Note that this assignment is due on Thursday, rather than Friday, so that you may review the solutions before the exam. There is a mailbox for Math 42 in the mail room the first floor of the Kassar building. I will post solutions at 5pm, so assignments must be submitted by that time.

1. Let $\sigma(n)$ denote the sum of all positive integer divisors of n, *including* 1 *and* n.

   (a) Prove that if m and n are relatively prime then $\sigma(mn) = \sigma(m)\sigma(n)$ (you will probably want to cite a lemma that I will prove in class on Friday).

   (b) Suppose that p is prime, and $e \geq 1$. Find a formula for $\sigma(p^e)$.

2. Evaluate $\sigma(10)$, $\sigma(20)$, $\sigma(1728)$, and $\sigma(4100)$.

3. Prove the following two statements (used in the proof of the Euclid-Euler theorem on even perfect numbers).

   (a) Suppose that n is the number $2^k m$, where $k \geq 1$ and m is odd. Also suppose that n is a perfect number, meaning that $\sigma(n) = 2n$. Prove that there exists an integer ℓ such that $\sigma(m) = \ell \cdot 2^{k+1}$ and $m = \ell \cdot (2^{k+1} - 1)$.

   (b) Show that if a, b are two integers, with $a \geq 2$ and $b \geq 2$. Prove that

   $$\sigma\left(a \cdot (2^b - 1)\right) > a \cdot 2^b.$$

   Why did you need to assume that a and b are both at least 2?

   (c) Deduce from part (b) that the number ℓ from part (a) must, in fact, be equal to 1.

4. (a) Suppose that p is a prime number. Prove that if a, b are any two integers such that $a^2 \equiv b^2 \pmod{p}$, then either $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$.

   (b) Suppose that m is a positive integer (not necessarily prime). Prove that if there are two different integers a, b, both between 1 and $\frac{1}{2}m$ (inclusive) such that $a^2 \equiv b^2 \pmod{m}$, then m must be composite.

   (c) Compute (without using a calculator) that 150^2 is congruent to another (smaller) square modulo 22331, and deduce that the number 22331 must be composite.

   Note. In fact, once two congruent squares are found modulo m, there is a very efficient way to factor m into two parts (I encourage you to try to see how). This observation is the basis of an algorithm called the *quadratic sieve*, which is the most efficient algorithm known for factoring numbers of up to roughly 100 digits. The most difficult aspect of the quadratic sieve is efficiently searching for the two congruent squares, which requires some ideas from linear algebra.