This handout gives (in my opinion) a more compelling reason why binary quadratic forms are relevant to number theory. This has to do with unique factorization in the Gaussian integers \( \mathbb{Z}[i] = \{ x + yi : x, y \in \mathbb{Z} \} \), the similarly defined ring \( \mathbb{Z}[\sqrt{-6}] \) discussed on pages 21–23, etc.

Recall that a subring of \( \mathbb{C} \) is a subset \( S \) of \( \mathbb{C} \) that contains 1, and is closed under addition, subtraction, and multiplication (but not necessarily division). Examples include \( \mathbb{Z} \), \( \mathbb{Z}[i] \), \( \mathbb{R} \), and \( \mathbb{C} \) itself.

First of all, fix an integer \( d < 0 \) which is square free. Let

\[
\theta = \begin{cases} 
\frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4} \\
\sqrt{d} & \text{otherwise ,}
\end{cases} \quad \text{and let } \quad D = \begin{cases} 
d & \text{if } d \equiv 1 \pmod{4} \\
4d & \text{otherwise .}
\end{cases}
\]

Then \( D \equiv 0 \) or 1 \( \pmod{4} \), and it is a fundamental discriminant (see Ex. 3.5.15 on page 163).

Next, let

\[ S = \{ a + b \theta : a, b \in \mathbb{Z} \} . \]

Note that if \( d \equiv 1 \pmod{4} \), then

\[
\theta^2 = \left( \frac{1+\sqrt{d}}{2} \right)^2 = \frac{\sqrt{d}}{2} \cdot \frac{1 + d}{4} = \theta + \frac{d-1}{4} \in S ,
\]

so \( \theta^2 \in S \) for all choices of \( d \) as above. Therefore \( S \) is a subring of \( \mathbb{C} \) for all square-free \( d < 0 \).

Finally, let \( \alpha \) and \( \beta \) be elements of \( S \), and let

\[ M = \{ x \alpha + y \beta : x, y \in \mathbb{Z} \} . \]

Assume that \( \alpha \) and \( \beta \) are chosen such that

(ii). \( \theta \alpha, \theta \beta \in M ; \) and

(i). the determinant of the matrix

\[
\begin{bmatrix} \alpha & \bar{\alpha} \\ \beta & \bar{\beta} \end{bmatrix}
\]

lies in the upper half plane:

\[
\operatorname{Im} \begin{vmatrix} \alpha & \bar{\alpha} \\ \beta & \bar{\beta} \end{vmatrix} > 0 . \quad (*)
\]

Note that (*) implies that \( \alpha \) and \( \beta \) are nonzero, and that neither is a rational multiple of the other.

By construction, \( M \) is closed under addition and subtraction, and by (i) we have \( sm \in M \) for all \( s \in S \) and all \( m \in M \). (Also, since \( M \subseteq S \), \( M \) is closed under multiplication, but this fact will not be needed here.)
Examples of such choices include $\alpha = \theta$, $\beta = 1$ (this gives $M = S$).

Objects $M$ are called modules. (Actually, if you’ve taken Math 113, they are ideals in the ring $S$.)

Given such $\alpha$ and $\beta$, we can define a positive definite binary quadratic form
\[
  f(x, y) = \frac{|x\alpha + y\beta|^2}{\det \begin{bmatrix} t & u \\ v & w \end{bmatrix}},
\]
where $\alpha = t + u\theta$ and $\beta = v + w\theta$ with $t, u, v, w \in \mathbb{Z}$.

The coefficients of $f$ are integers because $f(x, y) \in \mathbb{Z}$ for all $(x, y) \in \mathbb{Z}^2 \setminus \{0\}$.

The latter fact is proved using methods from Math 113, plus other facts. It will not be proved here.

We next show that, up to equivalence, $f$ depends only on the module $M$.

**Proposition 1.** Let $\alpha'$ and $\beta'$ be another pair of elements of $S$ that satisfy the above conditions, and let $g(x, y)$ be the binary quadratic form that they determine. If $\alpha'$ and $\beta'$ determine the same module $M$ as $\alpha$ and $\beta$, then the forms $f$ and $g$ are equivalent.

**Proof.** Since $\alpha', \beta' \in M$, there is a $2 \times 2$ matrix $A$ with entries in $\mathbb{Z}$ such that
\[
  \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = A^t \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.
\]
Similarly, since $\alpha, \beta \in M$, there is a $2 \times 2$ matrix $B$ with entries in $\mathbb{Z}$ such that
\[
  \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = B^t \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix}.
\]
Also, $A$ and $B$ are inverses of each other, so $\det A = \pm 1$.

Since $\begin{bmatrix} \alpha' & \alpha'' \\ \beta' & \beta'' \end{bmatrix} = A^t \begin{bmatrix} \alpha & \alpha'' \\ \beta & \beta'' \end{bmatrix}$ and $\det A \in \mathbb{R}$, we have
\[
  \text{Im} \begin{bmatrix} \alpha' & \alpha'' \\ \beta' & \beta'' \end{bmatrix} = (\det A) \text{Im} \begin{bmatrix} \alpha & \alpha'' \\ \beta & \beta'' \end{bmatrix},
\]
so $\det A = 1$ by (*). In particular, $A \in \Gamma$.

If we write $\alpha' = t' + u'\theta$ and $\beta' = v' + w'\theta$ with $t', u', v', w' \in \mathbb{Z}$, then
\[
  \begin{bmatrix} t' & u' \\ v' & w' \end{bmatrix} = A^t \begin{bmatrix} t & u \\ v & w \end{bmatrix},
\]
so
\[
  \det \begin{bmatrix} t' & u' \\ v' & w' \end{bmatrix} = (\det A) \det \begin{bmatrix} t & u \\ v & w \end{bmatrix} = \det \begin{bmatrix} t & u \\ v & w \end{bmatrix}.
\]

(1)

Also, writing
\[
  A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},
\]
we have
\[
  x\alpha' + y\beta' = x(a_{11}\alpha + a_{21}\beta) + y(a_{12}\alpha + a_{22}\beta) = (a_{11}x + a_{12}y)\alpha + (a_{21}x + a_{22}y)\beta.
\]

(2)

Combining (1) and (2) gives
\[
  g(x, y) = f(a_{11}x + a_{12}y, a_{21}x + a_{22}y).
\]

In other words, $A$ takes $f$ to $g$. $\square$
Proposition 2. All forms as in (**) have discriminant $D$.

Proof. Let the notation be as in (**), write $f(x, y) = ax^2 + bxy + cy^2$, and let
\[ \delta = \left| \det \begin{bmatrix} t & u \\ v & w \end{bmatrix} \right|. \]
Then
\[ \delta a = \delta f(1, 0) = |\alpha|^2, \]
\[ \delta c = \delta f(0, 1) = |\beta|^2, \quad \text{and} \]
\[ \delta b = \delta (f(1, 1) - a - c) = |\alpha + \beta|^2 - |\alpha|^2 - |\beta|^2 = \alpha \beta + \alpha \bar{\beta}. \]

Then
\[ \delta^2(b^2 - 4ac) = (\alpha \beta + \alpha \bar{\beta})^2 - 4|\alpha|^2|\beta|^2 
= \alpha^2 \beta^2 + 2|\alpha|^2|\beta|^2 + \alpha^2 \beta^2 - 4|\alpha|^2|\beta|^2 
= \alpha^2 \beta^2 - 2|\alpha|^2|\beta|^2 + \alpha^2 \beta^2 
= (\alpha \beta - \alpha \bar{\beta})^2 
= \left| \begin{array}{c} \alpha \\ \beta \end{array} \right|^2 \left| \begin{array}{c} \bar{\beta} \\ \bar{\alpha} \end{array} \right|^2. \]

By definition of $t, u, v, w$, we have
\[ \left| \begin{array}{c} \alpha \\ \bar{\alpha} \end{array} \right| = \left| \begin{array}{c} t \\ u \end{array} \right| \left| \begin{array}{c} 1 \\ \bar{\theta} \end{array} \right|; \]
therefore
\[ b^2 - 4ac = \left| \begin{array}{c} \alpha \\ \beta \end{array} \right|^2 = \left| \begin{array}{c} 1 \\ \theta \end{array} \right|^2 = (\theta - \bar{\theta})^2 = \left\{ \begin{array}{ll} d & \text{if } d \equiv 1 \pmod{4} \\ 4d & \text{otherwise} \end{array} \right\} = D. \]

A converse of this result is also true.

Proposition 3. All positive definite binary quadratic forms of discriminant $D$ occur as in (**) for some $\alpha, \beta \in S$.

Proof. Let $f(x, y) = ax^2 + bxy + cy^2$ be a positive definite form of discriminant $D$.

We consider two cases, keeping in mind that $d < 0$.

Case 1: $d \not\equiv 1 \pmod{4}$. Then $D = 4d$ and $\theta = \sqrt{d}$, so
\[ 4af(x, y) = (2ax + by)^2 - Dy^2 = |(2ax + by) + (2y\sqrt{-d})i|^2 
= |x(2a) + y(b + 2\theta)|^2 = |x\alpha + y\beta|^2, \]
where the first step uses (3.3) on page 151, $\alpha = 2a$, and $\beta = b + 2\theta$. Therefore
\[ \left| \begin{array}{c} t \\ u \\ v \\ w \end{array} \right| = \left| \begin{array}{c} 2a \\ 0 \\ b \\ 2 \end{array} \right| = 4a, \]
so (since $a > 0$) $f(x, y)$ equals the form given by (**) with these choices of $\alpha$ and $\beta$.
Proposition 4. Let $f$. the same $x$.

Proof. (a). Clearly $\theta$ is an equivalence relation. This is how it is shown that $\theta$ is well defined on the set of equivalence classes of modules for $S$.

(b). This part is true because

$$\begin{vmatrix} t & u \\ v & w \end{vmatrix} = \begin{vmatrix} 2a & 0 \\ b-1 & 2 \end{vmatrix} = 4a .$$

Next we show that multiplying $\alpha$ and $\beta$ by any nonzero $s \in S$ does not change $f$.

Proposition 4. Let $\alpha, \beta \in S$, $M$, and $f$ be as above, and let $s \in S \setminus \{0\}$. Let $\alpha' = s\alpha$, let $\beta' = s\beta$, and let $M' = \{x\alpha' + y\beta' : x, y \in \mathbb{Z}\}$. Then

(a). The pair $(\alpha', \beta')$ satisfies the above conditions (i) and (ii).

(b). We have $M' = sM$, where $sM = \{sm : m \in M\}$.

(c). Let $f'$ be the binary quadratic form determined by $\alpha'$ and $\beta'$ as in (**). Then $f' = f$.

Proof. (a). Clearly $\alpha', \beta' \in S$.

If $\theta\alpha = x\alpha + y\beta$ with $x, y \in \mathbb{Z}$, then $\theta\alpha' = x(s\alpha) + y(s\beta) = x\alpha' + y\beta' \in M'$ for the same $x$ and $y$. The same is true for $\beta$ as well, so $\alpha'$ and $\beta'$ satisfy condition (i).

Also, $\alpha'$ and $\beta'$ satisfy condition (ii) because

$$\begin{vmatrix} s\alpha & \overline{s}\alpha \\ s\beta & \overline{s}\beta \end{vmatrix} = |s|^2 \begin{vmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{vmatrix} .$$

(b). This part is true because

$M' = \{x\alpha + ys\beta : x, y \in \mathbb{Z}\} = \{s(x\alpha + y\beta) : x, y \in \mathbb{Z}\} = \{sm : m \in M\}$.

(c). Replacing $\alpha$ and $\beta$ with $s\alpha$ and $s\beta$ multiplies both the numerator and denominator of (***) by the same factor $|s|^2$. For the numerator this is easy to see. For the denominator: details are available upon request.

Let $\sim$ be the following relation on the set of modules for $S$. Let $M$ and $M'$ be modules for $S$. We say that $M \sim M'$ if $sM = s'M'$ for some nonzero $s, s' \in S$. It is easy to check that $\sim$ is an equivalence relation.

Then Propositions 1 and 2 say that (***) gives a well-defined map from the set of modules $M$ for $S$ to the set of equivalence classes of positive definite forms of discriminant $D$; Proposition 3 says that this map is surjective, and Proposition 4 says that it is well defined on the set of equivalence classes of modules for $S$.

In more advanced books on number theory, it is proved that the above map is injective, hence bijective. (Therefore, by the example in Exercise 3.5.6, it would not be injective if one allowed $\Gamma$ to contain matrices of determinant $-1$.)

Therefore $H(D)$ also equals the number of equivalence classes of modules for $S$ (where $S$ and $D$ are defined from $d$ as on the first page of this handout).

This is how it is shown that $H(D) = 1$ if and only if $S$ has unique factorization.
We conclude with some examples that discuss automorphs.

**Example.** Let \( d = -3 \). Then \( \theta = (1 + \sqrt{-3})/2 = e^{2\pi i/6} \). It is a primitive sixth root of unity in \( \mathbb{C} \) (meaning that \( \theta^6 = 1 \) but \( \theta^n \neq 1 \) for all \( 1 \leq n < 6 \)).

Let \( \alpha = \theta \) and \( \beta = 1 \); then

\[
f(x, y) = \frac{|x\theta + y|^2}{\det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}} = \left(\frac{x}{2} + y\right) + x \frac{\sqrt{3}}{2}i = \left(\frac{x}{2} + y\right)^2 + 3 \frac{x^2}{4} = x^2 + xy + y^2.
\]

This form has discriminant \(-3\), and has 6 automorphs. The latter is because \( S \) contains six roots of unity. In fact, you can take \( \alpha' = \theta^2 \) and \( \beta' = \theta \). The matrix \( A \) to go from \( \alpha, \beta \) to \( \alpha', \beta' \) is one of the six automorphs, and the other automorphs are powers of \( A \).

You can do the same thing with \( d = -1, \ D = -4, \ \theta = \sqrt{-1} = i \); you will find that \( f(x, y) = x^2 + y^2 \) when you take \( \alpha = i \) and \( \beta = 1 \), and you get four automorphs because \( S = \mathbb{Z}[i] \) has four roots of unity \( i, -1, -i, 1 \).