8-1-1965

Algorithm for the solution of quadratic congruences with small prime modulus (<= 100)

Rosa B. Whaley Johnson
Atlanta University

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

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. [3;1]

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 intermixed 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. /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 $A^{P-1}-1$ 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 x≡b (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 Quadric Reciprocity Law. Also, Gauss is given credit for the current congruence notation (≡). /1;285/ Lebesque found the number of sets of solutions of

$A_1 x_1^m \ldots A_k x_k^m \equiv A \pmod{p}$ where P is A prime such that P - 1 is divisible by M. /2;57/

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.

$\equiv$	congruent to
$\not\equiv$	incongruent to
$\perp\!\!\!\perp$	is prime to
$(P-1)!$	the product of P-1 primes $2\cdot 3\cdot 5\cdot\cdots P-1$
g. c. d.	greatest common divisor
$(A, P)=1$	A and P are relatively prime
$\emptyset$ m	the number of positive integers less than M and prime to M, where M is a positive integer.
$\mod_p$	$\mod_p$

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-b, then a is said to be congruent to b (mod m).

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

Residue. - For $a \equiv b \pmod{m}$, 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, $x^2 \equiv a \pmod{p}$. 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 $x^2 \equiv -1 \pmod{p}$ has a solution. [4;3] Euler's criterion gives a necessary and sufficient condition that $x^2 \equiv a \pmod{p}$ 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

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

$6! \equiv -1 \pmod 7$

$720 \equiv 20 \equiv 6 \equiv -1 \pmod 7$.

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

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

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

$2^{\frac{p-1}{2}} \equiv -1 \pmod 7$ because -1 is a nonresidue (mod 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 $A^{\frac{p-1}{2}}$ $3^3 \equiv 27 \equiv 6 \equiv -1 \pmod 7$; therefore, $x^2 \equiv 3 \pmod 7$ has no solution because -1 is a nonresidue (mod 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 (mod 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 (mod 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 $x^3 - x \equiv 0 \pmod 6$ has six roots (0, 1, 2, 3, 4, and 5). The congruence $x^2 + 2x \equiv 0 \pmod 8$ 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 congruences do not have roots. However, certain congruences always have solutions. For example $x^2 \equiv a \pmod p$ always has a solution if $\underline{a}$ 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 $4k + 3$, then $x^2 \equiv -1 \pmod p$ has no solution. If P is of the form $4k + 1$ 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

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

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

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

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

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

Example: Solve the congruence

$2x^2 - 3x + 1 \equiv 0 \pmod 5$. Hence

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

$\therefore \quad x \equiv 1 \pmod 5$ 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, ..., 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 (mod 5).

and reduce the squares to their least positive residues (mod 5).

$1^2 = 1,\ 2^2 = 4,\ 3^2 = 9 \equiv 4,\ 4^2 = 16 \equiv 1$

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 $x^3 + 2x + 1 \equiv 0 \pmod 5$.

Making a residue table for $x^3 + 2x + 1 \equiv 0 \pmod 5$. we have

x	$x^3 + 2x + 1 \pmod 5$
1	4
2	3
3	4
4	3

From the table we see that no number is congruent to $\underline{0}$ (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 algebratic 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 $u=x-\frac{p-1}{2}$ and $v=x+\frac{p-1}{2}$ may be used to solve quadratic congruences of the form $x^2\equiv a \pmod{p}$, $x^2+bx+c\equiv 0 \pmod{p}$ and any other congruence that can be represented by the form $x^2\equiv a \pmod{p}$.

To solve any congruence $x^2\equiv a \pmod{p}$ using the algorithm $u=x-\frac{p-1}{2}$ and $v=x+\frac{p-1}{2}$, first, make a table of residues for $n=1$ through $n=P-1$; next, use the table and evaluate $\frac{p-1}{2}$ and $(\frac{p-1}{2})^2$; next, write

$$x^2\equiv a \pmod{p} \text{ as } x^2-(\tfrac{p-1}{2})^2\equiv a_1 \pmod{p}$$

where $(\frac{p-1}{2})^2+a_1\equiv a \pmod{p}$; next, set $u^2-u-a_1=0$ and solve for u;

and then, subetitute in $u=x-(\frac{p-1}{2})$ and solve for x.

Applications.

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

Solution: $\frac{p-1}{2} = 11$, $(\frac{p-1}{2})^2 = 6$,

$u=x-11$, and $v=x+11$.

$x^2\equiv 2 \pmod{23}$

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

$u^2 - u - 19 = 0$

$u = \frac{1\pm\sqrt{1+76}}{2} = \frac{1\pm\sqrt{77}}{2}$

$= \frac{1\pm\sqrt{8}}{2}$

(A)

To find the $\sqrt{8}$ set

$x_1^2\equiv 8 \pmod{23}$

$x_1^2 - 6 \equiv 2 \pmod{23}$

$u_1^2 - u_1 - 2 = 0$

$(u_1+1)(u_1-2)=0$

$\therefore u_1 = 2$

$u_1 = x_1 - 11 \rightarrow 2 = x_1 - 11 \rightarrow x_1 = 13$ 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

$x = 11+17 = 28 \equiv 5 \pmod{23}$.

x	$x^2 \pmod{23}$
1	1
2	4
3	9
4	16
5	2
6	13
7	3
8	18
9	12
10	8
(11	6)
12	6
13	8
14	12
15	18
16	3
17	13
18	2
19	16
20	9
21	4
22	1

$\therefore$ x≡5 is a solution and p - x

≡13 is also a solution.

*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 (mod 23). Two times 12 is congruent to 1 (mod 23); therefore, 11 (1/2) is equal to 11 (1^2) (mod 23).

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

$\frac{p-1}{2} = 6$, $(\frac{p-1}{2})^2 = 10$, u=x - 6, v=x + 6

$x^2 \equiv 3 \pmod{13}$

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

$u^2 - u - 6 = 0$

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

$u = \frac{1 \pm \sqrt{12}}{2}$

To find $\sqrt{12}$

$x_1^2 \equiv 12 \pmod{13}$

$x_1^2 - 10 \equiv 2 \pmod{13}$

$u_1^2 - u_1 - 2 = 0$

$(u_1 - 2)(u_1 + 1) = 0$

$u_1 = 2$, $u_1 = x_1 - 6 \rightarrow x_1 = 8$

substituting to find u

$u = \frac{1 + 8}{2} = 9\,(1/2) = 9\,(7) = 63 \equiv 11 \pmod{13}$

$u = x - 6 \rightarrow 11 = x - 6$, $x = 17 \equiv 4 \pmod{13}$

$\therefore$ x=4 is a solution also P - x = 9 is a solution.

x	$x^2 \pmod{13}$
1	1
2	4
3	9
4	3
5	12
(6	10)
7	10
8	12
9	3
10	9
11	4
12	1

To use the algorithm to solve a congruence of the form $x^2 + bx + c \equiv 0 \pmod{p}$, we must first change $x^2 + bx + c = 0$ into the form $x^2 \equiv a \pmod{p}$. Let $x = y - \frac{b}{2}$ then $x^2 + bx + c = 0$ becomes

$$(y-\tfrac{b}{2})^2 + b(y-\tfrac{b}{2}) + c = 0 \text{ or}$$

$$y^2 - by + \frac{b^2}{4} + by - \frac{b^2}{2} + c = 0$$

$$y^2 - \frac{b^2}{4} + c = 0$$

$$y^2 \equiv \frac{b^2}{4} - c.$$

Example: Solve $x^2 + 16x + 5 \equiv 0 \pmod{23}$ using the algorithm

$u = x - \frac{p-1}{2}$ and $v = x + \frac{p-1}{2}$.

Solution: $u = y - 11$, $v = y + 11$, $x = y + 15$, $y^2 \equiv 13$

$y^2 \equiv 13 \pmod{23}$

$y^2 - 6 \equiv 7 \pmod{23}$

$u^2 - u - 7 = 0$

$$u = \frac{1 \pm \sqrt{1 + 28}}{2} = \frac{1 \pm \sqrt{29}}{2}$$

$$= \frac{1 \pm \sqrt{6}}{2}$$

$$u = \frac{1 + 11}{2} = 6$$

$u = y - 11 \rightarrow y = 17$

$x = y + 15 \rightarrow x = 17 + 15 \equiv 9 \pmod{23}$

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

is also a root.

x	$x^2 \pmod{23}$
1	1
2	4
3	9
4	16
5	2
6	13
7	3
8	18
9	12
10	8
11	6

Example: Solve $x^2 + 8x \equiv -17 \pmod{37}$ using the algorithm.

$x^2 + 8x \equiv -17 \pmod{37}$

Substituting:

$x = y - 4, \quad y^2 \equiv 36$

$u = y - 18, \quad v = y + 18$

$y^2 \equiv 36 \pmod{37}$

$y^2 - 28 \equiv 8 \pmod{37}$

$u^2 - u - 8 = 0$

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

$$u = \frac{1 + 25}{2} = 13$$

$13 = y - 18 \rightarrow y = 31$

$x = y - 4 \rightarrow x = 31 - 4$

$\therefore x = 27$ is a solution.

To find the second solution

$$u = \frac{1 - 25}{2} = \frac{1 + 12}{2}$$

$= 13\,(1/2) = 13\,(19) = 247 \equiv 25 \pmod{37}$

$25 = y - 18 \rightarrow y = 43 \equiv 6$

$x = y - 4 \rightarrow x = 4 - 6$

$\therefore x = 2$ is a solution.

x	$x^2 \pmod{37}$
1	1
2	4
3	9
4	16
5	25
6	36
7	12
8	27
9	7
10	26
11	10
12	33
13	21
14	11
15	3
16	34
17	30
(18	28)
19	28
20	30
21	34
22	3
23	11
24	21
25	33
26	10
27	26
28	7
29	27
30	12
31	36
32	25
33	16
34	9
35	4
36	1

Solve $x^4 + 6x^3 - 17x^2 - 6x \equiv -16 \pmod{41}$

$\frac{p-1}{2} = 20$, $u = x - 20$, $v = x + 20$.

factoring

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

$x^2 \equiv 1 \pmod{41}$

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

$u^2 - u - 11 = 0$

$u = \frac{1 \pm \sqrt{1 + 44}}{2} = \frac{1 \pm \sqrt{4}}{2} = \frac{1 + 39}{2} = 20$

$20 = x - 20$

$\therefore x = 40$ is a solution.

$x = 1$ is also a solution.

$x^2 + 6x - 16 \equiv 0 \pmod{41}$ $\quad x = y - 3$

$y^2 \equiv 25 \pmod{41}$ $\quad y^2 \equiv 25$

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

$u^2 - u - 35 = 0$

$u \quad \frac{1 \pm \sqrt{1 + 140}}{2} \quad \frac{1 \pm \sqrt{18}}{2} \quad \frac{1 \pm 31}{2}$

$u = \frac{1 + 31}{2} = 16$ and

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

$16 = y - 20$ and $26 = y - 20$

$x = y \Theta 3$ therefore

$x = 36 - 3$ and $x = 46 - 3$

$\therefore$ $x = 33$ and $x = 2$ are solutions.

x	$x^2 \pmod{41}$
1	1
2	4
3	9
4	16
5	25
6	36
7	8
8	23
9	40
10	18
11	39
12	21
13	5
14	32
15	20
16	10
18	37
19	33
20	31

The four roots of the congruence are $x \equiv 1, 2, 33,$ and 40.

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

$\frac{p-1}{2} = 26$, $u = x - 26$, $v = x + 26$

$x^4 - 7x^2 + 12 \equiv 0 \pmod{53}$

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

$x^2 \equiv 4 \pmod{53}$

$x^2 - 40 \equiv 17 \pmod{53}$

$u^2 - u - 17 = 0$

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

$u = \frac{1 \pm 49}{2} = 25$

$25 = x - 26$

$\therefore x = 51$ and $x = 2$.

* $x^2 - 3 \equiv 0 \pmod{53}$

$x^2 \equiv 3 \pmod{53}$

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

$u^2 - u - 16 = 0$

$u = \frac{1 \pm \sqrt{1 + 64}}{2} \quad \frac{1 \pm \sqrt{12}}{2}$

x	$x^2 \pmod{53}$
1	1
2	4
3	9
4	16
5	25
6	36
7	49
8	11
9	28
10	47
11	15
12	38
13	10
14	37
15	13
16	44
17	24
18	6
19	43
20	29
21	17
22	7
23	52
24	46
25	42
26	40

* This particular congruence has no integral solution because 12 is not a quadratic residue mod 53.

Therefore, the two roots of this congruence is $x = 2$ and $x = 51$.

Solve $x^4 + x^3 - 11x^2 - 9x \equiv -18 \pmod{67}$

$u = x - 33$, $v = x + 33$, $\frac{p-1}{2} = 33$

$x^4 + x^3 - 11x^2 - 9x + 18 \equiv 0 \pmod{67}$

$(x^2 - 9)(x^2 + x - 2) \equiv 0 \pmod{67}$

$x^2 \equiv 9 \pmod{67}$

$x^2 - 17 \equiv 59 \pmod{67}$

$u^2 - u - 59 = 0$

$u = \frac{1 \pm \sqrt{1 + 236}}{2} \quad \frac{1 \pm 61}{2}$

$u = \frac{1 + 61}{2} = 31$ and

$u = \frac{1 - 61}{2} = -30 = 37$

$31 = x - 33$ and $37 = x - 33$

$\therefore x = 64$ and $x = 3$

$x^2 + x - 2 \equiv 0 \pmod{67}$ $\quad x = y - 34$

$y^2 \equiv 19 \pmod{67}$ $\quad y^2 = 19$

$y^2 - 17 \equiv 2 \pmod{67}$ $\quad u = y - 33$

$u^2 - u - 2 = 0$

$(u - 2)(u + 1) = 0$

$\therefore u = 2$ and $u = -1$

$2 = y - 33$ and $-1 = y - 33$

$y = 35$ and $y = 32$

$x = y - 34$ so

$x = 35 - 34$ and $x = 32 - 34$

$x = 1$ and $x = -2 = 65$

The four roots are $x = 1, 3, 64$ and 65.

x	$x^2 \pmod{67}$
1	1
2	4
3	9
4	16
5	25
6	36
7	49
8	64
9	14
10	33
11	54
12	10
13	35
14	62
15	24
16	55
17	21
18	56
19	26
20	65
21	39
22	15
23	60
24	40
25	22
26	6
27	59
28	47
29	37
30	29
31	23
32	19
33	17

Solve $x^2 + 4x \equiv 12 \pmod{73}$

$u = y - 36$, $v = y + 36$

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

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

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

$u^2 - u - 34 = 0$

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

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

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

$u = y - 36$

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

$y = 69$ and $y = 77 = 4$

$x = y - 2$

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

$x = 67$ and $x = 2$

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

x	$x^2 \pmod{73}$
1	1
2	4
3	9
4	16
5	25
6	36
7	47
8	64
9	8
10	27
11	48
12	71
13	23
14	50
15	6
16	37
17	70
18	32
19	69
20	35
21	3
22	46
23	18
24	65
25	41
26	19
27	72
28	54
29	38
30	24
31	12
32	2
33	67
34	61
35	57
36	55

Solve $x^6 + 8x^5 + 10x^4 - 40x^3 - 71x^2 - 32x + 60 \equiv 0 \pmod{83}$

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

$x^2 \equiv 4 \pmod{83}$ $\quad \frac{p-1}{2} = 41$

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

$u^2 - u - 66 = 0$

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

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

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

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

$u^2 - u - 63 = 0$

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

$u = y - 41$

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

$y = 82$ and $y = 1$

x	$x^2 \pmod{83}$
1	1
2	4
3	9
4	16
5	25
6	36
7	49
8	64
9	81
10	17
11	38
12	61
13	3
14	30
15	59
16	7
17	40
18	75
19	29
20	68
21	26
22	69
23	31
24	78
25	44
26	12
27	65
28	37
29	11
30	70
31	48
32	28
33	10
34	77
35	62
36	51
37	41
38	33
39	27
40	23
41	21

$x = y \neq 4$

$x - 86 = 3 \qquad x = 5$

The six solutions are $x = 1, 2, 3, 5, 81$, and 82.

Solve $x^6 - 10x^5 + x^4 - 200x^3 - 356x^2 \equiv -1344 \pmod{97}$

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

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

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

$u^2 - u - 28 = 0$

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

$47 = x - 48$ and $51 = x - 48$

$\therefore x = 95$ and $x = 99 \equiv 2$

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

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

$u^2 - u - 40 = 0$

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

$45 = x - 48$ and $53 = x - 48$

$\therefore x = 93$ and $x = 101 \equiv 4$

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

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

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

$u^2 - u - 28 = 0$

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

$u = y - 48$

$47 = y - 48$ and $51 = y - 48$

$y = 95$ and $y = 99 \equiv 2$

$x = y + 5$ $\quad \therefore x = 3$ and $x = 7$

x	$x^2 \pmod{97}$
1	1
2	4
3	9
4	16
5	25
6	36
7	49
8	64
9	81
10	3
11	24
12	47
13	72
14	2
15	31
16	62
17	95
18	33
19	70
20	12
21	53
22	96
23	44
24	91
25	43
26	94
27	50
28	8
29	65
30	27
31	88
32	54
33	22
34	89
35	61
36	35
37	11
38	86
39	66
40	48
41	32
42	18

The six solutions are $x = 2$, 3, 4, 7, 93, and 95.

43	6
44	93
45	85
46	79
47	75
48	73

Bibliography

1. E. Cahen, Theorie des Nombres, Vol. II, Paris, A. Herman et F'ils, 1924.

2. L. E. Dickerson, History of the Theory of Numbers, Vol. II, New York, G. E. Stechert and Company, 1934.

3. W. J. LeVeque, Topics in Number Theory, Reading, Addison-Wesley Publishing Company, 1956.

4. I. Niven and H. Zuckerman, An Introduction to the Theory of Numbers, New York, John Wiley and Sons, Incorporated, 1960.

5. J. V. Uspensky and M. A. Heaslet, Elementary Number Theory, New York, McGraw - Hill Company, 1934.