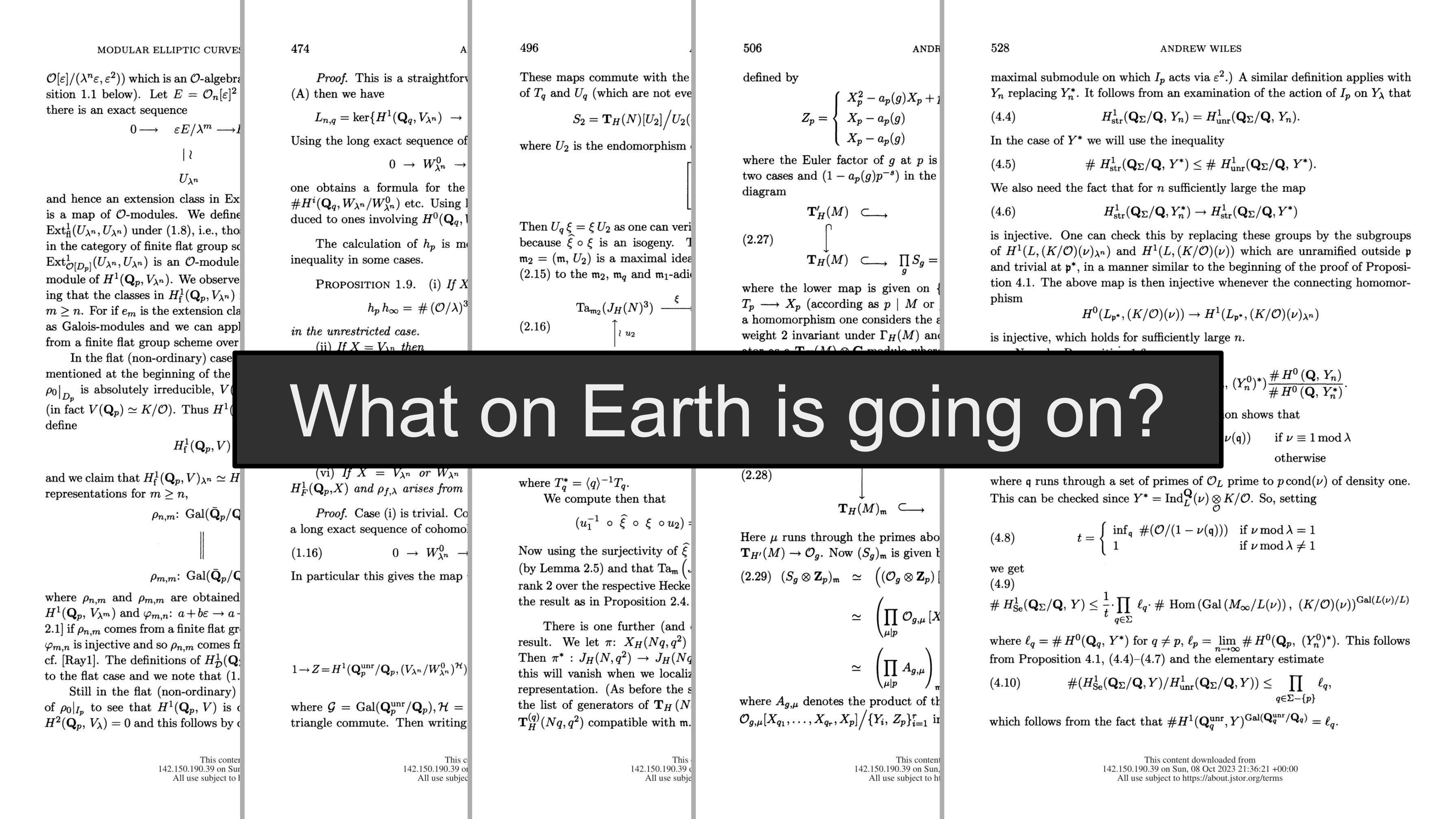
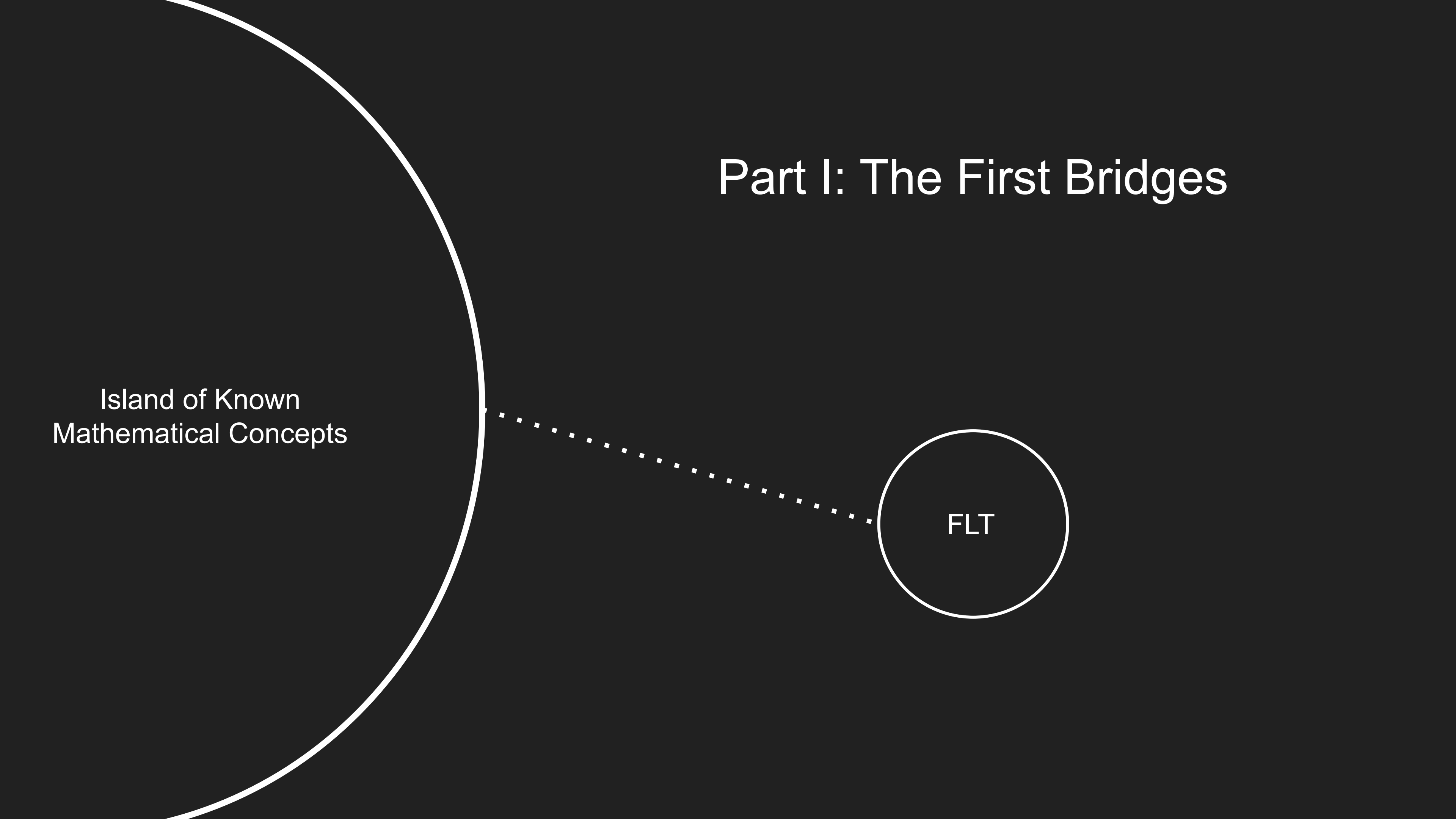
Fermat's Last Theorem

How Andrew Wiles Proved It

What on Earth is going on?




Part I: The First Bridges
Island of Known
Mathematical Concepts
FLT

Infinite Descent (1630s)

Pierre de Fermat laid the groundwork for many early attempts at proving FLT.

He proved FLT for $n = 4$ using “Infinite Descent”, the go-to method for early FLT proof attempts .

Infinite Descent is still commonly used in number theory, and in work involving Diophantine equations.

Proofs for Specific Exponents (1630s - 1839)

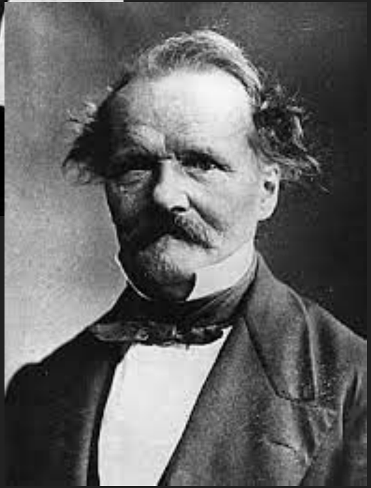
Over the next 200 years, mathematicians successfully proved FLT for specific cases of n:

- n = 4 (Fermat, 1630s)
- n = 3 (Euler, 1770)
- n = 5 (Dirichlet & Legendre, 1825)
- n =7 (Lamé, 1839)

Early Breakthroughs (early to mid-1800s)

Sophie Germain provided the first general propositions related to FLT in 1820. She split FLT into 2 “cases”; the first would be the case most commonly worked on for the next century and a half.

Ernest Kummer’s work in algebraic number theory would also produce significant contributions to FLT.



Computational Efforts (1950s - 1990s)

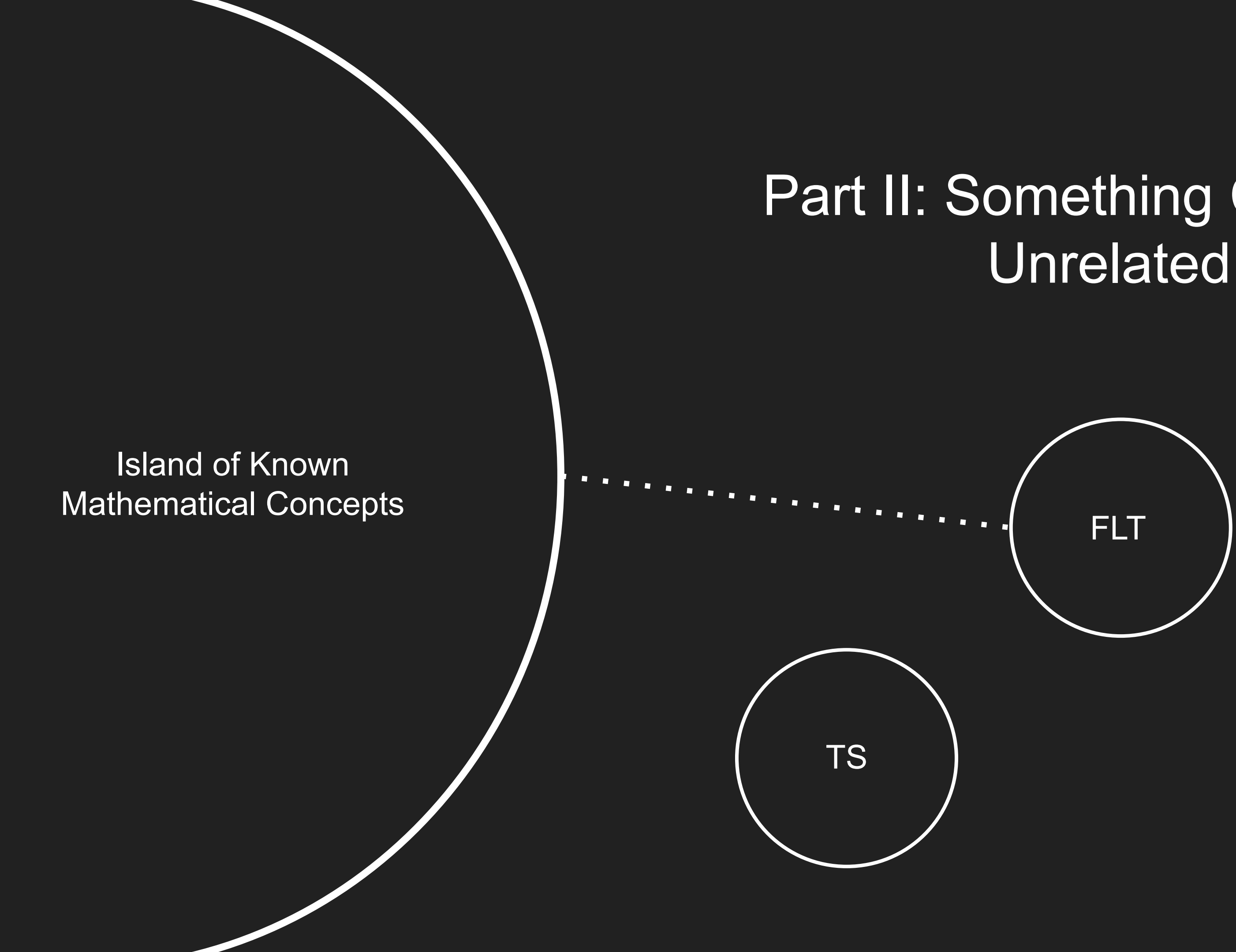
Following the invention of computers in the middle of the 20th century, mathematicians and computer scientists began using them extensively to prove many theorems, including FLT.

While unable to prove FLT in its entirety, they were able to prove it for “small” values of n:

- ≤ 2521 (Harry Vandiver, 1951)
- $< 125{,}000$ (Samuel Wagstaff, 1978)
- $< 4{,}000{,}000$ (various mathematicians, up to 1993)

By the 1980s, mathematicians had come to the consensus that a full proof of FLT was either impossible, or not yet possible with current mathematical tools…

Part II: Something Completely Unrelated…

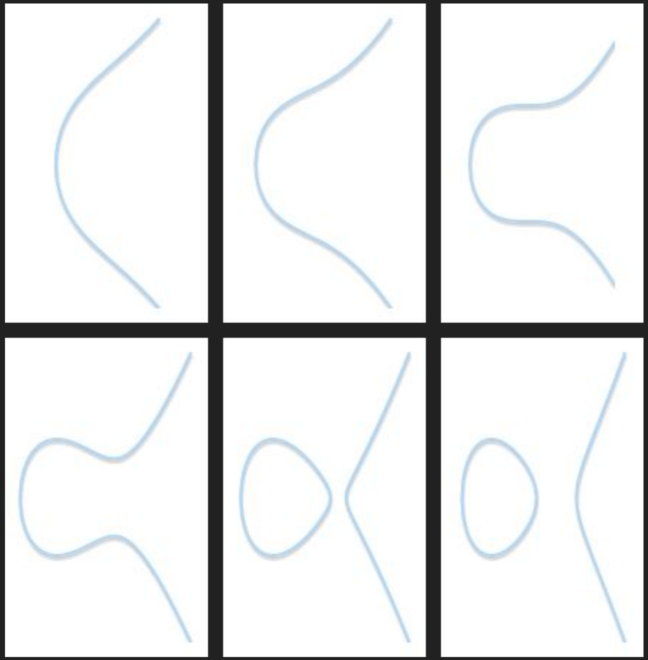


Elliptic Curves & Modular Forms - A Primer

While a full understanding of these terms require a course in algebraic geometry, complex analysis, and algebraic topology, we can describe some of their properties at a much lower level

An elliptic curve is, for our purposes, a curve that can be described by the following equation:

$$y^2 = x^3 + ax + b$$



Elliptic Curves & Modular Forms - A Primer

Modular Forms are a very high-level structure. We will describe them at a very low level, but a full description would require a graduate course.

A modular form is a function that maps the upper half of the xy-plane to the complex numbers, while also satisfying some key conditions. The theory surrounding them was largely developed in the late 1800s and early 1900s by Klein, Hecke, Taniyama, and Shimura.

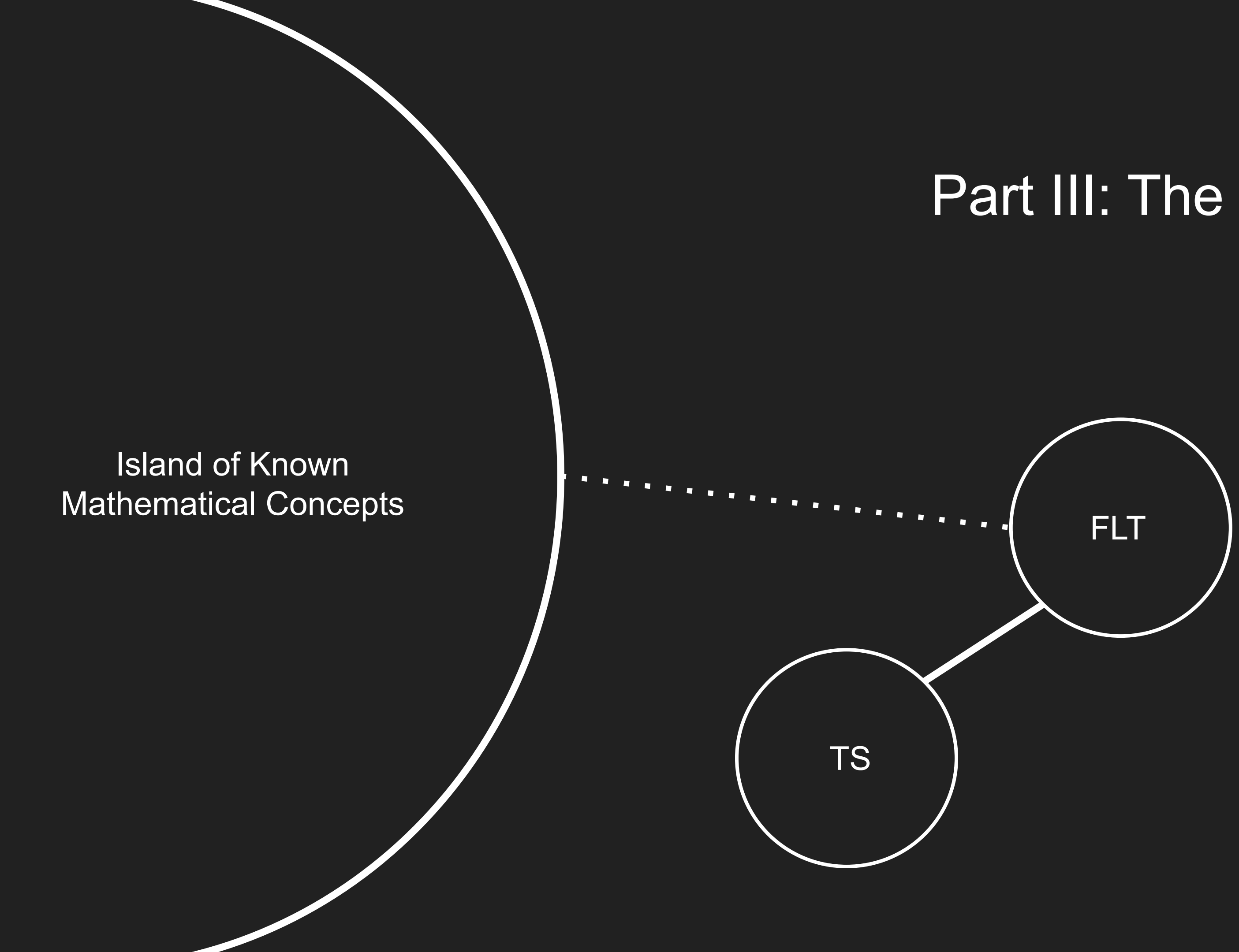
The Taniyama-Shimura Conjecture (1955)

Yutaka Taniyama first conjectured a relationship between elliptic curves and modular forms in 1955. Him and Goro Shimura worked on the problem until 1957.

The conjecture argues that certain elliptic curves are “related” to a modular form. We call such curves “modular”.

The conjecture remained unsolved for decades, and was determined by many to be inaccessible with current mathematical tools.

Part III: The Link



A Link Between FLT and Elliptic Curves (1975)

Yves Hellegouarch first showed a relationship between hypothetical solutions to FLT and elliptic curves.

If a hypothetical solution (a,b,c) existed for some exponent n, then the following elliptic curve can be constructed:

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

The curve is also “semistable” (this becomes important later).

Frey Curves & Their Properties (1982 - 1985)

In the early to mid 1980s, Gerhard Frey began to notice a strange pattern in these curves: they didn’t appear to be modular.

Although he did not prove it, he conjectured that such curves were not modular. It meant that they violated the Taniyama-Shimura Conjecture.

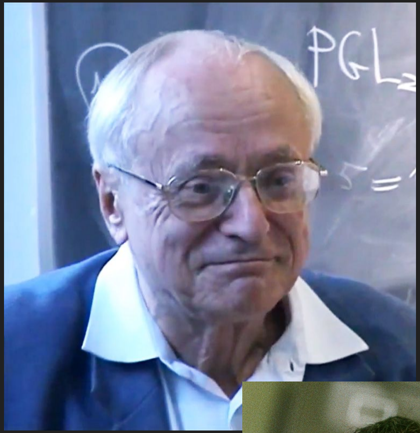
Because of his efforts, such curves are called “Frey Curves”.

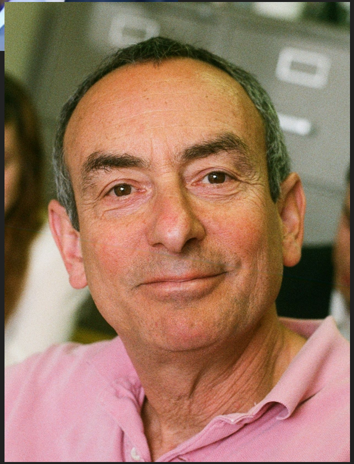
Serre’s and Ribet’s Theorems (1986)

While attempting to prove a conjecture that linked Galois representations to Taniyama-Shimura, Jean-Pierre Serre was able to partially prove that Frey curves were not modular.

The gap in his proof, then called the Epsilon Conjecture, was later proven by Ken Ribet in 1986.

This proof now meant that the Taniyama-Shimura conjecture and FLT were permanently linked:





Fermat’s Last Theorem is False

$\downarrow$

(a,b,c) is a solution of $x^n + y^n = z^n$

$\downarrow$

A Frey Curve can be constructed

AND

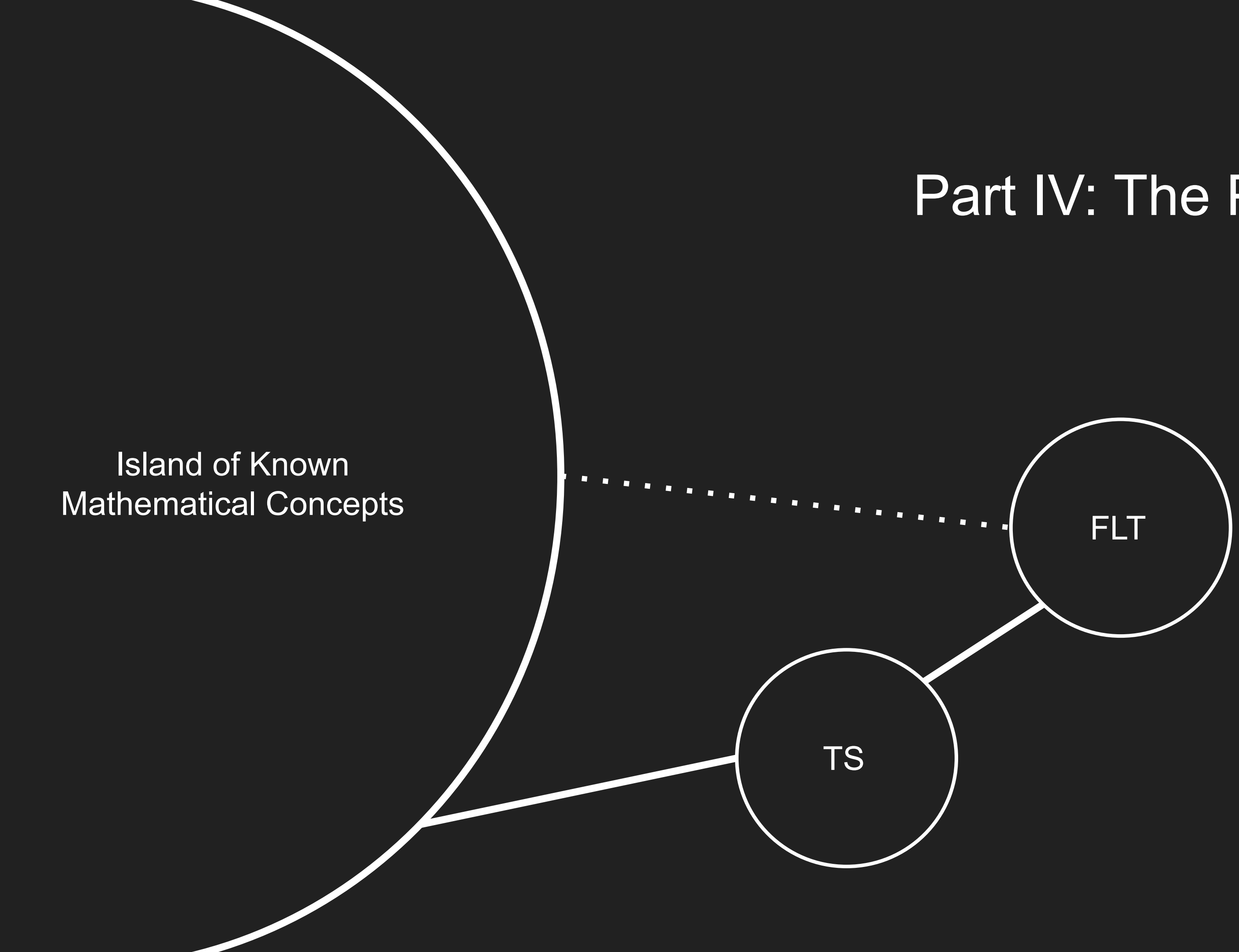
The Frey Curve is not modular

$\downarrow$

Taniyama-Shimura is False

If you could prove that every semistable elliptic curve was modular, then you would have proved Fermat’s Last Theorem.

Part IV: The Proof



Andrew Wiles Gets to Work (1986 - 1993)

Wiles, who had a childhood fascination with FLT, realized that this was likely his best shot at proving it.

His 7 years of work was done entirely in secret,

Wiles believed that the proof required induction, and studied several different approaches for how to perform the inductive step.

Wiles Presents his Findings (June 21-23, 1993)

In June 1993, Wiles presented his findings in a 3-part lecture.

The lectures showcased many new theorems and other findings related to elliptic curves, modular forms, and Galois representations.

At the end of the lectures, Wiles stated, to the shock of everyone, that these findings were sufficient to prove FLT*.

Wiles proving that every semistable elliptic curve is modular (photo by Ken Ribet)

Nick Katz discovered an error in Wiles’ proof 2 months after it was presented.

The error was found in a proof of a key Lemma needed for the rest of the paper.

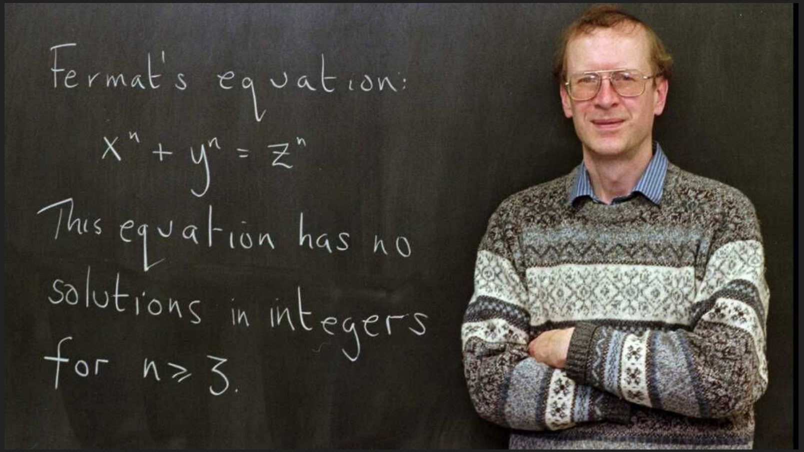
Wiles began attempts to fix the error shortly after, but quickly realized that it was not a simple fix.

Wiles Finally Proves It (1995)

Wiles almost gave up after a year of failing to fix the error.

He suddenly saw the fix on September 19, 1994, realizing that certain unrelated methods could be used to fix to the proof.

The final proof was published in Annals of Mathematics in May 1995, 358 years after Fermat's Last Theorem was conjectured.



Are There More Bridges?