Melbourne High School
Maths Extension Group 2023
Term 3 Holiday Handout

For too much rest itself becomes a pain.

—Homer, *Odyssey* (c. 8th or 7th century BC)

Problems

1. The number x is 111 when written in base b, but it is 212 when written in base $b-2$. What is x in base 10? AIMO 2017/1

2. Find the number of permutations x_1, x_2, x_3, x_4, x_5 of numbers $1, 2, 3, 4, 5$ such that the sum of five products AIME II 2021/3

$$x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2$$

is divisible by 3

3. Let ABC be a triangle and P be any point on the circumcircle of ABC. Let X, Y, Z be the feet of the perpendiculars from P onto lines BC, CA and AB. Prove that points X, Y, Z are collinear. Simson Line

4. Find all functions $f : \mathbb{R}\backslash\{-1, 1\} \to \mathbb{R}$ for which

$$f\left(\frac{x-3}{x+1}\right) + f\left(\frac{3+x}{1-x}\right) = x$$

for all $x, y \in \mathbb{R}\backslash\{-1, 1\}$.

5. Prove that a convex pentagon with integer side lengths and an odd perimeter can have two right angles, but cannot have more than two right angles. AMO 2022/1

6. Having conquered *The Trial*, Harold is now reading *Gulliver's Travels*, a 319 page picture book. Eager as he is to dive into the travels of Gulliver, he also has a brilliant idea as to how he is going to read the book. He tells you that he is going to form the set of ordered pairs

$$\{(1,1), (1,2), \dots, (1,11), (2,1), (2,2), \dots, (2,11),$$
$$(3,1), (3,2), \dots, (29,1), \dots, (29,11)\}.$$

As he is a genius (and a good friend too), you don't doubt him.

As if that was not distressing enough, he then says that he will randomly arrange those ordered pairs by giving each a number. So if the above set was the arrangement, the pair $(1,1)$ would be 1, $(1,2)$ would be 2, and so on. To find the nth page that he reads, he takes the nth ordered pair (x_n, y_n) and forms the number $11x_n + 29y_n$; if this number is too big he subtracts off a multiple of 319 until he gets a page in the book. He then reads that page.

Show that regardless of how Harold arranges the ordered pairs, he will be able to read the entire book without reading the same page twice.

The king, although he be as learned a person as any in his dominions, had been educated in the study of philosophy, and particularly mathematics; yet when he observed my shape exactly, and saw me walk erect, before I began to speak, conceived I might be a piece of clock-work (which is in that country arrived to a very great perfection) contrived by some ingenious artist.

—J. Swift, *Gulliver's Travels* (1726)

A Golden Conjecture: Part 2

Easily summarised is the story so far. We first discovered that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv -1 \pmod 4 \end{cases}$$

and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8; \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Recall that the rule for $(-1|p)$ is more succinctly written as

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

As a side note, $(2|p)$ has a succinct rule too, namely

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)(p+1)/8}.$$

Verifying this by enumerating p shreds any incredulity.

We then took a slight detour to gather more numerical evidence; the following two conjectures resulted:

- The value of $(a|p)$ depends only on the residue class of p modulo $4a$, or, equivalently, the value of r when p is written as $p = 4ak + r$. In other words, if $p \equiv q \pmod{4a}$ then
$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$
- The value of $(a|p)$ is the same for $p = 4ak + r$ as it is for $p = 4ak - r$. In other words, if $p \equiv -q \pmod{4a}$ then
$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Note this conjecture holds regardless of whether r is positive or negative or whether r is between $-p/2$ and $p/2$. For $(2|p)$ it was prudent to split the residue classes modulo 8 into ± 1 and ± 3; but we could have chosen ± 7 and ± 5 instead, because $7 \equiv -1$, $-7 \equiv 1$, and similarly for ± 5.

These two conjectures found firm ground in two special cases that were proved using Gauss's Lemma. They are

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}; \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}, \end{cases}$$

and

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \text{ or } p \equiv \pm 11 \pmod{20}; \\ -1 & \text{if } p \equiv \pm 3 \text{ or } p \equiv \pm 13 \pmod{20}. \end{cases}$$

Euler was the first to make the two conjectures that we have also made; therefore from here they will be referred to as Euler's Conjectures. He was, however, unable to supply a proof. The problem of Gauss's Lemma not being discovered yet might have had something to do with it.

It's fairly rare to find a conjecture that eluded Euler, but this is one of them.

Amendment, 24 September 2023: The following proof is **wrong**. The way the inequalities are simplified works only when integers are added to both ends. It is also not true that, as I will apparently prove, the parity of the number of numbers in every interval we are concerned with is the same as the parity of the numbers in the interval $(r/2a, r/a)$; for that would mean when the number of intervals is even, the parity of all the numbers in all the intervals is always even. This is plainly false, as if it were true 5 would be a quadratic residue modulo p regardless of the residue class of p modulo 20.

I could silently replace what follows by the correct proof, but I have left it to serve as an illustration that mathematics demands the most exacting and relentless eye, and that mistakes are inevitable. The correct proof is attached at the end.

Be assured the conjecture itself is true. The problem is in the proof, and thus the fault is mine, not Euler's.

We begin the proof of Euler's conjectures by applying Gauss's Lemma in full generality. Form the set

$$\left\{a, 2a, \dots, \frac{p-1}{2}a\right\};$$

how many of those multiples of a become negative when reduced to be in the range $(-p/2, p/2)$? Answer: all those that have least positive residues in the range $(p/2, p)$. This means we need to determine the parity of all the multiples of a in all the intervals

$$\left(\frac{p}{2}, p\right), \left(\frac{3p}{2}, 2p\right), \left(\frac{5p}{2}, 3p\right), \dots . \tag{1}$$

Since we are assuming that a is not a multiple of p (because if it were the Legendre symbol, by definition, is equal to 0), none of the endpoints of any of the intervals can be multiplies of a. Therefore we don't have to worry about whether we need to count them or not.

Let's take one of these intervals, say the interval

$$\left(\frac{(2t-1)p}{2}, tp\right) \tag{2}$$

for some positive integer t. Now the question becomes how many numbers x satisfy the inequality

$$\frac{(2t-1)p}{2} < ax < tp.$$

Let this number be μ.

Dividing through by a yields

$$\frac{(2t-1)p}{2a} < x < \frac{tp}{a}. \tag{3}$$

Before continuing, let's take a step back and think about what we want to prove. Our conjecture is that $(a|p)$ depends only on the residue of p modulo $3a$. So let's write $p = 4ak + r$ for a positive integer value of r. Substitute this into our interval above, and, after a cumbersome expansion and simplification, we get

$$4tk + \frac{tr}{a} - 2k - \frac{r}{2a} < x < 4tk + \frac{tr}{a}.$$

Since we are interested only in the number of values of x (actually we are interested in the *parity* of that number) that satisfy the inequality, and not what those values actually are, we can manipulate the inequality by adding the same value to both endpoints, and the number of

Recall that we are interested only in the parity because of Gauss's Lemma, which tells us that $(a|p) = (-1)^v$ where v is the number of numbers in all the intervals in (1).

values of x that satisfy it will not change. For example, two values of x satisfy $3 < x < 6$ (4 and 5), but two values of x also satisfy $5 < x < 8$ or $1 < x < 4$.

Therefore, we can get rid of all the terms involving t in the inequality, which means we are looking for the number of values of x that satisfy

$$-2k - \frac{r}{2a} < x < 0.$$

It is easier to work with positive numbers, so add $2k$ and r/a to both sides to obtain the inequality

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

The smallest integer greater than $r/2a$ is $\lceil r/2a \rceil$ and the largest integer less than $2k + r/a$ is $2k + \lfloor r/a \rfloor$. Therefore the number of numbers in the sequence

$$\lceil r/2a \rceil, \lceil r/2a \rceil + 1, \ldots, 2k + \lfloor r/a \rfloor$$

is μ, the magic number we are looking for. Calculating μ is very simple because

$$\mu = 2k + \lfloor r/a \rfloor - \lceil r/2a \rceil + 1.$$

Since we are only interested in the parity of μ, we note that

$$2k + \lfloor r/a \rfloor - \lceil r/2a \rceil + 1 \equiv \lfloor r/a \rfloor - \lceil r/2a \rceil + 1 \pmod 2$$

and hence $\mu \equiv \mu' \pmod 2$ if μ' is the number of integers in the interval

$$\left(\frac{r}{2a}, \frac{r}{a}\right).$$

Take a breath. What have we shown? Answer: regardless of which interval in (1) we choose, the parity of the number of numbers in that interval is equal to the parity of the number of numbers in the interval $(r/2a, r/a)$.

Now consider what happens if, instead of writing $p = 4ak + r$, we write $p = r$ instead. That is, substitute $p = r$ into (3). Expand and we get

$$\frac{tr}{a} - \frac{r}{2a} < x < \frac{tr}{a}.$$

Again we can manipulate the interval like we did before; getting rid of the tr/a term and adding r/a to both sides yields

$$\frac{r}{2a} < x < \frac{r}{a}.$$

Bingo! This is the interval we ended up getting when we put $p = 4ak + r$. This means that for each interval in (1), the parity of the number of numbers in that interval is the same when $p = 4ak + r$ and when $p = r$; therefore the parity of the total number of numbers in all the intervals is the same in both cases. Thus, the glorious conclusion, after much work, is that $(a|p)$ does not depend on k if $p = 4ak + r$, but only on r, the residue class of p modulo $4a$. We have proved the first part of Euler's Conjecture.

The second part of Euler's Conjecture is, quite thankfully, a little easier to prove. We need to show that replacing r by $-r$ does not change the parity of the number of numbers in the intervals in (1).

We have shown that the parity of the number of numbers in each of the intervals in (1) is the same as the parity of the number of numbers in the interval

$$\left(\frac{r}{2a}, \frac{r}{a}\right).$$

Note that the $\lceil x \rceil$ is the *ceiling function*; it is the smallest integer greater than or equal to x.

Is the use of floor and ceiling functions here dependent on r being positive?

If this is baffling, remember the example from last time. How many numbers x satisfy $5 \leq x \leq 9$? The answer is $9 - 5 + 1 = 5$.

If we replace r by $-r$, we get the interval

$$\Big(\frac{-r}{a}, \frac{-r}{2a}\Big);$$

note the reversal of the endpoints because $-r$ is negative. Now just add $3r/2a$ to both sides and we get the interval $(r/2a, r/a)$, which shows that replacing r by $-r$ has no effect on the parity of the numbers in the intervals in (1). Hence the second part of the conjecture is also true.

What we have proved can be thus summarised: if $p \equiv r \pmod{4a}$ and $q \equiv r \pmod{4a}$, or if $p \equiv r \pmod{4a}$ and $q \equiv -r \pmod{4a}$, then

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

More succinctly: if $p \equiv \pm q \pmod{4a}$ then

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

Where does this leave us? It leaves us on the precipice of the most famous theorem in this area of number theory.

A Golden Conjecture: Part 2 (Take 2)

I very much hope this proof is correct.

As before, let p be an odd prime and a be an integer not divisible by p. The multiples of a (i.e., the numbers $a, 2a, \ldots, (p-1)a/2$) can be divided into the intervals

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

The multiples of a in the odd intervals are the ones that become negative when reduced to be in the range $(-p/2, p/2)$; therefore we aim to find the parity of the number of multiples of a in the intervals

$$\left(\frac{p}{2}, p\right), \left(\frac{3p}{2}, 2p\right), \left(\frac{5p}{2}, 3p\right) \ldots.$$

Let v be the number of multiples of a in the above intervals and v_t be the number of multiples of a in the particular interval

$$\left(\frac{(2t-1)p}{2}, tp\right)$$

for some positive integer t. In other words, v_t is the number of values of x that satisfy

$$\frac{(2t-1)p}{2} < ax < tp.$$

Dividing through by a yields

$$\frac{(2t-1)p}{2a} < x < \frac{tp}{a}.$$

By substituting $p = 4ak + r$ into the above inequality it becomes

$$4tk - 2k + \frac{(2t-1)r}{2a} < x < 4tk + \frac{tr}{a}.$$

Here we really can ignore $4tk$ because it is an integer; therefore v_t is also the number of values of x that satisfy

$$-2k + \frac{(2t-1)r}{2a} < x < \frac{tr}{a}.$$

To determine the value of v_t, we observe that the smallest integer greater than $-2k + (2t-1)r/2a$ is $-2k + \lceil (2t-1)r/2a \rceil$, and the largest integer less than tr/a is $\lfloor tr/a \rfloor$. Thus

$$-2k + \left\lceil \frac{(2t-1)r}{2a} \right\rceil \leq x \leq \left\lfloor \frac{tr}{a} \right\rfloor.$$

From this inequality we can calculate v_t as

$$v_t = \left\lfloor \frac{tr}{a} \right\rfloor - \left(-2k + \left\lceil \frac{(2t-1)r}{2a} \right\rceil \right) + 1.$$

Notice that

$$v_t \equiv \left\lfloor \frac{tr}{a} \right\rfloor - \left\lceil \frac{(2t-1)r}{2a} \right\rceil + 1 \pmod 2$$

because $-2k \equiv 0 \pmod 2$. Hence the parity of v_t is the same as the parity of the number of numbers that satisfy

$$\frac{(2t-1)r}{2a} < x < \frac{tr}{a}.$$

But observe that this inequality can be obtained precisely by replacing p with r rather than $4ak + r$, meaning that the parity of v_t, and by extension v, is the same for $p = 4ak + r$ as it is for $p = r$. This completes the proof of the first part of the conjecture: the quadratic character of a modulo p depends only on r, the remainder when p is divided by $4a$.

If we now replace r by $-r$ we get

$$-\frac{tr}{a} < x < \frac{(1-2t)r}{2a}.$$

The effect is simply that of flipping the bounds; the number of integers that satisfy the inequality remains the same because both the width of the interval and the magnitude of the endpoints remain the same. Therefore there is no effect on v_t for every value of t, and, consequently, there is no effect on v either. This completes the proof of the second part of the conjecture.

Summarising, we have proved that if $p \equiv \pm q \pmod{4a}$ then

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