Math 346B: Number Theory
Midterm Test (March 5, 1997)

Time: 1 hour

1. (a) Find the gcd of 350 and 4001 and express it as a linear combination of 350 and 4001.

   (b) Is 350 invertible modulo 4001? If so, what is it's inverse?

2. Determine whether the following assertions are true or false. If true, prove the result, and if false, give a counterexample.

   (a) If $a^3|c^2$ then $a|c$;

   (b) If $a^2|c^3$ then $a|c$;

   (c) If $p$ is a prime and $p \nmid x$ then $x^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$;

   (d) If $\varphi$ is Euler's function then $\varphi(mn) = \varphi(m)\varphi(n)$.

3. Solve the system of congruences

$$9x \equiv 12 \pmod{33},$$
$$12x \equiv 4 \pmod{55}.$$

4. Show that $2^{50} \equiv -1 \pmod{125}$. Explain why this implies that 2 is a primitive root modulo 125. What is the order of 32 modulo 125?