Melbourne High School
Maths Extension Group 2023
Term 4 Week 3 Handout Solutions

Problems

1. Note that we can't have a blue boy, otherwise the whole circle would be boys. Then clearly the boys are all red and alternate, with the girls in between. Hence we can determine the precise number of boys (10 boys and 10 girls).

2. Let M be the midpoint of AC, then $OM \perp AC$, since $\triangle PXY$ is similar to $\triangle APC$, $XY|AC$ and hence $XY \perp OM$. Similarly, $OX \perp YM$ and $OY \perp XM$, and so M coincides with H. Since M is a fixed point, we are done.

3. We need a minimum of 50 dollars since the free operation does not change the parity of the number of places of the counters. Since each counter needs to change parity, we need at least 100 changes, which means 50 non-free operations. We will now show it is achievable with 50 dollars. Colour the places in the row into four colours: $abcdabcdabcd \ldots abcd$. Let us interchange all pairs bc and da for 49 dollars. Now move the counters 1 and 100 to the adjacent positions and then interchange them remaining 1 dollar. Now all the counters that were standing on the colour a are standing on the colour d, and counters that were standing on colour b are standing on the colour c etc. Thus we can finish off rearranging them using the free operations.

4. Let N be a point on the extension of ML such that $LN = ML$. Since $KMLC$ is cyclic, we have $\angle BLN = \angle AKM$ and so $\triangle AMK \cong \triangle LBN (SAS)$. Because $\angle LBN = \angle MAK$, we have that $\angle MBN = 90^\circ$. Thus L is the circumcentre of $\triangle MBN$ and hence $BL = ML$ since they are the radii.

The Jacobi Symbol

Firstly, the motivation: we know how to evaluate $(a|p)$ now, but the difficulty is that we have to factorise a. For small values of a factorisation is easy; but in general computing the prime factorisation of a number is terribly difficult. This problem would be solved if we could flip $(a|p)$ and then reduce modulo p modulo a, which would reduce the size of the numbers we are dealing with. If we keep doing this we will get Legendre symbols that are easier to evaluate. Thus we define a new symbol, a generalised version of the Legendre symbol.

That symbol is defined as

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$$

and is known as the *Jacobi Symbol.* As we shall show, this symbol has properties that are remarkably similar to that of the Legendre symbol. Remember throughout that the bottom number, b, must be a positive odd integer for the symbol to have any meaning.

Firstly, what does the symbol mean? If $(a|b) = 1$, does it mean that the congruence

$$x^2 \equiv a \pmod{b}$$

has a solution? From the definition, $(a|b)$ is the product of r Legendre symbols, each of which is either 1 or -1, assuming that a and b are coprime. Of course if they are not, then $(a|b) = 0$, which is analogous to $(a|p) = 0$ when $a \equiv 0 \pmod{p}$.

So if there are an even number of Legendre symbols that have the value -1, then $(a|b) = 1$, and if there are an odd number, $(a|b) = -1$. However, for a to be a quadratic residue modulo b, the congruence

$$a \equiv x^2 \pmod{p_i}$$

must be soluble for all values of i; that is, a must be a quadratic residue modulo every prime that divides b. But if there are two primes in the prime factorisation of b for which a is a quadratic nonresidue, then $(a|b)$ still equals 1. Therefore when $(a|b) = 1$ it is not always true that a is a quadratic residue modulo b. However, when $(a|b) = -1$, it is indeed true that a is a quadratic nonresidue modulo b.

First things first: let's prove that the Jacobi symbol satisfies the same multiplicative property as the Legendre symbol. Let $b = p_1 p_2 \cdots p_r$ be a product of odd primes and $a = a_1 a_2$. Then

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1 a_2}{p_1}\right)\left(\frac{a_1 a_2}{p_2}\right)\cdots\left(\frac{a_1 a_2}{p_r}\right).$$

Each Legendre symbol can then be separated using its multiplicative property, viz.

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{p_1}\right)\left(\frac{a_2}{p_1}\right)\left(\frac{a_1}{p_2}\right)\left(\frac{a_2}{p_2}\right)\cdots\left(\frac{a_1}{p_r}\right)\left(\frac{a_2}{p_r}\right).$$

Now collect all the Legendre symbols with a_1 at the top; the value of all these multiplied together is $(a_1|b)$ by definition; the same goes for $(a_2|b)$. Therefore

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right).$$

That looks to be a good start. Now let's tackle $(-1|b)$. By definition

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_r}\right).$$

The only Legendre symbols that matter are those with primes congruent to 3 modulo 4 at the bottom, because we know that $(-1|p) = 1$ when $p \equiv 1 \pmod 4$ and $(-1|p) = -1$ when $p \equiv 3 \pmod 4$. Let s be the number of primes in the prime factorisation of b that are congruent to 3 modulo 4. Then $(-1|b) = \pm 1$ according to whether s is even or odd. If s is even, then $b \equiv 1 \pmod 4$ because the product of an even number of numbers congruent to 3 modulo 4 is congruent to 1 modulo 4. Similarly if s is odd, then $b \equiv 3 \pmod 4$. Thus we derive the following result:

Perhaps an easier way is to think of 3 as -1 modulo 4, so multiplying x numbers together that are each 3 modulo 4 is the same as computing $(-1)^x$ modulo 4, which is ± 1 according to whether x is even or odd.

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

Now let's tackle $(2|b)$. By definition

$$\left(\frac{2}{b}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_r}\right).$$

Again we ignore any primes that are congruent to 1 or -1 modulo 8, because the value of the Legendre symbols in these cases is 1. The number of Legendre symbols that equal -1 is the number of primes in the prime factorisation of b that are congruent to 3 or 5 modulo 8, so if this number is even then $(-1|b) = 1$ and if it is odd then $(-1|b) = -1$; let this number be s. If s even then b must be congruent to 1 or -1 modulo 8, for if we take 5 to be -3 modulo 8, the product of two numbers that are congruent to ± 3 modulo 8 is $\pm 3 \times \pm 3 \equiv \pm 9 \equiv \pm 1 \pmod 8$. Similarly if s is odd then b is congruent to 3 or 5 modulo 8. Thus we have

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

Note how the two properties of the Jacobi symbol are virtually identical to that of the Legendre symbol. This observation leads us to believe that there is an equivalent formulation of the law of quadratic reciprocity for the Jacobi symbol.

Consider the Jacobi symbol $(a|b)$ where this time we also impose the condition that a is positive and odd. If a is negative then we can factor our $(-1|b)$ from the multiplicative property proved earlier; similarly, if a is even we can factor as many $(2|b)$ terms as is necessary to make it odd. We know how to evaluate $(-1|b)$ and $(2|b)$, so all that is left to do is evaluate $(a|b)$ for positive odd values of a.

Once again we start from the definition of the Jacobi symbol and write

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right).$$

Each of the Legendre symbols can then be expanded by factorising a as $a = q_1 q_2 \cdots q_s$, thusly:

$$\left(\frac{a}{b}\right) = \prod_{k=1}^{s}\left(\frac{q_k}{p_1}\right)\prod_{k=1}^{s}\left(\frac{q_k}{p_2}\right)\cdots\prod_{k=1}^{s}\left(\frac{q_k}{p_r}\right). \tag{1}$$

Each of the products of Legendre symbols can be flipped from the law of quadratic reciprocity. If we could flip every single Legendre symbol without introducing any minus signs (for example, if every p_i is 1 modulo 4), then we would get

$$\left(\frac{a}{b}\right) = \prod_{k=1}^{s}\left(\frac{p_1}{q_k}\right)\prod_{k=1}^{s}\left(\frac{p_2}{q_k}\right)\cdots\prod_{k=1}^{s}\left(\frac{p_r}{q_k}\right).$$

Expanding the products again, we get

$$\left(\frac{a}{b}\right) = \left(\frac{p_1}{a}\right)\left(\frac{p_2}{a}\right)\cdots\left(\frac{p_r}{a}\right) = \left(\frac{b}{a}\right).$$

Evidently, however, in general a certain number of minus signs will be introduced when flipping the Legendre symbols.

First let's consider the case where $a \equiv b \equiv 3 \pmod 4$. In this case there are an odd number of primes in the prime factorisations of a and b that are 3 modulo 4. Suppose that p_1 is one of those primes for b and consider the product

$$\prod_{k=1}^{s}\left(\frac{q_k}{p_1}\right),$$

one of the products in Equation (1). When each Legendre symbol in this product is flipped, a minus sign will be added whenever $q_k \equiv 3 \pmod 4$. Since $a \equiv 3 \pmod 4$ by assumption, there will be an odd number of minus signs, and so

$$\prod_{k=1}^{s}\left(\frac{q_k}{p_1}\right) = -\prod_{k=1}^{s}\left(\frac{p_1}{q_k}\right).$$

This is true not only of p_1, but of any prime p_i that is congruent to 3 modulo 4. Since there are an odd number of such primes in the prime factorisation of b, flipping every Legendre symbol introduces an odd number of minus signs; hence

$$\left(\frac{a}{b}\right) = -\left(\frac{b}{a}\right).$$

That's one case out of the way. Now let $b \equiv 1 \pmod 4$ and $a \equiv 3 \pmod 4$. Clearly all of the prime factors of b might be congruent to 1 modulo 4, in which case every single Legendre symbol in Equation (1) can be flipped without changing any signs, leaving us with

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

If b does have some prime factors congruent to 3 modulo 4, then there must be an even number of them. Suppose p_1 is one of these primes, and consider the product

$$\prod_{k=1}^{s}\left(\frac{q_k}{p_1}\right)$$

again. The number of prime factors of a that are congruent to 3 modulo 4 is odd because $a \equiv 3 \pmod 4$; from this it follows that in flipping all the Legendre symbols of the product an odd number of minus signs are introduced. So

$$\prod_{k=1}^{s}\left(\frac{q_k}{p_1}\right) = -\prod_{k=1}^{s}\left(\frac{p_1}{q_k}\right),$$

and likewise for any other p that is 3 modulo 4. But there are an even number of such primes, meaning that the minus signs cancel and we get

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

We should be able to convince ourselves that we get the same result when $a \equiv 1 \pmod 4$ and $b \equiv 3 \pmod 4$, but for the sake of completeness here is the argument. Again, if every prime factor of a is 1 modulo 4, then clearly

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

If that is not the case, we use the same reasoning as before, except in this case we know that at least one of the primes composing b is 3 modulo 4, and that there are an odd number of them. Suppose such a prime is p_1. The product

$$\prod_{k=1}^{s} \left(\frac{q_k}{p_1} \right)$$

can be flipped without changing the sign because there are either 0 or an even number of q_k that are congruent to 3 modulo 4; in the former case no minus signs are introduced, and in the latter case an even number of minus are introduced. This means we can flip every product in Equation (1) without worrying about any signs, and so

$$\left(\frac{a}{b} \right) = \left(\frac{b}{a} \right)$$

once again.

Now for the final case. This is the case where $a \equiv b \equiv 1 \pmod 4$. Perhaps it is clear by now what the outcome is to be: all the products in Equation (1) can be flipped without adding any minus signs, because for any product in which the bottom prime is congruent to 3 modulo 4, the number of minus signs introduced in flipping it is either 0 or an even number, there being 0 or an even number of q_k that are congruent to 3 modulo 4. Therefore

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

Summarising, we have shown that

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

This is sometimes called the *generalised law of quadratic reciprocity.*

The three results we have proved can be expressed as three equations that are exactly the same as those for the Legendre symbol:

$$\left(\frac{-1}{b} \right) = (-1)^{\frac{b-1}{2}} \qquad \left(\frac{2}{b} \right) = (-1)^{\frac{b^2-1}{8}} \qquad \left(\frac{a}{b} \right) \left(\frac{b}{a} \right) = (-1)^{\frac{a-1}{2} \frac{b-1}{2}}.$$