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

> *If we arrive at an equation containing on each side the same term but with different coefficients, we must take equals from equals until we get one term equal to another term. But, if there are on one or on both sides negative terms, the deficiencies must be added on both bides until all the terms on both sides are positive. Then we must take equals from equals until one term is left on each side.*
>
> —Diophantus,[1] *Arithmetica* (c. 250 AD)

Problems in factorisation and Diphantine equations

1. Find integers (x, y) such that $x^2 = 12 + y^2$.

2. Find all paris of integers (b, c) such that

$$2b + 3c = bc.$$

3. Determine all non negative integral pairs (x, y) for which INMO

$$(xy - 7)^2 = x^2 + y^2.$$

4. The integer n is positive. There are exactly 2005 ordered pairs (x, y) of positive integers satisfying BMO Round 3 2015

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}.$$

   Prove that n is a perfect square.

5. Determine all pairs (x, y) of integers such that IMO 2006/4

$$1 + 2^x + 2^{2x+1} = y^2.$$

[1] As quoted by Thomas Little Heath in *Diophantus of Alexandria* (1885)

The mathematician's patterns, like the painter's or the poet's, must be beautiful*; the ideas, like the colours or the words, must fit together in a harmonious way. Beuaty is the first test: there is no permanent place in the world for ugly mathematics.*

—G. H. Hardy, *A Mathematician's Apology* (1940)

Quadratic Residues

Be aware that we are now entering a most beautiful area of number theory; prepare yourself.

Having conquered linear congruences, let's turn to quadratic congruences. The central question in this area of number theory is:

When is the congruence $x^2 \equiv a \pmod{m}$ solvable?

Note that we are primarily interested in *when* the congruence has a solution, not what the solutions are (if there are any).

As should be familiar by now, we start by considering when m is prime. Therefore our main goal is to determine when

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

is solvable. Let's begin with the congruence

$$x^2 \equiv 3 \pmod{7},$$

Is there a solution? Since the modulus is small it is easy to run through all the possibilities, like so:

$$\begin{aligned} 1^2 &\equiv 1 \pmod{7} \\ 2^2 &\equiv 4 \pmod{7} \\ 3^2 &\equiv 2 \pmod{7} \\ 4^2 &\equiv 2 \pmod{7} \\ 5^2 &\equiv 4 \pmod{7} \\ 6^2 &\equiv 1 \pmod{7} \end{aligned}$$

It looks like our equation is not solvable, as when numbers are squared modulo 7, the only possible residues are 1, 2, and 4. We note that $3^2 \equiv 4^2$, $2^2 \equiv 5^2$, $1^2 \equiv 6^2$, but after some thought this is hardly surprising, as $1 \equiv= 6$, $2 \equiv -5$, and $3 \equiv -4$ modulo 7.

Let's try another example, this time with the congruence

$$x^2 \equiv 10 \pmod{7}.$$

If we run through the possible values of x again, we find that the squares are congruent to $1, 4, 9, 5, 3$ only. Therefore our congruence is not solvable.

The numbers that are congruent to squares modulo a particular prime—$1, 2, 4$ in the case of modulo 7 and $1, 4, 9, 5, 3$ in the case of modulo 11—have a special name; they are called *quadratic residues*. Numbers that are not quadratic residues are called *quadratic nonresidues*. In other words if a is a quadratic residue modulo p, the congruence

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

is solvable; if a is a quadratic nonresidue, then the congruence is not solvable. We always exclude 0 has a quadratic residue, not only because it is trivial, but also because it simplifies many of our arguments, as will be seen shortly. Additionally, in general we consider only odd

primes, leaving 2 for special cases because modulo 2 every number is a quadratic residue.

All the quadratic residues of a given prime can be found by running x through a set of positive residues, like we did above. As one further example, let's find the quadratic residues modulo 13: $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 3$, $5^2 \equiv 12$, and $6^2 \equiv 10$. As you might have realised already, we do not need to go further than 6, for the residues repeat. Therefore the quadratic residues modulo 13 are $1, 4, 9, 3, 12, 10$.

That is, $7^2 \equiv 10$, $8^2 \equiv 12$, and so on, as you can verify.

Let's turn to the general case. The first question, which you may have already answered, is: How many quadratic residues are there modulo an odd prime p? (Remember that we exclude 2 from all of these investigations.) From the examples above, it seems that the numbers

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

are all incongruent and therefore form quadratic residues, and all the numbers greater than $(p-1)/2$ and less than p form the same set of quadratic residues but in reverse order. A consequence of this is that there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues, which is consistent with the above examples.

How do we prove this hypothesis? An easy way is using primitive roots. If $a \equiv x^2$ is a quadratic residue and α is the index of x, then

Another way is to show that if a and b are both less than $p/2$, then $a^2 \not\equiv b^2$.

$$a \equiv g^{2\alpha} \pmod{p}.$$

The index of a is 2α reduced modulo $p-1$, and since $p-1$ is even, the index of a is even. Hence if a is a quadratic residue then its index is even. The contrapositive: if the index of a is odd, then a is a quadratic nonresidue. Combining these two statements, it follows that the quadratic residues modulo p are precisely those numbers with even indices, and the quadratic nonresidues are precisely those numbers with odd indices. Indices range from 1 to $p-1$, and as there are $(p-1)/2$ even numbers and $(p-1)/2$ odd numbers in that range, there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues.

You may verify this by constructing a table of indices for 11 using 2 as the primitive root; you will see that the indices of the quadratic residues 1, 4, 9, 5, and 3 are the even numbers 10, 2, 6, 4, and 8 respectively.

The connection between primitive roots and quadratic residues allows us to formulate a simple multiplicative property. Recall that multiplying numbers modulo p is equivalent to adding their indices and reducing that index modulo $p-1$ if necessary. If two quadratic residues are multiplied, the sum of their indices, which are both even, is also even, and so the product is another quadratic residue. If a quadratic residue is multiplied by a quadratic nonresidue, an even index and an odd index are added together; the resulting index is odd and so the product is a quadratic nonresidue. Finally, if two quadratic nonresidues are multiplied, the resulting index is even because the sum of two odd numbers is even. It follows that the product of two quadratic nonresidues is a quadratic residue.

These multiplicative rules bear a strange resemblance to the rules governing the multiplication of positive and negative numbers. Indeed, if we take a quadratic residue to be represented by the number 1 and a quadratic nonresidue to be represented by the number -1, the multiplicative properties hold, for

$$\begin{aligned} 1 \times 1 &= 1, \\ 1 \times -1 &= -1, \\ -1 \times -1 &= 1. \end{aligned}$$

These multiplicative properties led Legendre to come up with a convenient symbol, called the *Legendre symbol*, to represent whether a

certain number a is a quadratic residue modulo some prime p. It is defined as follows.

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

For ease of display, when the Legendre symbol is to be used inline, it will be denoted (a|p).

Problems

1. Is the congruence
$$x^2 \equiv -1 \pmod{17}$$
solvable?

2. Prove the following two properties of the Legendre symbol:
   (a) $(ab|p) = (a|p)(b|p)$.
   (b) If $a \equiv b \pmod{p}$ then $(a|p) = (b|p)$.

3. Wilson's Theorem states that
$$(p-1)! \equiv -1 \pmod{p}.$$
Use Wilson's Theorem and the results about quadratic residues developed above to find for which primes -1 is a quadratic residue and for which primes -1 is a quadratic nonresidue.

This result is a very famous one and forms the first supplement to the *Law of Quadratic Reciprocity*.