Math 4527 (Number Theory 2)

Lecture #1 of 38 $\sim$ January 20, 2021

Introduction + Pythagorean Triples

- Pythagorean Triples (part 2)
- Linear Diophantine Equations
- The Frobenius Coin Problem

This material represents §6.1.1-6.1.3 from the course notes.

More Pythagorean Triples, I

Recall from last time:

Definition

We say a Pythagorean triple (x, y, z) *satisfying* $x^2 + y^2 = z^2$ *is* primitive *if* $\gcd(x, y, z) = 1$.

Theorem (Primitive Pythagorean Triples)

Every primitive Pythagorean triple of the form (x, y, z) *with* x *even is of the form* $(x, y, z) = (2st,\ s^2 - t^2,\ s^2 + t^2)$*, for some relatively prime integers* $s > t$ *of opposite parity. Conversely, any such triple is Pythagorean and primitive.*

I gave two proofs last time (one using arithmetic in $\mathbb{Z}$ and another using arithmetic in $\mathbb{Z}[i]$). Now I will do the third proof, which uses geometry.

More Pythagorean Triples, II

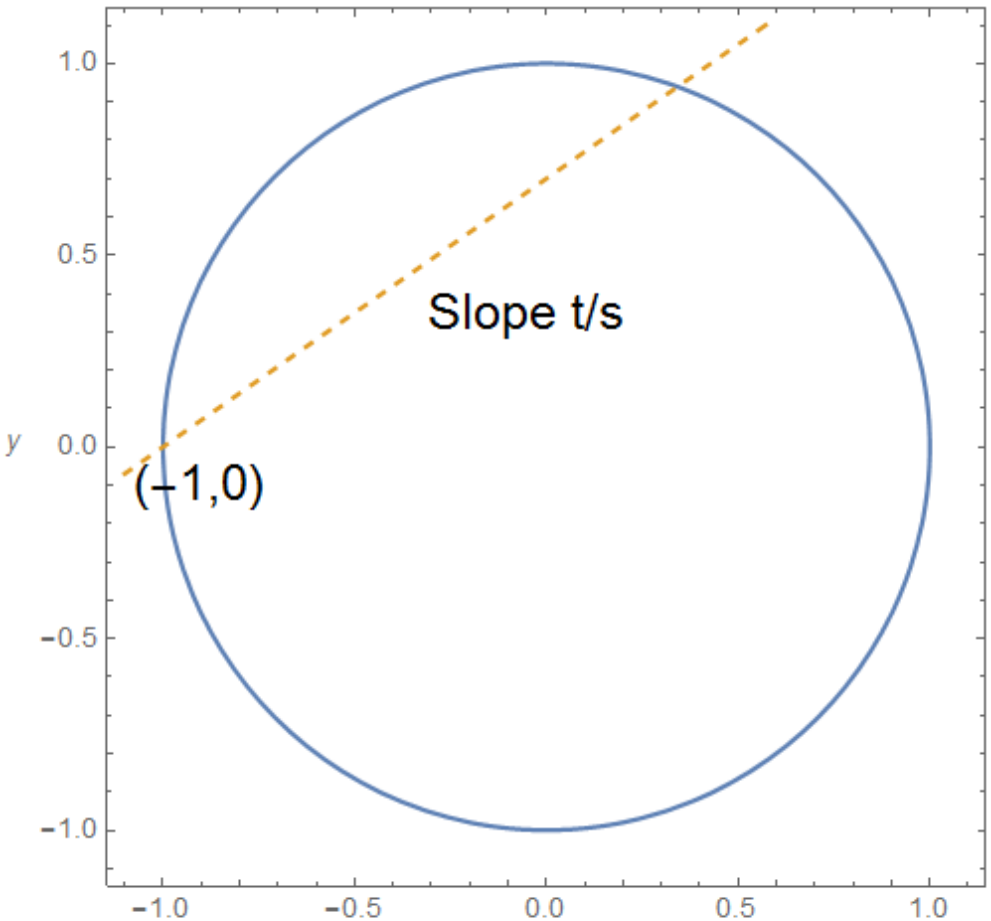
Proof #3:

- Suppose $x^2 + y^2 = z^2$ and x, y, z are relatively prime.
- Dividing by z^2 yields the equivalent equation $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$.
- Each Pythagorean triple (x, y, z) therefore yields a point $(a, b) = (x/z, y/z)$ with rational coordinates on the unit circle $x^2 + y^2 = 1$.
- Conversely, if we have a point (a, b) with rational coordinates on the unit circle, then if z is the lcm of the denominators so that $(a, b) = (x/z, y/z)$, we obtain a primitive triple (x, y, z) with $x^2 + y^2 = z^2$.
- Therefore, finding the primitive Pythagorean triples is equivalent to describing all points (a, b) on the unit circle $x^2 + y^2 = 1$ whose coordinates are both rational numbers.

More Pythagorean Triples, III

Proof #3 (continued):

- To do this, consider a line passing through the point $(-1, 0)$ with a finite slope:



- Such a line will intersect the circle $x^2 + y^2 = 1$ in exactly one other point.
- If the coordinates of this point are rational, then the line will have rational slope.
- Conversely, if the line has rational slope, its other intersection point with the circle will be rational.

More Pythagorean Triples, IV

Proof #3 (continued more):

- Explicitly, if the line has slope $\frac{t}{s}$, its equation is $y = \frac{t}{s}(x+1)$.
- We can then simply plug in $y = \frac{t}{s}(x+1)$ to $x^2 + y^2 = 1$ and solve to see that the other intersection point is $(x, y) = \left(\frac{s^2 - t^2}{s^2 + t^2}, \frac{2st}{s^2 + t^2}\right)$, which is rational.
- Thus, the rational points on the unit circle are those of the form $\left(\frac{s^2 - t^2}{s^2 + t^2}, \frac{2st}{s^2 + t^2}\right)$ for some integers s and t.
- Clearing the denominator immediately yields the desired Pythagorean triples.

More Pythagorean Triples, V

If you've never seen it before, the idea in the third proof actually has a surprisingly useful application in calculus.

- Specifically, if we write $u = s/t$, then we obtain a rational parametrization of the unit circle in terms of u.
- Explicitly, we have $\cos\theta = \dfrac{1-u^2}{1+u^2}$ and $\sin\theta = \dfrac{2u}{1+u^2}$.
- Using some elementary geometry, it is not hard to see that this parameter is $u = \tan(\theta/2)$.
- The upshot: if we make the substitution $u = \tan(\theta/2)$, then both $\sin\theta$ and $\cos\theta$ are rational functions in u.
- This substitution is called the Weierstrass substitution and can be used to evaluate integrals like $\displaystyle\int \frac{1}{3+\sin\theta}\,d\theta$ that are quite hard otherwise.

More Pythagorean Triples, VI

Using the characterization above, we can easily generate a list of Pythagorean triples with hypotenuse ≤ 80:

s	t	Primitive Triple	Other Triples
2	1	$(3,4,5)$	$(6,8,10)$, $(9,12,15)$, ... , $(48,64,80)$
3	2	$(5,12,13)$	$(10,24,26)$, ..., $(30,72,78)$
4	1	$(8,15,17)$	$(16,30,34)$, ..., $(32,60,68)$
4	3	$(7,24,25)$	$(14,48,50)$, $(21,72,75)$
5	2	$(20,21,29)$	$(40,41,58)$
5	4	$(9,40,41)$	
6	1	$(12,35,37)$	$(24,70,74)$
6	5	$(11,60,61)$	
7	2	$(28,45,53)$	
7	4	$(33,56,65)$	
8	1	$(16,63,65)$	
8	3	$(48,55,73)$	

More Pythagorean Triples, VI

Example: Find all Pythagorean right triangles having one side of length 20.

- Any such right triangle has legs of lengths $k(2st)$ and $k(s^2 - t^2)$, with hypotenuse $k(s^2 + t^2)$, where $s > t$ are unique positive integers of opposite parity and k is some unique positive integer. Now we just try each possibility:

More Pythagorean Triples, VI

Example: Find all Pythagorean right triangles having one side of length 20.

- Any such right triangle has legs of lengths $k(2st)$ and $k(s^2 - t^2)$, with hypotenuse $k(s^2 + t^2)$, where $s > t$ are unique positive integers of opposite parity and k is some unique positive integer. Now we just try each possibility:

1. Suppose $20 = 2stk$.
   - Then $10 = stk$, so $(s, t, k) = (10, 1, 1)$ or $(5, 2, 1)$.
   - This yields 20-99-101 and 20-21-29 triangles.

More Pythagorean Triples, VI

Example (continued): Find all Pythagorean right triangles having one side of length 20.

2. Suppose $20 = k(s^2 - t^2)$.
   - Then k must be divisible by 4 since $s^2 - t^2$ is odd.
   - Since $k \neq 20$ we see $k = 4$. Then $s^2 - t^2 = 5$ requires $s = 3$ and $t = 2$.
   - This yields a 15-20-25 triangle.
3. Suppose $20 = k(s^2 + t^2)$.
   - Then since $s^2 + t^2 \geq 5$, the only possibilities are $k = 4$ (then $s = 2$, $t = 1$), $k = 2$ (then $s = 3$, $t = 1$ but these are not of opposite parity) or $k = 1$ (then $s = 4$ and $t = 2$ but again these don't work).
   - This yields a 12-16-20 triangle.

So we get 4 triples: (20,99,101), (20,21,29), (15,20,25), (12,16,20).

Linear Diophantine Equations, I

We will now take a step in the "easier" direction and talk about the simpler class of linear Diophantine equations.

- Solving a linear equation in one variable over the integers is trivial (the solution to $ax = b$ is $x = b/a$, assuming a is nonzero and divides b).
- So the simplest interesting equations are linear equations in two variables.
- The general form of a linear equation in two variables is $ax + by = c$, for some fixed integers a, b, and c.
- Our goal is to determine when this equation has an integral solution (x, y), and then to characterize all the solutions.
- In keeping with our theme of "exploiting other rings to solve problems in $\mathbb{Z}$", we will use modular arithmetic to reduce the two-variable equation to a one-variable equation.

Linear Diophantine Equations, II

We will use the following proposition about linear congruences modulo m:

Proposition (Linear Equations Mod m)

The equation $ax \equiv b \pmod{m}$ has a solution for x if and only if $d = \gcd(a, m)$ divides b.

If $d|b$, then the set of all such x is given by the residue class $\overline{r}$ modulo m/d, where r is any solution to the equation.

Linear Diophantine Equations, II

We will use the following proposition about linear congruences modulo m:

Proposition (Linear Equations Mod m)

The equation $ax \equiv b \pmod{m}$ has a solution for x if and only if $d = \gcd(a, m)$ divides b.

If $d|b$, then the set of all such x is given by the residue class $\overline{r}$ modulo m/d, where r is any solution to the equation.

Examples:

1. The equation $9x \equiv 5 \bmod 12$ has no solutions, because $\gcd(9, 12) = 3$ does not divide 5. The point is: any multiple of 9 will always be divisible by 3 modulo 12, so it can't equal 5.
2. The equation $9x \equiv 6 \bmod 12$ has solutions, since $\gcd(9, 12) = 3$ does divide 6. Since $x = 2$ is a solution, the full set of solutions is $x \equiv 2 \bmod 4$.

Linear Diophantine Equations, III

Proof:

- If x is a solution to the congruence $ax \equiv b \pmod{m}$, then there exists an integer k with $ax - mk = b$. Since $d = \gcd(a, m)$ divides the left-hand side, it must divide b.
- Now suppose $d = \gcd(a, m)$ divides b, and set $a' = a/d$, $b' = b/d$, and $m' = m/d$.
- Then the original equation becomes $a'dx \equiv b'd \pmod{m'd}$, which is equivalent to $a'x \equiv b' \pmod{m'}$. This is a property of congruences that is easy to verify if you write it in terms of divisibility.
- But since a' and m' are relatively prime, a' is a unit modulo m', so we can simply multiply by its inverse to obtain $x \equiv b' \cdot (a')^{-1} \pmod{m'}$. This means that there is a unique solution to the congruence modulo $m' = m/d$, as claimed.

Linear Diophantine Equations, IV

By reducing modulo one of the coefficients, we can solve linear Diophantine equations in two variables:

Theorem (Linear Diophantine Equations in 2 Variables)

Let a, b, c be integers with $ab \neq 0$, and set $d = \gcd(a, b)$.

If $d \nmid c$, the equation $ax + by = c$ has no integer solutions (x, y).

If $d \mid c$, $ax + by = c$ has infinitely many integer solutions (x, y). If (x_0, y_0) is one solution, then all the others are $(x_0 - bt/d,\ y_0 + at/d)$, for some integer t.

Linear Diophantine Equations, IV

By reducing modulo one of the coefficients, we can solve linear Diophantine equations in two variables:

Theorem (Linear Diophantine Equations in 2 Variables)

Let a, b, c be integers with $ab \neq 0$, and set $d = \gcd(a, b)$.

If $d \nmid c$, the equation $ax + by = c$ has no integer solutions (x, y).

If $d \mid c$, $ax + by = c$ has infinitely many integer solutions (x, y). If (x_0, y_0) is one solution, then all the others are $(x_0 - bt/d,\ y_0 + at/d)$, for some integer t.

Examples:

1. The equation $9x + 12y = 5$ has no integer solutions, since $\gcd(6, 9) = 3$ does not divide 5.
2. The equation $9x + 12y = 6$ has integer solutions because $\gcd(9, 12) = 3$ does divide 6. One solution is $(x, y) = (2, -1)$, so the full set is $(x, y) = (2 - 4t, -1 + 3t)$ for integers t.

Linear Diophantine Equations, V

Proof:

- If $a = b = 0$, then the equation $ax + by = c$ is either trivially true (if $c = 0$) or trivially false (if $c \neq 0$), so we can assume that the gcd d is nonzero.
- If one of a, b is zero, the equation is also trivial, so we may also deal only with the case where $ab \neq 0$.
- In this case, observe that there is an integral solution to $ax + by = c$ if and only if there is a solution to the congruence $ax \equiv c \pmod{b}$, since then $y = \dfrac{c - ax}{b}$.
- From our proposition above, we know that $ax \equiv c \pmod{b}$ has a solution only if $d = \gcd(a, b)$ divides c. This is the first part of the theorem.

Linear Diophantine Equations, VI

Proof (continued):

- For the second part, suppose $d = \gcd(a, b)$ does divide c, and consider the values of x satisfying $ax + by = c$.
- In this case, again by the proposition we just proved, if we set $a' = a/d$, $b' = b/d$, and $c' = c/d$, the set of all such x is given by the residue class $\overline{x_0}$ modulo b', where $x_0 \equiv c' \cdot (a')^{-1} \pmod{b'}$.
- Now if (x, y) is any solution, then by the above, we see that $x = x_0 - bt/d$ for some integer t, and then we can directly compute $y = y_0 + at/d$ where $ax_0 + by_0 = c$.
- Since these are all solutions, this yields the full characterization of the solutions given above.

Linear Diophantine Equations, VII

Example: Find all solutions to $14x + 18y = 12$ in integers (x, y).

Linear Diophantine Equations, VII

Example: Find all solutions to $14x + 18y = 12$ in integers (x, y).

- First, we compute $\gcd(14, 18) = 2$, and then divide through by the gcd to get $7x + 9y = 6$.
- This is equivalent to solving $7x \equiv 6 \pmod 9$.
- We compute (via the Euclidean algorithm or guess-and-check) that the inverse of 7 mod 9 is 4, so multiplying both sides by 4 yields $x \equiv 24 \equiv 6 \pmod 9$.
- Hence one solution is $(x, y) = (6, -4)$. The set of all solutions is then $(x, y) = \boxed{(6 - 9t, -4 + 7t)}$ for $t \in \mathbb{Z}$.

Linear Diophantine Equations, VIII

Example: Find all solutions to $372x + 948y = 42$ in integers (x, y).

- Using the Euclidean algorithm we can quickly compute $\gcd(372, 948) = 12$.
- Since 12 does not divide 42, there are no solutions.

Linear Diophantine Equations, IX

We can solve linear Diophantine equations in two variables by making changes of variable. Here's an example:

Example: Find all solutions to the equation $4x + 13y = 5$.

- By the division algorithm, we have $13 = 3 \cdot 4 + 1$, so we can write the system in the form $4x + (3 \cdot 4 + 1)y = 5$, and rearrange this into the form $4(x + 3y) + 1y = 5$.
- If we substitute $u = x + 3y$, this new system becomes $4u + y = 5$, which we can easily solve to get $y = 5 - 4u$.
- Substituting back yields $x = u - 3y = u - 3(5 - 4u) = -15 + 13u$.
- Thus, we obtain the general solution $(x, y) = (-15 + 13u,\ 5 - 4u)$.

Linear Diophantine Equations, X

This method, using changes of variable, is the most efficient way to solve systems of linear Diophantine equations involving more variables or equations.

- The approach is essentially the same as the standard linear algebra procedure of row-reducing a matrix to solve a system of equations.
- The easiest approach is convert the system into matrix form, and then perform row and column operations on the matrix until it is in a sufficiently simple form that the solution to the original system is obvious.
- The general procedure for solving a system of linear equations over $\mathbb{Z}$ is essentially the same, except for the added complication that all of the row and column operations need to be done over $\mathbb{Z}$.

Linear Diophantine Equations, XI

As with a system of equations over a field, the end result will be either that the system has no solution, a unique solution, or an infinite family of solutions with some number of free parameters.

- I won't bother going into the technical details or proving that this procedure always works, since it really is a topic from abstract algebra.
- For those curious: it is in fact equivalent to the procedure for converting a presentation of a finitely generated additive abelian group into a description of the abelian group as a direct product of cyclic groups, which is in turn a special case of the general classification theorem for finitely-generated modules over a principal ideal domain.

So I'll just give an example and let you see the general idea.

Linear Diophantine Equations, XII

Example: Find all solutions to $3x + 7y + 8z = 13$ in integers (x, y, z).

- Motivated by the division algorithm, we rewrite the equation as $3(x + 2y + 2z) + y + 2z = 13$, and then substitute $w = x + 2y + 2z$.
- The new equation is $3w + y + 2z = 13$, which we can easily solve for y, yielding $y = 13 - 3w - 2z$.
- Then $x = w - 2y - 2z = 7w + 2z - 26$.
- So we obtain the general solution $(x, y, z) = (7w + 2z - 26, 13 - 3w - 2z, z)$ where w and z are arbitrary integers.

The Frobenius Coin Problem, I

In various settings (some of which are actually motivated by real-world concerns for once!), we are sometimes also interested in knowing for which values of c the equation $ax + by = c$ has a solution in *nonnegative* integers (x, y).

- For example, if there are postage stamps worth 5 cents and stamps worth 13 cents, is it possible to use them to put exactly 79 cents' worth of postage on an envelope? (Here we want to solve $5x + 13y = 79$.)
- Another version occurs in sports: In American football, a team can score 3 points for a field goal, or 7 points for a touchdown. What possible scores can a team obtain? (Ignore safeties, missed extra points, and so forth.)

We remark that we can reduce to the situation with a, b relatively prime by dividing through by their gcd.

The Frobenius Coin Problem, II

The most obvious method is simply to make a list of totals that are attainable.

- For example, for $5x + 13y$, we obtain values 0, 5, 10, 13, 15, 18, 20, 23, 25, 26, 28, 30, 31, 33, 35, 36, 38, 39, 40, 41, 43, 44, 45, 46, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, ...
- Likewise, for $3x + 7y$ we obtain values 0, 3, 6, 7, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, ...
- In each case, it seems like we miss only finitely many values.

The Frobenius Coin Problem, III

The problem of describing the largest integer that cannot be written as a nonnegative linear combination of two integers (also called the Frobenius coin problem) was first solved by Sylvester:

Theorem (Sylvester)

If a and b are relatively prime integers, then there are exactly $\frac{1}{2}(a-1)(b-1)$ integers that cannot be written in the form $ax+by$ with $x, y \geq 0$, and the largest such integer is $ab-a-b$.

Remark: In mathematics competition circles, this result is often known as the "Chicken McNuggets Theorem".

The Frobenius Coin Problem, IV

Proof:

- For brevity, we say an integer is "representable" if it can be written in the form $ax + by$ with $x, y \geq 0$.
- Without loss of generality, assume $a < b$. Arrange the nonnegative integers in an array in the following manner:

$$\begin{array}{ccccc} 0 & 1 & 2 & \cdots & a-1 \\ a & a+1 & a+2 & \cdots & 2a-1 \\ 2a & 2a+1 & 2a+2 & \cdots & 3a-1 \\ \vdots & \vdots & \vdots & & \vdots \\ ab-a & ab-a+1 & ab-a+2 & \cdots & ab-1 \end{array}$$

- Now we use the array to mark all of the representable integers. We first box all of the multiples of b: then an integer is representable precisely if it appears in the same column as some multiple of b, lower down.

The Frobenius Coin Problem, V

Proof (continued):

- For illustration, here is the array with $a = 4$ and $b = 7$:

$\boxed{0}$	1	2	3
4	5	6	$\boxed{7}$
8	9	10	11
12	13	$\boxed{14}$	15
16	17	18	19
20	$\boxed{21}$	22	23
24	25	26	27

The Frobenius Coin Problem, VI

Proof (continueder):

- Since a and b are relatively prime, the integers 0, b, $2b$, ... , $(a-1)b$ all lie in different columns. Thus, the largest element that is left unmarked is the element one row above $(a-1)b$, which is $ab-a-b$, so this is the largest integer not expressible as $ax+by$ with $x, y \geq 0$.
- For the other part, we simply count the number of unmarked integers in the array.
- The number of integers lying above kb is $\lfloor kb/a \rfloor$, so there are a total of $\sum_{k=0}^{a-1} \left\lfloor \frac{kb}{a} \right\rfloor$ unmarked integers in the array.

The Frobenius Coin Problem, VII

Proof (continuederer):

- We can interpret the sum $\sum_{k=0}^{a-1} \left\lfloor \frac{kb}{a} \right\rfloor$ geometrically as the number of lattice points lying under the line $y = (b/a)x$, with $1 \leq x \leq a-1$.
- Equivalently, this is the total number of lattice points lying strictly inside the rectangle with vertices $(0,0)$, $(a,0)$, (a,b), $(0,b)$ and below the diagonal.
- By symmetry, since there are no lattice points on the interior of the diagonal, exactly half of the lattice points inside the $a \times b$ rectangle are below the diagonal.
- Since this full set of points forms an $(a-1) \times (b-1)$ rectangle, there are $(a-1)(b-1)$ such lattice points. Therefore, the number of unmarked integers in the array is $\frac{1}{2}(a-1)(b-1)$, as claimed.

The Frobenius Coin Problem, VIII

Example: There are postage stamps worth 5 cents and stamps worth 13 cents. What is the largest non-attainable amount of postage, and how many non-attainable amounts are there?

The Frobenius Coin Problem, VIII

Example: There are postage stamps worth 5 cents and stamps worth 13 cents. What is the largest non-attainable amount of postage, and how many non-attainable amounts are there?

- By Sylvester's theorem with $a = 5$ and $b = 13$, the largest non-representable integer is $5 \cdot 13 - 13 - 5 = 47$.
- In total, there are $\frac{1}{2} \cdot 4 \cdot 12 = 24$ unattainable totals.

The Frobenius Coin Problem, IX

We could of course generalize this problem, to ask: for given integers a_1, a_2, ... , a_k, what is the largest integer n that cannot be written as a nonnegative integer linear combination of the a_i?

- It turns out that there is no known general formula when $k > 2$ (though the result is fairly effectively computable for $k = 3$).
- For a fixed number of denominations k, there does exist a polynomial-time algorithm (polynomial in $\log a_k$, specifically) for computing this maximum integer n, but it is not appreciably faster than merely attempting to list the possibilities!
- For a variable number of denominations k, it is known that computing n is NP-hard.

Summary

We discussed a bit more about Pythagorean triples.

We discussed how to solve linear Diophantine equations in two variables and made some remarks about larger systems.

We discussed the Frobenius coin problem.

Next lecture: The Farey sequences and rational approximation.