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

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

Solution: Because $q = 2$, a is even, $aq \equiv 0 \pmod 4$.

When $p \equiv 1 \pmod 4$, $aq = p+3$ ($a = \frac{p+3}{2}$) is the first case $\left\lfloor \frac{aq}{p} \right\rfloor = 1$. And when $a = p-1$, $\left\lfloor \frac{aq}{p} \right\rfloor = \left\lfloor \frac{2(p-1)}{p} \right\rfloor = 1$. So

$$\mu = \sum_{\substack{a=(p+3)/2 \\ a \text{ is even}}}^{p-1} 1 = (p-1-(p+3)/2)/2 + 1 = (p-1)/4.$$

When $p \equiv 3 \pmod 4$, $aq = p+1$ ($a = \frac{p+1}{2}$) is the first case $\left\lfloor \frac{aq}{p} \right\rfloor = 1$. So

$$\mu = \sum_{\substack{a=(p+1)/2 \\ a \text{ is even}}}^{p-1} 1 = (p-1-(p+1)/2)/2 + 1 = (p+1)/4.$$

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

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

Solution:

$$\mu = \begin{cases} (p-1)/4 \equiv 0 \pmod 2, & \text{if } p \equiv 1 \pmod 8 \\ (p+1)/4 \equiv 0 \pmod 2, & \text{if } p \equiv 7 \pmod 8 \\ (p+1)/4 \equiv 1 \pmod 2, & \text{if } p \equiv 3 \pmod 8 \\ (p-1)/4 \equiv 1 \pmod 2, & \text{if } p \equiv 5 \pmod 8). \end{cases}$$

Because $\left(\frac{2}{p}\right) = (-1)^{\mu}$, we have

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

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 $(m-1)/2$.

Solution: We may write $\sin x$ in the form $\frac{e^{ix}-e^{-ix}}{2i}$. Recall that m is an odd integer. Thus

$$\frac{\sin mx}{\sin x} = \frac{\frac{e^{imx}-e^{-imx}}{2i}}{\frac{e^{ix}-e^{-ix}}{2i}} = \frac{e^{imx} - e^{-imx}}{e^{ix} - e^{-ix}} = e^{i(m-1)x} + e^{i(m-3)x} + \cdots + e^{-i(m-1)x},$$

where the last equality may be seen to be true by multiplication (and cancelation of terms). We may group opposite terms. Pick any odd k from 1 to m. In general we have that any sum of the form $c_{k-1}e^{i(k-1)x} + c_{k-3}e^{i(k-3)x} + \cdots + c_{-(k-1)}e^{-i(k-1)x}$, where the coefficients c_i are symmetric about c_0 (i.e. $k_\ell = k_{-\ell}$ for all ℓ), can be expressed as a sum of powers of $e^{ix} - e^{-ix}$: Simply subtract $c_{k-1}(e^{ix} - e^{-ix})^{k-1}$ from the sum, obtaining another sum with symmetric coefficients, but missing the terms at the ends, so by an induction argument the claim follows.

Evidently the highest power is $(e^{ix} - e^{-ix})^{k-1}$, and only even powers are needed (including possibly 0). It follows now that in our case the highest power of $e^{ix} - e^{-ix}$ is $m-1$, its coefficient is 1, and only even powers are present. Since $e^{ix} - e^{-ix} = 2i\sin(x)$, it follows that $\sin mx/\sin x$ is a polynomial in $(2i\sin(x))^2 = -4\sin^2 x$ and thus a polynomial in $\sin^2$.

(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.

Solution: From part (a) we have that the polynomial has degree $m-1$ in $e^{ix} - e^{-ix}$, thus degree $(m-1)/2$ in $(e^{ix} - e^{-ix})^2$, and thus also degree $(m-1)/2$ in $\sin^2 x$.

Let P_m be the polynomial in $\sin^2 x$. Then this means that $\sin mx/\sin x = P_m(\sin^2 x)$ for all x. If x is a root of $\sin mx/\sin x$, then $\sin^2 x$ is a root of P_m.

Observe that whenever x is a multiple of π/m, we have that $\sin mx = 0$. However, if x is also a multiple of π, then $\sin x = 0$ as well, and in fact we get by L'Hopital's rule (or whatever other method you want to use) that the function approaches (and if we fill in the missing value, equals) m or $-m$ at such points. (In particular, it is not 0.) However, $\pi j/m$ for j from 1 to $(m-1)/2$ (or really up through $m-1$) are all roots of $\sin mx/\sin x$. Moreover, $\sin^2(\pi j/m)$ is distinct for each of these values of j up to $(m-1)/2$ (since $\sin^2 x$ is increasing from 0 up through $(1/2)\pi$). We have thus found $(m-1)/2$ distinct roots of the polynomial. Since we have shown that the polynomial has degree $(m-1)/2$, it follows that these are all the 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.

Solution: From part (b), we know that the roots of the polynomial are precisely $\sin^2(\pi j/m)$ for $j = 1, \ldots, (m-1)/2$. Thus $\sin mx/\sin x$ must be a constant multiple of $\prod_{j=1}^{(m-1)/2}(\sin^2 x - \sin^2(\pi j/m))$. We know by part (a), second-to-last sentence, that the leading term of $\sin mx/\sin x$, when written as a polynomial in $-4\sin^2 x$, is 1. Thus as a polynomial in $\sin^2 x$ it has leading coefficient $(-4)^{(m-1)/2}$. We conclude that multiple of the product $\prod_{j=1}^{(m-1)/2}(\sin^2 x - \sin^2(\pi j/m))$, which by itself would have leading coefficient 1, must be $(-4)^{(m-1)/2}$.

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 $\alpha^2 = -1$.

Solution: When $p \equiv 1 \pmod 4$,

$$p - 1 \equiv 0 \pmod 4 \Rightarrow \frac{p-1}{2} \equiv 0 \pmod 2.$$

Thus $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$. There exists element $\alpha \in \mathbb{Z}/(p\mathbb{Z})$ s.t. $\alpha^2 = -1$ in $\mathbb{Z}/(p\mathbb{Z})$. Let $x = 1$, $y = \alpha$, $a = x + iy$, $b = x - iy$, we have

$$a \cdot b = x^2 + y^2 = 1 + -1 = 0.$$

(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.

Solution: First we show that for $x, y \in \mathbb{Z}/(p\mathbb{Z})$, $x^2 + y^2 = 0$ if and only if $x = y = 0$:

When $x = y = 0$, it is obvious that $x^2 + y^2 = 0$.
When $x^2+y^2 = 0$, if $x = 0$, we have $y^2 = 0$, and thus $y = 0$. If $x \neq 0$, we have $y^2 = -x^2 \neq 0$. On one hand, we know

$$\left(\frac{y^2}{p}\right) = 1$$

On the other hand,

$$\left(\frac{y^2}{p}\right) = \left(\frac{-x^2}{p}\right) = (-x^2)^{(p-1)/2} = (-1)^{(p-1)/2} \cdot \left(\frac{x^2}{p}\right) = -1 \cdot 1 = -1.$$

Therefore, we proved $x^2 + y^2 = 0$ if and only if $x = y = 0$.

For all $a = x + iy \in R_p$, let $b = (x^2 + y^2)^{-1}(x - iy)$, then

$$a \cdot b = (x^2 + y^2)^{-1}(x^2 + y^2) = 1$$

(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 $x + iy$.)

Solution: Let $g = x + iy$. Because $(x + iy)(x - iy) = x^2 + y^2 = 1$, $g^{-1} = x - iy$. Because $g^2 = i$, $g^8 = 1$.

We claim

$$(2x)^2 = (g + g^{-1})^2 = g^2 + g^{-2} + 2 = 2.$$

This is because

$$g^2(g^2 + g^{-2}) = g^4 + 1 = -1 + 1 = 0 \Rightarrow g^2 + g^{-2} = 0.$$

Consider $(g + g^{-1})^p$, on one hand, we have

$$(g + g^{-1})^p = (2x)^p = 2x$$

One the other hand, suppose $p \equiv r \pmod 8$, where $r \in \{1, 3, -3, -1\}$. Because $g^8 = 1$, we have $g^p = g^r$. Then

$$(g + g^{-1})^p = g^p + g^{-p} = g^r + g^{-r}$$

If $r = \pm 1$,

$$g^r + g^{-r} = g + g^{-1} = 2x$$

If $r = \pm 3$,

$$g^r + g^{-r} = g^3 + g^{-3} = g^4 \cdot g^{-1} + g^{-4}g = -g^{-1} - g = -2x \neq 2x$$

Therefore, $p \equiv \pm 1 \pmod 8$.

We prove $p \equiv \pm 1 \pmod 8$ is sufficient by finding $\zeta \in \mathbb{F}_{p^2}^\times$ of order p^2-1, and let $g = \zeta^{\frac{p^2-1}{8}}$. Then $g^2 = i$. Next, we can prove $2x = g+g^{-1} \in \mathbb{F}_p$ and $-2y = i(g-g^{-1}) = g^2(g-g^{-1}) \in \mathbb{F}_p$ by showing

$$(2x)^p = g^p + g^{-p} = g + g^{-1} = 2x$$
$$(-2y)^p = g^{2p}(g - g^{-1})^p = g^2(g^p - g^{-p}) = -2y.$$

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

Solution:

$$\left(\frac{11}{q}\right) = (-1)^{(11-1)(q-1)/4}\left(\frac{q}{11}\right) = (-1)^{(q-1)/2}\left(\frac{q}{11}\right)$$

$$(-1)^{(q-1)/2} = \begin{cases} 1, & \text{if } q \equiv 1 \pmod 4, \\ -1 & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

$$\left(\frac{q}{11}\right) = \begin{cases} 0, & \text{if } q = 11, \\ 1, & \text{if } q \equiv 1, 3, 4, 5, 9 \pmod{11}, \\ -1, & \text{if } q \equiv 2, 6, 7, 8, 10 \pmod{11}. \end{cases}$$

Considering the congruence modulo 44, we have

$$\left(\frac{11}{q}\right) = \begin{cases} 0, & \text{if } q = 11, \\ 1, & \text{if } q \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}, \\ -1, & \text{if } q \equiv 3, 11, 13, 17, 21, 23, 27, 29, 31, 33, 41 \pmod{44}. \end{cases}$$

Comment: The case $q = 11$ should be included.

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 $N = (p_1 p_2 \cdots p_m)^2 + 2$. When is $(\frac{-2}{p}) = 1$?)

Solution: Suppose for the sake of contradiction that there are only finitely many primes primes $p_1, \ldots, p_m$ congruent to 3 mod 8. Set $N = (p_1 p_2 \cdots p_m)^2 + 2$. Let q be any prime dividing q. Then $(p_1 p_2 \cdots p_m)^2 \equiv -2 \pmod q$. Certainly q is an odd prime. But by problem 1 we have that $\left(\frac{2}{q}\right)$ is 1 if q is congruent to 1 or 7 mod 8 and is -1 if 1 is congruent to 3 or 5. By a result proved earlier we also know that $\left(\frac{-1}{q}\right) = 1$ if q is congruent to 1 mod 4 and that $\left(\frac{-1}{q}\right) = -1$ if q is congruent to 3 mod 4. It follows that the product $\left(\frac{-2}{q}\right)$ equals 1 if and only if q is congruent to 1 or to 3 mod 8.

Since we know that -2 is in fact a square mod q, it follows that either $q \equiv 1 \pmod 8$ or $q \equiv 3 \pmod 8$. If the first possibility held for all prime divisors q of N, it would follow that N itself was congruent to 1 mod 8, but this is impossible as $(p_1 p_2 \cdots p_n)^2$ is, by virtue of being a square of an odd number, congruent to 1 mod 8 (check the 4 cases), and thus N is congruent to 3 mod 8. It follows that for some q dividing N, we have $q \equiv 3 \pmod 8$. But $p_1, \ldots, p_n$ were allegedly the only primes of this form, implying that q equals one of them and thus divides $(p_1 p_2 \cdots p_n)^2$. We therefore obtain $q|2$, contradiction.