THEORY OF CONGRUENCES

APPROVED:

George Copp
Major Professor

N.C. Parrish

Minor Professor

N.C. Parrish

Director of the Department of Mathematics

Robert Toulouse
Dean of the Graduate School
THEORY OF CONGRUENCES

THESIS

Presented to the Graduate Council of the
North Texas State College in Partial
Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

By

Harold Rugby Green, B. A., M. A.

Denton, Texas

June, 1961
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. SOME PROPERTIES OF INTEGERS</td>
<td>1</td>
</tr>
<tr>
<td>II. CONGRUENCES</td>
<td>4</td>
</tr>
<tr>
<td>III. BELONGING TO AN EXPONENT AND PRIMITIVE ROOTS</td>
<td>17</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>25</td>
</tr>
</tbody>
</table>
CHAPTER I

SOME PROPERTIES OF INTEGERS

The word "number" and the word "integer" will be used to indicate a rational integer unless otherwise indicated. When letters are used they will represent integers. Rational integers may be positive negative or zero.

Definition 1.1. Let a be different from zero. If there is a number c such that ac = b, then a divides b. This is written a|b. Also a is said to be a divisor of b and b a multiple of a.

Definition 1.2. If ab = 1, then a and b are units. The only integers which are units are 1 and -1.

Definition 1.3. An integer p, such that |p| > 1 is called a prime number or simply a prime if its only divisors are ±1 and ±p.

Definition 1.4. A number n, such that |n| > 1, which is not a prime is composite.

From the above definitions every integer belongs to one and only one of the following classes:

(1) Zero
(2) The units
(3) The primes
(4) The composite numbers.
Definition 1.5. If $a|b$ and $a|c$, then $a$ is a common divisor of $b$ and $c$. A number $d$ is the greatest common divisor of two or more distinct numbers if:

1. $d > 0$,
2. $d$ is a common divisor of the numbers, and
3. every common divisor of these numbers divides $d$.

The notation $d = (a, b)$ will indicate that $d$ is the greatest common divisor of $a$ and $b$.

Definition 1.6. If $(a, b) = 1$, $a$ and $b$ are relatively prime, or simply $a$ is prime to $b$. This does not imply that either $a$ or $b$ is a prime number.

Definition 1.7. If $a|c$ and $b|c$, then $c$ is a common multiple of $a$ and $b$. A number $m$ is called the least common multiple of two or more distinct numbers if:

1. $m > 0$,
2. $m$ is a common multiple of the numbers, and
3. $m$ divides every common multiple of the numbers.

The notation $m = [a, b]$ will indicate that $m$ is the least common multiple of $a$ and $b$.

The following theorems are stated, without proof, to be used for reference.

Theorem 1.8. If $b|ac$, where $(a, b) = 1$, then $b|c$.

Theorem 1.9. If a number is relatively prime to each of several numbers, it is relatively prime to their product.
Theorem 1.10. If \( d = (a, b) \) with \( a = a_1d \) and \( b = b_1d \), then \( (a_1, b_1) = 1 \).

Theorem 1.11. If a prime \( p \) is not relatively prime to \( n \), then \( p \mid n \).

Theorem 1.12. If a prime \( p \) divides a product, then it divides one of the factors of the product.

Theorem 1.13. If a positive prime \( p \) divides a product of positive prime factors, then \( p \) is equal to one of the prime factors.

Theorem 1.14. Every number \( n > 1 \) is divisible by some prime.

Theorem 1.15. If \( d = (a, b) \), there exist integers \( p \) and \( s \) such that \( d = pa + sb \).\(^1\)

Theorem 1.16. Every positive composite number can be expressed as a product of positive primes in one and only one way, except for the order of the factors.

Theorem 1.17. If a number is divisible by each of several relatively prime numbers, then it is divisible by their product.

CHAPTER II

CONGRUENCES

Definition 2.1. Let \( a, b, \) and \( m \) be integers. If \( m \) divides \((a - b)\), then \( a \) is said to be congruent to \( b \) modulo \( m \). This is written \( a \equiv b \pmod{m} \). If \( m \) does not divide \((a - b)\), then \( a \not\equiv b \pmod{m} \).

From this definition, \( a \equiv b \pmod{m} \) means there exists an integer \( k \), such that \( a = b + km \). Using \( a = b + km \) as a definition for \( a \equiv b \pmod{m} \), mod 0 is ordinary equality and is therefore trivial. Since 1 divides every number, mod 1 is also trivial. Since \(-m\) divides any number that \( m \) divides, \( m \) may be used as a positive integer. Therefore if \( m \) is used as a modulus, \( m \geq 2 \).

Theorem 2.2. Congruence modulo \( m \) is: (a) Reflexive \( (a \equiv a \mod{m}) \), (b) Symmetric \( (If \ a \equiv b \mod{m}, \ then \ b \equiv a \mod{m}) \), (c) Transitive \( (If \ a \equiv b \mod{m}, \ and \ b \equiv c \mod{m}, \ then \ a \equiv c \mod{m}) \).

Proof: (a) Reflexive: Since \( a - a = 0 \), \( m \mid (a - a) \). Therefore \( a \equiv a \pmod{m} \). (b) Symmetric: If \( a \equiv b \pmod{m} \), then \( a - b = km \), and \( b - a = -km \). Therefore \( b \equiv a \pmod{m} \). (c) Transitive: If \( a \equiv b \pmod{m} \), and \( b \equiv c \pmod{m} \), then \( a - b = km \) and \( b - c = nm \). Therefore \( a - c = (k + n)m \), and \( a \equiv c \pmod{m} \).
Theorem 2.3. If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then \( a + c \equiv b + d \pmod{m} \).

Proof: Since \( a \equiv b \pmod{m} \), \( a - b = km \). Since \( c \equiv d \pmod{m} \), \( c - d = jm \). Therefore \( (a + c) - (b + d) = (k + j)m \) or \( a + c \equiv b + d \pmod{m} \).

Theorem 2.4. If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then \( a - c \equiv b - d \pmod{m} \).

Proof: Since \( a \equiv b \pmod{m} \), \( a - b = km \). Since \( c \equiv d \pmod{m} \), \( c - d = jm \). Therefore \( (a - c) - (b - d) = (k - j)m \) or \( a - c \equiv b - d \pmod{m} \).

Theorem 2.5. If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then \( ac \equiv bd \pmod{m} \).

Proof: Since \( a \equiv b \pmod{m} \), \( a = b + km \). Since \( c \equiv d \pmod{m} \), \( c = d + jm \). Therefore \( ac = bd + dkm + bjm + kmjm \), or \( ac - bd = (dk + bj + kmj)m \), and \( ac \equiv bd \pmod{m} \).

Corollary 2.5.1. If \( a \equiv b \pmod{m} \), then \( a^n \equiv b^n \pmod{m} \).

Theorem 2.6. If \( a \equiv b \pmod{m} \) and if \( d \) divides \( m \), then \( a \equiv b \pmod{d} \).

Proof: Since \( d \mid m \), \( jd = m \). If \( a \equiv b \pmod{m} \), then \( a - b = km \), or \( a - b = (kj)d \). Therefore \( a \equiv b \pmod{d} \).

Theorem 2.7. If \( a \equiv b \pmod{m} \), then \( ac \equiv bc \pmod{mc} \).

Proof: Since \( a \equiv b \pmod{m} \), \( a - b = km \) and \( ac - bc = k \pmod{mc} \). Therefore \( ac \equiv bc \pmod{mc} \).

Theorem 2.8. If \( a \equiv b \pmod{m} \), and \( d \) is a common divisor of \( a \) and \( b \), and \( j = (m, d) \), then \( \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{j}} \).
Proof: Since \( a \equiv b \pmod{m} \), \( a - b = km \). Now 
\[
\left(\frac{a}{d} - \frac{b}{d}\right) \frac{d}{j} = \frac{mk}{j}, \text{ and by Theorem 1.10 it follows that } \left(\frac{a}{d}, \frac{m}{j}\right) = 1. \text{ Therefore, } \frac{m}{j} \mid \left(\frac{a}{d} - \frac{b}{d}\right), \text{ and } \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{j}}.
\]

**Corollary 2.8.1.** If \( a \equiv b \pmod{m} \), and \( d \) is a divisor of \( a \) and \( b \), with \( (m, d) = 1 \), then \( \frac{a}{d} \equiv \frac{b}{d} \pmod{m} \).

**Theorem 2.9.** If \( ab \equiv cd \pmod{m} \), \( b \equiv d \pmod{m} \), and \( (b, m) = 1 \), then \( a \equiv c \pmod{m} \).

Proof: Since \( ab \equiv cd \pmod{m} \), \( ab - cd = mk \). Since \( b \equiv d \pmod{m} \), \( b - d = mj \). Therefore \( ab - c(b - mj) = mk \) and \( ab - bc = (k - cj)m \). Therefore \( ab \equiv bc \pmod{m} \). Since \( (b, m) = 1 \), \( a \equiv c \pmod{m} \).

**Theorem 2.10.** If \( a \equiv b \pmod{m} \), then \( (a, m) = (b, m) \).

Proof: Since \( a \equiv b \pmod{m} \), \( a = b + mk \). Since any number which divides \( b \) and \( m \) divides the right side of the equation, it also divides \( a \). If the equation is written \( b = a - mk \), any number which divides \( a \) and \( m \) also divides \( b \). Therefore, if \( a \equiv b \pmod{m} \), then \( (a, m) = (b, m) \).

**Theorem 2.11.** If \( a \equiv b \pmod{m_1} \), \( a \equiv b \pmod{m_2} \), \ldots, \( a \equiv b \pmod{m_k} \), where the \( m_i \) are relatively prime in pairs, then \( a \equiv b \pmod{m_1 m_2 \cdots m_k} \).

Proof: Since \( a - b \) is divisible by each of the relatively prime integers \( m_i \), it is divisible by their product by Theorem 1.17.

**Definition 2.12.** The \( \phi \)-function. For \( m = 1 \), let \( \phi(1) = 1 \). When \( m > 1 \), let \( \phi(m) \) be the number of positive
integers less than \( m \) and relatively prime to \( m \). For example, since the only positive integers less than 12 and relatively prime to 12 are 1, 5, 7, and 11, \( \varphi(12) = 4 \).

**Definition 2.13.** All of the numbers which are congruent to each other, modulo \( m \), form a residue class modulo \( m \).

It follows from this definition that all of the numbers of a residue class have the same remainder \( r \), when divided by \( m \). For example, 10, 7, and 4, each has a remainder of 1 when divided by 3. Therefore 10, 7, and 4 belong to the same residue class modulo 3. The numbers of this residue class are of the form \( 3q + 1 \), where \( q \) is an integer.

**Theorem 2.14.** Every integer is congruent modulo \( m \) to one and only one of the numbers 0, 1, 2, \ldots, \( m - 1 \).

**Proof:** When an integer \( a \) is divided by \( m \), the remainder will be congruent to \( a \) and will be contained in the set: 0, 1, 2, \ldots, \( m - 1 \). Therefore, the first part of the theorem is true. The second part of the theorem follows from the fact that no two numbers of the set: 0, 1, 2, \ldots, \( m - 1 \) are congruent modulo \( m \), since their difference is less than \( m \), their difference is not zero, and therefore their difference is not divisible by \( m \).

**Definition 2.15.** Any set of \( m \) integers such that no two of them belong to the same residue class forms a complete residue system modulo \( m \).

**Definition 2.16.** Any set of \( \varphi(m) \) integers such that no two of them belong to the same residue class, and such that
each of the integers is prime to \( m \), forms a reduced residue system modulo \( m \).

**Theorem 2.17.** If \( r_1, r_2, \ldots, r_{\phi(m)} \) form a reduced residue system modulo \( m \) and if \( (a, m) = 1 \), then \( ar_1, ar_2, \ldots, ar_{\phi(m)} \) also form a reduced residue system modulo \( m \).

**Proof:** There are \( \phi(m) \) numbers in the set \( ar_1, ar_2, \ldots, ar_{\phi(m)} \). Now \( (r_1, m) = 1 \) and \( (a, m) = 1 \). Assume that \( (ar_1, m) = d > 1 \). Then \( d | ar_1 \) and \( d | m \). Assume that \( (a, d) = c > 1 \). Then \( c | a \) and \( c | d \) and therefore \( c | m \). This contradicts \( (a, m) = 1 \). Therefore \( (a, d) = 1 \). Since \( d | ar_1 \) and \( (a, d) = 1 \) it follows from Theorem 1.8 that \( d | r_1 \). This contradicts \( (r_1, m) = 1 \). Therefore \( (ar_1, m) = 1 \). No two distinct \( ar_1 \) and \( ar_k \) are congruent mod \( m \), for if \( ar_1 \equiv ar_k \pmod{m} \), then \( r_1 \equiv r_k \pmod{m} \) by Corollary 2.3.1. But \( r_1 \equiv r_k \pmod{m} \) would imply that \( i = k \), since \( r_1 \) and \( r_k \) are in a reduced residue system mod \( m \). Therefore \( ar_1, ar_2, \ldots, ar_{\phi(m)} \) forms a reduced residue system mod \( m \).

**Theorem 2.18.** If \( (a, m) = 1 \), then \( \phi(m) \equiv 1 \pmod{m} \).

**Proof:** Let \( r_1, r_2, \ldots, r_{\phi(m)} \) be a reduced residue system mod \( m \). Since \( (a, m) = 1 \), \( ar_1, ar_2, \ldots, ar_{\phi(m)} \) is also a reduced residue system mod \( m \). Therefore each \( ar_1 \) is congruent mod \( m \) to one and only one \( r_{\alpha_1} \), where \( i = 1, 2, \ldots, \phi(m) \) and \( \alpha_1, \alpha_2, \ldots, \alpha_{\phi(m)} \) is some permutation of \( 1, 2, \ldots, \phi(m) \). If these congruences are multiplied, then
\[ a^{\phi(m)} \equiv r_1 r_2 \cdots r_\phi(m) \pmod{m}. \]

Since \((r_1, m) = 1\), it follows from Corollary 2.8.1 that
\[ a^{\phi(m)} \equiv 1 \pmod{m}. \]

**Theorem 2.19.** If \( p \) is a prime and \((a, p) = 1\), then
\[ a^{p-1} \equiv 1 \pmod{p}. \]

**Proof:** This follows directly from Theorem 2.18, since \( \phi(p) = p - 1 \).

**Corollary 2.19.1.** If \( p \) is a prime and \( a \) is any integer, then \( a^p \equiv a \pmod{p} \).

**Proof:** If \( a \) and \( p \) are not relatively prime, then \( p \mid a \) since \( p \) is a prime. In this case \( p \mid a^p \) and \( p \mid a \), and therefore \( p \mid a^p - a \). If \((a, p) = 1\), the corollary follows from \( a^{p-1} \equiv 1 \pmod{p} \).

Another method of proving Theorem 2.19 is by use of induction.

**Proof:** Show first that \( p \mid a^p - a \), where \( p \) is a prime. Let \( a = 1 \). Since \( p \mid 1 - 1 \) the theorem is true for \( a = 1 \).
Assume that \( p \mid a^p - a \) for \( a = k \), that is \( p \mid k^p - k \). Let \( a = k + 1 \). Then \( a^p - a \) is \((k + 1)^p \) - \((k + 1) \). This can be written \( k^p + c(p, 1)k^{p-1}(1) + \cdots + c(p, r)k^{p-r} + \cdots + 1^p - k - 1 \),
where \( c(p, r) = \frac{p(p - 1) \cdots (p - r + 1)}{1 \cdot 2 \cdots r} \), for \( 1 \leq r < p \).
To show that \( p \mid c(p, r) \) for \( 1 \leq r < p \), write \( 1 \cdot 2 \cdots r \cdot c(p, r) = p(p - 1) \cdots (p - r + 1) \). Since \( p \) divides the right side of the equation it also divides the left side of the equation. Since \( p \) is a prime and \( r < p \), the product
1.2... r is not divisible by p. Therefore \( p \mid c(p, r) \). Since

\[(k + 1)^p - (k + 1) = (k^p - k) + \sum_{r=1}^{p-1} \frac{c(p, r)}{k^{p-r}} \]

by assumption and \( p \mid c(p, r) \), the theorem is true for \( a = k + 1 \). Therefore \( a^p \equiv a \pmod{p} \), where \( p \) is a prime. If \( (a, p) = 1 \), then \( a^{p-1} \equiv 1 \pmod{p} \).

The converse of Theorem 2.19 is that if \( a^{n-1} \equiv 1 \pmod{n} \), where \( (a, n) = 1 \), then \( n \) is a prime. This theorem is false as can be shown by the following counter-example:

\( 1^3 \equiv 1 \pmod{4} \) and \( (1, 4) = 1 \), but 4 is not a prime. However, the following theorem which is a converse of Theorem 2.19, with an extra condition added to the hypothesis, is true.

**Theorem 2.20.** If there exists an integer \( a \), where \( (a, n) = 1 \), such that \( a^{n-1} \equiv 1 \pmod{n} \) and if there does not exist an integer \( s < n - 1 \) such that \( a^s \equiv 1 \pmod{n} \), then the integer \( n \) is a prime number.

**Proof:** Assume that \( n \) is composite. Then \( \phi(n) < n - 1 \). Let \( a = \phi(n) \). Since \( a^{\phi(n)} \equiv 1 \pmod{n} \), when \( (a, n) = 1 \), by Theorem 2.18, then \( a^s \equiv 1 \pmod{n} \). This contradicts the hypothesis, and therefore \( n \) is a prime.

**Theorem 2.21.** If \( p \) and \( q \) are different primes, then

\[ p^{q-1} + q^{p-1} \equiv 1 \pmod{pq} \]

**Proof:** Since \( (p, q) = 1 \), it follows from Theorem 2.19 that \( p^{q-1} \equiv 1 \pmod{q} \) and \( q^{p-1} \equiv 1 \pmod{p} \). Therefore \( p^{q-1} = 1 + qk \) and \( q^{p-1} = 1 + ph \). Now,
\[ pq^{-1}q^{p-1} = 1 + qk + ph + qkph \] and
\[ pq^{-1}q^{p-1} = 1 + pq^{-1} - 1 + q^{p-1} - 1 + qkph. \] Therefore
\[ pq^{-1} + q^{p-1} = pq^{-1}q^{p-1} - khpq + 1, \] or
\[ pq^{-1} + q^{p-1} = 1 + (pq^{-2}q^{p-2} - kh)pq. \] Since \( p \geq 2 \) and \( q \geq 2 \), then \( pq^{-2}q^{p-2} \) is an integer. Therefore
\[ pq^{-1} + q^{p-1} \equiv 1 \pmod{pq}. \]

**Theorem 2.22.** If \( d \) is the least value of \( x > 0 \) for which \( a^x \equiv 1 \pmod{m} \), where \( (a, m) = 1 \), then \( d \mid \phi(m) \).

**Proof:** Assume that \( \phi(m) = qd + r \), where \( 0 \leq r < d \). Now \( a^{\phi(m)} = a^{qd+r} = a^{qd} \cdot a^r \equiv 1 \pmod{m} \). But \( a^d \equiv 1 \pmod{m} \), and \( a^{qd} \equiv 1^d \pmod{m} \). Therefore it follows from Theorem 2.9 that \( a^r \equiv 1 \pmod{m} \). Since \( r < d \) and \( d \) is the least value of \( x > 0 \) such that \( a^x \equiv 1 \pmod{m} \), then \( r = 0 \). Therefore \( \phi(m) = qd \) and \( d \mid \phi(m) \).

**Theorem 2.23.** If \( d \) is the least value of \( x > 0 \) for which \( a^x \equiv b^x \pmod{p} \), where \( p \) is a prime which does not divide \( a \) or \( b \), then \( p - 1 \equiv 0 \pmod{d} \).

**Proof:** Assume that \( p - 1 = dq + r \), where \( 0 \leq r < d \).
Since \( a^{p-1} \equiv 1 \pmod{p} \) and \( b^{p-1} \equiv 1 \pmod{p} \) by Theorem 2.19, then \( a^{p-1} \equiv b^{p-1} \pmod{p} \), or \( a^{dq+r} \equiv b^{dq+r} \pmod{p} \). This can be written \( a^{dq} \cdot a^r \equiv b^{dq} \cdot b^r \pmod{p} \). In the hypothesis \( a^d \equiv b^d \pmod{p} \). Therefore \( a^{dq} \equiv b^{dq} \pmod{p} \). Since \( (a, p) = 1 \) and \( (b, p) = 1 \), then \( a^r \equiv b^r \pmod{p} \). Since \( r < d \) and \( d \) is the least value of \( x > 0 \), then \( r = 0 \). Therefore \( p - 1 \equiv dq \), and \( d \mid p - 1 \), or \( p - 1 \equiv 0 \pmod{d} \).
Theorem 2.24. If $p$ is a prime, then 

$$(p - 1)! + 1 \equiv 0 \pmod{p}.$$ 

Proof:

Case I. Let $p = 2$. Since $(2 - 1)! + 1 = 2 \equiv 0 \pmod{2}$, the theorem is true for $p = 2$.

Case II. Consider $p > 2$.

The numbers $1, 2, \cdots, p - 1$ form a reduced residue system since there are $\phi(p) = p - 1$ of them, no two of them belong to the same residue class, and each of the integers is prime to $p$. Let $a$ be any number in this residue system. Then $a, 2a, \cdots, (p-1)a$ also form a reduced residue system since $(a, p) = 1$. Since no two numbers in a reduced residue system belong to the same residue class, one and only one of the numbers $a, 2a, 3a, \cdots, (p - 1)a$ is congruent to $1 \pmod{p}$. Thus for any $a$, where $a = 1, 2, \cdots, p - 1$, there is one and only one number $a_1$ in the same set such that $aa_1 \equiv 1 \pmod{p}$. Such two numbers are sometimes called associate numbers or reciprocals. If a number is identical to its associate, then $a^2 \equiv 1 \pmod{p}$ and 

$$(a - 1)(a + 1) \equiv 0 \pmod{p}.$$ 

Therefore $a \equiv 1 \pmod{p}$ and $a = 1$ or $a \equiv -1 \pmod{p}$ and $a = p - 1$. Therefore 1 and $p - 1$ are identical to their associates. Using the remaining numbers of the set, $2, 3, \cdots, p - 2$, the associates can be paired so that congruences of the form $aa_1 \equiv 1 \pmod{p}$ can be obtained. Upon multiplying all of these congruences, the
congruence is obtained: \( 2 \cdot 3 \cdots (p - 2) \equiv 1 \pmod{p} \). Then multiplying this congruence by \( 1 \pmod{p} \), the result is \( 1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv -1 \pmod{p} \), or \((p - 1)! + 1 \equiv 0 \pmod{p}\).

**Theorem 2.25.** If \( n \) is a number such that \((n - 1)! + 1 \equiv 0 \pmod{n}\), then \( n \) is a prime.

**Proof:** If \((n - 1)! + 1 \equiv 0 \pmod{n}\), then \((n - 1)! = -1 + kn\), or \((n - 1)! - kn = -1\). Assume that \( n \) is composite. Then there exists a divisor \( d \) of \( n \), where \( 1 < d < n \). Since \( d < n \), \( d \mid (n - 1)! \) and \( d \) divides the left side of the equation \((n - 1)! - kn = -1\). Since \( d \) does not divide \(-1\), the assumption that \( n \) was composite is false and therefore \( n \) is a prime.

Therefore a necessary and sufficient condition for an integer \( n \) to be prime is that \((n - 1)! + 1 \equiv 0 \pmod{n}\).

The following example illustrates one use of Theorem 2.24. Show that \( 18! + 1 \equiv 0 \pmod{437} \).

\[ 18! + 1 \equiv 0 \pmod{19}, \text{ since } 19 \text{ is a prime, or } 18! \equiv -1 \pmod{19}. \]

Also \( 22! + 1 \equiv 0 \pmod{23}, \text{ since } 23 \text{ is a prime, or } 22! \equiv -1 \pmod{23}. \) But

\[ 22! = 18! \cdot 19 \cdot 20 \cdot 21 \cdot 22 \equiv 18! \cdot 12 \cdot 2 \equiv 18! \equiv -1 \pmod{23}. \] Since \( 18! \equiv -1 \pmod{19} \) and \( 18! \equiv -1 \pmod{23}, \text{ and } (19, 23) = 1, \text{ it follows from Theorem 2.11 that } 18! \equiv -1 \pmod{437}, \text{ or } 18! + 1 \equiv 0 \pmod{437}. \]
Theorem 2.26. If \( n \) is composite, \( n > 0 \), and \( n \neq 4 \), then 
\[ (n - 1)! \equiv 0 \pmod{n}. \]

Proof: Since \( n \) is composite it can be written as \( n = pr \), where \( p \) is a positive prime.

Case I. Assume \( p \neq r \).

Since \( n \) is composite, \( n > 2 \). Therefore \( 2n > n + 2 \), or \( 2n - 2 > n \), and \( n - 1 > \frac{n}{2} \). This is true even though \( \frac{n}{2} \) may not be an integer. Since \( p \geq 2 \), and \( n = pr \), then \( r \leq \frac{n}{2} \). Since \( n - 1 > \frac{n}{2} \) and \( \frac{n}{2} \geq r \), then \( n - 1 > r \). Therefore \( r \) is a factor of \( (n - 1)! \). Since \( r \geq 2 \), then \( p \leq \frac{n}{2} \). Therefore \( n - 1 > p \).

Thus \( p \) is also a factor of \( (n - 1)! \). Since \( p \neq r \), \( p \) and \( r \) are distinct factors of \( (n - 1)! \). Therefore \( n \mid (n - 1)! \).

Case II. Let \( p = r \).

Since \( n = pr \), then \( n = p^2 \). In the hypothesis \( n \neq 4 \), therefore \( p^2 \neq 4 \) and \( p \neq 2 \). Hence \( p > 2 \) and \( p \geq 3 \). Therefore, \( p^2 \geq 3p \), and \( p^2 - 1 \geq 3p - 1 \). Since \( p > 1 \), \(-p < -1\). Therefore \( 3p - 1 > 3p - p = 2p \) and \( p^2 - 1 > 2p \). But \( p^2 = n \), so that \( n - 1 > 2p \). Also \( 2p > p \) so that \( n - 1 > p \). Since \( 2p \neq p \), \( 2p \) and \( p \) are distinct factors of \( (n - 1)! \). Therefore \( p^2 \mid (n - 1)! \) and \( n \mid (n - 1)! \), so that \( (n - 1)! \equiv 0 \pmod{n} \) when \( n \) is composite, \( n > 0 \), and \( n \neq 4 \).

Theorem 2.27. If \( p \) is a positive prime of the form \( 4n + 1 \), then \( \left( \frac{p - 1}{2} \right)! \) is a solution of \( x^2 + 1 \equiv 0 \pmod{p} \).
Proof: \[ 4n \equiv -1 \pmod{p}, \text{ where } p = 4n + 1. \]

\[ 4n - 1 \equiv -2 \pmod{p}, \]

\[ 4n - 2 \equiv -3 \pmod{p}, \]

\[ \vdots \]

\[ 2n + 1 \equiv -2n \pmod{p}, \]

\[ 2n \equiv 2n \pmod{p}, \]

\[ 2n - 1 \equiv 2n - 1 \pmod{p}, \]

\[ \vdots \]

\[ 2 \equiv 2 \pmod{p}, \]

\[ 1 \equiv 1 \pmod{p}. \]

Therefore \((4n)! \equiv [(2n)!] 2 \cdot [-1]^{2n} \pmod{p}\), or \((4n)! \equiv [(2n)!] 2 \pmod{p}\). By Theorem 2.24,

\((4n)! + 1 \equiv 0 \pmod{p}\), where \(p = 4n + 1\). Therefore \((4n)! \equiv -1 \pmod{p}\). Since \((4n)! \equiv [(2n)!] 2 \pmod{p}\), then \([(2n)!] 2 \equiv -1 \pmod{p}\), or \([(2n)!] 2 + 1 \equiv 0 \pmod{p}\).

But \(p = 4n + 1\), so that \(4n = p - 1\), and \(2n = \frac{p - 1}{2}\).

Therefore \(\left[\left(\frac{p - 1}{2}\right)\right] 2 + 1 \equiv 0 \pmod{p}\).

**Theorem 2.28.** If \(p\) is a positive prime of the form \(4n + 3\), then \(\left(\frac{p - 1}{2}\right)!\) is a solution of \(x^2 - 1 \equiv 0 \pmod{p}\).

Proof: \[ 4n + 2 \equiv -1 \pmod{p}, \text{ where } p = 4n + 3. \]

\[ 4n + 1 \equiv -2 \pmod{p}, \]

\[ 4n \equiv -3 \pmod{p}, \]

\[ \vdots \]
\[ 2n + 3 \equiv -2n \pmod{p}, \]
\[ 2n + 2 \equiv -2n - 1 \pmod{p}, \]
\[ 2n + 1 \equiv 2n + 1 \pmod{p}, \]
\[ 2n \equiv 2n \pmod{p}, \]
\[ \vdots \]
\[ 2 \equiv 2 \pmod{p}, \]
\[ 1 \equiv 1 \pmod{p}. \]

Therefore \((4n + 2)! \equiv \left[ (2n + 1)! \right]^2 \cdot (-1)^{2n+1} \pmod{p}\), or \((4n + 2)! \equiv -1 \cdot \left[ (2n + 1)! \right]^2 \pmod{p}\). But 
\((4n + 2)! + 1 \equiv 0 \pmod{p}\), for \(p = 4n + 3\), by Theorem 2.24, or \((4n + 2)! \equiv -1 \pmod{p}\). Therefore 
\[- \left[ (2n + 1)! \right]^2 \equiv -1 \pmod{p}, \quad \text{or} \quad \left[ (2n + 1)! \right]^2 \equiv 1 \pmod{p}.\]

Since \(p = 4n + 3\), then \(p - 1 = 4n + 2\), and \(\frac{p - 1}{2} = 2n + 1\).

Therefore \(\left( \frac{p - 1}{2} \right)! \equiv 1 \pmod{p}\), or 
\[ \left( \frac{p - 1}{2} \right)!^2 - 1 \equiv 0 \pmod{p}. \]

**Theorem 2.29.** If \(p\) is a positive odd prime, then 
\[ 2(p - 3)! + 1 \equiv 0 \pmod{p}. \]

**Proof:** \(p - 1 \equiv -1 \pmod{p}, \)
\(p - 2 \equiv -2 \pmod{p}, \) and 
\(p - 3 \equiv (p - 3)! \pmod{p}. \)

Therefore \((p - 1)(p - 2)(p - 3)! \equiv (-1)(-2)(p - 3)! \pmod{p}\).

But \((p - 1)(p - 2)(p - 3)! \equiv (p - 1)!\), and by Theorem 2.24 
\((p - 1)! + 1 \equiv 0 \pmod{p}\), or \((p - 1)! \equiv -1 \pmod{p}\). Therefore 
\((-1)(-2)(p - 3)! \equiv -1 \pmod{p}, \) or \(2(p - 3)! + 1 \equiv 0 \pmod{p}. \)
CHAPTER III

BELONGING TO AN EXPONENT

AND PRIMITIVE ROOTS

Let \( a \) be any number which is relatively prime to \( m \), where \( m \) is used as a modulus. Each term of the series

\[ 1, a, a^2, a^3, \ldots \]

is relatively prime to \( m \) and is therefore congruent to some term of a reduced residue system modulo \( m \). Since the reduced residue system modulo \( m \) contains \( \phi(m) \) terms and the series of powers of \( a \) is infinite, there must be at least two terms of the infinite series which are congruent modulo \( m \). Suppose that these terms are \( a^r \) and \( a^s \) and assume that \( r > s \). Since \((a^s, m) = 1\), both sides of the congruence

\[ a^r \equiv a^s \pmod{m} \]

may be divided by \( a^s \). Therefore \( a^{r-s} \equiv 1 \pmod{m} \).

Hence there is a positive exponent \( k \), where \( k = r - s \), such that \( a^k \equiv 1 \pmod{m} \). Since there is a positive exponent \( k \), such that \( a^k \equiv 1 \pmod{m} \), there must be a smallest positive exponent \( h \), such that \( a^h \equiv 1 \pmod{m} \).

**Definition 3.1.** If \( h \) is the smallest positive exponent such that \( a^h \equiv 1 \pmod{m} \), where \((a, m) = 1\), then \( a \) is said to belong to the exponent \( h \) modulo \( m \). This will be written \( a \rightarrow h \pmod{m} \).

**Theorem 3.2.** If \( a \rightarrow h \pmod{m} \), and if \( a^u \equiv 1 \pmod{m} \), then \( h \mid u \).
Proof: Assume that \( u = qh + r \), where \( 0 \leq r < h \). Now \( a^u \equiv 1 \pmod{m} \), and therefore \( a^{qh+r} \equiv 1 \pmod{m} \), or \( a^{qh} \cdot a^r \equiv 1 \pmod{m} \). But \( a^h \equiv 1 \pmod{m} \), and therefore \( (a^h)^q \equiv 1 \pmod{m} \). Since \( (a^{qh}, m) = 1 \), \( a^r \equiv 1 \pmod{m} \). Therefore \( r = 0 \), since \( a \rightarrow h \pmod{m} \). Therefore \( u = qh \) or \( h \mid u \).

**Corollary 3.21.** If \( a \rightarrow h \pmod{m} \), then \( h \mid \phi(m) \).

**Proof:** This follows from Theorem 2.18 and Theorem 3.2.

**Theorem 3.3.** If \( a \rightarrow h \pmod{m} \), then \( a^k \equiv a^s \pmod{m} \) if and only if \( k - s \equiv 0 \pmod{h} \).

**Proof:** Assume that \( k > s \) and that \( a^k \equiv a^s \pmod{m} \). Since \( (a, m) = 1 \), \( a^{k-s} \equiv 1 \pmod{m} \). Therefore \( h \mid k - s \).

Conversely, if \( h \mid k - s \), let \( k - s = hg \). Since \( a \rightarrow h \pmod{m} \), then \( (a^h)^g \equiv 1 \pmod{m} \) and \( a^{k-s} \equiv 1 \pmod{m} \), or \( a^k \equiv a^s \pmod{m} \).

**Theorem 3.4.** If \( a \rightarrow h \pmod{m} \) and \( b \rightarrow k \pmod{m} \), where \( (h, k) = 1 \), then \( ab \rightarrow hk \pmod{m} \).

**Proof:** Assume that \( ab \rightarrow r \pmod{m} \). Then \( (ab)^r \equiv 1 \pmod{m} \), or \( a^r b^r \equiv 1 \pmod{m} \). But \( a^h \equiv 1 \pmod{m} \), so that \( a^r \equiv 1 \pmod{m} \). Therefore \( b^r \equiv 1 \pmod{m} \). Hence \( k \mid r \).

Since \( (h, k) = 1 \), \( k \mid r \). Similarly \( (ab)^r \equiv 1 \pmod{m} \), or \( a^r b^r \equiv 1 \pmod{m} \). Since \( b^k \equiv 1 \pmod{m} \), then \( b^r \equiv 1 \pmod{m} \). Therefore \( a^r \equiv 1 \pmod{m} \) and \( h \mid r \).

Since \( (h, k) = 1 \), \( h \mid r \). Since \( (h, k) = 1 \), \( h k \mid r \). Therefore \( h k \leq r \). But \( a^h \equiv 1 \pmod{m} \) and \( b^k \equiv 1 \pmod{m} \). Therefore \( a^{hk} \equiv 1 \pmod{m} \), \( b^{hk} \equiv 1 \pmod{m} \), so that \( (ab)^{hk} \equiv 1 \pmod{m} \).
Since by assumption $ab \to r \mod m$, and since $hk \leq r$, $hk > 0$, and $(ab)^{hk} \equiv 1 \mod m$, then $ab \to hk \mod m$.

**Theorem 3.5.** If $ab \equiv 1 \mod m$, then $a$ and $b$ belong to the same exponent modulo $m$.

**Proof:** Let $(a, m) = h$. Since $ab \equiv 1 \mod m$, then $ab = mk + 1$. Now $h|ab$ and hence $h|mk + 1$. Since $h|mk$, then $h|1$ and $h = 1$. In the same manner it can be shown that $(b, m) = 1$. Therefore each of $a$ and $b$ belongs to an exponent mod $m$. Assume that $a \to x \mod m$ and $b \to y \mod m$. Since $a^x \equiv 1 \mod m$ and $b^y \equiv 1 \mod m$, then $a^x b^y \equiv 1 \mod m$.

Since $ab \equiv 1 \mod m$, then $a^x b^y \equiv 1 \mod m$. Therefore, $a^x b^y \equiv a^x b^x \mod m$ and $b^y \equiv b^x \mod m$. Assume that $y > x$. Since $(b, m) = 1$, $b^{y-x} \equiv 1 \mod m$. But $0 < y-x < y$. This contradicts the assumption that $b \to y \mod m$ for $y > x$. Assume that $x > y$. Then since $ab \equiv 1 \mod m$, $a^y b^y \equiv 1 \mod m$.

Therefore $a^x b^y \equiv a^y b^y \mod m$, and since $(b, m) = 1$, $a^x \equiv a^y \mod m$. Since $(a, m) = 1$, and $x > y$, $a^{x-y} \equiv 1 \mod m$.

But $0 < x-y < x$ and this contradicts the assumption that $a \to x \mod m$ for $x > y$. Therefore $x = y$.

**Theorem 3.6.** If $p$ is an odd prime and $a \to t \mod p$, where $t > l$, then

$$
\sum_{k=1}^{t-1} a^k \equiv -1 \mod p.
$$

**Proof:** $a \neq 1$, since $a \to t \mod p$ with $t > l$ and for $a = 1$, $a \to 1 \mod p$. Therefore, using the formula for the sum
of a geometric progression,

\[ a + a^2 + \cdots + a^{t-1} = \frac{a - a^t}{1 - a} = \frac{a^t - a}{a - 1}. \]

Assume that \( \frac{a^t - a}{a - 1} \equiv k \pmod{p} \). Then

\[ a^t - a \equiv k (a - 1)(\mod p), \text{ or } a^t \equiv k (a - 1) + a \pmod{p}. \]

But \( a^t \equiv 1 \pmod{p} \). Therefore \( k (a - 1) + a \equiv 1 \pmod{p} \).

Then \( k (a - 1) + (a - 1) = (k + 1)(a - 1) \equiv 0 \pmod{p} \).

Since \( p \) is a prime, either \( k + 1 \equiv 0 \pmod{p} \), or \( (a - 1) \equiv 0 \pmod{p} \). If \( a - 1 \equiv 0 \pmod{p} \), then \( a \equiv 1 \pmod{p} \).

This is impossible since \( a \rightarrow t \pmod{(p)} \), where \( t > 1 \). Therefore \( k + 1 \equiv 0 \pmod{p} \), or \( k \equiv -1 \pmod{p} \). Therefore

\[ \sum_{k=1}^{t-1} a^k \equiv -1 \pmod{p}. \]

**Theorem 3.7.** If \( a \rightarrow t \pmod{(m)} \), then \( a^u \rightarrow t \pmod{(m)} \), where \( d = (u, t) \).

**Proof:** Since \( a^t \equiv 1 \pmod{(m)} \), \( (a^t)^d \equiv 1 \pmod{(m)} \).

Therefore \( (a^u)^d \equiv 1 \pmod{(m)} \). Assume that \( a^u \rightarrow k \pmod{(m)} \).

Then \( t \mid \frac{a^u}{d} \). But from the congruence \( (a^u)^k \equiv 1 \pmod{(m)} \), or \( a^{uk} \equiv 1 \pmod{(m)} \), \( t \mid uk \) since \( a \rightarrow t \pmod{(m)} \). Therefore \( t \mid \frac{u}{d} \).

But \( d = (u, t) \) and hence \( \left(\frac{u}{d}, \frac{t}{d}\right) = 1 \). Therefore \( \frac{t}{d} \mid k \). Since \( k \mid \frac{t}{d} \)

and \( \frac{t}{d} \mid k \), where \( k > 0, t > 0 \), and \( d > 0 \), \( k = \frac{t}{d} \). Therefore \( a^u \rightarrow t \pmod{(m)} \).
Definition 3.8. If the number to which \( a \) belongs modulo \( m \) is \( \phi(m) \), then \( a \) is a primitive root of \( m \).

Theorem 3.9. If \( a \rightarrow \frac{p-1}{2} \) (mod \( p \)), where \( p \) is a prime of the form \( 4n-1 \), then \( -a \) is a primitive root of \( p \).

Proof: Since for \( p \) a prime, \( \phi(p) = p - 1 \), if \( b \) is a primitive root of \( p \), then \( b \) must belong to \( p - 1 \) (mod \( p \)). Since \( a \rightarrow \frac{p-1}{2} \) (mod \( p \)) and \( p = 4n - 1 \),
\[
a \rightarrow \frac{(4n-1)-1}{2} \equiv \frac{4n-2}{2} \equiv 2n-1 \pmod{p},
\]
or \( a \rightarrow 2n-1 \pmod{p} \). Also \((-1)^{p-1} \equiv 1 \pmod{p} \), for \( p > 2 \), and \((-1)^{2} \equiv 1 \pmod{p} \).
Therefore \(-1 \rightarrow 2 \pmod{p} \). Since \( 2n - 1 \) is odd and the only divisors of 2 are \( \pm 1 \) and \( \pm 2 \), \( (2n - 1, 2) = 1 \). Therefore \((-1)(a) \rightarrow 2 \left(\frac{p - 1}{2}\right) \pmod{p} \), or \( -a \rightarrow p - 1 \pmod{p} \) by Theorem 3.4. Hence \(-a \) is a primitive root of \( p \).

Definition 3.10. If the integers \( x_1, x_2, \ldots, x_{\phi(m)} \) of a reduced residue system also satisfy the condition \( 0 < x_1 < m \), then this set of integers will be called a least positive reduced residue system modulo \( m \).

Definition 3.11. Let \((a, m) = 1\). Then the powers of \( a: a, a^2, a^3, \ldots \) are prime to \( m \) and each of the powers of \( a \) is congruent to some term in a least positive reduced residue system modulo \( m \). The terms of this system which are congruent to some power of \( a \) modulo \( m \) are called power residues of \( a \) modulo \( m \).

For example, the powers of 2: 2, 4, 8, 16, 32, 64, 128, 256, 512, \ldots when taken modulo 9 are congruent respectively
to 2, 4, 8, 7, 5, 1, 2, 4, \ldots. Therefore the complete set of power residues of 2 mod 9 is the set: 2, 4, 8, 7, 5, 1. Also the complete set of power residues of 5 modulo 12 is the set: 5, 1.

**Theorem 3.12.** If \( p \) is an odd prime and \((b, p) = 1\), then \( p - 1 \) is a power residue of \( b \) (mod \( p \)) if and only if the exponent to which \( b \) belongs is even.

**Proof:** Assume that \( b \rightarrow t \) (mod \( p \)). If \( b^x \equiv p - 1 \) (mod \( p \)), and since \( 0 \equiv -p \) (mod \( p \)), then \( b^x \equiv -1 \) (mod \( p \)). Then \( b^{2x} \equiv 1 \) (mod \( p \)). Therefore \( t \mid 2x \), or \( 2x = kt \), and \( 2 \mid kt \). Since 2 is a prime, \( 2 \mid k \) or \( 2 \mid t \). If \( 2 \mid k \), then \( x \equiv st \). Therefore \( b^x = (b^t)^s \equiv -1 \) (mod \( p \)). But \( b^t \equiv 1 \) (mod \( p \)), and \( (b^t)^s \equiv 1 \) (mod \( p \)). For \( p > 2 \), \( -1 \not\equiv 1 \) (mod \( p \)). Therefore \( 2 \) does not divide \( k \), and hence \( 2 \mid t \). Therefore \( t \) is even.

If \( b \rightarrow t \) (mod \( p \)), where \( t = 2n \), then \( b^{2n} \equiv 1 \) (mod \( p \)). Therefore \( b^{2n} - 1 \equiv 0 \) (mod \( p \)), or \((b^n-1)(b^n+1) \equiv 0 \) (mod \( p \)). Therefore \( b^n \equiv 1 \) (mod \( p \)) or \( b^n \equiv -1 \) (mod \( p \)). Since \( 2n = t \), \( 0 < n < t \). But \( b \rightarrow t \) (mod \( p \)). Therefore \( b^n \not\equiv 1 \) (mod \( p \)). Hence \( b^n \equiv -1 \) (mod \( p \)). Since \( 0 \equiv p \) (mod \( p \)), \( b^n \equiv p - 1 \) (mod \( p \)) and \( 0 < p - 1 < p \). Therefore \( b \) has \( p - 1 \) as a power residue.

**Theorem 3.13.** If \( p \) is an odd prime and \( a \rightarrow 2t \) (mod \( p \)), then \( a^t \equiv -1 \) (mod \( p \)).

**Proof:** Assume that \( a^t \equiv b \) (mod \( p \)). Then \( a^{2t} \equiv b^2 \) (mod \( p \)). But \( a^{2t} \equiv 1 \) (mod \( p \)). Therefore \( b^2 \equiv 1 \) (mod \( p \)), or \( b^2 - 1 \equiv 0 \) (mod \( p \)). Hence
\[(b + 1)(b - 1) \equiv 0 \pmod{\text{p}} \text{ and } b \equiv 1 \pmod{\text{p}} \text{ or } b \equiv -1 \pmod{\text{p}}.\]

If \(b \equiv 1 \pmod{\text{p}}\), then \(a^t \equiv 1 \pmod{\text{p}}\). But \(0 < t < 2t\) and \(a \rightarrow 2t \pmod{\text{p}}\). Therefore \(b \equiv -1 \pmod{\text{p}}\) and \(a^t \equiv -1 \pmod{\text{p}}\).

**Theorem 3.14.** If \(p\) is a positive odd prime and \(a\) is a primitive root of \(p\), then the product of a complete set of power residues of \(a\) is congruent to \(-1 \pmod{p}\).

**Proof:** The numbers \(a, a^2, \ldots, a^{p-1}\) are incongruent mod \(p\). For if \(a^j \equiv a^k \pmod{p}\), where \(0 < k < j \leq p - 1\), then \(a^{j-k} \equiv 1 \pmod{p}\). This is impossible since \(0 < j - k \leq p - 1\) and \(a \rightarrow p - 1 \pmod{p}\). The numbers \(1, 2, \ldots, p - 1\) are the elements of a least positive reduced residue system modulo \(p\). Since there are \(p - 1\) numbers in the set \(a, a^2, \ldots, a^{p-1}\), and they are incongruent modulo \(p\), the power residues of these numbers are \(1, 2, \ldots, p - 1\) in some order. Therefore \(1, 2, \ldots, p - 1\) is a complete set of power residues of \(a\) modulo \(p\), since \((a, p) = 1\) implies that no power of \(a\) is congruent to \(0 \pmod{p}\), and by a previous theorem every integer is congruent mod \(p\) to one and only one of the numbers \(0, 1, 2, \ldots, p - 1\). Therefore

\[a \cdot a^2 \cdot \ldots \cdot a^{p-1} \equiv 1 \cdot 2 \cdot \ldots \cdot (p - 1) \pmod{p}.

Since \(p\) is odd, \(p - 1\) is even. Let \(p - 1 = 2t\). Then

\[a \cdot a^2 \cdot \ldots \cdot a^{p-1} = a^{\frac{(p-1)p}{2}}.

Therefore \(a^t \cdot p ! \equiv (p - 1)! \pmod{p}\).

But \(a^t \equiv a^{t[(p-1) + 1]} \equiv a^{t(p-1)} \cdot a^t \pmod{p}\). Since \(a \rightarrow p - 1 \pmod{p}\), \(a^{t(p-1)} \equiv 1 \pmod{p}\). Therefore

\((p - 1)! \equiv a^t \pmod{p}\). By Theorem 3.13 if \(a \rightarrow 2t \pmod{p}\), then
\[ a^t \equiv -1 \pmod{p}, \text{ for } p \text{ is an odd prime. Therefore, } \]
\[ a \cdot a^2 \cdots a^{p-1} \equiv (p - 1)! \equiv -1 \pmod{p}, \text{ or } \]
\[ (p - 1)! + 1 \equiv 0 \pmod{p}. \] This is another proof for
Theorem 2.24, where \( p \) is an odd prime.

**Theorem 3.15.** If \( g \) is a primitive root of \( p \), where \( p \) is a prime of the form \( 4n + 1 \), then \(-g\) is also a primitive root of \( p \).

**Proof:** \( g^{4n} \equiv 1 \pmod{p} \), where \( p = 4n + 1 \). Therefore \((g)^{4n} \equiv 1 \pmod{p} \), since \( 4n \) is an even integer.

Case I. Assume that \((-g)^{2n+k} \equiv 1 \pmod{p} \), where \( 1 \leq k < 2n \). If \( k \) were even then \( 2n + k \) would be even and \((-g)^{2n+k} = g^{2n+k} \equiv 1 \pmod{p} \). This is impossible since \( 2n + k < 4n \) and \( g \rightarrow 4n \pmod{p} \). Therefore \( k \) is odd.

\((-g)^{2n+k} = (g)^{2n} (-g)^k \equiv 1 \pmod{p} \). Now \( g^{2n} \equiv -1 \pmod{p} \) by Theorem 3.13. Therefore \((-g)^k \equiv -1 \pmod{p} \). Since \( k \) is odd, \((-g)^k = -(g)^k \). Therefore \(-\!(g)^k \equiv -1 \pmod{p} \), or \( g^k \equiv 1 \pmod{p} \). This is impossible since \( k < 4n \) and \( g \rightarrow 4n \pmod{p} \).

Case II. Assume that \((-g)^{2k+1} \equiv 1 \pmod{p} \), where \( k = 0, 1, \ldots, n - 1 \). As before \((-g)^h \not\equiv 1 \pmod{p} \) where \( h < 4n \) and \( h \) is even. Now \((-g)^{2k+1} = -(g)^{2k+1} \equiv 1 \pmod{p} \).

Therefore \( g^{2k+1} \equiv -1 \pmod{p} \). Then \((g^{2k+1})^2 \equiv (-1)^2 \pmod{p} \), or \( g^{4k+2} \equiv 1 \pmod{p} \). But \( k \leq n - 1 \). Therefore
\( 4k + 2 \leq 4n - 2 < 4n \). This is impossible since \( g \rightarrow 4n \pmod{p} \).
Since \((-g)^{4n} \equiv 1 \pmod{p} \) and \((-g)^m \not\equiv 1 \pmod{p} \) for \( m < 4n \),
\(-g\) is a primitive root of \( p \).
BIBLIOGRAPHY


