Fermat’s Last Theorem: From Integers to Elliptic Curves

Manindra Agarwal

IIT Kanpur

December 2005
Fermat’s Last Theorem

Theorem

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

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

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

I have discovered a truly 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.
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 $n \leq 100$. 
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.
When \( n = 2 \)

- The equation is \( x^2 + y^2 = z^2 \).
- The solutions to this equation are Pythagorean triples.
- The smallest one is \( x = 3, y = 4 \) and \( z = 5 \).

The general solution is given by \( x = 2ab, y = a^2 - b^2, z = a^2 + b^2 \) for integers \( a > b > 0 \).
When $n = 2$

- The equation is $x^2 + y^2 = z^2$.
- The solutions to this equation are Pythagorean triples.
- The smallest one is $x = 3$, $y = 4$ and $z = 5$.

The general solution is given by $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$ for integers $a > b > 0$. 
When \( n = 2 \)

- The equation is \( x^2 + y^2 = z^2 \).
- The solutions to this equation are \textit{Pythagorian triples}.
- The smallest one is \( x = 3, y = 4 \) and \( z = 5 \).

The general solution is given by \( x = 2ab, y = a^2 - b^2, z = a^2 + b^2 \) for integers \( a > b > 0 \).
**When \( n = 4 \)**

- Suppose \( u^4 + v^4 = w^4 \) for some relatively prime integers \( u, v, w \).
- So we must have coprime integers \( a \) and \( b \) such that \( u^2 = 2ab \), \( v^2 = a^2 - b^2 \) and \( w^2 = a^2 + b^2 \).
- Since \( a, b \) are coprime, there exist coprime integers \( \alpha \) and \( \beta \) such that \( u = \alpha \beta \) and
  \[
  2a = \alpha^2, \quad b = \beta^2 \quad \text{or} \quad a = \alpha^2, \quad 2b = \beta^2.
  \]
- Similarly, there exist coprime integers \( \gamma \) and \( \delta \) such that \( v = \gamma \delta \) and
  \[
  a - b = \gamma^2, \quad a + b = \delta^2.
  \]
When $n = 4$

- Suppose $u^4 + v^4 = w^4$ for some relatively prime integers $u$, $v$, $w$.
- So we must have coprime integers $a$ and $b$ such that $u^2 = 2ab$, $v^2 = a^2 - b^2$ and $w^2 = a^2 + b^2$.
- Since $a$, $b$ are coprime, there exist coprime integers $\alpha$ and $\beta$ such that $u = \alpha \beta$ and

\[
2a = \alpha^2, \quad b = \beta^2 \quad \text{or} \quad a = \alpha^2, \quad 2b = \beta^2.
\]

- Similarly, there exist coprime integers $\gamma$ and $\delta$ such that $v = \gamma \delta$ and

\[
a - b = \gamma^2, \quad a + b = \delta^2.
\]
When $n = 4$

- Suppose $u^4 + v^4 = w^4$ for some relatively prime integers $u, v, w$.
- So we must have coprime integers $a$ and $b$ such that $u^2 = 2ab$, $v^2 = a^2 - b^2$ and $w^2 = a^2 + b^2$.
- Since $a, b$ are coprime, there exist coprime integers $\alpha$ and $\beta$ such that $u = \alpha \beta$ and
  \[2a = \alpha^2, \quad b = \beta^2 \quad \text{or} \quad a = \alpha^2, \quad 2b = \beta^2.\]
- Similarly, there exist coprime integers $\gamma$ and $\delta$ such that $v = \gamma \delta$ and
  \[a - b = \gamma^2, \quad a + b = \delta^2.\]
When \( n = 4 \)

- Suppose the first case: \( 2a = \alpha^2 \).
- Then,

\[
\gamma^2 + \delta^2 = (a - b) + (a + b) = 2a = \alpha^2.
\]

- In addition, 2 divides \( \alpha \) and \( \alpha, \gamma, \delta \) are coprime to each other.
- So both \( \gamma \) and \( \delta \) are odd numbers.
- Let \( \gamma = 2k + 1 \) and \( \delta = 2\ell + 1 \) and consider the equation modulo 4:

\[
0 = \alpha^2 \pmod{4} = (2k + 1)^2 + (2\ell + 1)^2 \pmod{4} = 2 \pmod{4}.
\]

- This is impossible.
- The second case can be handled similarly, using infinite descent method. [Try it!]

**Manindra Agarwal (IIT Kanpur)**
**Fermat's Last Theorem**
December 2005
When $n = 4$

- Suppose the first case: $2a = \alpha^2$.
- Then,

\[
\gamma^2 + \delta^2 = (a - b) + (a + b) = 2a = \alpha^2.
\]

- In addition, 2 divides $\alpha$ and $\alpha$, $\gamma$, $\delta$ are coprime to each other.
- So both $\gamma$ and $\delta$ are odd numbers.
  - Let $\gamma = 2k + 1$ and $\delta = 2\ell + 1$ and consider the equation modulo 4:

\[
0 = \alpha^2 \pmod{4} = (2k + 1)^2 + (2\ell + 1)^2 \pmod{4} = 2 \pmod{4}.
\]

- This is impossible.
- The second case can be handled similarly, using infinite descent method. [Try it!]

Manindra Agarwal (IIT Kanpur)  Fermat's Last Theorem  December 2005 8 / 30
When \( n = 4 \)

- Suppose the first case: \( 2a = \alpha^2 \).
- Then,

\[
\gamma^2 + \delta^2 = (a - b) + (a + b) = 2a = \alpha^2.
\]

- In addition, \( 2 \) divides \( \alpha \) and \( \alpha, \gamma, \delta \) are coprime to each other.
- So both \( \gamma \) and \( \delta \) are odd numbers.
- Let \( \gamma = 2k + 1 \) and \( \delta = 2\ell + 1 \) and consider the equation modulo 4:

\[
0 = \alpha^2 \pmod{4} = (2k + 1)^2 + (2\ell + 1)^2 \pmod{4} = 2 \pmod{4}.
\]

- This is impossible.
- The second case can be handled similarly, using infinite descent method. [Try it!]
When \( n = 4 \)

- Suppose the first case: \( 2a = \alpha^2 \).
- Then,

\[
\gamma^2 + \delta^2 = (a - b) + (a + b) = 2a = \alpha^2.
\]

- In addition, \( 2 \) divides \( \alpha \) and \( \alpha, \gamma, \delta \) are coprime to each other.
- So both \( \gamma \) and \( \delta \) are odd numbers.
- Let \( \gamma = 2k + 1 \) and \( \delta = 2\ell + 1 \) and consider the equation modulo 4:

\[
0 = \alpha^2 \pmod{4} = (2k + 1)^2 + (2\ell + 1)^2 \pmod{4} = 2 \pmod{4}.
\]

- This is impossible.
- The second case can be handled similarly, using infinite descent method. [Try it!]
A More General Approach

- Approach for $n = 4$ does not generalize.
- Different approaches can be used to prove $n = 3, 5, \ldots$ cases.
- However, none of these approaches generalized.
- A different idea was needed to make it work for all $n$.
- This came in the form of rational points on curves.
A More General Approach

- Approach for $n = 4$ does not generalize.
- Different approaches can be used to prove $n = 3, 5, \ldots$ cases.
- However, none of these approaches generalized.
- A different idea was needed to make it work for all $n$.
- This came in the form of rational points on curves.
A More General Approach

- Approach for \( n = 4 \) does not generalize.
- Different approaches can be used to prove \( n = 3, 5, \ldots \) cases.
- However, none of these approaches generalized.
- A different idea was needed to make it work for all \( n \).
- This came in the form of rational points on curves.
Rational Points on Curves

- Let \( f(x, y) = 0 \) be a curve of degree \( n \) with rational coefficients.
- We wish to know how many rational points lie on this curve.
- Consider the curve \( F_n(x, y) = x^n + y^n - 1 = 0 \).
- Let \( F_n(\alpha, \beta) = 0 \) where \( \alpha = \frac{a}{c} \) and \( \beta = \frac{b}{c} \) are rational numbers.
- Then, \( a^n + b^n = c^n \) giving an integer solution to Fermat’s equation.
- Conversely, any integer solution to Fermat’s equation yields a rational point on the curve \( F_n(x, y) = 0 \).
Let $f(x, y) = 0$ be a curve of degree $n$ with rational coefficients.

We wish to know how many rational points lie on this curve.

Consider the curve $F_n(x, y) = x^n + y^n - 1 = 0$.

Let $F_n(\alpha, \beta) = 0$ where $\alpha = \frac{a}{c}$ and $\beta = \frac{b}{c}$ are rational numbers.

Then, $a^n + b^n = c^n$ giving an integer solution to Fermat’s equation.

Conversely, any integer solution to Fermat’s equation yields a rational point on the curve $F_n(x, y) = 0$. 
Let $f(x, y) = 0$ be a curve of degree $n$ with rational coefficients.

We wish to know how many rational points lie on this curve.

Consider the curve $F_n(x, y) = x^n + y^n - 1 = 0$.

Let $F_n(\alpha, \beta) = 0$ where $\alpha = \frac{a}{c}$ and $\beta = \frac{b}{c}$ are rational numbers.

Then, $a^n + b^n = c^n$ giving an integer solution to Fermat’s equation.

Conversely, any integer solution to Fermat’s equation yields a rational point on the curve $F_n(x, y) = 0$.  

Faltings Theorem

**Theorem (Faltings)**

For any curve except for lines, conic sections, and elliptic curves, the number of rational points on the curve is finite.

- This implies that the equation $x^n + y^n = z^n$ will have at most finitely many solutions for any $n > 4$ (equations for $n = 3, 4$ can be transformed to elliptic curves).
- Not strong enough!
Theorem (Faltings)

For any curve except for lines, conic sections, and elliptic curves, the number of rational points on the curve is finite.

- This implies that the equation \( x^n + y^n = z^n \) will have at most finitely many solutions for any \( n > 4 \) (equations for \( n = 3, 4 \) can be transformed to elliptic curves).
- Not strong enough!
A Different Approach

- One idea is to transform the curves $x^n + y^n = 1$ to a family of curves that have no rational points on it.
- The eventual solution came by a similar approach – the problem was transformed to a problem on elliptic curves.
- Interestingly, elliptic curves can have infinitely many rational points!
One idea is to transform the curves $x^n + y^n = 1$ to a family of curves that have no rational points on it.

The eventual solution came by a similar approach – the problem was transformed to a problem on elliptic curves.

Interestingly, elliptic curves can have infinitely many rational points!
A Different Approach

- One idea is to transform the curves $x^n + y^n = 1$ to a family of curves that have no rational points on it.
- The eventual solution came by a similar approach – the problem was transformed to a problem on elliptic curves.
- Interestingly, elliptic curves can have infinitely many rational points!
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.
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. \([\text{Verify!}]\)
- If \( x^3 + Ax + B = (x - \alpha)(x - \beta)(x - \gamma) \) then
  \[
  \Delta = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.
  \]
A Special Elliptic Curve

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

**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.
- We aim to show that no elliptic curve exists whose discriminant is a 6th or higher power.
Let \((a, b, c)\) be a solution of the equation \(x^n + y^n = z^n\) for some \(n > 2\).

**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.
- We aim to show that no elliptic curve exists whose discriminant is a 6th or higher power.
A Special Elliptic Curve

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

**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.
- We aim to show that no elliptic curve exists whose discriminant is a 6th or higher power.
A Special Elliptic Curve

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

**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.

- We aim to show that no elliptic curve exists whose discriminant is a 6th or higher power.
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.
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 $E$

$P + Q = R$

$(x, y)$

$R = (x, -y)$
**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 $E$

$(1,0) + (1,0) = O$
The nice additive structure of rational points in $E(\mathbb{Q})$ allows us to “count” them.

For each prime $p$, define $E(F_p)$ to be the set of points $(u, v)$ such that $0 \leq u, v < p$ and

$$v^2 = u^3 + Au + B \pmod{p}.$$ 

A point in $E(\mathbb{Q})$ yields a point in $E(F_p)$.

The set $E(F_p)$ is clearly finite: $|E(F_p)| \leq p^2$. 
The nice additive structure of rational points in $E(\mathbb{Q})$ allows us to “count” them.

For each prime $p$, define $E(F_p)$ to be the set of points $(u, v)$ such that $0 \leq u, v < p$ and

$$v^2 = u^3 + Au + B \pmod{p}.$$ 

A point in $E(\mathbb{Q})$ yields a point in $E(F_p)$.

The set $E(F_p)$ is clearly finite: $|E(F_p)| \leq p^2$. 


The nice additive structure of rational points in $E(\mathbb{Q})$ allows us to “count” them.

For each prime $p$, define $E(F_p)$ to be the set of points $(u, v)$ such that $0 \leq u, v < p$ and

$$v^2 = u^3 + Au + B \pmod{p}.$$ 

A point in $E(\mathbb{Q})$ yields a point in $E(F_p)$.

The set $E(F_p)$ is clearly finite: $|E(F_p)| \leq p^2$. 
Hasse’s Theorem

**Theorem (Hasse)**

\[ p + 1 - 2\sqrt{p} \leq |E(F_p)| \leq p + 1 + 2\sqrt{p}. \]

- Let \( a_p = p + 1 - |E(F_p)| \), \( a_p \) measures the difference from the mean value.
- Thus we get an infinite sequence of numbers \( a_2, a_3, a_5, a_7, a_{11}, \ldots \), one for each prime.
Hasse’s Theorem

Theorem (Hasse)

\[ p + 1 - 2\sqrt{p} \leq |E(F_p)| \leq p + 1 + 2\sqrt{p}. \]

- Let \( a_p = p + 1 - |E(F_p)| \), \( a_p \) measures the difference from the mean value.
- Thus we get an infinite sequence of numbers \( a_2, a_3, a_5, a_7, a_{11}, \ldots \), one for each prime.
Generating Function for Rational Points

- For the sake of completeness, we define $a$'s for non-prime indices too:

$$a_n = \prod_{i=1}^{k} a_{p_i^{e_i}},$$

where $n = \prod_{i=1}^{k} p_i^{e_i}$.

- Numbers $a_{p_i^{e_i}}$ are defined from $a_p$ using certain symmetry considerations, e.g., $a_{p^2} = a_p^2 - p$.

- We can now define a generating function for this sequence:

$$G_E(z) = \sum_{n>0} a_n \cdot z^n.$$

- By studying properties of $G_E(z)$, we hope to infer properties of curve $E$. 

Manindra Agarwal (IIT Kanpur)  Fermat's Last Theorem  December 2005  23 / 30
Generating Function for Rational Points

- For the sake of completeness, we define $a$'s for non-prime indices too:

\[ a_n = \prod_{i=1}^{k} a_{p_i^{e_i}}, \]

where $n = \prod_{i=1}^{k} p_i^{e_i}$.

- Numbers $a_{p_i^{e_i}}$ are defined from $a_p$ using certain symmetry considerations, e.g., $a_{p^2} = a_p^2 - p$.

- We can now define a generating function for this sequence:

\[ G_E(z) = \sum_{n>0} a_n \cdot z^n. \]

- By studying properties of $G_E(z)$, we hope to infer properties of curve $E$. 

Manindra Agarwal  (IIT Kanpur)  
Fermat’s Last Theorem  
December 2005  
23 / 30
For the sake of completeness, we define $a$’s for non-prime indices too:

$$a_n = \prod_{i=1}^{k} a_{p_i^e}^i,$$

where $n = \prod_{i=1}^{k} p_i^{e_i}$.

Numbers $a_{p_i^e}$ are defined from $a_p$ using certain symmetry considerations, e.g., $a_{p^2} = a_p^2 - p$.

We can now define a generating function for this sequence:

$$G_E(z) = \sum_{n>0} a_n \cdot z^n.$$

By studying properties of $G_E(z)$, we hope to infer properties of curve $E$. 

---

**Generating Function for Rational Points**
Generating Function for Rational Points

- For the sake of completeness, we define $a$’s for non-prime indices too:

$$a_n = \prod_{i=1}^{k} a_{p_i^{e_i}},$$

where $n = \prod_{i=1}^{k} p_i^{e_i}$.

- Numbers $a_{p_i^{e_i}}$ are defined from $a_p$ using certain symmetry considerations, e.g., $a_{p^2} = a_p^2 - p$.

- We can now define a generating function for this sequence:

$$G_E(z) = \sum_{n>0} a_n \cdot z^n.$$ 

- By studying properties of $G_E(z)$, we hope to infer properties of curve $E$. 
**Definition**

A function $f$, defined over complex numbers, is modular of level $\ell$ and conductance $N$ if for every $2 \times 2$ matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that all its entries are integers, $\det M = 1$ and $N$ divides $c$,

$$f\left(\frac{ay + b}{cy + d}\right) = (cy + d)^\ell \cdot f(y)$$

for all complex numbers $y$ with $\Im(y) > 0$. 
Some Properties of Modular Functions

Choose $M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then:

$$f(y + 1) = f(y).$$

Thus, $f$ is periodic.

Choose $M = \begin{bmatrix} 1 & 0 \\ kN & 1 \end{bmatrix}$. Then:

$$f\left(\frac{y}{kNy + 1}\right) = (kNy + 1)^\ell \cdot f(y).$$

So $f(y) \rightarrow \infty$ as $|y| \rightarrow 0$. 
Some Properties of Modular Functions

Choose $M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then:

$$f(y + 1) = f(y).$$

Thus, $f$ is periodic.

Choose $M = \begin{bmatrix} 1 \\ kN \\ 0 \\ 1 \end{bmatrix}$. Then:

$$f\left(\frac{y}{kNy + 1}\right) = (kNy + 1)^{\ell} \cdot f(y).$$

So $f(y) \to \infty$ as $|y| \to 0$. 
Generating Functions for $E_n$ are Not Modular

- Define a special generating function derived from $G_E(z)$:

$$SG_E(y) = G_E(e^{2\pi iy}) = \sum_{n>0} a_n \cdot e^{2\pi iy}.$$ 

- Recall that curve $E_n$ was defined by a solution of Fermat’s equation:

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

**Theorem (Ribet)**

Functions $SG_{E_n}$ are not modular for $n > 2$. 
Generating Functions for $E_n$ are Not Modular

- Define a special generating function derived from $G_E(z)$:

$$SG_E(y) = G_E(e^{2\pi iy}) = \sum_{n>0} a_n \cdot e^{2\pi iy}.$$ 

- Recall that curve $E_n$ was defined by a solution of Fermat’s equation:

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

Theorem (Ribet)

Functions $SG_{E_n}$ are not modular for $n > 2$. 
Generating Functions for $E_n$ are Not Modular

- Define a special generating function derived from $G_E(z)$:
  \[
  SG_E(y) = G_E(e^{2\pi i y}) = \sum_{n>0} a_n \cdot e^{2\pi i y}.
  \]

- Recall that curve $E_n$ was defined by a solution of Fermat’s equation:
  \[
  y^2 = x(x - a^n)(x + b^n).
  \]

**Theorem (Ribet)**

Functions $SG_{E_n}$ are not modular for $n > 2$. 
**Theorem (Wiles)**

*Function* $SG_E$ *for any elliptic curve is modular.*
In mathematics, answers to problems are often found in unexpected ways.

Elliptic curves have found applications in a number of places:
- In factoring integers.
- In designing cryptosystems.
In mathematics, answers to problems are often found in unexpected ways.

Elliptic curves have found applications in a number of places:
- In factoring integers.
- In designing cryptosystems.
Remarks

- In mathematics, answers to problems are often found in unexpected ways.
- Elliptic curves have found applications in a number of places:
  - In factoring integers.
  - In designing cryptosystems.
In mathematics, answers to problems are often found in unexpected ways.

Elliptic curves have found applications in a number of places:

- In factoring integers.
- In designing cryptosystems.
A Fun Problem

Manindra Agarwal (IIT Kanpur)

Fermat's Last Theorem

December 2005 29 / 30
A Fun Problem
A Fun Problem
A Fun Problem

Find a non-trivial value of $n \ (n \neq 0, 1)$ for which the number of balls needed is a perfect square.