6 Representations by Quadratic Forms

With the various things we have learned about quadratic forms so far, let us return to the basic representation problem of determining what values a given form $Q(x,y) = ax^2 + bxy + cy^2$ can take on when x and y are integers, or in other words, which numbers can be represented as $ax^2 + bxy + cy^2$ for some choice of integers x and y. Remember that it suffices to restrict attention to the values of Q appearing in the topograph since these are the values for primitive pairs (x,y), and to get all other values one just multiplies the values in the topograph by arbitrary squares. With this in mind we will adopt the following convention in the rest of the book:

When we say that a form Q represents a number n we mean that $n = Q(x,y)$ for some **primitive** *pair of integers $(x,y) \neq (0,0)$.*

This differs from the traditional terminology in which any solution of $n = Q(x,y)$ is called a representation of n, without requiring (x,y) to be a primitive pair, and when (x,y) is primitive it is called a proper or primitive representation of n. However, since we will rarely consider the case that (x,y) is not a primitive pair, it will save many words not to have to insert the extra modifier for every representation.

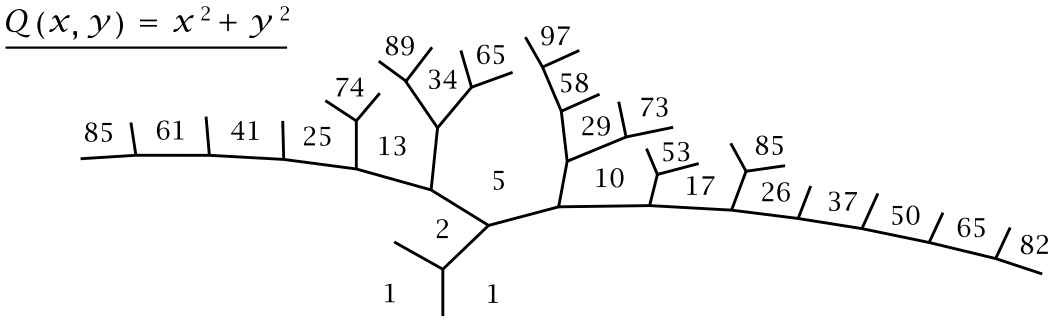
We will focus on forms that are either elliptic or hyperbolic, as these are the most interesting cases.

6.1 Three Levels of Complexity

In this section we will look at a series of examples to try to narrow down what sort of answer one could hope to obtain for the representation problem. The end result will be a reasonable guess that will be verified in the rest of this chapter and the next one, at least for fundamental discriminants. For nonfundamental discriminants there is sometimes a small extra wrinkle that seems to be rather subtle and more difficult to analyze.

As a first example let us try to find a general pattern in the values of the form $x^2 + y^2$. In view of the symmetry of the topograph for this form it suffices to look just in the first quadrant of the topograph. Part of this quadrant is shown in the figure

below, somewhat distorted to fit more numbers into the picture. What is shown is all the numbers in the topograph that are less than 100.



At first glance it may be hard to detect any patterns here. Both even and odd numbers occur, but none of the even numbers are divisible by 4 so they are all twice an odd number, and in fact an odd number that appears in the topograph. Considering the odd numbers, one notices they are all congruent to 1 mod 4 and not 3 mod 4, which is the other possibility for odd numbers. On the other hand, not all odd numbers congruent to 1 mod 4 appear in the topograph. Up to 100, the ones that are missing are 9, 21, 33, 45, 49, 57, 69, 77, 81, and 93. Each of these has at least one prime factor congruent to 3 mod 4, while all the odd numbers that do appear have all their prime factors congruent to 1 mod 4. Conversely, all products of primes congruent to 1 mod 4 are in the topograph.

This leads us to guess that the following might be true:

Conjecture. *The numbers that appear in the topograph of $x^2 + y^2$ are precisely the numbers $n = 2^a p_1 p_2 \cdots p_k$ where $a \le 1$ and each p_i is a prime congruent to 1 mod 4. Consequently, the values of the quadratic form $Q(x, y) = x^2 + y^2$ as x and y range over all integers (not just the primitive pairs) are exactly the numbers $n = m^2 p_1 p_2 \cdots p_k$ where m is an arbitrary integer and each p_i is either 2 or a prime congruent to 1 mod 4.*

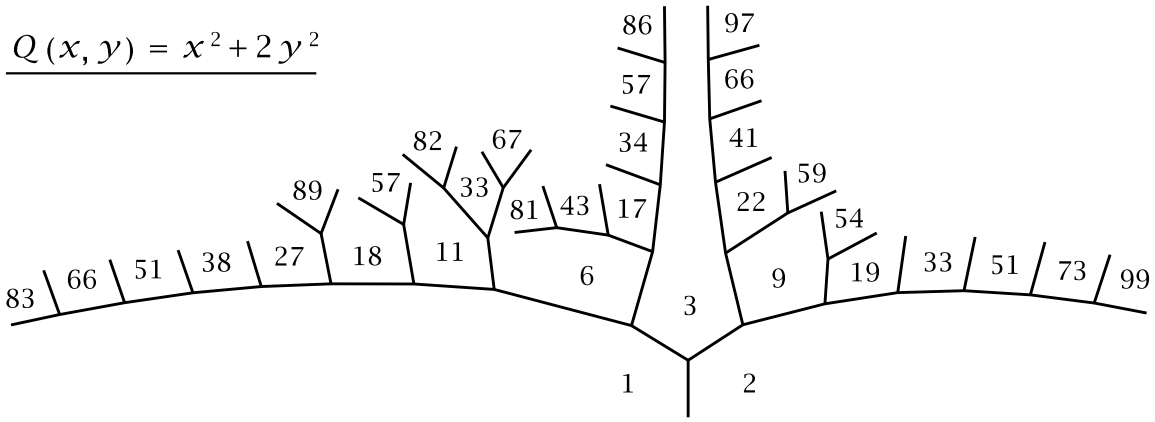
In both statements the index k denoting the number of prime factors p_i is allowed to be zero as well as any positive integer. The restriction $a \le 1$ in the first statement disappears in the second statement since higher powers of 2 can occur when we multiply by arbitrary squares. We will prove the conjecture later in the chapter.

A weaker form of the conjecture can be proved just by considering congruences mod 4 as follows. An even number squared is congruent to 0 mod 4 and an odd number squared is congruent to 1 mod 4, so $x^2 + y^2$ must be congruent to 0, 1, or 2 mod 4. Moreover, the only way that $x^2 + y^2$ can be 0 mod 4 is for both x and y to be even, which cannot happen for primitive pairs. Thus all numbers in the topograph must be congruent to 1 or 2 mod 4. This says that the odd numbers in the topograph are congruent to 1 mod 4 and the even numbers are each twice an odd number.

However, these simple observations say nothing about the role played by primes and prime factorizations, nor do they include any positive assertions about which

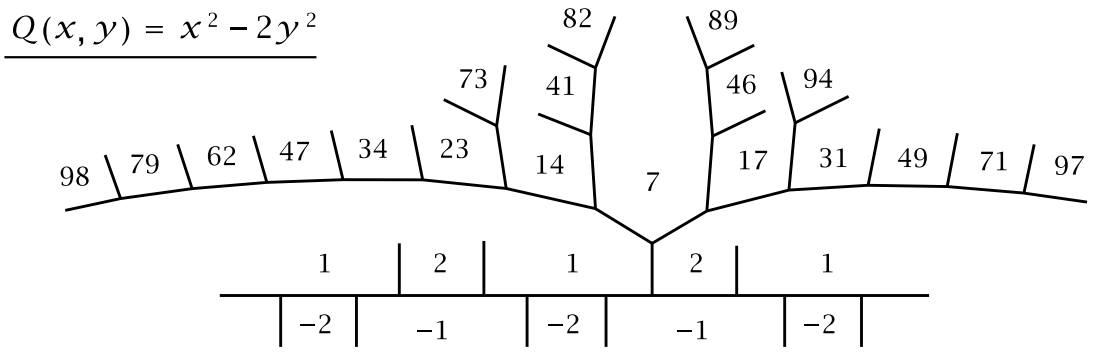
numbers actually are represented by $x^2 + y^2$. It definitely takes more work to show for example that every prime $p = 4k+1$ can be represented as the sum of two squares.

Let us look at a second example to see whether the same sorts of patterns occur, this time for the form $Q(x, y) = x^2 + 2y^2$. Here is a portion of its topograph showing all values less than 100, with the lower half of the topograph omitted since it is just the mirror image of the upper half:



Again the even values are just the doubles of the odd values. The odd prime values are $3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97$ and the other odd values are all the products of these primes. The odd prime values are not determined by their values mod 4 in this case, but instead by their values mod 8 since the primes we just listed are exactly the primes less than 100 that are congruent to 1 or 3 mod 8. Apart from this change, the answer to the representation problem for $x^2 + 2y^2$ is completely analogous to the answer for $x^2 + y^2$. Namely, the numbers represented by $x^2 + 2y^2$ are the numbers $n = 2^a p_1 p_2 \cdots p_k$ with $a \le 1$ and each p_i a prime congruent to 1 or 3 mod 8. Using congruences mod 8 we could easily prove the weaker statement that all numbers represented by $x^2 + 2y^2$ must be congruent to $1, 2, 3$, or 6 mod 8, so all odd numbers in the topograph must be congruent to 1 or 3 mod 8 and all even numbers must be twice an odd number.

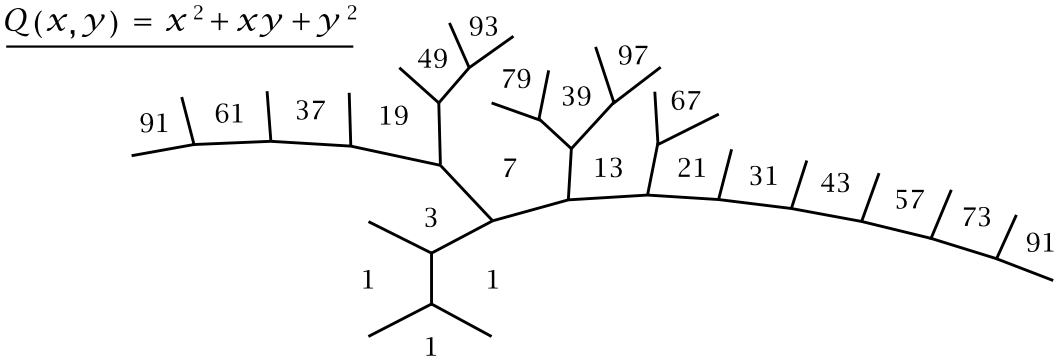
These two examples were elliptic forms, but the same sort of behavior can occur for hyperbolic forms as we see in the next example, the form $x^2 - 2y^2$. The negative values of this form happen to be just the negatives of the positive values, so we need only show the positive values in the topograph:



Here the primes that occur are 2 and primes congruent to ± 1 mod 8. The nonprime values that occur are the products of primes congruent to ± 1 mod 8 and twice these products. Again there is a weaker statement that can be proved using just congruences mod 8.

In these three examples the guiding principle was to look at prime factorizations and at primes modulo certain numbers, the numbers 4, 8, and 8 in the three cases. Notice that these numbers are just the absolute values of the discriminants -4, -8, and 8. Looking at primes mod $|\Delta|$ turns out to be a key idea for all quadratic forms.

Another example of the same sort is the form $x^2 + xy + y^2$ of discriminant -3. This time it is the prime 3 that plays a special role rather than 2.



We only have to draw one-sixth of the topograph because of all the symmetries. Notice that all the values are odd, so the prime 2 plays no role here. Since the discriminant is -3 we are led to consider congruences mod 3. The primes in the topograph are 3 and the primes congruent to 1 mod 3 (which in particular excludes the prime 2), namely the primes $7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97$. The nonprime values are the products of these primes with the restriction that the prime 3 never has an exponent greater than 1. This is analogous to the prime 2 never having an exponent greater than 1 in the preceding examples. In all four examples the "special" primes whose exponents are restricted are just the prime divisors of the discriminant. This is a general phenomenon, that primes dividing the discriminant behave differently from primes that do not divide the discriminant.

A special feature of the discriminants -4, -8, 8, and -3 is that in each case all forms of that discriminant are equivalent. We will see that the representation problem always has the same type of answer for discriminants with a single equivalence class of forms.

Before going on to the next level of complexity let us digress to describe a nice property that forms of the first level of complexity have. As we know, if an equation $Q(x,y) = n$ has an integer solution (x,y) then so does $Q(x,y) = m^2 n$ for every integer m. The converse is not always true however. For example the equation $2x^2 + 7y^2 = 9$ has the solution $(x,y) = (1,1)$ but $2x^2 + 7y^2 = 1$ obviously has no solution with x and y integers. Nevertheless, this converse property does hold for

forms such as those in the preceding four examples where the numbers n for which $Q(x,y) = n$ has an integer solution are exactly the numbers that can be factored as $n = m^2 p_1 p_2 \cdots p_k$ for primes p_i satisfying certain conditions and m an arbitrary integer. This is because if a number n has a factorization of this type then we can cancel any square factor of n and the result still has a factorization of the same type.

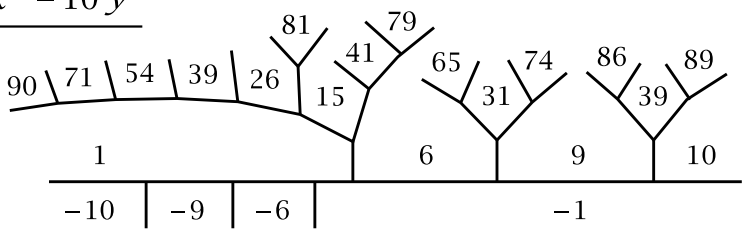
Let us apply this "square-cancellation" property in the case of the form x^2+y^2 to determine the numbers n such that the circle $x^2 + y^2 = n$ contains a rational point, and hence, as in Chapter 0, an infinite dense set of rational points. Suppose first that the circle $x^2 + y^2 = n$ contains a rational point, so after putting the two coordinates over a common denominator the point is $(x,y) = (a/c, b/c)$. The equation $x^2+y^2 = n$ then becomes $a^2 + b^2 = c^2 n$. This means that the equation $x^2 + y^2 = c^2 n$ has an integer solution. Then the square-cancellation property implies that the original equation $x^2 + y^2 = n$ has an integer solution. Thus we see that if there are rational points on the circle $x^2 + y^2 = n$ then there are integer points on it. This is not something that is true for all quadratic curves, as shown by the example of the ellipse $2x^2 + 7y^2 = 1$ which has rational points such as $(1/3, 1/3)$ but no integer points.

From the solution to the representation problem for $x^2 + y^2$ we deduce that the circle $x^2 + y^2 = n$ contains rational points exactly when $n = m^2 p_1 p_2 \cdots p_k$ where m is an arbitrary integer and each p_i is either 2 or a prime congruent to 1 mod 4. The first few values of n satisfying this condition are $1,2,4,5,8,9,10,13,16,17,18,20,\cdots$.

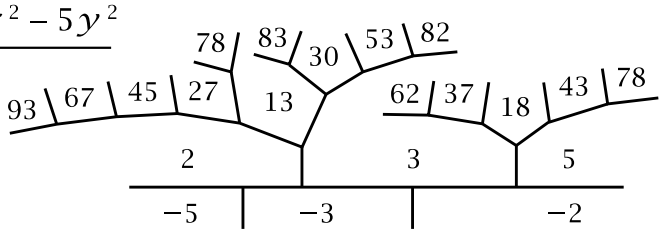
The Second Level of Complexity

For an example with slightly greater complexity consider discriminant 40 where the class number is 2 and two nonequivalent forms are $x^2 - 10y^2$ and $2x^2 - 5y^2$. The topographs below show the positive values less than 100.

$Q_1(x,y) = x^2 - 10y^2$



$Q_2(x,y) = 2x^2 - 5y^2$



The topographs are periodic and also have mirror symmetry so it suffices to show half of one period. There is no need to show any more of the negative values since these

will just be the negatives of the positive values.

For the form $x^2 - 10y^2$ the prime values less than 100 are $31, 41, 71, 79, 89$. These are the primes congruent to ± 1 or ± 9 mod 40, the discriminant. However, in contrast to what happened in the previous examples, there are many nonprime values of this form that are not products of these prime values. The prime factors of these nonprime values are $2, 3, 5, 13, 37, 43$, none of which occur in the topograph of the first form. Rather miraculously, these prime values are realized instead by the second form $2x^2 - 5y^2$. The prime values this form takes on are 2 and 5, which are the prime divisors of the discriminant 40, along with primes congruent to ± 3 and ± 13 mod 40, namely $3, 13, 37, 43, 53, 67$, and 83.

Apart from the primes 2 and 5 that divide the discriminant, the possible values of primes mod 40 are $\pm 1, \pm 3, \pm 7, \pm 9, \pm 11, \pm 13, \pm 17, \pm 19$ since even numbers and multiples of 5 are excluded. There are sixteen different congruence classes here, and exactly half of them, eight, are realized by one or the other of the two forms $x^2 - 10y^2$ and $2x^2 - 5y^2$, with four classes realized by each form. The other eight congruence classes are not realized by any form of discriminant 40 since every form of discriminant 40 is equivalent to one of the two forms $x^2 - 10y^2$ or $2x^2 - 5y^2$, as is easily checked by the methods from the previous chapter.

This turns out to be a general phenomenon valid for elliptic and hyperbolic forms of any discriminant Δ: If one excludes the primes that divide Δ, then the prime values of quadratic forms of discriminant Δ are exactly the primes in half of the congruence classes mod Δ of numbers coprime to Δ. This will be proved in Proposition 6.23. Also, each form represents primes in the same number of congruence classes. For $\Delta = 40$ this is four congruence classes for each form.

The primes 2 and 5 that divide the discriminant occur in the topographs only to the first power, and in fact no numbers in the topographs are divisible by 2^2 or 5^2. This is similar to what happened in the earlier examples where there was only one prime dividing the discriminant. Apart from this restriction it appears that each product of primes represented by Q_1 or Q_2 is also represented by Q_1 or Q_2. The problem is to decide which form represents which products. For numbers in the topographs not divisible by 2 or 5 it seems that these numbers are subject to the same congruence conditions as for primes, so they are congruent to ± 1 or ± 9 for Q_1 and to ± 3 or ± 13 for Q_2.

If one includes numbers divisible by 2 or 5 the following statements seem to be true, provided that numbers divisible by 2^2 or 5^2 are excluded:

- The product of two numbers represented by Q_1 is again represented by Q_1.
- The product of two numbers represented by Q_2 is represented by Q_1.
- The product of a number represented by Q_1 with a number represented by Q_2 is represented by Q_2.

To illustrate the first statement, the numbers 6, 9, and 10 appear in the topograph of Q_1 hence so do $6\cdot9$, $9\cdot9$, and $9\cdot10$, but not $6\cdot10$ since this is divisible by 2^2. For the second statement, the numbers 2, 3, and 5 are in the topograph of Q_2 so $2\cdot3$, $3\cdot3$, $2\cdot5$, and $3\cdot5$ are in the topograph of Q_1 but not $2\cdot2$ or $5\cdot5$. The product $2\cdot3\cdot5$ is then in the topograph of Q_2 by the third statement.

An abbreviated way of writing the three rules is by the formulas $Q_1Q_1 = Q_1$, $Q_2Q_2 = Q_1$, and $Q_1Q_2 = Q_2$. One can see that these are formally the same as the rules for addition of integers mod 2: $0+0=0$, $1+1=0$, and $0+1=1$. The two formulas $Q_1Q_1 = Q_1$ and $Q_1Q_2 = Q_2$ say that Q_1 serves as an identity element for this multiplication operation, and then the formula $Q_2Q_2 = Q_1$ can be interpreted as saying that Q_2 is equal to its own inverse, so $Q_2 = Q_2^{-1}$.

This way of "multiplying" forms is more than just shorthand notation, and in Chapter 7 we will develop a general method for forming products of primitive forms of a fixed discriminant that will be a key ingredient in reducing the representation problem to the special case of representing primes.

The various observations we have made so far about the two forms of discriminant 40 lead to the following:

Conjecture. *The positive numbers represented by either Q_1 or Q_2 are exactly the products $2^a5^bp_1p_2\cdots p_k$ where $a,b\le1$ and each p_i is a prime congruent to ±1, ±3, ±9, or ±13 mod 40. The form Q_1 represents the primes $p_i\equiv\pm1$ and ±9 while Q_2 represents 2, 5, and the primes $p_i\equiv\pm3$ and ±13. One can determine which form will represent a product $2^a5^bp_1p_2\cdots p_k$ by the rule that if the number of terms in the product that are represented by Q_2 is even then the product is represented by Q_1 and if it is odd then the product is represented by Q_2.*

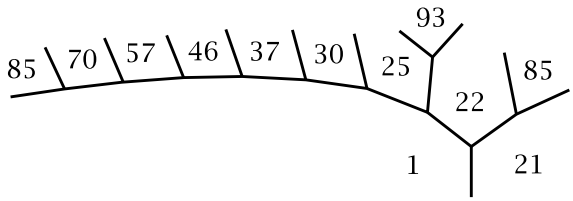
For example, the topograph of Q_1 contains the even powers of 3 while the topograph of Q_2 contains the odd powers. Another consequence is that the even values in one topograph are just the doubles of the odd values in the other topograph.

This characterization of numbers represented by these two forms also implies that no number is represented by both Q_1 and Q_2. However, for some discriminants it is possible for two nonequivalent forms of that discriminant to represent the same nonzero number, as we will see.

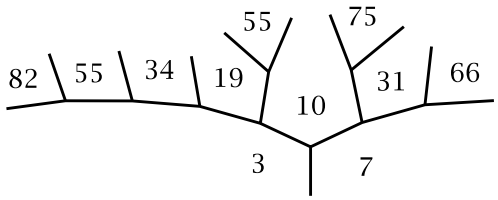
The Conjecture will be proved piece by piece as we gradually develop the necessary general theory. The first statement will be an application of Theorem 6.8 together with later facts in Section 6.2. The second statement will be an application of Proposition 6.19 and the rest of the Conjecture will use results from Chapter 7, particularly Theorem 7.7.

Let us look at another example where the representation problem has an answer that is qualitatively similar to the preceding example but just a little more complicated, the case of discriminant -84. Here there are twice as many equivalence classes of forms, four instead of two, with topographs shown below.

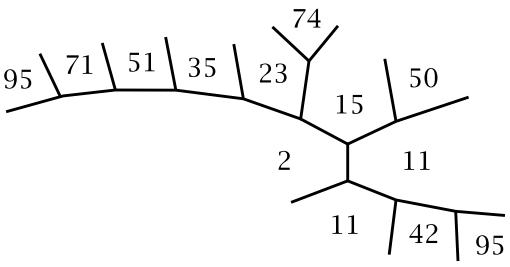
$Q_1(x,y) = x^2+21y^2$



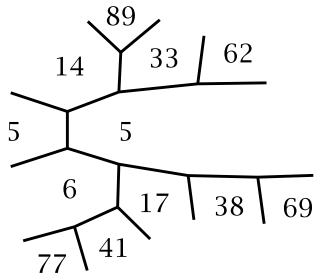
$Q_2(x,y) = 3x^2+7y^2$



$Q_3(x,y) = 2x^2+2xy+11y^2$



$Q_4(x,y) = 5x^2+4xy+5y^2$



The primes dividing the discriminant -84 are 2, 3, and 7, and these primes are each represented by one of the forms. In fact the divisors of the discriminant that appear in the topographs are $1, 2, 3, 6, 7, 14, 21$, and 42 which are precisely the squarefree divisors of the discriminant. These squarefree divisors of Δ are exactly the numbers appearing on reflector lines of mirror symmetries of the topographs. This was the case also in the previous examples, as one can check, and is a general phenomenon for fundamental discriminants as we saw in Propositions 5.6 and 5.7.

For the primes not dividing the discriminant, we will show in Section 6.3 that the primes represented by each form are as follows:

- For Q_1 the primes $p \equiv 1, 25, 37 \bmod 84$.
- For Q_2 the primes $p \equiv 19, 31, 55 \bmod 84$.
- For Q_3 the primes $p \equiv 11, 23, 71 \bmod 84$.
- For Q_4 the primes $p \equiv 5, 17, 41 \bmod 84$.

This agrees with what is shown in the four topographs above, and one could expand the topographs to get further evidence that these are the right answers. Passing from primes to arbitrary numbers appearing in at least one of the topographs, these appear to be exactly the products $2^a 3^b 7^c p_1 \cdots p_k$ with $a, b, c \le 1$ and each p_i one of the other primes represented by Q_1, Q_2, Q_3, or Q_4.

One can work out hypothetical rules for multiplying the forms by considering how products of two primes are represented. For example, 3 is represented by Q_2 and 11 is represented by Q_3, while their product $3 \cdot 11 = 33$ is represented by Q_4, so

we might guess that $Q_2Q_3 = Q_4$. Some other products that give the same conclusion are $3\cdot2 = 6$, $3\cdot23 = 69$, $7\cdot2 = 14$, $7\cdot11 = 77$, and $31\cdot2 = 62$. In the same way one can determine tentative rules for all the products Q_iQ_j, with the following results:

- The principal form Q_1 acts as the identity, so $Q_1Q_i = Q_i$ for each i.
- $Q_iQ_i = Q_1$ for each i so each Q_i equals its own inverse.
- The product of any two out of Q_2, Q_3, Q_4 is equal to the third.

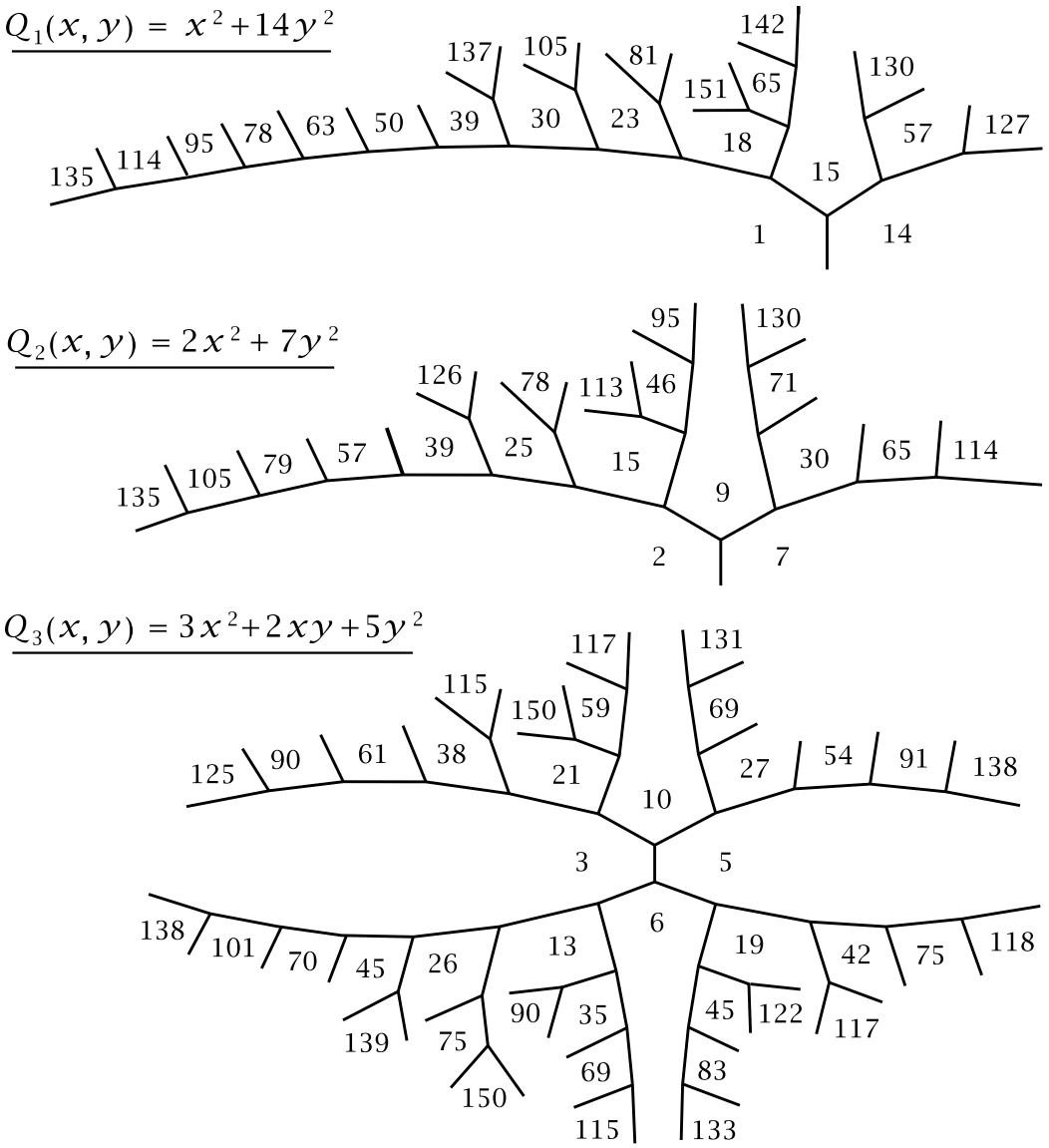
These multiplication rules are formally identical to how one would add pairs (m,n) of integers mod 2 by adding their two coordinates separately. The form Q_1 corresponds to $(0,0)$ and the first of the three rules above becomes $(0,0)+(m,n) = (m,n)$. The forms Q_2, Q_3, and Q_4 correspond to $(1,0)$, $(0,1)$, and $(1,1)$ in any order, and the second rule above becomes $(m,n)+(m,n) = (0,0)$ which is valid for addition mod 2, while the third rule becomes the fact that the sum of any two of $(1,0)$, $(0,1)$, and $(1,1)$ is equal to the third if we do addition mod 2.

The multiplication rules determine which form represents a given number n by replacing each prime in the prime factorization of n by the form Q_i that represents it, then multiplying out the resulting product using the three multiplication rules, keeping in mind that 2, 3, and 7 can never occur with an exponent greater than 1. For example, for $n = 70 = 2\cdot5\cdot7$ we get the product $Q_3Q_4Q_2$ which equals Q_1 and so 70 is represented by Q_1, as the topograph shows. For $n = 66 = 2\cdot3\cdot11$ we get $Q_3Q_2Q_3 = Q_2$ and 66 is represented by Q_2. In general, for a number $n = 2^a3^b7^cp_1\cdots p_k$ we can determine which form represents n by the following steps. First compute the number q_i of prime factors of n represented by Q_i. Next compute the sum $q_1(0,0) + q_2(1,0) + q_3(0,1) + q_4(1,1) = (q_2+q_4, q_3+q_4)$ where $(0,0),(1,0),(0,1),(1,1)$ correspond to Q_1,Q_2,Q_3,Q_4 respectively. The resulting sum (r,s) mod 2 then tells which form represents n.

An interesting feature of all the forms at the first or second level of complexity that we have examined so far is that their topographs have mirror symmetry. This is actually a general phenomenon: Whenever all the forms of a given discriminant have mirror symmetry, then one can determine which primes are represented by each form just in terms of congruence conditions modulo the discriminant. And in fact this is the only time when congruences modulo the discriminant determine how primes are represented, at least if one restricts attention just to primitive forms. This will be shown in Corollary 6.29. In Chapter 5 we called discriminants for which all primitive forms have mirror symmetry *fully symmetric* discriminants, and we observed that they are unfortunately rather rare, with only 101 negative discriminants known to have this property, and probably no more.

The Third Level of Complexity

A deeper degree of complexity is illustrated by the case $\Delta = -56$ where there are three equivalence classes of forms, with topographs shown below. The first two topographs have mirror symmetry but the third topograph does not, so the third form counts twice when determining the class number for discriminant -56, which is therefore 4 rather than 3.



The behavior of divisors of the discriminant is the same as in the previous examples. Only the squarefree divisors appear, 1, 2, 7, and 14, and these are the numbers appearing on the reflector lines.

In the examples at the first two levels of complexity it was possible to determine which numbers are represented by a given form by looking at primes and which congruence classes they fall into modulo the discriminant. The primes represented by a given form were exactly the primes in certain congruence classes modulo the discriminant. This is no longer true for discriminant -56 however. For example the primes 23 and 79 are congruent mod 56, and yet 23 is represented by $Q_1 = x^2 + 14y^2$ since

$Q_1(3,1) = 23$, while 79 is represented by $Q_2 = 2x^2 + 7y^2$ since $Q_2(6,1) = 79$.

Another nice property that held in the previous examples was that no number appeared in more than one topograph for the given discriminant, but this too fails for discriminant -56 since there are many nonprimes that occur in the topographs of both Q_1 and Q_2 starting with $15, 30, 39, 57, 65, 78, 95, 105, 114, 130$, and 135.

Apart from the primes 2 and 7 that divide the discriminant -56, all other primes belong to the following 24 congruence classes mod 56, corresponding to odd numbers less than 56 not divisible by 7:

$$\underline{1}\ \overline{3}\ \overline{5}\ \underline{9}\ 11\ \overline{13}\ \underline{15}\ 17\ \overline{19}\ \underline{23}\ \underline{25}\ \overline{27}\ 29\ 31\ 33\ 37\ \underline{39}\ 41\ 43\ \overline{45}\ 47\ 51\ 53\ 55$$

The six congruence classes whose prime elements are represented by Q_1 or Q_2 are indicated by underlines, and the six congruence classes whose prime elements are represented by Q_3 are indicated by overlines. Primes not represented by any of the three forms are in the remaining twelve congruence classes.

The new thing that happens in this example is that one cannot tell whether a prime is represented by Q_1 or Q_2 just by considering congruence classes mod the discriminant. We saw this for the pair of primes 23 and 79, and another such pair visible in the topographs is 71 and 127. By extending the topographs we could find many more such pairs. One might try using congruences modulo some other number besides 56, but it is known that this does not help.

Congruences mod 56 suffice to tell which primes are represented by Q_3, but there is a different sort of novel behavior involving Q_3 when we look at representing products of primes. To illustrate this, observe that the primes 3 and 5 are represented by Q_3 but their product 15 is represented by both Q_1 and Q_2. This means there is some ambiguity about whether the product Q_3Q_3 should be Q_1 or Q_2. The same thing happens in fact for any pair of coprime numbers represented by Q_3, for example 5 and 6 whose product is represented by both Q_1 and Q_2.

For other products Q_iQ_j there seems to be no ambiguity. The principal form Q_1 acts as the identity for multiplication, while $Q_2Q_2 = Q_1$ and $Q_2Q_3 = Q_3$, although this last formula is somewhat odd since it seems to imply that Q_3 does not have a multiplicative inverse since if it did, we could multiply the equation $Q_2Q_3 = Q_3$ by this inverse to get $Q_2 = Q_1$.

There is a way out of these difficulties, discovered by Gauss. The troublesome form Q_3 is different from the other forms in this example and in the preceding examples in that it does not have mirror symmetry. Thus the equivalence class of Q_3 splits into two proper equivalence classes, with Q_3 having a mirror image form $Q_4 = 3x^2 - 2xy + 5y^2$ obtained from Q_3 by changing the sign of either x or y and hence changing the coefficient of xy to its negative. Using Q_4 we can then resolve the ambiguous product Q_3Q_3 by setting $Q_3Q_3 = Q_2 = Q_4Q_4$ and $Q_3Q_4 = Q_1$ so that Q_4 is the inverse of Q_3. This means that each Q_i has its inverse given by the mirror image topograph since Q_1 and Q_2 have mirror symmetry and equal their own inverses.

The rigorous justification for the formulas $Q_3Q_3 = Q_2 = Q_4Q_4$ and $Q_3Q_4 = Q_1$ will come in Chapter 7, but for the moment one can check that these formulas are at least consistent with the topographs.

Since $Q_3^2 = Q_2$ we have $Q_3^4 = Q_2^2 = Q_1$. Multiplying the equation $Q_3^4 = Q_1$ by Q_4, the inverse of Q_3, gives $Q_3^3 = Q_4$. Thus all four proper equivalence classes of forms are powers of the single form Q_3 since $Q_3^2 = Q_2$, $Q_3^3 = Q_4$, and $Q_3^4 = Q_1$. This is corroborated by the representations of powers of 3 since 3 is represented by Q_3, 3^2 by $Q_3^2 = Q_2$, 3^3 by $Q_3^3 = Q_4$, and 3^4 by $Q_3^4 = Q_1$. Products of powers Q_3^i are computed by adding exponents mod 4 since Q_3^4 is the identity. Thus multiplication of the four forms is formally identical with addition of integers mod 4. The earlier doubtful formula $Q_2Q_3 = Q_3$ is resolved into the two formulas $Q_2Q_3 = Q_4$ and $Q_2Q_4 = Q_3$, which become $Q_3^2Q_3 = Q_3^3$ and $Q_3^2Q_3^3 = Q_3^5 = Q_3$.

The appearance of the same number in two different topographs is easy to explain now that we have two forms Q_3 and Q_4 representing exactly the same numbers. For example, to find all appearances of the number $15 = 3\cdot 5$ in the topographs we observe that its prime factors 3 and 5 appear in the topographs of both Q_3 and Q_4 so 15 will appear in the topographs of $Q_3Q_3 = Q_2$, $Q_3Q_4 = Q_1$, and $Q_4Q_4 = Q_2$, although this last formula gives no new representations.

The procedure for finding which forms represent a number $n = 2^a7^bp_1\cdots p_k$ with $a, b \le 1$ and primes p_i different from 2 or 7 is to replace each prime factor in this product by a form Q_j that represents it, then multiply out the resulting product of forms Q_j. There is also an extra condition that will be justified in Chapter 7: Whenever a prime p_i appears more than once in the prime factorization of n, we should replace all of its appearances by the same Q_j. For example, the forms representing $18 = 2\cdot 3^2$ are just the products $Q_2Q_3^2 = Q_1$ and $Q_2Q_4^2 = Q_1$ and not $Q_2Q_3Q_4 = Q_2$, as one can see in the topographs. Similarly, $9 = 3\cdot 3$ is represented only by $Q_3^2 = Q_2 = Q_4^2$ and not by $Q_3Q_4 = Q_1$.

We will show in Chapter 7 that the set of proper equivalence classes of primitive forms of fixed discriminant always has a multiplication operation compatible with multiplying values of forms of that discriminant in the way illustrated by the preceding examples. This multiplication operation gives this set the structure of a group, that is, a set with an associative multiplication operation for which there is an element of the set that functions as an identity for the multiplication, and such that each element of the set has a multiplicative inverse in the set whose product with the given element is the identity element. The set of proper equivalence classes of primitive forms with this group structure is called the *class group* for the given discriminant. The identity element is the class of the principal form, and the inverse of a class is obtained by taking the mirror image topograph.

The class group has the additional property that the multiplication is commutative. This makes its algebraic structure much simpler than the typical noncommuta-

tive group. An example of a noncommutative group that we have seen is the group $LF(\mathbb{Z})$ of linear fractional transformations, where the multiplication comes from multiplication of 2×2 matrices, or equivalently, composition of the transformations.

For a given discriminant, if the numbers represented by two primitive forms cannot be distinguished by congruences modulo the discriminant, then these two forms are said to belong to the same ***genus***. Thus in the preceding example of discriminant -56 the two forms Q_1 and Q_2 are of the same genus while Q_3 is of a different genus from Q_1 and Q_2, so there are two different genera ("genera" is the plural of "genus").

Equivalent forms always belong to the same genus since their topographs contain exactly the same numbers. The first two of the three levels of complexity we have described correspond to the discriminants where there is only one equivalence class in each genus. As we stated earlier, this desirable situation is also characterized by the condition that all primitive forms of the given discriminant have mirror symmetry. For larger discriminants there can be large numbers of genera and large numbers of equivalence classes within a genus. However, for a fixed discriminant there are always the same number of proper equivalence classes within each genus, as we will show in Corollary 7.27. This is illustrated by the case $\Delta = -56$ where one genus consists of Q_1 and Q_2 and the other genus consists of Q_3 and Q_4.

Dirichlet's Theorem on Primes in Arithmetic Progressions

The examples in this section show the significance of primes in certain congruence classes for solving the representation problem. In the examples there seems to be no shortage of primes in each of the relevant congruence classes. For example, for the form $x^2 + y^2$ the primes represented, apart from 2, seem to be the primes congruent to 1 mod 4, the primes of the form $4k + 1$ starting with $5, 13, 17, 29, 37, 41, 53, \cdots$. The other possibility for odd primes is the sequence $3, 7, 11, 19, 23, 31, 43, 47, \cdots$, primes of the form $4k + 3$, or equivalently $4k - 1$.

Such sequences form arithmetic progressions $an + b$ for fixed positive integers a and b and varying $n = 0, 1, 2, 3, \cdots$. It is natural to ask whether there are infinitely many primes in each arithmetic progression $an + b$. For this to be true an obvious restriction is that a and b should be coprime since any common divisor of a and b will divide every number $an + b$, so there could be at most one prime in the progression.

A famous theorem of Dirichlet from 1837 asserts that every arithmetic progression $an + b$ with a and b coprime contains an infinite number of primes. This can be rephrased as saying that within each congruence class of numbers $x \equiv b$ mod a there are infinitely many primes whenever a and b are coprime. Dirichlet's theorem actually says more, that primes are approximately equally distributed among the various congruence classes mod a for a fixed a. For example, there are approximately as many primes $p = 4n + 1$ as there are primes $p = 4n - 1$.

Dirichlet's Theorem is not easy to prove, and a proof would require methods quite different from anything else in this book so we will not be giving a proof. However a few special cases of Dirichlet's Theorem can be proved by elementary arguments. The simplest case is the arithmetic progression $3, 7, 11, \cdots$ of numbers $n = 4n - 1$, using a variant of Euclid's proof that there are infinitely many primes. First let us recall how Euclid's argument goes: Suppose that $p_1, \cdots, p_k$ is a finite list of primes, and consider the number $N = p_1 \cdots p_k + 1$. This must be divisible by some prime p, but p cannot be any of the primes p_i on the list since dividing p_i into N gives a remainder of 1. Thus no finite list of primes can be complete and hence there must be infinitely many primes.

To adapt this argument to primes of the form $4n-1$, suppose that $p_1, \cdots, p_k$ is a finite list of such primes, and consider the number $N = 4p_1 \cdots p_k - 1$. The prime divisors of N must be odd since N is odd. If all these prime divisors were of the form $4n + 1$ then N would be a product of numbers of the form $4n + 1$ hence N itself would have this form, contradicting the fact that N has the form $4n - 1$. Hence N must have a prime factor $p = 4n - 1$. This p cannot be any of the primes p_i since dividing p_i into N gives a remainder of -1. Thus no finite list of primes $4n - 1$ can be a complete list.

This argument does not work for primes $p = 4n + 1$ since a number $N = 4p_1 \cdots p_k + 1$ can be a product of primes of the form $4n - 1$, for example $21 = 3 \cdot 7$, so one could not deduce that N had a prime factor $p = 4n + 1$.

However, the quadratic form $x^2 + y^2$ can be used to show there are infinitely many primes $p = 4n + 1$. In Proposition 6.18 we will show that for each discriminant Δ there are infinitely many primes represented by forms of discriminant Δ. In the case $\Delta = -4$ all forms are equivalent to the form $x^2 + y^2$, so this form must represent infinitely many primes. None of these primes can be of the form $4n-1$ since all values of $x^2 + y^2$ are congruent to 0, 1, or 2 mod 4, as squares are always 0 or 1 mod 4. Thus there must be infinitely many primes $p = 4n + 1$.

The same arguments work also for primes $p = 3n + 1$ and $p = 3n - 1$. For $p = 3n - 1$ one argues just as for $4n - 1$, using numbers $N = 3p_1 \cdots p_k - 1$. For $p = 3n + 1$ one uses the form $x^2 + xy + y^2$ of discriminant -3. Here again all forms of this discriminant are equivalent so Proposition 6.18 says that $x^2 + xy + y^2$ represents infinitely many primes. All values of $x^2 + xy + y^2$ are congruent to 0 or 1 mod 3 as one can easily check by listing the various possibilities for x and y mod 3. Thus there are infinitely many primes $p = 3n + 1$.

We can try these arguments for arithmetic progressions $5n \pm 1$ and $5n \pm 2$ but there are problems. The Euclidean argument we have given fails in each case for much the same reason that it failed for primes $p = 4n + 1$. For the approach via quadratic forms we would use the form $x^2 + xy - y^2$ of discriminant 5. This is the only form of this discriminant, up to equivalence, so Proposition 6.18 implies that it represents

infinitely many primes. The methods in the next section will show that the primes represented by this form are the primes $p = 5n \pm 1$, so there are infinitely many primes $p = 5n+1$ or $p = 5n-1$ but we cannot be more specific than this. Dirichlet's Theorem says there are infinitely primes of each type, and in fact there are fancier forms of the Euclidean argument that prove this, but these Euclidean arguments do not work for the other cases $p = 5n \pm 2$.

We have just seen three quadratic forms that represent infinitely many primes, for discriminants -4, -3, and 5, and Proposition 6.18 provides other examples for each discriminant with class number 1. (Nonprimitive forms obviously cannot represent infinitely many primes, so these forms can be ignored.) For discriminants with larger class numbers Proposition 6.18 only implies that there is at least one form representing infinitely many primes. However there is another hard theorem of Dirichlet which does say that each primitive form of nonsquare discriminant represents infinitely many primes.

Exercises

1. For the form $Q(x,y) = x^2 + xy - y^2$ do the following things:

(a) Draw enough of the topograph to show all the values less than 100 that occur in the topograph. This form is hyperbolic and it takes the same negative values as positive values, so you need not draw all the negative values.

(b) Make a list of the primes less than 100 that occur in the topograph, and a list of the primes less than 100 that do not occur.

(c) Characterize the primes in the two lists in part (b) in terms of congruence classes mod $|\Delta|$ where Δ is the discriminant of Q.

(d) Characterize the nonprime values in the topograph in terms of their factorizations into primes in the lists in part (b).

(e) Summarize the previous parts by giving a simple criterion for determining the numbers n such that $Q(x,y) = n$ has an integer solution (x,y), primitive or not. The criterion should say something like $Q(x,y) = n$ is solvable if and only if $n = m^2 p_1 \cdots p_k$ where each p_i is a prime such that ...

(e) Check that all forms having the same discriminant as Q are equivalent to Q.

2. Do the same things for the form $x^2 + xy + 2y^2$, except that this time you only need to consider values less than 50 instead of 100.

3. For discriminant $\Delta = -24$ do the following:

(a) Verify that the class number is 2 and find two quadratic forms Q_1 and Q_2 of discriminant -24 that are not equivalent.

(b) Draw topographs for Q_1 and Q_2 showing all values less than 100. (You do not have to repeat parts of the topographs that are symmetric.)

(c) Divide the primes less than 100 into three lists: those represented by Q_1, those represented by Q_2, and those represented by neither Q_1 nor Q_2. (No primes are represented by both Q_1 and Q_2.)

(d) Characterize the primes in the three lists in part (c) in terms of congruence classes mod $|\Delta| = 24$.

(e) Characterize the nonprime values in the topograph of Q_1 in terms of their factorizations into primes in the lists in part (c), and then do the same thing for Q_2. Your answers should be in terms of whether there are an even or an odd number of prime factors from certain of the lists.

(f) Summarize the previous parts by giving a criterion for which numbers n the equation $Q_1(x, y) = n$ has an integer solution and likewise for the equation $Q_2(x, y) = n$.

4. This problem will show how things can be more complicated than in the previous problems.

(a) Show that the number of equivalence classes of forms of discriminant -23 is 2 while the number of proper equivalence classes is 3, and find reduced forms Q_1 and Q_2 of discriminant -23 that are not equivalent.

(b) Draw the topographs of Q_1 and Q_2 up to the value 70. (Again you do not have to repeat symmetric parts.)

(c) Find a number n that occurs in both topographs, and find the x and y values that give $Q_1(x_1, y_1) = n = Q_2(x_2, y_2)$. (This sort of thing never happens in the previous problems.)

(d) Find a prime p_1 in the topograph of Q_1 and a different prime p_2 in the topograph of Q_2 such that p_1 and p_2 are congruent mod $|\Delta| = 23$. (This sort of thing also never happens in the previous problems.)

5. Show there are infinitely many primes of the form $6m - 1$ by an argument similar to the one used for $4m - 1$.

6. Consider a discriminant $\Delta = q^2$, $q > 0$, corresponding to 0-hyperbolic forms. Using the description of the topographs of such forms obtained in the previous chapter, show:

(a) Every number is represented by at least one form of discriminant Δ, so in particular all primes are represented.

(b) The primes represented by a given form of discriminant Δ are exactly the primes in certain congruence classes mod q (and hence also mod Δ).

(c) For $q = 1, 2, 7$, and 15 determine the class number for discriminant $\Delta = q^2$ and find which primes are represented by the forms in each equivalence class.

6.2 Representations in a Fixed Discriminant

The problem of determining the numbers represented by a given form is difficult in general, so in this section we will consider the somewhat easier question of determining which numbers n are represented by at least one form of a given discriminant Δ, without specifying which form this will be. We refer to this as *representing n in discriminant Δ*.

On several occasions we will make use of the following fact: A form Q represents a number a if and only if Q is equivalent to a form $ax^2+bxy+cy^2$ with leading coefficient a. To see this, note first that the form $ax^2+bxy+cy^2$ obviously represents a when $(x,y) = (1,0)$, hence any form equivalent to $ax^2+bxy+cy^2$ also represents a. Conversely, if a form Q represents a then a appears in the topograph of Q, and by applying a suitable linear fractional transformation we can bring the region where a appears to the $1/0$ region, changing Q to an equivalent form $ax^2+bxy+cy^2$ where c is the new label on the $0/1$ region and b is the new label on the edge between the $1/0$ and $0/1$ regions.

Here is our first use of this principle:

Proposition 6.1. *If a number n is represented in discriminant Δ then so is every divisor of n.*

Thus for representations in a given discriminant, if we find which primes are represented and then which products of these primes are represented, we will have found all numbers that are represented.

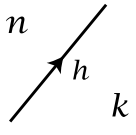
Proof: If n is represented in discriminant Δ then there is a form $nx^2+bxy+cy^2$ of discriminant Δ. If n factors as $n = n_1n_2$ then n_1 is represented by the form $n_1x^2+bxy+n_2cy^2$ which has the same discriminant as $nx^2+bxy+cy^2$. □

There is a simple congruence criterion for when a number is represented in a given discriminant:

Proposition 6.2. *There exists a form of discriminant Δ that represents n if and only if Δ is congruent to a square mod $4n$.*

Note that if n is negative then "mod $4n$" means the same thing as "mod $4|n|$" since being divisible by a number d is equivalent to being divisible by $-d$ when we are considering both positive and negative numbers.

Proof: Suppose n is represented by a form Q of discriminant Δ, so n appears in the topograph of Q. If we look at an edge of the topograph bordering a region labeled n then we obtain an equation $\Delta = h^2-4nk$ where h is the label on the edge and k is the label on the region on the opposite



side of this edge. The equation $\Delta = h^2 - 4nk$ implies the congruence $\Delta \equiv h^2 \bmod 4n$ so Δ is a square mod $4n$.

Conversely, suppose that Δ is the square of some integer h mod $4n$. This means that $h^2 - \Delta$ is an integer times $4n$, or in other words $h^2 - \Delta = 4nk$ for some k. This equation can be rewritten as $\Delta = h^2 - 4nk$, so the form $nx^2 + hxy + ky^2$ has discriminant Δ, and this form represents n when $(x, y) = (1, 0)$. □

Let us see what this proposition implies about representing small numbers n. For $n = 1$ it says that there is a form of discriminant Δ representing 1 if and only if Δ is a square mod 4. The squares mod 4 are 0 and 1, and we already know that discriminants of forms are always congruent to 0 or 1 mod 4. So we conclude that for every possible value of the discriminant there exists a form that represents 1. This is not new information, however, since the principal forms $x^2 + dy^2$ and $x^2 + xy + dy^2$ represent 1 and there is a principal form in each discriminant.

In the next case $n = 2$ the possible values of the discriminant mod $4n = 8$ are $0, 1, 4, 5$, and the squares mod 8 are $0, 1, 4$ since $0^2 = 0$, $(\pm1)^2 = 1$, $(\pm2)^2 = 4$, $(\pm3)^2 \equiv 1$, and $(\pm4)^2 \equiv 0$. Thus 2 is not represented by any form of discriminant Δ when $\Delta \equiv 5 \bmod 8$, but for all other discriminants there is a form representing 2. Explicit forms representing 2 are $2x^2 - ky^2$ for $\Delta = 8k$, $2x^2 + xy - ky^2$ for $\Delta = 8k+1$, and $2x^2 + 2xy - ky^2$ for $\Delta = 8k + 4$.

Moving on to the next case $n = 3$, the discriminants mod 12 are $0, 1, 4, 5, 8, 9$ and the squares mod 12 are $0, 1, 4, 9$ since $0^2 = 0$, $(\pm1)^2 = 1$, $(\pm2)^2 = 4$, $(\pm3)^2 = 9$, $(\pm4)^2 \equiv 4$, $(\pm5)^2 \equiv 1$, and $(\pm6)^2 \equiv 0$. The excluded discriminants are thus those congruent to 5 or 8 mod 12. Again explicit forms are easily given, the forms $3x^2 + hxy - ky^2$ with $\Delta = 12k + h^2$ for $h = 0, 1, 2, 3$.

We could continue in this direction, exploring which discriminants have forms that represent a given number, but this is not really the question we want to answer, which is to start with a given discriminant and decide which numbers are represented in this discriminant. The sort of answer we are looking for, based on the various examples we looked at earlier, is also a different sort of congruence condition, with congruence modulo the discriminant rather than congruence mod $4n$. So there is more work to be done before we would have the sort of answer we want. Nevertheless, the representability criterion in Proposition 6.2 is the starting point.

Our approach will be to reduce the representation problem in discriminant Δ first to the case of representing prime powers and then to representing primes themselves. Here is the first step.

Proposition 6.3. *If two coprime numbers m and n are both represented in discriminant Δ then so is their product mn.*

Applying this repeatedly, we see that if a number n has the prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes p_i, and if $p_i^{e_i}$ is represented in discriminant Δ for

each i, then n is represented in discriminant Δ.

The main ingredient in the proof of the proposition will be the following:

Lemma 6.4. *If a number x is a square mod m_1 and also a square mod m_2 where m_1 and m_2 are coprime, then x is a square mod m_1m_2.*

For example, the number 2 is a square mod 7 (since $3^2 \equiv 2 \mod 7$) and also mod 17 (since $6^2 \equiv 2 \mod 17$) so 2 must also be a square mod $7\cdot17 = 119$. And in fact $2 \equiv 11^2 \mod 119$.

Proof: This will be a consequence of the Chinese Remainder Theorem. If x is a square mod m_1 and also a square mod m_2 then there are numbers a_1 and a_2 such that $x \equiv a_1^2 \mod m_1$ and $x \equiv a_2^2 \mod m_2$. If m_1 and m_2 are coprime then by the Chinese Remainder Theorem there is a number a that is congruent to $a_1 \mod m_1$ and to $a_2 \mod m_2$, hence $a^2 \equiv a_1^2 \mod m_1$ and $a^2 \equiv a_2^2 \mod m_2$. Thus $x \equiv a^2 \mod m_1$ and $\mod m_2$. This implies $x \equiv a^2 \mod m_1m_2$ since the difference $x - a^2$ is divisible by both m_1 and m_2 and hence by their product m_1m_2 since m_1 and m_2 are coprime. This shows that x is a square mod m_1m_2. □

Proof of Proposition 6.3: Let m and n be coprime. At least one of them must be odd, say n is odd. If m and n are represented in discriminant Δ then Δ is a square mod $4m$ and mod $4n$, hence also mod n. Since $4m$ and n are coprime, the lemma then says that Δ is a square mod $4mn$, so mn is represented in discriminant Δ. □

Next we try to reduce further from prime powers to primes themselves. This is possible for most primes by the following more technical result:

Lemma 6.5. *If a number x is a square mod p for an odd prime p not dividing x, then x is also a square mod p^r for each $r > 1$. The corresponding statement for the prime $p = 2$ is that if an odd number x is a square mod 8 then x is also a square mod 2^r for each $r > 3$.*

For example, 2 is a square mod 7 since $2 \equiv 3^2 \mod 7$, so 2 is also a square mod 7^2, namely $2 \equiv 10^2 \mod 49$. It is also a square mod $7^3 = 343$ since $2 \equiv 108^2 \mod 343$. Likewise it must be a square mod 7^4, mod 7^5, etc. The proof of the lemma will give a method for refining the initial congruence $2 \equiv 3^2 \mod 7$ to each subsequent congruence $2 \equiv 10^2 \mod 49$, $2 \equiv 108^2 \mod 343$, etc.

For the prime $p = 2$ we have to begin with squares mod 8 since 3 is a square mod 2 but not mod 4, while 5 is a square mod 4 but not mod 8.

Proof of Lemma 6.5: We will show that if x is a square mod p^r then it is also a square mod p^{r+1}, assuming $r \geq 1$ in the case that p is odd and $r \geq 3$ in the case $p = 2$. By induction this will prove the lemma.

We begin by assuming that x is a square mod p^r, so there is a number y such that $x \equiv y^2 \mod p^r$ or in other words p^r divides $x - y^2$, say $x - y^2 = p^r l$ for

some integer l. We would like to find a number z such that $x \equiv z^2 \mod p^{r+1}$, so it is reasonable to look for a z with $z \equiv y \mod p^r$, or in other words $z = y + kp^r$ for some k. Thus we want to choose k so that $x \equiv (y + kp^r)^2 \mod p^{r+1}$. In other words we want p^{r+1} to divide $x - (y + kp^r)^2$. This can be rewritten as:

$$\begin{aligned} x - (y + kp^r)^2 &= x - (y^2 + 2kp^r y + k^2 p^{2r}) \\ &= x - y^2 - 2kp^r y - k^2 p^{2r} \\ &= p^r l - 2kp^r y - k^2 p^{2r} \quad \text{since } x - y^2 = p^r l \\ &= p^r (l - 2ky - k^2 p^r) \end{aligned}$$

For this to be divisible by p^{r+1} means that p should divide $l - 2ky - k^2 p^r$. Since we assume $r \geq 1$ this is equivalent to p dividing $l - 2ky$, or in other words, $l - 2ky = pq$ for some integer q. Rewriting this as $l = 2yk + pq$, we see that this linear Diophantine equation with unknowns k and q always has a solution when p is odd since $2y$ and p are coprime if p is odd, in view of the fact that p does not divide y since $x \equiv y^2 \mod p^r$ and we assume x is not divisible by p. This finishes the induction step in the case that p is odd.

When $p = 2$ this argument breaks down at the last step since the equation $l = 2yk + pq$ becomes $l = 2yk + 2q$ and this will not have a solution when l is odd. To modify the proof so that it works for $p = 2$ we would like to get rid of the factor 2 in the equation $l = 2yk + pq$ which arose when we squared $y + kp^r$. To do this, suppose that instead of trying $z = y + k \cdot 2^r$ we try $z = y + k \cdot 2^{r-1}$. Then we would want 2^{r+1} to divide $x - (y + k \cdot 2^{r-1})^2$. Again this can be rewritten:

$$\begin{aligned} x - (y + k \cdot 2^{r-1})^2 &= x - y^2 - k \cdot 2^r y - k^2 2^{2r-2} \\ &= 2^r l - k \cdot 2^r y - k^2 2^{2r-2} \quad \text{since } x - y^2 = 2^r l \\ &= 2^r (l - ky - k^2 2^{r-2}) \end{aligned}$$

Assuming $r \geq 3$, this means 2 should divide $l - ky$, or in other words $l = yk + 2q$ for some integer q. The number y is odd since $y^2 \equiv x \mod 2^r$ and x is odd by assumption. This implies the equation $l = yk + 2q$ has a solution (k, q). □

Proposition 6.6. *If a prime p not dividing the discriminant Δ is represented by a form of discriminant Δ then every power of p is also represented by a form of discriminant Δ.*

Proof: First we consider odd primes p. If p is represented in discriminant Δ then Δ is a square mod $4p$ and hence mod p. The preceding lemma then says that Δ is a square mod each power p^r. From this it follows by Lemma 6.4 that Δ is also a square mod $4p^r$ since Δ is always a square mod 4. Thus by Proposition 6.2 all powers of p are represented in discriminant Δ.

For $p = 2$ the argument is almost the same. In this case the representability of 2 implies that Δ is a square mod $4 \cdot 2 = 8$ so the lemma implies that Δ is also a square mod $4 \cdot 2^r$ for all $r \geq 1$ so all powers of 2 are represented. □

In the examples for the representation problem that we looked at in the preceding section we saw that primes that divide the discriminant behave differently from primes that do not, and the differences begin at this point:

Proposition 6.7. *Each prime dividing the discriminant Δ is represented in discriminant Δ. If a prime p divides Δ but not the conductor of Δ then no form of discriminant Δ represents p^2 or any higher power of p.*

Recall that the conductor for discriminant Δ is the largest positive number d such that $\Delta = d^2\Delta'$ for some discriminant Δ'. This Δ' is then a fundamental discriminant. Fundamental discriminants are those with conductor 1.

Proof: The representability of primes dividing Δ follows from Proposition 5.7, but it can also be deduced from the congruence criterion of Proposition 6.2 as follows. For a prime p dividing Δ we have $\Delta \equiv 0 \mod p$ so Δ is a square mod p, namely 0^2. When p is odd it follows that Δ is also a square mod $4p$ since Δ is always a square mod 4. Hence p is represented in discriminant Δ in this case. If p is 2 and divides Δ then $\Delta \equiv 0 \mod 4$ so $\Delta = 8k$ or $8k+4$. Thus $\Delta \equiv 0$ or $4 \mod 8$ and so Δ is a square mod 8, which means that 2 is represented in discriminant Δ.

Suppose now that p is a prime dividing Δ and some form of discriminant Δ represents p^2. This form is equivalent to a form $p^2x^2 + bxy + cy^2$ with p dividing $\Delta = b^2 - 4p^2c$ so p must divide b^2. Since p is prime it must then divide b, so in fact p^2 divides b^2. Therefore p^2 divides $\Delta = b^2 - 4p^2c$ and we have $\Delta = p^2\Delta'$ for some integer Δ'.

Consider first the case that p is odd. Then $p^2 \equiv 1 \mod 4$ so $\Delta \equiv \Delta' \mod 4$. This means that Δ' is also a discriminant, so by the definition of the conductor, p divides the conductor. Thus if p divides Δ but not the conductor then p^2 cannot be represented by any form of discriminant Δ.

In the case that $p = 2$ the assumption that p divides Δ means that Δ is even and hence so is b. The discriminant equation $\Delta = b^2 - 4p^2c$ is now $\Delta = b^2 - 4\cdot 2^2c$ so $\Delta \equiv b^2 \mod 16$. The only squares of even numbers mod 16 are 0 and 4, as one sees by checking 0^2, $(\pm2)^2$, $(\pm4)^2$, $(\pm6)^2$, and $(\pm8)^2$, so Δ is either $16k = 4(4k)$ or $16k+4 = 4(4k+1)$. In both cases Δ is 4 times a discriminant so 2 divides the conductor.

Once we know that p^2 is not represented in discriminant Δ then neither is any multiple of p^2 by Proposition 6.1, and in particular higher powers of p are not represented. □

Here is a summary of what we have shown so far in the case of fundamental discriminants:

Theorem 6.8. *If Δ is a fundamental discriminant then the numbers $n > 1$ that are represented by at least one form of discriminant Δ are exactly the numbers*

that factor as a product $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ *of powers of distinct primes* p_i *each of which is represented by some form of discriminant* Δ*, with the restriction that* $e_i \le 1$ *for primes* p_i *dividing* Δ*.*

The situation for nonfundamental discriminants is more complicated and will be described later in Theorem 6.11.

Quadratic Reciprocity

For the problem of determining which primes are represented in a given discriminant we already know when 2 is represented and we know that primes dividing the discriminant are always represented. After these special cases what remains are the odd primes not dividing the discriminant, which can be regarded as the generic case.

An odd prime p will be represented in discriminant Δ exactly when Δ is a square mod p. Let us introduce some convenient notation for this condition. For p an odd prime and a an integer not divisible by p, define the ***Legendre symbol*** $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is not a square mod } p \end{cases}$$

Using this notation we can say:

- *An odd prime* p *that does not divide* Δ *is represented in discriminant* Δ *if and only if* $\left(\frac{\Delta}{p}\right) = +1$*.*

It will therefore be useful to know how to compute $\left(\frac{a}{p}\right)$. The following four basic properties of the Legendre symbol make this a feasible task:

(1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(2) $\left(\frac{-1}{p}\right) = +1$ if $p \equiv 1 \mod 4$ and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv 3 \mod 4$.

(3) $\left(\frac{2}{p}\right) = +1$ if $p \equiv \pm 1 \mod 8$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3 \mod 8$.

(4) If p and q are distinct odd primes then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless p and q are both congruent to $3 \mod 4$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Property (1), applied repeatedly, reduces the calculation of $\left(\frac{a}{p}\right)$ to the calculation of $\left(\frac{q}{p}\right)$ for the various prime factors q of a, along with $\left(\frac{-1}{p}\right)$ when a is negative. Note that $\left(\frac{q^2}{p}\right) = +1$ so we can immediately reduce to the case that $|a|$ is a product of distinct primes. Property (2) will be used when dealing with negative discriminants, and property (3) will be used for certain even discriminants.

Property (4) is called ***quadratic reciprocity***. This is by far the most subtle of the four properties, and proving it is considerably more difficult than for the other three properties. We will give a proof in Section 6.4, obtaining proofs of the first three properties along the way.

For a quick illustration of the usefulness of these properties let us see how they can be used to compute the values of Legendre symbols. Suppose for example that

one wanted to know whether 78 was a square mod 89. The naive approach would be to list the squares of all the numbers $\pm1, \cdots, \pm44$ and see whether any of these was congruent to 78 mod 89, but this would be rather tedious. Since 89 is prime we can instead evaluate $\left(\frac{78}{89}\right)$ using the basic properties of Legendre symbols. First we factor 78 to get $\left(\frac{78}{89}\right) = \left(\frac{2}{89}\right)\left(\frac{3}{89}\right)\left(\frac{13}{89}\right)$. By property (3) we have $\left(\frac{2}{89}\right) = +1$ since $89 \equiv 1 \mod 8$. Next, reciprocity gives $\left(\frac{3}{89}\right) = \left(\frac{89}{3}\right)$ and $\left(\frac{13}{89}\right) = \left(\frac{89}{13}\right)$ since $89 \equiv 1 \mod 4$. After this we use the fact that $\left(\frac{a}{p}\right)$ depends only on the value of $a \mod p$ to reduce $\left(\frac{89}{3}\right)$ to $\left(\frac{2}{3}\right)$ and $\left(\frac{89}{13}\right)$ to $\left(\frac{11}{13}\right)$. Using property (3) again, we have $\left(\frac{2}{3}\right) = -1$, confirming the obvious fact that 2 is not a square mod 3. For $\left(\frac{11}{13}\right)$, reciprocity says this equals $\left(\frac{13}{11}\right)$. This reduces to $\left(\frac{2}{11}\right) = -1$. Summarizing, we have:

$$\left(\frac{78}{89}\right) = \left(\frac{2}{89}\right)\left(\frac{3}{89}\right)\left(\frac{13}{89}\right) = (+1)(-1)(-1) = +1$$

Thus we see that 78 is a square mod 89, even though we have not found an actual number x such that $x^2 \equiv 78 \mod 89$.

In this example we used the fact that the modulus 89 was prime, but we have already seen how to reduce to the case of prime moduli. For example, if we wanted to determine whether 78 is a square mod 88 we know this is the case exactly when it is a square mod 8 and mod 11. The squares mod 8 are 0, 1, and 4 whereas $78 \equiv 6 \mod 8$ so 78 is not a square mod 8 and therefore not mod 88 either, even though $78 \equiv 1 \mod 11$ so 78 is a square mod 11.

Returning now to quadratic forms, let us see what the basic properties of Legendre symbols tell us about which primes are represented by some of the forms discussed at the beginning of the chapter. In the first four cases the class number is 1 so we will be determining which primes are represented by the given form, and Theorem 6.8 will then say exactly which numbers are represented by this form, confirming the conjectures made when we looked at the topographs.

Example: $x^2 + y^2$ with $\Delta = -4$. This form obviously represents 2, the only prime dividing Δ, and it represents an odd prime p exactly when $\left(\frac{-4}{p}\right) = +1$. Using the first of the four properties we have $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)$, and the second property says this is $+1$ exactly for primes $p = 4k + 1$. Thus we see the primes represented by $x^2 + y^2$ are 2 and the primes $p = 4k + 1$.

Example: $x^2 + 2y^2$ with $\Delta = -8$. Again the only prime dividing Δ is 2, and it is represented. For odd primes p we have $\left(\frac{-8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^3 = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$. In the four cases $p \equiv 1, 3, 5, 7 \mod 8$ this is, respectively, $(+1)(+1)$, $(-1)(-1)$, $(+1)(-1)$, and $(-1)(+1)$. We conclude that the primes represented by the form $x^2 + 2y^2$ are 2 and primes congruent to 1 or 3 mod 8.

Example: $x^2 - 2y^2$ with $\Delta = 8$. The only prime dividing Δ is 2 which is represented when $(x, y) = (2, 1)$. For odd primes p we have $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right)$ so property (3) implies that the primes represented by $x^2 - 2y^2$ are 2 and $p \equiv \pm1 \mod 8$.

Example: x^2+xy+y^2 with $\Delta=-3$. The only prime dividing the discriminant is 3 and it is represented. The prime 2 is not represented since $\Delta\equiv 5 \bmod 8$. For primes $p>3$ we can evaluate $\left(\frac{-3}{p}\right)$ using quadratic reciprocity:

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=\begin{cases}(+1)\left(\frac{p}{3}\right) & \text{if } p=4k+1\\ (-1)\left(-\left(\frac{p}{3}\right)\right) & \text{if } p=4k+3\end{cases}$$

So we get $\left(\frac{p}{3}\right)$ in both cases. Since $\left(\frac{p}{3}\right)$ only depends on $p \bmod 3$, we have $\left(\frac{p}{3}\right)=+1$ if $p\equiv 1 \bmod 3$ and $\left(\frac{p}{3}\right)=-1$ if $p\equiv 2 \bmod 3$. (Since $p\neq 3$ we do not need to consider the possibility $p\equiv 0 \bmod 3$.) The conclusion is that the primes represented by x^2+xy+y^2 are 3 and the primes $p\equiv 1 \bmod 3$.

Example: $\Delta=40$. Here all forms are equivalent to either x^2-10y^2 or $2x^2-5y^2$. The primes dividing 40 are 2 and 5 so these are represented by one form or the other, and in fact both are represented by $2x^2-5y^2$ as the topographs showed. For other primes p we have $\left(\frac{40}{p}\right)=\left(\frac{2}{p}\right)^3\left(\frac{5}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{p}{5}\right)$. The factor $\left(\frac{2}{p}\right)$ depends only on $p \bmod 8$ and $\left(\frac{p}{5}\right)$ depends only on $p \bmod 5$, so their product depends only on $p \bmod 40$. The following table lists all the possibilities for congruence classes mod 40 not divisible by 2 or 5:

	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
$\left(\frac{2}{p}\right)$	+1	−1	+1	+1	−1	−1	+1	−1	−1	+1	−1	−1	+1	+1	−1	+1
$\left(\frac{p}{5}\right)$	+1	−1	−1	+1	+1	−1	−1	+1	+1	−1	−1	+1	+1	−1	−1	+1

The product $\left(\frac{2}{p}\right)\left(\frac{p}{5}\right)$ is $+1$ in exactly the eight cases $p\equiv 1,3,9,13,27,31,37,39 \bmod 40$. We conclude that these are the eight congruence classes containing primes (other than 2 and 5) represented by one of the two forms x^2-10y^2 and $2x^2-5y^2$. This agrees with our earlier observations based on the topographs. However, we have yet to verify our earlier guesses as to which congruence classes are represented by which form. We will see how to do this in the next section.

In the examples above we were able to express $\left(\frac{\Delta}{p}\right)$ in terms of Legendre symbols $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, and $\left(\frac{p}{p_i}\right)$ for odd primes p_i dividing Δ. The following result shows that this can be done for all Δ:

Proposition 6.9. *Let the nonzero integer Δ be factored as $\Delta=\varepsilon 2^s p_1\cdots p_k$ for $\varepsilon=\pm 1$, $s\geq 0$, and each p_i an odd prime. (We allow $k=0$ when $\Delta=\varepsilon 2^s$.) Then for odd primes p not dividing Δ the Legendre symbol $\left(\frac{\Delta}{p}\right)$ has the value given in the following table*:

Δ	$\left(\frac{\Delta}{p}\right)$
$2^{2l}(4m+1)$	$\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_k}\right)$
$2^{2l}(4m+3)$	$\left(\frac{-1}{p}\right)\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_k}\right)$
$2^{2l+1}(4m+1)$	$\left(\frac{2}{p}\right)\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_k}\right)$
$2^{2l+1}(4m+3)$	$\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_k}\right)$

Proof: For $\Delta = \varepsilon 2^s p_1 \cdots p_k$ quadratic reciprocity gives

$$\left(\frac{\Delta}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{2}{p}\right)^s \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_k}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{2}{p}\right)^s \left(\frac{\omega}{p}\right)\left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_k}\right)$$

where ω is $+1$ or -1 according to whether there are an even or an odd number of factors $p_i \equiv 3 \mod 4$. The exponent s in this formula can be replaced by 0 or 1 according to whether s is even or odd. In the first and third rows of the table the odd part of Δ is $4m+1$ so we have $\varepsilon = \omega$ and therefore $\left(\frac{\varepsilon}{p}\right)\left(\frac{\omega}{p}\right) = 1$. In the second and fourth rows the factor $4m+1$ is replaced by $4m+3$ and we have $\varepsilon = -\omega$, hence $\left(\frac{\varepsilon}{p}\right)\left(\frac{\omega}{p}\right) = \left(\frac{-1}{p}\right)$. □

Corollary 6.10. *The representability of an odd prime p in discriminant Δ depends only on the congruence class of p mod Δ.*

Proof: The class of p mod Δ determines its class mod p_i for each i and this determines $\left(\frac{p}{p_i}\right)$. For the terms $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ in the last three rows of the table, note first that l must be at least 1 in these rows since Δ is a discriminant. In the second row the class of p mod Δ determines its class mod 4 so it determines $\left(\frac{-1}{p}\right)$. In the third and fourth rows the class of p mod Δ determines its class mod 8 so both $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ are determined. Thus in all cases the factors of $\left(\frac{\Delta}{p}\right)$ are determined by the class of p mod Δ so $\left(\frac{\Delta}{p}\right)$ is determined. □

Complications for Nonfundamental Discriminants

Our next result generalizes Theorem 6.8 to cover all discriminants. As one can see, the general statement is considerably more complicated than for fundamental discriminants.

Theorem 6.11. *A number $n > 1$ is represented by at least one form of discriminant Δ exactly when n factors as a product $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ of powers of distinct primes p_i each of which is represented by some form of discriminant Δ, where $e_i \le 1$ for primes p_i dividing Δ but not the conductor, while for primes $p = p_i$ dividing the conductor the allowed exponents $e = e_i$ are given by the following rules. First write $\Delta = p^s q$ with p^s the highest power of p dividing Δ. Then if p is odd the allowable exponents e are those for which either*

(a) $e \le s$ *or*

(b) $e > s$, s *is even, and* $\left(\frac{q}{p}\right) = +1$.

If $p = 2$ then the allowable exponents e are those for which either

(a) $e \le s-2$ *or*

(b) s *is even and e is as in the following table:*

q mod 8	1	3	5	7
e	all	$\le s-1$	$\le s$	$\le s-1$

Examples will be given following the proof. The main part of the proof is contained in a lemma:

Lemma 6.12. *Suppose that a number x divisible by a prime p factors as $p^s q$ where p does not divide q, so p^s is the largest power of p dividing x. Then*:

(a) *x is a square mod p^r for each $r \le s$.*

(b) *If $r > s$ and s is odd then x is not a square mod p^r.*

(c) *If $r > s$ and s is even then x is a square mod p^r if and only if q is a square mod p^{r-s}.*

Proof: Part (a) is easy since x is 0 mod p^s hence also mod p^r if $r \le s$, and 0 is always a square mod anything.

For (b) we assume $r > s$ and s is odd. Suppose $p^s q$ is a square mod p^r, so $p^s q = y^2 + lp^r$ for some integers y and l. Then p^s divides $y^2 + lp^r$ and it divides lp^r (since $r > s$) so p^s divides y^2. Since s is assumed to be odd and the exponent of p in y^2 must be even, this implies p^{s+1} divides y^2. It also divides lp^r since $s+1 \le r$, so from the equation $p^s q = y^2 + lp^r$ we conclude that p divides q, contrary to the definition of q. This contradiction shows that $p^s q$ is not a square mod p^r when $r > s$ and s is odd, so statement (b) is proved.

For (c) we assume $r > s$ and s is even. As in part (b), if $p^s q$ is a square mod p^r we have an equation $p^s q = y^2 + lp^r$ and this implies that p^s divides y^2. Since s is now even, this means $y^2 = p^s z^2$ for some number z. Canceling p^s from $p^s q = y^2 + lp^r$ yields an equation $q = z^2 + lp^{r-s}$, which says that q is a square mod p^{r-s}. Conversely, if q is a square mod p^{r-s} we have an equation $q = z^2 + lp^{r-s}$ and hence $p^s q = p^s z^2 + lp^r$. Since s is even, this says that $p^s q$ is a square mod p^r. □

Proof of Theorem 6.11: As in the proof of Theorem 6.8 the question reduces to representing powers of primes. We know from Proposition 6.6 that all powers of a prime not dividing the discriminant Δ are represented if the prime itself is represented. By Proposition 6.7 we also know that primes p dividing Δ are represented, and their powers p^e with $e > 1$ cannot be represented unless p divides the conductor. For the remaining case of primes dividing the conductor we will apply the preceding lemma with $x = \Delta$.

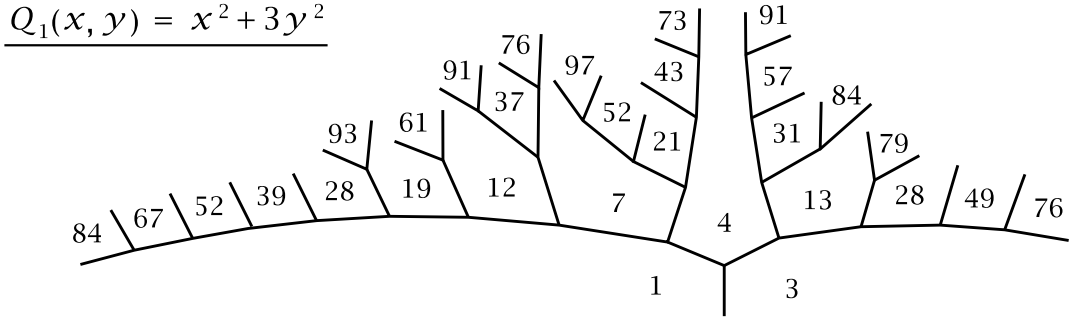
For odd p dividing Δ we need to determine when Δ is a square mod p^e. By the lemma the times this happens are when $e \le s$, or when $e > s$ and s is even and q is a square mod p^{e-s}. When $e > s$ this last condition amounts just to q being a square mod p by Lemma 6.5, or in other words $\left(\frac{q}{p}\right) = +1$.

When $p = 2$ we need to determine when Δ is a square mod $4 \cdot 2^e = 2^{e+2}$. By the lemma this happens only when $e \le s - 2$ or when s is even and q (which is odd) is a square mod 2^{e+2-s}. If $e = s - 1$ then $e + 2 - s = 1$ and every q is a square mod $2^{e+2-s} = 2$. If $e = s$ then $e + 2 - s = 2$ and q is a square mod $2^{e+2-s} = 4$ only when

$q = 4k+1$. And if $e \geq s+1$ then $e+2-s \geq 3$ and q is a square mod 2^{e+2-s} only when it is a square mod 8, which means $q = 8k+1$. □

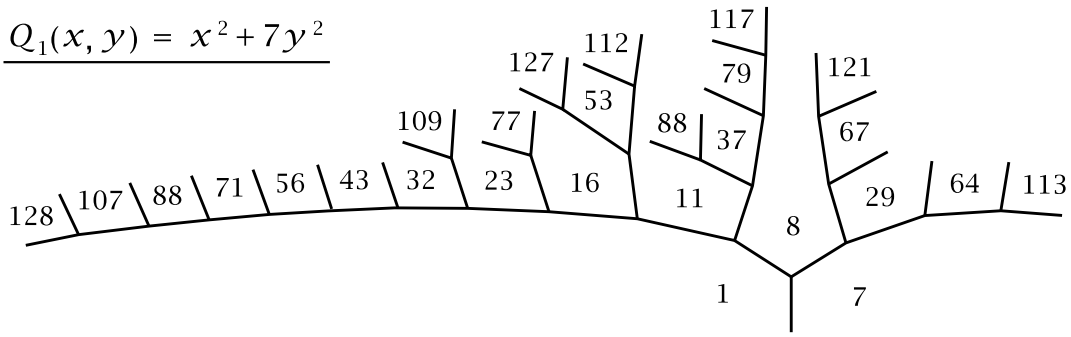
Let us look at two examples illustrating some of the more subtle possibilities in the preceding theorem. The examples involve the rather simple forms x^2+ny^2 whose discriminant $-4n$ is sometimes not a fundamental discriminant such as when n is congruent to 3 mod 4. The examples will be the cases $n = 3, 7$.

Example: $\Delta = -12$ with conductor 2. The two forms here are $Q_1 = x^2+3y^2$ and the nonprimitive form $Q_2 = 2x^2+2xy+2y^2$.



The primes represented in discriminant -12 are 2, 3, and primes p with $\left(\frac{-12}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = +1$, so these are the primes $p \equiv 1 \bmod 3$. By Theorem 6.11 the numbers represented in discriminant -12 are the numbers $n = 2^a 3^b p_1 \cdots p_k$ with $a \leq 2$, $b \leq 1$, and each p_i a prime congruent to 1 mod 3. (When we apply the theorem for $p_i = 2$ we have $s = 2$ and $q = -3$.) We can in fact determine which of Q_1 and Q_2 is giving these representations. The form Q_2 is twice x^2+xy+y^2 and we have already determined which numbers the latter form represents, namely the products $3^b p_1 \cdots p_k$ with $b \leq 1$ and each prime $p_i \equiv 1 \bmod 3$. Thus, of the numbers represented by Q_1 or Q_2, the numbers represented by Q_2 are those with $a = 1$. None of these numbers with $a = 1$ are represented by Q_1 since x^2+3y^2 is never 2 mod 4, as x^2 and y^2 must be 0 or 1 mod 4.

Example: $\Delta = -28$ with conductor 2 again. Here the only two forms up to equivalence are $Q_1 = x^2+7y^2$ and $Q_2 = 2x^2+2xy+4y^2$ which is not primitive.



The primes represented in discriminant -28 are 2, 7, and odd primes p with $\left(\frac{-28}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = +1$ so $p \equiv 1, 2, 4 \bmod 7$. According to Theorem 6.11 the numbers

represented by Q_1 or Q_2 are the numbers $n = 2^a 7^b p_1 \cdots p_k$ with $b \le 1$ and each p_i an odd prime congruent to 1, 2, or 4 mod 7. There is no restriction on a since when we apply the theorem with $p_i = 2$ we have $s = 2$ and $q = -7 = 8l + 1$.

We can say exactly which numbers are represented by Q_2 since it is twice the form $x^2 + xy + 2y^2$ of discriminant -7, which is a fundamental discriminant of class number 1 so Theorem 6.8 tells us which numbers this form represents. These are the numbers $7^b p_1 \cdots p_k$ with $b \le 1$ and primes $p_i \equiv 1, 2, 4 \mod 7$, including now the possibility $p_i = 2$. Thus Q_2 represents exactly the numbers $2^a 7^b p_1 \cdots p_k$ with $a \ge 1$, $b \le 1$ and odd primes $p_i \equiv 1, 2, 4 \mod 7$. Hence Q_1 must represent at least the numbers $2^a 7^b p_1 \cdots p_k$ with $a = 0$, $b \le 1$, and odd primes $p_i \equiv 1, 2, 4 \mod 7$. These numbers are all odd since $a = 0$, but Q_1 also represents some even numbers since $x^2 + 7y^2$ is even whenever both x and y are odd.

From the topograph we might conjecture that Q_1 represents exactly the numbers $2^a 7^b p_1 \cdots p_k$ with $a \ne 1, 2$ and the same conditions on b and the primes p_i as before. For example one can see that 8, 16, 32, 64, and 128 are represented. It is not difficult to exclude $a = 1$ and $a = 2$ by considering the values of $x^2 + 7y^2 \mod 4$ and mod 8. To see that Q_1 represents all the predicted numbers with $a \ge 3$ we use the following result.

Proposition 6.13. *For a prime p, if a product $p^k q$ with $k > 0$ is represented by a primitive form of discriminant Δ then $p^{k+2} q$ is represented by a primitive form of discriminant $p^2 \Delta$.*

Applying this to the case at hand with $p = 2$, the form $x^2 + xy + 2y^2$ represents all the products $2^a 7^b p_1 \cdots p_k$ as above with $a \ge 1$, so $x^2 + 7y^2$ represents all these products with $a \ge 3$.

Proof: Suppose we have a primitive form of discriminant Δ representing $p^k q$, so the topograph of this form has a region labeled $p^k q$. If $k > 0$ then at least one of the regions adjacent to this region must have a label not divisible by p, otherwise a vertex in the boundary of this region would have all three adjacent labels divisible by p so the form would be p times another form, making it nonprimitive. Thus the given form is equivalent to a form $p^k q x^2 + bxy + cy^2$ with c not divisible by p. The form $p^{k+2} q x^2 + pbxy + cy^2$ has discriminant $p^2 \Delta$ and is primitive since its coefficients are not all divisible by p, nor are they divisible by any other prime since such a prime would have to divide q, b, and c making the previous form $p^k q x^2 + bxy + cy^2$ nonprimitive. □

For nonfundamental discriminants Theorem 6.11 says nothing about whether the representing forms are primitive. As we will see in Theorem 7.7, determining the numbers represented by primitive forms of a given discriminant also reduces to the special case of representing prime powers by primitive forms. Namely, a product of powers $p_i^{k_i}$ of distinct primes p_i is represented by a primitive form exactly when each

of the prime powers $p_i^{k_i}$ is represented by a primitive form. Most prime powers are represented only by primitive forms, according to the following easy result:

Proposition 6.14. *A form of discriminant Δ representing a power p^k of a prime p not dividing the conductor of Δ is primitive.*

Proof: If a form Q representing p^k is not primitive it is a multiple of another form by some integer $d > 1$. This number d divides every number represented by Q so in particular d divides p^k and hence p divides d. Since d divides the conductor, this means that p divides the conductor. Thus if p does not divide the conductor then Q must be primitive. □

For primes dividing the conductor one can get some idea of the complications that can occur from the table on the next page. This lists all the equivalence classes of forms, both primitive and nonprimitive, for nonfundamental negative discriminants up to -99, along with the prime powers p^k represented by these forms for primes p dividing the conductor d. To save space the table uses the abbreviated notation $[a,b,c]$ for the form $ax^2+bxy+cy^2$.

Some information in the table can be deduced from the earlier Proposition 6.13, such as the fact that if nonprimitive forms of a given discriminant represent all powers p^k with $k \ge 1$ then primitive forms of that discriminant represent all powers p^k with $k \ge 3$. This statement is optimal for some discriminants such as -28 and -60 but not for others such as -72 and -99 where p^2 is also represented by a primitive form.

In the table one can see that primitive forms represent powers of primes dividing the conductor but not these primes themselves. As we will show in Proposition 6.15, a prime can only be represented by a single equivalence class of forms of a given discriminant, and a prime p dividing the conductor for discriminant Δ is represented by p times the principal form of discriminant Δ/p^2, so p is represented by a nonprimitive form and hence cannot also be represented by a primitive form. The uniqueness of forms representing primes holds also for powers of primes that do not divide the conductor, but we see from the table that this uniqueness may not hold for primes that do divide the conductor, even if we restrict attention just to primitive forms, as for example in the case $\Delta = -32$ where 2^3 is represented by two nonequivalent primitive forms, or discriminants -72 and -99 where there are infinitely many different powers p^k represented by different primitive forms.

The entries in the table where Theorem 6.11 says that only finitely many powers p^k are represented can be checked just by drawing topographs, but in the other cases one must use general theory. We already explained the first case $\Delta = -28$ in the earlier analysis of the form x^2+7y^2. For the next case $\Delta = -60$ the methods in the next section will suffice. A technique for handling the last few cases in the table will be explained at the end of Chapter 8.

Δ	d	Q prim.	p^k	Q nonprim.	p^k
-12	2	$[1,0,3]$	2^2	$2[1,1,1]$	2^1
-16	2	$[1,0,4]$	$2^2, 2^3$	$2[1,0,1]$	$2^1, 2^2$
-27	3	$[1,1,7]$	$3^2, 3^3$	$3[1,1,1]$	$3^1, 3^2$
-28	2	$[1,0,7]$	$2^3, 2^4, 2^5, \cdots$	$2[1,1,2]$	$2^1, 2^2, 2^3, \cdots$
-32	2	$[1,0,8]$	2^3	$2[1,0,2]$	$2^1, 2^2$
		$[3,2,3]$	$2^2, 2^3$		
-36	3	$[1,0,9]$	3^2	$3[1,0,1]$	3^1
		$[2,2,5]$	3^2		
-44	2	$[1,0,11]$	—	$2[1,1,3]$	2^1
		$[3,2,4]$	2^2		
-48	4	$[1,0,12]$	2^4	$2[1,0,3]$	$2^1, 2^3$
		$[3,0,4]$	$2^2, 2^4$	$4[1,1,1]$	2^2
-60	2	$[1,0,15]$	$2^4, 2^6, 2^8, 2^{10}, \cdots$	$2[1,1,4]$	$2^1, 2^3, 2^5, 2^7, \cdots$
		$[3,0,5]$	$2^3, 2^5, 2^7, 2^9, \cdots$	$2[2,1,2]$	$2^2, 2^4, 2^6, 2^8, \cdots$
-63	3	$[1,1,16]$	—	$3[1,1,2]$	3^1
		$[2,1,8]$	3^2		
		$[4,1,4]$	3^2		
-64	4	$[1,0,16]$	$2^4, 2^5$	$2[1,0,4]$	$2^1, 2^3, 2^4$
		$[4,4,5]$	$2^2, 2^4, 2^5$	$4[1,0,1]$	$2^2, 2^3$
-72	3	$[1,0,18]$	$3^3, 3^4, 3^5, 3^6, \cdots$	$3[1,0,2]$	$3^1, 3^2, 3^3, 3^4, \cdots$
		$[2,0,9]$	$3^2, 3^3, 3^4, 3^5, \cdots$		
-75	5	$[1,1,19]$	5^2	$5[1,1,1]$	5^1
		$[3,3,7]$	5^2		
-76	2	$[1,0,19]$	—	$2[1,1,5]$	2^1
		$[4,2,5]$	2^2		
-80	2	$[1,0,20]$	—	$2[1,0,5]$	2^1
		$[4,0,5]$	2^2	$2[2,2,3]$	2^2
		$[3,2,7]$	2^3		
-92	2	$[1,0,23]$	$2^5, 2^8, 2^{11}, 2^{14}, \cdots$	$2[1,1,6]$	$2^1, 2^4, 2^7, 2^{10}, \cdots$
		$[3,2,8]$	$2^3, 2^4, 2^6, 2^7, \cdots$	$2[2,1,3]$	$2^2, 2^3, 2^5, 2^6, 2^8, 2^9, \cdots$
-96	2	$[1,0,24]$	—	$2[1,0,6]$	2^1
		$[3,0,8]$	2^3	$2[2,0,3]$	2^2
		$[5,2,5]$	2^3		
		$[4,4,7]$	2^2		
-99	3	$[1,1,25]$	$3^3, 3^4, 3^5, 3^6, \cdots$	$3[1,1,3]$	$3^1, 3^2, 3^3, 3^4, \cdots$
		$[5,1,5]$	$3^2, 3^3, 3^4, 3^5, \cdots$		

Unique Representability for Primes and Prime Powers

In Section 6.1 we saw examples where two nonequivalent forms of the same discriminant both represent the same number. However, this does not happen for representations of 1 or primes or powers of most primes:

Proposition 6.15. *If Q_1 and Q_2 are two forms of the same discriminant that both represent the same prime p or both represent 1, then Q_1 and Q_2 are equivalent. The same conclusion holds when Q_1 and Q_2 both represent the same power p^k of an odd prime p that does not divide the discriminant.*

The last statement is also true for $p = 2$ but the proof is more difficult so we will wait until the next chapter to deduce this from a more general result, Theorem 7.7. Examples showing that powers of primes dividing the discriminant can be represented by nonequivalent forms of the same discriminant can be found in the table on the previous page. In these examples the prime in question divides the conductor, not just the discriminant, but this has to be the case since for primes p dividing the discriminant but not the conductor the only power p^k represented by a form of the given discriminant is p itself, by Proposition 6.7.

Proof: Suppose that Q is a form representing a number p that is either 1 or a prime. The topograph of Q then has a region labeled p, and we have seen that the h-labels on the edges adjacent to this p-region form an arithmetic progression with increment $2p$ when these edges are all oriented in the same direction. We have the discriminant formula $\Delta = h^2 - 4pq$ where h is the label on one of these edges and q is the value of Q for the region on the other side of this edge. Since p is nonzero the equation $\Delta = h^2 - 4pq$ determines q in terms of Δ and h. This implies that Δ and the arithmetic progression determine the form Q up to equivalence since the progression determines p, and any h-value in the progression then determines the q-value corresponding to this h-value, so Q is equivalent to $px^2 + hxy + qy^2$.

In the case that $p = 1$ the increment in the arithmetic progressions is 2 so the two possible progressions of h-values adjacent to the p-region are the even numbers and the odd numbers. We know that h has the same parity as Δ, so Δ determines which of the two progressions we have. As we saw in the preceding paragraph, this implies that the form is determined by Δ, up to equivalence.

Now we consider the case that p is prime. Let Q_1 and Q_2 be two forms of the same discriminant Δ both representing p. For Q_1 choose an edge in its topograph adjacent to the p-region, with h-label h_1 and q-label q_1. For the form Q_2 we similarly choose an edge with associated labels h_2 and q_2. Both h_1 and h_2 have the same parity as Δ. We have $\Delta = h_1^2 - 4pq_1 = h_2^2 - 4pq_2$ and hence $h_1^2 \equiv h_2^2 \mod 4p$. This implies $h_1^2 \equiv h_2^2 \mod p$, so p divides $h_1^2 - h_2^2 = (h_1 + h_2)(h_1 - h_2)$. Since p is prime, it must divide one of the two factors and hence we must have $h_1 \equiv \pm h_2 \mod p$. By

changing the orientations of the edges in the topograph for Q_1 or Q_2 if necessary, we can assume that $h_1 \equiv h_2 \mod p$.

If p is odd we can improve this congruence to $h_1 \equiv h_2 \mod 2p$ since we know that $h_1 - h_2$ is divisible by both p and 2 (since h_1 and h_2 have the same parity), hence $h_1 - h_2$ is divisible by $2p$. The congruence $h_1 \equiv h_2 \mod 2p$ implies that the arithmetic progression of h-values adjacent to the p-region for Q_1 is the same as for Q_2 since $2p$ is the increment for both progressions. By what we showed earlier, this implies that Q_1 and Q_2 are equivalent.

When $p = 2$ this argument needs to be modified slightly. We still have $h_1^2 \equiv h_2^2 \mod 4p$ so when $p = 2$ this becomes $h_1^2 \equiv h_2^2 \mod 8$. Since $2p = 4$ the four possible arithmetic progressions of h-values are $h \equiv 0, 1, 2,$ or $3 \mod 4$. We can interchange the possibilities 1 and 3 just by reorienting the edges, leaving only the possibilities $h \equiv 0$, 1, or 2 mod 4. These are distinguished from each other by the congruence $h_1^2 \equiv h_2^2 \mod 8$ since $(4k)^2 \equiv 0 \mod 8$, $(4k+1)^2 \equiv 1 \mod 8$, and $(4k+2)^2 \equiv 4 \mod 8$.

Finally we have the case that Q_1 and Q_2 both represent the power p^k of an odd prime p not dividing Δ, with $k > 1$. Following the line of proof above we see that p^k divides $h_1^2 - h_2^2 = (h_1 + h_2)(h_1 - h_2)$. If p^k divides either factor we can proceed exactly as before to show that Q_1 and Q_2 are equivalent since we assume p is odd, hence also p^k. If p^k does not divide either factor then both factors are divisible by p, hence p divides their sum $2h_1$. Since p is odd this implies that p divides h_1, and so p divides $\Delta = h_1^2 - 4p^k q_1$. Thus if p does not divide Δ then the case that p^k divides neither $h_1 + h_2$ nor $h_1 - h_2$ does not arise. □

The same argument shows another interesting fact:

Proposition 6.16. *If the topograph of a form has two regions with the same label n where n is either 1, a prime, or a power of an odd prime not dividing the discriminant, then there is a symmetry of the topograph that takes one region labeled n to the other. Similarly, for positive discriminants and for the same numbers n, if there is one region labeled n and another labeled $-n$ then there is a skew symmetry taking one region to the other.*

Proof: Suppose first that there are two regions having the same label n. As we saw in the proof of the preceding proposition, each of these regions is adjacent to an edge with the same label h and hence the labels q across these edges are also the same. This means there is a symmetry taking one region labeled n to the other.

The other case is that one region is labeled n and the other $-n$. The topographs of the given form Q and its negative $-Q$ then each have a region labeled n so there is an equivalence from Q to $-Q$ taking the n-region for Q to the n-region for $-Q$. This equivalence can be regarded as a skew symmetry of Q taking the n-region to the $-n$-region. □

For the last result in this section we will use a variant of Euclid's proof that there are infinitely many primes to prove the following general statement:

Proposition 6.18. *For each discriminant Δ the set of primes represented in discriminant Δ is infinite.*

Proof: In each discriminant Δ there is a form $Q(x,y) = x^2 + bxy + cy^2$ representing 1. We can assume c is nonzero since in the topograph of Q there will always be at least one region adjacent to the 1 region that is not labeled by 0. (Only parabolic and 0-hyperbolic forms can have a 0 region and they have at most two 0 regions.) Let $p_1, \cdots, p_k$ be any finite list of primes. We allow repetitions on this list so we can make k as large as we like just by repeating some p_i often enough. Let P be the product $p_1 \cdots p_k$ and consider the number $n = Q(1,P) = 1 + bP + cP^2$. This is represented by Q since $(1,P)$ is a primitive pair. If k is large enough we will have $|n| > 1$ since $|cP^2|$ will be much larger than $|1 + bP|$. Any prime p dividing n will also be represented by some form of discriminant Δ. This p must be different from any of the primes p_i on the initial list since dividing p_i into $n = 1 + P + cP^2$ gives a remainder of 1, whereas p divides n evenly. Thus we have shown that for any finite list of primes there is another prime not on the list that is represented in discriminant Δ. Hence the set of primes represented in discriminant Δ must be infinite. □

Exercises

1. Determine discriminants Δ for which there exists a quadratic form of discriminant Δ that represents 5, and also the discriminants for which there does not exist a form representing 5. When 5 is represented, find a form that gives the representation.

2. The following is a generalization of Lemma 6.4. Let $P(x)$ be a polynomial with integer coefficients and let n be an integer. Show that if the congruence $P(x) \equiv n$ has a solution mod m_1 and also a solution mod m_2 where m_1 and m_2 are coprime, then it has a solution mod $m_1 m_2$. Give an example where this fails without the coprimeness condition.

3. Verify that the statement of quadratic reciprocity is true for the following pairs of primes (p,q): $(3,5)$, $(3,7)$, $(3,13)$, $(5,13)$, $(7,11)$, and $(13,17)$.

4. Evaluate the following Legendre symbols: $\left(\frac{30}{101}\right)$, $\left(\frac{99}{101}\right)$, $\left(\frac{506}{967}\right)$.

5. Show that $\left(\frac{a}{p}\right)$ can always be computed just from the four basic properties of Legendre symbols.

6. Determine which numbers in the range from 40 to 50 are squares mod 132.

7. (a) Using quadratic reciprocity determine which primes are represented by some form of discriminant 17.

(b) Show that all forms of discriminant 17 are equivalent to the form $x^2 + xy - 4y^2$.

(c) Draw enough of the topograph of $x^2 + xy - 4y^2$ to show all values between -70 and 70, and verify that the primes that occur are precisely the ones predicted by your answer in part (a).

8. Determine which primes are represented by at least one form of the following discriminants: (a) 21 (b) -19 (c) -20 (d) -24.

9. Show that every prime is represented by at least one of the forms x^2+y^2, x^2+2y^2, and $x^2 - 2y^2$.

10. Consider forms $Q = ax^2+bxy+cy^2$ of discriminant Δ. Show that the following three conditions are equivalent:

(1) The coefficients a, b, and c of Q are all odd.

(2) Q represents only odd numbers.

(3) $\Delta \equiv 5 \bmod 8$.

11. For which fundamental discriminants Δ is there a form of discriminant Δ representing $|\Delta|$? What about nonfundamental discriminants?

12. In terms of their prime factorizations, which numbers are sums of two nonzero squares? Which squares are sums of two nonzero squares?

13. Show that if the form $x^2 + ny^2$ represents 2^k with n odd and $k > 0$ then $n \equiv 7 \bmod 8$ except when $(n,k) = (1,1)$ and $(3,2)$.

14. Show that for each prime p dividing the conductor for discriminant Δ there is at least one primitive form of discriminant Δ that represents a power of p. *Hint*: Use induction on the highest power of p dividing the conductor, along with Theorem 6.11 and Propositions 6.13 and 6.14.

15. This exercise involves using quadratic reciprocity to apply Legendre's Theorem (Theorem 2.6) on rational points on quadratic curves.

(a) Determine the values of n for which the curve $2x^2 + ny^2 = 1$ contains rational points, assuming n is odd and squarefree. For each of the first three positive values of n for which the curve contains rational points find two of these rational points that lie in the first quadrant.

(b) For the same equation show that the case that n is even and squarefree reduces to the case n is odd and squarefree.

(c) Determine the values of n for which the curve $3x^2 + ny^2 = 1$ contains rational points, assuming n is odd, squarefree, and coprime to 3.

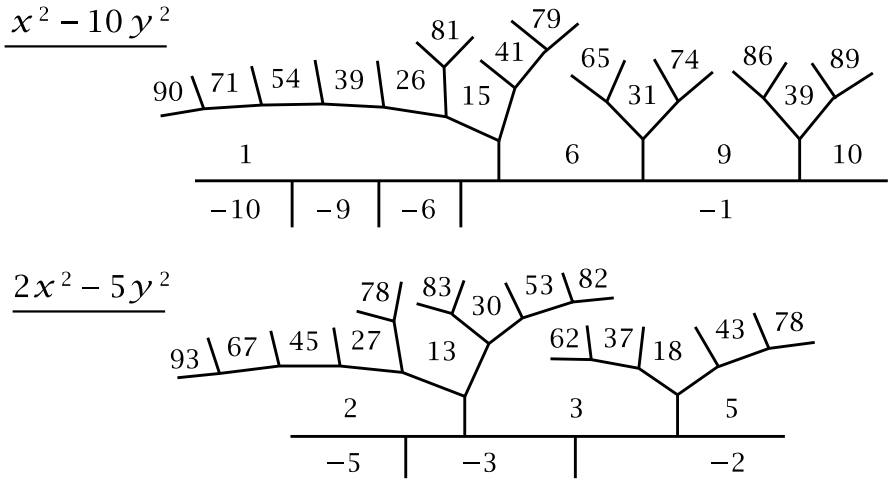
6.3 Genus and Characters

In the previous section we obtained a reasonably complete answer to the question of which numbers are represented by at least one form of a given discriminant. Legendre symbols determine which primes are represented, and in a fairly simple way this determines which nonprimes are represented. For discriminants of class number 1 this gives a complete answer to the question of which numbers are represented by a given form.

The main goal of the present section is to see how Legendre symbols, along with a few extensions of them for the special prime 2, can give additional information when the class number is not 1. In particular, in favorable cases we will be able to determine fully which forms represent which primes. Underlying this method is the following basic result:

Proposition 6.19. *Let Q be a form of discriminant Δ and let p be an odd prime dividing Δ. Then the Legendre symbol $\left(\frac{n}{p}\right)$ has the same value for all numbers n in the topograph of Q that are not divisible by p.*

Before proving this let us see how it applies in the case $\Delta = 40$ with $p = 5$. The class number here is 2 corresponding to the forms $x^2 - 10y^2$ and $2x^2 - 5y^2$.



According to the proposition, for each of the two forms the value of $\left(\frac{n}{5}\right)$ must be the same for all numbers n in the topograph not divisible by 5. To determine the value of $\left(\frac{n}{5}\right)$ for each form it therefore suffices to compute it for a single number n. The simplest thing is just to compute it for $(x, y) = (1, 0)$ or $(0, 1)$. Choosing $(1, 0)$, for $x^2 - 10y^2$ we have $\left(\frac{1}{5}\right) = +1$ and for $2x^2 - 5y^2$ we have $\left(\frac{2}{5}\right) = -1$. The proposition then says that all numbers n in the topograph of $x^2 - 10y^2$ not divisible by 5 have $\left(\frac{n}{5}\right) = +1$, hence $n \equiv \pm 1 \mod 5$, while for $2x^2 - 5y^2$ we have $\left(\frac{n}{5}\right) = -1$, hence $n \equiv \pm 2 \mod 5$. Thus the last digits of the numbers in the topograph of $x^2 - 10y^2$ must be 0, 1, 4, 5, 6, or 9 and for $2x^2 - 5y^2$ the last digits must be 0, 2, 3, 5, 7, or 8.

Note that the congruences $n \equiv \pm 1$ and $n \equiv \pm 2 \bmod 5$ are consistent with the fact that for both forms the negative values are just the negatives of the positive values. (The proposition holds for negative as well as positive numbers in topographs.)

We know that $\left(\frac{40}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{5}\right)$ must equal $+1$ for primes $p \neq 2, 5$ represented by either form, so for $x^2 - 10y^2$ this product must be $(+1)(+1)$ while for $2x^2 - 5y^2$ it must be $(-1)(-1)$.

	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
$\left(\frac{2}{p}\right)$	$+1$	-1	$+1$	$+1$	-1	-1	$+1$	-1	-1	$+1$	-1	-1	$+1$	$+1$	-1	$+1$
$\left(\frac{p}{5}\right)$	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$
	Q_1	Q_2		Q_1		Q_2					Q_2		Q_1		Q_2	Q_1

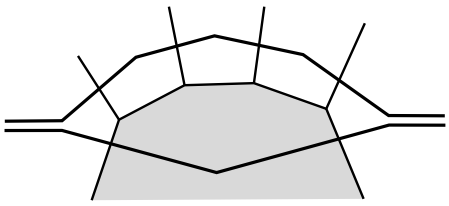
From the table we can see exactly which primes each of these two forms represents, namely $x^2 - 10y^2$ represents primes $p \equiv 1, 9, 31, 39 \bmod 40$ while $2x^2 - 5y^2$ represents primes $p \equiv 3, 13, 27, 37 \bmod 40$.

Proof of Proposition 6.19: For an edge in the topograph labeled h with adjacent regions labeled n and k we have $\Delta = h^2 - 4nk$. If p is a prime dividing Δ this implies that $4nk \equiv h^2 \bmod p$. Thus if neither n nor k is divisible by p and p is odd then the Legendre symbol $\left(\frac{4nk}{p}\right)$ is defined and $\left(\frac{4nk}{p}\right) = \left(\frac{h^2}{p}\right) = +1$. Since $\left(\frac{4nk}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{n}{p}\right)\left(\frac{k}{p}\right)$ and $\left(\frac{4}{p}\right) = +1$ this implies $\left(\frac{n}{p}\right) = \left(\frac{k}{p}\right)$. In other words, the symbol $\left(\frac{n}{p}\right)$ takes the same value on any two adjacent regions of the topograph of Q labeled by numbers not divisible by p. To finish the proof we will use the following fact:

Lemma 6.20. *Given a form Q and a prime p dividing the discriminant of Q, then any two regions in the topograph of Q where the value of Q is not divisible by p can be connected by a path passing only through such regions.*

Assuming this, Proposition 6.19 easily follows since we have seen that the value of $\left(\frac{n}{p}\right)$ is the same for any two adjacent regions with label not divisible by p. □

Proof of the Lemma: Let us call regions in the topograph of Q whose label is not divisible by p *good* regions, and the other regions *bad* regions. We can assume that at least one region is good, otherwise there is nothing to prove. What we will show is that no two bad regions can be adjacent. Thus a path in the topograph from one good region to another cannot pass through two consecutive bad regions, and if it does pass through a bad region then a detour around this region allows this bad region to be avoided, creating a new path passing through one fewer bad region as in the figure at the right. By repeating this detouring process as often as necessary we eventually obtain a path avoiding bad regions entirely, still starting and ending at the same two given good regions.



To see that no two adjacent regions are bad, suppose this is false, so there are two adjacent regions whose Q values n and k are both divisible by p. If the edge separating these two regions is labeled h then we have an equation $\Delta = h^2 - 4nk$, and since we assume p divides Δ this implies that p divides h as well as n and k. Thus the form $nx^2 + hxy + ky^2$, which is equivalent to Q, is equal to p times another form. This implies that all regions in the topograph of Q are bad. This contradicts an earlier assumption so we conclude that there are no adjacent bad regions. □

A useful observation is that the value of $\left(\frac{n}{p}\right)$ for numbers n in the topograph of a form $ax^2 + bxy + cy^2$ with discriminant divisible by p can always be determined just by looking at the coefficients a and c. This is because a and c appear in adjacent regions of the topograph, so if both these coefficients were divisible by p, this would imply that b was also divisible by p since p divides $b^2 - 4ac$, so the whole form would be divisible by p. Excluding this uninteresting possibility, we see that at least one of a and c is not divisible by p and we can use this to compute $\left(\frac{n}{p}\right)$.

Let us look at another example, the discriminant $\Delta = -84 = -2^2 \cdot 3 \cdot 7$ with three different prime factors. For this discriminant there are four equivalence classes of forms: $Q_1 = x^2 + 21y^2$, $Q_2 = 3x^2 + 7y^2$, $Q_3 = 2x^2 + 2xy + 11y^2$, and $Q_4 = 5x^2 + 4xy + 5y^2$. The topographs of these forms were shown in Section 6.1. To see which odd primes are represented in discriminant -84 we compute:

$$\left(\tfrac{-84}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{3}{p}\right)\left(\tfrac{4}{p}\right)\left(\tfrac{7}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{3}{p}\right)\left(\tfrac{7}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{p}{3}\right)\left(\tfrac{p}{7}\right)$$

As in the example of $\Delta = 40$ we can make a table of the values of these Legendre symbols for the 24 numbers mod 84 that are not divisible by the prime divisors $2, 3, 7$ of 84. Using the fact that the squares mod 3 are $(\pm 1)^2 = 1$ and the squares mod 7 are $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, and $(\pm 3)^2 \equiv 2$, we obtain the following table:

	1	5	11	13	17	19	23	25	29	31	37	41
$\left(\frac{-1}{p}\right)$	+1	+1	−1	+1	+1	−1	−1	+1	+1	−1	+1	+1
$\left(\frac{p}{3}\right)$	+1	−1	−1	+1	−1	+1	−1	+1	−1	+1	+1	−1
$\left(\frac{p}{7}\right)$	+1	−1	+1	−1	−1	−1	+1	+1	+1	−1	+1	−1
	Q_1	Q_4	Q_3		Q_4	Q_2	Q_3	Q_1		Q_2	Q_1	Q_4

	43	47	53	55	59	61	65	67	71	73	79	83
$\left(\frac{-1}{p}\right)$	−1	−1	+1	−1	−1	+1	+1	−1	−1	+1	−1	−1
$\left(\frac{p}{3}\right)$	+1	−1	−1	+1	−1	+1	−1	+1	−1	+1	+1	−1
$\left(\frac{p}{7}\right)$	+1	−1	+1	−1	−1	−1	+1	+1	+1	−1	+1	−1
				Q_2					Q_3			

The twelve cases when the product $\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)\left(\frac{p}{7}\right)$ is $+1$ give the congruence classes of primes not dividing Δ that are represented by one of the four forms, and we can determine which form it is by looking at the values of $\left(\frac{p}{3}\right)$ and $\left(\frac{p}{7}\right)$ for each of the four

forms. As noted earlier, these values can be computed directly from the coefficients of x^2 and y^2 that are not divisible by 3 for $\left(\frac{p}{3}\right)$ or by 7 for $\left(\frac{p}{7}\right)$. For example, for $Q_2 = 3x^2 + 7y^2$ the coefficient of y^2 tells us that $\left(\frac{p}{3}\right) = \left(\frac{7}{3}\right) = +1$ and the coefficient of x^2 tells us that $\left(\frac{p}{7}\right) = \left(\frac{3}{7}\right) = -1$. Thus the pair $\left(\frac{p}{3}\right), \left(\frac{p}{7}\right)$ is $+1, -1$ for Q_2. In a similar way we find that $\left(\frac{p}{3}\right), \left(\frac{p}{7}\right)$ is $+1, +1$ for $Q_1 = x^2 + 21y^2$, while it is $-1, +1$ for $Q_3 = 2x^2 + 2xy + 11y^2$ and $-1, -1$ for $Q_4 = 5x^2 + 4xy + 5y^2$. This allows us to determine which congruence classes of primes are represented by which form, as indicated in the table, since the product $\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)\left(\frac{p}{7}\right)$ must be $+1$.

Another case we looked at was $\Delta = -56$ where there were three inequivalent forms $Q_1 = x^2 + 14y^2$, $Q_2 = 2x^2 + 7y^2$, and $Q_3 = 3x^2 + 2xy + 5y^2$. Here we have $\left(\frac{-56}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{7}\right)$. The table of values for these Legendre symbols for congruence classes of numbers mod 56 not divisible by 2 or 7 is:

	1	3	5	9	11	13	15	17	19	23	25	27
$\left(\frac{2}{p}\right)$	$+1$	-1	-1	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	$+1$	-1
$\left(\frac{p}{7}\right)$	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	-1	-1	$+1$	$+1$	-1
	$\binom{Q_1}{Q_2}$	Q_3	Q_3	$\binom{Q_1}{Q_2}$		Q_3	$\binom{Q_1}{Q_2}$		Q_3	$\binom{Q_1}{Q_2}$	$\binom{Q_1}{Q_2}$	Q_3

	29	31	33	37	39	41	43	45	47	51	53	55
$\left(\frac{2}{p}\right)$	-1	$+1$	$+1$	-1	$+1$	$+1$	-1	-1	$+1$	-1	-1	$+1$
$\left(\frac{p}{7}\right)$	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	-1	-1	$+1$	$+1$	-1
					$\binom{Q_1}{Q_2}$			Q_3				

From the table we see that $\left(\frac{2}{p}\right)\left(\frac{p}{7}\right)$ is $(+1)(+1)$ for $p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$ and $(-1)(-1)$ for $p \equiv 3, 5, 13, 19, 27, 45 \bmod 56$. Thus the primes that are represented in discriminant -56 are the primes in these twelve congruence classes, along with 2 and 7, the prime divisors of 56. Moreover, since $\left(\frac{p}{7}\right)$ has the value $+1$ for numbers in the topographs of Q_1 and Q_2 not divisible by 7, and the value -1 for numbers in the topograph of Q_3 not divisible by 7, we can deduce that primes $p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$ are represented by Q_1 or Q_2 while primes $p \equiv 3, 5, 13, 19, 27, 45 \bmod 56$ are represented by Q_3. However the values of the Legendre symbols in the table do not allow us to distinguish between Q_1 and Q_2.

Each row in one of the tables above can be regarded as a function assigning a number ± 1 to each congruence class of numbers n coprime to the discriminant Δ. Such a function is called a ***character*** and the table is called a ***character table***. There is one column in the table for each congruence class of numbers coprime to Δ so the number of columns is $\varphi(|\Delta|)$ where φ is the Euler phi function from Section 2.3. For each odd prime p dividing Δ there is a character given by the Legendre symbol $\left(\frac{n}{p}\right)$. There is sometimes also a character associated to the prime 2 in a somewhat less transparent way. In the example $\Delta = -84$ this is the character defined by the first row of the table, which assigns the values $+1$ to numbers $n = 4k + 1$ and -1 to

numbers $n = 4k + 3$. We will denote this character by χ_4 to indicate that its values $\chi_4(n) = \pm 1$ depend only on the value of n mod 4. Thus $\chi_4(p) = \left(\frac{-1}{p}\right)$ when p is an odd prime, but $\chi_4(n)$ is defined for all odd numbers n, not just primes. One can check that an explicit formula for χ_4 is $\chi_4(n) = (-1)^{(n-1)/2}$ although we will not be needing this formula.

In the example with $\Delta = -56$ the character corresponding to the prime 2 is given by the row labeled $\left(\frac{2}{p}\right)$. This character associates the value $+1$ to an odd number $n \equiv \pm 1$ mod 8 and the value -1 when $n \equiv \pm 3$ mod 8. We will denote it by χ_8 since its values $\chi_8(n) = \pm 1$ depend only on n mod 8. We have $\chi_8(p) = \left(\frac{2}{p}\right)$ for all odd primes p, but $\chi_8(n)$ is defined for all odd numbers n. There is again an explicit formula $\chi_8(n) = (-1)^{(n^2-1)/8}$ that we will not use.

By analogy we can also introduce the notation χ_p for the earlier character defined by $\chi_p(n) = \left(\frac{n}{p}\right)$ for p an odd prime and n not divisible by p.

As another example illustrating the use of characters let us determine which powers of 2 are represented by the two forms $x^2 + 15y^2$ and $3x^2 + 5y^2$ of discriminant -60. This is not a fundamental discriminant since it is 4 times the fundamental discriminant -15, so the conductor is 2 which is why the question of determining the forms representing powers of 2 is more subtle, as we saw in the previous section. In both the discriminants -15 and -60 we have the characters χ_3 and χ_5 and we can use either one of these for this application so we will use χ_3.

First consider discriminant -15 where the class number is 2 corresponding to the two forms $x^2 + xy + 4y^2$ and $2x^2 + xy + 2y^2$. The second form represents 2 which does not divide the discriminant -15 so all powers of 2 are represented by one or the other of these two forms. To determine which form it is for each power we use the character χ_3. This has the value $+1$ on numbers not divisible by 3 in the topograph of $x^2 + xy + 4y^2$ since 1 is one of these numbers and $\chi_3(1) = +1$. Similarly χ_3 has the value -1 for the other form $2x^2 + xy + 2y^2$ since 2 appears in the topograph of this form and $\chi_3(2) = -1$. We have $\chi_3(2^k) = (-1)^k$ since $\chi_3(2^k) = \left(\frac{2^k}{3}\right) = \left(\frac{2}{3}\right)^k$. Hence $x^2 + xy + 4y^2$ represents only the even powers of 2 and $2x^2 + xy + 2y^2$ represents only the odd powers.

For discriminant -60 the class number is also 2, corresponding to the forms $x^2 + 15y^2$ and $3x^2 + 5y^2$. Obviously neither of these forms represents 2 or 4. However by Proposition 6.13 each power 2^k with $k \geq 3$ is represented by at least one of the two forms since all powers 2^k with $k \geq 1$ are represented by one of the forms of discriminant -15. The value of χ_3 for $x^2 + 15y^2$ is $+1$ since this form represents 1 and $\chi_3(1) = +1$, and the value of χ_3 for $3x^2 + 5y^2$ is -1 since this form represents 5 and $\chi_3(5) = -1$. From this it follows as before that $x^2 + 15y^2$ represents just the even powers of 2 starting with 2^4 and $3x^2 + 5y^2$ represents just the odd powers starting with 2^3. This is the answer that was given in the large table in the preceding section.

Characters for the Prime 2

Let us consider now how characters can be associated to the prime 2 in general. Since characters arise from primes that divide the discriminant, this means we are interested in even discriminants, and the characters we are looking for should assign a value ± 1 to each number not divisible by 2, that is, to each odd number. We would like the analogue of Proposition 6.19 to hold, so characters for the prime 2 should take the same value on all odd numbers in the topograph of a form of the given discriminant. By Lemma 6.20 this just means that the characters should have the same value for odd numbers in adjacent regions of the topographs.

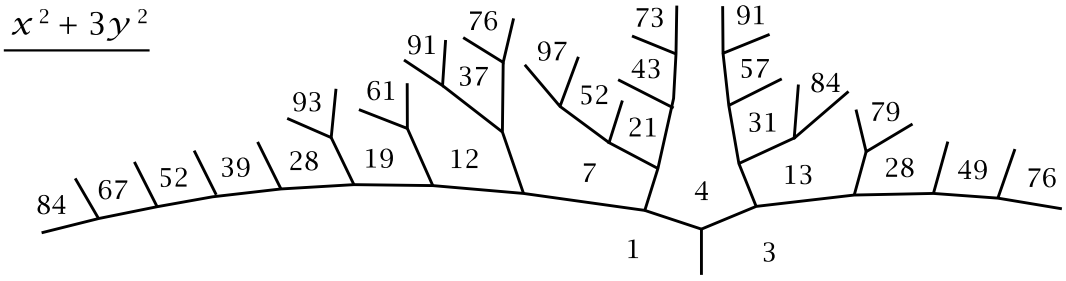
Even discriminants are multiples of 4 so can be written as $\Delta = 4\delta$. For adjacent regions in a topograph with labels n and k we have $\Delta = h^2 - 4nk$ where h is the label on the edge between the two regions. Since Δ is even, so is h and we can write $h = 2l$. The discriminant equation then becomes $4\delta = 4l^2 - 4nk$ or just $\delta = l^2 - nk$.

There will be six different cases. The first two are when δ is odd, which means that Δ is divisible by 4 but not 8. In these two cases we consider congruences mod 4, the highest power of 2 dividing Δ. Since δ is odd and both n and k are odd, the equation $\delta = l^2 - nk$ implies that l must be even, so $l^2 \equiv 0 \mod 4$ and we have $nk \equiv -\delta \mod 4$. Multiplying both sides of this congruence by k, we get $n \equiv -\delta k \mod 4$ since $k^2 \equiv 1 \mod 4$, k being odd. Multiplying the congruence $n \equiv -\delta k$ by k again gives the previous congruence $nk \equiv -\delta$ so the two congruences are equivalent.

Case 1: $\delta = 4m-1$. The congruence condition $n \equiv -\delta k \mod 4$ is then $n \equiv k \mod 4$. Thus Lemma 6.20 implies that the character χ_4 assigning $+1$ to integers $4s+1$ and -1 to integers $4s-1$ has the same value for all odd numbers in the topograph of a form of discriminant $\Delta = 4(4m-1)$. We might try reversing the values of χ_4, assigning the value $+1$ to integers $4s-1$ and -1 to integers $4s+1$, but this just gives the function $-\chi_4$ which does not really give any new information that χ_4 does not give. In practice χ_4 turns out to be more convenient to use than $-\chi_4$ would be.

An example for the case $\delta = 4m-1$ is the discriminant $\Delta = -84$ considered earlier, where the first row of the character table gave the values for χ_4.

Case 2: $\delta = 4m+1$. The difference from the previous case is that the congruence condition is now $n \equiv -k \mod 4$. This means the mod 4 value of odd numbers in the topograph is not constant, and so we do not get a character for the prime 2. As an example, consider the form x^2+3y^2 with $\Delta = -12$ and $\delta = -3$.



Here there are odd numbers in the topograph congruent to both 1 and 3 mod 4. The situation is not improved by considering odd numbers mod 8 instead of mod 4 since the topograph contains numbers congruent to each of $1,3,5,7$ mod 8. Trying congruences modulo higher powers of 2 does not help either.

The absence of a character for the prime 2 when $\delta = 4m+1$ could perhaps have been predicted from the calculation of $\left(\frac{\Delta}{p}\right)$. Since δ is odd we have $\Delta = 4\delta = 4p_1 \cdots p_r$ for odd primes $p_1, \cdots, p_r$ and so $\left(\frac{\Delta}{p}\right) = \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_r}{p}\right)$. This equals $\left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_r}\right)$ since the number of primes p_i congruent to 3 mod 4 is even when $\delta = 4m+1$. Thus the value of $\left(\frac{\Delta}{p}\right)$ depends only on the characters associated to the odd prime factors of Δ.

There remain the cases that δ is even. The next two cases are when Δ is divisible by 8 but not by 16. After that is the case that Δ is divisible by 16 but not by 32, and finally the case that Δ is divisible by 32. In all these cases we will consider congruences mod 8, so the equation $\delta = l^2 - nk$ becomes $\delta \equiv l^2 - nk$ mod 8. Since δ is now even while n and k are still odd, this congruence implies l is odd, and so $l^2 \equiv 1$ mod 8 and the congruence can be written as $nk \equiv 1 - \delta$ mod 8. Since $k^2 \equiv 1$ mod 8 when k is odd, we can multiply both sides of the congruence $nk \equiv 1 - \delta$ by k to obtain the equivalent congruence $n \equiv (1-\delta)k$ mod 8.

Case 3: $\delta \equiv 2$ mod 8. The congruence is then $n \equiv -k$ mod 8. It follows that in the topograph of a form of discriminant $\Delta = 4(8m+2)$ either the odd numbers must all be congruent to ± 1 mod 8 or they must all be congruent to ± 3 mod 8. Thus the character χ_8 which takes the value $+1$ on numbers $8s \pm 1$ and -1 on numbers $8s \pm 3$ has a constant value, either $+1$ or -1, for all odd numbers in the topograph.

An example for this case is $\Delta = 40$. Here the two rows of the character table computed earlier in this section gave the values for χ_8 and χ_5.

Case 4: $\delta \equiv 6$ mod 8. Now the congruence $n \equiv (1-\delta)k$ mod 8 becomes $n \equiv -5k$, or equivalently $n \equiv 3k$ mod 8. This implies that all odd numbers in the topograph of a form of discriminant $\Delta = 4(8m+6)$ must be congruent to 1 or 3 mod 8, or they must all be congruent to 5 or 7 mod 8. The character associated to the prime 2 in this case has the value $+1$ on numbers $8s+1$ and $8s+3$, and the value -1 on numbers $8s+5$ and $8s+7$. We have not encountered this character previously, so let us give it the new name χ'_8. However, it is not entirely new since it is actually just the product $\chi_4\chi_8$ as one can easily check by evaluating this product on $1,3,5$, and 7.

A simple example is $\Delta = -8$ with class number 1. Here we have $\left(\frac{\Delta}{p}\right) = \left(\frac{-8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ which equals $+1$ for $p \equiv 1,3$ mod 8 and -1 for $p \equiv 5,7$ mod 8 so this is just the character χ'_8.

Another example is $\Delta = 24$ where there are the two forms $Q_1 = x^2 - 6y^2$ and $Q_2 = 6x^2 - y^2$. We have $\left(\frac{\Delta}{p}\right) = \left(\frac{24}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)$. The character table has the following form:

	1	5	7	11	13	17	19	23
χ_8'	+1	−1	−1	+1	−1	+1	+1	−1
χ_3	+1	−1	+1	−1	+1	−1	+1	−1

Thus Q_1 represents primes $p \equiv 1, 19 \bmod 24$ and Q_2 represents primes $p \equiv 5, 23 \bmod 24$.

Case 5: $\delta \equiv 4 \bmod 8$. Now we have the congruence $n \equiv -3k \bmod 8$. Thus in the topograph of a form of discriminant $\Delta = 4(8m+4)$ all odd numbers must be congruent to 1 or 5 mod 8, or they must all be congruent to 3 or 7 mod 8. More simply, one can say that all odd numbers in the topograph must be congruent to 1 mod 4 or they must all be congruent to 3 mod 4. Thus we obtain the character χ_4 again.

An example is $\Delta = -48$ where we have the two forms $Q_1 = x^2 + 12y^2$ and $Q_2 = 3x^2 + 4y^2$ as well as a pair of nonprimitive forms $Q_3 = 2x^2 + 6y^2$ and $Q_4 = 4x^2 + 4xy + 4y^2$. We have $\left(\frac{\Delta}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. This is the character χ_3. We also have the character χ_4 that we just described. Here is the character table:

	1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
χ_4	+1	+1	−1	−1	+1	+1	−1	−1	+1	+1	−1	−1	+1	+1	−1	−1
χ_3	+1	−1	+1	−1	+1	−1	+1	−1	+1	−1	+1	−1	+1	−1	+1	−1
	Q_1		Q_2		Q_1		Q_2		Q_1		Q_2		Q_1		Q_2	

The columns repeat every four columns since $\left(\frac{-1}{p}\right)$ and $\left(\frac{p}{3}\right)$ are determined by the value of p mod 12. In contrast with earlier examples, the representability of a prime $p > 3$ in discriminant -48 is determined by one character, χ_3, and the other character χ_4 serves only to decide which of the forms Q_1 and Q_2 achieves the representation. The character χ_4 says nothing about the nonprimitive forms Q_3 and Q_4 whose values are all even. On the other hand, from χ_3 we can deduce that all values of Q_3 not divisible by 3 must be congruent to 2 mod 3 while for Q_4 they must be congruent to 1 mod 3. This could also have been deduced from applying χ_3 to the associated primitive forms $x^2 + 3y^2$ and $x^2 + xy + y^2$.

Case 6: $\delta \equiv 0 \bmod 8$, so Δ is a multiple of 32. In this case the congruence $n \equiv (1-\delta)k \bmod 8$ becomes simply $n \equiv k \bmod 8$. Thus all odd numbers in the topograph of a form of discriminant $\Delta = 32m$ must lie in the same congruence class mod 8. The two characters χ_4 and χ_8 can now both occur independently, as shown in the following chart listing their values on the four classes $1, 3, 5, 7 \bmod 8$:

	1	3	5	7
χ_4	+1	−1	+1	−1
χ_8	+1	−1	−1	+1

As an example consider the discriminant $\Delta = -32$. Here there are two primitive forms $Q_1 = x^2 + 8y^2$ and $Q_2 = 3x^2 + 2xy + 3y^2$ along with one nonprimitive form $Q_3 = 2x^2 + 4y^2$. We have $\left(\frac{\Delta}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ with the two factors being the

two independent characters for the prime 2. The full character table is then just a four-fold repetition of the previous shorter table:

	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
χ_4	+1	−1	+1	−1	+1	−1	+1	−1	+1	−1	+1	−1	+1	−1	+1	−1
χ_8	+1	−1	−1	+1	+1	−1	−1	+1	+1	−1	−1	+1	+1	−1	−1	+1
	Q_1	Q_2			Q_1	Q_2			Q_1	Q_2			Q_1	Q_2		

This finishes the analysis of the six cases for characters associated to the prime 2. To summarize we have:

Proposition 6.21. *The characters associated to the prime* 2 *are given in the following table*:

Δ	$4(4m+1)$	$4(4m+3)$	$8(4m+1)$	$8(4m+3)$	$16(2m+1)$	$32m$
χ	—	χ_4	χ_8	$\chi_8' = \chi_4\chi_8$	χ_4	χ_4, χ_8

We have now defined a set of characters for each discriminant Δ, with one character for each odd prime dividing Δ and either zero, one, or two characters for the prime 2 when Δ is even. The character table for discriminant Δ has one row for each of these characters.

If one restricts attention to fundamental discriminants then the only relevant columns in the table in the preceding proposition are the second, third, and fourth columns on the right. Thus the characters for the prime 2 that arise in the three cases of fundamental discriminants are exactly χ_4, χ_8, and χ_8'.

A nice property satisfied by characters is that they are multiplicative, so $\chi(mn) = \chi(m)\chi(n)$ for all m and n for which χ is defined. For the characters χ_p associated to odd primes p this is just the basic property $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$ of Legendre symbols. For the prime 2 the characters χ_4 and χ_8 are multiplicative as well. For χ_4 this holds since $\chi_4(1\cdot 1) = +1 = \chi_4(1)\chi_4(1)$, $\chi_4(1\cdot 3) = -1 = \chi_4(1)\chi_4(3)$, and $\chi_4(3\cdot 3) = +1 = \chi_4(3)\chi_4(3)$. Similarly for χ_8 we have $\chi_8(\pm 1\cdot \pm 1) = +1 = \chi_8(\pm 1)\chi_8(\pm 1)$, $\chi_8(\pm 1\cdot \pm 3) = -1 = \chi_8(\pm 1)\chi_8(\pm 3)$, and $\chi_8(\pm 3\cdot \pm 3) = +1 = \chi_8(\pm 3)\chi_8(\pm 3)$. The multiplicativity of χ_8' follows since $\chi_8' = \chi_4\chi_8$.

In fact χ_4, χ_8, and χ_8' are the only multiplicative functions from the odd integers mod 8 to $\{\pm 1\}$, apart from the trivial function assigning $+1$ to all four of $1, 3, 5, 7$. To see this, note first that each of $3, 5, 7$ has square equal to 1 mod 8 and the product of any two of $3, 5, 7$ is the third, mod 8. This means that a multiplicative function χ from odd integers mod 8 to $\{\pm 1\}$ is completely determined by the two values $\chi(3)$ and $\chi(5)$ since $\chi(1) = \chi(3)\chi(3)$ and $\chi(7) = \chi(3)\chi(5)$. For χ_4 the values on 3 and 5 are $-1, +1$, for χ_8 they are $-1, -1$, and for $\chi_8' = \chi_4\chi_8$ they are $+1, -1$. The only other possibility is $+1, +1$ but this leads to the trivial character.

As we know, an odd prime p is represented in discriminant Δ exactly when $\left(\frac{\Delta}{p}\right) = +1$. This criterion can also be expressed in terms of characters via the following restatement of Proposition 6.9 in different notation:

Proposition 6.22. *$\left(\frac{\Delta}{p}\right) = X_\Delta(p)$ for X_Δ the product of characters given in the table below, where $\Delta = \varepsilon 2^s p_1 \cdots p_k$ for $\varepsilon = \pm 1$ with each p_i an odd prime.* □

Δ	$\left(\frac{\Delta}{p}\right)$	X_Δ
$2^{2l}(4m+1)$	$\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_k}\right)$	$\chi_{p_1}\cdots\chi_{p_k}$
$2^{2l}(4m+3)$	$\left(\frac{-1}{p}\right)\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_k}\right)$	$\chi_4\chi_{p_1}\cdots\chi_{p_k}$
$2^{2l+1}(4m+1)$	$\left(\frac{2}{p}\right)\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_k}\right)$	$\chi_8\chi_{p_1}\cdots\chi_{p_k}$
$2^{2l+1}(4m+3)$	$\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_k}\right)$	$\chi'_8\chi_{p_1}\cdots\chi_{p_k}$

The value $X_\Delta(n) = \pm 1$ is defined whenever n is coprime to Δ. If n is represented in discriminant Δ then $X_\Delta(n) = +1$ since each prime factor p of n is then represented, so $X_\Delta(p) = +1$, and $X_\Delta(n)$ is the product of these terms $X_\Delta(p)$ since X_Δ is multiplicative, being a product of multiplicative functions. If n is not a prime it can happen that $X_\Delta(n) = +1$ even when n is not represented in discriminant Δ. For example for $\Delta = -4$ we have $X_\Delta(21) = \chi_4(21) = \chi_4(3)\chi_4(7) = (-1)(-1) = +1$ but 21 is not represented by the form $x^2 + y^2$, the only form in this discriminant up to equivalence.

Next let us verify that some of the special features of the character tables in the earlier examples hold in general.

Proposition 6.23. (a) *The columns of a character table contain all possible combinations of $+1$ and -1, and each such combination occurs in the same number of columns.*
(b) *If the discriminant Δ is not a square then half of the columns have $X_\Delta(n) = +1$ and half have $X_\Delta(n) = -1$ for numbers n in the congruence class corresponding to the column.*

For example, if Δ is a fundamental discriminant then X_Δ is just the product of all the characters in the character table, so the combinations of ± 1's that give $X_\Delta = +1$ in these cases are the combinations with an even number of -1's. This need not be true for nonfundamental discriminants as the earlier example $\Delta = -48$ shows.

From statement (b) in the proposition we immediately deduce:

Corollary 6.24. *For hyperbolic and elliptic forms, the primes not dividing the discriminant Δ that are represented in discriminant Δ are the primes in exactly half of the congruence classes mod Δ of numbers coprime to Δ.*

For the proof of Proposition 6.23 we will need the following fact:

Lemma 6.25. *For a power p^r of an odd prime p exactly half of the $p^r - p^{r-1}$ congruence classes mod p^r of numbers a not divisible by p satisfy $\left(\frac{a}{p}\right) = +1$.*

Proof: First we do the case $r = 1$. The $p-1$ nonzero congruence classes mod p are $\pm1, \pm2, \cdots, \pm\frac{1}{2}(p-1)$. The two numbers $+a$ and $-a$ in each pair $\pm a$ have the same square, so there are at most $\frac{1}{2}(p-1)$ different nonzero squares mod p. In fact there are exactly this many since if $a^2 \equiv b^2 \mod p$ then p divides $a^2 - b^2 = (a-b)(a+b)$, so since p is prime it must divide either $a-b$ or $a+b$ which means that either $a \equiv b$ or $a \equiv -b \mod p$. Thus exactly half of the $p-1$ nonzero congruence classes mod p are squares, so the lemma is proved when $r = 1$.

Now suppose $r > 1$. The value of $\left(\frac{a}{p}\right)$ depends only on the congruence class of a mod p so there are the same number of numbers a with $\left(\frac{a}{p}\right) = +1$ in each of the intervals $[0,p]$, $[p,2p]$, $[2p,3p]$, etc. There are p^{r-1} of these intervals in $[0,p^r]$. Thus half of the $p^{r-1}(p-1) = p^r - p^{r-1}$ congruence classes mod p^r of numbers a not divisible by p have $\left(\frac{a}{p}\right) = +1$ and half have $\left(\frac{a}{p}\right) = -1$. □

Proof of Proposition 6.23: Let us write $\Delta = \varepsilon 2^s p_1^{r_1} \cdots p_k^{r_k}$ where $\varepsilon = \pm1$, $s \geq 0$, and the p_i's are the distinct odd prime divisors of Δ. Thus the characters for this discriminant are $\chi_{p_1}, \cdots, \chi_{p_k}$ and either zero, one, or two characters associated to the prime 2 when $s > 0$.

To prove statement (a) choose numbers a_i realizing any combination of preassigned values $\chi_{p_i}(a_i) = \pm1$. When $s > 0$ we also choose a number 1, 3, 5, or 7 to realize any preassigned pair of values for χ_4 and χ_8, hence for any preassigned values for the characters associated to the prime 2. By the Chinese Remainder Theorem there is a number a congruent to each a_i mod $p_i^{r_i}$ and to the chosen number $1, 3, 5, 7$ mod 8. The number a is coprime to Δ since it is nonzero mod p_i for each i and is odd when $s > 0$. Thus the column in the character table corresponding to a realizes the chosen values for all the characters.

To prove the second half of statement (a) we will count the number of columns in the character table realizing a given combination of values ±1 and see that this number does not depend on which combination is chosen. By the preceding lemma the number of choices for a_i mod $p_i^{r_i}$ in the previous paragraph is $\frac{1}{2}p_i^{r_i-1}(p_i-1)$, so the Chinese Remainder Theorem implies that when $s = 0$ the number of congruence classes mod Δ realizing a given combination of values ±1 is the product of these numbers $\frac{1}{2}p_i^{r_i-1}(p_i-1)$. When $s > 0$ but there is no character for the prime 2, the product of the numbers $\frac{1}{2}p_i^{r_i-1}(p_i-1)$ is multiplied by 2^{s-1} since this is the number of odd congruence classes mod 2^s. If there is one character for the prime 2 the number 2^{s-1} is cut in half, and if there are two characters for the prime 2 it is cut in half again. Thus in all cases the number of columns realizing a given combination of ±1's is independent of the combination.

For (b), consider the definition of X_Δ which has four different cases depending

on the prime factorization of Δ. If Δ is a square then the applicable formula is the first of the four formulas since an odd square is $1 \bmod 4$, and in fact the formula degenerates to just the constant $+1$ since its terms all cancel out, as each prime factor of Δ occurs to an even power. When Δ is not a square, the terms in the first of the four formulas do not all cancel out, and in the other three formulas there is also at least one term remaining after cancellations, either χ_4, χ_8, or χ_8'.

In view of property (a), to prove (b) it will suffice to show that when Δ is not a square, the set of combinations of values ± 1 in columns of the character table that give $X_\Delta = +1$ has the same number of elements as the set of combinations that give $X_\Delta = -1$. But this is obviously true since we can interchange these two sets by choosing one term in the formula for X_Δ that remains after cancellation and switching the sign of the value ± 1 for this term, keeping the values for the other characters unchanged. □

Genus

Recall the concept of genus that was introduced informally in Section 6.1. The idea was that if two forms of the same discriminant cannot be distinguished by looking only at their values modulo the discriminant then they should be regarded as having the same genus. Here it is best to restrict attention just to primitive forms. We can now give this notion a more precise definition by saying that two primitive forms of discriminant Δ have the same ***genus*** if each character for discriminant Δ takes the same value on the two forms, where the value of a character on a form means its value on all numbers in the topograph not divisible by the prime associated to the character.

In fact there is always a single number in the topograph that can be used to evaluate all the characters, according to the following general result:

Proposition 6.26. *Given a positive integer n and a primitive form Q that represents at least one positive number, then Q represents a positive number coprime to n.*

For the application to evaluating characters we choose $n = |\Delta|$ for Δ the discriminant of Q, which we assume is nonzero.

Proof: Let $Q = ax^2 + bxy + cy^2$. We can replace Q by any equivalent form so we can arrange that $a > 0$ and $c > 0$ by choosing two adjacent regions in the topograph of Q with positive labels a and c. We can also assume $b \geq 0$ since changing the sign of b produces an equivalent form.

The case $n = 1$ is trivial since every positive number is coprime to 1, so we may assume $n > 1$. Suppose first that n is a prime p. One of the following three cases will apply:

(1) If p does not divide a let (x, y) be a primitive pair with p dividing y but not x. Then p will not divide $ax^2 + bxy + cy^2$. For example we could take $(x, y) = (1, p)$.

(2) If p divides a but not c let (x, y) be a primitive pair with p dividing x but not y. Then p will not divide $ax^2 + bxy + cy^2$. For example we could take $(x, y) = (p, 1)$.

(3) If p divides both a and c then it will not divide b since Q is primitive. In this case let (x, y) be a primitive pair with neither x nor y divisible by p. Then p will not divide $ax^2 + bxy + cy^2$. For example we could take $(x, y) = (1, 1)$.

This finishes the proof when n is prime. For a general n let $p_1, \cdots, p_k$ be its distinct prime divisors. For each p_i let (x_i, y_i) be $(1, p_i)$, $(p_i, 1)$, or $(1, 1)$ according to which of the three cases above applies to p_i. Now let $x = x_1 \cdots x_k$ and $y = y_1 \cdots y_k$. Then x and y are coprime since no p_i is a factor of both x and y. If the number $ax^2 + bxy + cy^2$ is not coprime to n it will be divisible by some p_i. If case (1) applies to p_i then p_i divides y but not x so p_i does not divide $ax^2 + bxy + cy^2$. Likewise if cases (2) or (3) apply to p_i then p_i does not divide $ax^2 + bxy + cy^2$. Thus no p_i can divide $ax^2 + bxy + cy^2$. Finally, $ax^2 + bxy + cy^2$ is positive since x and y are positive as are the coefficients except possibly b which is either positive or zero. □

The number of genera in discriminant Δ is at most 2^κ where κ is the number of characters in discriminant Δ. In all the character tables we have looked at, only half of the 2^κ possible combinations of ± 1's were actually realized by forms, and in fact this is true generally:

Theorem 6.27. *If Δ is not a square then the number of genera of primitive forms of discriminant Δ is $2^{\kappa-1}$ where κ is the number of characters in discriminant Δ.*

This turns out to be fairly hard to prove. The original proof by Gauss required a somewhat lengthy digression into the theory of quadratic forms in three variables. An exposition of this proof can be found in the book by Flath listed in the Bibliography. We will give a different proof that deduces the result rather quickly from things we have already done, together with Dirichlet's Theorem about primes in arithmetic progressions discussed at the end of Section 6.1, which we will not prove. We will not need the full strength of Dirichlet's Theorem, and in fact all we will actually need is that each congruence class of numbers $x \equiv b \bmod a$ contains at least one prime greater than 2 if a and b are coprime. One might think this would be easier to prove than that there are infinitely many primes in the congruence class, but this seems not to be the case.

Proof of Theorem 6.27 using Dirichlet's Theorem: We have seen that for each primitive form Q of discriminant Δ there is a number n coprime to Δ that is represented by Q. Then $X_\Delta(n)$ is defined, and we saw when we defined X_Δ that $X_\Delta(n) = +1$ when n is represented by a form of discriminant Δ. In the proof of Proposition 6.23 we showed that exactly half of the 2^κ possible combinations of ± 1's have $X_\Delta = +1$, so the number of genera of forms is at most $2^{\kappa-1}$.

To show that the number of genera is at least $2^{\kappa-1}$ consider a combination of ±1's with $X_\Delta = +1$. By Proposition 6.23 this combination occurs in some column of the character table. This column corresponds to some number n coprime to Δ. By Dirichlet's Theorem there exists a prime p congruent to n mod Δ. We have $X_\Delta(p) = +1$, so since p is prime this implies that p is represented by some form of discriminant Δ. This form must be primitive, otherwise every number it represents would be divisible by some number $d > 1$ dividing Δ so it could not represent p which is coprime to Δ. Thus every combination of ±1's with $X_\Delta = +1$ is realized by some primitive form, so the number of genera is at least $2^{\kappa-1}$. □

From this theorem we can deduce two very strong corollaries.

Corollary 6.28. *For a nonsquare discriminant the number of genera is equal to the number of equivalence classes of primitive forms that have mirror symmetry.*

This may seem a little surprising since there is no apparent connection between genera and mirror symmetry. A possible explanation might be that each genus contains exactly one equivalence class of primitive forms with mirror symmetry, but this is not always true. For example when $\Delta = -56$ we saw in Section 6.1 that there are two genera and two equivalence classes of mirror symmetric forms, but both these forms belong to the same genus. The true explanation will come in Chapter 7 when we study the class group.

Proof: For a nonsquare discriminant the number of equivalence classes of primitive forms with mirror symmetry was computed in Theorem 5.9 to be 2^{k-1} in most cases, where k is the number of distinct prime divisors of Δ. The exceptions are discriminants $\Delta = 4(4m+1)$ when 2^{k-1} is replaced by 2^{k-2}, and $\Delta = 32m$ when 2^{k-1} is replaced by 2^k. In the nonexceptional cases we have $k = \kappa$, the number of characters in discriminant Δ since there is one character for each prime dividing Δ. When $\Delta = 4(4m+1)$ there is no character for the prime 2 so $\kappa = k-1$, and when $\Delta = 32m$ there are two characters for the prime 2 so $\kappa = k+1$. The result follows. □

Corollary 6.29. *For a nonsquare discriminant, each genus of primitive forms consists of a single equivalence class of forms if and only if all the topographs of primitive forms have mirror symmetry.*

Proof: Let $E(\Delta)$ be the set of equivalence classes of primitive forms of discriminant Δ and let $G(\Delta)$ be the set of genera of primitive forms of discriminant Δ. There is a natural function $\Phi: E(\Delta) \to G(\Delta)$ assigning to each equivalence class of forms the genus of these forms. The function Φ is onto since there is at least one form in each genus, by the definition of genus. If all primitive forms of discriminant Δ have mirror symmetry then Corollary 6.28 says that the sets $E(\Delta)$ and $G(\Delta)$ have the same number of elements. Then since Φ is onto it must also be one-to-one. This means that each genus consists of a single equivalence class of forms.

Conversely, if each genus consists of a single equivalence class then Φ is one-to-one. Since Φ is also onto, this means it is a one-to-one correspondence so $E(\Delta)$ and $G(\Delta)$ have the same number of elements. By Corollary 6.28 this means that the equivalence classes of primitive forms with mirror symmetry account for all the elements of $E(\Delta)$, and the proof is complete. □

Exercises

1. For the following discriminants determine the class number and a form in each class, then use a character table to determine which primes are represented by each of the forms, at least to the extent that this can be determined by characters. Also determine the various genera.
(a) -24 (b) 24 (c) -39 (d) -96

2. Determine which primes are represented by each of the following forms:
(a) x^2+8y^2 (b) x^2+9y^2 (c) x^2+25y^2 (d) x^2-12y^2 and $12x^2-y^2$

3. Show that each genus consists of a single equivalence class of forms for the following discriminants: (a) -168 (b) -660 (c) 105

4. Find the smallest positive discriminant for which the number of genera is 16. How does the answer change if only fundamental discriminants are allowed?

5. Show that for a positive nonsquare discriminant Δ, if the principal form represents -1 then all odd primes p dividing Δ must satisfy $p \equiv 1 \bmod 4$. *Hint*: Use χ_p.

6. Use Propositions 6.1 and 6.26 to show that in each nonzero discriminant there exists a form that represents an infinite number of primes.

6.4 Proof of Quadratic Reciprocity

First let us show that quadratic reciprocity can be expressed more concisely as a single formula:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Here p and q are distinct odd primes. Since they are odd, the fractions $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are integers. The only way the exponent $\frac{p-1}{2}\cdot\frac{q-1}{2}$ can be odd is for both factors to be odd, so $\frac{p-1}{2} = 2k+1$ and $\frac{q-1}{2} = 2l+1$, which is equivalent to saying $p = 4k+3$ and $q = 4l+3$. Thus the only time that the right side of the formula shown above is -1 is when p and q are both congruent to $3 \bmod 4$, and quadratic reciprocity is the assertion that the left side of the formula has exactly this property.

There will be three main steps in the proof of quadratic reciprocity. The first is to derive an explicit algebraic formula for $\left(\frac{a}{p}\right)$ due originally to Euler. The second

step is to use this formula to give a somewhat more geometric interpretation of $\left(\frac{a}{p}\right)$ in terms of the number of dots in a certain triangular pattern. Then the third step is the actual proof of quadratic reciprocity using symmetry properties of the patterns of dots. This proof is due to Eisenstein, first published in 1844, simplifying an earlier proof by Gauss who was the first to give a full proof of quadratic reciprocity.

Step 1. In what follows we will always use p to denote an odd prime, and the symbol a will always denote an arbitrary nonzero integer not divisible by p. When we write a congruence such as $a \equiv b$ this will always mean congruence mod p, even if we do not explicitly say that the modulus is p.

Euler's formula is

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

For example, for $p = 11$ Euler's formula says $\left(\frac{2}{11}\right) \equiv 2^5 = 32 \equiv -1 \mod 11$ and $\left(\frac{3}{11}\right) \equiv 3^5 = 243 \equiv +1 \mod 11$. These are the correct values since the squares mod 11 are $(\pm1)^2 = 1$, $(\pm2)^2 = 4$, $(\pm3)^2 = 9$, $(\pm4)^2 \equiv 5$, and $(\pm5)^2 \equiv 3$.

Euler's formula determines the value of $\left(\frac{a}{p}\right)$ uniquely since $+1$ and -1 are not congruent mod p if $p > 2$. It is not immediately obvious that the number $a^{\frac{p-1}{2}}$ should always be congruent to either $+1$ or $-1 \mod p$, but when we prove Euler's formula we will see that this has to be true.

As a special case, taking $a = -1$ in Euler's formula gives the calculation of $\left(\frac{-1}{p}\right)$:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3 \end{cases}$$

Before proving Euler's formula we will need to derive a few preliminary facts about congruences modulo a prime p. First let us note that each of the numbers $a = 1, 2, \cdots, p-1$ has a multiplicative inverse mod p. This is a special case of the fact that each number coprime to a number n has a multiplicative inverse mod n as we saw in Section 2.3. (This was because the equation $ax + ny = 1$ has an integer solution (x, y) whenever a and n are coprime.) Any two choices for an inverse to a mod p are congruent mod p since if $ax \equiv 1$ and $ax' \equiv 1$ then multiplying both sides of $ax' \equiv 1$ by x gives $xax' \equiv x$, and $xa \equiv 1$ so we conclude that $x \equiv x'$.

Which numbers equal their own inverse mod p? If $a \cdot a \equiv 1$, then we can rewrite this as $a^2 - 1 \equiv 0$, or equivalently $(a+1)(a-1) \equiv 0$. This is certainly a valid congruence if $a \equiv \pm1$, so suppose that $a \not\equiv \pm1$. The factor $a+1$ is then not congruent to 0 mod p so it has a multiplicative inverse mod p, and if we multiply the congruence $(a+1)(a-1) \equiv 0$ by this inverse, we get $a - 1 \equiv 0$ so $a \equiv 1$, contradicting the assumption that $a \not\equiv \pm1$. This argument shows that the only numbers among $1, 2, \cdots, p-1$ that are congruent to their inverses mod p are 1 and $p-1$.

An application of this fact is a result known as ***Wilson's Theorem***:

$$(p-1)! \equiv -1 \mod p \quad \text{whenever } p \text{ is prime.}$$

To see why this is true, observe that in the product $(p-1)! = (1)(2)\cdots(p-1)$ each factor other than 1 and $p-1$ can be paired with its multiplicative inverse mod p and these two terms multiply together to give 1 mod p, so the whole product is congruent to just $(1)(p-1)$ mod p. Since $p-1 \equiv -1 \mod p$ this gives Wilson's Theorem.

Now let us prove the following congruence known as ***Fermat's Little Theorem***:

$$a^{p-1} \equiv 1 \mod p \text{ whenever } p \text{ is an odd prime not dividing } a.$$

To show this, note first that the numbers $a, 2a, 3a, \cdots, (p-1)a$ are all distinct mod p since we know that a has a multiplicative inverse mod p, so in a congruence $ma \equiv na$ we can multiply both sides by the inverse of a to deduce that $m \equiv n$. Let us call this property that $ma \equiv na$ implies $m \equiv n$ the *cancellation property* for congruences mod p.

It follows from the cancellation property that the set $\{a, 2a, 3a, \cdots, (p-1)a\}$ is the same mod p as $\{1, 2, 3, \cdots, p-1\}$ since both sets have $p-1$ elements and neither set contains numbers that are 0 mod p. (If $ma \equiv 0$ then multiplying by the inverse of a gives $m \equiv 0$.) If we take the product of all the numbers in each of these two sets we obtain the following congruence:

$$(a)(2a)(3a)\cdots(p-1)a \equiv (1)(2)(3)\cdots(p-1) \mod p$$

We can cancel the factors $2, 3, \cdots, p-1$ from both sides by repeated applications of the cancellation property. The result is the congruence $a^{p-1} \equiv 1$ claimed by Fermat's Little Theorem.

Now we can prove Euler's formula for $\left(\frac{a}{p}\right)$. The first case is that $\left(\frac{a}{p}\right) = +1$. Then $a \equiv x^2$ for some $x \not\equiv 0$ and $a^{\frac{p-1}{2}} \equiv x^{p-1}$ so by Fermat's Little Theorem we have $a^{\frac{p-1}{2}} \equiv 1$. Thus Euler's formula $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ is valid in this case since both sides are $+1$.

The other case is that $\left(\frac{a}{p}\right) = -1$ so a is not a square mod p. Observe first that the congruence $xy \equiv a$ has a solution y mod p for each $x \not\equiv 0$ since x has an inverse x^{-1} mod p so we can take $y = x^{-1}a$. Moreover the solution y is unique mod p since $xy_1 \equiv xy_2$ implies $y_1 \equiv y_2$ by the cancellation property. Since we are in the case that a is not a square mod p the solution y of $xy \equiv a$ satisfies $y \not\equiv x$. Thus the numbers $1, 2, 3, \cdots, p-1$ are divided up into $\frac{p-1}{2}$ pairs $\{x_1, y_1\}$, $\{x_2, y_2\}$, $\cdots$, $\{x_{\frac{p-1}{2}}, y_{\frac{p-1}{2}}\}$ with $x_i y_i \equiv a$ for each i. Multiplying these $\frac{p-1}{2}$ pairs together, we get:

$$a^{\frac{p-1}{2}} \equiv x_1 y_1 x_2 y_2 \cdots x_{\frac{p-1}{2}} y_{\frac{p-1}{2}}$$

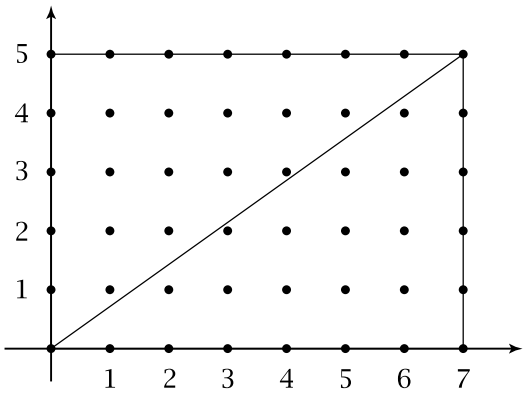
The product on the right is just a rearrangement of $(1)(2)(3)\cdots(p-1)$, and Wilson's Theorem says that this product is congruent to -1 mod p. Thus we see that Euler's formula $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ holds also when $\left(\frac{a}{p}\right) = -1$, completing the proof in both cases.

A consequence of Euler's formula is the multiplicative property of Legendre symbols that we stated and used earlier in the chapter:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

This holds since $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$.

Step 2. Our goal here will be to express the Legendre symbol $\left(\frac{a}{p}\right)$ in more geometric terms. To begin, consider a rectangle in the first quadrant of the xy-plane that is p units wide and a units high, with one corner at the origin and the opposite corner at the point (p, a). The picture at the right shows the case $(p, a) = (7, 5)$. We will be interested in points that lie strictly in the interior of the rectangle and whose coordinates are integers. Points satisfying the latter condition are called *lattice points*. The number of lattice points in the interior is then $(p-1)(a-1)$ since their x-coordinates can range from 1 to $p-1$ and their y-coordinates from 1 to $a-1$, independently.



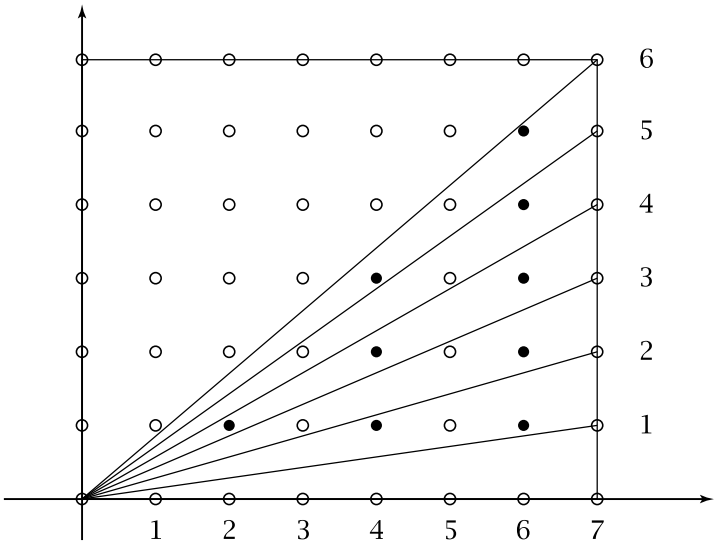
The diagonal of the rectangle from $(0, 0)$ to (p, a) does not pass through any of these interior lattice points since we assume that the prime p does not divide a, so the fraction a/p, which is the slope of the diagonal, is in lowest terms. (If there were an interior lattice point on the diagonal, the slope of the diagonal would be a fraction with numerator and denominator smaller than a and p.) Since there are no interior lattice points on the diagonal, exactly half of the lattice points inside the rectangle lie on each side of the diagonal, so the number of lattice points below the diagonal is $\frac{1}{2}(p-1)(a-1)$. This is an integer since p is odd, which makes $p-1$ even.

A more refined question one can ask is how many lattice points below the diagonal have even x-coordinate and how many have odd x-coordinate. Here there is no guarantee that these two numbers must be equal, and indeed if they were equal then both numbers would have to be $\frac{1}{4}(p-1)(a-1)$ but this fraction need not be an integer, for example when $p = 7$ and $a = 4$.

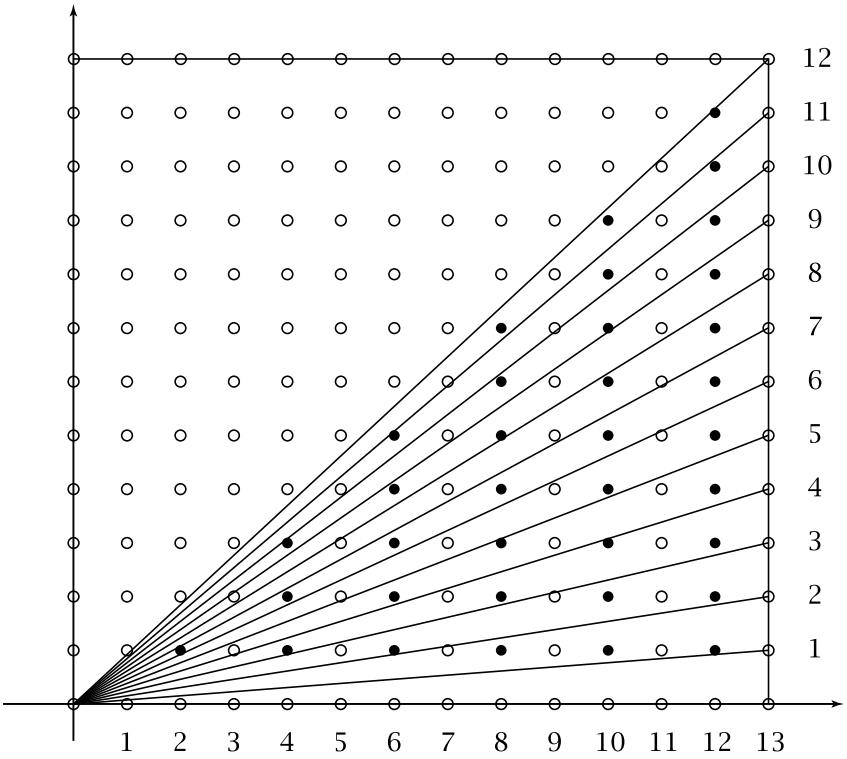
We denote the number of lattice points that are below the diagonal and have even x-coordinate by the letter e. The cases $p = 7$ and $p = 13$ are illustrated in the figures on the next page, with a ranging from 1 to 6 when $p = 7$ and from 1 to 12 when $p = 13$. The corresponding values of e count the number of black dots below the line from the origin to the point (p, a). The values of $\left(\frac{a}{p}\right)$ are also listed. The way that e varies with a seems somewhat unpredictable, but one can observe that $\left(\frac{a}{p}\right)$ is $+1$ when e is even and -1 when e is odd in these examples with $p = 7$ and $p = 13$.

We will show that this simple relationship between e and $\left(\frac{a}{p}\right)$ holds in general:

$$\left(\frac{a}{p}\right) = (-1)^e$$



a	e	$\left(\frac{a}{7}\right)$
6	9	−1
5	7	−1
4	6	+1
3	3	−1
2	2	+1
1	0	+1



a	e	$\left(\frac{a}{13}\right)$
12	36	+1
11	33	−1
10	30	+1
9	26	+1
8	23	−1
7	21	−1
6	15	−1
5	13	−1
4	10	+1
3	6	+1
2	3	−1
1	0	+1

To prove the formua $\left(\frac{a}{p}\right) = (-1)^e$ we first derive a formula for e. The segment of the vertical line $x = u$ between the x-axis and the diagonal has length $u \cdot {}^a\!/_p = {}^{ua}\!/_p$ since the slope of the diagonal is ${}^a\!/_p$. If u is a positive integer, the number of lattice points on this line segment is $\lfloor {}^{ua}\!/_p \rfloor$, the greatest integer $n \leq {}^{ua}\!/_p$. If we add up these numbers of lattice points for u running through the set of even numbers $E = \{2, 4, \cdots, p-1\}$ we get:

$$e = \sum_E \lfloor {}^{ua}\!/_p \rfloor$$

The way to compute $\lfloor {}^{ua}\!/_p \rfloor$ is to apply the division algorithm for integers, dividing p into ua to obtain $\lfloor {}^{ua}\!/_p \rfloor$ as the quotient with a remainder that we denote $r(u)$.

Thus we have:

$$ua = p\lfloor ua/p \rfloor + r(u) \tag{1}$$

The formula $ua = p\lfloor ua/p \rfloor + r(u)$ implies that $\lfloor ua/p \rfloor$ has the same parity as $r(u)$ since u is even and p is odd. Hence $\sum_E \lfloor ua/p \rfloor$ has the same parity as $\sum_E r(u)$. Since $e = \sum_E \lfloor ua/p \rfloor$, this implies that the number $(-1)^e$ that we are interested in can be computed as:

$$(-1)^e = (-1)^{\sum_E r(u)} \tag{2}$$

With this last expression in mind we will focus our attention on the remainders $r(u)$.

The number $r(u)$ lies strictly between 0 and p and can be either even or odd, but in both cases we can say that $(-1)^{r(u)}r(u)$ is congruent to an even number in the interval $(0, p)$ since if $r(u)$ is odd, so is $(-1)^{r(u)}r(u)$ and then adding p to this gives an even number between 0 and p. Thus there is always an even number $s(u)$ between 1 and p that is congruent to $(-1)^{r(u)}r(u)$ mod p. Obviously $s(u)$ is unique since no two numbers in the interval $(0, p)$ are congruent mod p.

A key fact about these even numbers $s(u)$ is that they are all distinct as u varies over the set E. For suppose we have $s(u) = s(v)$ for another even number v in E. Thus $r(u) \equiv \pm r(v) \mod p$, which implies $au \equiv \pm av \mod p$ in view of the equation (1) above. We can cancel the a from both sides of the congruence $au \equiv \pm av$ to get $u \equiv \pm v$. However we cannot have $u \equiv -v$ because the number between 0 and p that is congruent to $-v$ is $p - v$, so we would have $u = p - v$ which is impossible since u and v are even while p is odd. Thus we must have $u \equiv +v$, hence $u = v$ since these are numbers strictly between 0 and p. This shows that the numbers $s(u)$ are all distinct.

Now consider the product of all the numbers $(-1)^{r(u)}r(u)$ as u ranges over the set E. Written out, this is:

$$\Big[(-1)^{r(2)}r(2)\Big]\Big[(-1)^{r(4)}r(4)\Big]\cdots\Big[(-1)^{r(p-1)}r(p-1)\Big] \tag{3}$$

By equation (1) we have $r(u) \equiv ua \mod p$, so this product is congruent mod p to:

$$\Big[(-1)^{r(2)}2a\Big]\Big[(-1)^{r(4)}4a\Big]\cdots\Big[(-1)^{r(p-1)}(p-1)a\Big]$$

On the other hand, by the definition of the numbers $s(u)$ the product (3) is congruent mod p to $[s(2)][s(4)]\cdots[s(p-1)]$. There are $\frac{1}{2}(p-1)$ factors here and they are all distinct even numbers in the interval $(0, p)$ as we showed in the previous paragraph, so they are just a rearrangement of the numbers $2, 4, \cdots, p-1$. Thus we have the following congruence:

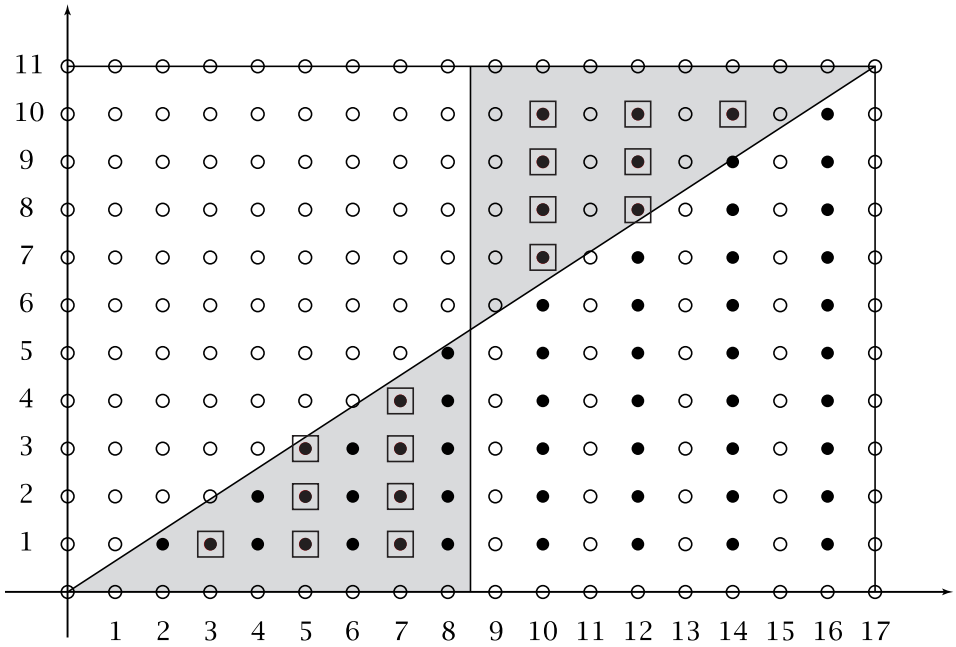
$$\Big[(-1)^{r(2)}2a\Big]\Big[(-1)^{r(4)}4a\Big]\cdots\Big[(-1)^{r(p-1)}(p-1)a\Big] \equiv (2)(4)\cdots(p-1) \mod p$$

Canceling the factors $2, 4, \cdots, p-1$ from both sides of this congruence gives:

$$(-1)^{\sum_E r(u)}a^{\frac{p-1}{2}} \equiv 1 \mod p$$

Both the factors $(-1)^{\sum_E r(u)}$ and $a^{\frac{p-1}{2}}$ are ± 1 mod p and their product is 1 so they must be equal mod p (using the fact that 1 and -1 are not congruent modulo an odd prime). By Euler's formula we have $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$ mod p, so from the earlier formula (2) we conclude that $\left(\frac{a}{p}\right) = (-1)^e$. This finishes Step 2.

Step 3. Now we specialize the value of a to be an odd prime q distinct from p. As in Step 2 we consider lattice points in the interior of a $p \times q$ rectangle.



From Step 2 we know that $\left(\frac{q}{p}\right) = (-1)^e$ where e is the number of lattice points with even x-coordinate inside the rectangle and below the diagonal. Suppose that we divide the rectangle into two equal halves separated by the vertical line $x = p/2$ which does not pass through any lattice points since p is odd. This vertical line cuts off two smaller triangles from the two large triangles above and below the diagonal of the rectangle. In the figure above, these smaller triangles are the shaded triangles. Call the lower small triangle L and the upper one U, and let l and u denote the number of lattice points with even x-coordinate in the interiors of L and U respectively. Note that u has the same parity as the number of lattice points with even x-coordinate in the interior of the quadrilateral below U in the right half of the rectangle since each column of lattice points inside the rectangle has $q-1$ points, an even number. Thus e has the same parity as $l+u$, hence $(-1)^e = (-1)^{l+u}$.

The next thing to notice is that rotating the triangle U by 180 degrees about the center of the rectangle carries it onto the triangle L. This rotation takes the lattice points inside U with even x-coordinate onto the lattice points inside L with odd x-coordinate. Thus we obtain the formula $\left(\frac{q}{p}\right) = (-1)^t$ where t is the total number of lattice points inside the triangle L.

Reversing the roles of p and q, we can also say that $\left(\frac{p}{q}\right) = (-1)^{t'}$ where t' is the number of lattice points inside the triangle L' with edges on the diagonal of the

rectangle, the horizontal line $y = q/2$, and the y-axis. Then $t + t'$ is the number of lattice points in the interior of the small rectangle formed by L and L' together. This number is just $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Thus we have

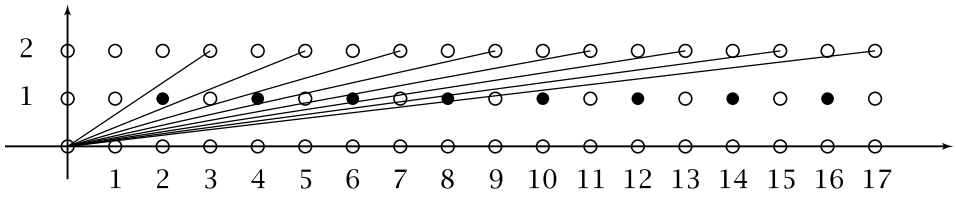
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^t(-1)^{t'} = (-1)^{t+t'} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

which finally finishes the proof of quadratic reciprocity. □

We can also use the geometric interpretation of $\left(\frac{a}{p}\right)$ to prove the formula for $\left(\frac{2}{p}\right)$ that was given in Section 6.2, namely:

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p = 8k \pm 1 \\ -1 & \text{if } p = 8k \pm 3 \end{cases}$$

We have shown that $\left(\frac{2}{p}\right) = (-1)^e$ where e is the number of lattice points inside a $p \times 2$ rectangle lying below the diagonal and having even x-coordinate, as indicated in the following figure which shows the diagonals for $p = 3, 5, 7, \cdots, 17$:



p	3	5	7	9	11	13	15	17
e	1	1	2	2	3	3	4	4

Another way to describe e is to say that it is equal to the number of even integers in the interval from $p/2$ to p. We do not need to assume that p is prime in order to count these points below the diagonals, just that p is odd. One can see what the pattern is just by looking at the figure: Each time p increases by 2 there is one more even number at the right end of the interval $(p/2, p)$, and there may or may not be one fewer even number at the left end of the interval, depending on whether p is increasing from $4k - 1$ to $4k + 1$ or from $4k + 1$ to $4k + 3$. It follows that the parity of e depends only on the value of p mod 8 as in the table for $p \le 17$, so e is even for $p \equiv \pm 1 \bmod 8$ and e is odd for $p \equiv \pm 3 \bmod 8$.

Exercises

1. As a sort of converse to Wilson's Theorem, show that if n is not a prime then $(n-1)!$ is not congruent to -1 mod n. More precisely, when $n > 4$ and n is not prime, show that n divides $(n-1)!$, so $(n-1)! \equiv 0 \bmod n$. What happens when $n = 4$?

2. In Step 2 of the proof of quadratic reciprocity there were figures depicting the geometric interpretation of $\left(\frac{a}{7}\right)$ and $\left(\frac{a}{13}\right)$. Draw analogous figures for $\left(\frac{a}{5}\right)$ and $\left(\frac{a}{11}\right)$.

3. Show that the calculation of the Legendre symbol $\left(\frac{-1}{p}\right)$ can also be obtained using the method in the proof of quadratic reciprocity involving counting certain lattice points in a $(p-1) \times p$ rectangle.