Math 4527 (Number Theory 2)

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

Introduction + Pythagorean Triples

- Welcome to Math 4527 + Course Logistics
- Pythagorean Triples

This material represents §6.1.3 from the course notes.

Welcome!

Welcome to Math 4527 (Number Theory 2)! Here are some course-related locations to bookmark:

- The course webpage is here: `https://web.northeastern.edu/dummit/teaching_sp21_4527.html` . Most course-related information is posted there.
- Course-related discussion will be done via Piazza: `https://piazza.com/class/kj7dl2uyqpq2he` .
- Homework assignments will be submitted via the course's Canvas page.

Course Topics: Number Theory

As you might expect based on the title, we will be covering some topics in number theory in this course. The catalog description is fairly accurate, but here is the more updated plan:

6. Rational approximation and Diophantine equations
7. Elliptic curves
8. Quadratic integer rings
9. Geometry of numbers
10. Analytic number theory

One of the themes of the course is to build on some of the basic results from Math 3527 (which is why the chapter numbering starts at 6). However, I won't assume very much background from 3527, and anything that is referenced I am happy to explain, so if you haven't taken it, don't worry.

Lectures + Office Hours

The course lectures will be conducted via Zoom. All lectures are recorded for later viewing. For security reasons (since these lecture slides are posted publicly) the links to upcoming and past lectures are only available via the Canvas page or via the Piazza page.

- The course meets Mon/Wed/Thu from 10:30am-11:35am Eastern time. All lectures are recorded.
- I have office hours Wed/Thu from 3:00pm-4:15pm Eastern time, Thu from 12:15pm-1:15pm, or by appointment. Office hours are not recorded. You are highly encouraged to drop by.

Lecture attendance is not required. However, I would prefer if you attended each lecture live, and (if possible) turn your camera on and participate, because otherwise the lectures are not nearly as valuable.

Grades

Your course grade consists of 1/3 homework and 2/3 exams.

- There will be a take-home midterm and a take-home final. These are not timed, and are arranged essentially like a "solo" homework assignment.
- The homeworks are assigned weekly.
- Assignments are due via Canvas. This is to make it easier to record grading comments.

The lowest homework grade is dropped, in case you have an emergency or something comes up. I am also moderately flexible about homework deadlines, so it is okay if you need to submit an *occasional* assignment a day or so late. But please do notify me if you aren't going to be able to submit by the deadline.

Miscellaneous Info

Here is some other miscellaneous information:

- I will write lecture notes for the course (in lieu of an official textbook) as the semester progresses. I am drawing material from a number of different sources so it is hard to give a good textbook recommendation, but if you really want one I can give you some suggestions during office hours.
- Course prerequisites: A basic comfort level with groups, polynomials, and modular arithmetic is expected. Math 3527 is not required, although it will make the course material feel a bit more natural.
- Collaboration: You are allowed to work on, and discuss, homework assignments together, as long as the actual submissions are your own work. Collaboration is, of course, not allowed on exams.

Other Boilerplate, I

- Statement on Academic Integrity: A commitment to the principles of academic integrity is essential to the mission of Northeastern University. Academic dishonesty violates the most fundamental values of an intellectual community and undermines the achievements of the entire University. Violations of academic integrity include (but are not limited to) cheating on assignments or exams, fabrication or misrepresentation of data or other work, plagiarism, unauthorized collaboration, and facilitation of others' dishonesty. Possible sanctions include (but are not limited to) warnings, grade penalties, course failure, suspension, and expulsion.

Other Boilerplate, II

- Statement on Accommodations: Any student with a disability is encouraged to meet with or otherwise contact the instructor during the first week of classes to discuss accommodations. The student must bring a current Memorandum of Accommodations from the Office of Student Disability Services.
- Statement on Classroom Behavior: Disruptive classroom behavior will not be tolerated. In general, any behavior that impedes the ability of your fellow students to learn will be viewed as disruptive.
- Statement on Inclusivity: Faculty are encouraged to address students by their preferred name and gender pronoun. If you would like to be addressed using a specific name or pronoun, please let your instructor know.

Other Boilerplate, III

- Statement on Evaluations: Students are requested to complete the TRACE evaluations at the end of the course.
- Miscellaneous Disclaimer: The instructor reserves the right to change course policies, including the evaluation scheme of the course (e.g., in the event of natural disaster or global pandemic). Notice will be given in the event of any substantial changes.

Transition Into Actual Content

Pause here for questions about course logistics.

Note to self: don't read this slide out loud.

Overview of Course

In this course, we will study a bunch of topics in number theory.

- Number theory is a vast and ancient subject, and it is hard to collect two millennia of work into a two-semester sequence.
- I could try to pretend that there is a 100% coherent theme to the topics we'll be discussing, but the only true theme is "interesting things in elementary number theory that Prof. Dummit wants to teach in this course".
- Nonetheless, one recurring motif this semester will be the famous Fermat equation $x^n + y^n = z^n$.
- My hope is that by the end of the semester, I will have been able to develop enough of the background to be able to give you a 40,000-foot overview of Wiles's celebrated proof of Fermat's conjecture that there are no nontrivial integer solutions to the Fermat equation with $n \geq 3$.

Diophantine Equations, I

In this first chapter, we discuss Diophantine equations, which is the general name to the problem of solving equations over the integers.

- Example: Find all integer solutions to $a^7 + b^7 = c^7$.
- Example: Find all integer solutions to $14x^2 - 5xy + 3y^2 = 11$.

But before you get excited, I will deflate some of your hopes with the following theorem:

Theorem (Matiyasevich, 1970)

The problem of determining whether an arbitrary Diophantine equation possesses any integer solutions is undecidable, as is the problem of finding all solutions to an arbitrary Diophantine equation.

For the non-CS majors, this means that there is no general algorithm that can solve arbitrary Diophantine equations.

Diophantine Equations, II

However, for number theorists at least, Matiyasevich's theorem is actually good, because it keeps us in business! (There are always new Diophantine equations to solve.)

- Many of the methods for solving Diophantine equations feel rather *ad hoc*, and so the goals in this chapter are provide a survey of various elementary techniques.
- One recurring theme, however, will be to exploit the structure of the rings $\mathbb{Z}/m\mathbb{Z}$ (i.e., by using modular arithmetic) and $\mathbb{Z}[\sqrt{D}]$.
- Since I am not assuming that you are intimately familiar with the ring theory language, let me try to get you up to speed quickly.

Brief Algebra Interlude, I

Definition

A commutative ring with 1 is a set R having two closed binary operations $+$ and $\cdot$ such that $+$ and $\cdot$ are commutative and associative with $\cdot$ distributing over $+$, there is an additive identity 0 and every element has an additive inverse, and there is a multiplicative identity $1 \neq 0$.

Some famous examples of commutative rings with 1:

1. The integers $\mathbb{Z}$.
2. The rational numbers $\mathbb{Q}$.
3. The real numbers $\mathbb{R}$.
4. The complex numbers $\mathbb{C}$.
5. The ring $\mathbb{Z}/m\mathbb{Z}$ of integers modulo m.

There are also noncommutative rings, such as the ring of $n \times n$ matrices and the quaternions, but we won't worry about them now.

Brief Algebra Interlude, II

One of the magical facts about number theory is that, even though most of our questions are asked about $\mathbb{Z}$, we often want to use the structure of other rings to solve them.

- One important class of rings, which we will discuss and use extensively, are the quadratic rings $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$.
- The arithmetic operations in these rings look like $(a + b\sqrt{D}) + (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$ and $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + Dbd) + (ad + bc)\sqrt{D}$.
- When $D = -1$, we get the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.
- We will usually assume that D is a squarefree integer not equal to 1 when we are discussing these rings.

Brief Algebra Interlude, III

The elements with multiplicative inverses in a ring R are special:

Definition

If R is a ring with 1, we say an element $a \in R$ is a unit if it has a multiplicative inverse: that is, if there exists $b \in R$ such that $ab = 1 = ba$.

Examples:

1. In $\mathbb{Z}$, the units are 1 and -1.
2. In $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, every nonzero element is a unit. (This is really just another way of saying that these rings are fields.)
3. In $\mathbb{Z}/m\mathbb{Z}$, a residue class $\overline{a}$ is a unit if and only if it is relatively prime to m.
4. In $\mathbb{Z}[i]$, the units are 1, i, -1, and $-i$.

The set of units in a commutative ring forms an abelian group under multiplication.

Brief Algebra Interlude, IV

Ring arithmetic often behaves like arithmetic in $\mathbb{Z}$, but there is one situation that is a bit different:

Definition

If R is a ring with 1, we say an element $a \in R$ is a zero divisor if $a \neq 0$ but there exists a nonzero $b \in R$ such that $ab = 0$.

Examples:

1. There are no zero divisors in any ring that is a subset of a field, such as $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{Z}[\sqrt{D}]$.
2. In $\mathbb{Z}/6\mathbb{Z}$, the elements $\overline{2}$ and $\overline{3}$ are zero divisors since $\overline{2} \cdot \overline{3} = \overline{0}$.
3. More generally, the zero divisors in $\mathbb{Z}/m\mathbb{Z}$ are the nonzero residue classes not relatively prime to m.

Brief Algebra Interlude, V

Definition

A commutative ring with 1 having no zero divisors is called an integral domain.

Integral domains (per the name) behave a lot like the integers $\mathbb{Z}$.

- For example, in an integral domain, we can cancel nonzero elements under multiplication: if $ab = ac$ and $a \neq 0$, then $b = c$. (Proof: Rearrange this to $a(b - c) = 0$ and then deduce that $b - c = 0$ using the definition of integral domain.)
- We can also give sensible definitions of things like divisibility in arbitrary integral domains (and they will have most of the properties we'd expect): for example, we say $a|b$ (a divides b) if there exists some c such that $b = ac$.
- I will mention these things as they come up in the course.

Brief Algebra Interlude, VI

One of the themes of modern number theory is to study which rings have various properties of integer arithmetic still hold (e.g., existence of GCDs, unique prime factorization, etc.).

- We will get more into that particular discussion in Chapter 8 where we make a more focused study of quadratic integer rings (essentially the rings $\mathbb{Z}[\sqrt{D}]$).
- I've mentioned these things today for two reasons: one, to make sure you're comfortable with these ideas now because they'll show up many times in this course, and two, so that I can refer to some facts about $\mathbb{Z}[i]$ in the rest of today's lecture.
- Specifically, I will refer to the fact that $\mathbb{Z}[i]$ has unique prime factorization, and some minor facts about some of the Gaussian prime factors of particular elements.

Pythagorean Triples, I

With all of that out of the way, let's spend the rest of today looking at a simple but quite famous Diophantine equation: $x^2 + y^2 = z^2$.

- Triples of positive integers (x, y, z) satisfying this equation are called Pythagorean triples (see if you can figure out why).
- Some well-known Pythagorean triples are $(3, 4, 5)$, $(5, 12, 13)$, $(6, 8, 10)$, and $(8, 15, 17)$.
- But there are lots more, like $(11, 60, 61)$, $(20, 21, 29)$, $(1344, 1508, 2020)$, and even $(2021, 47472, 47515)$.

Just like the ancient Greeks, we would like to come up with a recipe for all of the Pythagorean triples.

- As should be familiar from elementary geometry, and is also easy to see from the equation $x^2 + y^2 = z^2$, if we have one solution (a, b, c) then we can scale it to get others: (ka, kb, kc) for any positive integer k.

Pythagorean Triples, II

We would like to exclude these essentially repetitious cases:

Definition

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

It is enough to characterize the primitive triples, since we may then scale them arbitrarily to get all the triples.

- First, notice that if (x, y, z) is a primitive Pythagorean triple, x and y cannot both be even, since then z would also be even.
- Also, x and y cannot both be odd, since then $x^2 + y^2 \equiv 2 \pmod 4$, but 2 is not a square modulo 4.
- So in a primitive triple, z must be odd, and also exactly one of x and y is also odd.

Pythagorean Triples, III

We now characterize the primitive Pythagorean triples:

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.

Pythagorean Triples, III

We now characterize the primitive Pythagorean triples:

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.

As a consequence we can characterize all Pythagorean triples:

Corollary (Pythagorean Triples)

The positive-integer solutions (x, y, z) to $x^2 + y^2 = z^2$ can be uniquely written as $(x, y, z) = (2kst, k(s^2 - t^2), k(s^2 + t^2))$ for a unique positive integer k and relatively prime positive integers $s > t$ of opposite parity.

Pythagorean Triples, IV

Proof (easy parts):

- First, it is easy to see that $(2st)^2 + (s^2 - t^2)^2 = (s^2 + t^2)^2$ simply by multiplying everything out.
- It is also easy to check that if s and t are relatively prime and have opposite parity, that $\gcd(s^2 - t^2, s^2 + t^2) = 1$, so this triple is primitive. (Any common factor would divide both $2s^2$ and $2t^2$ hence could only be 1 or 2, but it cannot be 2 because $s^2 + t^2$ is odd.)
- Also, the corollary (the characterization of all triples) follows from our earlier discussion of primitive triples above, since we may take $k = \gcd(x, y, z)$.

Pythagorean Triples, IV

Proof (preamble):

- It remains to prove that if (x, y, z) is primitive then it has the claimed form. We will give three different proofs that illustrate different approaches.
- The central idea in the first proof is to rearrange the equation and use the arithmetic of $\mathbb{Z}$.
- The central idea in the second proof is to exploit the fact that $\mathbb{Z}[i]$ has unique factorization.
- The central idea in the third proof is to use the geometry of the dehomogenized curve $x^2 + y^2 = 1$ to study the rational solutions.

Pythagorean Triples, V

Proof #1:

- Suppose $x^2 + y^2 = z^2$ and x, y, z are relatively prime.
- Since y and z are both odd and x is even, we can rewrite the equation as $\frac{z-y}{2} \cdot \frac{z+y}{2} = \left(\frac{x}{2}\right)^2$.
- Now we claim that $\frac{z-y}{2}$ and $\frac{z+y}{2}$ are relatively prime: their gcd divides their sum z and their difference y, and since y and z are relatively prime, the gcd must be 1.
- Since $\frac{z-y}{2}$ and $\frac{z+y}{2}$ share no prime divisors and their product is a square, each of them must individually be a square, by the uniqueness of prime factorization.
- Thus $\frac{z-y}{2} = t^2$ and $\frac{z+y}{2} = s^2$ for some s and t.
- Then $z = s^2 + t^2$ and $y = s^2 - t^2$, and then clearly $x = 2st$.
- Furthermore, s and t are necessarily relatively prime and have opposite parity, since (x, y, z) is primitive. Victory ensues.

Pythagorean Triples, VI

Proof #2:

- Suppose $x^2 + y^2 = z^2$ and x, y, z are relatively prime.
- In $\mathbb{Z}[i]$, factor the equation as $(x + iy)(x - iy) = z^2$.
- Now we claim that $x + iy$ and $x - iy$ are relatively prime as elements of $\mathbb{Z}[i]$: any greatest common divisor in $\mathbb{Z}[i]$ must divide $2x$ and $2y$, so since x and y are relatively prime integers, the gcd must divide 2.
- In $\mathbb{Z}[i]$, the prime factorization of 2 is $2 = -i(1 + i)^2$, and the unique irreducible element in this factorization is $1 + i$, so this is the only possible Gaussian prime factor that could appear in the gcd.
- However, $x + iy$ is not divisible by the Gaussian prime $1 + i$, since x and y are of opposite parity. Therefore, the gcd is 1, and so $x + iy$ and $x - iy$ are relatively prime.

Pythagorean Triples, VII

Proof #2 (continued):

- Hence, since $x + iy$ and $x - iy$ are relatively prime and have product equal to a square (namely z^2), by the uniqueness of prime factorization in $\mathbb{Z}[i]$, there exists some $s + it \in \mathbb{Z}[i]$ and some unit $u \in \{1, i, -1, -i\}$ such that $x + iy = u(s + it)^2$.
- Multiplying out yields $x + iy = u\left[(s^2 - t^2) + (2st)i\right]$.
- Since x is positive and even while y is odd, we must have $u = -i$: then $x + iy = 2st + (t^2 - s^2)i$ and so $x = 2st$, $y = t^2 - s^2$. Then $z = t^2 + s^2$, and so we are done.

Pythagorean Triples, IX

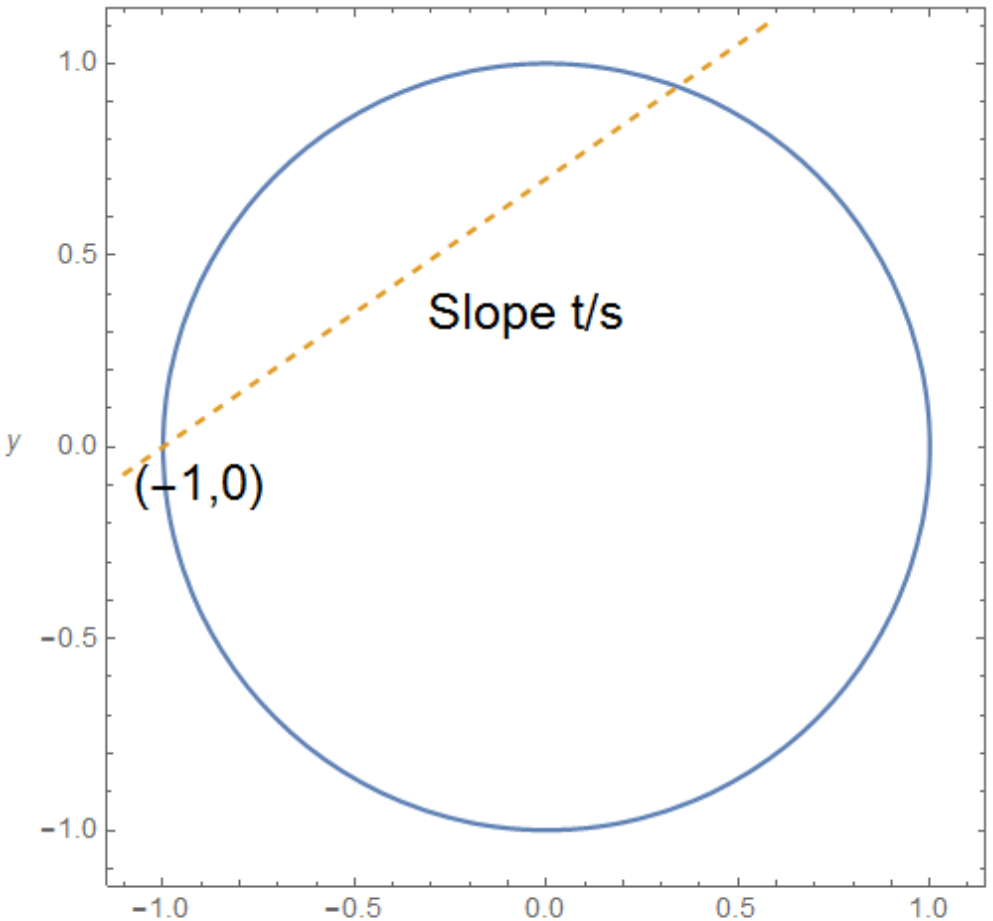
Proof #3:

- 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.

Pythagorean Triples, X

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.

Pythagorean Triples, XI

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.

Pythagorean Triples, XII

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.

Pythagorean Triples, XIII

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	$(48,55,73)$	

Summary

We discussed the logistics for Math 4527.

We discussed Pythagorean triples and gave a recipe for generating all of them.

Next lecture: Linear Diophantine equations.