Digitized by the Internet Archive
in 2013

http://archive.org/details/congruencesinnum00nebe
CONGRUENCES IN NUMBER THEORY

BY

DORA MYRTLE NEBEL

B. A. University of Illinois, 1914

THESIS

Submitted in Partial Fulfillment of the Requirements for the

Degree of

MASTER OF ARTS

IN MATHEMATICS

IN

THE GRADUATE SCHOOL

OF THE

UNIVERSITY OF ILLINOIS

1914
UNIVERSITY OF ILLINOIS
THE GRADUATE SCHOOL

JUNE 2, 1914

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

DORA MYRTLE NEBEL

ENTITLED CONGRUENCES IN NUMBER THEORY

BE ACCEPTED AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF ARTS

In Charge of Major Work

Head of Department

Recommendation concurred in:

Committee on Final Examination

284618
TABLE OF CONTENTS.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. An Historical Introduction</td>
<td>1</td>
</tr>
<tr>
<td>II. Some Theorems Relating to Binomial Congruences</td>
<td>6</td>
</tr>
</tbody>
</table>
Bibliography.

Ball: A Short History of Mathematics.


Henry Smith: Transactions of British Association, 1859-1865.


Reid: The Elements of the Theory of Algebraic Numbers.

CONGRUENCES IN NUMBER THEORY.

CHAPTER I.

AN HISTORICAL INTRODUCTION TO THE THEORY OF CONGRUENCES.

The first part of this paper will deal with an historical introduction to Congruences and their place in Number Theory. The second part will treat certain theorems on some special congruences propounded by Dr. Gustaf Wahlin of the Mathematics Department of the University of Illinois.

Number theory is one of the oldest branches of mathematics, for we read in the history of Pythagoras that in number theory, he was chiefly concerned with four different classes of problems which dealt with polygonal numbers, with rational proportion, with the factors of numbers, and with numbers in series. He used geometrical methods in treating many of his arithmetical inquiries. In Euclid's Elements books seven, eight, nine and ten are devoted to the theory of numbers. The science of numbers as it was called had special reference to ratio, proportion, and the theory of numbers. In book seven the greatest common measure of two numbers, and the least common multiple of numbers are discussed, and many theorems on prime numbers which are found in modern text books on algebra, are given.

In the eighth and ninth book he treats of numbers in geometrical progression and proves the rule for the summation of a series of \( n \) terms, although the proof is limited to the case where \( n \) is four. He also shows that the number of primes is infinite and discusses the properties of odd and even numbers. The tenth book deals with irrational magnitudes.**

*Ball, A Short History of Mathematics, pp. 24-25.
**Ball, Short History, pp. 58-60.
The next early mathematician of note to add to number theory was Dio-
phantes who gives in his arithmetic such theorems as the following: the
difference of the cubes of two numbers can always be expressed as the sum
of the cubes of two other numbers; no number of the form $4n-1$ can be ex-
pressed as the sum of two squares; and no number of the form $8n-1$ can be
expressed as the sum of three squares.*

Nothing new was added to the theory of numbers until the seventeenth
century when Fermat gave his famous theorem: If $p$ be a prime and $a$ prime
to $p$ then $a^{p-1}-1$ is divisible by $p$. The proof of this is due to Euler.
This was the beginning to an awakening to the broadness of the field in
number theory and from this time on to the present day great strides have
been made in its development. Such men as Euler, Lagrange, Legendre,
Gauss, Jacobi, Dirichlet, Eisenstein, Henry Smith, Kummer, Dedekind, Kro-
necke, Georg Cantor, and others have been interested in Number Theory
and have contributed to its development. And yet the statement of Gauss
made in 1847 in regard to number theory still holds true: "The higher
arithmetic presents us with an inexhaustible store of interesting truths
which are not isolated, but stand in a close internal connection, and be-
tween which, as our knowledge increases, we are continually discovering
new and sometimes wholly unexpected ties. A great part of its theory de-
rives an additional charm from the peculiarity that important propositions
with the impress of simplicity upon them are often discoverable by induc-
tion, and yet are so profound in character that we cannot find their de-
monstration until after many vain attempts; and even then, when we do
succeed, it is often by some tedious and artificial process, while the

* Ball, Short History, pp. 109-110.
Eisenstein divided number theory into two main divisions: the theory of congruences and the theory of forms. The theory of congruences relates to the solution of indeterminate equations of the form

\[ a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = Py \]

in which \( a_n, a_{n-1}, \ldots, a_1, a_0 \) and \( P \) are given integers and \( x \) and \( y \) are unknown numbers. The theory of forms relates to the solution of indeterminate equations of the form \( F(x_1, x_2, \ldots, x_m) = N \), in which \( N \) is a given integral number, and \( F \) is an homogeneous function of any order, with integral coefficients. Gauss discussed both of these divisions in his *Disquisitiones Arithmeticae*.

It is with the theory of congruences that we shall be especially interested in this paper. "The idea of a congruence, that it involves only one of the most elementary arithmetical conceptions, that of division," says Henry Smith in his report on number theory. If \( a \) minus \( b \) is divisible by \( m \), then we say that \( a \) is congruent to \( b \) with respect to the modulus \( m \) and write

\[ a \equiv b, \text{ mod } m. \]

This notation is due to Gauss. From the form of the expression and the definition of a congruence we see that this can be written in the form of an equation; and hence we conclude that the rules of addition, subtraction, multiplication, and division may with a little modification be applied. We may note also, that a congruence of the form

\[ \varphi(x) \equiv 0, \text{ mod } m, \]

where \( \varphi(x) \) is a rational integral function of \( x \) with integral coefficients.

has a set of solutions, rather than a single solution. If \( x = a \) is a solution it is evident that \( x = a + my \) is also a solution. However these solutions are all congruent to each other.

Euler defined the set of numbers less than \( m \), which are incongruent each to each with respect to the modulus \( m \), as a complete residue system. He called those incongruent numbers less than and prime to \( m \) a reduced residue system. Gauss designated the number of numbers in such a system by the function \( \varphi(m) \). The general expression for \( \varphi(m) \) is due to Euler.

A congruence of the form

\[
ax + b \equiv 0 \pmod{m},
\]

has been defined as a linear congruence. The theory of linear congruences may be considered complete, both in the determination of roots and the number of roots. Gauss left the solution of a set of linear congruences incomplete but the work has been completed with the aid of determinants.

Fermat's theorem, which has been given, leads to a study of congruences of a higher order. The theory of these is not complete. Conditions have been given for their solution but are of little practical value. Euler's criterion is perhaps the most practical necessary and sufficient condition which has been given. The study of binomial congruences leads to the study of primitive roots. Smith says that the problem of determining the primitive roots of a prime number is one of the "cruces" of the theory of numbers. Euler gave the first proof of the existence of primitive roots but Gauss gave the first rigorous proof. Tables of indices and the laws of quadratic residues are of great value in the study of binomial congruences. Jacobi in his Canon Arithmeticus gives tables of indices for all prime numbers less than one thousand.
The literature on the theory of numbers is rich. The classical works on the subject are Gauss's *Disquisitiones Arithmeticae* and Legendre's *Théorie des Nombres*.
CHAPTER II.

SOME THEOREMS RELATING TO BINOMIAL CONGRUENCES.

Theorem 1. If \( n \) and \( a \) are two integers relatively prime to \( p \), and if the congruence
\[
x^n \equiv a, \mod p,
\]
has a solution, then the congruence
\[
x^n \equiv a, \mod p^s
\]
has a solution for every rational integral value of \( s \).

Assume that the congruence
\[
x^n \equiv a, \mod p^k
\]
has a solution for \( k=1 \). Let \( A \) be such a solution. Then \( A \) is also relatively prime to \( p \) and there exists a number \( b \) such that the congruence
\[
nA^{n-1}b \equiv a - \frac{A^n}{p^k}, \mod p
\]
is true. (Reid, §9, page 58)

This reduces to
\[
A^n + np^kbA^{n-1} \equiv a, \mod p^{k+1}.
\]

If we expand \((A+p^k b)^n\) we get
\[
(A+p^k b)^n = A^n + np^kbA^{n-1} + \ldots \ldots + p^{k+n}b^n.
\]

We know that
\[
(A+p^k b)^n \equiv A^n + np^kA^{n-1}b, \mod p^{k+1},
\]
because all the terms in the expansion are divisible by \( p^{k+1} \) except the first two. It follows from this that
\[
(A + p^k b)^n \equiv a, \mod p^{k+1};
\]

* Another discussion of this theorem is found in "Rendiconti del Circolo Matematico di Palermo": 1897, vol. 11, page 4S. "Sulla Risoluzione della Congruenza \( x^{2^k} \equiv b \pmod{p^k} \). Nota del Dr. Nicola Amici, in Monte- cassino.
and \( x = a + p^k b \) is a solution of the congruence
\[
x^n \equiv a, \mod p^{k+1}.
\]
By inductive reasoning it follows that if the congruence
\[
x^n \equiv a, \mod p
\]
has a solution, then the congruence
\[
x^n \equiv a, \mod p^s
\]
has a solution for every rational integral value of \( s \).

**Theorem 11.** If \( n \) and \( a \) are two integers and \( a \) is relatively prime to \( p \), and if the congruence
\[
x^p \equiv a, \mod p^{n+2}
\]
has a solution \( A \), then the congruence
\[
x^p \equiv a, \mod p^{n+1}
\]
has a solution for arbitrary \( i \).

Suppose that the congruences
\[
A^p \equiv a, \mod p^{n+k}
A^p \not\equiv a, \mod p^{n+k+1}
\]
are true for \( k > 1 \). Then there exists a number \( b \) such that
\[
\frac{A^p}{p^{n+k}} - 2 \equiv -A^{p-1}b, \mod p.
\]
This reduces to
\[
A^p + A^{p-1}bp^{n+k} \equiv a, \mod p^{n+k+1}
\]
In the expansion of \((A+p^k)^p\) the power of \( p \) in the general term is
\[
\frac{p^n - 1 - i + S_i - p^n + i + S_{p-1} + k}{p - 1}
\]
which reduces to
\[
\frac{S_i + S_{n-1} - 1}{p - 1}; \quad \text{Hensel: Zahlentheorie, chap. 8.}
\]
But if \( i = a_v p^v + a_{v+1} p^{v+1} + \ldots + a_{n-1} p^{n-1} \) then \( p^n - i = (p - a_v)p^v + \ldots \).
\[(p - 1 - a_{v+1})p^{v+1} + \ldots + (p - 1 - a_{n-1})p^{n-1},\] where \(p^v\) is the highest power of \(p\) in the integer \(i\).

\[S_i = \sum_{i=1}^{n} a_i,\]

\[S_{p^{n-1}} = p(n - v) - (n - v - 1) - S_1,\]

\[\frac{S_i + S_{p^{n-1}} - 1}{p - 1} = n - v.\]

Therefore the power of \(p\) in the \(i\)th term in the above expansion is

\[n - v + ik \geq n - v + p^v k \]

\[= n + k + v(k - 1)\]

\[p^v \geq 2^v = (1+1)^v = 1 + v + \ldots \geq 1 + v.\]

Since \(k\) is an integer greater than one, it must be equal to or greater than two and hence \(k - 1 \geq 1\). Therefore

\[n - v + ik \geq n + k + 1.\]

Therefore the power of \(p\) in the \(i\)th term is greater than or at least equal to \(n + k + 1\). In the last term the power of \(p\) is \(k\)\(p^n\) which is greater than \(n + k\); from which it follows that

\[kp^n \geq n + k + 1.\]

Therefore

\[(A + b_0k)p^n \equiv A^p + A^{p-1}b_0^n + k, \mod p^{n+k+1}.\]

But we have seen that

\[A^p + A^{p-1}b_0^n + k \equiv a, \mod p^{n+k+1}.\]

From this it follows that

\[(A + b_0k)p^n \equiv a, \mod p^{n+k+1}\]

and

\[x = (A + b_0k)\]

is a solution of the congruence

\[xp^n \equiv a, \mod p^{n+k+1},\]

where \(A\) is a solution of the congruence.
\[ x^{p^n} \equiv a, \mod p^{n+k}. \]

By mathematical induction it follows that the congruence
\[ x^{p^n} \equiv a, \mod p^{n+1} + 1 \]
has a solution for every \( i > 1 \) if it has a solution for \( i = 1 \).

It is evident that the conditions of these two theorems are both necessary and sufficient. Furthermore, the nature of the proof is such that it furnishes a method for the computation of a solution of the congruence \( x^n \equiv a, \mod p^{k+1} \), in the first case, and of \( x^{p^n} \equiv a, \mod p^{n+k+1} \) in the second case, when the solutions are known for the moduli \( p^k \) and \( p^{n+k} \) respectively.

The results of these two theorems can be expressed by the following recursive formulae:

Case I (Theorem I).

Let \( A_k \) be a solution of the congruence
\[ x^n \equiv a, \mod p^k, \]
and \( A_{k+1} \) be a solution of the congruence
\[ x^n \equiv a, \mod p^{k+1}. \]

Then
\[ A_{k+1} \equiv A_k + a - \frac{A_k^{p^n}}{p^n + 1}, \mod p^{k+1} \]
since \( n \) and \( A \) are relatively prime to \( p \).

Case II (Theorem II).

Let \( A_{k+1} \) be a solution of
\[ x^{p^n} \equiv a, \mod p^{n+k+1}, \; k > 1, \]
and \( A_k \) a solution of
\[ x^{p^n} \equiv a, \mod p^{n+k}. \]

Then
\[ A_{k+1} \equiv A_k + a - \frac{A_k^{p^n}}{p^n + 1}, \mod p^{k+1}. \]

These two recursive formulae are of the same form in \( a, A_k \) and the expo-
Furthermore, we observe that if

\[ c \equiv d, \mod p^{k+1} \]

then

\[ c = d + kp^{k+1} \]

and

\[ c^{p^n} = d^{p^n} + \ldots. \]

In the same way as above it can be shown that all the terms following \( d^{p^n} \) are divisible by \( p^{n+k+1} \) and hence all numbers given by these formulae are solutions.

**Theorem III.** The necessary and sufficient condition that the congruence

\[ x^n \equiv a, \mod m \]

shall have a solution is that

\[ \Phi(p_i) \quad a \equiv 1, \mod p_i; \quad (i=1,2,\ldots,r) \]

where \( n \) and \( a \) are relatively prime to \( m \); where \( m=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_r^{\alpha_r} \); and where \( \delta_i \) is the greatest common divisor of \( n \) and \( p_i-1 \).

From Euler's criterion we know that the congruence

\[ x^n \equiv a, \mod p_i \]

has a solution \( A_i \) when and only when

\[ a^{p_i-1} \equiv 1, \mod p_i. \]

If the congruence

\[ x^n \equiv a, \mod m \]

has a solution then

\[ x^n \equiv a, \mod p_i \]

also has a solution and therefore

\[ a^{p_i-1} \equiv 1, \mod p_i. \]

Therefore the condition is necessary. Conversely if

\[ a^{p_i-1} \equiv 1, \mod p_i \quad \text{for} \quad i=1,2,\ldots,r, \]

then the congruence

\[ x^n \equiv a, \mod p_i \quad (i=1,2,\ldots,r) \]

has a solution. By theorem I we know that the congruence

\[ x^n \equiv a, \mod p_i^{\alpha_i} \]
has a solution. If we denote this solution by $A_i$ and let $c_i$ be a rational integer such that
\[ c_i \equiv 0, \mod p_i^{a_i} \quad \text{for } j \neq i \]
and
\[ c_i \equiv 1, \mod p_i^{a_i} \]
then
\[ A = \sum_{i=1}^{r} c_i A_i \]
is an integer such that $A \equiv A_i, \mod p_i^{a_i}$

From this it follows that $A^n \equiv a, \mod p_i^{a_i}, (i=1,2,3,\ldots,r)$.

This says that $A^n-a$ is divisible by $p_1^{a_1}, p_2^{a_2}, \ldots, p_r^{a_r}$ and therefore it must be divisible by $m$.

\[ A^n \equiv a, \mod m. \]

Hence the given condition is sufficient.

**Theorem IV.** The necessary condition that
\[ x^{p^{n+k+1}} \equiv a, \mod p^{n+k+1} \]
shall have a solution for $k$ greater than one is that the congruence
\[ a^{p-1} \equiv 1, \mod p^{n+1} \]
shall have a solution.

Suppose
\[ x^{p^{n+k+1}} \equiv a, \mod p^{n+k+1} \quad (1) \]
has a solution. By a previous theorem we have seen that the necessary and sufficient condition for (1) to have a solution is that
\[ x^{p^{n}} \equiv a, \mod p^{n+2} \quad (2) \]
shall have a solution. If we raise both sides of equation (2) to the $(p-1)^{th}$ power we get
\[ x^{p^{n}(p-1)} \equiv a^{p-1}, \mod p^{n+2}. \]

But
\[ \varphi(p^{n+1}) = p^n(p-1). \]

Hence
\[ x^{p^{n}(p-1)} \equiv 1, \mod p^{n+1} \quad \text{[Fermat's theorem]} \]
and hence
\[ a^{p-1} \equiv 1, \mod p^{n+1}. \]
Therefore a necessary condition is that

\[ a^{p-1} \equiv 1, \mod p^{n+1} \]

shall have a solution.