Chapter 8
PRIMARY REPRESENTATIONS.

In this chapter we begin the adventure of presenting Dirichlet's formula for the size of the class group $\text{CL}(\Delta)$. It will take five chapters. As always, $\Delta$ is nonsquare discriminant.

8.1 Lemma: Let $C \in \text{CL}(\Delta)$. There is an $F = [a, b, c] \in C$ with $a > 0$.

Proof: Pick any $G = [a, b, c] \in C$. If $\Delta < 0$, $G$ Gaussian shows $a > 0$. Suppose $\Delta > 0$, but $a < 0$. Since $G(r, s) = ar^2 + brs + cs^2 = a(r + (b/2a)s)^2 + (-\Delta/4a)s^2$, we see that for integers $s$ and $r$, with $(-\Delta/4a)s^2 > -a$ and $r$ with $|r + (b/2a)s| < 1$, $G(r, s) > 0$. Let $\text{GCD}(r, s) = d$. Lemma 1.3(i) shows $G$ is properly equivalent to a form $F$ whose leading coefficient is $G(r/d, s/d) > 0$.

Temporary notation: For a short time, we will focus attention on a Gaussian form $F = [a, b, c]$ with $a > 0$. We will also assume $k > 0$ is an integer. (Later, we will also assume $\text{GCD}(k, \Delta) = 1$.)

Definition: Suppose $F(r, s) = k$. If $\text{GCD}(r, s) = 1$, we will say this is a proper representation of $k$ by $F$.

Our immediate goal will be to count the number of proper representations of $k$ by $F$. We will see that if there are any proper representations of $k$ by $F$, then there are exactly $|l_{\Delta,+}|$ of them, with $l_{\Delta,+}$ as in Chapter 5. When $\Delta < 0$, we know $|l_{\Delta,+}|$ is finite, which serves our purpose. When $\Delta > 0$, that set is infinite, and so we will put a further restriction on which proper representations we consider, which will eliminate all but finitely many.
8.2 Lemma: Let \( F(r, s) = k > 0 \) be a proper representation. Then there is exactly one proper substitution \( S \) such that for some integers \( u \) and \( t \), \( [S] = \begin{bmatrix} rs \\ tu \end{bmatrix} \), and such that \( SF = [k, h, m] \) with \( 0 \leq h < 2k \).

Proof: Let \( S' \) be a proper substitution such that \([S']\) has the form \( \begin{bmatrix} r & s \\ t' & u' \end{bmatrix} \). As in Chapter 1, let \( T_n \) be the proper substitution with \( [T_n] = \begin{bmatrix} 10 \\ n \end{bmatrix} \). We claim the set \((S \mid S \text{ is a proper substitution and } [S] \text{ has the form } \begin{bmatrix} rs \\ tu \end{bmatrix} \text{ for some } t \text{ and } u)\) equals the set \((T_n \circ S' \mid n \in \mathbb{Z})\). Suppose \( S \) is in the first set. Being a proper substitution, we have \( ru - st = 1 = ru' - st' \). A well known (and easily proven fact) says there is an integer \( n \) with \( t = t' + nr \) and \( u = u' + ns \). We thus see that \( \begin{bmatrix} rs \\ tu \end{bmatrix} = \begin{bmatrix} 10 \\ n \end{bmatrix} \begin{bmatrix} rs \\ t' & u' \end{bmatrix} \), which is \( [S] = [T_n][S'] \). By Lemma 1.2(a), \( S = T_n \circ S' \), which shows one inclusion of our claim. The other is easy, via that same lemma.

By Lemma 1.2(f), we know that for any \( S \) in the first set, \( SF \) has the form \([k, h, \star]\). We must show exactly one such \( SF \) also has \( 0 \leq h < 2k \). Suppose \( S'F = [k, h', \star] \). Then \( SF = (T_n \circ S')F = T_n[k, h', \star] = [k, h' + 2nk, \star] \). A unique \( n \) gives \( 0 \leq h' + 2nk < 2k \), and we are done.

Let \( F(r, s) = k \) be a proper representation, and let \( S \) be the unique proper substitution given by the preceding lemma. Suppose \( F(r', s') = k \) is another proper representation of \( k \) by \( F \). That lemma tells us there is a unique proper substitution \( S' \) with \([S']\) having the form \( \begin{bmatrix} r's' \\ t' & u' \end{bmatrix} \), and such that \( S'F = [k, h', m'] \) with \( 0 \leq h' < 2k \). It might happen that \( S'F = SF \), even when \((r', s') \neq (r, s)\). We next determine when it does happen.
8.3 Lemma: Let $F(r, s) = k$ be a proper representation of $k$ by $F$. Let $S$ be the unique proper substitution arising from this proper representation, via Lemma 8.2. The following two sets are equal.

a) $(r', s') | F(r', s') = k$ is a proper representation and the unique proper substitution $S'$ arising from it via Lemma 8.2 satisfies $S'F = SF$.

b) $(r, s)A | A \in \text{Aut}^+(F)$.

Proof: Suppose $(r', s')$ is in the set in (a). As $S$ and $S'$ are both proper and $SF = S'F$, we see that $A = [S]^{-1} \circ [S'] \in \text{Aut}^+(F)$.

Let $[S] = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ and $[S'] = \begin{bmatrix} r's' \\ t'u' \end{bmatrix}$. As $(r, s) = (1, 0)[S]$ and $(r', s') = (1, 0)[S']$, we see $(r', s') = (r, s)A$.

Conversely, suppose $A \in \text{Aut}^+(F)$, and let $(r', s') = (r, s)A$. We must show $(r', s')$ is in the set in (a).

Since $(r, s) = (r', s')A^{-1}$, $r$ and $s$ are both linear combinations of $r'$ and $s'$. As we know $\gcd(r, s) = 1$, we must have $\gcd(r', s') = 1$.

We know $A = [T]$, for some proper automorphism $T$ of $F$.

Write $A = [T] = \begin{bmatrix} v & z \\ p & q \end{bmatrix}$. Since $T$ is an automorphism of $F$, we have $F(X, Y) = TF(X, Y) = F(vX + pY, zX + qY) = F((X, Y)A)$. Letting $(X, Y) = (r, s)$, we get $k = F(r, s) = F((r, s)A) = F(r', s')$.

Since we already know $\gcd(r', s') = 1$, we now see that $F(r', s') = k$ is a proper representation. Lemma 8.2 tells us it leads to a unique proper substitution $S'$ such that $[S']$ has top row $(r', s')$, and such that $S'F = [k, h', m']$ with $0 \leq h' < 2k$. We must show $S'F = SF$. Since $TF = F$, it will suffice to show $S' = SoT$.

A two part description of $S'$ (uniquely defining it), was just given in the previous paragraph. We will show $SoT$ satisfies that description. Firstly, since $(1, 0)[S\circ T] = (1, 0)[S][T] = (r, s)[T] = (r, s)A = (r', s')$, we see that $[S\circ T]$ has the top row required of $[S']$. Secondly, we know $(S\circ T)F = S(FT) = SF = [k, h, m]$, with $0 \leq h < 2k$. Thus $S\circ T$ also satisfies the second part of the description of $S'$, and we are done.
Let \( k > 0 \) and let \( F(r, s) = k \) be a proper. Suppose
Lemma 8.2 applied to this proper representation produces the
form \([k, h, m]\). Then Lemma 8.3 tells us how to find all proper
representations of \( k \) by \( F \) which lead to the same form. Namely,
consider all possible \( F(r', s') \) where \((r', s') = (r, s)A\), as \( A \) ranges
over \( \text{Aut}^+(F) \).
We must ask if two different choices for \( A \) can produce
equal values of \((r', s')\)? If \( F \) is primitive, the answer is no, as
we now see. Actually, we will prove a bit more. Recall the
map \( \Gamma_F : Q[\sqrt{\Delta}] \to M_2(Q) \) was defined in Chapter 6.

8.4 Lemma: Let \( F = [a, b, c] \) be a primitive form of
discriminant \( \Delta \), and let \( r \) and \( s \) be numbers with \( F(r, s) \neq 0 \).
As \( A \) varies over all elements in the image of \( \Gamma_F \), \((r, s)A\) takes
on distinct values. In particular, that is true as \( A \) varies over
all elements of \( \text{Aut}^+(F) \).

Proof: If \( A \) is in the image of \( \Gamma_F \), then for some rational \( v \) and
\( w, A = vI + wLF = \begin{bmatrix} v-bw & 2aw \\ -2cw & v+bw \end{bmatrix} \). One easily verifies that
\((r, s)A = (v, w) \begin{bmatrix} r & \quad s \\ -rb-2cs & 2ar+sb \end{bmatrix} \). The last matrix displayed
has determinant \( 2F(r, s) \neq 0 \), and so is nonsingular. Distinct
values of \( A \) arise from distinct values of \((v, w)\), which by the
nonsingularity just mentioned, give distinct values of \((r, s)A\).
The last sentence of the result is true since Proposition
6.10 shows \( \text{Aut}^+(F) \) is part of the image of \( \Gamma_F \).

8.5 Corollary: Let \( F = [a, b, c] \) with \( a > 0 \) be Gaussian, and let
\( k > 0 \). If there is a proper representation \( F(r, s) = k \) which
leads (via Lemma 8.2) to the form \([k, h, m]\), then the number
of such proper representations which lead to \([k, h, m]\) is \( l/\Delta, +, 1 \).

Proof: By Lemmas 8.3 and 8.4, the number we want equals
\( |\text{Aut}^+(F)| = l/\Delta, +, 1 \) (by Proposition 6.10).
If $\Delta < 0$, Exercise 5.4 shows that $|\mathbb{U}_{\Delta+1}|$ is 6 if $\Delta = -3$, 4 if $\Delta = -4$, and 2 if $\Delta < -4$. Thus, when $\Delta < 0$, the count made in the previous corollary leads to a finite number. However, if $\Delta > 0$, then $|\mathbb{U}_{\Delta+1}|$ equals infinity, and so that Corollary counts infinitely many things. That is too many for our purposes. Therefore, we now introduce a way of focusing attention on just one of them, by introducing primary representations (which may or may not also be proper).

Definition: Let $F = [a, b, c]$, with $a > 0$. Suppose $k > 0$ and $F(r, s) = k$. We will call $F(r, s)$ a primary representation of $k$ by $F$ if either

i) $\Delta < 0$ (i.e., when $\Delta < 0$, any representation is primary), or

ii) $\Delta > 0$ and $L^* > 0$ and $1 \leq L/L^* < \tau_\Delta^2$, where $L = 2ar + (b + \sqrt{\Delta})s$, $L^*$ is the conjugate of $L$ in $\mathbb{Q}[\sqrt{\Delta}]$, and $\tau_\Delta$ is as in Corollaries 5.6 and 5.7.

8.6 Remarks: a) If $F(r, s) = k$, then $LL^* = 4ak$, as an easy calculation shows. Since we are working with $k > 0$, and since we want $L^* > 0$ and $1 \leq L/L^*$, so that $L > 0$, we must have $a > 0$.

b) Suppose $\Delta > 0$, and suppose there is a representation of $k$ by $F$. If it is proper, then Corollary 8.5 shows there are infinitely many representations of $k$ by $F$, (since $|\mathbb{U}_{\Delta+1}$ is infinite). In fact, an easy exercise shows the same is also true for non-proper representations.

c) Suppose $\Delta > 0$. We claim there are only finitely many primary representations of $k$ by $F$. For primary representations, we have $1 \leq L/L^* < \tau_\Delta^2$, which when multiplied by $4ak = LL^*$, gives $4ak \leq L^2 < 4ak \tau_\Delta^2$, so that $2\sqrt{ak} \leq L < 2\tau_\Delta \sqrt{ak}$. (Recall $L > 0$, from (a).) Thus there are bounds on the $L$ arising from a primary representation. Now $L = 4ak/L = L - L^* = 2s\sqrt{\Delta}$. Thus $s = (L - 4ak/L)/2\sqrt{\Delta}$. Calculus shows for $L > 0$, $s$ monotonically increases as $L$ does. We easily verify that as $L$ goes from the allowable bounds $2\sqrt{ak}$ to
$2\tau_\Delta \sqrt{ak}$, $s$ goes from 0 to $\frac{\sqrt{ak}}{\sqrt{\Delta}}(\tau_\Delta - 1/\tau_\Delta)$. Therefore, only finitely many choices of integers $s$ can produce a primary representation of $k$ by $F$. The quadratic formula now shows for each possible $s$, there are at most two choices of $r$ satisfying $F(r, s) = k$. This proves our claim.

d) Suppose $\Delta < 0$. Since $a > 0$ and $-\Delta/4a > 0$, and since $F(r, s) = a(r + (b/2a)s)^2 + (-\Delta/4a)s^2$, if $F(r, s) = k$ then $|s| \leq \sqrt{4ak/(-\Delta)}$. Thus only finitely many $s$ are possible, each giving rise to at most two possible $r$. Therefore, there are only finitely many representations of $k$ by $F$, (all of which are primary).

e) By (c) and (d), we see there are only finitely many primary representations of $k$ by $F$.

8.7 Lemma: Let $F = [a, b, c]$ be a Gaussian form of discriminant $\Delta > 0$, with $a > 0$. Let $k > 0$. If there is a proper representation $F(r, s) = k$ which leads (via Lemma 8.2) to the form $[k, h, m]$, then there is exactly one primary proper representation $F(r', s') = k$ which leads to the form $[k, h, m]$.

Proof: For $u$ and $v$ integers, let $L(u, v) = 2au + (b + \sqrt{\Delta})v$. Let $I_F = (L(u, v) \mid u$ and $v$ are integers). Let $R_\Delta$ be as in Chapter 5. In Exercise 8.8 below, we see that if $\alpha \in R_\Delta$ and $L(u, v) \in I_F$, then $\alpha L(u, v) \in I_F$. Specifically, $\alpha L(u, v) = L(u', v')$ where $(u', v') = (u, v)\Gamma_F(\alpha)$ with $\Gamma_F$ as in Chapter 6. (Note that Lemma 6.5(a) shows the entries of $(u', v') = (u, v)\Gamma_F(\alpha)$ are integers.) This multiplication rule says $\alpha L(u, v) = L((u, v)\Gamma_F(\alpha))$.

Now consider the given proper representation $F(r, s) = k$. By Lemma 8.3, we know every proper representation $F(r', s') = k$ which leads to $[k, h, m]$ is obtained by letting $(r', s') = (r, s)A$, over all $A \in \text{Aut}^+(F)$. We will show that exactly one choice of $A$ produces a primary proper representation. By Proposition 6.10, the set of such $A$ is
(\Gamma_F(\alpha) \mid \alpha \text{ is a unit of norm } 1 \text{ in } R_\Delta). \text{ Our multiplication rule shows that } L(r', s') = L((r, s)A) = L((r, s)\Gamma_F(\alpha)) = \alpha L(r, s).

However, as \( \alpha \) is a unit of norm 1, by Corollary 5.7(b), \( \alpha = \pm \tau_\Delta^n \) for some \( n \), and so \( L(r', s') = \pm \tau_\Delta^n L(r, s) \).

Let \( L = L(r, s) \) and \( L' = L(r', s') \). Thus \( L' = \pm \tau_\Delta^n L \) and so using that \( \tau_\Delta^* = 1/\tau_\Delta \) (since \( \tau_\Delta \tau_\Delta^* = N(\tau_\Delta) = 1 \)), we have \( L'^* = \pm \tau_\Delta^{-n} L^* \).

For \( F(r', s') = k \) to be a primary representation, we need \( L'^* > 0 \) and \( 1 \leq L'/L'^* < \tau_\Delta^2 \). However, \( L'/L'^* = (L/L^*)(\tau_\Delta)^{2n} \). Since it is easily seen that \( L \neq 0 \), \( L/L^* \) is defined and nonzero, and so the last equation shows there is a single choice of \( n \) making \( 1 \leq L'/L'^* < \tau_\Delta^2 \) true. For that \( n \), let \( \alpha = \pm \tau_\Delta^n \), where the sign is chosen to make \( L'^* = \pm \tau_\Delta^{-n} L^* < 0 \). That uniquely defined \( \alpha \) gives the unique \( A = \Gamma_F(\alpha) \in \text{Aut}^+(F) \) which we seek.

8.8 Exercises: a) Suppose \( \Delta \) is even, so \( \delta = \sqrt{\Delta}/2 \).

Let \( \alpha = x + y\delta \in R_\Delta \). Note that \( \alpha = x + (y/2)\sqrt{\Delta} \) and \( \Gamma_F(\alpha) = \begin{bmatrix} x - \frac{by}{2} & ay \\ -cy & x + \frac{by}{2} \end{bmatrix} \). With \( L(u, v) \) as in the previous proof, show \( \alpha L(u, v) = L((u, v)\Gamma_F(\alpha)) \). Then show the same is true when \( \Delta \) is odd (and \( \delta = 1/2 + \sqrt{\Delta}/2 \)).

b) Show \( I_F \) (in the previous proof) is an ideal of \( R_\Delta \).

Notation: The letter \( w \) will be used to denote a particular integer, defined as follows: \( w = 1 \) if \( \Delta > 0 \); \( w = 2 \) if \( \Delta < -4 \); \( w = 4 \) if \( \Delta = -4 \); \( w = 6 \) if \( \Delta = -3 \).
8.9 Theorem: Let \( F = [a, b, c] \) be Gaussian with \( a > 0 \). Let \( F(r, s) = k > 0 \) be a proper representation, and suppose it leads (via Lemma 8.2) to the form \([k, h, m]\) with \(0 \leq h < 2k\). Then there are exactly \( w \) primary proper representations \( F(r', s') = k \) which lead to \([k, h, m]\) via Lemma 8.2.

Proof: The case \( \Delta < 0 \) is done by Corollary 8.5 and the discussion following it. The case \( \Delta > 0 \) is by Lemma 8.7.

We have been starting with a proper representation \( F(r, s) = k \), and using Lemma 8.2 to find \([k, h, m]\) (which obviously is properly equivalent to \( F \)). We now reverse things and begin with a form \([k, h, m]\) properly equivalent to \( F \).

8.10 Lemma: Let \( F = [a, b, c] \) be Gaussian with \( a > 0 \), and let \( k > 0 \). Suppose \([k, h, m]\) is a form properly equivalent to \( F \), with \( 0 \leq h < 2k \). Then there are exactly \( w \) primary proper representations \( F(r, s) = k \) which lead (via Lemma 8.2) to \([k, h, m]\).

Proof. Suppose the proper substitution which converts \( F \) to \([k, h, m]\) is given by \( \begin{bmatrix} r & s \\ t & u \end{bmatrix} \). Since Lemma 1.2(f) shows this substitution converts \( F \) to a form whose leading coefficient is \( F(r, s) \), we know \( F(r, s) = k \). Since \( ru - st = 1 \), we know \( \text{GCD}(r, s) = 1 \). Thus \( F(r, s) = k \) is a proper representation which clearly leads to \([k, h, m]\) via Lemma 8.2. The result now follows from Theorem 8.9.

Let \( F = [a, b, c] \) be a Gaussian form with \( a > 0 \), and let \( k > 0 \). Combining Lemma 8.2 and Theorem 8.9, we see that primary proper representations of \( k \) by \( F \) come in families of size \( w \), and each such family leads to a form \([k, h, m]\) properly equivalent to \( F \), with \( 0 \leq h < 2k \). Lemma 8.10 then tells us that conversely, every \([k, h, m]\) which is properly equivalent to \( F \) and has \( 0 \leq h < 2k \) comes from such a family. We have proven the following.
8.11 Corollary: Let \( F = [a, b, c] \) be a Gaussian form with \( a > 0 \). Let \( k > 0 \). Then the number of primary proper representations of \( k \) by \( F \) equals \( w \) times the number of forms \([k, h, m]\) which are properly equivalent to \( F \) and which have \( 0 \leq h < 2k \).

We are now ready to turn to the real goal of this chapter. Consider the class group \( \text{CL}(\Delta) \), and from each proper equivalence class, select a representative. Suppose the resulting list of forms of discriminant \( \Delta \) (one from each proper equivalence class) is \( F_1, F_2, ..., F_{|\text{CL}(\Delta)|} \). Using Lemma 8.1, we will also assume that the leading coefficient of each of these forms is positive.

Notation: Let \( k > 0 \) be an integer with \( \text{GCD}(k, \Delta) = 1 \). Let \( \psi_\Delta(k) \) be the sum over all \( F_i \) (for \( 1 \leq i \leq |\text{CL}(\Delta)| \)) of the number of primary representations of \( k \) by \( F_i \). Let \( \psi_{\Delta\text{prop}}(k) \) be the sum over all \( F_i \) of the number of primary proper representations of \( k \) by \( F_i \).

The goal of this chapter is to prove \( \psi_\Delta(k) = w \sum x_\Delta(r^*) \) where \( x_\Delta \) is the Kronecker symbol defined in Chapter 2, \( r \) runs over all positive divisors of \( k \), and \( w \) is as above. (Note since \( \text{GCD}(k, \Delta) = 1 \), \( \text{GCD}(r, \Delta) = 1 \), and so \( x_\Delta(r^*) \) is defined.) We will begin by calculating \( \psi_{\Delta\text{prop}}(k) \). For that, we need to recall some facts from elementary number theory, which we list in the next lemma (which is a cousin to Lemma 4.3). They are well known, and their proofs can be found in most elementary number theory texts.

8.12 Lemma: a) Let \( n = n_1n_2...n_t \) with the various \( n_t \) pairwise relatively prime. Then the number of solutions of \( x^2 \equiv m \mod n \) with \( 0 \leq x < n \) equals the product (over \( i \in \{1, 2, ..., t\} \)) of the numbers of solutions of \( x^2 \equiv m \mod n_i \) with \( 0 \leq x < n_i \).
b) Let $p$ be an odd prime and let $e \geq 1$. Let $m$ be an integer with $p$ not dividing $m$. Then the number of solutions of $x^2 \equiv m \pmod{p^e}$ with $0 \leq x < p^e$ is 2 if $m$ is a quadratic residue mod $p$ and 0 otherwise.

c) Let $e \geq 3$ and let $m$ be an odd integer. Then the number of solutions of $x^2 \equiv m \pmod{2^e}$, $0 \leq x < 2^e$ is 4 if $m \equiv 1 \pmod{8}$ and 0 otherwise.

8.13 Proposition: Suppose $k > 0$ and $\text{GCD}(k, \Delta) = 1$. Then

$\Psi_{\Delta_{\text{prop}}}(k) = w\Sigma_{\Delta}(f^*)$, where the summation runs over all square-free positive divisors $f$ of $k$.

Proof: Let $F_i$ be one of our class representatives. Then automatically $F_i$ is Gaussian, and by fiat we assumed the leading coefficient of $F_i$ is positive.

By Corollary 8.11, $\Psi_{\Delta_{\text{prop}}}(k)$ equals $w$ times the summation over $1 \leq i \leq |\text{CL}(\Delta)|$ of the number of forms $[k, h, m]$ properly equivalent to $F_i$ and having $0 \leq h < 2k$. Therefore, it will suffice to show that summation equals $\Sigma_{\Delta}(f^*)$, as above. In fact we will show that both of these numbers equal the number of $h$ which satisfy $h^2 \equiv \Delta \pmod{4k}$ and $0 \leq h < 2k$.

We first show the number of forms $[k, h, m]$ properly equivalent to any one of our $F_i$ and having $0 \leq h < 2k$ equals the number of $h$ which satisfy $h^2 \equiv \Delta \pmod{4k}$ and $0 \leq h < 2k$.

First suppose $h^2 \equiv \Delta \pmod{4k}$ with $0 \leq h < 2k$. Then there is a (unique) $m$ with $h^2 - 4km = \Delta$, so that $[k, h, m]$ is a form of discriminant $\Delta$. If any prime $p$ divides both $k$ and $h$, it would also divide $\Delta$, contradicting $\text{GCD}(k, \Delta) = 1$. Thus $\text{GCD}(k, h) = 1$, and so $[k, h, m]$ is Gaussian. Therefore, $[k, h, m]$ must be properly equivalent to one of $F_1, F_2, ..., F_{|\text{CL}(\Delta)|}$. Thus, our solution $h$ produced a unique $m$ and one of our forms $[k, h, m]$. Conversely, let $[k, h, m]$ be such a form. Since this form is properly equivalent to one of our $F_i$, $h^2 - 4km = \Delta$, and so $h^2 \equiv \Delta \pmod{4k}$. This completes half the argument.

It remains to show that the number of $h$ satisfying $h^2 \equiv \Delta \pmod{4k}$ with $0 \leq h < 2k$ equals $\Sigma_{\Delta}(f^*)$, over the positive square-free divisors $f$ of $k$.

We first note that $h^2 \equiv \Delta \pmod{4k}$ with $0 \leq h < 2k$ IFF $(h + 2k)^2 \equiv \Delta \pmod{4k}$ with $2k \leq h + 2k < 4k$. Therefore,
\( h^2 \equiv \Delta \mod 4k \) has twice as many solutions in the interval 
\([0, 4k)\) as in the interval \([0, 2k)\). Therefore, it will suffice to 
show the number of solutions to

\[(*) \quad h^2 \equiv \Delta \mod 4k \text{ with } 0 \leq h < 4k \]

equals \( 2\Sigma x_\Delta(f^*) \).

Let the prime decomposition of \( 4k \) be
\( 4k = 2^d p_1^{d_1} p_2^{d_2} \ldots p_t^{d_t} \). Lemma 8.12(a) shows that to find how 
many solutions \((*)\) has, it will suffice to take the product of 
the number of solutions of each of

\[(**) \quad x^2 \equiv \Delta \mod p^d, \quad 0 \leq x < p^d \]

over \( p^d \in (2^{d_1}, p_1^{d_1}, p_2^{d_2}, \ldots, p_t^{d_t}) \).

First let \( p \) be an odd prime divisor of \( 4k \) (and hence of \( k \),
so that \( p \) does not divide \( \Delta \)). Lemma 8.12(b) says the number 
of solutions of \((**)\) is 2 when \( (\frac{\Delta}{p}) = +1 \) and 0 when \( (\frac{\Delta}{p}) = -1 \).

Thus, the number of solutions is \( 1 + (\frac{\Delta}{p}) = 1 + x_\Delta(p^*) \), the last 
equality directly from our definition of the Kronecker symbol. This holds for \( p \in (p_1, p_2, \ldots, p_t) \).

Now let \( p = 2 \). We need to count the solutions of
\( x^2 \equiv \Delta \mod 2^d, \quad 0 \leq x < 2^d \).

Suppose \( k \) is odd. Then \( d = 2 \), and that number of
solutions is always 2, since \( \Delta \equiv 0 \text{ or } 1 \mod 4 \). In this case, the
number of solutions of \((*)\) is \( 2\Pi(1 + x_\Delta(p_j^*)) \) (over \( j = 1, 2, \ldots, t \)).
However, the Kronecker symbol is a multiplicative group
homomorphism (Proposition 2.17(b)), and so expanding the
above product (and using \( k \) is odd) we get
\( 2\Pi(1 + x_\Delta(p_j^*)) = 2\Sigma x_\Delta(f^*) \), over all positive square-free divisors \( f \) of \( k \), which
completes the proof for odd \( k \).

Now suppose \( k \) is even. Then \( d \geq 3 \). Since GCD(\( k, \Delta \)) = 1,
\( \Delta \) is odd. Since we know \( \Delta \equiv 1 \mod 4, \Delta \equiv 1 \text{ or } 5 \mod 8 \).
By Lemma 2.22, if \( \Delta \equiv 1 \mod 8 \) then \( x_\Delta(2^*) = 1 \), while if
\( \Delta \equiv 5 \mod 8 \) then \( x_\Delta(2^*) = -1 \). Now Lemma 8.12(c) shows that
in either case, the number of solutions to \( x^2 \equiv \Delta \mod 2^d, \)
\( 0 \leq x < 2^d \) equals \( 2(1 + x_\Delta(2^*)) \). Therefore, when \( k \) is even the
number of solutions to \((*)\) is \( 2(1 + x_\Delta(2^*) \Pi(1 + x_\Delta(p_j^*)) \) (over
\( j = 1, 2, \ldots, t \)) = 2\Sigma x_\Delta(f^*) \), over all positive square-free divisors \( f \)
of (the even) \( k \), completing the proof.
We come to the main result of this chapter.

8.14 Theorem: Let \( \gcd(\Delta, k) = 1 \), with \( k > 0 \). Then
\[
\psi_\Delta(k) = w \sum x_\Delta(r^*),
\]
where this sum is over all positive divisors \( r \) of \( k \).

Proof: Let \( F = [a, b, c] \) be a Gaussian form of discriminant \( \Delta \), with \( a > 0 \). Suppose \( r \) and \( s \) are integers with \( \gcd(r, s) = g \). Then it is easily seen that \( F(r, s) = k \) is a representation of \( k \)
IFF \( F(r/g, s/g) = k/g^2 \) is a proper representation of \( k/g^2 \).

Now consider the definition of primary representation.
We assume \( \Delta > 0 \). Using the definition of \( L \) in that definition,
we see \( F(r, s) = k \) leads to \( L = 2ar + (b + \sqrt{\Delta})s \), while \( F(r/g, s/g) = k/g^2 \)
leads to \( L' = 2a(r/g) + (b + \sqrt{\Delta})(s/g) = L/g \). Therefore
\( L'/L^* = L/L^* \), and since \( g > 0 \), \( L'^* > 0 \) IFF \( L' > 0 \). Therefore, we
see that \( F(r, s) = k \) is a primary representation IFF
\( F(r/g, s/g) = k/g^2 \) is a primary proper representation.
However, this is also true when \( \Delta < 0 \) (since then any
representation is primary).

The preceding shows that \( \psi_\Delta(k) = \Sigma \psi_{\Delta_{\text{prop}}}(k/g^2) \) over all
positive \( g \) such that \( g^2|k \). Using Proposition 8.13, we have
\( \psi_\Delta(k) = w \sum (\sum x_\Delta(f^*)) \) (the outside sum over \( g > 0 \), \( g^2|k \); the inside
sum over \( f \) a square-free positive divisor of \( k/g^2 \)). However, if \( f \) and \( g \)
are divisors of \( k \) (and so relatively prime to \( \Delta \), since
the Kronecker symbol is a homomorphism onto \( \{+1, -1\} \)) we see
\( x_\Delta((fg^2)^*) = x_\Delta(f^*) \). Thus we can write \( \psi_\Delta(k) = w \sum (\sum x_\Delta((fg^2)^*)) \)
(over \( g > 0 \), \( g^2|k \), \( f > 0 \) square-free, \( f|k/g^2 \)). Now for \( f \) and \( g \) as
just described, clearly \( r = fg^2 \) is a positive divisor of \( k \).
Conversely, if \( r \) is any positive divisor of \( k \), we can write
\( r = fg^2 \) (uniquely) with \( f > 0 \) square-free, so \( g^2|k \) and \( f|k/g^2 \).
Therefore, \( \psi_\Delta(k) = w \sum x_\Delta(r) \) over all positive divisors \( r \) of \( k \).

We close with an algorithm for finding all representations
of \( k \) by \( F \). The case \( \Delta < 0 \) is easy, since the argument in
Remark 8.6(d) shows a finite search (with a known bound on
the \( |sl| \) in \( F(r, s) = k \)) suffices. We now consider the case \( \Delta > 0 \).
8.15 Algorithm: Let \( F = [a, b, c] \) be a Gaussian form of discriminant \( \Delta > 0 \), with \( a > 0 \). Let \( k > 0 \). If \( F(r, s) = k \) is a representation of \( k \) by \( F \) with \( \text{GCD}(r, s) = g \), then \( F(r/g, s/g) = k/g^2 \) is a proper representation of \( k/g^2 \). Therefore, it will suffice to find an algorithm for finding proper representations, which we then apply to \( k/g^2 \) over all \( g^2 \) which divide \( k \), from whence we get all representations of \( k \).

We note that there is an algorithm for finding all \( A \in \text{Aut}^+(F) \). This follows from the fact that Proposition 6.10 gives an explicit bijection between the set of those \( A \) and the set \( U_{\Delta, +1} = \{ \pm \tau_{\Delta}^n \mid n \in \mathbb{Z} \} \) (Corollary 5.7(b)), and the fact that there is an algorithm for finding \( \tau_{\Delta} \) (5.10).

If \( F(r, s) = k \) is a proper representation, Lemmas 8.3 shows for all \( A \in \text{Aut}^+(F) \), \( F((r, s)A) = k \) is also a proper representation, and Lemma 8.7 shows exactly one of those \( F((r, s)A) = k \) is a primary proper representation. Therefore, if we can find all primary proper representations of \( k \) by \( F \), then multiplying them by all matrices in \( \text{Aut}^+(F) \) will produce all proper representations of \( k \) by \( F \).

We have reduced our problem to finding an algorithm for finding all primary proper representations of \( k \) by \( F \). However, the argument in Remark 8.6(c) shows that can be done by a finite search (with a known limits on the \( s \) in \( F(r, s) = k \)). (We leave to the reader the task of using Lemma 8.1 to extending this algorithm to deal with \( a < 0 \), and then extending it to deal with \( k < 0 \) by replacing \( F \) by \(-F\), and then using Lemma 8.1.)