Chapter 11
FUNDAMENTAL DISCRIMINANTS

Notation: Let $f$ be a square-free integer, not 0 or 1. If $f \equiv 2 \text{ or } 3 \mod 4$, let $\Delta_f = 4f$, and let $\delta_f = \sqrt{f}$. If $f \equiv 1 \mod 4$, let $\Delta_f = f$, and let $\delta_f = 1/2 + \sqrt{f}/2$.

Remark: Concerning the above notation, in either case $\Delta_f$ is a discriminant. The definition of $\delta_f$ in terms of the discriminant $\Delta_f$ is consistent with the definition of $\delta$ in terms of $\Delta$ given at the start of chapter 5.

Definition: A discriminant $\Delta$ of form $\Delta_f$ for some square-free integer $f$ is called a fundamental discriminant.

11.1 Exercises: Let $\Delta$ be a nonsquare discriminant.

a) Show that $\Delta$ is a fundamental discriminant IFF it is impossible to write $\Delta = m^2\Delta'$ with $\Delta'$ a discriminant and $m > 1$.

b) Show that we can uniquely write $\Delta = m^2\Delta'$ with $\Delta'$ a fundamental discriminant. (Write $\Delta = k^2f$ with $f$ square-free. Let $\Delta'$ be either $f$ or $4f$.)

c) Let $\Delta_f$ be a fundamental discriminant. Show $\mathbb{Q}[\sqrt{\Delta}] = \mathbb{Q}[\sqrt{\Delta_f}]$ IFF there is a positive $m$ such that $\Delta = m^2\Delta_f$.

Definition: $\Delta$ is an atomic discriminant if either $\Delta = -4$, or $\Delta = \pm 8$, or $\Delta = p$ with $p$ prime and $p \equiv 1 \mod 4$, or $\Delta = -q$ with $q$ prime and $q \equiv 3 \mod 4$. (Note that these are all fundamental discriminants.)

Lemma 11.2: (a) Any fundamental discriminant $\Delta$ is a product of pairwise relatively prime atomic discriminants.

(b) A product of pairwise relatively prime atomic discriminants is a fundamental discriminant.
Proof: (a) We will do the case that the fundamental discriminant $\Delta$ has the form $\Delta = 4f$ with $f$ square-free and $f \equiv 3 \mod 4$, leaving the other cases to the reader. Now $f$ has the form $f = \pm p_1 p_2 \ldots p_m q_1 q_2 \ldots q_k$ with the $p_i$ being (distinct) primes congruent to 1 mod 4, and the $q_j$ being (distinct) primes congruent to 3 mod 4. First suppose $f > 0$. Since $f \equiv 3 \mod 4$, we must have $k$ odd. Writing $\Delta = 4f = (-4)p_1 p_2 \ldots p_m (-q_1) (-q_2) \ldots (-q_k)$ satisfies the lemma. Now suppose $f < 0$. Then since $-f \equiv 1 \mod 4$, we must have $k$ even. Writing $\Delta = 4f = (-4)(-f) = (-4)p_1 p_2 \ldots p_m (-q_1) (-q_2) \ldots (-q_k)$ satisfies the lemma.

(b) We will do the case that one of the atomic discriminants in this product is $-4$, leaving the other cases to the reader. Thus our product has the form $(-4)p_1 p_2 \ldots p_m (-q_1) (-q_2) \ldots (-q_k)$, where the $p_i$ are (distinct) primes congruent to 1 mod 4 and the $q_j$ are (distinct) primes congruent to 3 mod 4. Suppose $k$ is odd. Then this product equals $4p_1 p_2 \ldots p_m q_1 q_2 \ldots q_k$. On the other hand, if $k$ is even, our product equals $4(-1)p_1 p_2 \ldots p_m q_1 q_2 \ldots q_k$. In either case, the product has the form $4f$ where $f$ is square-free and $f \equiv 3 \mod 4$, showing our product is a fundamental discriminant.

11.3 Lemma: Let $\Delta$ and $\Delta'$ both be discriminants, and let $h$ be an integer. Then (clearly) $\Delta \Delta'$ is a discriminant, and $x_\Delta(h^*) x_\Delta(h^*) = x_\Delta \Delta'(h^*)$.

(We mention that $h^*$ has three different meanings in the above, depending on whether we work modulo $\Delta$, modulo $\Delta'$, or modulo $\Delta \Delta'$.)

Proof: Suppose $\text{GCD}(h, \Delta \Delta') \neq 1$. Then either $\text{GCD}(h, \Delta) \neq 1$ or $\text{GCD}(h, \Delta') \neq 1$, and so by the convention introduced in chapter 9, both sides of the above equation equal 0, and the lemma is true in this case. Now suppose $\text{GCD}(h, \Delta \Delta') = 1$. By Dirichlet’s theorem, there is an odd prime $p$ with
\[ p \equiv h \mod \Delta \Delta'. \] Of course \( p \equiv h \mod \Delta \) and \( p \equiv h \mod \Delta' \). By the definition of the Kronecker symbol (chapter 2), we have
\[ x_\Delta(h^*)x_{\Delta'}(h^*) = \left( \frac{\Delta}{p} \right)\left( \frac{\Delta'}{p} \right) = \left( \frac{\Delta\Delta'}{p} \right) = x_\Delta \Delta'(h^*). \]

11.4 Lemma: Let \( \Delta^\# \) be a discriminant, and let \( m \neq 0 \) be an integer. Let \( \Delta = m^2\Delta^\# \) (which is clearly a discriminant). Let \( k \) be an integer with \( \text{GCD}(k, m) = 1 \). Then \( x_\Delta(k^*) = x_{\Delta^\#}(k^*) \). In particular, that conclusion is true if \( \text{GCD}(k, \Delta) = 1 \).

Proof: If \( \text{GCD}(k, \Delta) = 1 \), then by Dirichlet's theorem, there is an odd prime \( p \) with \( p \equiv k \mod \Delta \) (and also \( \mod \Delta^\# \)). By definition, \( x_\Delta(k^*) = \left( \frac{\Delta}{p} \right) = \left( \frac{m^2\Delta^\#}{p} \right) = \left( \frac{\Delta^\#}{p} \right) = x_{\Delta^\#}(k^*) \). On the other hand, if \( \text{GCD}(k, \Delta) \neq 1 \), then since \( \text{GCD}(k, m) = 1 \), we must have \( \text{GCD}(k, \Delta^\#) \neq 1 \). Thus \( x_\Delta(k^*) = 0 = x_{\Delta^\#}(k^*) \). Since \( \text{GCD}(k, \Delta) = 1 \) implies \( \text{GCD}(k, m) = 1 \), the final sentence is clear.

The proof of our next result proceeds by reducing from the case of arbitrary discriminants to the case of atomic discriminants. The atomic case follows easily from Quadratic Reciprocity. In other words, the next result is essentially an extension of Quadratic Reciprocity.

11.5 Lemma: Let \( \Delta \) and \( \Delta' \) both be discriminants with \( \text{GCD}(\Delta, \Delta') = 1 \). Then
\[ x_\Delta(|\Delta'|^*)x_{\Delta'}(|\Delta|^*) = \begin{cases} -1 & \text{if } \Delta < 0 \text{ and } \Delta' < 0 \\ +1 & \text{otherwise} \end{cases} \]

Proof: We first reduce to the case that \( \Delta \) and \( \Delta' \) are both fundamental discriminants. By Exercise 11.1(b), we see we may write \( \Delta = m^2\Delta^\# \) for some \( m \), with \( \Delta^\# \) a fundamental discriminant. Applying Lemma 11.4 to \( k = |\Delta'| \), we see
\[ x_\Delta(|\Delta'|^*) x_\Delta(|\Delta|^*) = x_\Delta(|\Delta'|^*) x_\Delta(|m^2 \Delta|^*) = x_\Delta(|\Delta'|^*) x_\Delta(|\Delta|^*). \]

Since \( \Delta \) is positive IFF \( \Delta^\# \) is positive, this shows we may replace \( \Delta \) by \( \Delta^\# \), and similarly, we may assume \( \Delta' \) is fundamental.

We next reduce to the case that \( \Delta \) is atomic, and then symmetrically to the case that \( \Delta \) and \( \Delta' \) are both atomic. Suppose the lemma holds whenever \( \Delta \) is atomic. (We will show it holds for \( \Delta \) fundamental.)

By Lemma 11.2(a), we may write our given fundamental \( \Delta \) as a product \( \Delta = \prod \Delta_i \) of atomic discriminants \( \Delta_i \). Using Lemma 11.3, we see

\[ x_\Delta(|\Delta'|^*) x_\Delta(|\Delta|^*) = [\prod x_{\Delta_i}(|\Delta'|^*)] x_\Delta(|\Delta|^*) = [\prod x_{\Delta_i}(|\Delta'|^*)] [\prod x_{\Delta_i}(|\Delta|^*)] = \prod [x_{\Delta_i}(|\Delta'|^*) x_{\Delta_i}(|\Delta|^*)]. \]

Since each \( \Delta_i \) is atomic, by our assumption the lemma holds for each factor in this last product, and an easy exercise shows it therefore holds for \( x_\Delta(|\Delta'|^*) x_\Delta(|\Delta|^*) \). Similarly, we may assume \( \Delta' \) is atomic as well.

We now have reduced to the case that \( \Delta \) and \( \Delta' \) are both atomic. Suppose for instance that \( \Delta = -q \) and \( \Delta' = -r \) with \( q \) and \( r \) both primes congruent to 3 mod 4. Then

\[ x_\Delta(|\Delta'|^*) x_\Delta(|\Delta|^*) = x_{-q}(r^*) x_{-r}(q^*) = (\text{using Proposition 2.17(c)}) \left( \frac{r}{q} \right) \left( \frac{q}{r} \right) = -1, \]

by Quadratic Reciprocity. Since we had \( \Delta < 0 \) and \( \Delta' < 0 \), this shows the lemma holds in this case. Similarly, Quadratic Reciprocity shows the lemma holds whenever \( \Delta \) and \( \Delta' \) are both odd atomic discriminants.

Finally, we consider the case that one of \( \Delta \) or \( \Delta' \) is even. (As \( \text{GCD}(\Delta, \Delta') = 1 \), not both are even). We may assume \( \Delta \) is even and \( \Delta' \) is odd. We have \( \Delta \in \{-4, 8, -8\} \) and \( \Delta' \) is either \( p \) for \( p \) prime with \( p \equiv 1 \) mod 4, or \( -q \) for \( q \) prime with \( q \equiv 3 \) mod 4. In all, that gives six possibilities for the pair \( \Delta, \Delta' \). We will do the case \( \Delta = -8, \Delta' = -q \), (which involves two subcases) leaving the other cases to the reader. Note that since \( \Delta = -8 < 0 \) and \( \Delta' = -q < 0 \), we must show

\[ x_\Delta(|\Delta'|^*) x_\Delta(|\Delta|^*) = -1. \]

We have

\[ (#) \quad x_\Delta(|\Delta'|^*) x_\Delta(|\Delta|^*) = x_{-8}(q^*) x_{-q}(8^*) = x_{-8}(q^*) x_{-q}(2^*). \]
As \( q \equiv 3 \mod 4 \), either \( q \equiv 3 \mod 8 \) or \( q \equiv 7 \mod 8 \).

First suppose \( q \equiv 3 \mod 8 \). Then we have \( x_{-8}(q^*) = x_{-8}(3^*) = \left( \frac{-8}{3} \right) = +1 \). Also, since \( q \equiv 3 \mod 8 \), we have \( \Delta' = -q \equiv 5 \mod 8 \), and so by Lemma 2.22, \( x_{-q}(2) = -1 \). Substituting these into \((\#)\) gives \( x_\Delta(\lvert \Delta' \rvert^*) x_\Delta(\lvert \Delta \rvert^*) = -1 \), as desired. Next, suppose \( q \equiv 7 \mod 8 \). Then \( x_{-8}(q^*) = x_{-8}(7^*) = \left( \frac{-8}{7} \right) = -1 \). Also, \( \Delta' = -q \equiv 1 \mod 8 \), and so Lemma 2.22 shows \( x_{-q}(2^*) = +1 \). In this case, \((\#)\) gives \( x_\Delta(\lvert \Delta' \rvert^*) x_\Delta(\lvert \Delta \rvert^*) = -1 \), as desired. (The other five cases for the pair \( \Delta, \Delta' \) are similar, the two cases involving \( \Delta = -4 \) not requiring subcases.)

11.6 Lemma: Let \( \Delta \) be a discriminant. Then \[ \sum_{r=1}^{\lvert \Delta \rvert-1} x_\Delta(r^*) = 0. \]

Proof: By Proposition 2.17(b), \( x_\Delta \) is an onto homomorphism from \( U_\Delta \), the group of units modulo \( \Delta \), to the multiplicative group \((+1, -1)\). Thus \( x_\Delta(r^*) = +1 \) for exactly half the elements in \( U_\Delta \), and equals \(-1\) for the other half. Also, for \( r^* \) not in \( U_\Delta \), \( x_\Delta(r^*) = 0 \).

We come to the goal of this chapter (which might well be considered an extension of Corollary 10.6).

11.7 Proposition: Let \( \Delta \) be a fundamental discriminant, and let \( n > 0 \) be an integer. Then \[ \sum_{r=0}^{\lvert \Delta \rvert-1} x_\Delta(r^*) e^{2\pi i n r / \lvert \Delta \rvert} = x_\Delta(n^*) \sqrt{\Delta}. \]

(Here, we specify that for \( x < 0 \), by \( \sqrt{-x} \) we mean the root having form \( i \times \) a positive real number, while for \( x > 0 \), \( \sqrt{x} > 0 \) as is standard. Also, we use the earlier convention that if \( \gcd(n, \Delta) \neq 1 \), then \( x_\Delta(n^*) = 0 \).)

Proof: In view of Lemma 11.2, it will clearly suffice to show the following two statements hold.

(A) The proposition holds for any atomic discriminant.
(B) If $\Delta$ and $\Delta'$ are fundamental discriminants which are relatively prime, and for which the proposition is true, then the proposition is true for $\Delta \Delta'$. (Note that Lemma 11.2 and the relative primeness of $\Delta$ and $\Delta'$ show $\Delta \Delta'$ is again a fundamental discriminant.)

Before proving (A), we prove the following claim. If $\Delta$ is a fundamental discriminant and $\text{GCD}(n, \Delta) = 1$, then the proposition holds for $n$ IFF it holds for 1. To see this,

let $T(\Delta, n) = \sum_{r=0}^{\lfloor \Delta \rfloor - 1} x_\Delta(r^*)e^{2\pi i n r / \lfloor \Delta \rfloor}$. Since $x_\Delta(r^*) = x_\Delta((n^2 r)^*)$, (even if $\text{GCD}(r, \Delta) > 1$), we see

$$T(\Delta, n) = \sum_{r=0}^{\lfloor \Delta \rfloor - 1} x_\Delta((n^2 r)^*)e^{2\pi i n r / \lfloor \Delta \rfloor} = x_\Delta(n^*) \sum_{r=0}^{\lfloor \Delta \rfloor - 1} x_\Delta((nr)^*)e^{2\pi i n r / \lfloor \Delta \rfloor} = x_\Delta(n^*)T(\Delta, 1),$$

the last equality since as $r$ runs from 0 to $\lfloor \Delta \rfloor - 1$, $nr$ runs through a complete set of congruence class representatives modulo $\lfloor \Delta \rfloor$. Therefore, $T(\Delta, n) = x_\Delta(n^*)\sqrt{\Delta}$ IFF $T(\Delta, 1) = x_\Delta(1^*)\sqrt{\Delta} = \sqrt{\Delta}$, proving the claim.

We now prove statement (A). Therefore, suppose $\Delta$ is an atomic discriminant. First suppose $\Delta \in \{-4, 8, -8\}$. Of these, we will do $\Delta = -8$, leaving the other two to the reader. Thus suppose $\Delta = -8$. Let $\rho = e^{2\pi i / 8} = (1 + i)/\sqrt{2}$. We have

$$T(\Delta, n) = T(-8, n) = \sum_{r=0}^{7} x_{-8}(r^*)e^{2\pi i n r / 8} =$$

$$x_{-8}(1^*)(\rho^n) + x_{-8}(3^*)(\rho^3 n) + x_{-8}(5^*)(\rho^5 n) + x_{-8}(7^*)(\rho^7 n) =$$

$$\rho^n + \rho^3 n - \rho^5 n - \rho^7 n = (\text{using } \rho^2 = i \rho^n(1 + i n - (-1)n - (-i)n)).$$

If $n = 1$, this equals $\rho(2 + 2i) = ((1 + i)/\sqrt{2})(2 + 2i) = i2\sqrt{2} = x_{-8}(1^*)\sqrt{-8}$. This shows the proposition holds for $n = 1$, and so by the previous claim (and the fact $\Delta = -8$) it also holds for all
odd $n$. On the other hand, if $n = 2m$ is even, the above
expression equals $p^n(1 + (-1)^m - 1^m - (-1)^m) = 0$, and the
proposition holds for even $n$ as well. The case $\Delta = 8$ is similar,
and the case $\Delta = -4$ is easier.

It remains to do the cases $\Delta = p$ with $p$ prime and
$p \equiv 1 \mod 4$, and $\Delta = -q$ with $q$ prime and $q \equiv 3 \mod 4$. We
will do the second of these, the first being similar. Thus
suppose $\Delta = -q$ with $q$ prime and $q \equiv 3 \mod 4$. We have

$$T(\Delta, n) = \sum_{r=0}^{q-1} x_{-q}(r*)e^{2\pi inr/q}.$$ 
Suppose $\text{GCD}(n, -q) > 1$. This means $q \mid n$, and so
$e^{2\pi inr/q} = 1$, showing $T(\Delta, n) = \sum_{r=0}^{q-1} x_{-q}(r*)$. By
Lemma 11.6 and the fact that $x_{\Delta}(0*) = 0$, we see $T(\Delta, n) = 0$.
Since $x_{-q}(n*) = 0$, this proves the proposition for $\text{GCD}(n, -q) > 1$.

As for the case $\text{GCD}(n, -q) = 1$, by the previous claim we
may take $n = 1$. Then

$$T(\Delta, 1) = \sum_{r=0}^{q-1} x_{-q}(r*)e^{2\pi ir/q} = \sum_{r=1}^{q-1} x_{-q}(r*)e^{2\pi ir/q}.$$ 

By Proposition 2.17(c), for $1 \leq r \leq q - 1$, $x_{-q}(r*) = \left(\frac{r}{q}\right)$, and so

using Corollary 10.6, $T(\Delta, 1) = \sum_{r=1}^{q-1} \left(\frac{r}{q}\right)e^{2\pi ir/q} = i\sqrt{q} = \sqrt{-q} = x_{-q}(1*)\sqrt{-q}$. That proves the proposition when $\Delta = -q$, and the
case $\Delta = p$ is similar. This completes the proof of statement (A).

We now prove statement (B). Therefore, suppose $\Delta$ and $\Delta'$
are fundamental discriminants which are relatively prime, and
for which the proposition is true. That is, we are assuming
$T(\Delta, n) = x_{\Delta}(n*)\sqrt{\Delta}$ and $T(\Delta', n) = x_{\Delta'}(n*)\sqrt{\Delta'}$. We must show that
$T(\Delta\Delta', n) = x_{\Delta\Delta'}(n*)\sqrt{\Delta\Delta'}$. We start by proving

$$T(\Delta\Delta', n) = x_{\Delta}(|\Delta'|*)x_{\Delta'}(|\Delta|*)T(\Delta, n)T(\Delta', n).$$

135
We have $T(\Delta, n)T(\Delta', n) =$

$$\left( \sum_{r=0}^{\lfloor \Delta \rfloor - 1} x_{\Delta}(r^*) e^{2\pi i r/|\Delta|} \right) \left( \sum_{s=0}^{\lfloor \Delta' \rfloor - 1} x_{\Delta'}(s^*) e^{2\pi i s/|\Delta'|} \right) = \sum x_{\Delta}(r^*) x_{\Delta'}(s^*) e^{2\pi i (r|\Delta'| + s|\Delta|)/|\Delta \Delta'|},$$

the sum over all pairs $r, s$ with $0 \leq r \leq |\Delta| - 1$ and $0 \leq s \leq |\Delta'| - 1$. Multiplying by $x_{\Delta}(|\Delta'|^*) x_{\Delta'}(|\Delta|^*)$ we get

$$x_{\Delta}(|\Delta'|^*) x_{\Delta'}(|\Delta|^*) T(\Delta, n) T(\Delta', n) =$$

$$\sum x_{\Delta}(r^*) x_{\Delta'}(s^*) e^{2\pi i (r|\Delta'| + s|\Delta|)/|\Delta \Delta'|}.$$

Recall that $0 \leq r \leq |\Delta| - 1$ and $0 \leq s \leq |\Delta'| - 1$. For such a pair $r, s$, let $t = r|\Delta'| + s|\Delta|$. We will rewrite the above in terms of $t$. First, since $r|\Delta'| \equiv r|\Delta'| + s|\Delta| = t \mod |\Delta|$, we have $x_{\Delta}(r^*|\Delta'|^*) = x_{\Delta}(t^*)$, and similarly $x_{\Delta'}(s^*|\Delta|) = x_{\Delta'}(t^*)$. Next note that as $r$ and $s$ vary over their allowable values, Lemma 10.7 shows $t$ varies over a complete set of congruence class representatives mod $|\Delta \Delta'|$. Therefore, we see

$$x_{\Delta}(|\Delta'|^*) x_{\Delta'}(|\Delta|^*) T(\Delta, n) T(\Delta', n) = \sum x_{\Delta}(t^*) x_{\Delta'}(t^*) e^{2\pi i t/|\Delta \Delta'|}$$

$$= \sum x_{\Delta}(t^*) e^{2\pi i t/|\Delta \Delta'|} \text{ (using Lemma 11.3)},$$

where the $t$ in the sum runs over a complete set of congruence class representatives mod $|\Delta \Delta'|$. As any other complete set of congruence class representatives mod $|\Delta \Delta'|$ would serve as well, we may take the sum to be over $0 \leq t \leq |\Delta \Delta'| - 1$. However, this shows the last expression above is just $T(\Delta \Delta', n)$. This proves (%).

Now using (%) and our assumption on $T(\Delta, n)$ and $T(\Delta', n)$, we see $T(\Delta \Delta', n) = x_{\Delta}(|\Delta'|^*) x_{\Delta'}(|\Delta|^*) T(\Delta, n) T(\Delta', n)$

$$= x_{\Delta}(|\Delta'|^*) x_{\Delta'}(|\Delta|^*) x_{\Delta}(n^*) x_{\Delta'}(n^*) \sqrt{\Delta \Delta'} = x_{\Delta}(|\Delta'|^*) x_{\Delta'}(|\Delta|^*) x_{\Delta}(n^*) \sqrt{\Delta \Delta'}.$$
Therefore, it will suffice to show this last expression equals $x_{\Delta\Delta}(n^*)\sqrt{\Delta\Delta'}$. That is, we must show

$$x_\Delta(|\Delta'|^*)x_{\Delta'}(|\Delta|^*)\sqrt{\Delta\sqrt{\Delta'}} = \sqrt{\Delta\Delta'}.$$

Recall we have specified exactly what we mean by the square root of a real number. Using that specification, we see $\sqrt{\Delta\sqrt{\Delta'}} = \pm\sqrt{\Delta\Delta'}$, the minus sign appearing only when $\Delta < 0$ and $\Delta' < 0$. Therefore, Lemma 11.5 completes the argument.

11.8 Exercise: Use $\Delta = 12$ and $n = 1$ to show Proposition 11.7 may not hold when $\Delta$ is not fundamental.