HOMEWORK ASSIGNMENT #9, DUE WEDNESDAY, 12/01/2010

(1) Use the identity $e^{ix} = \cos x + i \sin x$ and the binomial theorem to write $\sin 3x, \sin 5x$ as polynomials in $\sin x$.

The next three exercises explain some basic properties of a generalization of the Legendre symbol known as the *Jacobi symbol*. Let m be a positive odd integer, and let $m = p_1^{e_1} \dots p_r^{e_r}$ be its prime factorization. Let a be any integer. Then the Jacobi symbol of $a \mod m$ is written $\left(\frac{a}{m}\right)$, and is defined by

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i}.$$

For instance, if $m = 45 = 3^2 \cdot 5$, then $\left(\frac{17}{45}\right) = \left(\frac{17}{3}\right)^2 \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$. Notice that the Jacobi symbol is the same as the Legendre symbol if m is an odd prime.

(2) (20 points)
   (a) Show that $\left(\frac{a}{m}\right) = 0$ if and only if $\gcd(a, m) > 1$.
   (b) If $a \equiv b \mod m$, show that $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.
   (c) If m, n are positive odd integers, show that $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
   (d) Show that if $\left(\frac{a}{m}\right) = -1$, then a is a quadratic non-residue mod m.
   (e) In contrast to the above, exhibit an example of a, m such that $\left(\frac{a}{m}\right) = 1$, but a is not a quadratic residue mod m.

(3) (20 points) Show that the following extensions of properties of the Legendre symbol are true for the Jacobi symbol:
   (a) If a, b are integers, then

$$\left(\frac{a}{m}\right)\left(\frac{b}{m}\right) = \left(\frac{ab}{m}\right).$$

   (b)

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}.$$

   (c)

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

   (d) If m, n are relatively prime positive odd integers, then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

   (Hint: in this problem, instead of writing $m = p_1^{e_1} \dots p_r^{e_r}$, say, let $m = p_1 p_2 \dots p_r$, where the p_i are not necessarily distinct. This does not change the mathematics at all, but might simplify notation.)

(4) (a) Using only Legendre symbols (ie, pretend you have never heard of Jacobi symbols when doing this problem), determine whether 693 is a quadratic residue mod 713 or not.
   (b) Using Jacobi symbols, determine whether 693 is a quadratic residue mod 713 or not. Which method was faster?

For the last two questions you should write a paragraph or two. There is no 'correct' answer, but you should be provide some detail in your responses.

(5) Write about your favorite theorem, idea, proof, concept, or application you learned in this class. Besides describing what your favorite theorem, etc. was, also give a brief explanation of why it is your favorite, and if applicable, describe how it was applied to other topics in this class.

(6) Describe a topic or two that you would have liked to learn more about in this class. You can either write about an extension of an idea that we did not fully cover, or about something which was not covered at all in this class but is still number theory (perhaps something you read about somewhere, such as a magazine, on the Internet, or in other parts of the textbook).