WXML Final Report

Uniformity of Solutions of Diophantine Equations

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

Winter 2018

1 Introduction

A Diophantine Equation is a polynomial equation, usually with two or more unknowns with integer coefficients, in which we look for integer or rational solutions. The simplest case is where we look for integral solutions (x, y) in the linear equation:

$$ax + by = c$$

where a, b, c are known integers.

The study of Diophantine Equations and their analyses dates back to the year AD 300, when a Greek mathematician, Diophantus of Alexandria, wrote about them in his series of books, *Arithmetica*. In fact, a problem in Diophantus' *Arithmetica* led Pierre de Fermat in 1637 to annotate a statement within the margins of his own copy, famously known as Fermat's Last Theorem which would go on unresolved for the next 4 centuries.

This quarter, for our study of Diophantine Equations, we investigated equations represented as plane curves with a genus of 2, with the following questions in mind: Are there any solutions to these equations? If so, how many are there? Can we provide a bound on the number of rational solutions? What does this bound depend on?

1.1 The Initial Problem

We initially found that Diophantine equations looked easy to solve but upon further study we found that the underlying theorems run very deep. This brought up questions surrounding understanding the set of solutions to specific Diophantine equations, and how solutions to some equations provide approximations to certain algebraic numbers. In general, no method or algorithm exists for finding sets of solutions to all Diophantine equations, so we studied specific cases in an attempt to find some sort of pattern. Specifically, Hilbert's Tenth Problem asks whether such an algorithm can be found.

2 Progress

2.1 Theoretical

2.1.1 Genus

We consider Diophantine equations represented as plane curves to understand the relationship between singularities, genus, and the number of rational solutions. First, we begin by defining a few terms. A curve is called **non-singular (or smooth)** if it has no singular points. Let C be a curve, then $m_P(C)$ is the **multiplicity** of a singular point P of C and represents the number of times P appears as a root of C. Furthermore, a singular point P on the curve is called an **ordinary multiple point** if it has $m_P(C)$ distinct tangents at P. The figures below give visual examples of curves with ordinary multiple points and non-ordinary multiple points.

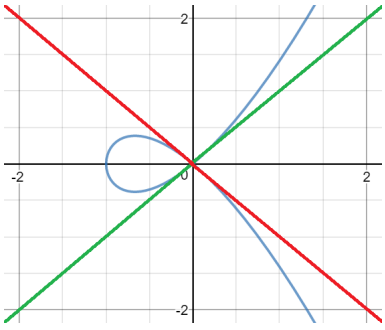

Figure 1: Curve represented by $y^2 = x^3 + x^2$ with one ordinary multiple point at (0,0).

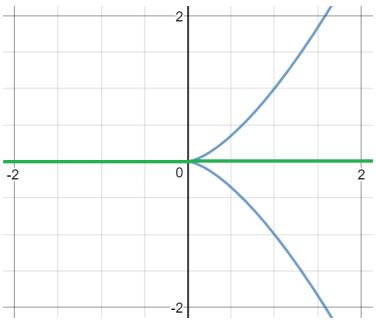

Figure 2: Curve represented by $y^2 = x^3$ with one non-ordinary point at $(0, 0)$.

The curve in Figure 1 has two defined distinct tangents at $(0, 0)$ and no other singular points so we have one multiple ordinary point with multiplicity 2. The case is different for the curve in Figure 2. Intuitively, there are two branches passing through the origin, so if we consider them separately, we would have two tangent lines that would eventually merge at $y = 0$. When computing the multiplicity of this point on $y^2 = x^3$, we do get that the tangent at $y = 0$ has multiplicity 2. Thus, we do not have $m_P(C)$ distinct tangents at $(0, 0)$, making $(0, 0)$ a non-ordinary point.

Finally, if C only has ordinary multiple points, then the genus is given by the following formula

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P \in sing(C)} \frac{m_P(C)(m_P(C)-1)}{2} \text{ , where } d = \deg(C).$$

On the other hand, if C does not only have ordinary multiple points, the formula gives us an upper bound for g, meaning that C could have a lower genus than the right side of the above formula. Now we have a way of computing the genus of a curve in a way that only depends on the degree and multiplicity of singular points. Consider the elliptic curve $y^2 = x^3 - x$. Elliptic curves are smooth, and thus non-singular, which means that the sum in the above formula is 0. Thus, the genus of such curve depends only on the degree which is 3 in this case. We can easily compute the genus of this curve to be

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P \in sing(C)} \frac{m_P(C)(m_P(C)-1)}{2} = \frac{(3-1)(3-2)}{2} - 0 = 1$$

2.1.2 Faltings' Theorem

The genus is an important curve property as it can provide a bound for the number of rational points:

Theorem. ***Faltings' Theorem (1983)*** *Let C be a smooth curve defined over $\mathbb{Q}$ of genus ≥ 2. Then, the number of rational points on C is finite.*

In other words, Faltings' theorem tells us that all curves which have genus 2 or higher cannot have an infinite number of rational points. This theorem is actually stronger since it applies to finite extensions of $\mathbb{Q}$, but for our purposes, we will consider smooth curves over $\mathbb{Q}$. The Lang conjecture, which is a conjectural generalization of Faltings' theorem in higher dimensions is one of the most important conjectures in Diophantine geometry. Caporaso, Harris, and Mazur proved in their paper that if the Lang Conjecture is true, then the following conjecture must also be true.

2.1.3 Uniformity Conjecture

Conjecture. ***Uniformity Conjecture*** *Let $g \geq 2$ be an integer. There exists a number $B(g)$, depending only on g, such that for any smooth curve C with fixed genus g defined over $\mathbb{Q}$, the number of rational points on C is less than $B(g)$.*

This is a very powerful conjecture because it states that all curves of the same genus g will have the same upper bound for the number of rational points. If this conjecture is proven wrong, then the Lang conjecture would also be untrue. However, there exists a large amount of evidence supporting the Uniformity Conjecture. One example is the following theorem:

Theorem. ***Katz-Rabinoff-Zureick-Brown (2016)*** *Let C be any smooth curve of genus g and let $r = rank(J_C)$. Suppose that $r \leq g - 3$. Then,*

$$\#C(\mathbb{Q}) \leq 84g^2 - 98g + 28$$

We can see that this theorem provides an upper bound on the number of rational points that is solely dependent on the genus of a curve, thus supporting the Uniformity Conjecture. Furthermore, it is important to note that this theorem does not apply to genus 2 curves because we require r to be greater than or equal to 0 and $r \leq g - 3$. The main motivation for us

to look at curves of genus 2 is that no such bound has been discovered for such curves yet. Additionally, we wanted to see if we could come up with new results using Michael Stoll's algorithm for computing rational points on hyperelliptic curves.

2.2 Computational

2.2.1 Michael Stoll's Algorithm for Finding Rational Points on Hyperelliptic Curves

We imported Michael Stoll's C program into CoCalc and added Sage scripts so that we could input curves that are not in a standardized form. Using CoCalc also allows us to parallelize our code such that we can compute the rational points for multiple curves simultaneously. For a little bit of background, Michael Stoll's C program uses an optimized quadratic sieving algorithm to find rational points. The current record for the curve with the highest number of rational points, totalling 642, was found in a systematic search using this algorithm. (CITE: http://www.mathe2.uni-bayreuth.de/stoll/recordcurve.html)

2.3 Results

2.3.1 L-Functions and Modular Forms Database (LMFDB)

After implementing the algorithm in sage and ensuring it worked for a select number of test cases, we moved toward testing a much larger number of hyperelliptic curves. The L-Functions and Modular Forms Database (LMFDB) is an online database of mathematical objects that appear primarily in number theory. This database maintains a list of genus 2 plane curves, along with data surrounding their rank, number of rational points, and whether the number of rational points found has been verified or not. If the set of rational points associated to curves is verified then that set contains every rational point. Unverified curves may or may not have undiscovered points. We used the data from the LMFDB in order to calculate rational points using the given curves.

2.3.2 Our Results

We ended up with some fascinating and exciting results. In the case of LMFDB curves with verified points, we were able to corroborate these points, since our algorithm found all the same ones. For unverified points, we ended up finding more rational points than were listed in the database. The following figures show the difference in the spread of calculated data between our calculated points and those on the LMFDB:

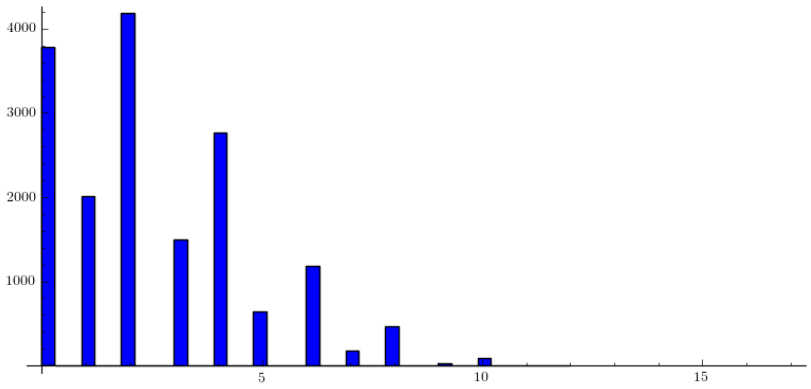

Figure 3: Points calculated by the LMFDB. The x-axis represents number of rational points and y-axis is frequency.

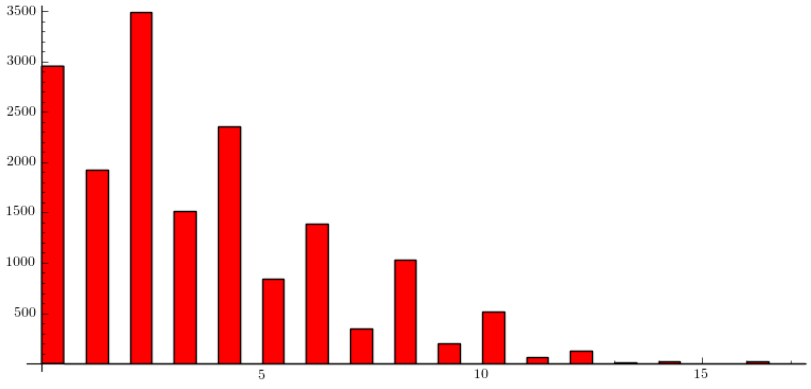

Figure 4: Points calculated by our implementation. The x-axis represents number of rational points and y-axis is frequency.

3 Future directions

We aim to continue collecting significant data for curves of genus ≥ 2.

We also plan to further study the Mathematics behind properties of these curves, specifically with regards to the Jacobian and its rank.

References

[1] L. Caporaso, J. Harris, and B. Mazur. Uniformity of rational points. *J. Amer. Math. Soc.*, 10(1):1–35, 1997.

[2] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[3] E. Katz, J. Rabinoff, and D. Zureick-Brown. Uniform bounds for the number of rational points on curves of small Mordell-Weil rank. *Duke Math. J.*, 165(16):3189–3240, 2016.

[4] T. LMFDB Collaboration. The l-functions and modular forms database. http://www.lmfdb.org, 2013. [Online; accessed 16 September 2013].

[5] SageMath. *CoCalc Collaborative Computation Online*, 2016. `https://cocalc.com/`.

[6] M. Stoll. *Documentation for the Ratpoints Program*, 2011. `http://www.mathe2.uni-bayreuth.de/stoll/programs/ratpoints-doc.pdf`.

[7] U. Zannier. *Lecture notes on Diophantine analysis*, volume 8 of *Appunti. Scuola Normale Superiore di Pisa (Nuova Serie) [Lecture Notes. Scuola Normale Superiore di Pisa (New Series)]*. Edizioni della Normale, Pisa, 2009. With an appendix by Francesco Amoroso.