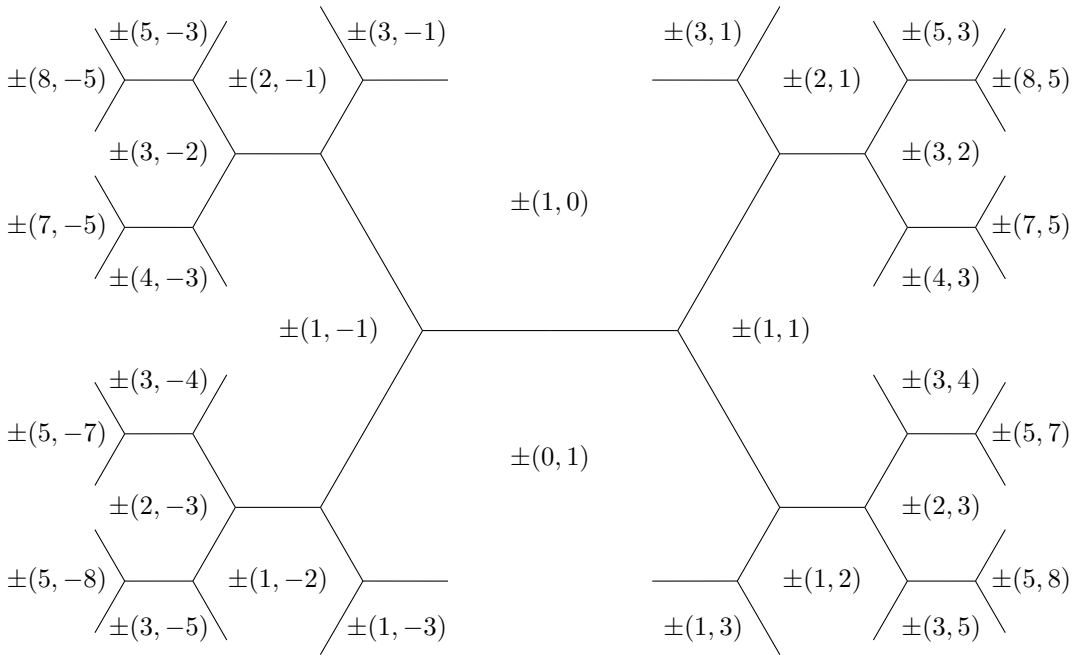
Quadratic Forms

These notes develop the theory of quadratic forms from the perspective of Conway's topograph.

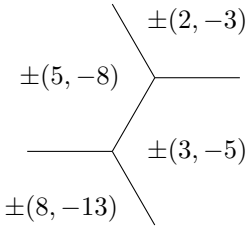
1 Conway's Topograph

Definition 1. A (binary integral) **quadratic form** is a function $f(x, y) = ax^2 + hxy + by^2$ with integer coefficients $a, b, h \in \mathbb{Z}$.

One of our goals will be to understand the values $f(v)$ at integer vectors $v \in \mathbb{Z}^2$. But $f(rv) = r^2 f(v)$, so it will be enough to understand the values $f(v)$ at the **primitive vectors**, those satisfying $\gcd(x, y) = 1$. And we have $f(-v) = f(v)$, so we will combine the primitive vectors v and $-v$ into a single object denoted $\pm v$ which Conway calls a **lax vector**. These lax vectors can be arranged geometrically as cells of a tree.

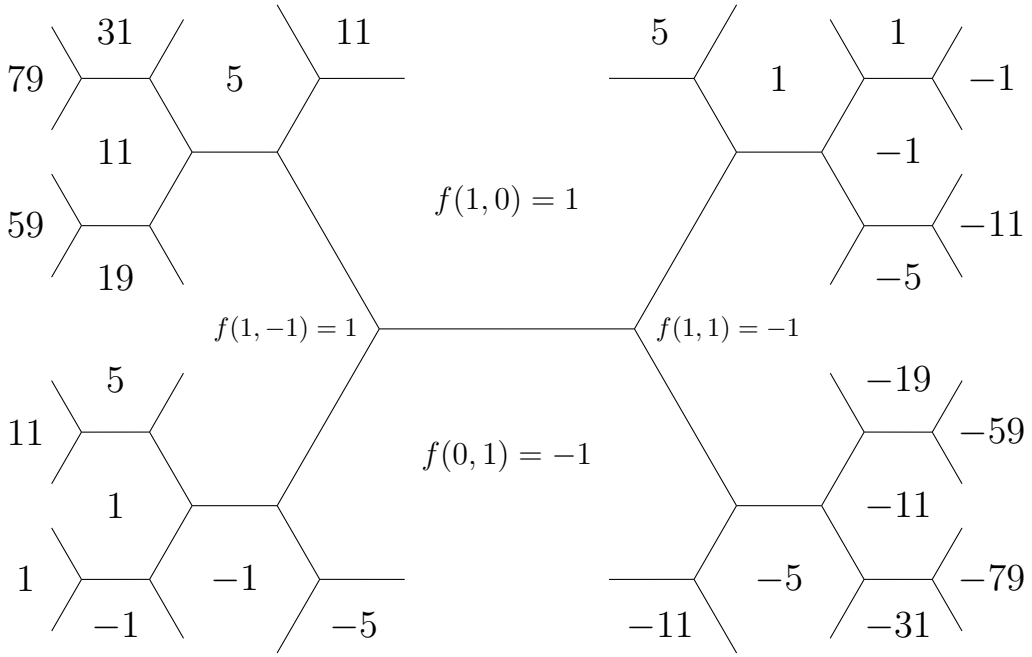


The lax vectors are arranged so that if $\pm v$ and $\pm w$ are neighbors on either side of an edge, then the lax vectors at the ends of the edge are $\pm(v + w)$ and $\pm(v - w)$. This then gives a recipe for extending the tree further. For instance, if we want to extend the tree one step further in the southwest direction, we look at the lax vectors $\pm(5, -8)$ and $\pm(3, -5)$. The lax vector at one end of the edge is the subtraction $\pm(2, -3)$, so the lax vector at the other end of the edge should be the addition $\pm(8, -13)$.



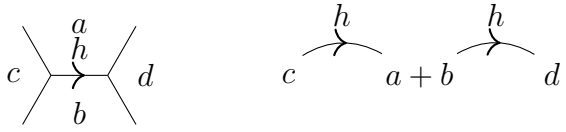
It is not obvious that extending the tree by iterating this recipe will produce every lax vector without duplicates. A proof can be found in the first chapter of *The Sensual (quadratic) Form* by John H. Conway. Plugging the tree of lax vectors into a quadratic form $f(x, y)$ results in the **topograph** of $f(x, y)$.

Example 2. Plugging the tree of lax vectors into the quadratic form $f(x,y) = x^2 - xy - y^2$ gives the topograph of $f(x,y) = x^2 - xy - y^2$.



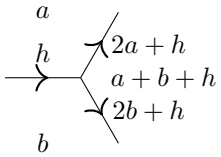
$$f(x,y) = x^2 - xy - y^2$$

It is quite tedious to first compute the tree of lax vectors and then plug each one into the quadratic form. Luckily, there is a shortcut called the **arithmetic progression rule**. If a and b are neighbors on either side of an edge, and if c and d are at the ends of the edge, then the sequence c, $a+b$, d forms an arithmetic progression. We will often draw an arrow in the positive direction labeled with the common difference h.



For example, the northwest corner of Example 2 has an arithmetic progression 5, 42, 79 with common difference 37. Solving for whichever of c or d is unknown gives a recipe for extending the topograph further. As we extend the topograph by iterating this recipe, each new value on the topograph will only depend on the preceeding three values. In particular, if the same three values show up again in the same configuration later on, then the topograph will be periodic in that direction. This explains why the 1's and -1's keep repeating in the northeast and southwest corners of Example 2.

To explain the increasingly large values in the northwest and southeast corners of Example 2, consider what happens when two positive values $a > 0$ and $b > 0$ are neighbors on either side of an edge labeled with h. By the arithmetic progression rule, the value at the end of that edge in the direction of the arrow will be $a + b + h$, and the two edges that branch off will be labeled with $2a + h$ and $2b + h$.



These two branches are in the same situation as we started with, only with larger values. By iterating this analysis, we can see that following the arrows forward will result in increasingly large values with the arrows continuing to point away from where we started. This is known as the **climbing lemma**. There is also a negative version which states that if two negative values are neighbors on either side of an edge, then following the arrows backwards will result in increasingly negative values with the arrows continuing to point back towards where we started.

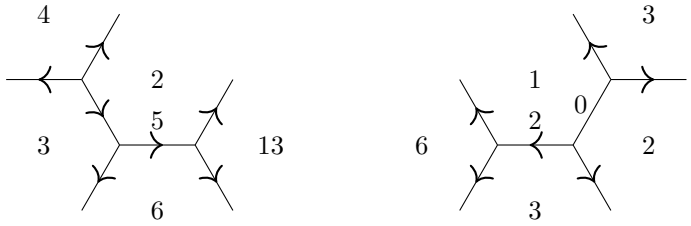
2 Topographic Features

We can classify quadratic forms by what values appear on their topograph. For example, we will say that a quadratic form has type 0+ if its topograph has both zero and positive values but no negative values. Under this classification, the seven possible types are +, −, +−, 0+−, 0+, 0−, and 0.

2.1 Wells

Suppose that a quadratic form has type +. This means that the topograph only has positive values. The climbing lemma says that following the arrows forward will result in increasingly large values. So following the arrows backward will result in increasingly small values. But these positive integer values cannot decrease forever, so we must eventually reach a vertex with no inward arrow to follow backwards. There are two possibilities. Either all three edges have outward arrows (a **simple well**) or one edge is labeled with 0 and all four edges branching off of it have outward arrows (a **double well**).

Example 3. By following the arrows backward, we find that the topograph of f_1 has a simple well, and the topograph of f_2 has a double well.



$f_1(x, y) = 2x^2 + 5xy + 6y^2$ $\qquad$ $f_2(x, y) = x^2 - 2xy + 3y^2$

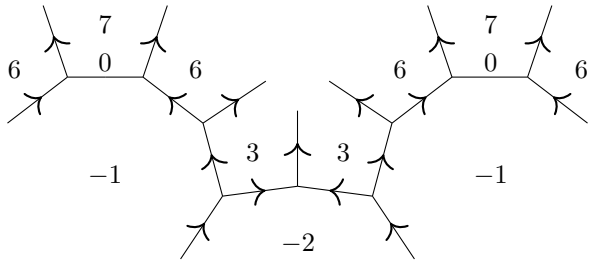
The climbing lemma tells us that following the arrows forward away from the well will result in increasingly large values with the arrows continuing to point away from the well. In particular, there will never be another well, so the well is unique.

The same analysis holds for quadratic forms of type −, except with the arrows reversed. If a quadratic form has type −, then it has a unique well, either a simple well with three inward arrows or a double well with a zero-edge and four inward arrows.

2.2 Rivers

Now suppose that a quadratic form has type +−. This means that the topograph has both positive and negative values, but zero does not appear. Then somewhere on the topograph there must be a positive value neighboring a negative value on either side of an edge. This edge can be extended into an infinite **river** by repeatedly following the branch that stays between a positive value and a negative value.

Example 4. The topograph of f has an infinite river. By following the river, we eventually see the values start to repeat, so the river is periodic. We will show later that every infinite river is eventually periodic.

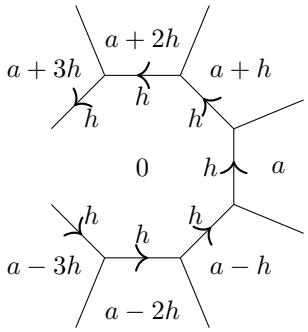


$f(x, y) = 7x^2 - y^2$

A river has a positive side and a negative side. On the positive side, the climbing lemma tells us that following the arrows forward away from the river will result in increasingly large values with the arrows continuing to point away from the river. On the negative side, the climbing lemma tells us that following the arrows backward away from the river will result in increasingly negative values with the arrows continuing to point back towards the river. In particular, there cannot be another river, so the river is unique.

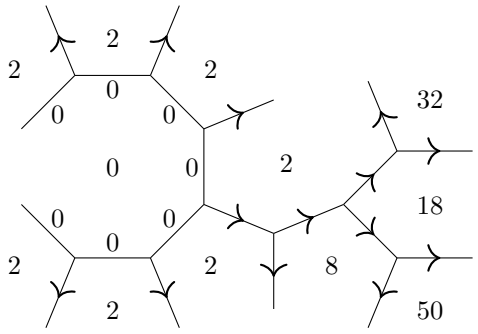
2.3 Lakes

The remaining types that we must study are 0+−, 0+, 0−, and 0, all of which feature a region with value zero. A region with value zero is called a **lake**. The arithmetic progression rule implies that the arrows around a lake are all labeled with the same value h, and that the values around a lake form an arithemetic progression with constant difference h.



If $h = 0$ and $a > 0$, then the topograph has a single lake surrounded by positive values. If $h = 0$ and $a < 0$, then the topograph has a single lake surrounded by negative values. If $h = 0$ and $a = 0$, then the topograph is the zero topograph consisting entirely of lakes.

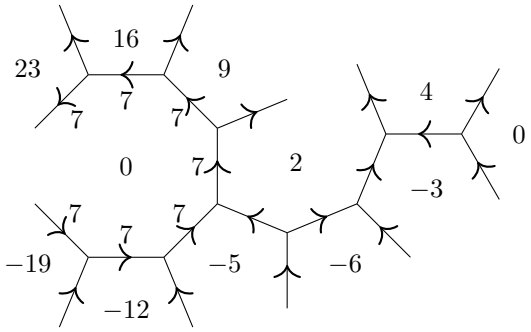
Example 5. The topograph of f has a single lake surrounded by positive values of the form $2n^2$.



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

If $h \neq 0$, then at some point around the lake the arithmetic progression will cross over from negative values to positive values. This will spawn a river that can be followed. As mentioned in Example 4, every infinite river is eventually periodic, necessarily in both directions. But a river that starts at a lake cannot be periodic in both directions, so it must eventually end, and the only way it can end is at another lake.

Example 6. The topograph of f has a lake that spawns a river that ends at another lake.



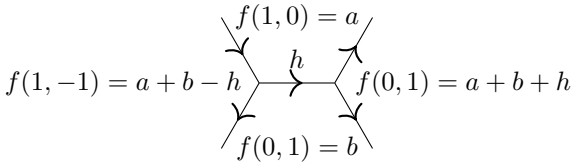
$$f(x, y) = 16x^2 - 7xy$$

One final possibility is that the arithmetic progression around the lake includes the value zero rather than skipping over zero when crossing over from negative values to positive values. This will result in two adjacent lakes, which Conway calls a **weir**. This can be viewed as the degenerate case where the two lakes are connected by a river of length zero.

2.4 The Discriminant

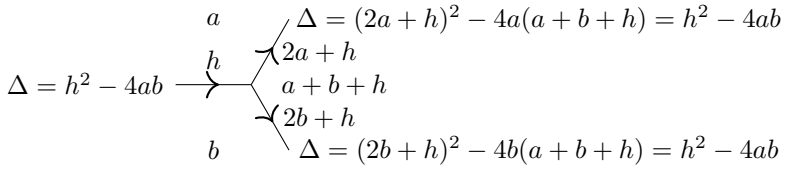
Definition 7. The **discriminant** of a quadratic form $f(x, y) = ax^2 + hxy + by^2$ is $\Delta = h^2 - 4ab$.

The coefficients a, b, and h appearing in the discriminant formula $\Delta = h^2 - 4ab$ also appear on the topograph as the values $f(1, 0)$ and $f(0, 1)$ and the label h of the arrow between them.

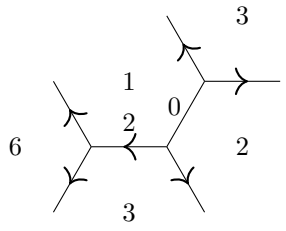


$$f(x, y) = ax^2 + hxy + by^2$$

Thus, the discriminant can be computed directly from these values of a, b, and h appearing at the starting edge of the topograph. But in fact, the same discriminant formula $\Delta = h^2 - 4ab$ can actually be applied to the values of a, b, and h at any edge of the topograph, always giving the same answer. To verify this, it is enough to check that the discriminant formula gives the same answer after a single step in any direction.

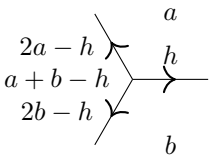


Example 8. The quadratic form $f(x,y) = x^2 - 2xy + 3y^2$ has discriminant $\Delta = (-2)^2 - 4 \cdot 1 \cdot 3 = -8$, but we can also compute the discriminant at the zero-edge as $\Delta = 0^2 - 4 \cdot 1 \cdot 2 = -8$, giving the same answer.



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

Since the discriminant can be computed at any edge of the topograph, we now study what happens when the discriminant is computed at a well, a river, or a lake. In the case of a well, suppose that the smallest arrow at the well is labeled with $h \geq 0$, with $h = 0$ corresponding to the case of a double well.

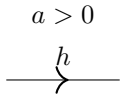


The minimality of h gives the inequalities $h \leq 2a - h$ and $h \leq 2b - h$. Equivalently, $a \geq h$ and $b \geq h$. Then evaluating the discriminant formula $\Delta = h^2 - 4ab$ at this minimal edge gives the constraints

$$\Delta = h^2 - 4ab \leq h^2 - 4h^2 = -3h^2 \leq 0, \qquad 0 \leq h \leq \sqrt{-\Delta/3}, \qquad ab = \frac{-\Delta + h^2}{4}. \tag{1}$$

But $\Delta = 0$ would require $h = 0$ and $ab = 0$, which is impossible since then the topograph would have a lake. Thus, a topograph with a well must have $\Delta < 0$.

In the case of a river, consider a river segment with $a > 0$ and $b < 0$. Here we allow h to be zero, or even negative, with negative values of h corresponding to an arrow in the opposite direction.



Then evaluating the discriminant formula $\Delta = h^2 - 4ab$ at this river segment gives the constraints

$$\Delta = h^2 - 4ab = h^2 + 4a(-b) > 0, \qquad |h| < \sqrt{\Delta}, \qquad a(-b) = \frac{\Delta - h^2}{4}. \tag{2}$$

Thus, a topograph with a river must have $\Delta > 0$. One important observation is that the constraints $|h| < \sqrt{\Delta}$ and $a(-b) = (\Delta - h^2)/4$ show that for a fixed discriminant $\Delta > 0$, there are only finitely many possible river segments with $a > 0$, $b < 0$, and h satisfying $h^2 - 4ab = \Delta$. So if a river goes on long enough, eventually a river segment must be re-used, at which point the river becomes periodic in both directions. This proves our claim in Example 4 that every infinite river is eventually periodic.

In the case of a lake, computing the discriminant at an edge along the lake gives $\Delta = h^2$. Conversely, if the discriminant $\Delta = h^2 - 4ab$ of a quadratic form $f(x,y) = ax^2 + hxy + by^2$ is a perfect square, then the quadratic formula gives a nonzero rational solution $(x,y) \in \mathbb{Q}^2$ to the equation $f(x,y) = 0$. Rescaling gives a primitive lattice point $(x,y) \in \mathbb{Z}^2$ with $f(x,y) = 0$, corresponding to a lake on the topograph. Thus, a topograph has a lake if and only if the discriminant is a perfect square.

Our classification of topographs is summarized in the following table, along with the more traditional nomenclature for the various cases.

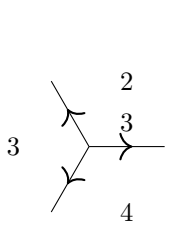
type	topographic features	standard terminology	discriminant
$+$	well (simple or double)	positive definite	$\Delta < 0$
$-$	well (simple or double)	negative definite	$\Delta < 0$
$+-$	infinite periodic river	indefinite	$\Delta > 0$, not a perfect square
$0+-$	two lakes, finite river	indefinite	$\Delta > 0$, a perfect square
$0+$	one lake, no river	positive semidefinite	$\Delta = 0$
$0-$	one lake, no river	negative semidefinite	$\Delta = 0$
0	entirely lakes	zero	$\Delta = 0$

One defect of the standard terminology is that it fails to distinguish between type $+-$ and type $0+-$. But as we have seen, these cases are sufficiently distinct to warrant independent interest.

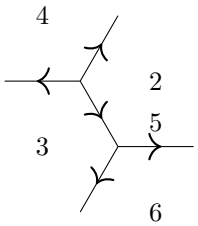
3 Equivalence

Definition 9. Two topographs are said to be **equivalent** if they differ by rotation and translation. Two quadratic forms $f(x, y)$ and $g(x, y)$ are said to be **equivalent** if their topographs are equivalent.

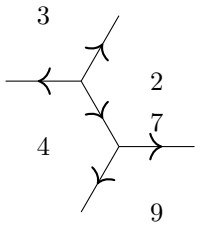
Example 10. The topographs of f_1 and f_3 both have a simple well surrounded by the values 4, 3, 2 clockwise. These simple wells will generate equivalent topographs. Therefore, f_1 and f_3 are equivalent. The topograph of f_2 has a simple well surrounded by the values 4, 3, 2 counterclockwise. This simple well will generate the mirror image of the other two topographs. So the topograph of f_2 will differ from the topographs of f_1 and f_3 by reflection, but not by rotation and translation. Therefore, f_2 is not equivalent to f_1 and f_3.



$f_1(x, y) = 2x^2 + 3xy + 4y^2$

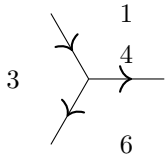


$f_2(x, y) = 2x^2 + 5xy + 6y^2$

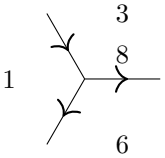


$f_3(x, y) = 2x^2 + 7xy + 9y^2$

Example 11. The topograph of f_1 has a vertex surrounded by the values 6, 3, 1 clockwise. The topograph of f_2 has a vertex surrounded by the values 6, 3, 1 counterclockwise. These two topographs will be reflections of each other, so you might be tempted to conclude that f_1 and f_2 are not equivalent.

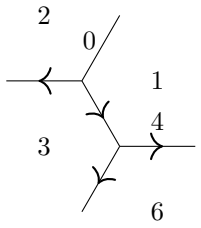


$f_1(x, y) = x^2 + 4xy + 6y^2$

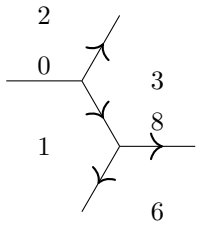


$f_2(x, y) = 3x^2 + 8xy + 6y^2$

But, if we explore a little more of each topograph, then we see that these two topographs both have a double well bordered by the values 1 and 2. So f_1 and f_2 are actually equivalent! The subtlety is that mirror image topographs will actually be equivalent whenever the topograph in question has reflectional symmetry.



$f_1(x, y) = x^2 + 4xy + 6y^2$



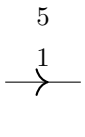
$f_2(x, y) = 3x^2 + 8xy + 6y^2$

All this fuss about reflection might lead you to wonder why we decided to disallow reflection in the first place. In fact, historically, Lagrange and Legendre did consider mirror image topographs as equivalent. It was only later that Gauss realized the importance of only distinguishing mirror image topographs. Gauss discovered that equivalence classes of primitive quadratic forms of a given discriminant form a finite abelian group in which reflection corresponds to inversion. Declaring mirror image topographs to be equivalent would have the effect of identifying inverse elements of the group, but this would destroy the group structure.

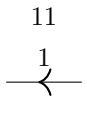
Algorithm 12. To determine whether two quadratic forms are equivalent:

1. First check whether they have the same discriminant Δ.
2. If $\Delta < 0$, then check whether their wells differ by rotation and translation.
3. If $\Delta > 0$, then check whether their rivers differ by rotation and translation.
4. If $\Delta = 0$, then check whether their lakes are surrounded by the same value.

Example 13. The quadratic forms f_1 and f_2 have the same discriminant $\Delta = 221 > 0$. To determine whether f_1 and f_2 are equivalent, we must check whether their rivers differ by rotation and translation.

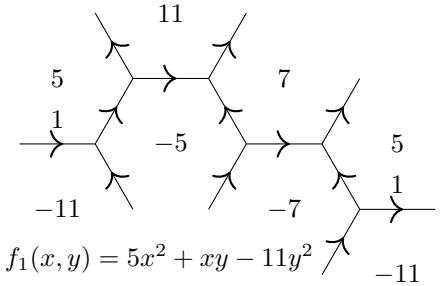


$f_1(x, y) = 5x^2 + xy - 11y^2$



$f_2(x, y) = 11x^2 - xy - 5y^2$

After traversing an entire period of the river of f_1, we can see that the river segment of f_2 does not appear anywhere along the river of f_1. Therefore, f_1 and f_2 are not equivalent.



$f_1(x, y) = 5x^2 + xy - 11y^2$

4 Classification

We now study the set of equivalence classes of quadratic forms of a fixed discriminant Δ. This set will be finite whenever $\Delta \neq 0$.

Theorem 14. *The number of equivalence classes of quadratic forms of a given discriminant $\Delta \neq 0$ is finite.*

Proof. If $\Delta < 0$, then the topograph has a well. The constraints $0 \leq h \leq \sqrt{-\Delta/3}$ and $ab = (-\Delta+h^2)/4$ from (1) show that there are only finitely many possibilities for the well, and hence only finitely many possibilities for the topograph, up to equivalence.

If $\Delta > 0$ is not a perfect square, then the topograph has an infinite periodic river. The constraints $|h| < \sqrt{\Delta}$ and $a(-b) = (\Delta - h^2)/4$ from (2) show that there are only finitely many possibilities for a river segment, and hence only finitely many possibilities for the topograph, up to equivalence.

If $\Delta > 0$ is a perfect square, then the topograph has two lakes connected by a finite river. If we concentrate on the lake whose values increase clockwise, then these values constitute an arithmetic progression with common difference $\sqrt{\Delta}$. There are exactly $\sqrt{\Delta}$ possibilities for this arithmetic progression, and hence exactly $\sqrt{\Delta}$ possibilities for the topograph, up to equivalence. □

The proof of Theorem 14 reveals an algorithm for classifying quadratic forms of a given discriminant.

Algorithm 15. To classify equivalence classes of quadratic forms of discriminant Δ:

1. If $\Delta < 0$, then classify all wells by finding all integer solutions to $ab = (-\Delta + h^2)/4$ with $a \geq h$, $b \geq h$, and $0 \leq h \leq \sqrt{-\Delta/3}$. But be careful to check your final list for duplicates since swapping a and b will result in an equivalent quadratic form whenever $h = a$, $h = b$, or $h = 0$. This will only classify the positive definite quadratic forms, but their negatives will classify the negative definite quadratic forms.

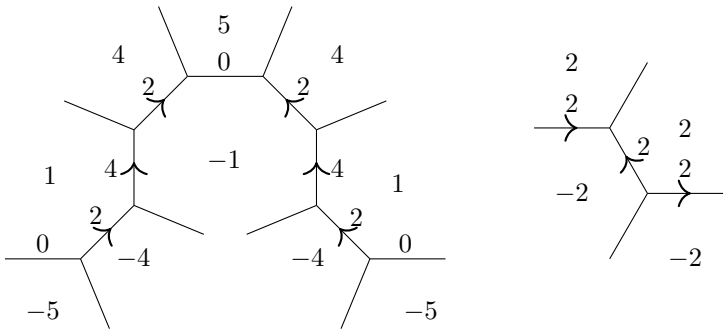
2. If $\Delta > 0$ is not a perfect square, then classify all river segments by finding all integer solutions to $a(-b) = (\Delta - h^2)/4$ with $a > 0$ and $b < 0$. Follow the rivers generated by these river segments until they start to repeat. Each river will give an equivalence class of quadratic forms of discriminant Δ.

3. If Δ is a perfect square, then the values around the clockwise lake will constitute a single congruence class modulo $\sqrt{\Delta}$. There is one equivalence class for each congruence class modulo $\sqrt{\Delta}$. In fact, this remains true for $\Delta = 0$ if you keep in mind that a congruence class modulo 0 consists of a single integer.

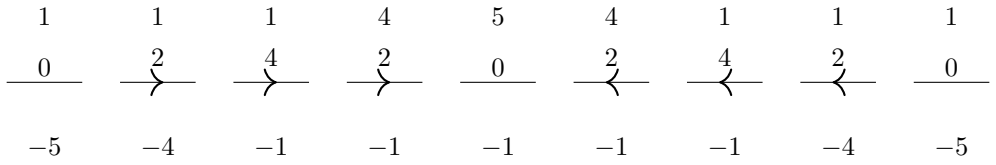
Example 16. To classify quadratic forms of discriminant $\Delta = 20$, we run through the possible values for h in the range $|h| \leq \sqrt{\Delta}$ satisfying $h \equiv \Delta \pmod 2$. For $\Delta = 20$, the possible values for h are $h = 0$, $h = \pm 2$, and $h = \pm 4$. For each value of h, we must find all factorizations $a(-b) = (\Delta - h^2)/4$. The resulting possibilities for a, b, and h are listed in the following table.

h	a	b
0	1	-5
0	5	-1
± 2	1	-4
± 2	2	-2
± 2	4	-1
± 4	1	-1

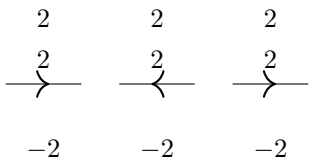
Following the rivers generated by these 10 river segments results in 2 periodic rivers.



The first river has period 8, using up all but 2 of the river segments.



The remaining 2 river segments form one short period that alternates between the two river segments.

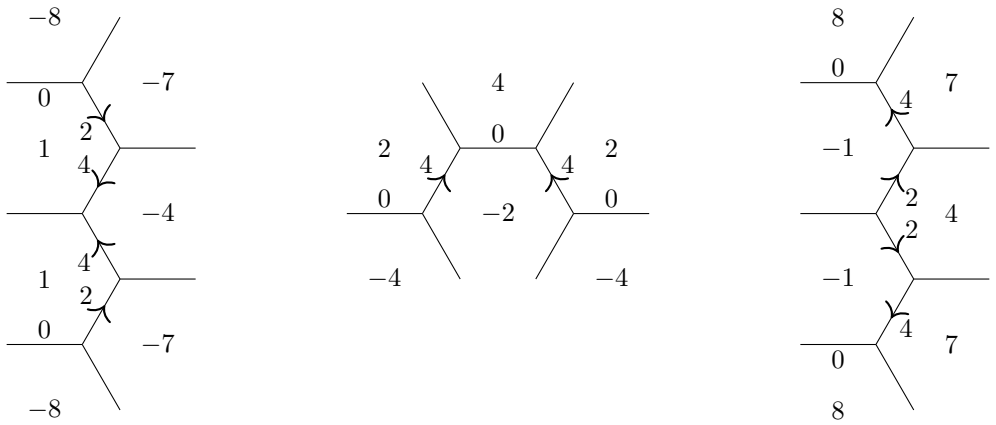


Thus, there are exactly two equivalence classes of quadratic forms of discriminant $\Delta = 20$, represented by $x^2 - 5y^2$ and $2x^2 + 2xy - 2y^2$.

Example 17. To classify quadratic forms of discriminant $\Delta = 32$, we run through the possible values for h in the range $|h| \leq \sqrt{\Delta}$ satisying $h \equiv \Delta \pmod 2$. For $\Delta = 32$, the possible values for h are $h = 0$, $h = \pm 2$, and $h = \pm 4$. For each value of h, we must find all factorizations $a(-b) = (\Delta - h^2)/4$. The resulting possibilities for a, b, and h are listed in the following table.

h	a	b
0	1	−8
0	2	−4
0	4	−2
0	8	−1
±2	1	−7
±2	7	−1
±4	1	−4
±4	2	−2
±4	4	−1

Following the rivers generated by these 14 river segments results in 3 periodic rivers.

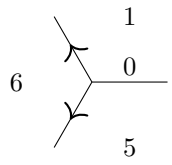


Thus, there are exactly three equivalence classes of quadratic forms of discriminant $\Delta = 32$, represented by $x^2 - 8y^2$, $2x^2 - 4y^2$, and $8x^2 - y^2$.

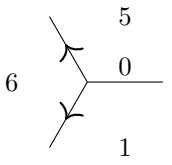
Example 18. To classify positive definite quadratic forms of discriminant $\Delta = -20$, we run through the possible values for h in the range $0 \leq h \leq \sqrt{-\Delta/3}$ satisfying $h \equiv \Delta \pmod 2$. For $\Delta = -20$, the possible values for h are $h = 0$ and $h = 2$. For each of value of h, we must find all factorizations $ab = (-\Delta + h^2)/4$ with $a \geq h$ and $b \geq h$. The resulting possibilities for a, b, and h are listed in the following table.

h	a	b
0	1	5
0	5	1
2	2	3
2	3	2

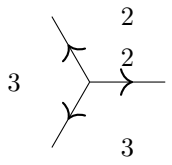
Of these 4 possibilities, $5x^2+y^2$ is equivalent to x^2+5y^2, and $3x^2+2xy+2y^2$ is equivalent to $2x^2+2xy+3y^2$.



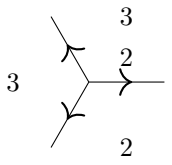
$x^2 + 5y^2$



$5x^2 + y^2$



$2x^2 + 2xy + 3y^2$



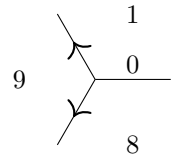
$3x^2 + 2xy + 2y^2$

Thus, there are exactly two equivalence classes of positive definite quadratic forms of discriminant $\Delta = -20$, represented by $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$.

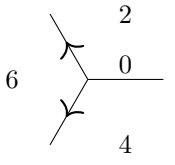
Example 19. To classify positive definite quadratic forms of discriminant $\Delta = -32$, we run through the possible values for h in the range $0 \leq h \leq \sqrt{-\Delta/3}$ satisfying $h \equiv \Delta \pmod 2$. For $\Delta = -32$, the possible values for h are $h = 0$ and $h = 2$. For each of value of h, we must find all factorizations $ab = (-\Delta + h^2)/4$ with $a \geq h$ and $b \geq h$. The resulting possibilities for a, b, and h are listed in the following table.

h	a	b
0	1	8
0	2	4
0	4	2
0	8	1
2	3	3

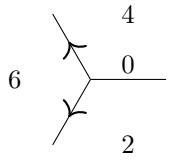
Of these 5 possibilities, $4x^2 + 2y^2$ is equivalent to $2x^2 + 4y^2$, and $8x^2 + y^2$ is equivalent to $x^2 + 8y^2$.



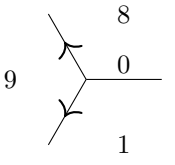
$x^2 + 8y^2$



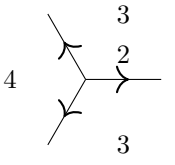
$2x^2 + 4y^2$



$4x^2 + 2y^2$



$8x^2 + y^2$



$3x^2 + 2xy + 3y^2$

Thus, there are exactly three equivalence classes of positive definite quadratic forms of discriminant $\Delta = -32$, represented by $x^2 + 8y^2$, $2x^2 + 4y^2$, and $3x^2 + 2xy + 3y^2$.

5 The Class Group

We now seek to define a group operation on equivalence classes of quadratic forms of a fixed non-square discriminant Δ. But we will need to restrict our attention to quadratic forms with coprime coefficients.

Definition 20. A quadratic form $ax^2 + hxy + by^2$ is said to be **primitive** if $\gcd(a, b, h) = 1$.

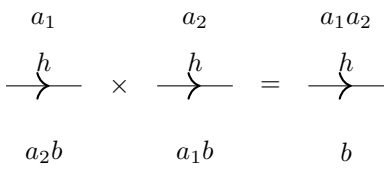
Definition 21. For $\Delta < 0$, the **class group** of discriminant Δ is the set of equivalence classes of primitive positive definite quadratic forms of discriminant Δ. For non-square $\Delta > 0$, the **class group** of discriminant Δ is the set of equivalence classes of primitive indefinite quadratic forms of discriminant Δ.

The class group will denoted by $C(\Delta)$, and the cardinality $H(\Delta) = |C(\Delta)|$ is called the **class number**.

Example 22. From examples 16, 17, 18, and 19, we have $H(20) = 1$ and $H(32) = H(-20) = H(-32) = 2$.

The set $C(\Delta)$ is called the class group because it can be given the structure of a finite abelian group. But the group operation is quite subtle to define as we can only specify it on certain pairs of quadratic forms.

Definition 23. If $a_1x^2 + hxy + a_2by^2$ and $a_2x^2 + hxy + a_1by^2$ are primitive quadratic forms of the same discriminant $\Delta = h^2 - 4a_1a_2b$, then we define their **composition** to be the quadratic form $a_1a_2x^2 + hxy + by^2$.



The remarkable fact is that even though composition is only defined on certain pairs of quadratic forms, it nevertheless gives rise to a well-defined binary operation on $C(\Delta)$. A proof can be found in Chapter 7 of *Topology of Numbers* by Allen Hatcher. The proof is quite technical, but we can at least demonstrate how to compute the group operation in practice.

Algorithm 24. To compute the composition of two equivalence classes $c_1, c_2 \in C(\Delta)$:

1. Find values a_1 and a_2 on the topographs with $\gcd(a_1, a_2) = 1$.
2. Find edges around a_1 and a_2 with the same arrow h (including orientation).
3. The values b_1 and b_2 on the other side of these edges will factor as $b_1 = a_2b$ and $b_2 = a_1b$.
4. The quadratic forms $a_1x^2 + hxy + b_1y^2$ and $a_2x^2 + hxy + b_2y^2$ have composition $a_1a_2x^2 + hxy + by^2$.

The first step is made possible by the primitive constraint. Even after fixing a_1, it is always possible to find a value a_2 on the second topograph satisfying $\gcd(a_1, a_2) = 1$. For the second step, the edges around a_1 form an arithmetic progression with common difference $2a_1$, and the edges around a_2 form an arithmetic progression with common difference $2a_2$. Since these arithmetic progressions have the same parity as Δ, the condition $\gcd(a_1, a_2) = 1$ ensures that these arithmetic progressions will have terms in common. In the third step, the discriminant gives $a_1b_1 = a_2b_2$. But $\gcd(a_1, a_2) = 1$, so we must have $a_2 \mid b_1$ and $a_1 \mid b_2$.

Example 25. The primitive quadratic forms f_1 and f_2 have the same discriminant $\Delta = -191$. To compute their product we will select the coprime values $a_1 = 4$ and $a_2 = 9$.

$f_1(x, y) = 4x^2 + xy + 12y^2$ $\qquad$ $f_2(x, y) = 6x^2 + 5xy + 9y^2$

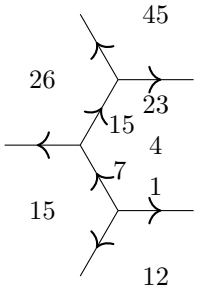
The edges around $a_1 = 4$ will form the arithmetic progression

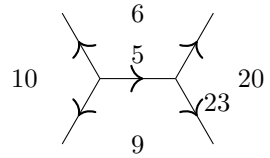
$$\ldots, -31, -23, -15, -7, 1, 9, 17, 25, 33, \ldots$$

with common difference $2a_1 = 8$. The edges around $a_2 = 9$ will form the arithmetic progression

$$\ldots, -41, -23, -5, 13, 31, \ldots$$

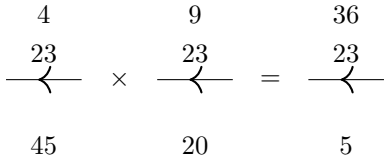
with common difference $2a_2 = 18$. Note that this arithmetic progression starts at -5 rather than 5 since the arrow is pointing clockwise around 9 rather than counterclockwise. The common term -23 can be found by following the edges clockwise around the values $a_1 = 4$ and $a_2 = 9$.



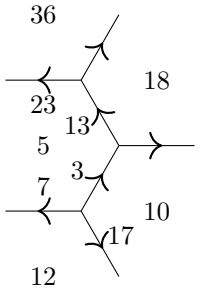


$f_1(x, y) = 4x^2 + xy + 12y^2$ $\qquad$ $f_2(x, y) = 6x^2 + 5xy + 9y^2$

We could also have computed $b_1 = (-\Delta+h^2)/(4a_1) = 720/16 = 45$ and $b_2 = (-\Delta+h^2)/(4a_2) = 720/36 = 20$ directly without the help of the topograph. Regardless, we can now compute the composition of f_1 and f_2.

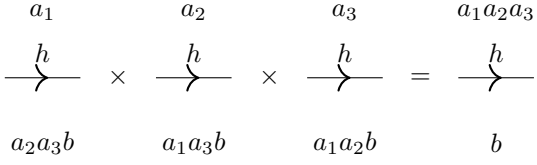


We will usually want to determine the equivalence class of the composition by navigating to the well or river.

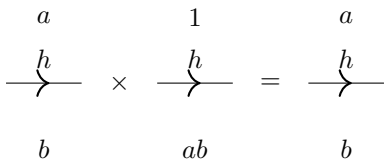


Thus, the composition of $4x^2 + xy + 12y^2$ and $6x^2 + 5xy + 9y^2$ is $5x^2 + 3xy + 10y^2$, up to equivalence.

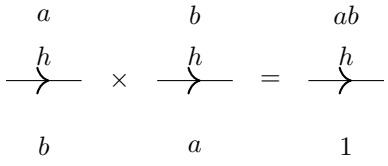
The operation of composition makes $C(\Delta)$ into a finite abelian group. This means that composition satisfies commutativity $c_1c_2 = c_2c_1$ and associativity $(c_1c_2)c_3 = c_1(c_2c_3)$, that there is an identity class $c \cdot 1 = c$, and that every class has an inverse $c \cdot c^{-1} = 1$. Commutativity is clear from the definition, and associativity can be seen by picking pairwise coprime values a_1, a_2, and a_3 on the respective topographs.



Any quadratic form with 1 on its topograph will serve as an identity for the group operation of composition.



And mirror image topographs will be inverses to each other under composition.



From a group-theoretic perspective, identity elements should be unique since if 1 and $1'$ are both identity elements, then we would have $1 = 1 \cdot 1' = 1'$. So any two quadratic forms of the same discriminant that both represent 1 on their topograph should be equivalent. Indeed, this is true. The edges h around $a = 1$ form an arithmetic progression with common difference 2 and with the same parity as Δ. There is only one such arithmetic progression. And the values of b on the other side of these edges are determined by the discriminant $\Delta = h^2 - 4ab$. So the quadratic forms of a given non-square discriminant Δ that represent 1 on their topograph constistute a single equivalence class $1 \in C(\Delta)$ called the **principal class**.

6 Genus Theory

Now fix a non-square discriminant Δ, and suppose that Δ is divisible by an odd prime p. We will study the class group $C(\Delta)$ by reducing the quadratic forms modulo p. We can also consider topographs modulo p, and this gives a notion of equivalence modulo p.

So let f be a primitive quadratic form of discriminant Δ, and consider the topograph of f modulo p. Since f is primitive, the topograph has a value $a \not\equiv 0 \pmod{p}$. The edges h around a form an arithmetic progression with common difference $2a$. Since p is an odd prime, we can find an edge $h \equiv 0 \pmod{p}$. And then the value b on the other side of this edge must satisfy $b \equiv 0 \pmod{p}$ since $\Delta \equiv 0 \pmod{p}$. Thus, f is equivalent to ax^2 modulo p. One peculiar consequence of this is that f will represent either quadratic residues modulo p or quadratic non-residues modulo p, depending on whether or not a is a square modulo p. Since composition multiplies coprime values, this defines a homomorphism $\psi_p \colon C(\Delta) \to \{\pm 1\}$.

Example 26. Example 18 showed the class group $C(-20)$ consists of the principal class represented by $x^2 + 5y^2$ and one other class represented by $2x^2 + 2xy + 3y^2$. The form $x^2 + 5y^2$ represents quadratic residues modulo 5, whereas the form $2x^2 + 2xy + 3y^2$ represents quadratic non-residues modulo 5. So in this case the homomorphism $\psi_5 \colon C(-20) \to \{\pm 1\}$ is actually an isomorphism.

We can also define homomorphisms for $p = 2$, but the theory is slightly more complicated. Suppose that Δ is divisible by 2, let f be a primitive quadratic form of discriminant Δ, and consider the topograph of f modulo 2^k. Since f is primitive, the topograph has a value $a \not\equiv 0 \pmod{2}$. The edges h around a form an arithmetic progression with common difference $2a$ and with the same parity as Δ. Then we can find an edge $h \equiv 0 \pmod{2^k}$. If we know $\Delta \pmod{2^{k+2}}$, then we can solve for $b \pmod{2^k}$.

Usually this will not give a homomorphism. For example, if $k = 2$ and we know that $\Delta \equiv 4 \pmod{16}$, then we can solve for $b \equiv -a \pmod{4}$. Thus, f is equivalent to $a(x^2 - y^2)$ modulo 4. Unfortunately, this does not sufficiently constrain the values of f to produce a homomorphism $C(\Delta) \to \{\pm 1\}$.

But in a few cases, we do get a homomorphism. There is sometimes a homomorphism ψ_{-1} obtained by considering the topograph modulo 4, and there are sometimes homomorphisms ψ_2 or ψ_{-2} obtained by considering the topograph modulo 8. We now give an exhaustive list of these cases.

- For $\Delta \equiv 0, 12 \pmod{16}$, there is a homomorphism $\psi_{-1} \colon C(\Delta) \to \{\pm 1\}$ determined by whether the class represents $1 \pmod 4$ or $3 \pmod 4$.
  - For $\Delta \equiv 0 \pmod{16}$, every class in $C(\Delta)$ is equivalent to ax^2 modulo 4.
  - For $\Delta \equiv 12 \pmod{16}$, every class in $C(\Delta)$ is equivalent to $a(x^2 + y^2)$ modulo 4.
- For $\Delta \equiv 0, 8 \pmod{32}$, there is a homomorphism $\psi_2 \colon C(\Delta) \to \{\pm 1\}$ determined by whether the class represents $1, 7 \pmod 8$ or $3, 5 \pmod 8$.
  - For $\Delta \equiv 0 \pmod{32}$, every class in $C(\Delta)$ is equivalent to ax^2 modulo 8.
  - For $\Delta \equiv 8 \pmod{32}$, every class in $C(\Delta)$ is equivalent to $a(x^2 - 2y^2)$ modulo 8.
- For $\Delta \equiv 0, 24 \pmod{32}$, there is a homomorphism $\psi_{-2} \colon C(\Delta) \to \{\pm 1\}$ determined by whether the class represents $1, 3 \pmod 8$ or $5, 7 \pmod 8$.
  - For $\Delta \equiv 0 \pmod{32}$, every class in $C(\Delta)$ is equivalent to ax^2 modulo 8.
  - For $\Delta \equiv 24 \pmod{32}$, every class in $C(\Delta)$ is equivalent to $a(x^2 + 2y^2)$ modulo 8.

For each non-square discriminant Δ, we will package all of the applicable homomorphisms into a single homomorphism $\psi \colon C(\Delta) \to \{\pm 1\}^\mu$ called the **genus**. Let $p_1, \ldots, p_r$ be the distinct odd primes dividing Δ.

Δ	μ	ψ
$\Delta \equiv 1 \pmod 4$ $\Delta \equiv 4 \pmod{16}$	r	$\psi_{p_1}, \ldots, \psi_{p_r}$
$\Delta \equiv 12 \pmod{16}$ $\Delta \equiv 16 \pmod{32}$	$r+1$	$\psi_{-1}, \psi_{p_1}, \ldots, \psi_{p_r}$
$\Delta \equiv 8 \pmod{32}$	$r+1$	$\psi_2, \psi_{p_1}, \ldots, \psi_{p_r}$
$\Delta \equiv 24 \pmod{32}$	$r+1$	$\psi_{-2}, \psi_{p_1}, \ldots, \psi_{p_r}$
$\Delta \equiv 0 \pmod{32}$	$r+2$	$\psi_{-1}, \psi_2, \psi_{p_1}, \ldots, \psi_{p_r}$

We choose to exclude ψ_{-2} when $\Delta \equiv 0 \pmod{32}$ since it is equal to the product $\psi_{-1}\psi_2$ and thus gives no additional information. We should also point out that $\Delta = h^2 - 4ab$ always satisfies $\Delta \equiv 0, 1 \pmod 4$, which is why the cases $\Delta \equiv 2, 3 \pmod 4$ are missing from the table.

Example 27. Here is the genus on each of the class groups computed in Examples 16, 17, 18, and 19.

$C(20)$	ψ_5
$x^2 - 5y^2$	1

$C(-20)$	ψ_{-1}	ψ_5
$x^2 + 5y^2$	1	1
$2x^2 + 2xy + 3y^2$	-1	-1

$C(32)$	ψ_{-1}	ψ_2
$x^2 - 8y^2$	1	1
$8x^2 - y^2$	-1	1

$C(-32)$	ψ_{-1}	ψ_2
$x^2 + 8y^2$	1	1
$3x^2 + 2xy + 3y^2$	-1	-1

Example 28. Here is the genus on the class group $C(-56)$.

$C(-56)$	ψ_2	ψ_7
$x^2 + 14y^2$	1	1
$2x^2 + 7y^2$	1	1
$3x^2 + 2xy + 5y^2$	-1	-1
$5x^2 + 2xy + 3y^2$	-1	-1

In this case, we say that there there are two **genera**: the **principal genus** consisting of the principal class represented by $x^2 + 14y^2$ and the class represented by $2x^2 + 7y^2$, and one other genus consisting of the class represented by $3x^2 + 2xy + 5y^2$ and the class represented by $5x^2 + 2xy + 3y^2$.

7 Ambiguous Forms

In order to count the number of genera, we will need a group-theoretic analog of the rank-nullity theorem.

Lemma 29. *If $f\colon A \to B$ is a group homomorphism, then* $|\text{image}(f)| \cdot |\text{kernel}(f)| = |A|$.

The kernel of f is just the set of elements of A that f maps to the identity element of B. We will apply Lemma 29 twice, once to the genus $\psi\colon C(\Delta) \to \{\pm 1\}^\mu$ and once to the squaring map $\text{sq}\colon C(\Delta) \to C(\Delta)$. The key observation is that every element of $\{\pm 1\}^\mu$ squares to 1, so

$$\psi(\text{sq}(c)) = \psi(c^2) = \psi(c)^2 = 1.$$

Thus, $\text{image}(\text{sq}) \subseteq \text{kernel}(\psi)$. In particular, we have $|\text{kernel}(\psi)| \geq |\text{image}(\text{sq})|$. Then Lemma 29 gives

$$\#\text{genera} = |\text{image}(\psi)| = \frac{|C(\Delta)|}{|\text{kernel}(\psi)|} \leq \frac{|C(\Delta)|}{|\text{image}(\text{sq})|} = |\text{kernel}(\text{sq})| = \#\text{ambiguous classes}. \tag{3}$$

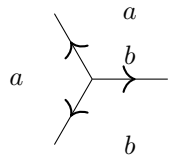
A class $c \in C(\Delta)$ is in the kernel of the squaring map when $c^2 = 1$. Equivalently, when $c = c^{-1}$, which occurs exactly when the topograph of c has reflectional symmetry.

Definition 30. A quadratic form is said to be **ambiguous** if its topograph has reflectional symmetry.

Example 31. In Example 27, all of the classes in $C(20)$, $C(-20)$, $C(32)$, and $C(-32)$ are ambiguous. In Example 28, the classes $x^2 + 14y^2$ and $2x^2 + 7y^2$ are ambiguous, but the classes $3x^2 + 2xy + 5y^2$ and $5x^2 + 2xy + 3y^2$ are not. For all of these discriminants, the inequality (3) is actually an equality.

There is no obstruction to directly counting ambiguous classes, besides the tedium of working through the various cases. Incredibly, the number of ambiguous classes always turns out to be exactly $2^{\mu-1}$, despite the convoluted piecewise definition of μ. To give a sense of how surprising this is, we will work through this calculation in the three cases that will arise in our proof of quadratic reciprocity.

- Suppose that $\Delta < 0$ and $\Delta \equiv 1 \pmod 4$. Let $p_1, \ldots, p_r$ be the distinct odd primes dividing Δ. Every ambiguous topograph of discriminant Δ will have a simple well surrounded by a repeated value $a > 0$ and a third value $b > 0$, possibly equal to a.



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

  The values a and b need to satisfy $2a > b$ for the last arrow to point away from the well, $b(4a - b) = -\Delta$ for the topograph to have the correct discriminant, and $\gcd(a, b) = 1$ for the topograph to be primitive. In particular, b must be one of the 2^r positive divisors of $-\Delta$ satisfying $\gcd(b, -\Delta/b) = 1$. Solving for a gives $a = (-\Delta/b + b)/4$ which will always be an integer since $\Delta \equiv 1 \pmod 4$. Then the inequality $2a > b$ becomes $b^2 < -\Delta$. This inequality will be satisfied by exactly half of the 2^r initial possibilities for b. Thus, the number of ambiguous classes is exactly 2^{r-1}.

- Suppose that $\Delta > 0$ and $\Delta \equiv 1 \pmod 4$. Let $p_1, \ldots, p_r$ be the distinct odd primes dividing Δ. Every ambiguous topograph of discriminant Δ will have an infinite periodic river with two points of symmetry per period. Each point of symmetry will be of the above form $ax^2 + bxy + by^2$, but now a and b will differ in sign. We will restrict to the case where $a < 0$ and $b > 0$. This will only give us half of the possibilities, but this will cancel out the factor of 2 coming from the two points of symmetry per period.

The values a and b need to satisfy $b(b-4a) = \Delta$ and $\gcd(a,b) = 1$. As before, b must be one of the 2^r positive divisors of Δ satisfying $\gcd(b, \Delta/b) = 1$. Solving for a gives $a = (b - \Delta/b)/4$ which will always be an integer since $\Delta \equiv 1 \pmod 4$. Then the inequality $a < 0$ becomes $b^2 < \Delta$. This inequality will be satisfied by exactly half of the 2^r initial possibilities for b. Thus, the number of ambiguous classes is exactly 2^{r-1}.

- Suppose that $\Delta > 0$ and $\Delta \equiv 4 \pmod{16}$. Let $p_1, \ldots, p_r$ be the distinct odd primes dividing Δ. As before, every ambiguous topograph of discriminant Δ will have an infinite periodic river with two points of symmetry per period. In this case though, it is impossible to have $b(b-4a) = \Delta$. For b would need to be even, say $b = 2b'$, giving $b'(b' - 2a) = \Delta/4$, and b' would need to be odd, so a would need to be even, violating the primitive condition.

  So this time, every point of symmetry will be of the form $ax^2 + by^2$ with $a < 0$ and $b > 0$. The values a and b need to satisfy $-ab = \Delta/4$ and $\gcd(a,b) = 1$. Now b must be one of the 2^r positive divisors of $\Delta/4$ satisfying $\gcd(b, (\Delta/4)/b) = 1$. But we must divide by 2 since there are two points of symmetry per period. Thus, the number of ambiguous classes is exactly 2^{r-1}.

There are many more cases, but we will omit them for the sake of brevity. The ultimate conclusion is that

$$\#\text{genera} \leq \#\text{ambiguous classes} = 2^{\mu-1}. \tag{4}$$

8 Quadratic Reciprocity

We are now in a position to present Gauss' proof of quadratic reciprocity. In fact, Gauss had many proofs of quadratic reciprocity, but the proof using quadratic forms is perhaps his deepest and most elegant. Recall that for each odd prime p, we have the **Legendre symbol**

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod p. \end{cases}$$

The first connection between Legendre symbols and quadratic forms is given by the following proposition.

Proposition 32. *Let $\Delta \equiv 0, 1 \pmod 4$, and let p be an odd prime not dividing Δ. Then p is represented by a primitive quadratic form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$.*

Proof. By rotating and translating the topograph, we know that p is represented by a primitive quadratic form of discriminant Δ if and only if there is an equivalent primitive quadratic form $ax^2 + hxy + py^2$ with discriminant $h^2 - 4ap = \Delta$. Note that $p \nmid \Delta$ implies $p \nmid h$, so such a quadratic form is automatically primitive. The equation $h^2 - 4ap = \Delta$ has an integer solution if and only if the congruence $h^2 \equiv \Delta \pmod{4p}$ has a solution. By the Chinese remainder theorem, this is equivalent Δ being a quadratic residue modulo p. □

As a warmup, let's prove the first and second supplements to the law of quadratic reciprocity.

Theorem 33 (The First Supplement to the Law of Quadratic Reciprocity)**.** *Let p be an odd prime. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Suppose that $p \equiv 1 \pmod 4$. The quadratic form $px^2 - y^2$ has discriminant $4p$ and represents -1. But by (4), there is only one genus (the principal genus), so $\left(\frac{-1}{p}\right) = 1$. Conversely, suppose that $\left(\frac{-1}{p}\right) = 1$. Then $\left(\frac{-4}{p}\right) = 1$. By Proposition 32, p is represented by a primitive quadratic form of discriminant -4. But every quadratic form of discriminant -4 is equivalent to $x^2 + y^2$. Then $p \equiv x^2 + y^2 \equiv 1 \pmod 4$. □

Theorem 34 (The Second Supplement to the Law of Quadratic Reciprocity)**.** *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Proof. Suppose that $p \equiv \pm 1 \pmod 8$. The quadratic form $2x^2 + xy - \frac{-1 \pm p}{8} y^2$ has discriminant $\pm p$ and represents 2. But by (4), there is only one genus (the principal genus), so $\left(\frac{2}{p}\right) = 1$. Conversely, suppose that $\left(\frac{2}{p}\right) = 1$. Then $\left(\frac{8}{p}\right) = 1$. By Proposition 32, p is represented by a primitive quadratic form of discriminant 8. But every quadratic form of discriminant 8 is equivalent to $x^2 - 2y^2$. Then $p \equiv x^2 - 2y^2 \equiv 1, 7 \pmod 8$. □

And finally, the main event!

Theorem 35 (The Law of Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

Proof. First we will use a common trick to simplify the statement of quadratic reciprocity. Let

$$q^* = \begin{cases} q & \text{if } q \equiv 1 \pmod 4, \\ -q & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

You can think of q^* as the version of q that is tweaked to always be $1 \pmod 4$. Then with the help of the first supplement, we can see that quadratic reciprocity is equivalent to the statement that

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right).$$

Suppose that $\left(\frac{q^*}{p}\right) = 1$. By Proposition 32, p is represented by a quadratic form of discriminant q^*. But by (4), there is only one genus (the principal genus), so $\left(\frac{p}{q}\right) = 1$. Conversely, we must prove that $\left(\frac{p}{q}\right) = 1$ implies $\left(\frac{q^*}{p}\right) = 1$. If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then this is the same as $\left(\frac{p^*}{q}\right) = 1$ implying $\left(\frac{q}{p}\right) = 1$, which has already been proven. So assume that $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. The two quadratic forms $px^2 - qy^2$ and $qx^2 - py^2$ have discriminant $4pq$. Under ψ_q, the first maps to 1 and the second maps to -1. But by (4), there are at most two genera, so the first must lie in the principal genus, giving $\left(\frac{q^*}{p}\right) = 1$. □

9 The Duplication Theorem

With quadratic reciprocity in hand, we can finally tie up the last remaining loose threads from our discussion of genus theory. In particular, we will be able to prove that the inequality in (3) is always an equality.

For each non-square discriminant Δ, we will define a homomorphism $\chi\colon (\mathbb{Z}/\Delta\mathbb{Z})^\times \to \{\pm 1\}^\mu$, analogous to the genus $\psi\colon C(\Delta) \to \{\pm 1\}^\mu$. First we must define the following homomorphisms $(\mathbb{Z}/\Delta\mathbb{Z})^\times \to \{\pm 1\}$,

$$\text{for each odd prime } p \mid \Delta, \quad \chi_p(q) = \left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } q \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } q \text{ is not a quadratic residue modulo } p, \end{cases}$$

$$\text{when } 4 \mid \Delta, \qquad \chi_{-1}(q) = \left(\frac{-1}{q}\right) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4, \\ -1 & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

$$\text{when } 8 \mid \Delta, \qquad \chi_2(q) = \left(\frac{2}{q}\right) = \begin{cases} 1 & \text{if } q \equiv 1, 7 \pmod 8, \\ -1 & \text{if } q \equiv 3, 5 \pmod 8, \end{cases}$$

$$\text{when } 8 \mid \Delta, \qquad \chi_{-2}(q) = \left(\frac{-2}{q}\right) = \begin{cases} 1 & \text{if } q \equiv 1, 3 \pmod 8, \\ -1 & \text{if } q \equiv 5, 7 \pmod 8. \end{cases}$$

Note that even though the initial Legendre symbol definitions of these homomorphisms only make sense when q is an odd prime, the final piecewise definition makes sense for all q coprime to Δ. To define the homomorphism $\chi\colon (\mathbb{Z}/\Delta\mathbb{Z})^\times \to \{\pm 1\}^\mu$, let $p_1, \ldots, p_r$ be the distinct odd primes dividing Δ.

Δ	μ	χ
$\Delta \equiv 1 \pmod 4$ $\Delta \equiv 4 \pmod{16}$	r	$\chi_{p_1}, \ldots, \chi_{p_r}$
$\Delta \equiv 12 \pmod{16}$ $\Delta \equiv 16 \pmod{32}$	$r+1$	$\chi_{-1}, \chi_{p_1}, \ldots, \chi_{p_r}$
$\Delta \equiv 8 \pmod{32}$	$r+1$	$\chi_2, \chi_{p_1}, \ldots, \chi_{p_r}$
$\Delta \equiv 24 \pmod{32}$	$r+1$	$\chi_{-2}, \chi_{p_1}, \ldots, \chi_{p_r}$
$\Delta \equiv 0 \pmod{32}$	$r+2$	$\chi_{-1}, \chi_2, \chi_{p_1}, \ldots, \chi_{p_r}$

This definition has several key properties. First, the Chinese Remainder Theorem tells us that

1. The homomorphism $\chi\colon (\mathbb{Z}/\Delta\mathbb{Z})^\times \to \{\pm 1\}^\mu$ is surjective.

Second, the direct similarity between ψ and χ ensures that

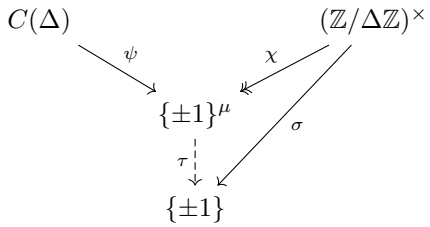
2. If a class $c \in C(\Delta)$ represents an odd prime q not dividing Δ, then $\psi(c) = \chi(q)$.

Lastly, the Legendre symbol $\left(\frac{\Delta}{q}\right)$ can be recovered from χ. For example, if $\Delta \equiv 12 \pmod{16}$, then we can write $\Delta = -4(p_1^*)^{k_1} \cdots (p_r^*)^{k_r}$ and

$$\left(\frac{\Delta}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p_1^*}{q}\right)^{k_1} \cdots \left(\frac{p_r^*}{q}\right)^{k_r} = \chi_{-1}(q)\chi_{p_1}(q)^{k_1} \cdots \chi_{p_r}(q)^{k_r}.$$

In particular, these factorizations of $\left(\frac{\Delta}{q}\right)$ show that

3. The Legendre symbol $\left(\frac{\Delta}{q}\right)$ defines a homomorphism $\sigma\colon (\mathbb{Z}/\Delta\mathbb{Z})^\times \to \{\pm 1\}$ that factors through χ.



Theorem 36. *The image of the genus $\psi\colon C(\Delta) \to \{\pm 1\}^\mu$ contains the kernel of τ.*

Proof. Let $\varepsilon \in \text{kernel}(\tau)$. By the first property of χ (along with Dirichlet's theorem on primes in arithmetic progressions), we can find an odd prime q not dividing Δ with $\chi(q) = \varepsilon$. Then the third property of χ gives $\left(\frac{\Delta}{q}\right) = \sigma(q) = \tau(\chi(q)) = \tau(\varepsilon) = 1$. By Proposition 32, q is represented by some class $c \in C(\Delta)$. By the second property of χ, we have $\psi(c) = \chi(q) = \varepsilon$. Thus, $\varepsilon \in \text{image}(\psi)$. □

In particular, we have the inequality $|\text{image}(\psi)| \geq |\text{kernel}(\tau)|$. Then Lemma 29 gives

$$\#\text{genera} = |\text{image}(\psi)| \geq |\text{kernel}(\tau)| = \frac{|\{\pm 1\}^\mu|}{|\text{image}(\tau)|} \geq \frac{2^\mu}{2} = 2^{\mu-1} = \#\text{ambiguous classes} \tag{5}$$

Thus, (3) is actually an equality, so we must have $\text{kernel}(\psi) = \text{image}(\text{sq})$.

Corollary 37 (The Duplication Theorem)**.** *Let Δ be a non-square discriminant. Then the principal genus in $C(\Delta)$ is exactly the subgroup of squares $C(\Delta)^2$. The genus $\psi\colon C(\Delta) \to \{\pm 1\}^\mu$ is injective if and only if every primitive topograph of discriminant Δ has reflectional symmetry.*

10 Representing Primes

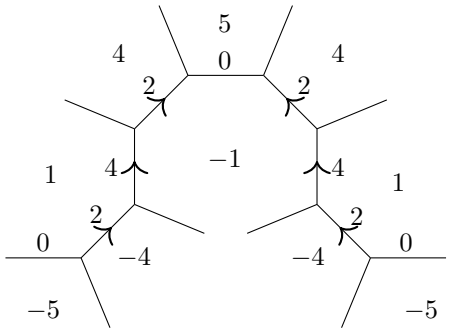
If q is an odd prime not dividing Δ, then Proposition 32 states that q is represented by some class $c \in C(\Delta)$ if and only if $\left(\frac{\Delta}{q}\right) = 1$. But we can now be more specific. If $\left(\frac{\Delta}{q}\right) = 1$, then q is represented by some class $c \in C(\Delta)$ of genus $\psi(c) = \chi(q)$ and not by classes of any other genus. In particular, the primes represented by a given genus are exactly those primes satisfying the congruence conditions arising from the genus.

When the genus $\psi\colon C(\Delta) \to \{\pm 1\}^\mu$ is injective, there is only class per genus, so the primes represented by a given class are exactly those primes satisfying the congruence conditions arising from the genus. This gives an algorithm to determine which primes are represented by a quadratic form f.

Algorithm 38. To determine which primes are represented by a quadratic form f:

1. Compute the discriminant Δ of f and check that Δ is not a perfect square.
2. Classify primitive quadratic forms of discriminant Δ up to equivalence.
3. Check that these topographs all have reflectional symmetry (so that the genus will be injective).
4. Search the topograph of f to determine whether 2 and primes dividing Δ are represented by f.
5. Compute the genus of f.
6. Use the Chinese Remainder Theorem to obtain a congruence condition on odd primes not dividing Δ.

Example 39. We will determine which primes are represented by $x^2 - 5y^2$. The discriminant $\Delta = 20$ is not a perfect square. In Example 16, we classified all primitive quadratic forms of discriminant 20 and saw that their topographs all have reflectional symmetry. From the topograph of $x^2 - 5y^2$, we can see that $x^2 - 5y^2$ represents 5 but not 2.

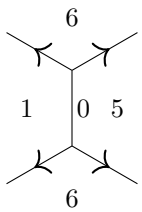


In Example 27, we saw that the genus of $x^2 - 5y^2$ is $\psi_5 = 1$, and we have

$$\left(\frac{p}{5}\right) = 1 \iff p \equiv 1, 4 \pmod 5.$$

Thus, the primes represented by $x^2 - 5y^2$ are exactly $p = 5$ and the primes $p \equiv 1, 4 \pmod 5$.

Example 40. We will determine which primes are represented by $x^2 + 5y^2$. The discriminant $\Delta = -20$ is not a perfect square. In Example 18, we classified all primitive quadratic forms of discriminant -20 and saw that their topographs all have reflectional symmetry. From the topograph of $x^2 + 5y^2$, we can see that $x^2 + 5y^2$ represents 5 but not 2.

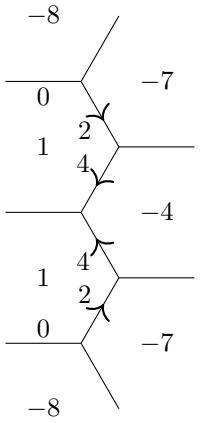


In Example 27, we saw that the genus of x^2+5y^2 is $\psi_{-1}=1$ and $\psi_5=1$, and we have

$$\left(\frac{-1}{p}\right)=1 \text{ and } \left(\frac{p}{5}\right)=1 \iff p\equiv 1 \pmod 4 \text{ and } p\equiv 1,4 \pmod 5 \iff p\equiv 1,9 \pmod{20}.$$

Thus, the primes represented by x^2+5y^2 are exactly $p=5$ and the primes $p\equiv 1,9 \pmod{20}$.

Example 41. We will determine which primes are represented by x^2-8y^2. The discriminant $\Delta=32$ is not a perfect square. In Example 17, we classified all primitive quadratic forms of discriminant 32 and saw that their topographs all have reflectional symmetry. From the topograph of x^2-8y^2, we can see that x^2-8y^2 does not represent 2.

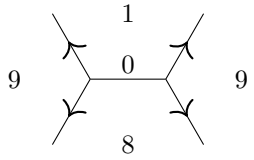


In Example 27, we saw that the genus of x^2-8y^2 is $\psi_{-1}=1$ and $\psi_2=1$, and we have

$$\left(\frac{-1}{p}\right)=1 \text{ and } \left(\frac{2}{p}\right)=1 \iff p\equiv 1 \pmod 4 \text{ and } p\equiv 1,7 \pmod 8 \iff p\equiv 1 \pmod 8.$$

Thus, the primes represented by x^2-8y^2 are exactly the primes $p\equiv 1 \pmod 8$.

Example 42. We will determine which primes are represented by x^2+8y^2. The discriminant $\Delta=-32$ is not a perfect square. In Example 19, we classified all primitive quadratic forms of discriminant -32 and saw that their topographs all have reflectional symmetry. From the topograph of x^2+8y^2, we can see that x^2+8y^2 does not represent 2.

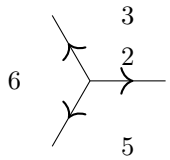


In Example 27, we saw that the genus of x^2+8y^2 is $\psi_{-1}=1$ and $\psi_2=1$, and we have

$$\left(\frac{-1}{p}\right)=1 \text{ and } \left(\frac{2}{p}\right)=1 \iff p\equiv 1 \pmod 4 \text{ and } p\equiv 1,7 \pmod 8 \iff p\equiv 1 \pmod 8.$$

Thus, the primes represented by x^2+8y^2 are exactly the primes $p\equiv 1 \pmod 8$.

Example 43. We will not be able determine which primes are represented by x^2+14y^2 since there is a primitive positive definite quadratic form of discriminant -56 whose topograph lacks reflectional symmetry.



$$3x^2 + 2xy + 5y^2$$

What we can say is that a prime $p \neq 2, 7$ is represented by some class in $C(-56)$ if and only if $\left(\frac{-56}{p}\right) = 1$, and the genus gives congruences that distinguish between different genera.

$$\left(\frac{-56}{p}\right) = 1 \iff \begin{cases} p = x^2 + 14y^2 \\ p = 2x^2 + 7^2 \end{cases} \iff \left(\frac{2}{p}\right) = \left(\frac{p}{7}\right) = 1 \iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56},$$
$$\begin{cases} p = 3x^2 + 2xy + 5y^2 \\ p = 5x^2 + 2xy + 3y^2 \end{cases} \iff \left(\frac{2}{p}\right) = \left(\frac{p}{7}\right) = -1 \iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}.$$

But congruences cannot distinguish between the classes $x^2 + 14y^2$ and $2x^2 + 7y^2$ within the same genus.

For further reading on this subject, I highly recommend *Primes of the Form $x^2 + ny^2$* by David A. Cox.

11 Tables

Algorithm 38 allows us to classify primes represented by a quadratic form of non-square discriminant Δ whenever $C(\Delta) \cong (\mathbb{Z}/2\mathbb{Z})^k$ for some nonnegative integer k. There are probably infinitely many positive discriminants $\Delta > 0$ with $C(\Delta) \cong (\mathbb{Z}/2\mathbb{Z})^k$, but it is known that there are only finitely many negative discriminants $\Delta < 0$ with $C(\Delta) \cong (\mathbb{Z}/2\mathbb{Z})^k$. Here they are, listed by class group:

$(\mathbb{Z}/2\mathbb{Z})^0$: $-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163,$

$(\mathbb{Z}/2\mathbb{Z})^1$: $-15, -20, -24, -32, -35, -36, -40, -48, -51, -52, -60, -64, -72, -75, -88, -91, -99, -100,$
$-112, -115, -123, -147, -148, -187, -232, -235, -267, -403, -427,$

$(\mathbb{Z}/2\mathbb{Z})^2$: $-84, -96, -120, -132, -160, -168, -180, -192, -195, -228, -240, -280, -288, -312, -315,$
$-340, -352, -372, -408, -435, -448, -483, -520, -532, -555, -595, -627, -708, -715,$
$-760, -795, -928, -1012, -1435,$

$(\mathbb{Z}/2\mathbb{Z})^3$: $-420, -480, -660, -672, -840, -960, -1092, -1120, -1155, -1248, -1320, -1380, -1428,$
$-1540, -1632, -1848, -1995, -2080, -3003, -3040, -3315,$

$(\mathbb{Z}/4\mathbb{Z})^4$: $-3360, -5280, -5460, -7392.$

For example, $C(-20) \cong \mathbb{Z}/2\mathbb{Z}$ and $C(-32) \cong \mathbb{Z}/2\mathbb{Z}$.

In this table, n is the number of primitive river segments, $C(\Delta)$ is the class group, and $H = |C(\Delta)|$.

Δ	n	H	$C(\Delta)$
5	2	1	$\mathbb{Z}/1\mathbb{Z}$
8	4	1	$\mathbb{Z}/1\mathbb{Z}$
12	6	2	$\mathbb{Z}/2\mathbb{Z}$
13	6	1	$\mathbb{Z}/1\mathbb{Z}$
17	10	1	$\mathbb{Z}/1\mathbb{Z}$
20	8	1	$\mathbb{Z}/1\mathbb{Z}$
21	8	2	$\mathbb{Z}/2\mathbb{Z}$
24	12	2	$\mathbb{Z}/2\mathbb{Z}$
28	14	2	$\mathbb{Z}/2\mathbb{Z}$
29	10	1	$\mathbb{Z}/1\mathbb{Z}$
32	10	2	$\mathbb{Z}/2\mathbb{Z}$
33	20	2	$\mathbb{Z}/2\mathbb{Z}$
37	14	1	$\mathbb{Z}/1\mathbb{Z}$
40	20	2	$\mathbb{Z}/2\mathbb{Z}$
41	22	1	$\mathbb{Z}/1\mathbb{Z}$
44	18	2	$\mathbb{Z}/2\mathbb{Z}$
45	12	2	$\mathbb{Z}/2\mathbb{Z}$
48	16	2	$\mathbb{Z}/2\mathbb{Z}$
52	20	1	$\mathbb{Z}/1\mathbb{Z}$
53	14	1	$\mathbb{Z}/1\mathbb{Z}$
56	20	2	$\mathbb{Z}/2\mathbb{Z}$
57	32	2	$\mathbb{Z}/2\mathbb{Z}$
60	24	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
61	22	1	$\mathbb{Z}/1\mathbb{Z}$
65	32	2	$\mathbb{Z}/2\mathbb{Z}$
68	16	1	$\mathbb{Z}/1\mathbb{Z}$
69	20	2	$\mathbb{Z}/2\mathbb{Z}$
72	24	2	$\mathbb{Z}/2\mathbb{Z}$
73	42	1	$\mathbb{Z}/1\mathbb{Z}$
76	34	2	$\mathbb{Z}/2\mathbb{Z}$
77	16	2	$\mathbb{Z}/2\mathbb{Z}$
80	20	2	$\mathbb{Z}/2\mathbb{Z}$
84	28	2	$\mathbb{Z}/2\mathbb{Z}$
85	28	2	$\mathbb{Z}/2\mathbb{Z}$
88	36	2	$\mathbb{Z}/2\mathbb{Z}$
89	42	1	$\mathbb{Z}/1\mathbb{Z}$
92	26	2	$\mathbb{Z}/2\mathbb{Z}$
93	24	2	$\mathbb{Z}/2\mathbb{Z}$
96	28	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
97	54	1	$\mathbb{Z}/1\mathbb{Z}$
101	22	1	$\mathbb{Z}/1\mathbb{Z}$
104	32	2	$\mathbb{Z}/2\mathbb{Z}$
105	52	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
108	30	2	$\mathbb{Z}/2\mathbb{Z}$
109	34	1	$\mathbb{Z}/1\mathbb{Z}$
112	36	2	$\mathbb{Z}/2\mathbb{Z}$
113	46	1	$\mathbb{Z}/1\mathbb{Z}$
116	32	1	$\mathbb{Z}/1\mathbb{Z}$
117	20	2	$\mathbb{Z}/2\mathbb{Z}$
120	40	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
124	50	2	$\mathbb{Z}/2\mathbb{Z}$
125	22	1	$\mathbb{Z}/1\mathbb{Z}$
128	26	2	$\mathbb{Z}/2\mathbb{Z}$
129	64	2	$\mathbb{Z}/2\mathbb{Z}$
132	28	2	$\mathbb{Z}/2\mathbb{Z}$
133	36	2	$\mathbb{Z}/2\mathbb{Z}$
136	52	4	$\mathbb{Z}/4\mathbb{Z}$
137	54	1	$\mathbb{Z}/1\mathbb{Z}$
140	36	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
141	36	2	$\mathbb{Z}/2\mathbb{Z}$
145	76	4	$\mathbb{Z}/4\mathbb{Z}$
148	48	3	$\mathbb{Z}/3\mathbb{Z}$
149	30	1	$\mathbb{Z}/1\mathbb{Z}$
152	36	2	$\mathbb{Z}/2\mathbb{Z}$
153	56	2	$\mathbb{Z}/2\mathbb{Z}$
156	52	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
157	38	1	$\mathbb{Z}/1\mathbb{Z}$
160	48	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
161	64	2	$\mathbb{Z}/2\mathbb{Z}$
164	32	1	$\mathbb{Z}/1\mathbb{Z}$
165	36	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
168	48	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
172	58	2	$\mathbb{Z}/2\mathbb{Z}$
173	26	1	$\mathbb{Z}/1\mathbb{Z}$
176	40	2	$\mathbb{Z}/2\mathbb{Z}$
177	76	2	$\mathbb{Z}/2\mathbb{Z}$
180	40	2	$\mathbb{Z}/2\mathbb{Z}$
181	50	1	$\mathbb{Z}/1\mathbb{Z}$
184	68	2	$\mathbb{Z}/2\mathbb{Z}$
185	68	2	$\mathbb{Z}/2\mathbb{Z}$
188	38	2	$\mathbb{Z}/2\mathbb{Z}$
189	36	2	$\mathbb{Z}/2\mathbb{Z}$
192	40	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
193	94	1	$\mathbb{Z}/1\mathbb{Z}$
197	30	1	$\mathbb{Z}/1\mathbb{Z}$
200	44	2	$\mathbb{Z}/2\mathbb{Z}$
201	88	2	$\mathbb{Z}/2\mathbb{Z}$
204	64	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
205	52	4	$\mathbb{Z}/4\mathbb{Z}$
208	52	2	$\mathbb{Z}/2\mathbb{Z}$
209	76	2	$\mathbb{Z}/2\mathbb{Z}$
212	44	1	$\mathbb{Z}/1\mathbb{Z}$
213	36	2	$\mathbb{Z}/2\mathbb{Z}$
216	52	2	$\mathbb{Z}/2\mathbb{Z}$
217	100	2	$\mathbb{Z}/2\mathbb{Z}$
220	72	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
221	40	4	$\mathbb{Z}/4\mathbb{Z}$
224	48	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
228	44	2	$\mathbb{Z}/2\mathbb{Z}$
229	58	3	$\mathbb{Z}/3\mathbb{Z}$
232	72	2	$\mathbb{Z}/2\mathbb{Z}$
233	78	1	$\mathbb{Z}/1\mathbb{Z}$
236	54	2	$\mathbb{Z}/2\mathbb{Z}$
237	40	2	$\mathbb{Z}/2\mathbb{Z}$
240	56	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
241	118	1	$\mathbb{Z}/1\mathbb{Z}$
244	72	1	$\mathbb{Z}/1\mathbb{Z}$
245	36	2	$\mathbb{Z}/2\mathbb{Z}$
248	44	2	$\mathbb{Z}/2\mathbb{Z}$
249	108	2	$\mathbb{Z}/2\mathbb{Z}$
252	48	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
253	56	2	$\mathbb{Z}/2\mathbb{Z}$
257	78	3	$\mathbb{Z}/3\mathbb{Z}$
260	44	2	$\mathbb{Z}/2\mathbb{Z}$
261	48	2	$\mathbb{Z}/2\mathbb{Z}$
264	72	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
265	120	2	$\mathbb{Z}/2\mathbb{Z}$
268	82	2	$\mathbb{Z}/2\mathbb{Z}$
269	42	1	$\mathbb{Z}/1\mathbb{Z}$
272	40	2	$\mathbb{Z}/2\mathbb{Z}$
273	100	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
276	68	2	$\mathbb{Z}/2\mathbb{Z}$
277	58	1	$\mathbb{Z}/1\mathbb{Z}$
280	88	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
281	98	1	$\mathbb{Z}/1\mathbb{Z}$
284	66	2	$\mathbb{Z}/2\mathbb{Z}$
285	48	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
288	52	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
292	60	1	$\mathbb{Z}/1\mathbb{Z}$
293	34	1	$\mathbb{Z}/1\mathbb{Z}$
296	68	2	$\mathbb{Z}/2\mathbb{Z}$
297	88	2	$\mathbb{Z}/2\mathbb{Z}$
300	64	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
301	72	2	$\mathbb{Z}/2\mathbb{Z}$
304	80	2	$\mathbb{Z}/2\mathbb{Z}$
305	100	4	$\mathbb{Z}/4\mathbb{Z}$
308	52	2	$\mathbb{Z}/2\mathbb{Z}$
309	64	2	$\mathbb{Z}/2\mathbb{Z}$
312	72	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
313	130	1	$\mathbb{Z}/1\mathbb{Z}$
316	102	6	$\mathbb{Z}/6\mathbb{Z}$
317	42	1	$\mathbb{Z}/1\mathbb{Z}$
320	48	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
321	124	6	$\mathbb{Z}/6\mathbb{Z}$
325	60	2	$\mathbb{Z}/2\mathbb{Z}$
328	88	4	$\mathbb{Z}/4\mathbb{Z}$
329	108	2	$\mathbb{Z}/2\mathbb{Z}$

Δ	H	$C(\Delta)$
-3	1	$\mathbb{Z}/1\mathbb{Z}$
-4	1	$\mathbb{Z}/1\mathbb{Z}$
-7	1	$\mathbb{Z}/1\mathbb{Z}$
-8	1	$\mathbb{Z}/1\mathbb{Z}$
-11	1	$\mathbb{Z}/1\mathbb{Z}$
-12	1	$\mathbb{Z}/1\mathbb{Z}$
-15	2	$\mathbb{Z}/2\mathbb{Z}$
-16	1	$\mathbb{Z}/1\mathbb{Z}$
-19	1	$\mathbb{Z}/1\mathbb{Z}$
-20	2	$\mathbb{Z}/2\mathbb{Z}$
-23	3	$\mathbb{Z}/3\mathbb{Z}$
-24	2	$\mathbb{Z}/2\mathbb{Z}$
-27	1	$\mathbb{Z}/1\mathbb{Z}$
-28	1	$\mathbb{Z}/1\mathbb{Z}$
-31	3	$\mathbb{Z}/3\mathbb{Z}$
-32	2	$\mathbb{Z}/2\mathbb{Z}$
-35	2	$\mathbb{Z}/2\mathbb{Z}$
-36	2	$\mathbb{Z}/2\mathbb{Z}$
-39	4	$\mathbb{Z}/4\mathbb{Z}$
-40	2	$\mathbb{Z}/2\mathbb{Z}$
-43	1	$\mathbb{Z}/1\mathbb{Z}$
-44	3	$\mathbb{Z}/3\mathbb{Z}$
-47	5	$\mathbb{Z}/5\mathbb{Z}$
-48	2	$\mathbb{Z}/2\mathbb{Z}$
-51	2	$\mathbb{Z}/2\mathbb{Z}$
-52	2	$\mathbb{Z}/2\mathbb{Z}$
-55	4	$\mathbb{Z}/4\mathbb{Z}$
-56	4	$\mathbb{Z}/4\mathbb{Z}$
-59	3	$\mathbb{Z}/3\mathbb{Z}$
-60	2	$\mathbb{Z}/2\mathbb{Z}$
-63	4	$\mathbb{Z}/4\mathbb{Z}$
-64	2	$\mathbb{Z}/2\mathbb{Z}$
-67	1	$\mathbb{Z}/1\mathbb{Z}$
-68	4	$\mathbb{Z}/4\mathbb{Z}$
-71	7	$\mathbb{Z}/7\mathbb{Z}$
-72	2	$\mathbb{Z}/2\mathbb{Z}$
-75	2	$\mathbb{Z}/2\mathbb{Z}$
-76	3	$\mathbb{Z}/3\mathbb{Z}$
-79	5	$\mathbb{Z}/5\mathbb{Z}$
-80	4	$\mathbb{Z}/4\mathbb{Z}$
-83	3	$\mathbb{Z}/3\mathbb{Z}$
-84	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-87	6	$\mathbb{Z}/6\mathbb{Z}$
-88	2	$\mathbb{Z}/2\mathbb{Z}$
-91	2	$\mathbb{Z}/2\mathbb{Z}$
-92	3	$\mathbb{Z}/3\mathbb{Z}$
-95	8	$\mathbb{Z}/8\mathbb{Z}$
-96	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-99	2	$\mathbb{Z}/2\mathbb{Z}$
-100	2	$\mathbb{Z}/2\mathbb{Z}$
-103	5	$\mathbb{Z}/5\mathbb{Z}$
-104	6	$\mathbb{Z}/6\mathbb{Z}$
-107	3	$\mathbb{Z}/3\mathbb{Z}$
-108	3	$\mathbb{Z}/3\mathbb{Z}$
-111	8	$\mathbb{Z}/8\mathbb{Z}$
-112	2	$\mathbb{Z}/2\mathbb{Z}$
-115	2	$\mathbb{Z}/2\mathbb{Z}$
-116	6	$\mathbb{Z}/6\mathbb{Z}$
-119	10	$\mathbb{Z}/10\mathbb{Z}$
-120	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-123	2	$\mathbb{Z}/2\mathbb{Z}$
-124	3	$\mathbb{Z}/3\mathbb{Z}$
-127	5	$\mathbb{Z}/5\mathbb{Z}$
-128	4	$\mathbb{Z}/4\mathbb{Z}$
-131	5	$\mathbb{Z}/5\mathbb{Z}$
-132	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-135	6	$\mathbb{Z}/6\mathbb{Z}$
-136	4	$\mathbb{Z}/4\mathbb{Z}$
-139	3	$\mathbb{Z}/3\mathbb{Z}$
-140	6	$\mathbb{Z}/6\mathbb{Z}$
-143	10	$\mathbb{Z}/10\mathbb{Z}$
-144	4	$\mathbb{Z}/4\mathbb{Z}$
-147	2	$\mathbb{Z}/2\mathbb{Z}$
-148	2	$\mathbb{Z}/2\mathbb{Z}$
-151	7	$\mathbb{Z}/7\mathbb{Z}$
-152	6	$\mathbb{Z}/6\mathbb{Z}$
-155	4	$\mathbb{Z}/4\mathbb{Z}$
-156	4	$\mathbb{Z}/4\mathbb{Z}$
-159	10	$\mathbb{Z}/10\mathbb{Z}$
-160	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-163	1	$\mathbb{Z}/1\mathbb{Z}$
-164	8	$\mathbb{Z}/8\mathbb{Z}$
-167	11	$\mathbb{Z}/11\mathbb{Z}$
-168	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-171	4	$\mathbb{Z}/4\mathbb{Z}$
-172	3	$\mathbb{Z}/3\mathbb{Z}$
-175	6	$\mathbb{Z}/6\mathbb{Z}$
-176	6	$\mathbb{Z}/6\mathbb{Z}$
-179	5	$\mathbb{Z}/5\mathbb{Z}$
-180	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-183	8	$\mathbb{Z}/8\mathbb{Z}$
-184	4	$\mathbb{Z}/4\mathbb{Z}$
-187	2	$\mathbb{Z}/2\mathbb{Z}$
-188	5	$\mathbb{Z}/5\mathbb{Z}$
-191	13	$\mathbb{Z}/13\mathbb{Z}$
-192	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-195	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-196	4	$\mathbb{Z}/4\mathbb{Z}$
-199	9	$\mathbb{Z}/9\mathbb{Z}$
-200	6	$\mathbb{Z}/6\mathbb{Z}$
-203	4	$\mathbb{Z}/4\mathbb{Z}$
-204	6	$\mathbb{Z}/6\mathbb{Z}$
-207	6	$\mathbb{Z}/6\mathbb{Z}$
-208	4	$\mathbb{Z}/4\mathbb{Z}$
-211	3	$\mathbb{Z}/3\mathbb{Z}$
-212	6	$\mathbb{Z}/6\mathbb{Z}$
-215	14	$\mathbb{Z}/14\mathbb{Z}$
-216	6	$\mathbb{Z}/6\mathbb{Z}$
-219	4	$\mathbb{Z}/4\mathbb{Z}$
-220	4	$\mathbb{Z}/4\mathbb{Z}$
-223	7	$\mathbb{Z}/7\mathbb{Z}$
-224	8	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
-227	5	$\mathbb{Z}/5\mathbb{Z}$
-228	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-231	12	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
-232	2	$\mathbb{Z}/2\mathbb{Z}$
-235	2	$\mathbb{Z}/2\mathbb{Z}$
-236	9	$\mathbb{Z}/9\mathbb{Z}$
-239	15	$\mathbb{Z}/15\mathbb{Z}$
-240	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-243	3	$\mathbb{Z}/3\mathbb{Z}$
-244	6	$\mathbb{Z}/6\mathbb{Z}$
-247	6	$\mathbb{Z}/6\mathbb{Z}$
-248	8	$\mathbb{Z}/8\mathbb{Z}$
-251	7	$\mathbb{Z}/7\mathbb{Z}$
-252	4	$\mathbb{Z}/4\mathbb{Z}$
-255	12	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
-256	4	$\mathbb{Z}/4\mathbb{Z}$
-259	4	$\mathbb{Z}/4\mathbb{Z}$
-260	8	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
-263	13	$\mathbb{Z}/13\mathbb{Z}$
-264	8	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
-267	2	$\mathbb{Z}/2\mathbb{Z}$
-268	3	$\mathbb{Z}/3\mathbb{Z}$
-271	11	$\mathbb{Z}/11\mathbb{Z}$
-272	8	$\mathbb{Z}/8\mathbb{Z}$
-275	4	$\mathbb{Z}/4\mathbb{Z}$
-276	8	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
-279	12	$\mathbb{Z}/12\mathbb{Z}$
-280	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-283	3	$\mathbb{Z}/3\mathbb{Z}$
-284	7	$\mathbb{Z}/7\mathbb{Z}$
-287	14	$\mathbb{Z}/14\mathbb{Z}$
-288	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-291	4	$\mathbb{Z}/4\mathbb{Z}$
-292	4	$\mathbb{Z}/4\mathbb{Z}$
-295	8	$\mathbb{Z}/8\mathbb{Z}$
-296	10	$\mathbb{Z}/10\mathbb{Z}$
-299	8	$\mathbb{Z}/8\mathbb{Z}$
-300	6	$\mathbb{Z}/6\mathbb{Z}$