LECTURE NOTES: QUADRATIC FORMS

BENJAMIN BAKKER

These notes are a basic outline of what we proved in lecture about quadratic forms; Jones & Jones does not cover this material, though it is treated in Davenport and some of the other references given in the syllabus. Our treatment borrows heavily from Davenport and Niven & Zuckerman.

1. Quadratic forms and equivalence

1.1. Quadratic Diophantine equations. We have seen that the techniques we’ve developed can be used to understand the problem of classifying integers \( n \) such that \( n = x^2 + y^2 \) has a solution with \( x, y \in \mathbb{Z} \). We know that this problem is intimately connected with factorization in the Gaussian integers \( \mathbb{Z}[i] \), and this has allowed us to prove that

**Proposition 1.** Suppose \( n \in \mathbb{N} \). \( n = x^2 + y^2 \) has solutions with \( x, y \in \mathbb{Z} \) if and only if every prime \( p \equiv 3 \mod 4 \) appearing in the prime factorization of \( n \) appears to an even power. The number of solutions is \( 4(\tau_1(4)(n) - \tau_4(4)(n)) \), where \( \tau_1(4)(n) \) is the number of divisors \( d \) of \( n \) with \( d \equiv 1 \mod 4 \) and \( \tau_4(4)(n) \) is the number of divisors \( d \) of \( n \) with \( d \equiv 3 \mod 4 \).

There is a similarly nice characterization of \( n \in \mathbb{N} \) such that \( n = x^2 + 2y^2 \) is solvable, and of how many solutions there are, and it is related to the fact that there is unique factorization in \( \mathbb{Z}[\sqrt{-2}] \) as well. The answer is:

**Proposition 2.** Suppose \( n \in \mathbb{N} \). \( n = x^2 + 2y^2 \) has solutions with \( x, y \in \mathbb{Z} \) if and only if every prime \( p \equiv 5, 7 \mod 8 \) appearing in the prime factorization of \( n \) appears to an even power. The number of solutions is \( 2(\tau_1(8)(n) + \tau_3(8)(n) - \tau_5(8)(n) - \tau_7(8)(n)) \), where now \( \tau_k(8)(n) \) is the number of divisors \( d \mid n \) with \( d \equiv k \mod 8 \).

**Exercise 1.** Prove this!

On the other hand, we have seen that unique factorization fails in \( \mathbb{Z}[\sqrt{-5}] \); explicitly, 6 has two factorizations into irreducibles:

\[ 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \]

This is related to the fact that there is no theorem similar to the two above that characterizes the \( n \) for which \( n = x^2 + 5y^2 \) is solvable in terms of certain primes appearing to an even power in the prime factorization of \( n \). Indeed, \( 6 = x^2 + 5y^2 \) has solutions, but neither \( 2 = x^2 + 5y^2 \) nor \( 3 = x^2 + 5y^2 \) does.

Finally, we can also look at the equation \( n = x^2 - dy^2 \) for fixed \( d, n \); it will turn out that this equation has very different behavior from the previous few examples, but can still be understood using the theory of quadratic forms.

1.2. Binary quadratic forms. The notion of a binary quadratic form gives us a common language with which to discuss the natural generalizations to the questions of the last section.

**Definition 1.** A binary quadratic form \( q(x, y) \) is a degree 2 polynomial in two variables with integer coefficients, i.e.

\[ q(x, y) = ax^2 + bxy + cy^2, \text{ with } a, b, c \in \mathbb{Z} \]

An integer \( n \in \mathbb{Z} \) is represented by \( q \) if there are \( x, y \in \mathbb{Z} \) with \( n = q(x, y) \) and properly represented by \( q \) if there are coprime \( x, y \in \mathbb{Z} \) with \( n = q(x, y) \). The number of representations \( R_q(n) \) of \( n \) by \( q \) is the number of solutions to \( n = q(x, y) \), and the number of proper representations \( P_q(n) \) is the number of solutions with \( \gcd(x, y) = 1 \). Note that either of these may be infinite or zero. We will denote by \( N(q) \subset \mathbb{Z} \) the set of integers represented by a quadratic form \( q \).

So for example, \( x^2 + y^2, x^2 + 2y^2, x^2 + 5y^2, x^2 - dy^2 \) are all binary quadratic forms.
Example 1. $q(x, y) = x^2 + y^2$ is the quadratic form we’re most familiar with. From the last section, we know $q$ represents every prime $p \equiv 1 \bmod 4$ eight times, $2$ four times, and primes $p \equiv 3 \bmod 4$ not at all. Using this together with factorization in $\mathbb{Z}[i]$, we have shown that $R_q(n) = 4(\tau_1(n) - \tau_3(n))$ as in the last section. We can also say what integers are properly represented.

Proposition 3. $n \in \mathbb{N}$ is properly represented by $x^2 + y^2$ if and only if every odd prime dividing $n$ is $1 \bmod 4$ and $4|n$.

Proof. This is an immediate consequence of Proposition 1 and Lemma 1.

Lemma 1. Suppose $n \in \mathbb{N}$ is representable by $x^2 + y^2$. $n$ is properly representable if and only if it is neither divisible by $4$ nor a prime $p \equiv 3 \bmod 4$.

Proof. We know solutions to $n = x^2 + y^2$ exactly correspond to $\alpha = x + iy \in \mathbb{Z}[i]$ with $|\alpha|^2 = n$. $4|n$ if and only if one of $(1 + i)^2 = 2i, (1 + i)(1 - i) = 2, (1 - i)^2 = -2i$ divides $\alpha$, which happens if and only if $2|\gcd(x, y)$. Similarly, $p|n$ with $p \equiv 3 \bmod 4$ if and only if $p|\alpha$ since $p$ remains prime in $\mathbb{Z}[i]$, and this happens if and only if $p|\gcd(x, y)$.

We can build a new quadratic form $Q(x, y)$ from an old one $q(x, y)$ by substituting integral combinations of $x, y$ in for the variables in $q(x, y)$. This means we take $x = \alpha x' + \beta y', y = \gamma x' + \delta y'$, with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, and define

$$Q(x', y') := q(x, y) = q(\alpha x' + \beta y', \gamma x' + \delta y')$$

We say that this new form $Q$ is obtained by integral substitution from $q$.

Lemma 2. For $Q$ obtained from integral substitution from $q$, $N(Q) \subset N(q)$.

Proof. Suppose $n$ is represented by $Q$, so $n = Q(x', y')$ for some $x', y' \in \mathbb{Z}$. Setting $x = \alpha x' + \beta y', y = \gamma x' + \delta y'$, then by definition

$$n = Q(x', y') = q(x, y)$$

so $n$ is represented by $q$.

Example 2. Take $q(x, y) = x^2 + y^2$ and $Q(x, y) = q(x + y, y) = x^2 + 2xy + 2y^2$. Then $10 = Q(2, -3), 0 = Q(2, -3) = q(2 + (-3), -3) = q(-1, -3)$.

If we can solve the substitution $x = \alpha x' + \beta y', y = \gamma x' + \delta y'$ for $x', y'$ as integral combinations of $x, y$, then $q$ will be obtained by substitution from $Q$, and therefore applying the lemma again yields $N(q) = N(Q)$. In this case we say that the substitution is invertible. In fact it’s easy to tell when the substitution is invertible using some linear algebra. We can write our substitution as:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

As long as the determinant $\Delta = \alpha \delta - \beta \gamma \neq 0$, then we can solve for $x', y'$ over the rationals:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \frac{1}{\Delta} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

(1)

The problem is that this new substitution may not be integral.

Lemma 3. (1) is an integral substitution if and only if $\Delta = \pm 1$.

Proof. Suppose $d = \gcd(\alpha, \beta, \gamma, \delta)$. If $\Delta$ is an integral substitution, $\Delta$ divides every entry of the matrix, i.e., $\Delta | d$. $d$ divides all four of $\alpha, \beta, \gamma, \delta$, so $d^2 | \Delta$, and thus $d = 1$. But then $\Delta | d$ so $\Delta = \pm 1$. In the converse direction, if $\Delta = \pm 1$ the substitution is clearly integral.

For future convenience, let’s introduce some notation. Given an integral substitution $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and a binary quadratic form $q(x, y)$, define $q^A(x, y) = q(ax + \beta y, \gamma x + \delta y)$ to be the form obtained by the substitution $A$ from $q$. The matrix notation is nice because if we perform a substitution $A$ on $q$ and then a substitution $B$, we’ll get $(q^A)^B = q^{AB}$. 2
In view of the preceding remarks, it makes sense to treat two binary quadratic forms connected by an invertible integral substitution as the same:

**Definition 2.** We say two binary quadratic forms \(q, Q\) are equivalent, written \(q \sim Q\), if \(Q = q^A\) for an invertible integral substitution \(A\) with \(\det A = \pm 1\). We say that \(q, Q\) are properly equivalent if \(Q = q^A\) as before but with \(\det A = 1\).

**Example 3.** Let’s find some quadratic forms (properly) equivalent to \(q(x, y) = x^2 + y^2\).

- In Example 2 we used the substitution \(A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\), which has determinant 1, to get \(Q(x, y) = x^2 + 2xy + 2y^2\), which is properly equivalent to \(q\).
- \(A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\) has determinant 1, and
  \[Q(x, y) = q(2x + y, x + y) = (2x + y)^2 + (x + y)^2 = 5x^2 + 6xy + 2y^2\]
  is properly equivalent to \(q\).
- \(A = \begin{pmatrix} -5 & 2 \\ -7 & 3 \end{pmatrix}\) has determinant \(-1\), and
  \[Q(x, y) = q(-5x + 2y, -7x + 3y) = (-5x + 2y)^2 + (-7x + 3y)^2 = 74x^2 - 62xy + 13y^2\]
  is equivalent to \(q\) (it will turn out it is not properly equivalent).

These are all equivalent to \(q\).

1.3. Consequences of equivalence. As far as what integers are represented and how frequently, two equivalent quadratic forms are the same:

**Proposition 4.** If \(q \sim Q\), then for all \(n \in \mathbb{N}\), \(R_q(n) = R_Q(n)\) and \(P_q(n) = P_Q(n)\).

**Proof.** Suppose \(Q = q^A\) is obtained by the invertible integral substitution \(A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\) from \(q\). Then for every solution \((x', y')\) of \(n = Q(x', y')\) we obtain a solution \(n = q(\alpha x' + \beta y', \gamma x' + \delta y')\). Every solution \((x, y)\) of \(n = q(x, y)\) can be obtained in this way, by setting
\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = A^{-1} \begin{pmatrix} x \\ y \end{pmatrix}
\]
and furthermore, two solutions \((x', y'), (x'', y'')\) give the same \((x, y)\) if and only if
\[
A \begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x'' \\ y'' \end{pmatrix}
\]
if and only if \((x', y') = (x'', y'')\), by multiplying by \(A^{-1}\); this shows that \(R_q(n) = R_Q(n)\) for all \(n \in \mathbb{N}\). To show that \(P_q(n) = P_Q(n)\), we need only show that proper solutions correspond to proper solutions, i.e.

**Lemma 4.** Suppose \(A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\) is an invertible integral substitution, and \(x', y' \in \mathbb{Z}\) with \(\gcd(x', y') = 1\). Set \(\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x' \\ y' \end{pmatrix}\). Then \(\gcd(x, y) = 1\) as well.

**Proof.** Since \(\gcd(x', y') = 1\), there are \(u', v' \in \mathbb{Z}\) with \(u'x' + v'y' = 1\). In terms of matrices,
\[
\begin{pmatrix} u' & v' \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = 1
\]
We just need to find \(u, v \in \mathbb{Z}\) doing the same for \(\begin{pmatrix} x \\ y \end{pmatrix}\) to conclude \(\gcd(x, y) = 1\). Take:
\[
\begin{pmatrix} u & v \end{pmatrix} = \begin{pmatrix} u' & v' \end{pmatrix} A^{-1}
\]
so that
\[
\begin{pmatrix} u & v \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \left(\begin{pmatrix} u' & v' \end{pmatrix} A^{-1}\right) \left(\begin{pmatrix} x' \\ y' \end{pmatrix}\right) = \begin{pmatrix} u' & v' \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = 1
\]
\[\square\]
Corollary 1. If \( q \sim Q \), then \( N(q) = N(Q) \).

as we stated above.

1.4. A digression on matrices. Though slightly tangential, it is nonetheless sometimes important that for any quadratic form \( q(x, y) = ax^2 + bxy + cy^2 \) I can write:

\[
2q(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}^T \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}
\]

We will denote this matrix by \( M(2q) = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \). This provides a nice way to think about what happens when I perform the substitution \( A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \) since

\[
2q^A(x, y) = \begin{pmatrix} x \\ y \end{pmatrix}^T \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} (A^T M(2q) A) \begin{pmatrix} x \\ y \end{pmatrix}
\]

so \( M(2q^A) = A^T M(2q) A \).

2. The Discriminant

2.1. The discriminant as an invariant. In general it’s a subtle problem figuring out when two binary quadratic forms are equivalent. One extremely important tool for addressing this question is the discriminant, which you may recognize from our treatment of the quadratic formula:

Definition 3. Let \( q(x, y) = ax^2 + bxy + cy^2 \) be a binary quadratic form. The discriminant of \( q \) is \( d(q) = b^2 - 4ac \).

Example 4. The quadratic forms \( x^2 + y^2, x^2 + 2y^2, x^2 + 5y^2 \) have discriminants \(-4, -8, -20\).

Remark 1. Note that for a binary quadratic form \( q(x, y) = ax^2 + bxy + cy^2 \), the discriminant \( d(q) \) is 1 or 0 mod 4.

The most important property of the discriminant is:

Proposition 5. Let \( q \sim Q \) be equivalent binary quadratic forms. Then \( d(q) = d(Q) \).

First some examples:

Example 5. It therefore follows immediately that the three forms from Example 4 are not equivalent.

Example 6. The discriminants of the three forms from Example 3 that are all equivalent to \( q(x, y) = x^2 + y^2 \) should be equal to \( d(q) = -4 \). Indeed,

- \( Q(x, y) = x^2 + 2xy + 2y^2, d(Q) = (2)^2 - 4(1)(2) = 4 - 8 = -4 \).
- \( Q(x, y) = 5x^2 + 6xy + 2y^2, d(Q) = (6)^2 - 4(5)(2) = 36 - 40 = -4 \).
- \( Q(x, y) = 74x^2 - 62xy + 13y^2, d(Q) = (-62)^2 - 4(74)(13) = 3844 - 3848 = -4 \).

Proof of Proposition 5. This is by direct substitution. Suppose \( Q = q^A \) for \( A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \) and \( q(x, y) = ax^2 + bxy + cy^2 \). Then

\[
Q(x, y) = q(\alpha x + \beta y, \gamma x + \delta y)
= a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2
= (aa^2 + b\alpha \gamma + c\gamma^2)x^2 + (2a\alpha \beta + b(\alpha \delta + \beta \gamma) + 2c\gamma \delta)xy + (a \beta^2 + b\beta \delta + c \delta^2)y^2
\]

Now amazingly if we look at the coefficients of \( a^2, c^2, ab, bc \) in

\[
d(Q) = (2a\alpha \beta + b(\alpha \delta + \beta \gamma) + 2c \gamma \delta)^2 - 4(aa^2 + b\alpha \gamma + c \gamma^2)(a \beta^2 + b \beta \delta + c \delta^2)
\]
they’re all zero, while the coefficient of $b^2$ is
\[(\alpha \delta + \beta \gamma)^2 - 4\alpha \beta \gamma \delta = (\alpha \delta - \beta \gamma)^2\]
and the coefficient of $ac$ is
\[8\alpha \beta \gamma \delta - 4(\alpha^2 \delta^2 + \beta^2 \gamma^2) = -4(\alpha \delta - \beta \gamma)^2\]
so that
\[d(Q) = (\alpha \delta - \beta \gamma)^2(b^2 - 4ac) = (\det A)^2d(q)\]
and since $\det A = \pm 1$, $d(Q) = d(q)$. □

**Remark 2.** Let’s note here for the record that the formula (2) for performing a substitution $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ on a form $q$ takes the form:
\[q^A(x, y) = q(\alpha, \gamma)x^2 + Bxy + q(\beta, \delta)y^2\]
In particular this means that the integers that are properly representable by $q$ are exactly the integers that appear as the coefficient of $x^2$ in equivalent forms (the representation is proper since $\alpha \delta - \beta \gamma = \gcd(\alpha, \gamma) = 1$).

**Remark 3.** Continuing the digression in Section 1.4, note that $d(q) = -\det M(2q)$. This provides us with a much cleaner proof. From before,
\[M(2Q) = A^T M(2q) A\]
It’s now clear from the multiplicativity of $\det$ that
\[d(Q) = -\det M(2Q) = (\det A)^2(-\det M(2q)) = (\det A)^2d(q)\]

**2.2. The discriminant and positivity.** The discriminant $d(q)$ encodes a surprising amount of information about the binary quadratic form $q$. One property it can detect is the definiteness of $q$:

**Definition 4.** A binary quadratic form $q$ is positive if $q(x, y) > 0$ for all $x, y \in \mathbb{Z}$ not both zero. It is negative if $-q$ is positive; $q$ is definite if it is either positive or negative. If $q$ takes positive and negative values, then $q$ is indefinite.

**Example 7.** The forms $x^2 + y^2, x^2 + 2y^2, x^2 + 5y^2$ are all positive definite, and this is one reason why their behavior is so similar. The form $x^2 - dy^2$ is indefinite for $d > 0$ and is phenomenologically very different from these three, as alluded to before.

We can completely characterize the definiteness of quadratic forms using the discriminant:

**Proposition 6.** Let $q(x, y) = ax^2 + bxy + cy^2$ be a binary form. $q$ is positive definite if and only if $d(q) < 0$ and both $a > 0$ and $c > 0$.

Note that if $d(q) < 0$, then since $0 \leq b^2 < 4ac$, $a > 0$ if and only if $c > 0$.

**Proof.** Suppose $q$ is positive definite. Then $q(1, 0) = a > 0$ and $q(0, 1) = c > 0$. Note that we can write
\[q(x, y) = \frac{1}{4a}((2ax + by)^2 + (4ac - b^2)y^2) = \frac{1}{4a}((2ax + by)^2 - d(q)y^2)\]
Thus $q(-b, 2a) = -d(q)a > 0$, which implies that $d(q) < 0$.

Conversely, it’s clear from (3) that if $d(q) < 0$ and $a > 0$, then $q(x, y)$ is positive. □

One nice property of positive forms is that they represent any integer only finitely many times:

**Proposition 7.** Let $q$ be a positive binary quadratic form. Then for any $n \in \mathbb{N}$, $R_q(n)$ is finite (though it may still be 0).

**Proof.** Suppose $n \in \mathbb{N}$ given and set $d = d(q)$; we’ll show that there are finitely many $(x, y)$ with $q(x, y) \leq n$.

From (3), if $q(x, y) \leq n$, then
\[dy^2 \leq 4an\]
and therefore
\[-2\sqrt{\frac{an}{-d}} \leq y \leq 2\sqrt{\frac{an}{-d}}\]
Thus, for all \((x, y)\) with \(q(x, y) \leq n\), \(y\) must be one of only finitely many values. However any such a \((x, y)\) with a fixed value \(y\) satisfies, by (3),
\[
(2ax + by)^2 \leq 4an + dy^2
\]
and there are only finitely many values of \(x\) that for which this holds for any given \(y\). It then follows that the number of \((x, y)\) for which \(q(x, y) \leq n\) is finite.

**Remark 4.** The proof means there exists a simple algorithm for finding the smallest integer represented by a positive form \(q\). \(a = q(1, 0)\) is represented, so just take \(n = a - 1\) in the proof and check all values of \((x, y)\) allowed by the two inequalities in the proof.

### 3. Classification of Positive Forms

#### 3.1. Reduced forms

We now come to the problem of determining how many different quadratic forms there are of a given discriminant, up to equivalence. This is in general a subtle problem, but by the end of the next section we will be able to show, for example:

**Example 8.** Every positive form of discriminant \(-4\) is equivalent to \(x^2 + y^2\), and similarly every positive form of discriminant \(-8\) is equivalent to \(x^2 + 2y^2\). This is related to the fact that these two forms behave so similarly, cf. Section 1.1. On the other hand, every positive form of discriminant \(-20\) is equivalent to *either* \(x^2 + 5y^2\) or \(2x^2 + 2xy + 3y^2\), and these two forms are *not* equivalent. This is why \(x^2 + 5y^2\) behaves slightly differently from the other two.

We start with a definition:

**Definition 5.** A positive binary quadratic form \(q(x, y) = ax^2 + bxy + cy^2\) is a *reduced form* if \(0 \leq b \leq a \leq c\).

**Example 9.** Clearly our favorite three positive forms, \(x^2 + y^2, x^2 + 2y^2, x^2 + 5y^2\), are all reduced forms. \(2x^2 + 2xy + 3y^2\) is also reduced; note that it’s positive since it’s discriminant is \(-20\) and the coefficient of \(x^2\) is positive.

Reduced forms are interesting because it’s easy to tell when they’re equivalent:

**Proposition 8.** Two reduced forms are equivalent if and only if they are equal.

**Proof.** Suppose \(q(x, y) = ax^2 + bxy + cy^2\) and \(Q(x, y) = Ax^2 + Bxy + Cy^2\) are reduced forms; we may assume that \(a \geq A\). Certainly if \(q = Q\) then they are equivalent, via the identity substitution.

Now suppose that \(Q\) is obtained by the invertible integral substitution \(A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\) from \(q\). From (2),
\[
Q(x, y) = (a\alpha^2 + b\alpha\gamma + c\gamma^2)x^2 + (2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta)xy + (a\beta^2 + b\beta\delta + c\delta^2)y^2
\]

**Claim.** \(1 \geq |\alpha\gamma|\).

**Proof.** Since \(0 \leq b \leq a \leq c\),

\[
A = a\alpha^2 + b\alpha\gamma + c\gamma^2 \\
\geq a\alpha^2 + c\gamma^2 - b|\alpha\gamma| \\
\geq a(\alpha^2 + \gamma^2) - b|\alpha\gamma| \\
\geq a|\alpha\gamma|
\]

where to get to the last line we used \(\alpha^2 + \gamma^2 \geq 2|\alpha\gamma|\). We assumed \(a \geq A > 0\) (by positivity), so it must be the case that \(1 \geq |\alpha\gamma|\).

To conclude \(a = A\), we just need to show \(a \leq A\): if \(1 = |\alpha\gamma|\), then this is (5). Otherwise, one of \(\alpha\) or \(\gamma\) is 0 (they can’t both be zero), and either \(A = a\alpha^2\) or \(A = c\gamma^2\); in both cases \(A \geq a\).

So now \(a = A\). Note that if we show that either \(b = B\) or \(c = C\), then \(q = Q\), since we know \(d(q) = b^2 - 4ac = d(Q) = B^2 - 4AC\) and the facts that \(a = A > 0\) and \(b, B \geq 0\) allow us to conclude that both \(b = B\) and \(c = C\) given only one of these equalities.

There are several possibilities:

**Case (a):** \(c = C\). By the above, \(q = Q\).
Case (b): \( c < C \). By swapping \( q, Q \) (which we can do because we’ve proved that \( a = A \)) we can assume \( c > C \) instead.

Case (c): \( c > C \). If \( 1 = |\alpha\gamma| \), then since \( \gamma^2 = \alpha^2 = 1 \), (4) gives \( A = a = 2a - b \) which is a contradiction, since \( b \leq a \). Thus, either \( \alpha = 0 \) or \( \gamma = 0 \) (they can’t both be zero). In the former case, \( A = c\gamma^2 \geq c \) contradicts \( c > C \geq A \); in the latter, \( A = a\alpha^2 \) implies \( \alpha = \pm 1 \) and since \( \alpha\delta - \beta\gamma = 1 \), \( \delta = \pm 1 \) as well. It then follows that \( B = 2a\alpha\beta \pm b \).

Thus, at this point the only case left to analyze is when: \( a = A \), \( c > C \), \( B = 2a\alpha\beta \pm b \), \( a = \pm 1 = \delta \) and \( \gamma = 0 \). Note that \( 0 \leq b \leq a \) and \( 0 \leq B \leq A = a \) imply that (**) \( -a \leq B - b \leq a \) and (**) \( 0 \leq b + B \leq 2a \).

Case (i): \( B = 2a\alpha\beta + b \). From (**), \( -a \leq 2a\alpha\beta \leq a \), which is impossible unless \( \beta = 0 \), so \( B = b \) and therefore \( q = Q \), a contradiction since \( c > C \).

Case (ii): \( B = 2a\alpha\beta - b \). From (**), \( 0 \leq 2a\alpha\beta \leq 2a \), so either \( \beta = 0 \), in which case \( b = B \) and thus \( q = Q \), or \( \alpha\beta = 1 \), and \( B = 2a - b \geq a = A \) implies \( B = A \), but then \( b = 2a - A = B \) and thus \( q = Q \), a contradiction.

Example 10. \( x^2 + 5y^2 \) and \( 2x^2 + 2xy + 3y^2 \) are both reduced forms of discriminant \(-20\) and they are therefore inequivalent.

The previous example shows how easy it is to find (provably) inequivalent positive forms of the same discriminant: any two distinct reduced forms of the same discriminant will do. Further we can computationally classify reduced forms of the same discriminant:

**Proposition 9.** There are finitely many reduced forms of a given discriminant.

Proof. Suppose we fix a discriminant \( d < 0 \). For \( q(x, y) = ax^2 + bxy + cy^2 \) to be reduced, we need \( 0 \leq b \leq a \leq c \), but then

\[
-d = 4ac - b^2 \geq 4ac - ac = 3a^2
\]

so there are only finitely many values of \( a > 0 \) for which \( q(x, y) \) is reduced, and since \( 0 \leq b \leq a \), there are only finitely many possibilities for the pair \( a, b \). Finally, given \( a, b, c \) at most one \( c \) will exist such that \( d = b^2 - 4ac \) since \( a > 0 \).

Moreover, the proof provides an effective algorithm for finding them. For example,

**Lemma 5.**

(a) The only reduced form of discriminant \(-4\) is \( x^2 + y^2 \).
(b) The only reduced form of discriminant \(-8\) is \( x^2 + 2y^2 \).
(c) The only reduced forms of discriminant \(-20\) are \( x^2 + 5y^2, 2x^2 + 2xy + 3y^2 \).

Proof. (a) Suppose \( q(x, y) = ax^2 + bxy + cy^2 \) is a reduced form of discriminant \( b^2 - 4ac = -4 \), so \( 0 \leq b \leq a \leq c \). From the proof, we know \( 0 < 3a^2 \leq -d = 4 \). This implies \( a = 1 \), and \( b = 0, 1 \). If \( (a, b) = (1, 0) \), then \( b^2 - 4ac = -4 \) implies \( c = 1 \), and \( q(x, y) = x^2 + y^2 \). If \( (a, b) = (1, 1) \), \( b^2 - 4ac = -4 \) has no solutions.

(b) This is very similar to the above case.
(c) Suppose \( q(x, y) = ax^2 + bxy + cy^2 \) is a reduced form with \( b^2 - 4ac = -20 \), so \( 0 \leq b \leq a \leq c \). Again, \( 0 < 3a^2 \leq 20 \), so \( a = 1 \) or \( 2 \). Thus, \( (a, b) = (1, 0), (1, 1), (2, 0), (2, 1) \), or \( (2, 2) \). Trying to solve \( b^2 - 4ac = -20 \) in these cases rules out all but the first and the fifth, where \( (a, b, c) = (1, 0, 5), (2, 2, 3) \). □

3.2. Classification of positive forms. Classifying reduced forms is not very useful if it doesn’t tell us about the classification of all positive forms up to equivalence. The last fundamental result about reduced forms is that every positive form is equivalent to a reduced one (in fact a unique one in view of the above), so that listing reduced forms of a given discriminant is the same as listing positive forms of a given discriminant up to equivalence.

**Proposition 10.** Every positive form is equivalent to a reduced form.

This, for example, enables us to immediately conclude from Lemma 5 that

**Proposition 11.**

(a) Every positive form of discriminant \(-4\) is equivalent to \( x^2 + y^2 \).
(b) Every positive form of discriminant \(-8\) is equivalent to \(x^2 + 2y^2\).

(c) Every positive form of discriminant \(-20\) is equivalent to one of \(x^2 + 5y^2, 2x^2 + 2xy + 3y^2\).

Proof of Proposition 10. Suppose given a positive form \(Q(x, y) = Ax^2 + Bxy + Cy^2\), and let \(a\) be the smallest integer represented by it (of course, \(a > 0\)). Thus, for some \(\alpha, \gamma \in \mathbb{Z}\), \(a = Q(\alpha, \gamma)\). \((\alpha, \gamma)\) must in fact be a proper representation, i.e. \(\gcd(\alpha, \gamma) = 1\), for if the gcd were \(d\), then \(\frac{a}{d} = Q\left(\frac{\alpha}{d}, \frac{\gamma}{d}\right)\) would be a smaller integer. Thus there exist integers \(\beta, \delta \in \mathbb{Z}\) with \(a\delta - \beta\gamma = 1\).

Consider now the substitution \(A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\), which we know has \(\det A = 1\). Suppose we make this substitution into \(Q\), so we get a form
\[
q(x, y) = Q(\alpha x + \beta y, \gamma x + \delta y) = ax^2 + bxy + c^2
\]
Notice the fact that the coefficient of \(x^2\) being \(a\) is not a typo; by (2), the coefficient of \(x^2\) in the substituted form is exactly \(Q(\alpha, \gamma)\). \(q\) may or may not be reduced, but we know it’s positive and we know \(a\) is the smallest integer it represents. Consider making a further substitution \(\begin{pmatrix} 1 & -k \\ 0 & \gamma \end{pmatrix}\), so we get
\[
q'(x, y) = q(x - ky, y) = a(x - ky)^2 + b(x - ky)y + cy^2 = ax^2 + (b - 2ak)xy + (ak^2 - bk + c)y^2
\]
Taking \(k\) to be as close as possible to \(\frac{b}{2a}\), then
\[
\frac{1}{2} \leq \frac{b}{2a} - k \leq \frac{1}{2} \Rightarrow -a \leq b - 2ak \leq a \Rightarrow |b - 2ak| \leq a
\]
So if we call \(q'(x, y) = ax^2 + b'xy + c'y^2\), then we’ve arranged \(|b'| \leq a\) and \(a\) is the smallest integer represented. Now \(q'(x, y)\) automatically represents \(c'\), so \(a \leq c'\). If \(b' \geq 0\), we’re done. If \(b' \leq 0\), by performing the final substitution \(\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\), we only change the sign of \(b'\) and leave \(a, c'\) the same, so we get a reduced form. \(\square\)

3.3. Properly reduced forms. As far as understanding representation of integers by forms, we need only understand forms up to equivalence and the theory of reduced forms is adequate. Unfortunately, to discuss the class group later on, we need to understand forms up to proper equivalence; this is done using properly reduced forms:

Definition 6. A positive binary quadratic from \(q(x, y) = ax^2 + bxy + cy^2\) is said to be properly reduced if either: \(-a < b \leq a < c\) or \(0 \leq b \leq a = c\).

Thus, if \(q(x, y)\) is properly reduced, either it is reduced or \(q(-x, y) = ax^2 - bxy + cy^2\). Conversely, if we have a list of reduced forms of a particular discriminant, we can get a list of properly reduced forms by adding forms with the sign of \(b\) changed (if \(a \neq c\)).

Example 11. The unique reduced forms of discriminant \(-4, -8\), i.e. \(x^2 + y^2, x^2 + 2y^2\) are also the unique properly reduced forms.

We know there are 2 reduced forms of discriminant \(-20\):
\[
x^2 + 5y^2 \\
2x^2 + 2xy + 3y^2
\]
and thus there are also 2 properly reduced forms:
\[
x^2 + 5y^2 \\
2x^2 + 2xy + 3y^2
\]
Since \(2x^2 - 2xy + 3y^2\) is NOT properly reduced.

As a final example, consider positive forms of discriminant \(-31\). Using the inequality \(3a^2 \leq -d = 31\), we know \(a = 1, 2, 3\). Trying the various possibilities gives 2 reduced forms:
\[
x^2 + xy + 8y^2 \\
2x^2 + xy + 4y^2
\]
and thus there are three properly reduced forms:
\[ x^2 + xy + 8y^2 \]
\[ 2x^2 + xy + 4y^2 \]
\[ 2x^2 - xy + 4y^2 \]

From the results of the previous two sections, we can easily derive:

**Corollary 2.**

(a) Two properly reduced forms are properly equivalent if and only if they are equal.

(b) There are finitely many properly reduced forms of a given discriminant.

(c) Every positive form is properly equivalent to a properly reduced form.

A binary quadratic form \( q(x, y) = ax^2 + bxy + cy^2 \) is called primitive if \( \gcd(a, b, c) = 1 \). The number of primitive properly reduced forms of a given discriminant \( d < 0 \)—which is equal to the number of proper equivalence classes of primitive positive forms of discriminant \( d \)—is called the class number \( C(d) \) and is a very important and delicate invariant. We’ll try to touch on some of the properties of \( C(d) \).

**Example 12.** \( C(-4) = 1, C(-8) = 1, C(-20) = 2, C(-31) = 3. \)

4. Representing integers by quadratic forms.

4.1. Proper Representation. We now return to the question of determining when \( n = q(x, y) \) is solvable. It turns out it’s basically trivial to classify which \( n \) are represented by some quadratic form of a given discriminant; the difficult part is to determine which reduced form represents it.

**Proposition 12.** Suppose given \( d \in \mathbb{Z} \). \( n \in \mathbb{N} \) is properly representable by a binary quadratic form of discriminant \( d \) if and only if \( d \) is a square mod \( 4n \), i.e. \( z^2 \equiv d \mod 4n \) is solvable.

**Proof.** Suppose \( n \) is properly represented by \( q(x, y) = ax^2 + bxy + cy^2 \) with \( d = d(q) \), so for some \( \alpha, \beta \in \mathbb{Z} \) with \( \gcd(\alpha, \gamma) = 1 \), \( n = q(\alpha, \gamma) \). Since \( \alpha, \gamma \) are coprime, there are \( \beta, \delta \in \mathbb{Z} \) with \( a\delta - \beta\gamma = 1 \), and performing the substitution \( \begin{pmatrix} \alpha \\ \gamma \\ \beta \\ \delta \end{pmatrix} \) on \( q \), we know (e.g. from the proof of Proposition 10) we get a form

\[ q'(x, y) = nx^2 + b'xy + c'y^2 \]

for some \( b', c' \in \mathbb{Z} \). We must have \( d = d(Q) = b'^2 - 4nc' \), and therefore \( z = b' \) solves \( z^2 \equiv d \mod 4n \).

Conversely, suppose \( z^2 \equiv d \mod 4n \) for some \( z \in \mathbb{Z} \). Then \( d = z^2 - 4nm \) for some integer \( m \in \mathbb{Z} \), and \( n \) is representable by \( q(x, y) = nx^2 + zxy + my^2 \). \( \Box \)

**Example 13.** Let’s consider \( q(x, y) = x^2 + y^2 \), which up to proper equivalence is the only positive form of discriminant \(-4\). If \( n \) is odd, \(-4\) is a square mod \( 4n \) if and only if it is a square mod \( 4 \) and mod \( n \), which happens if and only if every prime dividing \( n \) is 1 mod 4. If \( n \) is even, \( n = 2^e m \) with \( m \) odd, then since \(-4\) is not a square mod \( 16 \), \(-4\) is a square mod \( n \) if and only if \( e = 1 \) and every odd prime dividing \( n \) is 1 mod 4. We thus recover Proposition 3.

**Corollary 3.** Let \( d \in \mathbb{Z} \). An odd prime \( p \) coprime to \( d \) is properly representable by a quadratic form of discriminant \( d \) if and only if \( \left( \frac{d}{p} \right) = 1 \).

**Proof.** \( d \) is a square mod \( 4p \) if and only if it is a square mod \( 4 \) and mod \( p \). By Remark 1, \( d \) is always a square mod \( 4 \), so \( p \) is properly representable if and only if \( d \) is a square mod \( p \). \( \Box \)

Combining this with our classification from the previous sections, we have

**Proposition 13.** Suppose \( d \in \mathbb{Z} \), \( d < 0 \), and \( C(d) = 1 \). Take any \( n \in \mathbb{N} \). The following are equivalent:

(a) \( n \) is properly representable by some positive binary quadratic form of discriminant \( d \).

(b) \( n \) is properly representable by every positive binary quadratic form of discriminant \( d \).

(c) \( d \) is a square mod \( 4n \).

Unfortunately, if \( C(d) \neq 1 \), then it’s easy to tell when \( n \in \mathbb{N} \) is representable by a positive form of discriminant \( d \), but it may be hard to tell which properly reduced form represents it. For example, take \( d = -20 \). \( 2x^2 + 2xy + 3y^2 \) represents 2, 3 but not 6, while \( x^2 + 5y^2 \) represents 6 but not 2 or 3.
Definition 7. We say that $d \in \mathbb{Z}$ has class number one if

- $d > 0$ and all primitive binary quadratic forms of discriminant $d$ are properly equivalent.
- $d < 0$ and all primitive positive binary quadratic forms of discriminant $d$ are properly equivalent, i.e. $C(d) = 1$.

4.2. Number of proper representations. We are going to understand the number of representations of a given $n \in \mathbb{Z}$ by a form $q$, in two steps:

$$\left\{ \text{proper solutions to } n = q(x, y) \right\} \overset{\varphi}{\rightarrow} \left\{ \text{invertible integral substitutions } A \text{ with } \det A = 1 \text{ such that } q^A = nx^2 + bxy + cy^2, 0 \leq b < 2n \right\} \overset{\chi}{\rightarrow} \left\{ q' = nx^2 + bxy + cy^2 \approx q \right\}$$

We can understand the rightmost set using the theory developed, and by getting a handle on the two maps $\varphi, \chi$, we can relate proper solutions to this set. Let's first define and analyze $\varphi$:

Given a proper solution $n = q(\alpha, \gamma)$, we know there are $\beta, \delta$ such that $\alpha \delta - \beta \gamma = 1$, so $A$ is a proper substitution, and $q^A = nx^2 + bxy + cy^2$. However, there are many such $\beta, \delta$; in fact, the general solution is $\beta' = \beta + k\alpha$, $\delta' = \delta + k\gamma$, for any $k \in \mathbb{Z}$, and the associated transformation is

$$A' = \left( \begin{array}{cc} \alpha & \beta + k\alpha \\ \gamma & \delta + k\gamma \end{array} \right) = \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right) \left( \begin{array}{cc} 1 & k \\ 0 & 1 \end{array} \right)$$

Applying $A'$ to $q$ is the same as applying $A$ and then $\left( \begin{array}{cc} 1 & k \\ 0 & 1 \end{array} \right)$, so $q^{A'} = nx^2 + (b + 2kn)xy + c'y^2$, and there is a unique value of $k$ such that $0 \leq b + 2kn < 2n$. We take the image of $(\alpha, \gamma)$ under $\varphi$ to be $A'$ for this value of $k$. We now clearly have:

Lemma 6. $\varphi$ is a bijection.

Proof. We need to show that every $A$ with $q^A = nx^2 + bxy + cy^2$ and $0 \leq b < 2n$ comes in this way from one and only one proper solution to $n = q(x, y)$. The first part is easy: if $A = \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right)$ is such a substitution, then $n = q(\alpha, \gamma)$ is a proper solution that goes to $A$ under $\varphi$. The other part is even easier: we can recover the proper solution $(\alpha, \gamma)$ as the first column of the image $A = \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right)$ of $(\alpha, \gamma)$, so if two proper solutions $(\alpha, \gamma), (\alpha', \gamma')$ have the same image under $\varphi$, then we must have $(\alpha, \gamma) = (\alpha', \gamma')$. \qed

$\chi$ is much easier to define: given $A$ such that $q^A = nx^2 + bxy + y^2$ with $0 \leq b < 2n$, the image of $A$ under $\chi$ is simply $q^A$. $\chi$ it turns out is not bijective, but is easy to understand in terms of proper automorphisms of $q$:

Definition 8. Let $q$ be a binary quadratic form. An integral substitution $A$ with $\det A = \pm 1$ such that $q^A = q$ is an automorphism of $q$; if $\det A = 1$ it is a proper automorphism. The number of proper automorphisms of $q$ is called $w(q)$.

Example 14. The trivial substitution $A = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)$ is a proper automorphism of any $q$, as is $A = \left( \begin{array}{cc} -1 & 0 \\ 0 & -1 \end{array} \right)$.

$q(x, y) = x^2 + y^2$ has two additional proper automorphisms, $\left( \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right)$ and $\left( \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right)$. It also has the automorphism $\left( \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right)$, but this isn’t proper. $q(x, y) = x^2 + xy + y^2$ has $w(d) = 6$:

$$\left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right), \left( \begin{array}{cc} -1 & 0 \\ 0 & -1 \end{array} \right), \left( \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right), \left( \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right), \left( \begin{array}{cc} 0 & -1 \\ 1 & 1 \end{array} \right), \left( \begin{array}{cc} 0 & 1 \\ -1 & -1 \end{array} \right),$$

We have

Lemma 7. Let $q$ be a positive binary quadratic form. If $d(q) \neq -3, -4$, then $w(q) = 2$. $w(x^2 + y^2) = 4$ and $w(x^2 + xy + y^2) = 6$.

Proof. Left as an exercise. \qed

10
Now:

**Lemma 8.** \( \chi \) is surjective. \( \psi(A) = \psi(A') \) if and only if \( A'A^{-1} \) is an automorphism of \( q \).

**Proof.** First surjectivity: if \( q' = nx^2 + bxy + xy^2 \approx q \), then there is some \( A \) for which \( q' = qA \), and then \( A \) goes to \( q' \) under \( \psi \). Further, if \( qA = qA' \), then performing the inverse substitution associated with \( A \), \( q = (qA')A^{-1} = qA'A^{-1} \), so \( A'A^{-1} \) is an automorphism. Finally, if \( B \) is an automorphism, then for any \( A \) in the middle set above, \( A' = BA \) is still in the set since \( qA' = qBA = qA \). Thus, \( \psi(A) = \psi(A') \) if and only if \( A'A^{-1} \) is an automorphism of \( q \). □

We can immediately conclude

**Corollary 4.** Let \( q \) be a binary quadratic form such that \( w(q) \) is finite. Then for any \( n \in \mathbb{Z} \),

\[
\frac{1}{w(q)} P_q(n) = \# \left\{ q' = nx^2 + bxy + cy^2 \approx q \mid \text{with } 0 \leq b < 2n \right\}
\]

There are two ways to proceed from here. If \( C(d) = 1 \), any form \( q' = nx^2 + bxy + cy^2 \) with \( 0 \leq b < 2n \) will be properly equivalent to \( q \), and the number of such forms is equal to the number of solutions to \( z^2 \equiv d \mod 4n \) with \( 0 \leq z < 2n \): given any solution, \( b^2 = d + 4nc \) for some \( c \in \mathbb{Z} \), and \( nx^2 + bxy + cy^2 \) is the corresponding form. Thus

**Proposition 14.** For \( d < 0 \), suppose \( C(d) = 1 \), and let \( q \) be any positive binary quadratic form of discriminant \( d \). Then for any \( n \in \mathbb{N} \),

\[
\frac{1}{w(q)} P_q(n) = \# \{ \text{solutions to } z^2 \equiv d \mod 4n \text{ with } 0 \leq z < 2n \}
\]

We can do even better if \( d = 4m \). Then for any \( n \in \mathbb{N} \), \( z^2 \equiv d \mod 4n \) has as many integer solutions with \( 0 \leq z < 2n \) as \( z^2 \equiv m \mod n \) does with \( 0 \leq z < n \), after dividing out by 2. But the latter number is just the number of \( m \) solutions to \( z^2 \equiv m \mod n \), and thus we conclude

**Corollary 5.** For \( d = 4m < 0 \), with \( C(d) = 1 \), let \( q \) be any positive form of discriminant \( d \). Then for any \( n \in \mathbb{N} \), \( \frac{1}{w(q)} P_q(n) \) is a multiplicative function whose value at an odd prime power \( p \) is

\[
\frac{1}{w(q)} P_q(p^e) = \begin{cases} 
0 & \text{if } \left( \frac{d}{p} \right) = -1 \\
2 & \text{if } \left( \frac{d}{p} \right) = 1
\end{cases}
\]

In general the evaluation at 2-powers is less clean but just as doable. So for example, we recover the sum-of-squares story:

**Example 15.** Consider \( q(x, y) = x^2 + y^2 \). For \( p \equiv 1 \mod 4 \), \( \frac{1}{w(q)} P_q(p^e) = 2 \) and if \( p \equiv 3 \mod 4 \), \( \frac{1}{w(q)} P_q(p^e) = 0 \). If \( n = 2^e \), then \( z^2 \equiv -1 \mod n \) has 1,0 solutions depending on whether \( e < 2, e \geq 2 \), and thus we recover our previous results.

If \( C(d) \neq 1 \), for any solution of \( z^2 \equiv d \mod 4n \) with \( 0 \leq z < 2n \), we can still construct the form \( nx^2 + zxy + cy^2 \), but we are no longer guaranteed it will be properly equivalent to a given \( q \). But it will be equivalent to some proper reduced form, and so we can say

**Proposition 15.** For \( d < 0 \), enumerate the properly reduced forms \( q_1, \ldots, q_e \) of discriminant \( d \) with \( c = C(d) \). Then for any \( n \in \mathbb{N} \),

\[
\sum_i \frac{1}{w(q_i)} P_{q_i}(n) = \# \{ \text{solutions to } z^2 \equiv d \mod 4n \text{ with } 0 \leq z < 2n \}
\]

and again we get as a Corollary

**Corollary 6.** For \( d = 4m < 0 \), enumerate the properly reduced forms \( q_1, \ldots, q_e \) of discriminant \( d \) with \( c = C(d) \). Then for any \( n \in \mathbb{N} \), \( \sum_i \frac{1}{w(q_i)} P_{q_i}(n) \) is a multiplicative function whose value at an odd prime power \( p \) is

\[
\frac{1}{w(q)} P_q(p^e) = \begin{cases} 
0 & \text{if } \left( \frac{d}{p} \right) = -1 \\
2 & \text{if } \left( \frac{d}{p} \right) = 1
\end{cases}
\]
Corollary 7. In the same setup as the proposition, let \( p \) be an odd prime not dividing \( d \) with \( \left( \frac{d}{p} \right) = 1 \). Then \( p \) is either represented by two distinct properly reduced forms of discriminant \( d \) twice each and no others, or four times by one properly reduced form of discriminant \( d \) and no others.

Proof. By the previous Corollary, \( \sum_i P_{q_i}(n) = 4 \). Because \( w(q_i) \)

Example 16. Each of these possibilities occur.

- \( d = -44 \). You can show there are 4 properly reduced forms,

\[
x^2 + 11y^2, 2x^2 + 2xy + 6y^2, 3x^2 + 2xy + 4y^2, 3x^2 - 2xy + 4y^2
\]

Take \( p = 3 \), which is coprime to \( d \) and \( d \equiv 1 \mod 3 \) is a square. The third and fourth forms each represent 3 twice (both at \((\pm 1, 0)\)), and no others do.

- \( d = -36 \). There are 3 properly reduced forms,

\[
x^2 + 9y^2, 2x^2 + 2xy + 5y^2, 3x^2 + 3y^2
\]

Take \( p = 5 \), which is coprime to \( d \) and \( d \equiv -1 \mod 5 \) is a square. The second form represents 5 four times, at \((0, \pm 1)\) and \((-1, 1), (1, -1)\).

Example 17. Here’s a final example, involving \( d = -20 \); there are two properly reduced forms,

\[
x^2 + 5y^2, 2x^2 + 2xy + 3y^2
\]

First consider \( n = 2 \). \( z^2 \equiv -20 \mod 8 \), \( 0 \leq z < 4 \) has one solution, \( z = 2 \). Thus, only one of these two forms can represent 2, and it must do so twice. Indeed, the second represents it at \((\pm 1, 0)\). Similarly, taking \( n = 3 \), by the Corollary either both forms represent 3 twice or one represents it four times; its the latter that happens, since the second form represents 3 at \((0, \pm 1), (-1, 1), (1, -1)\). Finally, taking \( n = 6 \), \( z^2 \equiv -20 \mod 24 \) can be split up into \( z^2 \equiv 4 \mod 8 \) and \( z^2 \equiv 1 \mod 3 \), which have two solutions with \( 0 \leq z < 12 \). The first form represents 6 four times, at \((\pm 1, \pm 1)\).

5. Composition of forms

5.1. The Pell form. Given \( d \in \mathbb{Z} \), there is a particularly important binary quadratic form of discriminant \( d \). Not that from the homework we know the only possible discriminants are \( d \equiv 0, 1 \mod 4 \).

Definition 9. Given \( d \in \mathbb{Z} \), the Pell form \( p_d \) of discriminant \( d \) is the form

- \( p_d(x, y) = x^2 - my^2 \) if \( d = 4m \).
- \( p_d(x, y) = x^2 + xy - my^2 = 1 \) if \( d = 4m + 1 \).

The Pell conic of discriminant \( d \) is the equation \( p_d(x, y) = 1 \).

The amazing property of the Pell form is that the set of integers \( N(p_d) \) that \( p_d \) represents is closed under multiplication, since we can write:

\[
(x^2 - my^2)(u^2 - mv^2) = (xu + myv)^2 - m(xv + myu)^2
\]

and therefore, for any two solutions \( n = p_d(x, y) \) and \( n' = p_d(u, v) \), then

\[
nn' = p_d(xu + myv, xv + myu)
\]

This also works for the Pell form of discriminant \( d \equiv 1 \mod 4 \):

\[
(x^2 + xy - my^2)(u^2 + uv - mv^2) = (xu + myv)^2 + (xu + myv)(vx + uy + vy) - m(vx + uy + vy)^2
\]
5.2. **Gauss composition.** Let $Q(d)$ be the set of binary quadratic forms of discriminant $d$, and $\overline{Q}(d)$ the set of proper equivalence classes of binary quadratic forms of discriminant $d$. We’re interested in how the representation of integers by forms of discriminant $d$ interacts with multiplication. For instance, taking $d = -20$, why is it the case that $2, 3$ are only represented (up to equivalence) by $2x^2 + 2xy + 3y^2$, but their product $6$ is representable only (up to equivalence) by $x^2 + 5y^2$? We can answer this question by understanding, given two quadratic forms $q, q'$ of discriminant $d$, when we can reorganize a product into a quadratic form $Q$ of discriminant $d$

$$q(x, y)q'(u, v) = Q(X, Y)$$

where $X, Y$ are now going to be expressions quadratic in $x, y, u, v$. We define:

**Definition 10.** Given $q, q' \in Q(d)$, a **Gauss composition** is a $Q \in Q(d)$ such that

$$Q(\alpha_1 xu + \beta_1 xv + \gamma_1 yu + \delta_1 yv, \alpha_2 xu + \beta_2 xv + \gamma_2 yu + \delta_2 yv) = q(x, y)q'(uv)$$

for some $\alpha_1, \beta_1, \gamma_1, \delta_1 \in \mathbb{Z}$. We also require $\alpha_1\beta_2 - \alpha_2\beta_1 = q(1, 0)$ and $\alpha_1\gamma_2 - \alpha_2\gamma_1 = q'(1, 0)$.

The point of this definition is that a Gauss composition $Q$ represents products of all integers represented by $q, q'$, and the substitution defining $Q$ tells us exactly how it is represented.

**Example 18.** $Q(x, y) = x^2 + 5y^2$ is a Gauss composition of $q(x, y) = q'(x, y) = 2x^2 + 2xy + 3y^2$. Indeed, you can check that

$$q(x, y)q'(u, v) = (2x^2 + 2xy + 3y^2)(2u^2 + 2uv + 3v^2) = Q(2xu + xv + yu + yv)$$

There’s a systematic way of forming Gauss compositions due to Dirichlet, using the fact that:

**Lemma 9.** Given $a, b, c, a', b', c' \in \mathbb{Z}$ with $d = b^2 - 4ac = b'^2 - 4a'c'$, set $e = \gcd(a, a', \frac{b+b'}{2})$. There is a unique integer $B \mod \frac{4aa'}{e^2}$ solving the system:

$$B \equiv b \mod \frac{2a}{e}$$

$$B \equiv b' \mod \frac{2a'}{e}$$

$$B^2 \equiv d \mod \frac{4aa'}{e^2}$$

**Proposition 16.** Given $q(x, y) = ax^2 + bxy + cy^2, q(x, y) = a'x^2 + b'xy + c'y^2$ binary quadratic forms of discriminant $d$, and $B$ as in the lemma, a Gauss composition of $q$ and $q'$ is given by:

$$Q(x, y) = \frac{aa'}{e^2}x^2 + Bxy + \frac{e^2(B^2 - d)}{4aa'}y^2$$

**Example 19.** Take $q(x, y) = q'(x, y) = 2x^2 + 2xy + 3y^2$ again. $B = 2$ satisfies the lemma, so a Gauss composition is

$$Q(x, y) = x^2 + 2xy + 6y^2$$

Note this is not the same as the composition obtained in the previous example, but it is equivalent to it:

$$x^2 + 2xy + 6y^2 = (x + y)^2 + 5y^2$$

This leads us to

**Proposition 17.** Given $q, q' \in Q(d)$, any two Gauss compositions are equivalent.

**Corollary 8.** In particular, any Gauss composition of $q, q' \in Q(d)$ is also in $Q(d)$. 

13