1972

The Distribution of Primitive Roots in Fields of Order $P^2$

Marilyn Sol Gerjets

Follow this and additional works at: https://openprairie.sdstate.edu/etd

Recommended Citation
https://openprairie.sdstate.edu/etd/4690

This Thesis - Open Access is brought to you for free and open access by Open PRAIRIE: Open Public Research Access Institutional Repository and Information Exchange. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Open PRAIRIE: Open Public Research Access Institutional Repository and Information Exchange. For more information, please contact michael.biondo@sdstate.edu.
THE DISTRIBUTION OF PRIMITIVE ROOTS
IN FIELDS OF ORDER $p^2$

By

Marilyn Sol Gerjets

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

1972
The Distribution of Primitive Roots
in Fields of Order $P^2$

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 Dept.

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 Dr. K. L. Yocom for reading the manuscript and making many helpful suggestions, and Gerald W. Danek for the work done on the computer programs used to obtain the necessary data.

MSG
### TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>II. FIELDS OF ORDER $P^2$ WHERE $P$ IS OF THE FORM $4K + 3$</td>
<td>5</td>
</tr>
<tr>
<td>III. FIELDS OF ORDER $P^2$ WHERE $P$ IS AN ODD PRIME</td>
<td>20</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>31</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure                        Page
1. Distribution of generators modulo 3        7
2. Distribution of generators modulo 7        7
3. Distribution of generators modulo 11       7
4. Distribution of generators modulo 19       8
5. Distribution of generators where
   \( p = 5 \) and \( \theta = \sqrt{3} \)    21
6. Distribution of generators where
   \( p = 7 \) and \( \theta = \sqrt{3} \)    21
7. Distribution of generators where
   \( p = 11 \) and \( \theta = \sqrt{2} \)    22
8. Distribution of generators where
   \( p = 13 \) and \( \theta = \sqrt{2} \)    23
LIST OF TABLES

Table | Description | Page
--- | --- | ---
1. | Distribution of powers of $\gamma = 1 + 2i$ modulo 7 | 12
2. | Distribution of powers of $\gamma = 1 + 3i$ modulo 11 | 12
3. | Counterexamples to the converse of Theorem 2.12 | 17
4. | Distribution of powers of $\lambda = 1 + \theta$ modulo 5 where $\theta = \sqrt{3}$ | 25
5. | Distribution of powers of $\lambda = 1 + \theta$ modulo 7 where $\theta = \sqrt{3}$ | 25
6. | Distribution of powers of $\lambda = 1 + 5\theta$ modulo 11 where $\theta = \sqrt{2}$ | 26
7. | Distribution of powers of $\lambda = 1 + 2\theta$ modulo 13 where $\theta = \sqrt{2}$ | 27
I. INTRODUCTION

Throughout this paper, small case Latin letters, with the exception of $i$ which has its usual mathematical meaning, will denote rational integers where we let $\mathbb{Z}$ represent the set of all rational integers. We call $\mu = a + bi$ a Gaussian integer iff $a$ and $b$ are rational integers and we denote the set of all Gaussian integers by $\mathbb{Z}(i)$. The set of Gaussian integers can be represented geometrically by the set of lattice points in a Cartesian coordinate system whose horizontal and vertical grid lines are one unit apart.

Since $\mu = a + bi$ is a complex number, it has a complex conjugate denoted by $\bar{\mu} = a - bi$. The norm of $\mu$, written as $N(\mu)$, is defined as $N(\mu) = \mu\bar{\mu} = a^2 + b^2$. It is a trivial matter to show that the norm is multiplicative so that $N(\alpha\beta) = N(\alpha)N(\beta)$.

We say that $\alpha \neq 0$ divides $\beta$ iff there exists a $\mu$ such that $\beta = \alpha\mu$, we write $\alpha|\beta$. A Gaussian integer $\omega$ is called a unit iff $\omega|\alpha$ for all $\alpha$. Since the norm is multiplicative, it can be shown that $\omega$ is a unit iff $N(\omega) = 1$. Hence, the units of $\mathbb{Z}(i)$ are $\pm 1$ and $\pm i$. For any $\mu$, we call $\omega\mu$ an associate iff $\omega$ is a unit. A Gaussian integer $\rho$ is said to be prime iff whenever $\rho = \alpha\beta$, one of $\alpha$ or $\beta$ is a unit, but not both. We call $\rho$ a real prime iff $\rho$ is a prime in $\mathbb{Z}(i)$ and $\mathbb{Z}$. In contrast, primes in $\mathbb{Z}$ which are not primes in $\mathbb{Z}(i)$ are called rational primes. It is obvious that all of the associates of $\rho$ as well as $\bar{\rho}$ are prime if $\rho$ is prime.
For any Gaussian integer \( \mu \), we say that \( \alpha \) and \( \beta \) are congruent modulo \( \mu \), written \( \alpha \equiv \beta \pmod{\mu} \), iff \( \mu | (\alpha - \beta) \). Since congruence modulo \( \mu \) is an equivalence relation on the set \( \mathbb{Z}(i) \), it partitions \( \mathbb{Z}(i) \) into a collection of pairwise disjoint sets whose union is \( \mathbb{Z}(i) \). Hence, as is the case with the rational integers, we define a complete residue system modulo \( \mu \) as a nonempty collection \( S \) of elements of \( \mathbb{Z}(i) \) such that (1) no two elements of \( S \) are congruent modulo \( \mu \), and (2) every element of \( \mathbb{Z}(i) \) not in \( S \) is congruent to some element of \( S \). A complete residue system modulo \( \mu \) is abbreviated as C.R.S.(mod \( \mu \)).

In [3] and [5], we find several representations of a C.R.S.(mod \( \mu \)). In particular, we find the following in [3].

**Theorem 1.1.** For any \( \mu \), let \( A \) be the set of Gaussian integers inside the square with vertices at \((\pm 1 \pm i)\mu/2\) and let \( B \) be the set of Gaussian integers on the half open line segments \((\pm(-1 + i)\mu/2, (-1 - i)\mu/2] \). Then \( R = A \cup B \) is a C.R.S.(mod \( \mu \)).

In [5], Jordan and Potratz have shown

**Theorem 1.2.** The cardinality of a C.R.S.(mod \( \mu \)) is \( N(\mu) \).

Since we will be interested in complete residue systems modulo \( \mu \) where \( \mu \) is a prime, it is convenient to have the following theorem whose proof can be found in [6, p. 198].
Theorem 1.3. The prime elements $\rho$ of $\mathbb{Z}(i)$ are of three types:

(a) $\rho = \pm 1 \pm i$,

(b) $\rho = a + bi$ is a real prime iff $\rho = a$ is a rational prime congruent to three modulo four, and

(c) $\rho = a + bi$ is a nonreal prime iff $N(\rho)$ is a rational prime congruent to one modulo four.

For a given $\mu$, let us denote the set of elements of Theorem 1.1 by $\hat{\mu}$. It is a well-known fact that $\hat{\mu}$ is a field with respect to the binary operations of addition and multiplication modulo $\mu$ provided $\mu$ is a prime. In particular, if $\mu$ is a real prime, say $p$, then $\hat{\mu}$ is a field with $p^2$ elements.

The following definitions and theorems are well known and can be found in [1].

Definition 1.1. An element $\mu$ of a field is called a primitive root, generator, iff for any $\beta \neq 0$ in the field, there exists an integer $j$ (positive, negative, or zero) such that $\mu^j = \beta$.

Definition 1.2. If $F$ is a field with unity 1, then the order of an element $\alpha$ in $F$ is the smallest positive integer $n$ to which $\alpha$ must be raised to equal 1. If no such $n$ exists, then $\alpha$ is said to be of infinite order. In the former case, we write $O(\alpha) = n$ while in the latter case we write $O(\alpha) = \infty$. 
Theorem 1.4. Every field with a finite number of elements has at least one primitive root.

Theorem 1.5. If $F$ is a field with $n$ elements, then the order of every element in $F$ is a divisor of $n - 1$.

Theorem 1.6. Let $a$ be an element of a field $F$ where $O(a) = t$.

If $a^m = 1$, then $t | m$.

The purpose of this paper is to investigate the distribution of primitive roots in several special fields of order $p^2$. 
II. FIELDS OF ORDER $p^2$ WHERE $P$ IS OF THE FORM $4k + 3$

By Theorem 1.4, a field with $p^2$ elements has at least one generator. Our first aim in this chapter will be to establish a formula for the total number of generators in a field with $p^2$ elements. Throughout the remainder of this chapter, $\gamma$ will be a generator unless stated otherwise.

Theorem 2.1. If in a field with $p^2$ elements, the order of $\gamma^n$ is $(p^2 - 1)/d$ where $d = (p^2 - 1, n)$.

Proof. -- Let $O(\gamma^n) = k$. Since $d = (p^2 - 1, n)$, there exist integers $x$ and $y$ such that $dk = nkx + (p^2 - 1)ky$. Hence, $\gamma^{dk} = 1$. But $O(\gamma) = p^2 - 1$. Therefore, $(p^2 - 1)|kd$ or $[(p^2 - 1)/d]|k$.

Since $O(\gamma^n) = k$ and $(\gamma^n)^{(p^2 - 1)/d} = 1$, we have $k|[(p^2 - 1)/d]$. Hence, $(p^2 - 1)/d = k$.

An immediate consequence of Theorem 2.1 is

Corollary 2.1. In a field with $p^2$ elements, $\gamma^n$ is a primitive root iff $(n, p^2 - 1) = 1$. 

Using Corollary 2.1, we see that it is possible to find the total number of generators for a finite field if we can find a way of counting the number of natural numbers less than or equal to and relatively prime to \( p^2 - 1 \). Since the Euler \( \phi \)-function counts the natural numbers less than or equal to and relatively prime to a given integer, we have

**Theorem 2.2.** The number of primitive roots for the field with \( p^2 \) elements is \( \phi(p^2 - 1) \) where \( \phi \) is the Euler \( \phi \)-function.

Throughout the remainder of this chapter, we will assume \( p \) is a real prime of the form \( 4k + 3 \) and will discuss the distribution of primitive roots in the field \( \mathbb{F}_p \). Examining Figures 1 through 4 on pages seven and eight, we make the following conjectures.

1. No non-zero element on the x or y axis is a primitive root.
2. The primitive roots are symmetric with respect to the x and y axes and the origin.
3. For \( p > 3 \), no primitive root is on the diagonal.
4. The primitive roots are symmetric with respect to the lines \( y = \pm x \).

Examining Tables 1 and 2 which give the exponent to which \( \gamma \) is raised in order to obtain \( a + bi \), we also make the following conjectures.

5. A power of \( \gamma \) is on the x axis iff the exponent is a multiple of \( p + 1 \).
Distribution of generators modulo 3

-1 0 1
1 x x 1
0 0
-1 x x -1
-1 0 1

Figure 1

Distribution of generators modulo 7

-3 -2 -1 0 1 2 3
3 x x x 3
2 x x x 2
1 x x x 1
0 0 0
-1 x x x -1
-2 x x x -2
-3 x x x -3
-3 -2 -1 0 1 2 3

Figure 2

Distribution of generators modulo 11

-5 -4 -3 -2 -1 0 1 2 3 4 5
5 x x x x x 5
4 x x x x 4
3 x x x 3
2 x x x x 2
1 x x x 1
0 0 0
-1 x x x -1
-2 x x x x -2
-3 x x x -3
-4 x x x x -4
-5 x x x x -5
-5 -4 -3 -2 -1 0 1 2 3 4 5

Figure 3
Distribution of generators modulo 19

| -9 | -8 | -7 | -6 | -5 | -4 | -3 | -2 | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|---|
| x  | x  | x  | x  | x  | x  | x  | x  | x  | x | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 9  | 8  | 7  | 6  | 5  | 4  | 3  | 2  | 1  | 0 | -1| -2| -3| -4| -5| -6| -7| -8| -9| -9|

Figure 4
6. A power of \( \gamma \) is on the \( y \) axis iff the exponent is an odd multiple of \((p + 1)/2\).

7. A power of \( \gamma \) is on the diagonal iff the exponent is an odd multiple of \((p + 1)/4\).

Throughout the remainder of this chapter, we shall establish the validity of these conjectures. Furthermore, we shall exhibit several results which are only immediate after a more careful examination of Figures 1 through 4 and Tables 1 and 2.

In Hardman and Jordan [4], we find

**Theorem 2.3.** If \( a \) is on the \( x \) or \( y \) axis, then

\[ a^{(p^2 - 1)/2} \equiv 1 \pmod{p}. \]

Conjecture one is an immediate result of Theorem 2.3 since the order of an element on the \( x \) or \( y \) axis is less than or equal to \((p^2 - 1)/2\). Hence,

**Theorem 2.4.** If \( a = s \) or \( a = si \), then \( O(a) < p^2 - 1 \).

Conjecture two is equivalent to the following.

**Theorem 2.5.** If \( \gamma \) is a primitive root, then \( \gamma, -\gamma \), and \(-\gamma\) are primitive roots.

**Proof.** We shall first show that \( O(-\gamma) = p^2 - 1 \). Let \( O(-\gamma) = h \). Then \( h | (p^2 - 1) \) and \((-\gamma)^h \equiv 1 \pmod{p} \). Hence, \( \gamma^{2h} \equiv 1 \pmod{p} \) so that
(p^2 - 1)|2h or 2h = (p^2 - 1)d for some d. Since p = 4k + 3 for some k, we have 2h = 8(k + 1)(2k + 1)d or h = 4(k + 1)(2k + 1)d. Therefore, h is even and (-γ)^h ≡ γ^h ≡ 1(\text{mod } p). Hence, (p^2 - 1)|h and h = p^2 - 1.

Next, let 0(γ) = h. Then h|(p^2 - 1) and γ^h ≡ 1(\text{mod } p). Therefore, γ^h ≡ 1(\text{mod } p) or γ^h ≡ 1(\text{mod } p). Hence, (p^2 - 1)|h and h = p^2 - 1.

By using the first part of the proof of this theorem, we see that 0(-γ) = p^2 - 1 and the theorem is proved.

Since symmetry with respect to the axes and origin has been established, we need only consider the distribution of primitive roots in the first quadrant.

In order to establish conjecture three, we have

**Theorem 2.6.** If p > 7, then 0(a ± ai) < p^2 - 1.

**Proof.** By Fermat's little theorem, we have

\[(a + ai)^4(p - 1) = (-4a^4)^p - 1 \equiv 1(\text{mod } p).\]

Therefore, 0(a + ai) < 4(p - 1) < (p + 1)(p - 1) = p^2 - 1.

Conjecture four is equivalent to

**Theorem 2.7.** Let γ = a + bi. Then 0(b + ai) = p^2 - 1.
Proof. -- If $O(b + ai) = h$, then $h | (p^2 - 1)$. Now

$$(a - bi)^{4h} = (-i)^{4h}(b + ai)^{4h} \equiv 1 \pmod{p}.$$  

But $O(a - bi) = O(a + bi) = p^2 - 1$. Therefore, $(p^2 - 1)|4h$ or $4h = (p^2 - 1)q$ for some $q$. However, $p$ is of the form $4k + 3$ for some $k$ so that $4h = 8(k + 1)(2k + 1)q$ and $h$ is even. Suppose $h = 4t + 2$, then

$$(a - bi)^{2h} = (a - bi)^{4(2t + 1)} = (-i)^{4(2t + 1)}(b + ai)^{2h} \equiv 1 \pmod{p}.$$  

Hence, $(p^2 - 1)|2h$ or $(p^2 - 1)q = 2h = 4(2t + 1)$ so that $8(2k + 1)(k + 1)q = 4(2t + 1)$. Since $2t + 1$ is odd, we have a contradiction. Therefore, $h = 4t$ and

$$(a - bi)^h = (a - bi)^{4t} = (-i)^{4t}(b + ai)^{4t} \equiv (b + ai)^h \equiv 1 \pmod{p}.$$  

Hence, $(p^2 - 1)|h$ and $h = p^2 - 1$.

An immediate consequence of Theorem 2.5 and 2.7 is

**Corollary 2.2.** A generator times a unit is a generator.

Before proving conjectures five through seven, we state a result which can be found in Hardman and Jordan [4].

**Theorem 2.8.** If $\gamma$ is a primitive root modulo the Gaussian prime $p$, then $\gamma^{p^2 + 1}$ is a primitive root modulo the rational prime $p$. 
Table 1

<table>
<thead>
<tr>
<th></th>
<th>-3</th>
<th>-2</th>
<th>-1</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>14</td>
<td>9</td>
<td>35</td>
<td>28</td>
<td>29</td>
<td>39</td>
<td>26</td>
</tr>
<tr>
<td>2</td>
<td>27</td>
<td>6</td>
<td>31</td>
<td>20</td>
<td>1</td>
<td>18</td>
<td>21</td>
</tr>
<tr>
<td>1</td>
<td>17</td>
<td>37</td>
<td>22</td>
<td>36</td>
<td>34</td>
<td>43</td>
<td>47</td>
</tr>
<tr>
<td>0</td>
<td>16</td>
<td>8</td>
<td>24</td>
<td>48</td>
<td>32</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>-1</td>
<td>23</td>
<td>19</td>
<td>10</td>
<td>12</td>
<td>46</td>
<td>13</td>
<td>41</td>
</tr>
<tr>
<td>-2</td>
<td>45</td>
<td>42</td>
<td>25</td>
<td>44</td>
<td>7</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>-3</td>
<td>2</td>
<td>15</td>
<td>5</td>
<td>11</td>
<td>33</td>
<td>38</td>
<td>-3</td>
</tr>
<tr>
<td>-3</td>
<td>-2</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Distribution of powers of
\[ \gamma = 1 + 2i \mod 7 \]

Table 2

<table>
<thead>
<tr>
<th></th>
<th>-5</th>
<th>-4</th>
<th>-3</th>
<th>-2</th>
<th>-1</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>51</td>
<td>47</td>
<td>70</td>
<td>113</td>
<td>68</td>
<td>102</td>
<td>88</td>
<td>103</td>
<td>110</td>
<td>97</td>
<td>21</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>75</td>
<td>92</td>
<td>14</td>
<td>71</td>
<td>6</td>
<td>1</td>
<td>94</td>
<td>112</td>
<td>45</td>
<td>17</td>
</tr>
<tr>
<td>3</td>
<td>20</td>
<td>22</td>
<td>3</td>
<td>49</td>
<td>55</td>
<td>54</td>
<td>6</td>
<td>1</td>
<td>94</td>
<td>112</td>
<td>45</td>
</tr>
<tr>
<td>2</td>
<td>13</td>
<td>4</td>
<td>29</td>
<td>87</td>
<td>26</td>
<td>18</td>
<td>106</td>
<td>57</td>
<td>19</td>
<td>104</td>
<td>83</td>
</tr>
<tr>
<td>1</td>
<td>118</td>
<td>31</td>
<td>95</td>
<td>16</td>
<td>99</td>
<td>30</td>
<td>69</td>
<td>116</td>
<td>25</td>
<td>41</td>
<td>38</td>
</tr>
<tr>
<td>0</td>
<td>12</td>
<td>36</td>
<td>84</td>
<td>48</td>
<td>6</td>
<td>1</td>
<td>94</td>
<td>112</td>
<td>45</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>-1</td>
<td>98</td>
<td>101</td>
<td>85</td>
<td>56</td>
<td>9</td>
<td>90</td>
<td>39</td>
<td>76</td>
<td>35</td>
<td>91</td>
<td>-1</td>
</tr>
<tr>
<td>-2</td>
<td>23</td>
<td>44</td>
<td>79</td>
<td>117</td>
<td>46</td>
<td>78</td>
<td>86</td>
<td>27</td>
<td>89</td>
<td>64</td>
<td>73</td>
</tr>
<tr>
<td>-3</td>
<td>100</td>
<td>2</td>
<td>33</td>
<td>59</td>
<td>5</td>
<td>114</td>
<td>115</td>
<td>109</td>
<td>63</td>
<td>82</td>
<td>80</td>
</tr>
<tr>
<td>-4</td>
<td>77</td>
<td>105</td>
<td>52</td>
<td>34</td>
<td>61</td>
<td>66</td>
<td>11</td>
<td>74</td>
<td>32</td>
<td>15</td>
<td>67</td>
</tr>
<tr>
<td>-5</td>
<td>81</td>
<td>37</td>
<td>50</td>
<td>43</td>
<td>28</td>
<td>42</td>
<td>8</td>
<td>53</td>
<td>10</td>
<td>107</td>
<td>111</td>
</tr>
<tr>
<td>-5</td>
<td>-4</td>
<td>-3</td>
<td>-2</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

Distribution of powers of
\[ \gamma = 1 + 3i \mod 11 \]
Throughout the remainder of this chapter, \( g \) will represent a primitive root modulo the rational prime \( p \).

To prove conjecture five, we have

**Theorem 2.9.** If \( y^d \equiv c \pmod{p} \), then \( d = n(p + 1) \) for some \( n \) and conversely.

**Proof.**—First let \( y^d \equiv c \pmod{p} \). Then \( (y^d)^p - 1 \equiv 1 \pmod{p} \).

Thus, \((p^2 - 1)|(p - 1)d\) or \((p + 1)|d\) so that \( d = n(p + 1) \) for some \( n \).

Conversely, suppose \( d = n(p + 1) \). Since \( y^{(p + 1)} \equiv g \pmod{p} \), \( y^d = (y^{p + 1})^n \equiv g^n \equiv c \pmod{p} \) and the theorem is proved.

Conjecture six can be written as

**Theorem 2.10.** A necessary and sufficient condition for \( y^d \equiv \pm ri \pmod{p} \) is that \( d = [n(p + 1)]/2 \) for some odd integer \( n \).

**Proof.**—Set \( y^d \equiv ri \pmod{p} \). Then \( y^{2d} \equiv (ri)^2 \equiv -r^2 \pmod{p} \).

By Theorem 2.9, \( 2d = n(p + 1) \) or \( d = [n(p + 1)]/2 \). If \( n \) is of the form \( 2k \), then \( d = k(p + 1) \) so that \( y^d \equiv r \pmod{p} \). This contradicts our hypothesis. Hence, \( n \) must be odd.

Conversely, let \( d = [n(p + 1)]/2 \) where \( n \) is odd. Then

\[ y^{2d} \equiv (s + ri)^2 \equiv m \pmod{p} \].
Hence,

\[\gamma^{2d} - (s + ri)^2 \equiv [(\gamma^d - (s + ri))(\gamma^d + (s + ri))] \equiv 0 \pmod{p}\]

and \(m \equiv (s^2 - r^2) + 2sri \pmod{p}\). Therefore, \(2sr \equiv 0 \pmod{p}\) so that \(s = 0\) or \(r = 0\). Assume \(r = 0\). Then \([\gamma^d - s](\gamma^d + s) \equiv 0 \pmod{p}\)
or \(\gamma^d \equiv \pm s \pmod{p}\). Hence, \(d = k(p + 1)\) for some \(k\) or

\(k(p + 1) = [n(p + 1)]/2\) which implies that \(n = 2k\). This contradicts our hypothesis so that \(r \neq 0\). Therefore, \(s = 0\), and we have

\[\gamma^d \equiv \pm ri \pmod{p}\].

Conjecture seven is equivalent to

**Theorem 2.11.** A necessary and sufficient condition for

\(\gamma^d \equiv r \pm ri \pmod{p}\) is that \(d = [n(p + 1)]/4\) for some odd integer \(n\).

**Proof.** Let \(\gamma^d \equiv r + ri \pmod{p}\). Now

\[\gamma^{4d} = [r(1 + i)]^4 \equiv -4r^4 \pmod{p}\].

Therefore, by Theorem 2.9, \(4d = n(p + 1)\) or \(d = [n(p + 1)]/4\).

If \(n = 2k\) where \(k\) is odd, then \(\gamma^d \equiv ri \pmod{p}\) by Theorem 2.10.

If \(n = 4k\), then \(\gamma^d \equiv r \pmod{p}\) by Theorem 2.9. In either case, we have a contradiction to our hypothesis. Hence, \(n\) must be odd.

By symmetry, the result is true if \(\gamma^d \equiv r - ri \pmod{p}\).
Now let \( d = \lfloor n(p + 1) \rfloor / 4 \) where \( n \) is odd. Then

\[
\gamma^{4d} \equiv \gamma^{(p + 1)n} \equiv (r + si)^4 \equiv c \pmod{p}
\]

or

\[
(r + si)^4 = r^4 - 6r^2s^2 + s^4 + (4r^3s - 4rs^3)i \equiv c \pmod{p}.
\]

Therefore, \( 4r^3s - 4rs^3 \equiv 0 \pmod{p} \) or \( r = \pm s \) and \( \gamma^d \equiv r \pm ri \pmod{p} \).

This completes the proofs of the conjectures which we arrived at by examining Figures 1 through 4 together with Tables 1 and 2. However, there are several other interesting observations that one makes after a more careful examination of collected data.

For example, we can show

**Lemma 2.1.** For any \( \beta \), \( \beta^p \equiv \overline{\beta} \pmod{p} \).

**Proof.** Let \( \beta = (u + vi) \). Then

\[
\beta^p = (u + vi)^p \equiv u^p + (vi)^p \pmod{p}.
\]

The result is immediate by use of Fermat's little theorem and the fact that \( p \) is a prime of the form \( 4k + 3 \).

Because of Theorem 2.8 and Lemma 2.1, we have

**Theorem 2.12.** If \( \gamma \) is a generator modulo the Gaussian prime \( p \), then \( \gamma \gamma \) is a generator modulo the rational prime \( p \).

**Proof.** Since \( \gamma^p \equiv \overline{\gamma} \pmod{p} \), \( \gamma^{(p + 1)} \equiv \gamma \gamma \equiv g \pmod{p} \).
The converse of Theorem 2.12 presents us with some serious difficulties and several unanswered questions. Investigating the values of $\beta$ for which $\beta \overline{\beta} \equiv g \pmod{p}$, we see that the converse appears to be true if $p$ is such that $p = 8k + 7$ and $4k + 7$ is also a prime. That is, for $p = 7$ and $p = 31$, we observe that whenever $\beta \overline{\beta} \equiv g \pmod{p}$, then $\beta$ is a generator modulo the Gaussian prime $p$. At this time we are unable to establish the validity of this statement for all primes of the proper form.

When $p = 8k + 7$ and $4k + 7$ is not a prime, we find, for the examples investigated, that the converse of Theorem 2.12 is false. For example, let $k = 2$ so that $p = 23$ and $4k + 7 = 15$. If $\beta = 1 + 4i$, then $\beta \overline{\beta} \equiv 17 \pmod{23}$. It can be shown that 17 is a generator modulo the rational prime 23 while $1 + 4i$ is not a primitive root modulo the Gaussian prime 23 since $O(1 + 4i) = 176$.

The author conjectures that whenever the prime $p$ is of the form stated above there exist a counterexample to Theorem 2.12. Even though a proof of this fact has not been established, we do have

**Theorem 2.13.** If $\beta \overline{\beta} \equiv g \pmod{p}$ where $p$ is of the form $8k + 7$ and $O(\beta) < p^2 - 1$, then $\beta$ is not on the diagonal.

**Proof.** Assume $\beta = r(1 + i)$. From Hardman and Jordan [4], we have $[r(1 + i)](p^2 - 1)/2 \equiv (-1)(p + 1)/4 \pmod{p}$. But $p = 8k + 7$. Therefore, $\beta^{(p^2 - 1)/2} \equiv 1 \pmod{p}$. Hence,
\[ \beta \left( \frac{p^2 - 1}{2} \right) \equiv \left[ \beta \left( \frac{p + 1}{2} \right) \right] \left( \frac{p - 1}{2} \right) \equiv (\beta \overline{\beta}) \left( \frac{p - 1}{2} \right) \equiv 1 \pmod{p} \]

which contradicts \( \beta \overline{\beta} \) being a generator. Therefore, \( \beta \) is not on the diagonal. By symmetry, \( \beta \neq r(1 - i) \) and the theorem is proved.

Let us now examine the converse of Theorem 2.12 where \( p \) is a prime of the form \( 8k + 3 \). For \( p = 11, 19, 43, 59, \) and \( 67 \), it was possible to find a \( \beta \) such that \( \beta \overline{\beta} \) is a primitive root modulo \( p \) while \( \beta \) is not a primitive root modulo the Gaussian prime \( p \).

(See Table 3.)

Table 3

<table>
<thead>
<tr>
<th>( p )</th>
<th>( \beta )</th>
<th>( \beta \overline{\beta} \equiv g \pmod{p} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>( 1 + i )</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>( 1 + i )</td>
<td>2</td>
</tr>
<tr>
<td>43</td>
<td>( 3 + 3i )</td>
<td>18</td>
</tr>
<tr>
<td>59</td>
<td>( 1 + i )</td>
<td>2</td>
</tr>
<tr>
<td>67</td>
<td>( 1 + i )</td>
<td>2</td>
</tr>
</tbody>
</table>

Counterexamples to the converse of Theorem 2.12

The author feels that there exist a counterexample to the converse of Theorem 2.12 for every prime \( p \) of the form \( 8k + 3 \), where \( k \geq 1 \); however, the proof of this statement defies him at the present time. After a more careful examination of the distribution of those \( \beta \) for which \( \beta \overline{\beta} \) is a generator modulo the rational prime \( p \) while \( \beta \) is not a generator modulo the Gaussian prime \( p \), we have
Theorem 2.14. Let $\beta \equiv g \pmod{p}$ where $\beta$ is not a primitive root and $p$ is of the form $8k + 3$. If $2k + 1$ is a prime, then $\beta$ is on the diagonal.

Proof. Let $(r + si) = \beta \equiv \gamma^n \pmod{p}$ and $d = (n, p^2 - 1)$.

Since $\beta \equiv g \pmod{p}$, $(\gamma^n)(p + 1) \equiv g \pmod{p}$. But $\gamma(p + 1)$ is a generator modulo the rational prime $p$. Therefore, $(n, p - 1) = 1$ which implies that $n$ is odd. Hence,

$$d = (n, p^2 - 1) = (n, p + 1) = (n, 4(2k + 1)) = (n, 2k + 1).$$

However, $2k + 1$ is a prime. Therefore, $d = 2k + 1$.

Now $(\gamma^n)(p + 1)/d = [\gamma(p + 1)]^{n/d} \equiv c \pmod{p}$ for some $c$. Hence,

$$\beta^4 \equiv c \pmod{p}$$

so that $r = \pm s$ by the argument of Theorem 2.11 and the theorem is proved.

The results of Theorem 2.14 can be extended even if $2k + 1$ is not prime. That is, by an argument similar to that of Theorem 2.14 we can show

Theorem 2.15. Let $\beta \equiv g \pmod{p}$ where $O(\beta) < p^2 - 1$.

Let $\beta \equiv \gamma^n \pmod{p}$ where $d = (n, p^2 - 1)$, and $p$ is of the form $8k + 3$. If $(2k + 1)|d$, then $\beta$ is on the diagonal.

Note that Theorem 2.15 tells us when counterexamples of a very special type must fall on the diagonal. However, it does not tell us
that all counterexamples are on the diagonal. In fact, if \( p = 59 \), we find that \( 1 + 8i \) is a counterexample which is not on the diagonal.

It also appears that there are some relationships between the number of generators modulo the rational prime \( p \) and the number of counterexamples to the converse of Theorem 2.12. The author did not feel that it was significant at this time to further study these relationships.

In conclusion, we have

**Theorem 2.16.** Let \( \Theta(u) = p - 1 \). Then there exist an \( n \) such that \( (\gamma \gamma)^n \equiv u \pmod{p} \).

**Proof.** Let \( \gamma^t \equiv u \pmod{p} \). By Theorem 2.9, \( t = n(p + 1) \).

Since \( \gamma^{(p + 1)} \equiv \gamma \gamma \pmod{p} \), we have

\[
\gamma^t \equiv (\gamma^{(p + 1)})^n \equiv (\gamma \gamma)^n \equiv u \pmod{p}.
\]
III. FIELDS OF ORDER $P^2$ WHERE $P$ IS AN ODD PRIME

In this chapter, we dispose of the restriction placed on $p$; that is, we no longer require that $p$ be a prime of the form $4k + 3$. Hence, we will discuss the distribution of primitive roots in fields of order $p^2$ where $p$ is an odd rational prime. For this reason, we recall that $GF(p) = \{x \mid -p/2 < x < p/2, x \in \mathbb{Z}\}$ is a field with $p$ elements under the usual operations of addition and multiplication modulo $p$. Furthermore, we use the well known fact that

$$GF(p^2) = \{x + y\theta \mid \theta^2 = g, x, y \in GF(p)\}$$

where $g$ is a primitive root modulo $p$ in a field with $p$ elements [1, p. 447]. Finally, we agree to adopt the notation that

$\lambda = a + b\theta$ is always a primitive root of $GF(p^2)$.

For convenience, we state the following.

**Definition 3.1.** If $\beta = c + d\theta$, then the conjugate of $\beta$, denoted by $\bar{\beta}$, is written as $\bar{\beta} = c - d\theta$.

Furthermore, we accept the following results which can be found in Giudici [2].

**Theorem 3.1.** If $\lambda$ is a primitive root of $GF(p^2)$, then

$\lambda^{p + 1}$ is a primitive root modulo $p$. 

Distribution of generators where \( p = 5 \) and \( \theta = \sqrt{3} \):

\[
\begin{array}{ccccccc}
-2 & -1 & 0 & 1 & 2 & 3 \\
20 & x & x & x & 20 & 20 \\
0 & x & x & x & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
-20 & x & x & x & -20 & -20 \\
-30 & x & x & x & x & x & 30 \\
-3 & -2 & -1 & 0 & 1 & 2 & 3 \\
\end{array}
\]

Figure 5

Distribution of generators where \( p = 7 \) and \( \theta = \sqrt{3} \):

\[
\begin{array}{ccccccc}
-3 & -2 & -1 & 0 & 1 & 2 & 3 \\
30 & x & x & x & x & x & 30 \\
20 & x & x & 20 & 20 \\
0 & x & x & x & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
-30 & x & x & x & x & x & -30 \\
-3 & -2 & -1 & 0 & 1 & 2 & 3 \\
\end{array}
\]

Figure 6
Distribution of generators

where $p = 11$ and $\theta = \sqrt{2}$

\[-5 -4 -3 -2 -1 0 1 2 3 4 5\]

\[
\begin{array}{ccccccc}
5\theta & x & x & x & x & x & 5\theta \\
4\theta & x & x & x & x & x & 4\theta \\
3\theta & x & x & x & x & x & 3\theta \\
2\theta & x & x & x & x & x & 2\theta \\
\theta & x & x & x & x & x & 0 \\
0 & x & x & x & x & 0 & 0 \\
-\theta & x & x & x & x & x & -\theta \\
-2\theta & x & x & x & x & x & -2\theta \\
-3\theta & x & x & x & x & x & -3\theta \\
-4\theta & x & x & x & x & x & -4\theta \\
-5\theta & x & x & x & x & x & -5\theta \\
\end{array}
\]

Figure 7
Distribution of generators

where $p = 13$ and $\theta = \sqrt{2}$

\begin{tabular}{cccccccccc}
-6 & -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
60 & x & x & x & x & x & 60 \\
50 & x & x & x & x & x & 50 \\
40 & x & x & x & x & x & 40 \\
30 & x & x & x & x & x & 30 \\
20 & x & x & x & x & x & x & 20 \\
10 & x & x & x & x & x & x & 10 \\
0 & x & x & x & x & x & x & 0 \\
0 & x & x & x & x & x & x & 0 \\
-10 & x & x & x & x & x & x & -10 \\
-20 & x & x & x & x & x & x & -20 \\
-30 & x & x & x & x & x & x & -30 \\
-40 & x & x & x & x & x & x & -40 \\
-50 & x & x & x & x & x & x & -50 \\
-60 & x & x & x & x & x & x & -60 \\
-6 & -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\end{tabular}

Figure 8
**Theorem 3.2.** If \( p \equiv 3 \pmod{4} \), then \((r\theta)^{(p^2 - 1)/2} \equiv 1 \pmod{p}\).

**Theorem 3.3.** If \( p \) is an odd prime, then \( r^{(p^2 - 1)/2} \equiv 1 \pmod{p} \).

A careful examination of Figures 5 through 8 together with Figures 1 through 4 tells us that we no longer have one of the nice symmetry properties given in Chapter II. That is, it is easy to see that we no longer have symmetry with respect to the lines \( y = \pm x \). In fact, symmetry does not even exist with respect to the lines \( y = \pm \theta x \). However, it does appear that we still have symmetry with respect to the axes and origin. Since the proof of this fact is similar to that of Theorem 2.5, we merely state the theorem.

**Theorem 3.4.** If \( \lambda \) is a primitive root, then \( \overline{\lambda}, -\overline{\lambda}, \) and \(-\lambda\) are primitive roots.

Continuing the examination of Figures 5 through 8, it appears that conjecture one of Chapter II is still valid. Stated as a theorem, we have

**Theorem 3.5.** If \( \alpha = r \) or \( \alpha = r\theta \), then \( O(\alpha) < p^2 - 1 \).

**Proof.** By use of Theorems 3.2 and 3.3, we need only show that \( O(r\theta) < p^2 - 1 \) for \( p \equiv 1 \pmod{4} \).

Since

\[
(r\theta)^{8k} = (r^{4k})^2(\theta^2)^{4k} \equiv g^{4k} \equiv g^{p - 1} \equiv 1 \pmod{p}
\]
Table 4

<table>
<thead>
<tr>
<th></th>
<th>-2</th>
<th>-1</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>11</td>
<td>2</td>
<td>21</td>
<td>22</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>4</td>
<td>17</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>24</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>-0</td>
<td>20</td>
<td>13</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>-0</td>
<td>20</td>
<td>7</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>-2</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Distribution of powers of \( \lambda = 1 + \theta \) modulo 5

where \( \theta = \sqrt{3} \)

<table>
<thead>
<tr>
<th></th>
<th>-3</th>
<th>-2</th>
<th>-1</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>23</td>
<td>19</td>
<td>10</td>
<td>12</td>
<td>46</td>
<td>13</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>27</td>
<td>6</td>
<td>31</td>
<td>20</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>16</td>
<td>8</td>
<td>24</td>
<td>48</td>
<td>32</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>-0</td>
<td>45</td>
<td>42</td>
<td>25</td>
<td>44</td>
<td>7</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>-0</td>
<td>20</td>
<td>14</td>
<td>9</td>
<td>35</td>
<td>28</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>-3</td>
<td>-2</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

Distribution of powers of \( \lambda = 1 + \theta \) modulo 7

where \( \theta = \sqrt{3} \)
Table 6

| 50 | 7  | 75 | 92 | 14 | 71 | 6  | 1  | 94 | 112 | 45 | 17 | 50 |
| 40 | 118| 31 | 95 | 16 | 99 | 30 | 69 | 116| 25 | 41 | 38 | 40 |
| 30 | 23 | 44 | 79 | 117| 46 | 78 | 86 | 27 | 89 | 64 | 73 | 30 |
| 20 | 81 | 37 | 50 | 43 | 28 | 42 | 8  | 53 | 10 | 107| 111| 20 |
| 0  | 20 | 22 | 3  | 49 | 55 | 54 | 65 | 119| 93 | 62 | 40 | 0  |
| 0  | 12 | 36 | 84 | 48 | 60 | 120| 108| 24 | 96 | 72 | 0  | 0  |
| -10| 100| 2  | 33 | 59 | 5  | 114| 115| 109| 63 | 82 | 80 | -10|
| -20| 51 | 47 | 70 | 113| 68 | 102| 88 | 103| 110| 97 | 21 | -20|
| -30| 13 | 4  | 29 | 87 | 26 | 18 | 106| 57 | 19 | 104| 83 | -30|
| -40| 98 | 101| 85 | 56 | 9  | 90 | 39 | 76 | 35 | 91 | 58 | -40|
| -50| 77 | 105| 52 | 34 | 61 | 66 | 11 | 74 | 32 | 15 | 67 | -50|

Distribution of powers of

\[ \lambda = 1 + 50 \mod 11 \]

where \( \theta = \sqrt{2} \)
Table 7

<table>
<thead>
<tr>
<th></th>
<th>60</th>
<th>50</th>
<th>40</th>
<th>30</th>
<th>20</th>
<th>10</th>
<th>0</th>
<th>10</th>
<th>20</th>
<th>30</th>
<th>40</th>
<th>50</th>
<th>60</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>44</td>
<td>129</td>
<td>52</td>
<td>41</td>
<td>134</td>
<td>103</td>
<td>133</td>
<td>79</td>
<td>146</td>
<td>113</td>
<td>88</td>
<td>81</td>
<td>152</td>
</tr>
<tr>
<td>50</td>
<td>78</td>
<td>156</td>
<td>57</td>
<td>47</td>
<td>73</td>
<td>32</td>
<td>77</td>
<td>164</td>
<td>25</td>
<td>23</td>
<td>153</td>
<td>96</td>
<td>90</td>
</tr>
<tr>
<td>40</td>
<td>46</td>
<td>61</td>
<td>2</td>
<td>104</td>
<td>167</td>
<td>39</td>
<td>91</td>
<td>87</td>
<td>71</td>
<td>92</td>
<td>110</td>
<td>37</td>
<td>10</td>
</tr>
<tr>
<td>30</td>
<td>9</td>
<td>43</td>
<td>11</td>
<td>142</td>
<td>150</td>
<td>64</td>
<td>63</td>
<td>76</td>
<td>18</td>
<td>82</td>
<td>59</td>
<td>139</td>
<td>33</td>
</tr>
<tr>
<td>20</td>
<td>17</td>
<td>22</td>
<td>135</td>
<td>144</td>
<td>100</td>
<td>97</td>
<td>21</td>
<td>1</td>
<td>40</td>
<td>108</td>
<td>159</td>
<td>34</td>
<td>137</td>
</tr>
<tr>
<td>10</td>
<td>99</td>
<td>38</td>
<td>132</td>
<td>115</td>
<td>65</td>
<td>30</td>
<td>119</td>
<td>138</td>
<td>89</td>
<td>67</td>
<td>120</td>
<td>74</td>
<td>27</td>
</tr>
<tr>
<td>0</td>
<td>98</td>
<td>42</td>
<td>56</td>
<td>28</td>
<td>154</td>
<td>84</td>
<td>168</td>
<td>70</td>
<td>112</td>
<td>140</td>
<td>126</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>-10</td>
<td>111</td>
<td>158</td>
<td>36</td>
<td>151</td>
<td>5</td>
<td>54</td>
<td>35</td>
<td>114</td>
<td>149</td>
<td>31</td>
<td>48</td>
<td>122</td>
<td>15</td>
</tr>
<tr>
<td>-20</td>
<td>23</td>
<td>138</td>
<td>75</td>
<td>24</td>
<td>124</td>
<td>85</td>
<td>105</td>
<td>13</td>
<td>16</td>
<td>60</td>
<td>51</td>
<td>106</td>
<td>101</td>
</tr>
<tr>
<td>-30</td>
<td>117</td>
<td>55</td>
<td>143</td>
<td>166</td>
<td>102</td>
<td>160</td>
<td>147</td>
<td>148</td>
<td>66</td>
<td>58</td>
<td>95</td>
<td>127</td>
<td>93</td>
</tr>
<tr>
<td>-40</td>
<td>94</td>
<td>121</td>
<td>26</td>
<td>8</td>
<td>155</td>
<td>3</td>
<td>7</td>
<td>123</td>
<td>83</td>
<td>20</td>
<td>86</td>
<td>145</td>
<td>130</td>
</tr>
<tr>
<td>-50</td>
<td>6</td>
<td>12</td>
<td>69</td>
<td>107</td>
<td>109</td>
<td>80</td>
<td>161</td>
<td>116</td>
<td>157</td>
<td>131</td>
<td>141</td>
<td>72</td>
<td>162</td>
</tr>
<tr>
<td>-60</td>
<td>68</td>
<td>165</td>
<td>4</td>
<td>29</td>
<td>62</td>
<td>163</td>
<td>49</td>
<td>19</td>
<td>50</td>
<td>125</td>
<td>136</td>
<td>45</td>
<td>128</td>
</tr>
</tbody>
</table>

Distribution of powers of

\[ \lambda = 1 + 2\theta \text{ modulo } 13 \]

where \( \theta = \sqrt{2} \)
if \( p = 4k + 1 \), we have \( O(r) \leq 8k < p^2 - 1 \) and the theorem is proved.

Using the lines \( y = \pm ox \) as the diagonals, we see, after examining Figures 5 through 8, that conjecture four of Chapter II is not valid. Setting \( p = 5 \) and \( o^2 = 2 \), we find that there are no primitive roots on the diagonals \( y = \pm \sqrt{2}x \). It appears therefore that the property of a primitive root being on a diagonal is dependent upon the primitive root, \( g \), of \( GF(p) \).

Examining Tables 4 through 7, it looks like conjectures five and six of Chapter II remain valid. Since the proofs are similar to those of Theorems 2.9 and 2.10, we shall state the theorems without proofs.

**Theorem 3.6.** A necessary and sufficient condition for 
\[ \lambda^d \equiv c \pmod{p} \] is that \( d = n(p + 1) \).

**Theorem 3.7.** A necessary and sufficient condition for 
\[ \lambda^d \equiv \pm r \pmod{p} \] is that \( d = [n(p + 1)]/2 \) for some odd integer \( n \).

Examining the exponents along the lines \( y = \pm ox \) in Tables 4 through 7, we see that conjecture six of Chapter II is false. However, we do have
Theorem 3.8. Let $\lambda^m$ fall on $y = \theta x$ where $m$ is the smallest such exponent, then $\lambda^d = r + r\theta$ iff $d = m + t(p + 1)$ for some $t$.

Proof.---Let $\lambda^m = u + u\theta$. If $d = m + t(p + 1)$ for some $t$, then

$$\lambda^d \equiv (u + u\theta)c \equiv (uc + uc\theta)(\text{mod } p)$$

by Theorem 3.6. Letting $uc = r$,

$$\lambda^d \equiv r + r\theta(\text{mod } p).$$

Conversely, suppose $\lambda^d \equiv r + r\theta(\text{mod } p)$. Let $c$ be the solution of $ux \equiv r(\text{mod } p)$, then $\lambda^d \equiv (uc + uc\theta) \equiv \lambda^m c(\text{mod } p)$. Hence,

$$\lambda^d - m \equiv c(\text{mod } p)$$

so that by Theorem 3.8 we have $d = m + t(p + 1)$ for some $t$ and the theorem is proved.

By a similar argument, it can be shown that the following is true.

Theorem 3.9. Let $\lambda^m$ fall on $y = -\theta x$ where $m$ is the smallest such exponent, then $\lambda^d = r - r\theta$ iff $d = m + t(p + 1)$ for some $t$.

In order to generalize the result of Theorem 2.12, we first establish

Lemma 3.1. For any $\beta = c + d\theta$, $\beta^p \equiv \beta(\text{mod } p)$.
Proof.---By Fermat's theorem, we have \( b^p \equiv c + d\theta^p \pmod{p} \).

Since \( \theta^p - 1 \equiv g^{(p - 1)/2} \equiv -1 \pmod{p} \), we conclude that
\[
\beta^p \equiv c - d\theta \equiv \bar{\beta} \pmod{p}.
\]

Using Theorem 3.1 together with Lemma 3.1 and following the argument of Theorem 2.12, we have

**Theorem 3.10.** If \( \lambda \) is a generator of \( GF(p^2) \), then \( \lambda \bar{\lambda} \) is a generator of \( GF(p) \).

Whenever \( p \) is a prime of the form \( 4k + 3 \) we have the same problems with the converse of Theorem 3.10 as we had with the converse of Theorem 2.12. However, the converse of Theorem 3.10 is false if \( p \) is of the form \( 4k + 1 \) since \( \theta \bar{\theta} \equiv -\theta^2 \equiv -g \pmod{p} \) while \( O(-g) = O(g) = p - 1 \) and \( O(\theta) < p^2 - 1 \) by Theorem 3.5.

In conclusion, we have

**Theorem 3.11.** Let \( O(u) = p - 1 \). Then there exist an \( n \) such that \( (\lambda \bar{\lambda})^n \equiv u \pmod{p} \).

The proof of Theorem 3.11 is similar to that of Theorem 2.15 and is therefore omitted.
REFERENCES


