MATH 3320, HOMEWORK #8

DUE FRIDAY, OCTOBER 19

To ensure that you get full credit, be sure to *show your work* in the problems that require calculations. Very little credit is given for answers without justification. Please write in complete sentences to help us understand what you are doing.

You may collaborate with classmates in solving the problems, including the extra credit problems. If you do so, please list their names on your assignment. However, you should not consult *any* other people (except the instructors or TAs), or use online resources. (Seriously, it's very obvious to us when this occurs, and there are drastic consequences, so don't do it!) If you use results that were not proved in class, please provide your own proof.

1. There is a variant of Gauss's lemma (sometimes called Eisenstein's lemma) that says that if p is an odd prime and q is an integer that is relatively prime to p, then we can express the Legendre symbol as

$$\left(\frac{q}{p}\right) = (-1)^{\mu},$$

where

$$\mu = \sum_{\substack{a=1 \\ a \text{ is even}}}^{p-1} \left\lfloor \frac{aq}{p} \right\rfloor.$$

(Recall that for any real number x, we write $\lfloor x \rfloor$ for the largest integer less than or equal to x.)

(a) (5 points) If $q = 2$, prove that

$$\mu = \begin{cases} (p-1)/4, & \text{if } p \equiv 1 \pmod 4 \\ (p+1)/4, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(b) (5 points) Using the previous part and Eisenstein's lemma, prove that

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & \text{if } p \equiv 1, 7 \pmod 8 \\ -1, & \text{if } p \equiv 3, 5, \pmod 8. \end{cases}$$

2. Prove the following trigonometric formula, which is used to give a proof of quadratic reciprocity: let m be an odd integer. Then

$$\frac{\sin mx}{\sin x} = (-4)^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \left(\sin^2 x - \sin^2 \frac{2\pi j}{m} \right).$$

Use the following steps:

(a) (5 points) Show that the left hand side of the inequality is a polynomial in $\sin^2 x$.

Another Hint: Th Euler/deMoivre formulas say that $e^{i\theta} = \cos\theta + i \sin\theta$ or equivalently $\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2}$ and $\sin\theta = \frac{e^{i\theta}-e^{-i\theta}}{2i}$. Using $a^m - b^m = (a-b)(a^{m-1} + a^{m-2}b + \cdots + b^{m-1})$, show that $\frac{\sin mx}{\sin x} = e^{i(m-1)x} + e^{i(m-3)x} + \cdots + e^{-i(m-1)x}$. All powers are even because m is odd. You can write $e^{i(m-1)x} + e^{-i(m-1)x} = \left(e^{2ix} + e^{-2ix}\right)^{(m-1)/2}$ + lower powers of $\left(e^{2ix} + e^{-2ix}\right)$. By induction all the terms can be replaced by powers of $\left(e^{2ix} + e^{-2ix}\right)$. But $e^{2ix} + e^{-2ix} =$

$2\cos(2x) = 2 - 4\sin^2 x$. So in the end you get a polynmoial in $\sin^2 x$ with highest power $(m-1)/2$.

(b) (5 points) Compute the degree of the polynomial, and show that $\sin^2 \frac{2\pi j}{m}$ with $j \in \{1, 2, \ldots, \frac{m-1}{2}\}$ are all of its roots.

(c) (10 points) Explain why the left hand side is a multiple of the right hand side. Find the multiple by plugging in a well-chosen value.

Another Hint: You can compare the coefficients of $e^{i(m-1)x}$ occuring in the Left Hand Side with the product in the Right Hand Side; it comes from $\sin^{m-1} x$ only.

3. Let p be an odd prime. Let $R_p = \{x + iy : x, y \in \mathbb{Z}/(p\mathbb{Z})\}$. The set R_p is equipped with an addition and multiplication:

$$(x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i(y_1 + y_2)$$
$$(x_1 + iy_1) \cdot (x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1).$$

The triple $(R_p, +, \cdot)$ consisting of a set with two binary operations is an example of a *ring*. A ring is a set which has a commutative addition and multiplication that satisfy the associativity and distributivity laws; it has a neutral additive element 0 ($0 = 0 + i0$ for our R_p); and a neutral multiplicative element 1 ($1 = 1 + i0$ for our R_p).

(a) (5 points) Show that if $p \equiv 1 \pmod 4$, then there are two nonzero elements $a, b \in R_p$ such that $a \cdot b = 0$.

Hint: $(x + iy)(x - iy) = x^2 + y^2$ ($i^2 = -1$). So you need to find $x, y \in \mathbb{Z}/(p\mathbb{Z})$ so that $x^2 + y^2 = 1$; use the fact that there is $\alpha \in \mathbb{Z}/(p\mathbb{Z})$ satisfying $\alpha^2 = -1$.

(b) (5 points) Show that if $p \equiv -1 \pmod 4$, then every nonzero element $a \in R_p$ has an inverse $a' \in R_p$.

Hint: Consider again the elements $x + iy$ and $x - iy$, and the relation $(x + iy)(x - iy) = x^2 + y^2$. This time show that $x^2 + y^2 = 0$ if and only if $x = y = 0$. Then divide by $x^2 + y^2$ to get the inverse.

(c) (10 points) For which p can you find an element $x + iy \in R_p$ such that $x^2 + y^2 = 1$ and $(x + iy)^2 = i$? (Note: $x^2 + y^2 = (x + iy)(x - iy)$ is called the *norm* of $x + iy$.)

4. (20 points) Using quadratic reciprocity, what is $(\frac{11}{q})$ for all odd primes q? (You should have a few different cases.)

5. (Extra Credit) For (10 points), deduce that there are infinitely many primes p such that $p \equiv 3 \pmod 8$. (Hint: Consider numbers of the form $N = (p_1p_2 \cdots p_m)^2 + 2$. When is $(\frac{-2}{p}) = 1$?)