1. For this problem $x, y \geq 0$ always. We’ll prove the following claim: if $x^2 - 2y^2 = 1$ then $x + \sqrt{2}y = (3 + 2\sqrt{2})^k$ for some $k \geq 0$. (Last HW we showed the converse.)

(a) Show that $(x, y) = (1, 0)$ and $(3, 2)$ are the only solutions with $x \leq 3$.

If $x = 0$ then we need $y^2 = -1/2$ which has no solution. If $x = 1$ then we need $y = 0$. If $x = 2$ then we need $y^2 = 3/2$ which has no solution. If $x = 3$ then we need $y^2 = 4$ which has only $y = 2$ as a solution. (We require $y \geq 0$ in this problem.)

(b) Now suppose $(x, y)$ is a solution with $x > 3$. Let $u, v$ be such that $x + \sqrt{2}y = (3 + 2\sqrt{2})(u + \sqrt{2}v)$. We’ll show that $(u, v)$ is also a solution with $u, v > 0$ and $u < x$. Why is this enough to prove the claim?

By part (a), the statement of the problem is true if $x \leq 3$. Suppose now that the statement is true for all solutions $(x, y)$ with $x \leq n$ for some $n \geq 3$. We want to show that it is true for a solution with $x = n+1 > 3$. Given part (b), $x + \sqrt{2}y = (3 + 2\sqrt{2})(u + \sqrt{2}v)$ where $(u, v)$ is a solution and $u < x, u, v > 0$. By induction, $u + \sqrt{2}v = (3 + 2\sqrt{2})^k$ for some $k \geq 0$ and so $x + \sqrt{2}y$ is of the desired form.

(c) Use the fact that $(x, y)$ is a solution to show that $x > \sqrt{2}y$.

We have $x = 1 + 2y^2 > 2y^2 > \sqrt{2}y$.

(d) Use the fact that $(x, y)$ is a solution and $x > 3$ to show that $y > (2/3)x$.

We have $2y^2 = x^2 - 1 > (8/9)x^2$ since $x > 3$ and thus $y > (2/3)x$.

(e) Solve for $u, v$ in terms of $x, y$. Show that $u, v$ are integer.

Multiplying both sides of $x + \sqrt{2}y = (3 + 2\sqrt{2})(u + \sqrt{2}v)$ by $3 - 2\sqrt{2}$ gives $u + \sqrt{2}v = (3 - 2\sqrt{2})(x + \sqrt{2}y) = (3x - 4y) + (-2x + 3y)\sqrt{2}$. By an earlier HW this implies $u = 3x - 4y, v = -2x + 3y$. Since $x, y$ are integer so are $u, v$.

(f) Show that $u^2 - 2v^2 = 1$.

Plugging in the formulas from (e) and simplifying shows that $u^2 - 2v^2 = x^2 - 2y^2 = 1$. (Remember that if we define $N(z_1 + \sqrt{2}z_2) :=$
2. Let $T_n := n(n+1)/2$ for $n \geq 0$. $T_n$ is called a triangular number because if $n \geq 1$ you can imagine arranging $T_n = n + (n-1) + (n-2) + \cdots + 2 + 1$ points into a triangle with $n$ points on layer 1, $n-1$ points on layer 2, etc. Sometimes you can arrange $T_n$ points into a square grid, e.g. $T_0 = 0, T_1 = 1, T_8 = 36 = 6^2$, and $T_{48} = 1225 = 35^2$. We’ll show that $T_n$ is a square for infinitely many $n \geq 0$ and determine which $n$.

(a) Show that $T_n = m^2$ if and only if $(2n + 1)^2 - 2(2m)^2 = 1$.

This is just algebra, $n(n+1)/2 = m^2 \iff (2n + 1)^2 - 2(2m)^2 = 1$.

(b) Show that if $x^2 - 2y^2 = 1$ then $x$ is odd and $y$ is even.

If $x^2 - 2y^2 = 1$ then $x^2 \equiv 1 \pmod{2}$ and so $x$ is odd. Thus $x^2 \equiv 1 \pmod{4}$ and so $2y^2 \equiv x^2 - 1 \equiv 0 \pmod{4}$. Thus $y^2 \equiv 0 \pmod{2}$ and so $y$ is even.

(c) Show that $T_n = m^2$ with $n,m \geq 0$ if and only if $n = (x - 1)/2$ and $m = y/2$ where $x^2 - 2y^2 = 1$ and $x,y \geq 0$.

Clear from parts (a) and (b).

(d) Let $n_0 = 0, m_0 = 0$. For $k \geq 0$, let $n_{k+1} = 3n_k + 4m_k + 1, m_{k+1} = 2n_k + 3m_k + 1$ for $k \geq 0$. Show that $T_n = m^2$ with $n,m \geq 0$ iff $(n,m) = (n_k, m_k)$ for some $k \geq 0$. (Hint: Let $x_k, y_k, k \geq 0$ be such that $x_k + \sqrt{2}y_k = (3 + 2\sqrt{2})^k$. (Note $x_0 = 1, y_0 = 0$.) Recall the formulas you had for $x_{k+1}, y_{k+1}$ in terms of $x_k, y_k$.)

We know from problem 1, that $(x,y)$ is a solution to $x^2 - 2y^2 = 1$ if $x + \sqrt{2}y = (x_k + \sqrt{2}y_k) = (3 + 2\sqrt{2})^k$ for some $k \geq 0$. Thus by part (c), the solutions to $T_n = m^2$ are $(n,m) = (n_k, m_k)$ where $n_k = (x_k - 1)/2$ and $m_k = y_k/2$ for $k \geq 0$. Since $x_0 = 1, y_0 = 0$, we have $n_0 = 0, m_0 = 0$. By an earlier HW we have $x_{k+1} = 3x_k + 4y_k, y_{k+1} = 2x_k + 3y_k$ for $k \geq 0$. Plugging our
formulas relating $n_k, m_k$ and $x_k, y_k$ into these equations we get

$$(2n_{k+1} + 1) = 3(2n_k + 1) + 2(2m_k) \quad \text{(or } n_{k+1} = 3n_k + 2m_k + 1)$$

and

$$2m_{k+1} = 2(2n_k + 1) + 3(2m_k) \quad \text{(or } m_{k+1} = 2n_k + 3m_k + 1).$$

Both equations $n_{k+1} = 3n_k + 2m_k + 1, m_{k+1} = 2n_k + 3m_k + 1$ hold for $k \geq 0$.

3. Early on in class we proved Fermat’s theorem that if $p$ is a prime, $p \equiv 1 \pmod{p}$ then $p$ can be represented as a sum of two squares. Prove it again using Minkowski’s theorem. (In class we used Minkowski’s theorem to prove Lagrange’s theorem that every prime is representable as a sum of four squares.)

(a) Let $p$ be a prime with $p \equiv 1 \pmod{4}$. Recall that this means we can find $a$, such that $a^2 \equiv -1 \pmod{p}$. Let $A = AZ^2$, where

$$A = \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}.$$ 

In other words, $\Lambda = \{(u, (p, 0)) + v \cdot (a, 1) : u, v \in \mathbb{Z}\}$.

Show that if $(x, y) \in \Lambda$ then $x^2 + y^2 \equiv 0 \pmod{p}$.

This is just a straightforward verification. $(x, y) \in \Lambda$ iff $x = pu + av$ and $y = v$ for some integer $u, v$ and thus $x^2 + y^2 \equiv (a^2 + 1)v \equiv 0 \pmod{p}$.

(b) Use Minkowski’s theorem that we stated in class (6.21 from the book) to show that there is $(x, y) \in \Lambda$, $(x, y) \neq (0, 0)$ such that $x^2 + y^2 < 2p$. (Which convex body $C$ would you use?)

Let $C := \{(z, w) : z^2 + w^2 < 2p, z, w \in \mathbb{R}\}$ be the disc of radius $\sqrt{2p}$ centered at the origin in $\mathbb{R}^2$. Clearly $C$ is convex and centrally symmetric. Also the area of $C$, $|C| = \pi(\sqrt{2p})^2 = 2\pi p > 4|\det(A)| = 4p$ so $C$ must contain a point $(x, y) \in \Lambda$ with $(x, y) \neq (0, 0)$ by Minkowski’s theorem.

(c) Show that this proves Fermat’s theorem.

Since the point $(x, y) \in \Lambda$ we found in part (b) satisfies $0 < x^2 + y^2 < 2p$ and also $x^2 + y^2 \equiv 0 \pmod{p}$ by part (a), we have $x^2 + y^2 = p$.

4. (a) Show that $f = x^2 + xy + 5y^2$ is the only reduced positive definite binary quadratic form of discriminant $-19$.

We know that if $g = ax^2 + bxy + cy^2$ is a reduced positive definite binary quadratic form of discriminant $d = b^2 - 4ac = -19$
then $0 < a \leq \sqrt{-d/3} \leq 2.52$ (by Theorem 3.19 of the book) and that $-a < b \leq a$, so we need only check the cases $(a, b) = (2, 2), (2, 1), (2, 0), (2, -1), (1, 1), \text{ and } (1, 0)$. Solving $b^2 - 4ac = -19$ for $c$ in each of these cases gives us an integer value of $c = (b^2 + 19)/4a$ only in the case $(a, b) = (1, 1)$. In this case $c = 5$.

(b) Why does this show that $H(-19) = 1$?

$H(-19)$ is the number of inequivalent positive definite binary quadratic forms of discriminant $-19$. Since every form is equivalent to a reduced form, and there is only one possible reduced form by part (a), there is only one class.

(c) Which odd primes are represented by $f$?

By Corollary 3.14 and the fact that $H(-19) = 1$ we know that an odd prime $p$ is represented by $f$ iff $p | d$ or $(\frac{d}{p}) = 1$. The last equality holds by quadratic reciprocity. For example if $p = 4k + 3$, $(\frac{1}{p}) = -1$ and $(\frac{19}{p}) = -(\frac{p}{19})$. The case $p = 4k + 1$ is analogous. Only the numbers $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2 \text{ or } 1, 4, 9, 16, 6, 17, 11, 7, 5 \mod 19$ are quadratic residues. Thus $p$ is represented by $f$ iff $p = 19$ or $p \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \mod 19$.

(d) Show that you can solve $x^2 \equiv -19 \pmod{4}$ but not $x^2 \equiv -19 \pmod{2^a}$ for $a \geq 3$.

$x^2 \equiv -19 \pmod{4}$ or $x^2 \equiv 1 \pmod{4}$ has solutions $x \equiv 1, 3 \pmod{4}$. However, since $x^2 \equiv 0, 1, \text{ or } 4 \pmod{8}$ we can’t solve $x^2 \equiv -19 \equiv 5 \pmod{8}$. Thus $x^2 \equiv -19 \pmod{2^a}$ is not solvable for $a \geq 3$.

(e) Which numbers are properly represented by $f$?

We know that $n = 0$ cannot be properly represented. By Theorem 3.13 of the book, and the fact that $H(-19) = 1$ we have that $n$ is represented properly by $f$ iff $n > 0$ (since $f$ is positive definite) and $x^2 \equiv -19 \pmod{4n}$. Suppose the prime factorization of $n$ is $n = 2^a \prod p_i^{a_i}$ where the product extends over odd primes $p_i$. By the Chinese Remainder Theorem, $x^2 \equiv -19 \pmod{4n}$ is solvable iff $x^2 \equiv -19 \pmod{4 \cdot 2^a}$ and $x^2 \equiv -19 \pmod{p_i^{a_i}}$ are all solvable. By part (d), $x^2 \equiv -19 \pmod{4 \cdot 2^a}$ is solvable iff $a = 0$. Now
we have to determine if \( x^2 \equiv -19 \pmod{p^a} \) is solvable where \( p \) is an odd prime and and \( a \geq 1 \).

First suppose \( p \neq 19 \). Let \( f(x) = x^2 + 19 \). If \( f(x) \) has a root \( r \) mod \( p \), then \( r \not\equiv 0 \pmod{p} \). This means \( r \) is non-singular (\( f'(r) = 2r \not\equiv 0 \pmod{p} \)) and so \( r \) lifts to a root mod \( p^a \) for every \( a \geq 1 \). So in this case, \( x^2 \equiv -19 \pmod{p} \) is solvable iff \( x^2 \equiv -19 \pmod{p^a} \) is solvable.

Now suppose \( p = 19 \). Clearly \( f(x) \) has only the roots \( r = 0 \) mod 19. \( r = 0 \) is a singular root though \( f'(r) = 0 \). We have \( f(0) = 19 \not\equiv 19^2 \), so \( f(x) \) has no roots mod 192 and hence no roots for 19a for \( a \geq 2 \).

Thus \( n \) is properly represented iff \( n \) is of the form \( n = 19^a \prod p_i^{e_i} \)

where \( a = 0, 1 \) and where the \( p_i \) are odd primes of the form \( p_i \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19} \).

(f) Which numbers are represented by \( f \)?

We know that a number \( N \) is represented iff \( N = nb^2 \) where \( n \) is properly represented. Thus by part (e) the only numbers represented are \( N = 0 \) and \( N = 2^{2a} \prod p_i^{a_i} \prod q_i^{2b_i} \) where the \( p_i \) are primes of the form \( p_i \equiv 0, 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19} \) and the \( q_i \) are primes of the form \( p_i \equiv 2, 3, 8, 10, 12, 13, 14, 15, 18 \pmod{19} \). Note 19 can occur to any power in \( N \). because it can appear to the power \( a = 0 \) or \( a = 1 \) in \( n \) by part (e), and hence to the power \( 2k + 0 \) or \( 2k + 1 \) in \( N = nb^2 \).