1972

A Minimum Problem Connected with Complete Residue Systems in the Eisenstein Integers

David Peter Ochsner

A MINIMUM PROBLEM CONNECTED WITH
COMPLETE RESIDUE SYSTEMS
IN THE EISENSTEIN INTEGERS

BY

DAVID PETER OCHSNER

A thesis submitted
in partial fulfillment of the requirements for the
degree Master of Science, Major in
Mathematics, South Dakota
State University

1972

A MINIMUM PROBLEM CONNECTED WITH

COMPLETE RESIDUE SYSTEMS

IN THE EISENSTEIN INTEGERS

This thesis is approved as a creditable and independent investigation by a candidate for the degree, Master of Science, and is acceptable for meeting the thesis requirements for this degree. Acceptance of this thesis does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department.

Thesis Adviser   Date

Head, Mathematics Department   Date

ACKNOWLEDGMENTS

I would like to express my sincere appreciation to Dr. G. E. Bergum of the Mathematics Department for the time and effort he afforded to put this thesis in its final form. I would also like to thank Professor Milo Bryn for reading the manuscript and making many helpful suggestions.

DPO

TABLE OF CONTENTS

Chapter Page

I. INTRODUCTION 1

II. PROOF OF THEOREM 1.2 5

III. PRIMES AND $T_2 = \emptyset$. 16

REFERENCES 22

LIST OF FIGURES

Figure | Page

1. C.R.S. (mod 18ω) 7
2. C.R.S. (mod $6 - 12\omega$) 7
3. C.R.S. (mod 14ω) 8
4. C.R.S. (mod $5 + 15\omega$) 9
5. C.R.S. (mod 13ω) 11
6. C.R.S. (mod $7 - 14\omega$) 11
7. C.R.S. (mod $-7 + 8\omega$) 14
8. C.R.S. (mod $5 - 7\omega$) 14
9. C.R.S. (mod $2 + 16\omega$) 17
10. C.R.S. (mod $4 - 12\omega$) 18
11. C.R.S. (mod $3 - 6\omega$) where $(3 - 6\omega) = (-1)(2 + \omega)^2(2 + 3\omega)$ 19
12. C.R.S. (mod $7 + 14\omega$) where $(7 + 14\omega) = (-\omega)(2 + \omega)(2 + 3\omega)(3 + 2\omega)$ 19
13. C.R.S. (mod $-9 + 4\omega$) where $(-9 + 4\omega) = (2 + 3\omega)(3 + 5\omega)$ 20
14. C.R.S. (mod $-8 + 9\omega$) where $(-8 + 9\omega) = (2 + 3\omega)(5 + 6\omega)$ 21

CHAPTER I

INTRODUCTION

History tells us that one of the most interesting topics of mathematics is elementary number theory, the arithmetic Gauss spoke of when he said, "Mathematics is the queen of the sciences and arithmetic the queen of mathematics." We will investigate one conjecture concerning the theory of numbers.

Throughout this paper small case Latin letters with the exception of e and i will represent integers where the set of rational integers is denoted by Z. The Latin letters e and i respectively represent the base for the natural logarithms and the so-called imaginary unit for the set of complex numbers. An Eisenstein integer, α, is a complex number that can be written as $\alpha = a + b\omega$ where a and b are rational integers and ω is the cube root of unity, $e^{2\pi i/3}$, so that $\omega = (-1 + i\sqrt{3})/2$. We denote the set of Eisenstein integers by $Z(\omega) = \{a + b\omega \mid a,b \in Z\}$ and let the Greek letters α, β, γ, ρ, and δ represent integers in $Z(\omega)$. Since ω is a cube root of unity, $\omega^2 + \omega + 1 = 0$.

The set of integers in $Z(\omega)$ will be represented geometrically by the lattice points in a Cartesian coordinate system formed by the intersections of the lines through the points (m,0) and making angles of 60° or 120° with the x-axis. The system is a honeycomb of equilateral triangles.

If α and β are elements of $Z(\omega)$ where $\alpha \neq 0$, we say that α divides β, written as $\alpha | \beta$, iff there exists a γ in $Z(\omega)$ such that $\beta = \alpha\gamma$. Furthermore, if $\delta | \alpha$ for all α in $Z(\omega)$, then δ is called a unit. Since α is a complex number, it has a complex conjugate denoted by $\overline{\alpha}$. It is easy to show if $\alpha = a + b\omega$, then $\overline{\alpha} = a - b(1 + \omega)$. Since the norm of α, denoted by $N(\alpha)$, is defined as $N(\alpha) = \alpha\overline{\alpha}$, we see that $N(\alpha) = a^2 - ab + b^2$. Obviously $N(\alpha\beta) = N(\alpha)N(\beta)$ for all α and β, and $N(\alpha) \geq 0$ for any α. Using these two facts, it can be shown that δ is a unit iff $N(\delta) = 1$. Hence, the units of $Z(\omega)$ are ± 1, $\pm\omega$, $1 + \omega$, and $-1 - \omega$. Throughout the remainder of this paper we shall let the Greek letter δ represent any unit of $Z(\omega)$. We define α and β as associates iff $\alpha = \beta\delta$. If $\alpha = a + b\omega$, then we define $|\alpha|$ as $|\alpha| = \sqrt{a^2 - ab + b^2}$.

We say that α and β are congruent modulo γ iff $\gamma | (\alpha - \beta)$. We write $\alpha \equiv \beta \pmod{\gamma}$. It is a trivial matter to show that congruence modulo γ is an equivalence relation on $Z(\omega)$. Hence, as in the real case, we define a complete residue system modulo γ as a nonempty collection S of elements in $Z(\omega)$ such that (1) no two elements of S are congruent modulo γ, and (2) every element of $Z(\omega)$ not in S is congruent to some element in S. A complete residue system modulo γ is abbreviated as C.R.S. (mod γ).

In [1], Bergum exhibits several representations of a C.R.S. (mod γ). In particular, the following is observed:

Theorem 1.1. For any γ, let $\nabla = \gamma(1 - \omega)/3$. Let T_1 be the set of points interior to the hexagon ABCDEF whose vertices are respectively given by $\nabla e^{\pi k i/3}$ where $1 \leq k \leq 6$. Let T_2 be the set of points on the line segments $(-\nabla, \nabla e^{4\pi i/3}]$, $[\nabla e^{4\pi i/3}, \nabla e^{5\pi i/3}]$, and $[\nabla e^{5\pi i/3}, \nabla)$. Let $T = T_1 \cup T_2$. The set T is a C.R.S. (mod γ).

Furthermore, Bergum [1] shows that $T = T_1 \cup T_2$ is an "absolute minimal representation" where such a representation is defined as follows:

Definition 1.1. A representation T of a C.R.S. (mod γ) is said to be an absolute minimal representation iff for any representation R of a C.R.S. (mod γ) we have

$$\sum_{\alpha\epsilon T} |\alpha| \leq \sum_{\beta\epsilon R} |\beta|.$$

A problem suggested in [1] is that of finding necessary and sufficient conditions for an absolute minimal representation of a C.R.S. (mod γ) to be unique. It is quite apparent that $T = T_1 \cup T_2$ is unique iff $T_2 = \emptyset$. It is the purpose of this thesis, therefore, to establish necessary and sufficient conditions for T_2 to be empty.

The appropriate result, which is established in Chapter II, is stated as follows:

Theorem 1.2. The "absolute minimal representation" T of a C.R.S. (mod γ) has $T_2 = \emptyset$ iff $(a - 2b, a + b, b - 2a) = 1$ where $\gamma = a + b\omega$ and $(a - 2b, a + b, b - 2a)$ denotes the greatest common divisor of the ordered triple.

In Chapter III, we introduce the concept of prime Eisenstein integers and discuss the relationship of the prime decomposition of $\gamma = a + b\omega$ to T_2 being empty.

CHAPTER II

PROOF OF THEOREM 1.2

If $\gamma = a + b\omega$, then the coordinates of A, B, and C are respectively $\left(\frac{a-b}{2}, \frac{a+b}{6}\sqrt{3}\right)$, $\left(-\frac{b}{2}, \frac{2a-b}{6}\sqrt{3}\right)$, and $\left(-\frac{a}{2}, \frac{a-2b}{6}\sqrt{3}\right)$. Since the hexagon is symmetric with respect to the origin, the coordinates of D, E, and F are obvious. Using the distance formula, we find that the length of each side of the hexagon is $|\gamma|/\sqrt{3}$ units so that the hexagon is regular.

The linear equation for the line through A and B is

$$y = x\left(\frac{2b - a}{3a}\right)\sqrt{3} + \frac{N(\gamma)}{3a}\sqrt{3}$$

if $a \neq 0$ and $x = -b/2$ if $a = 0$ while the equation of the line through B and C is

$$y = x\left(\frac{a + b}{3(a - b)}\right)\sqrt{3} + \frac{N(\gamma)}{3(a - b)}\sqrt{3}$$

if $a \neq b$ and $x = -b/2$ if $a = b$. Similarly, the line through C and D is expressed by

$$y = x\left(\frac{b - 2a}{3b}\right)\sqrt{3} - \frac{N(\gamma)}{3b}\sqrt{3}$$

if $b \neq 0$ and $x = -a/2$ if $b = 0$. By symmetry, the equations for the lines DE, EF, and FA are seen to be respectively the same as the equations for the sides AB, BC, and CD except for the y-intercept which is of the opposite sign.

Lemma 2.1. Let $\gamma = a + b\omega$. If $(a - 2b, a + b, b - 2a) = 3d$, then $T_2 \neq \emptyset$. (See figures 1 and 2).

Proof.--Choose $\alpha = \left(\frac{b - 2a}{3}\right) - \left(\frac{a + b}{3}\right)\omega = \left(\frac{b - a}{2}\right) - \left(\frac{a + b}{6}\right)\sqrt{3}i$. Since $3|3d$, α is in $Z(\omega)$. Using the equation of the line through D and E, we have

$$\left(\frac{b - a}{2}\right)\left(\frac{2b - a}{3a}\right)\sqrt{3} - \frac{N(\gamma)}{3a}\sqrt{3} = -\left(\frac{a + b}{6}\right)\sqrt{3}$$

if $a \neq 0$. If $a = 0$, then $\alpha = \frac{b}{2} - \frac{b}{6}\sqrt{3}i$. Hence, in either case, we see that α is on DE. Since α is the point D, $T_2 \neq \emptyset$ and the lemma is proved.

Lemma 2.2. If $\gamma = a + b\omega$ and $(a - 2b, a + b, b - 2a) = 3d + 2$, then $T_2 \neq \emptyset$. (See figures 3 and 4).

Proof.--We first observe that $(3d + 2)|3b$ and $(3d + 2)|3a$. However $(3d + 2, 3) = 1$ so that $(3d + 2)|a$ and $(3d + 2)|b$.

Let $x = \frac{3d(b - a) + (2b - a)}{2(3d + 2)}$ and $y = \frac{-a - d(a + b)}{2(3d + 2)}$ so that $x + y = \frac{(b - a) + d(b - 2a)}{3d + 2}$. Obviously $(x + y)$ and $2y$ are rational integers so that

$$\alpha = (x + y) + 2y\omega = x + y\sqrt{3}i$$

is in $Z(\omega)$.

C.R.S. (mod 18ω)

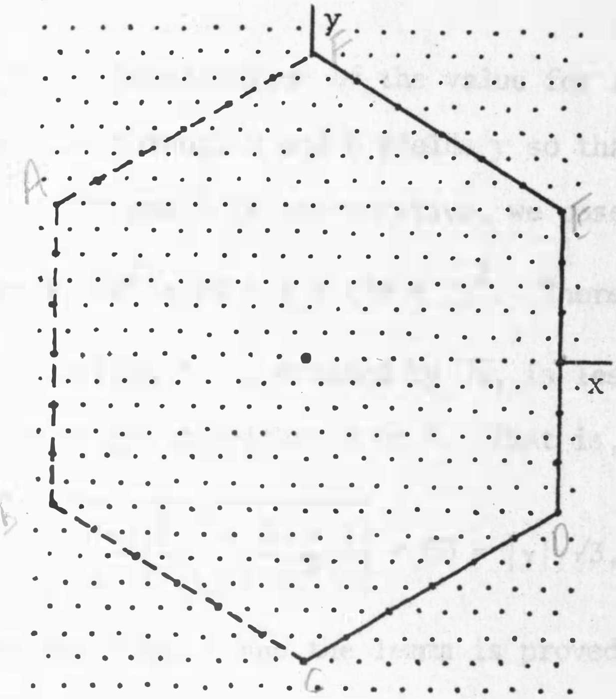

FIG. 1

C.R.S. (mod 6 - 12ω)

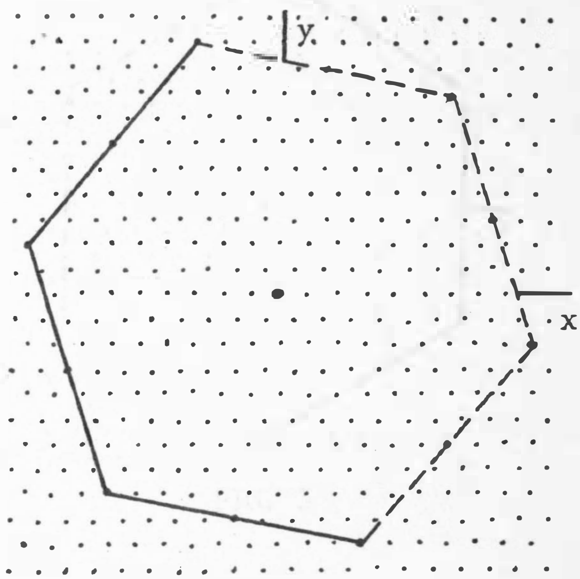

FIG. 2

If a = 0, then we find that $\alpha = \frac{b}{2} - \frac{db\sqrt{3}i}{2(3d + 2)}$ and α is on the line DE.

Suppose $a \neq 0$. Substitution of the value for x into the equation of the line through D and E yields y so that α is on DE.

Since $3d + 2 > 0$ and d is non-negative, we observe that $3d + 1 > 0$. Hence, $9d^2 + 9d + 3 < (3d + 2)^2$. Therefore, the distance from the origin to α, denoted by $\overline{O\alpha}$, is less than the distance from the origin to either D or E. That is,

$$\overline{O\alpha} = \sqrt{\frac{N(\gamma)}{3}\left(\frac{9d^2 + 9d + 3}{(3d + 2)^2}\right)} < \overline{OD} = |\gamma|/\sqrt{3},$$

so that α is between D and E and the lemma is proved.

C.R.S. (mod 14ω)

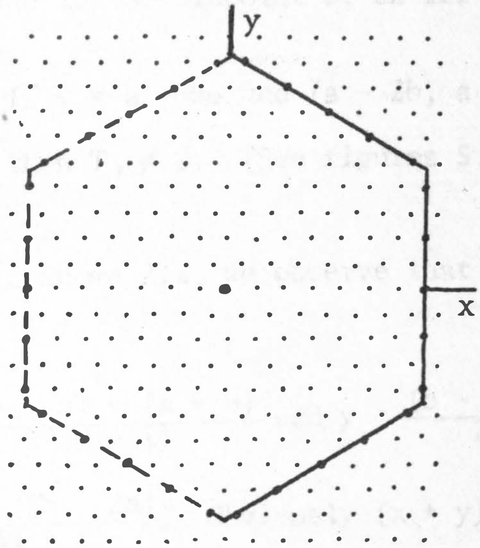

FIG. 3

C.R.S. (mod $5 + 15\omega$)

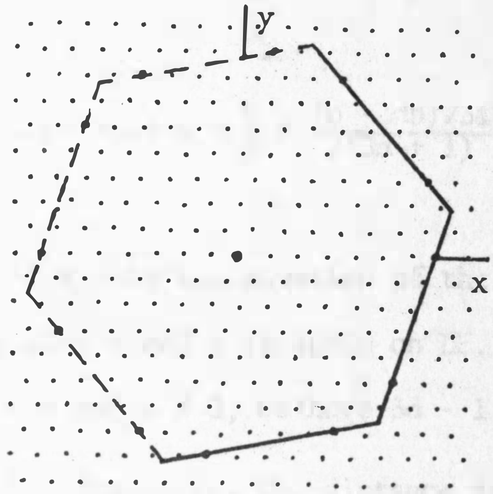

FIG. 4

Comparing the coordinates of α with those of D and the midpoint of DE, we have

<u>Corollary 2.1.</u> The point α, as described in Lemma 2.2, is never D and is the midpoint of DE iff $d = 0$.

<u>Lemma 2.3.</u> If $\gamma = a + b\omega$ and $(a - 2b, a + b, b - 2a) = 3d + 1$ with $d \neq 0$, then $T_2 \neq \emptyset$. (See figures 5 and 6).

<u>Proof.</u>--As in Lemma 2.2, we observe that $(3d + 1)|a$ and $(3d + 1)|b$.

Let $x = \dfrac{3d(b - a) + (a + b)}{2(3d + 1)}$ and $y = \dfrac{(b - a) - d(a + b)}{2(3d + 1)}$ so that $x + y = \dfrac{b + d(b - 2a)}{3d + 1}$. Obviously $(x + y)$ and $2y$ are rational integers so that

$$\alpha = (x + y) + 2y\omega = x + y\sqrt{3}i$$

is in $Z(\omega)$.

If $a = 0$, we find that $\alpha = \frac{b}{2} + \frac{(b - db)\sqrt{3}i}{2(3d + 1)}$ and α is on the line DE.

Substitution of x into the equation of the line through D and E with $a \neq 0$ yields y and α is again on DE.

Since $3d + 1 > 0$ and $d \neq 0$, we have $3d - 1 > 0$ so that $(3d + 1)^2 > 9d^2 + 3$. Therefore, the distance from the origin to α, denoted by $\overline{O\alpha}$, is less than the distance from the origin to D or E. That is,

$$\overline{O\alpha} = \sqrt{\frac{N(\gamma)}{3}\left(\frac{9d^2 + 3}{(3d + 1)^2}\right)} < \overline{OD} = |\gamma|/\sqrt{3}.$$

Hence, α is between D and E and the lemma is proved.

Examination of the coordinates of α, D, and the midpoint of the line joining D and E yields the following result:

<u>Corollary 2.2.</u> The point α, as described in Lemma 2.3, is never D and is the midpoint of DE iff $d = 1$.

Combining Lemmas 2.1, 2.2, and 2.3, we have

<u>Corollary 2.3.</u> Let $\gamma = a + b\omega$. If $(a - 2b, a + b, b - 2a) \neq 1$, then $T_2 \neq \emptyset$. Equivalently, if $T_2 = \emptyset$, then $(a - 2b, a + b, b - 2a) = 1$.

C.R.S. (mod 13ω)

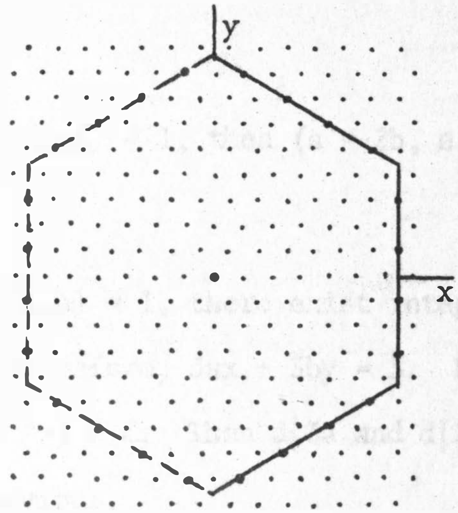

FIG. 5

C.R.S. (mod $7 - 14\omega$)

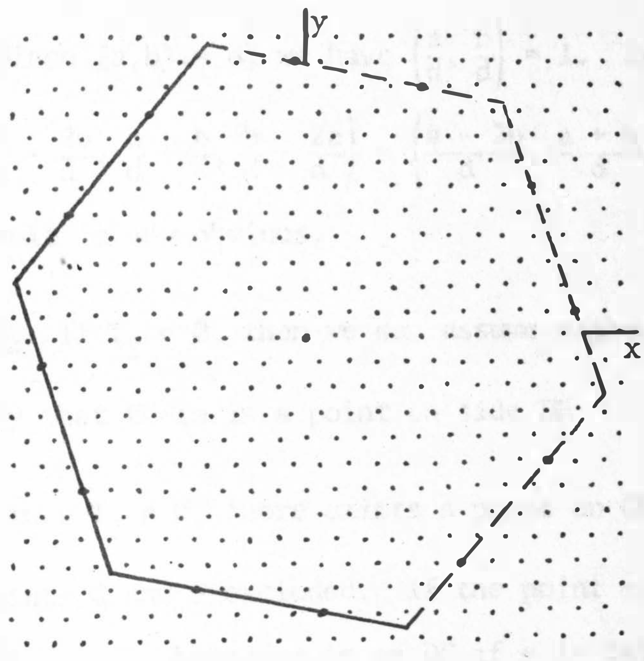

FIG. 6

To prove the converse of Corollary 2.3, we first establish several lemmas.

Lemma 2.4. If $(a,b) = 1$, then $(a - 2b, a + b, b - 2a) = 1$ or 3.

Proof.--Since $(a,b) = 1$, there exist integers x and y such that $ax + by = 1$. Therefore, $3ax + 3by = 3$. Let $(a - 2b, a + b, b - 2a) = d$. Then $d|3a$ and $d|3b$ so that $d|3$. The result is now obvious.

Lemma 2.5. If $(a,b) = d$, then $(a - 2b, a + b, b - 2a) = d$ or $3d$.

Proof.--Since $(a,b) = d$, we have $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. By Lemma 2.4, we see that $\left(\frac{a}{d} - \frac{2b}{d}, \frac{a}{d} + \frac{b}{d}, \frac{b}{d} - \frac{2a}{d}\right) = \left(\frac{a - 2b}{d}, \frac{a + b}{d}, \frac{b - 2a}{d}\right) = 1$ or 3. The result is now obvious.

Lemma 2.6. If $T_2 \neq \emptyset$, then we can assume without loss of generality that there is a point on side DE.

Proof.--Since $T_2 \neq \emptyset$, there exists a point on CD, DE, or EF with the points C and F excluded. If the point α is on CD, then $\alpha(1 + \omega)$ is on DE while $-\omega\alpha$ is on DE if α is between E and F.

<u>Theorem 2.1.</u> If $\gamma = a + b\omega$ and $T_2 \neq \emptyset$, then $(a - 2b, a + b, b - 2a) \neq 1$. (See figures 7 and 8).

<u>Proof.</u>--By Lemma 2.5, the result follows vacuously if $(a,b) = d \neq 1$. Suppose $(a,b) = 1$ and $\alpha = u + v\omega$ is on the line through D and E. Obviously, $a \neq 0$ so that

$$N(\gamma) = -a(u + v) + b(2u - v).$$

Because $a(a - b) + bb = N(\gamma)$ and $(a,b) = 1$, we know that the linear Diophantine equation $ax + by = N(\gamma)$ is solvable and all solutions are given by

$$\left.\begin{array}{l} x = (a - b) + bt \\ y = b - at \end{array}\right\} \text{ for some } t.$$

Hence,

$$\left.\begin{array}{r} 2u - v = b - at \\ u + v = b - a - bt \end{array}\right\} \text{ for some } t,$$

or

$$3u = (2b - a) - t(a + b).$$

Let the directed distance from D to α be denoted by $|D\alpha|$. Then since $a \neq -b$,

$$|D\alpha| = \left|\frac{3u + (2a - b)}{a + b}\right| |\gamma|/\sqrt{3}$$
$$= |1 - t|\,|\gamma|/\sqrt{3}.$$

The point α is between D and E, in a directed sense, iff $1 - t = 0$ or 1. If $t = 0$, then $u = \frac{2b - a}{3}$ and $v = \frac{b - 2a}{3}$. But u and v are rational integers so that (a - 2b, a + b, b - 2a) $\neq$ 1. If t = 1, then $u = \frac{b - 2a}{3}$ and $v = \frac{-(a + b)}{3}$. Hence, we again have (a - 2b, a + b, b - 2a) $\neq$ 1 and the theorem is proved.

C.R.S. (mod -7 + 8ω)

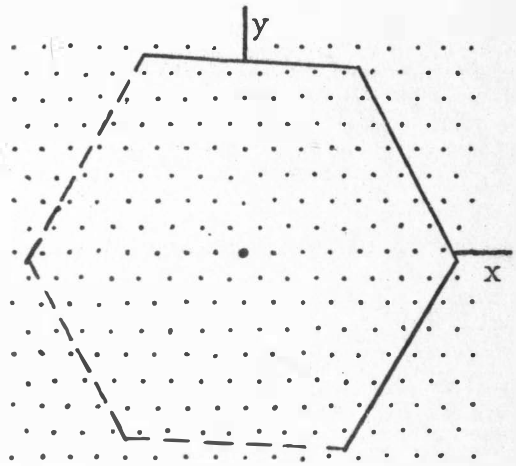

FIG. 7

C.R.S. (mod 5 - 7ω)

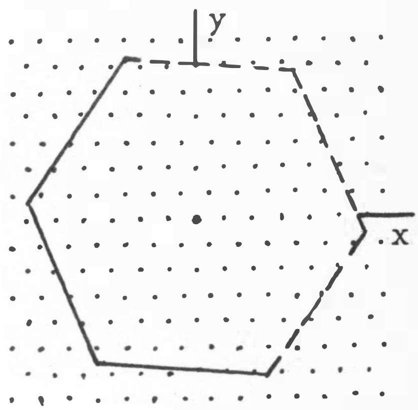

FIG. 8

As a consequence of Theorem 2.1, we have

<u>Corollary 2.4.</u> Let $\gamma = a + b\omega$. If $T_2 \neq \emptyset$ and $(a,b) = 1$, then the only points in T_2 are D and E.

Theorem 1.2 is a direct result of Corollary 2.3 and Theorem 2.1.

CHAPTER III

PRIMES AND $T_2 = \emptyset$

We say that $\rho = a + b\omega$ is a prime iff $\rho = \alpha\beta$ implies that α or β is a unit but not both. Obviously, all of the associates of ρ and $\bar{\rho}$ are prime if ρ is prime. If ρ is a prime in $Z(\omega)$ and Z, we call ρ a real prime. Primes p in Z are, in contrast, referred to as rational primes.

In [3], we find a discussion of primes. In particular we find

Theorem 3.1. (a) $\rho = 2 + \omega$ is a prime.

(b) ρ is a real prime iff ρ is a rational prime congruent to 2 modulo 3.

(c) $\rho = a + b\omega$, where ρ is not an associate of a prime in (a) or (b), is a non-real prime iff $N(\rho)$ is a rational prime congruent to 1 modulo 3.

Since $Z(\omega)$ is a Euclidean domain it is a unique factorization domain. Hence, every γ in $Z(\omega)$ can be written as a product of primes in $Z(\omega)$ and the representation is unique up to order and units.

Lemma 3.1. Let $\gamma = a + b\omega$. If the prime decomposition of γ contains at least one rational prime p, then $T_2 \neq \emptyset$. (See figures 9 and 10).

Proof.--Since $p|\gamma$, we know that $p|(a,b)$. The result follows from Lemma 2.5 and Corollary 2.3.

C.R.S. (mod 2 + 16ω)

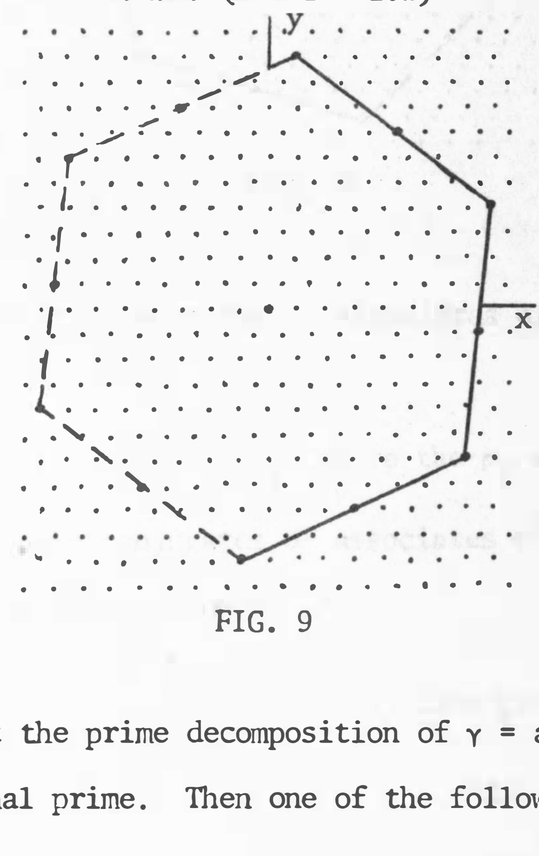

FIG. 9

Assume that the prime decomposition of $\gamma = a + b\omega$ does not contain a rational prime. Then one of the following must be true:

(a) $\gamma = \delta\rho_1^{n_1}\rho_2^{n_2}\cdots\rho_k^{n_k}$ where the ρ_i are all non-real primes and no two are conjugates or associates of each other.

(b) $\gamma = \delta(2 + \omega)^n\rho_1^{n_1}\rho_2^{n_2}\cdots\rho_k^{n_k}$ where the ρ_i are all non-real

C.R.S. (mod 4 - 12ω)

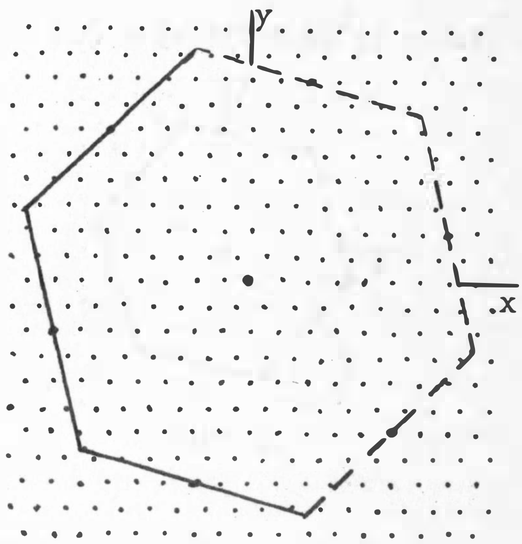

FIG. 10

primes and no two are conjugates or associates of each other and $\delta = \pm 1$.

(c) $\gamma = \delta(2 + \omega)\rho_1^{n_1}\rho_2^{n_2}\ldots\rho_k^{n_k}$ where the ρ_i are all non-real primes and no two are conjugates or associates of each other and δ is a unit different from ± 1.

Lemma 3.2. If $\gamma = a + b\omega$ is of the form given in (b) or (c), then $T_2 \neq \emptyset$. (See figures 11 and 12).

Proof.--Since $\gamma = a + b\omega = (2 + \omega)(u + v\omega)$, we see that $a = 2u - v$ and $b = u + v$. By adding, we conclude that $3|(a + b)$. Subtracting 2b from a we have $3|(a - 2b)$. Hence, $(a - 2b, a + b, b - 2a) \neq 1$. Therefore, by Corollary 2.3, we are finished.

C.R.S. (mod $3 - 6\omega$) where

$$(3 - 6\omega) = (-1)(2 + \omega)^2(2 + 3\omega)$$

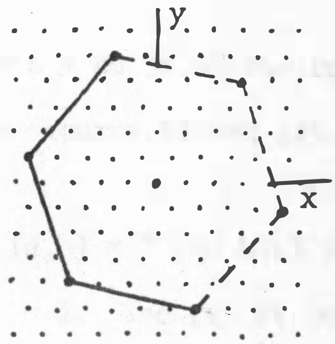

FIG. 11

C.R.S. (mod $7 + 14\omega$) where

$$(7 + 14\omega) = (-\omega)(2 + \omega)(2 + 3\omega)(3 + 2\omega)$$

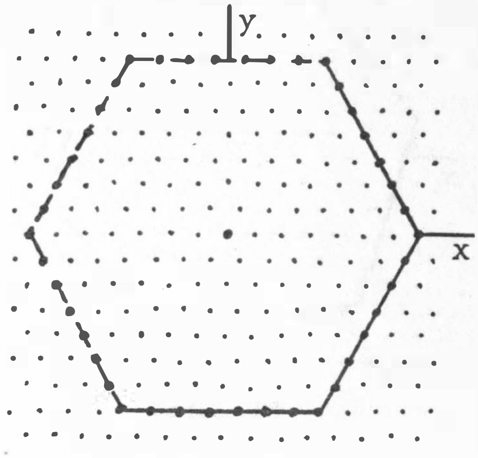

FIG. 12

Lemma 3.3. Let $\gamma = a + b\omega$ where $(a,b) = 1$ and $N(\gamma) \equiv 1 \pmod 3$. Then $(a - 2b, a + b, b - 2a) = 1$.

Proof.--Since $(a,b) = 1$ we know that $(a - 2b, a + b, b - 2a) = 1$ or 3. Assume that $(a - 2b, a + b, b - 2a) = 3$. Then $3|(a - 2b)$

and $3|(a + b)$ so that $3|(a^2 - ab - 2b^2)$. But $3|(a^2 - ab + b^2 - 1)$. Hence, $3|(3b^2 - 1)$ which is impossible and the lemma is proved.

Lemma 3.4. If $\gamma = a + b\omega$ is of the form given in (a) above, then $T_2 = \emptyset$. (See figures 13 and 14).

Proof.--Obviously $(a,b) = 1$ and $N(\gamma) \equiv 1 \pmod 3$ so that $(a - 2b, a + b, b - 2a) = 1$. The result now follows from Theorem 2.1.

C.R.S. (mod $-9 + 4\omega$) where

$(-9 + 4\omega) = (2 + 3\omega)(3 + 5\omega)$

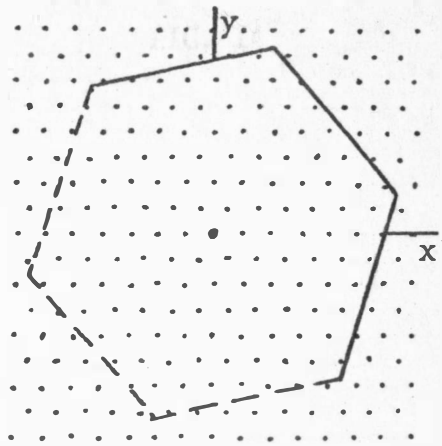

FIG. 13

Combining Lemmas 3.1, 3.2, and 3.4 we have

Theorem 3.2. The set $T_2 = \emptyset$ iff $\gamma = \delta\rho_1^{n_1}\rho_2^{n_2}\ldots\rho_k^{n_k}$ where the ρ_i are all non-real primes and no two are conjugates or associates of each other.

C.R.S. (mod $-8 + 9\omega$) where

$(-8 + 9\omega) = (2 + 3\omega)(5 + 6\omega)$

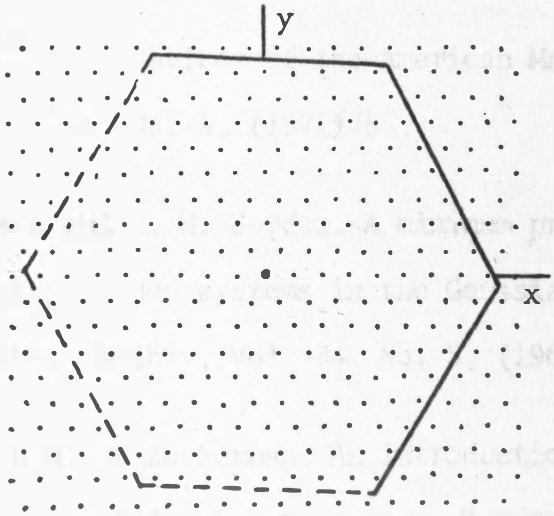

FIG. 14

REFERENCES

[1] G. E. Bergum, Complete residue systems in the quadratic domain $Z(e^{2\pi i/3})$, Notices of the American Mathematical Society, Vol. 18, No. 5, (1971)755.

[2] N. R. Hardman and J. H. Jordan, A minimum problem connected with complete residue systems in the Gaussian integers, American Math. Monthly, Vol. 74, No. 5, (1967)559-561.

[3] I. Niven and H. S. Zuckerman, An introduction to the theory of numbers, John Wiley and Sons Inc., New York, 1962, Chapter 9.