ELEMENTARY NUMBER THEORY

BY

EDMUND LANDAU

TRANSLATED BY

JACOB E. GOODMAN
Columbia University

WITH EXERCISES BY

PAUL T. BATEMAN
Professor of Mathematics
University of Illinois

AND

EUGENE E. KOHLBECKER
Asst. Professor of Mathematics
University of Utah

CHELSEA PUBLISHING COMPANY
NEW YORK, N. Y.

THE PRESENT WORK IS A TRANSLATION INTO ENGLISH, BY JACOB E. GOODMAN, OF THE GERMAN-LANGUAGE WORK ELEMENTARE ZAHLENTHEORIE (VOL. I_1 OF VORLESUNGEN UEBER ZAHLENTHEORIE), BY EDMUND LANDAU, WITH ADDED EXERCISES BY PAUL T. BATEMAN AND E. E. KOHLBECKER

LIBRARY OF CONGRESS CATALOGUE CARD NO. 57-8494

PRINTED IN THE UNITED STATES OF AMERICA

CONTENTS

PART ONE

Foundations of Number Theory

CHAPTER I: The Greatest Common Divisor of Two Numbers.... 11

CHAPTER II: Prime Numbers and Factorization into Prime Factors 18

CHAPTER III: The Greatest Common Divisor of Several Numbers.. 26

CHAPTER IV: Number-Theoretic Functions 29

CHAPTER V: Congruences 37

CHAPTER VI: Quadratic Residues 53

CHAPTER VII: Pell's Equation 76

PART TWO

Brun's Theorem and Dirichlet's Theorem

Introduction 87

CHAPTER I: Some Elementary Inequalities of Prime Number Theory 88

CHAPTER II: Brun's Theorem on Prime Pairs................. 94

CHAPTER III: Dirichlet's Theorem on the Prime Numbers of an Arithmetic Progression 104

§ 1: Further Theorems on Congruences 104

§ 2: Characters 109

§ 3: *L*-Series 115

§ 4: Dirichlet's Proof 125

PART THREE

Decomposition into Two, Three, and Four Squares

Introduction 129

CHAPTER I: Farey Fractions 131

CHAPTER II: Decomposition into Two Squares.............. 135

CHAPTER III: Decomposition into Four Squares 141
Introduction 141
§ 1: Lagrange's Theorem 142
§ 2: Determination of the Number of Solutions. 146
CHAPTER IV: Decomposition into Three Squares 151
§ 1: Equivalence of Quadratic Forms......... 151
§ 2: A Necessary Condition for Decomposability into Three Squares 161
§ 3: The Necessary Condition is Sufficient..... 162

PART FOUR

The Class Number of Binary Quadratic Forms

Introduction 167
CHAPTER I: Factorable and Unfactorable Forms 170
CHAPTER II: Classes of Forms 172
CHAPTER III: The Finiteness of the Class Number............... 175
CHAPTER IV: Primary Representations by Forms 180
CHAPTER V: The Representation of $h(d)$ in terms of $K(d)$ 191
CHAPTER VI: Gaussian Sums 197
Appendix 202
Introduction 202
§ 1: Kronecker's Proof 203
§ 2: Schur's Proof 207
§ 3: Mertens' Proof 213
CHAPTER VII: Reduction to Fundamental Discriminants........... 219
CHAPTER VIII: The Determination of $K(d)$ for Fundamental Discriminants 221
CHAPTER IX: Final Formulas for the Class Number............. 227

APPENDIX

Exercises

Exercises for Part One 233
Exercises for Part Two 242
Exercises for Part Three 247
INDEX OF CONVENTIONS; INDEX OF DEFINITIONS.................. 253
INDEX 254

CHAPTER I

THE GREATEST COMMON DIVISOR OF TWO NUMBERS

Until further notice, lower case italic letters will always represent integers, i.e.

$1, \quad 2, \quad 3, \ldots$ (positive integers or natural numbers),
0 (zero),
$-1, -2, -3, \ldots$ (negative integers).

The following facts will be used constantly: If a is an integer, then so are $-a$ and $|a|$; if a and b are integers, then so are $a+b$, $a-b$, and ab; if $a>b$, then $a \geqq b+1$; and if $a<b$, then $a \leqq b-1$.

Definition 1: *Let $a \neq 0$; let b be arbitrary. Then b is said to be divisible by a if there exists a number q such that*

$$b=qa.$$

This q, namely $q=\frac{b}{a}$, is then uniquely determined.

We also say that: b is a multiple of a, a is a divisor of b, a divides b, or a goes into b. In symbols,

$$a/b$$

If $a \neq 0$ and b is not divisible by a, then we write

$$a \nmid b.$$

Examples: $2/6$, $4 \nmid 6$, $3 \nmid 4$, $2/-4$,
$a/0$ for every $a \neq 0$,
$1/a$ and $-1/a$ for every a,
a/a and $a/-a$ for every $a \neq 0$.

Theorem 1: *If a/b, then*

$$a/-b, \quad -a/b, \quad -a/-b, \quad |a|\,/\,|b|.$$

Proof: By hypothesis we have $b=qa$; furthermore $a \neq 0$, and therefore $-a \neq 0$ and $|a| \neq 0$. It follows that

$$-b=(-q)a, \quad b=(-q)(-a), \quad -b=q(-a), \quad |b|=|q|\,|a|.$$

Theorem 2: *If $a|b$ and $b|c$, then $a|c$.*

This is also expressed as follows: Divisibility is transitive.

Proof: By hypothesis $a \neq 0$, and there exist two numbers q_1, q_2 for which

$$b=q_1 a, \quad c=q_2 b.$$

From this it follows that

$$c=q_2 q_1 \cdot a.$$

Theorem 3: 1) *If $ac|bc$, then $a|b$.*

2) *If $a|b$ and $c \neq 0$, then $ac|bc$.*

Proof: 1) Since $ac \neq 0$, we have $a \neq 0$ and $c \neq 0$. Moreover, $bc=qac$; hence $b=qa$.

2) Since $a \neq 0$, we have $ac \neq 0$. Moreover $b=qa$; hence $bc=qac$.

Theorem 4: *If $a|b$, then $a|bx$ for every x.*

Proof: $b=qa$, $bx=qx \cdot a$.

Theorem 5: *If $a|b$ and $a|c$, then $a|(b+c)$ and $a|(b-c)$.*

Proof: $b=q_1 a$, $c=q_2 a$, $b \pm c=(q_1 \pm q_2)a$.

Theorem 6: *If $a|b$ and $a|c$, then $a|(bx+cy)$ for any x and y.*

Proof: By Theorem 4,

$$a|bx, \quad a|cy;$$

therefore, by Theorem 5,

$$a|bx+cy.$$

Theorem 7: *If $a>0$ and b is arbitrary, then there is exactly one pair of numbers q and r such that*

$$(1) \qquad b=qa+r, \quad 0 \leqq r < a.$$

($r=0$ corresponds to the case $a|b$.)

"Dividend = (incomplete) quotient times the divisor + remainder,
0 ≦ remainder < divisor."

Proof: 1) I first show that (1) has at least one solution.

Among all the numbers of the form $b-ua$ there occur negative and positive ones (namely, for sufficiently large positive u and for negative u having sufficiently large absolute value, respectively). The smallest non-negative number $b-ua$ occurs for $u=q$. If I set

$$b-qa=r,$$

then

$$r=b-qa\geqq 0,\ r-a=b-(q+1)a<0,$$

so that (1) is satisfied.

2) The proof of uniqueness goes as follows: If (1) holds and if $u<q$, then

$$u\leqq q-1,\ b-ua\geqq b-(q-1)a=r+a\geqq a;$$

if (1) holds and if $u>q$, then

$$u\geqq q+1,\ b-ua\leqq b-(q+1)a=r-a<0.$$

The desired relations

$$0\leqq b-ua<a$$

thus hold only when $u=q$.

THEOREM 8 (for $g=10$ this is the familiar representation of a in the decimal system): *Let* $g>1$. *Then any number* $a>0$ *can be expressed in one and only one way in the form:*

$$a=c_0+c_1g+\cdots+c_ng^n,\ n\geqq 0,\ c_n>0,\ 0\leqq c_m<g \textit{ for } 0\leqq m\leqq n.$$

Proof: 1) I first prove the *existence* of such a representation (using mathematical induction).

For $a=1$, the existence is obvious ($n=0$, $c_0=1$, $0<c_0<g$).

Let $a>1$, and assume the assertion true for $1, 2, \ldots, a-1$. a belongs to one of the intervals $1\leqq a<g$, $g\leqq a<g^2$, $g^2\leqq a<g^3$, ... (ad infinitum). Hence there is some $n\geqq 0$ for which $g^n\leqq a<g^{n+1}$. By Theorem 7, we have

$$a=c_ng^n+r,\ 0\leqq r<g^n.$$

c_n must be >0, since $c_ng^n=a-r>g^n-g^n=0$; in addition, $c_n<g$, since $c_ng^n\leqq a<g^{n+1}$.

If $r=0$, we are finished ($a=0+0\cdot g+\cdots+0\cdot g^{n-1}+c_ng^n$, $0<c_n<g$). If $r>0$, then, since $r<g^n\leqq a$, we have

$$r=b_0+b_1g+\cdots+b_tg^t,\ t\geqq 0,\ b_t>0,\ 0\leqq b_m<g \text{ for } 0\leqq m\leqq t.$$

t must be $<n$, since $g^n>r\geqq b_tg^t\geqq g^t$; therefore

$$a=b_0+b_1g+\cdots+b_tg^t+0\cdot g^{t+1}+\cdots+0\cdot g^{n-1}+c_ng^n.$$

2) The proof of *uniqueness* goes as follows: Let

$$a=c_0+c_1g+\cdots+c_ng^n=d_0+d_1g+\cdots+d_rg^r,\ n\geqq 0,\ c_n>0,\ 0\leqq c_m<g$$

$$(\text{for } 0\leqq m\leqq n),\ r\geqq 0,\ d_r>0,\ 0\leqq d_m<g\ (\text{for } 0\leqq m\leqq r).$$

The assertion is that $n=r$ and that $c_m=d_n$ for $0\leqq m\leqq n$. If this were not so, then, by subtraction, we would have

$$0=e_0+\cdots+e_sg^s,\ s>0,\ e_s\neq 0,\ -g<e_m<g \text{ for } 0\leqq m\leqq s;$$

hence

$$g^s\leqq|e_sg^s|=|e_0+\cdots+e_{s-1}g^{s-1}|\leqq(g-1)(1+\cdots+g^{s-1})=g^s-1.$$

THEOREM 9: *Let $a>0$ and $b>0$. Of all the common multiples of a and b* (there are such multiples, and even positive ones: for example, ab and $3ab$), *let m be the smallest positive one and let n be any of them* $\left(n\gtreqless 0\right)$. *Then*

$$m/n.$$

In words: Every common multiple is divisible by the smallest positive one.

Proof: By Theorem 7, the numbers q and r can be chosen such that

$$n=qm+r,\ 0\leqq r<m.$$

From

$$r=n-qm=n\cdot 1+m(-q)$$

and

$$a/n,\ a/m,\ b/n,\ b/m,$$

it follows by Theorem 6 that

$$a/r,\ b/r.$$

Hence, by the definition of m, r cannot be >0. Therefore

$$r=0,\ n=qm,\ m/n.$$

THEOREM 10: *If $a\neq 0$ and b/a, then*

$$|b|\leqq|a|,$$

so that every $a\neq 0$ has only a finite number of divisors.

Proof: $a=qb$ and $q\neq 0$;

therefore

$$|q|\geqq 1,\ |a|=|q||b|\geqq|b|.$$

THEOREM 11: *Let a and b not both be* 0. *Let d be the greatest common divisor of a and b.* (d exists and is >0; for at least one of the numbers a, b is $\neq 0$ and hence, according to Theorem 10, has only finitely many divisors; and the number 1 is certainly a common divisor of a and b.)

1) *If f is any common divisor of a and b, then*

$$f/d.$$

In words: Every common divisor goes into the greatest common divisor.

2) *If $a>0$, $b>0$, and m is the smallest positive common multiple of a and b, then*

$$md=ab.$$

In particular, then: If $a>0$, $b>0$, and $d=1$, then $m=ab$.

Proof: Case I: Let $a>0$ and $b>0$. Since ab is a common multiple of a and b, then by Theorem 9,

$$m/a\,b,$$

$$\frac{a\,b}{m} \text{ is an integer.}$$

Setting

$$\frac{a\,b}{m}=g,$$

we shall prove the following:

a) that if f/a and f/b, then

$$f/g,$$

b) that

$$g=d$$

(which will prove all our assertions in Case I).

In fact,

a) If f/a and f/b, then

$$a/a\frac{b}{f},\quad b/b\frac{a}{f}.$$

$\frac{a\,b}{f}$ is thus a common multiple of a and b; hence by Theorem 9,

$$m\Big/\frac{a\,b}{f},$$

$$\frac{a\,b}{g}\Big/\frac{a\,b}{f},$$

so that the quotient

$$\frac{a\,b}{f}:\frac{a\,b}{g}=\frac{g}{f}$$

is an integer, and consequently

$$f/g.$$

b) Since

$$\frac{a}{g}=\frac{m}{b},\quad \frac{b}{g}=\frac{m}{a}$$

are integers, we have

$$g/a,\quad g/b;$$

g is thus a common divisor of a and b. Since, by a), every common divisor f of a and b goes into g, and $g>0$, we have by Theorem 10,

$$f \leqq g,$$

so that g is the greatest common divisor of a and b.

Case II: Suppose that the assumption $a>0$, $b>0$ is not satisfied but that a and b are still both $\neq 0$. Then 1) follows from Case I, since a has the same divisors as $|a|$ and b the same divisors as $|b|$. In fact, d is the greatest common divisor not only of a and b but of $|a|$ and $|b|$ as well.

Case III: Let one of the two numbers be 0, say $a=0$, so that $b\neq 0$. Then obviously $d=|b|$, and from $f/0$ and f/b it follows that f/d.

NOTATION: *For any a and b which do not both vanish, the greatest common divisor of a and b is denoted by (a, b).*

Examples: $(4,6)=2$; $(0,-3)=3$; $(-4,-6)=2$; $(1,0)=1$.

THEOREM 12: *If a and b are not both 0, then*

$$(a, b)=(b, a)$$

Proof: The definition of (a, b) is obviously symmetrical in a and b.

DEFINITION 2: *If $(a, b)=1$, that is, if 1 is the only positive common divisor of a and b, then a and b are called relatively prime.*

We also say: a is relatively prime to b. 1 and -1 are then the only common divisors of a and b.

Examples: 1) $(6, 35)=1$, since 6 has 1, 2, 3, and 6 as its only positive divisors, and none of the numbers 2, 3, and 6 goes into 35.

2) $(a, 0)=1$ for $a=1$ and for $a=-1$, but for no other a.

THEOREM 13: *If $(a, b)=d$, then* $\left(\frac{a}{d}, \frac{b}{d}\right)=1$.

Proof: If $f>0$, $f\Big/\frac{a}{d}$, $f\Big/\frac{b}{d}$, then by Theorem 3, 2) we have

$$fd/a,\ fd/b,$$

and therefore by Theorem 11

$$fd/d,$$

so that by Theorem 3, 1)

$$f/1,\ f=1.$$

THEOREM 14: *If $c>0$, c/a, c/b,* $\left(\frac{a}{c}, \frac{b}{c}\right)=1$, *then* $c=(a, b)$.

Proof: Since $\frac{a}{c}$ and $\frac{b}{c}$ do not both vanish, a and b are not both 0. If we set $(a, b)=d$, then c/d by Theorem 11, so that $\frac{d}{c}$ is an integer. From

$$\frac{d}{c}\,\frac{a}{d}=\frac{a}{c},\quad \frac{d}{c}\,\frac{b}{d}=\frac{b}{c}$$

it follows that

$$\frac{d}{c}\Big/\frac{a}{c},\quad \frac{d}{c}\Big/\frac{b}{c},$$

and therefore, since $\left(\frac{a}{c},\ \frac{b}{c}\right)=1$, $d>0$, $c>0$,

$$\frac{d}{c}=1,\quad c=d.$$

THEOREM 15: *If a/bc and $(a, b)=1$, then a/c.*

In words: If a number divides the product of two numbers and is relatively prime to one of them, then it divides the other.

Proof: By assumption, $a\neq 0$.

1) If $b=0$, then $a=\pm 1$, since $(a, 0)=1$; and hence a/c.

2) If $b\neq 0$, let m be the smallest positive common multiple of the relatively prime positive numbers $|a|$ and $|b|$. By Theorem 11,

$$m=|a|\,|b|.$$

Since, by hypothesis, bc is a common multiple of $|a|$ and $|b|$, we have, by Theorem 9,

$$|a|\,|b|/bc,$$
$$ab/bc \qquad \text{(Theorem 1)},$$
$$a/c \qquad \text{(Theorem 3, 1))}.$$

THEOREM 16: *If $a/\prod_{n=1}^{v} a_n$, $v\geqq 2$, $(a, a_n)=1$ for $1\leqq n<v$, then*

$$a/a_v.$$

Proof: For $v=2$, this is shown by Theorem 15. For $v>2$, Theorem 15 yields, successively,

$$a/\prod_{n=2}^{v} a_n,\ a/\prod_{n=3}^{v} a_n,\ \ldots,\ a/\prod_{n=v-1}^{v} a_n,\ a/a_v.$$

CHAPTER II

PRIME NUMBERS AND FACTORIZATION INTO PRIME FACTORS

The number 1 has only one positive divisor, namely 1; every number $a>1$ has at least two positive divisors, namely 1 and a.

DEFINITION 3: *A number $a>1$ is called a prime number (or simply a prime) if it has only two positive divisors* (namely 1 and a).

Examples: The first few primes are 2, 3, 5, 7, 11.

The letter p will be reserved for prime numbers only; likewise, symbols such as $p_1, p_2, \dots, p', p'', \dots$ will always represent primes.

Our next aim will be to prove that every number $a>1$ can be represented as a product of primes (this will be easy) and that this representation is unique apart from the order of the factors (this is somewhat deeper).

THEOREM 17: *Every $a>1$ can be represented as a product of prime numbers:*

$$a=\prod_{n=1}^{r} p_n, \quad r\geqq 1. \tag{2}$$

(For primes $a=p$, this is obvious, and the product reduces to $p=\prod_{n=1}^{1} p_n$.)

Proof (by mathematical induction): 1) For $a=2$ the assertion is true, since 2 is a prime.

2) Let $a>2$ and assume the theorem true for $2, 3, \dots, a-1$.

21) If a is prime, the assertion is true.

22) Otherwise, by Definition 3, there exists a factorization

$$a=a_1a_2, \quad 1<a_1<a, \quad 1<a_2<a.$$

Thus a_1 and a_2, and therefore a also, are representable as products of primes.

Theorem 17 justifies the following definition:

DEFINITION 4: *Every number >1 which is not a prime is called a composite number.*

The natural numbers thus fall into three classes:

1) The number 1;
2) The primes;
3) The composite numbers.

There are, of course, infinitely many composite numbers; for example, all numbers of the form 2^n, $n \geqq 2$.

THEOREM 18: *There are infinitely many primes.*

Proof: We must show that to any finite set of primes there can be adjoined yet another prime.

Let $p_1, \ldots, p_v$ be distinct prime numbers. Then

$$a = 1 + \prod_{n=1}^{v} p_n$$

is, to begin with, >1 and, in addition, is not divisible by any of the prime numbers $p_1, \ldots, p_v$, so that by Theorem 17 it is divisible by a prime number different from $p_1, \ldots, p_v$.

Theorem 18 can be expressed as follows: For any $\xi > 0$, let $\pi(\xi)$ represent the number of primes $\leqq \xi$. Then as ξ approaches infinity, so does $\pi(\xi)$; i.e., given $\omega > 0$ there exists $\eta = \eta(\omega)$ such that

$$\pi(\xi) > \omega \quad \text{if} \quad \xi > \eta = \eta(\omega).$$

The question as to whether, and with what degree of accuracy, $\pi(\xi)$ can be approximated by the functions of analysis, can be answered only later on. In Part 7, Chapter 2, § 3 of my *Vorlesungen über Zahlentheorie,* the reader will find a very accurate result, the methods used being those of complex function theory. This result contains as a special case the "Prime Number Theorem"

$$\lim_{\xi = \infty} \frac{\pi(\xi)}{\frac{\xi}{\log \xi}} = 1;$$

this theorem can be found in Part 7, Chapter 1, § 2 of the work cited.

Let us also note here that the question, for example, of whether there exist infinitely many primes whose decimal representations end in the digit 7 will be answered (in the affirmative) in Part Two, Chapter III; specifically, the answer will appear as a special case of Dirichlet's well-known Theorem on Arithmetic Progressions (Theorem 155).

None of this will be made use of, however, until it has first been proved.

THEOREM 19: *If $p \nmid a$, then $(p, a)=1$.*

Proof: p has as positive divisors only 1 and p. Hence $(p, a)=1$ or p and, since $p \nmid a$, the latter is impossible.

THEOREM 20: *If*

$$p \,\Big|\, \prod_{n=1}^{v} a_n,$$

then for at least one n we have

$$p \mid a_n.$$

Proof: If, for all n, $p \nmid a_n$, then by Theorem 19 we would always have $(p, a_n)=1$, so that, by Theorem 16,

$$p \nmid \prod_{n=1}^{v} a_n.$$

THEOREM 21: *If*

$$p \,\Big|\, \prod_{n=1}^{v} p_n,$$

then for at least one n we have

$$p=p_n.$$

Proof: By Theorem 20,

$$p \mid p_n$$

for at least one n; but since the prime p_n has 1 and p_n as its only positive divisors, and since $p \neq 1$, it follows that $p=p_n$.

THEOREM 22: *The representation* (2) *of any number $a>1$ is unique up to the order of its factors.*

In words: Every prime number appearing in a decomposition into "prime factors" of a given number appears equally often in every such decomposition.

Every $a>1$ is therefore of the form

$$a=\prod_{p \mid a} p^l,$$

where p runs through the various primes that divide a; and where every $l=l_{a,p}>0$ and is uniquely determined by a and p. (This is the so-called canonical decomposition of a.)

Example: $12=2 \cdot 2 \cdot 3=2 \cdot 3 \cdot 2=3 \cdot 2 \cdot 2=2^2 \cdot 3=3 \cdot 2^2$.

Proof: It is obviously sufficient to prove the following: If

$$a=\prod_{n=1}^{v} p_n=\prod_{n=1}^{v'} p'_n, \quad p_1 \leqq p_2 \leqq \cdots \leqq p_v, \quad p'_1 \leqq p'_2 \leqq \cdots \leqq p'_{v'}$$

then

$$v=v', \quad p_n=p'_n \text{ for } 1 \leqq n \leqq v.$$

1) For $a=2$ the assertion is true, since we merely have

$$v=v'=1,\ p_1=p_1'=2.$$

2) Let $a>2$ and suppose that the assertion has been proved for 2, 3, 4, . . . , $a—1$.

21) If a is a prime, then

$$v=v'=1,\ p_1=p_1'=a.$$

22) Otherwise, we have $v>1$ and $v'>1$. Since

$$p_1' \,/ \prod_{n=1}^{v} p_n,\ p_1 \,/ \prod_{n=1}^{v'} p_n',$$

it follows by Theorem 21 that

$$p_1'=p_n,\ p_1=p_m'.$$

for at least one n and at least one m. Since

$$p_1\leqq p_n=p_1'\leqq p_m'=p_1,$$

we have

$$p_1=p_1'.$$

Now (since $1<p_1<a$, p_1/a) we have

$$1<\frac{a}{p_1}=\prod_{n=2}^{v} p_n=\prod_{n=2}^{v'} p_n'<a,$$

and hence (by the induction hypothesis)

$$v—1=v'—1,\ v=v'$$

and

$$p_n=p_n' \text{ for } 2\leqq n\leqq v.$$

THEOREM 23: *Let $a>1$, let $T(a)$ be the number of positive divisors of a, and let*

$$a=\prod_{n=1}^{r} p_n^{l_n}$$

be the canonical decomposition of a (i.e., $p_1, \ldots, p_r$ are distinct and every $l_n>0$). *Then a has for its positive divisors the numbers*

$$(3)\qquad \prod_{n=1}^{r} p_n^{m_n},\ 0\leqq m_n\leqq l_n \textit{ for } 1\leqq n\leqq r$$

and no others. Hence

$$T(a)=\prod_{n=1}^{r}(l_n+1).$$

(That the numbers (3) are distinct follows from Theorem 22.)

Proof: 1) Each number of the form (3) obviously divides a.

2) If $d>0$ and d/a, then $a=qd$, so that d cannot contain any prime factor that does not divide a, nor can d contain any prime factor of a a greater number of times than that factor appears in a itself.

DEFINITION 5: *For any real number ξ, let $[\xi]$ denote the largest integer $\leqq\xi$, that is, the integer g for which*

$$g\leqq\xi<g+1.$$

Obviously

$$\xi-1<[\xi]\leqq\xi,$$

and if

$$a\leqq\xi$$

then

$$a\leqq[\xi],$$

and if

$$a>\xi$$

then

$$a\geqq[\xi]+1>[\xi].$$

THEOREM 24: *The number q of Theorem 7 is equal to* $\left[\frac{b}{a}\right]$.

Proof:

$$qa\leqq b=qa+r<(q+1)a,$$

$$q\leqq\frac{b}{a}<q+1.$$

THEOREM 25: *If $k>0$ and $\eta>0$, then the number of positive multiples of k which are $\leqq\eta$ is*

$$\left[\frac{\eta}{k}\right].$$

Proof: Since $h>0$ and $hk\leqq\eta$, it follows that

$$0<h\leqq\frac{\eta}{k}$$

and conversely; but the number of natural numbers $\leqq\xi$ is $[\xi]$ for every $\xi>0$.

THEOREM 26: *If $k>0$ and $\eta\gtreqless0$, then*

$$\left[\frac{\eta}{k}\right]=\left[\frac{[\eta]}{k}\right].$$

(For $\eta>0$ this also follows from Theorem 25, for there are just as many positive multiples of k up to η as there are up to $[\eta]$.)

Proof: From

$$g \leqq \frac{\eta}{k} < g+1$$

it follows that

$$kg \leqq \eta < k(g+1),$$

$$kg \leqq [\eta] < k(g+1),$$

$$g \leqq \frac{[\eta]}{k} < g+1.$$

THEOREM 27: *Let $n>0$, and let p be any prime. Then p divides $n!$ exactly*

$$\sum_{m=1}^{\infty}\left[\frac{n}{p^m}\right]$$

times.

(This infinite series converges, since the general term vanishes for sufficiently large m, and in particular for $m > \frac{\log n}{\log p}$, since we then have $p^m > n$, $0 < \frac{n}{p^m} < 1$. The series can therefore also be written as $\sum\limits_{1 \leqq m \leqq \frac{\log n}{\log p}} \left[\frac{n}{p^m}\right]$, where, in case $p>n$, the sum stands for zero—as shall every empty sum henceforth.)

In other words: We have

$$(4) \qquad n! = \prod_{p \leqq n} p^{\sum\limits_{m=1}^{\infty}\left[\frac{n}{p^m}\right]}$$

(where, in case $n=1$, the product represents the number 1—as shall every empty product henceforth); for the primes $p>n$ do not divide $n!$. We can equally well write

$$n! = \prod_{p} p^{\sum\limits_{m=1}^{\infty}\left[\frac{n}{p^m}\right]}$$

where the product is taken over all primes arranged in increasing order of magnitude, for every factor is 1 for $p>n$.

Proof: In preparation for later on, I present two proofs.

1) The number of positive multiples of the number p up to n is, by Theorem 25, $\left[\frac{n}{p}\right]$; the number of positive multiples of p^2 up to n is $\left[\frac{n}{p^2}\right]$; etc.

The multiplicity with which p divides $n!$ therefore

$$= \sum_{m=1}^{\infty} \text{number of positive multiples of } p^m \text{ up to } n$$

$$= \sum_{m=1}^{\infty}\left[\frac{n}{p^m}\right];$$

for each of the numbers $1, \ldots, n$ is counted l times (and so not at all if $l=0$) as a multiple of p^m for $m=1, 2, \ldots, l$, if p divides it exactly l times ($l\geqq 0$).

2) (This proof is longer than the former, and introduces the logarithmic function—which can, of course, be eliminated by the use of exponents—but the proof is otherwise useful.) Let us henceforth set

$$\Lambda(a)=\begin{cases}\log p & \text{for } a=p^c,\ c\geqq 1,\\ 0 & \text{for all other } a>0.\end{cases} \tag{5}$$

(thus $\Lambda(1)=0$, $\Lambda(2)=\log 2$, $\Lambda(3)=\log 3$, $\Lambda(4)=\log 2$, $\Lambda(5)=\log 5$, $\Lambda(6)=0, \ldots$). Let the symbol

$$\sum_{d/a} f(d)$$

mean, on principle, for $a>0$, that the sum is taken over all positive divisors d of a.

Then we have

$$\log a=\sum_{d/a}\Lambda(d). \tag{6}$$

For (6) is obvious if $a=1$ ($0=0$), and if

$$a=\prod_{p/a} p^r \quad (r=r_{a,\,p})$$

is the canonical decomposition of $a>1$, then

$$\log a=\sum_{p/a} r\log p=\sum_{p/a}(\Lambda(p)+\Lambda(p^2)+\cdots+\Lambda(p^r))=\sum_{d/a}\Lambda(d).$$

From (6) it now follows that

$$\log\ ([\xi]!)=\sum_{a=1}^{[\xi]}\log a=\sum_{a=1}^{[\xi]}\ \sum_{d/a}\Lambda(d)=\sum_{d=1}^{[\xi]}\Lambda(d)\left[\frac{\xi}{d}\right]; \tag{7}$$

(I am generalizing the result somewhat, in that I replace n by any real $\xi>0$); for $\Lambda(d)$ appears only for $1\leqq d\leqq[\xi]$, and for each such d it appears as many times as there are positive multiples of d up to ξ, that is, $\left[\frac{\xi}{d}\right]$ times, by Theorem 25. By the definition (5) of Λ we have, by (7),

$$\log\ ([\xi]!)=\sum_{p\leqq\xi}\log p\left[\frac{\xi}{p}\right]+\sum_{p\leqq\xi}\log p\left[\frac{\xi}{p^2}\right]+\cdots \text{ ad inf.}=\sum_{p\leqq\xi}\log p\sum_{m=1}^{\infty}\left[\frac{\xi}{p^m}\right],$$

so that the assertion (4) is proved if we set $\xi=n$.

If we wish to apply Theorem 27, we should note that for every $n>0$ and every p, the terms of

$$\sum_{m=1}^{\infty}\left[\frac{n}{p^m}\right]$$

can be most expeditiously computed one after the other by use of the result

$$\left[\frac{n}{p^{m+1}}\right]=\left[\frac{\left[\frac{n}{p^m}\right]}{p}\right],$$

which follows from Theorem 26.

Example: $n=1000$, $p=3$; the calculations should not proceed as follows (every ϑ is >0 and <1)

$$\frac{1000}{3}=333+\vartheta_1,\quad \frac{1000}{9}=111+\vartheta_2,\quad \frac{1000}{27}=37+\vartheta_3,\quad \frac{1000}{81}=12+\vartheta_4,$$
$$\frac{1000}{243}=4+\vartheta_5,\quad \frac{1000}{729}=1+\vartheta_6;$$

but rather

$$\frac{1000}{3}=333+\vartheta_7,\quad \frac{333}{3}=111,\quad \frac{111}{3}=37,\quad \frac{37}{3}=12+\vartheta_8,\quad \frac{12}{3}=4,$$
$$\frac{4}{3}=1+\vartheta_9,$$

in order to compute the terms 333, 111, 37, 12, 4, 1, and the final result of 498.

CHAPTER III

THE GREATEST COMMON DIVISOR OF SEVERAL NUMBERS

THEOREM 28: *Let* $a \geqq 1$ *and* $b \geqq 1$. *Let their canonical decompositions be written*

$$a=\prod_{p|a} p^l,\ b=\prod_{p|b} p^m \qquad (l=l_{a,p}>0,\ m=m_{b,p}>0)$$

(where, in case a or $b=1$, the empty product shall mean 1). *If l and m are allowed to assume the value* 0, *then a and b may be written in uniform notation as*

$$a=\prod_{p|ab} p^l, \qquad b=\prod_{p|ab} p^m.$$

Then

$$(a, b)=\prod_{p|ab} p^{\text{Min}\,(l,m)}\,. \tag{8}$$

If $\gamma_1, \ldots, \gamma_r$ are real numbers, then Min $(\gamma_1, \ldots, \gamma_r)$ represents here—as it shall from now on—the smallest and Max $(\gamma_1, \ldots, \gamma_r)$ the largest, of the numbers $\gamma_1, \ldots, \gamma_r$.

Examples: Min $(-3, 0, -3)=-3$; Max $(1, 0)=1$.

Proof: The positive divisors of a are (by Theorem 23) the numbers $\prod_{p|ab} p^t$, $0 \leqq t \leqq l$; those of b are the numbers $\prod_{p|ab} p^u$, $0 \leqq u \leqq m$; the common positive divisors are therefore the numbers $\prod_{p|ab} p^v$, $0 \leqq v \leqq$ Min (l, m) and the right-hand side of (8) is the largest of them.

NOTATION: *If the numbers* $a_1, \ldots, a_r$ $(r \geqq 2)$ *are not all* 0, *then their greatest common divisor* (which of course exists) *is denoted by* $(a_1, \ldots, a_r)$ (in agreement with our former notation for $r=2$).

Examples: $(6, 10, 15)=1$, $(2, 0, -4)=2$.

DEFINITION 6: *If* $r \geqq 2$ *and* $(a_1, \ldots, a_r)=1$, *then* $a_1, \ldots, a_r$ *are called relatively prime.* (For $r=2$ this is our old definition.)

THEOREM 29: *If $r \geqq 2$ and if $a_1, \ldots, a_r$ are not all* 0, *then* $(a_1, \ldots, a_r)$ *is divisible by every common divisor of* $a_1, \ldots, a_r$.

Proof: If only one of the numbers $a_1, \ldots, a_r$ is different from 0, then the assertion is trivial.

Otherwise, without loss of generality, let $a_1, \ldots, a_r$ all be >0; for if they are not, then we merely discard those that equal zero and change the sign of those that are negative.

1) For $r=2$ the assertion is true by Theorem 11.

2) For $r>2$, I give two proofs.

21) Set

$$a_1 = \prod_{p/a_1 \cdots a_r} p^{l_1}, \ldots, a_r = \prod_{p/a_1 \cdots a_r} p^{l_r} \quad (l_1 \geqq 0, \ldots, l_r \geqq 0).$$

Then (compare the proof of Theorem 28), we obviously have

$$(a_1, \ldots, a_r) = \prod_{p/a_1 \cdots a_r} p^{\text{Min}\,(l_1, \ldots, l_r)},$$

and every common divisor is

$$\pm \prod_{p/a_1 \cdots a_r} p^{v},\ 0 \leqq v \leqq \text{Min}\,(l_1, \ldots, l_r),$$

and hence goes into $(a_1, \ldots, a_r)$.

22) Let the assertion be already proved for $r-1$. Every common divisor of $a_1, \ldots, a_r$ divides $a_1, \ldots, a_{r-1}$ and hence $(a_1, \ldots, a_{r-1})$; it also divides a_r, and hence $((a_1, \ldots, a_{r-1}), a_r)$. This number divides $(a_1, \ldots, a_{r-1})$ and a_r, and hence $a_1, a_2, \ldots, a_{r-1}, a_r$; it is therefore equal to $(a_1, \ldots, a_r)$.

We should make note of the relation

$$(9) \qquad (a_1, \ldots, a_r) = ((a_1, \ldots, a_{r-1}), a_r)$$

for $r>2$, $a_1>0, \ldots, a_r>0$, which we found during the second proof.

THEOREM 30: *Let $r \geqq 2$, $a_1>0, \ldots,$ and $a_r>0$. Then every common multiple of n of $a_1, \ldots, a_r$ is divisible by their smallest positive common multiple v* (which obviously exists).

Proof: 1) For $r=2$, we know this by Theorem 9.

2) For $r>2$, I give two proofs (as for Theorem 29).

21) In the notation of the previous proof, we clearly have

$$v = \prod_{p/a_1 \cdots a_r} p^{\text{Max}\,(l_1, \ldots, l_r)}.$$

Either $n=0$ (so that it is certainly divisible by v), or $|n|$ contains every $p|a_1 \ldots a_r$ at least l_1 times, . . . , at least l_r times, and therefore at least Max $(l_1, \ldots, l_r)$ times.

22) Let the assertion already be proved for $r-1$. Let w represent the smallest positive common multiple of $a_1, \ldots, a_{r-1}$, so that n is divisible by $a_1, \ldots, a_{r-1}$ and hence by w; but it is also divisible by a_r and hence by the smallest positive common multiple of w and a_r. Since this number is itself a positive common multiple of $a_1, \ldots, a_{r-1}, a_r$, it must equal v.

CHAPTER IV

NUMBER-THEORETIC FUNCTIONS

DEFINITION 7: *A function $F(a)$ which is defined for every $a>0$ is called a number-theoretic function.*

The value of the function is not required to be a positive integer, nor an integer, a rational number, or even a real number.

Examples: $F(a)=a!$, $F(a)=\sin a$, $F(a)=(a+2)^{-1}$, $F(a)=T(a)$ (the number of positive divisors of Theorem 23), $F(a)=\Lambda(a)$ (Formula (5)), $F(a)=\sum_{d|a} d=S(a)$ (the sum of the positive divisors of a).

THEOREM 31: *If $a>1$ and $a=\prod_{p|a} p^l$ is its canonical decomposition, then*

$$S(a)=\prod_{p|a}\frac{p^{l+1}-1}{p-1}.$$

Proof: If we add the positive divisors $p_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}$ of a enumerated in (3), and use the fact that

$$\sum_{m=0}^{l} p^m=\frac{p^{l+1}-1}{p-1},$$

then the result follows.

DEFINITION 8: *Any divisor of a other than a itself is called a proper divisor of a.*

DEFINITION 9: *a is called even if $2|a$; odd, if $2\nmid a$.*

Examples: 0 is even; of two successive numbers a and $a+1$, exactly one is always even, the other odd; every $p>2$ is odd.

DEFINITION 10: *$a>0$ is called a perfect number if a equals the sum of its proper divisors, that is, if*

$$S(a)=2a.$$

Examples: $6=1+2+3$, $28=1+2+4+7+14$.

This old-fashioned concept of perfect number, and the questions associated with it, are not especially important; we consider them only because, in so doing, we will encounter two questions that remain unanswered to this day: Are there infinitely many perfect numbers? Is there an odd perfect number? Modern mathematics has solved many (apparently) difficult problems, even in number theory; but we stand powerless in the face of such (apparently) simple problems as these. Of course, the fact that they have never been solved is irrelevant to the rest of this work. We will leave no gaps; when we come to a bypath which leads to an insurmountable barrier, we will turn around, rather than—as is so often done—continue on beyond the barrier.

THEOREM 32: *If* $p=2^n-1$ (so that $n>1$; for example, $n=2$, $p=3$; $n=3$, $p=7$), *then*

$$\frac{p+1}{2}p=2^{n-1}(2^n-1)$$

is an (of necessity even) *perfect number, and there are no other even perfect numbers.*

Proof: 1) For

$$a=2^{n-1}(2^n-1),\quad 2^n-1=p$$

we have, by Theorem 31,

$$S(a)=\frac{2^n-1}{2-1}\,\frac{p^2-1}{p-1}=(2^n-1)\,(p+1)=(2^n-1)\,2^n=2a.$$

2) If a is an even perfect number, then

$$a=2^{n-1}u,\quad n>1,\quad u>0 \text{ and odd,}$$

so that, by Theorem 31,

$$2^n u=2a=S(a)=\frac{2^n-1}{2-1}S(u)=(2^n-1)S(u)$$

and

$$S(u)=\frac{2^n u}{2^n-1}=u+\frac{u}{2^n-1}.$$

In this formula, $\frac{u}{2^n-1}$ $(=S(u)-u)$ is an integer, and hence (since $n>1$) it is a proper divisor of u. The sum $S(u)$ of all the divisors of u is therefore equal to the sum of u and a certain proper divisor. Hence u is a prime, and the proper divisor $\frac{u}{2^n-1}=1$, so that $u=2^n-1$. This proves the theorem.

Now, are there infinitely many perfect numbers? I do not know. It was already mentioned above that $2^n—1$ is prime for $n=2$ and $n=3$. For $n=4$, $2^n—1=15$ is composite. More generally, $2^n—1$ is always composite if n is composite; for if $n=bc$, with $b>1$ and $c>1$, then

$$2^n—1=2^{bc}—1=(2^b—1)(2^{b(c-1)}+2^{b(c-2)}+\cdots+2^b+1),$$

where both factors are >1.

For $n=5$, $2^n—1=2^5—1=31$ is a prime that yields the perfect number $16\cdot 31=496$; for $n=7$, $2^n—1=2^7—1=127$ is a prime that yields the perfect number $64\cdot 127=8128$; for $n=11$, $2^n—1=2^{11}—1=2047=23\cdot 89$ is composite. The question is, therefore, whether there are infinitely many primes p for which $2^p—1$ is a prime. Even this is not known.

Are there infinitely many odd perfect numbers? I do not even know whether there is a single one.

However, I should like to ask the reader not to meditate too long over these two questions; he will meet with many more promising and gratifying problems in his study of this work.

The analogous problem of finding all the numbers $a>1$ which are equal to the product of their factors, i.e., for which

$$\prod_{d|a} d=a^2,\ a>1 \tag{10}$$

is trivial. For the following simple theorem holds:

THEOREM 33: (10) *holds if and only if*

$$a=p^3 \text{ or } a=p_1p_2,\ p_1\neq p_2.$$

Proof: 1) As d runs through all the positive divisors of a, so, obviously, does $\frac{a}{d}$. It therefore follows from (10) that

$$a^4=a^2a^2=\prod_{d|a} d\cdot\prod_{d|a}\frac{a}{d}=\prod_{d|a}\left(d\cdot\frac{a}{d}\right)=\prod_{d|a} a=a^{T(a)},$$

$$T(a)=4;$$

and hence, by Theorem 23,

$$(l_1+1)\dots(l_r+1)=4$$

in the canonical decomposition $a=p_1^{l_1}\cdots p_r^{l_r}$, so that either $r=1$ and $l_1=3$, or $r=2$ and $l_1=l_2=1$.

2) Conversely, in these cases,

$$\prod_{d/p_1^3} d=1\cdot p_1\cdot p_1^2\cdot p_1^3=p_1^6=(p_1^3)^2 \text{ and } \prod_{d/p_1p_2} d=1\cdot p_1\cdot p_2\cdot p_1p_2=(p_1p_2)^2,$$

respectively.

DEFINITION 11: *The number-theoretic function* $\mu(a)$ (the Möbius Function) *is defined by*

$$\mu(a)=\begin{cases} 1 \textit{ if } a=1, \\ (-1)^r \textit{ if } a \textit{ is the product of } r\ (\geqq 1) \textit{ distinct primes}, \\ 0 \textit{ otherwise, i.e., if the square of at least one prime divides } a. \end{cases}$$

The numbers $a\geqq 1$ that are not divisible by the square of any prime (or, equivalently, by any perfect square >1) are also called square-free numbers; this quite customary terminology is just as logical as saying that two numbers are prime to each other when they have exactly one positive common divisor (namely, 1). In this sense of square-free, we say: $\mu(a)=\pm 1$ if a is square-free, and $\mu(a)=0$ otherwise.

Examples: $\mu(1)=1, \mu(2)=-1$, $\mu(3)=-1$ ($\mu(p)$ is always $=-1$), $\mu(4)=0$, $\mu(5)=-1$, $\mu(6)=1$, $\mu(7)=-1$, $\mu(8)=0$, $\mu(9)=0$, $\mu(10)=1$.

THEOREM 34: *If* $a>0$, $b>0$, *and* $(a, b)=1$, *then*

$$\mu(ab)=\mu(a)\mu(b).$$

Proof: 1) If a or b is not square-free, then neither is ab, so that

$$\mu(ab)=0=\mu(a)\mu(b).$$

2) If a and b are square-free, then since $(a, b)=1$, ab is also square-free. If $a=1$ or $b=1$, then the statement is obviously true; otherwise the number of prime factors of ab equals the sum of the number of prime factors of a and of b.

THEOREM 35: $\sum\limits_{d/a}\mu(d)=\begin{cases} 1 \textit{ for } a=1, \\ 0 \textit{ for } a>1. \end{cases}$

Proof: 1) $\sum\limits_{d/1}\mu(d)=\mu(1)=1.$

2) If $a>1$ and if $a=p_1^{l_1}\cdots p_r^{l_r}$ is the canonical decomposition of a, then obviously

$$\sum_{d/a}\mu(d)=\sum_{d/p_1\cdots p_r}\mu(d)=1+\binom{r}{1}(-1)+\binom{r}{2}+\cdots+\binom{r}{r}(-1)^r$$
$$=\sum_{s=0}^{r}\binom{r}{s}(-1)^s=(1-1)^r=0;$$

for if $s=1, 2, \ldots, r$, then there are exactly $\binom{r}{s}$ divisors of $p_1 \ldots p_r$ which consist of exactly s prime factors, and for these we have $\mu(d)=(-1)^s$.

THEOREM 36: *If $\xi \geqq 1$, then*

$$\sum_{n=1}^{[\xi]} \mu(n)\left[\frac{\xi}{n}\right]=1.$$

Proof: Let the formula of Theorem 35 be summed over $a=1, 2, \ldots, [\xi]$. This gives

$$1=\sum_{a=1}^{[\xi]} \sum_{d/a} \mu(d)=\sum_{d=1}^{[\xi]} \mu(d)\left[\frac{\xi}{d}\right];$$

for, by Theorem 25, the number of positive multiples of d up to ξ is $\left[\frac{\xi}{d}\right]$.

THEOREM 37: *If $x \geqq 1$, then*

$$\left|\sum_{n=1}^{x} \frac{\mu(n)}{n}\right| \leqq 1.$$

Remark: The infinite series

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n}$$

therefore either converges, or else it oscillates between finite limits. The question as to which of these two alternatives holds does not interest us at the moment; the reader can learn the answer in Part Seven, Chapter 12, § 1 of my *Vorlesungen über Zahlentheorie.*

Gordan used to say something to the effect that "Number Theory is useful since one can, after all, use it to get a doctorate with." In 1899 I received my doctorate by answering this question.

Proof: We have

$$0 \leqq \frac{x}{n}-\left[\frac{x}{n}\right] \begin{cases} <1 & \text{for } 1 \leqq n < x, \\ =0 & \text{for } n=x. \end{cases}$$

Hence, by Theorem 36,

$$\left| x\sum_{n=1}^{x} \frac{\mu(n)}{n}-1\right| = \left|\sum_{n=1}^{x} \mu(n)\left(\frac{x}{n}-\left[\frac{x}{n}\right]\right)\right| \leqq \sum_{n=1}^{x} \left(\frac{x}{n}-\left[\frac{x}{n}\right]\right) \leqq x-1,$$

$$\left| x\sum_{n=1}^{x} \frac{\mu(n)}{n}\right| \leqq 1+(x-1)=x.$$

THEOREM 38: *Let $F(a)$ be any number-theoretic function whatever. Let $G(a)$ be the number-theoretic function*

$$G(a)=\sum_{d/a} F(d).$$

Then

$$F(a)=\sum_{d/a}\mu(d)\,G\left(\frac{a}{d}\right).$$

(This is the so-called Möbius Inversion.)

Remark: The fact that $F(a)$ is uniquely determined at all, in reverse, by $G(a)$ is clear to start with; for from

$$G(1)=F(1),\ G(2)=F(2)+\cdots,\ G(3)=F(3)+\cdots,\ \ldots$$

we can successively compute $F(1), F(2), F(3), \ldots.$

Proof: For every positive d/a we have

$$G\left(\frac{a}{d}\right)=\sum_{b/\frac{a}{d}} F(b),$$

$$\mu(d)G\left(\frac{a}{d}\right)=\sum_{b/\frac{a}{d}} \mu(d)F(b),$$

$$\sum_{d/a}\mu(d)G\left(\frac{a}{d}\right)=\sum_{d/a}\ \sum_{b/\frac{a}{d}} \mu(d)F(b)=\sum_{b/a}\ \sum_{d/\frac{a}{b}} \mu(d)F(b)$$

(for b only runs through positive divisors of a, and to every such b there corresponds exactly to those d for which d/a, and in fact for which db/a, that is, for which $d/\frac{a}{b}$)

$$=\sum_{b/a}F(b)\sum_{d/\frac{a}{b}}\mu(d)=F(a),$$

since, by Theorem 35,

$$\sum_{d/\frac{a}{b}}\mu(d)=\begin{cases}1 \text{ for } b=a,\\ 0 \text{ for } b/a,\ b<a.\end{cases}$$

DEFINITION 12: *The number-theoretic function* $\varphi(a)$ (Euler's Function) *represents the number of numbers n in the sequence* $1, 2, \ldots, a$ *for which* $(n, a)=1$.

GCD

Examples: $\varphi(1)=1\,(n=1)$, $\varphi(2)=1\,(n=1)$, $\varphi(3)=2\,(n=1,\ 2)$, $\varphi(4)=2\,(n=1,\ 3)$, $\varphi(5)=4\,(n=1,\ 2,\ 3,\ 4)$, $\varphi(6)=2\,(n=1,.5)$, $\varphi(p)=p-1\,(n=1, 2, \ldots, p-1)$.

Theorem 39: $\sum\limits_{d|a} \varphi(d) = a.$

Proof: Divide all the a numbers $n=1, \ldots, a$ into classes according to the value of $d=(n, a)$. Only those numbers $d>0$ that divide a enter into consideration. To each $d|a$ let there belong the $n=kd$ for which $(kd, a)=d$, i.e. (by Theorems 13 and 14), $\left(k, \frac{a}{d}\right)=1$ and moreover for which $0<kd\leqq a$, i.e., $0<k\leqq \frac{a}{d}$. But by Definition 12 there are exactly $\varphi\left(\frac{a}{d}\right)$ such numbers. Hence

$$a=\sum_{d|a} \varphi\left(\frac{a}{d}\right)=\sum_{d|a} \varphi(d),$$

since $\frac{a}{d}$ runs through all the positive divisors of a when d does.

Theorem 40: $\varphi(a)=a\sum\limits_{d|a}\frac{\mu(d)}{d}.$

Proof: By Theorems 39 and 38 (with $F(a)=\varphi(a)$ and $G(a)=a$), we have

$$\varphi(a)=\sum_{d|a}\mu(d)\frac{a}{d}=a\sum_{d|a}\frac{\mu(d)}{d}:$$

Theorem 41: $\varphi(a)=a\prod\limits_{p|a}\left(1-\frac{1}{p}\right).$

Proof: 1) For $a=1$ we have $\varphi(1)=1$ (the product in the statement of the theorem is empty).

2) For $a>1$ let $a=p_1^{l_1}\cdots p_r^{l_r}$ be its canonical decomposition. Then by Theorem 40 we have

$$\varphi(a)=a\sum_{d|p_1\cdots p_r}\frac{\mu(d)}{d}=a\prod_{n=1}^{r}\left(1-\frac{1}{p_n}\right),$$

as is seen by calculating the 2^r terms of the product.

Theorem 42: *For $a>1$ we have, in the canonical notation,*

$$\varphi(a)=\prod_{n=1}^{r} p_n^{l_n-1}(p_n-1).$$

Proof: By Theorem 41,

$$\varphi(a)=\prod_{n=1}^{r} p_n^{l_n}\cdot\prod_{n=1}^{r}\left(1-\frac{1}{p_n}\right)=\prod_{n=1}^{r} p_n^{l_n}\left(1-\frac{1}{p_n}\right).$$

THEOREM 43: *For $l>0$ we have*

$$\varphi(p^l)=p^{l-1}(p-1).$$

Two proofs: 1) Special case of Theorem 42.

2) (Direct proof.) Of the numbers $1, 2, \ldots, p^l$, those not relatively prime to p^l are precisely all the multiples of p; their number is p^{l-1}; hence

$$\varphi(p^l)=p^l-p^{l-1}.$$

All of Theorem 42 itself can be proven directly by counting the numbers n which are not relatively prime to a and for which $1\leqq n\leqq a$; but this is somewhat more laborious and is a good exercise for the reader. (The solution of this exercise is, however, not essential for the remainder of this book.)

THEOREM 44: *If $a>0$, $b>0$, and $(a, b)=1$, then*

$$\varphi(ab)=\varphi(a)\varphi(b).$$

Proof: Without loss of generality let (canonically) $a=\prod\limits_{n=1}^{r} p_n^{l_n}>1$ and $b=\prod\limits_{m=1}^{s} q_m^{k_m}>1$. From Theorem 42 it follows that

$$\varphi(a)=\prod_{n=1}^{r} p_n^{l_n-1}(p_n-1), \quad \varphi(b)=\prod_{m=1}^{s} q_m^{k_m-1}(q_m-1).$$

Since $(a, b)=1$,

$$ab=\prod_{n=1}^{r} p_n^{l_n}\prod_{m=1}^{s} q_m^{k_m}$$

is the canonical decomposition of ab; hence, by Theorem 42,

$$\varphi(ab)=\prod_{n=1}^{r} p_n^{l_n-1}(p_n-1)\cdot\prod_{m=1}^{s} q_m^{k_m-1}(q_m-1)=\varphi(a)\varphi(b).$$

The reader will find another proof of Theorem 44, one based directly on the definition of φ, in Theorem 74.

CHAPTER V

CONGRUENCES

In this chapter m will always be >0.

Definition 13: *a is said to be congruent to b modulo m, written*

$$a \equiv b \pmod{m},$$

if

$$m \mid (a-b).$$

a is called incongruent to b modulo m, written

$$a \not\equiv b \pmod{m},$$

if

$$m \nmid (a-b).$$

Examples:

$$31 \equiv -9 \pmod{10},$$
$$627 \equiv 587 \pmod{10},$$
$$5 \not\equiv 4 \pmod{2},$$
$$a \equiv b \pmod{1} \text{ for arbitrary } a \text{ and } b.$$

Any concept such as "congruent," "equivalent," "equal," or "similar," in mathematics must satisfy three properties (the so-called reflexivity, symmetry, and transitivity), which are expressed here by means of the following three theorems.

Theorem 45 (Reflexivity): *We always have*

$$a \equiv a \pmod{m}.$$

Proof: $m \mid 0,\ m \mid (a-a)$.

Theorem 46 (Symmetry): *If*

$$a \equiv b \pmod{m}$$

then

$$b \equiv a \pmod{m}.$$

Proof: $m/(a-b)$, and hence, by Theorem 1, $m/(b-a)$.

THEOREM 47 (Transitivity): *If*

$$a \equiv b \pmod{m}, \quad b \equiv c \pmod{m}$$

then

$$a \equiv c \pmod{m}.$$

Proof: $m/a-b$, $m/b-c$, $m/(a-b)+(b-c)$, $m/a-c$.

Thus, just like equations, congruences (with the same modulus) can be written in sequence as a congruence with more than two terms; for example,

$$a \equiv b \equiv c \pmod{m}.$$

The following theorem (which, incidentally, makes Theorems 45-47 self-evident) provides a useful necessary and sufficient condition for the validity of a congruence.

THEOREM 48: *According to Theorem 7, given the numbers c and m, there is a uniquely determined number r such that*

$$c = qm + r, \; 0 \leqq r < m;$$

let this number r be called the residue of c modulo m. Then

$$a \equiv b \pmod{m}$$

holds if and only if a and b have the same residue modulo m.

Proof: 1) If

$$a = q_1 m + r, \quad b = q_2 m + r$$

then

$$a - b = (q_1 - q_2) m,$$
$$m/a-b.$$

2) If

$$a = q_1 m + r, \quad 0 \leqq r < m, \quad a \equiv b \pmod{m}$$

then

$$b = a + qm = (q_1 + q) m + r = q_2 m + r.$$

Theorem 48 shows that, given a number m, all the numbers fall into m classes ("residue classes") in such a way that any two numbers in the same class are congruent, and any two numbers in different classes are incongruent. One of the classes consists of the multiples of m.

Theorems 49-56 which follow are analogous to the corresponding theorems on equalities; they make clear the usefulness of the congruence sign; looking at it intrinsically, one might have objected that no new symbol is needed for $m|(a-b)$. Since the modulus m in Theorems 49-56 remains the same throughout, we shall not bother to write it for the time being.

THEOREM 49: *If*

$$a\equiv b,\ c\equiv d$$

then

$$a+c\equiv b+d,\ a-c\equiv b-d.$$

Proof: $m|a-b,\ m|c-d,\ m|(a-b)\pm(c-d),\ m|(a\pm c)-(b\pm d).$

THEOREM 50: *If*

$$a_n\equiv b_n \text{ for } n=1,\ldots,v,$$

then

$$\sum_{n=1}^{v} a_n\equiv\sum_{n=1}^{v} b_n$$

Proof: Follows by induction from Theorem 49.

THEOREM 51: *If*

$$a\equiv b,$$

then, for every c,

$$ac\equiv bc.$$

Proof: $m|(a-b),\ m|(a-b)c,\ m|(ac-bc).$

THEOREM 52: *If*

$$a\equiv b \text{ and } c\equiv d,$$

then

$$ac\equiv bd.$$

Proof: By Theorem 51 it follows from the first part of the hypothesis that $ac\equiv bc$ and from the second that $bc\equiv bd$; hence, by Theorem 47, the conclusion follows.

THEOREM 53: *If*

$$a_n\equiv b_n \text{ for } n=1,\ldots,v,$$

then

$$\prod_{n=1}^{v} a_n\equiv\prod_{n=1}^{v} b_n.$$

Proof: By induction, using Theorem 52.

Theorem 54: *If*

$$a \equiv b,\ v > 0,$$

then

$$a^v \equiv b^v.$$

Proof: Follows from Theorem 53.

Theorem 55: *Let*

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n = \sum_{v=0}^{n} c_v x^v \quad (n \geqq 0)$$

be any rational integral function with integer coefficients. If

$$a \equiv b,$$

then

$$f(a) \equiv f(b).$$

The solutions (if any exist) of the congruence

$$f(x) \equiv 0$$

thus fall into complete residue classes mod m.

Proof: By Theorem 54 it follows from the hypothesis that

$$a^v \equiv b^v \text{ for } 0 < v \leqq n,$$

so that, by Theorem 51,

$$c_v a^v \equiv c_v b^v \text{ for } 0 < v \leqq n;$$

since

$$c_0 \equiv c_0$$

our result

$$\sum_{v=0}^{n} c_v a^v \equiv \sum_{v=0}^{n} c_v b^v.$$

follows by Theorem 50.

Theorem 55 justifies:

Definition 14: *By the number of solutions, or roots, of a congruence*

$$f(x) \equiv 0 \pmod{m}$$

we shall mean the number of those numbers of the set $x = 0, \ldots, m-1$ that satisfy the congruence, that is, the number of residue classes all of whose members satisfy the congruence.

Thus the number of solutions is always either 0 or some other finite number.

Example: $x^2 \equiv 1 \pmod 8$ has four solutions, since $x=1, 3, 5, 7$ (but not $x=0, 2, 4, 6$) satisfy the congruence. This fact, that $8/(x^2-1)$ for every odd number x, should be kept in mind.

THEOREM 56: *If*

$$ac \equiv bc, \quad (c, m)=1$$

then

$$a \equiv b.$$

Proof: $m/(ac-bc)$, $m/(a-b)c$; since $(m, c)=1$, it follows from Theorem 15 that

$$m/(a-b).$$

THEOREM 57: *If*

$$ac \equiv bc \pmod m).,$$

then

$$a \equiv b \left(\operatorname{mod} \frac{m}{(c, m)}\right).$$

(If $(c, m)=1$, this reduces to Theorem 56.)

Proof:

$$m/(a-b)\, c,$$

hence, by Theorem 3,

$$\frac{m}{(c, m)} \Big/ (a-b) \frac{c}{(c, m)}.$$

By Theorem 13 it follows that

$$\left(\frac{m}{(c, m)}, \frac{c}{(c, m)}\right)=1,$$

so that by Theorem 15,

$$\frac{m}{(c, m)} \Big/ a-b.$$

THEOREM 58: *Let* $c>0$. *If*

$$a \equiv b \pmod m,$$

then

$$ac \equiv bc \pmod{c\, m},$$

and conversely.

Proof: Since $c>0$, it follows from Theorem 3 that the relations $m/(a-b)$ and $cm/c(a-b)$ *are equivalent.*

THEOREM 59: *If*

$$a \equiv b \pmod m, \quad n>0, \quad n/m,$$

then

$$a \equiv b \pmod n.$$

Proof: $m/(a-b)$ and n/m; hence $n/(a-b)$.

THEOREM 60: *If*

$$a \equiv b \pmod{m_n} \text{ for } n=1,\ 2, \ldots, v \quad (v \geqq 2)$$

then, if m is the smallest common positive multiple of $m_1, \ldots, m_v$, we have

$$a \equiv b \pmod{m}.$$

Proof: $a-b$ is divisible by $m_1, \ldots, m_v$, and hence, according to Theorem 30, by m.

THEOREM 61: *If*

$$a \equiv b \pmod{m},$$

then

$$(a, m) = (b, m).$$

In particular: If $(a, m)=1$, then $(b, m)=1$. Consequently the numbers in a residue class are either all relatively prime to m, or none of them is.

Proof: From $b=a+mq$ it follows that $(a, m)|b$, so that $(a, m)|(b, m)$; similarly, $(b, m)|(a, m)$.

DEFINITION 15: *By a complete set of residues* mod m *is meant a set of m numbers each of which is congruent to exactly one of the numbers* $0, 1, \ldots, m-1 \pmod{m}$, *that is, which represents the m classes into which all the integers* mod m *fall.*

It suffices, of course, to require that at least one of the m numbers belong to each class. "If m objects are put into m pigeon-holes and each pigeon-hole contains at least one object, then each pigeon-hole contains *exactly* one object."

Alternatively: It suffices to require that each pair of m numbers be incongruent. "If m objects are put into m pigeon-holes and each pigeon-hole contains at most one object, then each pigeon-hole contains exactly one object."

Examples: Any m consecutive numbers, for example $1, \ldots, m$, or the integers of the interval $-\frac{m}{2}$ (exclusive) to $\frac{m}{2}$ (inclusive) constitute a complete set of residues, since they are incongruent to each other.

Our old Definition 14 can now be expressed as follows: The number of solutions of

$$f(x) \equiv 0 \pmod{m}$$

is the number of its solutions taken from any complete set of residues.

DEFINITION 16: *By a reduced set of residues* mod m *is meant a set of $\varphi(m)$ numbers exactly one of which belongs to each of the classes all of whose numbers are relatively prime to m.*

Once again it suffices, given $\varphi(m)$ numbers, to require *either* that at least one belong to each of the above-mentioned $\varphi(m)$ classes *or* that each of the $\varphi(m)$ numbers be relatively prime to m and that each pair of them be incongruent.

THEOREM 62: *If* $(k, m)=1$, *then the numbers*

$$0 \cdot k, 1 \cdot k, 2 \cdot k, \ldots, (m-1) \cdot k$$

constitute a complete set of residues mod m.

More generally: *If* $(k, m)=1$ *and* $a_1, \ldots, a_m$ *is any complete set of residues, then so is* $a_1 k, \ldots, a_m k$.

Proof: From

$$a_r k \equiv a_s k \pmod{m}, \quad 1 \leqq r \leqq m, \quad 1 \leqq s \leqq m$$

it follows by Theorem 56, since by assumption $(k, m)=1$, that

$$a_r \equiv a_s \pmod{m}$$

and

$$r=s;$$

the terms $a_r k$ are therefore mutually incongruent.

THEOREM 63: *If* $(k, m)=1$ *and if* $a_1, \ldots, a_{\varphi(m)}$ *constitute a reduced set of residues* mod m, *then so do* $a_1 k, \ldots, a_{\varphi(m)} k$.

Proof: Each of these $\varphi(m)$ numbers is relatively prime to m (for any common factor of $a_r k$ and m would have to go into a_r and m); hence any two are incongruent, by Theorem 62.

THEOREM 64: *If* $(a, m)=1$, *then the congruence*

$$ax+a_0 \equiv 0 \pmod{m}$$

has exactly one solution.

Proof: By Theorem 62,

$$a \cdot 0, \ a \cdot 1, \ \ldots, \ a(m-1)$$

constitute a complete set of residues; hence exactly one of these numbers is $\equiv -a_0 \pmod{m}$.

THEOREM 65: 1) *The congruence*

$$ax+a_0 \equiv 0 \pmod{m} \tag{11}$$

is solvable if and only if

$$(a, m) \mid a_0.$$

2) *In that case the number of solutions* $=(a, m)$, *and the congruence is satisfied by precisely all of the numbers* x *in a certain residue class* mod $\left(\frac{m}{(a, m)}\right)$.

Remark: Theorem 64 is obviously a special case of this theorem, but is made use of to prove it.

Proof: 11) If (11) is solvable, then

$$ax+a_0\equiv 0 \pmod{(a, m)},$$
$$a_0\equiv 0 \pmod{(a, m)}.$$

12) If

$$a_0\equiv 0 \pmod{(a, m)},$$

then, by Theorem 64, the congruence

$$(12) \qquad \frac{a}{(a, m)}x+\frac{a_0}{(a, m)}\equiv 0 \left(\operatorname{mod} \frac{m}{(a, m)}\right)$$

is solvable. Hence, by Theorem 58, (11) is satisfied.

2) If $(a, m)/a_0$, then (12) has exactly one solution mod $\frac{m}{(a, m)}$, according to Theorem 64; since (11) and (12) have the same solutions, by Theorem 58, it follows that (11) has (a, m) solutions (solutions mod m, as usual), since if $d>0$ and d/m, then a residue class mod $\frac{m}{d}$ breaks up into d residue classes mod m.

THEOREM 66: *Let* $n>1$ *and let at least one of the numbers* $a_1, \dots, a_n$ *be different from* 0; *set*

$$(a_1, \dots, a_n)=d.$$

We claim that the diophantine equation (i.e., equation with integral coefficients and unknowns)

$$a_1x_1+\cdots+a_nx_n=c$$

is solvable if and only if

$$d/c.$$

Hence, in particular: If $(a, b)=1$, then

$$(13) \qquad ax+by=1$$

is solvable.

Proof: 1) If exactly one coefficient does not vanish, say a_1, then

$$a_1x_1+0\cdot x_2+\cdots+0\cdot x_n=c$$

is obviously solvable if a_1/c, that is, if

$$(a_1, 0, \ldots, 0)/c.$$

2) If at least two coefficients do not vanish, then we may assume without loss of generality that no coefficient vanishes; for otherwise we simply omit those terms a_mx_m for which $a_m=0$, and this does not alter the value of the greatest common divisor of the coefficients; the number of terms that remain is then still $\geqq 2$.

Without loss of generality we may even take all the coefficients to be >0; for we merely have to replace each negative a_m by $-a_m$ (which does not alter the greatest common divisor) and the corresponding x_m by $-x_m$.

We may therefore assume that

$$n>1,\ a_1>0,\ \ldots,\ a_n>0.$$

21) If our diophantine equation is solvable, then obviously

$$d/a_1x_1+\cdots+a_nx_n,$$
$$d/c.$$

22) Let

$$d/c.$$

221) If $n=2$, then we merely have to show that

$$a_1x_1\equiv c \pmod{a_2}$$

is solvable for x_1. This follows from Theorem 65, since

$$(a_1, a_2)/-c.$$

222) Let $n>2$, and assume the assertion proved for $2, \ldots, n-1$; if we set

$$(a_1, \ldots, a_{n-1})=a$$

then, by (9),

$$(a, a_n)=d.$$

From what we showed in 221), it follows that

$$ax+a_nx_n=c.$$

for suitably chosen x, x_n. By our induction hypothesis for $n-1$, it follows in addition, since

$$(a_1, \ldots, a_{n-1})/ax,$$

that

$$a_1x_1+\cdots+a_{n-1}x_{n-1}=ax$$

for suitably chosen $x_1, \ldots, x_{n-1}$, so that, finally,

$$a_1x_1+\cdots+a_{n-1}x_{n-1}+a_nx_n=c.$$

THEOREM 67: *If $(a, b)=d$ and $d|c$, then*

$$ax+by=c$$

is solvable, by Theorem 66; then, given any solution x_0, y_0, all the solutions are of the form

$$x=x_0+h\frac{b}{d},\ y=y_0-h\frac{a}{d},$$

where h is arbitrary.

Proof: 1) The fact that such a pair x, y satisfies the equation follows from the relation

$$a\left(x_0+h\frac{b}{d}\right)+b\left(y_0-h\frac{a}{d}\right)=ax_0+by_0=c.$$

2) The fact that no other solutions exist is seen as follows. Without loss of generality, let $b\neq0$. (Otherwise interchange a and b, and observe that as h runs through all the integers, so does $-h$.) Since

$$ax+by=c=ax_0+by_0,$$

it follows that

$$ax-c\equiv0 \pmod{|b|},$$
$$ax_0-c\equiv0 \pmod{|b|},$$

and hence by Theorem 65 (with $a_0=-c$, $m=|b|$), we have

$$x\equiv x_0 \left(\bmod \frac{|b|}{d}\right),$$

$$x=x_0+h\frac{b}{d},$$

$$by=c-ax=c-a\left(x_0+h\frac{b}{d}\right)=(c-ax_0)-b\frac{ha}{d}=by_0-b\frac{ha}{d}=b\left(y_0-h\frac{a}{d}\right),$$

$$y=y_0-h\frac{a}{d}.$$

THEOREM 68: *If* $(a, b)=1$ *and if* x_0, y_0 *is any solution of* (13), *then all the solutions are of the form*

$$x=x_0+hb, \; y=y_0-ha\,,$$

where h is arbitrary.

Proof: This follows from Theorem 67, with $d=c=1$.

THEOREM 69: 1) *The congruences*

$$x\equiv a_1 \pmod{m_1}, \tag{14}$$

$$x\equiv a_2 \pmod{m_2} \tag{15}$$

have a common solution if and only if

$$(m_1, m_2)/a_1-a_2. \tag{16}$$

In particular, therefore, they always do if $(m_1, m_2)=1$.

2) *If condition* (16) *is satisfied and if m represents the smallest common multiple of* m_1 *and* m_2, *then the common solutions of* (14) *and* (15) *consist of all the numbers in a certain residue class* mod m.

Proof: 11) If we set $(m_1, m_2)=d$, then it follows from (14) and (15) that

$$\begin{gathered} x\equiv a_1 \pmod{d}, \\ x\equiv a_2 \pmod{d}, \\ a_1\equiv a_2 \pmod{d}, \\ d\;/\;a_1-a_2. \end{gathered}$$

12) If

$$d\;/\;a_1-a_2,$$

then from among all solutions of (14) of the form

$$x=a_1+ym_1 \;\;(\,y \;\text{ arbitrary})$$

we can certainly choose one for which (15) holds. For we need

$$a_1+ym_1\equiv a_2 \pmod{m_2};$$

this is equivalent to

$$m_1y+(a_1-a_2)\equiv 0 \pmod{m_2} \tag{17}$$

which, by Theorem 65, 1), is solvable.

2) If (16) is satisfied, and therefore (14) and (15) along with it, then congruence (17) is satisfied for suitably chosen y_0 precisely by

$$y \equiv y_0 \left(\mathrm{mod}\, \frac{m_2}{d}\right)$$

by virtue of Theorem 65, 2). Therefore, since $\frac{m_1 m_2}{d} = m$ (by Theorem 11), all the numbers x satisfying (14) and (15) are given by the formulas

$$x = a_1 + \left(y_0 + h\frac{m_2}{d}\right)m_1 = a_1 + m_1 y_0 + h\frac{m_1 m_2}{d} = a_1 + m_1 y_0 + hm, \; h \text{ arbitrary},$$

but these constitute a certain residue class mod m.

THEOREM 70: *Let $r > 1$, and let every pair from among the numbers $m_1, \ldots, m_r$ be relatively prime. Then the congruences*

(18) $$x \equiv a_n \pmod{m_n}, \; n = 1, \ldots, r$$

are consistent, and their common solutions consist of all the numbers in a certain residue class mod $m_1 m_2 \ldots m_r$.

Proof: 1) For $r = 2$ this follows from Theorem 69, since $m = m_1 m_2$ in that case.

2) Let $r > 2$, and assume the theorem proved for $r—1$. Then the first $r—1$ congruences (18) are covered by

$$x \equiv a \pmod{m_1 \cdots m_{r-1}}.$$

for a suitably chosen a. Hence, by Theorem 69, the conclusion follows, since $m_1 \cdots m_{r-1}$ is relatively prime to m_r.

THEOREM 71: *Let $r > 1$, and let each pair of numbers from among $m_1, \ldots, m_r$ be relatively prime. Then the number of solutions of*

(19) $$f(x) \equiv 0 \pmod{m_1 m_2 \cdots m_r}$$

equals the product of the numbers of solutions of

(20) $$f(x) \equiv 0 \pmod{m_1}, \ldots, f(x) \equiv 0 \pmod{m_r}.$$

In particular: If $m > 1$ and $m = \prod_{n=1} p_n^{l_n}$ is its canonical decomposition then, if $r > 1$, the number of solutions of

$$f(x) \equiv 0 \pmod{m}$$

equals the product of the numbers of solutions of

$$f(x) \equiv 0 \pmod{p_n^{l_n}}.$$

Proof: First of all, it is clear that (19) is satisfied if and only if the r congruences in (20) are simultaneously satisfied. Hence if one of these has no solution, then neither does (19). If the congruences in (20) are all solvable then, by Theorem 70, to each residue class mod m_1 that satisfies the first congruence in (20) there corresponds one-to-one a residue class mod $m_1 \ldots m_r$ that satisfies (19); similarly for $m_2, \ldots, m_r$.

THEOREM 72: *If*

$$f(x)=c_0+c_1x+\cdots+c_nx^n, \quad p\nmid c_n,$$

then the congruence

$$f(x)\equiv 0 \pmod p \tag{21}$$

has at most n solutions.

Proof: 1) For $n=0$ this is obvious, since for every x,

$$c_0 \not\equiv 0 \pmod p,$$

so that (21) has no root.

2) Let $n>0$, and assume the theorem true for $n-1$. If (21) had at least the $n+1$ (incongruent) roots $x_0, x_1, \ldots, x_n$, then if we note that

$$f(x)-f(x_0)=\sum_{r=1}^{n} c_r(x^r-x_0{}^r)=(x-x_0)\sum_{r=1}^{n} c_r(x^{r-1}+x_0x^{r-2}+\cdots+x_0{}^{r-1})$$
$$=(x-x_0)g(x)$$

and

$$g(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}, \quad b_{n-1}=c_n, \quad p\nmid b_{n-1},$$

it would follow that

$$(x_k-x_0)g(x_k)\equiv f(x_k)-f(x_0)\equiv 0-0\equiv 0 \pmod p,$$

for $k=1, \ldots, n$, so that

$$g(x_k)\equiv 0 \pmod p,$$

contrary to the induction hypothesis for $n-1$.

THEOREM 73: *Let $a>0$, $b>0$, and $(a, b)=1$. Let x range over a complete set of residues* mod b *and y over a complete set of residues* mod a. *Then $ax+by$ ranges over a complete set of residues* mod ab.

Proof: Of the ab numbers $ax+by$, any two are incongruent mod ab. For if

$$ax_1+by_1\equiv ax_2+by_2 \pmod{ab},$$

then

$$ax_1+by_1\equiv ax_2+by_2 \pmod b,$$
$$ax_1\equiv ax_2 \pmod b,$$
$$x_1\equiv x_2 \pmod b,$$

and similarly, by symmetry,

$$y_1 \equiv y_2 \pmod{a}.$$

THEOREM 74: *Let* $a>0$, $b>0$, *and* $(a, b)=1$. *Let* x *and* y *range over reduced sets of residues* mod b *and* mod a, *respectively. Then* $ax+by$ *ranges over a reduced set of residues* mod ab.

Remark: This is the direct proof of Theorem 44 which we announced earlier. Since Theorem 43 was also proved directly, there thus results a new, direct proof of Theorem 42, and consequently of Theorems 41 and 40; up to this point, everything had been obtained from the Möbius Inversion formula.

Proof: If $(x, b)>1$, then certainly $(ax+by, ab)>1$; for (x, b) divides $ax+by$ and ab, and hence divides $(ax+by, ab)$. If $(y, a)>1$, then, by symmetry, $(ax+by, ab)>1$ as well.

What remains to be shown, by Theorem 73, is that if

$$(x, b)=1 \text{ and } (y, a)=1,$$

then

$$(ax+by, ab)=1.$$

In fact, let $p|(ax+by, ab)$. Then we would have $p|ab$, so that, without loss of generality, $p|a$; moreover, $p|(ax+by)$, so that $p|by$, and consequently (since $(a, b)=1$) $p|y$, contrary to the assumption that $(y, a)=1$.

THEOREM 75 (The so-called Little Fermat Theorem): *If* $(a, m)=1$, *then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Remark: It is not known whether the so-called Last Theorem of Fermat, which is discussed in Parts 12 and 13 of my *Vorlesungen über Zahlentheorie,* is true or not. I would therefore rather refer to it as the Fermat Conjecture, and to Theorem 75 simply as Fermat's Theorem.

Proof: Let $a_1, \ldots, a_{\varphi(m)}$ be a reduced set of residues mod m. Then, by Theorem 63, $aa_1, \ldots, aa_{\varphi(m)}$ is also such a set. Hence the numbers a_n are congruent to the numbers aa_n $(n=1, \ldots, \varphi(m))$, apart from their order. Hence the product of the a_n is congruent to the product of the aa_n, or

$$1 \cdot \prod_{n=1}^{\varphi(m)} a_n \equiv \prod_{n=1}^{\varphi(m)} a_n \equiv \prod_{n=1}^{\varphi(m)} (aa_n) \equiv a^{\varphi(m)} \prod_{n=1}^{\varphi(m)} a_n \pmod{m},$$

so that, by Theorem 56,

$$1 \equiv a^{\varphi(m)} \pmod{m}.$$

THEOREM 76: *If $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p};$$

for any a at all we have

$$a^p \equiv a \pmod{p}.$$

Proof: The first statement follows from Theorem 75, since $\varphi(p)=p-1$; the second follows from the first by Theorem 51 if $p \nmid a$; and if p/a, it is trivial, since

$$a^p \equiv 0 \equiv a \pmod{p}.$$

THEOREM 77 (The so-called Theorem of Wilson): $(p-1)! \equiv -1 \pmod{p}$.

Two Proofs: 1) For $p=2$ and $p=3$, the statement is obvious. For $p>3$, I consider the $p-3$ numbers

$$2, 3, \ldots, p-3, p-2. \tag{22}$$

For each r in this sequence, $p \nmid r$, and hence, by Theorem 64, there is exactly one s in the sequence $0, 1, \ldots, p-1$ for which

$$rs \equiv 1 \pmod{p}. \tag{23}$$

$s=0$ does not obtain here; nor do $s=1$ and $s=p-1$, since otherwise r would be $\equiv \pm 1$. The s therefore occurs in the sequence (22) as well. Moreover,

$$s \neq r;$$

for

$$r^2 \equiv 1 \pmod{p}$$

would give

$$p/(r-1)(r+1),$$
$$r \equiv \pm 1 \pmod{p}.$$

Hence to each r in (22) there corresponds exactly one $s \neq r$ in (22) for which (23) holds. Since $rs=sr$, it follows, conversely, that r is uniquely determined by s. The $p-3$ numbers in (22) thus break up into $\frac{p-3}{2}$ pairs in such a way that the product of the numbers in each pair is $\equiv 1$. Hence

$$(p-2)! \equiv 2 \cdot 3 \cdots (p-2) \equiv 1^{\frac{p-3}{2}} \equiv 1 \pmod{p},$$
$$(p-1)! \equiv (p-1)\,(p-2)! \equiv -(p-2)! \equiv -1 \pmod{p}.$$

2) If we set

$$f(x)=x^{p-1}-1-\prod_{m=1}^{p-1}(x-m),$$

then clearly

$$f(x)=c_0+c_1x+\cdots+c_{p-2}x^{p-2}.$$

By Theorem 76, the congruence

$$f(x)\equiv 0 \pmod{p}$$

has at least the $p-1$ roots $x\equiv 1, 2, \ldots, p-1$. Hence, by

$$c_0\equiv c_1\equiv\cdots\equiv c_{p-2}\equiv 0 \pmod{p}.$$

Our result then follows from the fact that

$$c_0=-1-(-1)^{p-1}(p-1)!$$