AN ALGORITHM FOR THE SOLUTION OF QUADRATIC
CONGRUENCES WITH SMALL PRIME MODULUS (≤100)

A THESIS
SUBMITTED TO THE FACULTY OF ATLANTA UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE
DEGREE OF MASTER OF SCIENCE

BY
ROSA B. WHALEY JOHNSON

ATLANTA, GEORGIA
AUGUST 1965
Acknowledgements

The writer is especially grateful to and wishes to thank her calculus teacher, Mr. Louis Dale, Sr., whose help and timely advice during the school year gave her the inspiration and courage necessary to continue her studies and eventually to write this thesis.

The writer wishes to express her sincere appreciation to Dr. Lloyd K. Williams, Chairman of the Mathematics Department, for his kind and patient guidance during the writing of this thesis. She also wishes to express her appreciation to Mrs. Julia D. King for typing this thesis.
## Table Of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th></th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Introduction</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Historical Background</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Purpose of Thesis</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>II. Fundamentals, Definitions, Basic Theorems and Implementations</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Notations</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Definitions</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Basic Theorems</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Interpretations</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>III. An Algorithm For Solving Quadratic Congruences With Prime Modulus</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>Bibliography</td>
<td></td>
<td>24</td>
</tr>
</tbody>
</table>
Chapter I

Introduction

The theory of numbers, one of the oldest branches of mathematics, has engaged the attention of many gifted mathematicians during the past 2300 years. The theory of numbers, also called higher arithmetic, is concerned in part with the properties of integers. As an established mathematical discipline, it is one of the youngest; yet its roots go deep into history. \( \sqrt{3; \frac{1}{7}} \)

Peculiarities of individual numbers or classes of numbers were observed as early as 3500 B.C. Such speculations on numbers, far from being a real study of their properties, developed at first into a peculiar number mysticism prevalent among ancient civilized people. Such numbers as 3 and 7 were accepted as omens of good luck. Later, such terms as feminine numbers, amicable numbers, and perfect numbers were used with no appreciation as to whether the concepts were of a strictly mathematical nature or merely of mystical properties.

The first rudiments of a scientific approach to the study of numbers, still intermingled with a good deal of number mysticism, can be traced back to Pythagoras (600 B.C.) and his disciples. It is believed that the distinction between prime and composite numbers was made in the Pythagorean School. By the time of Euclid (about 300 B.C.), the
Greeks possessed quite a number of strictly scientific facts about numbers, mostly pertaining to divisibility. \(\sqrt{5;2}\)

The topic "Congruent Numbers" or "Congruences Involving Unknowns" is one of the most important topics in the theory of numbers. There are many important names that might be associated with the development of the theory of congruences.

Fermat, in 1640, stated what is now known as "little Fermat theorem." The theorem states, if \(P\) is a prime and \(A,\) any integer not divisible by \(P,\) then \(A^{P-1}\) is divisible by \(P.\) In 1736, Euler proved Fermat's theorem and later generalized from the case of a prime \(P\) to any integer \(M.\) Lagrange proved that a congruence of degree \(N\) has at most \(N\) incongruent roots, if the modulus is a prime. Gauss noted that \(A \cdot b \equiv (\mod p)\) is solvable if and only if \(b\) is divisible by the g. c. d. of \(A\) and \(P.\) Gauss developed six proofs of the Quadratic Reciprocity Law. Also, Gauss is given credit for the current congruence notation \((\equiv).\)

\(\sqrt{1;2857}\) Lebesque found the number of sets of solutions of

\[
A_1 x_1^m \cdots A_k x_k^m \equiv A \pmod{P}
\]

where \(P\) is a prime such that \(P - 1\) is divisible by \(M.\)

\(\sqrt{2;577}\)

It is the purpose of this thesis to introduce and demonstrate, by use of many applications, an algorithm for solving quadratic congruences with prime modulus.

Included in the first two chapters are the notations, definitions, theorems, and interpretations necessary for an understanding of the algorithm and its application.
Chapter II

Fundamentals, Definitions, Basic Theorems, and Interpretations

1. Notation: An understanding of the meaning of the following symbols is necessary for the understanding of this thesis.

\[ = \quad \text{congruent to} \]
\[ \neq \quad \text{incongruent to} \]
\[ \pi \quad \text{is prime to} \]
\[ (P - \Phi) ! \quad \text{the product of P - 1 primes} \ 2 \cdot 3 \cdot 5 \cdots P - 1 \]
\[ \text{g.c.d.} \quad \text{greatest common divisor} \]
\[ (A, P) = 1 \quad A \text{ and } P \text{ are relatively prime} \]
\[ \Phi m \quad \text{the number of positive integers less than } M \text{ and prime to } M, \text{ where } M \text{ is a positive integer.} \]
\[ \text{mod } p \quad \text{modulo } p \]

2. Definitions:

**Composite Number.** - A number \( M \) is a composite number if it is divisible by factors other than \( M \) itself and 1.

**Prime Number.** - A number \( P \) is a prime number if it is divisible by only \( P \) itself and 1.
Relatively prime. - Two integers \( a \) and \( b \) that are not both zero are relatively prime if their greatest common divisor is 1.

Congruent. - If \( M \) is a divisor of \( a \equiv b \) (mod \( m \)), then \( a \) is said to be congruent to \( b \) (mod \( m \)).

Incongruent. - If \( M \) is not a divisor of \( a \equiv b \) (mod \( m \)), then \( a \) is said to be incongruent to \( b \) (mod \( m \)).

Residue. - For \( a \equiv b \) (mod \( m \)), \( b \) is called a residue of \( a \) with respect to the modulus \( M \).

Quadratic Residues. - Those numbers in the residue system (mod \( p \)) are such that for some \( x \), \( x^2 \equiv a \) (mod \( p \)). If there is no such \( x \), then \( a \) is called a quadratic nonresidue (mod \( p \)).

3. Basic Theorems:

Fermat's theorem and Wilson's theorem can be used to determine those primes \( P \) for which \( x^2 \equiv 1 \) (mod \( p \)) has a solution. Euler's criterion gives a necessary and sufficient condition that \( x^2 \equiv a \) (mod \( p \)) be solvable.

While the proof of these theorems will not be given here the use of each will be illustrated with several examples.

Fermat's theorem.

If \( P \) is any prime and \( A \) any number prime to \( P \), then

\[
A^{p-1} \equiv 1 \pmod{p}.
\]

Examples: (1) Consider 3 and 7, let \( 3 \) a and \( P \) 7

then \( A^{P-1} \equiv 1 \pmod{p} \) becomes
$3^6 \equiv 1 \pmod{7}$

\[ \therefore 729 \equiv 1 \pmod{7}. \]

(2) **Consider a = 3 and P = 5**

then $A^{P-1} \equiv 1 \pmod{P}$ becomes

$3^4 \equiv 1 \pmod{5}$

\[ \therefore 81 \equiv 1 \pmod{5}. \]

(3) **Consider a = 4 and P = 5, then**

$A^{P-1} \equiv 1 \pmod{P}$ becomes

$4^4 \equiv 1 \pmod{5}$

\[ \therefore 256 \equiv 1 \pmod{5}. \]

**Wilson's theorem.**

If $P$ is a prime, then $(P-1)! \equiv (-1) \pmod{P}$. 

**Examples:**

(1) **Consider P = 3, then according to**

Wilson's theorem $2!$ should be congruent to $-1 \pmod{3}$.

when $P = 3$

$(P-1)! \equiv -1 \pmod{P}$ becomes

$(3-1)! \equiv -1 \pmod{3}$

$2! \equiv -1 \pmod{3}$

$2 \equiv -1 \pmod{3}$

(2) **Consider P = 5, then**

$(P-1)! \equiv -1 \pmod{P}$ becomes

$(5-1)! \equiv -1 \pmod{5}$

$4! \equiv -1 \pmod{5}$
24 \equiv 4 \equiv -1 \pmod{5}

(3) Consider $p = 7$, then

$(P - 1)! \equiv -1 \pmod{p}$ becomes

$(7 - 1)! \equiv -1 \pmod{7}$

$6! \equiv -1 \pmod{7}$

$720 \equiv 20 \times 6 \equiv -1 \pmod{7}$,

**Euler's Criterion.**

The congruence $x^2 \equiv a \pmod{p}$ is solvable if and only if $a$ is a quadratic residue $\pmod{p}$. Using Fermat's theorem where

$A^{p-1} \equiv 1 \pmod{p}$

$A^{p-1} - 1 \equiv 0 \pmod{p}$ from which

$A^{p-1} - 1 \equiv (A^{\frac{p-1}{2}} - 1)(A^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$,

either $A^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $A^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, and both congruences cannot hold simultaneously. Consequently, $a$ is a quadratic residue or nonresidue of $p$ according as

$A^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $A^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

This theorem is known as "Euler's criterion."

Note: It must be pointed out here that $-1$ is a quadratic residue of primes of the form $4k + 1$, while $1$ is a quadratic residue of primes of the form $4k + 3$.

Examples: (1) $x^2 \equiv 2 \pmod{7}$ has no solution if

$2A^{\frac{p-1}{2}} \equiv -1 \pmod{7}$ because $-1$ is a nonresidue $\pmod{7}$ and $x^2 \equiv 2 \pmod{7}$
has 2 solutions if \( 2^{\frac{p-1}{2}} \equiv 1 \pmod{7} \).

Substituting in \( A^{\frac{p-1}{2}} \) for \( x^2 \equiv 2 \pmod{7} \) we get \( 2^3 \equiv 8 \equiv 1 \pmod{7} \); therefore, \( x^2 \equiv 2 \pmod{7} \) has 2 solutions, namely 3 and 4.

(2) Examine \( x^2 \equiv 3 \pmod{7} \): substituting in \( A^{\frac{p-1}{2}} \)

\( 3^2 \equiv 9 \equiv 2 \equiv -1 \pmod{7} \); therefore,

\( x^2 \equiv 3 \pmod{7} \) has no solution because

-1 is a nonresidue \( \pmod{7} \).

(3) Examine \( x^2 \equiv 2 \pmod{5} \): substituting in \( A^{\frac{p-1}{2}} \)

\( 2^2 \equiv -1 \pmod{5} \). But -1 is a

nonresidue \( \pmod{5} \); therefore,

\( x^2 \equiv 2 \pmod{5} \) has no solution.

(4) Examine \( x^2 \equiv 4 \pmod{5} \): substituting in \( A^{\frac{p-1}{2}} \)

\( 4^2 \equiv 16 \equiv 1 \pmod{5} \). Since 1 is a residue

\( \pmod{5} \) \( x^2 \equiv 4 \pmod{5} \)

has 2 solutions, namely 2 and 3.

4. Interpretations:

In this discussion we shall consider only congruences with prime modulus because it can be easily shown that the problem of solving a congruence with composite modulus can be reduced to solving a congruence with prime modulus.

Example: Find all roots of the congruence

\( x^2 \equiv 1 \pmod{21} \). The solution to this

congruence is the same as the solution
to the simultaneous equations $x^2 \equiv 1 \pmod{3}$
and $x^2 \equiv 1 \pmod{7}$. The two roots of the
congruence are 8 and 13.

In solving congruences it is desirable to know something
about the number of roots the congruence should have. In
general, the number of roots of a congruence $x^n \equiv a \pmod{p}$
does not exceed $n$. If the modulus is prime then $x^n \equiv a \pmod{p}$
will have no solution or a number of solutions less than $n$.
However, if the modulus is composite $x^n \equiv a \pmod{M}$ may have
any number of roots. Example, the congruence $x^3 \equiv x \equiv 0$
$\pmod{6}$ has six roots (0, 1, 2, 3, 4, and 5). The congruence
$x^2 \not\equiv 0 \pmod{8}$ has three roots (2, 4, and 8), while the
congruence $2x^2 - 3x - 3 \equiv 0 \pmod{6}$ has only one solution
(namely 3).

Just as all equations do not have integral roots all congru-
ences do not have roots. However, certain congruences always
have solutions. For example $x^2 \equiv a \pmod{p}$ always has a solu-
tion if $a$ is a quadratic residue $\pmod{p}$. If $x_0$ is a solution of
$x^2 \equiv a \pmod{p}$, then so is $p - x_0$. $x^2 \equiv -1 \pmod{p}$ either has no
solution or two solutions. If $P$ is of the form $4k + 1$, then
$x^2 \equiv -1 \pmod{p}$ has no solution. If $P$ is of the form $4k + 3$ then
$x^2 \equiv -1 \pmod{p}$ has two solutions. Congruences of the form
$ax^2 + by^2 \equiv c \pmod{p}$ is solvable if $(a, b, p) = 1$. The congruence
$ax^2 + bx + c \equiv 0 \pmod{p}$ has a general solution i.e., for the
general solution of $ax^2 + bx + c \equiv 0 \pmod{p}$ let $r_1$ be a root then

$$ax^2 + bx + c \equiv (x - r_1) q(x) \pmod{p}$$

$$q(x) \equiv (ax + d) \pmod{p}$$

$$ax + d \equiv 0 \pmod{p} \text{ where } (a, p) = 1$$

$\therefore \quad x \equiv r_2 \pmod{p}$ is a solution

$$ax + d \not\equiv 0 \pmod{p}.$$

Example: Solve the congruence

$$2x^2 + 3x \equiv 1 \pmod{5}.$$  Hence

$$(x - 1)(2x - 1) \equiv 0 \pmod{5}$$

$\therefore \quad x \equiv 1 \pmod{5} \text{ and}$$

$$2x - 1 \equiv 0 \pmod{5}$$

$$2x \equiv 1 \pmod{5}$$

$\therefore \quad x \equiv 3 \pmod{5}.$

The congruence $x^2 \equiv a \pmod{p}$ is solvable if and only if $a$ is a quadratic residue $\pmod{p}$. Quadratic residues and nonresidues have already been defined, but nothing has been said about finding the quadratic residues $\pmod{p}$.

To find the quadratic residues $\pmod{p}$ we may consider only the numbers $1, 2, 3, \ldots, p - 1$. To find all the distinct quadratic residues for an odd prime modulus it suffices to consider the squares

$$1^2, 2^2, 3^2, \ldots, (p - 1)^2,$$

reduce them to their least positive residues, and among these retain only the distinct ones.

Example: Find all quadratic residues $\pmod{5}$.
and reduce the squares to their least positive residues (mod 5).

\[ 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9 \equiv 4, \quad 4^2 \equiv 16 \equiv 1 \]

The resulting numbers 1 and 4 are quadratic residues mod 5, and the numbers 2 and 3 are quadratic nonresidues because they represent no number square mod 5. We should note that there are only \( \frac{p-1}{2} \) quadratic residues for an odd prime \( p \) and, consequently, exactly as many quadratic nonresidues.

Investigating the residue class relative to the modulus of a given congruence the existence or nonexistence of solutions to the congruence can be shown.

Example: Find all roots of \( x^3 \not\equiv 2x \not\equiv 1 \equiv 0 \) (mod 5).

Making a residue table for \( x^3 \not\equiv 2x \not\equiv 1 \equiv 0 \) (mod 5).

we have

<table>
<thead>
<tr>
<th>( x )</th>
<th>( x^3 \not\equiv 2x \not\equiv 1 ) (mod 5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>

From the table we see that no number is congruent to 0 (mod 5); therefore, the congruence has no solution.
Chapter III
An Algorithm For Solving Quadratic Congruences
With Small Modulus

In analogy with the problem of solving an algebraic equation, it is natural to consider the problem of solving a congruence. To solve a quadratic equation we may use factoring, graphing, completing the square, or use the quadratic formula. The method used to solve any equation would, more than likely, be determined by the equation in question. Likewise, the method to be used to solve a quadratic congruence will, more than likely, be determined by the congruence in question. However, for the remainder of this thesis the method of solution of congruences will be with an algorithm.

An algorithm in the form of \( u \cdot x - \frac{b-1}{2} \) and \( v \cdot x \not\equiv \frac{b-1}{2} \mod p \) may be used to solve quadratic congruences of the form \( x^2 \equiv a \mod p \), \( x^2 \not\equiv b \equiv c \equiv 0 \mod p \) and any other congruence that can be represented by the form \( x^2 \equiv a \mod p \).

To solve any congruence \( x^2 \equiv a \mod p \) using the algorithm \( u \cdot x = \frac{b-1}{2} \) and \( v \cdot x \not\equiv \frac{b-1}{2} \mod p \), first, make a table of residues for \( n = 1 \) through \( n = p-1 \); next, use the table and evaluate \( \frac{b-1}{2} \) and \( (\frac{b-1}{2})^2 \); next, write \( x^2 \equiv a \mod p \) as \( x^2 \equiv (\frac{b-1}{2})^2 \equiv a_1 \mod p \)

where \( (\frac{b-1}{2})^2 \not\equiv a_1 \equiv a \mod p \); next, set \( u^2 - u - a_1 = 0 \) and solve for \( u \);
and then, substitute in $u = x - \left(\frac{p-1}{2}\right)$ and solve for $x$.

Applications.

Example: Solve the congruence $x^2 \equiv 2 \pmod{23}$

Solution:

\[
\frac{p-1}{2} = 11, \quad \left(\frac{p-1}{2}\right)^2 = 6,
\]

\[u = x - 11, \text{ and } u \neq 11.\]

\[x^2 \equiv 2 \pmod{23}\]

\[x^2 - 6 \equiv 19 \pmod{23}\]

\[u^2 - u - 19 = 0\]

\[u = \frac{1 \pm \sqrt{1 + 112}}{2} = \frac{1 \pm \sqrt{77}}{2}
\]

\[\frac{1 \pm \sqrt{77}}{2} = \frac{1 \pm \sqrt{8}}{2}\]

(A)

To find the $\sqrt{8}$ set

\[x_1^2 \equiv 8 \pmod{23}\]

\[x_1^2 - 6 \equiv 2 \pmod{23}\]

\[u_1^2 - u_1 - 2 = 0\]

\[(u_1 \neq 1) (u_1 - 2) = 0\]

\[\therefore u_1 = 2\]

\[u_1 = x_1 - 11 \rightarrow 2 = x_1 - 11 \rightarrow x_1 = 13 \text{ or } 10\]

substituting the value for $x_1$ in (A) to find $u$ (A) becomes

\[\frac{1 + 10}{2} - \frac{11}{2} = 11 (\frac{1}{2}) = 11 (12)\]

\[\equiv 132 \equiv 17 \pmod{23}\]

$u = 17$ also $u = x - 11$, therefore

\[x = 11 \neq 17 = 28 \equiv 5 \pmod{23}.\]
In order to evaluate $11 (1/2)$ it is necessary to solve the equation

$1/2 = a$ or $1 = 2a$. In other words two times some number is congruent to $1 \pmod{23}$. Two times $12$ is congruent to $1 \pmod{23}$; therefore, $11 (1/2)$ is equal to $11 (1^2) \pmod{23}$.

Example: Solve the congruence $x^2 \equiv 3 \pmod{13}$.

\[
\frac{\frac{p-1}{2}}{2} = 6, \quad \left(\frac{p-1}{2}\right)^2 = 10, \quad u = x - 6, \quad v = x \neq 6
\]

\[
x^2 \equiv 3 \pmod{13}
\]

\[
x^2 - 10 \equiv 6 \pmod{13}
\]

\[
u^2 - u - 6 = 0
\]

\[
u = \frac{1 \pm \sqrt{1 + 24}}{2} = \frac{1 \pm \sqrt{25}}{2}
\]

\[
u = \frac{1 \pm 12}{2}
\]

To find $\sqrt{12}$

\[
x_1^2 \equiv 12 \pmod{13}
\]

\[
x_1^2 - 10 \equiv 2 \pmod{13}
\]

\[
u_1^2 - u_1 - 2 = 0
\]

\[(u_1 - 2) (u_1 + 1) = 0
\]

\[u_1 = 2, \quad u_1 = x_1 - 6 \rightarrow x_1 = 8
\]

Substituting to find $u$

\[u = \frac{1 + 8}{2} = 9 \pmod{13}
\]

\[u = x - 6 \rightarrow 9 = x - 6 \rightarrow x = 17 \equiv 4 \pmod{13}
\]

\[x = 4 \text{ is a solution also } P - x - 9 \text{ is a solution.}
\]
To use the algorithm to solve a congruence of the form \( x^2 \equiv bx \mod p \), we must first change \( x^2 \equiv bx \mod c = 0 \) into the form \( x^2 \equiv a \mod p \). Let \( x = y - \frac{b}{2} \), then \( x^2 \equiv b x \mod c = 0 \) becomes

\[
\left(y - \frac{b}{2}\right)^2 \equiv b \left(y - \frac{b}{2}\right) \equiv c = 0 \text{ or } \\
y^2 - by \equiv \frac{b^2}{4} \equiv by - \frac{b}{2} \equiv c = 0 \\
y^2 - \frac{b^2}{4} \equiv c = 0 \\
y^2 \equiv \frac{b^2}{4} - c.
\]

Example: Solve \( x^2 \equiv 16 x + 5 \equiv 0 \mod 23 \) using the algorithm

\[
u = x - \frac{b+1}{2} \text{ and } v = x \equiv \frac{b-1}{2}.
\]

Solution: \( u \equiv y \equiv 11, \; v \equiv y \equiv 11, \; x \equiv y \equiv 15, \; y^2 \equiv 13 \)

\[
y^2 \equiv 13 \mod 23 \\
y^2 - 6 \equiv 7 \mod 23 \\
u^2 - u - 7 = 0 \\
u = \frac{1 + \sqrt{1 + 28}}{2} = \frac{1 + \sqrt{29}}{2} \\
\frac{1 + \sqrt{29}}{2} = \frac{1 + \sqrt{6}}{2} \\
u = \frac{1 + 11}{2} = 6.
\]

\( u \equiv y \equiv 11 \Rightarrow y = 17 \)

\( x = y \equiv 15 \Rightarrow x = 17 \equiv 15 \equiv 9 \mod 23 \)

\( \therefore x_0 = 9 \) is a root and \( P - x_0 = 14 \)

is also a root.
Example: Solve $x^2 \equiv 8 \times x \equiv 17 \pmod{37}$ using the algorithm.

\[ x^2 \equiv 8 \times x \equiv 17 \pmod{37} \]

Substituting:

\[ x = y - 4, \quad y^2 \equiv 36 \]
\[ u = y - 18, \quad v = y / 16 \]

\[ y^2 \equiv 36 \pmod{37} \]
\[ y^2 - 28 \equiv 8 \pmod{37} \]
\[ u^2 - u - 8 = 0 \]

\[ u = \frac{1 \pm \sqrt{1 + 32}}{2} = \frac{1 \pm \sqrt{33}}{2} \]

\[ u = \frac{1 + \sqrt{33}}{2} = 13 \]
\[ u = \frac{1 - \sqrt{33}}{2} = 17 \]

\[ 13 = y - 18 \rightarrow y = 31 \]
\[ x = y - 4 \rightarrow x = 31 - 4 \]

\[ \therefore x = 27 \text{ is a solution.} \]

To find the second solution

\[ u = \frac{1 - \sqrt{33}}{2} = \frac{1 - 12}{2} \]
\[ = 13 (1/2) = 13 (19) = 247 \equiv 25 \pmod{37} \]

\[ 25 = y - 18 \rightarrow y = 43 \equiv 6 \]
\[ x = y - 4 \rightarrow x = 4 - 6 \]

\[ \therefore x = 2 \text{ is a solution.} \]

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x^2 \pmod{37}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>6</td>
<td>36</td>
</tr>
<tr>
<td>7</td>
<td>12</td>
</tr>
<tr>
<td>8</td>
<td>27</td>
</tr>
<tr>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>10</td>
<td>26</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>12</td>
<td>33</td>
</tr>
<tr>
<td>13</td>
<td>21</td>
</tr>
<tr>
<td>14</td>
<td>11</td>
</tr>
<tr>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>16</td>
<td>34</td>
</tr>
<tr>
<td>17</td>
<td>30</td>
</tr>
<tr>
<td>18</td>
<td>28</td>
</tr>
<tr>
<td>19</td>
<td>28</td>
</tr>
<tr>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>21</td>
<td>34</td>
</tr>
<tr>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>23</td>
<td>11</td>
</tr>
<tr>
<td>24</td>
<td>21</td>
</tr>
<tr>
<td>25</td>
<td>33</td>
</tr>
<tr>
<td>26</td>
<td>10</td>
</tr>
<tr>
<td>27</td>
<td>26</td>
</tr>
<tr>
<td>28</td>
<td>7</td>
</tr>
<tr>
<td>29</td>
<td>27</td>
</tr>
<tr>
<td>30</td>
<td>12</td>
</tr>
<tr>
<td>31</td>
<td>36</td>
</tr>
<tr>
<td>32</td>
<td>25</td>
</tr>
<tr>
<td>33</td>
<td>16</td>
</tr>
<tr>
<td>34</td>
<td>9</td>
</tr>
<tr>
<td>35</td>
<td>4</td>
</tr>
<tr>
<td>36</td>
<td>1</td>
</tr>
</tbody>
</table>
Solve $x^4 + 6x^3 - 17x^2 - 6x = 16 \pmod{41}$

\[ \frac{p-1}{2} = 20, \ u=x-20, \ v=x/20. \]

**factoring**

\[(x^2 - 1)(x^2 + 6x - 16) \equiv 0 \pmod{41} \]

\[ x^2 \equiv 1 \pmod{41} \]

\[ x^2 - 31 \equiv 11 \pmod{41} \]

\[ u^2 - u - 11 = 0 \]

\[ u = \frac{1 \pm \sqrt{1 + 4 	imes 11}}{2} = \frac{1 \pm \sqrt{45}}{2} = \frac{1 \pm 39}{2} = 20 \]

\[ 20 = x - 20 \]

\[ \therefore x = 40 \text{ is a solution.} \]

\[ x = 1 \text{ is also a solution.} \]

\[ x^2 + 6x - 16 \equiv 0 \pmod{41} \]

\[ x = y - 3 \]

\[ y^2 \equiv 25 \pmod{41} \]

\[ y^2 \equiv 25 \]

\[ y = 25 \]

\[ y^2 - 31 \equiv 35 \pmod{41} \]

\[ u^2 - u - 35 = 0 \]

\[ u = \frac{1 \pm \sqrt{1 + 4 	imes 35}}{2} = \frac{1 \pm \sqrt{140}}{2} \]

\[ u = \frac{1 \pm 11}{2} = 16 \text{ and } \frac{1 \pm 31}{2} = 15 \]

\[ u = \frac{1 - 31}{2} = 15 = 26 \]

\[ 16 \cdot y - 20 \text{ and } 26 = y - 20 \]

\[ x = y + 3 \text{ therefore } \]

\[ x = 36 - 3 \text{ and } x = 46 - 3 \]

\[ \therefore x = 33 \text{ and } x \neq 2 \text{ are solutions.} \]
The four roots of the congruence are \( x = 1, 2, 33, \) and 40.

Solve \( x^4 - 7x^2 \equiv -12 \pmod{53} \)

\[
\frac{D - 1}{2} = 26, \ u = x - 26, \ v = x \neq 26
\]

\[
x^4 - 7x^2 \equiv 0 \pmod{53}
\]

\[
(x^2 - 4) (x^2 - 3) \equiv 0 \pmod{53}
\]

\[
x^2 \equiv 4 \pmod{53}
\]

\[
x^2 \equiv 40 \equiv 17 \pmod{53}
\]

\[
u^2 - u - 17 = 0
\]

\[
u = \frac{1 \pm \sqrt{1 + 68}}{2} = \frac{1 \pm \sqrt{16}}{2}
\]

\[
u = \frac{1 + 16}{2} = 25
\]

\[25 = x - 26
\]

\[\therefore x = 51 \text{ and } x = -2.
\]

\[
x^2 - 3 \equiv 0 \pmod{53}
\]

\[
x^2 \equiv 3 \pmod{53}
\]

\[
x^2 - 40 \equiv 16 \pmod{53}
\]

\[
u^2 - u - 16 = 0
\]

\[
u = \frac{1 \pm \sqrt{1 + 64}}{2} = \frac{1 \pm \sqrt{12}}{2}
\]

\[\star \text{This particular congruence has no integral solution}
\]

because 12 is not a quadratic residue \( \pmod{53} \).

Therefore, the two roots of this congruence is

\[x = 2 \text{ and } x = 51.\]
Solve \( x^4 \neq x^3 - 11x^2 - 9x \equiv -18 \pmod{67} \)

\[
\begin{align*}
u &= x - 33, \quad v = x \neq 33, \quad -\frac{B_{\pm 1}}{2} = 33 \\
x^4 \neq x^3 - 11x^2 - 9x \equiv 18 \equiv 0 \pmod{67} \\
(x^2 - 9) (x^2 \neq x - 2) \equiv 0 \pmod{67} \\
x^2 \equiv 9 \pmod{67} \\
x^2 \equiv 19 \equiv 59 \pmod{67} \\
u^2 \neq u \equiv -59 \equiv 0 \\
&\quad \frac{1 \pm \sqrt{1 - 236}}{2} = \frac{1 \pm 61}{2} \\
u = 1 - \frac{61}{2} = 31 \text{ and} \\
u = 1 + \frac{61}{2} = -30 \equiv 37 \\
31 \equiv x - 33 \text{ and } 37 \equiv x - 33 \\
\therefore \quad x = 64 \text{ and } x = 3 \\
x^2 \neq x - 2 \equiv 0 \pmod{67} \quad x \equiv y - 34 \\
y^2 \equiv 19 \pmod{67} \quad y^2 \equiv 19 \\
y^2 - 17 \equiv 2 \pmod{67} \quad u \equiv y - 33 \\
u^2 - u - 2 \equiv 0 \\
(u - 2) (u \neq 1) = 0 \\
\therefore \quad u = 2 \text{ and } u \equiv -1 \\
2 \equiv y - 33 \text{ and } -1 \equiv y - 33 \\
y \equiv 35 \text{ and } y \equiv 32 \\
x \equiv y - 34 \equiv 0 \\
x = 35 - 34 \text{ and } x = 32 - 34 \\
x = 1 \quad \text{ and } x \equiv 2 \equiv 65 \\
\end{align*}
\]

The four roots are \( x = 1, 3, 64 \) and \( 65 \).
Solve $x^2 \not\equiv 4x \equiv 12 \pmod{73}$

$u = y - 36, \quad v = y \not\equiv 36$

$x = y - 2, \quad y^2 \equiv 16$

$y^2 \equiv 16 \pmod{73}$

$y^2 - 55 \equiv 34 \pmod{73}$

$u^2 - u - 34 = 0$

$u = \frac{1 \pm \sqrt{1 + 136}}{2} = \frac{1 \pm 65}{2}$

$u = \frac{1 + 65}{2} = 33$

$u = \frac{1 - 65}{2} = -32 \equiv 41$

$u = y - 36$

$33 = y - 36$ and $41 = y - 36$

$y = 69$ and $y = 77 \equiv 4$

$x = y - 2$

$x = 69 - 2$ and $x = 4 - 2$

$x = 67$ and $x = 2$

The two solutions are $x = 2$, and $x = 67$. 

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x^2 \pmod{73}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>6</td>
<td>36</td>
</tr>
<tr>
<td>7</td>
<td>47</td>
</tr>
<tr>
<td>8</td>
<td>64</td>
</tr>
<tr>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>27</td>
</tr>
<tr>
<td>11</td>
<td>48</td>
</tr>
<tr>
<td>12</td>
<td>71</td>
</tr>
<tr>
<td>13</td>
<td>23</td>
</tr>
<tr>
<td>14</td>
<td>50</td>
</tr>
<tr>
<td>15</td>
<td>6</td>
</tr>
<tr>
<td>16</td>
<td>37</td>
</tr>
<tr>
<td>17</td>
<td>70</td>
</tr>
<tr>
<td>18</td>
<td>32</td>
</tr>
<tr>
<td>19</td>
<td>69</td>
</tr>
<tr>
<td>20</td>
<td>35</td>
</tr>
<tr>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td>22</td>
<td>46</td>
</tr>
<tr>
<td>23</td>
<td>18</td>
</tr>
<tr>
<td>24</td>
<td>65</td>
</tr>
<tr>
<td>25</td>
<td>41</td>
</tr>
<tr>
<td>26</td>
<td>19</td>
</tr>
<tr>
<td>27</td>
<td>72</td>
</tr>
<tr>
<td>28</td>
<td>54</td>
</tr>
<tr>
<td>29</td>
<td>38</td>
</tr>
<tr>
<td>30</td>
<td>24</td>
</tr>
<tr>
<td>31</td>
<td>12</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
</tr>
<tr>
<td>33</td>
<td>67</td>
</tr>
<tr>
<td>34</td>
<td>61</td>
</tr>
<tr>
<td>35</td>
<td>57</td>
</tr>
<tr>
<td>36</td>
<td>55</td>
</tr>
</tbody>
</table>
Solve $x^6 \div 8x^5 \div 10x^4 - 40x^3 - 71x^2 - 32x \div 60 \equiv 0 \pmod{83}$

$(x^2 - 4) (x^2 - 1) (x^2 - 8x \div 15) \equiv 0 \pmod{83}$

$x^2 \equiv 4 \pmod{83} \quad \frac{b \pm \sqrt{b^2 - 4ac}}{2a} = 41$

$x^2 - 21 \equiv 66 \pmod{83} \cdot u = x - 41$

$u^2 - u - 66 = 0$

$u = \frac{1 \pm \sqrt{1 + 264}}{2} = \frac{1 \pm 79}{2} = 40$ and 44

$40 = -x - 41$ and 44 $x - 41$

$x = 81$ and $x = 2$

$x^2 \equiv 1 \pmod{83}$

$x^2 - 21 \equiv 63 \pmod{83}$

$u^2 - u - 63 = 0$

$u = \frac{1 \pm \sqrt{1 + 252}}{2} = \frac{1 \pm 81}{2} = 41$ and 43

$41 = x - 41$ and 43 $x - 41$

$x = 82$ and $x = 1$

$x^2 - 8x \div 15 \equiv 0 \pmod{83} \quad x = y \div 4$

$y^2 \equiv 1 \pmod{83} \quad y^2 = 1$

$y^2 - 21 \equiv 63 \pmod{83} \cdot u = y - 41$

$u^2 - u - 63 = 0$

$u = \frac{1 \pm \sqrt{1 + 252}}{2} = \frac{1 \pm 81}{2} = 41$ and 43

$u = y - 41$

$41 = y - 41$ and 43 $= y - 41$

$y = 82$ and $x = y = 1$
\[ x = y \div 4 \]

\[ x = 86 \div 3 \quad x = 5 \]

The six solutions are \( x = 1, 2, 3, 5, 81, \) and \( 82. \)
Solve $x^6 - 10x^5 + x^4 - 200x^3 - 356x^2 + 1344 \equiv 0 \pmod{97}$

$(x^2 - 4) \cdot (x^2 - 16) \cdot (x^2 - 10x + 21) \equiv 0 \pmod{97}$

$x^2 \equiv 4 \pmod{97} \quad u = x - 48$

$x^2 - 73 \equiv 28 \pmod{97}$

$u^2 - u - 28 = 0$

$u = \frac{1 \pm \sqrt{1 + 112}}{2} = \frac{1 \pm 93}{2} \equiv 47 \text{ and } 51$

$47 = x - 48 \quad \text{and} \quad 51 = x - 48$

$\therefore \quad x = 95 \quad \text{and} \quad x = 99 \not\equiv 2$

$x^2 \equiv 16 \pmod{97}$

$x^2 - 73 \equiv 40 \pmod{97}$

$u^2 - u - 40 = 0$

$u = \frac{1 \pm \sqrt{1 + 160}}{2} = \frac{1 \pm 89}{2} \equiv 45 \text{ and } 53$

$45 = x - 48 \quad \text{and} \quad 53 = x - 48$

$\therefore \quad x = 93 \quad \text{and} \quad x = 101 \equiv 4$

$x^2 - 10x + 21 \equiv 0 \pmod{97}$

$y^2 \equiv 4 \pmod{97}$

$y^2 - 73 \equiv 28 \pmod{97}$

$u^2 - u - 28 = 0$

$u = \frac{1 \pm \sqrt{1 + 112}}{2} = \frac{1 \pm 93}{2} \equiv 47 \text{ and } 51$

$u = y - 48$

$47 = y - 48 \quad \text{and} \quad 51 = y - 48$

$y = 95 \quad \text{and} \quad y = 99 \not\equiv 2$

$x = y - 5 \quad \therefore \quad x = 3 \quad \text{and} \quad x \equiv 7$

$x \quad \quad \quad x^2 \pmod{97}$

1 \quad 1
2 \quad 4
3 \quad 9
4 \quad 16
5 \quad 25
6 \quad 36
7 \quad 49
8 \quad 64
9 \quad 81
10 \quad 3
11 \quad 24
12 \quad 47
13 \quad 72
14 \quad 2
15 \quad 31
16 \quad 62
17 \quad 95
18 \quad 33
19 \quad 70
20 \quad 12
21 \quad 53
22 \quad 96
23 \quad 44
24 \quad 91
25 \quad 43
26 \quad 94
27 \quad 50
28 \quad 8
29 \quad 65
30 \quad 27
31 \quad 88
32 \quad 54
33 \quad 22
34 \quad 89
35 \quad 61
36 \quad 35
37 \quad 11
38 \quad 86
39 \quad 66
40 \quad 48
41 \quad 32
42 \quad 18
The six solutions are \( x = 2, 3, 4 \), \( 7, 93, \) and \( 95 \).
Bibliography


