Melbourne High School
Maths Extension Group 2023
Term 4 Week 2 Handout

> *The excitement that a gambler feels when making a bet is equal to the amount he might win times the probability of winning it.*
>
> —B. Pascal[1], ?? (??)

Not intended to glorify gambling.

Expected value problems

1. I have 12 addressed letters to mail, and 12 corresponding pre-addressed envelopes. For some wacky reason, I decide to put the letters into envelopes at random, one letter per envelope. What is the expected number of letters that get placed into their proper envelopes?

2. I flip a coin 10 times. What is the expected number of pairs of consecutive tosses that comes up heads? (For example, the sequence THHTHHHTHH has 4 pairs of consecutive HH's).

3. At a nursery, 2006 babies sit in a circle. Suddenly, each baby randomly pokes either the baby to its left or to its right. What is the expected value of the number of unpoked babies? HMMT 2006

4. A 10 digit binary number with four 1's is chosen at random. What is its expected value?

5. Let $p_n(k)$ be the number of permutations of the set $\{1, 2 \dots, n\}$, $n \geq 1$, which have exactly k fixed points. Prove that IMO 1987/1

$$\sum_{k=0}^{n} k \cdot p_n(k) = n!.$$

   (A *fixed point* of a permutation in this case is an element i such that i is in the i^{th} position of the permutation. For example, the permutation $(3, 2, 5, 4, 1)$ of $\{1, 2, 3, 4, 5\}$ has two fixed points: the 2 in the 2^{nd} spot and the 4 in the 4^{th} spot)

[1] As quoted by N. Rose in *Mathematical Maxims and Minims* (1988).

> *The fundamental theorem must certainly be regarded as one of the most elegant of its type.*
>
> —C. F. Gauss[2], *Disquisitiones Arithmeticae* (1801)

The Law of Quadratic Reciprocity

Let's cast our minds back and recall the following table, a table of values of odd primes p and q, and the associated Legendre symbol $(q|p)$.

q p	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

For the following discussion, ignore all the 0 entries in the table. That is, when we say "p runs through all the odd primes" we are eliding the further restriction that p does not equal the prime we are considering, or q in the most general case.

One of the patterns is that some rows are the same as some columns. For example, the column $q = 5$ is the same as the row $p = 5$, as is the column $q = 13$ and row $p = 13$. On the other hand, the row $q = 3$ is not the same as the column $p = 3$, and the same is true for $q = 7$ and $p = 7$.

By "the same" we mean the same sequence of 1's and -1's.

The primes in the table for which their row and column are the same are $5, 13, 17, 29, 37$; the others are $3, 7, 11, 19, 23, 31$. What is the distinguishing feature of these two classes of primes? Those in the first group are all of the form $4k + 1$ while those in the second are all of the form $4k + 3$.

Let's think about what this means. Let p be one of the primes in the first group, those of the form $4k + 1$. For concreteness suppose $p = 5$. The row $p = 5$ consists of $(q|5)$, where q runs through the odd primes $3, 5, 7, 11, ...$, while the column $q = 5$ consists of values of $(5|p)$, but this time it is p that runs through the odd primes. Since the row and column are the same, we conjecture that

Splitting the primes into these two classes is common; for example, Fermat's celebrated two square theorem states that all primes of the form $4k+1$ are the sum of two integer squares, while those of the form $4k + 3$ are not the sum of two integer squares.

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

for all odd primes p. Similarly, since the row $p = 13$ and the column $q = 13$ are also the same, it seems that

$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right).$$

There is nothing special about 5 or 13, other than that they are of the form $4k + 1$; therefore, we generalise our conjecture by hypothesising

[2] Translated from the Latin by A. A. Clarke, 1965.

that if $q \equiv 1 \pmod 4$ then

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

One further step: we chose q to have the condition, but we might as well have chosen p; for if we just swap p and q the condition becomes $p \equiv 1 \pmod 4$ but the Legendre symbols don't change. Hence the revised guess: if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ then

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

(Strictly speaking this tweak was not necessary, but it'll be useful to have this form of the conjecture in our minds.)

The other case is not quite so easy. Let's take $p = 3$. Examining the row $p = 3$ and the column $q = 3$, we notice that sometimes $(3|p) = (p|3)$ and sometimes $(3|p) = -(p|3)$—for example, $(5|3) = (3|5) = 1$, but $(7|3) = 1 = -(3|7)$. What is the distinction between the two cases?

Looking at the table closely, we see that $(3|p) = (p|3)$ for $p = 5, 13, 17, 29, 37$ and $(3|p) = -(p|3)$ for $p = 7, 11, 19, 23, 31$. Like before, the first group of primes are 1 modulo 4, the second 3 modulo 4. Therefore it seems that if $p \equiv 3 \pmod 4$ then

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

Again this distinction between the primes based on their residue class modulo 4 pops up.

Again, nothing was special about picking 3 here. We could have made the same conjecture for any prime from the second class of primes, those of the form $4k + 3$. Thus we conjecture that if *both* p and q are of the form $4k + 3$ then $(p|q) = -(q|p)$. Looking for other examples in the table supports the conjecture, as the columns that are not the same as the rows are the columns for which $q \equiv 3 \pmod 4$; and the differences between the row and column occur only when $p \equiv 3 \pmod 4$ as well. Summarising, we have made the following guess at the value of the general Legendre symbol $(p|q)$ for odd primes p and q:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4; \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

What we have just discovered is *The Law of Quadratic Reciprocity.* Euler and Legendre both made but were unable to prove the conjecture. Gauss supplied the first proof in 1801, and throughout his career he added over half a dozen more; since then, hundreds of proofs of the theorem have emerged, making quadratic reciprocity one of the most proved theorems in all of mathematics.

Pythagoras's Theorem is a contender, but quadratic reciprocity is hard to beat. Of course the hundreds of proofs are not all completely different; indeed many are based on the same ideas. However, some of the proofs have shown themselves capable of generalisation to higher powers, showing that not all mathematical proofs are equal. Those that connect significant and deep mathematical ideas are, justifiably, ranked as the greater achievements.

Now for the proof (or at least one of the proofs). We shall, in fact, show that the law is a corollary of the conjecture of Euler's that we proved previously, namely that if $p \equiv q \pmod{4a}$ then

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

We break the proof into two cases: when $p \equiv q \pmod 4$, and when $p \equiv -q \pmod 4$. One of these two cases much be true because p and q, being odd primes, can only be congruent to 1 or 3 modulo 4, and $3 \equiv -1 \pmod 4$.

Suppose $p \equiv q \pmod 4$. Then $p - q = 4a$ for some integer a. Note that this implies $p \equiv q \pmod{4a}$. Since $p = 4a + q$ and $q \equiv 0 \pmod q$ we have

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right).$$

We can show that Euler's conjecture can be deduced from quadratic reciprocity (if we supply a different proof of the latter, that is). Hence the two theorems are equivalent; both imply the other.

By the multiplicative property of the Legendre symbol $(4a|q) = (4|q)(a|q)$; but clearly $(4|q) = 1$ because $4 = 2^2$. Therefore

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

Let's apply the same process to $(q|p)$. Since $q = p - 4a$, we have

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right).$$

Again we may ignore the 4; hence

$$\left(\frac{q}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right).$$

Comparing $(q|p)$ and $(p|q)$ and applying the result $(a|p) = (a|q)$ we deduce that

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

We know that $(-1|p) = 1$ if $p \equiv 1 \pmod 4$ and $(-1|p) = -1$ if $p \equiv 3 \pmod 4$; consequently $(q|p) = (p|q)$ if $p \equiv q \equiv 1 \pmod 4$ and $(q|p) = -(p|q)$ if $p \equiv q \equiv 3 \pmod 4$. This completes the first case.

The second case: let $p \equiv -q \pmod 4$. Note that in this case we wish to prove $(p|q) = (q|p)$, since one of p and q must be congruent to 1 modulo 4.

If $p \equiv -q \pmod 4$ then $p + q = 4a$ for some integer a, from which it follows that $p \equiv -q \pmod{4a}$. Euler's conjecture assures us that once again $(a|p) = (a|q)$.

Substitute $p = 4a - q$ into $(p|q)$ to obtain

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{a}{q}\right).$$

Similarly, substitute $q = 4a - p$ into $(q|p)$ to obtain

$$\left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{a}{p}\right).$$

Since $(a|p) = (a|q)$

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

and the proof is complete.

The law of reciprocity, along with what we know about $(-1|p)$ and $(2|p)$, allows us to evaluate any Legendre symbol much more easily than by brute force. For example, consider $(34|97)$. Since $34 = 17 \times 2$,

$$\left(\frac{34}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{17}{97}\right).$$

Implementing the evaluation of a Legendre symbol as a computer program is an interesting exercise.

The modulus 97 is 1 modulo 8, so $(2|97) = 1$. We can flip $(17|97)$ because $17 \equiv 1 \pmod 4$; consequently

$$\left(\frac{17}{97}\right) = \left(\frac{97}{17}\right) = \left(\frac{12}{17}\right).$$

Apply the same procedure for $(12|17)$; as $12 = 3 \times 4$ we compute $(12|17) = (3|17)(4|17) = (3|17)$. Then $(3|17) = (17|3) = (2|3) = -1$. Hence

$$\left(\frac{34}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{17}{97}\right) = 1 \times (-1) = -1.$$