Math 322 Fall 2016
Number Theory HW 4
Due Friday, September 30

You may *not* discuss the starred problem with classmates, though you should of course feel free to discuss it with me as much as you like. Linguistic precision is important for this problem.

($\star$) **Starred Problem:** Show that multiplicative inverses $\mod m$ are unique up to congruence. That is, if a, b, c are integers, and m is a positive integer, and $ab \equiv 1 \mod m$ and $ac \equiv 1 \mod m$, then $b \equiv c \mod m$.

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. Use Fermat's method of squares to factor 14647.

2. Let S be a set of m integers such that no element of S is congruent to any other element of S mod m. Prove that S is a complete system of residues.

3. Let a, b, m, n be integers with $m, n > 0$ and $m|n$. Prove that if $a \equiv b \mod n$, then $a \equiv b \mod m$.

4. Prove that an integer is divisible by eleven if and only if the sum of its even-placed base 10 digits minus the sum of its odd-placed digits is divisible by eleven. That is, if $n = n_0 + n_1 \cdot 10 + n_2 \cdot 10^2 + \cdots + n_k 10^k$, then $11|n$ if and only if

$$11|\sum_{i \text{ even}} n_i - \sum_{i \text{ odd}} n_i = n_0 - n_1 + n_2 - n_3 + \ldots$$

5. Fix an integer $m > 0$, and suppose that m has the following property: if a is an integer and $m \nmid a$, then a has a multiplicative inverse $\mod m$. That is, m is an integer such that every integer is either divisible by m, or has a multiplicative inverse $\mod m$. Then prove that m is prime.

6. Find a solution to each system of congruences:

   (a)

$$5x \equiv 3 \mod 23$$

(b)

$$x \equiv 0 \mod 2 \qquad x \equiv 0 \mod 3$$
$$x \equiv 1 \mod 5 \qquad x \equiv 6 \mod 7$$

(c)

$$x \equiv 2 \mod 11 \qquad x \equiv 3 \mod 12$$
$$x \equiv 4 \mod 13 \qquad x \equiv 5 \mod 17$$
$$x \equiv 6 \mod 19$$