Math 567, Assignment #12: Solutions

1. Every integer is congruent to 0, ±1, ±2, ±3, or ±4 (mod 9), so every square is congruent to 0, 1, 4, 0, or 7 (mod 9). Forming two-term sums of 0, 1, 4, and 7 in all possible ways, we see that a sum of two squares must be congruent to $0+0$, $0+1$, $0+4$, $0+7$, $1+1$, $1+4$, $1+7$, $4+4$, $4+7$, or $7+7$ (mod 9); since none of these is congruent to 3 or 6 (mod 9), no number congruent to 3 or 6 (mod 9) can be a sum of two squares.

2. Suppose n cannot be written as the sum of the squares of two integers. Then by the Corollary to Theorem 12.3, there exists a prime $p \equiv 3 \pmod 4$ that divides n with odd exponent. If it were possible to write $n = (a/b)^2 + (c/d)^2$, then multiplying through, we would get $n(bd)^2 = a^2d^2 + b^2c^2$, so that $n(bd)^2$ could be written as a sum of two squares. Note, however, that p divides n with odd exponent and divides $(bd)^2$ with even exponent, and therefore divides $n(bd)^2$ with odd exponent; this contradicts the fact that the integer $n(bd)^2$ can be written as the sum of the squares of two integers (namely ad and bc).

3. Given that s and t are odd, it is easy to show that $2st$, $s^2 - t^2$, and $s^2 + t^2$ are all even, so that $\frac{x}{2}$, $\frac{y}{2}$, and $\frac{z}{2}$ are all integers. It is also easy to check that $(\frac{x}{2})^2 + (\frac{y}{2})^2 = (\frac{z}{2})^2$, so $\frac{x}{2}$, $\frac{y}{2}$, $\frac{z}{2}$ is a Pythagorean triple. It remains only to check primitivity. If p is prime dividing both $\frac{y}{2}$ and $\frac{z}{2}$, then p divides $\frac{y}{2} + \frac{z}{2} = s^2$ and $\frac{z}{2} - \frac{y}{2} = t^2$. Hence p divides both s and t, contradicting the assumption $\gcd(s,t) = 1$. Hence $\gcd(\frac{y}{2}, \frac{z}{2}) = 1$, and the Pythagorean triple is primitive.

4. First way: Every square is congruent to 0 or 1 (mod 8), so a number of the form $a^2 + 2b^2$ must be congruent to $0 + 2\cdot 0$, $1 + 2\cdot 0$, $0 + 2 \cdot 1$, or $1 + 2\cdot 1$ (mod 8); that is, it must be congruent to 0, 1, 2, or 3 (mod 8). Hence if p is an odd prime that can be written in the form $a^2 + 2b^2$, p must be congruent to 1 or 3 (mod 8).

Second way: If $a^2 + 2b^2 = p$, we have $a^2 \equiv -2b^2 \pmod p$. Taking Legendre symbols as we did in class, we conclude that $(\frac{-2}{p})$ must be $+1$. Since $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$, we can apply our formulas for $(\frac{-1}{p})$ and $(\frac{2}{p})$ (given by the first and second laws of quadratic reciprocity) to deduce that $(\frac{-2}{p}) = +1$ iff $p \equiv 1$ or $3 \pmod 8$.

5. *First method:* Let p be a prime of congruent to 1 or 3 (mod 8). The prime $p = 3$ can be dealt with on its own ($3 = 1^2 + 2 \cdot 1^2$), so we may henceforth assume $p \geq 11$.

Step 1: There exists a positive integer $M < p$ such that Mp is equal to a square plus twice a square (that is, is of the form $a^2 + 2b^2$ for some choice of integers a, b).

Proof: Since $(\frac{-2}{p}) = +1$, there exists A such that $A^2 \equiv -2 \pmod{p}$. Write $A^2 + 2 = Mp$. If we take $0 < A \leq (p-1)/2$, we have $A^2 + 2 \leq (p^2 - 2p + 9)/4 \leq (p^2 - p)/4$, so $M = (A^2 + 2)/p \leq (p-1)/4 < p$.

Step 2: For every positive integer $M > 1$ such that Mp is a square plus twice a square, there exists a positive integer M', $1 \leq M' < M$, such that $M'p$ is a square plus twice a square.

Proof: Say $A^2 + 2B^2 = Mp$. Reduce A and $B \pmod{M}$, using residues in the range $-M/2$ to $+M/2$: $A \equiv u \pmod{M}$ and $B \equiv v \pmod{M}$, with $-M/2 \leq u, v \leq +M/2$. We have $u^2 + 2v^2 \equiv A^2 + 2B^2 \equiv 0 \pmod{M}$; say $u^2 + 2v^2 = MM'$. Note that $1 \leq M' \leq ((M/2)^2 + 2(M/2)^2)/M = 3M/4 < M$. ($M'$ is clearly non-negative, and $M' = 0$ could only happen if we had A and B both multiples of M; as in the case of sums of two squares, this would imply that $M|p$, and both $M = 1$ and $M = p$ are ruled out.) I claim that $M'p$ can be written as a square plus twice a square, namely $((Au + 2Bv)/M)^2 + 2((Av - Bu)/M)^2 = M'p$.

Why is the formula true? Because the LHS becomes

$$\frac{A^2u^2 + 4B^2v^2 + 2A^2v^2 + 2B^2u^2}{M^2} = \frac{(A^2 + 2B^2)(u^2 + 2v^2)}{M^2} = \frac{(Mp)(MM')}{M^2},$$

which equals $M'p$.

Why are $(Au+2Bv)/M$ and $(Av-Bu)/M$ integers? Because $Au+2Bv \equiv A^2 + 2B^2 \equiv 0 \pmod{M}$ and $Av - Bu \equiv AB - BA \equiv 0 \pmod{M}$.

Step 3: $1p$ is the sum of a square and twice a square.

Proof: There cannot exist an infinite decreasing sequence of integers between 1 and M.

Second method: Let p be a prime with $p \equiv 1$ or $3 \pmod{8}$. Since $(\frac{-2}{p}) = 1$, there exists an integer a with $a^2 \equiv -2 \pmod{p}$. Since $\gcd(a, p) = 1$, Thue's Lemma asserts that the congruence $ax \equiv y \pmod{p}$ has a solution x_0, y_0 where $0 < |x| < \sqrt{p}$ and $0 < |y| < \sqrt{p}$. As a result we have

$$-2x_0^2 \equiv a^2x_0^2 \equiv (ax_0)^2 \equiv y_0^2 \pmod{p}$$

or $y_0^2 + 2x_0^2 \equiv 0 \pmod{p}$; that is, $y_0^2 + 2x_0^2 = kp$ for some integer $k \geq 1$. The inequalities on x_0 and y_0 imply that $0 < y_0^2 + 2x_0^2 < 3p$, whence $k = 1$ or 2. If

$k = 2$, then $y_0^2 + 2x_0^2 = 2p$, which means that y_0 is even, say $y_0 = 2y_1$. Thus $(2y_1)^2 + 2x_0^2 = 2p$ and $x_0^2 + 2y_1^2 = p$, so that p can be written as $a^2 + 2b^2$. If $k = 1$, then $p = y_0^2 + 2x_0^2$, again of the form $a^2 + 2b^2$.

6. Easy algebra gives $(s^2 - 2t^2)^2 + 2(2st)^2 = (s^2 + 2t^2)^2$, so to do the easy half of the problem, we only need to check that $s^2 - 2t^2$, $2st$, and $s^2 + 2t^2$ have no common factor when s and t are relatively prime and s is odd. Suppose p is a prime dividing all three numbers; since $s^2 + 2t^2$ is odd, p must be an odd prime. Since $p|(s^2 + 2t^2) + (s^2 - 2t^2) = 2s^2$ and $p|(s^2 + 2t^2) - (s^2 - 2t^2) = 4t^2$, we get $p|s$ and $p|t$, contradicting $\gcd(s, t) = 1$.

In the other (harder!) direction, suppose $x^2 + 2y^2 = z^2$ with x, y, z positive and $\gcd(x, y, z) = 1$. We first will check that $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$. Say some prime p divides both x and y; then $p|x^2 + 2y^2 = z^2$, whence p divides z as well, contradicting $\gcd(x, y, z) = 1$. Hence $\gcd(x, y) = 1$. Similarly, $\gcd(y, z) = 1$. For the third case, suppose p divides both x and z; then $p|z^2 - x^2 = 2y^2$. Since $\gcd(x, y, z) = 1$, p cannot divide y, so p must equal 2. But then x and z must be even, and $2y^2 = z^2 - x^2 \equiv 0 - 0 \equiv 0 \pmod 4$ implies that y must be even as well, which is again a contradiction. So $\gcd(x, z) = 1$.

We have just seen that x and z can't both be even. At the same time, $x^2 + 2y^2 = z^2$ implies $x^2 \equiv z^2 \pmod 2$, so x and z must have the same parity. Hence x and z must both be odd. Therefore $2y^2 \equiv z^2 - x^2 \equiv 1 - 1 \equiv 0 \pmod 4$, so y must be even.

Now rewrite $x^2 + 2y^2 = z^2$ as $2(\frac{y}{2})^2 = \frac{z+x}{2}\frac{z-x}{2}$. Let $u = \frac{z+x}{2}$, $v = \frac{z-x}{2}$, so that $y^2 = 2uv$. u and v are relatively prime, since any non-trivial common factor of u and v would also be a common factor of $u + v = z$ and $u - v = x$, and we have seen that $\gcd(x, z) = 1$. One of the numbers u and v must be even, since their product is even.

Case I: u is even. The only way the product of the two relatively prime integers $\frac{u}{2}$ and v can equal the perfect square $(\frac{y}{2})^2$ is if $\frac{u}{2}$ and v are both squares; say, $\frac{u}{2} = t^2$ and $v = s^2$, with s, t relatively prime positive integers. Then $x = u - v = 2t^2 - s^2$, $z = u + v = 2t^2 + s^2$, and $y = \sqrt{2uv} = 2st$.

Case II: v is even. Then, proceeding as in Case I, we see that there must exist relatively prime positive integers s, t with $u = s^2$ and $\frac{v}{2} = t^2$, yielding $x = u - v = s^2 - 2t^2$, $z = u + v = s^2 + 2t^2$, and $y = \sqrt{2uv} = 2st$.

In either case, we get $x = |s^2 - 2t^2|$, $y = 2st$, and $z = s^2 + 2t^2$. Note finally that s must be odd (since otherwise x, y, z would have the common factor 2).