Lecture 1

Prerequisites:

The official departmental prerequisite for this class is calc. 2, however it would be helpful if you've had a course on logic and proofs. This isn't strictly required, and we will quickly review proof techniques as necessary, but if you're already comfortable with things like proof by contradiction and mathematical induction, then you're one step ahead of the game.

The book we'll be using is the fourth edition of Joseph Silverman's "A Friendly Introduction to Number Theory." This book is unique because it's not really written for math majors, and doesn't follow the "theorem-proof-theorem-proof" format of most math texts.

Another interesting feature of the book is that it strongly encourages you to "experiment" with ideas in the problems. Though you don't necessarily need to use a computer

to perform these experiments, it's certainly helpful, and for this reason we will be using the software Sage in ~~class~~ this course.

Sage is a free, open source software package used by mathematicians all over the world and can be run online (http://cloud.sagemath.org) without requiring that you download or install any software on your own computer.

I am <u>not</u> requiring that you've had any previous experience with Sage or any other mathematics software before, and will give you an introduction to Sage during the course.

Collaborating w/classmates is strongly encouraged, but you must turn in your own copies of assignments, and you are responsible for understanding everything covered in each assignment.

You are <u>not</u> allowed to look up solutions to problems online/get copies of old assignments from friends who've had this class before, etc. On Sage assignments you will be expected to implement any algorithms you use, and not simply use Sage's built-in capabilities.

For example, we'll learn how to calculate the greatest common divisor of two numbers in class, and you will have an assignment where you are asked to write some Sage code for calculating these greatest common divisors. This means you should use the algorithm from class, and not simply type gcd into Sage.

As another example, I might ask you to write a list of numbers that satisfy some condition. Even though you could look a list up online, that's <u>not</u> what I want you to do — I want <u>you</u> to <u>think on your own</u> about how to generate that list. This will be difficult sometimes, but ultimately you'll learn a lot more if you think through the details on your own instead of just looking the answer up.

This class <u>will</u> be hard and will require a lot of working and studying outside of class to understand this material and do well in the class. You will sometimes feel very confused and frustrated by assignments, but this is completely normal. Just persevere and keep working, and you'll understand everything

we'll do in class.

What is number theory?

Number theory is primarily concerned with the study of relationships between the natural numbers. (a natural number is a positive whole number, e.g. 1, 2, 3, 4, 5, 6, ..., and the collection of all natural numbers is denoted $\mathbb{N}$.)

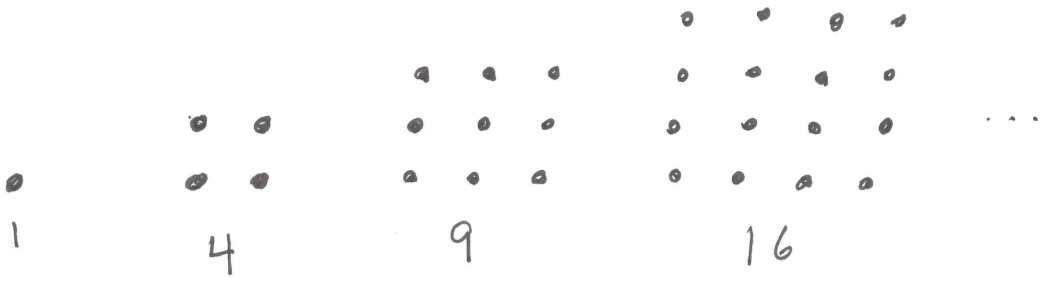
Number theory is a branch of pure mathematics, meaning math for the sake of math. This is unlike applied mathematics which is math that's developed and studied because it's useful in another field like physics or engineering. However, number theory does have applications, such as cryptography, it's just that most mathematicians who study number theory do so for its intrinsic beauty and interest. That beautiful mathematics is often useful mathematics is a happy coincidence.

One common theme in number theory is to divide the natural numbers into categories which have some prescribed property, and then ask questions about how the numbers in these categories are related to one another, or how they might be related to other categories.

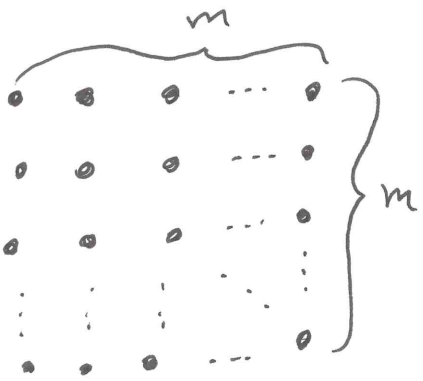
A few common categories are the following:

Square numbers

A **square number** is a natural number n where a square can be made of exactly n objects (pebbles, say):



Equivalently, n is square if there exists a natural number m such that $n = m^2$. In terms of the squares pictured above, m represents the length of the sides of the square.



$$n = m^2$$

The first few square numbers are

1	4	9	16	25	36	...
"	"	"	"	"	"	
1^2	2^2	3^2	4^2	5^2	6^2	

Here's an example of a question we may ask about squares numbers: Notice that sometimes when you add two squares together, you get a square — e.g.,

$$9 + 16 = 25 \qquad 25 + 144 = 169$$
$$3^2 + 4^2 = 5^2 \qquad 5^2 + 12^2 = 13^2$$

But this doesn't always happen: $4^2 + 5^2 = 16 + 25 = 41$, but 41 is not square! It's natural to ask when a sum of two squares yields a square.

- How many squares can be written as a sum of two squares? Are there infinitely many, or only finitely many?
- Is there an easy way to tell if a square can be written as a sum of two squares?
- Is there a way to produce a list of all the squares which may be written as a sum of two squares?

Triangular Numbers

A natural number n is *triangular* if we can take n objects and arrange them in a triangle with 1 object on the first row, 2 objects on the second row, three on third, and so on...

Here's a question about triangular numbers you may already know the answer to: Is there any pattern the triangular numbers must satisfy?

Notice if n is triangular, then there must exist a natural number m such that

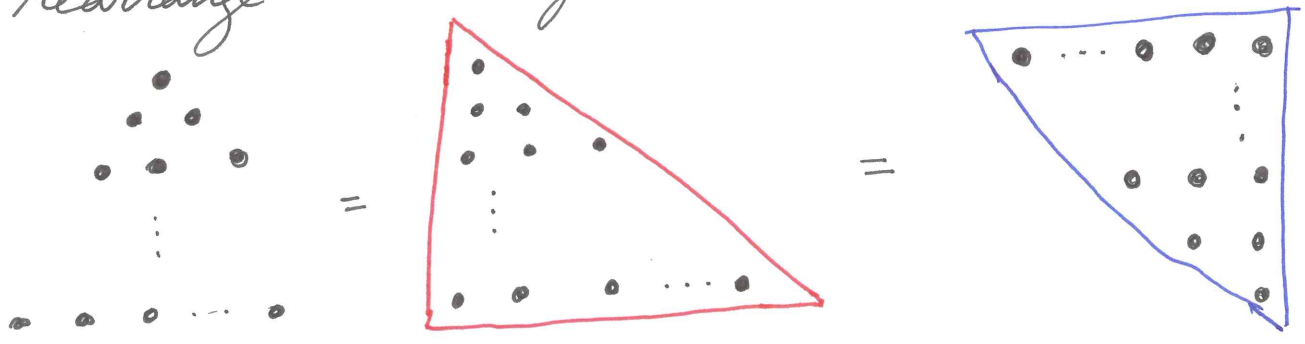
$$n = 1 + 2 + 3 + \cdots + (m-1) + m$$

(Precisely because there's one object on the first row, two on the second, etc...)

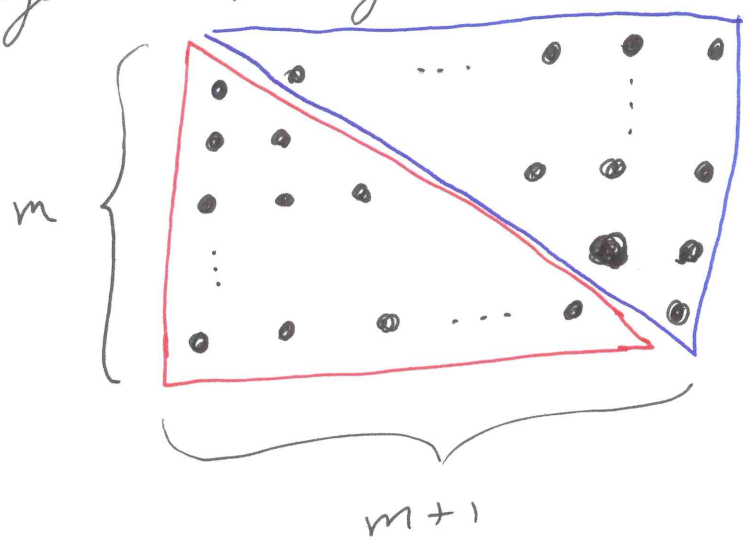
But there's a famous formula for these sums due to Gauss:

$$\sum_{i=1}^{m} i = \frac{m^2 + m}{2}$$

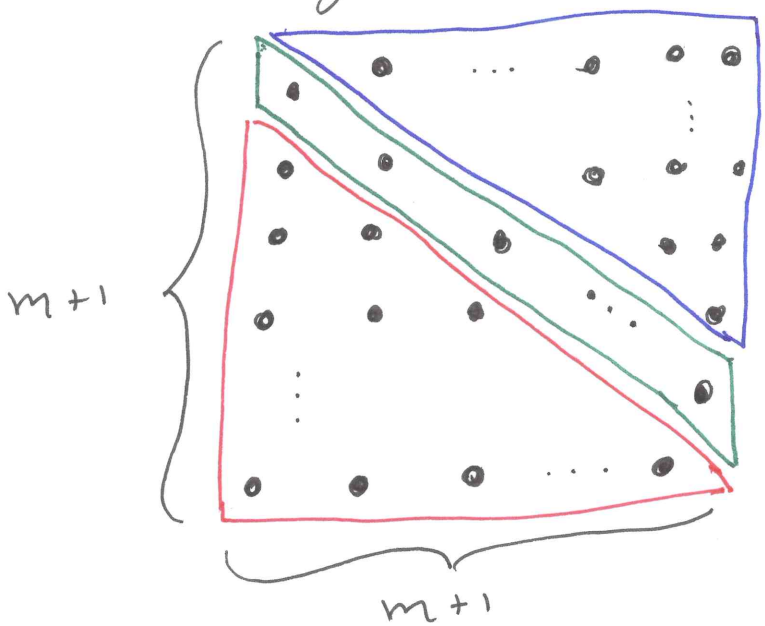
If you don't know this formula, it's pretty easy to prove. First, let's rearrange the objects in our triangle



We can now slide these triangles together to get an $(m+1) \times m$ rectangle



Let's make this a square by adding in the diagonal between the triangles:



But there are $(m+1)^2$ objects in this square, and thus we have

$$\left[\sum_{i=1}^{m} i\right] + [m+1] + \left[\sum_{i=1}^{m} i\right] = (m+1)^2$$

$$= m^2 + 2m + 1$$

$$\Rightarrow 2\sum_{i=1}^{m} i + [m+1] = m^2 + 2m + 1$$

$$\Rightarrow 2\sum_{i=1}^{m} i = m^2 + 2m + 1 - [m+1]$$

$$= m^2 + 2m + 1 - m - 1$$

$$= m^2 + m$$

$$\Rightarrow \sum_{i=1}^{m} i = \frac{m^2 + m}{2}$$

And these are precisely the triangular numbers:

$$1, \quad 3, \quad 6, \quad 10, \quad 15, \quad \ldots$$

$$\| \quad \| \quad \| \quad \| \quad \|$$

$$\frac{1^2+1}{2} \quad \frac{2^2+2}{2} \quad \frac{3^2+3}{2} \quad \frac{4^2+4}{2} \quad \frac{5^2+5}{2}$$

Prime numbers

A natural number n is *prime* if it's not divisible by any numbers other than 1 and n. The first few primes are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, ...

One obvious question we'll answer is later is are there infinitely-many primes or not.

Here's another interesting question: notice that sometimes primes come in pairs where n and $n+2$ are both prime:

3, 5 5, 7 11, 13 17, 19 29, 31

These are called twin primes. Are there infinitely-many twin primes? Even though this question has been around 160 years, no one has been able to solve it, yet.

We could also consider pairs $n, n+4$ which are both prime

3, 7 7, 11 13, 17 19, 23 37, 41

Or both $n, n+6$ are prime

5, 11 11, 17 13, 19 17, 23

Or n and n plus any other even number (Question to make sure you're awake: why do I only say "even" above?)

This question was completely open until 2013 when Yitang Zhang from the University of New Hampshire showed that there exists

some constant k, $k \leq 70{,}000{,}000$, such that there are infinitely prime pairs $n, n+k$

One of the most fascinating aspects of number theory is that easy-to-state problems can be very difficult to solve and require some very advanced mathematics. Maybe the most famous example of this is Andrew Wiles' proof of Fermat's Last Theorem.

In 1637, Pierre de Fermat conjectured that if $n > 2$, there are no integers a, b, c solving the equation

$$a^n + b^n = c^n$$

Fermat even boasted in the margins of one of his books that he had a marvelous proof of this fact, but it was too big to fit in the margins. Many mathematicians tried, and failed, to solve Fermat's last conjecture. A proof was finally obtained by Andrew Wiles in 1994, and the proof took seven years, and used very high-level mathematics developed only in the 20th century.

(Today no one believes Fermat actually had a correct proof in the 1600's.)

Now that we have an idea of what kind of questions are asked in number theory, how do we go about answering these questions? We will generally (but not always) apply the following procedure:

Step 1 - Experiment

Look at simple examples and gather data. If possible and appropriate, use a computer (ie., write Sage code) to generate lots of examples

Step 2 - Observation

Look for patterns in your data — are there any relationships that suddenly present themselves after you've looked at several examples?

Step 3 - Hypothesis

Make conjectures based on your observations

Step 4 - Test your hypotheses

After making some conjectures, put your ideas to the test by collecting more, newer data. A good hypothesis/conjecture should make predictions about what patterns or relationships you'll see in future experiments

Step 5 - Proof

Provide logical reasoning which shows why your conjectures must be true.

"Proof" is what distinguishes mathematics from the sciences. Science is a process of uncovering the nature of the universe by applying the scientific method, which consists of steps 1-4 above. However, no scientific theory is ever completely set in stone: new observational data can come along which challenges the current theory. When this happens, scientists then have to revise the theory to explain new observations. (E.g., Newton's laws of motion being supplanted by Einstein's theories of relativity.)

In mathematics, however, we are capable of knowing something with absolute certainty that can not be challenged by new observations — the Pythagorean theorem will not cease to be true tomorrow because someone discovered a right triangle where the Pythagorean theorem does not apply. This is the power of mathematics: the ability to say something is true and have it set in stone.

These "true statements" in mathematics are known as theorems, and the logical argument which shows a theorem must be true are called "proofs." Part of the business of doing mathematics is discovering new theorems

The famous mathematician Paul Erdös once said "a mathematician is a machine for turning coffee into theorems."

Proofs are usually, but not always, obtained by applying one of several common proof techniques, and throughout the course of this semester we will see, and apply, some of these common techniques. (If you're already familiar with proofs, that's great. If you're not, don't worry: we'll take the time to explain things as necessary.

#

Let's end this lecture by considering how to apply the 5-step process above to solve an exercise from the book.

Exercise 1.2 (pg 11)

Find a formula for the sum of the first m odd numbers, and provide a geometric proof the formula is correct.

Let's first be certain we know what an odd number is. A natural number n is odel if there exists a natural number m such that $n = 2m - 1$.

The first few odd numbers are

$$1 = 2\cdot 1 - 1$$
$$3 = 2\cdot 2 - 1$$
$$5 = 2\cdot 3 - 1$$
$$7 = 2\cdot 4 - 1$$
$$9 = 2\cdot 5 - 1$$
$$\vdots$$

So the m^{th} odd number is $2m-1$ ——

E.g., the $1,342^{nd}$ odd number is $2\cdot 1342 - 1 = 2683$.

Our goal is to find a formula for expressing the sum of the first m odds:

$$1 + 3 + 5 + 7 + \cdots + (2m-1) = \sum_{i=1}^{m} (2i-1)$$

So let's first write down a few simple examples and see if we notice a pattern:

m	Sum	
1	$\sum_{i=1}^{1} (2i-1) = 1$	$= 1$
2	$\sum_{i=1}^{2} (2i-1) = 1+3$	$= 4$
3	$\sum_{i=1}^{3} (2i-1) = 1+3+5$	$= 9$
4	$\sum_{i=1}^{4} (2i-1) = 1+3+5+7$	$= 16$
5	$\sum_{i=1}^{5} (2i-1) = 1+3+5+7+9$	$= 25$

Now we start to see a pattern: it looks like the sum of the first m odd numbers gives m^2, and so we have our conjecture:

Conjecture

$$\sum_{i=1}^{m} (2i-1) = m^2$$

If this conjecture is true, then it should be that the sum of the first 30 odds is $30^2 = 900$; and the sum of the first 1000 odds is $1000^2 = 1{,}000{,}000$. We can use a computer (or calculator, or pen & paper if you're masochistic) to see if this is the case. Sure enough, entering these sums into a computer tells us what we suspected:

$1+3+5+\ldots+57+59 = 900$ ← First 30 odds

$1+3+5+\ldots+1997+1999 = 1000000$ ← First 1000 odds

At this point it's worth noting that the patterns you observe from your data may not actually be there and can mislead you. Human beings are pretty good at pattern recognition, but as a consequence we sometimes mistake coincidence as meaningful patterns. So you need to be careful when looking for patterns, and always try to put any

patterns you notice to the test.

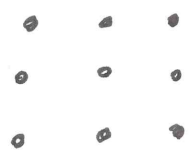
We now feel pretty confident that $\sum_{i=1}^{m} (2i-1) = m^2$, but we haven't proven it yet.

To prove this, since we're using the square numbers, let's examine some of the corresponding squares:

$1 = 1^2$

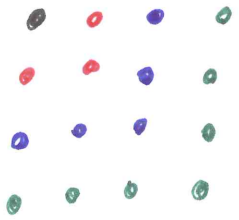
$4 = 2^2$

$9 = 3^2$



$16 = 4^2$

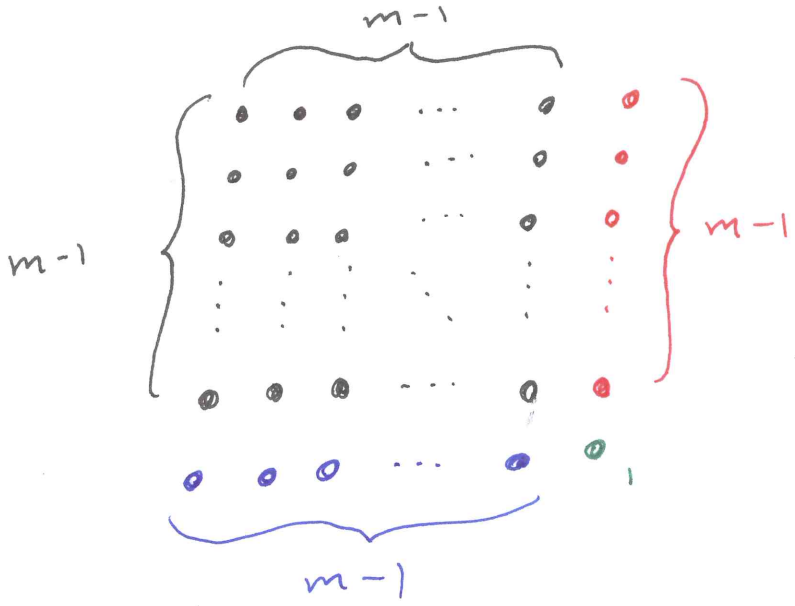
Notice we get an $m \times m$ square from an $(m-1) \times (m-1)$ square by adding an extra row and a column. Let's start off w/ the 1×1 square and work our way up to a 4×4 square, adding rows & columns of different colors



Notice we have 1 black dot, 3 red dots, 5 blue dots, and 7 green dots.

It certainly appears that the "outside edge" (right-hand column and bottom row) of an $m \times m$ square consists of $2m-1$ dots, but we need to be sure — we need to prove this is always the case.

To prove this always happens, notice if we build an $m \times m$ square from an $(m-1) \times (m-1)$ square, we attach another column ($m-1$ more dots), another row (another $m-1$ dots), and a corner (1 more dot)



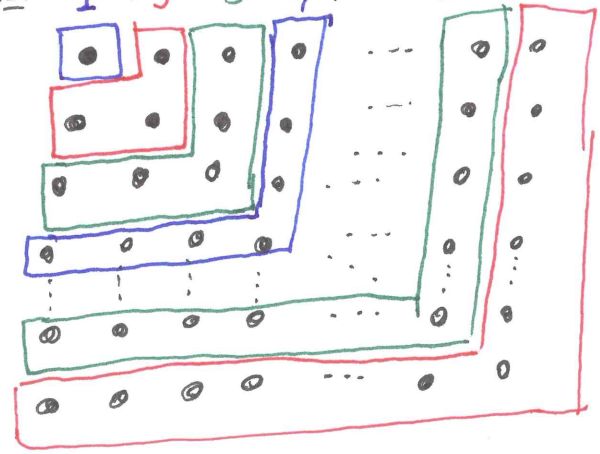
So we've added a total of

$$(m-1)+(m-1)+1$$
$$= 2m-2+1$$
$$= 2m-1$$

dots. Hence we know that the "outside edge" of an $m \times m$ square does indeed consist of $2m-1$ dots.

Building up an $m \times m$ square by successively adding on these outside edges gives the result:

$$\sum_{i=1}^{m} (2i-1) = 1 + 3 + 5 + 7 + \cdots + 2(m-1)-1 + 2m-1 = m^2$$



Homework

- Due Tues., Jan 13:
  Read Ch. 1 (6 pages) of Silverman
- Due Tues., Jan 20:
  Exercises 1.1, 1.5, 1.6 in Silverman
  (More exercises from Chs. 2 & 3 will be added)