Quadratic Reciprocity
Class activity, Week 10

Proposition: The quadratic modular congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

where p is an odd prime and $\gcd(a, p) = 1$, has a solution if and only if $y^2 \equiv b^2 - 4ac \pmod{p}$ has a solution. The solutions are then given by $x = (2a)^{-1}(-b \pm y)$ where y is a solution to $y^2 \equiv b^2 - 4ac \pmod{p}$.

proof: Since p is odd, we also have $\gcd(4a, p) = 1$. Therefore, solving $ax^2+bx+c \equiv 0 \pmod{p}$ is equivalent to solving $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$, which can be rewritten as $(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$. Suppose we have a solution y to $y^2 \equiv (b^2 - 4ac) \pmod{p}$. Then $y \equiv 2ax + b \pmod{p}$ and we can solve for x to obtain $x = (2a)^{-1}(-b \pm y)$ as the two solutions for our original equation.

Now let's focus back on which numbers modulo n have square roots, in other words, which numbers are quadratic residues.

Legendre Symbol

Recall how we defined the *Legendre symbol*:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p}, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

This notation will provide us with easy means of finding whether a given integer is a quadratic residue or not modulo p.

Note that we can rewrite Euler's criterion from previous week using the Legendre symbol as follows:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}\,.$$

Properties of the Legendre symbol: For p an odd prime,

i. $\left(\frac{0}{p}\right) = 0$ (by definition).

ii. $\left(\frac{1}{p}\right) = 1$ because _____.

iii. $\left(\frac{a^2}{p}\right) = 1$ because _____.

iv. $\left(\frac{-1}{p}\right) = 1$ for $p =$ _____ and $\left(\frac{-1}{p}\right) = -1$ for $p =$ _____. (By Theorem 5 of Week 8 class activity)

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

proof: From Euler's criterion, $\left(\frac{ab}{p}\right) =$ _____ $\equiv$ _____ . Therefore, $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = kp$ for some integer k. But by definition of the Legendre symbol, the only possible values for the left hand side of this equality are _____. Since p is an odd prime > 2, $k = 0$, and

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

vi. If we add the $\left(\frac{a}{p}\right)$ values for all distinct a modulo p, then we obtain 0.

proof:

1. Using the properties of the Legendre symbol, simplify and evaluate $\left(\frac{169}{347}\right), \left(\frac{-25}{101}\right), \left(\frac{193}{337}\right)$.

Quadratic Reciprocity

We will now see a remarkable relationship between the Legendre symbol values of two primes with respect to each other, hence leading to a practical method of determining the Legendre symbol values.

The first result we prove relates $\left(\frac{a}{p}\right)$ to the number of certain residue classes. We first calculate these numbers for specific a and p values to get concrete examples.

Given $a \pmod p$, we first find the least residues of $a, 2a, \ldots, \frac{p-1}{2}a$. Note that there are $\frac{p-1}{2}$ total numbers in this list, and no two numbers are equivalent modulo p. To see this, observe that $ia \equiv ja \pmod p$ means $p|(j-i)a$. But since a is relatively prime to p, this means $p|j-i$, which is a contradiction since $1 \leq i, j \leq \frac{p-1}{2}$.

We then count those numbers in the list $a, 2a, \ldots, \frac{p-1}{2}a$ which when reduced to the least residue, gives a number greater than $\frac{p}{2}$. Let us suppose there are s many such numbers. The first result we will prove claims that $\left(\frac{a}{p}\right) = (-1)^s$.

As an example, consider $a = 3$ and $p = 7$. We first need to find multiples $a \cdot k$ for $k = 1$ to $\frac{p-1}{2}$ and reduce them modulo p, so the numbers we are looking to reduce are $3, 6, 9$. When reduced to the least residue, we get $3, 6, 2$. Since $p/2 = 3.5$, there is only one number in the list with least residue greater than 3.5; so $s = 1$. Therefore, $\left(\frac{3}{7}\right) = (-1)^s = -1$, which is correct since 3 is not a quadratic residue modulo 7.

As another example, consider $a = 4$ and $p = 11$. We first find multiples of a up to the $\frac{p-1}{2}$ multiple: $4, 8, 12, 16, 20$. Then reduce them modulo p: $4, 8, 1, 5, 9$. Among these, we find those greater than $p/2$, which is 5.5 in this case: $8, 9$. Therefore, $s = 2$, and $\left(\frac{3}{7}\right) = (-1)^s = 1$, which is true because $a = 4$ is clearly a quadratic residue.

2. For each of the following parts, first determine the value of $\left(\frac{a}{p}\right)$ by finding whether a is a square modulo p. Then determine the value of s as described above, and check that $\left(\frac{a}{p}\right) = (-1)^s$.

a. $a = 2$ and $p = 7$

b. $a = 3$ and $p = 11$

c. $a = 2$ and $p = 11$

Theorem 1: (Gauss's Lemma) Let p be an odd prime, and a relatively prime to p. Let S_a be the set of least residues of the integers $a, 2a, 3a, \ldots, \frac{p-1}{2}a$. Let s be the number of elements in S_a which are greater than $\frac{p}{2}$. Then

$$\left(\frac{a}{p}\right) = (-1)^s .$$

proof: (Can be omitted.) Recall that from Euler's criterion,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} .$$

So it is enough to show that $(-1)^s \equiv a^{(p-1)/2} \pmod{p}$.

From the definition of S_a, if we multiply all the elements in S_a and reduce modulo p, we will get

$$\left(\frac{p-1}{2}\right)! \cdot a^{(p-1)/2} \pmod{p} .$$

We can first reduce each element in S_a and then multiply them as another way to obtain this same answer. Note that there are a total of $\frac{p-1}{2}$ elements in S_a. Let $b_1, b_2, \ldots, b_s$ be the elements whose least residues are greater than $p/2$, and let $\ell_1, \ell_2, \ldots, \ell_t$ be those whose least residues are less than $p/2$. Instead of b_i's, we will consider $p - b_i$'s, because $0 < p - b_i < p/2$. We claim that $p - b_i$'s along with the ℓ_j's will cover all possible residues between 0 and $p/2$. We already know that ℓ_j's and $p - b_i$'s are different among themselves. We also need $p - b_i \neq \ell_j$ for any i, j. Suppose this is not true, assume $p - b_i = \ell_j$ for some i, j. We will reach a contradiction. From the way we defined b_i and ℓ_j, this means that $p - m_i a \equiv m_j a \pmod{p}$ for some m_i, m_j satisfying $0 < m_i, m_j \leq \frac{p-1}{2}$. Rewriting, we find $p|(m_j - m_i)a$. As before, since a is relatively prime to p, this cannot happen with $0 < m_i, m_j \leq \frac{p-1}{2}$.

Now that we showed that the elements $p - b_1, p - b_2, \ldots, p - b_s$ along with $\ell_1, \ell_2, \ldots, \ell_t$ form all the elements from 1 to $(p-1)/2$, we can consider the product of all elements in S_a in a different way.

$$\ell_1 \cdot \ell_2 \cdots \ell_t \cdot b_1 \cdot b_2 \cdots b_s \equiv (-1)^s \ell_1 \cdot \ell_2 \cdots \ell_t \cdot (p - b_1) \cdot (p - b_2) \cdots (p - b_s) \equiv (-1)^s \left(\frac{p-1}{2}\right)! \pmod{p}$$

because $p - b_i$'s along with ℓ_j's cover all elements from 1 to $(p-1)/2$. The two answers for calculating the product of all elements in S_a should be equal modulo p, therefore,

$$\left(\frac{p-1}{2}\right)! \cdot a^{(p-1)/2} \equiv (-1)^s \left(\frac{p-1}{2}\right)! \pmod{p} .$$

Canceling $\left(\frac{p-1}{2}\right)!$ from both sides (justify why we can do this), we find that

$$a^{(p-1)/2} \equiv (-1)^s \pmod{p} ,$$

which is what we wanted to show. Hence, this finishes the proof of the theorem.

□

3. Let us apply Theorem 1 to find the value of $\left(\frac{2}{p}\right)$.

a. Find $\left(\frac{2}{p}\right)$ for $p = 13, 17, 19, 23, 41$ using Theorem 1.

b. Now consider p of the form $p = 1 + 8k$. In your above list, 17 and 41 were both of this type. What is the s as defined in the proof of Theorem 1 for $a = 2$? What do you conclude the value of $\left(\frac{2}{p}\right)$ is?

c. Repeat part b if p is of the form $p = 3 + 8k$.

d. Repeat part b if p is of the form $p = 5 + 8k$.

e. Repeat part b if p is of the form $p = 7 + 8k$.

Putting your results together in one theorem, we find that:

Theorem 2: Let p be an odd prime. Then $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 8$. Equivalently, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

We can use Theorem 1 to also come up with a relationship between $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ for two different odd primes, which is the famous Quadratic Reciprocity (QR). Using QR along with Theorem 2, and using the property that the Legendre symbol is multiplicative, we can calculate the Legendre symbol effectively.

Theorem 3: (Quadratic Reciprocity) Let p and q be distinct odd primes. Then

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

The proof of QR is achieved by using counting manipulations similar to the proof of Gauss's Lemma, which we will not do here. Instead let's see how we can evaluate Legendre symbol efficiently using QR.

Let $p = 19$ and $q = 283$. From QR, we have

$$\left(\frac{19}{283}\right)\left(\frac{283}{19}\right) = (-1)^{(282)(18)/4}.$$

Note that $\left(\frac{283}{19}\right) = \left(\frac{17}{19}\right)$ because $283 \equiv 17 \pmod{19}$. We can find the quadratic residues modulo 19 via trial-error, and see that 17 is a quadratic residue. Therefore, $\left(\frac{17}{19}\right) = 1$. Also simplifying the right hand side, $(-1)^{282\cdot 18/4} = -1$. So we have

$$\left(\frac{19}{283}\right) \cdot 1 = -1.$$

Therefore, 19 is a quadratic nonresidue modulo 283.

4. Use QR and possibly Theorem 2 and possibly the multiplicativity of the Legendre symbol to determine the following. (Note: You may need to use QR more than once.)

a. $\left(\frac{11}{31}\right)$

b. $\left(\frac{41}{103}\right)$

c. $\left(\frac{42}{997}\right)$

d. $\left(\frac{101}{103}\right)$

e. Determine the value of $\left(\frac{3}{p}\right)$.