ELEMENTARY NUMBER THEORY

MIDTERM 2

NAME: .....

problem	1	2	3	4	5	6	7	8	9	10
points to earn	10	10	10	10	10	10	10	10	10	10
points earned										

A few simple rules:

- Write clearly.
- Give a complete sentence as your answer.
- Always explain which theorem you are using.

(1) Define the Legendre symbol and the Jacobi symbol.
(2) Prove that -7 is a square modulo $p \neq 7$ if and only if $p \equiv 1, 2, 4 \bmod 7$.
(3) Solve the linear system of congruences

$$x \equiv 13 \bmod 17$$
$$x \equiv 17 \bmod 13$$

(4) Find all natural numbers m with $\phi(m) = 4$.
(5) Is 21 a quadratic residue modulo 101?
(6) Compute $3^{201} \bmod 75$.
(7) Prove that every prime factor of $3x^2 + 1$ is $\equiv 1 \bmod 3$. Then show that there exist infinitely many primes $p \equiv 1 \bmod 3$.
(8) Let $q \equiv 1 \bmod 4$ and $p = 2q + 1$ be primes.
  (a) Show that $(\frac{2}{p}) = -1$;
  (b) Show that 2 is a primitive root mod p.
(9) Assume that $p \equiv 5 \bmod 8$ is prime, and that $(\frac{a}{p}) = +1$.
  (a) Show that if $a^{(p-1)/4} \equiv 1 \bmod p$, then $x = a^{(p+3)/8}$ solves the congruence $x^2 \equiv a \bmod p$.
  (b) If $a^{(p-1)/4} \equiv -1 \bmod p$, then $x \equiv 2a(4a)^{(p-5)/8} \bmod p$ solves the congruence $x^2 \equiv a \bmod p$.
(10) Use Gauss's Lemma to show that $(\frac{2}{p}) = (-1)^{(p-1)/4}$ for primes $p \equiv 1 \bmod 4$.