1. Prove that for any odd prime, \( p \),
\[
\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \begin{cases} 
0 \pmod{2} & \text{if } p \equiv \pm 1 \pmod{8} \\
1 \pmod{2} & \text{if } p \equiv \pm 3 \pmod{8}.
\end{cases}
\]

Since \( p \equiv m \pmod{8} \) means \( p = 8k + m \) for some \( k \in \mathbb{Z} \) we will work with that. Here we consider \( m = \pm 1 \) or \( \pm 3 \). These are the only possible residues for \( p \pmod{8} \) since \( p \) is odd. Observe that
\[
\left\lfloor \frac{p}{4} \right\rfloor = \left\lfloor 2 + \frac{m}{4} \right\rfloor \equiv \begin{cases} 
0 \pmod{2} & \text{if } m = 1, 3 \\
1 \pmod{2} & \text{if } m = -1, -3.
\end{cases}
\]

Also observe that
\[
\frac{p-1}{2} = 4k + \frac{m-1}{2} \equiv \begin{cases} 
0 \pmod{2} & \text{if } m = 1, -3 \\
1 \pmod{2} & \text{if } m = -1, 3.
\end{cases}
\]

So
\[
\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \begin{cases} 
0 - 0 \equiv 0 \pmod{2} & \text{if } m = 1 \\
1 - 1 \equiv 0 \pmod{2} & \text{if } m = -1 \\
1 - 0 \equiv 1 \pmod{2} & \text{if } m = 3 \\
0 - 1 \equiv 1 \pmod{2} & \text{if } m = -3.
\end{cases}
\]

which is what we were trying to show.

2. Let \( n = 2^k m \) where \( k, m \in \mathbb{N} \) and \( m \) is odd. Show that \( a \) is a quadratic residue \((\pmod {n})\) iff \( a \) is a quadratic residue \((\pmod {2^k})\) and \( a \) is a quadratic residue \((\pmod {m})\).

If \( m \) is odd then \((2^k, m) = 1\). We see that \( a \) is a quadratic residue \((\pmod {n})\) iff there exists \( x \in \mathbb{Z} \) such that \( n|(a - x^2) \) which happens iff \( \exists x \in \mathbb{Z} \) such that \( 2^k, m|(a - x^2) \) which happens iff \( \exists x_1, x_2 \in \mathbb{Z} \) such that
\[
\begin{align*}
x_1^2 &\equiv a \pmod{2^k} \\
x_2^2 &\equiv a \pmod{m}
\end{align*}
\]
since a simultaneous solution \( x \in \mathbb{Z} \) produces \( x_1, x_2 \) and conversely \( x_1 \) and \( x_2 \) can produce \( x \) by the Chinese Remainder Theorem. This last iff gave that \( a \) is a quadratic residue \((\pmod {2^k})\) and \((\pmod {m})\) and we’re done.

3. Prove that
\[
f(x, y) = x^2 + y^2, \quad g(x, y) = x^2 - y^2, \quad h(x, y) = 2xy
\]
are all inequivalent quadratic forms.

We see \( \text{disc}(f) = -4 \) and \( \text{disc}(g) = \text{disc}(h) = 4 \) so \( f \) is not equivalent to \( g \) or \( h \) since equivalent forms have the same discriminant. Furthermore, we see \( h(x, y) \) is always even whereas \( g(1, 0) = 1 \). Since equivalent forms have the same set of values, we have that \( g \) is not equivalent to \( h \).

4. Prove that for 
\[
    f(x, y) = x^2 + xy + 5y^2 \quad \text{and} \quad g(x, y) = 7x^2 + 17xy + 11y^2,
\]
that \( f \sim g \) and find \( U \in SL_2(\mathbb{Z}) \) such that \( f \circ U = g \).

We observe that \( x^2 + xy + 5y^2 \) is in reduced form, so it should suffice to show that \( g \) reduced is equal to \( g \). Let \( G_0 \) be the matrix of \( g(x, y) \):
\[
    G_0 = \begin{bmatrix}
        7 & 17 \\
        \frac{17}{2} & 11
    \end{bmatrix}.
\]

We recall the “Step 1” and “Step 2” method to reduce a quadratic form from lecture. First we see that \( 7 < 11 \) so we can skip Step 1 for now, so we go to Step 2. We want to find \( n \in \mathbb{Z} \) such that \( 17 + 2(7)n \in (-7, 7] \). We see that \( n = -1 \) does this so we take
\[
    G_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 7 & \frac{17}{2} \\ \frac{17}{2} & 11 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \frac{7}{2} & \frac{3}{2} \\ \frac{3}{2} & 1 \end{bmatrix}
\]
to be our new matrix. But now we see that \( 7 > 1 \) so we do Step 1 to get
\[
    G_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 7 & \frac{3}{2} \\ \frac{3}{2} & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -\frac{3}{2} \\ -\frac{3}{2} & 7 \end{bmatrix}.
\]

But now \( -3 > 1 \) so we do Step 2 again, now we want to find \( n \in \mathbb{Z} \) such that \( -3 + 2(1)n \in (-1, 1] \). We see \( n = 2 \) does this so we get
\[
    G_3 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & -\frac{3}{2} \\ \frac{3}{2} & 5 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 5 \end{bmatrix}
\]
and we see \( G_3 \) is the matrix for \( f(x, y) \), so \( f \sim g \). Now
\[
    G_3 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} G_0 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 3 & -2 \end{bmatrix} G_0 \begin{bmatrix} 1 & 3 \\ -1 & -2 \end{bmatrix}.
\]

So we have \( f = g \circ \begin{bmatrix} 1 & 3 \\ -1 & -2 \end{bmatrix} \), which means that \( g = f \circ \begin{bmatrix} -2 & -3 \\ 1 & 1 \end{bmatrix} \).

5. a) Compute \( h(-19) \).
b) Show that for
\[ f(x, y) = 5x^2 + 21xy + 23y^2, \quad g(x, y) = 209x^2 + 247xy + 73y^2, \quad h(x, y) = 17x^2 + 61xy + 55y^2, \]
that \( f \sim g \sim h \).

a) Recall that \( h(d) \) is the number of equivalence classes of positive definite quadratic forms with discriminant \( d \). Since every quadratic form is equivalent to a reduced form and all reduced forms have coefficients that satisfy \( a, |b|, c \leq \frac{1}{3}|d| \), to compute \( h(-19) \) we just need to find all \( a, b, c \in \mathbb{Z} \) such that \( a, |b|, c \leq 6 \) and \( b^2 - 4ac = -19 \) with \(-a < b \leq a < c \) or \( 0 \leq b \leq a = c \).

Since \( |b| \leq 6 \) our options for \( b^2 \) are 0, 1, 4, 9, 16, 25, 36. Since \( b^2 + 19 = 4ac \) we require \( b^2 + 19 \) to be divisible by 4 so our only options are \( b^2 + 19 = 20, 28, 44 \). Respectively those each give \( ac = 5, 7, 11 \), but each of those are prime which means that if \( ac = 7, 11 \) then either \( a \) or \( c \) must be 7 or 11, breaking the bound of \( a, c \leq 6 \). So the only possible reduced form with \( \text{disc}(f) = -19 \) is \( f(x, y) = x^2 + xy + 5y^2 \) and so \( h(-19) = 1 \).

b) We see that \( \text{disc}(f) = 21^2 - 4(5)(23) = -19 \) and \( \text{disc}(g) = 247^2 - 4(209)(73) = -19 \) and \( \text{disc}(h) = 61^2 - 4(17)(55) = -19 \). So all \( f, g, h \) are equivalent to a reduced form with discriminant \(-19 \). By part (a) there is only one such form and so \( f, g, h \) are all equivalent to it and thus each other.

6. Prove that \(-8\) is a quadratic residue \( (\mod p) \) for a prime \( p \) if and only if \( p \equiv 1, 2, \) or \( 3 \) \( (\mod 8) \).

First we note that \(-8 \equiv 0 \pmod{2} \) so \(-8\) is a quadratic residue \( (\mod 2) \) and thus \( (\mod p) \) for all \( p \equiv 2 \pmod{8} \) since \( p = 2 \) is the only one.

So now we can suppose \( p \) is an odd prime, then \( p \equiv 1, \) or \( 3 \pmod{8} \). We have only to determine when \( \left( \frac{-8}{p} \right) = 1 \), so

\[
\left( \frac{-8}{p} \right) = \left( \frac{-2}{p} \right) \left( \frac{2}{p} \right)^2 = \left( \frac{-2}{p} \right) \left( \frac{2}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{2}{p} \right)
\]

so we have that \(-8\) is a quadratic residue \( (\mod p) \) iff \( \left( \frac{-1}{p} \right) = \left( \frac{2}{p} \right) = \pm 1 \). We see that

\[
\left( \frac{-1}{p} \right) = \left( \frac{2}{p} \right) = 1 \text{ exactly when } p \equiv 1 \pmod{8} \text{ and } \left( \frac{-1}{p} \right) = \left( \frac{2}{p} \right) = -1 \text{ exactly when } p \equiv 3 \pmod{8}.
\]

So \(-8\) is a quadratic residue \( (\mod 4p) \) for odd \( p \) exactly when \( p \equiv 1 \) or \( 3 \pmod{8} \) and so we are done.

7. Suppose \( n = x^2 + 2y^2 \) for \( x, y \in \mathbb{Z} \) such that \( p|n \) with \( p \) a prime where \( p \equiv 5 \) or 7 \( (\mod 8) \). Prove that \( p^2|n \) and that \( n/p^2 = (x')^2 + 2(y')^2 \) for some \( x', y' \in \mathbb{Z} \).
If \( n = x^2 + 2y^2 \) and \( p|n \) then \( x^2 = -2y^2 \pmod{p} \). So we must have \( x \equiv y \equiv 0 \pmod{p} \) or else \( x, y \) are invertible. In the latter case we get \((xy^{-1})^2 \equiv -2 \pmod{p}\) which means \(-2\) is a quadratic residue \( \pmod{p} \), but in the previous Problem we showed this can’t happen when \( p \equiv 5 \) or \( 7 \). So \( x \equiv y \equiv 0 \pmod{p} \) so \( x = x'p \) and \( y = y'p \) for \( x', y' \in \mathbb{Z} \) and we see \( n = (x'p)^2 + 2(y'p)^2 = p^2((x')^2 + 2(y')^2) \) and so \( p^2|n \) and \( n/p^2 = (x')^2 + 2(y')^2 \), and we’re done.

8. a) Compute \( h(-8) \).

b) Use part (a) and Problems 6 and 7 to show that for \( n \in \mathbb{N}, n = x^2 + 2y^2 \) for \( x, y \in \mathbb{Z} \) iff all primes \( p|n \) of the form \( p \equiv 5 \) or \( 7 \pmod{8} \) have even powers in the prime factorization of \( n \).

a) Following the same reasoning as in Problem 5, we just need to check \( a, |b|, c \leq \frac{1}{3} |−8| \) so \( a, |b|, c \leq 2 \). So the choices for \( b^2 \) are just 0, 1 and 4 and given \( b^2 - 4ac = -8 \) we have \( b^2 + 8 = 4ac \) so we must have \( b^2 = 0 \) or 4 for \( b^2 + 8 \) to be divisible by 4. If \( b^2 = 4 \) then \( ac = 3 \) which means \( a \) or \( c \) is 3, contradicting that \( a, c \leq 2 \) so \( b = 0 \) and \( ac = 2 \). Since \( c \geq a \) we get \( c = 2 \) and \( a = 1 \). So the only reduced quadratic form with discriminant \(-8\) is \( x^2 + 2y^2 \) and thus \( h(-8) = 1 \).

b) By Problem 7 we know that if \( p|n \) with \( p \equiv 5, 7 \pmod{8} \) then \( p^2|n \) and we can reduce the problem to \( n' \) where \( n = p^2n' \). We do this finitely many times until we can get rid of all the primes of this form in the factorization of \( n \) and we see that since we remove them by powers two at a time they must have even powers in the prime factorization.

To show that this is sufficient, suppose that all primes \( p|n \) of the form \( p \equiv 5 \) or \( 7 \pmod{8} \) have even powers in the prime factorization of \( n \). Note that if \( n = mr^2 \) with \( m, r \in \mathbb{N} \) where \( m \) is square-free (all the powers in the prime factorization are 1) then if \( m = x^2 + 2y^2 \) for \( x, y \in \mathbb{Z} \) then \( n = (xr)^2 + 2(yr)^2 \). So without loss of generality we can consider \( m \) which has no prime factors of the form \( p \equiv 5 \) or \( 7 \pmod{8} \) since they are all included in \( r^2 \).

Now, \( m = 2^kp_1 \cdots p_t \) where \( k = 0 \) or 1 and the primes \( p_j \equiv 1 \) or \( 3 \pmod{8} \). In lecture we proved that \( m \) can be properly represented by a quadratic form of discriminant \(-8 \) iff \(-8 \) is a quadratic residue \( \pmod{4m} \). So by the Chinese Remainder Theorem \(-8 \) is a quadratic residue \( \pmod{4m} \) iff \(-8 \) is a quadratic residue \( \pmod{4 \cdot 2^k} \) and \( \pmod{p_j} \) for all \( p_j \). But \(-8 \equiv 0 \pmod{4} \) and \( \pmod{8} \), thus \( \pmod{4 \cdot 2^k} \) and by Problem 6 we know that \(-8 \) is a quadratic residue for all \( p_j \). So \( m \) is properly represented by a quadratic form of discriminant \(-8 \), which must be equivalent to \( x^2 + 2y^2 \) by part (a) since there is only one reduced quadratic form of discriminant \(-8 \), and so \( m = x^2 + 2y^2 \) for \( x, y \in \mathbb{Z} \) and so we are done.

9. a) Compute \( h(-7) \).

b) Show that any prime \( p = x^2 + xy + 2y^2 \) for some \( x, y \in \mathbb{Z} \) iff \( p \not\equiv 3, 5 \) or \( 6 \pmod{7} \).
a) As in Problem 8 we just need to check $a, |b|, c \leq \frac{1}{3} | - 7 |$ so $a, |b|, c \leq 2$. The choices for $b^2$ are just 0, 1 and 4 and we need $b^2 + 7 = 4ac$ so $b = \pm 1$ and $ac = 2$ so $a = 1$ and $b = 2$ and since $b \in (-a, a]$ we have $b = 1$. So the only reduced form with discriminant $-7$ is $x^2 + xy + 2y^2$ and so $h(-7) = 1$.

b) From lecture we know that $n$ is properly represented by some quadratic form with discriminant $-7$ iff $-7$ is a quadratic residue (mod 4n). Primes can only be given as values of quadratic forms if they are properly represented because if $(x, y) = z > 1$ then $z^2 | f(x, y)$ and so $f(x, y)$ is not prime. Now by part (a) all quadratic forms with discriminant $-7$ are equivalent to $x^2 + xy + 2y^2$ so $p$ is given by $x^2 + xy + 2y^2$ iff $-7$ is a quadratic residue (mod 4p).

Now we see that $-7 \equiv 1 \pmod{8}$ and $-7 \equiv 7^2 \pmod{28}$ so we have representation in the only cases when $p \equiv 0, 2 \pmod{7}$. For everything else, $(-7, 4p) = 1$ and we observe that since $-7 \equiv 1 \pmod{4}$ so $-7$ is a quadratic residue (mod 4) and so we only have to check $\left( \frac{-7}{p} \right) = 1$ to see exactly when $-7$ is a quadratic residue mod 4p. Observe

$$\left( \frac{-7}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{7}{p} \right) = \left\{ \begin{array}{ll} \left( \frac{7}{p} \right) & \text{if } p \equiv 1 \pmod{4} \\ (-1) \left( \frac{-7}{p} \right) & \text{if } p \equiv 3 \pmod{4} \end{array} \right\} = \left( \frac{p}{7} \right)$$

and a quick search shows the only nonzero quadratic residues (mod 7) are 1, 2, and 4. So for $(-7, 4p) = 1$ we have $-7$ is a quadratic residue exactly when $p \equiv 1, 2$ or 4 and thus for all primes $p$ we have $p = x^2 + xy + 2y^2$ exactly when $p \not\equiv 3, 5$ or 6.

10. Let the prime $p$ be such that $p \equiv 7 \pmod{8}$. Show that

$$p = x^2 + y^2 + z^2$$

has no solutions for $x, y, z \in \mathbb{Z}$.

For any $x \in \mathbb{Z}$, $x^2 \equiv 0, 1$ or $4 \pmod{8}$. So there are only 10 ways to add three squares (mod 8):

$$0 + 0 + 0 \equiv 0, \quad 0 + 0 + 1 \equiv 1, \quad 0 + 0 + 4 \equiv 4, \quad 0 + 1 + 4 \equiv 5, \quad 0 + 1 + 1 \equiv 2, \quad 0 + 4 + 4 \equiv 0, \quad 1 + 1 + 1 \equiv 3, \quad 1 + 1 + 4 \equiv 6, \quad 1 + 4 + 4 \equiv 1, \quad 4 + 4 + 4 \equiv 4$$

none of these give 7 (mod 8), so if $p \equiv 7 \pmod{8}$, by reducing the equation to $7 \equiv x^2 + y^2 + z^2 \pmod{8}$ we see there are no possible solutions.