Chapter 4
THE GENUS GROUP

Our first lemma is very technical, but turns out to be the tool needed to get us as far as we can go (without much more work) in our quest to answer the question posed at the start of the previous chapter. As always, $\Delta$ is a nonsquare discriminant.

4.1 Lemma: a) Suppose the quadratic form $F(X, Y)$ represents both $g$ and $j$. Suppose further that $\text{GCD}(g, \Delta F) = 1 = \text{GCD}(j, \Delta F)$.

Let $t$ be an odd prime divisor of $\Delta F$. Then $\left( \frac{j}{t} \right) = \left( \frac{g}{t} \right)$.

b) Furthermore,

i) If $\Delta F \equiv 12, 16, \text{or } 28 \mod 32$ then $gj \equiv 1 \mod 4$.

ii) If $\Delta F \equiv 0 \mod 32$ then $gj \equiv 1 \mod 8$.

iii) If $\Delta F \equiv 8 \mod 32$ then $gj \equiv 1 \text{ or } 7 \mod 8$.

iv) If $\Delta F \equiv 24 \mod 32$ then $gj \equiv 1 \text{ or } 3 \mod 8$.

Proof: a) Let $F(X, Y) = ax^2 + bXY + cy^2$. As $F$ represents both $g$ and $j$, write $F(e, f) = g$ and $F(h, i) = j$. Consider the change of variable

$X \to eX + hY, \quad Y \to fX + iY$.

(Note that since $ei - fh$ might not be $\pm 1$, this might not be a substitution.)

By Lemma 1.2(f), applying this change of variable to $F(X, Y)$ gives $gX^2 + rXY + jY^2$ (some $r$). By Lemma 1.2(d), the discriminant of this new form, $r^2 - 4gj$, equals $(\Delta F)(ei - fh)^2$. In particular, we see $\Delta F$ divides $r^2 - 4gj$, so that $r^2 \equiv 4gj \mod \Delta F$. Therefore, if $t$ is an odd prime dividing $\Delta F$, then $r^2 \equiv 4gj \mod t$, showing $\left( \frac{4gj}{t} \right) = 1$. We have $1 = \left( \frac{4gj}{t} \right) = \left( \frac{4}{t} \right) \left( \frac{g}{t} \right) \left( \frac{j}{t} \right) = \left( \frac{g}{t} \right) \left( \frac{j}{t} \right)$. As both of these Legendre symbols equal $\pm 1$. 

\[ \frac{1}{4} \]
and as their product is +1, they are either both +1 or both -1.
In either case, we have \( \frac{g}{t} = \frac{1}{t} \).

(b). Recall from the proof of (a) we have \( r^2 - 4gj = (\Delta F)(e_1 - f_2 h)^2 = (\Delta F) y^2 \) with \( y = e_1 - f_2 h \). Since in all cases of part (b) we have \( \Delta F \equiv 0 \mod 4 \), we know \( r \) is even.

Let \( s = r/2 \). We get \( s^2 - gj = (\Delta F/4)y^2 \). Also, since \( g \) and \( j \) are relatively prime to \( \Delta F \), \( g \) and \( j \) are odd.

We now prove the three cases in (b)(i). Case 1: Suppose \( \Delta \equiv 12 \mod 32 \), and write \( \Delta = 12 + 32k \). We get \( s^2 - gj = (3 + 8k)y^2 \). As \( y^2 \equiv 0 \) or \( 1 \mod 4 \), the right hand side is congruent to \( 0 \) or \( 3 \mod 4 \). Being odd, we have \( gj \equiv 1 \) or \( 3 \mod 4 \). Suppose \( gj \equiv 3 \mod 4 \). As \( s^2 \equiv 0 \) or \( 1 \mod 4 \), we get \( s^2 - gj \equiv 1 \) or \( 2 \mod 4 \). This cannot equal the right hand side. Therefore, we must have \( gj \equiv 1 \mod 4 \), as desired.

Case 2: Suppose \( \Delta \equiv 28 \mod 32 \). This case is almost identical to the previous one.

Case 3: Suppose \( \Delta \equiv 16 \mod 32 \), and write \( \Delta = 16 + 32k \). We get \( s^2 - gj = (4 + 8k)y^2 \). The right hand side is congruent to \( 0 \mod 4 \), and so is even. As \( gj \) is odd, we have \( s \) is odd and \( s^2 \equiv 1 \mod 4 \), forcing \( gj \equiv 1 \mod 4 \). This completes the proof of (b)(i).

Next we do (b)(ii). Suppose \( \Delta F \equiv 0 \mod 32 \), and write \( \Delta F = 32k \). We get \( s^2 - gj = (8k)y^2 \equiv 0 \mod 8 \). The right hand side is even, and since \( gj \) is odd, we must have \( s \) odd, so that \( s^2 \equiv 1 \mod 8 \). Since \( 0 \equiv s^2 - gj \equiv 1 - gj \mod 8 \), we have \( gj \equiv 1 \mod 8 \), as desired. This proves (b)(ii).

We turn to (b)(iii). We suppose \( \Delta \equiv 8 \mod 32 \), and write \( \Delta = 8 + 32k \). We get \( s^2 - gj = (2 + 8k)y^2 \). The right hand side is congruent to \( 0 \) or \( 2 \mod 8 \), and so is even. That means \( s \) is odd and \( s^2 \equiv 1 \mod 8 \). It follows that \( gj \equiv 1 \) or \( 7 \mod 8 \), as desired, proving (b)(iii).

Finally, for (b)(iv), suppose \( \Delta \equiv 24 \mod 32 \) and write \( \Delta = 24 + 32k \). We get \( s^2 - gj = (6 + 8k)y^2 \equiv 0 \) or \( 6 \mod 8 \). We see \( s \) is odd and \( s^2 \equiv 1 \mod 8 \), forcing \( gj \) to be congruent to \( 1 \) or \( 3 \mod 8 \). This proves (b)(iv).

4.2 Examples: a) In Exercise 1.5, we saw that \( F = [1, 1, 10] \) and \( G = [2, 1, 5] \) are not equivalent. Let us now show that via Lemma 4.1. Obviously \( F \) represents 1 and \( G \) represents 2. If \( F \) and \( G \) are equivalent, then \( F \) also represents 2 (Lemma 1.2(e)). Since 1 and 2 are both relatively prime to \( \Delta F = -39 \),
Lemma 4.1(a) tells us that \( \frac{1}{t} = \frac{2}{t} \) for any odd prime divisor \( t \) of \( \Delta F = -39 \). However, if we take \( t = 3 \), we get \( \frac{1}{3} = 1 \) while \( \frac{2}{3} = -1 \). Therefore \( F \) is not equivalent to \( G \).

b) Now let \( H = [3, 3, 4] \). Exercise 1.5 shows \( F \) and \( H \) are inequivalent. Can we use Lemma 4.1 to reprove that? The answer is no, a fact which we will prove in this chapter. For now, let us just illustrate that fact. \( F(1, 0) = 1 \) and \( H(1, 4) = 79 \). Repeating the argument in part (a), suppose \( F \) and \( H \) are equivalent. Then \( F \) also represents \( 79 \). As \( \text{GCD}(1, \Delta F) = 1 = \text{GCD}(79, \Delta F) \), by Lemma 4.1 we must have \( \frac{1}{t} = \frac{79}{t} \) for any odd prime divisor \( t \) of \( \Delta F = -39 \). However, that statement is true! (Use \( 79 \equiv 1 \) mod 39.) Unlike part (a), we get no contradiction here.

Incidently, the statement \( F \) represents \( 79 \) is false. Were it true, Proposition 1.4 would show \( F \) and \( H \) are equivalent, which we know to be false. Lemma 4.1 fails to detect that \( F \) does not represent \( 79 \). Later in this chapter, we will see that Lemma 4.1 is unable to detect any difference between \( F \) and \( H \), or more to the point, between \( \text{EC}(F) \) and \( \text{EC}(H) \).

**PREVIEW:** Let \( F, H, \) and \( G \) be as in the previous example. Let \( K = [2, -1, 5] \), and recall \( \text{EC}(G) = \text{EC}(K) \). Part (a) of the previous example shows Lemma 4.1 can distinguish between \( \text{EC}(F) \) and \( \text{EC}(G) \). Similarly, it can distinguish between \( \text{E}(H) \) and \( \text{EC}(G) \). However, we will see it cannot distinguish between \( \text{EC}(F) \) and \( \text{EC}(H) \). We know from Example 1.13 that when \( \Delta = -39 \), \( \text{EC}(F), \text{EC}(H), \) and \( \text{EC}(G) = \text{EC}(K) \) are the only equivalence classes, but Lemma 4.1 has blurry vision and only sees \( (\text{EC}(F), \text{EC}(H)) \) and \( (\text{EC}(G)) \), clumping \( \text{EC}(F) \) and \( \text{EC}(H) \) together. (Note that these two clumps have different sizes.)

Let us switch to proper equivalence classes, recalling that \( \text{EC}(F) = \text{PEC}(F) \) and \( \text{EC}(H) = \text{PEC}(H) \), but \( \text{EC}(G) = \text{EC}(K) = \text{PEC}(G) \cup \text{PEC}(K) \). Lemma 4.1 sees two clumps, \( (\text{PEC}(F), \text{PEC}(H)) \) and \( (\text{PEC}(G), \text{PEC}(K)) \). Those clumps are officially called genuses. (Note both genuses have the same size.)
Continuing with this preview, (with \( \Delta = -39 \)) recall that in Example 3.9, we saw that \( \text{CL}(\Delta) = (\text{PEC}(F), \text{PEC}(H), \text{PEC}(G), \text{PEC}(K)) \) is generated by \( \text{PEC}(G) \), and the square of that is \( \text{PEC}(H) \). Also note that \( F \) is the Pell form, so that \( \text{PEC}(F) \) is the identity of \( \text{CL}(\Delta) \). Thus if \( SQ(\Delta) \) is the subgroup of squares of elements in the Abelian group \( \text{CL}(\Delta) \), then \( SQ(\Delta) = (\text{PEC}(F), \text{PEC}(H)) \).

The factor group \( \text{CL}(\Delta)/SQ(\Delta) \) consists of the cosets of \( SQ(\Delta) \).

\[
\text{CL}(\Delta)/SQ(\Delta) = \{(\text{PEC}(F), \text{PEC}(H)), (\text{PEC}(G), \text{PEC}(K))\}.
\]

Those cosets are the genera, not only in this example, but as we will see, always. We will cleverly call \( \text{CL}(\Delta)/SQ(\Delta) \) the genus group, \( \text{GEN}(\Delta) \). Since the genera are just cosets of \( SQ(\Delta) \), all genera have the same size. The genus \( SQ(\Delta) \) (equivalently, the genus containing \( \text{PEC}(F_\Delta) \)) is known as the principal genus.

(Caution: There is a coincidence here. \( (\text{PEC}(F), \text{PEC}(H)) \) is the set of elements of \( \text{CL}(\Delta) \) having order 1 or 2. That set will later be called \( \text{AMB}(\Delta) \). In this example \( \text{AMB}(\Delta) = SQ(\Delta) \). That is not always true.)

In this chapter, our initial presentation of \( \text{GEN}(\Delta) \), will not use \( SQ(\Delta) \). Instead, we will define a certain subgroup \( K_\Delta \) of \( W_\Delta \), and a homomorphism \( \Omega_\Delta : \text{CL}(\Delta) \rightarrow W_\Delta/K_\Delta \). Then we will define \( \text{GEN}(\Delta) \) to be \( \text{CL}(\Delta)/\text{Ker} \Omega_\Delta \). By doing things that way, we will be able to answer the question asked at the start of the previous chapter, at least as far as we can answer it. Finally, in later chapters, we will work hard to show \( \text{Ker} \Omega_\Delta = SQ(\Delta) \).

We now turn to defining \( K_\Delta \). (The connection between the following definition and Lemma 4.1 is obvious.)

**Definition:** Let \( \Delta \) be a nonsquare discriminant. Define \( K_\Delta \) to equal the set of \( n^* \in U_\Delta \) such that the following are true of \( n \).

i) \( \left( \frac{n}{\Delta} \right) = 1 \) for every odd prime divisor \( t \) of \( \Delta \).

ii) If \( \Delta \equiv 12, 16, \) or \( 28 \mod 32 \), then \( n \equiv 1 \mod 4 \).

iii) If \( \Delta \equiv 0 \mod 32 \), then \( n \equiv 1 \mod 8 \).

iv) If \( \Delta \equiv 8 \mod 32 \), then \( n \equiv 1 \) or \( 7 \mod 8 \).

v) If \( \Delta \equiv 24 \mod 32 \), then \( n \equiv 1 \) or \( 3 \mod 8 \).
4.3 Lemma: a) Let $p$ be an odd prime, and let $e \geq 1$. Then $((Y^*)^2 \mid Y^* \in U_p^e)$ has size $\Phi(p^e)/2$.

b) Let $e \geq 3$. $((Y^*)^2 \mid Y^* \in U_2^e)$ has size $2^{e-3}$.

c) Let $D = 2^e d$, with $d$ odd. Suppose $\text{GCD}(n, D) = 1$. Then $X^2 \equiv n \mod D$ has a solution IFF $X^2 \equiv n \mod t$ has a solution for all primes $t$ dividing $d$, and furthermore if $e = 2$, then $n \equiv 1 \mod 4$, while if $e \geq 3$ then $n \equiv 1 \mod 8$.

d) Let $D = 2^e d$ with $d$ odd, and let $d = p_1^{e_1} \cdots p_r^{e_r}$ with the $p_i$ distinct primes. If $e \leq 2$, the size of $((X^*)^2 \mid X^* \in U_D)$ equals $(1/2^r)\Phi(d)$. If $e \geq 3$, the size of $((X^*)^2 \mid X^* \in U_D)$ equals $(2^{e-r-3})\Phi(d)$.

Proof: Basically, this is all well known, and follows easily from standard facts found in many elementary number theory books (such as the one mentioned in the historical remark near the end of this chapter). We will only refresh the reader's memory. For (a), it is well known that if $\text{GCD}(n, p) = 1$, then $n$ is a quadratic residue $\mod p^e$ IFF $n$ is a quadratic residue $\mod p$. Since half of the numbers from 1 to $p - 1$ are quadratic residues $\mod p$, half of the $n$ (with $p \nmid n$) between 1 and $p^e - 1$ are quadratic residues $\mod p$, and hence $\mod p^e$. For part (b), a standard fact says for $e \geq 3$ and $n$ odd, $n$ is a quadratic residue $\mod 2^e$ IFF $n \equiv 1 \mod 8$. Thus the number of odd $n$ between 1 and $2^e - 1$ which are quadratic residues $\mod 2^e$ is $\Phi(2^e)/4 = 2^{e-3}$. Part (c) uses the two standard facts already mentioned and the Chinese remainder theorem. Part (d) uses part (c) and the Chinese remainder theorem to show the size of $((X^*)^2 \mid X^* \in U_D)$ is the product of the sizes of $((Y^*)^2 \mid Y^* \in U_{p_i}^{e_i})$ (over all $i$) and (when $e > 0$)

$(((Y^*)^2 \mid Y^* \in U_2^e))$. By part (a), the product of the various $\|((Y^*)^2 \mid Y^* \in U_{p_i}^{e_i})\|$ is $(1/2^r)\prod \Phi(p_i^{e_i}) = (1/2^r)\Phi(d)$. When $e = 0,$
we are done. When \( e \in (1, 2) \), the size of \(((Y^*)^2 \mid Y^* \in U_2e)\) is 1, and again we are done. When \( e \geq 3 \), the size of \(((Y^*)^2 \mid Y^* \in U_2e)\) is (by (b)) \(2e^{-3} \), which when multiplied by \((1/2^r)\phi(d)\), gives \((2e^{-r-3})\phi(d)\).

4.4 Proposition: a) If \( \Delta \) is odd or congruent to one of 0, 12, or 28 mod 32, then \( K_\Delta = ((X^*)^2 \mid X^* \in U_\Delta) \).

b) If \( \Delta \) is congruent to one of 8, 16, or 24 mod 32, then \( K_\Delta = ((X^*)^2 \mid X^* \in U_\Delta) \cup ((X^*)^2(1 - \Delta/4)^* \mid X^* \in U_\Delta) \).

c) If \( \Delta \) is congruent to either 4 or 20 mod 32, then \( K_\Delta = ((X^*)^2 \mid X^* \in U_\Delta) \cup ((X^*)^2(4 - \Delta/4)^* \mid X^* \in U_\Delta) \).

d) \( K_\Delta = (n^* \in U_\Delta \mid F_\Delta \text{ represents } n) \).

Proof: Each of (a), (b), and (c) says \( K_\Delta \) equals a set \( S \) (which varies by case). Let \( T = (n^* \in U_\Delta \mid F_\Delta \text{ represents } n) \). The proof will proceed by showing (in order) the following containments: \( S \subset T \subset K_\Delta \subset S \). This will prove the result (including (d)) in all cases.

In order to show \( S \subset T \), we work in cases. In each case (a), (b), and (c), we need (in part) to show that \(((X^*)^2 \mid X^* \in U_\Delta) \subset T \). However, the leading coefficient of \( F_\Delta \) is 1, and so \( F_\Delta(X, 0) = X^2 \), which gives that containment. For case (a), the definition of \( S \) shows \( S \subset T \) (as desired) in that case. In case (b), we also need to show that \(((X^*)^2(1 - \Delta/4)^* \mid X^* \in U_\Delta) \subset T \). However, in (b), \( 4 \mid \Delta \) and \( 1 - \Delta/4 \) is odd. We have \( \text{GCD}(\Delta, 1 - \Delta/4) = 1 \), so \((1 - \Delta/4)^* \in U_\Delta \). As \( \Delta \) is even, \( F_\Delta = X^2 - (\Delta/4)Y^2 \). Therefore, for \( X^* \in U_\Delta \), \((X^*)^2(1 - \Delta/4)^* = F_\Delta(X, X)^* \in T \), as desired, completing case (b). Case (c) is similar, using \( 4 - \Delta/4 \) is odd and \( F_\Delta(2X, X) = X^2(4 - \Delta/4) \).
We now show $T \subseteq K_\Delta$. Suppose $n^* \in T$. Then $n^* \in U_\Delta$ and we may assume $F_\Delta$ represents $n$. Since $F_\Delta(1, 0) = 1$, $F_\Delta$ also represents 1. Let $t$ be an odd prime divisor of $\Delta$. Applying Lemma 4.1(a), with $j = 1$ and $g = n$, we have $(\frac{n}{t}) = (\frac{1}{t}) = 1$,
showing $n^*$ satisfies the first criterion for membership in $K_\Delta$.
That it also satisfies the second criterion follows with equal ease from Lemma 4.1(b), since $jg = (1)(n) = n$.

We now show $K_\Delta \subseteq S$. Suppose $n^* \in K_\Delta$. We will treat the two cases that $n$ is, or is not, a quadratic residue mod $\Delta$.
We will also show that in case (a), $n$ must be a quadratic residue mod $\Delta$.
Suppose $n$ is a quadratic residue mod $\Delta$. Write $X^2 \equiv n \bmod \Delta$. Then $n^* = (X^2)^* \in ((X^2)^* \mid X^* \in U_\Delta) \subseteq S$ (in each of (a), (b), (c)).

Now we will show that in the case (a), $n^* \in K_\Delta$ implies $n$ is a quadratic residue mod $\Delta$. Write $\Delta = 2^e d$, with $d$ odd. Now $n^* \in K_\Delta$ tells us $(\frac{n}{t}) = 1$ for each prime divisor of $d$. If $\Delta$ is odd, then $e = 0$, and $\Delta = d$, and Lemma 4.3(c) shows $n$ is a quadratic residue mod $\Delta$. If $\Delta$ is congruent to 12 or 28 mod 32, then $e = 2$, and Lemma 4.3(c) shows that for $n$ to be a quadratic residue mod $\Delta$, we need $n \equiv 1 \bmod 4$. However, for these two $\Delta$, the definition of $K_\Delta$ tells us $n \equiv 1 \bmod 4$. Similarly, if $\Delta \equiv 0 \bmod 32$, then $e \geq 5$, and so to be a quadratic residue mod $\Delta$ we need $n \equiv 1 \bmod 8$. The definition of $K_\Delta$ gives that.
This paragraph together with the previous one, complete the entire proof for part (a).

We turn to the case (b). We have $n^* \in K_\Delta$, and want to show that $n^* \in S$, already knowing it is true if $n$ is a quadratic residue mod $\Delta$. Suppose $n$ is not a quadratic residue mod $\Delta$.
In (b), we previously saw that if $u = 1 - \Delta/4$, then GCD($u$, $\Delta$) = 1, so there is an integer $v$ with $uv \equiv 1 \bmod \Delta$. If $t$ is a prime divisor of $d$ (and so of $\Delta/4$), we have $1 = (\frac{1}{t}) = (\frac{1 - \Delta/4}{t}) = (\frac{u}{t}) = (\frac{v}{t})$, the last equality since $uv \equiv 1 \bmod t$. Since $n^* \in K_\Delta$, we also know $(\frac{n}{t}) = 1$, and so $(\frac{nv}{t}) = 1$. Recall that we are assuming
n is not a quadratic residue mod $\Delta$. If $n \equiv 1 \mod 8$, that contradicts Lemma 4.3(c). Thus we also know $n \not\equiv 1 \mod 8$.

We now look at the three cases in (b), starting with $\Delta \equiv 8 \mod 32$. In this case, $u = 1 - \Delta/4 \equiv 7 \mod 8$. Since $8 | \Delta$ and $uv \equiv 1 \mod \Delta$, we have $uv \equiv 1 \mod 8$, showing $v \equiv 7 \mod 8$. Since $n^* \in K_{\Delta}$, the definition shows $n$ is congruent to 1 or 7 mod 8, and we already know it is not congruent to 1 mod 8. Thus $n \equiv 7 \mod 8$, and so $nv \equiv 1 \mod 8$.

As $(\frac{nv}{t}) = 1$ for all primes $t$ dividing $d$, Lemma 4.3(c) shows $nv$ is a quadratic residue mod $\Delta$. Write $nv \equiv X^2 \mod \Delta$. Since $uv \equiv 1 \mod \Delta$, we get $n \equiv X^2 u = X^2 (1 - \Delta/4) \mod \Delta$, which shows $n^*$ is in $S$ (for the $S$ in (b)).

Still in (b), assume $\Delta \equiv 16 \mod 32$, so that $u = 1 - \Delta/4 \equiv 5 \mod 8$. As $uv \equiv 1 \mod 8$, we see $v \equiv 5 \mod 8$. The definition of $K_{\Delta}$ shows $n \equiv 1 \mod 4$, and since we know $n \not\equiv 1 \mod 8$, we have $n \equiv 5 \mod 8$. Thus $nv \equiv 1 \mod 8$, and so Lemma 4.3(c) shows $nv$ is a quadratic residue mod $\Delta$. Proceed as before.

The last case in (b) has $\Delta \equiv 24 \mod \Delta$. That gives $v \equiv u \equiv 3 \mod 8$, but the definition of $K_{\Delta}$ gives $n \equiv 3 \mod 8$, so $nv \equiv 1 \mod 8$. Proceed as before. This completes the entire proof for (b).

We turn (c). It follows the same pattern as the arguments used in (b), except we now let $u = 4 - \Delta/4$. For the $\Delta$ in (c), our new $u$ is odd, GCD($u, \Delta$) = 1, and there is still a $v$ with $uv \equiv 1 \mod \Delta$. As in (b), we still get $(\frac{nv}{t}) = 1$ for all primes $t$ dividing $d$. The two cases in (c) are $\Delta$ congruent to 4 or 20 mod 32. In both cases, $\Delta = 4d$ with $d$ odd. If $n \equiv 1 \mod 4$, Lemma 4.3(c) shows $n$ is a quadratic residue mod $\Delta$. As that case has already been done, suppose $n \equiv 3 \mod 4$. Note that $u = 4 - \Delta/4 \equiv 3 \mod 4$ (for either case of $\Delta$). As $uv \equiv 1 \mod \Delta$, and hence mod 4, we see $v \equiv 3 \mod 4$, and so $nv \equiv 1 \mod 4$. Lemma 4.3(c) shows $nv$ is a quadratic residue mod $\Delta$. Writing $nv \equiv X^2 \mod \Delta$ yields $n \equiv X^2 u = X^2 (4 - \Delta/4) \mod \Delta$, so that $n^*$ is in the $S$ of part (c).
4.5 Corollary: $K_{\Delta}$ is a subgroup of $W_{\Delta}$ containing the square of every element of $U_{\Delta}$.

Proof: It is straightforward from the definition to verify that $K_{\Delta}$ is a subgroup of $U_{\Delta}$ (using that $(1 \mod 8, 7 \mod 8)$ and $(1 \mod 8, 3 \mod 8)$ are both subgroups of $U_8$). Proposition 4.4(a)(b)(c) shows that $K_{\Delta}$ contains the square of any element in $U_{\Delta}$. We must show $K_{\Delta} \subseteq W_{\Delta}$. However, that follows from Proposition 4.4(d) and Lemma 2.24.

Later, we will see that $W_{\Delta}/K_{\Delta}$ is isomorphic to $CL(\Delta)/SQ(\Delta)$, which in our preview we called $GEN(\Delta)$. Thus $W_{\Delta}/K_{\Delta}$ and $GEN(\Delta)$ are isomorphic groups, defined in vastly different ways. In order to eventually prove that isomorphism, we will need to know the size of $W_{\Delta}/K_{\Delta}$, which we now determine.

4.6 Corollary: Let $\Delta$ be a nonsquare discriminant, and let $r$ be the number of distinct odd prime divisors of $\Delta$. Then $W_{\Delta}/K_{\Delta}$ is isomorphic to the direct product of $s$ copies of $Z_2$, where $s$ is given as follows. In particular, $|W_{\Delta}/K_{\Delta}| = 2^s$.

i) $s = r - 1$ if $\Delta$ is odd or $\Delta \equiv 4$ or $20 \mod 32$.

ii) $s = r$ if $\Delta \equiv 8, 12, 16, 24,$ or $28 \mod 32$.

iii) $s = r + 1$ if $\Delta \equiv 0 \mod 32$.

Proof: Since Corollary 4.5 shows $K_{\Delta}$ contains the square of every element of $W_{\Delta} \subseteq U_{\Delta}$, each element of $W_{\Delta}/K_{\Delta}$ has order 1 or 2, showing that group is a direct product of $s$ copies of $Z_2$ for some $s$. Thus $|W_{\Delta}/K_{\Delta}| = 2^s$. We must determine the size of $s$. We know the size of $U_{\Delta}$ is given by the Euler phi function $\phi(\Delta)$, and we know $W_{\Delta}$ has index 2 in $U_{\Delta}$ (Corollary 2.18), so that $|W_{\Delta}| = \phi(\Delta)/2$. In order to find the size of $W_{\Delta}/K_{\Delta}$, we need only determine the size of $K_{\Delta}$, which we will do using Proposition 4.4(a)(b)(c).
In Lemma 4.3(d) (with $D = \Delta$), we have formulas for the
size of $((X^{*})^{2} \mid X^{*} \in U_{\Delta})$. We also know for some $\Delta$, that set
equals $K_{\Delta}$. Let us dispose of those cases first. If $\Delta$ is odd or
congruent to 12 or 28 mod 32, then Proposition 4.4(a) tells us
$K_{\Delta} = ((X^{*})^{2} \mid X^{*} \in U_{\Delta})$. For those $\Delta$, we have $\Delta = 2^{e}d$ with $d$
odd and $e \in \{0, 2\}$. Now Lemma 4.3(d) tells us the size of $K_{\Delta}$ is
$(1/2^{r})\phi(d)$. As the size of $W_{\Delta}$ is $\phi(\Delta)/2 = \phi(2^{e})\phi(d)/2$, the size
of $W_{\Delta}/K_{\Delta}$ is $\phi(2^{e})2^{r-1}$. When $\Delta$ is odd, $e = 0$, and we get $2^{r-1}$,
as desired. When $\Delta$ is congruent to 12 or 28 mod 32, $e = 2$, and we get $2^{r}$, as desired. If $\Delta \equiv 0 \mod 32$, Proposition 4.4(a)
again tells us $K_{\Delta} = ((X^{*})^{2} \mid X^{*} \in U_{\Delta})$. Writing $\Delta = 2^{e}d$, we have $e \geq 5$. In this case, Lemma 4.3(d) tells us the size of $K_{\Delta}$ is
$(2^{e-r-3})\phi(d)$. The size of $W_{\Delta}$ is $\phi(\Delta)/2 = \phi(2^{e})\phi(d)/2 =$
$2^{e-2}\phi(d)$. The size of $W_{\Delta}/K_{\Delta}$ is $2^{r+1}$, as desired. That
completes the cases in Proposition 4.4(a), for which
$K_{\Delta} = ((X^{*})^{2} \mid X^{*} \in U_{\Delta})$.

For the remaining cases in Proposition 4.4(b)(c), we have
$K_{\Delta} = ((X^{*})^{2} \mid X^{*} \in U_{\Delta}) \cup ((X^{*})^{2}u^{*} \mid X^{*} \in U_{\Delta})$, where
$u = 1 - \Delta/4$ if $\Delta \equiv 8, 16$, or 24 mod 32, and $u = 4 - \Delta/4$ if
$\Delta \equiv 4$ or 20 mod 32. We claim that in these cases, the size of
$K_{\Delta}$ is twice the size of $((X^{*})^{2} \mid X^{*} \in U_{\Delta})$. Since $u$ is a unit
mod $\Delta$ (in all these cases), clearly $((X^{*})^{2}u^{*} \mid X^{*} \in U_{\Delta})$ has the
same size as $((X^{*})^{2} \mid X^{*} \in U_{\Delta})$, and so to prove our claim, we
need only show those last two sets have no overlap. If they
have an element in common, then since $((X^{*})^{2} \mid X^{*} \in U_{\Delta})$ is a
subgroup of (the Abelian) $U_{\Delta}$, we would have that $u^{*}$ is a
square in $U_{\Delta}$. Write $Z^{2} \equiv u \mod \Delta$. For $\Delta \equiv 8, 16$, or 24 mod
32, we have $8 \mid \Delta$, so $Z^{2} \equiv u \mod 8$, showing $u \equiv 1 \mod 8$.
However, for those $\Delta$, $u = 1 - \Delta/4 \equiv 1 \mod 8$, proving our claim.
For $\Delta \equiv 4$ or 20 mod 32, 4 $\mid \Delta$, and so $Z^{2} \equiv u \mod 4$, which
implies $u \equiv 1 \mod 4$. However, for those $\Delta$, $u = 4 - \Delta/4 \equiv$
1 mod 4, again proving the claim.
Suppose $\Delta \equiv 8, 16, \text{ or } 24 \mod 32$. Writing $\Delta = 2^e d, \ e \geq 3$ so that $|((X^*)^2 \mid X^* \in U_\Delta)| = (2^{e-r-3})\phi(d)$, and the size of $K_\Delta$ is twice that, equaling $(2^{e-r-2})\phi(d)$. Also, $|W_\Delta| = \phi(\Delta)/2 = (2^{e-2})\phi(d)$, and so $|W_\Delta/K_\Delta| = 2^r$, as desired.

Finally, suppose $\Delta \equiv 4 \text{ or } 20 \mod 32$, so $\Delta = 4d \text{ with } d \text{ odd}$. From Lemma 4.3(d), the size of $((X^*)^2 \mid X^* \in U_\Delta)$ is $(1/2^r)\phi(d)$, and the size of $K_\Delta$ is twice that, so equals $(1/2^{r-1})\phi(d)$. The size of $W_\Delta$ is $\Phi(\Delta)/2 = \Phi(d)$, and so the size of $W_\Delta/K_\Delta$ is $2^{r-1}$, as desired.

4.7 Example: Recall from Example 2.25 that $W_{-39} = (1^*, 2^*, 4^*, 5^*, 8^*, 10^*, 11^*, 16^*, 20^*, 22^*, 25^*, 32^*) \subseteq U_{-39}$. We now find $K_{-39}$. By Proposition 4.4(a), $K_\Delta = ((X^*)^2 \mid X^* \in U_\Delta) = (1^*, 4^*, 10^*, 16^*, 22^*, 25^*)$.

We now see $W_{-39}/K_{-39}$ has size 2 (as predicted by Corollary 4.6), and consists of the two cosets of $K_{-39}$ in $W_{-39}$, namely $(1^*, 4^*, 10^*, 16^*, 22^*, 25^*)$ and $(2^*, 5^*, 8^*, 11^*, 20^*, 32^*)$. (Recall that in our preview, we saw GEN(-39) also has two elements.)

4.8 Example: In Example 2.26, we saw that $W_{60} = (1^*, 7^*, 11^*, 17^*, 43^*, 49^*, 53^*, 59^*)$. We now find $K_{60}$. Since $60 \equiv 28 \mod 32$, by Corollary 4.6, $|W_{60}/K_{60}| = 4$, and since $|W_{60}| = 8$, we know $|K_{60}| = 2$. It also contains $(X^*)^2$ for all $X^* \in U_{60}$, and so it obviously contains $1^*$ and $49^*$. Thus, we see $K_{60} = (1^*, 49^*)$.

Therefore, $W_{60}/K_{60}$ consists of the four cosets of $K_{60}$ in $W_{60}$, namely $(1^*, 49^*)$, $(11^*, 59^*)$, $(7^*, 43^*)$, and $(17^*, 53^*)$.

4.9 Corollary: Let $F$ be a Gaussian form of discriminant $\Delta$. Then the set $(n^* \in U_\Delta \mid F \text{ represents } n)$ is a coset of $K_\Delta$ in $W_\Delta$.
Proof: By Lemma 1.15, $F$ does represent some number relatively prime to $\Delta$, showing the above set is not empty. Furthermore, Lemma 2.24 shows that set is a subset of $W_\Delta$.

Given one such $m^*$ in that set, we must show that set equals $m^*K_\Delta$. We may assume $F$ represents $m$.

For one containment, take an arbitrary $n^* \in U_\Delta$ such that $F$ represents $n$. We need $n^* \in m^*K_\Delta$. As we know $m^*$ and $n^*$ are both in $U_\Delta$, we can write $n^* = m^*k^*$ with $k^* \in U_\Delta$. We need $k^* \in K_\Delta$. Let $t$ be an odd prime divisor of $\Delta$. We have $n \equiv mk \mod \Delta$, so that $n \equiv mk \mod t$. Thus $(\frac{n}{t}) = (\frac{m}{t})(\frac{k}{t})$.

However, Lemma 4.1(a) also tells us $(\frac{n}{t}) = (\frac{m}{t})$, and so $(\frac{k}{t}) = 1$, showing $k^*$ satisfies the first criterion for inclusion in $K_\Delta$. As for the other criteria, we will only do the case $\Delta \equiv 8 \mod 32$, leaving the other cases to the reader. Since $n \equiv mk \mod \Delta$ and $8 \mid \Delta$, we see $n \equiv mk \mod 8$, and so $nm \equiv m^2k \mod 8$.

However, when $\Delta \equiv 8 \mod 32$, Lemma 4.1(b) tells us $nm$ is congruent to either 1 or 7 mod 8. Since $m^2 \equiv 1 \mod 8$, we see $k$ is congruent to 1 or 7 mod 8, completing the proof that $k^* \in K_\Delta$. The other cases are similar.

For the reverse containment, suppose $h^* \in m^*K_\Delta$. We must show $h^* = n^*$ for some $n$ which is represented by $F$. Write $h^* = m^*b^*$ with $b^* \in K_\Delta$. By Proposition 4.4(d), we may assume $F_\Delta$ represents $b$. We know $F$ represents $m$. By Lemma 3.5, in the group $CL(\Delta)$, the product $PEC(F)PEC(F_\Delta)$ represents $mb$. However, $PEC(F_\Delta)$ is the identity of that group, and so $PEC(F)$ represents $mb$. Thus $F$ represents $mb$. Take $n = mb$, and we are done.

Corollary 4.9 obviously relates a Gaussian form $F$ of discriminant $\Delta$ to a coset of $K_\Delta$ in $W_\Delta$. We use that fact to define the homomorphism $\Omega_\Delta$ mentioned in our preview.
Definition: Let $\Delta$ be a nonsquare discriminant. We define a function $\Omega_\Delta : \text{CL}(\Delta) \to W_\Delta/K_\Delta$ as follows. For any $\text{PEC}(F) \in \text{CL}(\Delta)$, find a number $n$ represented by $F$ with $n$ relatively prime to $\Delta$, and let $\Omega_\Delta(\text{PEC}(F)) = n^*k_\Delta \in W_\Delta/K_\Delta$.

4.10 Proposition: $\Omega_\Delta$ is a well-defined onto group homomorphism. $\text{CL}(\Delta)/\text{Ker } \Omega_\Delta$ is isomorphic to $W_\Delta/K_\Delta$.

Proof: Let $\text{PEC}(F) \in \text{CL}(\Delta)$. Since equivalent forms represent the same numbers, the definition of $\Omega_\Delta$ does not depend on which form in $\text{PEC}(F)$ we work with. Lemma 1.15 shows $F$ does represent an $n$ relatively prime to $\Delta$, and Lemma 2.24 shows $n^* \in W_\Delta$. Thus $\Omega_\Delta(\text{PEC}(F)) = n^*k_\Delta \in W_\Delta/K_\Delta$ is defined. That it is well-defined is immediate from Corollary 4.9. That $\Omega_\Delta$ is onto follows immediately from Lemma 2.24. To show we have a homomorphism, suppose $\Omega_\Delta(\text{PEC}(F)) = n^*k_\Delta$ and $\Omega_\Delta(\text{PEC}(G)) = m^*k_\Delta$ (where we may assume $F$ and $G$ represent $n$ and $m$, respectively). By Lemma 3.5, $\text{PEC}(F)\text{PEC}(G)$ represents $nm$, and so $\Omega_\Delta(\text{PEC}(F)\text{PEC}(G)) = (nm)^*k_\Delta = (n^*k_\Delta)(m^*k_\Delta) = \Omega_\Delta(\text{PEC}(F))\Omega_\Delta(\text{PEC}(G))$. The final statement is from the Fundamental Theorem of Homomorphisms.

We now give our initial definition of $\text{GEN}(\Delta)$, the genus group.

Definition: $\text{GEN}(\Delta) = \text{CL}(\Delta)/\text{Ker } \Omega_\Delta$. The elements of $\text{GEN}(\Delta)$, (i.e., the cosets of $\text{Ker } \Omega_\Delta$ in $\text{CL}(\Delta)$) are called the genuses. The genus containing $\text{PEC}(F_\Delta)$, with $F_\Delta$ the Pell form, is called the principal genus.

Recall that at the start of the previous chapter, we asked the following question. Suppose we know $\text{GCD}(n, \Delta) = 1$ and $\Delta$ represents $n$ (and $n > 0$ when $\Delta < 0$). Then we know there is a Gaussian form $F(X, Y)$ with discriminant $\Delta$ such that $F$ represents $n$. Can we determine which $F$?

We will give three examples, which illustrate how far our theory allows us to go towards answering that question.
In the first ($\Delta = 60$), every genus has size 1, which means our question can be completely answered. In other two ($\Delta = -39$, $\Delta = -87$) more common sort, the genuses have size greater than 1, and our question can only be answered "up to genus". The first and third example also show how knowing something about $W_\Delta/K_\Delta$ can help find $CL(\Delta)$. (In general, if one wishes to know the structure of a group, it is often useful to know something about a homomorphic image of that group, and $W_\Delta/K_\Delta$ is isomorphic to $GEN(\Delta) = CL(\Delta)/K_\Delta$). The "concordant" multiplication of $CL(\Delta)$ is awkward. However, hopefully one can find $W_\Delta/K_\Delta$ without great difficulty. Thus, an "easy" group helps us understand a "hard" group.)

4.11 Example: Let $\Delta = 60$. We leave to the reader the exercise of using Proposition 1.7 and the arguments in the examples following it, to show that any form of discriminant 60 is properly equivalent to one of $F = [1, 0, -15]$, $G = [-1, 0, 15]$, $H = [3, 0, -5]$, $K = [-3, 0, 5]$, $L = [2, 2, -7]$, $M = [2, -2, -7]$, $N = [-2, 2, 7]$, or $P = [-2, -2, 7]$ (all Gaussian).

We have determined 8 proper equivalence classes, but know there may be redundancies. We can find some by considering the genuses. From Example 4.8, we know $W_\Delta/K_\Delta$ consists of the four cosets of $K_\Delta$ in $W_\Delta$, namely $K_\Delta = (1^*, 49^*)$, $11^*K_\Delta = (11^*, 59^*)$, $7^*K_\Delta = (7^*, 43^*)$, and $17^*K_\Delta = (17^*, 53^*)$. Thus there are four genuses, and each can be associated (via the isomorphism between $GEN(\Delta)$ and $W_\Delta/K_\Delta$) with one of the above cosets of $K_\Delta$.

Since $F(1, 0) = 1$, $\Omega_\Delta(PEC(F)) = 1^*K_\Delta = K_\Delta$. Thus PEC(F) is in the genus associated with $K_\Delta$. Now $G(2, 1) = 11$, so that $W_\Delta(PEC(G)) = 11^*K_\Delta$. Thus PEC(G) is in the genus associated with $11^*K_\Delta$. Similarly, $H(2, 1) = N(0, 1) = P(0, 1) = 7$, and so PEC(H), PEC(N) and PEC(P) are all in the genus associated to $7^*K_\Delta$. Now $L(0, 1) = M(0, 1) = -7$, so PEC(L) and PEC(M) are both in the genus associated with $(-7)^*K_\Delta = (since \ -7 = 53 \ mod \ 60)\ 53^*K_\Delta = 17^*K_\Delta$, which also contains PEC(K), since $K(1, 2) = 17$. 

$\phi^6$
We have found that the genus associated to $K_\Delta$ contains only one proper equivalence class, namely $\text{PEC}(F)$. Since genuses are just cosets of $\text{Ker } \Omega_\Delta$, they all have the same size. Thus all genuses contain just one proper equivalence class, and so we now see $\text{PEC}(H) = \text{PEC}(N) = \text{PEC}(P)$, and $\text{PEC}(K) = \text{PEC}(L) = \text{PEC}(M)$. Furthermore, being in different genuses, $\text{PEC}(F)$, $\text{PEC}(G)$, $\text{PEC}(H)$, and $\text{PEC}(K)$ are all different. Therefore, $\text{CL}(60) = (\text{PEC}(F), \text{PEC}(G), \text{PEC}(H), \text{PEC}(K))$.

Having size 4, $\text{CL}(60)$ is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. We claim the latter. Since $\text{Ker } \Omega_\Delta$ only contains $\text{PEC}(F)$ (which is the identity of $\text{CL}(\Delta)$), since $F$ is the Pell form, by Proposition 4.10 we have $\text{CL}(\Delta) = \text{CL}(\Delta)/\text{Ker } \Omega_\Delta \cong W_\Delta / K_\Delta$. Thus Corollary 4.6 gives what we need.

We now turn to our earlier question. Suppose $\text{GCD}(n, 60) = 1$ and $\Delta = 60$ represents $n$. (Recall, Proposition 2.23 tell us when that is true.) We know at least one of $F$, $G$, $H$, or $K$ represents $n$. Can we determine (without a brute force search) which ones? In this example, the answer is yes.

Claim: $F$ represents $n$ IFF $n \equiv 1$ or $49 \pmod{60}$.
$G$ represents $n$ IFF $n \equiv 11$ or $59 \pmod{60}$.
$H$ represents $n$ IFF $n \equiv 7$ or $43 \pmod{60}$.
$K$ represents $n$ IFF $n \equiv 17$ or $53 \pmod{60}$.

Proof: Suppose $F$ represents $n$. As $\text{GCD}(n, 60) = 1$, the definition of $\Omega_\Delta$ shows $\Omega_\Delta(\text{PEC}(F)) = n^*K_\Delta$. But we already know $\Omega_\Delta(\text{PEC}(F)) = K_\Delta$. Thus $n^*K_\Delta = K_\Delta$, and so $n \equiv 1$ or $49 \pmod{60}$. This proves one direction of the first statement. Suppose $G$ represents $n$. Then $n^*K_\Delta = \Omega_\Delta(\text{PEC}(G)) = 11^*K_\Delta$. Thus $n^*K_\Delta = 11^*K_\Delta$, and so $n \equiv 11$ or $59 \pmod{60}$. This proves one direction of the second statement. The remaining two statements are argued similarly. We now have one direction of each statement. The other direction of all of them follows from that together with the fact that we know at least one of $F$, $G$, $H$, or $K$ must represent $n$. (Observe that in this example, exactly one of $F$, $G$, $H$, or $K$ will represent $n$. In later examples, two inequivalent forms might represent $n$, but that can only happen when those two forms are "in the same genus", i.e., their proper equivalence classes are in the same genus.)
As a final observation, note that the Gaussian form \( Q = [42, 138, 113] \) has discriminate 60, and so is properly equivalent to one of F, G, H, or K. Which one? Since each genus comprises a single proper equivalence class (when \( \Delta = 60 \)), there is an easy way to tell; just determine which of the four genera PEC(Q) belongs to. Now \( Q(0, 1) = 113 \equiv 53 \mod 60 \).
Thus \( \Omega_{\Delta}(\text{PEC}(Q)) = 53*K_{\Delta} = 17*K_{\Delta} = W_{\Delta}(\text{PEC}(K)), \) and so Q is properly equivalent to K.

In the previous example, each genus contains a single proper equivalence class, allowing us to answer our question completely. That particularly nice situation is uncommon. More usually, a genus will contain more than one proper equivalence class. In such cases, we will only be able to answer our question partially (up to genus).

4.12 Example: Let \( \Delta = -39 \). In Example 3.9, we saw that \( \text{CL}(\Delta) = (F, G, H, K) \) with \( F = [1, 1, 10], G = [2, 1, 5], H = [3, 3, 4], \) and \( K = [2, -1, 5] \). In Example 4.7, we saw \( W_{\Delta}/K_{\Delta} \) has size 2, and consists of the two cosets \( K_{\Delta} = (1*, 4*, 16*, 22*, 25*) \) and \( 2*K_{\Delta} = (2*, 5*, 8*, 11*, 20*, 32*) \). As \( |\text{CL}(\Delta)| = 4, \) but \( |W_{\Delta}/K_{\Delta}| = 2, \) we must have that the homomorphism \( \Omega_{\Delta} : \text{CL}(\Delta) \to W_{\Delta}/K_{\Delta} \) is "2 to 1", and each genus must contain 2 proper equivalence classes. Now \( F(1, 0) = 1 \) and \( H(0, 1) = 4 \), and so \( \Omega_{\Delta}(\text{PEC}(F)) = 1*K_{\Delta} = K_{\Delta} = 4*K_{\Delta} = \Omega_{\Delta}(\text{PEC}(H)) \). Thus \( (\text{PEC}(F), \text{PEC}(H)) \) is one genus (the principal genus, since \( F = F_{\Delta} \)), while the other must be \( (\text{PEC}(G), \text{PEC}(K)) \).

Suppose \( \text{GCD}(n, -39) = 1 \) and \( \Delta = -39 \) represents \( n > 0 \). Our question is which of F, G, H, and K represent \( n \)? Since G and K are (improperly) equivalent, we have \( \text{EC}(G) = \text{PEC}(G) \cup \text{PEC}(K) \). We also previously saw that \( \text{EC}(F) = \text{PEC}(F) \) and \( \text{EC}(H) = \text{PEC}(H) \). Since equivalent forms represent the same numbers, as far as our question is concerned, it might be more efficient to think of our two genera as \( (\text{EC}(F), \text{EC}(H)) \) and \( (\text{EC}(G)) \).

Claim: At least one of F or H represents \( n \) IFF \( n^* \in K_{\Delta} \) and G represents \( n \) IFF \( n^* \in 2*K_{\Delta} \).
Proof: Suppose $F$ represents $n$. Since $F(1, 0) = 1$, $n^*K_\Delta = \Omega_\Delta(PEC(F)) = 1^*K_\Delta = K_\Delta$. Suppose $H$ represents $n$. Since $H(0, 1) = 4$, $n^*K_\Delta = \Omega_\Delta(PEC(H)) = 4^*K_\Delta = K_\Delta$. This proves one direction of the first statement. Suppose $G$ represents $n$. Since $G(1, 0) = 2$, $n^*K_\Delta = \Omega_\Delta(PEC(G)) = 2^*K_\Delta$. This proves one direction of the second statement. The converse of both statements follows from that and the fact we know one of $F$, $G$, or $H$ must represent $n$. (Note $F(0, 1) = 10 = H(1, 1)$, so repetition is possible, but only since $PEC(F)$ and $PEC(H)$ are in the same genus.)

As a final observation, note that the Gaussian form $[142, 165, 48]$ has discriminant $-39$, and so is properly equivalent to one of $F$, $G$, $H$, or $K$. That form represents $142$, and $\text{GCD}(142, 39) = 1$. Now $142 \equiv 25 \mod 39$, and so the image of that form under $\Omega_\Delta$ is $142^*K_\Delta = K_\Delta$. Thus the proper equivalence class of that form is in the principal genus, and so that form is properly equivalent to either $F$ or $H$.

4.13 Let $\Delta = -87$. We leave to the reader the exercise of using Proposition 1.7 to show that every Gaussian form of discriminant $-87$ is properly equivalent to one of the following 8 forms $[1, \pm 1, 22]$, $[2, \pm 1, 11]$, $[3, \pm 3, 8]$, $[4, \pm 3, 6]$. We face the problem of potential redundancies. Let $F = [1, 1, 22]$, $K = [4, 3, 6]$, and $L = [4, -3, 6]$. By Lemma 1.2(h)(j), $PEC([1, -1, 22]) = PEC(F)$, and so we have at most 7 proper equivalence classes. Since $F(1, 0) = 1$ and $K(1, 0) = 4 = L(1, 0)$, by Corollary 4.5 we have $\Omega_\Delta(PEC(F)) = 1^*K_\Delta = K_\Delta = 4^*K_\Delta = \Omega_\Delta(PEC(K)) = \Omega_\Delta(PEC(L))$, so that $PEC(F)$, $PEC(K)$, and $PEC(L)$ are in the same genus. We claim these three classes are distinct.

As $L$ is improperly equivalent to $K$ (via $X \to X$, $Y \to -Y$), Proposition 3.7 shows $PEC(L)$ is the inverse of $PEC(K)$ in $CL(\Delta)$. If the order of $PEC(K)$ is not 1 or 2, then $PEC(K)$ and $PEC(L)$ are distinct, and also neither equals $PEC(F)$ (which is the identity of $CL(\Delta)$, since $F = F_\Delta$). Thus, to show $PEC(F)$, $PEC(K)$, and $PEC(L)$ are distinct, it will suffice to show $PEC(K)^2 \neq PEC(F)$.

To calculate $PEC(K)^2$, we find a pair of concordant forms in $PEC(K)$. We will use methods discussed theoretically in Chapter 3. We start with $K = [4, 3, 6]$. Note $K(1, 1) = 13$ and
GCD(13, 4) = 1. Since 1(1) - 1(0) = 1, we let S be the proper substitution \( X \rightarrow X, Y \rightarrow X + Y \), and see SK = \([13, 15, 6] \in \text{PEC}(K)\). K and SK have relatively prime leading coefficients, but different middle coefficients. We fix that. Applying the proper substitution T -18 to K gives \([4, -141, 1248]\). Applying T -6 to SK gives \([13, -141, 384]\). These last two forms are concordant, and in PEC(K). Now \([4, -141, 1248] \cdot [13, -141, 384] = [52, -141, 96]\). Thus PEC(K)² = PEC([52, -141, 96]). We claim this last is not PEC(F). Now [52, -141, 96] represents 7 (via \( X = Y = 1 \)). However, \( F(X, Y) = (X + Y/2)^2 + (87/4)Y^2 = \neq 7 \) for all \( X, Y \). We now know PEC(K)² = PEC(F).

We now see that one genus contains at least 3 distinct classes, PEC(F), PEC(K), and PEC(L). By Corollary 4.6, there are 2 genera. As a genus is simply a coset of \( \text{Ker} \, \Omega_{\Delta} \) in \( \text{CL}(\Delta) \), all genera have the same size. We know \(|\text{CL}(\Delta)| \leq 7\), and there are two genera, each of which has size at least three. That implies \(|\text{CL}(\Delta)| = 6\), and each genus has size three.

The principal genus is (PEC(F), PEC(K), PEC(L)). Being the kernel of \( \Omega_{\Delta} \), it is a group. Clearly PEC(K) has order 3.

The four forms not yet used, namely \([2, \pm 1, 11]\) and \([3, \pm 3, 8]\), must yield exactly 3 proper equivalence classes, which will fall in the other genus. We leave to the reader the exercise of showing that those three proper equivalence classes are PEC([3, 3, 8]), PEC([2, 1, 11]), and PEC([2, -1, 11]), of orders 2, 6, and 6, respectively.

Under the isomorphism between GEN(\(\Delta\)) and \( W_\Delta/K_\Delta \), the principal genus (i.e., the identity of GEN(\(\Delta\))) goes to \( K_\Delta \) (the identity of \( W_\Delta/K_\Delta \)). The other genus contains PEC([2, 1, 11]). Since \([2, 1, 11]\) represents 11, (and GCD(11, 60) = 1), we see that genus goes to 11*K_\Delta. (Note that we now know \( W_\Delta = K_\Delta \cup 11*K_\Delta \), despite not having calculated either \( W_\Delta \) or \( K_\Delta \).)

Claim: Suppose GCD(n, -87) = 1 and \( \Delta = -87 \) represents \( n > 0 \). At least one of \([1, 1, 22]\) or \([4, 3, 6]\) represents \( n \) IFF \( n^* \in K_\Delta \). At least one of \([3, 3, 8]\) or \([2, 1, 11]\) represents \( n \) IFF \( n^* \in 11*K_\Delta \).

We leave the proof as an exercise to the reader.
Examples 4.12 and 4.13 are illustrative of the best that can be done concerning our question, at least as far as having a nice linear answer goes. The claims made in those examples all involve linear conditions of the form "IFF \( n^* \in m^* K_\Delta \). Such linearity is lost if one tries to get past the "up to genus" ambiguity. It is beyond the scope of these notes to discuss why.

As mentioned in our preview, Gauss proved that the principal genus, Ker \( \Omega_\Delta \), equals \( (\text{PEC}(F))^2 \mid \text{PEC}(F) \in \text{CL}(\Delta) \). Note that Ker \( \Omega_\Delta \) is defined via the external groups \( \mathbb{W}_\Delta \) and \( K_\Delta \), while \( (\text{PEC}(F))^2 \mid \text{PEC}(F) \in \text{CL}(\Delta) \) is defined purely in terms of \( \text{CL}(\Delta) \). We now begin the journey of proving Gauss' result.

Notation: \( \text{SQ}(\Delta) = (\text{PEC}(F))^2 \mid \text{PEC}(F) \in \text{CL}(\Delta) \). (Note that since \( \text{CL}(\Delta) \) is Abelian, \( \text{SQ}(\Delta) \) is a subgroup of \( \text{CL}(\Delta) \).)

Our goal is to show \( \text{SQ}(\Delta) = \text{Ker} \Omega_\Delta \). One direction is easy. (The other is far from easy.)

Lemma 4.14: \( \text{SQ}(\Delta) \subseteq \text{Ker} \Omega_\Delta \).

Proof: Let \( C \in \text{CL}(\Delta) \). By Lemma 1.15, there is an integer \( b \) which \( C \) represents, with \( \text{GCD}(b, \Delta) = 1 \). The definitions show \( \Omega_\Delta(C) = b^* K_\Delta \). As \( \Omega_\Delta \) is a homomorphism, \( \Omega_\Delta(C^2) = (b^*)^2 K_\Delta = K_\Delta \) (using Corollary 4.5).

The map \( \text{CL}(\Delta) \to \text{CL}(\Delta) \) sending \( C \) to \( C^2 \) is a group homomorphism from the Abelian group \( \text{CL}(\Delta) \) to itself. The image of this map is obviously \( \text{SQ}(\Delta) \).

Definition: \( \text{AMB}(\Delta) \) will denote the kernel of the above "squaring" map from \( \text{CL}(\Delta) \) to itself. (\( \text{AMB} \) stands for ambiguous.)
4.15 Lemma: Let $C = \text{PEC}(F) \in \text{CL}(\Delta)$. $C \in \text{AMB}(\Delta)$ IFF $C$ is its own inverse in $\text{CL}(\Delta)$ IFF $F$ is improperly equivalent to itself IFF $\text{PEC}(F) = \text{EC}(F)$.

Proof: The first IFF is from the definition of $\text{AMB}(\Delta)$. The others are from Corollary 3.8.

The next result is crucial. It requires a fair amount of work, which will be presented in the coming chapters. Part of the work was already done, since we already determined the size of $\mathbb{W}_\Delta/K_\Delta$ (Corollary 4.6).

4.16 Proposition: $|\text{AMB}(\Delta)| = |\mathbb{W}_\Delta/K_\Delta|$.

4.17 Corollary (Gauss' duplication theorem): $\text{SQ}(\Delta) = \text{Ker } \Omega_\Delta$.

Proof: Since $\text{AMB}(\Delta)$ is the kernel of the squaring map on $\text{CL}(\Delta)$, by the Fundamental Theorem of Homomorphisms, $|\text{SQ}(\Delta)||\text{AMB}(\Delta)| = |\text{CL}(\Delta)|$. We also know that $\Omega_\Delta$ is a homomorphism from $\text{CL}(\Delta)$ onto $\mathbb{W}_\Delta/K_\Delta$. Therefore, $|\text{CL}(\Delta)| = |\text{Ker } \Omega_\Delta||\mathbb{W}_\Delta/K_\Delta|$. Thus $|\text{SQ}(\Delta)||\text{AMB}(\Delta)| = |\text{Ker } \Omega_\Delta||\mathbb{W}_\Delta/K_\Delta|$. Using Proposition 4.16, $|\text{SQ}(\Delta)||\mathbb{W}_\Delta/K_\Delta| = |\text{Ker } \Omega_\Delta||\mathbb{W}_\Delta/K_\Delta|$. Thus $|\text{SQ}(\Delta)| = |\text{Ker } \Omega_\Delta|$. Using Lemma 4.14, we see $\text{SQ}(\Delta) = \text{Ker } \Omega_\Delta$.

Historical remark: The proof just given used that $\Omega_\Delta$ is onto to prove that $\text{SQ}(\Delta) = \text{Ker } \Omega_\Delta$. Gauss did things the other way around. He first proved $\text{SQ}(\Delta) = \text{Ker } \Omega_\Delta$, and used it (via the same argument as just given) to prove $\Omega_\Delta$ is onto. The difference is due to the fact that we are using Dirichlet's theorem, which Gauss did not have at his disposal. Using that theorem, it is easy to show $\Omega_\Delta$ is onto (Dirichlet $\Rightarrow$ Corollary 2.20 $\Rightarrow$ Lemma 2.24 $\Rightarrow$ $\Omega_\Delta$ is onto). Our path is shorter, but uses Dirichlet's very difficult theorem. Gauss' path is longer. His very clever proof that $\text{SQ}(\Delta) = \text{Ker } \Omega_\Delta$, can be found in chapter 5 of [F]. That text contains various nice topics, including several proofs of quadratic reciprocity. It also
contains--Chapter 4, section 6--Gauss' lovely theory of reduction of forms of positive nonsquare discriminant, which we choose to not present. Furthermore, it gives an alternate proof of our Corollary 4.6, (not using Proposition 4.4). Finally, the alternate definition of the Kronecker symbol, mentioned in Chapter 2, can be found in that text. (The equivalence of the two definitions follows from an exercise there.)

4.18 Lemma: Let \( \Delta = -23 \). The reader can verify that any Gaussian form of discriminant \(-23\) is properly equivalent to one of \( F = [1, 1, 6] \), \( G = [2, 1, 3] \), or \( H = [2, -1, 3] \). By Corollary 4.6, \(|W_\Delta/K_\Delta| = 1\), and so by Proposition 4.10, there is only one genus. That does not help us at all in answering our earlier question. If \( \text{GCD}(n, -23) = 1 \), and \( \Delta = -23 \) represent \( n > 0 \), all we know is that one of the above three forms represents \( n \).

Concerning \( \text{CL}(\Delta) \), \( G \) represents \( 2 \), but \( F(X, Y) = (X + Y/2)^2 + (23/4)Y^2 \) does not. Thus \( \text{PEC}(F) \) is distinct from \( \text{PEC}(G) \). As \( F \) is the Pell form, \( \text{PEC}(F) \) is the identity of \( \text{CL}(\Delta) \). If \( \text{PEC}(G) \) is its own inverse, then \( |\text{AMB}(\Delta)| \geq 2 \), contradicting Proposition 4.16. Therefore, \( \text{CL}(\Delta) = (\text{PEC}(F), \text{PEC}(G), \text{PEC}(H)) \).

4.19 Corollary: Let \( F \) and \( G \) be Gaussian forms of discriminant \( \Delta \), and let \( a \) be any integer which \( F \) represents, with \( \text{GCD}(a, \Delta) = 1 \). Then \( \text{PEC}(F) \) and \( \text{PEC}(G) \) are in the same genus in \( \text{CL}(\Delta) \) if and only if there is an integer \( w \) with \( \text{GCD}(w, \Delta) = 1 \), such that \( G \) represents \( aw^2 \).

Proof: Suppose such a \( w \) exists. \( \text{PEC}(F) \) is in the inverse image under \( \Omega_\Delta \) of \( a^*K_\Delta \), and \( \text{PEC}(G) \) is in the inverse image of \( (aw^2)^*K_\Delta \). Since \( (w^*)^2 \in K_\Delta \) (Corollary 4.5), we have \( a^*K_\Delta = (aw^2)^*K_\Delta \). Thus those two inverse images are the same, which means \( \text{PEC}(F) \) and \( \text{PEC}(G) \) are in the same genus.

Conversely, suppose \( \text{PEC}(F) \) and \( \text{PEC}(G) \) are in the same genus. Using Corollary 4.17, they are in the same coset of \( \text{Ker} \Omega_\Delta = \text{SQ}(\Delta) \). Thus there is a Gaussian form \( H \) of discriminant \( \Delta \) such that \( \text{PEC}(G) = \text{PEC}(F)(\text{PEC}(H))^2 \). By Lemma
1.15. \( H \) represents an integer \( w \) which is relatively prime to \( \Delta \). By Lemma 3.5, \( \text{PEC}(G) \) represents \( aw^2 \). Thus \( G \) represents \( aw^2 \).

4.20 Exercise: Consider \( (\text{EC}(F) \mid F \) is Gaussian and \( \Delta F = \Delta) \). Suppose \( x \) is the number of \( \text{EC}(F) \) in that set such that \( \text{EC}(F) = \text{PEC}(F) \) and \( y \) is the number of \( \text{EC}(F) \) in that set such that \( \text{EC}(F) \) splits into two proper equivalence classes.

a) Show \( x = 2^s \) for some \( s \).

b) Suppose \( s \geq 1 \). Show \( y = 2^{s-1}r \) for some \( r \).
(Hint: Use that \( \text{AMB}(\Delta) \) is a subgroup of \( \text{CL}(\Delta) \).)

c) Suppose \( s \geq 1 \). Show \( |\text{SQ}(\Delta)| = 1 + r \).

It remains to prove Proposition 4.16. In order to do so, we need to do some ring theory.