Number Theory

Honors Discovery Seminar

April 5, 2023

Introduction

Definition

An **integer** is a whole number that can be positive or negative.

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

Number Theory is the study of integers and the study of integer solutions to equations.

Introduction

Definition

An positive integer $n > 1$ is a **prime number** if the only divisors of n are 1 and itself.

As you learn in your youth, every positive integer has a prime factorization, so primes are the 'building blocks' of all integers.

Introduction

We know both a lot and very little about prime numbers.
Things we know:

Things we don't know:

Introduction

We know both a lot and very little about prime numbers.

Things we know:

- There are infinitely many prime numbers.

Things we don't know:

Introduction

We know both a lot and very little about prime numbers.

Things we know:

- There are infinitely many prime numbers.
- If you pick a number at random from between 1 and N, the probability that it is prime is about $1/\ln(N)$.

Things we don't know:

Introduction

We know both a lot and very little about prime numbers.

Things we know:

- There are infinitely many prime numbers.
- If you pick a number at random from between 1 and N, the probability that it is prime is about $1/\ln(N)$.

Things we don't know:

- Are there infinitely many *twin primes* (primes that are 2 apart, like 3 and 5, or 41 and 43)?

Introduction

We know both a lot and very little about prime numbers.

Things we know:

- There are infinitely many prime numbers.
- If you pick a number at random from between 1 and N, the probability that it is prime is about $1/\ln(N)$.

Things we don't know:

- Are there infinitely many *twin primes* (primes that are 2 apart, like 3 and 5, or 41 and 43)?
- Are there infinitely many primes that are also Fibonacci numbers?

Introduction

We know both a lot and very little about prime numbers.

Things we know:

- There are infinitely many prime numbers.
- If you pick a number at random from between 1 and N, the probability that it is prime is about $1/\ln(N)$.

Things we don't know:

- Are there infinitely many *twin primes* (primes that are 2 apart, like 3 and 5, or 41 and 43)?
- Are there infinitely many primes that are also Fibonacci numbers?
- Are there infinitely many Mersenne primes (primes of the form $2^n - 1$)?

Introduction

We also use number theory to study integer solutions to equations. In this case, there is also a lot and yet very little we know.

Things we know:

Things we don't know:

Introduction

We also use number theory to study integer solutions to equations. In this case, there is also a lot and yet very little we know.

Things we know:

- There are infinitely many integer solutions to $x^2 + y^2 = z^2$ (solutions: Pythagorean triples)

Things we don't know:

Introduction

We also use number theory to study integer solutions to equations. In this case, there is also a lot and yet very little we know.

Things we know:

- There are infinitely many integer solutions to $x^2 + y^2 = z^2$ (solutions: Pythagorean triples)
- If none of x, y, z are 0, there are *no* integer solutions to $x^n + y^n = z^n$, $n > 2$. This is *Fermat's Last Theorem*, proved in 1995 by Andrew Wiles.)

Things we don't know:

Introduction

We also use number theory to study integer solutions to equations. In this case, there is also a lot and yet very little we know.

Things we know:

- There are infinitely many integer solutions to $x^2 + y^2 = z^2$ (solutions: Pythagorean triples)
- If none of x, y, z are 0, there are *no* integer solutions to $x^n + y^n = z^n$, $n > 2$. This is *Fermat's Last Theorem*, proved in 1995 by Andrew Wiles.)

Things we don't know:

- Can every positive even number be written as the sum of two primes?

Introduction

We also use number theory to study integer solutions to equations. In this case, there is also a lot and yet very little we know.

Things we know:

- There are infinitely many integer solutions to $x^2 + y^2 = z^2$ (solutions: Pythagorean triples)
- If none of x, y, z are 0, there are *no* integer solutions to $x^n + y^n = z^n$, $n > 2$. This is *Fermat's Last Theorem*, proved in 1995 by Andrew Wiles.)

Things we don't know:

- Can every positive even number be written as the sum of two primes?
- Starting with any n, does the sequence obtained by dividing n by 2 if n is even and multiplying n by 3 and adding 1 if n is odd always terminate?
- Can every positive integer n that does not have remainder of 4 or 5 when divided by 9 equal to the sum of three cubes?

Things we don't know, continued:

- Can every positive integer n that does not have remainder of 4 or 5 when divided by 9 equal to the sum of three cubes?
  Meaning: can we solve the equation $x^3 + y^3 + z^3 = n$?

Things we don't know, continued:

- Can every positive integer n that does not have remainder of 4 or 5 when divided by 9 equal to the sum of three cubes?
  Meaning: can we solve the equation $x^3 + y^3 + z^3 = n$?
- Even for small n, we don't know: the numbers ≤ 1000 for which we have no idea are $114, 390, 627, 633, 732, 921, 975$.

Things we don't know, continued:

- Can every positive integer n that does not have remainder of 4 or 5 when divided by 9 equal to the sum of three cubes?
  Meaning: can we solve the equation $x^3 + y^3 + z^3 = n$?
- Even for small n, we don't know: the numbers ≤ 1000 for which we have no idea are $114, 390, 627, 633, 732, 921, 975$.
- It was only in 2019 that a solution was found for 33 (Booker) and 42 (Booker and Sutherland) using over a million hours of computing time:

$$33 = 8\ 866\ 128\ 975\ 287\ 528^3 + (-8\ 778\ 405\ 442\ 862\ 239)^3 + (-2\ 736\ 111\ 468\ 807\ 040)^3$$

$$42 = (-80\ 538\ 738\ 812\ 075\ 974)^3 + 80\ 435\ 758\ 145\ 817\ 515^3 + 12\ 602\ 123\ 297\ 335\ 631^3$$

Application

While number theory is a stand-alone beautiful subject studying the counting numbers served up by the universe, it has many important applications. The main one we'll talk about today is **cryptography.**

Quick Introduction to Public Key-Private Key Encryption