k-Diophantine m-tuples in finite fields

Trajan Hammonds

Department of Mathematics, Princeton University, USA
trajanh@princeton.edu

Seoyoung Kim

Department of Mathematics and Statistics, Queen's University, Canada
sk206@queensu.ca

Steven J. Miller

Department of Mathematics and Statistics, Williams College, USA
sjm1@williams.edu

Arjun Nigam

University of Arizona, USA
arjunnigam1611@email.arizona.edu

Kyle Onghai

Department of Mathematics, University of California, Los Angeles, 520 Portola Plaza Box 951555, Los Angeles, CA 90095
onghaik@g.ucla.edu

Dishant Saikia

Department of Mathematical Sciences, Tezpur University, Tezpur 784028, India
saikiadishant@gmail.com

Lalit M. Sharma

Dyal Singh College, University of Delhi, Lodhi Road, Pragati Vihar, Delhi 110003, India
sharmalalit1729@gmail.com

In this paper, we define a k-Diophantine m-tuple to be a set of m positive integers such that the product of any k distinct positive integers is one less than a perfect square. We study these sets in finite fields $\mathbb{F}_p$ for odd prime p and guarantee the existence of a k-Diophantine m-tuple provided p is larger than some explicit lower bound. We also give a formula for the number of 3-Diophantine triples in $\mathbb{F}_p$ as well as an asymptotic formula for the number of k-Diophantine k-tuples.

Keywords: Character sums; Diophantine tuples; elliptic curves; finite fields.

Mathematics Subject Classification 2010: 11D45, 11D72

1. Introduction

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 an interesting 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 discovered that the Diophantine quadruple given by Fermat can be extended to form a rational Diophantine quintuple, namely $\left\{1, 3, 8, 120, \frac{777480}{8288641}\right\}$. These sets of numbers studied by Diophantus, Fermat and Euler are now known as **Diophantine m-tuples**, which we define below.

Definition 1.1. 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**. For a more in-depth overview of the history of this problem, see [6, p. 513-519].

The first important result concerning the size of Diophantine m-tuples was given by Baker and Davenport in 1969 [3]. 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 [2]. In 2004, Dujella proved that there is no Diophantine sextuple and that there are at most finitely many Diophantine quintuples [9]. In 2018, He, Togbé and Ziegler showed that there does not exist a Diophantine quintuple [20].

In the case of rationals, no absolute upper bound for the size of rational Diophantine m-tuples is known. Euler proved that there are infinitely many rational Diophantine quintuples. In 1999, Gibbs found the first rational Diophantine sextuple $\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$ [19]. In 2017, Dujella, Kazalicki, Mikić, Szikszai proved that there are infinitely many rational Diophantine sextuples [14]. It is not known whether there are rational Diophantine septuples.

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 $D(n)$*. Recently, Bliznac Trebješanin and Filipin proved that there is no $D(4)$-quintuple [4]. Dujella, Filipin and Fuchs proved that there does not exist a $D(-1)$-quintuple and that there are at most finitely many $D(-1)$-quadruples, all of them containing the element 1 [12,11]. Recently, Bonciocat, Cipu and Mignotte proved the nonexistence of

$D(-1)$-quadruples [5].

There is an interesting connection between Diophantine m-tuples and 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

$$y^2 = (ax + 1)(bx + 1)(cx + 1); \tag{1.1}$$

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. However, for the rationals we have the following characterization:

Lemma 1.2 ([8]). *If (x, y) is a point on the elliptic curve $E : y^2 = (ax + 1)(bx + 1)(cx + 1)$, then x will extend the triple $\{a, b, c\}$ if and only if $(x, y) - P \in 2E(\mathbb{Q})$, where $P = (0, 1)$.*

A more detailed survey on Diophantine m-tuples and its connections with elliptic curves can be found in [7] and [8].

While most of the work on Diophantine m-tuples has been done over integers and rationals, Diophantine m-tuples may be studied over any commutative ring with identity. Studies have been made over the ring of integers in a quadratic field ([16], [15] and [18]) by Franušić and Soldo. In 2013, Franušić also studied Diophantine quadruples over a cubic field [17]. Recently, Dujella and Kazalicki studied Diophantine m-tuples over finite fields $\mathbb{F}_p$ where p is an odd prime in [13]. 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 recent years, there has been a lot of activity on Diophantine m-tuples and its generalizations. To get an extensive list of papers on Diophantine m-tuples, we refer the interested reader to [7]

We study a generalization of Diophantine m-tuples called k-Diophantine m-tuples.

Definition 1.3. Let $S = \{a_1, a_2, \ldots, a_m\} \subseteq R \setminus \{0\}$ where R is a commutative ring with unity 1. 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** over R.

One motivation behind studying these sets is the relationship between k-Diophantine k-tuples and a well-known, open 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 can be clearly observed that if the elements of a k-Diophantine k-tuple are consecutive natural numbers starting 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. In 1993, Overholt proved that there are only finitely many

solutions to Brocard's problem provided that the *abc* conjecture is true [24]. Till now, computations for n up to a magnitude of 10^{15} have been done but yielded no further solutions for the problem.

Moreover, just as Brocard's problem is not a trivial exercise, the same can be said of finding k-Diophantine m-tuples. Similar to the connection between Diophantine triples, i.e., 2-Diophantine triples, and elliptic curves, a connection can also be made between 3-Diophantine triples and elliptic curves. Indeed, 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

$$y^2 = (abx + 1)(acx + 1)(bcx + 1). \tag{1.2}$$

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. As no efficient, general algorithm to find integral solutions of an elliptic curve has been found yet, there is no algorithm to find the number of ways to extend a 3-Diophantine triple to a 3-Diophantine quadruple. In fact, the same can be said about the problem of extending k-Diophantine k-tuples to k-Diophantine $(k + 1)$-tuples. It is worth noting that, unlike the case for Diophantine m-tuples (see Lemma 1.2), there is no if and only if condition for the rational solutions to Equation 1.2 because we cannot guarantee that $x \notin \{a, b, c\}$.

Inspired by the work of Dujella and Kazalicki [13], we studied k-Diophantine m-tuples in finite fields $\mathbb{F}_p$ where p is an odd prime. We show the existence of at least one k-Diophantine m-tuple for all primes p that are sufficiently large, and give a formula for the number of 3-Diophantine triples in $\mathbb{F}_p$.

In Section 2, we provide results that we need to present the proofs of our new results. Next, we show the following theorems.

Theorem 1.4. *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 $\mathbb{F}_p$.*

Then, we prove a theorem about the number of 3-Diophantine triples over $\mathbb{F}_p$.

Theorem 1.5. *Let $N_3(p)$ be the number of 3-Diophantine triples in $\mathbb{F}_p$. If $p \equiv 1 \bmod 3$, let a be an integer such that $a \equiv 2 \bmod 3$ and $p = a^2 + 3b^2$ for some integer $b > 0$. Then,*

$$N_3(p) = \begin{cases} \frac{a+1}{3} + \binom{p-1}{3}/2, & \text{for } p \equiv 1 \pmod 3 \\ \binom{p-1}{3}/2, & \text{for } p \equiv 2 \pmod 3. \end{cases} \tag{1.3}$$

To do this, we need to show the following.

Theorem 1.6. *We have*

$$\#\left\{(a, b, c) \in \mathbb{F}_p^3 : abc + 1 \equiv 0 \pmod p\right\} = \begin{cases} (p-2)(p-3) + 4, & \text{if } p \equiv 1 \pmod 3 \\ (p-2)(p-3), & \text{if } p \equiv 2 \pmod 3 \end{cases} \tag{1.4}$$

where $abc(a-b)(a-c)(b-c) \neq 0$.

Finally, we prove the following asymptotic formula for the number of k-Diophantine k-tuples in $\mathbb{F}_p$ holds.

Theorem 1.7. *Let* $N_k(p)$ *be the number of* k*-Diophantine* k*-tuples in* $\mathbb{F}_p$*. Then*

$$N_k(p) \sim \frac{p^k}{k! \cdot 2} + o(p^k). \tag{1.5}$$

2. Preliminaries

2.1. *Legendre Symbol and Their Sums*

First, let us define an operation from number theory known as the Legendre symbol.

We recall that if $a, p \in \mathbb{Z}$ with p prime, $\gcd(a,p) = 1$, then the **Legendre Symbol**, denoted as $\left(\frac{a}{p}\right)$ is

$$\left(\frac{a}{p}\right) \coloneqq \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases} \tag{2.1}$$

Note: In the finite field F_p where p is an odd prime, the Legendre symbol is equivalent to the quadratic character [23, p. 191].

In determining the formula for the number of 3-Diophantine triples in $\mathbb{F}_p$, we relied on two well-known sums of Legendre symbols. Consider a given polynomial f with integer coefficients. The two well-known sums are special cases of the sum

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right). \tag{2.2}$$

If f is linear, then we have the following result.

Lemma 2.1. *For arbitrary integers* a *and* b*, and a prime* $p \nmid a$*, we have*

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = 0. \tag{2.3}$$

Proof. See Lemma Appendix A.1. □

If f is quadratic, then we have this next result.

Lemma 2.2. *For arbitrary integers* a, b, c*, and a prime* p *such that* $p \nmid a$*, then*

$$\sum_{x=0}^{p-1} \left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2 - 4ac \\ -\left(\frac{a}{p}\right) & \text{otherwise.} \end{cases} \tag{2.4}$$

Proof. See Lemma Appendix A.2. □

2.2. *Gauss's Lemma*

Theorem 2.3. (Gauss) *Let $E(\mathbb{F}_p) : y^2 = x^3 + D$ be an elliptic curve. Then for $p \equiv 1$ mod 3*

$$\#E(\mathbb{F}_p) \;=\; \begin{cases} p+1+2a & \text{if } D \text{ is a sextic residue mod } p \\ p+1-2a & \text{if } D \text{ is cubic but not a quadratic residue mod } p \\ p+1-a\pm 3b & \text{if } D \text{ is a quadratic but not a cubic residue mod } p \\ p+1+a\pm 3b & \text{if } D \text{ is neither quadratic nor cubic residue mod } p \end{cases} \tag{2.5}$$

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

$$\#E(\mathbb{F}_p) \;=\; p+1. \tag{2.6}$$

Proof. See [21, p. 305, Thm. 4]. □

2.3. *Weil's Theorem and Quadratic Character Sums*

We first state Weil's theorem for the estimation of character sums; we require this result for the proof of Lemma 2.5.

Theorem 2.4 (Weil). *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*

$$\left|\sum_{x\in\mathbb{F}_q} \chi(f(x))\right| \;\leq\; (d-1)\sqrt{q}. \tag{2.7}$$

Proof. c.f. [22, Thm. 11.23]. □

Lemma 2.5 is needed in the proof of Lemma 2.6.

Lemma 2.5 ([23, Ex. 5.63]). *Let $a_1, \ldots, a_k$ be distinct elements of $\mathbb{F}_q$, q odd, and let $\epsilon_1, \ldots, \epsilon_k$ be k given integers, each of which is 1 or -1. Let $N(\epsilon_1, \ldots, \epsilon_k)$ denote the number of $c \in \mathbb{F}_q$ with $\eta(c + a_j) = \epsilon_j$ for $1 \leq j \leq k$, where η is the quadratic character of $\mathbb{F}_q$. Then*

$$N(\epsilon_1, \ldots, \epsilon_k) \;=\; \frac{1}{2^k} \sum_{c\in\mathbb{F}_q} [1 + \epsilon_1\eta(c + a_1)] \cdots [1 + \epsilon_k\eta(c + a_k)] - A, \tag{2.8}$$

where $0 \leq A \leq k/2$ and $A \in \mathbb{R}$.

Proof. See Lemma Appendix A.3. □

The final result we present in this section is necessary to prove the existence of k-Diophantine m-tuples in Subsection 3.1.

Lemma 2.6 ([23, Ex. 5.64]). *We have*

$$\left|N(\epsilon_1,\ldots,\epsilon_k)-\frac{q}{2^k}\right| \ \leq \ \left(\frac{k-2}{2}+\frac{1}{2^k}\right)q^{1/2}+\frac{k}{2}. \tag{2.9}$$

Proof. See Lemma Appendix A.4. □

We now proceed to the main results of this paper. First, we will prove that for all sufficiently large odd primes p, there exists at least one k-Diophantine m-tuple in $\mathbb{F}_p$.

3. Proofs of the main results

3.1. *Existence of k-Diophantine m-tuples*

Here, we prove that k-Diophantine m-tuples exist for a large enough prime. First, we establish the case when $k=3$.

Theorem 3.1. *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

$$p \ > \ 2^{3^2-3-2}(3^2+3(3)+4)^2 \ = \ 7744, \tag{3.1}$$

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

$$\begin{aligned} g \coloneqq \ &\#\left\{x\in\mathbb{F}_p : \left(\frac{a_ia_jx+1}{p}\right) \ = \ 1 \text{ where } i,j\in\mathbb{Z}, 1\leq i<j\leq m\right\} \\ =\ &\#\left\{x\in\mathbb{F}_p : \left(\frac{x+\overline{a_ia_j}}{p}\right) \ = \ \left(\frac{\overline{a_ia_j}}{p}\right)\right\} \end{aligned}$$

for all i, j such that $1\leq i<j\leq m$, 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 $1 \leq i < j \leq m$. By choosing pairs in $\mathbb{F}_p$ in $\binom{m}{2}$ ways and using Lemma 2.6,

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

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 $\mathbb{F}_p$. □

We now consider the same question for arbitrary k.

Theorem 1.4. *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 $\mathbb{F}_p$.*

Proof. We first prove the existence of a k-Diophantine k tuple in $\mathbb{F}_p$ by using induction on k. Then we proceed to prove the theorem by using induction on m. The base case in the induction process of m is the case when $m = k$ i.e the existence of a k-Diophantine k-tuple which we would have already proved.

Now, we prove that there exists a k-Diophantine k-tuple for $p > 4^k(3k+2)^2$. We prove this result by induction on $k \geq 2$. For $p > 1024$ and $k = 2$, we get the Diophantine pair $\{1, 3\}$ in $\mathbb{F}_p$.

Assume the statement holds for $k \geq 2$. We consider a prime $p > 4^{k+1}(3k+5)^2$. Since $p > 4^k(3k+2)^2$, there exists a k-Diophantine k-tuple $\{a_1, a_2, \ldots, a_k\}$ in $\mathbb{F}_p$. Let

$$g \coloneqq \#\left\{ x \in \mathbb{F}_p : \left(\frac{a_1 a_2 \ldots a_k x + 1}{p} \right) = 1 \right\}. \tag{3.2}$$

Let $\overline{a_i}$ denote the multiplicative inverse of a_i in $\mathbb{F}_p$. By Lemma 2.6,

$$\begin{aligned} g &= \#\left\{x \in \mathbb{F}_p : \left(\frac{x + \overline{a_1 a_2 \dots a_k}}{p}\right) = \left(\frac{\overline{a_1 a_2 \dots a_k}}{p}\right)\right\} \\ &\geq \frac{p}{2^{\binom{k}{k}}} - \left(\frac{\binom{k}{k} - 2}{2} + \frac{1}{2^{\binom{k}{k}}}\right)\sqrt{p} - \frac{\binom{k}{k}}{2} \\ &= \frac{p-1}{2} \\ &> k+1 \text{ for } p > 4^{k+1}(3k+5)^2. \end{aligned}$$

So, there exists at least one $x \in \mathbb{F}_p$ such that $\left(\frac{a_1 a_2 \dots a_k x + 1}{p}\right) = 1$ and hence we get a $(k+1)$-Diophantine $(k+1)$-tuple $\{a_1, a_2, \dots, a_k, x\}$ in $\mathbb{F}_p$. Thus, there exists a k-Diophantine k-tuple in $\mathbb{F}_p$ where $p > 4^k(3k+2)^2$ and $k \geq 2$. Therefore, the base case for the induction proof holds.

Let us now assume there exists at least one k-Diophantine m-tuple in $\mathbb{F}_p$ for $p > 4^{\binom{m}{k-1}+1}\left(\frac{\binom{m}{k-1}}{2} + m + 1\right)^2$. Now, we want to prove that there exists a k-Diophantine $(m+1)$-tuple in $\mathbb{F}_p$ where p is a prime such that $p > 4^{\binom{m+1}{k-1}+1}\left(\frac{\binom{m+1}{k-1}}{2} + m + 2\right)^2$. By the induction hypothesis, since $p > 4^{\binom{m}{k-1}+1}\left(\frac{\binom{m}{k-1}}{2} + m + 1\right)^2$, there exists a k-Diophantine m-tuple $\{a_1, a_2, \dots, a_m\}$ in $\mathbb{F}_p$. Define

$$g \coloneqq \#\left\{x \in \mathbb{F}_p : \left(\frac{a_{i_1} a_{i_2} \dots a_{i_{k-1}} x + 1}{p}\right) = 1\right\} \tag{3.3}$$

where $a_{i_1}, a_{i_2}, \dots, a_{i_{k-1}} \in \{a_1, a_2, \dots, a_m\}$. Let $\overline{a_i}$ denote the multiplicative inverse of a_i in $\mathbb{F}_p$.
By Lemma 2.6,

$$\begin{aligned} g &= \#\left\{x \in \mathbb{F}_p : \left(\frac{x + \overline{a_{i_1} a_{i_2} \dots a_{i_{k-1}}}}{p}\right) = \left(\frac{\overline{a_{i_1} a_{i_2} \dots a_{i_{k-1}}}}{p}\right)\right\} \\ &\geq \frac{p}{2^{\binom{m}{k-1}}} - \left(\frac{\binom{m}{k-1} - 2}{2} + \frac{1}{2^{\binom{m}{k-1}}}\right)\sqrt{p} - \frac{\binom{m}{k-1}}{2}. \end{aligned}$$

Now, we also see that $p > 4^{\binom{m}{k-1}+1}\left(\frac{\binom{m}{k-1}}{2} + m + 1\right)^2$ gives

$$\frac{\binom{m}{k-1}}{2} + m + 1 < \frac{\sqrt{p}}{2^{\binom{m}{k-1}+1}}. \tag{3.4}$$

Using (3.4), we get

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

Hence, we have $g > m+1$. Thus, there exists an $x \in \mathbb{F}_p, x \notin \{0, a_1, \ldots, a_m\}$ such that

$$\left(\frac{a_{i_1}a_{i_2}\ldots a_{i_{k-1}}x+1}{p}\right) = 1$$

where $a_{i_1}, a_{i_2}, \ldots, a_{i_{k-1}} \in \{a_1, a_2, \ldots, a_m\}$. So, there exists a k-Diophantine $(m+1)$-tuple $\{a_1, \ldots, a_m, x\}$ in $\mathbb{F}_p$. □

3.2. *Counting 3-Diophantine Triples*

A natural question to ask is exactly how many such k-Diophantine m-tuples exist for a given (k, m). The following result gives an answer for a special case.

Theorem 1.5. *Let $N_3(p)$ be the number of 3-Diophantine triples in $\mathbb{F}_p$. If $p \equiv 1 \bmod 3$, let a be an integer such that $a \equiv 2 \bmod 3$ and $p = a^2 + 3b^2$ for some integer $b > 0$. Then,*

$$N_3(p) = \begin{cases} \frac{a+1}{3} + \binom{p-1}{3}/2, & \text{for } p \equiv 1 \pmod 3 \\ \binom{p-1}{3}/2, & \text{for } p \equiv 2 \pmod 3. \end{cases} \tag{1.3}$$

Indeed, when we compare this formula with the results obtained computationally, we see trends in Table 1 and Figure 1 (in Appendix B) that give us some initial confidence in the formula's accuracy.

However, before giving the proof, we need some other results.

3.2.1. *Counting Problems*

In this subsection, we provide some lemmas that are needed to prove Theorem 1.5.

Lemma 3.2. *Let p be a prime and let $p \neq 2$. We have*

$$\#\left\{(a,b) \in \mathbb{F}_p^2 : a \neq b, ab+1 = 0 \pmod p\right\} = \begin{cases} p-3, & \text{if } p \equiv 1 \pmod 4 \\ p-1, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{3.5}$$

Proof. First, we solve the problem without the condition that $a \neq b$. As $\mathbb{F}_p$ is a field, for each $a \in \mathbb{F}_p \setminus \{0\}$ there exists a unique $a^{-1} \in \mathbb{F}_p$ such that $aa^{-1} = 1$. Hence, for each $a \in \mathbb{F}_p$, take $b = -a^{-1}$. It follows from this definition that $ab \equiv -1 \pmod{p}$. Since each b is unique for fixed a, there are exactly $p-1$ pairs $(a,b) \in \mathbb{F}_p^2$ such that $ab + 1 = 0$.

Now, with the condition $a \neq b$, notice that we need only find the odd primes p for which -1 is a quadratic residue. In other words, we wish to find when $\left(\frac{-1}{p}\right) = 1$ where $\left(\frac{a}{b}\right)$ is the Legendre symbol. By Euler's Criterion, this is equivalent to asking when $(-1)^{\frac{p-1}{2}} = 1$. This implies that -1 is a quadratic residue modulo p if and only if $\frac{p-1}{2}$ is even. Since $\frac{p-1}{2}$ is even when $p \equiv 1 \pmod 4$ and odd when $p \equiv 3 \pmod 4$, we have

$$\#\left\{(a,b) \in \mathbb{F}_p^2 : a \neq b, ab + 1 = 0 \pmod p\right\} = \begin{cases} p-3, & \text{if } p \equiv 1 \pmod 4 \\ p-1, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{3.6}$$

□

Theorem 1.6. *We have*

$$\#\left\{(a,b,c) \in \mathbb{F}_p^3 : abc + 1 \equiv 0 \pmod p\right\} = \begin{cases} (p-2)(p-3)+4, & \text{if } p \equiv 1 \pmod 3 \\ (p-2)(p-3), & \text{if } p \equiv 2 \pmod 3 \end{cases} \tag{1.4}$$

where $abc(a-b)(a-c)(b-c) \neq 0$.

Proof. We want to find

$$\sum_{l \in \mathbb{F}_p \setminus \{0\}} \#\left\{(a,b) \in \mathbb{F}_p^2 : \substack{ab \equiv l \pmod p \\ abc(a-b)(a-c)(b-c) \neq 0}\right\}.$$

If l is a quadratic residue modulo p, then there are two pairs (a,b) such that $ab = l$ and a, b are not distinct, for if $a = b = x$ is one such pair then $a = b = -x$ is the other pair. So, if l is a quadratic residue, then there are $p-3$ pairs. On the other hand, if l is a quadratic non-residue modulo p, then there are $p-1$ pairs such that $ab = l$ and a, b are distinct. Thus, we have that

$$\begin{aligned} \#\left\{(a,b) \in \mathbb{F}_p^2 : ab \equiv l \pmod p\right\} &= (p-1)\frac{p-1}{2} + (p-3)\frac{p-1}{2} \\ &= (p-1)(p-2). \end{aligned}$$

However, the theorem statement asks a slightly different question. Now, we must consider when $c = a$ or $c = b$.

Case 1. $p \equiv 2 \pmod 3$ We want to show that there are $\frac{p+1}{2}$ residues l for which there are $p-3$ distinct triples (a,b,c) and $\frac{p-3}{2}$ residues l for which there

are $p-5$ distinct triples (a,b,c). This would imply that, for $p \equiv 2 \pmod 3$,

$$\begin{aligned} \#\left\{(a,b,c) \in \mathbb{F}_p^3 : abc+1 \equiv 0 \pmod p\right\} &= (p-3)\frac{p+1}{2} + (p-5)\frac{p-3}{2} \\ &= (p-2)(p-3). \end{aligned}$$

The residues for which there are $p-5$ solutions satisfy $ab \equiv a^2 \equiv l \pmod p$ but not $abc \equiv a^3 \equiv -1 \pmod p$. In this case, there are two pairs such that $a = b$ and $ab \equiv l \pmod p$, i.e., (a,a) and $(-a,-a)$, and two pairs such that either $b = c$ and $abc \equiv ab^2 \equiv -1 \pmod p$ or $a = c$ and $abc \equiv a^2 b \equiv -1$. Hence, we have $p-1-4 = p-5$ solutions. We know there are $\frac{p-3}{2}$ such residues by Euler's Criterion.

The residues, l, for which there are $p-3$ solutions either do not satisfy $ab \equiv a^2 \equiv l \pmod p$ or contain a pair that forms a solution of $abc \equiv a^3 \equiv -1 \pmod p$ when extended by c. First, we restrict ourselves to the quadratic non-residues. There exist pairs (a,c) or (b,c), $a \neq b$ such that either $b = c$ and $abc \equiv -1 \pmod p$ or $a = c$ and $abc \equiv -1$. Since l is a quadratic non-residue, $a \neq b$. We know there are $\frac{p-1}{2}$ such quadratic non-residues. Now, for the cubic residues of -1, there are $q = \gcd(3, p-1)$ solutions to the congruence $x^3 \equiv -1 \pmod p$ by Euler's criterion. For $p \equiv 2 \pmod 3$, $q = 1$. Thus, there are $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ residues with $p-3$ solutions to $abc + 1 \equiv 0 \pmod p$.

Case 2. $p \equiv 1 \pmod 3$ In this case, instead of there being exactly 1 solution to $x^3 \equiv -1 \pmod p$, there are $q = \gcd(3, p-1) = 3$ solutions. So, there are $\frac{p-1}{2} + 3 = \frac{p+5}{2}$ residues for which there are $p-3$ triples satisfying $abc + 1 \equiv 0 \pmod p$, and $\frac{p-1}{2} - 3 = \frac{p-7}{2}$ residues for which there are $p-5$ triples satisfying $abc + 1 \equiv 0 \pmod p$. Thus,

$$\begin{aligned} \#\left\{(a,b,c) \in \mathbb{F}_p^3 : abc+1 \equiv 0 \pmod p\right\} &= (p-3)\frac{p+5}{2} + (p-5)\frac{p-7}{2} \\ &= (p-2)(p-3) + 4. \end{aligned}$$

□

Now we present the proof of Theorem 1.5.

Proof. We have

$$12N_3(p) = \sum \left(1 + \left(\frac{abc+1}{p}\right)'\right) \tag{3.7}$$

where the sum is evaluated over non-zero and distinct a, b, c, and we have defined $\left(\frac{a}{p}\right)' = \left(\frac{a}{p}\right)$ for $a \neq 0$ and $\left(\frac{a}{p}\right)' = 1$ for $a = 0$. Hence

$$\begin{aligned} 12N_3(p) &= \sum_{c \neq 0} \sum_{b \neq 0, c} \sum_{a \neq 0, b, c} 1 \\ &\quad + \sum_{c \neq 0} \sum_{b \neq 0, c} \sum_{a \neq 0, b, c} \left(\frac{abc+1}{p}\right) + \#\left\{(a,b,c) \in \mathbb{F}_p^3 : abc+1 \equiv 0 \pmod p\right\}. \end{aligned}$$

The first summand will just be $(p-1)(p-2)(p-3)$, and by Lemma 1.6 we already have the solution for the final summand. We use Lemmas 2.1 and 2.2 to evaluate the middle sum:

$$\sum_{c\neq 0}\sum_{b\neq 0,c}\sum_{a\neq 0,b,c}\left(\frac{abc+1}{p}\right) = -\sum_{c\neq 0}\sum_{b\neq 0,c}\left(\frac{1}{p}\right)+\left(\frac{b^2c+1}{p}\right)+\left(\frac{bc^2+1}{p}\right). \quad (3.8)$$

This gives

$$\begin{aligned}-\sum_{c\neq 0}\sum_{b\neq 0,c}1+\left(\frac{b^2c+1}{p}\right)+\left(\frac{bc^2+1}{p}\right) &= -\sum_{c\neq 0}(p-4)-2\left(\frac{c^3+1}{p}\right)\\ &= -(p-1)(p-4)+2\sum_{c\neq 0}\left(\frac{c^3+1}{p}\right).\end{aligned}$$

Using Theorem 2.3, we can evaluate the sum $\sum_{c\neq 0}\left(\frac{c^3+1}{p}\right)$. In particular we get

$$\sum_{c\neq 0}\left(\frac{c^3+1}{p}\right) = \begin{cases}2a-1 & \text{for } p\equiv 1 \pmod 3\\ -1 & \text{for } p\equiv 2 \pmod 3\end{cases}$$

$$\implies \sum_{c\neq 0}\sum_{b\neq 0,c}\sum_{a\neq 0,b,c}\left(\frac{abc+1}{p}\right) = \begin{cases}-(p-2)(p-3)+4a & \text{for } p\equiv 1 \pmod 3\\ -(p-2)(p-3) & \text{for } p\equiv 2 \pmod 3.\end{cases}$$

Combining this with the result from Theorem 1.6 we get the claim. □

As one might imagine, counting k-Diophantine k-tuples for a general k is not that simple due to the complexity of the following problem:

What are the total number of k-tuples $\{a_1, a_2, \ldots, a_k\}$ such that a_i are all distinct, non-zero and

$$\prod_{i=1}^{k} a_i + 1 \equiv 0 \bmod \text{p?} \quad (3.9)$$

3.3. *Asymptotic Formula*

While a general formula of the number of k-Diophantine k-tuples is difficult, an asymptotic formula is well within reach. We describe the formula in the following result.

Theorem 1.7. *Let $N_k(p)$ be the number of k-Diophantine k-tuples in $\mathbb{F}_p$. Then*

$$N_k(p) \sim \frac{p^k}{k!\cdot 2}+o(p^k). \quad (1.5)$$

Proof. We know that

$$k!\cdot 2\cdot N_k(p) = \sum\left(1+\left(\frac{1+a_1a_2\ldots a_k}{p}\right)'\right) \quad (3.10)$$

where the sum is taken over distinct and non-zero $a_1, a_2, \ldots, a_k$ and we have defined $\left(\frac{a}{p}\right)' = \left(\frac{a}{p}\right)$ for $a \neq 0$ and $\left(\frac{a}{p}\right)' = 1$ for $a = 0$ as before. The main term is $\sum 1 = (p-1)(p-2)\ldots(p-k) = p^k + o(p^k)$. Now

$$\sum \left(\frac{1+a_1a_2\ldots a_k}{p}\right)' = \sum \left(\frac{1+a_1a_2\ldots a_k}{p}\right) + \# \left\{(a_1, a_2, \ldots, a_k) \in \mathbb{F}_p^k : \prod_{i=1}^{k} a_i + 1 \equiv 0 \pmod{p}\right\}.$$

Using Weil's estimate for character sums (Theorem 2.4), we note that

$$\sum \left(\frac{1+a_1a_2\ldots a_k}{p}\right) \leq p^{k-1}\sqrt{p}. \tag{3.11}$$

We also note that

$$\# \left\{(a_1, a_2, \ldots, a_k) \in \mathbb{F}_p^k : \prod_{i=1}^{k} a_i + 1 \equiv 0 \pmod{p}\right\} \leq (p-1)^{k-1}. \tag{3.12}$$

Hence

$$\sum \left(\frac{1+a_1a_2\ldots a_k}{p}\right)' = o(p^k). \tag{3.13}$$

The result follows. □

4. Concluding remarks

In this paper, we attempted to answer two fundamental questions about k-Diophantine m-tuples:

(1) Given a sufficiently large prime p, is there always a k-Diophantine m-tuple in $\mathbb{F}_p$?
(2) Can we count the number of k-Diophantine m-tuples in $\mathbb{F}_p$ for a given prime p?

We give complete answer to (1) in Theorem 1.4. While we were unable to answer (2) for an arbitrary pair (k, m), we were able to come up with an asymptotic formula for the number of k-Diophantine k-tuples for any k (Theorem 1.7) and an explicit formula for $(k, m) = (3, 3)$ (Theorem 1.5).

Some questions asked for the usual Diophantine m-tuples can be asked for k-Diophantine m-tuples as well. For instance,

(1) Can we find a formula that, for a given n, allows us to count the number of k-Diophantine m-tuples with property $D(n)$, i.e. the set where k-wise products of distinct elements is n less than a perfect square? What about about n less than the t-th power?
(2) What can be said about the existence of such tuples in other commutative rings with unity, like Gaussian integers, integers, p-adic integers, polynomial rings etc?

Acknowledgements

This project was done as a part of the Polymath Jr. Program, a virtual undergraduate research program, during the summer 2021. We especially would like to thank the organizers of the Polymath Jr. Program to provide valuable experience during the COVID-19 pandemic. We would like to thank Professor Andrej Dujella for graciously granting us access to his book *Number Theory* [8], and Rowan Mckee for writing the computer program for calculating the number of 3-Diophantine triples.

Appendix A. Proofs from the Preliminaries

For completeness we include proofs of some standard results about sums of Legendre symbols.

Lemma Appendix A.1. *For arbitrary integers a and b, and a prime $p \nmid a$, we have*

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p} \right) \;=\; 0.. \tag{A.1}$$

Proof. As $p \nmid a$, $ax+b$ forms a complete set of residues modulo p as x runs through the integers 0 to $p-1$. Every such set contains $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues. Hence,

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p} \right) \;=\; \frac{p-1}{2} - \frac{p-1}{2} \;=\; 0. \tag{A.2}$$

□

Lemma Appendix A.2. *For arbitrary integers a, b, c, and a prime p such that $p \nmid a$, then*

$$\sum_{x=0}^{p-1} \left(\frac{ax^2+bx+c}{p} \right) \;=\; \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2-4ac \\ -\left(\frac{a}{p}\right) & \text{otherwise.} \end{cases} \tag{A.3}$$

Proof. Notice that this sum is equivalently written as

$$\begin{aligned} \left(\frac{4a}{p}\right) \sum_{x=0}^{p-1} \left(\frac{4a^2x^2+4abx+4ac}{p} \right) \;&=\; \left(\frac{a}{p}\right) \sum_{x=0}^{p-1} \left(\frac{(2ax+b)^2-(b^2-4ac)}{p} \right) \\ &=\; \left(\frac{a}{p}\right) S, \end{aligned}$$

where $S = \sum_{x=0}^{p-1} \left(\frac{(2ax+b)^2-(b^2-4ac)}{p} \right)$.

Since the numbers $ax+b$ form a complete set of residues modulo p as x varies from 0 to $p-1$, we have

$$S \;=\; \sum_{l=0}^{p-1}\left(\frac{l^2-(b^2-4ac)}{p}\right). \tag{A.4}$$

It is well known that $S \equiv -1 \pmod{p}$ and $|S| \leq p$ [1, Ex. 10.10]. From this, we obtain $S = -1, p-1$. If $S = p-1$, then $p-1$ terms in S must take the value 1 and there is exactly one term, i.e., when $l = l'$, that equals 0. As this l' must satisfy both $p \mid {l'}^2-(b^2-4ac)$ and $p \mid (-l')^2-(b^2-4ac)$, it follows that $l'=0$ and $p \mid b^2-4ac$. Conversely, if $p \mid b^2-4ac$, then

$$S \;=\; \sum_{l=0}^{p-1}\left(\frac{l^2}{p}\right) \;=\; 0+1\cdot p-1 \;=\; p-1. \tag{A.5}$$

Hence, $S=-1$ if and only if $p \nmid b^2-4ac$. Thus,

$$\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right) \;=\; \begin{cases}(p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2-4ac\\ -\left(\frac{a}{p}\right) & \text{otherwise.}\end{cases} \tag{A.6}$$

□

Lemma Appendix A.3 ([23, Ex. 5.63]). *Let $a_1,\ldots,a_k$ be distinct elements of $\mathbb{F}_q$, q odd, and let $\epsilon_1,\ldots,\epsilon_k$ be k given integers, each of which is 1 or -1. Let $N(\epsilon_1,\ldots,\epsilon_k)$ denote the number of $c \in \mathbb{F}_q$ with $\eta(c+a_j)=\epsilon_j$ for $1 \leq j \leq k$, where η is the quadratic character of $\mathbb{F}_q$. Then*

$$N(\epsilon_1,\ldots,\epsilon_k) \;=\; \frac{1}{2^k}\sum_{c\in\mathbb{F}_q}[1+\epsilon_1\eta(c+a_1)]\cdots[1+\epsilon_k\eta(c+a_k)]-A, \tag{A.7}$$

where $0 \leq A \leq k/2$ and $A \in \mathbb{R}$.

Proof. Notice that, for fixed c, if $\eta(c+a_j)=\epsilon_j$, then $\epsilon_j\eta(c+a_j)=1$; otherwise, $\epsilon_j\eta(c+a_j)=-1$ for $c+a_j \neq 0$ or $\eta(c+a_j)=0$. This implies that, if $\eta(c+a_j)=\epsilon_j$ for all $j \in \mathbb{N}$ such that $1 \leq j \leq k$ and c fixed, then

$$[1+\epsilon_1\eta(c+a_1)]\cdots[1+\epsilon_k\eta(c+a_k)] \;=\; 2^k. \tag{A.8}$$

Otherwise,

$$[1+\epsilon_1\eta(c+a_1)]\cdots[1+\epsilon_k\eta(c+a_k)] \;=\; 0 \tag{A.9}$$

if $\epsilon_i\eta(c+a_i)=-1$ for some $i \in \mathbb{N}$ such that $1 \leq i \leq k$, or

$$[1+\epsilon_1\eta(c+a_1)]\cdots[1+\epsilon_k\eta(c+a_k)] \;=\; 2^{k-1} \tag{A.10}$$

if $\epsilon_i\eta(c+a_i)=0$ for some $i\in\mathbb{N}$ and $\eta(c+a_j)=1$ for all $j\neq i$. Note that there is at most one a_i with the property that $\eta(c+a_i)=0$ since $a_1,\ldots,a_k$ are distinct and c is constant. Thus, we have

$$N(\epsilon_1,\ldots,\epsilon_k) \;=\; \frac{1}{2^k}\sum_{c\in\mathbb{F}_q}[1+\epsilon_1\eta(c+a_1)]\cdots[1+\epsilon_k\eta(c+a_k)]-A, \tag{A.11}$$

where $0\leq A\leq k/2$. □

Lemma Appendix A.4 ([23, Ex. 5.64]). *We have*

$$\left|N(\epsilon_1,\ldots,\epsilon_k)-\frac{q}{2^k}\right| \;\leq\; \left(\frac{k-2}{2}+\frac{1}{2^k}\right)q^{1/2}+\frac{k}{2}. \tag{A.12}$$

Proof. First, we expand the product in the expression for $N(\epsilon_1,\ldots,\epsilon_k)$ given above.

$$\begin{aligned}[1+\epsilon_1\eta(c+a_1)]\cdots[1+\epsilon_k\eta(c+a_k)] \;=\; 1+&\sum_{i=1}^{k}\epsilon_i\eta(c+a_i)+\sum_{j\neq i}^{k}\sum_{i=1}^{k}\epsilon_i\epsilon_j\eta(c+a_i)\eta(c+a_j)\\ &+\cdots+\epsilon_1\epsilon_2\cdots\epsilon_k\eta(c+a_1)\eta(c+a_2)\cdots\eta(c+a_k). \end{aligned}\tag{A.13}$$

By the multiplicative nature of the quadratic character, A.13 is equivalent to

$$\begin{aligned}&1+\sum_{i=1}^{k}\epsilon_i\eta(c+a_i)\\ &+\sum_{j\neq i}^{k}\sum_{i=1}^{k}\epsilon_i\epsilon_j\eta[(c+a_i)(c+a_j)]+\cdots+\epsilon_1\epsilon_2\cdots\epsilon_k\eta[(c+a_1)(c+a_2)\cdots(c+a_k)].\end{aligned}$$

We see that the product expands into a sum of quadratic characters of functions in c of various degrees. More specifically, we find that there are $\binom{k}{i}$ functions of degree i where $1\leq i\leq k$. By Theorem 2.4, we can show that

$$\begin{aligned}\left|\sum_{c\in\mathbb{F}_q}\sum_{d=1}^{k}\eta(f_d(x))\right| \;&\leq\; \sum_{d=1}^{k}\binom{k}{d}(d-1)\sqrt{q}\\ &=\; \sqrt{q}\left(\sum_{d=1}^{k}\binom{k}{d}d-\sum_{d=1}^{k}\binom{k}{d}\right)\\ &=\; \left(k2^{k-1}-2^{k-1}\right)\sqrt{q},\end{aligned}$$

where f_d are all the functions of degree d for which the quadratic character is evaluated. It follows that

$$\left|N(\epsilon_1,\ldots,\epsilon_k)-\frac{q}{2^k}\right|\leq\left(\frac{k-2}{2}+\frac{1}{2^k}\right)q^{1/2}+\frac{k}{2}. \tag{A.14}$$

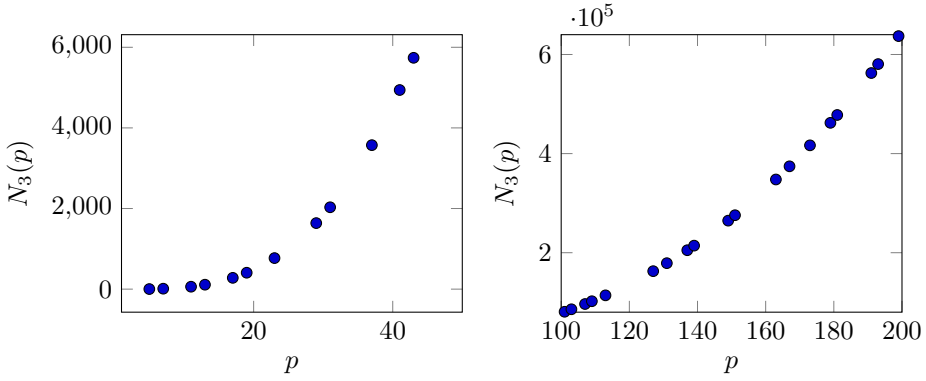
□

Appendix B. Tables and Graphs

The tables and graphs shown are shown here to offer some computational verification of the formula presented in Theorem 1.5 and demonstrate what the program we used is capable of. As the formula predicts, we see in Table 1 and Figure 1 a positive quadratic trend in the number of 3-Diophantine triples against the size of $\mathbb{F}_p$. The reason we decided not to plot values of p past 200 was the computational cost of doing so and that one can see this trend for $p < 300$. The program was not only able to give the number of k-Diophantine m-tuples in $\mathbb{F}_p$, but also the explicit m-tuples themselves, as seen in Table 2.

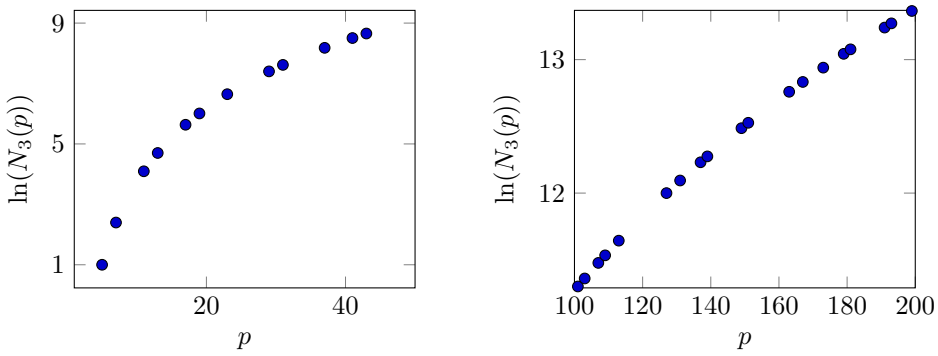
Table 1: Number of 3-Diophantine triples in $\mathbb{F}_p$ for various primes p.

p	$p \equiv 1, 2 \pmod 3$	$N_3(p)$	a (if $p \equiv 1 \pmod 3$)	Error term $(a+1)/3$
5	2	2	-	-
7	1	11	2	1
11	2	60	-	-
13	1	110	-1	0
17	2	280	-	-
19	1	407	-4	-1
23	2	770	-	-
29	2	1638	-	-
31	1	2031	2	1
37	1	3572	5	2
41	2	4940	-	-
43	1	5739	-4	-1
101	2	80850	-	-
229	1	97472	11	4



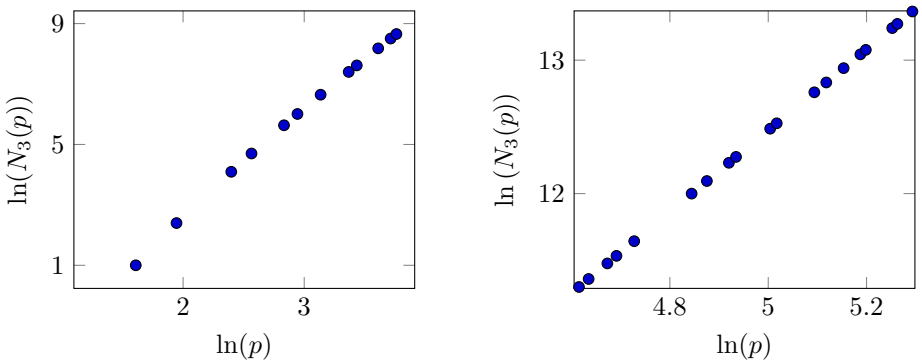
(a) $1 \leq p \leq 50$. (b) $100 \leq p \leq 200$.

Fig. 1: Graph of number of 3-Diophantine triples in $\mathbb{F}_p$ for various p.



(a) Semi-log graph for (small) p. (b) Semi-log graph for (large) p.

Fig. 2: Semi-log graph of Number of 3-Diophantine triples in $\mathbb{F}_p$ for various p.



(a) Graph for $0 < p < 50$.

(b) Graph for $100 < p < 200$.

Fig. 3: Log-log graph of number of 3-Diophantine triples in $\mathbb{F}_p$ for various p.

Table 2: List of all 3-Diophantine Quadruples in $\mathbb{F}_{23}$.

(1, 2, 4, 6)	(1, 2, 4, 20)	(1, 2, 6, 14)	(1, 2, 11, 12)	(1, 2, 13, 15)
(1, 2, 13, 19)	(1, 2, 15, 20)	(1, 2, 17, 19)	(1, 2, 19, 20)	(1, 3, 4, 10)
(1, 3, 4, 21)	(1, 3, 5, 8)	(1, 3, 8, 15)	(1, 3, 15, 18)	(1, 3, 16, 19)
(1, 3, 17, 19)	(1, 3, 19, 21)	(1, 4, 6, 12)	(1, 4, 7, 20)	(1, 4, 10, 21)
(1, 4, 17, 18)	(1, 4, 17, 21)	(1, 4, 19, 20)	(1, 5, 6, 9)	(1, 5, 6, 20)
(1, 5, 8, 9)	(1, 5, 16, 19)	(1, 6, 8, 20)	(1, 6, 9, 21)	(1, 6, 12, 21)
(1, 6, 19, 20)	(1, 6, 19, 21)	(1, 6, 21, 22)	(1, 7, 9, 11)	(1, 7, 9, 18)
(1, 7, 10, 12)	(1, 7, 11, 13)	(1, 7, 13, 20)	(1, 8, 9, 21)	(1, 8, 10, 13)
(1, 8, 10, 21)	(1, 8, 15, 20)	(1, 8, 20, 22)	(1, 9, 11, 13)	(1, 9, 14, 17)
(1, 9, 17, 18)	(1, 10, 12, 14)	(1, 10, 12, 16)	(1, 10, 14, 15)	(1, 11, 12, 21)
(1, 11, 13, 16)	(1, 11, 13, 19)	(1, 11, 16, 22)	(1, 11, 17, 19)	(1, 11, 17, 21)
(1, 11, 21, 22)	(1, 12, 16, 22)	(1, 12, 21, 22)	(1, 14, 15, 17)	(1, 14, 15, 18)
(1, 14, 16, 18)	(1, 15, 20, 22)	(1, 16, 18, 22)	(1, 18, 20, 22)	(2, 3, 4, 21)
(2, 3, 4, 22)	(2, 3, 5, 8)	(2, 3, 5, 14)	(2, 3, 8, 12)	(2, 3, 8, 22)
(2, 3, 9, 20)	(2, 3, 14, 20)	(2, 3, 19, 22)	(2, 4, 5, 13)	(2, 4, 5, 15)
(2, 4, 6, 22)	(2, 4, 9, 15)	(2, 4, 9, 20)	(2, 4, 10, 15)	(2, 4, 13, 21)
(2, 4, 20, 21)	(2, 5, 7, 10)	(2, 5, 7, 14)	(2, 5, 7, 16)	(2, 5, 8, 14)
(2, 5, 12, 15)	(2, 5, 13, 16)	(2, 5, 13, 21)	(2, 5, 16, 21)	(2, 6, 7, 16)
(2, 6, 11, 22)	(2, 6, 16, 21)	(2, 7, 9, 14)	(2, 7, 9, 15)	(2, 7, 9, 18)
(2, 7, 10, 15)	(2, 7, 12, 17)	(2, 7, 16, 18)	(2, 8, 10, 13)	(2, 8, 10, 19)
(2, 8, 10, 22)	(2, 8, 11, 16)	(2, 8, 13, 16)	(2, 8, 14, 19)	(2, 8, 18, 19)
(2, 9, 14, 16)	(2, 9, 15, 18)	(2, 9, 17, 22)	(2, 10, 13, 18)	(2, 10, 19, 22)
(2, 11, 12, 15)	(2, 11, 15, 18)	(2, 11, 15, 20)	(2, 11, 16, 18)	(2, 12, 17, 22)
(2, 13, 16, 17)	(2, 13, 18, 19)	(2, 14, 19, 20)	(2, 16, 17, 21)	(2, 17, 19, 22)
(3, 4, 6, 7)	(3, 4, 6, 22)	(3, 4, 10, 11)	(3, 4, 14, 16)	(3, 4, 14, 21)
(3, 5, 10, 18)	(3, 5, 10, 20)	(3, 5, 14, 17)	(3, 5, 18, 22)	(3, 6, 7, 17)
(3, 6, 9, 20)	(3, 6, 14, 17)	(3, 6, 14, 20)	(3, 6, 15, 22)	(3, 6, 16, 17)
(3, 6, 16, 20)	(3, 6, 18, 22)	(3, 7, 8, 12)	(3, 7, 9, 19)	(3, 7, 10, 11)
(3, 7, 10, 12)	(3, 7, 17, 19)	(3, 7, 19, 22)	(3, 9, 10, 12)	(3, 9, 12, 19)
(3, 9, 17, 20)	(3, 9, 19, 21)	(3, 10, 12, 20)	(3, 10, 13, 18)	(3, 10, 18, 20)
(3, 11, 12, 15)	(3, 11, 13, 14)	(3, 11, 13, 16)	(3, 11, 14, 16)	(3, 11, 15, 21)
(3, 12, 13, 16)	(3, 12, 15, 16)	(3, 12, 15, 20)	(3, 12, 16, 20)	(3, 14, 17, 20)
(3, 15, 18, 21)	(3, 16, 17, 20)	(4, 5, 6, 7)	(4, 5, 8, 18)	(4, 5, 18, 19)
(4, 6, 8, 11)	(4, 6, 8, 17)	(4, 6, 11, 22)	(4, 6, 12, 15)	(4, 6, 12, 17)
(4, 6, 15, 17)	(4, 7, 8, 14)	(4, 7, 9, 19)	(4, 7, 19, 20)	(4, 8, 11, 17)
(4, 8, 13, 14)	(4, 8, 13, 21)	(4, 8, 18, 21)	(4, 9, 10, 11)	(4, 9, 10, 19)
(4, 9, 13, 19)	(4, 9, 13, 20)	(4, 9, 16, 20)	(4, 10, 14, 15)	(4, 10, 18, 21)
(4, 11, 12, 19)	(4, 12, 13, 14)	(4, 12, 13, 20)	(4, 12, 15, 17)	(4, 13, 21, 22)
(4, 14, 15, 16)	(4, 16, 17, 20)	(4, 16, 20, 22)	(4, 17, 20, 22)	(4, 17, 21, 22)

(4, 20, 21, 22)	(5, 6, 7, 11)	(5, 6, 9, 20)	(5, 6, 10, 12)	(5, 6, 10, 18)
(5, 6, 11, 13)	(5, 6, 11, 18)	(5, 6, 12, 18)	(5, 7, 11, 21)	(5, 7, 14, 22)
(5, 7, 16, 22)	(5, 8, 9, 15)	(5, 8, 9, 18)	(5, 8, 9, 21)	(5, 8, 11, 21)
(5, 8, 14, 15)	(5, 8, 15, 19)	(5, 8, 18, 19)	(5, 9, 11, 18)	(5, 9, 12, 16)
(5, 9, 12, 18)	(5, 9, 15, 22)	(5, 9, 16, 21)	(5, 9, 16, 22)	(5, 9, 18, 22)
(5, 9, 20, 21)	(5, 10, 17, 18)	(5, 10, 19, 21)	(5, 11, 17, 18)	(5, 12, 17, 18)
(5, 13, 16, 17)	(5, 14, 17, 22)	(5, 15, 19, 21)	(5, 15, 20, 22)	(6, 7, 11, 13)
(6, 7, 13, 21)	(6, 7, 17, 21)	(6, 8, 11, 13)	(6, 8, 12, 17)	(6, 8, 12, 19)
(6, 8, 13, 14)	(6, 8, 15, 19)	(6, 9, 15, 22)	(6, 10, 12, 16)	(6, 10, 14, 17)
(6, 10, 16, 18)	(6, 11, 15, 19)	(6, 12, 15, 17)	(6, 12, 16, 21)	(6, 13, 14, 17)
(6, 14, 18, 22)	(6, 16, 17, 21)	(6, 16, 19, 20)	(6, 18, 19, 22)	(6, 19, 21, 22)
(7, 8, 10, 12)	(7, 8, 13, 16)	(7, 8, 13, 21)	(7, 8, 15, 16)	(7, 9, 14, 19)
(7, 9, 14, 21)	(7, 9, 15, 19)	(7, 10, 11, 15)	(7, 10, 11, 22)	(7, 11, 13, 20)
(7, 11, 15, 20)	(7, 12, 13, 18)	(7, 12, 13, 20)	(7, 12, 13, 22)	(7, 12, 14, 20)
(7, 12, 17, 18)	(7, 13, 15, 16)	(7, 13, 16, 22)	(7, 13, 18, 21)	(7, 14, 19, 20)
(7, 16, 18, 22)	(7, 18, 19, 22)	(8, 9, 10, 17)	(8, 9, 10, 19)	(8, 9, 15, 19)
(8, 9, 16, 19)	(8, 10, 12, 19)	(8, 10, 13, 22)	(8, 11, 13, 16)	(8, 11, 16, 20)
(8, 12, 17, 19)	(8, 12, 18, 21)	(8, 12, 20, 21)	(8, 13, 14, 22)	(8, 14, 15, 19)
(8, 14, 18, 22)	(8, 18, 20, 22)	(9, 10, 12, 19)	(9, 11, 12, 18)	(9, 11, 13, 20)
(9, 12, 13, 14)	(9, 12, 16, 22)	(9, 13, 14, 17)	(9, 13, 14, 19)	(9, 13, 15, 19)
(9, 14, 16, 19)	(9, 14, 16, 21)	(9, 14, 17, 22)	(10, 11, 16, 18)	(10, 11, 16, 20)
(10, 11, 16, 22)	(10, 11, 17, 18)	(10, 12, 14, 20)	(10, 12, 16, 20)	(10, 13, 14, 17)
(10, 13, 17, 18)	(10, 13, 18, 20)	(10, 14, 19, 20)	(10, 15, 16, 21)	(10, 16, 18, 21)
(10, 16, 20, 22)	(10, 19, 20, 22)	(11, 12, 14, 18)	(11, 12, 15, 21)	(11, 13, 14, 19)
(11, 14, 16, 18)	(11, 15, 17, 19)	(12, 13, 15, 16)	(12, 13, 15, 17)	(12, 13, 16, 22)
(12, 13, 17, 18)	(12, 15, 16, 21)	(12, 17, 19, 22)	(13, 15, 19, 21)	(13, 15, 21, 22)
(14, 15, 16, 21)	(14, 15, 18, 21)	(14, 16, 18, 21)	(14, 17, 21, 22)	(19, 20, 21, 22)

References

[1] T.M. Apostol. *Introduction to Analytic Number Theory*, page 222. Undergraduate Texts in Mathematics. Springer New York, 1998.
[2] 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.
[3] 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.
[4] M. Bliznac and A. Filipin. Nonexistence of $D(4)$-quintuples. *Journal of Number Theory*, 194:170–217, 2019.
[5] N. C. Bonciocat, M. Cipu, and M. Mignotte. There is no Diophantine $D(-1)$–quadruple. *J. London Math. Soc.*, Jan 2022
[6] L.E. Dickson. *History of the Theory of Numbers*, volume 2 of *Carnegie Institution of Washington publication*. Carnegie Institution of Washington, 1920.
[7] A. Dujella. Diophantine m-tuples. `https://web.math.pmf.unizg.hr/~duje/dtuples.html`.
[8] A. Dujella. *Number Theory (English Version), translated by P. Švob*. Textbooks of the Universtiy of Zagreb. University of Zagreb, Školska Knjiga, 2021.
[9] A. Dujella. There are only finitely many Diophantine quintuples. *J. Reine Angew. Math.*, 566:183–214, 2004.
[10] A. Dujella. What is ... a Diophantine m-tuple? *Notices Amer. Math. Soc.*, 63:772-774, 2016.
[11] A. Dujella, A. Filipin, and C. Fuchs. Effective solution of the $D(-1)$-quadruple conjecture. *Acta Arithmetica*, 128:319–338, 2007.
[12] A. Dujella and C. Fuchs. Complete solution of a problem of Diophantus and Euler. *Journal of the London Mathematical Society*, 71(1):33–52, 2005.
[13] A. Dujella and M. Kazalicki. Diophantine m-tuples in finite fields and modular forms. *Research in Number Theory*, 7(3), 2021.
[14] A. Dujella, M. Kazalicki, M. Mikić, and M. Szikszai. There are infinitely many rational Diophantine sextuples. *Int. Math. Res. Not. IMRN*, 2017(2):490–508, 2016.
[15] Z. Franušić. A Diophantine problem in $\mathbb{Z}[1 + \sqrt{d}/2]$. *Studia Scientiarum Mathematicarum Hungarica*, 46(1):103–112, 2009.
[16] Z. Franušić. Diophantine quadruples in $\mathbb{Z}[\sqrt{4k+3}]$. *Ramanujan J.*, 17:77–88, 2008.
[17] Z. Franušić. Diophantine quadruples in the ring of integers of $\mathbb{Q}(3\sqrt{2})$. *Miskolc Math. Notes*, 14(3):893–903, 2013.
[18] Z. Franušić and I. Soldo. The problem of Diophantus for integers of $\mathbb{Q}(\sqrt{-3})$. *Rad Hrvat. Akad. Znan. Umjet. Mat. Znan.*, 18:15–25, 2014.
[19] P. Gibbs. Some rational Diophantine sextuples. *Glas. Mat. Ser. III*, 41(2006):195–203.
[20] B. He, A. Togbé, and V. Ziegler. There is no Diophantine quintuple. *Transactions of the American Mathematical Society*, 371(9):6665–6709, May 2019.
[21] K. Ireland and M. Rosen. *A Classical Introduction To Modern Number Theory*, page 305. Number Volume 84 in Graduate Texts in Mathematics. Springer, 1990.
[22] H. Iwaniec and E. Kowalski. *Analytic Number Theory*, page 302. American Mathematical Society Colloquium Publications. American Mathematical Society, 2004.
[23] R. Lidl and H. Niederreiter. *Finite Fields*. Number v. 20, pt. 1 in EBL-Schweitzer. Cambridge University Press, 1997.
[24] M. Overholt. The Diophantine equation $n! + 1 = m^2$. *Bulletin of the London Mathematical Society*, 25(2):104–104, 03 1993.