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

Stupors however do not last for ever, and Farmer Oak recovered from his.

—T. Hardy, *Far From the Madding Crowd* (1874)

Keep this in mind if you ever fall into a stupor because you're stuck on a problem (or have lost all of your sheep).

AIMO Problems

1. Gaston and Jordan are two budding chefs who unfortunately always misread the cooking time required for a recipe. For example, if the required cooking time is written 1:32 meaning 1 hour and 32 minutes, Jordan reads it as 132 minutes while Gaston reads it as 1:32 hours. For one particular recipe, the difference between Jordan's and Gaston's misread time is exactly 90 minutes. What is the actually cooking time in minutes? AIMO 2019/1

2. Let x and y be positive integers that simultaneously satisfy the equations $xy = 2048$ and $\frac{x}{y} - \frac{y}{x} = 7.875$. Find x. AIMO 2014/3

3. There are 5 lily pads on a pond, arranged in a circle. A frog can only jump from each lily pad to an adjacent lily pad on either side. How many ways are there for the frog to start on one of these lily pads, make 11 jumps, and end up where it started. AIMO 2022/5

4. A triangle PQR is to be constructed so that the perpendicular of PQ cuts the side QR at N and the line PN splits the angle QPR into two angles, not necessarily of integer degrees, in the ratio 1:22. If $\angle QPR = p$ degrees, where p is an integer, find the maximum value of p. AIMO 2019/7

5. Prove that 38 is the largest even integer that is *not* the sum of two positive odd composite numbers. AIMO 2018/9

If we compared the Bernoullis to the Bach family, then Leonhard Euler is unquestionably the Mozart of mathematics…

—E. Maor, *e: The Story of a Number* (1994)

A Golden Conjecture

Here's the table of values of p, q, and $(p|q)$ from last time:

p \ q	3	5	7	11	13	17	19	23	29	31	37
3	0	−1	1	−1	1	−1	1	−1	−1	1	1
5	−1	0	−1	1	−1	−1	1	−1	1	1	−1
7	−1	−1	0	1	−1	−1	−1	1	1	−1	1
11	1	1	−1	0	−1	−1	−1	1	−1	1	1
13	1	−1	−1	−1	0	1	−1	1	1	−1	−1
17	−1	−1	−1	−1	1	0	1	−1	−1	−1	−1
19	−1	1	1	1	−1	1	0	1	−1	−1	−1
23	1	−1	−1	−1	1	−1	−1	0	1	1	−1
29	−1	1	1	−1	1	−1	−1	1	0	−1	−1
31	−1	1	1	−1	−1	−1	1	−1	−1	0	−1
37	1	−1	1	1	−1	−1	−1	−1	−1	−1	0

It contains a pattern central to the problem of evaluating $(q|p)$ for any odd prime q. For now, however, let's leave it, and instead try to gain more numerical evidence.

Have faith that this detour is not an unwise one.

So far, we have proved that $(-1|p) = 1$ for primes of the form $4k+1$ and $(-1|p) = -1$ for primes of the form $4k-1$. Using Gauss's Lemma we have also shown that $(2|p) = 1$ for primes of the form $8k \pm 1$ and $(2|p) = -1$ for primes of the form $8k \pm 3$. Recall that since

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_r}{p}\right)$$

the remaining step is to evaluate $(q|p)$ for an odd prime q.

Here 'evaluate' means to find the conditions on p and q that determine whether $(q|p) = 1$ or $(q|p) = -1$.

The natural way forward, given our route thus far, is to evaluate $(3|p)$, $(5|p)$, and so on. Perhaps if we solve enough special cases a pattern will appear. Let's tackle $(3|p)$.

As before, the weapon to use is Gauss's Lemma. The question: how many numbers in the set

$$\left\{3, 6, 9, \ldots, \frac{3(p-1)}{2}\right\}$$

are negative when reduced into the range $(-p/2, p/2)$?

Divide the numbers in the above set into the three intervals

$$\left(0, \frac{p}{2}\right), \left(\frac{p}{2}, p\right), \left(p, \frac{3p}{2}\right).$$

The numbers in the first interval are positive and less than $p/2$; hence they remain unchanged when reduced to be in the interval $(-p/2, p/2)$. All the numbers in the second interval will become negative because they are greater than $p/2$ but less than p. The numbers in the third interval, being greater than p but less than $3p/2$, will be reduced to be between 0 and $p/2$ and therefore remain positive. Hence the number of negative signs is the number of numbers in the second interval, $(p/2, p)$.

So there is some condition on p, most likely to do with its residue class modulo some number, that determines whether the number of

numbers in the interval $(p/2, p)$ is even or odd, and that is the same condition that determines whether $(3|p) = 1$ or $(3|p) = -1$.

Now is the time for the numerical evidence. By simply evaluating $(3|p)$ for many values of p, we find that $(3|p) = 1$ for

$$p = 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107$$

and $(3|p) = -1$ for

$$p = 5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101.$$

If we continue trying out values of p, we notice that the numbers in the first list are of the form $12k \pm 1$ while the numbers in the second are of the form $12k \pm 5$. So we conjecture that $(3|p) = 1$ for $p = 12k \pm 1$ and $(3|p) = -1$ for $p = 12k \pm 5$.

To prove the conjecture, let $p = 12k + r$, where $r = \pm 1, \pm 5$. We wish to know how many numbers a satisfy

Note that these values of r are the only values for which p could be prime. We leave out $p = 2$ because $(3|2) = (1|2)$, which is trivial.

$$\frac{p}{2} < 3a < p,$$

or

$$\frac{12k + r}{2} < 3a < 12k + r.$$

Dividing through by 3 and splitting the fraction yield

$$2k + \frac{r}{6} < a < 4k + \frac{r}{3}.$$

When $r = 1$, the inequality becomes

$$2k + \frac{1}{6} < a < 4k + \frac{1}{3}.$$

If $a > 2k + 1/6$, then $a \geq 2k + 1$ because a is an integer. Similarly if $a < 4k + 1/3$, then $a \leq 4k$. Therefore the inequality is equivalent to

$$2k + 1 \leq a \leq 4k.$$

The number of numbers in this interval is $4k - (2k + 1) + 1 = 2k$, which is even, and hence $(3|p) = 1$. Similarly, when $r = -1$ the interval becomes

How many numbers are between 5 and 9 inclusive of both? Answer: $5, 6, 7, 8, 9$, so 5, or $9 - 5 + 1$.

$$2k - \frac{1}{6} < a < 4k - \frac{1}{3}.$$

Using the same reasoning as before, the number of numbers in this interval is $4k - 1 - 2k + 1 = 2k$; therefore $(3|p) = 1$ when $r = -1$ too.

The second case is much the same as the first. When $r = 5$ the inequality becomes

$$2k + \frac{5}{6} < a < 4k + \frac{5}{3}$$

and when $r = -5$ the inequality becomes

$$2k - \frac{5}{6} < a < 4k - \frac{5}{3}.$$

In the former the number of values of a that satisfy the inequality is $4k+1-(2k+1)+1 = 2k+1$; in the latter case it is $4k-2-(2k)+1 = 2k-1$. In both cases the number is odd and hence $(3|p) = -1$.

We have successfully solved another special case of the Legendre symbol: the case $a = 3$. Is there a pattern we can spot? With only two cases completed, $a = 2$ and $a = 3$, it might seem hard to find a pattern. However two things are plain. Firstly, in the case $a = 2$ the condition on p is its residue class modulo 8; for $a = 3$ it is its residue class modulo 12. Secondly, $(2|p)$ is the same for $p = 8k + r$ and $8k - r$

The case $a = -1$ is special because -1 is not prime; we need it so evaluate $(a|p)$ when $a < 0$.

for $r = 1, 3$, just as $(3|p)$ is the same for $p = 12k + r$ and $12k - r$ for $r = 1, 5$. From these two observations, we may guess, perhaps tentatively, that $(a|p)$ is dependent on the modulo class of p modulo $4a$, and that the quadratic character of a modulo $p = 4a - r$ is the same as that of $p = 4a + r$.

Let's try another case: $a = 5$. Using a computer, the first few values of p for which $(5|p) = 1$ are

$$p = 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109, 131, 139, 149, 151$$

and those for which $(5|p) = -1$ are

$$p = 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 103, 107, 113, 127, 137.$$

From experience, it is likely that the pattern has something to do with the residue class of p modulo a multiple of 4; it was 8 for $a = 2$ and 12 for $a = 3$. Naturally we try 20 for $a = 5$. And, indeed, if we examine the values of p closely, it seems that $(5|p) = 1$ for $p = 20k \pm 1$ or $p = 20k \pm 11$ and $(5|p) = -1$ for $p = 20k \pm 3$ or $p = 20k \pm 13$. The proof of this is far less exciting than the observation because of the number of different cases, but it is left as an exercise for the devoted.

Note also how this preceding observation is consistent with our earlier conjecture about the quadratic character of a being the same for $p = 4ak+r$ as it is for $p = 4ak-r$. When new numerical data agrees with previous conjectures, it is more evidence that those conjectures have a grain of truth to them.

From our guesswork for the case $a = 5$ something else jumps out as being a possible pattern: if $p = 4ak + r$ the same values of r seem to yield the same values for the Legendre symbol. That is, all of $(2|p)$, $(3|p)$, and $(5|p)$ equal 1 when $r = \pm 1$, and $(2|p)$ and $(5|p)$ both equal -1 when $r = \pm 3$. Of course there is not enough data here, but, perhaps, there is an inkling of gold just beneath the surface.

Problems

1. If no patterns are apparent in the table on page 2, try again.
2. Prove our conjecture about $(5|p)$.
3. Tackle the case $a = 7$. Do our two hypotheses hold?
4. Let

   This is a hard problem.

   $$S(q, p) = \sum_{s=1}^{(p-1)/2} \left\lfloor \frac{sq}{p} \right\rfloor.$$

   Prove that

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