第 33 回数学史シンポジウム　津田塾大学　2023 年 10 月 14 日（土）

判別式が正の非平方数の整数係数２元２次形式の周期について

前田博信

1　はじめに

整数 D は正の非平方数とする．通常「ペル方程式」とよばれている次の不定方程式（1）の解法のうち，中世インドのチャクラヴァーラ（円環法）による方法（佐藤 [4]）と，判別式が正の非平方数の整数係数 2 元 2 次形式の被約形式鎖（フルヴィッツ [3]）を用いる方法を比較する．

$$x^2 - Dy^2 = 1 \tag{1}$$

どちらも「巡回性（周期性）」を用いる．チャクラヴァーラは（1）の解法に特化していて高速である．一方，被約形式鎖を用いる方法は計算量が多いが，（1）の解法以外にも応用がある．被約形式鎖を用いると（1）の左辺が取る整数値がわかり，特に，-1，-4，4 を取る場合からは既知の結果の初等的証明が得られる．

例えば，$D = 85$ のとき $t^2 - 85u^2 = -4$ には整数解，$(t, u) = (9, 1)$，$(62739, 6805)$，$\cdots$，がある．このとき，$h^2 - 4ac = 85$ をみたす a，h，c に対して，正式変数変換 $X = aux + \dfrac{hu+t}{2}y$，$Y = \dfrac{-hu+t}{2}x - cuy$ により (この場合の h は奇数である)，$-cX^2 - hXY - aY^2 = ax^2 + hxy + cy^2$ が成り立つ．すなわち，判別式が 85 の任意の 2 次形式 $[\,|\,a, h, c\,|\,]$ は $[\,|\,-c, -h, -a\,|\,]$ と正式同値（狭義同値）になる．

一方，$D = 77$ のときは，判別式が 77 の $f = [\,|\,a, h, c\,|\,] = x^2 + 7xy - 7y^2$ と $f' = [\,|\,-c, -h, -a\,|\,] = 7x^2 - 7xy - y^2$ は正式同値でない．mod 7 で考察すると，$f \equiv x^2$ は 1 を表すが，$f' \equiv -y^2$ は 1 を表さない．実際，$x^2 - 77y^2$ の取る負の整数値は，絶対値の小さい方から，-7，-13，-17，-19，-28，-41，-52，-61，-68，-73，-76，-77，$\cdots$，であり，-1 や -4 の値は取らないことが被約形式鎖の表からわかる．

また，被約形式鎖の表から 2 次形式の自己同型（等長変換）が読み取れる．例えば，$f = [\,|\,1, 7, -7\,|\,]$ の被約形式鎖の表から，$P = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$ が，$\det P = -1$，$P^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ をみたし，$\begin{bmatrix} X \\ Y \end{bmatrix} = P \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ x - y \end{bmatrix}$ により $X^2 + 7XY - 7Y^2 = x^2 + 7xy - 7y^2$ となること，すなわち，P は f の鏡映変換であること，がわかる．

文献

[1] J. H. Conway, The Sensual Quadratic Form, Carus Mathematical Monographs, Vol. 26, MAA, 1997.
（和訳, 細川尋史,『素数が香り、形がきこえる』, シュプリンガー・ジャパン, 2006. 再出版, 丸善出版, 2021.）

[2] C. F. Gauss, Disquisitiones Arithmeticae, Fleischer, 1801.
（和訳, 高瀬正仁,『ガウス整数論』, 朝倉書店, 1995.）

[3] A. Hurwitz, Ueber die Reduction der binären quadratischen Formen, Math. Ann., Bd.45 (1894), 85–117.

[4] 佐藤文広, チャクラヴァーラ — 中世インドのペル方程式の解 — について, 津田塾大学　数学・計算機科学研究所報 44 (2023), 61–94.

2　チャクラヴァーラアルゴリズムの概要

D は正の非平方数とする．$i \geqq 0$ に対して，第 i 行が

p_i	q_i	m_i	u_i

となる表を以下のように帰納的に定義する．第 0 行は，u_0 を $|u^2 - D|$ が最小となる正整数 λ として，

0	1	1	λ

とおく．第 $i+1$ 行は，$u_{i+1} > 0$ を $u_{i+1} \equiv -u_i \mod m_i$ かつ $|u_{i+1}^2 - D|$ が最小となるものの 1 つとし，$m_{i+1} = \dfrac{u_{i+1}^2 - D}{m_i}$ とおき，$p_{i+1} = \dfrac{q_i + p_i u_{i+1}}{m_i}$，$q_{i+1} = \dfrac{Dp_i + q_i u_{i+1}}{m_i}$ とおく．このとき，$i \geqq 0$ に対して，

$$q_i^2 - Dp_i^2 = m_i \tag{2}$$

が成り立ち，

$$m_0 = 1, u_1, m_1, u_2, \cdots, u_n, m_n, \cdots \tag{3}$$

は周期的な繰り返しがある（[4] 5.3 M.1 に基づくチャクラヴァーラの巡回性の証明）．したがって，$m_n = 1$ となる最小の自然数 n を N とすると，$q_{kN}^2 - Dp_{kN}^2 = 1$ $(k = 1, 2, \cdots)$ となり，(1) の解を得る．

列 (3) は一意的ではないが，「回文性」があるものを選ぶことができる．すなわち，N を変えずに，

$$0 \leqq i \leqq N \text{ のとき } \ m_i = m_{N-i}, \tag{4}$$

$$1 \leqq i \leqq N \text{ のとき } \ u_i = u_{N+1-i} \tag{5}$$

をみたすものが選べる（[4] 5.3.6 回文性）．

例 2.1. $D = 85$ のとき，チャクラヴァーラの表（の一つ）は次の通り．

	p	q	m	u
0	0	1	1	9
1	1	9	-4	9
2	-5	-46	-9	11
3	9	83	4	7
4	41	378	-1	9
5	-747	-6887	4	9
6	-3029	-27926	-9	7
7	6805	62739	-4	11
8	-30996	-285769	1	9
9	-564733	-5206581	-4	9
10	2854661	26318674	-9	11
11	-5144589	-47430767	4	7
12	-23433017	-216041742	-1	9
13	426938895	3936182123	4	9
14	1731188597	15960770234	-9	7
15	-3889316089	-35857722591	-4	11
16	17715391848	163327842721	1	9
17	322766369353	2975758891569	-4	9
18	-1631547238613	-15042122300566	-9	11
19	2940328107873	27108485709563	4	7
20	...	...	...	...

$N = 8$ である．表の 8 行目と 16 行目から

$$285769^2 - 85 \cdot 30996^2 = 1$$
$$163327842721^2 - 85 \cdot 17715391848^2 = 1$$

が読み取れ，1 行目と 7 行目から

$$9^2 - 85 \cdot 1^2 = -4$$
$$62739^2 - 85 \cdot 6805^2 = -4$$

が読み取れる．

チャクラヴァーラアルゴリズムによれば，u_3 は，$u_3 + 9 \equiv 0 \mod 4$，かつ $|u_3^2 - 85|$ が最小，となる正整数であるが，$11 \equiv 7 \equiv -9 \mod 4$ で $11^2 - 85 = 85 - 7^2 = 36$ であるから，u_3 には 2 つの可能性，11，7，がある．このように u_i が一意的に決まらない場合を「例外ケース」とよぶが，その場合でも回文性が成り立つように $\{m_i, u_i\}$ を取り換えることができる（[4] 5.3.4 例外ケースが現れる場合）

この表では，m_i, u_i $(0 \leqq i \leqq 4)$ に「回文性」，$m_i = m_{8-i}$，$u_i = u_{9-i}$，があることに注意する．

例 2.2. $D = 77$ のとき，チャクラヴァーラの表は次の通り．

	p	q	m	u
0	0	1	1	9
1	1	9	4	9
2	4	35	-7	7
3	-9	-79	4	7
4	-40	-351	1	9
5	-711	-6239	4	9
6	-2804	-24605	-7	7
7	6319	55449	4	7
8	28080	246401	1	9
9	499121	4379769	4	9
10	1968404	17272675	-7	7
11	-4435929	-38925119	4	7
12	-19712120	-172973151	1	9
13	-350382231	-3074591599	4	9
14	-1381816804	-12125393245	-7	7
15	3114015839	27325378089	4	7
16	13837880160	121426905601	1	9
17	245967827041	2158358922729	4	9
18	970033428004	8512008785315	-7	7
19	-2186034683049	-19182376493359	4	7
20	...	...	...	...

この場合は「例外ケース」は起こらず，表は一意的に決まる．

$N = 4$ であるから，4 行目，8 行目，12 行目，16 行目から

$$351^2 - 77 \cdot 40^2 = 1$$
$$246401^2 - 77 \cdot 28080^2 = 1$$
$$172973151^2 - 77 \cdot 19712120^2 = 1$$
$$1214269056 01^2 - 77 \cdot 13837880160^2 = 1$$

が得られる.

例 2.3. $D = 79$ のとき，チャクラヴァーラの表は次の通り.

	p	q	m	u
0	0	1	1	9
1	1	9	2	9
2	9	80	1	9
3	161	1431	2	9
4	1440	12799	1	9
5	25759	228951	2	9
6	230391	2047760	1	9
7	4121279	36630729	2	9
8	36861120	327628801	1	9
9	659378881	5860687689	2	9
10	5897548809	52418560400	1	9
11	105496499681	937673399511	2	9
12	943570948320	8386642035199	1	9
13	16878780570079	150021883234071	2	9
14	150965454182391	1341810307071440	1	9
15	2700499394712960	24002563644051800	2	9
16	24153529098234200	214681262489395000	1	9
17	432063024373503000	3840260161165060000	2	9
18	3864413690263300000	34347660187996200000	1	9
19	69127383400365800000	614417623222766000000	2	9
20	...	...	...	...

$N=2$ である．i が奇数のときは，$q_i^2 - 79p_i^2 = 2$ が成り立ち，i が偶数のときは，$q_i^2 - 79p_i^2 = 1$ が成り立つ.
一方，$p_2 = 9$，$q_2 = 80$ が得られた時点で，ブラフマグプタ（7 世紀）の公式

$$(x^2 - Dy^2)(u^2 - Dv^2) = (xu + Dyv)^2 - D(yu + xv)^2$$

を用いても，$p_{2k+2} = 9 \cdot q_{2k} + 80 \cdot p_{2k}$，$q_{2k+2} = 80 \cdot q_{2k} + 79 \cdot 9 \cdot p_{2k}$，（$k = 1, 2, \cdots$）が得られる.

注意 2.1. チャクラヴァーラの「回文性」を用いると，D が素数 p の場合に下記の性質がわかる.
(1) $p = 2$ のとき，$m_0 = 1, u_1 = 1, m_1 = -1, u_2 = 1, m_2 = 1$，$N = 2$ である.
(2) $p = 3$ のとき，$m_0 = 1, u_1 = 2, m_1 = 1$，$N = 1$ である.
(3) $p > 3$ のとき $N = 2M$（偶数）であり，m_M は -1，2，-2 のどれかの値をとる.
　$(3-1)$ $m_M = -1 \iff p \equiv 1 \mod 4$，さらに，$M$ も偶数である $\iff$ 例外ケースが現れる,
　$(3-2)$ $m_M = 2 \iff p \equiv 7 \mod 8$,
　$(3-3)$ $m_M = -2 \iff p \equiv 3 \mod 8$

(4) $m_k=-1$（$k>0$）ならば $m_{2k}=1$，である（[4]， 補題 5.3.11）から，奇素数 p について，

$$x^2-py^2=-1 \text{ の整数解が存在する} \iff p\equiv 1 \mod 4\ .$$

3　2 元 2 次形式の正式同値と非正式同値，被約形式，原始形式

一方，ペル方程式（1）の左辺 x^2-Dy^2 は判別式が $4D$ の 2 次形式である．一般に，

定義 3.1. 3 つの整数 a，h，c から定まる 2 次形式 $ax^2+hxy+cy^2=\begin{bmatrix}x\\y\end{bmatrix}^T\begin{bmatrix}a & h/2\\ h/2 & c\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}$ を $[\,|\,a,h,c\,|\,]$ と表し，$d=h^2-4ac$ を 2 次形式 $[\,|\,a,h,c\,|\,]$ の判別式とよぶ.

定義 3.2. (1) $f=[\,|\,a,h,c\,|\,]$ と $f'=[\,|\,a',h',c'\,|\,]$ が「正式同値」であるとは，ある $X=\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\in GL_2(\mathbb{Z})$ により

$$X^T\begin{bmatrix}a & h/2\\ h/2 & c\end{bmatrix}X=\begin{bmatrix}a' & h'/2\\ h'/2 & c'\end{bmatrix}\ ,\det X=1$$

が成り立つことをいう．すなわち，4 つの整数 α，β，γ，δ により

$$\begin{aligned}a'&=a\alpha^2+h\alpha\gamma+c\gamma^2\\ h'/2&=a\alpha\beta+h(\alpha\delta+\beta\gamma)/2+c\gamma\delta\\ c'&=a\beta^2+h\beta\delta+c\delta^2\\ 1&=\alpha\delta-\beta\gamma\end{aligned}$$

が成り立つことである．これを $f\xrightarrow{X}f'$ と略記し，X を f から f' への「正式変換」とよぶ.
(2) (1) の定義において，$\det X=-1$，すなわち 4 つ目の式を $-1=\alpha\delta-\beta\gamma$ とした場合に，f と f' は「非正式同値」であるといい，X を「非正式変換」とよぶ.

$SL_2(\mathbb{Z})=\{X\in GL_2(\mathbb{Z})\ ;\ \det X=1\}$ は，群として 2 つの元 $L=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix},R=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$ で生成される．

$LR^{-1}L=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$ と $LR^{-1}LLR^{-1}L=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$ に注意する．以下，行列 M の転置行列を M^T と表す．

$L^T\begin{bmatrix}a & h/2\\ h/2 & c\end{bmatrix}L=\begin{bmatrix}a & a+h/2\\ a+h/2 & a+h+c\end{bmatrix}$，すなわち，$[\,|\,a,h,c\,|\,]\xrightarrow{L}[\,|\,a,2a+h,a+h+c\,|\,]$

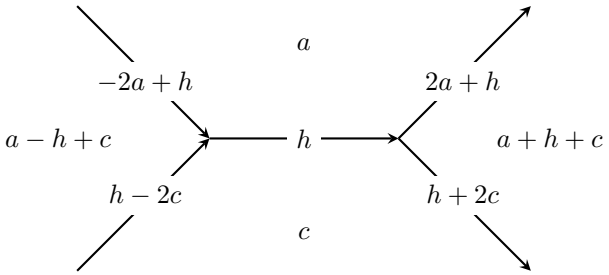
$R^T\begin{bmatrix}a & h/2\\ h/2 & c\end{bmatrix}R=\begin{bmatrix}a+h+c & h/2+c\\ h/2+c & c\end{bmatrix}$，すなわち，$[\,|\,a,h,c\,|\,]\xrightarrow{R}[\,|\,a+h+c,h+2c,c\,|\,]$

$(L^{-1})^T\begin{bmatrix}a & h/2\\ h/2 & c\end{bmatrix}L^{-1}=\begin{bmatrix}a & -a+h/2\\ -a+h/2 & a-h+c\end{bmatrix}$，すなわち，$[\,|\,a,h,c\,|\,]\xrightarrow{L^{-1}}[\,|\,a,-2a+h,a-h+c\,|\,]$

$(R^{-1})^T\begin{bmatrix}a & h/2\\ h/2 & c\end{bmatrix}R^{-1}=\begin{bmatrix}a-h+c & h/2-c\\ h/2-c & c\end{bmatrix}$，すなわち，$[\,|\,a,h,c\,|\,]\xrightarrow{R^{-1}}[\,|\,a-h+c,h-2c,c\,|\,]$

である．これらの操作を繰り返すことにより $[\,|\,a,h,c\,|\,]$ と正式同値な 2 次形式がすべて得られる．

$[|\, a,h,c \,|]$ を，面 a と面 c が辺 h を挟むように表した樹状グラフがコンウェイ [1] のトポグラフである．



注意 3.1. $[|\, a,h,c \,|]$ と $[|\, a',h',c' \,|]$ が正式同値または非正式同値ならば，a，h，c の最大公約数と a'，h'，c' の最大公約数は等しい．

定義 3.3. （[3]）判別式が正の非平方数の $[|\, a,h,c \,|]$ は $a>0$ かつ $c<0$ のとき「被約」であるという．

判別式が正の非平方数 d である被約な 2 次形式は有限個（常に偶数）である．

注意 3.2. ガウス [2] では中間係数 h が偶数の 2 次形式のみを扱う．$[|\, a,2b,c \,|] = x^2+2bxy+cy^2 = \begin{bmatrix} x \\ y \end{bmatrix}^T \begin{bmatrix} a & b \\ b & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$ を [2] では (a,b,c) と表す．$d_0 = b^2-ac$（[2] では Determinante とよぶ）が正の非平方数である (a,b,c) が，ガウスの意味で被約であるとは，

$$0<b<\sqrt{d_0} \quad \text{かつ} \quad \sqrt{d_0}-b<|a|<\sqrt{d_0}+b \quad \text{をみたす}$$

ことである．ガウスの意味で被約な (a,b,c) は，$ac=b^2-d_0<0$ をみたすから，$a>0$ かつ $c<0$ であれば定義 3.3 の被約形式であり，$a<0$ かつ $c>0$ のときは (a,b,c) と正式同値な $(c,-b,a)=[|\, c,-2b,a \,|]$ に置き換えれば，ガウスの意味での被約形式は定義 3.3 による被約形式にすべて含まれる．

注意 3.3. $[|\, 1,0,-D \,|] = (1,0,-D)$ は定義 3.3 では被約形式であるが，ガウスの意味では被約形式でない．

定理 3.1. ([3], Satz 17) 判別式が正の非平方数の 2 次形式は被約な 2 次形式と正式同値になる．

証明. $f=[|\, a,h,c \,|]$ の判別式 $d=h^2-4ac>0$ が非平方数であるから，$ac\neq 0$ である．このとき，2 次方程式 $at^2+ht+c=0$ は異なる 2 つの実数解をもち，そのうちの 1 つの前後で 2 次関数 $F(t)=at^2+ht+c$ の値の符号が負から正に変わるとしてよい．そこで，Farey 数列（負の場合も含む）から，隣り合う 2 つの既約分数 $\dfrac{\beta}{\delta}<\dfrac{\alpha}{\gamma}$ であって，$F\left(\dfrac{\alpha}{\gamma}\right)=\dfrac{a\alpha^2+h\alpha\gamma+c\gamma^2}{\gamma^2}>0$，$F\left(\dfrac{\beta}{\delta}\right)=\dfrac{a\beta^2+h\beta\delta+c\delta^2}{\delta^2}<0$，をみたすものを選び，$X=\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL_2(\mathbb{Z})$ とおく．このとき，

$$X^T \begin{bmatrix} a & h/2 \\ h/2 & c \end{bmatrix} X = \begin{bmatrix} a\alpha^2+h\alpha\gamma+c\gamma^2 & a\alpha\beta+h(\alpha\delta+\beta\gamma)/2+c\gamma\delta \\ a\alpha\beta+h(\alpha\delta+\beta\gamma)/2+c\gamma\delta & a\beta^2+h\beta\delta+c\delta^2 \end{bmatrix}$$

より，f は被約形式 $[|\, a\alpha^2+h\alpha\gamma+c\gamma^2, 2a\alpha\beta+h(\alpha\delta+\beta\gamma)+2c\gamma\delta, a\beta^2+h\beta\delta+c\delta^2 \,|]$ と正式同値になる．

□

定義 3.4. a，h，c の最大公約数が 1 であるような 2 次形式 $f=[\,|\,a,h,c\,|\,]$ を「原始形式」とよぶ.

注意 3.4. 2 次形式 $f=[\,|\,a,h,c\,|\,]$ について,

(1) 中間係数 h が偶数のときは，判別式 $d=h^2-4ac$ は，$d\equiv 0 \mod 4$ であり，$d/4$ が平方因子を含まなければ f は原始形式である.

(2) 中間係数 h が奇数のときは，$d\equiv 1 \mod 4$ である．d が平方因子を含まなければ，f は原始形式である.

(3) ガウス [2] では $f=[\,|\,a,2b,c\,|\,]$ を，a，b，c の最大公約数が 1 のとき，原始形式とよび，さらに，a，$2b$，c の最大公約数も 1 のとき「正式原始形式」とよび，a，$2b$，c の最大公約数が 2 のとき「非正式原始形式」，とよぶ．例えば，$f=[\,|\,a,h,c\,|\,]$ が定義 3.4 における原始形式ならば，$2f=[\,|\,2a,2h,2c\,|\,]$ は，ガウスの意味で，「非正式原始形式」である.

4　被約形式鎖の表

$[\,|\,a_0,h_0,c_0\,|\,]$ は判別式が正の非平方数 d の被約形式とする．このとき，$i\geqq 0$ に対して，第 i 行が

a_i	h_i	c_i	$2a_i+h_i$	h_i+2c_i	$a_i+h_i+c_i$	p_i	q_i	r_i	s_i

となる表を作る．第 0 行は

a_0	h_0	c_0	$2a_0+h_0$	h_0+2c_0	$a_0+h_0+c_0$	1	0	0	1

とする．第 $i+1$ 行は，第 i 行で $a_i+h_i+c_i>0$ ならば

$a_i+h_i+c_i$	h_i+2c_i	c_i	$2a_i+3h_i+4c_i$	h_i+4c_i	$a_i+2h_i+4c_i$	p_i+q_i	q_i	r_i+s_i	s_i

とし，$a_i+h_i+c_i<0$ ならば

a_i	$2a_i+h_i$	$a_i+h_i+c_i$	$4a_i+h_i$	$4a_i+3h_i+2c_i$	$4a_i+2h_i+c_i$	p_i	p_i+q_i	r_i	r_i+s_i

とする.

i 行目から $i+1$ 行目のへの移行は，$SL_2(\mathbb{Z})$ の元 L または R による正式変換である.

$f_i=[\,|\,a_i,h_i,c_i\,|\,]$，$M_i=\begin{bmatrix} a_i & h_i/2 \\ h_i/2 & c_i \end{bmatrix}$，$X_i=\begin{bmatrix} p_i & q_i \\ r_i & s_i \end{bmatrix}$ とおくと，$X_0=E=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ であり,

(1) $a_i+h_i+c_i>0$ のとき，$X_{i+1}=X_iR$，$M_{i+1}=R^TM_iR$,

(2) $a_i+h_i+c_i<0$ のとき，$X_{i+1}=X_iL$，$M_{i+1}=L^TM_iL$

である．各 i について，$a_i>0$，$c_i<0$，$\det M_i=\det M_0=-d/4$，であるから，f_i は判別式が d の被約形式である．もし，$a_i+h_i+c_i=0$ となるなら，$d=(a_i-c_i)^2$ となり，d が非平方数であることに反する．ゆえに，表は無際限に延長することができる．この表を「被約形式鎖（Kette reducirter Formen）の表」とよぶ.

この表より，$i=0,1,2,\ldots$ のとき,

$$\begin{bmatrix} p_i & r_i \\ q_i & s_i \end{bmatrix}\begin{bmatrix} a_0 & h_0/2 \\ h_0/2 & c_0 \end{bmatrix}\begin{bmatrix} p_i & q_i \\ r_i & s_i \end{bmatrix}=\begin{bmatrix} a_i & h_i/2 \\ h_i/2 & c_i \end{bmatrix},\ d=h_i^2-4a_ic_i,\ a_i>0,\ c_i<0,\ p_is_i-q_ir_i=1$$

が成り立つ．特に，$a_i=a_0p_i^2+h_0p_ir_i+c_0r_i^2$，$c_i=a_0q_i^2+h_0q_is_i+c_0s_i^2$，である.

$a_i - h_i + c_i$ の符号により L^{-1} または R^{-1} で正式変換すれば，表は逆向きにも無際限に延長できる．

判別式が d の被約形式は有限個しかないので，被約形式鎖の表で f_i は必ず巡回する．コンウェイ [1] のトポグラフでは，巡回する $\{f_i\}$ を「周期的な川」（repeated river）とよぶ．

5　フルヴィッツによる被約形鎖の表

判別式 $d = 4 \cdot 35 = 140$ の被約形式 $[|\, 13, -2 \cdot 3, -2 \,|]$ の被約形式鎖の表（フルヴィッツ [3]，108 頁）．

1. Beispiel.

$f = 62x^2 - 2 \cdot 95xy + 145y^2 \equiv (62, -95, 145)$.

Man erhält die folgende Tabelle:

Erste Wurzel.

	$\frac{\xi_1}{\eta_1}$	$\frac{\xi_2}{\eta_2}$	f_1	f_{12}	f_2	f_{13}	f_{23}	f_3
π_0	$\frac{1}{0}$	$\frac{0}{1}$	62	− 95	145	− 33	50	17
π_1	$\frac{1}{0}$	$\frac{1}{1}$	62	− 33	17	29	− 16	13
π_2	$\frac{2}{1}$	$\frac{1}{1}$	13	− 16	17	− 3	1	− 2
$\pi_3^{(1)}$	$\frac{2}{1}$	$\frac{3}{2}$	13	− 3	− 2	10	− 5	5
$\pi_4^{(1)}$	$\frac{5}{3}$	$\frac{3}{2}$	5	− 5	− 2	0	− 7	− 7
$\pi_5^{(1)}$	$\frac{5}{3}$	$\frac{8}{5}$	5	0	− 7	5	− 7	− 2
$\pi_6^{(1)}$	$\frac{5}{3}$	$\frac{13}{8}$	5	5	− 2	10	3	13
$\pi_7^{(1)}$	$\frac{18}{11}$	$\frac{13}{8}$	13	3	− 2	16	1	17
$\pi_8^{(1)}$	$\frac{31}{19}$	$\frac{13}{8}$	17	1	− 2	18	− 1	17
$\pi_9^{(1)}$	$\frac{44}{27}$	$\frac{13}{8}$	17	− 1	− 2	16	− 3	13
$\pi_{10}^{(1)}$	$\frac{57}{35}$	$\frac{13}{8}$	13	− 3	− 2			

Zweite Wurzel.

	$\frac{\xi_1}{\eta_1}$	$\frac{\xi_2}{\eta_2}$	f_1	f_{12}	f_2	f_{13}	f_{23}	f_3
$\pi_3^{(2)}$	$\frac{3}{2}$	$\frac{1}{1}$	− 2	1	17	− 1	18	17
$\pi_4^{(2)}$	$\frac{3}{2}$	$\frac{4}{3}$	− 2	− 1	17	− 3	16	13
$\pi_5^{(2)}$	$\frac{3}{2}$	$\frac{7}{5}$	− 2	− 3	13	− 5	10	5
$\pi_6^{(2)}$	$\frac{3}{2}$	$\frac{10}{7}$	− 2	− 5	5	− 7	0	− 7
$\pi_7^{(2)}$	$\frac{13}{9}$	$\frac{10}{7}$	− 7	0	5	− 7	5	− 2
$\pi_8^{(2)}$	$\frac{23}{16}$	$\frac{10}{7}$	− 2	5	5	3	10	13
$\pi_9^{(2)}$	$\frac{23}{16}$	$\frac{33}{23}$	− 2	3	13	1	16	17
$\pi_{10}^{(2)}$	$\frac{23}{16}$	$\frac{56}{39}$	− 2	1	17			

Die zu der Form f gehörige Kette reducirter Formen entsteht aus der periodischen Wiederholung der Formen:
$(13, -3, -2)$, $(5, -5, -2)$, $(5, 0, -7)$, $(5, 5, -2)$, $(13, 3, -2)$, $(17, 1, -2)$, $(17, -1, -2)$.

対応は次の通り．$h/2 = b$ に注意する．

f_1	f_{12}	f_2	f_{13}	f_{23}	f_3	ξ_1	ξ_2	η_1	η_2
a	$h/2$	c	$a+h/2$	$h/2+c$	$a+h+c$	p	q	r	s

	a	b	c	a+b	b+c	a+2b+c	p	q	r	s
π_3	13	-3	-2	10	-5	5	2	3	1	2
π_4	5	-5	-2	0	-7	-7	5	3	3	2
π_5	5	0	-7	5	-7	-2	5	8	3	5
π_6	5	5	-2	10	3	13	5	13	3	8
π_7	13	3	-2	16	1	17	18	13	11	8
π_8	17	1	-2	18	-1	17	31	13	19	8
π_9	17	-1	-2	16	-3	13	44	13	27	8
π_10	13	-3	-2	10	-5	5	57	13	35	8

フルヴィッツの表にはガウスの意味の被約形式がすべて現れる．ガウスの意味の「被約形式の周期」(Periode)（ガウス [2]，186 条）は $\{\pi_8^{(2)} = (-2, 5, 5),\ \pi_6^{(1)} = (5, 5, -2)\}$ である．また，表には $[|\, 1\ , 0\ , -35\, |]$ や $[|\, 7\ , 0\ , -5\, |]$ が現れないことから判別式が $4 \cdot 35$ の正式同値類が 2 つ以上（実は 4 つ）あることもわかる．

6　被約形式鎖の表を用いたペル方程式の解法

D は正の非平方数とする．判別式が $4D$ の被約形式 $f_0 = [\,|\,1, 0, -D\,|\,]$ の被約形式鎖において，$f_0 = f_N$（$N > 0$）ならば，$a_{kN} = 1 = p_{kN}^2 - D \cdot r_{kN}^2$（$k = 1, 2, 3, \cdots$）となり，ペル方程式（1）の解が得られる．

例 6.1. 判別式が $4 \cdot 85 = 340$ の被約形式 $[\,|\,a_0, h_0, c_0\,|\,] = [\,|\,1, 0, -85\,|\,]$ の被約形式鎖の表は次の通り．

	a	h	c	2a+h	h+2c	a+h+c	p	q	r	s
0	1	0	-85	2	-170	-84	1	0	0	1
1	1	2	-84	4	-166	-81	1	1	0	1
2	1	4	-81	6	-158	-76	1	2	0	1
3	1	6	-76	8	-146	-69	1	3	0	1
4	1	8	-69	10	-130	-60	1	4	0	1
5	1	10	-60	12	-110	-49	1	5	0	1
6	1	12	-49	14	-86	-36	1	6	0	1
7	1	14	-36	16	-58	-21	1	7	0	1
8	1	16	-21	18	-26	-4	1	8	0	1
9	1	18	-4	20	10	15	1	9	0	1
10	15	10	-4	40	2	21	10	9	1	1
11	21	2	-4	44	-6	19	19	9	2	1
12	19	-6	-4	32	-14	9	28	9	3	1
13	9	-14	-4	4	-22	-9	37	9	4	1
14	9	4	-9	22	-14	4	37	46	4	5
15	4	-14	-9	-6	-32	-19	83	46	9	5
16	4	-6	-19	2	-44	-21	83	129	9	14
17	4	2	-21	10	-40	-15	83	212	9	23
18	4	10	-15	18	-20	-1	83	295	9	32
19	4	18	-1	26	16	21	83	378	9	41
20	21	16	-1	58	14	36	461	378	50	41
21	36	14	-1	86	12	49	839	378	91	41
22	49	12	-1	110	10	60	1217	378	132	41
23	60	10	-1	130	8	69	1595	378	173	41
24	69	8	-1	146	6	76	1973	378	214	41
25	76	6	-1	158	4	81	2351	378	255	41
26	81	4	-1	166	2	84	2729	378	296	41
27	84	2	-1	170	0	85	3107	378	337	41
28	85	0	-1	170	-2	84	3485	378	378	41
29	84	-2	-1	166	-4	81	3863	378	419	41
30	81	-4	-1	158	-6	76	4241	378	460	41
31	76	-6	-1	146	-8	69	4619	378	501	41
32	69	-8	-1	130	-10	60	4997	378	542	41
33	60	-10	-1	110	-12	49	5375	378	583	41
34	49	-12	-1	86	-14	36	5753	378	624	41
35	36	-14	-1	58	-16	21	6131	378	665	41
36	21	-16	-1	26	-18	4	6509	378	706	41
37	4	-18	-1	-10	-20	-15	6887	378	747	41
38	4	-10	-15	-2	-40	-21	6887	7265	747	788
39	4	-2	-21	6	-44	-19	6887	14152	747	1535
40	4	6	-19	14	-32	-9	6887	21039	747	2282
41	4	14	-9	22	-4	9	6887	27926	747	3029
42	9	-4	-9	14	-22	-4	34813	27926	3776	3029
43	9	14	-4	32	6	19	34813	62739	3776	6805
44	19	6	-4	44	-2	21	97552	62739	10581	6805
45	21	-2	-4	40	-10	15	160291	62739	17386	6805
46	15	-10	-4	20	-18	1	223030	62739	24191	6805
47	1	-18	-4	-16	-26	-21	285769	62739	30996	6805
48	1	-16	-21	-14	-58	-36	285769	348508	30996	37801
49	1	-14	-36	-12	-86	-49	285769	634277	30996	68797
50	1	-12	-49	-10	-110	-60	285769	920046	30996	99793
51	1	-10	-60	-8	-130	-69	285769	1205815	30996	130789
52	1	-8	-69	-6	-146	-76	285769	1491584	30996	161785
53	1	-6	-76	-4	-158	-81	285769	1777353	30996	192781
54	1	-4	-81	-2	-166	-84	285769	2063122	30996	223777
55	1	-2	-84	0	-170	-85	285769	2348891	30996	254773
56	1	0	-85	2	-170	-84	285769	2634660	30996	285769

この表では $p_i^2 - 85r_i^2 = a_i$，$q_i^2 - 85s_i^2 = c_i$ である．28 行目から，$378^2 - 85 \cdot 41^2 = -1$ が，56 行目から，$285769^2 - 85 \cdot 30996^2 = 1$ が得られる．被約形式鎖の表はチャクラヴァーラの表（例 2.1）に比べて作表に必要な計算量が多いが，副産物として，2 次形式，$x^2 - 85y^2$，のとる可能な整数値と，そのときの x，y の値がわかる．例えば，$x^2 - 85y^2 = 21$ の整数解（$19^2 - 85 \cdot 2^2 = 21$），$x^2 - 85y^2 = -21$ の整数解（$8^2 - 85 \cdot 1^2 = -21$）が得られる．また，14 行目からは $4^2 + 4 \cdot 9^2 = 4 \cdot 85$，すなわち判別式の平方数への分解 $2^2 + 9^2 = 85$ も得る．

例 6.2. 判別式が $4 \cdot 77 = 308$ の被約形式 $[\,|\, a_0, h_0, c_0 \,|\,] = [\,|\, 1, 0, -77 \,|\,]$ の被約形式鎖の表は次の通り．

	a	h	c	2a+h	h+2c	a+h+c	p	q	r	s
0	1	0	-77	2	-154	-76	1	0	0	1
1	1	2	-76	4	-150	-73	1	1	0	1
2	1	4	-73	6	-142	-68	1	2	0	1
3	1	6	-68	8	-130	-61	1	3	0	1
4	1	8	-61	10	-114	-52	1	4	0	1
5	1	10	-52	12	-94	-41	1	5	0	1
6	1	12	-41	14	-70	-28	1	6	0	1
7	1	14	-28	16	-42	-13	1	7	0	1
8	1	16	-13	18	-10	4	1	8	0	1
9	4	-10	-13	-2	-36	-19	9	8	1	1
10	4	-2	-19	6	-40	-17	9	17	1	2
11	4	6	-17	14	-28	-7	9	26	1	3
12	4	14	-7	22	0	11	9	35	1	4
13	11	0	-7	22	-14	4	44	35	5	4
14	4	-14	-7	-6	-28	-17	79	35	9	4
15	4	-6	-17	2	-40	-19	79	114	9	13
16	4	2	-19	10	-36	-13	79	193	9	22
17	4	10	-13	18	-16	1	79	272	9	31
18	1	-16	-13	-14	-42	-28	351	272	40	31
19	1	-14	-28	-12	-70	-41	351	623	40	71
20	1	-12	-41	-10	-94	-52	351	974	40	111
21	1	-10	-52	-8	-114	-61	351	1325	40	151
22	1	-8	-61	-6	-130	-68	351	1676	40	191
23	1	-6	-68	-4	-142	-73	351	2027	40	231
24	1	-4	-73	-2	-150	-76	351	2378	40	271
25	1	-2	-76	0	-154	-77	351	2729	40	311
26	1	0	-77	2	-154	-76	351	3080	40	351

この表の 26 行目から，$351^2 - 77 \cdot 40^2 = 1$，が得られる．また，$9^2 - 77 \cdot 1^2 = 4$ と $35^2 - 77 \cdot 4^2 = -7$ も得られるが，これは例 2.2 のチャクラヴァーラの表からも得られる．しかし，$x^2 - 77y^2$ の取る整数値のうちで，1 の次に大きいのが 4 であること，負の整数では絶対値最小のものが -7 であること，をチャクラヴァーラの表から読み取るのは難しい．

7　被約形式鎖の回文構造とアンビグ形式

被約形式鎖に含まれる 2 次形式は互いに正式同値であるが，逆も成り立つ（フルヴィッツ [3]，Satz 20）．

定理 7.1. 判別式が正の非平方数の被約形式であって，互いに正式同値なものは同一の被約形式鎖に含まれる．

証明. トポグラフは連結で閉路のない樹状グラフであり，$f=[\,|\,a,h,c\,|\,]$ のトポグラフは f と正式同値な 2 次形式をすべて含む．f が被約形式なら，f は正の値の面と負の値の面に挟まれた「周期的な川」，すなわち被約形式鎖，の上にある．周期的な川は 1 本しかない（[1]，p.20）から，被約形式 g が被約形式 f と正式同値であれば，g は f の被約形式鎖に含まれる． □

注意 7.1. 判別式が正の非平方数の被約形式 $f=[\,|\,a\,,h\,,c\,|\,]$ が，自分自身と非正式同値であって $h\neq 0$ のときは，f の被約形式鎖の表に $[\,|\,a\,,-h\,,c\,|\,]$ が含まれる．

被約形式鎖にも「回文性」がある．$[\,|\,a_0\,,h_0\,,c_0\,|\,]=[\,|\,a_n\,,h_n\,,c_n\,|\,]$ をみたす最小の自然数を N とする．

定理 7.2. ある m $(1\leqq m\leqq N)$ に対して，$a_m=a_0$，$h_m=-h_0$，$c_m=c_0$，が成り立つならば，
各 i $(1\leqq i\leqq m)$ に対して，$a_i=a_{m-i}$，$h_i=-h_{m-i}$，$c_i=c_{m-i}$，が成り立つ．

証明. $a_i=a_{m-i}$，$h_i=-h_{m-i}$，$c_i=c_{m-i}$，を仮定する．$a_i+h_i+c_i>0$ の場合は，$a_{i+1}=a_i+h_i+c_i$，$h_{i+1}=h_i+2c_i$，$c_{i+1}=c_i$，であるから，$a_{m-i}-h_{m-i}+c_{m-i}=a_i+h_i+c_i>0$，である．したがって，$a_{m-i-1}=a_{m-i}-h_{m-i}+c_{m-i}=a_i+h_i+c_i=a_{i+1}$，$c_{m-i-1}=c_{m-i}=c_i=c_{i+1}$，$h_{m-i-1}=h_{m-i}-2c_{m-i}=-h_i-2c_i=-h_{i+1}$，となる．$a_i+h_i+c_i<0$ の場合も，同様の計算で，$a_{m-i-1}=a_{i+1}$，$h_{m-i-1}=-h_{i+1}$，$c_{m-i-1}=c_{i+1}$，が示される． □

定理 7.3. ある m' $(1\leqq m'\leqq N)$ に対して，$a_{m'}=-c_0$，$h_{m'}=h_0$，$c_{m'}=-a_0$，が成り立つならば，
各 i $(1\leqq i\leqq m')$ に対して，$a_{m'-i}=-c_i$，$h_{m'-i}=h_i$，$c_{m'-i}=-a_i$，が成り立つ．

証明. $a_{m'-i}=-c_i$，$h_{m'-i}=h_i$，$c_{m'-i}=-a_i$，を仮定する．$a_i+h_i+c_i>0$ の場合は，$a_{i+1}=a_i+h_i+c_i$，$h_{i+1}=h_i+2c_i$，$c_{i+1}=c_i$，であるから，$a_{m'-i}-h_{m'-i}+c_{m'-i}=-c_i-h_i-a_i<0$，である．したがって，$a_{m'-i-1}=a_{m'-i}=-c_i=-c_{i+1}$，$h_{m'-i-1}=-2a_{m'-i}+h_{m'-i}=2c_i+h_i=h_{i+1}$，$c_{m'-i-1}=a_{m'-i}-h_{m'-i}+c_{m'-i}=-c_i-h_i-a_i=-a_{i+1}$，となる．$a_i+h_i+c_i<0$ の場合も，同様の計算で，$a_{m'-i-1}=-c_{i+1}$，$h_{m'-i-1}=h_{i+1}$，$c_{m'-i-1}=-a_{i+1}$，が示される． □

下記の定義では判別式 d は一般でよい．

定義 7.1. $[\,|\,a,h,c\,|\,]$ は，h が a で割り切れるとき，「アンビグ形式」とよぶ．

$h=ka$ とすると，

$$\begin{bmatrix}1&-k\\0&1\end{bmatrix}^T\begin{bmatrix}a&ka/2\\ka/2&c\end{bmatrix}\begin{bmatrix}1&-k\\0&1\end{bmatrix}=\begin{bmatrix}a&-ka/2\\-ka/2&c\end{bmatrix}$$

であるから，アンビグ形式 $[\,|\,a,ka,c\,|\,]$ は自分自身と非正式同値な $[\,|\,a,-ka,c\,|\,]$ と正式同値である．

定義 7.2. 自分自身と非正式同値である 2 次形式を含む正式同値類をアンビグ類とよぶ．

アンビグ類はアンビグ形式を含む ([2]，165 条)．すなわち，

定理 7.4. 自分自身と非正式同値な 2 次形式は，あるアンビグ形式と正式同値である．

定理 7.4 は判別式 d が一般で成り立つが，d が正の非平方数の場合に被約形式鎖を用いて証明する．

証明. 判別式が正の非平方数の 2 次形式 F は定理 3.1 により，ある被約形式 $f=[\,|\,a\,,h\,,c\,|\,]$ と正式同値になり，F が自分自身と非正式同値ならば，f も自分自身と非正式同値である．$h=0$ の場合は f 自身がアンビグ形式であるから，$h\neq 0$ としてよい．注意 7.1 により，f を含む被約形式鎖の表に $[\,|\,a\,,-h\,,c\,|\,]$ が現れる．$f=[\,|\,a_0\,,h_0\,,c_0\,|\,]$ とおき，$[\,|\,a_0\,,-h_0\,,c_0\,|\,]=[\,|\,a_m\,,h_m\,,c_m\,|\,]$ とする．m は $0<m<N$ としてよい．
(1) $m=2M$（偶数）の場合．定理 7.2 より，$h_M=-h_{m-M}=-h_M$ となるから，$h_M=0$ となる．$[\,|\,a_M,0,c_M\,|\,]$ はアンビグ形式である．
(2) $m=2L+1$（奇数）の場合．定理 7.2 より $h_{L+1}=-h_L$ となる．$a_L+h_L+c_L>0$ のときは，$h_{L+1}=2c_L+h_L$ であるから，$h_L=-c_L$ となり，$[\,|\,a_L,-c_L,c_L\,|\,]$ はアンビグ形式 $[\,|\,c_L,c_L,a_L\,|\,]$ と正式同値である．$a_L+h_L+c_L<0$ のときは，$h_{L+1}=2a_L+h_L$ であるから，$h_L=-a_L$ となり，$[\,|\,a_L,-a_L,c_L\,|\,]$ はアンビグ形式である． □

例 7.1.（注意 2.1 参照）アンビグ形式の例として，$f_0=[\,|\,1\,,0\,,-p\,|\,]$（$p$ は奇素数）を考察する．f_0 の被約形式鎖において，$f_0=f_n$ となる最小の自然数 n を N とする．
(1) $N=2M$（偶数）の場合．定理 7.2 より，$h_M=-h_{N-M}=-h_M$ となり，$h_M=0$ となる．このとき，$-a_Mc_M=p$ であるが，N の最小性により，$a_M=p$，$c_M=-1$ でなければならない．この場合は，$x^2-py^2=-1$ に整数解が存在する．
(2) $N=2L+1$（奇数）の場合．定理 7.2 より，$h_L=-h_{N-L}=-h_{L+1}$ となる．一方，$h_{L+1}=2a_L+h_L$，または $h_{L+1}=h_L+2c_L$ であるから，$h_L=-a_L$，または $h_L=-c_L$ となり，$4p=h_L^2-4h_La_L$，または $4p=h_L^2-4h_Lc_L$ である．$[\,|\,a_L\,,h_L\,,c_L\,|\,]$ の可能な場合は $[\,|\,2\,,-2,\,,(1-p)/2\,|\,]$，または $[\,|\,(p-1)/2\,,2,\,,-2\,|\,]$ である．ここで，$(p-1)/2$ が偶数ならば，a_L，h_L，c_L の最大公約数が 2 で割り切れるから注意 3.1 に矛盾．したがって，この場合は，$p\equiv -1 \mod 4$ でなければならない． $\mod 4$ で $x^2-py^2\equiv x^2+y^2$ は -1 を表せないから，$[\,|\,1\,,0\,,-p\,|\,]$ の被約形式鎖の表は，$[\,|\,p\,,0\,,-1\,|\,]$ を含まない．$[\,|\,2\,,-2\,,(1-p)/2\,|\,]$ を含む場合は，$x^2-py^2=2$ の整数解が存在し，$[\,|\,(p-1)/2\,,2\,,-2\,|\,]$ を含む場合は，$x^2-py^2=-2$ の整数解が存在する．

8 アンビグ形式と鏡映変換

判別式 d は一般とする．f をアンビグ形式 $[\,|\,a,ak,c\,|\,]$ とすると，

$$\begin{bmatrix}1 & k\\ 0 & -1\end{bmatrix}^T\begin{bmatrix}a & ak/2\\ ak/2 & c\end{bmatrix}\begin{bmatrix}1 & k\\ 0 & -1\end{bmatrix}=\begin{bmatrix}a & ak/2\\ ak/2 & c\end{bmatrix},\ \det\begin{bmatrix}1 & k\\ 0 & -1\end{bmatrix}=-1,\ \begin{bmatrix}1 & k\\ 0 & -1\end{bmatrix}^2=E=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

をみたすから，$X=\begin{bmatrix}1 & k\\ 0 & -1\end{bmatrix}$ は f の非正式な自己同型であって，位数が 2 である．

定義 8.1. 2 次形式 $f=[\,|\,a,h,c\,|\,]$ の自己同型 Y が，$\det Y=-1$，$Y^2=E$ をみたすとき，「鏡映変換」とよぶ．

定理 8.1. $f=[\,|\,a,h,c\,|\,]$ の判別式 d が非平方数の場合は，f の非正式自己同型は鏡映変換になる．すなわち，

$M = \begin{bmatrix} a & h/2 \\ h/2 & c \end{bmatrix}$, $Y = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ が，$Y^T M Y = M$，$\det Y = -1$ をみたせば，$Y^2 = E$ が成り立つ．

証明.

$$Y^T M = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \begin{bmatrix} a & h/2 \\ h/2 & c \end{bmatrix} = \begin{bmatrix} \alpha a + \gamma h/2 & \alpha h/2 + \gamma c \\ \beta a + \delta h/2 & \beta h/2 + \delta c \end{bmatrix}$$

と

$$MY^{-1} = \begin{bmatrix} a & h/2 \\ h/2 & c \end{bmatrix} \begin{bmatrix} -\delta & \beta \\ \gamma & -\alpha \end{bmatrix} = \begin{bmatrix} -a\delta + \gamma h/2 & a\beta - \alpha h/2 \\ -\delta h/2 + c\gamma & \beta h/2 - c\alpha \end{bmatrix}$$

を比較して，$ac \neq 0$ であることに注意すると，$\alpha + \delta = 0$ であることがわかり，$Y^2 = E$ がわかる． □

注意 8.1. $f = [\,|\, a, h, c \,|\,]$ は判別式が正の非平方数の被約形式であって，自分自身と非正式同値であるとする．このとき，f の鏡映変換 P_1 と P_2 であって，$Q = P_2 P_1$ が無限位数であるものが存在する．第 4 節の記号を用いる．$f = f_0 = [\,|\, a_0, h_0, c_0 \,|\,]$ とし，$N > 0$ を $f_0 = f_N$ となる最小の自然数とする．$E' = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ とする．

(1) $h_0 = 0$ の場合．${E'}^T M_0 E' = M_0$ であるから，$Y = X_N E'$ は $Y^T M_0 Y = M_0$，$\det Y = -1$ をみたし，f_0 の鏡映変換である．${X_{2N}}^T M_0 X_{2N} = M_0$ であるから，$Z = X_{2N} E'$ も $Z^T M_0 Z = M_0$，$\det Z = -1$ をみたし，f_0 の鏡映変換である．一方，$X_N X_k = X_{N+k}$ が成り立ち，特に $X_{2N} = {X_N}^2$ が成り立つから，$Z = X_N Y$ となり，$Y^2 = E$ より，$ZY = X_N$ となり，$P_2 = Z$，$P_1 = Y$，$Q = X_N$ が条件をみたす．

(2) $h_0 \neq 0$ の場合．ある $m\,(0 < m < N)$ について，$f_m = [\,|\, a_0, -h_0, c_0 \,|\,]$ である．したがって，${X_m}^T M_0 X_m = M_m = {E'}^T M_0 E'$ より，$Y = X_m E'$ は，$Y^T M_0 Y = M_0$，$\det Y = -1$ をみたし，f_0 の鏡映変換である．$f_{N+m} = [\,|\, a_0, -h_0, c_0 \,|\,]$ であるから，$Z = X_{N+m} E'$ も，$Z^T M_0 Z = M_0$，$\det Z = -1$，をみたし，f_0 の鏡映変換である．$X_{N+m} = X_N X_m$ であるから，$Z = X_N Y$ となり，$Y^2 = E$ より，$ZY = X_N$ となり，$P_2 = Z$，$P_1 = Y$，$Q = X_N$ が条件をみたす．

例 8.1. 判別式が 77 の $[\,|\, 1, 7, -7 \,|\,]$ の被約形式鎖の表は次の通り．

	a	h	c	2a+h	h+2c	a+h+c	p	q	r	s
0	1	7	-7	9	-7	1	1	0	0	1
1	1	-7	-7	-5	-21	-13	1	0	1	1
2	1	-5	-13	-3	-31	-17	1	1	1	2
3	1	-3	-17	-1	-37	-19	1	2	1	3
4	1	-1	-19	1	-39	-19	1	3	1	4
5	1	1	-19	3	-37	-17	1	4	1	5
6	1	3	-17	5	-31	-13	1	5	1	6
7	1	5	-13	7	-21	-7	1	6	1	7
8	1	7	-7	9	-7	1	1	7	1	8
9	1	-7	-7	-5	-21	-13	8	7	9	8
10	1	-5	-13	-3	-31	-17	8	15	9	17

$N = 8$ である．$M_0 = \begin{bmatrix} 1 & 7/2 \\ 7/2 & -7 \end{bmatrix}$ とし，$Q = \begin{bmatrix} p_8 & q_8 \\ r_8 & s_8 \end{bmatrix} = \begin{bmatrix} 1 & 7 \\ 1 & 8 \end{bmatrix}$ とおくと，$Q^T M_0 Q = M_0$ であり，$\{Q^n \,;\, n \in \mathbb{Z}\} \cong \mathbb{Z}$ である．

$$P_1=\begin{bmatrix}p_2 & q_2\\ r_2 & s_2\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 1 & -1\end{bmatrix},\ P_2=\begin{bmatrix}p_9 & q_9\\ r_9 & s_9\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=\begin{bmatrix}8 & -7\\ 9 & -8\end{bmatrix}\ \text{とおくと},$$

$$P_1{}^T M_0 P_1=M_0,\quad P_2{}^T M_0 P_2=M_0,\quad \det P_1=-1,\quad \det P_2=-1$$

であるから，P_1 と P_2 は $f_0=[\,|\,1,7,-7\,|\,]$ の鏡映変換であり，$Q=P_2P_1$ をみたす．

9　合成による自己同型

定理 9.1. $f=[\,|\,a\ ,h\ ,c\,|\,]$ は判別式 d が正の非平方数の「原始形式」とする．

(1) $d\equiv 1 \mod 4$ のとき，

$$P=\begin{bmatrix}\dfrac{t-hu}{2} & -cu\\ au & \dfrac{t+hu}{2}\end{bmatrix},\ t^2-du^2=4$$

は f の正式自己同型になる．

(2) $d\equiv 0 \mod 4$ のとき，

$$P=\begin{bmatrix}t-\dfrac{h}{2}u & -cu\\ au & t+\dfrac{h}{2}u\end{bmatrix},\ t^2-\frac{d}{4}u^2=1$$

は f の正式自己同型になる．

証明. (1) $d\equiv 1 \mod 4$ の場合.

$2f$ の判別式は $4d$ で，$2a$, $2h$, $2c$, 1, $-d$ の最大公約数は 1 であるから，$2f=[\,|\,2a\ ,2h\ ,2c\,|\,]$ と $[\,|\,1\ ,0\ ,-d\,|\,]$ を合成することができる．変数変換 $X=xx'-hxy'-2cyy'$，$Y=2axy'+yx'+hyy'$ により，

$$2aX^2+2hXY+2cY^2=(2ax^2+2hxy+2cy^2)(x'^2-dy^2)$$

が成り立つ．変数変換を行列で表し，

$$\begin{bmatrix}X\\ Y\end{bmatrix}=\begin{bmatrix}x'-hy' & -2cy'\\ 2ay' & x'+hy'\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}$$

の係数行列を P とする．P が整数行列となるためには，f が原始形式であるから，$2x'\in\mathbb{Z}$，$2y'\in\mathbb{Z}$，$x'-y'\in 2\mathbb{Z}$ であればよいことがわかる．そこで $x'=t/2$，$y'=u/2$（$t\equiv u \mod 2$）とおくと，$\det P=x'^2-dy'^2=\dfrac{t^2-du^2}{4}$ となり，$\det P=1$ となるためには $t^2-du^2=4$ であればよい．このとき，変数変換

$$\begin{bmatrix}X\\ Y\end{bmatrix}=\begin{bmatrix}\dfrac{t-hu}{2} & -cu\\ au & \dfrac{t+hu}{2}\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}$$

により $aX^2+hXY+cY^2=ax^2+hxy+cy^2$ となり，P は f の正式自己同型になる．

(1) $d\equiv 0 \mod 4$ の場合.

$d=4d'$ とおく．h は偶数である．$[\,|\,1\ ,0\ ,-d'\,|\,]$ の判別式は d であるから $f=[\,|\,a\ ,h\ ,c\,|\,]$ と合成できる．変数変換 $X=xx'-\dfrac{h}{2}xy'-cyy'$，$Y=axy'+yx'+\dfrac{h}{2}yy'$ により，

$$aX^2+hXY+cY^2=(ax^2+hxy+cy^2)(x'^2-d'y'^2)$$

が成り立つ．変数変換を行列で表し，

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} x' - \dfrac{h}{2}y' & -cy' \\ ay' & x' + \dfrac{h}{2}y' \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

の係数行列を P とする．P が整数行列であるためには，f が原始形式であるから，$x', y' \in \mathbb{Z}$ であればよい．また，$\det P = 1$ であるためには，整数 x', y' が $x'^2 - d'y'^2 = 1$ をみたせばよい． □

例 9.1. $f = [\,|\,1, 7, -7\,|\,]$ の判別式 $77 \equiv 1 \mod 4$ である．$t^2 - 77u^2 = 4$ の整数解として，$t=9$，$u=1$ を取ると，$\begin{bmatrix} \dfrac{t-hu}{2} & -cu \\ au & \dfrac{t+hu}{2} \end{bmatrix} = \begin{bmatrix} 1 & 7 \\ 1 & 8 \end{bmatrix}$ は f の自己同型になる．一方，例 8.1 の表からも $\begin{bmatrix} p_8 & q_8 \\ r_8 & s_8 \end{bmatrix} = \begin{bmatrix} 1 & 7 \\ 1 & 8 \end{bmatrix}$ が f を f に移すことがわかる．

例 9.2. $f = [\,|\,3, -6, -2\,|\,]$ の判別式は $60 \equiv 0 \mod 4$ である．$[\,|\,1, 0, -15\,|\,]$ の被約形式鎖の表

	a	h	c	2a+h	h+2c	a+h+c	p	q	r	s
0	1	0	-15	2	-30	-14	1	0	0	1
1	1	2	-14	4	-26	-11	1	1	0	1
2	1	4	-11	6	-18	-6	1	2	0	1
3	1	6	-6	8	-6	1	1	3	0	1
4	1	-6	-6	-4	-18	-11	4	3	1	1
5	1	-4	-11	-2	-26	-14	4	7	1	2
6	1	-2	-14	0	-30	-15	4	11	1	3
7	1	0	-15	2	-30	-14	4	15	1	4

から，$t^2 - 15u^2 = 1$ の整数解，$t=4$，$u=1$ を得，f の自己同型 $\begin{bmatrix} t - \dfrac{h}{2}u & -cu \\ au & t + \dfrac{h}{2}u \end{bmatrix} = \begin{bmatrix} 7 & 2 \\ 3 & 1 \end{bmatrix}$ を得る．

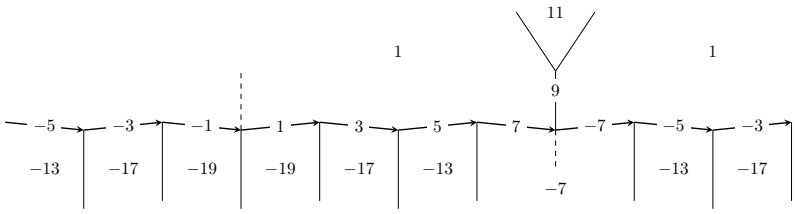
一方，$[\,|\,3, -6, -2\,|\,] = f_0$ の被約形式鎖の表

	a	h	c	2a+h	h+2c	a+h+c	p	q	r	s
0	3	-6	-2	0	-10	-5	1	0	0	1
1	3	0	-5	6	-10	-2	1	1	0	1
2	3	6	-2	12	2	7	1	2	0	1
3	7	2	-2	16	-2	7	3	2	1	1
4	7	-2	-2	12	-6	3	5	2	2	1
5	3	-6	-2	0	-10	-5	7	2	3	1
6	3	0	-5	6	-10	-2	7	9	3	4
7	3	6	-2	12	2	7	7	16	3	7
8	7	2	-2	16	-2	7	23	16	10	7
9	7	-2	-2	12	-6	3	39	16	17	7
10	3	-6	-2	0	-10	-5	55	16	24	7

から $f_5 = f_0$ であり，$\begin{bmatrix} p_5 & q_5 \\ r_5 & s_5 \end{bmatrix} = \begin{bmatrix} 7 & 2 \\ 3 & 1 \end{bmatrix}$ が f_0 の自己同型であることがわかる．

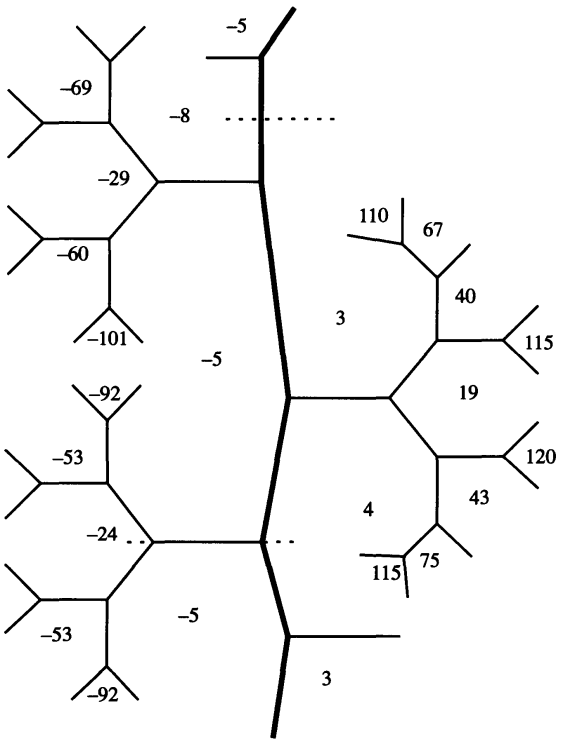
10　目で見る鏡映変換

$[|\,1,7,-7\,|]$ のトポグラフは次のようになり，2 つの鏡映変換（破線が対称軸）が読み取れる．



下図は $[|\,3,6,-5\,|]$ のトポグラフ（コンウェイ [1] の 22 頁）．

22 **THE SENSUAL (quadratic) FORM**



$$3, 4, 19, 40, 43, 67, 75, 110, 115, 120, \ldots$$

nestle between the branches of essentially just one shape of tree (and its mirror image). If we multiply these numbers by squares, we obtain all the values of the form. We see in particular that the Diophantine equations

$$3x^2 + 6xy - 5y^2 = 7 \quad \text{and} \quad 3x^2 + 6xy - 5y^2 = -100$$

are insoluble in integers.

We can also see in this figure the isometry group of f (which by definition consists of those linear transformations that preserve f).

11　正式同値と広義同値について

d は一般の整数とし，判別式が d の $f=[\,a,h,c\,]$ と $f'=[\,-c,-h,-a\,]$ の関係を考察する．

判別式を $4d$ にそろえて，$2f=[\,2a,2h,2c\,]$ と $[\,d,0,-1\,]$ を合成する．変数変換 $X=2axx'+hyx'+yy'$，$Y=-hxx'+xy'-2cyx'$ により，

$$-2cX^2-2hXY-2aY^2=(2ax^2+2hxy+2cy^2)(dx'^2-y'^2)$$

となる．したがって，$dx'^2-y'^2=1$ をみたす整数 x'，y' が存在すれば，正式変換

$$\begin{bmatrix}X\\Y\end{bmatrix}=\begin{bmatrix}2ax' & hx'+y'\\ -hx'+y' & -2cx'\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} \tag{6}$$

により $-2cX^2-2hXY-2aY^2=2ax^2+2hxy+2cy^2$，すなわち，$-cX^2-hXY-aY^2=ax^2+hxy+cy^2$ となり，$f'=[\,-c,-h,-a\,]$ は，$f=[\,a,h,c\,]$ と「正式同値」になる．

一方，d が一般であっても $dx'^2-y'^2=-1$ をみたす整数 x'，y' は常に存在し，変数変換（6）は非正式変換となり，$f'=[\,-c,-h,-a\,]$ は，$-f=[\,-a,-h,-c\,]$ と「非正式同値」になる．したがって，「g は $-f$ と非正式同値である」ことと「g は f' と正式同値である」ことは同値である．そこで，

定義 11.1. g が $f=[\,a,h,c\,]$ または $f'=[\,-c,-h,-a\,]$ と正式同値であるとき，g は f と「広義同値」であるという．

$f=[\,a,h,c\,]$ の広義同値類は f の正式同値類と $f'=[\,-c,-h,-a\,]$ の正式同値類の和集合である．f' が f と正式同値であれば f の広義同値類は f の正式同値類のみであり，f' が f と正式同値でなければ f の広義同値類は f の正式同値類と f' の正式同値類の直和になる．

注意 11.1. ガウス [2] は 2 次形式の正式同値と非正式同値を考察しているが，広義同値は扱っていない．

定義 11.2. n が，整数 ξ，η により $n=a\xi^2+h\xi\eta+c\eta^2$ と表せるとき，$[\,a,h,c\,]$ は n を表す，という．

$[\,a,h,c\,]$ は a と c を表す．$[\,a,h,c\,]$ と $[\,a',h',c'\,]$ が正式同値または非正式同値であるとき，$[\,a,h,c\,]$ が n を表すことと，$[\,a',h',c'\,]$ が n を表すことは同値である．

定義 11.3. d は一般の整数とする．
(1)　$d\equiv 1 \mod 4$ のとき，$[\,1,1,\dfrac{1-d}{4}\,]=x^2+xy+\dfrac{1-d}{4}y^2$
(2)　$d\equiv 0 \mod 4$ のとき，$[\,1,0,-\dfrac{d}{4}\,]=x^2-\dfrac{d}{4}y^2$
を d に付随する主形式（Hauptform）とよび，主形式を含む正式同値類を主類（Hauptklasse）とよぶ．

d に付随する主形式の判別式は d である．主形式は 1 を表す．逆に，

定理 11.1. 判別式が d の 2 次形式 f が 1 を表すならば，f は d に付随する主形式と正式同値である．

証明. $f=[\,a,h,c\,]$ とし，整数 α，γ が $a\alpha^2+h\alpha\gamma+c\gamma^2=1$ をみたすとする．

(1) $d \equiv 1 \mod 4$ のとき．h は奇数であり，$\beta = \dfrac{1-h}{2}\alpha - c\gamma$，$\delta = \dfrac{1+h}{2}\gamma + a\alpha$ とおくと，$\alpha\delta - \beta\gamma = 1$ である．$X = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL_2(\mathbb{Z})$ とおくと，$X^T \begin{bmatrix} a & \frac{h}{2} \\ \frac{h}{2} & c \end{bmatrix} X = \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1-d}{4} \end{bmatrix}$ である．

(2) $d \equiv 0 \mod 4$ のとき．h は偶数であり，$\beta = -\dfrac{h}{2}\alpha - c\gamma$，$\delta = \dfrac{h}{2}\gamma + a\alpha$ とおくと，$\alpha\delta - \beta\gamma = 1$ である．$X = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL_2(\mathbb{Z})$ とおくと，$X^T \begin{bmatrix} a & \frac{h}{2} \\ \frac{h}{2} & c \end{bmatrix} X = \begin{bmatrix} 1 & 0 \\ 0 & -\frac{d}{4} \end{bmatrix}$ である． □

定理 11.2. 主類は合成に関する単位元である．

証明. $[\,|\, a, h, c \,|\,]$ の判別式が d とする．

(1) $d \equiv 1 \mod 4$ のとき．h は奇数であり，変数変換 $X = xx' + \dfrac{-h+1}{2}xy' - cyy'$, $Y = axy' + yx' + \dfrac{h+1}{2}yy'$ により，$aX^2 + hXY + cY^2 = (ax^2 + hxy + cy^2)(x'^2 + x'y' + \dfrac{1-d}{4}y'^2)$ となる．

(2) $d \equiv 0 \mod 4$ のとき．h は偶数であり，変数変換 $X = xx' - \dfrac{h}{2}xy' - cyy'$，$Y = axy' + yx' + \dfrac{h}{2}yy'$ により，$aX^2 + hXY + cY^2 = (ax^2 + hxy + cy^2)(x'^2 - \dfrac{d}{4}y'^2)$ となる． □

定理 11.3. $[\,|\, a, h, c \,|\,]$ と $[\,|\, a, -h, c \,|\,]$ の合成は主形式と正式同値である．

証明. 変数変換 $X = axx' + hyx' - cyy'$, $Y = xy' + yx'$ により，$X^2 - hXY + acY^2 = (ax^2 + hxy + cy^2)(ax'^2 - hx'y' + cy'^2)$ となり，左辺の $[\,|\, 1, -h, ac \,|\,]$ は 1 を表すから定理 11.1 により主形式と正式同値である． □

注意 11.2. 定理 11.3 より，A がアンビグ類なら A と A の合成は主類である．アンビグ類でない正式同値類 B は，B と非正式同値な B^{-1} と対で現れるから，アンビグ類でない正式同値類は存在すれば偶数個である．

定理 11.4. d は一般の整数とする．判別式 d の 2 次形式 $f = [\,|\, a, h, c \,|\,]$ が，$f' = [\,|\, -c, -h, -a \,|\,]$ と正式同値になるための必要十分条件は，d に付随する主形式が -1 を表すこと，である．

証明. (1) $d \equiv 1 \mod 4$ のとき．

判別式が d の $f = [\,|\, a, h, c \,|\,]$ と $[\,|\, \dfrac{d-1}{4}, -1, -1 \,|\,]$ を合成する．変数変換 $X = axx' + \dfrac{1+h}{2}yx' + yy'$, $Y = \dfrac{1-h}{2}xx' + xy' - cyx'$ により，$-cX^2 - hY^2 - aY^2 = (ax^2 + hxy + cy^2)(\dfrac{d-1}{4}x'^2 - x'y' - y'^2)$ となる．したがって，$\dfrac{d-1}{4}\xi^2 - \xi\eta - \eta^2 = 1$ をみたす整数 ξ，η が存在するならば，正式変換

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} a\xi & \frac{1+h}{2}\xi + \eta \\ \frac{1-h}{2}\xi + \eta & -c\xi \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

により，$[\,|\, -c, -h, -a \,|\,]$ は $[\,|\, a, h, c \,|\,]$ と正式同値になる．

逆を示す．$[\,|\, a, h, c \,|\,]$ と $[\,|\, -c, -h, -a \,|\,]$ が正式同値の場合，$[\,|\, -c, -h, -a \,|\,]$ と $[\,|\, a, -h, c \,|\,]$ の合成は主形式に正式同値になる．変数変換，$X = cxy' - ayx' + hyy'$，$Y = xy' + yx'$ により，$-X^2 + hXY - acY^2 = (-cx^2 - hxy - ay^2)(ax'^2 - hx'y' + cy'^2)$ となり，主形式に正式同値である左辺 $[\,|\, -1, h, -ac \,|\,]$ が -1 を表

すことがわかる．したがって，この場合，主形式が -1 を表す．

(2) $d \equiv 0 \mod 4$ のとき．$f = [\,|\, a, h, c \,|\,]$ と $[\,|\, \frac{d}{4}, 0, -1 \,|\,]$ を合成する．変数変換 $X = axx' + \frac{h}{2}yx' + yy'$，$Y = -\frac{h}{2}xx' + xy' - cyx'$ により，$-cX^2 - hXY - aY^2 = (ax^2 + hxy + cy^2)(\frac{d}{4}x'^2 - y'^2)$ となる．$\frac{d}{4}\xi^2 - \eta^2 = 1$ をみたす整数 ξ，η が存在するならば，正式変換

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} a\xi & \frac{h}{2}\xi + \eta \\ -\frac{h}{2}\xi + \eta' & -c\xi \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

により，$[\,|\, -c, -h, -a \,|\,]$ は $[\,|\, a, h, c \,|\,]$ と正式同値になる．

逆は (1) の場合と同じである． □

注意 11.3. $d \leqq 0$ のときは，主形式が -1 を表すことができないから，f の広義同値類は f の正式同値類と f' の正式同値類の直和になる．

注意 11.4. $d \equiv 1 \mod 4$ の場合，判別式が d の 2 次形式 $[\,|\, a, h, c \,|\,]$ のうちで，原始形式に限ると，

$[\,|\, a, h, c \,|\,]$ と $[\,|\, -c, -h, -a \,|\,]$ が正式同値である．$\iff$ $x^2 - dy^2 = -4$ が整数解をもつ．

が示される．($\Longrightarrow$ の証明) $[\,|\, 2a, 2h, 2c \,|\,]$ は $[\,|\, -2c, -2h, -2a \,|\,]$ と正式同値になり，判別式が $4d$ の主形式は $[\,|\, 1, 0, -d \,|\,]$ である．主形式が -1 を表せば -4 も表す．($\Longleftarrow$ の証明) 変数変換

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 2ax' & hx' + y' \\ -hx' + y' & -2cx' \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

により

$$-2cX^2 - 2hXY - 2aY^2 = (2ax^2 + 2hxy + 2cy^2)(dx'^2 - y'^2)$$

が成り立つ．行列 $X = \begin{bmatrix} 2ax' & hx' + y' \\ -hx' + y' & -2cx' \end{bmatrix}$ が整数行列であるためには，h が奇数であることと，$\{a, h, c\}$ の最大公約数が 1 であることから，$2x' \in \mathbb{Z}$，$2y' \in \mathbb{Z}$，$x' - y' \in 2\mathbb{Z}$ であればよいことがわかる．したがって，$y' = \frac{t}{2}$，$x' = \frac{u}{2}$ とおくと，$\det X = 1$ であるためには，t と u が $t^2 - du^2 = -4$ の整数解であればよい．このとき，正式変換 $\begin{bmatrix} au & \frac{hu + t}{2} \\ \frac{-hu + t}{2} & -cu \end{bmatrix}$ により，$[\,|\, a, h, c \,|\,]$ と $[\,|\, -c, -h, -a \,|\,]$ は正式同値になる．

例 11.1. $[\,|\, a, h, c \,|\,] = [\,|\, 8, -3, -7 \,|\,]$ の判別式は $233 = 1 + 4 \cdot 58$ である．判別式が 233 の主形式 $[\,|\, 1, 1, -58 \,|\,]$ の被約形式鎖の表から，$\eta^2 + \eta\xi - 58\xi^2 = -1$ の整数解 $\xi = 3034$，$\eta = 21639$ が得られ，定理 11.4 により $X = \begin{bmatrix} a\xi & \frac{1+h}{2}\xi + \eta \\ \frac{1-h}{2}\xi + \eta & -c\xi \end{bmatrix} = \begin{bmatrix} 24272 & 18605 \\ 27707 & 21238 \end{bmatrix} \in SL_2(\mathbb{Z})$ とおくと，$[\,|\, 7, 3, -8 \,|\,] \xrightarrow{X} [\,|\, 8, -3, -7 \,|\,]$ がわかる．または，注意 11.4 により，$t^2 - 233u^2 = -4$ の整数解，$t = 23156 \times 2 = 46312$，$u = 1517 \times 2 = 3034$，からも，$\begin{bmatrix} au & \frac{hu + t}{2} \\ \frac{-hu + t}{2} & -cu \end{bmatrix} = \begin{bmatrix} 24272 & 18605 \\ 27707 & 21238 \end{bmatrix}$ が得られる．あるいは，$f_0 = [\,|\, 7, 3, -8 \,|\,]$ の被約形式鎖の表から直ちに，$f_{39} = [\,|\, 8, -3, -7 \,|\,]$，$p_{39} = 24272$，$q_{39} = 18605$，$r_{39} = 27707$，$s_{39} = 21238$，が読み取れる．

12 例

以下の例では正式同値類 A の元 f と正式同値類 B の元 g の合成が正式同値類 C の元になるとき，$AB = C$ と表す．また，$AA = A^2$ などと表す．

例 12.1. 判別式が $3137 = 1 + 4 \cdot (28)^2$ の被約形式は全部で 418 個あり，次の 9 個の正式同値類に分けられる．

$A_0 = \{[\,1, 1, -784\,]], \cdots, [\,784, -1, -1\,]], \cdots, \}$（114 個）

$A_1 = \{[\,2, -33, -256\,]], \cdots, [\,256, 33, -2\,]], \cdots, \}$（62 個）

$A_2 = \{[\,4, -33, -128\,]], \cdots, [\,128, 33, -4\,]], \cdots, \}$（42 個）

$A_3 = \{[\,8, -33, -64\,]], \cdots, [\,64, 33, -8\,]], \cdots, \}$（26 個）

$A_4 = \{[\,16, -33, -32\,]], \cdots, [\,32, 33, -16\,]], \cdots, \}$（22 個）

$A_5 = \{[\,16, 33, -32\,]], \cdots, [\,32, -33, -16\,]], \cdots, \}$（22 個）

$A_6 = \{[\,8, 33, -64\,]], \cdots, [\,64, -33, -8\,]], \cdots, \}$（26 個）

$A_7 = \{[\,4, 33, -128\,]], \cdots, [\,128, -33, -4\,]], \cdots, \}$（42 個）

$A_8 = \{[\,2, 33, -256\,]], \cdots, [\,256, -33, -2\,]], \cdots, \}$（62 個）

A_0 が主類である．A_0 がただ一つのアンビグ類である．A_i（$i = 1, 2, 3, 4$）は A_{9-i} と非正式同値であるから，$A_i A_{9-i} = A_0$ である．

変数変換，$X = xx' + 128yy'$，$Y = 2xy' + 2yx' - 33yy'$，により，

$4X^2 - 33XY - 128Y^2 = (2x^2 - 33xy - 256y^2)(2x'^2 - 33x'y' - 256y'^2)$，となり，$A_1 A_1 = A_2$ である．

変数変換，$X = xx' + 64yy'$，$Y = 2xy' + 4yx' - 33yy'$，により，

$8X^2 - 33XY - 64Y^2 = (2x^2 - 33xy - 256y^2)(4x'^2 - 33x'y' - 128y'^2)$，となり，$A_1 A_2 = A_3$ である．

変数変換，$X = xx' + 32yy'$，$Y = 2xy' + 8yx' - 33yy'$，により，

$16X^2 - 33XY - 32Y^2 = (2x^2 - 33xy - 256y^2)(8x'^2 - 33x'y' - 64y'^2)$，となり，$A_1 A_3 = A_4$ である．

変数変換，$X = xx' + 16yy'$，$Y = 2xy' + 16yx' - 33yy'$，により，

$32X^2 - 33XY - 16Y^2 = (2x^2 - 33xy - 256y^2)(16x'^2 - 33x'y' - 32y'^2)$，となり，$A_1 A_4 = A_5$ である．

変数変換，$X = xx' + 8yy'$，$Y = 2xy' + 32yx' - 33yy'$，により，

$64X^2 - 33XY - 8Y^2 = (2x^2 - 33xy - 256y^2)(32x'^2 - 33x'y' - 16y'^2)$，となり，$A_1 A_5 = A_6$ である．

変数変換，$X = xx' + 4yy'$，$Y = 2xy' + 64yx' - 33yy'$，により，

$128X^2 - 33XY - 4Y^2 = (2x^2 - 33xy - 256y^2)(64x'^2 - 33x'y' - 8y'^2)$，となり，$A_1 A_6 = A_7$ である．

変数変換，$X = xx' + 2yy'$，$Y = 2xy' + 128yx' - 33yy'$，により，

$256X^2 - 33XY - 2Y^2 = (2x^2 - 33xy - 256y^2)(128x'^2 - 33x'y' - 4y'^2)$，となり，$A_1 A_7 = A_8$ である．

ゆえに，$A_1^k = A_k$（$k = 2, 3, 4, 5, 6, 7, 8$），$A_1^9 = A_0$ であり，$\mathcal{G} = \{A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8\}$ は群 $\mathbb{Z}/9\mathbb{Z}$ の構造をもつ．$x^2 + xy - 784y^2 = -1$ は整数解（$55^2 + 55 \cdot 2 - 784 \cdot 2^2 = -1$）をもつから，広義同値と正式同値は同じである．$\mathcal{G}$ の平方類は，$\mathcal{G}^2 = \{A_0^2, A_1^2, A_2^2, A_3^2, A_4^2, A_5^2, A_6^2, A_7^2, A_8^2\} = \{A_0, A_2, A_4, A_6, A_8, A_1, A_3, A_5, A_7\} = \mathcal{G}$ であるから，$\mathcal{G}$ の種数は $9/9 = 1$ である．

注意 12.1. 一般に，判別式が $p \equiv 1 \mod 4$ をみたす素数 p の場合，定理 7.4 により，アンビグ類の元は，$[|\,1,-1,(1-p)/4\,|]$ または $[|\,(p-1)/4,1,-1\,|]$ と正式同値になり，例 7.1 と注意 11.4 により，この 2 つは正式同値となるから，主類がただ一つのアンビグ類である．したがって，注意 11.2 より，正式同値類の個数は奇数である．特に，すべての類が主種（平方類）に属す．

例 12.2. 判別式が $4 \cdot 3719 = 14876$ の被約形式は全部で 890 個あり，次の 18 個の正式同値類に分けられる

$A_0 = \{[|\,1,0,-3719\,|],[|\,1,2,-3718\,|],\cdots,,\cdots,\}$（181 個）

$B_0 = \{[|\,3719,0,-1\,|],[|\,3718,-2,-1\,|],\cdots,,\cdots,\}$（181 個）

$A_1 = \{[|\,13,-2,-286\,|],\cdots,[|\,85,16,-43\,|],\cdots,[|\,49,-64,-55\,|],\cdots,\}$（25 個）

$A_8 = \{[|\,13,2,-286\,|],\cdots,[|\,85,-16,-43\,|],\cdots,[|\,49,64,-55\,|],\cdots,\}$（25 個）

$B_1 = \{[|\,286,2,-13\,|],\cdots,[|\,43,-16,-85\,|],\cdots,[|\,55,64,-49\,|],\cdots,\}$（25 個）

$B_8 = \{[|\,286,-2,-13\,|],\cdots,[|\,43,16,-85\,|],\cdots,[|\,55,-64,-49\,|],\cdots,\}$（25 個）

$A_2 = \{[|\,169,-2,-22\,|],\cdots,[|\,245,64,-11\,|],\cdots,\}$（27 個）

$A_7 = \{[|\,169,2,-22\,|],\cdots,[|\,245,-64,-11\,|],\cdots,\}$（27 個）

$B_2 = \{[|\,22,2,-169\,|],\cdots,[|\,11,64,-245\,|],\cdots,\}$（27 個）

$B_7 = \{[|\,22,-2,-169\,|],\cdots,[|\,11,-64,-245\,|],\cdots,\}$（27 個）

$A_3 = \{[|\,5,-16,-731\,|],\cdots,[|\,5,64,-539\,|],\cdots,\}$（43 個）

$A_6 = \{[|\,5,16,-731\,|],\cdots,[|\,5,-64,-539\,|],\cdots,\}$（43 個）

$B_3 = \{[|\,731,16,-5\,|],\cdots,[|\,539,-64,-5\,|],\cdots,\}$（43 個）

$B_6 = \{[|\,731,-16,-5\,|],\cdots,[|\,539,64,-5\,|],\cdots,\}$（43 個）

$A_4 = \{[|\,17,16,-215\,|],\cdots,[|\,385,-64,-7\,|],\cdots,\}$（37 個）

$A_5 = \{[|\,17,-16,-215\,|],\cdots,[|\,385,64,-7\,|],\cdots,\}$（37 個）

$B_4 = \{[|\,215,-16,-17\,|],\cdots,[|\,7,64,-385\,|],\cdots,\}$（37 個）

$B_5 = \{[|\,215,16,-17\,|],\cdots,[|\,7,-64,-385\,|],\cdots,\}$（37 個）

A_0 が主類である．アンビグ類は A_0 と B_0 である．$i = 1,2,3,4$ のとき，A_i は A_{9-i} と非正式同値であるから，$A_iA_{9-i} = A_0$ であり，B_i は B_{9-i} と非正式同値であるから，$B_iB_{9-i} = A_0$ である．

変数変換，$X = xx' + 22yy'$，$Y = 13xy' + 13yx' - 2yy'$，により，

$169X^2 - 2XY - 22Y^2 = (13x^2 - 2xy - 286y^2)(13x'^2 - 2x'y' - 286y'^2)$，となり，$A_1A_1 = A_2$ である．

変数変換，$X = 49xx' - 64yx' + 11yy'$，$Y = xy' + 5yx'$，により，

$5X^2 + 64XY - 539Y^2 = (49x^2 - 64xy - 55y^2)(245x'^2 + 64x'y' - 11y'^2)$，となり，$A_1A_2 = A_3$ である．

変数変換，$X = 5xx' - 16xy' + 43yy'$，$Y = 17xy' + yx'$，により，

$17X^2 + 16XY - 215Y^2 = (85x^2 + 16xy - 43y^2)(5x'^2 - 16x'y' - 731y'^2)$，となり，$A_1A_3 = A_4$ である．

変数変換，$X = 7xx' + yy'$，$Y = 64xx' + 7xy' + 55yx'$，により，

$385X^2 + 64XY - 7Y^2 = (49x^2 - 64xy - 55y^2)(385x'^2 - 64x'y' - 7y'^2)$，となり，$A_1A_4 = A_5$ である．

変数変換，$X = 17xx' - 16xy' + 43yy'$，$Y = 5xy' + yx'$，により，

$5X^2 + 16XY - 731Y^2 = (85x^2 + 16xy - 43y^2)(17x'^2 - 16x'y' - 215y'^2)$，となり，$A_1A_5 = A_6$ である．

変数変換，$X = xx' + 11yy'$，$Y = 49xy' + 5yx' - 64yy'$，により，

$245X^2 - 64XY - 11Y^2 = (49x^2 - 64xy - 55y^2)(5x'^2 - 64x'y' - 539y'^2)$，となり，$A_1A_6 = A_7$ である．

変数変換，$X = 13xx' - 2yx' + 22yy'$，$Y = xy' + 13yx'$，により，

$13X^2 + 2XY - 286Y^2 = (13x^2 - 2xy - 286y^2)(169x'^2 + 2x'y' - 22y'^2)$，となり，$A_1A_7 = A_8$ である．

ゆえに，$A_1^k = A_k$（$k = 2,3,4,5,6,7,8$），$A_1^9 = A_0$ である．また，$A_iB_0 = B_i$ であり，$B_0B_0 = A_0$，であるから，正式同値類の集合 $\mathcal{G} = \{A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, B_0, B_1, B_2, B_3, B_4, B_5, B_6, B_7, B_8\}$ は $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ と同型になる．各 i について，A_i と B_i は広義同値であるから，広義同値類の集合 $\bar{\mathcal{G}} = \{A_0 \cup B_0, A_1 \cup B_1, A_2 \cup B_2, A_3 \cup B_3, A_4 \cup B_4, A_5 \cup B_5, A_6 \cup B_6, A_7 \cup B_7, A_8 \cup B_8\}$ は $\mathbb{Z}/9\mathbb{Z}$ と同型になる．$\mathcal{G}$ の平方類は，$\mathcal{G}^2 = \{A_i^2, B_i^2 \ ; \ 0 \leqq i \leqq 8\} = \{A_0, A_2, A_4, A_6, A_8, A_1, A_3, A_5, A_7\}$ であるから，$\mathcal{G}$ の種数は $18/9 = 2$ である．

例 12.3. 判別式が $4 \cdot 210 = 840 = 2^3 \cdot 3 \cdot 5 \cdot 7$ の被約形式は 144 個あり，次の 8 つの正式同値類に分けられる．

$A_0 = \{[\,|\,1, 0, -210\,|\,], \cdots, [\,|\,15, 0, -14\,|\,], \cdots, \}$（30 個）

$B_0 = \{[\,|\,210, 0, -1\,|\,] \cdots, [\,|\,14, 0, -15\,|\,], \cdots, \}$（30 個）

$A_1 = \{[\,|\,2, 0, -105\,|\,], \cdots, [\,|\,30, 0, -7\,|\,], \cdots, \}$（18 個）

$B_1 = \{[\,|\,105, 0, -2\,|\,], \cdots, [\,|\,7, 0, -30\,|\,], \cdots, \}$（18 個）

$A_2 = \{[\,|\,3, 0, -70\,|\,], \cdots, [\,|\,5, 0, -42\,|\,], \cdots, \}$（14 個）

$B_2 = \{[\,|\,70, 0, -3\,|\,], \cdots, [\,|\,42, 0, -5\,|\,], \cdots, \}$（14 個）

$A_3 = \{[\,|\,6, 0, -35\,|\,], \cdots, [\,|\,10, 0, -21\,|\,], \cdots, \}$（10 個）

$B_3 = \{[\,|\,35, 0, -6\,|\,], \cdots, [\,|\,21, 0, -10\,|\,], \cdots, \}$（10 個）

A_0 が主類である．どの正式同値類も，中間係数が 0 のアンビグ形式を含むから，アンビグ類であり，$A_i^2 = B_i^2 = A_0$ である．また，$ac = -210$ のとき，変数変換，$X = axx' + yy'$，$Y = xy' - cyx'$ により，$-cX^2 - aY^2 = (ax^2 + cy^2)(210x'^2 - y'^2)$ となるから，$i = 1, 2, 3$ について，$A_iB_0 = B_i$ である．変数変換，$X = xx' + 35yy'$，$Y = 2xy' + 3yx'$ により $6X^2 - 35Y^2 = (2x^2 - 105y^2)(3x'^2 - 70y'^2)$ となり，$A_1A_2 = A_3$ である．したがって，$\mathcal{G} = \{A_0, A_1, A_2, A_3, B_0, B_1, B_2, B_3\} = \{A_0, A_1, A_2, A_3\} \cup \{A_0, A_1, A_2, A_3\}B_0$ は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ と同型である．

$x^2 - 210y^2 = -1$ は解をもたないから，$i = 0, 1, 2, 3$ について，A_i と B_i は正式同値でないが広義同値である．ゆえに，広義同値類の集合 $\{A_0 \cup B_0, A_1 \cup B_1, A_2 \cup B_2, A_3 \cup B_3\}$ は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ と同型である．

$\mathcal{G}$ の平方類は，$\mathcal{G}^2 = \{A_0^2, A_1^2, A_2^2, A_3^2, B_0^2, B_1^2, B_2^2, B_3^2\} = \{A_0\}$ であるから，$\mathcal{G}$ の種数は $8/1 = 8$ である．

13 おわりに

佐藤文広氏の解説 [4] にチャクラヴァーラと二元二次形式のガウスの簡約理論との関係についての記述があるが，ガウスの被約化写像を計算しようとすると，合同式の計算が必要で，面倒である．一方，フルヴィッツの被約形式鎖の表は整数の加減算と正負の判定のみで作成できる．両者の関係については別の機会にしたい．

（2024 年 1 月 16 日提出，まえだひろのぶ，sugakugauss[at]gmail.com）

付録 1 下記の表は，p が素数で $p \equiv 1 \mod 4$ のとき，判別式が p の 2 次形式の正式同値類の個数を $h^+(p)$ とした，$\{p, h^+(p)\}$ の表．$x^2 - py^2 = -4$ に整数解が存在するから，$h^+(p)$ は $\mathbb{Q}(\sqrt{p})$ の類数 $h(p)$ と等しい．

{5, 1}	{13, 1}	{17, 1}	{29, 1}	{37, 1}	{41, 1}	{53, 1}	{61, 1}	{73, 1}	{89, 1}
{97, 1}	{101, 1}	{109, 1}	{113, 1}	{137, 1}	{149, 1}	{157, 1}	{173, 1}	{181, 1}	{193, 1}
{197, 1}	{229, 3}	{233, 1}	{241, 1}	{257, 3}	{269, 1}	{277, 1}	{281, 1}	{293, 1}	{313, 1}
{317, 1}	{337, 1}	{349, 1}	{353, 1}	{373, 1}	{389, 1}	{397, 1}	{401, 5}	{409, 1}	{421, 1}
{433, 1}	{449, 1}	{457, 1}	{461, 1}	{509, 1}	{521, 1}	{541, 1}	{557, 1}	{569, 1}	{577, 7}
{593, 1}	{601, 1}	{613, 1}	{617, 1}	{641, 1}	{653, 1}	{661, 1}	{673, 1}	{677, 1}	{701, 1}
{709, 1}	{733, 3}	{757, 1}	{761, 3}	{769, 1}	{773, 1}	{797, 1}	{809, 1}	{821, 1}	{829, 1}
{853, 1}	{857, 1}	{877, 1}	{881, 1}	{929, 1}	{937, 1}	{941, 1}	{953, 1}	{977, 1}	{997, 1}
{1009, 7}	{1013, 1}	{1021, 1}	{1033, 1}	{1049, 1}	{1061, 1}	{1069, 1}	{1093, 5}	{1097, 1}	{1109, 1}
{1117, 1}	{1129, 9}	{1153, 1}	{1181, 1}	{1193, 1}	{1201, 1}	{1213, 1}	{1217, 1}	{1229, 3}	{1237, 1}
{1249, 1}	{1277, 1}	{1289, 1}	{1297, 11}	{1301, 1}	{1321, 1}	{1361, 1}	{1373, 3}	{1381, 1}	{1409, 1}
{1429, 5}	{1433, 1}	{1453, 1}	{1481, 1}	{1489, 3}	{1493, 1}	{1549, 1}	{1553, 1}	{1597, 1}	{1601, 7}
{1609, 1}	{1613, 1}	{1621, 1}	{1637, 1}	{1657, 1}	{1669, 1}	{1693, 1}	{1697, 1}	{1709, 1}	{1721, 1}
{1733, 1}	{1741, 1}	{1753, 1}	{1777, 1}	{1789, 1}	{1801, 1}	{1861, 1}	{1873, 1}	{1877, 1}	{1889, 1}
{1901, 3}	{1913, 1}	{1933, 1}	{1949, 1}	{1973, 1}	{1993, 1}	{1997, 1}	{2017, 1}	{2029, 7}	{2053, 1}
{2069, 1}	{2081, 5}	{2089, 3}	{2113, 1}	{2129, 1}	{2137, 1}	{2141, 1}	{2153, 5}	{2161, 1}	{2213, 3}
{2221, 1}	{2237, 1}	{2269, 1}	{2273, 1}	{2281, 1}	{2293, 1}	{2297, 1}	{2309, 1}	{2333, 1}	{2341, 1}
{2357, 1}	{2377, 1}	{2381, 1}	{2389, 1}	{2393, 1}	{2417, 1}	{2437, 1}	{2441, 1}	{2473, 1}	{2477, 1}
{2521, 1}	{2549, 1}	{2557, 3}	{2593, 1}	{2609, 1}	{2617, 1}	{2621, 1}	{2633, 1}	{2657, 1}	{2677, 3}
{2689, 1}	{2693, 1}	{2713, 3}	{2729, 1}	{2741, 1}	{2749, 1}	{2753, 1}	{2777, 3}	{2789, 1}	{2797, 1}
{2801, 1}	{2833, 1}	{2837, 1}	{2857, 3}	{2861, 1}	{2897, 1}	{2909, 1}	{2917, 3}	{2953, 1}	{2957, 1}
{2969, 1}	{3001, 1}	{3037, 1}	{3041, 1}	{3049, 1}	{3061, 1}	{3089, 1}	{3109, 1}	{3121, 5}	{3137, 9}
{3169, 1}	{3181, 5}	{3209, 1}	{3217, 1}	{3221, 3}	{3229, 3}	{3253, 5}	{3257, 1}	{3301, 1}	{3313, 1}
{3329, 1}	{3361, 1}	{3373, 1}	{3389, 1}	{3413, 1}	{3433, 1}	{3449, 1}	{3457, 1}	{3461, 1}	{3469, 1}
{3517, 1}	{3529, 1}	{3533, 1}	{3541, 1}	{3557, 1}	{3581, 1}	{3593, 1}	{3613, 1}	{3617, 1}	{3637, 1}
{3673, 1}	{3677, 1}	{3697, 1}	{3701, 1}	{3709, 1}	{3733, 1}	{3761, 1}	{3769, 1}	{3793, 1}	{3797, 1}
{3821, 1}	{3833, 1}	{3853, 1}	{3877, 3}	{3881, 1}	{3889, 3}	{3917, 1}	{3929, 1}	{3989, 1}	{4001, 3}
{4013, 1}	{4021, 1}	{4049, 1}	{4057, 1}	{4073, 1}	{4093, 1}	{4129, 1}	{4133, 1}	{4153, 1}	{4157, 1}
{4177, 1}	{4201, 1}	{4217, 1}	{4229, 7}	{4241, 1}	{4253, 1}	{4261, 1}	{4273, 1}	{4289, 1}	{4297, 1}
{4337, 1}	{4349, 1}	{4357, 5}	{4373, 1}	{4397, 1}	{4409, 9}	{4421, 1}	{4441, 5}	{4457, 1}	{4481, 3}
{4493, 3}	{4513, 1}	{4517, 1}	{4549, 1}	{4561, 1}	{4597, 3}	{4621, 1}	{4637, 1}	{4649, 3}	{4657, 1}
{4673, 1}	{4721, 1}	{4729, 3}	{4733, 1}	{4789, 1}	{4793, 1}	{4801, 1}	{4813, 1}	{4817, 1}	{4861, 1}
{4877, 1}	{4889, 5}	{4909, 1}	{4933, 3}	{4937, 1}	{4957, 1}	{4969, 1}	{4973, 1}	{4993, 1}	{5009, 1}
{5021, 1}	{5077, 1}	{5081, 3}	{5101, 1}	{5113, 1}	{5153, 1}	{5189, 1}	{5197, 1}	{5209, 1}	{5233, 1}
{5237, 1}	{5261, 3}	{5273, 7}	{5281, 3}	{5297, 3}	{5309, 1}	{5333, 3}	{5381, 1}	{5393, 1}	{5413, 1}
{5417, 7}	{5437, 1}	{5441, 1}	{5449, 1}	{5477, 3}	{5501, 1}	{5521, 9}	{5557, 1}	{5569, 1}	{5573, 1}
{5581, 1}	{5641, 1}	{5653, 1}	{5657, 1}	{5669, 1}	{5689, 1}	{5693, 1}	{5701, 1}	{5717, 1}	{5737, 1}
{5741, 3}	{5749, 1}	{5801, 1}	{5813, 1}	{5821, 3}	{5849, 1}	{5857, 1}	{5861, 1}	{5869, 1}	{5881, 1}
{5897, 1}	{5953, 1}	{5981, 1}	{6029, 1}	{6037, 1}	{6053, 3}	{6073, 1}	{6089, 1}	{6101, 1}	{6113, 5}
{6121, 1}	{6133, 3}	{6173, 1}	{6197, 1}	{6217, 1}	{6221, 1}	{6229, 1}	{6257, 1}	{6269, 1}	{6277, 1}
{6301, 1}	{6317, 1}	{6329, 1}	{6337, 1}	{6353, 1}	{6361, 1}	{6373, 1}	{6389, 1}	{6397, 1}	{6421, 1}
{6449, 1}	{6469, 1}	{6473, 1}	{6481, 5}	{6521, 1}	{6529, 1}	{6553, 1}	{6569, 1}	{6577, 1}	{6581, 1}
{6637, 3}	{6653, 1}	{6661, 1}	{6673, 1}	{6689, 1}	{6701, 1}	{6709, 1}	{6733, 1}	{6737, 1}	{6761, 1}
{6781, 1}	{6793, 1}	{6829, 1}	{6833, 1}	{6841, 1}	{6857, 1}	{6869, 1}	{6917, 1}	{6949, 5}	{6961, 1}
{6977, 1}	{6997, 3}	{7001, 1}	{7013, 1}	{7057, 21}	{7069, 1}	{7109, 1}	{7121, 1}	{7129, 1}	{7177, 1}
{7193, 1}	{7213, 1}	{7229, 5}	{7237, 1}	{7253, 1}	{7297, 1}	{7309, 1}	{7321, 1}	{7333, 1}	{7349, 1}
{7369, 1}	{7393, 1}	{7417, 1}	{7433, 1}	{7457, 1}	{7477, 1}	{7481, 3}	{7489, 1}	{7517, 1}	{7529, 1}
{7537, 3}	{7541, 1}	{7549, 1}	{7561, 1}	{7573, 9}	{7577, 1}	{7589, 1}	{7621, 1}	{7649, 1}	{7669, 1}
{7673, 3}	{7681, 1}	{7717, 1}	{7741, 1}	{7753, 3}	{7757, 1}	{7789, 1}	{7793, 1}	{7817, 5}	{7829, 1}

下記の表は，p が素数で $p \equiv 3 \mod 4$ のとき，判別式が $4p$ の 2 次形式の正式同値類の個数を $h^+(4p)$ とした，$\{p, h^+(4p)/2\}$ の表．$x^2 - py^2 = -1$ に整数解が存在しないから，$h^+(4p)/2$ は $\mathbb{Q}(\sqrt{p})$ の類数 $h(p)$ と等しい．

{3, 1}	{7, 1}	{11, 1}	{19, 1}	{23, 1}	{31, 1}	{43, 1}	{47, 1}	{59, 1}	{67, 1}
{71, 1}	{79, 3}	{83, 1}	{103, 1}	{107, 1}	{127, 1}	{131, 1}	{139, 1}	{151, 1}	{163, 1}
{167, 1}	{179, 1}	{191, 1}	{199, 1}	{211, 1}	{223, 3}	{227, 1}	{239, 1}	{251, 1}	{263, 1}
{271, 1}	{283, 1}	{307, 1}	{311, 1}	{331, 1}	{347, 1}	{359, 3}	{367, 1}	{379, 1}	{383, 1}
{419, 1}	{431, 1}	{439, 5}	{443, 3}	{463, 1}	{467, 1}	{479, 1}	{487, 1}	{491, 1}	{499, 5}
{503, 1}	{523, 1}	{547, 1}	{563, 1}	{571, 1}	{587, 1}	{599, 1}	{607, 1}	{619, 1}	{631, 1}
{643, 1}	{647, 1}	{659, 3}	{683, 1}	{691, 1}	{719, 1}	{727, 5}	{739, 1}	{743, 1}	{751, 1}
{787, 1}	{811, 1}	{823, 1}	{827, 1}	{839, 3}	{859, 1}	{863, 1}	{883, 1}	{887, 1}	{907, 1}
{911, 1}	{919, 1}	{947, 1}	{967, 1}	{971, 1}	{983, 1}	{991, 1}	{1019, 1}	{1031, 1}	{1039, 1}
{1051, 1}	{1063, 1}	{1087, 7}	{1091, 3}	{1103, 1}	{1123, 1}	{1151, 1}	{1163, 1}	{1171, 3}	{1187, 1}
{1223, 3}	{1231, 1}	{1259, 1}	{1279, 1}	{1283, 1}	{1291, 1}	{1303, 1}	{1307, 1}	{1319, 1}	{1327, 5}
{1367, 3}	{1399, 1}	{1423, 1}	{1427, 1}	{1439, 1}	{1447, 1}	{1451, 1}	{1459, 1}	{1471, 1}	{1483, 1}
{1487, 1}	{1499, 1}	{1511, 1}	{1523, 3}	{1531, 1}	{1543, 1}	{1559, 1}	{1567, 3}	{1571, 1}	{1579, 1}
{1583, 1}	{1607, 1}	{1619, 1}	{1627, 3}	{1663, 1}	{1667, 1}	{1699, 1}	{1723, 1}	{1747, 1}	{1759, 1}
{1783, 1}	{1787, 3}	{1811, 3}	{1823, 1}	{1831, 1}	{1847, 3}	{1867, 1}	{1871, 1}	{1879, 1}	{1907, 3}
{1931, 1}	{1951, 1}	{1979, 1}	{1987, 3}	{1999, 1}	{2003, 1}	{2011, 1}	{2027, 5}	{2039, 1}	{2063, 1}
{2083, 1}	{2087, 1}	{2099, 3}	{2111, 1}	{2131, 1}	{2143, 3}	{2179, 1}	{2203, 1}	{2207, 3}	{2239, 1}
{2243, 1}	{2251, 7}	{2267, 1}	{2287, 1}	{2311, 1}	{2339, 1}	{2347, 1}	{2351, 1}	{2371, 1}	{2383, 1}
{2399, 5}	{2411, 1}	{2423, 1}	{2447, 1}	{2459, 3}	{2467, 7}	{2503, 1}	{2531, 1}	{2539, 1}	{2543, 3}
{2551, 1}	{2579, 1}	{2591, 1}	{2647, 1}	{2659, 3}	{2663, 1}	{2671, 1}	{2683, 1}	{2687, 1}	{2699, 1}
{2707, 1}	{2711, 3}	{2719, 1}	{2731, 1}	{2767, 1}	{2791, 1}	{2803, 1}	{2819, 1}	{2843, 1}	{2851, 1}
{2879, 1}	{2887, 1}	{2903, 1}	{2927, 1}	{2939, 1}	{2963, 1}	{2971, 3}	{2999, 1}	{3011, 1}	{3019, 1}
{3023, 3}	{3067, 1}	{3079, 1}	{3083, 1}	{3119, 1}	{3163, 3}	{3167, 1}	{3187, 1}	{3191, 1}	{3203, 1}
{3251, 5}	{3259, 1}	{3271, 1}	{3299, 1}	{3307, 1}	{3319, 1}	{3323, 1}	{3331, 1}	{3343, 1}	{3347, 1}
{3359, 1}	{3371, 1}	{3391, 3}	{3407, 1}	{3463, 1}	{3467, 1}	{3491, 1}	{3499, 1}	{3511, 1}	{3527, 1}
{3539, 1}	{3547, 1}	{3559, 1}	{3571, 1}	{3583, 1}	{3607, 1}	{3623, 1}	{3631, 1}	{3643, 1}	{3659, 1}
{3671, 1}	{3691, 1}	{3719, 9}	{3727, 1}	{3739, 3}	{3767, 1}	{3779, 1}	{3803, 3}	{3823, 1}	{3847, 1}
{3851, 1}	{3863, 1}	{3907, 1}	{3911, 1}	{3919, 1}	{3923, 1}	{3931, 1}	{3943, 1}	{3947, 1}	{3967, 5}
{4003, 1}	{4007, 1}	{4019, 1}	{4027, 1}	{4051, 1}	{4079, 1}	{4091, 1}	{4099, 1}	{4111, 1}	{4127, 1}
{4139, 7}	{4159, 3}	{4211, 1}	{4219, 1}	{4231, 1}	{4243, 1}	{4259, 1}	{4271, 5}	{4283, 3}	{4327, 1}
{4339, 1}	{4363, 1}	{4391, 1}	{4423, 1}	{4447, 1}	{4451, 1}	{4463, 1}	{4483, 1}	{4507, 1}	{4519, 1}
{4523, 1}	{4547, 1}	{4567, 1}	{4583, 1}	{4591, 5}	{4603, 1}	{4639, 1}	{4643, 1}	{4651, 3}	{4663, 1}
{4679, 1}	{4691, 1}	{4703, 1}	{4723, 1}	{4751, 1}	{4759, 13}	{4783, 1}	{4787, 1}	{4799, 1}	{4831, 1}
{4871, 1}	{4903, 1}	{4919, 1}	{4931, 1}	{4943, 1}	{4951, 1}	{4967, 1}	{4987, 1}	{4999, 1}	{5003, 1}
{5011, 3}	{5023, 1}	{5039, 7}	{5051, 1}	{5059, 1}	{5087, 1}	{5099, 3}	{5107, 5}	{5119, 1}	{5147, 1}
{5167, 1}	{5171, 1}	{5179, 1}	{5227, 1}	{5231, 1}	{5279, 1}	{5303, 3}	{5323, 1}	{5347, 1}	{5351, 1}
{5387, 1}	{5399, 1}	{5407, 1}	{5419, 1}	{5431, 3}	{5443, 1}	{5471, 1}	{5479, 1}	{5483, 1}	{5503, 3}
{5507, 1}	{5519, 1}	{5527, 5}	{5531, 1}	{5563, 1}	{5591, 1}	{5623, 9}	{5639, 1}	{5647, 1}	{5651, 1}
{5659, 1}	{5683, 3}	{5711, 5}	{5743, 7}	{5779, 1}	{5783, 1}	{5791, 1}	{5807, 1}	{5827, 7}	{5839, 1}
{5843, 1}	{5851, 1}	{5867, 1}	{5879, 1}	{5903, 3}	{5923, 1}	{5927, 5}	{5939, 1}	{5987, 1}	{6007, 1}
{6011, 1}	{6043, 1}	{6047, 1}	{6067, 1}	{6079, 1}	{6091, 1}	{6131, 1}	{6143, 1}	{6151, 7}	{6163, 1}
{6199, 1}	{6203, 1}	{6211, 1}	{6247, 1}	{6263, 1}	{6271, 1}	{6287, 1}	{6299, 1}	{6311, 3}	{6323, 1}
{6343, 1}	{6359, 1}	{6367, 1}	{6379, 1}	{6427, 3}	{6451, 1}	{6491, 1}	{6547, 1}	{6551, 1}	{6563, 5}
{6571, 3}	{6599, 1}	{6607, 1}	{6619, 1}	{6659, 1}	{6679, 1}	{6691, 1}	{6703, 1}	{6719, 1}	{6763, 1}
{6779, 5}	{6791, 3}	{6803, 1}	{6823, 1}	{6827, 1}	{6863, 1}	{6871, 1}	{6883, 1}	{6899, 1}	{6907, 1}
{6911, 1}	{6947, 1}	{6959, 1}	{6967, 1}	{6971, 1}	{6983, 1}	{6991, 1}	{7019, 3}	{7027, 1}	{7039, 1}
{7043, 1}	{7079, 1}	{7103, 1}	{7127, 1}	{7151, 1}	{7159, 1}	{7187, 1}	{7207, 1}	{7211, 1}	{7219, 1}
{7243, 1}	{7247, 1}	{7283, 1}	{7307, 1}	{7331, 5}	{7351, 1}	{7411, 1}	{7451, 1}	{7459, 3}	{7487, 1}
{7499, 1}	{7507, 1}	{7523, 1}	{7547, 1}	{7559, 1}	{7583, 1}	{7591, 5}	{7603, 1}	{7607, 1}	{7639, 3}
{7643, 3}	{7687, 1}	{7691, 1}	{7699, 1}	{7703, 1}	{7723, 1}	{7727, 1}	{7759, 1}	{7823, 1}	{7867, 1}

付録 2 平方因子を含まない D（$2 \leqq D \leqq 444$）について，実 2 次体 $\mathbb{Q}(\sqrt{D})$ の「狭義類数」h_D^+ を被約形式鎖を用いて計算し，類数も h_D^+ になる場合は $\{D, -h_D^+\}$ を，類数が $h_D^+/2$ になる場合は $\{D, h_D^+/2\}$ を出力するプログラムの例（Wolfram Mathematica 12.2 for Linux ARM (32-bit) / Raspberry Pi 4 Computer）.

In[1]:=
```
klasse[D_] := ( disk = If[Mod[D, 4] == 1, D, 4*D];
    hauptForm = If[Mod[D, 4] == 1, {{1, 1, (1 - D)/4}}, {{1, 0, -D}}];
    umkehrForm = If[Mod[D, 4] == 1, {{(D - 1)/4, -1, -1}}, {{D, 0, -1}}];
    hMaximum = Floor[Sqrt[disk]];
    teiler[h_] := If[IntegerQ[(disk - h^2)/4], Flatten[Divisors[(disk - h^2)/4], 1], {}];
    quadraForm[a_, h_, c_] = If[a == 0, {}, {a, h, c}];
    redFormen[h_] := Map[quadraForm[#, h, -(disk - h^2)/(4*#)] &, teiler[h]];
    gesamteFormen = Flatten[ redFormen /@ Range[-hMaximum, hMaximum], 1];
    naechsteForm[{a_, h_, c_}] = If[a + h + c > 0, {{a + h + c, h + 2*c, c}}, {{a, 2*a + h, a + h + c}}];
    hinzuFormenListe[s_] := Append[s, First[naechsteForm[Last[s]]]];
    kette[s_] := If[Last[hinzuFormenListe[s]] == First[hinzuFormenListe[s]], s, kette[hinzuFormenListe[s]]];
    hauptklasse := kette[hauptForm];
    vorzeichen := If[MemberQ[hauptklasse, First[umkehrForm]], -1, 1/2];
    nehmen[s_] := If[First[s] == {}, {}, kette[List[First[s]]]];
    verblieb[s_] := Complement[s, nehmen[s]];
    klassenzahl[s_] := (i = vorzeichen; If[s == {}, i, vorzeichen + klassenzahl[verblieb[s]]]);
    klassenzahl[Complement[gesamteFormen, hauptklasse]]
            );
quadratFrei = Select[Range[2, 444], SquareFreeQ];
tabelle = Grid[Partition[Transpose[{quadratFrei, klasse /@ quadratFrei}], 10]]
```

Out[3]=

{2, -1}	{3, 1}	{5, -1}	{6, 1}	{7, 1}	{10, -2}	{11, 1}	{13, -1}	{14, 1}	{15, 2}
{17, -1}	{19, 1}	{21, 1}	{22, 1}	{23, 1}	{26, -2}	{29, -1}	{30, 2}	{31, 1}	{33, 1}
{34, 2}	{35, 2}	{37, -1}	{38, 1}	{39, 2}	{41, -1}	{42, 2}	{43, 1}	{46, 1}	{47, 1}
{51, 2}	{53, -1}	{55, 2}	{57, 1}	{58, -2}	{59, 1}	{61, -1}	{62, 1}	{65, -2}	{66, 2}
{67, 1}	{69, 1}	{70, 2}	{71, 1}	{73, -1}	{74, -2}	{77, 1}	{78, 2}	{79, 3}	{82, -4}
{83, 1}	{85, -2}	{86, 1}	{87, 2}	{89, -1}	{91, 2}	{93, 1}	{94, 1}	{95, 2}	{97, -1}
{101, -1}	{102, 2}	{103, 1}	{105, 2}	{106, -2}	{107, 1}	{109, -1}	{110, 2}	{111, 2}	{113, -1}
{114, 2}	{115, 2}	{118, 1}	{119, 2}	{122, -2}	{123, 2}	{127, 1}	{129, 1}	{130, -4}	{131, 1}
{133, 1}	{134, 1}	{137, -1}	{138, 2}	{139, 1}	{141, 1}	{142, 3}	{143, 2}	{145, -4}	{146, 2}
{149, -1}	{151, 1}	{154, 2}	{155, 2}	{157, -1}	{158, 1}	{159, 2}	{161, 1}	{163, 1}	{165, 2}
{166, 1}	{167, 1}	{170, -4}	{173, -1}	{174, 2}	{177, 1}	{178, 2}	{179, 1}	{181, -1}	{182, 2}
{183, 2}	{185, -2}	{186, 2}	{187, 2}	{190, 2}	{191, 1}	{193, -1}	{194, 2}	{195, 4}	{197, -1}
{199, 1}	{201, 1}	{202, -2}	{203, 2}	{205, 2}	{206, 1}	{209, 1}	{210, 4}	{211, 1}	{213, 1}
{214, 1}	{215, 2}	{217, 1}	{218, -2}	{219, 4}	{221, 2}	{222, 2}	{223, 3}	{226, -8}	{227, 1}
{229, -3}	{230, 2}	{231, 4}	{233, -1}	{235, 6}	{237, 1}	{238, 2}	{239, 1}	{241, -1}	{246, 2}
{247, 2}	{249, 1}	{251, 1}	{253, 1}	{254, 3}	{255, 4}	{257, -3}	{258, 2}	{259, 2}	{262, 1}
{263, 1}	{265, -2}	{266, 2}	{267, 2}	{269, -1}	{271, 1}	{273, 2}	{274, -4}	{277, -1}	{278, 1}
{281, -1}	{282, 2}	{283, 1}	{285, 2}	{286, 2}	{287, 2}	{290, -4}	{291, 4}	{293, -1}	{295, 2}
{298, -2}	{299, 2}	{301, 1}	{302, 1}	{303, 2}	{305, 2}	{307, 1}	{309, 1}	{310, 2}	{311, 1}
{313, -1}	{314, -2}	{317, -1}	{318, 2}	{319, 2}	{321, 3}	{322, 4}	{323, 4}	{326, 3}	{327, 2}
{329, 1}	{330, 4}	{331, 1}	{334, 1}	{335, 2}	{337, -1}	{339, 2}	{341, 1}	{345, 2}	{346, -6}
{347, 1}	{349, -1}	{353, -1}	{354, 2}	{355, 2}	{357, 2}	{358, 1}	{359, 3}	{362, -2}	{365, -2}
{366, 2}	{367, 1}	{370, -4}	{371, 2}	{373, -1}	{374, 2}	{377, 2}	{379, 1}	{381, 1}	{382, 1}
{383, 1}	{385, 2}	{386, 2}	{389, -1}	{390, 4}	{391, 2}	{393, 1}	{394, -2}	{395, 2}	{397, -1}
{398, 1}	{399, 8}	{401, -5}	{402, 2}	{403, 2}	{406, 2}	{407, 2}	{409, -1}	{410, 4}	{411, 2}
{413, 1}	{415, 2}	{417, 1}	{418, 2}	{419, 1}	{421, -1}	{422, 1}	{426, 2}	{427, 6}	{429, 2}
{430, 2}	{431, 1}	{433, -1}	{434, 4}	{435, 4}	{437, 1}	{438, 4}	{439, 5}	{442, -8}	{443, 3}