HOMEWORK ASSIGNMENT #9 SOLUTIONS

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

Solution. For $\sin 3x$, we have $e^{3ix} = \cos 3x + i \sin 3x = (e^{ix})^3 = (\cos x + i \sin x)^3$. So we will expand $(\cos x + i \sin x)^3$ using the binomial theorem, find the imaginary part, and then write that as a polynomial in $\sin x$:

$$(\cos x + i \sin x)^3 = \cos^3 x + 3i \cos^2 x \sin x - 3 \cos x \sin^2 x - i \sin^3 x.$$

This has imaginary part $3 \cos^2 x \sin x - \sin^3 x$. Since $\cos^2 x = 1 - \sin^2 x$, this is the same as $3(1 - \sin^2 x) \sin x - \sin^3 x = -4 \sin^3 x + 3 \sin x$.

As for $\sin 5x$, the binomial theorem is slightly more painful, but we get

$$(\cos x+i \sin x)^5 = \cos^5 x+5i \cos^4 x \sin x-10 \cos^3 x \sin^2 x-10i \cos^2 x \sin^3 x+5 \cos x \sin^4 x+i \sin^5 x.$$

This has imaginary part $5 \cos^4 x \sin x - 10 \cos^2 x \sin^3 x + \sin^5 x$. Using $\cos^2 x = 1 - \sin^2 x$, this gives

$$\sin 5x = 5(1 - \sin^2 x)^2 \sin x - 10(1 - \sin^2 x) \sin^3 x + \sin^5 x = 16 \sin^5 x - 20 \sin^3 x + 5 \sin x. \square$$

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 $m = p_1^{e1} \dots p_r^{er}$ 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 $\gcd(a, m) > 1$.

Solution. From the definition of the Jacobi symbol, $\left(\frac{a}{m}\right) = \prod \left(\frac{a}{p_i}\right)^{e_i}$. This product is equal to 0 if and only if at least one of the $\left(\frac{a}{p_i}\right)$ is equal to 0, and this happens if and only if $p_i \mid a$. So $\left(\frac{a}{m}\right) = 0$ if and only if $p_i \mid a$ for some p_i, which is the same as saying $\gcd(a, m) > 1$.

(b) If $a \equiv b \mod m$, show that $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.

Solution. If $a \equiv b \mod m$, then $a \equiv b \mod p_i$ for every prime divisor p_i of m. Therefore, $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$, and so looking at the definition of the Jacobi symbol this means $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.

(c) If m, n are positive odd integers, show that $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.

Solution. This is obvious from the definition of the Jacobi symbol.

(d) Show that if $\left(\frac{a}{m}\right) = -1$, then a is a quadratic non-residue mod m.

Solution. If $\left(\frac{a}{m}\right) = -1$, then $\gcd(a, m) = 1$ from part (a). Next, $\left(\frac{a}{m}\right) = -1$ implies that $\left(\frac{a}{p_i}\right) = -1$ for some prime divisor p_i of m, but this means that a

is a quadratic non-residue mod p_i, and therefore cannot be a quadratic residue mod m. (Recall that a is a quadratic residue mod m if and only if it is so every $p_i^{e_i}$, and since all p_i are odd, this is the same as being a quadratic residue mod p_i.)

(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.

Solution. Perhaps the simplest example is $a = 2, m = 9$; 2 is not a quadratic residue mod 9 because it is not so mod 3 (or you can just check this using brute force), but $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = 1$. □

(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

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

Solution.

$$\left(\frac{ab}{m}\right) = \prod_{p_i}\left(\frac{ab}{p_i}\right)^{e_i} = \prod_{p_i}\left(\left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)\right)^{e_i} = \prod_{p_i}\left(\frac{a}{p_i}\right)^{e_i}\prod_{p_i}\left(\frac{b}{p_i}\right)^{e_i} = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$

The first equality is the definition of the Jacobi symbol, the second is the multiplicative property of the Legendre symbol, the third is just reordering the terms in the product, and the last is again the definition of the Jacobi symbol.

(b)

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

Solution. Recall that $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \mod 4$, and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv 3 \mod 4$. It is easy to see that $(-1)^{\frac{m-1}{2}} = 1$ if and only if $m \equiv 1 \mod 4$, and is -1 if and only if $m \equiv 3 \mod 4$.

We will slightly adjust notation, and let $m = p_1 p_2 \dots p_r$, where now the p_i do not have to be distinct. Then it is still true that

$$\left(\frac{-1}{m}\right) = \prod_{p_i}\left(\frac{-1}{p_i}\right),$$

since if the prime p appears e times in the list $p_1, \dots, p_r$, then the symbol $\left(\frac{-1}{p}\right)$ appears exactly e times in the product on the right hand side.

Suppose exactly N of the primes, say $p_1, \dots, p_N$ (which is possible after relabeling) are congruent to $3 \mod 4$. Then $\left(\frac{-1}{m}\right) = (-1)^N$, since these N primes are exactly the primes p_i which satisfy $\left(\frac{-1}{p_i}\right) = -1$. On the other hand, the product $p_1 \dots p_r = m$ is congruent to 3 mod 4 exactly when N is odd, because $m = p_1 \dots p_r \equiv 3^N \cdot 1^{r-N} \equiv (-1)^N \mod 4$, and this is equivalent to $3 \equiv -1$ mod 4 exactly when N is odd. Therefore $(-1)^N = -1$ if and only if N is odd, which is true if and only if $m \equiv 3 \mod 4$. Since $\left(\frac{-1}{m}\right) = (-1)^N = -1$ if and only if $m \equiv 3 \mod 4$, and $(-1)^{\frac{m-1}{2}} = -1$ if and only if $m \equiv 3 \mod 4$, this proves what we wanted to show. □

(c)

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

Solution. Recall that $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1, 7 \mod 8$, and $\left(\frac{2}{p}\right) = -1$ if $p \equiv 3, 5 \mod 8$. It is easy to see that $(-1)^{\frac{m^2-1}{8}} = 1$ if and only if $m \equiv 1, 7 \mod 8$, and is -1 if and only if $m \equiv 3, 5 \mod 8$.

Like before, we will slightly adjust notation, and let $m = p_1 p_2 \dots p_r$, where now the p_i do not have to be distinct. Then it is still true that

$$\left(\frac{2}{m}\right) = \prod_{p_i} \left(\frac{2}{p_i}\right),$$

since if the prime p appears e times in the list $p_1, \dots, p_r$, then the symbol $\left(\frac{2}{p}\right)$ appears exactly e times in the product on the right hand side. Notice that the product of any two numbers congruent to $1, 7 \equiv \pm 1 \mod 8$ is still $\pm 1 \mod 8$, and the product of any two numbers congruent to $3, 5 \mod 8$ is also $\pm 1 \mod 8$. On the other hand, the product of a number congruent to 1 or 7 mod 8 with a number congruent to 3 or 5 mod 8 will be $3, 5 \mod 8$.

Suppose exactly N of the primes $p_1, \dots, p_r$, say $p_1, \dots, p_N$ (which is possible after reordering) are congruent to 3 or 5 mod 8. Then $\left(\frac{2}{m}\right) = (-1)^N$. On the other hand, the product of these N primes is $\equiv 3, 5 \mod 8$ if and only if N is odd. Since $p_{N+1} \dots p_r$, the product of the remaining primes in the factorization of m, is still congruent to $1, 7 \mod 8$, being the product of primes congruent to $1, 7 \mod 8$, we see that $m \equiv 3, 5 \mod 8$ if and only if N is odd. But N is odd if and only if $(-1)^N = -1 = \left(\frac{2}{m}\right)$. This is what we wanted to prove. □

(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.)

Solution. Let $m = p_1 \dots p_r, n = q_1 \dots q_s$, where the p_i are not necessarily distinct and the q_s are also not necessarily distinct. Nevertheless, because m, n are relatively prime, none of the p_i equal any of the q_j, and of course all the p, qs are odd. Therefore, we can manipulate all Legendre symbols $\left(\frac{q_j}{p_i}\right), \left(\frac{p_i}{q_j}\right)$ using quadratic reciprocity.

First, notice that

$$\left(\frac{m}{n}\right) = \prod_{p_i, q_j} \left(\frac{p_i}{q_j}\right),$$

where the product runs over all the r primes p_i and s primes q_j. This is true from the definition of the Jacobi symbol in terms of the Legendre symbol, and because of the property $\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right)$.

In a similar fashion,

$$\left(\frac{n}{m}\right) = \prod_{p_i, q_j} \left(\frac{q_j}{p_i}\right),$$

so taking the the product of these two expressions for $\left(\frac{m}{n}\right), \left(\frac{n}{m}\right)$, we get

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{p_i, q_j} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right).$$

Because the q, p are distinct odd primes, we can use quadratic reciprocity for Legendre symbols to evaluate each term in this product. Namely,

$$\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = -1$$

if and only if both $p_i, q_j \equiv 3 \mod 4$, and is congruent to 1 otherwise. Let us count the number of such products $\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$ equal to -1. Suppose exactly M of the primes $p_1, \ldots, p_r$ are congruent to 3 mod 4, and suppose that exactly N of the primes $q_1, \ldots, q_s$ are congruent to 3 mod 4. Then exactly MN of the products $\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$ equal -1, because there are M choices for p_i and N choices for q_j making this true. Therefore

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

On the other hand, $(-1)^{\frac{m-1}{2}\frac{n-1}{2}} = -1$ if and only if both $m \equiv 3 \mod 4, n \equiv 3 \mod 4$. So we want to show that MN is odd if and only if both $m \equiv 3 \mod 4, n \equiv 3 \mod 4$. But MN is odd if and only if both M, N are odd, and for instance, M is odd if and only if $m \equiv 3 \mod 4$, since $m = p_1 \ldots p_r \equiv 3^M 1^{r-M} \equiv (-1)^M \mod 4$, so that $m \equiv 3 \equiv -1 \mod 4$ if and only if M is odd. Therefore MN is odd if and only if both M, N are odd if and only if $m, n \equiv 3 \mod 4$, as desired. □

(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.

Solution. First we need to factor 713. Trial division shows that $713 = 23 \cdot 31$. Therefore we want to check whether 693 is a quadratic residue mod $23, 31$. For instance, mod 31, $\left(\frac{693}{31}\right) = \left(\frac{11}{31}\right)$, because $693 = 31 \cdot 22 + 11$, and $\left(\frac{11}{31}\right) = -\left(\frac{31}{11}\right)$ by quadratic reciprocity. Since $-\left(\frac{31}{11}\right) = -\left(\frac{9}{11}\right)$, and $\left(\frac{9}{11}\right) = 1$ (because $\gcd(9, 11) = 1$ and 9 is a square mod 11), this shows that 693 is not a quadratic residue mod 31, and hence is not a quadratic residue mod 713.

(b) Using Jacobi symbols, determine whether 693 is a quadratic residue mod 713 or not. Which method was faster?

Solution. Using Jacobi symbols, and the properties proven earlier, with the fact that $713 \equiv 1 \mod 4$, say,

$$\left(\frac{693}{713}\right) = \left(\frac{713}{693}\right) = \left(\frac{20}{693}\right) = \left(\frac{4}{693}\right)\left(\frac{5}{693}\right) = \left(\frac{5}{693}\right) = \left(\frac{693}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

The Jacobi symbol of 693 mod 713 is -1, and we showed earlier that if this is so then 693 is not a quadratic residue mod 713.

This method seems faster than using Legendre symbols, because we did not have to factor 713, nor did we have to work as hard when calculating Euclidean divisions (contrast 713 by 693 versus 693 by 31.)

For the last two questions you should write a paragraph or two. There is no 'correct' answer, but you should 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).

Solution. Obviously these two problems had no right or wrong answer. The intent of these questions was for you to reflect on what we covered throughout the term and perhaps think about things which might interest you for further study. The webpage will soon have more information on resources or classes you might be interested in taking if you wish to learn more number theory.