# Two Problems of Number Theory

Manindra Agarwal

IIT Kanpur

LSR Delhi, September 18, 2009

# Outline

1. Introduction

2. Fermat's Last Theorem

3. Counting Primes

# Number Theory

- Number Theory is the study of properties of numbers.
- Here, by numbers, we mean integers.
- Properties of reals and complex numbers fall in a different area called Analysis.

# Number Theory

- Number Theory is the study of properties of numbers.
- Here, by numbers, we mean integers.
- Properties of reals and complex numbers fall in a different area called Analysis.

# Number Theory

- Number Theory is the study of properties of numbers.
- Here, by numbers, we mean integers.
- Properties of reals and complex numbers fall in a different area called Analysis.

# Fundamental Theorem of Arithmetic

- The study starts with Fundamental Theorem of Arithmetic: every number can be written uniquely as a product of prime numbers.
- Hence, prime numbers are of great importance in number theory.
- Most of the problems of numbers translate to problems on prime numbers via the Fundamental Theorem.

# Fundamental Theorem of Arithmetic

- The study starts with Fundamental Theorem of Arithmetic: every number can be written uniquely as a product of prime numbers.
- Hence, prime numbers are of great importance in number theory.
- Most of the problems of numbers translate to problems on prime numbers via the Fundamental Theorem.

# Diophantine Problems

- A class of problems, called Diophantine Problems, address the question whether an equation has integer solutions.
- For example, consider
$$x^2 + y^2 = z^2.$$
- Are there integer values of $x$, $y$, and $z$ that satisfy this equation?
- Answer: yes!
$$x = 3, y = 4, z = 5$$
is one solution.
- In fact, for any pair of integers $u$ and $v$,
$$x = u^2 - v^2, y = 2uv, z = u^2 + v^2$$
is a solution to the equation.
- The solutions are called Pythagorean triples.

# Diophantine Problems

- A class of problems, called Diophantine Problems, address the question whether an equation has integer solutions.
- For example, consider

$$x^2 + y^2 = z^2.$$

- Are there integer values of $x$, $y$, and $z$ that satisfy this equation?
- Answer: yes!

$$x = 3, y = 4, z = 5$$

  is one solution.
- In fact, for any pair of integers $u$ and $v$,

$$x = u^2 - v^2, y = 2uv, z = u^2 + v^2$$

  is a solution to the equation.
- The solutions are called Pythagorean triples.

# Diophantine Problems

- A class of problems, called Diophantine Problems, address the question whether an equation has integer solutions.
- For example, consider

$$x^2 + y^2 = z^2.$$

- Are there integer values of $x$, $y$, and $z$ that satisfy this equation?
- Answer: yes!

$$x = 3, y = 4, z = 5$$

  is one solution.
- In fact, for any pair of integers $u$ and $v$,

$$x = u^2 - v^2, y = 2uv, z = u^2 + v^2$$

  is a solution to the equation.
- The solutions are called Pythagorean triples.

# Diophantine Problems

- A class of problems, called Diophantine Problems, address the question whether an equation has integer solutions.
- For example, consider

$$x^2 + y^2 = z^2.$$

- Are there integer values of $x$, $y$, and $z$ that satisfy this equation?
- Answer: yes!

$$x = 3, y = 4, z = 5$$

  is one solution.
- In fact, for any pair of integers $u$ and $v$,

$$x = u^2 - v^2, y = 2uv, z = u^2 + v^2$$

  is a solution to the equation.
- The solutions are called Pythagorean triples.

# Diophantine Problems

- Another example is Pell's equations:

$$x^2 - ny^2 = 1$$

  for non-square $n$.

- A solution of Pell's equation gives a good rational approximation of $\sqrt{n}$:

$$(\frac{x}{y})^2 = n + \frac{1}{y^2}.$$

- Budhayana (ca. 800 BC) gave two soltions of $x^2 - 2y^2 = 1$: $(17, 12)$ and $(577, 408)$.
- Lagrange (1736 - 1813) showed that all Pell's equations have infinitely many solutions.
- Notice that it is much more difficult to find solutions of equations in integers than it is in reals!

# Diophantine Problems

- Another example is Pell's equations:

$$x^2 - ny^2 = 1$$

  for non-square $n$.

- A solution of Pell's equation gives a good rational approximation of $\sqrt{n}$:

$$(\frac{x}{y})^2 = n + \frac{1}{y^2}.$$

- Budhayana (ca. 800 BC) gave two soltions of $x^2 - 2y^2 = 1$: $(17, 12)$ and $(577, 408)$.
- Lagrange (1736 - 1813) showed that all Pell's equations have infinitely many solutions.
- Notice that it is much more difficult to find solutions of equations in integers than it is in reals!

# Diophantine Problems

- Another example is Pell's equations:

$$x^2 - ny^2 = 1$$

  for non-square $n$.

- A solution of Pell's equation gives a good rational approximation of $\sqrt{n}$:

$$(\frac{x}{y})^2 = n + \frac{1}{y^2}.$$

- Budhayana (ca. 800 BC) gave two soltions of $x^2 - 2y^2 = 1$: $(17, 12)$ and $(577, 408)$.
- Lagrange (1736 - 1813) showed that all Pell's equations have infinitely many solutions.
- Notice that it is much more difficult to find solutions of equations in integers than it is in reals!

# Counting Prime Numbers

- Many questions on prime numbers are about counting:
  - How many prime numbers exist? [infinite]
  - How many prime numbers are less than $n$? [About $\frac{n}{\ln n}$]
  - How many twin primes (primes numbers at distance 2) are there?
  - What is the maximum gap between two consecutive primes?
- The first question was answered by Euclid (ca. 300 BC):
  - Assume there are finitely many primes.
  - Let $n$ be the largest prime.
  - But prime factorization of $n! + 1$ does not include any prime less than or equal to $n$.
  - Contradiction.

# Counting Prime Numbers

- Many questions on prime numbers are about counting:
  - How many prime numbers exist? [infinite]
  - How many prime numbers are less than $n$? [About $\frac{n}{\ln n}$]
  - How many twin primes (primes numbers at distance 2) are there?
  - What is the maximum gap between two consecutive primes?
- The first question was answered by Euclid (ca. 300 BC):
  - Assume there are finitely many primes.
  - Let $n$ be the largest prime.
  - But prime factorization of $n! + 1$ does not include any prime less than or equal to $n$.
  - Contradiction.

# Counting Prime Numbers

- Many questions on prime numbers are about counting:
  - How many prime numbers exist? [infinite]
  - How many prime numbers are less than $n$? [About $\frac{n}{\ln n}$]
  - How many twin primes (primes numbers at distance 2) are there?
  - What is the maximum gap between two consecutive primes?
- The first question was answered by Euclid (ca. 300 BC):
  - Assume there are finitely many primes.
  - Let $n$ be the largest prime.
  - But prime factorization of $n! + 1$ does not include any prime less than or equal to $n$.
  - Contradiction.

# Counting Prime Numbers

- Many questions on prime numbers are about counting:
  - How many prime numbers exist? [infinite]
  - How many prime numbers are less than $n$? [About $\frac{n}{\ln n}$]
  - How many twin primes (primes numbers at distance 2) are there?
  - What is the maximum gap between two consecutive primes?
- The first question was answered by Euclid (ca. 300 BC):
  - Assume there are finitely many primes.
  - Let $n$ be the largest prime.
  - But prime factorization of $n! + 1$ does not include any prime less than or equal to $n$.
  - Contradiction.

# Counting Prime Numbers

- Many questions on prime numbers are about counting:
  - How many prime numbers exist? [infinite]
  - How many prime numbers are less than $n$? [About $\frac{n}{\ln n}$]
  - How many twin primes (primes numbers at distance $2$) are there?
  - What is the maximum gap between two consecutive primes?
- The first question was answered by Euclid (ca. 300 BC):
  - Assume there are finitely many primes.
  - Let $n$ be the largest prime.
  - But prime factorization of $n! + 1$ does not include any prime less than or equal to $n$.
  - Contradiction.

# Counting Prime Numbers

- Many questions on prime numbers are about counting:
  - How many prime numbers exist? [infinite]
  - How many prime numbers are less than $n$? [About $\frac{n}{\ln n}$]
  - How many twin primes (primes numbers at distance 2) are there?
  - What is the maximum gap between two consecutive primes?
- The first question was answered by Euclid (ca. 300 BC):
  - Assume there are finitely many primes.
  - Let $n$ be the largest prime.
  - But prime factorization of $n! + 1$ does not include any prime less than or equal to $n$.
  - Contradiction.

# Counting Prime Numbers

- Many questions on prime numbers are about counting:
  - How many prime numbers exist? [infinite]
  - How many prime numbers are less than $n$? [About $\frac{n}{\ln n}$]
  - How many twin primes (primes numbers at distance 2) are there?
  - What is the maximum gap between two consecutive primes?
- The first question was answered by Euclid (ca. 300 BC):
  - Assume there are finitely many primes.
  - Let $n$ be the largest prime.
  - But prime factorization of $n! + 1$ does not include any prime less than or equal to $n$.
  - Contradiction.

# Counting Prime Numbers

- Many questions on prime numbers are about counting:
  - How many prime numbers exist? [infinite]
  - How many prime numbers are less than $n$? [About $\frac{n}{\ln n}$]
  - How many twin primes (primes numbers at distance $2$) are there?
  - What is the maximum gap between two consecutive primes?
- The first question was answered by Euclid (ca. 300 BC):
  - Assume there are finitely many primes.
  - Let $n$ be the largest prime.
  - But prime factorization of $n! + 1$ does not include any prime less than or equal to $n$.
  - Contradiction.

# Two Special Problems

- In this talk, we consider two problems.
- First problem: how many solutions exist for the equation

$$x^n + y^n = z^n$$

  when $n > 2$?
- Second problem: how many prime numbers exist less than $x$?
- Both the problems have a long history and have beeen instrumental in development of number theory.

# Two Special Problems

- In this talk, we consider two problems.
- First problem: how many solutions exist for the equation

$$x^n + y^n = z^n$$

  when $n > 2$?
- Second problem: how many prime numbers exist less than $x$?
- Both the problems have a long history and have beeen instrumental in development of number theory.

# Two Special Problems

- In this talk, we consider two problems.
- First problem: how many solutions exist for the equation

$$x^n + y^n = z^n$$

  when $n > 2$?
- Second problem: how many prime numbers exist less than $x$?
- Both the problems have a long history and have beeen instrumental in development of number theory.

# Two Special Problems

- In this talk, we consider two problems.
- First problem: how many solutions exist for the equation

$$x^n + y^n = z^n$$

when $n > 2$?

- Second problem: how many prime numbers exist less than $x$?
- Both the problems have a long history and have beeen instrumental in development of number theory.

# Outline

1. Introduction
2. Fermat's Last Theorem
3. Counting Primes

# Fermat's Last Theorem

**Theorem**

*There are no non-zero integer solutions of the equation $x^n + y^n = z^n$ when $n > 2$.*

# Fermat's Last Theorem

Towards the end of his life, Pierre de Fermat (1601-1665) wrote in the margin of a book:

I have discovered a truely remarkable proof of this theorem, but this margin is too small to write it down.

After more than 300 years, when the proof was finally written, it did take a little more than a margin to write.

# Fermat's Last Theorem

Towards the end of his life, Pierre de Fermat (1601-1665) wrote in the margin of a book:

I have discovered a truely remarkable proof of this theorem, but this margin is too small to write it down.

After more than 300 years, when the proof was finally written, it did take a little more than a margin to write.

# A Brief History

1660s: Fermat proved the theorem for $n = 4$.

1753: Euler proved the theorem for $n = 3$.

1825: Dirichlet and Legendre proved the theorem for $n = 5$.

1839: Lame proved the theorem for $n = 7$.

1857: Kummer proved the theorem for all $n \leq 100$.

# A Brief History

1660s: Fermat proved the theorem for $n = 4$.

1753: Euler proved the theorem for $n = 3$.

1825: Dirichlet and Legendre proved the theorem for $n = 5$.

1839: Lame proved the theorem for $n = 7$.

1857: Kummer proved the theorem for all $n \leq 100$.

# A Brief History

1660s: Fermat proved the theorem for $n = 4$.

1753: Euler proved the theorem for $n = 3$.

1825: Dirichlet and Legendre proved the theorem for $n = 5$.

1839: Lame proved the theorem for $n = 7$.

1857: Kummer proved the theorem for all $n \leq 100$.

# A Brief History

1660s: Fermat proved the theorem for $n = 4$.

1753: Euler proved the theorem for $n = 3$.

1825: Dirichlet and Legendre proved the theorem for $n = 5$.

1839: Lame proved the theorem for $n = 7$.

1857: Kummer proved the theorem for all $n \leq 100$.

# A Brief History

1660s: Fermat proved the theorem for $n = 4$.

1753: Euler proved the theorem for $n = 3$.

1825: Dirichlet and Legendre proved the theorem for $n = 5$.

1839: Lame proved the theorem for $n = 7$.

1857: Kummer proved the theorem for all $n \leq 100$.

# A Brief History

1983: Faltings proved that for any $n > 2$, the equation $x^n + y^n = z^n$ can have at most finitely many integer solutions.

1994: Wiles proved the theorem.

# A Brief History

1983: Faltings proved that for any $n > 2$, the equation $x^n + y^n = z^n$ can have at most finitely many integer solutions.

1994: Wiles proved the theorem.

# The Outline of Proof

- The proof transforms the problem to a problem in Geometry and then to a problem in Complex Analysis!
- The proof came after more than 325 years and was more than 100 pages long!
- First observe that we can assume $n$ to be a prime number:
  - Suppose $n = p \cdot q$ where $p$ is prime, and let solution $(a, b, c)$ satisfy $x^n + y^n = z^n$.
  - Then $(a^q, b^q, c^q)$ satisfies $x^p + y^p = z^p$.
- We now translate the problem to Elliptic curves.

# The Outline of Proof

- The proof transforms the problem to a problem in Geometry and then to a problem in Complex Analysis!
- The proof came after more than 325 years and was more than 100 pages long!
- First observe that we can assume $n$ to be a prime number:
  - Suppose $n = p \cdot q$ where $p$ is prime, and let solution $(a, b, c)$ satisfy $x^n + y^n = z^n$.
  - Then $(a^q, b^q, c^q)$ satisfies $x^p + y^p = z^p$.
- We now translate the problem to Elliptic curves.

# The Outline of Proof

- The proof transforms the problem to a problem in Geometry and then to a problem in Complex Analysis!
- The proof came after more than 325 years and was more than 100 pages long!
- First observe that we can assume $n$ to be a prime number:
  - Suppose $n = p \cdot q$ where $p$ is prime, and let solution $(a, b, c)$ satisfy $x^n + y^n = z^n$.
  - Then $(a^q, b^q, c^q)$ satisfies $x^p + y^p = z^p$.
- We now translate the problem to Elliptic curves.

# The Outline of Proof

- The proof transforms the problem to a problem in Geometry and then to a problem in Complex Analysis!
- The proof came after more than 325 years and was more than 100 pages long!
- First observe that we can assume $n$ to be a prime number:
  - Suppose $n = p \cdot q$ where $p$ is prime, and let solution $(a, b, c)$ satisfy $x^n + y^n = z^n$.
  - Then $(a^q, b^q, c^q)$ satisfies $x^p + y^p = z^p$.
- We now translate the problem to Elliptic curves.

# Elliptic Curves

### Definition

An elliptic curve is given by equation:

$$y^2 = x^3 + Ax + B$$

for numbers $A$ and $B$ satisfying $4A^3 + 27B^2 \neq 0$.

- We will be interested in curves for which both $A$ and $B$ are rational numbers.
- Elliptic curves have truly amazing properties as we shall see.

# Elliptic Curves

## Definition

An elliptic curve is given by equation:

$$y^2 = x^3 + Ax + B$$

for numbers $A$ and $B$ satisfying $4A^3 + 27B^2 \neq 0$.

- We will be interested in curves for which both $A$ and $B$ are rational numbers.
- Elliptic curves have truly amazing properties as we shall see.

# Elliptic Curves

## Definition

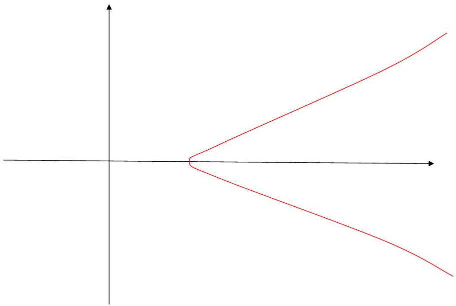
An elliptic curve is given by equation:

$$y^2 = x^3 + Ax + B$$

for numbers $A$ and $B$ satisfying $4A^3 + 27B^2 \neq 0$.

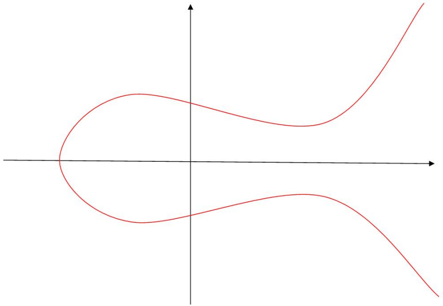
- We will be interested in curves for which both $A$ and $B$ are rational numbers.
- Elliptic curves have truly amazing properties as we shall see.

# Elliptic Curve Examples



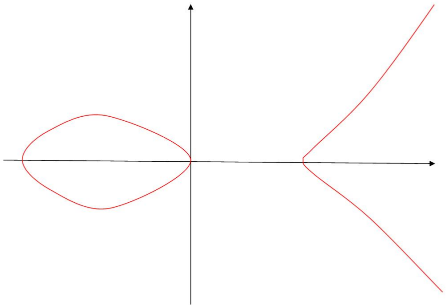
$y^2 = x^3 - 1$

# Elliptic Curve Examples



$$y^2 = x^3 - 3x + 3$$

# Elliptic Curve Examples



$y^2 = x^3 - x$

# Discriminant of an Elliptic Curve

- Let $E$ be an elliptic curve given by equation $y^2 = x^3 + Ax + B$.
- Discriminant $\Delta$ of $E$ is the number $4A^3 + 27B^2$.
- We require the discriminant of $E$ to be non-zero.
- This condition is equivalent to the condition that the three (perhaps complex) roots of the polynomial $x^3 + Ax + B$ are distinct. [Verify!]
- If $x^3 + Ax + B = (x - \alpha)(x - \beta)(x - \gamma)$ then

$$\Delta = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

# Discriminant of an Elliptic Curve

- Let $E$ be an elliptic curve given by equation $y^2 = x^3 + Ax + B$.
- Discriminant $\Delta$ of $E$ is the number $4A^3 + 27B^2$.
- We require the discriminant of $E$ to be non-zero.
- This condition is equivalent to the condition that the three (perhaps complex) roots of the polynomial $x^3 + Ax + B$ are distinct. [Verify!]
- If $x^3 + Ax + B = (x - \alpha)(x - \beta)(x - \gamma)$ then

$$\Delta = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

# Rational Points on an Elliptic Curve

- Let $E(\mathbb{Q})$ be the set of rational points on the curve $E$.
- We add a "point at infinity," called $O$, to this set.

**Amazing Fact**

We can define an "addition" operation on the set of points in $E(\mathbb{Q})$ just like integer addition.

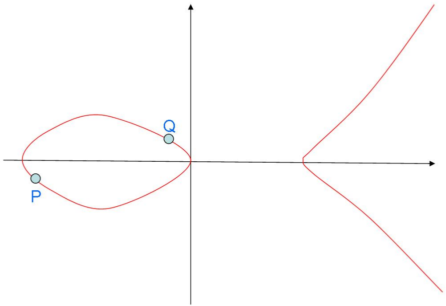
# Rational Points on an Elliptic Curve

- Let $E(\mathbb{Q})$ be the set of rational points on the curve $E$.
- We add a "point at infinity," called $O$, to this set.

**Amazing Fact**

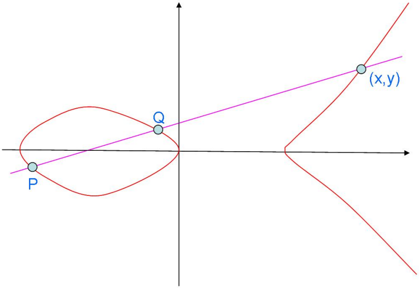
We can define an "addition" operation on the set of points in $E(\mathbb{Q})$ just like integer addition.

# Addition of Points on $E$

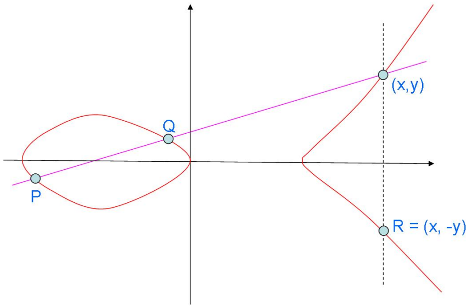



Adding points P & Q on curve $y^2 = x^3 - x$

# Addition of Points on $E$

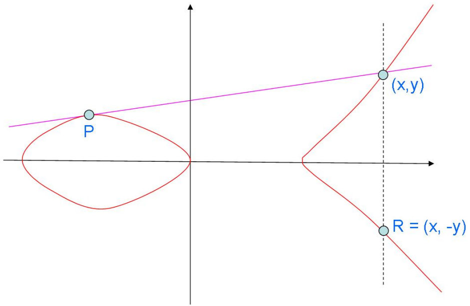


# Addition of Points on $E$



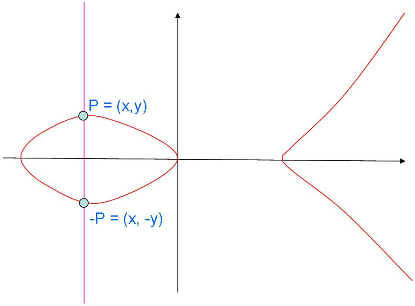

P + Q = R

# Addition of Points on $E$




P + P = R

# Addition of Points on $E$




P + (-P) = O

# Addition of Points on $E$

- Observe that if points $P$ and $Q$ on $E$ are rational, then point $P + Q$ is also rational. [Verify!]
- The point addition obeys same laws as integer addition with point at infinity $O$ acting as the "zero" of point addition.
- The point addition has some additional interesting properties too.

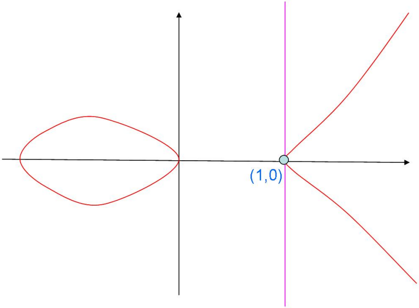
# Addition of Points on $E$

- Observe that if points $P$ and $Q$ on $E$ are rational, then point $P + Q$ is also rational. [Verify!]
- The point addition obeys same laws as integer addition with point at infinity $O$ acting as the "zero" of point addition.
- The point addition has some additional interesting properties too.

# Addition of Points on $E$

- Observe that if points $P$ and $Q$ on $E$ are rational, then point $P+Q$ is also rational. [Verify!]
- The point addition obeys same laws as integer addition with point at infinity $O$ acting as the "zero" of point addition.
- The point addition has some additional interesting properties too.

# Addition of Points on $E$




(1,0) + (1,0) = O

# A Special Elliptic Curve

Let $(a, b, c)$ be an integer solution of the equation $x^n + y^n = z^n$ for some prime $n > 2$.

**Definition**

Define an elliptic curve $E_n$ by the equation:

$$y^2 = x(x - a^n)(x + b^n).$$

- Discriminant of this curve is:

$$\Delta_n = (a^n)^2 \cdot (b^n)^2 \cdot (a^n + b^n)^2 = (abc)^{2n}.$$

- So the discriminant is $2n$th power of an integer.

# A Special Elliptic Curve

Let $(a, b, c)$ be an integer solution of the equation $x^n + y^n = z^n$ for some prime $n > 2$.

**Definition**

Define an elliptic curve $E_n$ by the equation:

$$y^2 = x(x - a^n)(x + b^n).$$

- Discriminant of this curve is:

$$\Delta_n = (a^n)^2 \cdot (b^n)^2 \cdot (a^n + b^n)^2 = (abc)^{2n}.$$

- So the discriminant is $2n$th power of an integer.

# A Special Elliptic Curve

Let $(a, b, c)$ be an integer solution of the equation $x^n + y^n = z^n$ for some prime $n > 2$.

### Definition

Define an elliptic curve $E_n$ by the equation:

$$y^2 = x(x - a^n)(x + b^n).$$

- Discriminant of this curve is:

$$\Delta_n = (a^n)^2 \cdot (b^n)^2 \cdot (a^n + b^n)^2 = (abc)^{2n}.$$

- So the discriminant is $2n$th power of an integer.

# A Special Elliptic Curve

Let $(a, b, c)$ be an integer solution of the equation $x^n + y^n = z^n$ for some prime $n > 2$.

**Definition**

Define an elliptic curve $E_n$ by the equation:

$$y^2 = x(x - a^n)(x + b^n).$$

- Discriminant of this curve is:

$$\Delta_n = (a^n)^2 \cdot (b^n)^2 \cdot (a^n + b^n)^2 = (abc)^{2n}.$$

- So the discriminant is $2n$th power of an integer.

# A Special Elliptic Curve

- So if there is no elliptic curve whose discriminant is a $2n$th power for some prime $n > 2$ then FLT is true.
- Ribet (1988) showed that any elliptic curve of this kind is not modular.
  - Modularity is a property of a function related to a curve.
  - This function is defined over complex numbers.

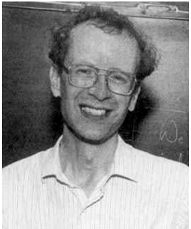
# A Special Elliptic Curve

- So if there is no elliptic curve whose discriminant is a $2n$th power for some prime $n > 2$ then FLT is true.
- Ribet (1988) showed that any elliptic curve of this kind is not modular.
  - Modularity is a property of a function related to a curve.
  - This function is defined over complex numbers.

# A Special Elliptic Curve

- So if there is no elliptic curve whose discriminant is a $2n$th power for some prime $n > 2$ then FLT is true.
- Ribet (1988) showed that any elliptic curve of this kind is not modular.
  - Modularity is a property of a function related to a curve.
  - This function is defined over complex numbers.

# Wiles Theorem



**Theorem (Wiles, 1994)**

*Every elliptic curve is modular.*

# Outline

# Density of Prime Numbers

- Define $\pi(x)$ to be the number of primes less than $x$.
- We wish to obtain an estimate for $\pi(x)$.
- It is easier to count prime numbers with their "weights". Let

$$\psi(x) = \sum_{1 \leq n < x} \Lambda(n)$$

where

$$\Lambda(n) = \begin{cases} \ln p, & \text{if } n = p^k \text{ for some prime } p \\ 0, & \text{otherwise} \end{cases}$$

# Density of Prime Numbers

- Define $\pi(x)$ to be the number of primes less than $x$.
- We wish to obtain an estimate for $\pi(x)$.
- It is easier to count prime numbers with their "weights". Let

$$\psi(x) = \sum_{1 \leq n < x} \Lambda(n)$$

where

$$\Lambda(n) = \begin{cases} \ln p, & \text{if } n = p^k \text{ for some prime } p \\ 0, & \text{otherwise} \end{cases}$$

# Bernhard Riemann (1826 - 1866)

- Riemann was a student of Gauss.
- In 1859, he wrote a paper on estimating $\psi(x)$ which had immense impact on the development of mathematics.

# Estimating $\psi(x)$

- It is generally easier to handle infinite series.
- So we will extend the sum in $\psi(x)$ to an infinite sum.
- Define

$$\delta(x) = \begin{cases} 1, & \text{if } x > 1 \\ 0, & \text{if } 0 < x < 1 \end{cases}$$

- Then we can write

$$\psi(x) = \sum_{n \geq 1} \Lambda(n)\delta(\frac{x}{n})$$

assuming that $x$ is not an integer.

# Estimating $\psi(x)$

- It is generally easier to handle infinite series.
- So we will extend the sum in $\psi(x)$ to an infinite sum.
- Define

$$\delta(x) = \begin{cases} 1, & \text{if } x > 1 \\ 0, & \text{if } 0 < x < 1 \end{cases}$$

- Then we can write

$$\psi(x) = \sum_{n \geq 1} \Lambda(n) \delta(\frac{x}{n})$$

assuming that $x$ is not an integer.

# Estimating $\psi(x)$

- It is generally easier to handle infinite series.
- So we will extend the sum in $\psi(x)$ to an infinite sum.
- Define
$$\delta(x) = \begin{cases} 1, & \text{if } x > 1 \\ 0, & \text{if } 0 < x < 1 \end{cases}$$
- Then we can write
$$\psi(x) = \sum_{n \geq 1} \Lambda(n) \delta\left(\frac{x}{n}\right)$$

  assuming that $x$ is not an integer.

# Defining $\delta$

- It is possible to give a nice definition of $\delta$ over complex plane:

$$\delta(x) = \int_{c-i\infty}^{c+i\infty} \frac{x^s}{s} ds$$

for any $c > 0$.

- This is shown using Cauchy's Theorem which states that

$$\oint_C f(s) ds = 0$$

for any closed contour $C$ in the complex plane, for any differentiable function $f$ that has no poles inside $C$.

# Defining $\delta$

- It is possible to give a nice definition of $\delta$ over complex plane:

$$\delta(x) = \int_{c-i\infty}^{c+i\infty} \frac{x^s}{s} ds$$

  for any $c > 0$.
- This is shown using Cauchy's Theorem which states that

$$\oint_C f(s) ds = 0$$

  for any closed contour $C$ in the complex plane, for any differentiable function $f$ that has no poles inside $C$.

# Approximating $\delta$

- The same approach gives an approximation of $\delta$ too:

$$\delta(x) = \int_{c-iR}^{c+iR} \frac{x^s}{s} ds + O(\frac{x^c}{R|\ln x|})$$

for any $R > 0$, any $c > 0$.

- This approximation will be more useful for us.
- We can write:

$$\begin{aligned} \psi(x) &= \sum_{n \geq 1} \Lambda(n) \delta(\frac{x}{n}) \\ &= \sum_{n \geq 1} \Lambda(n) \int_{c-iR}^{c+iR} \frac{x^s}{xn^s} ds + O(\sum_{n \geq 1} \frac{\Lambda(n) x^c}{Rn^c |\ln \frac{x}{n}|}) \end{aligned}$$

# Approximating $\delta$

- The same approach gives an approximation of $\delta$ too:

$$\delta(x) = \int_{c-iR}^{c+iR} \frac{x^s}{s} ds + O(\frac{x^c}{R|\ln x|})$$

for any $R > 0$, any $c > 0$.

- This approximation will be more useful for us.
- We can write:

$$\begin{aligned}\psi(x) &= \sum_{n\geq 1} \Lambda(n)\delta(\frac{x}{n}) \\ &= \sum_{n\geq 1} \Lambda(n) \int_{c-iR}^{c+iR} \frac{x^s}{xn^s} ds + O(\sum_{n\geq 1} \frac{\Lambda(n)x^c}{Rn^c|\ln \frac{x}{n}|})\end{aligned}$$

# Estimating $\psi$

- Taking the sum inside the integral, we get

$$\begin{aligned}\psi(x) &= \int_{c-iR}^{c+iR} \frac{x^s}{s} \sum_{n \geq 1} \frac{\Lambda(n)}{n^s} ds + O(\sum_{n \geq 1} \frac{\Lambda(n) x^c}{R n^c |\ln \frac{x}{n}|}) \\ &= \int_{c-iR}^{c+iR} \frac{x^s}{s} \sum_{n \geq 1} \frac{\Lambda(n)}{n^s} ds + O(\frac{x \ln^2 x}{R})\end{aligned}$$

for $c = 1 + \frac{1}{\ln x}$.

# The Zeta Function

- Let

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}.$$

- This can be expressed in another way:

$$\begin{aligned} \zeta(s) &= \sum_{n \geq 1} \frac{1}{n^s} \\ &= \prod_{p, p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right) \\ &= \prod_{p, p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}. \end{aligned}$$

# The Zeta Function

- Let
$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}.$$
- This can be expressed in another way:
$$\begin{aligned}\zeta(s) &= \sum_{n \geq 1} \frac{1}{n^s} \\ &= \prod_{p, p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right) \\ &= \prod_{p, p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}.\end{aligned}$$

# The Zeta Function

- Taking log, we get:

$$\ln \zeta(s) = -\sum_{p, p \text{ prime}} \ln(1 - \frac{1}{p^s}).$$

- Differentiating with respect to $s$, we get:

$$\begin{aligned}
\frac{\zeta'(s)}{\zeta(s)} &= -\sum_{p, p \text{ prime}} \frac{(\ln p)p^{-s}}{1 - \frac{1}{p^s}} \\
&= -\sum_{p, p \text{ prime}} (\ln p)p^{-s}(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots) \\
&= -\sum_{p, p \text{ prime}} \sum_{k \geq 1} \frac{\ln p}{p^{ks}} \\
&= -\sum_{n \geq 1} \frac{\Lambda(n)}{n^s}.
\end{aligned}$$

# The Zeta Function

- Taking log, we get:

$$\ln \zeta(s) = - \sum_{p, p \text{ prime}} \ln(1 - \frac{1}{p^s}).$$

- Differentiating with respect to $s$, we get:

$$\begin{aligned}
\frac{\zeta'(s)}{\zeta(s)} &= - \sum_{p, p \text{ prime}} \frac{(\ln p) p^{-s}}{1 - \frac{1}{p^s}} \\
&= - \sum_{p, p \text{ prime}} (\ln p) p^{-s} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots) \\
&= - \sum_{p, p \text{ prime}} \sum_{k \geq 1} \frac{\ln p}{p^{ks}} \\
&= - \sum_{n \geq 1} \frac{\Lambda(n)}{n^s}.
\end{aligned}$$

# Estimating $\psi$

- Substituting in the expression for $\psi$, we get:

$$\psi(x) = -\int_{c-iR}^{c+iR} \frac{x^s}{s}\frac{\zeta'(s)}{\zeta(s)} ds + O(\frac{x \ln^2 x}{R})$$

  for $c = 1 + \frac{1}{\ln x}$.

- So if we can estimate the integral

$$I(x, R) = -\int_{c-iR}^{c+iR} \frac{x^s}{s}\frac{\zeta'(s)}{\zeta(s)} ds$$

  well, we will have an expression for $\psi(x)$.

# Estimating $\psi$

- Substituting in the expression for $\psi$, we get:

$$\psi(x) = -\int_{c-iR}^{c+iR} \frac{x^s}{s}\frac{\zeta'(s)}{\zeta(s)}ds + O(\frac{x\ln^2 x}{R})$$

  for $c = 1 + \frac{1}{\ln x}$.
- So if we can estimate the integral

$$I(x,R) = -\int_{c-iR}^{c+iR} \frac{x^s}{s}\frac{\zeta'(s)}{\zeta(s)}ds$$

  well, we will have an expression for $\psi(x)$.

# Estimating $I(x, R)$

- We again use Cauchy's Theorem.
- Define the contour $C$ to be $c - iR \mapsto c + iR \mapsto -U + iR \mapsto -U - iR \mapsto c - iR$.
- However, we need to extend the definition of $\zeta(s)$ to the entire region as the definition $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ diverges for $\Re(s) \leq 1$!
- Fortunately, this can be done using some tricks.
- Unfortunately, the function

$$\frac{x^s}{s} \frac{\zeta'(s)}{\zeta(s)}$$

  with the extended definition has many poles inside $C$!
- Some of the poles are at $s = 0, 1$, $s = -2m$ for every positive integer $m$.
- In addition to these, there are infinitely many poles within the strip $0 \leq \Re(s) \leq 1$!!

# ESTIMATING $I(x, R)$

- We again use Cauchy's Theorem.
- Define the contour $C$ to be
  $c - iR \mapsto c + iR \mapsto -U + iR \mapsto -U - iR \mapsto c - iR$.
- However, we need to extend the definition of $\zeta(s)$ to the entire region as the definition $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ diverges for $\Re(s) \leq 1$!
- Fortunately, this can be done using some tricks.
- Unfortunately, the function

$$\frac{x^s}{s} \frac{\zeta'(s)}{\zeta(s)}$$

  with the extended definition has many poles inside $C$!
- Some of the poles are at $s = 0, 1$, $s = -2m$ for every positive integer $m$.
- In addition to these, there are infinitely many poles within the strip $0 \leq \Re(s) \leq 1$!!

# ESTIMATING $I(x, R)$

- We again use Cauchy's Theorem.
- Define the contour $C$ to be
  $c - iR \mapsto c + iR \mapsto -U + iR \mapsto -U - iR \mapsto c - iR$.
- However, we need to extend the definition of $\zeta(s)$ to the entire region as the definition $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ diverges for $\Re(s) \leq 1$!
- Fortunately, this can be done using some tricks.
- Unfortunately, the function

$$\frac{x^s}{s} \frac{\zeta'(s)}{\zeta(s)}$$

  with the extended definition has many poles inside $C$!
- Some of the poles are at $s = 0, 1$, $s = -2m$ for every positive integer $m$.
- In addition to these, there are infinitely many poles within the strip $0 \leq \Re(s) \leq 1$!!

# Estimating $I(x, R)$

- We again use Cauchy's Theorem.
- Define the contour $C$ to be $c - iR \mapsto c + iR \mapsto -U + iR \mapsto -U - iR \mapsto c - iR$.
- However, we need to extend the definition of $\zeta(s)$ to the entire region as the definition $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ diverges for $\Re(s) \leq 1$!
- Fortunately, this can be done using some tricks.
- Unfortunately, the function

$$\frac{x^s}{s} \frac{\zeta'(s)}{\zeta(s)}$$

  with the extended definition has many poles inside $C$!
- Some of the poles are at $s = 0, 1$, $s = -2m$ for every positive integer $m$.
- In addition to these, there are infinitely many poles within the strip $0 \leq \Re(s) \leq 1$!!

# Handling Poles

- A generalized version of Cauchy's Theorem states that the value of contour integral equals the sum of residues of poles inside the contour.
- We find that the residue of $\frac{\zeta'(s)}{\zeta(s)}$ at $s = 1$ is $-1$, and at all other poles is $1$.
- The residue of $\frac{x^s}{s}$ at $s = 0$ is $1$.
- Hence,

$$-\oint_C \frac{x^s}{s}\frac{\zeta'(s)}{\zeta(s)} ds = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + \sum_{0 < 2m < U} \frac{x^{-2m}}{2m} - \frac{\zeta'(0)}{\zeta(0)}.$$

# Handling Poles

- A generalized version of Cauchy's Theorem states that the value of contour integral equals the sum of residues of poles inside the contour.
- We find that the residue of $\frac{\zeta'(s)}{\zeta(s)}$ at $s = 1$ is $-1$, and at all other poles is $1$.
- The residue of $\frac{x^s}{s}$ at $s = 0$ is $1$.
- Hence,

$$-\oint_C \frac{x^s}{s}\frac{\zeta'(s)}{\zeta(s)} ds = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + \sum_{0 < 2m < U} \frac{x^{-2m}}{2m} - \frac{\zeta'(0)}{\zeta(0)}.$$

# Handling Poles

- A generalized version of Cauchy's Theorem states that the value of contour integral equals the sum of residues of poles inside the contour.
- We find that the residue of $\frac{\zeta'(s)}{\zeta(s)}$ at $s = 1$ is $-1$, and at all other poles is $1$.
- The residue of $\frac{x^s}{s}$ at $s = 0$ is $1$.
- Hence,

$$- \oint_C \frac{x^s}{s} \frac{\zeta'(s)}{\zeta(s)} ds = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + \sum_{0 < 2m < U} \frac{x^{-2m}}{2m} - \frac{\zeta'(0)}{\zeta(0)}.$$

# Estimating $I(x, R)$

- A careful analysis of the extended definition of $\zeta(s)$ shows that we can choose large $U$ and $R$ such that

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| = O(\ln^2 |s|).$$

- Using this, it is straightforward to show that the integrals from $c + iR$ to $-U + iR$ and $-U - iR$ to $c - iR$ are bounded by $O(\frac{x \ln^2 R}{R \ln x})$.
- Similarly, the integral from $-U + iR$ to $-U - iR$ is bounded by $O(\frac{R \ln U}{U x^R})$.
- Taking limit $U \mapsto \infty$, we get:

$$I(x, R) = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + \sum_{2m > 0} \frac{x^{-2m}}{2m} + O\left(\frac{x \ln^2 R}{R \ln x}\right).$$

# Estimating $I(x, R)$

- A careful analysis of the extended definition of $\zeta(s)$ shows that we can choose large $U$ and $R$ such that

$$|\frac{\zeta'(s)}{\zeta(s)}| = O(\ln^2 |s|).$$

- Using this, it is straightforward to show that the integrals from $c + iR$ to $-U + iR$ and $-U - iR$ to $c - iR$ are bounded by $O(\frac{x \ln^2 R}{R \ln x})$.
- Similarly, the integral from $-U + iR$ to $-U - iR$ is bounded by $O(\frac{R \ln U}{U x^R})$.
- Taking limit $U \mapsto \infty$, we get:

$$I(x, R) = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + \sum_{2m > 0} \frac{x^{-2m}}{2m} + O(\frac{x \ln^2 R}{R \ln x}).$$

# Estimating $I(x, R)$

- A careful analysis of the extended definition of $\zeta(s)$ shows that we can choose large $U$ and $R$ such that

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| = O(\ln^2 |s|).$$

- Using this, it is straightforward to show that the integrals from $c + iR$ to $-U + iR$ and $-U - iR$ to $c - iR$ are bounded by $O(\frac{x \ln^2 R}{R \ln x})$.
- Similarly, the integral from $-U + iR$ to $-U - iR$ is bounded by $O(\frac{R \ln U}{U x^R})$.
- Taking limit $U \mapsto \infty$, we get:

$$I(x, R) = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + \sum_{2m > 0} \frac{x^{-2m}}{2m} + O(\frac{x \ln^2 R}{R \ln x}).$$

# ESTIMATING $I(x, R)$

- A careful analysis of the extended definition of $\zeta(s)$ shows that we can choose large $U$ and $R$ such that

$$|\frac{\zeta'(s)}{\zeta(s)}| = O(\ln^2 |s|).$$

- Using this, it is straightforward to show that the integrals from $c + iR$ to $-U + iR$ and $-U - iR$ to $c - iR$ are bounded by $O(\frac{x \ln^2 R}{R \ln x})$.
- Similarly, the integral from $-U + iR$ to $-U - iR$ is bounded by $O(\frac{R \ln U}{U x^R})$.
- Taking limit $U \mapsto \infty$, we get:

$$I(x, R) = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + \sum_{2m>0} \frac{x^{-2m}}{2m} + O(\frac{x \ln^2 R}{R \ln x}).$$

# Estimating $\psi(x)$

- Thus we get:

$$\psi(x) = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + \sum_{2m>0} \frac{x^{-2m}}{2m} + O(\frac{x \ln^2 R}{R \ln x}) + O(\frac{x \ln^2 x}{R}).$$

- Notice that

$$\sum_{2m>0} \frac{x^{-2m}}{2m} = \ln(1 - \frac{1}{x^2})$$

which is close to zero for large $x$.

- Hence

$$\psi(x) = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + O(\frac{x \ln^2 R}{R \ln x}) + O(\frac{x \ln^2 x}{R}).$$

# Estimating $\psi(x)$

- Thus we get:

$$\psi(x) = x - \sum_{-R \le \Im(\rho) \le R} \frac{x^\rho}{\rho} + \sum_{2m>0} \frac{x^{-2m}}{2m} + O(\frac{x \ln^2 R}{R \ln x}) + O(\frac{x \ln^2 x}{R}).$$

- Notice that

$$\sum_{2m>0} \frac{x^{-2m}}{2m} = \ln(1 - \frac{1}{x^2})$$

which is close to zero for large $x$.

- Hence

$$\psi(x) = x - \sum_{-R \le \Im(\rho) \le R} \frac{x^\rho}{\rho} + O(\frac{x \ln^2 R}{R \ln x}) + O(\frac{x \ln^2 x}{R}).$$

# Estimating $\psi(x)$

- Thus we get:

$$\psi(x) = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + \sum_{2m>0} \frac{x^{-2m}}{2m} + O(\frac{x \ln^2 R}{R \ln x}) + O(\frac{x \ln^2 x}{R}).$$

- Notice that

$$\sum_{2m>0} \frac{x^{-2m}}{2m} = \ln(1 - \frac{1}{x^2})$$

  which is close to zero for large $x$.

- Hence

$$\psi(x) = x - \sum_{-R \leq \Im(\rho) \leq R} \frac{x^\rho}{\rho} + O(\frac{x \ln^2 R}{R \ln x}) + O(\frac{x \ln^2 x}{R}).$$

# The Riemann Hypothesis

## Riemann Hypothesis

All the zeroes of $\zeta(s)$ in $0 \leq \Re(s) \leq 1$ lie at the line $\Re(s) = \frac{1}{2}$.

- Note that the zeroes of $\zeta(s)$ become poles of $-\frac{\zeta'(s)}{\zeta(s)}$!
- Further, the poles of $-\frac{\zeta'(s)}{\zeta(s)}$ in the strip $0 \leq \Re(s) \leq 1$ are precisely the zeroes of $\zeta(s)$ there except for the pole at $s = 1$.

# The Riemann Hypothesis

## Riemann Hypothesis

All the zeroes of $\zeta(s)$ in $0 \leq \Re(s) \leq 1$ lie at the line $\Re(s) = \frac{1}{2}$.

- Note that the zeroes of $\zeta(s)$ become poles of $-\frac{\zeta'(s)}{\zeta(s)}$!
- Further, the poles of $-\frac{\zeta'(s)}{\zeta(s)}$ in the strip $0 \leq \Re(s) \leq 1$ are precisely the zeroes of $\zeta(s)$ there except for the pole at $s = 1$.

# Using Riemann Hypothesis

- If the Hypothesis is true, then $|\frac{x^\rho}{\rho}| = \frac{x^{1/2}}{|\rho|}$.
- Applying this and simplifying, we get:

$$\psi(x) = x + O(x^{1/2}\ln^2 R) + O(\frac{x\ln^2 R}{R\ln x}) + O(\frac{x\ln^2 x}{R}).$$

- Now set $R = x^{1/2}$ and we get:

$$\psi(x) = x + O(x^{1/2}\ln^2 x).$$

# Using Riemann Hypothesis

- If the Hypothesis is true, then $|\frac{x^\rho}{\rho}| = \frac{x^{1/2}}{|\rho|}$.
- Applying this and simplifying, we get:

$$\psi(x) = x + O(x^{1/2}\ln^2 R) + O(\frac{x\ln^2 R}{R\ln x}) + O(\frac{x\ln^2 x}{R}).$$

- Now set $R = x^{1/2}$ and we get:

$$\psi(x) = x + O(x^{1/2}\ln^2 x).$$

# Using Riemann Hypothesis

- If the Hypothesis is true, then $|\frac{x^\rho}{\rho}| = \frac{x^{1/2}}{|\rho|}$.
- Applying this and simplifying, we get:

$$\psi(x) = x + O(x^{1/2}\ln^2 R) + O(\frac{x\ln^2 R}{R\ln x}) + O(\frac{x\ln^2 x}{R}).$$

- Now set $R = x^{1/2}$ and we get:

$$\psi(x) = x + O(x^{1/2}\ln^2 x).$$

# The Prime Number theorem

- Hadamard (1896) and Vallee Poussin (1896) showed that no zero of $\zeta(s)$ lies on $\Re(s) = 1$.
- Using this, they showed that

$$\psi(x) = x + o(x)$$

or, equivalently

$$\lim_{x \mapsto \infty} \pi(x) \mapsto \frac{x}{\ln x}.$$

- This is the famous Prime Number Theorem.

# The Prime Number theorem

- Hadamard (1896) and Vallee Poussin (1896) showed that no zero of $\zeta(s)$ lies on $\Re(s) = 1$.
- Using this, they showed that

$$\psi(x) = x + o(x)$$

or, equivalently

$$\lim_{x \mapsto \infty} \pi(x) \mapsto \frac{x}{\ln x}.$$

- This is the famous Prime Number Theorem.

# How About Riemann Hypothesis?

- Despite attempts for last 150 years, it remains unproven.
- It is widely considered to be the most important unsolved problem of mathematics.
- There is a $1 million prize on the proof of the hypothesis!

# How About Riemann Hypothesis?

- Despite attempts for last 150 years, it remains unproven.
- It is widely considered to be the most important unsolved problem of mathematics.
- There is a $1 million prize on the proof of the hypothesis!

# How About Riemann Hypothesis?

- Despite attempts for last 150 years, it remains unproven.
- It is widely considered to be the most important unsolved problem of mathematics.
- There is a $1 million prize on the proof of the hypothesis!

# Unsolved Problems in Number Theory

- A large number of problems in Number Theory remain unsolved:

  Goldbach's Conjecture: Every even integer $> 2$ is a sum of two prime numbers.

  Twin Prime Conjecture: There exist infinitely many prime pairs of the form $(p, p+2)$.

  Prime Gaps: For every $n$, there exits a prime number between $n$ and $n + \ln^2 n$.

# Unsolved Problems in Number Theory

- A large number of problems in Number Theory remain unsolved:

  Goldbach's Conjecture: Every even integer $> 2$ is a sum of two prime numbers.

  Twin Prime Conjecture: There exist infinitely many prime pairs of the form $(p, p+2)$.

  Prime Gaps: For every $n$, there exits a prime number between $n$ and $n + \ln^2 n$.

# Unsolved Problems in Number Theory

- A large number of problems in Number Theory remain unsolved:

  Goldbach's Conjecture: Every even integer $> 2$ is a sum of two prime numbers.

  Twin Prime Conjecture: There exist infinitely many prime pairs of the form $(p, p+2)$.

  Prime Gaps: For every $n$, there exits a prime number between $n$ and $n + \ln^2 n$.

# Unsolved Problems in Number Theory

- A large number of problems in Number Theory remain unsolved:

  Goldbach's Conjecture: Every even integer $> 2$ is a sum of two prime numbers.

  Twin Prime Conjecture: There exist infinitely many prime pairs of the form $(p, p+2)$.

  Prime Gaps: For every $n$, there exits a prime number between $n$ and $n + \ln^2 n$.