Melbourne High School
Maths Extension Group 2023
Term 3 Week 5 Handout

Greek algebra before Diophantus was essentially rhetorical.

—T. Dantzig, *Number: The Language of Science* (1954)

More factorisation and Diophantine equation problems

1. Show that for every integer $n > 1$ it is possible to write $\frac{1}{n}$ as a sum of two reciprocals of distinct positive integers.

2. Find $3x^2y^2$ if x and y are integers such that $y^2 + 3x^2y^2 = 30x^2 + 517$. AIME 1987/5

3. Find all integer solutions to the equation
$$(x - y)^2 = x + y.$$

4. Tyler has a large number of square tiles, all the same size. He has four times as many blue tiles as red tiles. He builds a large rectangle using all the tiles, with the red tiles forming a boundary 1 tile wide around the blue tiles. He then breaks up this rectangle and uses the tiles to make two smaller rectangles. Like the large rectangle, each of the smaller rectangles has four times as many blue tiles as red tiles, and the red tiles form a boundary 1 tile wide around the blue tiles. How many blue tiles does Tyler have? AMC Intermediate 2021/30

5. Factor $a^4 + 4b^4$. Sophie Germain's Identity

…knowledge of every truth is a worthy matter in itself…

—L. Euler[1], *Theorems on Divisors of Numbers* (1748)

Euler's Criterion

Refer to the previous handout for particulars.

Let's recap what has been covered so far in the story of quadratic residues. A quadratic residue modulo some odd prime p is a nonzero number a such that the congruence

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

is solvable. A number that is not a quadratic residue is a quadratic nonresidue, or just nonresidue for short if there is no chance of ambiguity. Among the numbers $1, 2, \ldots, p-1$ there are the same number of quadratic residues as nonresidues; there are $(p-1)/2$ of each. A consequence of this fact is that quadratic residues and nonresidues satisfy the same multiplicative property as 1 and -1. That is, the product of a residue and a nonresidue is a nonresidue, and the product of two residues or two nonresidues is a residue. This can be summarised using the Legendre symbol:

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

where

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

To continue our investigations, we look for a new goal. The most obvious one is to find a way to tell whether a given number is a quadratic residue of a prime. In other words, is there an easy way to evaluate $(a|p)$?

As a sneak peek for things to come, this problem can be broken down into three stages. First we need a way to evaluate $(-1|p)$, then $(2|p)$, and finally $(q|p)$ for any odd prime q. Since $(ab|p) = (a|p)(a|p)$ solving those three cases suffices to let us find $(a|p)$ for any a.

Of course, the brute force approach of enumerating the quadratic residues is guaranteed to give the right answer, but clearly the mathematician has no interest in this method. It is tedious, inelegant, and given the hints of beauty in the theory already developed, it is likely that there is a better way—some connection or theorem we have yet to discover.

Let's go back to Fermat's Little Theorem. It states that

$$a^{p-1} \equiv 1 \pmod{p}$$

for all $a \not\equiv 0$. Since p is an odd prime, $p-1$ is even, and therefore if we set $P = (p-1)/2$, the left-hand side can be factorised to give

$$(a^P - 1)(a^P + 1) \equiv 1 \pmod{p}.$$

Since the modulus is prime, either

$$a^P \equiv 1 \pmod{p}$$

or

$$a^P \equiv -1 \pmod{p}.$$

What is the distinction between these two cases? Clearly some numerical data would be useful. Suppose that $p = 7$. Let's run a through the values $1, \ldots, 6$ and compute a^P.

[1] Translated by David Zhao from Latin, in which the title was *Theoremata Circa Divisores Numerorum.*

a	1	2	3	4	5	6
$a^3 \pmod 7$	1	1	-1	1	-1	-1

One example may not be enough to establish the pattern, so here is another. This time $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$a^5 \pmod{11}$	1	-1	1	1	1	-1	-1	-1	1	-1

The first thing we notice about the two examples is that -1 and 1 appear the same number of times; there are $(p-1)/2$ of each. This alone is enough to suggest that there is some connection with quadratic residues. This connection is obvious if we look a little closer. Each 1 appears whenever a is a quadratic residue and each -1 appears whenever a is a quadratic nonresidue.

Verify this by finding the quadratic residues by hand. Then try a few more values of p to convince yourself that the pattern does indeed continue.

A few more examples would be enough to allow us to make a conjecture. We conjecture that $a^P \equiv 1$ if a is a quadratic residue and $a^p \equiv -1$ if a is a quadratic nonresidue. But 1 and -1 are exactly the possibilities of the Legendre symbol (excluding 0 because right from the beginning in using Fermat's Little Theorem we have taken $a \not\equiv 0$), so our conjecture can be expressed as

$$a^P \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$$

for $a \not\equiv 0$. In fact the conjecture is also true, albeit trivially so, when $a \equiv 0$.

The result we have just discovered is known as *Euler's Criterion*. At this point we have some intuition as to why it is true, but a proper proof is needed. Here is that proper proof.

If a is a quadratic residue, then

$$a \equiv x^2 \pmod p.$$

Hence

$$a^P \equiv a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$$

by Fermat's Little Theorem. The first part of the proof is complete.

Now consider the general congruence

$$x^{(p-1)/2} - 1 \equiv 0 \pmod p.$$

From Lagrange's Theorem there are at most $(p-1)/2$ solutions, and we have just shown that if a is a quadratic residue, then it is a solution to that equation. Since there are exactly $(p-1)/2$ quadratic residues, it follows that every quadratic residue is a solution to the above equation, and every solution to the above equation is a quadratic residue. The two statements are thus equivalent.

Recall that Lagrange's Theorem guarantees that a polynomial congruence of degree d modulo a prime has at most d incongruent roots.

For the second part of the proof, the case where a is a quadratic nonresidue, we have to go back to the equation

$$(a^P - 1)(a^P + 1) \equiv 0 \pmod p.$$

We know that either $a^P - 1 \equiv 0$ or $a^P + 1 \equiv 0$; but the former cannot be true because we have just proved that if that were the case, then a would be a quadratic residue. Thus the latter is true and

$$a^P \equiv a^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p,$$

completing the proof of the theorem.

How does this help us evaluate the Legendre symbol? The answer is that it doesn't, at least not directly, because it is often inconvenient

to calculate $a^{(p-1)/2}$. The only value of a for which it gives us a direct solution to the problem is $a = -1$, for substituting this in gives

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

Since both sides are equal to either -1 or 1, we may do away with the congruence and write it as an equation:

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

(We don't have this liberty for other values of a.) From this equation it is clear that $(a|p)$ is equal to 1 or -1 depending on whether $(p-1)/2$ is even or odd, and $(p-1)/2$ is even if $p \equiv 1 \pmod 4$ and odd if $p \equiv 3 \pmod 4$. Thus -1 is a quadratic residue of all primes of the form $4k+1$ and a nonresidue of all those of the form $4k+3$.

This is the result proved in the last exercise to last week's handout; the difference is that there it was proved using primitive roots. Euler's Criterion gives an immediate proof.

Although Euler's Criterion gives us a direct way to evaluate $(-1|p)$ only, it will be needed to prove *Gauss's Lemma*. And Gauss's Lemma is central to this entire theory and is used to prove the ultimate, beautiful, golden theorem.

Problems

1. Show that if $p \equiv 1 \pmod 4$, then the quadratic character of a (whether it is a residue or nonresidue) is the same as that of $p-a$, and if $p \equiv 3 \pmod 4$, then the quadratic character of a is opposite that of $p-a$.

2. Prove Euler's Criterion using primitive roots and indices. (Hint: If g is a primitive root and $g^l \equiv 1$, then l must be a multiple of $p-1$.)

3. Use Wilson's Theorem to come up with a construction for the solutions to the equation

   $$x^2 + 1 \equiv 0 \pmod{p}$$

   when $p \equiv 1 \pmod 4$.

This is a hard problem.