

SOLUTIONS TO QUADRATIC EQUATIONS OVER FINITE FIELDS

PUCHONG WONGKUMPRA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR MASTER OF SCIENCE
IN MATHEMATICS
FACULTY OF SCIENCE
BURAPHA UNIVERSITY
2022

COPYRIGHT OF BURAPHA UNIVERSITY

94494079
BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10
62910234_94494079

SOLUTIONS TO QUADRATIC EQUATIONS OVER FINITE FIELDS

944940 79
BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

PUCHONG WONGKUMPRA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR MASTER OF SCIENCE
IN MATHEMATICS
FACULTY OF SCIENCE
BURAPHA UNIVERSITY
2022

COPYRIGHT OF BURAPHA UNIVERSITY

The Thesis of Puchong Wongkumpra has been approved by the examining committee to be partial fulfilment of the requirements for the Master of Science in Mathematics of Burapha University

Advisory Committee

Principal advisor

..... Committee

(Asst. Prof. Dr. Detchat Samart)

Examining Committee

..... Committee

(Assoc. Prof. Dr. Chatchawan Panraksa)

..... Committee

(Asst. Prof. Dr. Detchat Samart)

..... Committee

(Asst. Prof. Dr. Areerak Chaiworn)

..... Dean of the Faculty of Science

(Assoc. Prof. Dr. Usavadee Tuntiwaranuruk)

Date January 30, 2023

This Thesis has been approved by Graduate School Burapha University to be partial fulfillment of the requirements for the Master of Science in Mathematics of Burapha University

..... Dean of Graduate School

(Assoc. Prof. Dr. Nujjaree Chaimongkol)

Date 17 February 2023

BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

ACKNOWLEDGEMENT

First, I would like to thank my thesis advisor, Asst. Prof. Dr. Detchat Samart, for supervising my thesis and teaching me mathematics. I will make all my knowledge useful in the future.

I also thank the Faculty of Science and the Department of Mathematics of Burapha University that have provided me with an ideal environment for studying and scholarship.

Finally, I would like to thank my family members for supporting my education. I hope they will be delighted with my academic achievement.

Puchong Wongkumpra

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

62910234 : MAJOR: MATHEMATICS; M.Sc. (MATHEMATICS)
KEYWORDS : FINITE FIELDS, QUADRATIC EQUATIONS.

PUCHONG WONGKUMPRA : SOLUTIONS TO QUADRATIC EQUATIONS OVER FINITE FIELDS. ADVISORY COMMITTEE: DETCHAT SAMART, Ph.D. 14 P. 2021.

In this thesis, we study equation $x^2 + y^2 = z^2 - k$ over finite fields, we find the number of solutions to this equation over finite fields and try to describe an elementary method for finding all solutions over $\mathbb{Z}_p$ where p is prime. Then, we describe a relationship between the solutions over some finite fields and the solutions over $\mathbb{Z}$.

944994079
BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

CONTENTS

Page

ABSTRACT ..... E

CONTENTS ..... F

CHAPTER

1. INTRODUCTION 1

Introduction 1

Research objectives 2

Scope of the study 3

2. PRELIMINARIES AND LITERATURE REVIEWS 4

Literature Reviews 5

Solutions to $x^2 + y^2 = (x + t)^2 - k$ over $\mathbb{Z}$ 5

Solutions over finite fields 6

Squares over finite fields 11

3. RESEARCH METHODOLOGY 13

4. SOLUTIONS TO QUADRATIC EQUATIONS OVER ..... FINITE FIELDS 14

4.1 The number of solutions to $x^2 + y^2 = z^2 - k$ over finite fields 14

4.2 The set of solutions to $x^2 + y^2 = z^2 - k$ over some finite fields ... 18

4.3 Solutions to $x^2 + y^2 = (x + t)^2 - k$ over the integers 21

5. CONCLUSION AND DISCUSSION 26

REFERENCES 29

BIOGRAPHY 30

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

CHAPTER 1

INTRODUCTION

Introduction

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

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 find integer solutions to linear Diophantine equations. However, this is not the case for quadratic equations.

In 2017, Boyer, MacGillivray, Morrison, Mynhardt and Nasserasr tried to find the integer solutions to

$$x^2 + y^2 = z^2 - k$$

for a fixed integer value k. Letting $z = x + t$ for some integer t, they have

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

and they find conditions on t for which the equation has integer solutions.

For the case $t = 0$, they have $y^2 = -k$ which has a solution if and only if $-k$ is a perfect square.

For the case $t > 0$, they have $y^2 = 2xt + t^2 - k$ which has a solution if and only if $y^2 \equiv t^2 - k \pmod{2t}$ has a solution.

For the case $t < 0$, they have $y^2 = 2(-x)(-t) + t^2 - k$ which has a solution if and only if $y^2 \equiv t^2 - k \pmod{-2t}$ has a solution.

For example, consider

$$x^2 + y^2 = z^2 - 3.$$

First, let $z = x + t$ where $t \in \mathbb{Z}$, then we have $x^2 + y^2 = (x + t)^2 - 3$.
If $t = 0$, we have $y^2 = -3$, which has no solutions.
If $t = 1$, we have $y^2 = 2x - 2$, whise has a solution if and only if $y^2 \equiv -2 \pmod 2$ has a solution. Since $0^2 \equiv -2 \pmod 2$, $y^2 = 2x - 2$ has a solution and we have $y = 2n$, $x = 2n^2 + 1$, $z = 2n^2 + 2$, where $n \in \mathbb{Z}$.

In this thesis, we will consider the same equation $x^2 + y^2 = z^2 - k$, but we consider only the solutions over finite fields.

For example, find all solutions to $x^2 + y^2 = z^2 - 1$ over $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.
Let $z = x + t$ where $t \in \mathbb{Z}_3$.
If $t = \bar{0}$, we have $y^2 = -1$ which has no solution.
If $t = \bar{1}$, we have $y^2 = 2x$ which has solutions $(x, y, z) = (\bar{0}, \bar{0}, \bar{1}), (\bar{2}, \bar{1}, \bar{0}), (\bar{2}, \bar{2}, \bar{0})$.
If $t = \bar{2}$, we have $y^2 = x$ which has solutions $(x, y, z) = (\bar{0}, \bar{0}, \bar{2}), (\bar{1}, \bar{1}, \bar{0}), (\bar{1}, \bar{2}, \bar{0})$.
Hence $x^2 + y^2 = z^2 - 1$ has 6 solutions over $\mathbb{Z}_3$.

Research objectives

1. Give conditions on t and k for which the equation $x^2 + y^2 = (x + t)^2 - k$ has a solution over finite fields.

2. Find the number of solutions to $x^2 + y^2 = z^2 - k$ over finite fields.

3. Describe an elementary method for finding all solutions over some finite fields.

4. Describe a relationship between the solutions over some finite field and the solutions over $\mathbb{Z}$.

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

Scope of the study

In this thesis, we study the equation $x^2 + y^2 = z^2 - k$ over finite fields and try to find the number of solutions over finite fields, describe method for finding solutions over some finite fields, and describe a relationship between the solutions over some finite fields and the solutions over $\mathbb{Z}$.

94494079
BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

94494079
BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

CHAPTER 2

PRELIMINARIES AND LITERATURE REVIEWS

In this chapter, we briefly discuss some background on finite fields, a quadratic residue, and preliminary results about solutions of quadratic equations over the integers and finite fields.

Definition 2.1. *(Mullen and Panario, 2013) A ring $(R, +, \cdot)$ is a nonempty set R together with two operations, $+$ and $\cdot$ such that :*
(1) $(R, +, \cdot)$ is an abelian group;
(2) $\cdot$ is associative, that is for all $a, b, c \in R, a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
(3) left and right distributive laws hold: for all $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and } (b + c) \cdot a = b \cdot a + c \cdot a.$$

Definition 2.2. *(Mullen and Panario, 2013) Let R be a ring.*
(1) R is a ring with identity if the ring has a multiplicative identity;
(2) R is commutative if $\cdot$ is commutative;
(3) R is an integral domain if it is commutative with identity and $a \cdot b = 0$ implies $a = 0$ or $b = 0$, for any $a, b \in R$;
(4) R is a division ring (also called a skew field) if the nonzero element of R form a group under $\cdot$;
(5) R is a field if it is a commutative division ring.

Examples of fields : $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{p-1}\}$ where $\bar{a} = \{kp + a : k \in \mathbb{Z}\}$ and p is prime.

Definition 2.3. *A field $\mathbb{F}$ is a finite field if $\mathbb{F}$ is a finite set.*

Definition 2.4. *(Mullen and Panario, 2013) The order of a finite field $\mathbb{F}$ is the number of distinct elements in $\mathbb{F}$.*

Examples of finite fields include $\mathbb{Z}_p$, where p is prime and $\mathbb{Z}_p[x]/\langle f(x)\rangle$, where $\mathbb{Z}_p[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : n \in \mathbb{N} \cup \{0\}$ and $a_0, a_1, a_2, ..., a_n \in \mathbb{Z}_p\}$, $f(x)$ is irreducible in $\mathbb{Z}_p[x]$. If $deg(f(x)) = m$, then $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a finite field of order p^m.

Definition 2.5. *(Mullen and Panario, 2013) If R is a ring and there exists a positive integer n such that $nr = 0$ for all $r \in R$, then the least such positive integer n is called the characteristic of R. Otherwise, we say that R has characteristic zero.*

Definition 2.6. *(Mullen and Panario, 2013) A field containing no proper subfield is called a prime field.*

Theorem 2.7. *(Mullen and Panario, 2013) Let $\mathbb{F}$ be a finite field. The cardinality of $\mathbb{F}$ is p^n, where p is p is the prime characteristic of $\mathbb{F}$ and n is the dimension of $\mathbb{F}$ over its prime subfield. A finite field with q elements is denoted by $\mathbb{F}_q$.*

Definition 2.8. *(Apostol, 1976) Let $n \in \mathbb{Z}$ and $p \in \mathbb{N}$.*
If the congruence $x^2 \equiv n \pmod{p}$ has a solution we say that n is a quadratic residue modulo p .
If the congruence $x^2 \equiv n \pmod{p}$ has no solution we say that n is a quadratic non-residue modulo p .

Literature Reviews

Solutions to $x^2 + y^2 = (x + t)^2 - k$ over $\mathbb{Z}$

In the article Integer solutions to $x^2 + y^2 = z^2 - k$ for a fixed integer value k the authors studied the integer solutions of equation $x^2 + y^2 = (x + t)^2 - k$. They obtain many important results as follows.

Theorem 2.9. *(Boyer et al., 2017) Let t is positive integer, then the equation $x^2 + y^2 = (x + t)^2 - k$ has an integer solution if and only if $y^2 \equiv t^2 - k \pmod{2t}$ has a solution.*

To illustrate theorem 2.9, let us consider the following example.

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

Example 2.10. *Consider* $x^2 + y^2 = (x+2)^2 - 1$.
Since $y^2 \equiv 3 \pmod 4$ *has no solution,* $x^2 + y^2 = (x+2)^2 - 1$ *has no integer solution.*

Theorem 2.11. *(Boyer et al., 2017) Let* t *is odd, we have*
(1) If k *is even, then* $x^2 + y^2 = (x+t)^2 - k$ *has an integer solution if and only if* $y^2 \equiv -k \pmod t$ *has an odd solution.*
(2) If k *is odd, then* $x^2 + y^2 = (x+t)^2 - k$ *has an integer solution if and only if* $y^2 \equiv -k \pmod t$ *has an even solution.*

To illustrate theorem 2.11, let us consider the following example.

Example 2.12. *Consider* $x^2 + y^2 = (x+3)^2 - 4$.
Since $y^2 \equiv -4 \pmod 3$ *has no odd solution,* $x^2 + y^2 = (x+3)^2 - 4$ *has no integer solution.*

Example 2.13. *Consider* $x^2 + y^2 = (x+5)^2 - 1$.
Since $y^2 \equiv -1 \pmod 5$ *has an even solution,* $x^2 + y^2 = (x+5)^2 - 1$ *has an integer solution.*

Theorem 2.14. *(Boyer et al., 2017) Let* t *is even, then* $x^2 + y^2 = (x+t)^2 - k$ *has an integer solution if and only if* $y^2 \equiv -k \pmod{2t}$ *has a solution.*

To illustrate theorem 2.14, let us consider the following example.

Example 2.15. *Consider* $x^2 + y^2 = (x+4)^2 - 3$.
Since $y^2 \equiv -3 \pmod 8$ *has no solution,* $x^2 + y^2 = (x+4)^2 - 3$ *has no solution.*

Solutions over finite fields

Aabrandt and Hansen studied the number of solutions over finite fields of some quadratic equations as follows :

1. The circle equation $x^2 + y^2 = 1$

Theorem 2.16. *(Aabrandt and Hansen, 2018) For any finite field* $\mathbb{F}_{p^n}$ *of characteristic* p*, the number of solutions to* $x^2 + y^2 = 1$ *is* $p^n - \sin\left(p^n \frac{\pi}{2}\right)$.

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

2. The hyperbolic equation $x^2 - y^2 = 1$

Theorem 2.17. *(Aabrandt and Hansen, 2018) Over the finite field $\mathbb{F}_{2^n}$, the number of solutions to $x^2 - y^2 = 1$ is 2^n.*

Theorem 2.18. *(Aabrandt and Hansen, 2018) Over the finite field $\mathbb{F}_{p^n}$,where $p \geq 3$, the number of solutions to $x^2 - y^2 = 1$ is $p^n - 1$.*

3. The parabolic equation $y = x^2$

Theorem 2.19. *(Aabrandt and Hansen, 2018) Over the finite field $\mathbb{F}_{p^n}$, the number of solutions to $y = x^2$ is p^n.*

4. The quadratic equation with mixed term $x^2 + xy + y^2 = 1$

Theorem 2.20. *(Aabrandt and Hansen, 2018) Over the finite field $\mathbb{F}_{2^n}$, the number of solutions to $x^2 + xy + y^2 = 1$ is $2^n + (-1)^{n-1}$.*

Theorem 2.21. *(Aabrandt and Hansen, 2018) Over the finite field $\mathbb{F}_{3^n}$, the number of solutions to $x^2 + xy + y^2 = 1$ is $2 \cdot 3^n$.*

Theorem 2.22. *(Aabrandt and Hansen, 2018) Over the finite field $\mathbb{F}_{7^n}$, the number of solutions to $x^2 + xy + y^2 = 1$ is $7^n - 1$.*

To illustrate the results of Aabrandt and Hansen, we consider the solutions of the four equations above over $\mathbb{Z}_3$

Example 2.23. *Over $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, we have the following.*

equations	number of solutions	solutions
$x^2 + y^2 = 1$	$3^1 - \sin\left(\frac{3^1\pi}{2}\right) = 4$	$(\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{0}, \bar{2}), (\bar{2}, \bar{0})$
$x^2 - y^2 = 1$	$3^1 - 1 = 2$	$(\bar{1}, \bar{0}), (\bar{2}, \bar{0})$
$y = x^2$	$3^1 = 3$	$(\bar{0}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})$
$x^2 + xy + y^2 = 1$	$2 \cdot 3^1 = 6$	$(\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{2}), (\bar{2}, \bar{0}), (\bar{2}, \bar{1})$

We briefly discuss a method that Aabrandt and Hansen use to prove Theorem 2.16 below. The remaining theorem can be proven in a similar manner. Let N_{p^n} be a number of solutions to $x^2 + y^2 = 1$ over $\mathbb{F}_{p^n}$. For the case $p = 2$, over $\mathbb{F}_{2^n}$, we have

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

$$(x+y)^2 = x^2 + y^2 \text{ and } (xy)^2 = x^2y^2 \text{ for any } x, y \in \mathbb{F}_{2^n}.$$

It can be shown that the power map $x^2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an isomorphism, so

$$(x+y)^2 = 1 \text{ if and only if } x + y = 1.$$

This implies that for every $x \in \mathbb{F}_{2^n}$, there exists a unique $y = 1 - x \in \mathbb{F}_{2^n}$ such that

$$x^2 + y^2 = (x+y)^2 = 1.$$

This proves that the equation $x^2 + y^2 = 1$ has exactly 2^n solutions. Therefore

$$N_{2^n} = 2^n = 2^n - \sin\left(2^n \frac{\pi}{2}\right).$$

For the case $p \geq 3$, let $q = p^n$. The multiplicative group $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ is a cyclic group of order $q-1$, generated by some element $g \in \mathbb{F}_q^\times$. Thus for every element $x \in \mathbb{F}_q^\times$ we have $x = g^k$, where $k \in \{0, 1, 2, ..., q-2\}$.

Define the multiplicative homomorphism $\eta : \mathbb{F}_q^\times \to \mathbb{S}$ of $\mathbb{F}_q^*$ onto the multiplicative group $\mathbb{S} = \{-1, 1\}$ by

$$\eta(g^k) = (-1)^k \text{ for every } g^k \in \mathbb{F}_q^\times.$$

For convenience we set $\eta(0) = 0$.

Consider the squaring homomorphism $x^2 : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ map the element $g^l \in \mathbb{F}_q^\times$ to $g^{2l} \in \mathbb{F}_q^\times$. Thus

$$c = g^k \text{ is a square in } \mathbb{F}_q^\times \text{ if and only if } k \text{ is even.}$$

Then

$$c = g^k \text{ is a square in } \mathbb{F}_q^\times \text{ if and only if } \eta(c) = 1.$$

Hence there are equally many squares and non-squares in $\mathbb{F}_q^\times$ and η does not depend on g. It follows that

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

The number of solutions N_q equal to a sum of products of the number of solutions $N_q(x^2 = c_1)$ and $N_q(y^2 = c_2)$ to the equations $x^2 = c_1$ and $y^2 = c_2$ for $c_1, c_2 \in \mathbb{F}_q$ with $c_1 + c_2 = 1$. Hence

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

$$N_q = \sum_{c_1+c_2=1} N_q(x^2 = c_1)N_q(y^2 = c_2).$$

Consider $z^2 = c$ over $\mathbb{F}_q^\times$.

If c is a square then $z^2 = c$ has exactly two solutions.

If c is a non-square then $z^2 = c$ has no solutions. Thus

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

Let

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

We have that S is the number of solutions in $\mathbb{F}_q$ to the quadratic equation

$$(2c-1)^2 - 1 = a^2, \text{ which can be rewritten as}$$

$$(2c-1+a)(2c-1-a) = 1.$$

Let $\alpha = 2c-1+a$, then $\alpha^{-1} = 2c-1-a$.

Thus $a = 2^{-1}(\alpha - \alpha^{-1})$ and $c = 2^{-1}[\alpha + 1 - 2^{-1}(\alpha - \alpha^{-1})]$. Suppose there exist $\alpha, \beta \in \mathbb{F}_q^\times$ such that $2^{-1}(\alpha - \alpha^{-1}) = 2^{-1}(\beta - \beta^{-1})$ and $2^{-1}[\alpha + 1 - 2^{-1}(\alpha - \alpha^{-1})] = 2^{-1}[\beta + 1 - 2^{-1}(\beta - \beta^{-1})]$. Then it follows easily that $\alpha + 1 = \beta + 1$, so $\alpha = \beta$.

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

Since a and c are uniquely determined by a choice of $\alpha \in \mathbb{F}_q^\times$ and since the order of $\mathbb{F}_q^\times$ is $q-1$, we conclude that $S = q-1$. Hence

$$\begin{aligned} N_q &= q + \eta(-1)(-q) + \eta(-1)(q-1) \\ &= q - \eta(-1). \end{aligned}$$

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

Next, we find the value of $\eta(-1)$, i.e. to determine whether -1 is a square in $\mathbb{F}_q^\times$.
Suppose $x = g^l$, $1 \leq l < \dfrac{q-1}{2}$, is an element with $x^2 = g^{2l} = -1$.
Then $g^{4l} = g^{2l}g^{2l} = (-1)(-1) = 1 = g^0$. Thus

$$4l \equiv 0 \ \ (mod \ \ q-1).$$

Since q is odd, $q = 4k+1$ or $q = 4k+3$, for k a non-negative integer.
If $q = 4k+1$, we have $1 \leq l < 2k$ and

$$4l \equiv 0 \ \ (mod \ \ 4k)$$

has a solution if k divides l. Since $l = k$ such that k divides l, the congruence has a solution. Hence -1 is a square in $\mathbb{F}_q^\times$ for $q = 4k+1$.
If $q = 4k+3$, we have $1 \leq l < 2k+1$ and

$$4l \equiv 0 \ \ (mod \ \ 4k+2)$$

has a solution if $2k+1$ divides $2l$. Since the odd number $2k+1$ can never be a proper factor in an even number $2l < 4k+2$, this implies that the congruence has no solutions. Hence -1 is a non-square in $\mathbb{F}_q^\times$ for $q = 4k+3$.
Therefore

$$\eta(-1) = \begin{cases} 1 & \text{if } q \equiv 1 \ \ (mod \ \ 4), \\ -1 & \text{if } q \equiv 3 \ \ (mod \ \ 4). \end{cases}$$

So

$$\eta(-1) = \sin\left(q\frac{\pi}{2}\right).$$

Finally, we have

$$N_{p^n} = p^n - \sin\left(p^n\frac{\pi}{2}\right).$$

We expect that the method of Aabrandt and Hansen could be applied to obtain similar results for the equation $x^2 + y^2 = (x+t)^2 - k$.

Squares over finite fields

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 basic result.

Theorem 2.24. *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 a paper *A note on powers in finite fields*. □

By the proof of Theorem 2.24 (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 of a in $\mathbb{F}_p$.

Theorem 2.25. *(Cohen et al., 2006) 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 involved; there are no known formulas similar to those in Theorem 2.25. Although there are certain algorithms such as the Tonelli-Shanks algorithm and Cipolla's

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

algorithm which can be used 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 thesis.

94494079
BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

CHAPTER 3

RESEARCH METHODOLOGY

In this chapter, we will describe the process of studying the equation

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

as follows:

1. We find solutions of the equation over $\mathbb{Z}_p$ where p is prime. At the beginning, we do computations over some $\mathbb{Z}_p$ by substituting elements of $\mathbb{Z}_p$. Then we make an observation about t and k for which the equation has solutions and we make a prediction about the number of solutions to $x^2 + y^2 = z^2 - k$ over $\mathbb{Z}_p$ from our observation.

2. We prove our conjectures about the number of solutions of the equation over $\mathbb{Z}_p$.

3. We try to extend the result above to finite fields $\mathbb{F}_{p^n}$.

4. We describe a method for finding solutions over some finite fields.

5. We compare solutions of the equation over $\mathbb{Z}$ with solutions over some finite fields and try to find a relationship between them.

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

CHAPTER 4

SOLUTIONS TO QUADRATIC EQUATIONS OVER FINITE FIELDS

In this section, we establish results concerning the number of solutions to $x^2 + y^2 = z^2 - k$ over an arbitrary finite field. We also find the set of solutions to $x^2 + y^2 = z^2 - k$ 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 $x^2 + y^2 = (x + t)^2 - k$.

4.1 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 4.1. *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 2.24 (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 2.16. 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 $\mathbb{F}_q^\times = \{g^k \mid 1 \leq k \leq q - 1\}$. 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 2.24 (ii) that

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

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

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 for the sake of completeness.

Proposition 4.2. *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 2.24 (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. □

Theorem 4.3. *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 2.24(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 $z_0 = x_0 + t_0$. 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 $\mathbb{F}_q$. □

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

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

Lemma 4.4. *Let $q = p^n$, where p is an odd prime and $n \in \mathbb{N}$. Over $\mathbb{F}_q$, the equation*

$$x^2 + y^2 = z^2, \text{ with } z \neq 0, \tag{4.1}$$

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 2.16. Since there are $q - 1$ nonzero elements in $\mathbb{F}_q$, we have that (4.1) has $(q-1)(q - \sin(q\pi/2))$ solutions in total. □

Theorem 4.5. *Let $q = p^n$, where p is an odd prime and $n \in \mathbb{N}$. Over $\mathbb{F}_q$, the equation*

$$x^2 + y^2 = z^2, \tag{4.2}$$

has q^2 solutions.

Proof. Let N_q be the number of solutions of the form $(x_0, y_0, 0)$. Then by Lemma 4.4 and Proposition 4.2 we have that the number of solutions to (4.2) 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 4.6. *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 4.1, 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 $x^2 + y^2 = z^2 - k$ 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 4.2, this equation has either $2q - 1$ or 1 solutions in $\mathbb{F}_q$, depending on

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

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 4.1, 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 $M_q + (q-2)(q - \sin\frac{q\pi}{2}) = q(q + \sin(q\pi/2))$. □

4.2 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 $x^2 + y^2 = z^2 - k$ over any finite field $\mathbb{F}_q$. Next, we will describe a method for finding all solutions of $x^2 + y^2 = z^2 - k$ 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 not congruent to 1 modulo 8. The case when q is a prime congruent to 1 modulo 8 seems much harder to analyze due to the lack of explicit formulas for square roots in $\mathbb{F}_q$. We again start by considering solutions over finite fields of characteristic 2.

Theorem 4.7. *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 4.3 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 2.24 (i) that $w = k^{2^{n-1}} = k^{\frac{q}{2}}$. □

Example 4.8. *The Galois field of order 4 is the set $\{0, 1, a, b\}$ with addition and multiplication defined by the following Cayley tables.*

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

$+$	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 4.7, 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 2.25 to establish the following results.

Lemma 4.9. *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 2.25 (i) that $(x,y) = (\pm t^{\frac{p+1}{4}}, \pm(1-t)^{\frac{p+1}{4}})$. □

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

Theorem 4.10. *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 4.2, 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 4.9, 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 4.11. *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 4.12. *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

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

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

It follows from Theorem 4.11 that all solutions to $x^2 + y^2 = z^2 - 4$ over $\mathbb{Z}/7\mathbb{Z}$ are

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

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

Remark. One can use a similar approach to obtain formulas for the solutions to $x^2 + y^2 = z^2 - k$ over $\mathbb{F}_p$, where p is a prime congruent to 5 modulo 8, with the aid of Theorem 2.25 (ii)-(iii). However, the calculation seems much more involved in these cases, so we decided not to include them here.

4.3 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 $x^2 + y^2 = (x + t)^2 - k$. More precisely, we find the conditions on t and k for which $x^2 + y^2 = (x + t)^2 - k$ has solutions. In some cases, we also obtain formulas for computing the set of integer solutions as by-products.

By Theorem 4.7, we immediately obtain the following result.

Proposition 4.13. *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 4.14. *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 4.13, 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 4.15. *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 4.16. *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.*

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

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 4.14 (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 4.15 (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 4.14 (iv) and Theorem 4.15 (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 4.14 (iii)-(iv) and Theorem 4.15 (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 t even, we have the following criterion.

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

Theorem 4.17. *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 Theorem 2.14 (Boyer et al., 2017).

□

Example 4.18. *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 4.16. □

Example 4.19. *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 4.16, $x^2 + y^2 = (x + 5)^2 - 4$ 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

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

□

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

Example 4.20. *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 4.16, $x^2 + y^2 = (x-7)^2 + 15$ 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 4.21. *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 4.17 (ii), $x^2 + y^2 = (x+2)^2 - 3$ has an integer solution. □

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

CHAPTER 5

CONCLUSION AND DISCUSSION

In this section, we give a conclusion of this thesis. We will specify the following as set out in the research objectives:

1. We find that for any t and k the equation $x^2 + y^2 = (x + t)^2 - k$ always has solutions over finite fields, as a result of Theorem 4.3 and Theorem 4.6 which that the number of solutions of the equation $x^2 + y^2 = z^2 - k$ over any finite field is a non-zero, then implies.

2. From Section 4.1, we obtain the number of solutions of the equation $x^2 + y^2 = z^2 - k$ on finite fields as follows:

   2.1 (Theorem 4.3) 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.

   2.2 (Theorem 4.6) 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 $q\left(q - \sin\frac{q\pi}{2}\right)$ solutions.

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

3. We give the general solutions of the equation $x^2 + y^2 = z^2 - k$ over some finite fields as follows:

   3.1 (Theorem 4.7) 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 $\{(x_0, t - k^{\frac{q}{2}}, x_0 + t) \mid x_0, t \in \mathbb{F}_q\}$.

   3.2 (Theorem 4.11) 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 $\mathbb{F}_p$.

4. To describe the existence of integer solutions to the equation $x^2+y^2 = (x+t)^2-k$, we start by observing the solutions of the equation $x^2 + y^2 = (x + t)^2 - k$ over

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

$\mathbb{Z}_2$. Then we extend the result to the integer solutions as follows:

4.1 (Theorem 4.16) 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.

4.2 (Theorem 4.11) 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.

Although we have successfully proven many results concerning solutions to $x^2 + y^2 = z^2 - k$ and $x^2 + y^2 = (x+t)^2 - k$ 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 4.2. It is a challenging problem to find a complete set of solutions to $x^2 + y^2 = z^2 - k$ 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 $x^2 + xy + y^2 = 1$. 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.

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

Lastly, it would be desirable to obtain more complete results about the set of integer solutions to $x^2 + y^2 = (x + t)^2 - k$ 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.

94494079
BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10

REFERENCES

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

Aabrandt, A., & Hansen, V. L. (2018). On quadratic curves over finite fields. *Preprint.*

Aabrandt, A., & Hansen, V. L. (2018). The circle equation over finite fields. *Quaestiones Mathematicae, 41*(5), 665-674.

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

Boyer, W., MacGillivray, G., Morrison, L., Mynhardt, C. M., & Nasserasr, S. (2017). Integer solutions to $x^2 + y^2 = z^2 - k$ for a fixed integer valule k. *Involve a Journal of Mathematics, 10*(5), 881-892.

Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., & Vercauteren, F. (2006). Handbook of elliptic and hyperelliptic curve cryptography. *Discrete Mathematics and its Applications.*

Meemark, Y. (2015). *Abstract Algebra.* Bangkok: Danex Intercorporation Co., Ltd.

Mullen, G. L., & Panario, D. (2013). *Handbook of Finite Fields.* New York: CRC Press.

94494079 BUU iThesis 62910234 thesis / recv: 05012566 13:41:51 / seq: 10