1) We listed some open problems (so hard!)
2) Riemann zeta function (19th century) (powerful)
Most famous open problem: Riemann hyp.
3) Cantor's theory + transcendentals (late 19th century)
4) Groups (Giabios) (19th century)
5) Elliptic curves (20th - 21st century)

Today: FLT.
**FLT**: If \( n \) is an integer greater than 2, then \( x^n + y^n = z^n \) does not have solutions in integers \( > 0 \).

**Proof**: ETS this for \( n = \text{prime} \geq 5 \). Let \( p \) be such a prime. Suppose there exists a solution \( (a,b,c) \) with \( abc \neq 0 \). Then \( y^2 = x(x-a')(x-b') \) is an elliptic curve over \( \mathbb{Q} \). By Ribet's level lowering this ell. curve is not modular. But by the Taniyama–Shimura conjecture all elliptic curves over \( \mathbb{Q} \) are modular. Contr. D
Elliptic curves

Def: An elliptic curve is a smooth curve given by an equation of the form: \( E: y^2 = x^3 + Ax + B \)

if \( A, B \in \mathbb{Q} \), we say \( E \) is defined over \( \mathbb{Q} \)

\( E \) is smooth iff \( \Delta = -16(4A^3 + 27B^2) \neq 0 \)
Examples:

\[ y^2 = x^3 - 3x + 3 \]

\[ \Delta = -2160 \]

over \( \mathbb{R} \)
(2) $y^2 = x^3 + x$

$\Delta = -64$
(3) \( y^2 = x^3 + x^2 \)
(41) \text{msp}
What makes elliptic curves special?

There is a way to "add" points on them. This addition preserves the following property:

\[ A = (x_A, y_A), \quad B = (x_B, y_B) \]

\[ A + B = (x_{A+B}, y_{A+B}) \]

These points on \( E \) with entries in \( \mathbb{Q} \) form a group (the Mordell–Weil group).

\[ \text{mysterious object} \]
Modular forms are functions of complex variable, satisfying some symmetries.

Elliptic curves \( E \)

\[ L(s; E) \]
(certain zeta function)

Modular form \( f \)

\[ L(s; f) \]
(certain zeta function)

We say \( E \) is modular if \( \exists f \) such that

\[ L(s; E) = L(s; f) \]

Taniyama-Shimura: Every elliptic curve over \( \mathbb{Q} \) is modular.
Frey's idea: Imagine $E$ a solution to FLT, form from it an elliptic curve (maybe it would violate Taniyama-Shimura).

Ribet (1989) showed this curve is not modular. Wiles (1995) proved T-S.
Wiles's proof:

Given $E$, construct a Galois representation.

$\rho_E$

(these have zeta functions $L(s, \rho_E)$)

3 worlds:

elliptic curves $E$

easy

Galois repn's $\rho$

$\Rightarrow$

modular forms $f$

Wiles: every $\rho$ comes from $f$.

He showed it by counting $\rho$'s & $f$'s.

set of $\rho$'s $\sim$ set of $f$'s

+ structure $\sim$ + structure

Shinzel, Deligne, Serre (1970s)
KLOSIN  Math 550

11/12