHP.
- 9) 高倉 亘「負の判別式を有する簡約2次形式に関する考察」数学のいずみHP.
- 10) 高倉 亘「正の判別式を有する簡約2次形式に関する考察」数学のいずみHP.

<補遺1> 負の判別式を有する簡約2次形式の例

D	簡約2次形式	$\tilde{h}^+(D)$
- 3	$f(x, y) = x^2 + xy + y^2$	1
- 4	$f(x, y) = x^2 + y^2$	1
- 7	$f(x, y) = x^2 + xy + 2y^2$	1
- 8	$f(x, y) = x^2 + 2y^2$	1
- 11	$f(x, y) = x^2 + xy + 3y^2$	1
- 12	$f_1(x, y) = x^2 + 3y^2$ 、 $f_2(x, y) = 2x^2 + 2xy + 2y^2$	2
- 15	$f_1(x, y) = x^2 + xy + 4y^2$ 、 $f_2(x, y) = 2x^2 + xy + 2y^2$	2
- 16	$f_1(x, y) = x^2 + 4y^2$ 、 $f_2(x, y) = 2x^2 + 2y^2$	2
- 19	$f(x, y) = x^2 + xy + 5y^2$	1
- 20	$f_1(x, y) = x^2 + 5y^2$ 、 $f_2(x, y) = 2x^2 + 2xy + 3y^2$	2
- 23	$f_1(x, y) = x^2 + xy + 6y^2$ 、 $f_2(x, y) = 2x^2 + xy + 3y^2$ $f_3(x, y) = 2x^2 - xy + 3y^2$	3
- 24	$f_1(x, y) = x^2 + 6y^2$ 、 $f_2(x, y) = 2x^2 + 3y^2$	2
- 27	$f_1(x, y) = x^2 + xy + 7y^2$ 、 $f_2(x, y) = 3x^2 + 3xy + 3y^2$	2
- 28	$f_1(x, y) = x^2 + 7y^2$ 、 $f_2(x, y) = 2x^2 + 2xy + 4y^2$	2
- 31	$f_1(x, y) = 2x^2 + xy + 4y^2$ 、 $f_2(x, y) = 2x^2 - xy + 4y^2$ $f_3(x, y) = x^2 + xy + 8y^2$	3
- 32	$f_1(x, y) = x^2 + 8y^2$ 、 $f_2(x, y) = 3x^2 + 2xy + 3y^2$ $f_3(x, y) = 2x^2 + 4y^2$	3
- 35	$f_1(x, y) = x^2 + xy + 9y^2$ 、 $f_2(x, y) = 3x^2 + xy + 3y^2$	2
- 36	$f_1(x, y) = x^2 + 9y^2$ 、 $f_2(x, y) = 3x^2 + 3y^2$ $f_3(x, y) = 2x^2 + 2xy + 5y^2$	3
- 39	$f_1(x, y) = x^2 + xy + 10y^2$ 、 $f_2(x, y) = 2x^2 + xy + 5y^2$ $f_3(x, y) = 2x^2 - xy + 5y^2$ 、 $f_4(x, y) = 3x^2 + 3xy + 4y^2$	4
- 40	$f_1(x, y) = x^2 + 10y^2$ 、 $f_2(x, y) = 2x^2 + 5y^2$	2
- 43	$f(x, y) = x^2 + xy + 11y^2$	1
- 44	$f_1(x, y) = x^2 + 11y^2$ 、 $f_2(x, y) = 2x^2 + 2xy + 6y^2$ $f_3(x, y) = 3x^2 + 2xy + 4y^2$ 、 $f_4(x, y) = 3x^2 - 2xy + 4y^2$	4
- 47	$f_1(x, y) = x^2 + xy + 12y^2$ 、 $f_2(x, y) = 2x^2 + xy + 6y^2$ $f_3(x, y) = 2x^2 - xy + 6y^2$ 、 $f_4(x, y) = 3x^2 + xy + 4y^2$ $f_5(x, y) = 3x^2 - xy + 4y^2$	5

<補遺 2> 正の判別式を有する簡約2次形式の例および類数 $h(D)$ 、狭義の類数 $h^+(D)$

D	簡約2次形式	簡約2次無理数	連分数展開	$h(D)$	$h^+(D)$
5	$f(x, y) = x^2 - xy - y^2$	$\xi = \frac{1+\sqrt{5}}{2}$	$\xi = [1]$	1	1
8	$f(x, y) = x^2 - 2xy - y^2$	$\xi = 1 + \sqrt{2}$	$\xi = [2]$	1	1
12	$f_1(x, y) = 2x^2 - 2xy - y^2$ $f_2(x, y) = x^2 - 2xy - 2y^2$	$\xi_1 = \frac{1+\sqrt{5}}{2}$ $\xi_2 = 1 + \sqrt{3}$	$\xi_1 = [1, 2]$ $\xi_2 = [2, 1]$	1	2
13	$f(x, y) = x^2 - 3xy - y^2$	$\xi = \frac{3+\sqrt{13}}{2}$	$\xi = [3]$	1	1
17	$f_1(x, y) = x^2 - 3xy - 2y^2$ $f_2(x, y) = 2x^2 - xy - 2y^2$ $f_3(x, y) = 2x^2 - 3xy - y^2$	$\xi_1 = \frac{3+\sqrt{17}}{2}$ $\xi_2 = \frac{1+\sqrt{17}}{4}$ $\xi_3 = \frac{3+\sqrt{17}}{4}$	$\xi_1 = [3, 1, 1]$ $\xi_2 = [1, 3, 1]$ $\xi_3 = [1, 1, 3]$	1	1
20	$f_1(x, y) = 2x^2 - 2xy - 2y^2$ $f_2(x, y) = x^2 - 4xy - y^2$	$\xi_1 = \frac{1+\sqrt{5}}{2}$ $\xi_2 = 2 + \sqrt{5}$	$\xi_1 = [1]$ $\xi_2 = [4]$	2	2
21	$f_1(x, y) = x^2 - 3xy - 3y^2$ $f_2(x, y) = 3x^2 - 3xy - y^2$	$\xi_1 = \frac{3+\sqrt{21}}{2}$ $\xi_2 = \frac{3+\sqrt{21}}{6}$	$\xi_1 = [3, 1]$ $\xi_2 = [1, 3]$	1	2
24	$f_1(x, y) = x^2 - 4xy - 2y^2$ $f_2(x, y) = 2x^2 - 4xy - y^2$	$\xi_1 = 2 + \sqrt{6}$ $\xi_2 = \frac{2+\sqrt{6}}{2}$	$\xi_1 = [4, 2]$ $\xi_2 = [2, 4]$	1	2
28	$f_1(x, y) = x^2 - 4xy - 3y^2$ $f_2(x, y) = 2x^2 - 2xy - 3y^2$ $f_3(x, y) = 3x^2 - 2xy - 2y^2$ $f_4(x, y) = 3x^2 - 4xy - y^2$	$\xi_1 = 2 + \sqrt{7}$ $\xi_2 = \frac{1+\sqrt{7}}{2}$ $\xi_3 = \frac{1+\sqrt{7}}{3}$ $\xi_4 = \frac{2+\sqrt{7}}{3}$	$\xi_1 = [4, 1, 1, 1]$ $\xi_2 = [1, 1, 4, 1]$ $\xi_3 = [1, 4, 1, 1]$ $\xi_4 = [1, 1, 1, 4]$	1	2
29	$f(x, y) = x^2 - 5xy - y^2$	$\xi = \frac{5+\sqrt{29}}{2}$	$\xi = [5]$	1	1
32	$f_1(x, y) = x^2 - 4xy - 4y^2$ $f_2(x, y) = 2x^2 - 4xy - 2y^2$ $f_3(x, y) = 4x^2 - 4xy - y^2$	$\xi_1 = 2 + 2\sqrt{2}$ $\xi_2 = 1 + \sqrt{2}$ $\xi_3 = \frac{1+\sqrt{2}}{2}$	$\xi_1 = [4, 1]$ $\xi_2 = [2]$ $\xi_3 = [1, 4]$	2	3
33	$f_1(x, y) = 2x^2 - 3xy - 3y^2$ $f_2(x, y) = 3x^2 - 3xy - 2y^2$ $f_3(x, y) = x^2 - 5xy - 2y^2$ $f_4(x, y) = 2x^2 - 5xy - y^2$	$\xi_1 = \frac{3+\sqrt{33}}{4}$ $\xi_2 = \frac{3+\sqrt{33}}{6}$ $\xi_3 = \frac{5+\sqrt{33}}{2}$ $\xi_4 = \frac{5+\sqrt{33}}{4}$	$\xi_1 = [2, 5, 2, 1]$ $\xi_2 = [1, 2, 5, 2]$ $\xi_3 = [5, 2, 1, 2]$ $\xi_4 = [2, 1, 2, 5]$	1	2
37	$f_1(x, y) = 3x^2 - xy - 3y^2$ $f_2(x, y) = x^2 - 5xy - 3y^2$ $f_3(x, y) = 3x^2 - 5xy - y^2$	$\xi_1 = \frac{1+\sqrt{37}}{6}$ $\xi_2 = \frac{5+\sqrt{37}}{2}$ $\xi_3 = \frac{5+\sqrt{37}}{6}$	$\xi_1 = [1, 5, 1]$ $\xi_2 = [5, 1, 1]$ $\xi_3 = [1, 1, 5]$	1	1
40	$f_1(x, y) = 3x^2 - 2xy - 3y^2$ $f_2(x, y) = 2x^2 - 4xy - 3y^2$ $f_3(x, y) = 3x^2 - 4xy - 2y^2$ $f_4(x, y) = x^2 - 6xy - y^2$	$\xi_1 = \frac{1+\sqrt{10}}{3}$ $\xi_2 = \frac{2+\sqrt{10}}{2}$ $\xi_3 = \frac{2+\sqrt{10}}{3}$ $\xi_4 = 3 + \sqrt{10}$	$\xi_1 = [1, 2, 1]$ $\xi_2 = [2, 1, 1]$ $\xi_3 = [1, 1, 2]$ $\xi_4 = [6]$	2	2