1. Show that the primes that are properly represented by quadratic forms with discriminant \( d = -24 \) are all those equivalent to \( 1, 2, 3, 5, 7, 11 \) (mod 24).

We know that \( p \) is properly represented by a quadratic form with discriminant \( d \) if and only if \( d \) is a quadratic residue (mod 4 \( p \)). If \( p = 2 \) we know that \(-24 \equiv 0^2 \) (mod 4 \( 2 \)) so 2 is properly represented, and this is all primes equivalent to 2 (mod 24). If \( p \) is odd then \(-24 \) is a quadratic residue if and only if \(-24 \) is a quadratic residue (mod 4) and (mod \( p \)). Since \(-24 \equiv 0^2 \) (mod 4) we just need to check when \(-24 \) is a quadratic residue (mod \( p \)). Since \(-24 \equiv 0^2 \) (mod 3) we have all the primes equivalent to 3 (mod 24). Now we need to check primes \( p > 3 \), and

\[
\left( \frac{-24}{p} \right) = \left( \frac{-6}{p} \right) = \left( \frac{-3}{p} \right) \left( \frac{2}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{3}{p} \right) \left( \frac{2}{p} \right) = \left( \frac{p}{3} \right) \left( \frac{2}{p} \right).
\]

So \( p \equiv 1 \) (mod 3) and \( p \equiv \pm 1 \) (mod 8) or \( p \equiv 2 \) (mod 3) and \( p \equiv \pm 3 \) (mod 8). By the Chinese Remainder Theorem we get that that this means \( p \equiv 1, 7 \) (mod 24) or \( p \equiv 5, 11 \) (mod 24).

2. Use the results of Problem 1 to prove that the primes properly represented by \( f(x, y) = x^2 + 6y^2 \) are all those equivalent to 1 or 7 (mod 24).

First we compute the class number \( h(d) \) when \( d = -24 \). We know that \(|b| \leq -\frac{d}{4} = 8 \) so our choices for \( b^2 - d = 4ac \) are 24, 25, 28, 33, 40, 49, 60, 73, 88 and only the ones that are divisible by 4 are allowed so the choices for \( ac \) are 6, 7, 10, 15 and 22. for \( b = 0, 2, 4, 6 \) and 8 respectively. Since \( c \geq a \geq |b| \) and we see that we can ignore the \( (a, c) \) pairs \((1, 7)\) for \( b = 2 \), \((1, 10)\) and \((2, 5)\) for \( b = 4 \), \((1, 15)\) and \((3, 5)\) for \( b = 6 \) and \((1, 22)\) and \((2, 11)\) for \( b = 8 \). So we are only left with \( b = 0 \) and the \( (a, c) \) pairs \((1, 6)\) and \((2, 3)\). This means we have exactly two reduced quadratic forms with discriminant \(-24\) and they are

\[
x^2 + 6y^2 \quad \text{and} \quad 2x^2 + 3y^2.
\]

By Problem 1 we know that exactly the primes of the form \( p \equiv 1, 2, 3, 5, 7 \) or 11 (mod 24) are represented by some quadratic form with discriminant \(-24\). We see that \( x^2 + 6y^2 \equiv 0 \) or 1 (mod 3) and \( 2x^2 + 3y^2 \equiv 0 \) or 2 (mod 3). We also see that the smallest nonzero values of \( x^2 + 6y^2 \) are 1 and 4. This means that if \( x^2 + 6y^2 = p \) for \( p \) prime then \( p \not\equiv 2, 3, 5 \) or 11 (mod 24) and if \( 2x^2 + 3y^2 = p \) for \( p \) prime then \( p \not\equiv 1, 7 \) (mod 24). Thus \( x^2 + 6y^2 \) and \( 2x^2 + 3y^2 \) must each represent exactly the primes the other form fails to represent, so \( x^2 + 6y^2 \) represents exactly those primes which are equivalent to 1 and 7 (mod 24).
3. Consider the sequence of numbers $s_0 = 0$, $s_1 = 1$, $s_2 = 2$, $s_3 = 5$, $s_4 = 12 \ldots$ where each subsequent term in the sequence, $s_n$, is given by the recursive formula

$$s_n = 2s_{n-1} + s_{n-2}$$

for all $n \in \mathbb{N}$ with $n \geq 2$. Let $p_n/q_n$, where $(p_n, q_n) = 1$, denote the $n$-th convergent of $\sqrt{2}$, that is $p_n/q_n = [a_0, a_1, a_2, \ldots, a_n]$ where $\sqrt{2} = [a_0, a_1, a_2, \ldots]$.

Prove that $q_n = s_{n+1}$ for all $n \geq 0$ and use this to show that $s_{n+2}/s_{n+1}$, for $n \geq 0$, is the $n$-th convergent of $1 + \sqrt{2}$.

First we compute the continued fraction of $\sqrt{2}$. Since 2 is between 1 and 4 we know that $a_0 = [\sqrt{2}] = 1$ and so $\theta_1 = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{1} = \sqrt{2} + 1$. So $a_1 = [\sqrt{2} + 1] = 2$ and $\theta_2 = \frac{1}{\sqrt{2} - 1} = \theta_1$ so the algorithm repeats. Thus $\sqrt{2} = [1, 2]$. Now $p_0/q_0 = 1/1$ and $p_1/q_1 = 3/2$ so indeed $q_0 = s_1$ and $q_1 = s_2$. We also know that $q_n = a_nq_{n-1} + q_{n-2}$ for all $n \geq 2$ and since $a_n = 2$ for all $n \geq 1$ we have that $q_n = 2q_{n-1} + q_{n-2}$. This means that $q_n$ satisfy the same recursive formula as $s_n$ and both start with the same terms, therefore they must be the same sequence, just shifted, so $q_n = s_{n+1}$ for $n \geq 0$.

It is easy to see that $1 + \sqrt{2} = [2]$ since we are only changing the $a_0$ term from $\sqrt{2}$. Thus $\tilde{p}_n/\tilde{q}_n = [2(0), 2(1), \ldots, 2(n)]$ for all $n \geq 0$. Thus for $n \geq 2$ we have $\tilde{p}_n = 2\tilde{p}_{n-1} + p_{n-2}$ and $\tilde{q}_n = 2\tilde{q}_{n-1} + q_{n-2}$ which is the same recursive relationship as $s_n$. We also observe that $\tilde{p}_0/\tilde{q}_0 = 2/1$ and $\tilde{p}_1/\tilde{q}_1 = 5/2$. This means $\tilde{p}_n = s_{n+2}$ and $\tilde{q}_n = s_{n+1}$ for $n = 0, 1$ and since both satisfy the same recursive relationship as $s_n$ we have that $\tilde{p}_n = s_{n+2}$ and $\tilde{q}_n = s_{n+1}$ for all $n \geq 0$ and so we are done.

4. For $n \in \mathbb{N}$ define

$$f(n) := \begin{cases} 1 & \text{if } n \text{ is a square} \\ 0 & \text{otherwise,} \end{cases}$$

and let

$$g(n) := \sum_{d|n} f(d).$$

Show that, for $x > 1$,

$$\sum_{n \leq x} f(n) = [\sqrt{x}] = \sqrt{x} + O(1)$$

and use this and the fact that

$$\sum_{d \leq x} \frac{1}{d^2} = \frac{\pi^2}{6} + O \left( \frac{1}{x} \right)$$

to show that

$$\sum_{n \leq x} g(n) = \frac{\pi^2 x}{6} + O \left( \sqrt{x} \right).$$
We see that

$$S(x) = \sum_{n \leq x} f(n)$$

counts the number of squares less than $x$. Since $x > 1$ we know that $x \in [n^2, (n+1)^2)$ for some $n \in \mathbb{N}$ and so $S(x) = n$. But $\sqrt{x} \in [n, n+1)$ so $S(x) = n = \lfloor \sqrt{x} \rfloor$. Furthermore, $\lfloor \sqrt{x} \rfloor = \sqrt{x} - \{\sqrt{x}\}$ and $0 \leq \{\sqrt{x}\} < 1$ so $\lfloor \sqrt{x} \rfloor = \sqrt{x} + O(1)$.

Now

$$\sum_{n \leq x} g(n) = \sum_{n \leq x} \sum_{d|n} f(d) = \sum_{m \leq x} f(d) \sum_{d \leq x} 1 = \sum_{d \leq x} f(d) \lfloor \frac{x}{d} \rfloor$$

$$= x \sum_{d \leq x} \frac{f(d)}{d} + O\left( \sum_{d \leq x} f(d) \right) = x \sum_{d \leq x} \frac{1}{d^2} + O(\sqrt{x}) = x \sum_{d \leq \sqrt{x}} \frac{1}{d^2} + O(\sqrt{x})$$

$$= x \left( \frac{\pi^2}{6} + O\left( \frac{1}{\sqrt{x}} \right) \right) + O(\sqrt{x}) = \frac{\pi^2 x}{6} + O(\sqrt{x}).$$

5. Recall that a primitive root exists (mod $n$) if and only if $n = 2, 4, p^m$ or $2p^m$ where $p$ is an odd prime and $m \in \mathbb{N}$. Show that when a primitive root exists that the only solutions to $x^2 \equiv 1 \pmod{n}$ are $x \equiv \pm 1 \pmod{n}$. Use this and Problem 6 from the Midyear Exam to show that for odd $n \in \mathbb{N}_{\geq 3}$ the product of all the invertible elements $a_1, a_2, \ldots, a_{\phi(n)} \pmod{n}$ satisfies

$$a_1 a_2 \cdots a_{\phi(n)} \equiv \begin{cases} -1 \pmod{n} & \text{if } n = p^m \\ 1 \pmod{n} & \text{otherwise.} \end{cases}$$

We see that $\pm 1$ are always solutions to $x^2 \equiv 1 \pmod{n}$ so we only need to check that they are the only solutions. This is true when $n = 2$, since $1 \equiv -1 \pmod{2}$ and $0$ is not a solution. We also note that $n = 2$ is the only case where $1$ and $-1$ are not distinct. So let $n > 2$. If a primitive root, $g$, exists (mod $n$) then we can take indices with respect to that root. So $x^2 \equiv 1 \pmod{n}$ has a solution if and only if $2\text{ind}(x) \equiv 0 \pmod{\phi(n)}$ if and only if $\text{ind}(x) \equiv 0 \pmod{\phi(n)/2}$, which we know we can do because $\phi(n)$ is even for $n > 2$. This means that $\text{ind}(x) \equiv 0$ or $\phi(n)/2 \pmod{\phi(n)}$, which means there are only two possible choices for $x$, so we’re done.

From Problem 6 of the midyear exam we know that for $n \geq 3$,

$$a_1 a_2 \cdots a_{\phi(n)} = (-1)^k$$

where $k$ is the even number of solutions to $x^2 \equiv 1 \pmod{n}$. Let $n$ be odd. By the first part of this problem we know that if $n = p^m$ then $k = 2$ and so $a_1 a_2 \cdots a_{\phi(n)} \equiv -1 \pmod{n}$.
If $n$ is odd and not a prime power then $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ for distinct primes $p_j$. Since there are always 2 solutions to $x^2 \equiv 1 \pmod{p_j^{\alpha_j}}$ the Chinese Remainder Theorem gives us exactly $k = 2^t$ solutions to $x^2 \equiv 1 \pmod{n}$ and so $k/2 = 2^{t-1}$ which is even, so $a_1 \cdots a_{\phi(n)} \equiv 1 \pmod{n}$.

6. a) Suppose $a, n_1, n_2 \in \mathbb{N}$ are relatively prime and $a$ has order $d_1$ (mod $n_1$) and order $d_2$ (mod $n_2$). Prove that $a$ has order $d_1d_2/(d_1,d_2)$ (mod $n_1n_2$).

b) Take $b, r \in \mathbb{N}_{\geq 2}$ and let $n = b^r + 1$. Show that the order of $b$ (mod $n$) is $2r$.

a) We want to find the smallest $d \in \mathbb{N}$ such that $a^d \equiv 1 \pmod{n_1n_2}$, now since $(n_1, n_2) = 1$ we have that

$$a^d \equiv 1 \pmod{n_1n_2} \iff n_1n_2|(a^d-1) \iff n_1, n_2|(a^d-1) \iff a^d \equiv 1 \pmod{n_1} \text{ and } (mod \ n_2).$$

Since the last statement is true iff $d_1|d$ and $d_2|d$ we have that $d$ is the least common multiple of $d_1, d_2$, which we denote $\{d_1, d_2\}$. In lecture we showed that $(d_1, d_2)\{d_1, d_2\} = d_1d_2$ so $\{d_1, d_2\} = \frac{d_1d_2}{(d_1,d_2)}$ and we’re done.

b) We see that $b^r \equiv -1 \pmod{n}$ and so $b^{2r} \equiv 1 \pmod{n}$ and so the order of $b$ (mod $n$) must divide $2r$. But since $r \geq 2$, any divisor, $d$, of $2r$ that isn’t $2r$ itself is less than or equal to $r$ and then $1 < b^d \leq b^r < n$ so $b^d \not\equiv 1 \pmod{n}$. Thus the order of $b$ (mod $n$) is $2r$. 