SELECTED TOPICS IN NUMBER THEORY

Hansraj Gupta

SELECTED TOPICS IN NUMBER THEORY

Hansraj Gupta

SELECTED TOPICS IN NUMBER THEORY

Hansraj Gupta

Honorary Professor, Panjab University, Chandigarh, India

ABACUS
PRESS

First published in 1980 by

ABACUS PRESS

Abacus House,
Speldhurst Road,
Tunbridge Wells,
Kent,
TN4 0HU,
England

British Library Cataloguing in Publication Data

Gupta, H
Selected topics in number theory.
1. Numbers, Theory of
I. Title
512'.7 QA241

ISBN 0-85626-177-7

Typeset in Great Britain by
Pintail Studios Ltd
Ringwood, Hampshire
and printed and bound by
Tien Wah Press (Pte.) Ltd, Singapore

TO THE READER

To the Reader

Books live longer than their authors. This is what provided me with the urge to write or rather compile this book from my own published and unpublished work to a large extent. I am entirely responsible for the choice of topics discussed in the book. It is very difficult for me to say if my choice has been a happy one, but I am very hopeful that you will not dislike it.

Though I received my education through the medium of the English language mostly, English is not my mother-tongue. It is quite possible that in places you may find me rather obscure, but a little effort on your part will, I am sure, make my meaning clear. In several places I have not given all the steps in the proof of a theorem. This will give you a good exercise in understanding the subject if you fill the 'blanks', so to speak, giving references to the theorems and results used. At the end of the book I have given a list of books and papers which will help you in continuing your study of the subject. Of the twelve chapters in the book as many as four (Chapters 7–10) deal with partitions: therefore the papers concerned with this topic are listed separately. The presentation is on the whole expository and some of my friends who have looked through parts of the work in typescript before publication have been kind enough to say a good word about it.

Of all branches of mathematics, number theory is the one that has not only provided food for serious thought but also created enthusiasm for the subject among young and old alike. I mentioned to a small boy (a school lad) that if he would take any four consecutive numbers greater than 11, at least one of them would be divisible by a prime greater than 11. He immediately started checking my statement mentally. I know of a very good applied mathematician who started taking keen interest in number theory, or rather the properties of natural numbers, towards the end of his life. If you like to enthuse your own son or daughter about the study of mathematics, give him or her some enticing results from numbers. For example:

$$45^2 = 2025 \quad \text{and} \quad 45 = 20 + 25; \qquad 99^2 = 9801 \quad \text{and} \quad 99 = 98 + 01$$

Any amount of such material is available in Albert H. Beiler's 'Recreations in the Theory of Numbers' (Dover, 1964). It is not without sense that number theory has been called 'The Queen of Mathematics'.

For a large part of my life, I was working in a small township away from what was then the only University in the Panjab. There was no library worth the name in or around the place. I was, therefore, rediscovering for myself many known results. For example, I did not know that symmetric functions representing the sums of the products of the first n natural numbers taken r at a time, were Stirling's Numbers of the first kind. The work presented in Chapters 5 and 6 was done mostly during the years 1931–1935 and formed part of my thesis for the Ph.D. degree. I hardly made any reference to the work done by others on the topic. It is very possible that what I have claimed to be new may be just a result discovered by a previous mathematician and only rediscovered by me. A great part of the material presented in these two chapters was published in a small monograph by the University of Lucknow in 1938. It has been included here by the kind permission of the University. Chapter 9 presents a proof by Professor G. Szekeres of a conjecture which Auluck, Chowla and myself had made in 1942. The version of his proof given here was kindly examined by him and approved. The proof has been included here with his kind permission. My thanks to Professor Szekeres.

My thanks are due also to numerous workers in the field, some of whose results I have included in this book. I am particularly thankful to Professor M. V. Subbarao for his many useful suggestions during my stay at Edmonton, where a part of this book was written in 1969–1970, and to several friends and students who read through parts of the book and helped me in clarifying certain points.

I shall thank any of my readers heartily if they point out to me any mistakes or misprints that they may find in the printed work.

Allahabad
India
August 1979

H. Gupta

CONTENTS

CHAPTER 1

PRELIMINARY

1. Introduction

We assume that the reader has already taken a course in Elementary Number Theory. In this preliminary chapter, we just give a résumé of the results with which the reader is surely familiar but to which he may want to refer now and then during the course of his study of this book. We do not prove all the results.

2. Natural numbers

The numbers $1, 2, 3, \ldots, n, \ldots$, the so-called natural numbers, can be placed in three classes:

(i) Those which have just one divisor;
(ii) Those that have exactly two divisors; and
(iii) Those that have more than two divisors.

Class (i) consists of only one element namely 1. Natural numbers which fall in class (ii) are

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

and are called primes. We usually use p to denote a prime. The rest of the natural numbers are placed in class (iii) and are called composite.

3. The fundamental theorem of arithmetic

It is easy to prove inductively that every natural number >1 can be expressed as a product of primes. What is really important is to realize that, disregarding the order in which the primes are written, the expression for any given n as a product of primes is unique. This is the fundamental theorem of arithmetic. For the proof, we need the following

LEMMA. *If the theorem is true for a certain $m > 1$ and p is any prime divisor of m, then p must appear in the expression for m as a product of primes.*

Proof. If $m = p$, there is nothing to prove. Otherwise, let

$$m = p \, . \, m_1, \quad \text{where} \quad m_1 > 1.$$

Let

$$m_1 = p_1 p_2 p_3 \ldots p_k,$$

where the p's are not necessarily distinct. Then

$$m = pp_1 p_2 p_3 \ldots p_k$$

is *an* expression for m as a product of primes. But we have assumed that the fundamental theorem holds for m, that is, but for the order in which the p's are written, this expression is unique. Hence this is *the only* expression for m as a product of primes. Since p appears in the expression, the lemma is proved.

Incidentally we have proved here that the expression for m_1 is also unique.

Proof of the fundamental theorem by H. Davenport. If possible, assume that n is the least number which has at least two *distinct* representations as a product of primes, say

$$n = p_1 p_2 p_3 \ldots p_k, \quad k \geqslant 2; \tag{1}$$

and

$$n = p'_1 p'_2 p'_3 \ldots p'_j, \quad j \geqslant 2. \tag{2}$$

Evidently then no p can be a p', for if $p_1 = p'_1$ then n/p_1, which is certainly less than n, will have two distinct expressions as a product of primes. Without loss of generality, we can assume that

$$p_1 \leqslant p_2 \leqslant p_3 \leqslant \cdots \leqslant p_k;$$

and

$$p'_1 \leqslant p'_2 \leqslant p'_3 \leqslant \cdots \leqslant p'_j.$$

Hence, we must have

$$n \geqslant p_1^2, \quad n \geqslant p_1'^2. \tag{3}$$

Since $p_1 \neq p'_1$, the sign of equality cannot hold in both places in (3). Therefore

$$n > p_1 p'_1. \tag{4}$$

Let $n - p_1 p'_1 = N$. Since $p_1 \mid n$ and also $p'_1 \mid n$, both p_1 and p'_1 divide N. Since $N < n$, the theorem holds for N and the lemma shows that we can write

$$N = p_1 p'_1 m. \tag{5}$$

This gives

$$n = p_1 p'_1 (m + 1) = p_1 p'_1 q_1 q_2 \ldots q_h, \tag{6}$$

say, where the q's are primes, not necessarily distinct from others on the right of (6). From (1) and (6), we now have

$$p'_1 q_1 q_2 \ldots q_h = n/p_1 = p_2 p_3 \ldots p_k. \tag{7}$$

We have thus obtained two distinct expressions as product of primes for n/p_1, distinct because p'_1 appears on the left of (7) but not in the expression on its right. This contradicts the minimality of n and the theorem follows.

Thus, every natural number $n > 1$ can be expressed uniquely in the *canonical* form

$$n = p_1^{c_1} p_2^{c_2} \dots p_k^{c_k}$$

where each $c \geqslant 1$, $k \geqslant 1$, and we take

$$p_1 < p_2 < \cdots < p_k.$$

Remarks

1. Defining the empty product of primes as 1, the fundamental theorem can be stated in the form:

Disregarding the order in which the primes are written, every natural number can be expressed uniquely as a product of primes.

2. Does the fundamental theorem need a proof at all? Has any one ever come across an example where the theorem has failed? The following example will convince the reader about the necessity of a proof.

Take the set

$$\{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, \dots\} \tag{8}$$

of natural numbers. It is easy to see that the set is closed under multiplication. Call an element of the set a 'prime' if it has exactly two divisors in the set. Thus, the primes of the set are

$$4, 7, 10, 13, 19, 22, 25, 31, \dots.$$

We observe that 100 belongs to the set and it can be written as a product of the primes of the set in two distinct ways:

$$100 = 4.25; \quad \text{also} \quad 100 = 10.10.$$

Exercises

1. Which is the next element of the set in (8) which has at least two distinct representations as a product of the primes of the set?
2. Consider the set consisting of all the numbers of the form $4n + 1$, where $n = 0, 1, 2, 3, \dots$. Define the 'primes' of this set and find the least element of the set having at least two distinct representations as a product of the primes of the set.

4. Infinitude of primes

THEOREM 1. *The number of primes is infinite.*

Proof. Suppose the system of natural numbers has only k primes

$$p_1, p_2, p_3, \dots, p_k.$$

Divide this set of primes into two disjoint subsets in any manner. Let

$$n = P_1 + P_2$$

where P_1 is the product of the primes in the first subset and P_2 of those in the second. (If one of the subsets is empty we take 1 to be the product of the primes in that subset.) Since the number of primes is certainly more than 1, $n > p_k$.

If a certain prime p belongs to the first subset, it divides P_1 but it does not divide P_2. If it belongs to the second subset, it divides P_2 but not P_1. Thus, none of the primes $p_1, p_2, \ldots, p_k$ divides n. Hence either n is itself a prime $> p_k$, or it has a prime divisor not in our list of primes. This proves the theorem.

Exercises

1. Find all the primes that can be obtained in the above manner from the set $\{2, 3, 5, 7\}$.
2. Let p_k^* denote the kth prime with $p_1^* = 2$. Find the largest k for which the above process applied to the set $\{p_1^*, p_2^*, \ldots, p_k^*\}$ yields only primes.
3. Show that $p_k^* < 2^{2^{k-1}}$.
4. For $k > 1$, show that the numbers $k! + h$, $h = 2, 3, \ldots, k$, are all composite. How big can the difference between two consecutive primes be?

5. The p-potency of n

The highest power of a prime p which divides a given natural number n is said to be its potency to the base p and written $\text{pot}_p\, n$. This is zero only if $p \nmid n$, otherwise it >1. We extend this definition to rational numbers by taking

$$\text{pot}_p \frac{n}{m} = \text{pot}_p\, n - \text{pot}_p\, m. \qquad (1)$$

The reader can now prove the following results for himself.

$$\text{pot}_p(nm) = \text{pot}_p\, n + \text{pot}_p\, m;$$
$$\text{pot}_p\, n^k = k\, \text{pot}_p\, n, \text{ for all integers } k.$$

Thus

$$\text{pot}_3\, 54 = 3, \quad \text{pot}_2\, 54 = 1, \quad \text{pot}_5\, 54 = 0,$$
$$\text{pot}_5\, 975 = 2; \text{pot}_7(686/35) = 3 - 1 = 2.$$

Exercises

1. Can the concept of potency be extended to composite bases? Give reasons for your answer.
2. Find the values of

   (i) $\text{pot}_3\, 891$; (ii) $\text{pot}_5(11!)$; (iii) $\text{pot}_2(98/24)$.

6. The potency of $n!$ to any base p

In what follows, we write $[x]$ for the integer for which

$$[x] < x < [x] + 1$$

x being any real number positive or negative. Thus, we have

$$[8/3] = 2, \quad [-8/3] = -3, \quad [28\sqrt{3}] = 48, \quad [-e] = -3.$$

The function $[x]$ is spoken of as the greatest integer function.

We can now find the formula for $\mathrm{pot}_p(n!)$ as follows.

$$\begin{aligned}\mathrm{pot}_p(n!) &= \mathrm{pot}_p\, 1 + \mathrm{pot}_p\, 2 + \mathrm{pot}_p\, 3 + \cdots + \mathrm{pot}_p\, n\\ &= \mathrm{pot}_p\, p + \mathrm{pot}_p(2p) + \mathrm{pot}_p(3p) + \cdots + \mathrm{pot}_p([n/p]\, p),\end{aligned}$$

Since

$$\mathrm{pot}_p(jp) = \mathrm{pot}_p\, p + \mathrm{pot}_p\, j = 1 + \mathrm{pot}_p\, j,$$

we get

$$\mathrm{pot}_p(n!) = [n/p] + \mathrm{pot}_p([n/p]!).$$

Using this reduction formula repeatedly, we obtain

$$\mathrm{pot}_p(n!) = [n/p] + [n/p^2] + \cdots + [n/p^k]$$

where $p^k \leqslant n < p^{k+1}$, or what is the same thing,

$$\mathrm{pot}_p(n!) = \sum_{j=1}^{\infty} [n/p^j].$$

For example

$$\mathrm{pot}_7(1000!) = 142 + 20 + 2 = 164.$$

This means that the highest power of 7 which divides 1000! is the 164-th.

7. The p-potency of the combinatory function $\binom{p^c}{r}$

THEOREM 2. *For any given prime p and $r < p^c$,*

$$\mathrm{pot}_p \binom{p^c}{r} = c - \mathrm{pot}_p\, r.$$

Proof. The theorem is trivially true for $r = 1$. For $r > 1$, the following simple proof is due to D. H. Lehmer. By definition

$$\binom{p^c}{r} = \frac{p^c}{r} \cdot \frac{p^c - 1}{1} \cdot \frac{p^c - 2}{2} \cdot \cdots \cdot \frac{p^c - (r-1)}{r-1}.$$

Observe that for $0 < r < p^c$,

$$\mathrm{pot}_p(p^c - j) = \mathrm{pot}_p\, j, \quad j = 1, 2, \ldots, r-1;$$

while

$$\mathrm{pot}_p(p^c/r) = c - \mathrm{pot}_p\, r.$$

Hence the theorem.

8. The p-potency of $\binom{n}{r}$, $r < n$

Written in the scale of p, let

$$n = (a_h, a_{h-1}, \ldots, a_1, a_0)_p.$$

This simply means that

$$n = a_h p^h + a_{h-1} p^{h-1} + \cdots + a_1 p + a_0,$$

where

$$0 \leqslant a_j < p, \quad \text{for} \quad j = 0, 1, 2, \ldots, h-1;$$

and

$$1 \leqslant a_h < p.$$

Similarly, let

$$r = (b_i, b_{i-1}, \ldots, b_1, b_0)_p.$$

Since $r < n$, we have $i \leqslant h$.

THEOREM 3. *The p-potency of* $\binom{n}{r}$, $r < n$, *is the same as the number of values of* j, $0 \leqslant j \leqslant h$, *for which*

$$(a_j, a_{j-1}, \ldots, a_0)_p - (b_j, b_{j-1}, \ldots, b_0)_p \tag{1}$$

is negative. (*We take* $b_j = 0$ *for each* $i < j \leqslant h$.)

The proof depends on the fact that

$$[n/p^{j+1}] - [r/p^{j+1}] - [(n-r)/p^{j+1}] = 1 \text{ or } 0$$

according as (1) is or is not negative, and is left to the reader. A practical method of determining the potency of $\binom{n}{r}$ is the following. In the representations for n and r in the scale of p, replace

a_t by 1 and b_t by 0, if $a_t > b_t$;

a_t and b_t both by 0, if $a_t = b_t$;

and

a_t by 0 and b_t by 1, if $a_t < b_t$;

also change p to 10. We thus get two numbers n^* and r^* in place of n and r. The p-potency of $\binom{n}{r}$ is now the same as the total number of eights and nines in the number $(n^* - r^*)$.

Example. Let us evaluate $\text{pot}_5 \begin{pmatrix} 188 \\ 39 \end{pmatrix}$.

We have

$$188 = (1223)_5, \quad 39 = (124)_5.$$

Hence

$$n^* = (1100)_{10}, \quad r^* = (001)_{10}.$$

Now

$$n^* - r^* = 1099,$$

and we get

$$\text{pot}_5 \begin{pmatrix} 188 \\ 39 \end{pmatrix} = 2.$$

8.1. An alternative method

As before, let

$$n = (a_h, \ldots, a_2, a_1, a_0)_p.$$

Define

$$A(n,p) = \sum_{k=0}^{h} a_k.$$

Notice that $A(n,p)$ denotes the sum of the digits in the representation of n in the scale of p. Then, it will be readily seen that

$$n - A(n,p) = \sum_{k=0}^{h} a_k(p^k - 1)$$

so that

$$\frac{n - A(n,p)}{p-1} = \sum_{k=1}^{h} a_k(p^{k-1} + \cdots + p^2 + p + 1)$$

$$= \sum_{k=1}^{h} (a_h p^{h-k} + \cdots + a_{k+1} p + a_k)$$

$$= \sum_{k=1}^{h} [n/p^k]. \quad \text{[J. L. Lagrange]} \tag{2}$$

The right side of (2) is nothing but the p-potency of $n!$.

Hence

$$\text{pot}_p \begin{pmatrix} n \\ r \end{pmatrix} = \{A(r,p) + A(n-r,p) - A(n,p)\}/(p-1). \tag{3}$$

Evidently (3) implies that

$$\operatorname{pot}_p\binom{n}{r} = \operatorname{pot}_p\binom{n}{n-r}.$$

Exercises

1. Deduce theorem 2 from (3).
2. Write 50! in the canonical form.
3. Express $\binom{29}{5}$ as a product of primes.
4. Using each of the two methods given in the text, find

$$\text{(i) } \operatorname{pot}_5\binom{625}{20}; \quad \text{(ii) } \operatorname{pot}_7\binom{98}{7}; \quad \text{(iii) } \operatorname{pot}_7\binom{12}{6}.$$

5. For the p-potency of $\binom{n}{r}$ to be more than 0, is it necessary that p divide n?
6. If $n = (\ldots, a_2, a_1, a_0)_p$, $r = (\ldots, b_2, b_1, b_0)_p$ show that

$$\binom{n}{r} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2} \ldots \text{(mod } p). \quad \text{[E. Lucas 1887]}$$

9. The functions $d(n)$, $\sigma(n)$ and $\sigma_r(n)$

Recall that $d(n)$ denotes the number of divisors (positive) of n, $\sigma(n)$ the sum of these divisors and $\sigma_r(n)$ the sum of their rth powers. Thus

$$d(n) = \sigma_0(n), \quad \sigma(n) = \sigma_1(n).$$

If the canonical expression for n is

$$n = p_1^{c_1} p_2^{c_2} \ldots p_k^{c_k},$$

then, we have

$$d(n) = (c_1 + 1)(c_2 + 1) \ldots (c_k + 1); \tag{1}$$

and

$$\sigma_r(n) = \prod_{j=1}^{k} (p_j^{r(c_j+1)} - 1)/(p_j^r - 1). \tag{2}$$

Note that (1) can be deduced from (2).

10. Euler's totient function $\phi(n)$.

The function $\phi(n)$ denotes the number of positive integers which do not exceed n and are prime to it.

Writing (a, b) for the g.c.d. of two positive integers a and b (here and throughout this book), we have by definition