Homework 8
(Fermat's Last Theorem, Pythagorean triples, sums of squares.)
Due Monday, November 18 at 11:30am in class.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized; **this assignment has only one part and can be submitted as a single packet**.

(1) Show that $(25, 312, 313)$ is a primitive Pythagorean triple.

Proof. Note that 25 only has prime factors of 5. Since $5 \nmid 312$ and $5 \nmid 313$, we have that $\gcd(25, 312, 313) = 1$. One way to show that it is a Pythagorean triple is to square and add. A more interesting way is to apply Theorem 11.3 on p.223 (and focus on the possibilities for u and v from $b = 2uv$). We have that

$$\begin{aligned} 25 &= 169 - 144 = 13^2 - 12^2, \\ 312 &= 2(13)(12), \\ 313 &= 169 + 144 = 13^2 + 12^2. \end{aligned}$$

Letting $u = 12$ and $v = 13$, we note that $\gcd(u, v) = 1$, $u > v$, and u is even while v is odd (different parity). So, by Theorem 11.3, $(25, 312, 313)$ is a primitive Pythagorean triple. □

(2) Show that there is not Pythagorean triple (a, b, c) such that $a = 2b$. *Do not use the fact that $\sqrt{5}$ is irrational.* Conclude that $\sqrt{5}$ is irrational.

Proof. Suppose, towards a contradiction, that there is a Pythagorean triple (a, b, c) such that $a = 2b$. Then we have that

$$c^2 = a^2 + b^2 = 4b^2 + b^2 = 5b^2.$$

Thus c^2 is divisible by 5 and since 5 is prime, it must be that c is divisible by 5. Write $c = 5c_1$. Then

$$25c_1^2 = c^2 = 5b^2$$

and so $b^2 = 5c_1^2$. Thus b is divisbile by 5 and we can write $b = 5b_1$. Therefore,

$$25c_1^2 = 5b^2 = 5(5b_1)^2 = 125b_1^2.$$

Thus $c_1^2 = 5b_1^2$ and so c_1 is divisible by 5. Write $c_1 = 5c_2$. Repeating the same process, we arrive at $c_2 = 5c_3$ and $c_3 = 5c_4$ and so on. Thus we have an infinite sequence of positive integers c_i such that

$$c_1 = 5c_2 = 5c_3 = 5c_4 = \cdots$$

and so

$$c_1 > c_2 > c_3 > c_4 > \cdots$$

is an infinite decreasing sequence of positive integers, which is impossible. Therefore, we have reached a contradiction, and no such Pythagorean triple can exist. □

(3) (a) Show that if n is a sum of three perfect squares, then $n \not\equiv 7 \pmod 8$.
(Hint: Write $n = a^2 + b^2 + c^2$ and consider $n \pmod 8$. What values are perfect squares mod 8?)

Proof. Suppose that $n = a^2 + b^2 + c^2$. We have that

$$\begin{aligned}0^2 &\equiv 0 \pmod 8\\ 1^2 &\equiv 1 \pmod 8\\ 2^2 &\equiv 4 \pmod 8\\ 3^2 &\equiv 1 \pmod 8\\ 4^2 &\equiv 0 \pmod 8\\ 5^2 &\equiv 1 \pmod 8\\ 6^2 &\equiv 4 \pmod 8\\ 7^2 &\equiv 1 \pmod 8.\end{aligned}$$

So a^2, b^2, c^2 are congruent to 0, 1, or 4 mod 8. One way to solve this problem is to exhaust all the options and see that none are 7 (mod 8):

$$\begin{aligned}0+0+0 &\equiv 0 \pmod 8\\ 0+0+1 &\equiv 1 \pmod 8\\ 0+1+1 &\equiv 2 \pmod 8\\ 1+1+1 &\equiv 3 \pmod 8\\ 0+0+4 &\equiv 4 \pmod 8\\ 0+4+4 &\equiv 0 \pmod 8\\ 4+4+4 &\equiv 4 \pmod 8\\ 1+1+4 &\equiv 6 \pmod 8\\ 1+4+4 &\equiv 1 \pmod 8\\ 0+1+4 &\equiv 5 \pmod 8\end{aligned}$$

□

(b) Show that if n is a sum of three perfect squares and n is divisible by 4, then $\frac{n}{4}$ is also a sum of three perfect squares.
(Hint: Write $n = a^2 + b^2 + c^2$ and consider $n \pmod 4$. What values are perfect squares mod 4?)

Proof. Suppose that $n = a^2 + b^2 + c^2$ and n is divisible by 4. We have that

$$\begin{aligned}0^2 &\equiv 0 \pmod 4\\ 1^2 &\equiv 1 \pmod 4\\ 2^2 &\equiv 0 \pmod 4\\ 3^2 &\equiv 1 \pmod 4\end{aligned}$$

So a^2, b^2, c^2 are congruent to 0 or 1 mod 4. Since n is divisible by 4, we also have that

$$a^2 + b^2 + c^2 \equiv 0 \pmod 4.$$

Thus it must be that $a^2 \equiv b^2 \equiv c^2 \equiv 0 \pmod 4$ (if there are any 1's, then the congruence no longer holds). In other words, $\frac{a^2}{4}, \frac{b^2}{4}$, and $\frac{c^2}{4}$ are integers (and a, b, and c are even). Thus $4 \mid a^2$, $4 \mid b^2$, and $4 \mid c^2$. Thus

$$\frac{n}{4} = \frac{a^2 + b^2 + c^2}{4} = \frac{a^2}{4} + \frac{b^2}{4} + \frac{c^2}{4} = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2.$$

So $n/4$ is a sum of three squares.

□

(c) Show that if $n = 4^e(8k + 7)$, then n is not a sum of three perfect squares. (Hint: Proceed by contradiction.)

Proof. Suppose that $n = 4^e(8k+7)$ and, towards a contradiction, that $n = a^2+b^2+c^2$ for some $a, b, c \in \mathbb{Z}$. Repeatedly dividing by 4, by part (b), it follows that $n_1 = 4^{e-1}(8k + 7)$, $n_2 = 4^{e-2}(8k + 7), \ldots, n_e = 4^{e-e}(8k + 7) = 8k + 7$ are all sums of three squares as well. However, $n_e \equiv 7 \pmod 8$ which, by part (a), is a contradiction. So it must be that n is not a sum of three perfect squares. □