Week 14–MATH 4573 Elementary Number Theory

Spring 2021

Contents

1 Monday, April 12: Finishing the proof of Quadratic Reciprocity and Pythagorean Triples

1.1 Finishing the proof of Quadratic Reciprocity (15 minutes)

Let's review what where we left off:

We are trying to show that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$.

From the lemma from last Wednesday, we know that for

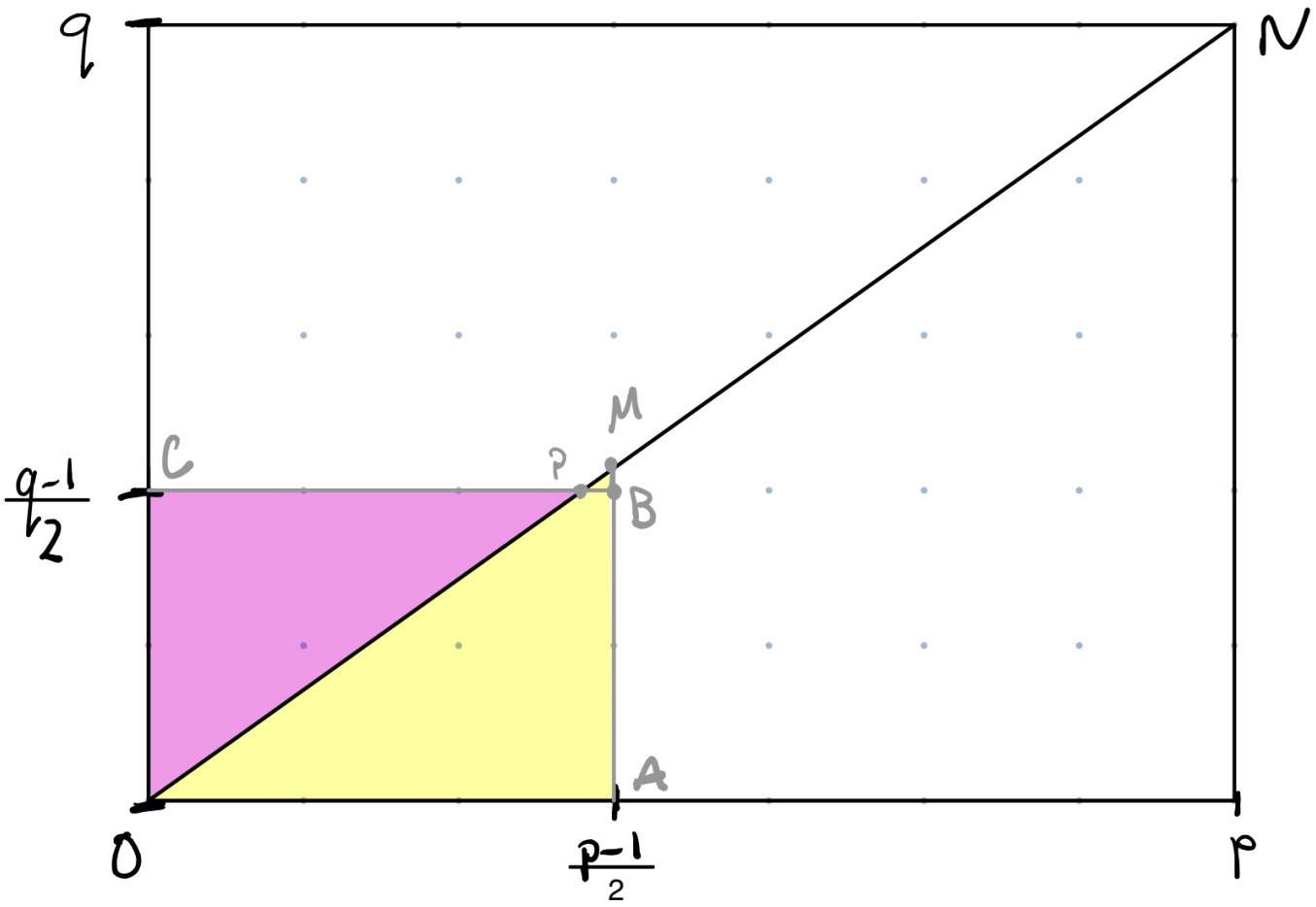
$$N_1 = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor, N_2 = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jp}{q} \right\rfloor$$

then

$$\left(\frac{q}{p}\right) = (-1)^{N_1}, \left(\frac{p}{q}\right) = (-1)^{N_2}.$$

We are trying to then show that $N_1 + N_2 = \frac{(p-1)}{2}\frac{(q-1)}{2}$.

We assumed that $p > q$ and drew the rectangle $O = (0,0), A = \left(\frac{p-1}{2}, 0\right), B = \left(\frac{p-1}{2}, \frac{q-1}{2}\right)$, and $C = \left(0, \frac{q-1}{2}\right)$, like in the graphic below:



We showed that here are $\frac{(p-1)}{2}\frac{(q-1)}{2}$. Our goal is to show that there are N_1 lattice points in the pink area and N_2 lattice points in the yellow. Last class, we showed that the triangle OMA and the quadrilateral $OPBA$ have the same number of lattice points. It is slightly easier to count points for the triangle, so we do that.

Proof. To find N_1, the number of lattice points in OPC, not including those on OC, we count how many lattice points on the line $y = j$ are to the left of ON for $j = 1, 2, \ldots, \frac{q-1}{2}$. Another was of saying this is for each j, we want the number of nonnegative integers less than $\frac{jp}{q}$

Thus, we have for each j, there are $\left\lfloor \frac{jp}{q} \right\rfloor$ lattice points in OPC. Thus, in total there are $N_1 = \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{jp}{q} \right\rfloor$ lattice points in OPC.

To find N_2, we use a similar counting method on OAM. Now, we count the lattice points on $x = j$ for $j = 1, 2, \ldots, \frac{p-1}{2}$. Thus, for each j, we want the number of nonnegative integers less than $\frac{jq}{p}$. Thus, we have for each j, there are $\left\lfloor \frac{jq}{p} \right\rfloor$ lattice points in OPC. Thus, in total there are $N_2 = \sum_{j=1}^{2} \left\lfloor \frac{jq}{p} \right\rfloor$ lattice points in

OMA. From the previous Lemma, $\left(\frac{p}{q}\right) = (-1)^{N_1}$ and $\left(\frac{q}{p}\right) = (-1)^{N_2}$. Thus,

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{p}{q}\right) &= (-1)^{N_1}(-1)^{N_2} \\ &= (-1)^{N_1+N_2} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\end{aligned}$$

with the result from the April 7 reading assignment. □

Quadratic reciprocity means that determining all quadratic residues (perfect squares) modulo an odd prime is a finite problem. In terms of Legendre symbol, this is finding all a where $\left(\frac{a}{p}\right) = 1$ for a given p. For example, when $p = 11$, we can check all positive integers a. However, what about the reverse? Quadratic reciprocity allows us to find all odd primes p where $\left(\frac{11}{p}\right) = 1$, even though there are infinitely many odd primes. This idea is also on Homework 12, Short Proofs.

1.2 Announcements (5 min)

We are going to leave quadratic reciprocity for nonprimes for independent study. Hopefully, if you need this information in the future, you have gained some of the skill of reading and working through mathematics.

In the interest of moving away from super technical topics, we are going to skip arithmetic functions and the Möbius inversion formula. This will make the last week a bit of a grab bag of number theory topics, but I want to move into Diophantine equations, which are more concrete. This will also keep us looking at things that are vaguely geometric.

We also are going to take a slightly different approach than the book, and use Pythagorean triples as our motivating example. This means we will do parts of Chapter 11 before Chapter 10.

1.3 Linear Diophantine equation review (10 minutes)

Definition. *A* Diophantine equation *is any equation in one or more variables to be solved in the integers.*
Definition. *Let $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$ with $a_1, a_2, \ldots, a_n$ not zero. A Diophantine equation of the form*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

is a linear Diophantine equation in the n variable $x_1, \ldots, x_n$.

The participation assignment classifies linear Diophantine equations in one variable.

The question of whether there are solutions to Diophantine equations becomes harder when there is more than one variable. Then next step is to classify Diophantine equations in two variables.
Theorem 1 (Theorem 1.13)**.** *Let $ax + by = c$ be a linear Diophantine equation in the variables x and y. Let $d = \gcd(a, b)$. If $d \nmid c$, then the equation has no solutions; if $d \mid c$, then the equation has infinitely many solutions. Furthermore, if x_0, y_0 is a particular solution of the equation, then all solution are given by $x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$ where $n \in \mathbb{Z}$.*
Breakout Room Problem (7 minutes)**.** *Find all solutions to* $803x + 154y = 11$.

1.4 Nonlinear Diophantine equations (5 minutes)

Definition. *A Diophantine equation is* nonlinear *if it is not linear.*

Example 1.
1. *The Diophantine equation $x^2+y^2 = z^2$ is our next section. Solutions are called Pythagorean triples.*
2. *Let $n \in \mathbb{Z}$ with $n \geq 3$. The Diophantine equation $x^n + y^n = z^n$ is the subject of the famous Fermat's Last Theorem. We will also prove one case of this.*
3. *Let $n \in \mathbb{Z}$. The Diophantine equation $x^2 + y^2 = n$ tells us which integers can be represented as the sum of two squares.*
4. *Let $d, n \in \mathbb{Z}$. The Diophantine equation $x^2 - dy^2 = n$ is known as Pell's equation.*

Sometimes we can use congruences to show that a particular nonlinear Diophantine equation has no solutions.

Example 2. *Prove that $3x^2 + 2 = y^2$ is not solvable.*

Assume that there is a solution. Then any solution to the Diophantine equation is also a solution to the congruence $3x^2 + 2 \equiv y^2 \mod 3$, which implies $2 \equiv y^2 \mod 3$, which we know is false. Thus there are no integer solutions to $3x^2 + 2 = y^2$.

Note: viewing the same equation modulo 2 says $x^2 \equiv y^2 \mod 2$, which does not give us enough information to prove a solution does not exist.

2 Wednesday, April 14: Pythagorean triples and Fermat's Last Theorem

Read Sections 6.1 The Pythagorean equation and 6.2 No solutions to a Diophantine equation through descent in Number Theory Revealed: A Master Class (Links to an external site.) (the link should take you to the start of Section 6.1)

In your own words, explain how the method of decent works.

2.1 Pythagorean triples (40 minutes)

One of the most famous math equations is $x^2 + y^2 = z^2$, probably because we learn it in high school. We are going to classify all integer solutions to the equation.

Definition. *A triple (x, y, z) of positive integers satisfying the Diophantine equation $x^2 + y^2 = z^2$ is called* Pythagorean triple.

Select the Pythagorean triples:

Poll question.
- *3,4,5*
- *5,12,13*
- *-3,4,5*
- *6,8,10*
- *0,1,1*

It is actually possible to classify all Pythagorean triples, just like we did for linear Diophantine equations in two variables. To simplify this process, we will work with $x, y, z > 0$, and $(x, y, z) = 1$. For any given

solution of this form, we have that $(-x, y, z), (x, -y, z), (x, y, -z), (-x, -y, z), (x, -y, -z), (-x, y, -z)$, and $(-x, -y, -z)$ are also solutions to the Diophantine equation, as is (nx, ny, nz) for any integer n. Thus, we call such a solution a *primitive Pythagorean triple*. We call $(0, n, \pm n)$ and $(n, 0, \pm n)$ the *trival solutions*.
Theorem 2. *For a primitive Pythagorean triple (x, y, z), exactly one of x and y is even.*

Proof. If x and y are both even, then z must also be even, contradicting that $(x, y, z) = 1$.

If x and y are both odd, then z is even. Now we can work modulo 4 to get a contradiction. Since x and y are odd, we have that $x^2 \equiv y^2 \equiv 1 \pmod 4$. Since z is even, we have that $z^2 \equiv 0 \pmod 4$, but $x^2 + y^2 \equiv 2 \pmod 4$.

Thus, the only remaining option is exactly one of x and y is even. □

Theorem 3. *There are infinitely many primitive Pythagorean triples x, y, z with y even. Furthermore, they are given precisely by the equations*

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

where $m, n \in \mathbb{Z}, m > n > 0, (m, n) = 1$ and exactly one of m and n is even.

Before proving this theorem, we illustrate it with some examples:
Breakout Room Problem. *(5 min)*

1. *$m = 2$ and $n = 1$ satisfy the conditions of m and n in the theorem. This gives $(3, 4, 5)$.*
2. *$m = 3$ and $n = 2$ gives $(5, 12, 13)$.*
3. *Try with your own values of m and n.*

Now we are going to prove
Theorem 4. *There are infinitely many primitive Pythagorean triples x, y, z with y even. Furthermore, they are given precisely by the equations*

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

where $m, n \in \mathbb{Z}, m > n > 0, (m, n) = 1$ and exactly one of m and n is even.

Proof. We first show that given a primitive Pythagorean triple with y even, there exist m and n as described. Since y is even, y and z are both odd. Moreover, $(x, y) = 1, (y, z) = 1$, and $(x, z) = 1$. Now,

$$y^2 = z^2 - x^2 = (x + z)(z - x)$$

implies that

$$\left(\frac{y}{2}\right)^2 = \frac{(x + z)}{2}\frac{(z - x)}{2}.$$

To show, $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = 1$, let $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = d$. Then $d \mid \frac{z+x}{2}$ and $d \mid \frac{z-x}{2}$. Thus, $d \mid \frac{z+x}{2} + \frac{z-x}{2} = z$ and $d \mid \frac{z+x}{2} - \frac{z-x}{2} = x$. Since $(x, z) = 1$, we have that $d = 1$. Thus, $\frac{(x+z)}{2}$ and $\frac{(z-x)}{2}$ are perfect squares.

Let

$$m^2 = \frac{(x+z)}{2}, \quad n^2 = \frac{(z-x)}{2}.$$

Then $m > n > 0, (m, n) = 1, m^2 - n^2 = x, 2mn = y$, and $m^2 + n^2 = z$. Also, $(m, n) = 1$ implies that not both m and n are both even. If both m and n are odd, we have that z and x are both even, but $(x, z) = 1$. This proves that every primitive Pythagorean triple has this form.

Now we prove that given any such m and n, we have a primitive Pythagorean triple. First, $(m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = (m^2 + n^2)^2$. We need to show that $(x, y, z) = 1$. Let $(x, y, z) = d$. Since exactly one of m and n is even, we have that x and z are both odd. Then d is odd, and thus $d = 1$ or d is divisible by some odd prime p. Assume that $p \mid d$. Thus, $p \mid x$ and $p \mid z$. Thus, $p \mid z + x$ and $p \mid z - x$. Thus, $p \mid (m^2 + n^2) + (m^2 - n^2) = 2m^2$ and $p \mid (m^2 + n^2) - (m^2 - n^2) = 2n^2$. Since p is odd, we have that $p \mid m^2$ and $p \mid n^2$, but $(m, n) = 1$, so $d = 1$. □

While this proof is not obvious, it does not use any concepts beyond chapter 1. Thus, this proof is considered *elementary*. Such elementary proofs often involve deep insights and intricate calculations, but no concepts beyond what we are learning in this course (and often not including things like divisor sums).

3 Friday, April 16: Fermat's Last Theorem and Sums of Squares

Read Section 9.1 in Number Theory Revealed: A Masterclass (Links to an external site.)

Turn in: Exercise 9.1.3. Find four distinct representations of $1105 = 5\ (13\ )(\ 17)$ as a sum of two squares.

3.1 Fermat's Last Theorem (35 minutes)

After the Diophantine equation $x^2 + y^2 = z^2$, one generalization is $x^n + y^n = z^n$ for $n \geq 3$. Fermat's Last Theorem was first conjectured in 1637 and proven in 1995 by Andrew Wiles. Attempts to solve this problem through the centuries have created new branches of mathematics.

Theorem 5 (Fermat's Last Theorem)**.** *The Diophantine equation $x^n + y^n = z^n$ has no nonzero integer solutions for $n \geq 3$.*

We will show that it suffices to prove Fermat's Last Theorem for the cases of n and odd prime and $n = 4$.

Theorem 6. *The Diophantine equation $x^n + y^n = z^n$ has a solution no solutions for $n \geq 3$ if and only if there are no solutions for n and odd prime or $n = 4$.*

Proof. Let $n \in \mathbb{Z}$ and $n \geq 3$. Let $n = ab$ where $a, b \in \mathbb{Z}$ and b is either an odd prime or 4. If x, y, z is a solution to $x^n + y^n = z^n$, then x^a, y^a, z^a is a solution to $x^b + y^b = z^b$. By contraposition, if $x^b + y^b = z^b$ has no solutions, then $x^n + y^n = z^n$ has no solutions. □

We will prove the case where $n = 4$ using the *method of decent.* This is the only case that Fermat proved. The next 400+ years were spent proving the theorem for odd primes.

The idea of the method of decent for proving no solution exists for a Diophantine equation is to assume a solution exists. Then use this solution to construct one that has one component that is strictly smaller than the original solution. This process could be repeated indefinitely, but it is not possible to construct an infinitely decreasing list of positive integers. Thus, no solution exists.

Theorem 7. *The Diophantine equation $x^4 + y^4 = z^2$ has not solutions in nonzero integers x, y, z.*

Chat blast. *Now why does this tell us there are no solutions to $x^4 + y^4 = z^4$?*

Proof. Assume by way of contradiction, that $x^4+y^4 = z^2$ has a solution x_1, y_1, z_1 nonzero integers. Without loss of generality, we may assume $x_1, y_1, z_1 > 0$ and $\gcd(x_1, y_1) = 1$. We will show that there is another solution x_2, y_2, z_2 positive integers such that $\gcd(x_2, y_2) = 1$ and $0 < z_2 < z_1$. Now, $(x_1)^2, (y_1)^2, z_1$ is a Pythagorean triple with $\gcd(x_1^2, y_1^2, z_1) = 1$, and without loss of generality, y_1^2 is even. Thus, by the first theorem of the day says that there exists $m, n \in \mathbb{Z}$ such that $\gcd(m, n) = 1, m > n > 0$, and exactly one of m and n is even such that $x_1^2 = m^2 - n^2, y_1^2 = 2mn, z_1 = m^2 + n^2$. Now, $x_1^2 = m^2 - n^2$ implies $x_1^2 + n^2 = m^2$ and x_1, m, n is a Pythagorean triple with $\gcd(x_1, m, n) = 1$ and n is even. Applying the same theorem again, we get that there exists $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1, a > b > 0$, exactly one of a and b is even, with $x_1 = a^2 - b^2, n = 2ab, m = a^2 + b^2$.

We want to show that m, a and b are perfect squares. Once we have done that, we can conclude that we have constructed another solution.

Breakout Room Problem (15 minutes)**.** *Show that m, a and b are perfect squares.*

See also: `https://ximera.osu.edu/math4573/April6/April6/April6`