110AH Section Worksheet 2

Warm-up. Recall from last week that for fixed integers a, b, c, the equation $ax + by = c$ has an integer solution (x_0, y_0) if and only if $\gcd(a, b) \mid c$ and that the solutions are then

$$(x_0, y_0) + \frac{k}{\gcd(a, b)}(b, a) \qquad \text{for } k \in \mathbb{Z}.$$

Use this to do the following:

- Find the solutions $X \in \mathbb{Z}/b\mathbb{Z}$ to $[a]X = [c]$ given a solution $X_0 \in \mathbb{Z}/b\mathbb{Z}$.
- Find the image of the multiplication-by-a map $X \mapsto [a]X$ on $\mathbb{Z}/b\mathbb{Z}$.

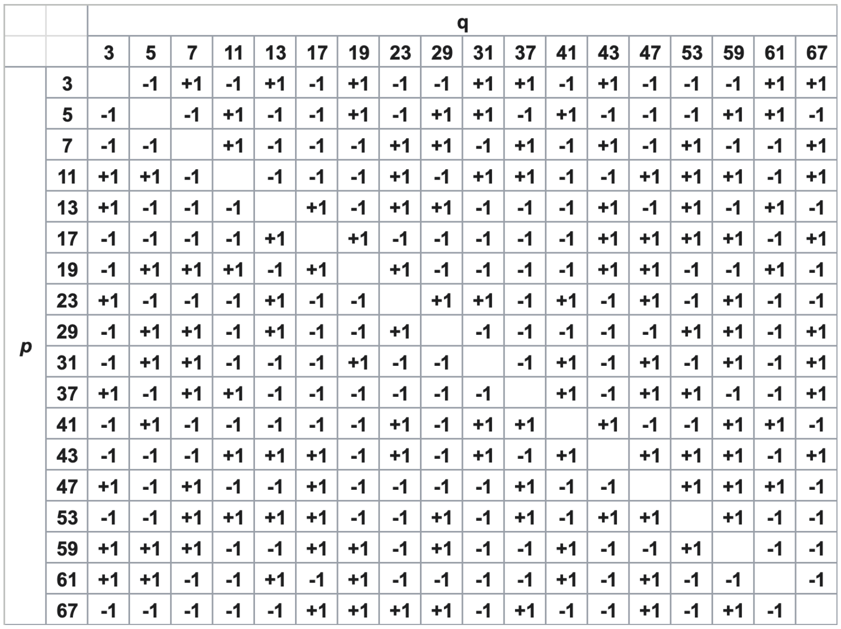
Legendre symbol. Let p be an odd prime. The *Legendre symbol* is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ is a square in } \mathbb{Z}/p\mathbb{Z} \\ -1 & a \text{ is not a square in } \mathbb{Z}/p\mathbb{Z} \end{cases}$$

for $p \nmid a \in \mathbb{Z}$. Fill out the rest of the following table of Legendre symbols. Show that the Legendre symbol is multiplicative, i.e. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. *Hint*: there are the same number of squares and nonsquares in $(\mathbb{Z}/p\mathbb{Z})^*$.

	1	2	3	4	5	6	7	8	9	10	11	12
3	$+1$	-1		$+1$	-1		$+1$	-1		$+1$	-1	
5												
7												
11												
13												

Quadratic reciprocity. Here is a filled-in larger table of Legendre symbols $\left(\frac{q}{p}\right)$ for q prime. Conjecture a relationship between $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$.



		q																	
		3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67
p	3		-1	+1	-1	+1	-1	+1	-1	-1	+1	+1	-1	+1	-1	-1	-1	+1	+1
	5	-1		-1	+1	-1	-1	+1	-1	+1	+1	-1	+1	-1	-1	-1	+1	+1	-1
	7	-1	-1		+1	-1	-1	-1	+1	+1	-1	+1	-1	+1	-1	+1	-1	-1	+1
	11	+1	+1	-1		-1	-1	-1	+1	-1	+1	+1	-1	-1	+1	+1	+1	-1	+1
	13	+1	-1	-1	-1		+1	-1	+1	+1	-1	-1	-1	+1	-1	+1	-1	+1	-1
	17	-1	-1	-1	-1	+1		+1	-1	-1	-1	-1	-1	+1	+1	+1	+1	-1	+1
	19	-1	+1	+1	+1	-1	+1		+1	-1	-1	-1	-1	+1	+1	-1	-1	+1	-1
	23	+1	-1	-1	-1	+1	-1	-1		+1	+1	-1	+1	-1	+1	-1	+1	-1	-1
	29	-1	+1	+1	-1	+1	-1	-1	+1		-1	-1	-1	-1	-1	+1	+1	-1	+1
	31	-1	+1	+1	-1	-1	-1	+1	-1	-1		-1	+1	-1	+1	-1	+1	-1	+1
	37	+1	-1	+1	+1	-1	-1	-1	-1	-1	-1		+1	-1	+1	+1	-1	-1	+1
	41	-1	+1	-1	-1	-1	-1	-1	+1	-1	+1	+1		+1	-1	-1	+1	+1	-1
	43	-1	-1	-1	+1	+1	+1	-1	+1	-1	+1	-1	+1		+1	+1	+1	-1	+1
	47	+1	-1	+1	-1	-1	+1	-1	-1	-1	-1	+1	-1	-1		+1	+1	+1	-1
	53	-1	-1	+1	+1	+1	+1	-1	-1	+1	-1	+1	-1	+1	+1		+1	-1	-1
	59	+1	+1	+1	-1	-1	+1	+1	-1	+1	-1	-1	+1	-1	-1	+1		-1	-1
	61	+1	+1	-1	-1	+1	-1	+1	-1	-1	-1	-1	+1	-1	+1	-1	-1		-1
	67	-1	-1	-1	-1	-1	+1	+1	+1	+1	-1	+1	-1	-1	+1	-1	+1	-1	

Remark: This is known as quadratic reciprocity and was first discovered and proved by Gauss. It is perhaps the most fundamental theorem in number theory. It motivated the development from 1850 to 1930 of class field theory, and class field theory in turn spawned the Langlands program, the largest program in modern math research.

Example computations. Using quadratic reciprocity, the fact that the Legendre symbol is multiplicative, and the so-called supplementary laws

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \text{and} \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

one can compute Legendre symbols by repeatedly flipping the symbol until the top is one of $-1, 1, 2$. For example, check that

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Compute $\left(\frac{37}{47}\right)$ and $\left(\frac{38}{47}\right)$.

Solution. Solving $[a]X = [c]$ is the same thing as solving $ax - c = by$: given a solution to the former, picking a representative x gives a unique y that satisfies the latter, whereas a solution of the latter gives a solution $X = [x]$ of the former. In particular, letting x_0 be a representative of X_0, we have $ax_0 - c = by_0$ for a unique integer y_0. By last week, the other solutions to this equation are

$$(x_0, y_0) + \frac{k}{\gcd(a,b)}(-b, a),$$

and as k runs through $0, \ldots, \gcd(a,b) - 1$, the values in the first coordinate run through the unique images in $\mathbb{Z}/b\mathbb{Z}$.

Similarly, the image of the multiplication-by-a map correspond to the values of c for which $ax - c = by$ have a solution, which by last week are precisely the multiples of $\gcd(a,b)$. □

Solution. Compute $(\mathbb{Z}/3\mathbb{Z})^2 = \{0,1\}$, $(\mathbb{Z}/5\mathbb{Z})^2 = \{0,1,4\}$, $(\mathbb{Z}/7\mathbb{Z})^2 = \{0,1,2,4\}$, $(\mathbb{Z}/11\mathbb{Z})^2 = \{0,1,3,4,5,9\}$, $(\mathbb{Z}/13\mathbb{Z})^2 = \{0,1,3,4,9,10,12\}$, and $(\mathbb{Z}/17\mathbb{Z})^2 = \{0,1,2,4,8,9,13,15,16\}$. Then the table is as follows.

	1	2	3	4	5	6	7	8	9	10	11	12
3	$+1$	-1	0	$+1$	-1	0	$+1$	-1	0	$+1$	-1	0
5	$+1$	-1	-1	$+1$	0	$+1$	-1	-1	$+1$	0	$+1$	-1
7	$+1$	$+1$	-1	$+1$	-1	-1	0	$+1$	$+1$	-1	$+1$	-1
11	$+1$	-1	$+1$	$+1$	$+1$	-1	-1	-1	$+1$	-1	0	$+1$
13	$+1$	-1	$+1$	$+1$	-1	-1	-1	-1	$+1$	$+1$	-1	$+1$

To see that the Legendre symbol is multiplicative, consider the three cases where a, b are squares, a is a square but b is not, and neither a nor b are squares.

- If $a = c^2$ and $b = d^2$ are squares, then $ab = (cd)^2$ is a square.
- If $a = c^2$ is a square and $ab = d^2$ is a square, then $b = d^2/a = (d/c)^2$ is a square.
- For the last case, note there are the same number of squares and nonsquares since the squaring function $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ is a two-to-one map: a and $-a$ have the same image, and if $a^2 = b^2$, then $(a+b)(a-b) = 0$, so $a = -b$ or $a = b$. Thus if neither a nor b are squares, then the second case says that multiplication by a is a bijection (with inverse multiplication by a^{-1}) from the nonsquares to the squares, hence takes the nonsquare b to a square ab. □

Solution. For a hint, lightly shade in the columns where $[q] = [1]$ and the rows where $[p] = [1]$ in $\mathbb{Z}/4\mathbb{Z}$, and examine the shaded region and the nonshaded region separately. The rough answer is that the shaded region is symmetric across the diagonal, whereas the nonshaded region is anti-symmetric across the diagonal. The intended final answer is that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

which is known as the law of quadratic reciprocity. □

Solution. We have

$$\left(\frac{37}{47}\right) = \left(\frac{47}{37}\right) = \left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -\left(\frac{37}{5}\right) = -\left(\frac{2}{5}\right) = 1,$$

whereas

$$\left(\frac{38}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{19}{47}\right) = \left(\frac{19}{47}\right) = -\left(\frac{47}{19}\right) = -\left(\frac{9}{19}\right) = -1.$$ □