My First Research Experience

Dishant Saikia

Undergraduate Student, Tezpur University, Assam, India

My first research paper titled 'k-Diophantine m-tuples in Finite Fields' [HKM21] has been uploaded recently on arXiv. It was a joint work done as a summer research project of the Polymath Jr. program 2021 supervised by Dr. Seoyoung Kim (Coleman Postdoctoral Fellow, Queen's University), Prof. Steven Miller (Professor, Williams College) and Trajan Hammonds (Graduate Student, Princeton University). The group of students involved with this paper included myself, Kyle Onghai (University of California, Los Angeles), Lalit Mohan Sharma (University of Delhi) and Arjun Nigam (University of Arizona). As it was my first tour into the research world of mathematics, I had quite a unique experience participating in this program. The Polymath Jr. is an online collaborative research program for undergraduates. It consists of research projects on a variety of math topics where each project is led by an active mathematician with additional mentors who are normally graduate students. All of the projects are presented in the first week and based on the student's priority options, they are selected with about 20-25 students involved with each project. They are introduced to the material through presentations, research papers and other resources in the first few weeks and then through more interactive sessions and meetings, the group decides on a particular problem or two to work on. There are variations done on this approach by a few mentors.

The lead mentor of our project, Dr. Kim split the larger 20-25 students into 3 smaller groups as the topic 'Diophantine m-tuples' is quite vast including many research articles published on it. The groups were made based on each student's interests and hence, I decided to join the group which studied Diophantine m-tuples in finite fields. There were meetings on a weekly basis with Dr. Kim, with Prof. Miller and the graduate student mentor Trajan joining occasionally and offering their suggestions.

Let us begin with the definition of the term 'Diophantine m-tuples'.

Definition 1. Let S be a set of m positive integers $\{a_1, a_2, \ldots, a_m\}$. If $a_i a_j + 1$ is a perfect square for all i, j such that $1 \leq i < j \leq m$, then S is a **Diophantine m-tuple**.

Similarly, we define a rational Diophantine m-tuple as follows. If S is a set of m positive rationals and satisfies the same condition, it is called a **rational Diophantine m-tuple**.

The study of Diophantine m-tuples can be traced to the work of Diophantus of Alexandria, and has caught the attention of numerous leading mathematicians since then. In the 3rd century, Diophantus observed that the set of four numbers: $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$ satisfy the property that the product of any two elements in the set is one less than a rational square. This is the first example of a rational Diophantine quadruple. In the 17th century, Fermat became interested in finding integer solutions and eventually found the Diophantine quadruple $\{1, 3, 8, 120\}$. Euler extended the Diophantine quadruple given by Fermat to form a rational Diophantine quintuple, namely $\left\{1, 3, 8, 120, \frac{777480}{8288641}\right\}$.

The definition leads to many questions relating to the size and existence of Diophantine m-tuples. A few modifications and generalisations can also made and similar questions can be asked about them. Here we present a few noteworthy results about Diophantine m-tuples.

The first important result concerning the size of Diophantine m-tuples was given by Baker and Davenport in 1969 [BD69]. They showed using Baker's theory on linear forms in logarithms of algebraic numbers that if d is a positive integer such that $\{1, 3, 8, d\}$ is a Diophantine quadruple, then d has to be 120, implying that $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple. In 1979, Arkin, Hoggatt and Strauss showed that any Diophantine triple can be extended to a Diophantine quadruple [AHS79]. In 2004, Dujella proved that there is no Diophantine sextuple and that there are at most finitely many Diophantine quintuples [Duj04]. In 2018, He, Togbé and Ziegler showed that there does not exist a Diophantine quintuple [HTZ18]. In the case of rationals, no absolute upper bound for the size of rational Diophantine m-tuples is known. Results have been obtained about rational Diophantine quintuples and sextuples.

There are many generalizations of Diophantine m-tuples. One natural generalization which has been extensively studied is if we replace the number 1 in "$a_i a_j + 1$" with n. These sets are called *Diophantine m-tuples with the property $D(n)$*. There have been significant results about the existence of Diophantine m-tuples with the property $D(n)$ for $n = 4, -1$ etc.

I assume one question must be bothering everyone: Why should we care? It is quite fair to ask this question as mentioned by Prof. Ravi Vakil (Professor, Stanford University) in his book '*The*

Rising Sea: Foundations of Algebraic Geometry':

> "*When introduced to a new idea, always ask why you should care. Do not expect an answer right away, but demand one eventually.*"

Also, this is probably the right moment to ask this as we have listed a few papers on Diophantine m-tuples. While not being an expert on the topic and hence my inability to mention many relations or uses of Diophantine m-tuples, I can mention quite a famous connection with everyone's favorite math word 'elliptic curves'.

If $\{a, b, c\}$ are assumed to form a Diophantine triple, then in order to extend this triple to a quadruple, the task is to find an integer x such that $ax + 1, bx + 1$ and $cx + 1$ are all squares of integers. Finding a solution $x \in \mathbb{Z}$ to the three simultaneous conditions implies that there exists $y \in \mathbb{Z}$ such that

$$y^2 \;=\; (ax + 1)(bx + 1)(cx + 1); \tag{0.1}$$

this equation describes an elliptic curve. Hence, extending a Diophantine triple to a Diophantine quadruple is equivalent to finding integer solutions of the mentioned elliptic curve. A more detailed exposition on Diophantine m-tuples including a list of papers published on them can be found at [Duj] and [DS21].

Now, coming back to my decision to study and work on Diophantine m-tuples in finite fields, I decided to pursue it as not much study has been done on Diophantine m-tuples over any commutative ring with identity and so many more results that might be analogous to the ones in integers can be found. But the downside was dealing with finite fields or commutative rings with identity are usually trickier than dealing with integers.

Studies have been made over the ring of integers in a quadratic field and a cubic field over the years. Recently, Dujella and Kazalicki studied Diophantine m-tuples over finite fields $\mathbb{F}_p$ where p is an odd prime in [DK21]. They proved the existence of a Diophantine m-tuple in $\mathbb{F}_p$ where p is a prime and $p > 2^{2m-2}m^2$. Using character sums, they also derive expressions for the number of Diophantine pairs, triples, and quadruples in $\mathbb{F}_p$ for given prime p, and provide an asymptotic formula for the number of Diophantine m-tuples.

In our work, we defined a new generalization of Diophantine m-tuples called k-Diophantine m-tuples. One of my project mates first had the idea of this generalisation and with the help of the references, we decided to proceed further and decode some properties of them. We define k-Diophantine m-tuples.

Definition 2. Let S be a set of m positive integers $\{a_1, a_2, \ldots, a_m\}$. If $1+\prod_{j=i_1}^{i_k} a_j$ is a perfect square for all $i_1, \ldots, i_k \in \{1, 2, \ldots, m\}$ such that $1 \leq i_1 < i_2 < \cdots < i_k \leq m$, then S is a **k-Diophantine m-tuple**.

Again, we can ask about the motivation behind this study. One motivation behind studying these sets is the relationship between k-Diophantine k-tuples and a well-known problem in number theory known as Brocard's problem. Brocard's problem asks for all integer solutions (n, m) to the

equation $n! + 1 = m^2$. It is clear that if the elements of a k-Diophantine k-tuple are consecutive natural numbers from 1, then it gives a solution for Brocard's problem. Currently, there are only three known pairs of numbers solving Brocard's problem: $(4, 5), (5, 11), (7, 71)$. Erdős conjectured that no other solutions exist.

Another motivation is the connection between 3-Diophantine triples and elliptic curves. Similar to the previous connection, the problem of extending a 3-Diophantine triple $\{a, b, c\}$ to a 3-Diophantine quadruple $\{a, b, c, d\}$ is equivalent to finding integer solutions of the elliptic curve

$$y^2 = (abx + 1)(acx + 1)(bcx + 1). \tag{0.2}$$

Hence, for even the simpler cases of k and m, finding k-Diophantine m-tuples is already of the same complexity and importance as finding integral solutions of an elliptic curve.

Throughout our work in this paper, the primary reference we used was the paper by Dujella and Kazalicki [DK21]. Similar to their study in the paper, we studied k-Diophantine m-tuples in finite fields $\mathbb{F}_p$ where p is an odd prime. Prof. Dujella was also very kind enough to grant us access to his book *Number Theory* [DS21] which was a huge help in understanding Diophantine m-tuple, its history and the various methods used to solve and interpret Diophantine m-tuples over the years. In our paper, we showed the existence of at least one k-Diophantine m-tuple for all primes p that are sufficiently large, and gave a formula for the number of 3-Diophantine triples in $\mathbb{F}_p$. We also gave an asymptotic formula for the number of k-Diophantine k-tuples. I briefly describe here each of our results.

In our search for the existence of a k-Diophantine m-tuple in $\mathbb{F}_p$ we tried a similar idea that was used before to prove the existence of Diophantine m-tuple in $\mathbb{F}_p$ and after doing a few modifications and dirty calculations, we were able to complete the proof. We first proved the theorem for $k = 3$ and then tried to expand and generalise the proof. Here's the statement of the theorem about the existence of k-Diophantine m-tuple in $\mathbb{F}_p$:

Theorem 3. *Let $m \geq k$ be an integer. If $p > 4^{\binom{m}{k-1}+1}\left(\frac{\binom{m}{k-1}}{2} + m + 1\right)^2$ is a prime, then there exists at least one k-Diophantine m-tuple in $\mathbb{F}_p$.*

The number $4^{\binom{m}{k-1}+1}\left(\frac{\binom{m}{k-1}}{2} + m + 1\right)^2$ was the result of a lot of dirty calculations and doesn't hold much importance. We observed that the existence should actually be true for a smaller bound but unfortunately, we couldn't prove it.

Being able to prove the existence made us more confident about our next task: counting k-Diophantine m-tuples. After studying similar results in other papers, we conjectured a formula for counting 3-Diophantine triples. The observations and intuition behind the conjecture were supported by our mentors. To get a verification and also the possibility of getting an insight, one of our project mates, Rowan McKee (California State University, East Bay) designed a computer program for writing the number of 3-Diophantine triples. When we compared the formula with the results obtained computationally, we saw trends that gave us the assurance about the formula's accuracy. Proceeding with the proof, we had three separate summands to work on, out of which one

was trivial, one required the help of certain results on Legendre symbols and the Gauss' Theorem 8 and the third one was dealt like a separate problem we termed as 'counting problem'. The counting problem was proved by using properties of quadratic residues and Euler's criterion about quadratic residues. The statements of the formula for determining number of 3-Diophantine m-tuples and the counting problem are given below:

Theorem 4. *Let $N_3(p)$ be the number of 3-Diophantine triples in $\mathbb{F}_p$. If $p \equiv 1$ mod 3, let a be an integer such that $a \equiv 2$ mod 3 and $p = a^2 + 3b^2$ for some integer $b > 0$. Then,*

$$N_3(p) \;=\; \begin{cases} \frac{a+1}{3} + \binom{p-1}{3}/2, & \text{for } p \equiv 1 \pmod 3 \\ \binom{p-1}{3}/2, & \text{for } p \equiv 2 \pmod 3. \end{cases} \tag{0.3}$$

Theorem 5.

$$\#\left\{(a,b,c) \in \mathbb{F}_p^3 : abc + 1 \equiv 0 \pmod p\right\} \;=\; \begin{cases} (p-2)(p-3)+4, & \text{if } p \equiv 1 \pmod 3 \\ (p-2)(p-3), & \text{if } p \equiv 2 \pmod 3. \end{cases} \tag{0.4}$$

Counting the number of k-Diophantine m-tuples in general is very difficult. Since we studied the formulation of an asymptotic formula for Diophantine m-tuples in finite fields in the paper by Dujella and Kazalicki [DK21], we also tried to see if an asymptotic formula is within reach. Even though we could not a find a wholly successful general formula, we found a formula for the special case: k-Diophantine k-tuples. We used Weil's Theorem 9 for character sums in proving the asymptotic formula.

Theorem 6. *Let $N_k(p)$ be the number of k-Diophantine k-tuples in $\mathbb{F}_p$. Then*

$$N_k(p) \;\sim\; \frac{p^k}{k! \cdot 2} + o(p^k). \tag{0.5}$$

Since the proofs of the above theorems are quite long and need the aid of preliminary results like Gauss' Theorem and Weil's Theorem, we will stick to proving a special case of Theorem 3 (when $k = 3$) in this article. This special case was the first result we proved and it marked the beginning of the research work in our project.

We state the case of Theorem 3 when $k = 3$:

Theorem 7. *Let $m \geq 3$ be an integer. If $p > 2^{m^2-m-2}(m^2+3m+4)^2$ is a prime, then there exists at least one 3-Diophantine m-tuple in $\mathbb{F}_p$.*

Proof. We prove this theorem by induction on m. For $m = 3$ and a prime p such that

$$p \;>\; 2^{3^2-3-2}(3^2+3(3)+4)^2 \;=\; 7744, \tag{0.6}$$

we have the 3-Diophantine triple $\{2, 3, 4\}$ in $\mathbb{F}_p$. Indeed, $p \geq 5$ is large enough to guarantee the existence of this 3-Diophantine triple. Suppose that there exists at least one 3-Diophantine m-tuple in $\mathbb{F}_p$.

Now, we want to prove that there exists a 3-Diophantine $(m+1)$-tuple in $\mathbb{F}_p$ where p is a prime such that $p > 2^{m^2+m-2}(m^2+5m+8)^2$. Let us take a prime p such that

$$\begin{aligned} p &> 2^{(m+1)^2-(m+1)-2}\{(m+1)^2+3(m+1)+4)\}^2 \\ &= 2^{m^2+m-2}(m^2+5m+8)^2. \end{aligned}$$

Clearly, $p > 2^{m^2-m-2}(m^2+3m+4)^2$. Thus, by the induction hypothesis, there exists a 3-Diophantine m-tuple $\{a_1, a_2, \ldots, a_m\}$ in $\mathbb{F}_p$. Define

$$g \coloneqq \#\left\{x \in \mathbb{F}_p : \left(\frac{a_i a_j x+1}{p}\right) = 1 \text{ where } i,j \in \mathbb{Z}, 1 \le i < j \le m\right\} \tag{0.7}$$

$$= \#\left\{x \in \mathbb{F}_p : \left(\frac{x+\overline{a_i}\overline{a_j}}{p}\right) = \left(\frac{\overline{a_i}\overline{a_j}}{p}\right)\right\} \tag{0.8}$$

for all i, j such that $1 \le i < j \le m$, where $\overline{a_i}$ denotes the multiplicative inverse of a_i in $\mathbb{F}_p$. We will prove that $g-(m+1) > 0$, which guarantees that there exists $x \in \mathbb{F}_p, x \notin \{0, a_1, \ldots, a_m\}$ such that $\left(\frac{a_i a_j x+1}{p}\right) = 1$ with $1 \le i < j \le m$. By choosing pairs in $\mathbb{F}_p$ in $\binom{m}{2}$ ways and using exercise 5.64 of [LN97],

$$\begin{aligned} \left|g - \frac{p}{2^{\binom{m}{2}}}\right| &\le \left\{\frac{\binom{m}{2}-2}{2} + \frac{1}{2^{\binom{m}{2}}}\right\}\sqrt{p} + \frac{\binom{m}{2}}{2} \\ g &\ge \frac{p}{2^{\binom{m}{2}}} - \left\{\frac{\binom{m}{2}-2}{2} + \frac{1}{2^{\binom{m}{2}}}\right\}\sqrt{p} - \frac{\binom{m}{2}}{2} \\ &\ge \frac{p}{2^{\frac{m(m-1)}{2}}} - \left(\frac{m(m-1)-4}{4} + \frac{1}{2^{\frac{m(m-1)}{2}}}\right)\sqrt{p} - \frac{m(m-1)}{4}. \end{aligned}$$

Since

$$\begin{aligned} &\left(\frac{m(m-1)}{4} - 1 + \frac{1}{2^{\frac{m(m-1)}{2}}}\right)\sqrt{p} + \frac{m(m-1)}{4} + m + 1 \\ &< \left(\frac{m^2-m}{4} - 1 + \frac{1}{2^{\frac{m(m-1)}{2}}} + \frac{1}{2^{\frac{m(m-1)}{2}+1}}\right)\sqrt{p} \\ &= \left(\frac{m^2-m}{4} - 1 + \frac{3}{2^{\frac{m(m-1)}{2}+1}}\right)\sqrt{p} \\ &< \frac{m(m-1)\sqrt{p}}{4} < \frac{p}{2^{\frac{m(m-1)}{2}}}, \end{aligned}$$

we find, $g > m+1$. So, there exists a 3-Diophantine $(m+1)$-tuple $\{a_1, \ldots, a_m, x\}$ in $\mathbb{F}_p$. □

Personally, I had a wonderful time working on the project. Besides working on the project, I learnt a lot about mathematics and its culture by interacting with my fellow mates and our mentors. It was the first time I tasted the joy of being a mathematician. The challenge that we and all the other students in various projects experienced made me realise that we were incredibly lucky to get a few results on our first research project within a limited time period.

Appendix

Theorem 8 (Gauss' Theorem)**.** *Let $E(\mathbb{F}_p) : y^2 = x^3 + D$ be an elliptic curve. Then for $p \equiv 1 \pmod 3$,*

$$\#E(\mathbb{F}_p) \;=\; \begin{cases} p+1+2a & \text{if } D \text{ is a sextic residue mod } p \\ p+1-2a & \text{if } D \text{ is cubic but not a quadratic residue mod } p \\ p+1-a\pm 3b & \text{if } D \text{ is a quadratic but not a cubic residue mod } p \\ p+1+a\pm 3b & \text{if } D \text{ is neither quadratic nor cubic residue mod } p \end{cases}$$

where a is an integer such that $a \equiv 2 \pmod 3$ and $p = a^2 + 3b^2$ for some integer $b > 0$. For $p \equiv 2 \pmod 3$,

$$\#E(\mathbb{F}_p) \;=\; p+1.$$

Proof. See [IR90, pg. 305, Theorem. 4]. □

Theorem 9 (Weil's Theorem)**.** *Let χ be an n^{th} order non-trivial multiplicative character in the finite field $\mathbb{F}_q$. Let $f(x)$ be a degree d polynomial in $\mathbb{F}_q$ such that $f(x) \neq kg(x)^n$ for any polynomial $g(x)$ and constant k in $\mathbb{F}_q$. Then*

$$\left|\sum_{x\in\mathbb{F}_q} \chi(f(x))\right| \;\leq\; (d-1)\sqrt{q}.$$

Proof. See [IK04, Theorem. 11.23]. □

References

[HKM21] T. Hammonds, S. Kim, S. J. Miller, A. Nigam, K. Onghai, D. Saikia and L. M. Sharma *k*-Diophantine *m*-tuples in Finite Fields. *arXiv*, 2022. `https://arxiv.org/abs/2201.06232`

[AHS79] J. Arkin, V. E. Hoggatt, and E. G. Strauss. On Euler's solution of a problem of Diophantus. *Fibonacci Quart.*, 17(4):333–339, 1979.

[BD69] A. Baker and H. Davenport. The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. *Quart. J. Math. Oxford Ser.*, 20(1):129–137, 1969.

[DK21] A. Dujella and M. Kazalicki. Diophantine m-tuples in finite fields and modular forms. *Research in Number Theory*, 7(3), 2021.

[DS21] A. Dujella. *Number Theory (English Version), translated by P. Švob.* Textbooks of the Universtiy of Zagreb. University of Zagreb, Školska Knjiga, 2021.

[Duj] A. Dujella. Diophantine m-tuples. `https://web.math.pmf.unizg.hr/~duje/dtuples.html`.

[Duj04] A. Dujella. There are only finitely many Diophantine quintuples. *J. Reine Angew. Math.*, 566:183–214, 2004.

[HTZ18] B. He, A. Togbé, and V. Ziegler. There is no Diophantine quintuple. *Transactions of the American Mathematical Society*, 371(9):6665–6709, May 2019.

[IK04] H. Iwaniec and E. Kowalski. *Analytic Number Theory*, page 302. American Mathematical Society Colloquium Publications. American Mathematical Society, 2004.

[IR90] K. Ireland and M. Rosen. *A Classical Introduction To Modern Number Theory*, page 305. Number Volume 84 in Graduate Texts in Mathematics. Springer, 1990.

[LN97] R. Lidl and H. Niederreiter. *Finite Fields.* Number v. 20, pt. 1 in EBL-Schweitzer. Cambridge University Press, 1997.