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

> *"Yes, universal history! It's the study of the successive follies of mankind and nothing more. The only subjects I respect are mathematics and natural science," said Kolya.*
>
> —F. Dostoevsky[1], *The Brothers Karamazov* (1880)

Don't listen to Kolya. History is a nice subject.

Problems

1. Twenty children stand in a circle (both boys and girls are present). For each boy, his clockwise neighbour is in a blue T-shirt, and for each girl, her counterclockwise neighbour is in a red T-shirt. Is it possible to determine the precise number of boys in the circle? ToT Spring 2016/1

2. Let ω be a circle with the centre O and two different points A and C on ω. For any point P on ω distinct from A and C let X and Y be the midpoints of AP and P respectively. Furthermore, let H be the point where the altitudes of triangle OXY meet. Prove that the position of the point H does not depend on the choice of P. ToT Fall 2019/2

3. There is a row of 100 cells each containing a token. For 1 dollar it is allowed to interchange two neighbouring tokens. Also it is allowed to interchange with no charge any two tokens such that there are exactly 3 tokens between them. What is the minimum price for arranging all the tokens in the reverse order? ToT Fall 2019/3

4. In a right-angled triangle ABC ($\angle C = 90^\circ$) points K, L and M are chosen on sides AC, BC and AB respectively so that $AK = BL = a$, $KM = LM = b$ and $\angle KML = 90^\circ$. Prove that $a = b$. ToT Fall 2015/4

[1] Translated from the Russian by C. Garnett

We may have succeeded at the price of too much eccentricity, or we may have failed; but we can hardly have failed completely, the subject matter being so attractive that only extravagant incompetence could make it dull.

—G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers* (1938)

Gauss, Eisenstein, and the Proof

The proof of quadratic reciprocity from Euler's conjecture is straightforward, but not the most beautiful, requiring complex manipulation of inequalities and intervals. Here we discuss a second proof that is decidedly simpler and more enlightening.

For this proof we have Gauss to thank. The geometric twist is due to Eisenstein.

Let's solidify some notation first. The pronumerals p and q refer to distinct odd primes. Let $P = (p-1)/2$ and $Q = (q-1)/2$. Let $v(a,p)$ be the number of minus signs in the set formed by reducing the numbers

$$a, 2a, \ldots, \frac{p-1}{2}a$$

into the range $(-p/2, p/2)$. From Gauss's Lemma

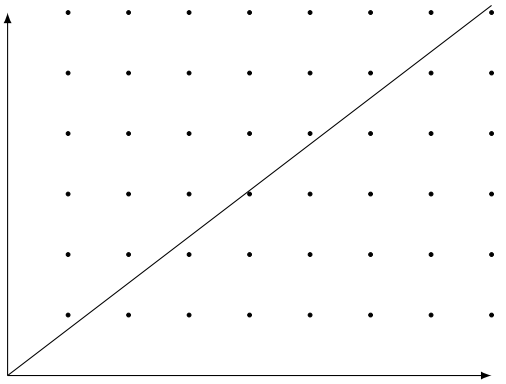
$$\left(\frac{a}{p}\right) = (-1)^{v(a,p)}.$$

(Before, this value was denoted just as v.) Next: let

Those who have done some of the previous exercises have no doubt already met this strange creature.

$$S(q,p) = \sum_{k=1}^{P} \left\lfloor \frac{kq}{p} \right\rfloor.$$

The value of $S(q,p)$ has a geometric meaning. In the example diagram below $p = 17$ and $q = 13$. Each dot is a lattice point, a point with



This diagram was a pain to create.

integer coordinates; in what follows disregard any lattice points on the coordinate axes.

The diagonal line is the line $y = 13x/17$. It does not cross any lattice points, because the first lattice point on the line that is not the origin is $(17, 13)$.

By definition, $S(13,17) = \sum_{k=1}^{8} \lfloor 13k/17 \rfloor$. The number $13k/17$ is the value of the line at the point $x = k$; and hence $\lfloor 13k/17 \rfloor$ is the *number of lattice points* below the line with x-coordinate equal to k. For example, if $x = 3$ the y-value is $39/17$, the floor of which is 2, corresponding to the 2 lattice points on the vertical line $x = 3$ that lie below the line $y = 13x/17$.

Hence $S(13,17)$ is the number of lattice points under the line $y = 13x/17$ bounded horizontally by the lines $x = 0$ and $x = 8$. If, however,

the plane is flipped so that the x-axis becomes the y-axis and the y-axis becomes the x-axis, the equation of the line becomes $y = 17x/13$ and the number of lattice points below the line bounded by the lines $x = 0$ and $x = 6$ is $S(17, 13)$. This number $S(17, 13)$ is the also the number of lattice points above the line $y = 13x/17$ bounded by the lines $y = 0$ and $y = 6$ in the original version of the plane. Plainly the total number of lattice points in the rectangle bounded by the x-axis, the y-axis, the line $x = 8$, and the line $y = 6$ is $6 \times 8 = 48$, so

Remember that we don't count the lattice points on the horizontal and vertical axes.

$$S(17, 13) + S(13, 17) = 48 = \frac{(13-1)}{2}\frac{(17-1)}{2}.$$

Note that the same argument applies even if p and q are unspecified. The line $y = qx/p$ splits the number of lattice points in the rectangle bounded by the axes and the lines $x = P$ and $y = Q$ into two triangles with no lattice point lying on the line itself. The number below the line is $S(q, p)$, the number above the line is $S(p, q)$, and the total number is PQ; hence

Isn't this beautiful?

$$S(q, p) + S(p, q) = PQ = \frac{(p-1)}{2}\frac{(q-1)}{2}.$$

Now consider the quotient when kq is divided p with a remainder that lies between $-p/2$ and $p/2$. That is, let

$$kq = q_k p + r_k \tag{1}$$

where $-p/2 < r_k < p/2$. Rearranging for kq/p yields

$$\frac{kq}{p} = q_k + \frac{r_k}{p}.$$

From this equation it follows that

$$\left\lfloor \frac{kq}{p} \right\rfloor = \begin{cases} q_k, & \text{if } r_k > 0; \\ q_k - 1, & \text{if } r_k < 0. \end{cases}$$

Therefore $S(q, p)$ is the sum of the quotients q_k minus the number of times $\lfloor kq/p \rfloor = q_k - 1$. How many times does this happen?

It happens whenever one of the remainders r_k is negative. These remainders are obtained by reducing multiples of q to be between $-p/2$ and $p/2$; hence the number of times $\lfloor kq/p \rfloor = q_k - 1$ is exactly $v(q, p)$. This implies

We don't need to consider the case $r_k = 0$ because p and q are distinct odd primes. The first positive value of k for which dividing qk by p leaves no remainder is $k = p$; here we consider only the values of k from 1 to $(p-1)/2$.

$$S(q, p) = \sum_{k=1}^{P} q_k - v(q, p). \tag{2}$$

Next: what is the sum of those quotients? From Equation (1)

$$q_k p = kq - r_k$$

and so, on summing both sides from $k = 1$ to $k = P$,

$$\sum_{k=1}^{P} q_k p = \sum_{k=1}^{P} kq - r_k.$$

Split the right-hand sum into two sums and take the constants p and q out of the summation signs to get

$$p \sum_{k=1}^{P} q_k = q \sum_{k=1}^{P} k - \sum_{k=1}^{P} r_k.$$

Consider this equation modulo 2. Since p and q are odd primes, they disappear, leaving

$$\sum_{k=1}^{P} q_k \equiv \sum_{k=1}^{P} k - \sum_{k=1}^{P} r_k \pmod 2.$$

The numbers r_k are the remainders on reducing numbers of the form kq to be in the range $(-p/2, p/2)$; from the proof of Gauss's Lemma, amongst these remainders the numbers $1, 2, \ldots, P$ appear exactly once, with either a positive or negative sign but not both. The signs don't matter since $-1 \equiv 1 \pmod 2$, and so

$$\sum_{k=1}^{P} r_k \equiv 1 + 2 + \cdots + P \equiv \sum_{k=1}^{P} k \pmod 2.$$

A quick proof if you haven't seen Gauss's Lemma: if $iq \equiv jq$ (same sign) then $i \equiv q$ and hence $i = q$. If two remainders appear with the opposite sign then $iq \equiv -jq$ and hence $i + j \equiv 0$, which is impossible because $i, j \leq (p-1)/2$ and hence $i+j \leq p-1$.

Therefore

$$\sum_{k=1}^{P} q_k \equiv \sum_{k=1}^{P} k - \sum_{k=1}^{P} k \equiv 0 \pmod 2.$$

Reduce Equation (2) modulo 2; since $\sum_{k=1}^{P} q_k \equiv 0 \pmod 2$ it is clear, then, that

$$S(q,p) \equiv -v(q,p) \equiv v(q,p) \pmod 2.$$

Gauss's Lemma implies

$$\left(\frac{q}{p}\right) = (-1)^{v(q,p)} = (-1)^{S(q,p)}.$$

Similarly

$$\left(\frac{p}{q}\right) = (-1)^{v(p,q)} = (-1)^{S(p,q)}.$$

The proof is almost complete. From here it follows naturally that

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

But $S(q,p) + S(p,q) = (p-1)(q-1)/4$ and, consequently,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{3}$$

This equation is, in fact, an equivalent formulation of the law of quadratic reciprocity, and the one that is most common in the literature. The proof is simple. The exponent on the right is even whenever $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, and $(q|p)(p|q) = 1$ implies $(q|p) = (p|q)$. Similarly, the exponent is odd whenever $p \equiv q \equiv 3 \pmod 4$, and $(q|p)(p|q) = -1$ implies $(q|p) = -(p|q)$.

Thus ends a glorious journey into the world of quadratic residues. The nuggets of gold discovered are best summarised by the following three equations:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Who would have thought there was so much in the simple question of which numbers are squares modulo primes?

Problem

Generalise the Legendre symbol. Define a new symbol $(a|b)$, where b is a positive odd integer with prime factorisation $b = p_1 p_2 \cdots p_r$ and a is any other integer, to have the value

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

Discover and prove properties of this symbol.

If you're thinking of naming this symbol after yourself, Jacobi has beaten you to it.