Melbourne High School
Maths Extension Group 2023
Term 3 Week 9 Handout Solutions

A Golden Conjecture

1. Some of the rows are the same as some of the columns. Which rows and which columns are these? What is the significance of those particular values of p and q? For example, the row $p = 3$ is not quite the same as the column $q = 3$, but the row $p = 5$ and the column $q = 5$ are the same. Thus, if the pattern continued for the rest of the table, it seems that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

for all odd primes p. What other such observations can be made from the table?

2. (Warning: what follows is tedious.) We aim to find the parity of the number of multiples of 5 in the two intervals

$$\left(\frac{p}{2}, p\right)$$

and

$$\left(\frac{3p}{2}, 2p\right).$$

Divide both intervals by 5 and the question becomes how many integers there are in the intervals

$$A = \left(\frac{p}{10}, \frac{p}{5}\right)$$

and

$$B = \left(\frac{3p}{10}, \frac{2p}{5}\right).$$

Let v_A be the number of integers in A and v_B be the number of integers in B; naturally $v = v_A + v_B$. First let $p = 20k + r$. The intervals A and B become

$$\left(2k + \frac{r}{10}, 4k + \frac{r}{5}\right)$$

and

$$\left(6k + \frac{3r}{10}, 8k + \frac{2r}{5}\right).$$

The work begins here. If we let $r = 1$ then $v_A = 4k-(2k+1)+1 = 2k$ and $v_B = 8k - (6k + 1) + 1 = 2k$; hence $v = 4k$, an even number. Similarly, if $r = -1$ then $v_A = (4k - 1) - (2k) + 1 = 2k$ and $v_B = (8k - 1) - 6k + 1 = 2k$; again $v = 4k$.

One case down. The next one: $r = \pm 11$. If $r = 11$ then $v_A = 4k+2-(2k+2)+1 = 2k+1$ and $v_B = 8k+4-(6k+4)+1 = 2k+1$. Therefore $v = 4k + 2$, which is even. If $r = -11$ instead then $v_A = v_B = 2k - 1$, so $v = 4k - 2$. This shows that $(5|p) = 1$ when $p \equiv \pm 1, \pm 11 \pmod{20}$.

A similar procedure shows that $v = 4k+1$ is odd when $r = 3$, and similarly for $r = -3$ and $r = \pm 7$, thus proving that $(5|p) = -1$ when $p \equiv \pm 3, \pm 7 \pmod{20}$.

Clearly this method is tedious and also not particularly illuminating. To illustrate the power of the theorem that hides in the table investigated in the first question, suppose that the pattern we observed about the row $p = 5$ being the same as the column $q = 5$ really does continue forever. That is, assume

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Now there is a much easier way of finding the primes p for which $(5|p) = 1$ and those for which $(5|p) = -1$, because we just have to evaluate $(p|5)$ for the possible values of p modulo 5. For example, if $p \equiv 1 \pmod 5$ then

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

If $p \equiv 2 \pmod 5$ then

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$$

from our earlier investigation into the quadratic character of 2 modulo odd primes. We need not bother with the case $p \equiv 4$ because clearly $(4|5) = 1$. For the case $p \equiv 3$ we have

$$\left(\frac{5}{p}\right) = \left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1.$$

Therefore in about half the time we have found the primes for which 5 is a quadratic residue:

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5; \\ -1 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

We can verify that this condition on p is the same as the condition on p modulo 20.

So now what happens if we are asked to evaluate

$$\left(\frac{5}{3593}\right)?$$

Without knowing anything about the theory it seems insurmountable; how are to verify whether 5 is a square modulo 3593? But, knowing what we now know, in about a second we realise that $3593 \equiv 3 \pmod 5$ and hence $(5|3593) = (3|5) = -1$.

3. Using a computer program we find that the first few primes for which $(7|p) = 1$ are

$$p = 19, 29, 31, 37, 47, 53, 59, 83, 103$$

and those for which $(7|p) = -1$ are

$$11, 13, 17, 23, 41, 43, 61, 67, 71, 73, 79, 89, 97.$$

4. Let $P = (p-1)/2$ and $Q = (q-1)/2$. On a Cartesian plane, consider the rectangle enclosed by the the horizontal and vertical axes, the line $y = qx/p$, the vertical line $x = P$, and the horizontal line $y = Q$. How many lattice points are in this rectangle, not counting those on the horizontal or vertical axes but counting those on the lines $x = P$ and $y = Q$? (Lattice points are points in which both the x and y coordinates are integers.) The width of the rectangle is P and the height is Q; therefore the number

of lattice points is $PQ = (p-1)(q-1)/4$. But the number of lattice points is also the number of lattice points in the triangle below the line $y = qx/p$ plus the number of lattice points in the triangle above the line $y = qx/p$. This is true because there cannot be any lattice points on the line itself, since q and p, being odd primes, are coprime. First consider the triangle below the line.

How many lattice points on the vertical line $x = s$ are in the triangle for some $1 \leq s \leq P$? (The line passes through the origin so we don't have to consider $s = 0$.) The y coordinate on the diagonal line at $x = t$ is $y = sq/p$; therefore the number of lattice points on that vertical line is $\lfloor sq/p \rfloor$. If we run s through the values 1 to P and sum them, we will get the number of lattice points in the triangle below the line. Hence the number of lattice points below the line is

$$\sum_{s=1}^{P} \left\lfloor \frac{sq}{p} \right\rfloor = S(q,p).$$

Exactly the same argument shows that the number of lattice points in the upper triangle is $S(p,q)$, because all we do is just swap p and q and the argument still holds. Therefore $S(q,p) + S(p,q)$ is the number of lattice points in the rectangle, meaning

$$S(q,p) + S(p,q) = \frac{(p-1)(q-1)}{4}.$$