Zeta Function of Elliptic Curves (1)

Reciprocity Laws on Prime Numbers

- **Fermat's Thm on Sums of Two Squares**

$$P = X^2 + Y^2 \iff P = 2 \text{ or } P \equiv 1 \pmod 4.$$

- **Quadratic Reciprocity Law**

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$$

- Are there Reciprocity Laws for ell. curves?

Surprising Answer `Yes' ($\Rightarrow$ **Modularity**)

Zeta Function of Elliptic Curves (2)

Elliptic curve

$$E : Y^2 = X^3 + AX + B$$

- Consider prime numbers $P \geq 5$ s.t.

$$\mathbf{4A^3 + 27B^2 \not\equiv 0 \pmod{P}}.$$

- N_P = # of mod P points on E
- **Reciprocity Law**: Are there any **laws** or **patterns** behind N_P for varying P?

Zeta Function of Elliptic Curves (3)

Example

$Y^2 = X^3 - X$

N_P = # of mod P points

$\mathbf{N_5 = 8}$ ∞,(0,0),(1,0),(2,1),(2,4),(3,2),(3,3),(4,0)

P	5	7	11	13	17	19	23
N_P	8	8	12	8	16	20	24

Zeta Function of Elliptic Curves (4)

Modularity Theorem

Every elliptic curve is **modular**, i.e., there is a **modular form**

$$\mathbf{f(q)} = q + C_2 q^2 + C_3 q^3 + C_4 q^4 + C_5 q^5 + \cdots$$

satisfying

$$\mathbf{C_P = P + 1 - N_P}.$$

- It was originally conjectured by Taniyama and Shimura in 1950's.

Zeta Function of Elliptic Curves (5)

Example $Y^2 = X^3 - X$

$f(q) = q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} + \cdots$

modular form

P	5	7	11	13	17	19	23
N_P	8	8	12	8	16	20	24
$P+1-N_P$	-2	0	0	6	2	0	0

Zeta Function of Elliptic Curves (6)

- **Modularity** is one of the **Reciprocity Laws** for elliptic curves.
- In 1990's, Wiles proved it with the help from Taylor for many elliptic curves.($\Rightarrow$ **Fermat's Last Thm**)
- The full modularity was finally proved by Breuil, Conrad, Diamond, and Taylor in 2001.

Andrew John Wiles (1953-)

https://en.wikipedia.org/wiki/Andrew_Wiles