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

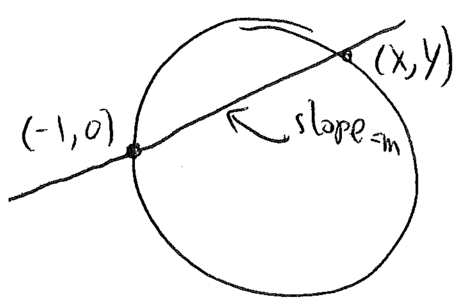
---

1) Diophantine Equations and Elliptic Curves

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

$\hookrightarrow$ $x^2+y^2=1$, $x,y \in \mathbb{Q}$

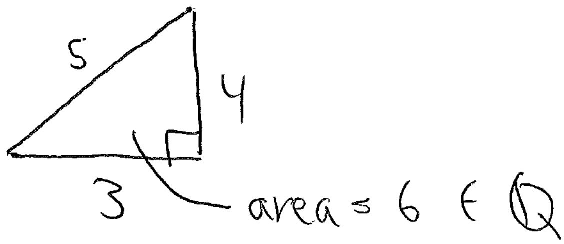
Rational points on unit circle:



$m = \frac{p}{q} \in \mathbb{Q} \iff x,y \in \mathbb{Q}$

Obtain
$$\left.\begin{aligned} a &= q^2 - p^2 \\ b &= 2pq \qquad p,q \in \mathbb{Z} \\ c &= p^2 + q^2 \end{aligned}\right\} \text{all Pythag. triples}$$

Elliptic Curves



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 E

Can "add" rational points to find more, so these points $E(\mathbb{Q})$ form a group

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

Tunnell: N congruent $\iff E: y^2 = x^3 - N^2 x$, $\operatorname{rank} E(\mathbb{Q}) \geq 1$

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

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

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 $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, 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 = L function of some modular form $\Rightarrow$ Fermat's Last Theorem~~

Simplest L-function: Riemann's ζ

$$\zeta(s) := \begin{cases} \sum_{n=1}^{\infty} \frac{1}{n^s}, & Re(s) > 1 \\ \text{analytic continuation}, & \text{else} \end{cases}$$

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

Euler product:

$$\zeta(s) = 1 + 2^{-s} + 3^{-s} + 4^{-s} + \cdots$$
$$= (1 + 2^{-s} + 4^{-s} + \ldots)(1 + 3^{-s} + 9^{-s} + \ldots) \cdots$$
$$= (1 + 2^{-s} + 2^{-2s} + \ldots)(1 + 3^{-s} + 3^{-2s} + \ldots) \cdots$$
$$= \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

So by understanding $\zeta(s)$, we can understand primes

- Prime # thm: (# primes $\leq N$) $\sim \dfrac{N}{\log(N)}$
- Riemann explicit formula involves zeroes of $\zeta(s)$
- Riemann hypothesis all (nontrivial) zeroes have $\mathrm{Re}(s) = \frac{1}{2}$
  - Puts tight bound on this count

---

3) Modular Forms

~~Generalizations of periodic functions, and we can do analysis~~

$SL_2(\mathbb{Z}) \circlearrowright$ upper half plane $\mathbb{H}$ (linear fractional transformation)

$f: \mathbb{H} \to \mathbb{H}$ modular form of weight k if

1) $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f\right)(z) = (cz+d)^k f(z)$

2) f is holo/meromorphic $\leftarrow$ f satisfies certain differential equations

3) f has "moderate growth"

"Generalizations" of periodic functions, and we can do analysis

Connect elliptic curves to hyperbolic geometry

L-Function of a modular form:

$$f(e^{2\pi i \theta}) = \sum_{n=1}^{\infty} a_n e^{2\pi i \theta} \quad \text{(Fourier series)}$$

$$L(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Modularity theorem: $\left\{ \begin{matrix} \text{L-functions for} \\ \text{elliptic curves} \end{matrix} \right\} = \left\{ \begin{matrix} \text{L-functions for} \\ \text{(some) modular forms} \end{matrix} \right\}$

$\Rightarrow$ Fermat's Last Theorem

Generalize: Instead of $\mathbb{H}$, use (a quotient of) a reductive group $G(\mathbb{R})$

Instead of $SL_2(\mathbb{Z})$, find functions invariant under some other "arithmetic subgroup" Γ. called automorphic forms

---

4) Tate's Thesis

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

A: 1) $|x-y|$ $(\mathbb{R})$

2) $\forall$ 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~~ "local factors" ($\mathbb{Q}_p$ and $\mathbb{R}$)

---

5) Automorphic Representations, and the Langlands Program

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

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

Can decompose this action into "automorphic representations" π

- $\exists$ L-function $L(s,\pi,r)$ associated to π
- Both π and $L(s,\pi,r)$ break up into local factors
- Local factors of π: p-adic representations

Langlands program: Set of conjectures about automorphic representations that encompass huge swaths of number theory

- Extremely difficult

Key conjecture: Langlands correspondence:

$$\left\{ \begin{array}{l} \text{L-functions of} \\ \text{repns of } \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \end{array} \right\} \rightleftharpoons \left\{ \begin{array}{l} \text{L-functions of (certain)} \\ \text{automorphic representations} \end{array} \right\}$$

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.