Math 845. 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) Find the inverse of $[121]$ in $\mathbb{Z}_{369}$.

(b) I computed earlier that $4 \cdot 80 - 11 \cdot 29 = 1$. (You do not need to check this.) Use this to find an explicit formula for all integers n that satisfy the congruences

$$\begin{cases} n \equiv 2 \pmod{29} \\ n \equiv 3 \pmod{80} \end{cases}$$

(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 $p \equiv 1 \pmod 3$. Show that $a \in \mathbb{Z}_p^\times$ has a cube root (i.e., an element b such that $b^3 = a$ in $\mathbb{Z}_p$) 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.