Preface

These lectures are intended as an introduction to the elementary theory of numbers. I use the word "elementary" both in the technical sense—complex variable theory is to be avoided—and in the usual sense—that of being easy to understand, I hope.

I shall not concern myself with questions of foundations and shall presuppose familiarity only with the most elementary concepts of arithmetic, i.e., elementary divisibility properties, g.c.d. (greatest common divisor), l.c.m. (least common multiple), essentially unique factorizaton into primes and the fundamental theorem of arithmetic: if $p \mid ab$ then $p \mid a$ or $p \mid b$.

I shall consider a number of rather distinct topics each of which could easily be the subject of 15 lectures. Hence, I shall not be able to penetrate deeply in any direction. On the other hand, it is well known that in number theory, more than in any other branch of mathematics, it is easy to reach the frontiers of knowledge. It is easy to propound problems in number theory that are unsolved. I shall mention many of these problems; but the trouble with the natural problems of number theory is that they are either too easy or much too difficult. I shall therefore try to expose some problems that are of interest and unsolved but for which there is at least a reasonable hope for a solution by you or me.

The topics I hope to touch on are outlined in the Table of Contents, as are some of the main reference books.

Most of the material I want to cover will consist of old theorems proved in old ways, but I also hope to produce some old theorems proved in new ways and some new theorems proved in old ways. Unfortunately I cannot produce many new theorems proved in really new ways.