Uniformity of Solutions to Diophantine Equations

Rohan Hiatt, Daria Mićović, Blanca Viña Patiño, Bryan Quah
Mentors: Travis Scholl, Amos Turchet

Washington Experimental Mathematics Lab (WXML)
University of Washington
What are Diophantine Equations?

- Polynomial equations with integer coefficients, where we look for integer or rational solutions.
- May have infinite or finite number of solutions.
- Named after Diophantus of Alexandria.

Examples:

\[ a^2 + b^2 = c^2 \]
\[ x^2 - Dy^2 = \pm1 \]
\[ x^3 + x^2y + 3xy^2 - y^3 = 17 \]
\[ y^2 = x^5 - 5x^3 + 4x - 1 \]
Motivation

- Investigate methods for solving Diophantine Equations - there is no general algorithm for solving Diophantine Equations (Hilbert’s 10th Problem)
- Understand the set of solutions to specific types of Diophantine Equations
- Search for more rational points for hyperelliptic curves of genus 2
Equations to Plane Curves

Consider: \[ y^2 = x^5 + 1 \]

This equation defines a curve in the plane.

Solutions to this equation, \( x = a \) and \( y = b \), correspond to points \((a,b)\) on the curve.

When \( a \) and \( b \) are rational numbers, these are called "rational points".
Faltings’ Theorem (1983)

Let $K$ be a number field. If $C$ is an algebraic curve over $K$ of genus $g \geq 2$, then there are only finitely many rational points, i.e., the set $C(K)$ of $K$-rational points is finite.

If $C$ is a smooth curve of degree $d$, the genus is given by

$$g = \frac{(d - 1)(d - 2)}{2}$$
Lang Conjecture
(1986)

If \( X \) is a variety of general type defined over a number field \( K \), then the set \( X(K) \) of \( K \)-rational points of \( X \) is not Zariski dense.

- One of the most important conjectures in Diophantine geometry
- Conjectural analogue of Faltings' theorem in higher dimensions. Caporaso, Harris, and Mazur proved that if the Lang Conjecture is true, then the following conjecture must also be true.
Uniformity Conjecture  
*(1997)*

Let \( g \geq 2 \) be an integer. There exists a number \( B(g) \), depending only on \( g \), such that every smooth curve of genus \( g \) defined over \( \mathbb{Q} \), has at most \( B(g) \) rational points.

- **Theorem (Katz–Rabinoff–Zureick-Brown) (2016):**  
  - Found a genus-dependent formula for the number of points on any smooth curve of genus at least 3.

\[
\#C(\mathbb{Q}) \leq 84g^2 - 98g + 28
\]
Computing Rational Points

- Setup the algorithm to work in parallel for efficiency
  - Ran it on the 48 core Sage machine!
- Wrote functions to calculate the discriminant and conductor of a given curve
  - Trying to reverse-engineer a curve not on LMFDB
- Data cleaning
Results - LMFDB Data

The graph shows the distribution of the number of curves versus the number of rational points. The x-axis represents the number of rational points, while the y-axis represents the number of curves. The data indicates a concentration of curves with a small number of rational points, with a significant drop as the number of rational points increases.
Results - Our Data

The histogram shows the distribution of the number of curves and their corresponding number of rational points. The x-axis represents the number of rational points, while the y-axis represents the number of curves. The data indicates a significant concentration of curves with a smaller number of rational points, with a peak around 5 rational points.
Future Directions

- Construct a hyperelliptic curve not found in the LMFDB and compute its rational points
- Continue to gather data for higher upper bound values in Stoll’s
- Understand rational functions, divisors of curves, and rank of curves.