What Is Number Theory?

1) Diophantine Equations and Elliptic Curves
2) L-Functions
3) Modular Forms
4) Tate's Thesis
5) Automorphic Representations and the Langlands Program

1) Diophantine Equations and Elliptic Curves

Pythagorean triples: \(a^2 + b^2 = c^2\), \(a, b, c \in \mathbb{Z}\)

By \(x^2 + y^2 = 1\), \(x, y \in \mathbb{Q}\)

Rational points on unit circle:

\[
\begin{align*}
  m &= \frac{y}{x}, \quad x, y \in \mathbb{Q} \\
  a &= b^2 - p^2, \quad p, q \in \mathbb{Z} \\
  b &= 2pq \\
  c &= p^2 + q^2
\end{align*}
\]

\(\bigcap\) all Pythagorean triples
Elliptic Curves

\[ \text{area} = 6 \in \mathbb{Q} \]

Congruent Number Problem: which integers \( N \) are the area of a rational right triangle?

\( N \) congruent number \( \iff y^2 = x^3 - N^2 x \) for (particular) \( x, y \in \mathbb{Q} \)

Elliptic curve: nonsingular curve of form \( y^2 = x^3 + ax + b \)

Want to find rational points on elliptic curves \( \mathcal{E} \)
Can "add" rational points to find more \( \mathcal{E}(\mathbb{Q}) \) forms a group

Mordell-Weil: \( \mathcal{E}(\mathbb{Q}) \) is finitely-generated abelian

Tunnell: \( N \) congruent \( \iff \) \( E: y^2 = x^3 - N^2 x \), \( E(\mathbb{Q}) \cong \mathbb{Z} \)

Birch & Swinnerton-Dyer: \( \text{rank} \mathcal{E}(\mathbb{Q}) = \text{order of zero of the Hasse-Weil } L\text{-function } L(\mathcal{E}, s) \) at \( s = 1 \).

\[ L(\mathcal{E}, s) = \prod_{p \text{ prime}} \left( 1 - \frac{a_p}{p^{s}} + \frac{\varepsilon(p)}{p^{1-2s}} \right)^{-1} \]

involves \( \# E(\mathbb{F}_p) \) \( 0 \) or \( 1 \)

So we've turned this congruent \# problem into complex analysis.
2) L-functions

- Functions attached to number-theoretic objects
e.g. elliptic curves, field extensions, reps of \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \),
  modular forms (later)
- Allow us to use complex analysis for number theoretic goals
- Equalities of different L-functions encode "reciprocity laws" and connections between different objects
  e.g. Modularity Theorem: L-function of elliptic curve \( \leftrightarrow \) L-function of some modular form \( \Rightarrow \) Fermat's Last Theorem

Simplest L-function: Riemann's \( \zeta \)
\[
\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{Re}(s) > 1
\]
\{ analytic continuation, else \}

Functional equation: \( \zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \zeta(1-s) \)

Euler product:
\[
\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}
\]

So by understanding \( \zeta(s) \), we can understand primes
Prime number theorem: \( \# \text{primes} \leq N \sim \frac{N}{\log(N)} \)

- Riemann explicit formula involves zeroes of \( \zeta(s) \)
- Riemann hypothesis: all (nontrivial) zeroes have \( \Re(s) = \frac{1}{2} \)
  - Puts tight bound on this count

3) Modular Forms

Generalizations of periodic functions, and we can do analysis on \( SL_2(\mathbb{Z}) \) upper half plane \( \mathbb{H} \) (linear fractional transformation)

\[ f : \mathbb{H} \to \mathbb{H} \] modular form of weight \( k \) if

1) \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f \cdot (z) = (cz + d)^k f \cdot (z) \)
2) \( f \) is holomorphic
3) \( f \) has "moderate growth"

"Generalizations" of periodic functions, and we can do analysis on elliptic curves to hyperbolic geometry

L-function of a modular form:

\[ f \left( e^{2\pi i \theta} \right) = \sum_{h=1}^{\infty} a_h e^{2\pi i h \theta} \] (Fourier series)

\[ L(s) = \sum_{h=1}^{\infty} \frac{a_h}{h^s} \]

Modularity theorem: \( \{ \text{L-functions for } \mathcal{E} \text{ elliptic curves} \} = \{ \text{L-functions for } \mathcal{M} \text{ modular forms} \} \)

\( \Rightarrow \) Fermat's Last Theorem
Generalizes instead of $\mathbb{H}$, use (a quotient of) a reductive group $G(\mathbb{R})$

Instead of $\text{SL}_2(\mathbb{Z})$, find functions invariant under some other arithmetic subgroup $\Gamma$, called automorphic forms.

---

4) Tate's Thesis

Q: How "far apart" are $x, y \in \mathbb{Q}$?

A: 1) $|x-y|$ (IR)

2) For primes $p$, $x \equiv y \pmod{p^k}$ for what $k$ ($\mathbb{Q}_p$: $p$-adic numbers)

Lash all these together: adeles ($\mathbb{A}$)

Tate: slick proof of analytic continuation and functional equation of Hecke $L$-functions

Idea: use the adeles, and split into "places" ($\mathbb{Q}_p$ and IR)

5) Automorphic Representations, and the Langlands Program

$G(\mathbb{A})$: reductive group over adeles

$G(\mathbb{A}) \otimes L^2(G(\mathbb{Q}) \backslash G(\mathbb{A}))$: vector space of automorphic forms

Can decompose this action into "automorphic representations" $\Pi$.

- $L$-function $L(s, \Pi, r)$ associated to $\Pi$

- Both $\Pi$ and $L(s, \Pi, r)$ break up into local factors

- Local factors of $\Pi$: $p$-adic representations
Langlands program: Set of conjectures about automorphic representations that encompass large swaths of number theory.

- Extremely difficult

Key conjecture: Langlands correspondence:

\[
\{ \text{L-functions of } \mathbb{Q} \} = \{ \text{L-functions of (certain) automorphic representations} \}
\]

Each of these areas has myriad offshoots.

Number theory doesn't fit in a neat little box. Instead, it encompasses anything that relates, even distantly, to these areas. Number theory is like a squid with tentacles reaching throughout mathematics.