Quadratic Residues Worksheet

Recap

Let p be an odd prime and let a be an integer with $\gcd(a, p) = 1$.We say that a is a *quadratic residue modulo* p if there exists an integer x such that

$$x^2 \equiv a \pmod{p}.$$

Otherwise, a is called a *quadratic non-residue modulo* p. We keep track of this via the *Legendre symbol*, which is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

A computationally efficient method to compute the Legendre symbol is **Euler's Criterion,** which says that

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

We also have **Gauss's Lemma:** Define $\mu(a, p)$ to be the number of elements among $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ whose least residue modulo p lies in the interval $(-p/2, 0)$. Then

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

Finally, we have a **Counting Lemma:** If a is odd, then

$$\mu(a, p) \equiv T(a, p) \pmod{2} \qquad \text{where} \qquad T(a, p) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor = \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor 2 \cdot \frac{a}{p} \right\rfloor \cdots + \left\lfloor \frac{p-1}{2} \cdot \frac{a}{p} \right\rfloor$$

Warmup problems

1. This is a good place to start if you would like to refresh yourself on the definitions.

   (a) For each $a \in \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, find a 'square root' of a in $\mathbb{Z}_7$. In other words, find a solution to the congruence equation $x^2 \equiv a \pmod 7$ or say why there isn't any!

   (b) Compute the following Legendre symbols:

   $$\left(\frac{101}{17}\right), \quad \left(\frac{17}{101}\right), \quad \left(\frac{7}{11}\right), \quad \left(\frac{11}{7}\right), \quad \left(\frac{7}{19}\right).$$

   (c) Find all quadratic residues modulo 11.

   (d) For which primes $p \leq 31$ is 11 a quadratic residue modulo p?

2. Now we get to work with $\mu(a, p)$ and $T(a, p)$!

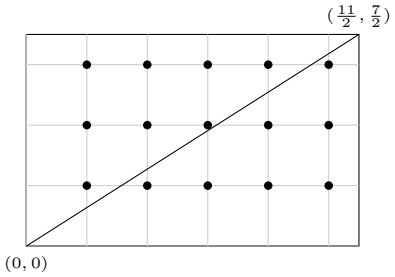
   (a) Compute $\mu(a, p)$ for the following pairs:

   $$(a, p) = (7, 11), \quad (11, 7), \quad (5, 13), \quad (7, 17).$$

   (b) For each example above, compute $T(a, p)$ and verify that $\mu(a, p) \equiv T(a, p) \pmod 2$ in each case.

Counting dots!

3. Consider the rectangle with corners $(0,0)$ and $\left(\frac{11}{2}, \frac{7}{2}\right)$.



   (a) How many integer lattice points lie **inside** this rectangle (do not include points on the perimeter)?

   (b) Consider the points lying *below* the diagonal line from $(0,0)$ to $\left(\frac{11}{2}, \frac{7}{2}\right)$. Show that this number is equal to $T(7,11)$ by counting the number of points in each column.

   (c) Now consider the points lying *above* this diagonal. Show that this number is related to $T(11,7)$.

4. Let p and q be distinct odd primes.

   (a) Find the number of lattice points inside a rectangle with corners $(0,0)$ and $\left(\frac{p}{2}, \frac{q}{2}\right)$. (Again, do not count points on the boundary.)

   (b) How many lattice points inside the rectangle lie below the diagonal?

   (c) How many lattice points inside the rectangle lie above the diagonal?

   (d) Find a formula for $(-1)^{\mu(p,q)+\mu(q,p)}$ in terms of p, q only. (*Hint:* Use the counting lemma.)

Computation and conjectures

5. Recall that in class, we made a conjecture that for any odd prime p, $(\frac{5}{p}) = (\frac{p}{5})$. Prove the conjecture using some of the results from the previous section! (If you get stuck trying to prove this, compile some data to support the conjecture.)

6. (a) For each odd prime $p \leq 31$, compute $(\frac{7}{p})$ and $(\frac{p}{7})$. From your data, guess a formula for $\left(\frac{7}{p}\right)$ in terms of $p \bmod 7$.

   (b) Conjecture a formula for $(\frac{7}{p})$ in terms of $(\frac{p}{7})$. Verify that it holds in your examples, and prove your formula!

7. Make a conjecture relating $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ for odd primes p, q.