Math 445. Exam #1

(1) Definitions/Theorem statements
   (a) State the definition of a **Pythagorean triple**.

   (b) State **Fermat's Little Theorem**.

   (c) State the definition of a **primitive root**.

   (d) State **Euler's criterion**.

(2) Computations.

(a)
- Use the definition of congruence to verify that

$$\begin{cases} 54 \equiv 10 \pmod{11} \\ 54 \equiv 3 \pmod{17} \end{cases}$$

- Explicitly describe the set of integers x that satisfies the two congruences

$$\begin{cases} x \equiv 10 \pmod{11} \\ x \equiv 3 \pmod{17} \end{cases}$$

(b) Find the inverse of $[121]$ in $\mathbb{Z}_{369}$.

(c) Determine if 83 is a quadratic residue modulo 97. (Both 83 and 97 are primes; you do not need to check this.)

(d) Find the smallest nonnegative integer n such that $17^{3202} \equiv n \pmod{250}$.

(3) Proofs.

(a) Without using the Sums of Two Squares Theorem, show there are no integers a, b, c such that $a^2 + b^2 + 1 = (2c)^2$.

(b) Let p, q be distinct primes and $a \in \mathbb{Z}$. Show that $[a]_{pq}$ has at most four square roots in $\mathbb{Z}_{pq}$. (Hint: Show that if $b^2 \equiv a \pmod{pq}$, then $b^2 \equiv a \pmod{p}$ and $b^2 \equiv a \pmod{q}$.)

(c) Let p be an odd prime such that $p \equiv 2 \pmod 3$. Show that every element of $\mathbb{Z}_p^\times$ has a cube root; i.e., if $a \in \mathbb{Z}_p^\times$, there is some $b \in \mathbb{Z}_p^\times$ such that $b^3 = a$.

Bonus: Let p be an odd prime such that $p \equiv 1 \pmod 3$. Show that $a \in \mathbb{Z}_p^\times$ has a cube root if and only if $a^{(p-1)/3} = [1]$.

Bonus: Characterize all rational numbers r such that the circle $x^2 + y^2 = r$ has a rational point.