Math 362 Assignment 2

Due: Wednesday, October 16

- Answer all questions. Each question is worth 5 marks. Full marks will be awarded only for answers that are both mathematically correct and coherently written.
- Please consider the markers and write neatly and legibly! I have instructed the markers to ignore work they cannot read. (And I won't read it, either.)

1. Use Wilson's Theorem to prove that if p is prime and $p \equiv 1 \pmod 4$, then

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p.$$

Note: Remember this problem!

2. (a) [2] Find infinitely many integers n such that $d(n) = 65$. (One line!)
   (b) [3] Find four solutions of $\phi(n) = 16$.

3. An integer n is called **triangular** if and only if $n = m(m+1)/2$ for some integer m. Prove that every even perfect number is triangular.

4. (a) [3] Let p be prime and let M_p denote the number $2^p - 1$. The number M_p is called a *Mersenne number*, and if it is prime, it is called a *Mersenne prime*. There is a test, called the **Lucas-Lehmer Test**, that gives a necessary and sufficient condition for M_p to be prime. It is always used to verify that a Mersenne number, suspected of being prime, is indeed a Mersenne prime. Give the statement of this test. Why is it a "fast" test for verifying primality?
   (Look it up in a book or on the internet.)
   (b) [2] Let p and q be odd primes. There is a necessary condition for q to divide M_p found by Fermat (one part) and Euler (the other part). State this condition. Follow the advice in (a).

5. Let k be a fixed positive integer. Show that if there is exactly one positive integer n such that $\phi(n) = k$, then $36|n$.

   [Hint: Assume $36 \nmid n$, write n as $n = 2^r 3^s m$, where $(m, 2) = (m, 3) = 1$, and consider the various possibilities for r and s.]

6. The following message has been encrypted using a Caesar cypher with constant shift. What does it say?

   "AX USFSVS AK LG KMJNANW, AL USF GFDQ KMJNANW AF EMLMSD JWKHWUL SFV AF DGNW XGJ GFW SFGLZWJ."

7. The following message has been encrypted using a Caesar cypher with random shift, each letter mapped to the same letter for every occurrence. (I.e., if "X" is mapped to "Y" in one instance, "X" is mapped to "Y" each time it occurs.) What does it say?

   "KO R QSOCSOIS, CVS MSXE VRQ CP RAXSS GKCV CVS QYEZSIC."