Melbourne High School
Maths Extension Group 2023
Term 3 Week 6 Handout

out[8]=

$$\left\{\left\{x \to -\frac{2i\pi c_1 + \ln 2 - \ln 3}{\ln 2 + \ln 3} \ \textit{if}\ c_1 \in \mathbb{Z}\right\},\right.$$
$$\left.\left\{x \to -1 - \frac{2i\pi c_1}{-\ln 2 + \ln 3} \ \textit{if}\ c_1 \in \mathbb{Z}\right\}\right\}$$

—Mathematica (2023)

Problems in solving equations

1. Find all x such that $-4 < \frac{1}{x} < 3$.
2. Solve the following system of equations
$$xy = 12\sqrt{6}$$
$$yz = 54\sqrt{2}$$
$$zx = 48\sqrt{3}.$$
3. Find all real numbers x for which
$$\frac{8^x + 27^x}{12^x + 18^x} = \frac{7}{6}.$$
4. Mr Fat is going to pick three non-zero real numbers and Mr Taf is going to arrange the three numbers as coefficients of a quadratic equation USSR 1990
$$\_\_\_\_x^2 + \_\_\_\_x + \_\_\_\_ = 0$$
Mr Fat wins the game if and only if the resulting equation has two distinct rational solutions. Who has the winning strategy?
5. Find a triple of rational numbers (a, b, c) such that ARML 1997
$$\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{a} + \sqrt[3]{b} + \sqrt[3]{c}.$$

! Missing delimiter (. inserted).

—`lualatex` (2023)

Gauss's Lemma

We have seen that Euler's Criterion doesn't provide a good way to evaluate $(a|p)$ except when $a = -1$. When $a \neq -1$, how do we attack the problem?

The answer is that Euler's Criterion can be used to prove something called *Gauss's Lemma*, which, in theory although not in practice, would allow us to evaluate $(a|p)$ for any a. In other words, using Gauss's Lemma we can find all the primes for which $2, 3, 5, 7, 11, \ldots$ are quadratic residues.

The lemma and its proof are hard to motivate despite their simplicity. In fact, the proof is very similar to Ivory's proof of Fermat's Little Theorem. But how anyone could have come up with the lemma in the first place is somewhat mystifying.

The fact that Gauss was one of the greatest mathematicians of all time might have had something to do with it.

The lemma is as follows. Given a number a and an odd prime p, let $P = (p-1)/2$ and form the set of numbers

$$A = a, 2a, \ldots, Pa.$$

The set of integers in the range $(-p/2, p/2)$ form a complete set of residues, so every number in the above list can be reduced to a number in that range. The rule for this reduction is simple; if ja reduced modulo p is greater than $p/2$, then reduce it further into the range $(-p/2, 0)$; otherwise, leave it because it's already in the range $(0, p/2)$. Let B be the set of numbers in A that are reduced in this manner. The numbers in B are all in the range $(-p/2, p/2)$.

In the set B clearly there are some numbers that are positive and some that are negative. If we count the number of negative numbers in the set and call that number v, then

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

This is Gauss's Lemma.

Let's make things a little clearer with a numerical example. Suppose $a = 3$ and $p = 7$. We would like to know if 3 is a quadratic residue modulo 7. Following the above procedure, we set $P = (7-1)/2 = 3$ and form the numbers $a, 2a, \ldots, Pa$. Thus we have

Numerical examples, although no substitute for proper proofs, are key in number theory because they allow us to formulate conjectures or verify the truth of a general case that would otherwise be impossible to guess. It is said that based on numerical evidence Gauss guessed the Prime Number Theorem, although the proof was not discovered until some years after his death.

$$A = \{3, 6, 9\}.$$

Reducing this set into the range $(-p/2, p/2) = (-7/2, 7/2)$ to get B, we have

$$B = \{3, -1, 2\}.$$

The number of negative numbers is 1, so

$$\left(\frac{3}{7}\right) = (-1)^1 = -1$$

and thus 3 is not a quadratic residue modulo 7.

Check this by enumerating the quadratic residues modulo 7 as shown in previous handouts.

Here is another example before we begin the proof. This time let $p = 11$ and $a = 5$. We would like to know whether 5 is a quadratic residue modulo 11.

As before, set $P = (11-1)/2 = 5$. Then form the set

$$A = \{5, 10, 15, 20, 25\}.$$

Reduce each element of that set into the range $(-11/2, 11/2)$ and we get

$$B = \{5, -1, 4, -2, 3\}.$$

The number of negative numbers is B is 2, and therefore

$$\left(\frac{5}{11}\right) = (-1)^2 = 1.$$

Verify this by noting that $4^2 \equiv 5 \pmod{11}$.

Now we begin the proof. Take the sets A and B to be the formed as described above. Two things are immediately clear to us about the numbers in B. No two numbers of the set are equal; if $ia \equiv ja \pmod{p}$ then $i \equiv j$ because $a \not\equiv 0$, and since $i, j < P$ we have $i = j$. On the other hand, it is also not possible for $ia \equiv -ja \pmod{p}$ (that is, if we take the absolute value of all the numbers in B, we won't get two duplicates); for if that is the case then $ia + ja \equiv 0 \pmod{p}$ and since $a \not\equiv 0$ we must have $i + j \equiv 0$. This is clearly impossible because $i, j \leq P$ and so $i + j \leq 2P = p - 1$.

Therefore the numbers $1, 2, \dots, P$ appear exactly once in B with either a positive or negative sign, but not both, and each number in B is congruent to one and only one number in A. Thus the products of the two sets are congruent. If we let v be the number of negative signs in B, we have

$$a \times 2a \times \cdots \times Pa \equiv (-1)^v 1 \times 2 \times \cdots \times P \pmod{p}.$$

Condensing the products yields

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

Clearly $P! \not\equiv 0 \pmod{p}$, so

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

This is where Euler's Criterion comes into play. Recall that it states

$$a^P \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Consequently we have

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

which is the result we're trying to prove; the quadratic character of a is dependent only on the number of negative numbers in the set B, which is denoted here by v.

As stated previously, Gauss's Lemma allows us to determine $(a|p)$ for any $a \not\equiv 0$, but it can do much more than that. In fact we can go the other way and ask for which primes p is $(a|p) = 1$ for given values of a. For example, for which primes p is $(2|p) = 1$? That is, for which primes is 2 a quadratic residue? Yet another way of phrasing the question is to ask for which primes p the equation

$$x^2 - 2 \equiv 0 \pmod{p}$$

is solvable.

Note how the theory of quadratic residues is actually connected with *solving quadratic congruences*. Linear congruences were simple enough, but it seems quadratic ones are a different thing altogether.

The most natural way to proceed, perhaps the only way, is to blindly follow the steps of Gauss's Lemma and see how far the general case can lead us. So let $P = (p-1)/2$ and form the set

$$A = \{2, 4, \dots, 2P\}.$$

Note that $2P = p - 1$. This means that every member of A is in the range $(0, p-1)$. Now the question is: if we reduce each member of A into the range $(-p/2, p/2)$ to make B, how many numbers in B are negative?

Since every member of A is already less than p, the number of negative numbers in B is the same as the number of numbers in A that are greater than $p/2$. Let u be the number in the range $(1, P)$ satisfying

$$2u < p/2$$

and

$$2(u+1) > p/2.$$

Thus u is the number of numbers in A that are *less than* $p/2$; therefore the number of numbers in A that are greater than $p/2$ is

$$v = P - u = (p-1)/2 - u.$$

Now we just need to determine the parity of v based on some condition regarding p, because we know that

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

But this information seems to depend on both p and u, so we cannot just plug in $p = 4k+1$ or $p = 4k+3$ like we did for the case $a = -1$. What do we do instead?

There's nothing quite like a good cliffhanger.

Problems

1. Use Gauss's Lemma to find $(5|19)$.

2. Determine whether 2 is a quadratic residue for as many primes as you can, starting $3, 5, 7, 11, \ldots$. Do you see any patterns that might give us a clue as to how to finish the above proof of the quadratic character of 2?

3. (Continuation of the above proof of the quadratic character of 2)

   (a) If
   $$a < u < b$$
   find a and b in terms of p.

   (b) If we are optimistic, perhaps $(2|p)$ has something to do with whether $p \equiv 1$ or $p \equiv -1$ modulo 4, as for the case $a = -1$. Let $p = 4k+1$ and $p = 4k+3$ and show in both cases that $u = k$.

   (c) Is the preceding information enough to pin down the parity of v and hence solve the problem?

   (d) If not, try other congruence classes for p. If you get the right one, you will have solved the problem of evaluating $(2|p)$.

This problem is much easier if you did question 2.