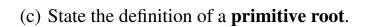
Math 445. Exam #1

(1)	Definitions/Theorem statemer (a) State the definition of a Py	ean trij	ole.

(b) State Fermat's Little Theorem.



(d) State Euler's criterion.

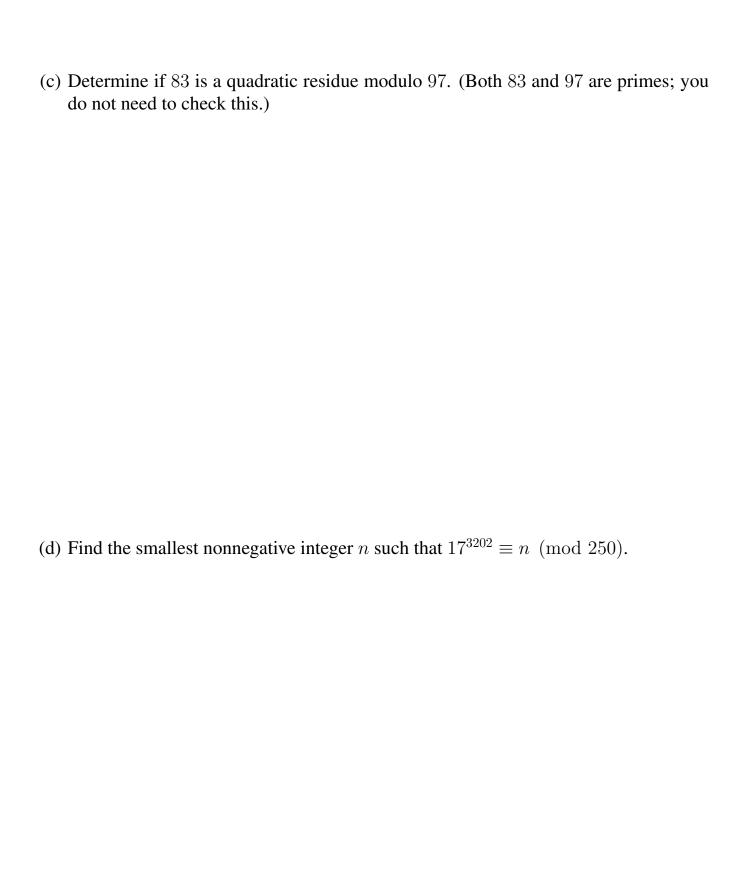
- (2) Computations.
 - (a) Use the definition of congruence to verify that

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

 \bullet 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} .



- (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 $a^{(p-1)/3} = [1]$.

