Math545 **Homework 3** **Due Wed, Sept 25, 2013**

Directions: Solve the following 6 problems. For computer problems, complete solutions include source code, an **English language overview** of your code, and the final answer. The overview should be sufficiently complete that an intelligent reader with no prior access to your code will understand how it works. See the course syllabus and the Homework Webpage on the course website for general directions and guidelines.

1. [NT 3-3.1] Prove that p is the smallest prime that divides $(p-1)! + 1$.

2. Let $f(n)$ be the number of representations of n as the sum of square numbers. For example, since $25 = 0^2 + 5^2$ and $25 = 3^2 + 4^2$, it follows that $f(25) \geq 2$. In fact, $f(25) = 2$ and 25 is the least integer n such that $f(n) \geq 2$. Similarly, $f(12) = 0$ since there is no way to write 12 as the sum of two squares. On the other hand, $f(18) = 1$ because the only way to express 18 as the sum of two squares is $18 = 3^2 + 3^2$.

   (a) Determine the least integer n such that $f(n) \geq 3$. What are the representations of n?

   (b) Determine the least integer n such that $f(n) \geq 20$. What are the representations of n? *[Hint: Using an algorithm computes $f(n)$ in a loop starting with $n = 1$ and working upward will probably be too slow. To be more efficient, try computing all the values $f(1), f(2), \ldots, f(n)$ all at once for a trial value of n. If we find any numbers with 20 distinct representations, we're done: just grab the smallest. Otherwise, double n and try again.]*

3. [NT 4-1.{1,2}] If possible, find integers x such that the following congruences hold:

   (a) $5x \equiv 4 \pmod 3$

   (b) $9x \equiv 8 \pmod 7$

   (c) $12x \equiv 9 \pmod 6$

4. [NT 4-1.5] Prove that if $|a| < k/2$, $|b| < k/2$, and $a \equiv b \pmod k$, then $a = b$.

5. [NT 4-2.4] Let $w(n)$ denote the number of primes in $[n]$ that do not divide n. For example, $w(15) = 4$ since the set of primes at most 15 that do not divide 15 is $\{2, 7, 11, 13\}$.

   (a) Is it the case that $w(n) < \phi(n)$ for each positive integer n? Either prove this is so or give a counter-example.

   (b) Let S be the set of all positive integers n such that $w(n) = \phi(n) - 1$. What is S? Prove that your answer is correct.

6. [NT 5-2.4] Let $k = \phi(m)$. Prove that if $r_1, \ldots, r_k$ is a reduced residue system modulo m and m is odd, then $r_1 + r_2 + \cdots + r_k \equiv 0 \pmod m$.

Note: No formal challenge problems on this assignment. However, the problem NT 4-3.2 is entertaining and, I believe, fairly challenging. I see one way of proving it (by examining the behavior of the base 2 representation of the card indices). The details would be somewhat messy to write down. Perhaps there is a better way– can you find one?