Duncan A. Buell

Binary Quadratic Forms

Classical Theory and Modern Computations

Springer-Verlag
New York Berlin Heidelberg
London Paris Tokyo Hong Kong

Chapter 3

Indefinite Forms

3.1 Reduction, Cycles

We now consider the indefinite forms, that is, the forms of positive discriminant $\Delta = D > 0$. Our treatment will closely follow that of Mathews, our goal again being the determination of canonical forms for the equivalence classes. In the case of negative discriminants, the "reduced" forms are essentially unique in a given equivalence class. For positive discriminants, however, it is not only the case that many reduced forms can lie in the same class, an elegant structure is possessed by the reduced forms–they form cycles. An indefinite form $(a,\ b,\ c)$ of discriminant $D > 0$ is called *reduced* if

$$\begin{aligned} 0 < b < \sqrt{D} \qquad (3.1) \\ \sqrt{D} - b < 2 \mid a \mid < \sqrt{D} + b \end{aligned}$$

We make several easy deductions.

Proposition 3.1. *If* $(a,\ b,\ c)$ *is reduced, then* $\sqrt{D} - b < 2 \mid c \mid < \sqrt{D} + b$.

Proof. Since $b^2 - 4ac = D$, we have

$$(\sqrt{D} - b) \cdot (\sqrt{D} + b) = -4ac = (2 \mid a \mid) \cdot (2 \mid c \mid).$$

Since $0 < b < \sqrt{D}$, $\sqrt{D} - b < \sqrt{D} + b$. We have the situation $xy = zw$, with $x < z < y$, and it follows that $x < w < y$.

Proposition 3.2. *The number of reduced forms of a given discriminant is finite.*

Proof. The number of values for b has been limited, so the finite number of reduced forms follows from the finite number of factorings of $b^2 - D$ into $4ac$.

Proposition 3.3. *Any indefinite form is equivalent to a reduced form of the same discriminant.*

Proof. We give a reduction algorithm. If $(a,\ b,\ c)$ is not reduced, we choose δ (which in this case is necessarily unique) such that

$$\sqrt{D} - 2 \mid c \mid < -b + 2c\delta < \sqrt{D},$$

and we have

$$(a,\ b,\ c) \sim (c,\ -b + 2c\delta,\ a - b\delta + c\delta^2)$$

If $\mid a - b\delta + c\delta^2 \mid < \mid c \mid$, the process is repeated. As in the reduction of definite forms, the reduction process must be finite, terminating when we get a form $(A,\ B,\ C)$ such that $\mid A \mid \leq \mid C \mid$ and $\sqrt{D} - 2 \mid A \mid < B < \sqrt{D}$. If this is true, then $\sqrt{D} - B < 2 \mid A \mid$. Further, since

$$\mid \sqrt{D} - B \mid \cdot \mid \sqrt{D} + B \mid = 4 \mid A \mid\mid C \mid,$$

we must then have $| \sqrt{D} + B | > 2 | C |$. We continue the inequality:

$$| \sqrt{D} + B | > 2 | C | > 2 | A | > \sqrt{D} - B.$$

Looking at the left and right ends of this, we see that B must be positive, so that $0 < B < \sqrt{D}$ and $(A,\ B,\ C)$ is reduced.

We define two reduced forms $(a,\ b,\ a')$ and $(a',\ b',\ c')$ to be *adjacent* if $b + b' \equiv 0 \pmod{2a'}$. It is easy to see that there is a unique reduced form adjacent to the right and to the left of any given reduced form.

Once again, there is a strong computational similarity between the reduction algorithm and the standard algorithm for the greatest common divisor. As will be seen later in this chapter, more than a mere similarity exists. Reduction of definite forms is identical with the continued fraction expansion of a related quadratic irrational, and the continued fraction algorithm applied to a rational number is precisely the Euclidean algorithm.

Proposition 3.4. *The set of reduced forms of a given discriminant can be partitioned into cycles of adjacent forms.*

Proof. We begin with any reduced form and proceed to the right through successively adjacent reduced forms. Since the set of reduced forms is finite, the list of successively adjacent forms must return to the original form. If there are no more reduced forms, the process is finished; otherwise, we choose a form not yet used and repeat the process.

Since adjacent forms are equivalent, under the matrix transformation

$$\begin{pmatrix} 0 & -1 \\ 1 & \frac{b+b'}{2a} \end{pmatrix},$$

and equivalence is transitive, all forms in a given cycle are equivalent to each other.

Proposition 3.4 is the easy half of the following major theorem. The difficult half of the proof will be presented in Section 3.3 so as not to disturb the continuity of the discussion.

Theorem 3.5. *Two reduced forms are equivalent if and only if they are in the same cycle.*

We call the form $(a,\ -b,\ c)$ the *opposite* of the form $(a,\ b,\ c)$. An ambiguous form is equivalent to its own opposite, since if $b = ka$, the choice $\delta = k$ gives

$$(a,\ b,\ c) \sim (c,\ -b,\ a) \sim (a,\ b - 2a\delta,\ c - b\delta + a\delta^2) = (a,\ b,\ c).$$

We further define forms $(a,\ b,\ c)$ and $(c,\ b,\ a)$ to be *associated.* We note that opposite forms are improperly equivalent (obtainable one from another by a matrix transformation of determinant -1) under

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and its negative, and associated forms are improperly equivalent under

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and its negative.

Proposition 3.6. *The number of forms in any cycle, called the period of the cycle, is always even.*

Proof. The first and last coefficients of any reduced form are of opposite sign. We may therefore form pairs of adjacent forms $(a,\ b,\ c) \sim$

$(c,\ b',\ c')$ in which the coefficient c is negative and a and c' are positive. Because the adjacency is clearly an adjacency of these pairs, it takes an integral number of pairs to form any cycle.

Proposition 3.7. *If the form f', associate to f, is in a different cycle from that of f, then this is true for all forms in both cycles, which we call associated cycles.*

Proof. Cycling forward (to the right) from f, the form adjacent to $f = (a,\ b,\ c)$ is $(c,\ b',\ a')$. Cycling backward (to the left) from f' yields $(a',\ b',\ c) \sim (c,\ b,\ a)$. That is, cycling forward from f we encounter the associates of the forms encountered when cycling backward from f'.

Proposition 3.8. *A cycle which contains any ambiguous form contains exactly two and is its own associate. Conversely, a cycle which is its own associate contains exactly two ambiguous forms.*

Proof. If a form f and its associate f' are in the same cycle, then we can cycle forward from f and backward from f' through pairs of associated forms. Since the cycles have finite length, we must eventually arrive at adjacent associated forms $(a',\ b,\ a) \sim (a,\ b,\ a')$. Since these are adjacent, we have $b + b \equiv 0 \pmod{2a}$; that is, $a|b$, so that $(a,\ b,\ a')$ is ambiguous. Similarly, cycling backward from f and forward from f' will produce a different ambiguous form. A self-associate cycle thus contains two ambiguous forms. It cannot contain more since the cycle is complete when the second ambiguous form is found. And it is easy to see that a cycle which contains an ambiguous form must be self-associate since the form $(a,\ ak,\ c)$ is the form adjacent to its own associate $(c,\ ak,\ a)$.

We call the reduced form $(1,\ b,\ c)$ the *principal form* for a given discriminant, and the cycle in which it lies the *principal cycle.*

General Examples and Observations

For negative discriminants, reduced forms are, in general, asymmetric since the third coefficient is at least as large as the first. For positive discriminants, this is not true. Indeed, reduced forms occur in groups: for any given lead coefficient a the existence of one reduced form $(a,\ b,\ c)$ implies the existence of the reduced forms $(a,\ b,\ c)$, $(-a,\ b,\ -c)$, $(c,\ b,\ a)$, and $(-c,\ b,\ -a)$. Further, since solutions to $b^2 \equiv D \pmod{a}$ occur in pairs, we also have reduced forms $(a,\ -b+2a\sigma,\ a-b\sigma+c)$, $(-a,\ -b+2a\sigma,\ -a+b\sigma-c)$, $(a-b\sigma+c,\ -b+2a\sigma,\ a)$, and $(-a+b\sigma-c,\ -b+2a\sigma,\ -a)$, where σ is the sign of a. These generally lead to further forms, and so on. The following examples of cycles will illustrate the previous discussion.

For $D = 1173 = 3 \cdot 17 \cdot 23$ there are four cycles:

A) $(1,\ 33,\ -21) \sim (-21,\ 9,\ 13) \sim (13,\ 17,\ -17) \sim (-17,\ 17,\ 13) \sim (13,\ 9,\ -21) \sim (-21,\ 33,\ 1)$

B) $(-1,\ 33,\ 21) \sim (21,\ 9,\ -13) \sim (-13,\ 17,\ 17) \sim (17,\ 17,\ -13) \sim (-13,\ 9,\ 21) \sim (21,\ 33,\ -1)$

C) $(3,\ 33,\ -7) \sim (-7,\ 23,\ 23) \sim (23,\ 23,\ -7) \sim (-7,\ 33,\ 3)$

D) $(-3,\ 33,\ 7) \sim (7,\ 23,\ -23) \sim (-23,\ 23,\ 7) \sim (7,\ 33,\ -3)$

For $D = 1313 = 13 \cdot 101$ there are also four cycles:

A) $(1,\ 35,\ -22) \sim (-22,\ 9,\ 14) \sim (14,\ 19,\ -17) \sim (-17,\ 15,\ 16) \sim (16,\ 17,\ -16) \sim (-16,\ 15,\ 17) \sim (17,\ 19,\ -14) \sim (-14,\ 9,\ 22) \sim$

$(22,\ 35,\ -1) \sim (-1,\ 35,\ 22) \sim (22,\ 9,\ -14) \sim (-14,\ 19,\ 17) \sim (17,\ 15,\ -16) \sim (-16,\ 17,\ 16) \sim (16,\ 15,\ -17) \sim (-17,\ 19,\ 14) \sim$

$(14,\ 9,\ -22) \sim (-22,\ 35,\ 1)$

B) $(13,\ 13,\ -22) \sim (-22,\ 31,\ 4) \sim (4,\ 33,\ -14) \sim (-14,\ 23,\ 14) \sim$
$(14,\ 33,\ -4) \sim (-4,\ 31,\ 22) \sim (22,\ 13,\ -13) \sim (-13,\ 13,\ 22) \sim$
$(22,\ 31,\ -4) \sim (-4,\ 33,\ 14) \sim (14,\ 23,\ -14) \sim (-14,\ 33,\ 4) \sim$
$(4,\ 31,\ -22) \sim (-22,\ 13,\ 13)$

C) $(7,\ 23,\ -28) \sim (-28,\ 33,\ 2) \sim (2,\ 35,\ -11) \sim (-11,\ 31,\ 8) \sim$
$(8,\ 33,\ -7) \sim (-7,\ 23,\ 28) \sim (28,\ 33,\ -2) \sim (-2,\ 35,\ 11) \sim$
$(11,\ 31,\ -8) \sim (-8,\ 33,\ 7)$

D) $(7,\ 33,\ -8) \sim (-8,\ 31,\ 11) \sim (11,\ 35,\ -2) \sim (-2,\ 33,\ 28) \sim$
$(28,\ 23,\ -7) \sim (-7,\ 33,\ 8) \sim (8,\ 31,\ -11) \sim (-11,\ 35,\ 2) \sim$
$(2,\ 33,\ -28) \sim (-28,\ 23,\ 7)$

A. O. L. Atkin has provided a labelling of the different kinds of cycles. Although the reasons for the existence or nonexistence of such cycles for a given discriminant will not appear until later, this labelling is now presented as an observation about examples.

Type 11: The complete ambiguous cycle is
$(1,\ a,\ -1) \sim (-1,\ a,\ 1)$.

Type 21: The complete ambiguous cycle is
$(a,\ abn,\ b) \sim (b,\ abn,\ a)$.

Type 12: The ambiguous cycle contains
$(a,\ ab,\ c) \sim \cdots \sim (x,\ y,\ -x) \sim \cdots \sim (-a,\ ab,\ -c) \sim \cdots$.

Type 22: The ambiguous cycle contains
$(a,\ ab,\ c) \sim \cdots \sim (f,\ de,\ d) \sim \cdots$
but does not contain the form $(-a,\ ab,\ -c)$.

Type 20: The ambiguous cycle contains
$(x,\ y,\ -x) \sim \cdots \sim (w,\ z,\ -w) \sim \cdots$.

Type 23: The cycle, which is not ambiguous, contains twice an even number of forms.

Type 13: The cycle, which is not ambiguous, contains twice an odd number of forms.

For reasons to be explained in the next section, the negative Pell equation $x^2 - \Delta y^2 = -4$ is solvable exactly for discriminants Δ which have cycles of Types 11, 12, and/or 13. For odd discriminants, the first occurrences of the different types are given below.

11) Type 11, $D = 5$, the cycle being
$(1, 1, -1) \sim (-1, 1, 1)$;

21) Type 21, $D = 21$, the cycle being
$(1, 3, -3) \sim (-3, 3, 1)$;

12) Type 12, $D = 17$, the cycle being
$(1, 3, -2) \sim (-2, 1, 2) \sim (2, 3, -1) \sim (-1, 3, 2) \sim$
$(2, 1, -2) \sim (-2, 3, 1)$;

22) Type 22, $D = 33$, the cycle being
$(1, 5, -2) \sim (-2, 3, 3) \sim (3, 3, -2) \sim (-2, 5, 1)$;

20) Type 20, $D = 205$, the cycle being
$(7, 3, -7) \sim (-7, 11, 3) \sim (3, 13, -3) \sim (-3, 11, 7)$;

23) Type 23, $D = 321$, the cycle being
$(5, 9, -12) \sim (-12, 15, 2) \sim (2, 17, -4) \sim (-4, 15, 6) \sim$
$(6, 9, -10) \sim (-10, 11, 5)$;

13) Type 13, $D = 145$, the cycle being
$(3, 7, -8) \sim (-8, 9, 2) \sim (2, 11, -3) \sim (-3, 7, 8) \sim$
$(8, 9, -2) \sim (-2, 11, 3)$.

Examples

Δ	h	Cycles
8	1	$(1,2,-1)(-1,2,1)$
12	2	$(1,2,-2)(-2,2,1)$
		$(-1,2,2)(2,2,-1)$
20	1	$(1,4,-1)(-1,4,1)$
24	2	$(1,4,-2)(-2,4,1)$
		$(-1,4,2)(2,4,-1)$
28	2	$(1,4,-3)(-3,2,2)(2,2,-3)(-3,4,1)$
		$(-1,4,3)(3,2,-2)(-2,2,3)(3,4,-1)$
32	2	$(1,4,-4)(-4,4,1)$
		$(-1,4,4)(4,4,-1)$
40	2	$(1,6,-1)(-1,6,1)$
		$(2,4,-3)(-3,2,3)(3,4,-2)(-2,4,3)(3,2,-3)(-3,4,2)$
44	2	$(1,6,-2)(-2,6,1)$
		$(-1,6,2)(2,6,-1)$
48	2	$(1,6,-3)(-3,6,1)$
		$(-1,6,3)(3,6,-1)$
52	1	$(1,6,-4)(-4,2,3)(3,4,-3)(-3,2,4)(4,6,-1)$
		$(-1,6,4)(4,2,-3)(-3,4,3)(3,2,-4)(-4,6,1)$
5	1	$(1,1,-1)(-1,1,1)$
13	1	$(1,3,-1)(-1,3,1)$
17	1	$(1,3,-2)(-2,1,2)(2,3,-1)(-1,3,2)(2,1,-2)(-2,3,1)$
21	2	$(1,3,-3)(-3,3,1)$
		$(-1,3,3)(3,3,-1)$
29	1	$(1,5,-1)(-1,5,1)$
33	2	$(1,5,-2)(-2,3,3)(3,3,-2)(-2,5,1)$
		$(-1,5,2)(2,3,-3)(-3,3,2)(2,5,-1)$
37	1	$(1,5,-3)(-3,1,3)(3,5,-1)(-1,5,3)(3,1,-3)(-3,5,1)$
41	1	$(1,5,-4)(-4,3,2)(2,5,-2)(-2,3,4)(4,5,-1)$
		$(-1,5,4)(4,3,-2)(-2,5,2)(2,3,-4)(-4,5,1)$
45	2	$(1,5,-5)(-5,5,1)$
		$(-1,5,5)(5,5,-1)$
53	1	$(1,7,-1)(-1,7,1)$

3.2 Automorphs, Pell's Equation

The equation $x^2 - dy^2 = 1$, with d a fixed integer and x and y assumed to be integer variables, has been called Pell's equation, although this is, in fact, a misattribution due to Euler. We shall, in general, refer to the equations $x^2 - \Delta y^2 = \pm 4$ as *Pell's equations*, and the equation with only the minus sign as the *negative Pell equation*; we note that if Δ is a discriminant of binary quadratic forms, then the existence of a solution to the Pell equations implies the existence of a solution to $x^2 - \Delta y^2 = \pm 1$, where the $\pm$ signs correspond. We recall that an automorph of a binary quadratic form is a nontrivial transformation (1.1) of determinant $+1$ under which the form is equivalent to itself.

Theorem 3.9. *If Δ is any discriminant of binary quadratic forms, then there exists a solution (x, y) to the Pell equation*

$$x^2 - \Delta y^2 = 4. \tag{3.2}$$

There is a one-to-one correspondence between automorphs of (definite or indefinite) forms $(a,\ b,\ c)$ of discriminant Δ and solutions of the Pell equation (3.2).

Proof. We have defined the *principal root* of a form for positive definite forms; for indefinite forms the definition is identical:

$$\omega = \frac{-b + \sqrt{\Delta}}{2a}.$$

Now, if an automorph exists for a reduced form under a transformation (1.1), then

$$\omega = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}.$$

This can be rewritten as a quadratic equation in ω:

$$\gamma\omega^2 + \omega(\delta - \alpha) - \beta = 0.$$

But we already have $a\omega^2 + b\omega + c = 0$, and the form $(a,\ b,\ c)$ is assumed to be primitive, so we must have $\gamma = ka$, $\delta - \alpha = kb$, and $\beta = -kc$ for k an integer. This gives

$$(\delta - \alpha)^2 + 4\gamma\beta = \Delta k^2.$$

We reduce this to get

$$(\alpha + \delta)^2 - \Delta k^2 = 4.$$

Given any automorph of a reduced form, then, we have a solution of the Pell equation $x^2 - \Delta y^2 = 4$. Given any solution of that equation, conversely, we have integers

$$\begin{aligned} \alpha &= (x - by)/2, \\ \beta &= -cy, \\ \gamma &= ay, \\ \delta &= (x + by)/2, \end{aligned}$$

and an automorph of the form $(a,\ b,\ c)$. The correspondence between automorphs and solutions is clear; only the existence of solutions is yet in question.

If Δ is a negative discriminant, then the equation is solvable only for $\Delta = -3$ or -4, and, of course, only for $+1$ on the right-hand side. This case was covered in Chapter 2.

It is only necessary, then, to consider positive discriminants Δ. If we begin with the principal form of discriminant Δ and move through the principal cycle, we obtain transformation matrices which produce from a reduced form the equivalent adjacent reduced form. At some point we finish the cycle and return to the principal form. The product of all the transformation matrices is thus a transformation matrix which takes the principal form to itself. Since it cannot, except in trivial instances, be the identity matrix, it is the matrix of an automorph of the principal form. From this we get a solution to (3.2), and the theorem is proved. An example is given at the end of this chapter.

For the remainder of this chapter, only positive discriminants $\Delta = D$ are considered. Among all the solutions (X, Y) to (3.2), there exists one for which X and Y are positive and $(X + Y\sqrt{D})/2$ is of least magnitude. We call this the *fundamental solution* of (3.2), noting that if X' and Y' are positive and (X', Y') is another solution of (3.2), then $X < X'$ and $Y < Y'$ must also be true.

Theorem 3.10. *All pairs* (X_n, Y_n) *generated by*

$$\frac{(X + Y\sqrt{D})^n}{2^n} = \frac{X_n + Y_n\sqrt{D}}{2}, \quad n \geq 1 \tag{3.3}$$

are solutions of equation (3.2). All solutions of equation (3.2) in positive rational integers are given by (3.3).

Proof. That X_n and Y_n are rational integers follows by induction and observations about the parity of X, Y, and D. We then observe that

$$\frac{(X - Y\sqrt{D})^n}{2^n} = \frac{X_n - Y_n\sqrt{D}}{2} \tag{3.4}$$

and thus

$$\frac{X_n^2 - DY_n^2}{4} = \frac{(X^2 - DY^2)^n}{4^n} = 1.$$

This proves the first part. To prove the second part, assume that another solution (T, U) exists. Then there exists an $n \geq 1$ such that

$$\frac{(X + Y\sqrt{D})^n}{2^n} < \frac{T + U\sqrt{D}}{2} < \frac{(X + Y\sqrt{D})^{n+1}}{2^{n+1}}.$$

We multiply by the (positive) value $(X_n - Y_n\sqrt{D})/2$ and get

$$2 < T' + U'\sqrt{D} < X + Y\sqrt{D},$$

with $2T' = TX_n + UY_n$ and $2U' = TY_n + UX_n$. Again, by parity arguments, T' and U' are integral. Now, since $T' + U'\sqrt{D} > 2$ and $(T' + U'\sqrt{D}) \cdot (T' - U'\sqrt{D}) = 4$, we find $0 < T' - U'\sqrt{D} < 2$, which allows us to see that T' and U' are both positive. This, however, would contradict the fact that $(X + Y\sqrt{D})/2$ was the fundamental solution.

3.3 Continued Fractions and Indefinite Forms

We define a *continued fraction expansion* of x (cf) to be a function

$$x = f(a_0, \ldots, a_N) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_N}}}. \tag{3.5}$$

At present x may be any sort of number, although soon only rational numbers and real quadratic irrationals will be considered. We define the values a_i to be the *partial quotients* of the cf. The above cf will be abbreviated as

$$[a_0, \ldots, a_N],$$

whose *n-th convergent* is

$$R(n) = [a_0, \ldots, a_n], \quad 0 \leq n \leq N.$$

Theorem 3.11. *Defining*

$$\begin{aligned} P_{-1} &= 1 \\ P_0 &= a_0 \\ P_n &= a_n \cdot P_{n-1} + P_{n-2}, \ for\ n \geq 1, \end{aligned}$$

and

$$\begin{aligned} Q_{-1} &= 0 \\ Q_0 &= 1 \\ Q_n &= a_n \cdot Q_{n-1} + Q_{n-2}, \ for\ n \geq 1, \end{aligned}$$

then

$$R_n = [a_0, \ldots, a_n] = P_n/Q_n \text{ for } n \geq 0. \tag{3.6}$$

Proof. The theorem holds for $n = 0$. We assume that it holds for $n \leq m$ and calculate

$$\begin{aligned}
[a_0, \ldots, a_{m+1}] &= [a_0, \ldots, a_m + 1/a_{m+1}] \\
&= \frac{(a_m + 1/a_{m+1}) \cdot P_{m-1} + P_{m-2}}{(a_m + 1/a_{m+1}) \cdot Q_{m-1} + Q_{m-2}} \\
&= \frac{a_{m+1} \cdot (a_m P_{m-1} + P_{m-2}) + P_{m-1}}{a_{m+1} \cdot (a_m Q_{m-1} + Q_{m-2}) + Q_{m-1}} \\
&= \frac{a_{m+1} P_m + P_{m-1}}{a_{m+1} Q_m + Q_{m-1}} \\
&= \frac{P_{m+1}}{Q_{m+1}},
\end{aligned}$$

where the penultimate equality is by induction.

There are three other formulas of interest, all of which can be proved by direct calculation and/or recursion:

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}, \; n \geq 0, \tag{3.7}$$

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_n Q_{n-1}}, \; n \geq 0, \tag{3.8}$$

$$P_n Q_{n-2} - P_{n-2} Q_n = a_n (-1)^{n-1}, \; n \geq 1. \tag{3.9}$$

We now restrict ourselves to the case when each a_i, $i \geq 1$, is positive and integral. These are called *simple* continued fractions (scf's). In this

case any finite scf represents a rational number x. Before proving the converse, we define the

Continued Fraction Algorithm: Define a_i, X_i, and Z_i by

$$x = a_0 + Z_0, \text{chosen so that } 0 \le Z_0 < 1, \tag{3.10}$$
$$X_i = 1/Z_{i-1} = a_i + Z_i,\ i \ge 1,\ 0 \le Z_i < 1.$$

The algorithm continues as long as $Z_i \neq 0$. The (not necessarily integral) values X_i are the *i-th complete quotients* in the cf expansion, that is,

$$x = [a_0, \ldots, X_i].$$

Theorem 3.12. *Any rational number x has a representation as a finite simple continued fraction.*

Proof. We shall not prove this. The proof is straightforward; indeed it is a rephrasing of the usual algorithm for computing the greatest common divisor of the numerator and denominator of the rational number x.

Example: Let $x = 267/111$. Then computing in order a_0 , Z_0 , X_1 , a_1 , Z_1 , ..., and then P_i and Q_i afterwards, we have

i	a_i	P_i	Q_i	Z_i	X_i	$\mid P_i \cdot 111 - Q_i \cdot 267 \mid$
-1		1	0			111
0	2	2	1	45/111		45
1	2	5	2	21/45	111/45	21
2	2	12	5	3/21	45/21	3
3	7	89	37	0	21/3	0

We now have one more major list of facts.

Theorem 3.13. *Let $x = [a_0, \ldots, a_N]$ be a finite scf. Then*

a) $R_{2n} < R_{2n+2}$ *and* $R_{2n-1} > R_{2n+1}$ *for all* $n \geq 0$.

b) $R_{2n} < R_{2i+1}$ *for all* $n, i \geq 0$.

c) $R_{2n} < x$ *and* $R_{2n-1} > x$ *for all convergents except the last.*

d) $Q_n > Q_{n-1}$ *for all* $n > 1$

e) $\gcd(P_n, Q_n) = 1$ *for all* n.

Proof. *a)* Looking at (3.9), and remembering that the a_i and Q_i are all positive, we see that the right-hand side of (3.9) is positive or negative according as n is even or odd.
b) In (3.8), it is clear that $R_{2n} < R_{2n+1}$ for all n. If $R_{2n} > R_{2i+1}$ were to hold for some $n < i$, then $R_{2i} > R_{2i+1}$ would hold since by part a R_{2n} is an increasing sequence. Similarly, if $R_{2n} > R_{2i+1}$ were to hold for some $n > i$, then $R_{2n} > R_{2n+1}$ would hold since the R_{2n+1} are decreasing. These are both contradictions.
c) This is obvious. x has some value, which is larger than the even convergents and smaller than the odd ones, except for the equality which holds for the last.
d) This is evident from the defining equations of Theorem 3.12 and the new assumption that the a_i are positive.
e) In (3.7), the gcd of P_n and Q_n must divide either -1 or $+1$ and hence must be 1.

We now pass from finite scf's to infinite ones.

Theorem 3.14. *If a_0 is an integer and $a_1, \ldots, a_n, \ldots$ is any sequence*

of positive integers, then

$$x = \lim_{n\to\infty}[a_0, \ldots, a_n, \ldots]$$

exists, and is greater than any even convergent and smaller than any odd convergent.

Proof. The even convergents are increasing and the odd convergents are decreasing, so if the limit exists the rest must be true. But by (3.8) and Theorem 3.13d we have

$$| R_{n+1} - R_n | = \frac{1}{Q_n Q_{n+1}} < \frac{1}{{Q_{n+1}}^2}.$$

The right hand side goes to 0 as $n \to 0$, so the limit does exist.

From this point on, only *periodic* simple continued fractions are considered, that is, scf's for which $a_i = a_{i+J}$ for all $i \geq I$ and some fixed J. We write this as

$$[a_0, \ldots, a_{I-1}, {*a}_I, \ldots, {*a}_{I+J-1}],$$

with the * indicating the period. We can now, at last, prove one of the main theorems and return to the discussion of quadratic forms.

Theorem 3.15.

a) If ω is an irrational root of a quadratic equation with integer coefficients, then the scf for ω is periodic.

b) If an scf is periodic, then its value is an irrational root of a quadratic equation with integer coefficients.

Proof. *a)* Let ω be the root of

$$a\omega^2 + b\omega + c = 0,$$

where without loss of generality we have $a > 0$. Writing $D = b^2 - 4ac$, we can see that $Z_1 = (-B + \sqrt{D})/(2A)$ with $A > 0$, $0 < B < \sqrt{D}$, and $B^2 - D = 4AC$ for a positive integer C. From there it is clear that all of the Z_i are of this form. But this limits the values of B to a finite list, and consequently there are only finitely many values Z_i which occur. Clearly, then, the cf is periodic since the choice of Z_{i+1} from Z_i is unique.

b) Let $\omega = [a_0, \ldots, a_{I-1}, *a_I, \ldots, *a_{I+J-1}]$. Then, in the notation of (3.10), X_I is the value of the purely periodic part. If P'/Q' and P''/Q'' are the last two convergents of $[a_I, \ldots, a_{I+J-1}]$, then

$$X_I = [*a_I, \ldots, *a_{I+J-1}, X_I]$$

so that

$$X_I = \frac{P'X_I + P''}{Q'X_I + Q''}.$$

(The left-hand X_I is the value of the periodic scf; the right-hand X_I are from applying the defining recursions of the P and Q convergents.) Thus, X_I is a quadratic irrational, satisfying an equation with integer coefficients. Now, we can also write

$$x = \frac{P_{I-1}X_I + P_{I-2}}{Q_{I-1}X_I + Q_{I-2}},$$

and hence x is a quadratic irrational, satisfying an equation which can be seen to have integer coefficients.

We now return to our main topic. Given a discriminant of binary quadratic forms $D > 0$, we define $\omega = \sqrt{D/4}$, if D is even, and $\omega = (-1 + \sqrt{D})/2$, if D is odd. These are the principal roots of forms $(1,\ 0,\ -D/4)$ and $(1,\ 1,\ (1-D)/4)$, respectively, which forms we write

as $f = (1,\ b,\ (b-D)/4)$. Expanding the cf for ω produces $\omega = a_0 + Z_0$, with $0 \leq Z_0 < 1$ and a_0 an integer. Under the transformation

$$\begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix},$$

f becomes $(1,\ b+2a_0,\ *)$, where $b+2a_0 < \sqrt{D} < b+2a_0+2$. This form is thus reduced, with principal root Z_0. At this point, expansion of the cf and cycling through the principal cycle of forms of discriminant D are essentially the same.

Let us now consider the equivalences

$$(1,\ b,\ (b-D)/4) \sim (1 = c_0,\ b_0,\ c_1) \sim (c_1,\ b_1,\ c_2) \sim \ldots$$

under the action of the above transformations T_i. Then the sequences $Z_i = (-b_i + \sqrt{D})/(2c_i)$ and $X_i = (b_i + \sqrt{D})/(2c_{i+1})$ are clear. We have the following theorem.

Theorem 3.16. *If $M = T_0 \ldots T_i$ transforms $(1,\ b,\ (b-D)/4)$ into $(c_i,\ b_i,\ c_{i+1})$, then*

$$(2P_i + Q_i)^2 - DQ_i^2 = 4c_{i+1}.$$

Proof. The proof follows from writing

$$\omega = \frac{X_{n+1}P_n + P_{n-1}}{X_{n+1}Q_n + Q_{n-1}}.$$

The rest follows simply by calculation.

In the expansion of the cf it may happen that $(1,\ b,\ (D-b)/4)$ and $(-1,\ b,\ (b-D)/4)$ lie in the same cycle; if this is true, the cycle of

forms is twice as long as the period of the cf, with the cf cycle being repeated in the period of forms. If this happens, we choose to call the length of the cf period to be the same as the length as the cycle of forms. (This is the case in our example at the end of this chapter. The cf for $(-5+\sqrt{41})/2$ has a period of length 10 and not 5.) With this convention, we obtain two theorems which together give us the precise determination of the solutions to the Pell equations.

Theorem 3.17. *If the continued fraction expansion of* $\omega = (-1+\sqrt{D})/2$ *(for odd* D*) or of* $\omega = \sqrt{D}/2$ *(for even* D*) is of length* n*, and if* $P = P_{n-1}$ *and* $Q = Q_{n-1}$ *are the penultimate convergents in the first period of the expansion, then* $(X,Y) = (2P+Q, Q)$ *is the fundamental solution of (3.2).*

Proof. Clearly $(2P+Q, Q)$ is a solution, but then $(2P+Q+Q\sqrt{D})/2 = ((X_/+Y\sqrt{D})/2)^n$ for some n. Then the expansion of the cf for $(2P+Q+Q\sqrt{D})/2$ contains n copies of the cf for the fundamental solution of (3.2). But no such repetition can occur, except for the double period that occurs if, as mentioned above, the $(-1, *, **)$ form appears in the principal cycle; however, that would, by Theorem 3.16, provide a solution to $x^2 - Dy^2 = -4$.

The following theorem can now be proved by carefully combining previous results.

Theorem 3.18. *Let* $\Delta = D$ *be a positive discriminant of quadratic forms. Solutions to the Pell equation*

$$x^2 - Dy^2 = -4 \tag{3.11}$$

exist if and only if the reduced forms $(1,b,c)$ *and* $(-1,b,-c)$ *of discriminant* D *lie in the same cycle. If this is true, then*

a) the length of the continued fraction expansion of $\omega = (-1+\sqrt{D})/2$ *(for odd* D*) or of* $\omega = \sqrt{D}/2$ *(for even* D*) (which is the length of the cycle of forms) is an even integer* $2n$*;*

b) if $P = P_{n-1}$ *and* $Q = Q_{n-1}$ *are the penultimate convergents in the first half-period of the expansion, then* $(X, Y) = (2P + Q, Q)$ *is the solution of (3.11) for which* X *and* Y *are positive integers and* $(X + Y\sqrt{D})/2$ *is of least magnitude;*

c) all solutions to (3.11) are given by the odd powers of $(X+Y\sqrt{D})/2$*;*

d) all solutions to (3.2) are given by the even powers of $(X+Y\sqrt{D})/2$*; the fundamental solution to (3.2) is*

$$\left(\frac{X + Y\sqrt{D}}{2}\right)^2.$$

The solution to (3.11), if it exists, will be called the *fundamental solution* to that equation.

We now prove Theorem 3.5.

Theorem 3.5. *Two reduced forms are equivalent if and only if they are in the same cycle.*

Proof. Our proof, which follows closely that of Mathews, will take several steps. We define a continued fraction to be *regular* if all the partial quotients after the first are positive.

Proposition 3.19. *If an infinite cf contains only a finite number of nonpositive partial quotients, it can be converted in a finite number of steps to a regular cf.*

Proof. Let a_r be the last nonpositive partial quotient (pq).
Case i. $a_r = 0$.
Since $[x, 0, y, z] = [x + y, z]$, we have

$$[\ldots, a_{r-1}, 0, a_{r+1}, a_{r+2}, \ldots] = [\ldots, a_{r-1} + a_{r+1}, a_{r+2}, \ldots].$$

We note that this shifts the last nonpositive pq to the left.

Case ii. $a_r = -k \neq -1$.
It can be shown that

$$[\ldots, a_{r-1}, -k, a_{r+1}, \ldots] = [\ldots, a_{r-1} - 1, k - 2, 1, a_{r-1} - 1, \ldots].$$

Since a_r is the last nonpositive pq, $a_{r+1} - 1$ is nonnegative. If it is zero or if k is 2, the reduction of the previous case has the effect of shifting the last nonpositive pq to the left.
Case iii. $a_r = -1$.
Since $[\ldots, x, -1, y, \ldots] = [\ldots, x - 2, 1, y - 2, \ldots]$
and $[\ldots, x, -1, 1, y, z, \ldots] = [\ldots, x - y - 2, 1, z - 1, \ldots]$,
the last nonpositive pq is again shifted to the left.

We can thus shift the nonpositive terms to the left, eventually eliminating them entirely. In each case the number of partial quotients changes by zero or by two.

Proposition 3.20. *If* $y = (\alpha x + \beta)/(\gamma x + \delta)$ *for some transformation in the modular group* Γ, *then* y *can be written*

$$y = [\pm t, a_1, \ldots, a_{2r}, \pm u, x] \ ,$$

with $a_1, \ldots, a_{2r}$ *all positive.*

Proof. Let $\pm t$ be chosen so that $-(\pm t - \beta/\delta)$ is a positive proper fraction. We can expand β/δ into a cf with an odd number of partial

quotients $\beta/\delta = [\pm t, a_1, \ldots, a_{2r}]$. (We can make the length $2r+1$ since $[z] = [z-1, 1]$.) If P/Q is the penultimate convergent, then by (3.7), $\beta Q - \delta P = 1 = \alpha\delta - \beta\gamma$. Then $\alpha = P \pm u\beta$ and $\gamma = Q \pm u\delta$ for some integer u. Then
$\alpha/\gamma = [\pm t, a_1, \ldots, a_{2r}, \pm u]$.
Consequently,

$$y = \frac{\alpha x + \beta}{\gamma x + \delta} = [\pm t, a_1, \ldots, a_{2r}, \pm u, x].$$

We now prove Theorem 3.5. Let $f = (a,\ b,\ c)$ and $f' = (a',\ b',\ c')$ be two reduced equivalent forms. With no loss of generality for our purposes, we can choose a and a' positive so that the principal roots ω and ω' are positive proper fractions. Since the forms are equivalent, a transformation of the usual sort exists so that

$$\omega' = (\alpha\omega + \beta)/(\gamma\omega + \delta).$$

Then $\omega' = [\pm t, a_1, \ldots, a_{2r}, \pm u, \omega]$

$= [\pm t, a_1, \ldots, a_{2r}, \pm u + d_1, *d_2, \ldots, *d_1]$

if $[*d_1, \ldots, *d_{2m}]$ is the cf for ω. We may use Proposition 3.18 to make all the partial quotients after the first positive and then note that the first partial quotient is zero since ω' is a positive proper fraction. It is easy to show that a purely periodic cf is unique for a given quadratic irrational so that the periodic part of the expansion of ω' is merely a cyclic permutation of that for ω. Indeed, since the operations of Proposition 3.18 change the number of partial quotients by zero or two each time, the period for ω' is a shift of that for ω by an even number of partial quotients. (This is important since the first coefficients of adjacent forms alternate in sign; without the evenness of the permutation

we could not distinguish cycles from their associates.) Thus, by cycling forward from f we arrive at a reduced form whose principal root is ω'. But the principal root and the discriminant uniquely determine the form, so this form is f'.

We prove one final theorem which will be used later.

Theorem 3.21. *Let Δ be a positive discriminant of binary quadratic forms and p be any prime. In the notation of Theorem 3.9, we have that*

a) there exists an n such that $p \mid Y_n$;

b) the least positive residues modulo p of the integers (X_n, Y_n) form a periodic sequence.

Proof. We only prove this for odd primes p; the proof for $p = 2$ is similar. If Δ is a discriminant of forms, then so is Δp^2; therefore, a solution exists to the equation $x^2 - \Delta p^2 y^2 = 4$. Part a follows from the fact that this solution (x, py) to $x^2 - \Delta y^2 = 4$ must be one of the pairs (X_n, Y_n).

We have that

$$\begin{aligned} \frac{X_p + Y_p\sqrt{\Delta}}{2} &= \left(\frac{X_1 + Y_1\sqrt{\Delta}}{2}\right)^p \\ &\equiv \frac{X_1 + Y_1\Delta^{(p-1)/2}\sqrt{\Delta}}{2} \\ &\equiv \frac{X_1 + Y_1\left(\frac{\Delta}{p}\right)\sqrt{\Delta}}{2}, \end{aligned}$$

where the congruences are taken modulo p, and the symbol $\left(\frac{\Delta}{p}\right)$ is the quadratic residue symbol if p does not divide Δ and 0 if it does. We may thus define $\bar{X} \equiv X_1$ and $\bar{Y} \equiv \left(\frac{\Delta}{p}\right) Y_1$ to be least positive

residues of these congruences (mod p). It is clear that the powers $(X_1+Y_1\sqrt{\Delta})/2)^n$ produce a sequence congruent modulo p to the powers of $(\bar{X}+\bar{Y}\sqrt{\Delta})/2)^n$, and this sequence is recurrent.

Example.

Let $D = 41$. The cf expansion of $(-1+\sqrt{41})/2$ is

i	a_i	P_i	Q_i	Z_i	X_i
-1		1	0		
0	2	2	1	$(\sqrt{41}-5)/2$	
1	1	3	1	$(\sqrt{41}-3)/8$	$(\sqrt{41}+5)/8$
2	2	8	3	$(\sqrt{41}-5)/4$	$(\sqrt{41}+3)/4$
3	2	19	7	$(\sqrt{41}-3)/4$	$(\sqrt{41}+5)/4$
4	1	27	10	$(\sqrt{41}-5)/8$	$(\sqrt{41}+3)/8$
5	5	154	57	$(\sqrt{41}-5)/2$	$(\sqrt{41}+5)/2$
6	1	181	67	$(\sqrt{41}-3)/8$	$(\sqrt{41}+5)/8$
7	2	516	191	$(\sqrt{41}-5)/4$	$(\sqrt{41}+3)/4$
8	2	1213	449	$(\sqrt{41}-3)/4$	$(\sqrt{41}+5)/4$
9	1	1729	640	$(\sqrt{41}-5)/8$	$(\sqrt{41}+3)/8$
10	5	9858	3649	$(\sqrt{41}-5)/2$	$(\sqrt{41}+5)/2$

The cycle is completed, and the cf is [2, *1, 2, 2, 1, *5]. The effect on the forms is this, where the equivalences after the first are done with transformations

$$T_i = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix},$$

for which the δ are $-1, 2, -2, 1, -5, 1, -2, 2, -1$:

$$(1,1,-10) \sim (1,5,-4) \sim (-4,3,2) \sim (2,5,-2) \sim$$
$$(-2,3,4) \sim (4,5,-1) \sim (-1,5,4) \sim (4,3,-2) \sim$$
$$(-2,5,2) \sim (2,3,-4) \sim (-4,5,1).$$

The cumulative equivalence is achieved by the transformations computed as follows:

$$T_0 = \begin{pmatrix} P_{-1} & P_0 \\ Q_{-1} & P_0 \end{pmatrix}$$

$$\begin{aligned} T_0T_1 &= T_0\begin{pmatrix} 0 & -1 \\ 1 & -a_1 \end{pmatrix} \\ &= \begin{pmatrix} P_0 & -P_1 \\ Q_0 & -Q_1 \end{pmatrix} \\ T_0T_1T_2 &= \begin{pmatrix} -P_1 & -P_2 \\ -Q_1 & -Q_2 \end{pmatrix} \\ T_0T_1T_2T_3 &= \begin{pmatrix} -P_2 & P_3 \\ -Q_2 & Q_3 \end{pmatrix} \\ T_0T_1T_2T_3T_4 &= \begin{pmatrix} P_3 & P_4 \\ Q_3 & Q_4 \end{pmatrix}. \end{aligned}$$

Thus, for example, $(1,1,-10) \sim (2,5,-2)$ under

$$\begin{pmatrix} -3 & -8 \\ -1 & -3 \end{pmatrix}.$$

We see that $(1,5,-4) \sim (-1,5,4)$ under

$$\begin{pmatrix} 7 & -40 \\ 10 & -57 \end{pmatrix}.$$

This provides us with the solution $64^2 - 41 \cdot 10^2 = -4$, which is the fundamental solution for (3.11). Continuing to the end of the cycle, we find that $(1,5,-4)$ first becomes equivalent to itself under

$$\begin{pmatrix} -449 & -2560 \\ -640 & -3649 \end{pmatrix}.$$

From this we get the solution $4098^2 - 41 \cdot 640^2 = 4$, which is the fundamental solution for (3.2).