โครงการ

การเรียนการสอนเพื่อเสริมประสบการณ์

ชื่อโครงการ คลาสของจำนวนเฉพาะที่เขียนได้ด้วยรูปแบบกำลังสอง

A class of primes represented by some quadratic forms

ชื่อนิสิต นางสาววรินทร พงษ์สำราญกุล 593 35448 23

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์

สาขาวิชา คณิตศาสตร์

ปีการศึกษา 2562

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

คลาสของจำนวนเฉพาะที่เขียนได้ด้วยรูปแบบกำลังสอง

นางสาววรินทร พงษ์สำราญกุล

โครงงานนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต

สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2562

A class of primes represented by some quadratic forms

Miss Warintorn Pongsumrankul

A Project Submitted in Partial Fulfillment of the Requirements

for the Degree of Bachelor of Science Program in Mathematics

Department of Mathematics and Computer Science

Faculty of Science

Chulalongkorn University

Academic Year 2019

หัวข้อโครงงาน	คลาสของจำนวนเฉพาะที่เขียนได้ด้วยรูปแบบกำลังสอง
โดย	นางสาววรินทร พงษ์สำราญกุล เลขประจำตัว 5933544823
สาขาวิชา	คณิตศาสตร์
อาจารย์ที่ปรึกษาโครงงาน	รองศาสตราจารย์ ดร.ตวงรัตน์ ไชยชนะ

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับโครงงานฉบับนี้เป็นส่วนหนึ่ง ของการศึกษาตามหลักสูตรปริญญาบัณฑิต ในรายวิชา 2301499 โครงงานวิทยาศาสตร์ (Senior Project)

.... หัวหน้าภาควิชาคณิตศาสตร์
และวิทยาการคอมพิวเตอร์

(ศาสตราจารย์ ดร.กฤษณะ เนียมมณี)

คณะกรรมการสอบโครงงาน

.... อาจารย์ที่ปรึกษาโครงงาน

(รองศาสตราจารย์ ดร.ตวงรัตน์ ไชยชนะ)

.... กรรมการ

(ศาสตราจารย์ ดร.พัฒนี อุดมกะวานิช)

.... กรรมการ

(รองศาสตราจารย์ ดร.เอื้อมพร ฟักสุวรรณ)

วรินทร พงษ์สำราญกุล: คลาสของจำนวนเฉพาะที่เขียนได้ด้วยรูปแบบกำลังสอง (A CLASS OF PRIMES REPRESENTED BY SOME QUADRATIC FORMS) อ.ที่ปรึกษาโครงงาน: รศ.ดร. ตวงรัตน์ ไชยชนะ, 43 หน้า

ให้ p เป็นจำนวนเฉพาะ เรากล่าวว่า p มีรูปแบบกำลังสองแบบทวินามเหนือจำนวนเต็ม $f(x,y) = ax^2 + bxy + cy^2$ ถ้ามีจำนวนเต็ม m และ n ที่ $f(m,n) = p$ ในโครงงานนี้เราหาคลาสของจำนวนเฉพาะที่เขียนแทนได้ด้วยรูปแบบกำลังสองแบบทวินามเหนือจำนวนเต็มบางรูปแบบ

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต วรินทร

สาขาวิชา คณิตศาสตร์ ลายมือชื่ออ.ที่ปรึกษาโครงงาน ตวงรัตน์

ปีการศึกษา 2562

5933544823 : MAJOR MATHEMATICS.

KEYWORDS: PRIME, BINARY QUADRATIC FORM

WARINTORN PONGSUMRANKUL: A CLASS OF PRIMES REPRESENTED BY SOME QUADRATIC FORMS. ADVISOR: ASSOC.PROF. TUANGRAT CHAICHANA, PH.D., 43 PP.

Let p be a prime number. An integral binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ represents p if there exist $m, n \in \mathbb{Z}$ such that $f(m, n) = p$. In this project, we find a class of primes represented by some integral binary quadratic forms.

Department	Mathematics and Computer Science	Student's Signature	Warintorn
Field of Study	Mathematics	Advisor's Signature	T. Chaichana
Academic Year	2019		

Acknowledgments

I sincerely thank to my project advisor, Assoc.Prof. Dr. Tuangrat Chaichana, for her valuable help and constant encouragement throughout the course of this project. I am most grateful to work with her. I have learnt many things from her by her teaching, her advice and our work experience. Thanks to my project committee: Prof.Dr. Patanee Udomkavanich and Assoc.Prof.Dr. Oumporn Phuksuwan for their suggestions and comments. In addition, I wish to express my thankfulness to His Majesty King Maha Vajiralongkorn Bodindradebayavarangkun for giving me the scholarship in two previous semester. Finally, thanks to my friends and my family for their support throughout my education. This project is funded by His Majesty King Maha Vajiralongkorn Bodindradebayavarangkun and Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University.

Contents

Chapter 1

Introduction

1.1 Background in Number theory

We begin by giving the basic definitions and theorems of number theory, see [2], which are used in this project.

1.1.1 Divisibility

First, we explain the concepts of divisibility of integers.

Definition 1.1. *Let a and b be integers such that $a \neq 0$. We say that b is* ***divisible by*** *a if there is an integer x such that $b = ax$, and we write $a \mid b$.*

Other language for the divisibility property $a \mid b$ is that a divides b. The integer a is called a ***divisor*** *of b, and that b is called a* ***multiple*** *of a.*

Theorem 1.2. *Let a, b, c and d be integers. Then*

1. $a \mid 0, 1 \mid a$ *and* $a \mid a$;
2. *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$;
3. *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$;
4. *If* $a > 0$ *and* $b > 0$ *and* $a \mid b$, *then* $a \leq b$;
5. $a \mid b$ *if and only if* $\forall m \in \mathbb{Z} \diagdown \{0\},\ ma \mid mb$;
6. *If* $a \mid b$ *and* $a \mid c$, *then* $\forall x, y \in \mathbb{Z},\ a \mid (bx + cy)$.

The next theorem is an important theorem about divisibility which will be used to create conditions regarding divisibility for further using.

Theorem 1.3. ***The division algorithm.*** *Given any integers a and b, with $a \neq 0$, there exist unique integer q and r such that*

$$b = qa + r, \ 0 \leq r < \mid a \mid .$$

If $a \nmid b$, then r satisfies the stronger inequalities $0 < r < \mid a \mid$.

*Here q is called the **quotient** and r is called the **remainder** obtained by dividing b by a.*

Definition 1.4. *Let b and c be integers. The integer a is a **common divisor** of b and c if $a \mid b$ and $a \mid c$. If at least one of b and c is not 0, the greatest among their common divisor is called the **greatest common divisor**, denoted by $gcd(b, c)$.*

Definition 1.5. *We say that a and b are **relatively prime** in case $gcd(a, b) = 1$, and that $a_1, a_2, ..., a_n$ are relatively prime in case $gcd(a_1, a_2, ..., a_n) = 1$. We say that $a_1, a_2, ..., a_n$ are **relatively prime in pair** in case $gcd(a_i, a_j) = 1$ for all $i = 1, 2, ..., n$ and $j = 1, 2, ..., n$ with $i \neq j$.*

Theorem 1.6. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $gcd(a, b) = 1$, then $a \mid c$.*

1.1.2 Congruences

Next, we will explain the concepts of the congruences.

Definition 1.7. *Given integers a, b, m with $m > 0$. We say that a is **congruent to** b **modulo** m, and we write*

$$a \equiv b \ (mod \ m),$$

*if m divides the difference $a - b$. The number m is called the **modulus** of the congruence.*

In other words, the congruence is equivalent to the divisibility relation

$$m \mid (a - b).$$

In particular, $a \equiv 0 \ (mod \ m)$ if and only if $m \mid a$. Hence $a \equiv b \ (mod \ m)$ if and only if $a - b \equiv 0 \ (mod \ m)$.

Remark.

1. *For all $n \in \mathbb{Z}$, n is even if and only if $n \equiv 0 \ (mod \ 2)$,*

2. *For all $n \in \mathbb{Z}$, n is odd if and only if $n \equiv 1 \ (mod \ 2)$,*

3. *For all* $a, b, m \in \mathbb{Z}$, *if* $a \equiv b \pmod{m}$, *then* $a \equiv b \pmod{d}$ *when* $d \mid m, d > 0$.

Theorem 1.8. *Congruence is an equivalence relation. that is, we have: For all* $m \in \mathbb{Z}^+$

1. ***reflexivity:*** $\forall a \in \mathbb{Z}, a \equiv a \pmod{m}$;
2. ***symmetry:*** $\forall a, b \in \mathbb{Z}$, *if* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$;
3. ***transitivity:*** $\forall a, b, c \in \mathbb{Z}$, *if* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.

Theorem 1.9. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then we have:*

1. $ax + cy \equiv bx + dy \pmod{m}$ *for all integer* x *and* y,
2. $ac \equiv bd \pmod{m}$,
3. $a^n \equiv b^n \pmod{m}$, *for every positive integer* n.

1.1.3 Quadratic Residue and the Quadratic Raciprocity Law

Definition 1.10. *Let* a *and* m *be relatively prime integers, with* $m \geq 1$. a *is called a* ***quadratic residue modulo*** m *if the congruence*

$$x^2 \equiv a \pmod{m}$$

has a solution. If it has no solution, then a *is called a* ***quadratic non-residue modulo*** m.

Examples 1.11. *To find the quadratic residues modulo* 12 *we square the numbers* $1, 2, ..., 11$ *and reduce mod* 12. *We obtain*

$$1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1, 2^2 \equiv 4^2 \equiv 8^2 \equiv 10^2 \equiv 4, 3^2 \equiv 9^2 \equiv 9 \pmod{12}.$$

Consequently, the quadratic residues modulo 12 *are* $1, 4, 9$, *and the non-residues are* $2, 3, 5, 6, 7, 8, 10, 11$.

Definition 1.12. *Let* p *be an odd prime and* n *an integer with* $n \not\equiv 0 \pmod{p}$. *We define* ***Legendre's symbol*** $\left(\frac{n}{p}\right)$ *as follows:*

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a quadratic residue mod } p, \\ -1 & \text{if } n \text{ is a quadratic nonresidue mod } p. \end{cases}$$

If $n \equiv 0 \pmod{p}$, *we define* $\left(\frac{n}{p}\right) = 0$.

Examples 1.13. *From* $4^2 \equiv 3$ $(mod\ 13)$, 3 *is a quadratic residue mod* 13. *Hence* $\left(\frac{3}{13}\right) = 1$.

Examples 1.14. *Since the congruence* $x^2 \equiv 2$ $(mod\ 13)$ *has no solution,* 2 *is a quadratic nonresidue mod* 13. *Hence* $\left(\frac{2}{13}\right) = -1$.

Corollary 1.15. *Let* p *be an odd prime. Then for all integers* m, n *we have* $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$ *whenever* $m \equiv n$ $(mod\ p)$.

Theorem 1.16. ***Euler's criterion.*** *Let* p *be an odd prime. Then for all integer* n *we have*

$$\left(\frac{n}{p}\right) \equiv n^{(p-1/2)} \ (mod\ p).$$

Examples 1.17. $\left(\frac{3}{13}\right) \equiv 3^{(13-1)/2} \equiv 3^{12/2} \equiv 3^6 \equiv 729 \equiv 1$ $(mod\ 13)$. *Therefore* $\left(\frac{3}{13}\right) = 1$ *and so* 3 *is a quadratic residue mod* 13.

Theorem 1.18. *Let* p *be an odd prime and* m, n *be integers. Then*

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

Theorem 1.19. *For an odd prime* p *we have*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } \ p \equiv 1 \ (mod\ 4), \\ -1 & \text{if } \ p \equiv 3 \ (mod\ 4). \end{cases}$$

Examples 1.20. $\left(\frac{-1}{13}\right) = 1$ *because* $13 \equiv 1$ $(mod\ 4)$ *and* $\left(\frac{-1}{7}\right) = -1$ *because* $7 \equiv 3$ $(mod\ 4)$.

Theorem 1.21. *For every odd prime* p *we have*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } \ p \equiv \pm 1 \ (mod\ 8), \\ -1 & \text{if } \ p \equiv \pm 3 \ (mod\ 8). \end{cases}$$

The following theorem provides a useful tool for computing Legendre symbols.

Theorem 1.22. ***The Quadratic Reciprocity law.*** *If* p *and* q *are distinct odd prims, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Examples 1.23. *From Theorem* 1.22*, we have*

$$\begin{aligned}\left(\frac{7}{13}\right) &= \left(\frac{13}{7}\right)(-1)^{\left(\frac{7-1}{2}\right)\left(\frac{13-1}{2}\right)} = \left(\frac{13}{7}\right) = \left(\frac{6}{7}\right) \\ &= \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = (-1)^{\left(\frac{7^2-1}{8}\right)}\left(\frac{3}{7}\right) = \left(\frac{3}{7}\right).\end{aligned}$$

Since

$$\left(\frac{3}{7}\right) \equiv 3^{\frac{7-1}{2}} \equiv 27 \equiv -1 \ (mod\ 7),$$

$\left(\frac{7}{13}\right) = 1$ *and so* 7 *is a quadratic nonresidue mod* 13.

Definition 1.24. *Let P be an odd integer with prime factorization*

$$P = \prod_{i=1}^{r} p_i^{\alpha_i}. \tag{1.1}$$

The ***Jacobi symbol*** $\left(\frac{n}{p}\right)$ *is defined for all integers n by the equation*

$$\left(\frac{n}{P}\right) = \prod_{i=1}^{r}\left(\frac{n}{p_i}\right)^{\alpha_i},$$

where $\left(\frac{n}{p_i}\right)$ *is the Legendre symbol. We also define* $\left(\frac{n}{1}\right) = 1$ *and the possible values of* $\left(\frac{n}{P}\right)$ *are* $1, -1,$ *or* 0.

Remark. *If the congruence*

$$x^2 \equiv n \ (mod\ P)$$

has a solution and $\left(\frac{n}{P}\right) = \prod_{i=1}^{r}\left(\frac{n}{p_i}\right)^{\alpha_i}$, *then* $\left(\frac{n}{p_i}\right) = 1$ *for each prime p_i, and hence* $\left(\frac{n}{P}\right) = 1$. *But the converse is not true because* $\left(\frac{n}{P}\right)$ *can be* 1 *if an even number of factors* -1 *appears in (1.1).*

Examples 1.25. *We have* $\left(\frac{2}{9}\right) = 1$ *but the congruence* $x^2 \equiv 2 \ (mod\ 9)$*has no solution.*

Theorem 1.26. *If P and Q are odd positive integers, then*

1. $\left(\frac{m}{P}\right)\left(\frac{n}{P}\right) = \left(\frac{mn}{P}\right)$,
2. $\left(\frac{n}{P}\right)\left(\frac{n}{Q}\right) = \left(\frac{n}{PQ}\right)$,

3. $\left(\frac{m}{P}\right) = \left(\frac{n}{P}\right)$ *whenever* $m \equiv n \ (mod\ P)$,

4. $\left(\frac{a^2n}{P}\right) = \left(\frac{n}{P}\right)$ *whenever* $gcd(a, P) = 1$.

The following theorem is the general version of the Quadratic Reciprocity Law.

Theorem 1.27. ***The Quadratic Reciprocity law for Jacobi symbols.*** *If P and Q are positive odd integers with $gcd(P, Q) = 1$, then*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

1.2 Minkowski Convex Body Theorem in $\mathbb{R}^2$

In this section, we introduce the Minkowski Convex Body Theorem that is mainly used in this project. We start this section by giving the definition of lattices in $\mathbb{R}^n$, see [7].

Definition 1.28. *Given n linearly independent vectors $b_1, b_2, ..., b_n \in \mathbb{R}^n$, the n-**dimensional lattice genereted by** them is defined as*

$$\mathcal{L}(b_1, b_2, ..., b_n) = \{\sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z}\}.$$

*We refer to $b_1, b_2, ..., b_n$ as a **basis** of the lattice. Equivalently, let B be the $n \times n$ matrix whose rows are $b_1, b_2, ..., b_n$, then the n-**dimensional lattice genereted by** B is*

$$\mathcal{L}(B) = \mathcal{L}(b_1, b_2, ..., b_n) = \{Bx \mid x \in \mathbb{Z}^n\}$$

*and we say that the **rank** of $\mathcal{L}(B)$ is n.*

Definition 1.29. *Let $\Lambda = \mathcal{L}(B)$ be a lattice of rank n. We define the **determinant** of Λ, denoted $det(\Lambda)$, by $det(\Lambda) := \mid det(B) \mid$.*

In this project, we deal with lattices in $\mathbb{R}^2$ which can be explained as follows: given 2 linearly independent vectors $u, v \in \mathbb{R}^2$, the 2-*dimensional lattice genereted by* them is defined as

$$\mathcal{L}(u, v) = \{x_1 u + x_2 v \mid x_1, x_2 \in \mathbb{Z}\}.$$

We refer to u, v as a **basis** of the lattice.The determinant $det(\Lambda)$ in $\mathbb{R}^2$ is $det(\mathcal{L}(u, v)) = \mid det(B) \mid$ where $B = \begin{bmatrix} u \\ v \end{bmatrix}$.

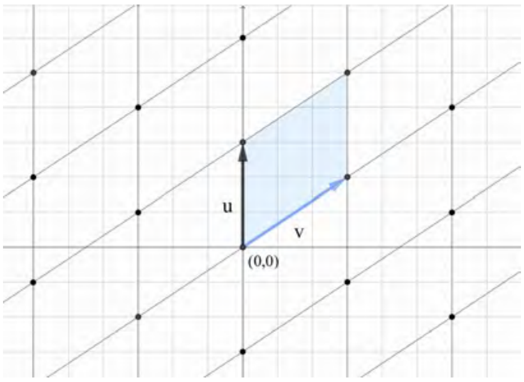

Figure 1.1: Lattice in $\mathbb{R}^2$ generated by vectors u and v

From the picture, the lattice points are the points at the intersection of two grid lines of the parallelograms.

Definition 1.30. *Let S be a subset of $\mathbb{R}^2$. S is said to be **convex** if*

$$\{u + t(v - u) : t \in [0, 1]\} \subset S$$

for every $u, v \in S$.

Examples 1.31. *A disk with center $(0, 0)$ and radius c is a convex subset in $\mathbb{R}^2$.*

Definition 1.32. *We say S is **symmetric with respsect to the origin** if $(-x_1, -x_2) \in S$ for all $(x_1, x_2) \in S$.*

The Minkowski Convex Body Theorem for a 2-dimensional Lattice states as follows.

Theorem 1.33. ***Minkowski Convex Body Theorem.*** *Suppose that Λ is a 2-dimensional lattice in $\mathbb{R}^2$ with determinant $det(\Lambda)$ and let S be a convex subset of $\mathbb{R}^2$ that is symmetric with respsect to the origin. Then if*

$$area(S) > 4det(\Lambda),$$

S must contain at least one lattice point besides the origin.

Here $det(\Lambda)$ can be considered as the area of the parallelogram having u and v as adjacent sides. A convex set S that has been considered in our entire project is the origin symetric ellipse whose its area is

$$\text{area}(S) = \pi ab,$$

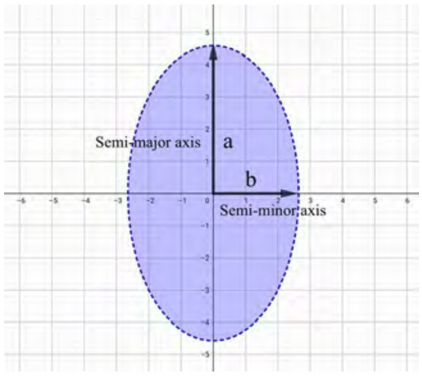

Figure 1.2: An origin symetric ellipse

where a is the length of semi-major axis and b is the length of semi-minor axis as shown in Figure 1.2.

By using a lattice $\Lambda = \mathcal{L}(u, v)$ and a symetric ellipse S centered at the origin, the Minkowski Convex Body Theorem can be interpreted as follow : "If the area of S is 4 times greater that the area of the parallelogram having u and v as adjecent sides, then there exists a lattice point apart from $(0, 0)$ that is contained in S."

1.3 Binary Quadratic Forms

In this section, we discuss a representation of integers by quadratic forms.

Definition 1.34. *An* ***integral binary quadratic form*** *is a quadratic polynomial $f(x, y)$ in two variables*

$$f(x, y) = ax^2 + bxy + cy^2$$

over $\mathbb{Z}$.

Definition 1.35. *We say that a binary quadratic form $f(x, y)$ is* ***primitive*** *if a, b and c are relatively prime.*

Definition 1.36. *The* ***discriminant*** *of form $f(x, y) = ax^2 + bxy + cy^2$ is defined as*

$$D = b^2 - 4ac.$$

Definition 1.37. *Let $f(x, y)$ be an integral binary quadratic form. An integer a is said to be* ***represented by f(x,y)*** *if there exist integers m and n such that $f(m, n) = a$.*

One of interesting problems relating to quadratic forms is representation of primes by integral binary quadratic forms, see e.g. [1], [3], [5], [6], [8] and [9]. Historically, a representation of primes of the form $p = x^2 + ny^2$ for arbitrary n have been widely studies. For example, Euler gave the rigorous proofs of the following four statements stated by Fermat, see e.g. [3] :

1. $p = x^2 + y^2$ if and only if $p = 2$ or $p \equiv 1 \ (mod 4)$;
2. $p = x^2 + 2y^2$ if and only if $p = 2$ or $p \equiv 1, 3 \ (mod 8)$;
3. $p = x^2 + 3y^2$ if and only if $p = 3$ or $p \equiv 1 \ (mod 3)$;
4. $p = x^2 + 4y^2$ if and only if $p \equiv 1 \ (mod 4)$.

and he also conjected that there is a prime p satisfying

$$p = x^2 + 6y^2 \text{ if and only if } p \equiv 1, 7 \ (mod 24).$$

This conjecture was proved by Kaplan [5] in 2014. The Fermat's statements and the result for the case n=7 were also shown in [5] by using the different techniques of proofs. In [4], Hammonds proved the statement that there are primes satisfying

1. $p = x^2 + y^2$ if and only if $p = 2$ or $p \equiv 1 \ (mod 4)$;
2. $p = x^2 + 2y^2$ if and only if $p = 2$ or $p \equiv 1, 3 \ (mod 8)$.

He mainly used the Minkowski Convex Body Theorem to proved this statement.

In this project, we find a class of primes represented by some binary quadratic form over $\mathbb{Z}$. To do so, we give some sufficient conditions for primes that can be represented by the form

$$f(x, y) = x^2 + ny^2,$$

where $n = 3, 5, 6, 7, 10, 13, 14$ and the form $f(x, y) = 2x^2 + 7y^2$ which are primitive and have negative discriminant.

Chapter 2

Representation of primes by quadratic forms

This chapter provides a class of primes that can be represented by the quadratic form x^2+ny^2 where $n = 3, 5, 6, 7, 10, 13, 14$ and the form $f(x, y) = 2x^2 + 7y^2$.

Lemma 2.1. *Let p be a prime. If $p \equiv 1 \ (mod\ 3)$, then -3 is a quadratic residue modulo p.*

Proof. Assume that $p \equiv 1 \ (mod\ 3)$. Then by Theorem 1.18, Theorem 1.19 and Theorem 1.22, we have

$$\begin{aligned}
\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{3-1}{2}\right)} \\
&= \left(\frac{1}{3}\right) \quad (\text{from } p \equiv 1 \ (mod\ 3)) \\
&= 1.
\end{aligned}$$

Hence -3 is a quadratic residue modulo p. $\square$

The following known result was mentioned in [4] without proof. Therefore, we show the proof in order to make this project self-contained.

Theorem 2.2. *Let p be a prime. If $p \equiv 1 \ (mod\ 3)$, then p is represented by the form $f(x, y) = x^2 + 3y^2$.*

Proof. Assume that $p \equiv 1$ $(mod\, 3)$. By the previous lemma, -3 is a quadratic residue modulo p. Thus there exists $u \in \mathbb{Z}$ such that

$$u^2 \equiv -3 \ (mod\ p). \tag{2.1}$$

Let

$$\Lambda = \mathcal{L}(v_1, v_2) = \{mv_1 + nv_2 \colon m, n \in \mathbb{Z}\}$$

be a lattice in $\mathbb{R}^2$ generated by $v_1 = (1, u)$ and $v_2 = (0, p)$. Thus

$$det\Lambda = \begin{vmatrix} 1 & u \\ 0 & p \end{vmatrix} = 1(p) - 0(u) = p.$$

We observe that if $(y, x) \in \Lambda$, there exist $m, n \in \mathbb{Z}$ such that $mv_1 + nv_2 = (y, x)$, i.e., $(m, mu) + (0, np) = (y, x)$. Then $x = mu + np$ and $y = m$ which give

$$\begin{aligned} x^2 + 3y^2 &= (mu + np)^2 + 3(m)^2 \\ &= m^2u^2 + 2munp + n^2p^2 + 3m^2 \\ &= p(2mun + n^2p) + m^2(u^2 + 3) \\ &\equiv m^2(u^2 + 3) \ (mod\ p) \\ &\equiv 0 \ (mod\ p) \text{ (by (2.1))}. \end{aligned}$$

Let S be the origin symetric ellipse defined by

$$S = \{(y, x) \in \mathbb{R}^2 \colon x^2 + 3y^2 < 3p\}.$$

Then the semi-major axis length is $\sqrt{3p}$ and semi-minor axis length is $\sqrt{p}$. We note that

$$area(S) = \pi(\sqrt{3p})(\sqrt{p}) = \pi(\sqrt{3})p > 4p = 4det(\Lambda).$$

By the Minkowski Convex Body Theorem, there exists a lattice point $(d, c) \in S \diagdown (0, 0)$ such that

$$0 < c^2 + 3d^2 < 3p \text{ and } c^2 + 3d^2 \equiv 0 \ (mod\ p).$$

Then $p \mid c^2 + 3d^2$, which implies that $c^2 + 3d^2 = p$ or $2p$.

Suppose, by contrary, that $c^2 + 3d^2 = 2p$. From $p \equiv 1$ $(mod\ 3)$, then $3 \mid p - 1$. Then there exists $k \in \mathbb{Z}$ such that $p = 3k + 1$. Thus

$$6k + 2 = 2p = c^2 + 3d^2 \equiv c^2 \ (mod\ 3).$$

Hence $2 \equiv c^2$ $(mod\ 3)$. That is 2 is a quadratic residue modulo 3. Thus $\left(\frac{2}{3}\right) = 1$ which contradicts Theorem 1.19. Hence $c^2 + 3d^2 = p$,i.e., p is represented by the form $x^2 + 3y^2$. $\square$

Examples 2.3. *Since* $7 \equiv 1 \ (mod\ 3)$*, then, by the above theorem,* 7 *can be represented by the form* $f(x, y) = x^2 + 3y^2$*. In fact,* $7 = 2^2 + 3(1)^2$*.*

Lemma 2.4. *If a prime* $p \equiv 1, 9 \ (mod\ 20)$*, then* -5 *is a quadratic residue modulo* p*.*

Proof. Assume that $p \equiv 1, 9 \ (mod\ 20)$. Then $\frac{p-1}{2}$ is even. Moreover, $p \equiv 1, 4 \ (mod\ 5)$, which are both square. Therefore $\left(\frac{p}{5}\right) = 1$. By Theorem 1.18, Theorem 1.19, Theorem 1.21 and Theorem 1.22, we have

$$\begin{aligned}\left(\frac{-5}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{5}{p}\right) \\ &= \left(\frac{p}{5}\right)(-1)^{\frac{p-1}{2}}(-1)^{\frac{5-1}{2}} \\ &= 1.\end{aligned}$$

Then -5 is a quadratic residue modulo p. □

Theorem 2.5. *Let* p *be a prime. If* $p \equiv 1, 9 \ (mod\ 20)$*, then* p *is represented by the form* $f(x, y) = x^2 + 5y^2$*.*

Proof. Assume that $p \equiv 1, 9 \ (mod\ 20)$. Then, by Lemma 2.4, -5 is a quadratic residue modulo p. Thus there exists $u \in \mathbb{Z}$ such that

$$u^2 \equiv -5 \ (mod\ p). \tag{2.2}$$

Let Λ be a lattice in $\mathbb{R}^2$ defined by

$$\Lambda = \mathcal{L}(v_1, v_2) = \{mv_1 + nv_2 \colon m, n \in \mathbb{Z}\},$$

where $v_1 = (1, u)$ and $v_2 = (0, p)$. Thus $det(\Lambda) = \begin{vmatrix} 1 & u \\ 0 & p \end{vmatrix} = 1(p) - 0(u) = p$. Note that if $(y, x) \in \Lambda$, there exist $m, n \in \mathbb{Z}$ such that $mv_1 + nv_2 = (y, x)$, i.e., $(m, mu) + (0, np) = (y, x)$. Then $x = mu + np$ and $y = m$. By direct computation as in Theorem 2.2, we have

$$\begin{aligned}x^2 + 5y^2 &= (mu + np)^2 + 5(m)^2 \\ &\equiv m^2(u^2 + 5) \ (mod\ p) \\ &\equiv 0 \ (mod\ p) \ (\text{by } (2.2)).\end{aligned}$$

Let S be the origin symetric ellipse with semi-major axis length $\sqrt{3p}$ and semi-minor axis length $\sqrt{\frac{3p}{5}}$ defined by

$$S = \{(y, x) \in \mathbb{R}^2 \colon x^2 + 5y^2 < 3p\}.$$

Then we have

$$area(S) = \pi(\sqrt{\frac{3p}{5}})(\sqrt{3p}) = \pi(\frac{3}{\sqrt{5}})p > 4p = 4det(\Lambda).$$

By the Minkowski Convex Body Theorem, there exists a lattice point $(d, c) \in S \diagdown (0, 0)$ be such that

$$0 < c^2 + 5d^2 < 3p \text{ and } c^2 + 5d^2 \equiv 0 \ (mod\ p).$$

These expressions show that we must consider two cases :

$$c^2 + 5d^2 = p \text{ or } 2p.$$

Suppose $c^2+5d^2 = 2p$. From $p \equiv 1, 9\ (mod\ 20)$, then $20 \mid p-1$ or $20 \mid p-9$.
Case $20 \mid p - 1$: Thus there exists $k \in \mathbb{Z}$ be such that $p = 20k + 1$. Then

$$40k + 2 = 2p = c^2 + 5d^2 \equiv c^2\ (mod\ 5).$$

Hence $2 \equiv c^2\ (mod\ 5)$. That is 2 is a quadratic residue modulo 5. Thus $\left(\frac{2}{5}\right) = 1$, a contradiction.
Case $20 \mid p - 9$: Thus there exists $k \in \mathbb{Z}$ be such that $p = 20k + 9$. Then

$$40k + 18 = 2p = c^2 + 5d^2 \equiv c^2\ (mod\ 5).$$

Hence $3 \equiv c^2\ (mod\ 5)$. That is 3 is a quadratic residue modulo 5. Thus $\left(\frac{3}{5}\right) = 1$. Since $3^{\frac{5-1}{2}} \equiv 9 \equiv -1\ (mod\ 5)$, we obtain a contradiction.

Hence $c^2 + 5d^2 = p$, that is, p is represented by the form $x^2 + 5y^2$. $\square$

Examples 2.6.

1. *Since* 41 *is an odd prime satisfying* $41 \equiv 1\ (mod\ 20)$*, we can conclude that* 41 *can be represented by the form* $f(x, y) = x^2 + 5y^2$*. In fact* $41 = 6^2 + 5(1)^2$.

2. *Since* 89 *is an odd prime satisfying* $89 \equiv 9\ (mod\ 20)$*, we can conclude that* 89 *can also be represented by the form* $f(x, y) = x^2 + 5y^2$*. Note that* $89 = 3^2 + 5(4)^2$.

Lemma 2.7. *If a prime $p \equiv 1, 7$ $(mod\ 24)$, then -6 is a quadratic residue modulo p.*

Proof. Assume that $p \equiv 1, 7$ $(mod\ 24)$.
Case $p \equiv 1$ $(mod\ 24)$: Then there exists $k \in \mathbb{Z}$ be such that $p = 24k + 1$. By Theorem 1.18, Theorem 1.19, Theorem 1.21 and Theorem 1.22, we have

$$\begin{aligned}
\left(\frac{-6}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}\left(\frac{3}{p}\right) \\
&= (-1)^{12k}(-1)^{72k^2+6k}\left(\frac{3}{p}\right) \\
&= \left(\frac{p}{3}\right)(-1)^{(\frac{p-1}{2})(\frac{3-1}{2})} \\
&= \left(\frac{p}{3}\right) \\
&= 1 \text{ (from } p \equiv 1 \ (mod\ 3)).
\end{aligned}$$

Case $p \equiv 7$ $(mod\ 24)$: Then there exists $k \in \mathbb{Z}$ be such that $p = 24k + 7$. By Theorem 1.18, Theorem 1.19, Theorem 1.21 and Theorem 1.22, we have

$$\begin{aligned}
\left(\frac{-6}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}\left(\frac{3}{p}\right) \\
&= (-1)^{12k+3}(-1)^{72k^2+42k+6}\left(\frac{3}{p}\right) \\
&= (-1)\left(\frac{3}{p}\right) \\
&= (-1)\left(\frac{p}{3}\right)(-1)^{(\frac{p-1}{2})(\frac{3-1}{2})} \\
&= \left(\frac{p}{3}\right) \\
&= 1 \text{ (from } p \equiv 1 \ (mod\ 3)).
\end{aligned}$$

Then -6 is a quadratic residue modulo p. □

Theorem 2.8. *Let p be a prime. If $p \equiv 1, 7$ $(mod\ 24)$, then p is represented by the form $f(x, y) = x^2 + 6y^2$.*

Proof. Assume that $p \equiv 1, 7 \ (mod\ 24)$. Then -6 is a quadratic residue modulo p. Thus there exists $u \in \mathbb{Z}$ such that

$$u^2 \equiv -6 \ (mod\ p). \tag{2.3}$$

Let Λ be a lattice in $\mathbb{R}^2$ defined by

$$\Lambda = \mathcal{L}(v_1, v_2) = \{mv_1 + nv_2 \colon m, n \in \mathbb{Z}\},$$

where $v_1 = (1, u)$ and $v_2 = (0, p)$. By the same argument as in previous theorem, we have $det(\Lambda) = p$ and if $(y, x) \in \Lambda$, then $x^2 + 6y^2 \equiv 0 \ (mod\ p)$ by (2.3). By letting

$$S = \{(y, x) \in \mathbb{R}^2 \colon x^2 + 6y^2 < 4p\},$$

we have

$$area(S) = \pi(\sqrt{\frac{4p}{6}})(\sqrt{4p}) = \pi(\frac{4}{\sqrt{6}})p > 4p = 4det(\Lambda).$$

Then there exists a lattice point $(d, c) \in S \diagdown (0, 0)$ such that

$$0 < c^2 + 6d^2 < 4p \text{ and } c^2 + 6d^2 \equiv 0 \ (mod\ p).$$

Consequently, we get $c^2 + 6d^2 = p$ or $2p$ or $3p$.

Suppose that $c^2 + 6d^2 = 2p$. From $p \equiv 1, 7 \ (mod\ 24)$, we have

$$2p \equiv 2, 14 \equiv 2 \ (mod\ 3)$$

and so

$$c^2 \equiv c^2 + 6d^2 \equiv 2p \equiv 2 \ (mod\ 3).$$

Therefore, $\left(\frac{2}{3}\right) = 1$, which is a contradiction.

Suppose that $c^2 + 6d^2 = 3p$. Then $3 \mid c^2 + 6d^2$. Suppose that d is multiple of 3. Then $3 \mid c^2$ and so $9 \mid c^2$. Thus $9 \mid c^2 + 6d^2$, i.e., $9 \mid 3p$. Therefore $3 \mid p$. This implies that $p = 3$, which is impossible. Then d is not a multiple of 3. Thus $d^2 \equiv 1 \ (mod\ 3)$. Hence $6d^2 \equiv 6 \equiv 0 \ (mod\ 3)$. Therefore

$$0 \equiv 3p \equiv c^2 + 6d^2 \equiv c^2 \ (mod\ 3).$$

Then $c^2 \equiv 0 \ (mod\ 3)$ which implies that $3 \mid c$. So there exists $l \in \mathbb{Z}$ be such that $c = 3l$. Now we have

$$c^2 + 6d^2 = (3l)^2 + 6d^2 = 3(3l^2 + 2d^2) = 3p.$$

Then $p \equiv 2d^2 \equiv 2 \ (mod\ 3)$, which is a contradiction.
Hence $c^2 + 6d^2 = p$, that is, p is represented by the form $x^2 + 6y^2$. $\square$

Examples 2.9.

1. *We have* 73 *is an odd prime with* $73 \equiv 1 \ (mod\ 24)$*. Then* 73 *is represented by the form* $f(x, y) = x^2 + 6y^2$*, that is,* $73 = 7^2 + 6(2)^2$*.*

2. *We have* 79 *is an odd prime and* $79 \equiv 7 \ (mod\ 24)$*. Then* 79 *is represented by the form* $f(x, y) = x^2 + 6y^2$*, that is,* $79 = 5^2 + 6(3)^2$*.*

Lemma 2.10. *If a prime* $p \equiv 1, 9, 11, 15, 23, 25 \ (mod\ 28)$*, then* -7 *is a quadratic residue modulo* p*.*

Proof. Assume that $p \equiv 1, 9, 11, 15, 23, 25 \ (mod\ 28)$.
By Theorem 1.18, Theorem 1.19, Theorem 1.21 and Theorem 1.22, we have

$$\begin{aligned} \left(\frac{-7}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{7-1}{2}\right)} \\ &= \left(\frac{p}{7}\right). \end{aligned} \tag{2.4}$$

Case $p \equiv 1, 15 \ (mod\ 28)$: Then $p \equiv 1 \ (mod\ 7)$ and so, by (2.4), we obtain

$$\left(\frac{-7}{p}\right) = \left(\frac{1}{7}\right) = 1.$$

Case $p \equiv 9, 23 \ (mod\ 28)$: Then $p \equiv 2 \ (mod\ 7)$. By (2.4) and Theorem 1.21, we obtain

$$\left(\frac{-7}{p}\right) = \left(\frac{2}{7}\right) = 1.$$

Case $p \equiv 11, 25 \ (mod\ 28)$: Then $p \equiv 4 \ mod\ 7$. By (2.4) and 4 is square, we obtain

$$\left(\frac{-7}{p}\right) = \left(\frac{4}{7}\right) = 1.$$

Then -7 is a quadratic residue modulo p. $\square$

Theorem 2.11. *Let* p *be a prime. If* $p \equiv 1, 9, 11, 15, 23, 25 \ (mod\ 28)$*, then* p *is represented by the form* $f(x, y) = x^2 + 7y^2$*.*

Proof. Assume that $p \equiv 1, 9, 11, 15, 23, 25 \ (mod\ 28)$. By the previous lemma, -7 is a quadratic residue modulo p. Thus there exists $u \in \mathbb{Z}$ such that

$$u^2 \equiv -7 \ (mod\ p). \tag{2.5}$$

Let Λ be a lattice in $\mathbb{R}^2$ defined by

$$\Lambda = \mathcal{L}(v_1, v_2) = \{mv_1 + nv_2 \colon m, n \in \mathbb{Z}\},$$

where $v_1 = (1, u)$ and $v_2 = (0, p)$. By the same argument as in previous theorem, we have $det(\Lambda) = p$ and if $(y, x) \in \Lambda$, $x^2 + 7y^2 \equiv 0 \ (mod\ p)$ by (2.5). By letting

$$S = \{(y, x) \in \mathbb{R}^2 \colon x^2 + 7y^2 < 4p\},$$

we have $area(S) = \pi(\sqrt{\frac{4p}{7}})(\sqrt{4p}) = \pi(\frac{4}{\sqrt{7}})p > 4p = 4det(\Lambda)$.
Then there exists a lattice point $(d, c) \in S \diagdown (0, 0)$ such that

$$0 < c^2 + 7d^2 < 4p \text{ and } c^2 + 7d^2 \equiv 0 \ (mod\ p).$$

Consequently, we get $c^2 + 7d^2 = p$ or $2p$ or $3p$.

Suppose that $c^2 + 7d^2 = 2p$. In order to obtain a contradiction we divide the proof into four case as follows.

Case c is even and d is odd : Thus there exist $k, l \in \mathbb{Z}$ be such that $c = 2k$ and $d = 2l + 1$. We have

$$\begin{aligned} 2p = c^2 + 7d^2 &= (2k)^2 + 7(2l + 1)^2 \\ &= 4k^2 + 7(4l^2 + 4l + 1) \\ &= 2(2k^2 + 14l^2 + 14l + 3) + 1. \end{aligned}$$

Thus $2p$ is odd, a contradiction.

Case c is odd and d is even : Thus there exist $k, l \in \mathbb{Z}$ be such that $c = 2k + 1$ and $d = 2l$. We have

$$\begin{aligned} 2p = c^2 + 7d^2 &= (2k + 1)^2 + 7(2l)^2 \\ &= (4k^2 + 4k + 1) + 7(4l^2) \\ &= 2(2k^2 + 2k + 14l^2) + 1. \end{aligned}$$

Thus $2p$ is odd, a contradiction.

Case c and d are even : Thus there exist $k, l \in \mathbb{Z}$ be such that $c = 2k$ and $d = 2l$. We have

$$\begin{aligned} 2p = c^2 + 7d^2 &= (2k)^2 + 7(2l)^2 \\ &= (4k^2) + 7(4l^2) \\ &= 2(2k^2 + 14l^2) \end{aligned}$$

and so $p = 2k^2 + 14l^2$. Thus p is even, a contradiction.

Case c and d are odd : Thus there exist $k, l \in \mathbb{Z}$ be such that $c = 2k + 1$

and $d = 2l + 1$. We have

$$\begin{aligned} 2p = c^2 + 7d^2 &= (2k+1)^2 + 7(2l+1)^2 \\ &= (4k^2 + 4k + 1) + 7(4l^2 + 4l + 1) \\ &= 2(2k^2 + 2k + 4 + 14l^2 + 14l). \end{aligned}$$

Therefore, we have

$$\begin{aligned} p &= 2k^2 + 2k + 4 + 14l^2 + 14l \\ &= 2(k^2 + k + 2 + 7l^2 + 7l). \end{aligned}$$

Thus p is even, a contradiction.

Suppose that $c^2+7d^2 = 3p$. Then $3 \mid c^2+7d^2$. Suppose that d is multiple of 3. Then $3 \mid c^2$ and so $9 \mid c^2$. Thus $9 \mid c^2 + 7d^2$, i.e., $9 \mid 3p$. Therefore $3 \mid p$. This implies that $p = 3$, which is impossible. Then d is not a multiple of 3. Thus $d^2 \equiv 1 \ (mod\ 3)$. Hence $7d^2 \equiv 7 \equiv 1 \ (mod\ 3)$. Therefore

$$0 \equiv 3p \equiv c^2 + 7d^2 \equiv c^2 + 1 \ (mod\ 3).$$

Then $c^2 \equiv -1 \ (mod\ 3)$ which implies that -1 is a quddratic residue modulo 3, then $\left(\frac{-1}{3}\right) = 1$, but from

$$\left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1 \not\equiv 1 \ (mod\ 3),$$

which is a contradiction.

Hence $c^2 + 7d^2 = p$, that is, p is represented by the form $x^2 + 7y^2$. $\square$

Examples 2.12.

1. *Since* 29 *is an odd prime with* $29 \equiv 1 \ (mod\ 28)$*, we get* 29 *can be represented by the form* $f(x,y) = x^2 + 7y^2$*. In fact,* $29 = 1^2 + 7(2)^2$.

2. *Since* 37 *is an odd prime with* $37 \equiv 9 \ (mod\ 28)$*, we get* 37 *can be represented by the form* $f(x,y) = x^2 + 7y^2$*. In fact, that is* $37 = 3^2 + 7(2)^2$.

3. *Since* 67 *is an odd prime with* $67 \equiv 11 \ (mod\ 28)$*, we get* 67 *can be represented by the form* $f(x,y) = x^2 + 7y^2$*. In fact, that is* $67 = 2^2 + 7(3)^2$.

4. *Since* 127 *is an odd prime with* $127 \equiv 15 \ (mod\ 28)$*, we get* 127 *can be represented by the form* $f(x,y) = x^2 + 7y^2$*. In fact, that is* $127 = 8^2 + 7(3)^2$.

5. *Since* 23 *is an odd prime with* $23 \equiv 23 \ (mod\ 28)$*, we get* 23 *can be represented by the form* $f(x,y) = x^2 + 7y^2$*. In fact, that is* $23 = 4^2 + 7(1)^2$.

6. *Since* 53 *is an odd prime with* $53 \equiv 25 \ (mod\ 28)$*, we get* 53 *can be represented by the form* $f(x,y) = x^2 + 7y^2$*. In fact, that is* $53 = 5^2 + 7(2)^2$.

Lemma 2.13. *Let* p *be a prime. If* $p \equiv 1, 9, 11, 19 \ (mod\ 40)$*, then* -10 *is a quadratic residue modulo* p*.*

Proof. Assume that $p \equiv 1, 9, 11, 19 \ (mod\ 40)$. By Theorem 1.18, Theorem 1.19, Theorem 1.21 and Theorem 1.22, we have

$$\begin{aligned}\left(\frac{-10}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)\left(\frac{2}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right)(-1)^{(\frac{p-1}{2})(\frac{5-1}{2})}\left(\frac{2}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right)\left(\frac{2}{p}\right). \qquad (2.6)\end{aligned}$$

Case $p \equiv 1 \ (mod\ 40)$: Then $\frac{p-1}{2}$ is even. Moreover $p \equiv 1 \ (mod\ 5)$ and $p \equiv 1 \ (mod\ 8)$. By (2.6), we have

$$\left(\frac{-10}{p}\right) = \left(\frac{1}{5}\right)\left(\frac{2}{p}\right) = 1.$$

Case $p \equiv 9 \ (mod\ 40)$: Then $\frac{p-1}{2}$ is even. Moreover $p \equiv 4 \ (mod\ 5)$ and $p \equiv 1 \ (mod\ 8)$. By (2.6), we have

$$\left(\frac{-10}{p}\right) = \left(\frac{4}{5}\right)\left(\frac{2}{p}\right) = 1.$$

Case $p \equiv 11 \ (mod\ 40)$: Then $\frac{p-1}{2}$ is odd. Moreover, $p \equiv 1 \ (mod\ 5)$ and $p \equiv 3 \ (mod\ 8)$. By (2.6), we have

$$\left(\frac{-10}{p}\right) = \left(\frac{1}{5}\right)\left(\frac{2}{p}\right) = -\left(\frac{1}{5}\right)(-1) = 1.$$

Case $p \equiv 19 \ (mod\ 40)$: Then $\frac{p-1}{2}$ is odd. Moreover, $p \equiv 4 \ (mod\ 5)$ and $p \equiv 3 \ (mod\ 8)$. By (2.6), we have

$$\left(\frac{-10}{p}\right) = -\left(\frac{5}{p}\right)\left(\frac{2}{p}\right) = -\left(\frac{5}{p}\right)(-1) = 1.$$

Then -10 is a quadratic residue modulo p. □

Theorem 2.14. *Let p be a prime. If $p \equiv 1, 9, 11, 19$ $(mod\ 40)$, then p is represented by the form $f(x, y) = x^2 + 10y^2$.*

Proof. Assume that $p \equiv 1, 9, 11, 19$ $(mod\ 20)$. By the previous lemma, -10 is a quadratic residue modulo p. Thus there exists $u \in \mathbb{Z}$ such that

$$u^2 \equiv -10\ (mod\ p). \tag{2.7}$$

Let Λ be a lattice in $\mathbb{R}^2$ defined by

$$\Lambda = \mathcal{L}(v_1, v_2) = \{mv_1 + nv_2 \colon m, n \in \mathbb{Z}\},$$

where $v_1 = (1, u)$ and $v_2 = (0, p)$. By the same argument, we have $det(\Lambda) = p$ and if $(y, x) \in \Lambda$, $x^2 + 10y^2 \equiv 0$ $(mod\ p)$ by (2.7). Put

$$S = \{(y, x) \in \mathbb{R}^2 \colon x^2 + 10y^2 < 5p\},$$

We have

$$area(S) = \pi(\sqrt{\frac{5p}{10}})(\sqrt{5p}) = \pi(\frac{5}{\sqrt{10}})p > 4p = 4det(\Lambda).$$

Then there exists a lattice point $(d, c) \in S \diagdown (0, 0)$ such that

$$0 < c^2 + 10d^2 < 5p \text{ and } c^2 + 10d^2 \equiv 0\ (mod\ p).$$

Then $c^2 + 10d^2 = p$ or $2p$ or $3p$ or $4p$.

Suppose that $c^2 + 10d^2 = 2p$.

Case $p \equiv 1$ $(mod\ 40)$: Then

$$2 \equiv 2p \equiv c^2 + 10d^2 \equiv c^2\ (mod\ 10).$$

Then $c^2 \equiv 2$ $(mod\ 10)$. It obvious that this congruence has no solution mod 10.

Case $p \equiv 9$ $(mod\ 40)$: Then

$$18 \equiv 2p \equiv c^2 + 10d^2 \equiv c^2\ (mod\ 10).$$

Then $c^2 \equiv 8$ $(mod\ 10)$. The congruence also has no solution mod 10.

Case $p \equiv 11$ $(mod\ 40)$: Then

$$22 \equiv 2p \equiv c^2 + 10d^2 \equiv c^2\ (mod\ 10).$$

Then $c^2 \equiv 2$ $(mod\ 10)$. The congruence also has no solution mod 10.

Case $p \equiv 19$ $(mod\ 40)$: Then

$$38 \equiv 2p \equiv c^2 + 10d^2 \equiv c^2\ (mod\ 10).$$

Then $c^2 \equiv 8$ (mod 10). The congruence also has no solution mod 10.

Suppose that $c^2 + 10d^2 = 3p$. Then $3 \mid c^2 + 10d^2$. Suppose that d is multiple of 3. Then $3 \mid c^2$ and so $9 \mid c^2$. Thus $9 \mid c^2 + 10d^2$, i.e., $9 \mid 3p$. Therefore $3 \mid p$. This implies that $p = 3$, which is impossible. Then d is not multiple of 3 and so $d^2 \equiv 1$ (mod 3). Hence $10d^2 \equiv 10 \equiv 1$ (mod 3). Thus

$$0 \equiv 3p \equiv c^2 + 10d^2 \equiv c^2 + 1 \ (mod\ 3).$$

Then $c^2 \equiv -1$ (mod 3) which implies that -1 is a quadratic residue modulo 3, then $\left(\frac{-1}{3}\right) = 1$. But from

$$\left(\frac{-1}{3}\right) \equiv (-1)^{\frac{3-1}{2}} \equiv -1 \not\equiv 1 \ (mod\ 3),$$

this is a contradiction.

Suppose that $c^2 + 10d^2 = 4p$. Then $4 \mid c^2 + 10d^2$ so there exists $k \in \mathbb{Z}$ such that $4k = c^2 + 10d^2$. Hence

$$c^2 = 4k - 10d^2 = 2(2k - 5d^2).$$

Then $2 \mid c^2$ and so $4 \mid c^2$. From $4 \mid c^2 + 10d^2$, then $4 \mid 10d^2$ we also get $2 \mid d$. Thus both c and d are even. Then there exist $m, n \in \mathbb{Z}$ such that $c = 2m$ and $d = 2n$. We have

$$\begin{aligned} 4p = c^2 + 10d^2 &= (2m)^2 + 10(2n)^2 \\ &= 4m^2 + 40n^2. \end{aligned}$$

Therefore $p = m^2 + 10n^2$. That is there exist $m, n \in \mathbb{Z}$ be such that $p = m^2 + 10n^2$. Hence p is represented by the form $f(x, y) = x^2 + 10y^2$.
For the last case that $c^2 + 10d^2 = p$, the theorem obviously holds. □

Examples 2.15.

1. *Since* 41 *is an odd prime with* $41 \equiv 1$ (mod 40)*, we get* 41 *can be represented by the form* $f(x, y) = x^2 + 10y^2$*. In fact,* $41 = 1^2 + 10(2)^2$.

2. *Similarly,* 89 *is an odd prime with* $89 \equiv 9$ (mod 40)*. So* 89 *can be represented by the form* $f(x, y) = x^2 + 10y^2$*. In fact,* $89 = 7^2 + 10(2)^2$.

3. 91 *is an odd prime with* $91 \equiv 11$ (mod 40)*. So* 91 *can be represented by the form* $f(x, y) = x^2 + 10y^2$*. In fact,* $91 = 1^2 + 10(3)^2$.

4. 59 *is an odd prime with* $59 \equiv 19$ (mod 40)*. So* 59 *can be represented by the form* $f(x, y) = x^2 + 10y^2$*. In fact,* $59 = 7^2 + 10(1)^2$.

Lemma 2.16. *Let p be a prime. If $p \equiv 1, 9, 17, 25, 29, 49$ $(mod\ 52)$, then -13 is a quadratic residue modulo p.*

Proof. Assume that $p \equiv 1, 9, 17, 25, 29, 49\ (mod\,52)$. Then $p \equiv 1, 9, 4, 25, 16, 49\ (mod\,13)$, respectively. Since they are all squares,

$$\left(\frac{p}{13}\right) = 1.$$

Moreover, in any case, $p \equiv 1$ $(mod\ 4)$. Therefore $\frac{p-1}{2}$ is even. By Theorem 1.18, Theorem 1.19, Theorem 1.21 and Theorem 1.22, we have

$$\begin{aligned}\left(\frac{-13}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{13}{p}\right)\\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p}{13}\right)(-1)^{(\frac{p-1}{2})(\frac{13-1}{2})}\\ &= 1.\end{aligned}$$

Hence -13 is a quadratic residue modulo p. □

Theorem 2.17. *Let p be a prime. If $p \equiv 1, 9, 17, 25, 29, 49$ $(mod\ 52)$, then p is represented by the form $f(x, y) = x^2 + 13y^2$.*

Proof. Assume that $p \equiv 1, 9, 17, 25, 29, 49\ (mod\ 52)$. By the previous lemma, -13 is a quadratic residue modulo p. Thus there exists $u \in \mathbb{Z}$ such that

$$u^2 \equiv -13\ (mod\ p). \tag{2.8}$$

Let Λ be a lattice in $\mathbb{R}^2$ defined by

$$\Lambda = \mathcal{L}(v_1, v_2) = \{mv_1 + nv_2 \colon m, n \in \mathbb{Z}\},$$

where $v_1 = (1, u)$ and $v_2 = (0, p)$. Then $det(\Lambda) = p$ and if $(y, x) \in \Lambda$, $x^2 + 13y^2 \equiv 0$ $(mod\ p)$ by (2.8). Put

$$S = \{(y, x) \in \mathbb{R}^2 \colon x^2 + 13y^2 < 5p\},$$

We have

$$area(S) = \pi(\sqrt{\frac{5p}{13}})(\sqrt{5p}) = \pi(\frac{5}{\sqrt{13}})p > 4p = 4det(\Lambda).$$

Then there exists a lattice point $(d, c) \in S\diagdown(0, 0)$ such that $0 < c^2+13d^2 < 5p$ and $c^2 + 13d^2 \equiv 0$ $(mod\ p)$. Consequently, we get $c^2 + 13d^2 = p$ or $2p$ or $3p$ or $4p$. The case $c^2 + 13d^2 = p$ is obvious.

Suppose that $c^2 + 13d^2 = 2p$.
Case $p \equiv 1\ (mod\ 52)$: Then

$$2 \equiv 2p \equiv c^2 + 13d^2 \equiv c^2\ (mod\ 13).$$

Thus $c^2 \equiv 2\ (mod\ 13)$. It obvious that this congruence has no solution mod 13.
Case $p \equiv 9\ (mod\ 52)$: Then

$$18 = 2p = c^2 + 13d^2 \equiv c^2\ (mod\ 13).$$

Thus $c^2 \equiv 5\ (mod\ 13)$. It obvious that this congruence has no solution mod 13.
Case $p \equiv 17\ (mod\ 52)$: Then

$$34 = 2p = c^2 + 13d^2 \equiv c^2\ (mod\ 13).$$

Thus $c^2 \equiv 8\ (mod\ 13)$. Similarly, this congruence has no solution mod 13.
Case $p \equiv 25\ (mod\ 52)$: Then

$$50 = 2p = c^2 + 13d^2 \equiv c^2\ (mod\ 13).$$

Thus $c^2 \equiv 11\ (mod\ 13)$. Similarly, this congruence has no solution mod 13.
Case $p \equiv 29\ (mod\ 52)$: Then

$$58 = 2p = c^2 + 13d^2 \equiv c^2\ (mod\ 13).$$

Thus $c^2 \equiv 6\ (mod\ 13)$. Similarly, this congruence has no solution mod 13.
Case $p \equiv 49\ (mod\ 52)$: Then

$$98 = c^2 + 13d^2 \equiv c^2\ (mod\ 13).$$

Thus $c^2 \equiv 7\ (mod\ 13)$. Similarly, this congruence has no solution mod 13.

Suppose that $c^2 + 13d^2 = 3p$. Then $3 \mid c^2 + 13d^2$.
Suppose that d is multiple of 3. Then $3 \mid c^2$ and so $9 \mid c^2$. Thus $9 \mid c^2 + 13d^2$, i.e., $9 \mid 3p$. Therefore $3 \mid p$ which implies that $p = 3$, which is impossible. Then d is not multiple of 3. Then $d^2 \equiv 1\ (mod\ 3)$. Hence $13d^2 \equiv 13 \equiv 1\ (mod\ 3)$. Thus

$$0 \equiv 3p \equiv c^2 + 13d^2 \equiv c^2 + 1\ (mod\ 3).$$

Then $c^2 \equiv -1\ (mod\ 3)$ which implies that -1 is a quadratic residue modulo 3. Then $\left(\frac{-1}{3}\right) = 1$. But from

$$\left(\frac{-1}{3}\right) \equiv (-1)^{\frac{3-1}{2}} \equiv -1 \not\equiv 1\ (mod\ 3),$$

this is a contradiction.

Suppose that $c^2 + 13d^2 = 4p$, then $4 \mid c^2 + 13d^2$. Suppose that d is odd, then there exists $n \in \mathbb{Z}$ be such that $d = 2n + 1$. Thus

$$13d^2 = 13(2n+1)^2 = 13(4n^2 + 4n + 1) \equiv 1 \ (mod\ 4).$$

Hence

$$0 \equiv 4p \equiv c^2 + 13d^2 \equiv c^2 + 1 \ (mod\ 4).$$

Then $c^2 \equiv -1 \ (mod\ 4)$, i.e., $4 \mid c^2 - 1$. Then c is odd. Thus $c^2 \equiv 1 \ (mod\ 4)$. Now we have

$$0 \equiv 4p \equiv c^2 + 13d^2 \equiv 1 + 1 \equiv 2 \ (mod\ 4),$$

which is a contradiction. Then d is even. Thus there exists $k \in \mathbb{Z}$ such that $d = 2k$ and then $4 \mid 13d^2$. From $4 \mid c^2 + 13d^2$, then $2 \mid c$ and so there exists $l \in \mathbb{Z}$ such that $c = 2l$. We have

$$\begin{aligned} 4p = c^2 + 13d^2 &= (2l)^2 + 13(2k)^2 \\ &= 4l^2 + 4(13k^2). \end{aligned}$$

This means that $p = l^2 + 13k^2$. Hence there exist $l, k \in \mathbb{Z}$ such that $p = l^2 + 13k^2$, i.e., p is represented by the form $f(x, y) = x^2 + 13y^2$.
Combining four cases, we can conclude that p is represented by the form $f(x, y) = x^2 + 13y^2$. □

Examples 2.18.

1. *From* 53 *is an odd prime with* $53 \equiv 1 \ (mod\ 52)$, 53 *can be represented by the form* $f(x, y) = x^2 + 13y^2$. *In fact,* $53 = 1^2 + 13(2)^2$.

2. *From* 61 *is an odd prime with* $61 \equiv 9 \ (mod\ 52)$, 61 *can be represented by the form* $f(x, y) = x^2 + 13y^2$. *In fact,* $61 = 3^2 + 13(2)^2$.

3. *From* 17 *is an odd prime with* $17 \equiv 17 \ (mod\ 52)$, 17 *can be represented by the form* $f(x, y) = x^2 + 13y^2$. *In fact,* $17 = 2^2 + 13(1)^2$.

4. *From* 181 *is an odd prime with* $181 \equiv 25 \ (mod\ 52)$, 181 *can be represented by the form* $f(x, y) = x^2 + 13y^2$. *In fact,* $181 = 8^2 + 13(3)^2$.

5. *From* 29 *is an odd prime with* $29 \equiv 29 \ (mod\ 52)$, 29 *can be represented by the form* $f(x, y) = x^2 + 13y^2$. *In fact,* $29 = 4^2 + 13(1)^2$.

6. *From* 101 *is an odd prime with* $101 \equiv 49 \ (mod\ 52)$, 101 *can be represented by the form* $f(x, y) = x^2 + 13y^2$. *In fact,* $101 = 7^2 + 13(2)^2$.

Lemma 2.19. *Let p be a prime. If $p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$, then -14 is a quadratic residue modulo p.*

Proof. Assume that $p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$. Then $p \equiv 1, 9, 1, 9, 25, 4 \pmod{7}$, respectively. Since they are all squares, we have

$$\left(\frac{p}{7}\right) = 1.$$

By Theorem 1.18, Theorem 1.19, Theorem 1.21 and Theorem 1.22, we have

$$\begin{aligned}
\left(\frac{-14}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{7}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{2}{p}\right)\left(\frac{p}{7}\right)(-1)^{(\frac{p-1}{2})(\frac{7-1}{2})} \\
&= \left(\frac{2}{p}\right)\left(\frac{p}{7}\right). \qquad (2.9)
\end{aligned}$$

Case $p \equiv 1 \pmod{56}$: Then $p \equiv 1 \pmod{8}$ and so $\left(\frac{2}{p}\right) = 1$. By (2.9), we have

$$\left(\frac{-14}{p}\right) = 1.$$

Case $p \equiv 9 \pmod{56}$: Then $p \equiv 1 \pmod{8}$ and so $\left(\frac{2}{p}\right) = 1$. By (2.9), we have

$$\left(\frac{-14}{p}\right) = 1.$$

Case $p \equiv 15 \pmod{56}$: Then $p \equiv -1 \pmod{8}$ and so $\left(\frac{2}{p}\right) = 1$. By (2.9), we have

$$\left(\frac{-14}{p}\right) = 1.$$

Case $p \equiv 23 \pmod{56}$: Then $p \equiv -1 \pmod{8}$ and so $\left(\frac{2}{p}\right) = 1$. By (2.9), we have

$$\left(\frac{-14}{p}\right) = 1.$$

Case $p \equiv 25 \ (mod\ 56)$: Then $p \equiv 1 \ (mod\ 8)$ and so $\left(\frac{2}{p}\right) = 1$. By (2.9), we have

$$\left(\frac{-14}{p}\right) = 1.$$

Case $p \equiv 39 \ (mod\ 56)$: Then $p \equiv -1 \ (mod\ 8)$ and so $\left(\frac{2}{p}\right) = 1$. By (2.9), we have

$$\left(\frac{-14}{p}\right) = 1.$$

Then -14 is a quadratic residue modulo p. □

Theorem 2.20. *Let p be a prime. If $p \equiv 1, 9, 15, 23, 25, 39 \ (mod\ 56)$, then p is represented by the form $x^2 + 14y^2$ or the form $2x^2 + 7y^2$.*

Proof. Assume that $p \equiv 1, 9, 15, 23, 25, 39 \ (mod\ 56)$. By the previous lemma, -14 is a quadratic residue modulo p. Thus there exists $u \in \mathbb{Z}$ be such that

$$u^2 \equiv -14 \ (mod\ p). \tag{2.10}$$

Let Λ be a lattice in $\mathbb{R}^2$ defined by

$$\Lambda = \mathcal{L}(v_1, v_2) = \{mv_1 + nv_2 \colon m, n \in \mathbb{Z}\},$$

where $v_1 = (1, u)$ and $v_2 = (0, p)$. Then we have $det(\Lambda) = p$ and if $(y, x) \in \Lambda$, $x^2 + 14y^2 \equiv 0 \ (mod\ p)$ by (2.10). By letting

$$S = \{(y, x) \in \mathbb{R}^2 \colon x^2 + 14y^2 < 5p\},$$

We have

$$area(S) = \pi(\sqrt{\frac{5p}{14}})(\sqrt{5p}) = \pi(\frac{5}{\sqrt{14}})p > 4p = 4det(\Lambda).$$

Then there exists a lattice point $(d, c) \in S \setminus (0, 0)$ such that

$$0 < c^2 + 14d^2 < 5p \text{ and } c^2 + 14d^2 \equiv 0 \ (mod\ p).$$

Then $p \mid c^2 + 14d^2$, i.e. $c^2 + 14d^2 = p$ or $2p$ or $3p$ or $4p$. The first case is obvious.

Suppose that $c^2 + 14d^2 = 2p$. Then $c^2 + 14d^2$ is even. From $14d^2$ is even, then c is even. Hence there exists $k \in \mathbb{Z}$ such that $c = 2k$

Case d is odd : Then there exists $l \in \mathbb{Z}$ such that $d = 2l + 1$. We have

$$\begin{aligned} 2p = c^2 + 14d^2 &= (2k)^2 + 14(2l+1)^2 \\ &= 4k^2 + 14(4l^2 + 4l + 1) \\ &= 2(2k^2 + 28l^2 + 28l + 7). \end{aligned}$$

Then

$$\begin{aligned} p &= 2(k^2) + 7(4l^2 + 4l + 1) \\ &= 2(k)^2 + 7(2l+1)^2. \end{aligned}$$

Case d are even : Thus there exists $l \in \mathbb{Z}$ such that $d = 2l$. We have

$$\begin{aligned} 2p = c^2 + 14d^2 &= (2k)^2 + 14(2l)^2 \\ 2p &= (4k^2) + 14(4l^2) \\ 2p &= 2(2k^2 + 28l^2). \end{aligned}$$

Then

$$\begin{aligned} p &= 2k^2 + 28l^2 \\ p &= 2(k^2) + 7(2l)^2. \end{aligned}$$

We can conclude that if $c^2 + 14d^2 = 2p$, then p is represented by the form $2x^2 + 7y^2$.

Suppose that $c^2 + 14d^2 = 3p$.

Case $p \equiv 1, 15 \ (mod\ 56)$: Then

$$c^2 \equiv c^2 + 14d^2 \equiv 3p \equiv 3 \ (mod\ 14).$$

Then

$$c^2 \equiv 3 \ (mod\ 14) \text{ and so } c^2 \equiv 3 \ (mod\ 7).$$

Then 3 is a quadratic residue modulo 7, i.e. $\left(\frac{3}{7}\right) = 1$. Thus

$$1 = \left(\frac{3}{7}\right) \equiv 3^{\frac{7-1}{2}} \equiv 27 \equiv 6 \ (mod\ 7),$$

a contradiction.

Case $p \equiv 9, 23 \ (mod\ 56)$: Then

$$c^2 \equiv c^2 + 14d^2 \equiv 3p \equiv -1 \ (mod\ 14).$$

Then $c^2 \equiv 6$ $(mod\ 7)$ and so 6 is a quadratic residue modulo 7, i.e. $\left(\frac{6}{7}\right) = 1$. Thus

$$1 = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = (-1)^{\frac{7^2-1}{8}}\left(\frac{7}{3}\right)(-1)^{(\frac{7-1}{2})(\frac{3-1}{2})} = (1)\left(\frac{1}{3}\right)(-1) = -1,$$

a contradiction.

Case $p \equiv 25, 39$ $(mod\ 56)$: Then

$$c^2 \equiv c^2 + 14d^2 \equiv 3p \equiv 5 \ (mod\ 14).$$

Then $c^2 \equiv 5$ $(mod\ 7)$ and so 5 is a quadratic residue modulo 7. i.e. $\left(\frac{5}{7}\right) = 1$. Thus

$$1 = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)(-1)^{(\frac{7-1}{2})(\frac{5-1}{2})} = \left(\frac{2}{5}\right)(1) = (-1)^{\frac{5^2-1}{8}} = (-1)^3 = -1,$$

a contradiction.

Suppose that $c^2 + 14d^2 = 4p$, then $4 \mid c^2 + 14d^2$. From $c^2 + 14d^2$ and $14d^2$ are even, then c is even, i.e., $c^2 \equiv 0$ $(mod\ 4)$. Suppose that d is odd, then $d^2 \equiv 1$ $(mod\ 4)$. We have

$$4p \equiv c^2 + 14d^2 \equiv 0 + 14(1) \equiv 2 \ (mod\ 4),$$

which is a contradiction. Hence d is even. From c and d are both even, then there exist $m, n \in \mathbb{Z}$ such that $c = 2m$ and $d = 2n$. We have

$$\begin{aligned} 4p = c^2 + 14d^2 &= (2m)^2 + 14(2n)^2 \\ &= 4(m^2 + 14n^2). \end{aligned}$$

This means that

$$p = m^2 + 14n^2.$$

Then p is represented by the form $x^2 + 14y^2$. $\square$

Examples 2.21.

1. *From* 113 *is an odd prime with* $113 \equiv 1$ $(mod\ 56)$, 113 *can be represented by the form* $x^2 + 14y^2$ *or the form* $2x^2 + 7y^2$. *In fact,* $113 = 2(5)^2 + 7(3)^2$.

2. *From* 233 *is an odd prime with* $233 \equiv 9$ $(mod\ 56)$, 233 *can be represented by the form* $x^2 + 14y^2$ *or the form* $2x^2 + 7y^2$. *In fact,* $233 = (3)^2 + 14(4)^2$.

3. *From* 71 *is an odd prime with* $71 \equiv 15 \pmod{56}$, 71 *can be represented by the form* x^2+14y^2 *or the form* $2x^2+7y^2$. *In fact,* $71 = 2(2)^2+7(3)^2$.

4. *From* 23 *is an odd prime with* $23 \equiv 23 \pmod{56}$, 233 *can be represented by the form* x^2+14y^2 *or the form* $2x^2+7y^2$. *In fact,* $23 = (3)^2+14(1)^2$.

5. *From* 137 *is an odd prime with* $137 \equiv 25 \pmod{56}$, 137 *can be represented by the form* x^2+14y^2 *or the form* $2x^2+7y^2$. *In fact,* $137 = (9)^2+14(2)^2$.

6. *From* 151 *is an odd prime with* $151 \equiv 39 \pmod{56}$, 151 *can be represented by the form* x^2+14y^2 *or the form* $2x^2+7y^2$. *In fact,* $151 = (5)^2+14(3)^2$.

Remark. *According to the form* x^2+11y^2, *we cannot find the sufficient congruent condition for representing primes by this form. From [10], we know that* -11 *is a quadratic residue modulo* p *if* $p \equiv 1, 5, 9, 25, 37 \pmod{44}$. *But we can find examples of prime numbers that satisfies the congruences* $p \equiv 1, 5, 9, 25, 37 \pmod{44}$ *but they cannot be represented by the form* x^2+11y^2 *as follows:*

Examples 2.22.

1. $89 \equiv 1 \pmod{44}$ *but* 89 *can not represented by the form* x^2+11y^2 *which can be shown as follows: If there exist* $m, n \in \mathbb{Z}$ *be such that* $m^2+11n^2 = 89$, *then*

$$n = -2, -1, 0, 1 \text{ or } 2.$$

In the case that $n = 0$, *we have* $m^2 = 89$, *a contradiction. In the case that* $n = 1$ *or* -1, *we get* $m^2 = 78$, *a contradiction. And in the case that* $n = 2$ *or* -2, *we then have* $m^2 = 45$, *a contradiction.*

2. $5 \equiv 5 \pmod{44}$. *If there exist* $m, n \in \mathbb{Z}$ *be such that* $m^2+11n^2 = 5$, *then* $n = 0$. *Therefore* $m^2 = 5$, *a contradiction. This implies that* 5 *can not represented by the form* x^2+11y^2.

3. $97 \equiv 9 \pmod{44}$ *but* 97 *can not represented by the form* x^2+11y^2 *which can be shown as follows: If there exist* $m, n \in \mathbb{Z}$ *be such that* $m^2+11n^2 = 97$, *then*

$$n = -2, -1, 0, 1 \text{ or } 2.$$

In the case that $n = 0$, $m^2 = 97$ *yield a contradiction. And in the case that* $n = 1$ *or* -1, $m^2 = 86$ *which is a contradiction. And in the case that* $n = 2$ *or* -2, *we have* $m^2 = 53$, *a contradiction.*

4. $113 \equiv 25 \ (mod\ 44)$ *but* 113 *can not represented by the form* $x^2 + 11y^2$ *which can be shown as follows: If there exist* $m, n \in \mathbb{Z}$ *be such that* $m^2 + 11n^2 = 113$, *then*

$$n = -3, -2, -1, 0, 1, 2 \ or\ 3.$$

In the case that $n = 0$, $m^2 = 113$ *yields a contradiction. And in the case that* $n = 1$ *or* -1, $m^2 = 102$ *which is a contradiction. And in the case that* $n = 2$ *or* -2, $m^2 = 69$ *yields a contradiction. And in the case that* $n = 3$ *or* -3, $m^2 = 14$ *which is a contradiction.*

5. $37 \equiv 37 \ (mod\ 44)$ *but* 37 *can not represented by the form* $x^2 + 11y^2$ *which can be shown as follows: If there exist* $m, n \in \mathbb{Z}$ *be such that* $m^2 + 11n^2 = 37$, *then*

$$n = -1, 0 \ or\ 1.$$

Similarly, in any case, we obtain a contradiction.

Bibliography

[1] D.A. Buell, *Binary Quadratic Forms : classical theory and modern computations*, Springer-Verlag, New York, 1989.

[2] T. Chaichana, *Theory of Numbers* 2301331, lecture note, Chulalongkorn University, 2018.

[3] D.A. Cox, *Primes of the Form* $x^2 + ny^2$ *: Fermat, Class Field Theory and Complex Multiplication*, John Wiley&Sons, New York, 1989.

[4] T. Hammonds, Quadratic Forms [Online]. Available from: www.andrew.cmu.edu [2018].

[5] J. Kaplan, Binary Quadratic Forms, Genus Theory, and Primes of the Form $p = x^2 + ny^2$ [Online]. Available from: http://www.math.uthicago.edu [2014].

[6] F. Lemmermeyer. Binary uadratic Forms [Online]. Available from: http://www.rzuser.uni-heidelberg.de/∼hb3/ [2010].

[7] O. Regev. Introduction. Tel Ariv University, 2004.

[8] R. L. Shepherd, Binary Quadratic Forms and Genus Theory. The University of North Carolina at Greensboro, 2013.

[9] B. K. Spearman and K. S. Williams, Representing Primes by Quadratic Forms. The American Mathematical Monthly, 99 (1992), 423-426.

[10] C. Thomas, On Representations of integers by the quadratic form $x^2 - Dy^2$. Rochester Institute of Technology, 2012.

[11] J. Vigil, Formula for the Area of an Ellipse [online]. Available from https://study.com/academy/lesson/formula-for-the-area-of-an-ellipse.html [2017].

The Project Proposal of Course 2301399 Project Proposal
Academic Year 2019

Project Title (Thai) คลาสของจำนวนเฉพาะที่เขียนได้ด้วยรูปแบบกำลังสอง

Project Title (English) A class of primes represented by some quadratic forms

Project Advisor Assoc.Prof.Tuangrat Chaichana

By Miss Warintorn Pongsumrankul

Mathematics, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University

---

Background and Rationale

An *integral binary quadratic form* is a quadratic polynomial of two variables

$$f(x,y) = ax^2 + bxy + cy^2$$

over $\mathbb{Z}$ and the integer $D = b^2 - 4ac$ is called the *discriminant* of form $f(x,y)$. We say that a binary quadratic form $f(x,y)$ is *primitive* if a, b and c are relatively prime. An integer m is said to be *represented by* f if there exist integers x and y such that $f(x,y) = m$.

One of interesting problems relating to quadratic forms is representation of primes by binary quadratic forms, see e.g. [1], [3], [5], [6], [8] and [9]. Historically, a representation of primes of the form $p = x^2 + ny^2$ for arbitrary n have been widely studies. For example, Euler gave the rigorous proofs of the following four statements stated by Fermat, see e.g. [3] :

(1) $p = x^2 + y^2$ if and only if $p = 2$ or $p \equiv 1 (mod\ 4)$;

(2) $p = x^2 + 2y^2$ if and only if $p = 2$ or $p \equiv 1, 3 (mod\ 8)$;

(3) $p = x^2 + 3y^2$ if and only if $p = 3$ or $p \equiv 1 (mod\ 3)$;

(4) $p = x^2 + 4y^2$ if and only if $p \equiv 1 (mod\ 4)$.

and he also conjected statement that there are primes satisfying

$$p = x^2 + 6y^2 \text{ if and only if } p \equiv 1, 7 (mod\ 24).$$

This conjecture was proved by Kaplan [5] in 2014. The Fermat's statements and the result for the case $n = 7$ were also shown in [5] by using the different techniques of proofs.

The failure of representability of primes by quadratic forms using the congruence condition was also studied. For example, in 1992, Spearman et al [9] proved that there do not exist positive integers $s, a_1, \dots, a_s, m$ with $(a_i, m) = 1\ (i = 1, \dots, s)$ such that for primes $p \neq 2,7$

$$p = x^2 + 14y^2 \text{ if and only if } p \equiv a_1, \ldots, a_s \ (mod\ \mathrm{m}).$$

In this project, we will find a class of primes represented by some binary quadratic form with negative discriminant.

Objectives

Find a class of primes represented by some binary quadratic form with negative discriminant.

Scope

In this project, we restrict our attention to the binary quadratic forms which are primitive, irreducible and have negative discriminant.

Project Activities

1. Review basic knowledge on binary quadratic forms
2. Study reseach papers related to our project
3. Present a proposal of the project
4. Find a class of primes represented by some binary quadratic forms with negative discriminant
5. Write the report

Duration

Procedue	August 2019 – April 2020								
	Aug.	Sep.	Oct.	Nov.	Dec.	Jan.	Feb.	Mar.	Apr.
1. Review basic knowledge on binary quadratic forms									
2. Study reseach papers related to our project									
3. Present a proposal of the project									
4. Find a class of primes represented by some binary quadratic forms with negative discriminant									
5. Write the report									

Benefits

1. Obtain the information searching skills and thinking skills
2. Obtain a class of primes represented by some binary quadratic forms with negative discriminant

Equipment

1. Computer
2. Microsoft word 2013
3. Latex
4. Stationery

Author’s profile

Miss Warintorn Pongsumrankul

ID 5933544823

Department of Mathematics and Computer Science

Faculty of Science Chulalongkorn University