MAT310 Test 3: Chapters 6, 7, 10, 11

Name:

Directions: Show your work! Answers without justification will likely result in few points. Your written work also allows me the option of giving you partial credit in the event of an incorrect final answer (but good reasoning). Indicate clearly your answer to each problem (e.g., put a box around it).
Note: you may of course use your calculators, but the use of the calculator without analysis will not result in many points. **Good luck!**

Problem 1 (10 pts) Prove Theorem 7.5, assuming that $a^{\phi(p^k)} \equiv 1 \pmod{p^k}$ if prime p doesn't divide a, $k > 0$:

If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1(\text{mod n})$.

Problem 2 (10 pts). Given $n = 38877300$. Compute

- $\tau(n)$

- $\sigma(n)$

- $\phi(n)$

- Is the function

$$\beta(n) = \sum_{d|n} \phi(d)$$

multiplicative? Why or why not?

Problem 3 (10 pts). In a Pythagorean triple x, y, z prove that not more than one of x, y, or z can be a perfect square.

Problem 4 (10 pts).

- Use Vigenère's Cypher to encrypt the message *What are you doing after the test?*, using the key word *sleeping*. Use the alphabet translation from the book, i.e.
  - a-z replaced by 0-25,
  - "?" by 28, and
  - space by 99.

- A message is to be encoded using RSA (the message is "send money" – use the same alphabet translation as given above): the person to whom you wish to send the message has chosen $p = 37$ and $q = 29$ as their primes, with $k = 41$.
  - Encode the message, using a block size of three (and tacking on xx to the end of the message).
  - What value of j will the target of your message need to use to decode the message? [Hint: 287=7*41.]

Problem 5 (10 pts).

- What formula will generate the even perfect numbers? Write down the first 5 of them.

- Demonstrate that the product of two odd primes is never a perfect number [Hint: expand the inequality $(p-1)(q-1) > 2$].

Problem 6 (10 pts). Demonstrate that, for any integer $n \geq 0$, $133 \mid 8^{108n+8} - 64$.

Extra Credit (3 pts). Describe the history of Fermat's last theorem.