Proceedings of the
26th Annual Meeting in Mathematics (AMM 2022)
School of Mathematics, Institute of Science
Suranaree University of Technology, Thailand

Solutions to a Quadratic Equation Over Finite Fields

Puchong Wongkumpra† and Detchat Samart‡

Department of Mathematics, Faculty of Science
Burapha University, Chonburi 20130, Thailand

Abstract

We study the equation $x^2+y^2 = z^2-k$ over finite fields. In particular, we find the number of solutions to this equation over an arbitrary finite field and describe an elementary method for finding all solutions over some finite fields. Finally, we use our results to obtain criterion for existence of integer solutions to this equation and a systematic method for computing integer solutions in some cases.

Keywords: Diophantine equation, Quadratic equation, Finite field.

2020 MSC: Primary 11D09; Secondary 11T06.

1 Introduction

Recall that a Diophantine equation is an equation whose solutions are restricted to integers. Finding integer solutions to a Diophantine equation is a major problem in number theory. There is a general method for finding integer solutions to linear Diophantine equations (See, for example, [7, Sect. 3.7]). However, this is not the case for quadratic equations.

Motivated by certain problems in graph theory, Boyer et al. [5] investigated the integer solutions to

$$x^2 + y^2 = z^2 - k \tag{1.1}$$

for a fixed integer value k. Letting $z = x + t$ for some integer t, they rewrote (1.1) as

$$x^2 + y^2 = (x + t)^2 - k \tag{1.2}$$

and found conditions on t for which the equation (1.2) has integer solutions. Observe that if $t = 0$, then (1.2) becomes $y^2 = -k$, which has a solution if and only if $-k$ is a perfect square. On the other hand, if $t \neq 0$, then (1.2) gives $y^2 = 2xt + t^2 - k$ which has a solution if and only if $y^2 \equiv t^2 - k \pmod{2|t|}$ has a solution. The authors of [5] then reduced the congruence above to either $y^2 \equiv -k \pmod{|t|}$ or $y^2 \equiv -k \pmod{2|t|}$, depending on whether t is odd or even. In the case when (1.2) has integer solutions, they showed that there are infinitely many solutions. They also deduced several results for some particular values of k. Below is an example for the case $k = 5$.

†Speaker. ‡Corresponding author.
Email: 62910234@go.buu.ac.th (P.Wongkumpra), petesamart@gmail.com (D.Samart).

Proposition 1.1. *[5, Prop. 20] Suppose t is odd with $5 \nmid t$. Then the equation*

$$x^2 + y^2 = (x + t)^2 - 5$$

has integer solutions x, y if and only if every prime divisor of t is congruent to $1, 3, 7, 9$ modulo 20. For any such t, there are infinitely many solutions.

In this article, we consider the same equation $x^2 + y^2 = z^2 - k$, but we mainly focus on the solutions over finite fields rather than integer solutions. Finally, we use our results to give criterion for existence of integer solutions of (1.2) and a general method for computing the integer solutions under certain assumptions, which complement results in [5]. The main results, which are divided into three parts, are presented in Section 3.

2 Preliminary results

Here and throughout we let p be a prime, q a prime power, $\mathbb{F}_q$ a finite field of order q, and $\mathbb{F}_q^\times = \mathbb{F}_q \backslash \{0\}$. In this section, we recall some auxiliary results which will be frequently invoked in the proofs of our main results.

Let $a, b \in \mathbb{F}_q$. If $a^2 = b$, then we say that b is a *square* in $\mathbb{F}_q$ and a is a *square root* of b. Determining whether an element of $\mathbb{F}_q$ is a square is quite easy, thanks to the following theorem.

Theorem 2.1. *Let $q = p^n$, where $n \in \mathbb{N}$.*

(i) If $p = 2$, then every element of $\mathbb{F}_q$ is a square.

(ii) If p is odd, then $a \in \mathbb{F}_q^\times$ is a square if and only if $a^{(q-1)/2} = 1$.

Proof. Let $q = 2^n$. Obviously, 0 is a square in $\mathbb{F}_q$. Since $\mathbb{F}_q^\times$ is a group of order $q - 1$ under multiplication, we have by Lagrange's theorem that for every $a \in \mathbb{F}_q^\times$,

$$\left(a^{2^{n-1}}\right)^2 = a^q = a(a^{q-1}) = a.$$

Therefore, we may conclude that every element of $\mathbb{F}_q$ is a square. Part (ii) is known as generalized Euler's criterion, whose proof can be found in [1, Thm. 2]. □

By the proof of Theorem 2.1 (i), one sees immediately that $a^{2^{n-1}}$ is a square root of a in $\mathbb{F}_{2^n}$. Note, however, that computing a square root of an element in $\mathbb{F}_q$ with q odd can be a hard problem. For an odd prime p not congruent to 1 modulo 8, there are explicit formulas for computing a square root in $\mathbb{F}_p$.

Theorem 2.2. *[6, Lem. 11.22] Let p be an odd prime and let b be a quadratic residue modulo p; i.e., there exists $a \in \mathbb{F}_p$ such that $a^2 \equiv b \pmod{p}$.*

(i) If $p \equiv 3 \pmod 4$, then $a \equiv \pm b^{(p+1)/4} \pmod p$.

(ii) If $p \equiv 5 \pmod 8$ and $b^{(p-1)/4} = 1$, then $a \equiv \pm b^{(p+3)/8} \pmod p$.

(iii) If $p \equiv 5 \pmod 8$ and $b^{(p-1)/4} = -1$, then $a \equiv \pm 2b(4b)^{(p-5)/8} \pmod p$.

For $p \equiv 1 \pmod 8$, the problem of finding a square root in $\mathbb{F}_p$ turns out to be much more complicated; there are no known formulas similar to those in Theorem 2.2. Although there are certain algorithms such as the Tonelli-Shanks algorithm and Cipolla's algorithm which can be applied to compute a square root in $\mathbb{F}_p$ for any prime p, they require randomness to run in polynomial time. This topic is beyond the scope of this paper and we refer the interested reader to [4].

Geometrically, the equation (1.1) defines an affine surface, so it is natural to look for similar results for algebraic curves and try to extend them to (1.1). In [3], Aabrandt and Hansen study the number of solutions over finite fields of the circle equation $x^2 + y^2 = 1$ and they prove the following result.

Theorem 2.3. *[3, Thm. 3.1] The number of solutions to $x^2+y^2=1$ over $\mathbb{F}_q$ is $q-\sin(q\pi/2)$.*

We will generalize the result above to a circle of arbitrary radius. The idea of our proof is essentially the same as that of [3, Thm. 3.1].

Theorem 2.4. *Let $m \in \mathbb{F}_q^\times$. The number of solutions to $x^2+y^2=m$ over $\mathbb{F}_q$ is $q-\sin(q\pi/2)$.*

Proof. If $q=2^n$ with $n \in \mathbb{N}$, then we have from Theorem 2.1 (i) that m is a square in $\mathbb{F}_q$, so the equation $x^2+y^2=m$ is equivalent to $x^2+y^2=1$, which has $q-\sin(q\pi/2)$ solutions by Theorem 2.3. Next, assume that $q=p^n$, where p is an odd prime and $n \in \mathbb{N}$. Then the multiplicative group $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$; i.e., there exists $g \in \mathbb{F}_q^\times$ such that $\mathbb{F}_q^\times = \{g^k \mid 1 \le k \le q-1\}$. Define the multiplicative homomorphism $\eta : \mathbb{F}_q^\times \to \{-1,1\}$ by $\eta(g^k)=(-1)^k$ and set $\eta(0)=0$. Observe that the squaring homomorphism $x^2 : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ maps $g^l \in \mathbb{F}_q^\times$ to $g^{2l} \in \mathbb{F}_q^\times$. Thus c is a square in $\mathbb{F}_q^\times$ if and only if $\eta(c)=1$. Since there are equally many odd powers and even powers of g in $\mathbb{F}_q^\times$, it follows that

$$\sum_{c\in\mathbb{F}_q} \eta(c) = 0.$$

Let N_q be the number of solutions to $x^2+y^2=m$ and for any $c \in \mathbb{F}_q$ let $N_q(x^2=c)$ denote the number of solution to $x^2=c$ in $\mathbb{F}_q$. Then we have

$$N_q = \sum_{c_1+c_2=m} N_q(x^2=c_1)N_q(y^2=c_2).$$

Consider $x^2=c$ over $\mathbb{F}_q^\times$. If c is a square then $z^2=c$ has exactly two solutions, and if c is a non-square then $z^2=c$ has no solutions. Thus

$$\begin{aligned}
N_q &= \sum_{c_1+c_2=m} [1+\eta(c_1)][1+\eta(c_2)] \\
&= \sum_{c_1+c_2=m} 1 + \sum_{c_1+c_2=m} \eta(c_1) + \sum_{c_1+c_2=m} \eta(c_2) + \sum_{c_1+c_2=m} \eta(c_1)\eta(c_2) \\
&= q + \sum_{c_1\in\mathbb{F}_q} \eta(c_1) + \sum_{c_2\in\mathbb{F}_q} \eta(c_2) + \sum_{c_1+c_2=m} \eta(c_1c_2) \\
&= q + 0 + 0 + \sum_{c\in\mathbb{F}_q} \eta(c(m-c)) \\
&= q + \sum_{c\in\mathbb{F}_q} \eta(-(c^2-cm)) \\
&= q + \eta(-1) \sum_{c\in\mathbb{F}_q} \eta(c^2-cm) \\
&= q + \eta(-1) \sum_{c\in\mathbb{F}_q} \eta(4)\eta(c^2-cm) \\
&= q + \eta(-1) \sum_{c\in\mathbb{F}_q} (-1 + [1+\eta((2c-m)^2-m^2)]) \\
&= q + \eta(-1)(-q) + \eta(-1) \sum_{c\in\mathbb{F}_q} [1+\eta((2c-m)^2-m^2)].
\end{aligned}$$

Let

$$S = \sum_{c\in\mathbb{F}_q} [1+\eta((2c-m)^2-m^2)].$$

We have that S is the number of solutions in $\mathbb{F}_q$ to the quadratic equation $(2c-m)^2-m^2=a^2$, which can be rewritten as $(2c-m+a)(2c-m-a)=m^2$. Let $\alpha=(2c-m+a)m^{-1}$. If we let a and c vary, it is easily seen that α can be any element of $\mathbb{F}_q^\times$. Moreover, we have $\alpha^{-1}=(2c-m-a)m^{-1}$. It then follows by simple calculation that $a=2^{-1}(\alpha-\alpha^{-1})m$ and $c=2^{-1}(\alpha+1-2^{-1}(\alpha-\alpha^{-1}))m$. Since a and c are uniquely determined by a choice of $\alpha\in\mathbb{F}_q^\times$ and $|\mathbb{F}_q^\times|=q-1$, we may conclude that $S=q-1$. In addition, we have from Theorem 2.1 (ii) that

$$\eta(-1)=\begin{cases}1 & \text{if } q\equiv 1 \pmod 4,\\ -1 & \text{if } q\equiv 3 \pmod 4\end{cases}=\sin\frac{q\pi}{2}.$$

Therefore, $N_q=q+\eta(-1)(-q)+\eta(-1)(q-1)=q-\eta(-1)=q-\sin(q\pi/2)$. □

We also record the following result in this section for the sake of completeness.

Proposition 2.5. *Let p be a prime, $n\in\mathbb{N}$, $q=p^n$, and let N_q denote the number of solutions of the equation $x^2+y^2=0$ over $\mathbb{F}_q$. Then*

$$N_q=\left(1+\sin\frac{q\pi}{2}\right)(q-1)+1=\begin{cases}q & \text{if } p=2,\\ 2q-1 & \text{if } q\equiv 1 \pmod 4,\\ 1 & \text{if } q\equiv 3 \pmod 4.\end{cases}$$

Proof. The case $p=2$ is clear since the solutions of $x^2+y^2=0$ over $\mathbb{F}_q$ are of the form (x_0,x_0), where $x_0\in\mathbb{F}_q$. Now assume that p is an odd prime. It is obvious that $(x,y)=(0,0)$ is a solution of $x^2+y^2=0$, while $(x,0)$ and $(0,y)$ with $x\neq 0, y\neq 0$ are not solutions of $x^2+y^2=0$. Now let $x,y\in\mathbb{F}_q^\times$. Then $x^2=-y^2$ if and only if $-1=m^2$ for some $m\in\mathbb{F}_q^\times$. By Theorem 2.1 (ii), the latter condition is equivalent to $(-1)^{(q-1)/2}=1$, which is true only when $q\equiv 1 \pmod 4$. Moreover, if $-1=m^2$ and $x^2=-y^2$, then $(x(my)^{-1})^2=1$, from which we may conclude that $x(my)^{-1}=\pm 1$, so $x=\pm my$. Therefore, the set of solutions of $x^2+y^2=0$ is $\{(\pm my_0,y_0)\mid y_0\in\mathbb{F}_q^\times\}\cup\{(0,0)\}$, which contains $2(q-1)+1=2q-1$ elements. □

3 Main Results

In this section, we establish results concerning the number of solutions to (1.1) over an arbitrary finite field. We also find the set of solutions to (1.1) in $\mathbb{F}_q$, where $q=2^n$ or q is a prime congruent to 3 modulo 4. Finally, we relate our results over $\mathbb{F}_2$ to integer solutions of (1.2).

3.1 The number of solutions to $x^2+y^2=z^2-k$ over finite fields

First, we consider the equation over finite fields of characteristic 2, which are relatively easy to deal with compared to the finite fields of odd characteristic. Our first main result is as follows.

Theorem 3.1. *Let $n\in\mathbb{N}$, $q=2^n$, and let $k\in\mathbb{F}_q$. Over $\mathbb{F}_q$, the equation $x^2+y^2=z^2-k$ has q^2 solutions.*

Proof. Let (x_0,y_0,z_0) be a solution to $x^2+y^2=z^2-k$. By Theorem 2.1 (i), there exists $w\in\mathbb{F}_q$ such that $k=w^2$. Since $x_0,z_0\in\mathbb{F}_{2^n}$, there is $t\in\mathbb{F}_{2^n}$ such that $z_0=x_0+t$. Plugging these into the original equation and rearranging terms yield

$$(t-y_0)^2=t^2-y_0^2=k=w^2.$$

Since $\mathrm{char}(\mathbb{F}_q)=2$, it follows that $t-y_0=w$, so $y_0=t-w$. On the other hand, it can be checked easily that $(x,y,z)=(x_0,t-w,x_0+t)$ satisfies $x^2+y^2=z^2-k$ for any $x_0,t\in\mathbb{F}_q$. Hence this equation has $2^n\cdot 2^n=2^{2n}=q^2$ solutions in $\mathbb{F}_q$. □

For finite fields of order p^n, where p is an odd prime and $n \in \mathbb{N}$, we start by looking at the case $k = 0$. For $k \neq 0$, we consider the square and non-square cases separately.

Lemma 3.2. *Let $q = p^n$, where p is an odd prime and $n \in \mathbb{N}$. Over $\mathbb{F}_q$, the equation*

$$x^2 + y^2 = z^2, \text{ with } z \neq 0, \tag{3.1}$$

has $(q-1)\left(q - \sin\dfrac{q\pi}{2}\right)$ solutions.

Proof. If $z \neq 0$, then $x^2 + y^2 = z^2$ is equivalent to $x'^2 + y'^2 = 1$ by the change of variables $x' = z^{-1}x, y' = z^{-1}y$. The latter equation has $q - \sin(q\pi/2)$ solutions by Theorem 2.3. Since there are $q-1$ nonzero elements in $\mathbb{F}_q$, we have that (3.1) has $(q-1)(q - \sin(q\pi/2))$ solutions in total. □

Theorem 3.3. *Let $q = p^n$, where p is an odd prime and $n \in \mathbb{N}$. Over $\mathbb{F}_q$, the equation*

$$x^2 + y^2 = z^2, \tag{3.2}$$

has q^2 solutions.

Proof. Let N_q be the number of solutions of the form $(x_0, y_0, 0)$. Then by Lemma 3.2 and Proposition 2.5 we have that the number of solutions to (3.2) over $\mathbb{F}_q$ is

$$(q - \sin(q\pi/2))(q-1) + N_q = (q - \sin(q\pi/2))(q-1) + (1 + \sin(q\pi/2))(q-1) + 1 = q^2.$$

□

Theorem 3.4. *Let $q = p^n$, where p is an odd prime and $n \in \mathbb{N}$ and let $k \in \mathbb{F}_q^\times$.*

(i) If k is not a square, then $x^2 + y^2 = z^2 - k$ has $q\left(q - \sin\dfrac{q\pi}{2}\right)$ solutions.

(ii) If k is a square, then $x^2 + y^2 = z^2 - k$ has $q\left(q + \sin\dfrac{q\pi}{2}\right)$ solutions.

Proof. Suppose k is not a square. Then $z^2 - k \neq 0$ for any $z \in \mathbb{F}_q$. By Theorem 2.4, for any fixed $l \in \mathbb{F}_q^\times$, the equation $x^2 + y^2 = l$ has $q - \sin(q\pi/2)$ solutions over $\mathbb{F}_q$. Thus the equation $x^2 + y^2 = z^2 - k$ has $q(q - \sin(q\pi/2))$ solutions.

Now assume that $k = m^2$ for some $m \in \mathbb{F}_q$. Then (1.1) becomes $x^2 + y^2 = z^2 - m^2$. If $z = m$ or $z = -m$, then this equation reduces to $x^2 + y^2 = 0$. By Proposition 2.5, this equation has either $2q-1$ or 1 solutions in $\mathbb{F}_q$, depending on whether q is congruent to 1 or 3 modulo 4. Let M_q denote the number of solutions of the form $(x_0, y_0, \pm m)$ over $\mathbb{F}_q$. Then we have

$$M_q = \begin{cases} 4q-2 & \text{if } q \equiv 1 \pmod 4, \\ 2 & \text{if } q \equiv 3 \pmod 4 \end{cases} = \left(1 + \sin\frac{q\pi}{2}\right)(2q-2) + 2.$$

If $z \neq \pm m$, then $x^2 + y^2 = z^2 - m^2 = l$, where $l \in \mathbb{F}_q^\times$. By Theorem 2.4, this equation has $q - \sin(q\pi/2)$ solutions. Thus $x^2 + y^2 = z^2 - m^2$ has $(q-2)(q - \sin(q\pi/2))$ solutions for which $z \neq \pm m$. Therefore, we have that the number of solutions to $x^2 + y^2 = z^2 - m^2$ over $\mathbb{F}_q$ is $M_q + (q-2)(q - \sin\dfrac{q\pi}{2}) = q(q + \sin(q\pi/2))$. □

3.2 The set of solutions to $x^2 + y^2 = z^2 - k$ over some finite fields

We have obtained complete results about the number of solutions to (1.1) over any finite field $\mathbb{F}_q$. Next, we will describe a method for finding all solutions of this equation over some finite fields. In particular, we will consider the solutions over $\mathbb{F}_q$, where q is a power of 2 or q is an odd prime which is congruent to 3 modulo 4. We again start by considering solutions over finite fields of characteristic 2.

Theorem 3.5. *Let $q = 2^n$ where $n \in \mathbb{N}$ and let $k \in \mathbb{F}_q$. Over $\mathbb{F}_q$, the set of solutions to $x^2 + y^2 = z^2 - k$ is $\{(x_0, t - k^{\frac{q}{2}}, x_0 + t) \mid x_0, t \in \mathbb{F}_q\}$.*

Proof. It follows from the proof of Theorem 3.1 that the solutions to this equation over $\mathbb{F}_q$ are $(x_0, t-w, x_0+t)$, where $x_0, t \in \mathbb{F}_q$ and w is the square root of k. (Note that we use "the" instead of "a" due to the fact that $w = -w$ in $\mathbb{F}_q$.) Moreover, one sees from the proof of Theorem 2.1 (i) that $w = k^{2^{n-1}} = k^{\frac{q}{2}}$. □

Example 3.6. The Galois field of order 4 is the set $\{0, 1, a, b\}$ with addition and multiplication defined by the following Cayley tables.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Note that this field is isomorphic to $\mathbb{Z}_2[t]/\langle t^2 + t + 1\rangle$, where the underlying isomorphism maps a and b to $t + \langle t^2 + t + 1\rangle$ and $t + 1 + \langle t^2 + t + 1\rangle$, respectively.
Find all solutions to $x^2 + y^2 = z^2 - a$ over the Galois field of order 4.

Solution. By Theorem 3.5, the solutions (x, y, z) are $(x_0, t - a^{\frac{4}{2}}, x_0 + t) = (x_0, t - b, x_0 + t)$, where $x_0, t \in \{0, 1, a, b\}$. Thus

$$\begin{aligned}(x, y, z) = &(0, 0-b, 0+0), (0, 1-b, 0+1), (0, a-b, 0+a), (0, b-b, 0+b),\\ &(1, 0-b, 1+0), (1, 1-b, 1+1), (1, a-b, 1+a), (1, b-b, 1+b)\\ &(a, 0-b, a+0), (a, 1-b, a+1), (a, a-b, a+a), (a, b-b, a+b)\\ &(b, 0-b, b+0), (b, 1-b, b+1), (b, a-b, b+a), (b, b-b, b+b)\\ = &(0, b, 0), (0, a, 1), (0, 1, a), (0, 0, b), (1, b, 1), (1, a, 0), (1, 1, b), (1, 0, a),\\ &(a, b, a), (a, a, b), (a, 1, 0), (a, 0, 1), (b, b, b), (b, a, a), (b, 1, 1), (b, 0, 0).\end{aligned}$$

□

We use the explicit formulas for square roots in Theorem 2.2 to establish the following results.

Lemma 3.7. *Let p be an odd prime with $p \equiv 3 \pmod 4$. The solutions to $x^2 + y^2 = 1$ over $\mathbb{F}_p$ are $(\pm t^{\frac{p+1}{4}}, \pm(1-t)^{\frac{p+1}{4}})$, where $t \in \mathbb{F}_p$ for which both t and $1 - t$ are squares in $\mathbb{F}_p$.*

Proof. Let $x^2 = t$. The equation $x^2 + y^2 = 1$ becomes $y^2 = 1 - t$, which has solutions iff $1 - t$ is a square. If solutions exist, we have from Theorem 2.2 (i) that $(x, y) = (\pm t^{\frac{p+1}{4}}, \pm(1-t)^{\frac{p+1}{4}})$. □

Theorem 3.8. *Let p be an odd prime with $p \equiv 3 \pmod 4$. The solutions to $x^2 + y^2 = z^2$ over $\mathbb{F}_p$ are $(\pm z_0 t^{\frac{p+1}{4}}, \pm z_0(1-t)^{\frac{p+1}{4}}, z_0)$, where $z_0 \in \mathbb{F}_p$ and $t \in \mathbb{F}_p$ for which both t and $1 - t$ are squares in $\mathbb{F}_p$.*

Proof. If $z = 0$, then we have $x^2+y^2 = 0$, which has only one (trivial) solution by Proposition 2.5, so $(x, y, z) = (0, 0, 0)$. If $z \neq 0$, then we rewrite the equation $x^2 + y^2 = z^2$ as $x'^2 + y'^2 = 1$, where $x' = z^{-1}x$ and $y' = z^{-1}y$. By Lemma 3.7, the solutions to this equation are $(\pm t^{\frac{p+1}{4}}, \pm(1-t)^{\frac{p+1}{4}})$, where both t and $1 - t$ are squares in $\mathbb{F}_p$. Hence the solutions to $x^2 + y^2 = z^2$ with $z \neq 0$ are $(\pm z_0 t^{\frac{p+1}{4}}, \pm z_0(1 - t)^{\frac{p+1}{4}}, z_0)$, where $z_0 \in \mathbb{F}_q^\times$. □

Theorem 3.9. *Let p be an odd prime with $p \equiv 3 \pmod 4$ and let $k \in \mathbb{F}_p^\times$. The solutions to $x^2 + y^2 = z^2 - k$ over $\mathbb{F}_p$ are $(\pm t^{\frac{p+1}{4}}, \pm s^{\frac{p+1}{4}}, \pm(t + s + k)^{\frac{p+1}{4}})$, where $s, t \in \mathbb{F}_p^\times$ for which s, t, and $t + s + k$ are all squares in $\mathbb{F}_p$.*

Proof. Let $x^2 = t$ and $y^2 = s$, then the equation $x^2 + y^2 = z^2 - k$ becomes $z^2 = t + s + k$. Hence this equation has a solutions if and only t, s and $t + s + k$ are a square, in which case we have that $(x, y, z) = (\pm t^{\frac{p+1}{4}}, \pm s^{\frac{p+1}{4}}, \pm(t + s + k)^{\frac{p+1}{4}})$. □

To illustrate the method outlined above, we give an example over $\mathbb{F}_7$ below.

Example 3.10. Find all solutions to $x^2 + y^2 = z^2 - 4$ over $\mathbb{F}_7 \cong \mathbb{Z}/7\mathbb{Z}$.

Solution. All square in $\mathbb{Z}/7\mathbb{Z}$ are $\bar{0}, \bar{1}, \bar{2}$, and $\bar{4}$, where $\bar{m}$ denotes the residue class of m modulo 7. We need to find t and s from this list such that $t + s + 4$ is also a square. Let $t * s = t + s + 4$. Then we have the following Cayley table for $*$.

$*$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{1}$
$\bar{1}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{2}$
$\bar{2}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{3}$
$\bar{4}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{5}$

Hence the triples $(s, t, s + t + 4)$ for which s, t, and $s + t + 4$ are all squares include

$$(\bar{0}, \bar{0}, \bar{4}), (\bar{0}, \bar{4}, \bar{1}), (\bar{1}, \bar{2}, \bar{0}), (\bar{1}, \bar{4}, \bar{2}), (\bar{2}, \bar{1}, \bar{0}), (\bar{2}, \bar{2}, \bar{1}), (\bar{4}, \bar{0}, \bar{1}), (\bar{4}, \bar{1}, \bar{2}).$$

It follows from Theorem 3.9 that all solutions to $x^2 + y^2 = z^2 - 4$ over $\mathbb{Z}/7\mathbb{Z}$ are

$$\begin{aligned}(x, y, z) = {} & (\pm\bar{0}^2, \pm\bar{0}^2, \pm\bar{4}^2), (\pm\bar{0}^2, \pm\bar{4}^2, \pm\bar{1}^2), (\pm\bar{1}^2, \pm\bar{2}^2, \pm\bar{0}^2), (\pm\bar{1}^2, \pm\bar{4}^2, \pm\bar{2}^2), (\pm\bar{2}^2, \pm\bar{1}^2, \pm\bar{0}^2),\\ & (\pm\bar{2}^2, \pm\bar{2}^2, \pm\bar{1}^2), (\pm\bar{4}^2, \pm\bar{0}^2, \pm\bar{1}^2), (\pm\bar{4}^2, \pm\bar{1}^2, \pm\bar{2}^2)\\ = {} & (\bar{0}, \bar{0}, \pm\bar{2}), (\bar{0}, \pm\bar{2}, \pm\bar{1}), (\pm\bar{1}, \pm\bar{4}, \bar{0}), (\pm\bar{1}, \pm\bar{2}, \pm\bar{4}), (\pm\bar{4}, \pm\bar{1}, \bar{0}),\\ & (\pm\bar{4}, \pm\bar{4}, \pm\bar{1}), (\pm\bar{2}, \bar{0}, \pm\bar{1}), (\pm\bar{2}, \pm\bar{1}, \pm\bar{4}).\end{aligned}$$

Remark 3.11. One can use a similar approach to obtain formulas for the solutions to (1.1) over $\mathbb{F}_p$, where p is a prime congruent to 5 modulo 8, with the aid of Theorem 2.2 (ii)-(iii). However, the calculation seems much more involved in these cases, so we decided not to include them here.

3.3 Solutions to $x^2 + y^2 = (x + t)^2 - k$ over the integers

In this section, we apply our result on $\mathbb{F}_2$ to systematically study integer solutions of (1.2). More precisely, we find the conditions on t and k for which (1.2) has solutions. In some cases, we also obtain formulas for computing the set of integer solutions as by-products.

By Theorem 3.5, we immediately obtain the following result.

Proposition 3.12. *Over $\mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, the solutions to $x^2 + y^2 = z^2$ are*

$$(\bar{0}, \bar{0}, \bar{0}), (\bar{1}, \bar{0}, \bar{1}), (\bar{0}, \bar{1}, \bar{1}), (\bar{1}, \bar{1}, \bar{0})$$

and the solutions to $x^2 + y^2 = z^2 + \bar{1}$ are

$$(\bar{0}, \bar{1}, \bar{0}), (\bar{1}, \bar{1}, \bar{1}), (\bar{0}, \bar{0}, \bar{1}), (\bar{1}, \bar{0}, \bar{0}).$$

Theorem 3.13. *Let $l \in \mathbb{Z}$. If the equation $x^2+y^2 = z^2+2l$ has an integer solution, then every solution (x_0, y_0, z_0) can be obtained from the list below:*

(i) $(x_0, y_0, z_0) = (2a, 2b, 2c)$ *and* $l = 2a^2 + 2b^2 - 2c^2$, *or*

(ii) $(x_0, y_0, z_0) = (2a+1, 2b, 2c+1)$ *and* $l = 2a^2 + 2b^2 - 2c^2 + 2a - 2c$, *or*

(iii) $(x_0, y_0, z_0) = (2a, 2b+1, 2c+1)$ *and* $l = 2a^2 + 2b^2 - 2c^2 + 2b - 2c$, *or*

(iv) $(x_0, y_0, z_0) = (2a+1, 2b+1, 2c)$ *and* $l = 2a^2 + 2b^2 - 2c^2 + 2a + 2b + 1$,

where $a, b, c \in \mathbb{Z}$.

Proof. Let (x_0, y_0, z_0) be a solution to $x^2+y^2 = z^2+2l$. Reducing modulo 2 yields $\bar{x}_0^2+\bar{y}_0^2 = \bar{z}_0^2$. By Proposition 3.12, we have $(\bar{x}_0, \bar{y}_0, \bar{z}_0) \in \{(\bar{0}, \bar{0}, \bar{0}), (\bar{1}, \bar{0}, \bar{1}), (\bar{0}, \bar{1}, \bar{1}), (\bar{1}, \bar{1}, \bar{0})\}$. The desired result then follows easily by writing x_0, y_0, and z_0 as an odd or even integer, depending on their residue classes modulo 2 and solving for l. □

One can prove the following result using the same arguments as above.

Theorem 3.14. *Let $l \in \mathbb{Z}$. If the equation $x^2 + y^2 = z^2 + 2l + 1$ has an integer solution, then every solution (x_0, y_0, z_0) can be obtained from the list below:*

(i) $(x_0, y_0, z_0) = (2a, 2b+1, 2c)$ *and* $l = 2a^2 + 2b^2 - 2c^2 + 2b$, *or*

(ii) $(x_0, y_0, z_0) = (2a+1, 2b+1, 2c+1)$ *and* $l = 2a^2 + 2b^2 - 2c^2 + 2a + 2b - 2c$, *or*

(iii) $(x_0, y_0, z_0) = (2a, 2b, 2c+1)$ *and* $l = 2a^2 + 2b^2 - 2c^2 - 2c - 1$, *or*

(iv) $(x_0, y_0, z_0) = (2a+1, 2b, 2c)$ *and* $l = 2a^2 + 2b^2 - 2c^2 + 2a$.

where $a, b, c \in \mathbb{Z}$.

Now let us consider the general equation $x^2+y^2 = (x+t)^2-k$ over the set of integers, where k and t are given. We first analyze the case when t is odd.

Theorem 3.15. *Let t be an odd integer and let $k \in \mathbb{Z}$. Then $x^2 + y^2 = (x+t)^2 - k$ has an integer solution if and only if $-k$ is a square modulo $|t|$. Moreover, if $x^2 + y^2 = (x+t)^2 - k$ has an integer solution, then all solutions are either*

(i) $(x_0, y_0) = (\frac{u^2-t^2+k}{2t}, u)$, *if k is an even integer, or*

(ii) $(x_0, y_0) = (\frac{v^2-t^2+k}{2t}, v)$, *if k is an odd integer,*

where u and v are odd and even solutions to $y^2 \equiv -k \pmod{|t|}$, respectively.

Proof. If $x^2 + y^2 = (x+t)^2 - k$ has an integer solution, then we have $y^2 = 2xt + t^2 - k \equiv -k \pmod{|t|}$, so $-k$ is a square modulo $|t|$. On the other hand, assume that there exists $\alpha \in \mathbb{Z}$ such that $\alpha^2 \equiv -k \pmod{|t|}$. Since t is odd, this quadratic congruence has both odd and even solutions. Let u be an odd solution and let v be an even solution.

If $k \equiv 0 \pmod 4$, we write $t = 2N+1$ where $N \in \mathbb{Z}$ and the congruence $u^2 \equiv -k \pmod{|t|}$ can be rewritten as $\frac{u^2-1}{4} \equiv \frac{t^2-1}{4} - \frac{k}{4} \pmod{|t|}$. It follows that

$$\frac{u^2-1}{4} = \frac{t^2-1}{4} - \frac{k}{4} + at,$$

for some $a \in \mathbb{Z}$. Letting $l = \frac{-k}{2}$, $u = 2b+1$ and $c = a+N$, we have $l = 2a^2+2b^2-2c^2+2b-2c$. By Theorem 3.13 (iii), $(2a, 2b+1, 2c+1)$ is an integer solution to $x^2 + y^2 = z^2 + 2l$. Thus $(2a, 2b+1) = \left(\frac{u^2-t^2+k}{2t}, u\right)$ is an integer solution to $x^2 + y^2 = (x+t)^2 - k$.

If $k \equiv 1 \pmod 4$, we write $t = 2M - 1$ where $M \in \mathbb{Z}$ and the congruence $v^2 \equiv -k \pmod{|t|}$ can be rewritten as $\frac{v^2}{4} \equiv \frac{(t+1)^2}{4} + \frac{-k-1}{4} \pmod{|t|}$. Thus

$$\frac{v^2}{4} = \frac{(t+1)^2}{4} + \frac{-k-1}{4} + at,$$

for some $a \in \mathbb{Z}$, and we can write $l = 2a^2 + 2b^2 - 2c^2 + 2a$ by letting $l = \frac{-k-1}{2}$, $v = 2b$ and $c = a + N$. By Theorem 3.14 (iv), $(2a+1, 2b, 2c)$ is an integer solution to $x^2 + y^2 = z^2 + 1 + 2l$. Thus $(2a+1, 2b) = \left(\frac{v^2-t^2+k}{2t}, v\right)$ is an integer solution to $x^2 + y^2 = (x+t)^2 - k$.

The cases $k \equiv 2 \pmod 4$ and $k \equiv 3 \pmod 4$ can be proven in a similar manner where the existence of integer solutions to $x^2 + y^2 = (x+t)^2 - k$ is guaranteed by Theorem 3.13 (iv) and Theorem 3.14 (iii), respectively. Moreover, they again correspond to the integer solutions of the form $\left(\frac{v^2-t^2+k}{2t}, v\right)$ and $\left(\frac{v^2-t^2+k}{2t}, v\right)$. Since each integer solution of $x^2 + y^2 = (x+t)^2 - k$ is uniquely determined by those in Theorem 3.13 (iii)-(iv) and Theorem 3.14 (iii)-(iv), we have obtained all integer solutions of this equation from the four cases above. □

Note that if t is an odd prime, the condition that $-k$ is a square modulo $|t|$ can be determined computationally using the Legendre symbol $\left(\frac{-k}{|t|}\right)$. If t is composite, one can still use the Legendre symbol corresponding to each prime factor of t to test squareness of $-k$. For more details, we refer the reader to [5, Lem. 8]. For t even, we have the following criterion.

Theorem 3.16. *Let t be a nonzero even integer and $k \in \mathbb{Z}$.*

(i) If $k \equiv 1, 2 \pmod 4$, then $x^2 + y^2 = (x+t)^2 - k$ has no integer solutions.

(ii) The equation $x^2 + y^2 = (x+t)^2 - k$ has an integer solution if and only if $y^2 \equiv -k \pmod{2|t|}$ has a solution.

Proof. (i) Since t is even, x and $x+t$ have the same parity. Moreover, for any $x \in \mathbb{Z}$, we have that either $x^2 \equiv 0 \pmod 4$ or $x^2 \equiv 1 \pmod 4$, depending on whether x is even or odd, so $x^2 \equiv (x+t)^2 \pmod 4$. Hence if $x^2 + y^2 = (x+t)^2 - k$ has an integer solution, then $y^2 \equiv -k \equiv 0, 1 \pmod 4$, implying $k \equiv 0, 3 \pmod 4$.

(ii) This follows directly from [5, Prop. 25].

□

Example 3.17. Determine whether $x^2 + y^2 = (x+13)^2 - 5$ has an integer solution.

Solution. Let $t = 13$ and $k = 5$. Since the congruence $\alpha^2 \equiv -5 \pmod{13}$ has no solutions, $x^2 + y^2 = (x+13)^2 - 5$ has no integer solutions by Theorem 3.15. □

Example 3.18. Determine whether $x^2 + y^2 = (x+5)^2 - 4$ has integer solutions.

Solution. Let $t = 5$ and $k = 4$. The congruence $\alpha^2 \equiv -k \equiv 1 \pmod 5$ has two solutions, namely $\alpha \equiv 1, 4 \pmod 5$. By Theorem 3.15, $x^2 + y^2 = (x+5)^2 - 4$ has integer solutions. Since k is even, we need to find all odd solutions to $\alpha^2 \equiv 1 \pmod 5$. If $\alpha \equiv 1 \pmod 5$, choose $u = 1 + 5(2n) = 10n + 1$, with $n \in \mathbb{Z}$, which gives the solution

$$(x, y) = \left(\frac{u^2 - t^2 + k}{2t}, u\right) = (10n^2 + 2n - 2, 10n + 1).$$

If $\alpha \equiv 4 \pmod 5$, choose $u = 4 + 5(2n+1) = 10n + 9$, with $n \in \mathbb{Z}$, which gives the solution

$$(x, y) = \left(\frac{u^2 - t^2 + k}{2t}, u\right) = (10n^2 + 18n + 6, 10n + 9).$$

Hence the set of integer solutions to $x^2 + y^2 = (x+5)^2 - 4$ is

$$(x, y) = \{(10n^2 + 2n - 2, 10n + 1) \mid n \in \mathbb{Z}\} \cup \{(10n^2 + 18n + 6, 10n + 9) \mid n \in \mathbb{Z}\}.$$

□

Example 3.19. Determine whether $x^2 + y^2 = (x-7)^2 + 15$ has integer solutions.

Solution. Let $t = -7$ and $k = -15$. The congruence $\alpha^2 \equiv -k \equiv 1 \pmod 7$ has solutions $\alpha \equiv 1, 6 \pmod 7$. Therefore, by Theorem 3.15, $x^2 + y^2 = (x-7)^2 + 15$ has integer solutions.
If $\alpha \equiv 1 \pmod 7$, let $v = 1 + 7(2n+1) = 14n + 8$, where $n \in \mathbb{Z}$. This gives the solution

$$(x, y) = \left(\frac{v^2 - t^2 + k}{2t}, v\right) = (-14n^2 - 16n, 14n + 8).$$

If $\alpha \equiv 6 \pmod 7$, let $v = 6 + 7(2n) = 14n + 6$, where $n \in \mathbb{Z}$. This gives the solution

$$(x, y) = \left(\frac{v^2 - t^2 + k}{2t}, v\right) = (-14n^2 - 12n + 2, 14n + 6).$$

Hence the set of integer solutions to $x^2 + y^2 = (x-7)^2 + 15$ is

$$(x, y) = \{(-14n^2 - 16n, 14n + 8) \mid n \in \mathbb{Z}\} \cup \{(-14n^2 - 12n + 2, 14n + 6) \mid n \in \mathbb{Z}\}.$$

□

Example 3.20. Determine whether $x^2 + y^2 = (x+2)^2 - 3$ has integer solutions.

Solution. Let $t = 2$ and $k = 3$. The congruence $y^2 \equiv -k \equiv -3 \pmod 4$ has a solution. By Theorem 3.16 (ii), $x^2 + y^2 = (x+2)^2 - 3$ has an integer solution. □

4 Concluding remarks

Although we have successfully proven many results concerning solutions to (1.1) and (1.2) over finite fields and the set of integers, several interesting problems remain open.

First of all, there are several cases which are not considered in Section 3.2. It is a challenging problem to find a complete set of solutions to (1.1) over an arbitrary finite field. As we mention above, the main challenges come from the fact that there are no known general formulas for square roots of elements in $\mathbb{F}_q$. For the case when q is an odd prime, one might try to develop a method for constructing the set of solutions using the Tonelli-Shanks or Cipolla's algorithm.

Secondly, our approach could also be applied to other families of quadratic equations. There are several known results in the two-variable cases over finite fields such as $x^2 - y^2 = 1$ and $x^2 + xy + y^2 = 1$ [2]. It might be plausible to investigate the number of solutions and the set of solutions of equations with three variables over finite fields or the integers using the results for equations with two variables.

Lastly, it would be desirable to obtain more complete results about the set of integer solutions to (1.2) when t is even. The computation seems much more involved in this case and does not require results over finite fields, so we plan to carry it out in our future work.

References

[1] A. Aabrandt and V. L. Hansen *A note on powers in finite fields*, Internat. J. Math. Ed. Sci. Tech. **47**(6) (2016), 987-–991.

[2] A. Aabrandt and V. L. Hansen *On quadratic curves over finite fields*, Preprint (2018) (arXiv:1802.10486)

[3] A. Aabrandt and V. L. Hansen *The circle equation over finite fields*, Quaest. Math. **41**(5) (2018), 665–674.

[4] J. Booher, *Square roots in finite fields and quadratic nonresidues*, Preprint (2012)

[5] W. Boyer, G. MacGillivray, L. Morrison, C. M. Mynhardt, and S. Nasserasr *Integer solutions to $x^2 + y^2 = z^2 - k$ for a fixed integer value k*, Involve **10**(5) (2017), 881–892.

[6] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[7] K. H. Rosen, *Elementary number theory and its applications*, 6th ed., Pearson, Massachusetts, 2011.