TEST 3

(Math 258 B)

1. (a) Show that if a divides b, then a^2 divides b^2. (30 pts)

   (b) Prove or disprove: If p and q are primes, then $p^2 + q^2$ is a prime.

   (c) Show that if a^2 is even, then it is divisible by 4.

2. Find the prime factorization of 1001. (10 pts)

3. Find the **gcd(a,b)** and **lcm(a,b)** of the following integers: (10 pts)

   $a = 2^3 \cdot 3^2 \cdot 7 \cdot 11^2 \cdot 17^2$ and $b = 2^2 \cdot 3^4 \cdot 5 \cdot 11$

4. Use the *extended Euclidean algorithm* to write the gcd(277,123) as a linear combination of 277 and 123. Use that relation to find the inverse of 123 in Z_{277}. (20 pts)

5. Show that if a is an odd integer, then $a^2 \equiv 1 \bmod 8$. (10 pts)

6. Solve the congruence $4x \equiv 5 \bmod 9$. List at least three integers that are solutions of the congruence. (10 pts)

7. Solve the system of congruences: (10 pts)

$$x \equiv 2 \bmod 3$$
$$x \equiv 1 \bmod 4$$
$$x \equiv 3 \bmod 5.$$