On The Fermat's Last Theorem Modulo a Prime

Rajiv Mishra

Graduate Student Seminar

Department of Mathematics and Statistics
Indian Institute of Science Education and Research, Kolkata

August 22, 2022

Background

Around 1637, Fermat wrote his "Last Theorem" in the margin of his copy of the Arithmetica next to Diophantus's sum of squares problem

It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general for any number that is a power greater than the second to be the sum of two like powers. I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain.

The margin note became known as Fermat's Last Theorem. Andrew Wiles proved it in 1995.

Fermat's Last Theorem

The equation $x^n + y^n = z^n$ does not have any solution in natural numbers for any $n \geq 3$.

- For $n = 2$, we have infinitely many solutions in natural numbers.

  Example: $x = 3, y = 4$ and $z = 5$ is a nontrivial solution of $x^2 + y^2 = z^2$.

General Idea

A polynomial equation does not have a solution in natural numbers under modulo p, for every prime p.

$$\Downarrow$$

The polynomial equation does not have a solution in natural numbers.

Schur's Approach

For any $n \geq 3$, the equation $x^n + y^n \equiv z^n (\text{mod } p)$ does not have a nontrivial solution for every prime p.

$$\Downarrow$$

The equation $x^n + y^n = z^n$ does not have any solution in natural numbers for any $n \geq 3$.

Schur's Approach

~~For any $n \geq 3$, the equation $x^n + y^n \equiv z^n \pmod{p}$ does not have a nontrivial solution for every prime p.~~

$$\Downarrow$$

The equation $x^n + y^n = z^n$ does not have any solution in natural numbers for any $n \geq 3$.

Main Result

Theorem (Schur)

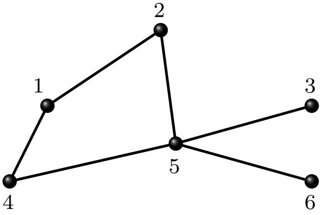
For every $n \in \mathbb{N}$, the equation $x^n + y^n \equiv z^n (\text{mod } p)$ has a solution in $\mathbb{N}$ for all prime p sufficiently large.

Example: $x = 1$, $y = 1$, $z = 2$ is a nontrivial solution of

$$x^4 + y^4 \equiv z^4 (\text{mod } 7).$$

Preliminaries

Graph: A graph $G(V, E)$ consists of a finite set of vertices V and a set of edges E consisting of unordered pairs of vertices.



Complete Graph K_n: A graph with n vertices where every pair of vertices are adjacent.

Pigeonhole principle: If n pigeons(items) are put into m holes(boxes), with $n > m$, then at least one hole(box) must contain more than one pigeon(items).

Generalized Pigeonhole principle: If n objects are placed into k boxes, then there is at least one box containing at least $\lceil \frac{n}{k} \rceil$ objects.

Ramsey Theory

&

Schur's Theorem

Ramsey Theory

Frank Plumpton Ramsey

(1903-1930)

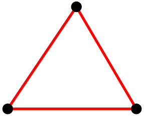
General Ramsey theory for triangles (K_3)

For any $r \in \mathbb{N}$ there exists $N = N(r) \in \mathbb{N}$ such that if the edges of the complete graph K_N are colored using r number of colors then there exists a monochromatic triangle as a subgraph of K_N.

Proof of the general Ramsey theory for triangles:

We apply induction on the number of colors r.

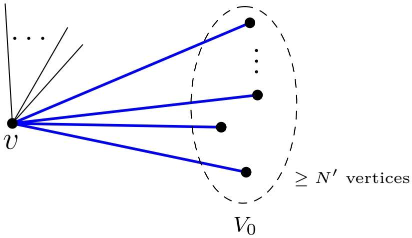
For $r = 1$, $N(r) = 3$ will work.



- **Induction hypothesis:** Claim holds for $r - 1$ colors with $N' = N(r-1)$.
- Consider $N = r(N' - 1) + 2$.
- Claim: N will work for r colors.

- Suppose K_N is colored using r colors. Choose any arbitrary vertex $v \in V(K_N)$.
- Degree of v is $N - 1 = r(N' - 1) + 1$.
- **PHP** implies there exists at least N' edges incident to v of the same color, say blue.
- Let $V_0 = \{\text{vertices joined to } v \text{ by a blue edge}\}$.

- If there is a blue edge inside V_0, we obtain a blue triangle.
- Otherwise, there are at most $r-1$ colors appearing among $|V_0| \geq N'$ vertices, and we have a monochromatic triangle by induction.



■

Theorem (Schur's Theorem)

For all $r \in \mathbb{N}$, $\exists\ S(r) \in \mathbb{N}$ such that if the numbers $\{1, 2, \ldots, S(r)\}$ are colored using r colors then $\exists$ a monochromatic solution to the equation $x + y = z$, where $x, y, z \in \{1, 2, \ldots, S(r)\}$.

The least positive number $S(r)$ for which the above theorem holds is called **Schur's number**.

Example:

1. For $r = 1$, $S(r) = 2$. As for $\{1, 2\}$, we have $1 + 1 = 2$.
2. For $r = 2$, $S(r) = 5$.

Example:

1. For $r = 1$, $S(r) = 2$. As for $\{1, 2\}$, we have $1 + 1 = 2$.
2. For $r = 2$, $S(r) = 5$.
3. For $r = 3$, $S(r) = 14$.
4. For $r = 4$, $S(r) = 45$.
5. For $r = 5$, $S(r) = 161$.

The proof that S(5) = 161 was announced in 2017 and took up 2 petabytes of space.

Proof of Schur's theorem

Proof: Let $\phi : [N] \to [r]$ be a coloring. We color the edges of K_{N+1} as follows:

$$\text{edge } \{i, j\}, i < j \text{ is colored by } \phi(j - i)$$

For N large enough, there exists a monochromatic triangle, say on the vertices $u < v < w$. Take $x = v - u$, $y = w - v$ and $z = w - u$ and the result follows. ■

Proof of the main theorem

Proof of the main theorem

Proof: Consider the group $G = ((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ and let

$$H = \{x^n : x \in G\} \text{ then } [G : H] \leq n$$

that is, cosets of H partition $\{1, 2, \ldots, p-1\}$ into at most n sets.

That is, we color all the elements of G using at most n colors.

By Schur's theorem, for p large enough, there exist monochromatic $X, Y, Z \in G$ such that

$$X + Y = Z$$

Also $X, Y, Z \in aH$ for some $a \in G$. Therefore $X = ax^n$, $Y = ay^n$ and $Z = az^n$ for some $x, y, z \in G$. Thus

$$ax^n + ay^n \equiv az^n (\text{mod } p).$$

Hence

$$x^n + y^n \equiv z^n (\text{mod } p).$$

Concluding Remarks

We've seen that looking at a problem in number theory through the lens of graph theory gives us a new perspective.

Roth's Theorem

Roth's Theorem

Every subset of the integers with positive upper density contains a 3-term arithmetic progression.

Consider the following graph theoretic problem:

Problem

What is the maximum number of edges in an n-vertex graph where every edge is contained in a unique triangle?

This seemingly simple question turns out to be quite enigmatic. Using **Szemerédi's regularity lemma**, we can prove that any such graph must have $o(n^2)$ edges. We can prove the Roth's theorem using this claim.

References I

Zhao, Y. (2019).

Graph theory and additive combinatorics.

MIT Opencourseware, 18.217.

Thank you!