Melbourne High School
Maths Extension Group 2023
Term 3 Week 8 Handout

Boiling water will soften a potato but harden an egg.

Don't ask how this is related to functional equations.

—J. Clear, *Atomic Habits* (2018)

Problems: functions and functional equations

1. The function $f(x) = x^2$ is not invertible. However, if we let $g(x) = \sqrt{x}$ then $f(g(x)) = (\sqrt{x})^2 = x$. So, why isn't f invertible?

2. Let $f(x)$ be a function such that $f(x + y) = x + f(y)$ for any two real numbers x and y, and $f(0) = 2$. What is the value of $f(1998)$? AHSME 1998/17

3. An involution is a function whose inverse is itself ($f(f(x) = x$ for all x in the domain of f). Show that an involution must be bijective.

4. Find all solutions to the equation

$$f(x + y) + f(x - y) = 2x^2 - 2y^2.$$

5. Find all functions $f : \mathbb{R} \to \mathbb{R}$ for which

$$f(x + y) - 2f(x - y) + f(x) - 2f(y) = y - 2$$

for all $x, y \in \mathbb{R}$.

As a six-year-old lad I could easier understand a mathematical proof than I could understand why I should take my cap off in the parlour, or why I should use a knife to cut a slice of meat rather than tearing it apart with a fork.

Soon Mr. Eisenstein is to play an important role in our story.

—G. Eisenstein[1], *Curriculum Vitae* (c. 1843)

Cliffhanger

Let's begin by revisiting the problem of finding $(2|p)$ for odd primes p. We shall not leave ourselves on a cliffhanger this time, but our method of solving the problem will be different. The method employed here will make our transition to the most general case ($(p|q)$ for odd primes p and q) easier and perhaps more enlightening.

The basis of our proof, like before, is Gauss's Lemma. Such a venerable lemma is easy to forget, so here it is again: given an odd prime p and some number a coprime with p,

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

where v is the number of numbers in the set

$$\left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\} \tag{1}$$

that have least positive residues greater than $p/2$. An equivalent definition of v is the number of negative numbers in the set formed by taking each element of (1) and reducing it to be between $-p/2$ and $p/2$, for if $ka > p/2$ then reducing it in this manner will make it negative.

Armed with this weapon, let's introduce another. This one is called the *floor function*; it is denoted by $\lfloor x \rfloor$. This symbol means the largest integer less than or equal to x. So if x is a positive number, $\lfloor x \rfloor$ is the integer part of x. For example, $\lfloor \pi \rfloor = 3$, $\lfloor e \rfloor = 2$, $\lfloor 28/5 \rfloor = 5$. Using this notation we can write any number x as

What happens when x is negative?

$$x = \lfloor x \rfloor + y$$

where $0 \leq y < 1$.

Now we can turn back to the original problem. For our specific case where $a = 2$, we have to find how many numbers in the set

$$\{2, 4, \ldots, p-1\}$$

are greater than $p/2$. Let u be the number of numbers in the set that are less than $p/2$ and v be the number of numbers in the set that are greater than $p/2$. In other words, u satisfies

Clearly only strict inequality signs are needed because $p/2$ is not an integer.

$$2u < \frac{p}{2}$$

and

$$2(u+1) > \frac{p}{2}.$$

Rearranging these two inequalities yields

$$u < \frac{p}{4}$$

and

$$u > \frac{p}{4} - 1,$$

[1]Translated from the German by M. Schmitz in *Res. Lett. Inf. Math. Set.,* 2004, Vol. 6, pp 1–13.

which is more succinctly written as

$$\frac{p}{4} - 1 < u < \frac{p}{4}.$$

A little thought convinces us that between $p/4$ and $p/4 - 1$ there is one and only one integer, and that integer is $\lfloor p/4 \rfloor$. Thus $u = \lfloor p/4 \rfloor$.

By definition, $u + v = (p-1)/2$, so $v = (p-1)/2 - \lfloor p/4 \rfloor$. To get rid of the floor function so that we can collect like terms, consider two cases: when $p \equiv 1 \pmod 4$ and when $p \equiv 3 \pmod 4$. If $p = 4k+1$, then $\lfloor p/4 \rfloor = \lfloor k + 1/4 \rfloor = k$; substituting this into the above equation for v we get $v = k$. But $k = (p-1)/4$, so we have

$$v = \frac{p-1}{4}.$$

Similarly, if $p = 4k+3$, then $\lfloor p/4 \rfloor = k$ and $v = k+1$. In this case $k = (p-3)/4$ so

$$v = \frac{p+1}{4}.$$

In the following section some of the calculations have been omitted for brevity; carry them out yourself if necessary to understand the logic.

Here is the final hurdle. As shown above, when $p = 4k+1$ we have $v = (p-1)/4$. If $p-1$ is divisible by 4, then $p - 1 + 2 = p + 1$ is not divisible by 4, but has the same quotient. That is,

$$\frac{p-1}{4} = \left\lfloor \frac{p+1}{4} \right\rfloor$$

when $p = 4k+1$. If $p = 4k+3$, we have $v = (p+1)/4$ anyway, and clearly $(p+1)/4 = \lfloor (p+1)/4 \rfloor$. Therefore we have shown that

$$v = \left\lfloor \frac{p+1}{4} \right\rfloor$$

regardless of whether p is 1 or 3 more than a multiple of 4.

From Gauss's Lemma

$$\left(\frac{2}{p}\right) = (-1)^v;$$

substituting in the value of v just found gives

$$\left(\frac{2}{p}\right) = (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor}. \tag{2}$$

Here is where we need numerical evidence to help us continue; we would be lost without a rough idea of what we're trying to prove because it is not clear how to proceed. In this case the best way is to evaluate $(2|p)$ for the first hundred primes to see if a pattern is apparent. If we do this, we find that $(2|p) = 1$ for

$$p = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97$$

and $(2|p) = -1$ for

$$p = 3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83.$$

If you successfully solved last week's problems you will know what comes next.

What is the difference between the two lists? If we look closely, we observe that all the numbers in the first list are congruent to ± 1 modulo 8 while the ones in the second are congruent to ± 3 modulo 8. Our conjecture, therefore, is that $(2|p) = 1$ if $p \equiv \pm 1 \pmod 8$ and $(2|p) = -1$ if $p \equiv \pm 3 \pmod 8$.

In this case the pattern is so overwhelming as to make the conjecture obvious once it is noticed, but in other cases, such as the one at the end of this handout, many different guesses might have to made before the correct one is landed upon and successfully proved.

To prove the conjecture, first put $p = 8k+1$ into Equation (2). We get

$$\left(\frac{2}{p}\right) = (-1)^{\lfloor 2k + 1/2 \rfloor} = (-1)^{2k} = 1.$$

Similarly if $p = 8k - 1$ then $\lfloor (p+1)/4 \rfloor = 2k$, which implies $(2|p) = (-1)^{2k} = 1$ again.

Now for the other case. If $p = 8k + 3$ then

$$\left(\frac{2}{p}\right) = (-1)^{\lfloor 2k+1 \rfloor} = (-1)^{2k+1} = -1.$$

Putting $p = 8k - 3$ instead yields

$$\left(\frac{2}{p}\right) = (-1)^{\lfloor 2k-1/2 \rfloor} = (-1)^{2k-1} = -1.$$

This proves our conjecture! Indeed it is true that the quadratic character of 2 modulo p depends on the the residue class of p modulo 8.

Let's summarise what we have discovered so far in the quest to evaluate the Legendre symbol. We have solved two cases: $a = -1$ and $a = 2$. In the former case $(-1|p) = -1$ if $p \equiv 1 \pmod 4$ and $(-1|p) = -1$ if $p \equiv -1 \pmod 4$; in the latter case $(2|p) = 1$ if $p \equiv \pm 1 \pmod 8$ and $(2|p) = -1$ if $p \equiv \pm 3 \pmod 8$.

Although it may not seem like it, we are in fact two thirds of the way towards evaluating any Legendre symbol. Suppose we want to find $(a|p)$. Using the multiplicative property $(ab|p) = (a|p)(b|p)$, if we write $a = q_1 q_2 \cdots q_r$, where all the q's are primes, then

Ok, maybe two thirds is an exaggeration, because the part left for us to discover (and prove) is much more difficult than what we have just done. But it's still good to be optimistic.

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

If $a < 0$ then stick at $(-1|p)$ at the front—we know how to evaluate that. So the only goal now is to evaluate $(q|p)$ when q is an odd prime.

This question is much more difficult to answer than the two we have already tackled. To get started, here is a table values of p, q, and $(p|q)$.

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

In the table there exists a pattern that is at the heart of what may be the most beautiful theorem in number theory. But for now, the story remains to be continued.

Admittedly I am biased.

Problem

Spot as many patterns as possible in the above table.