NUMBER THEORY

by Dr C. D. H. Cooper

5th EDITION January 2022

These notes were prepared for students at Macquarie University in Australia but are freely available to anyone. However if you make use of them and are not a Macquarie University student it would be nice if you could email me at christopherdonaldcooper@gmail.com to let me know where you are from. And, if you are from outside of Australia perhaps you could send me a postcard of where you are from to pin up on my wall (Christopher Cooper, 31 Epping Avenue, EASTWOOD, NSW 2122, Australia).

INTRODUCTION

Number Theory is one of the oldest branches of mathematics and until the latter half of the 20^{th} century was considered to be of no practical use. In fact number theorists often boasted about this, until the age of computers when suddenly prime numbers and the associated theory became the foundation for cryptography.

Number Theory explores the arithmetic of the integers, especially problems associated with divisibility. Prime numbers, having no non-trivial divisors, are especially important, yet often it is very difficult to prove theorems about them.

Greatest common divisors are discussed, including Euclid's algorithm. We show how we can work backwards through the calculations to express the GCD of m, n in the form
mh + nk. A new, and much improved, version of this algorithm is presented which sets the working out in tabular form and removes the need to work backwards.

Several chapters deal with congruence equations, where the equation holds modulo m, that is, integer equations after divisibility by m. We treat linear and quadratic congruences as well as congruences of the form $a^n \equiv 1 (\text{mod } m)$. The latter incorporates some new results. The chapter on quadratic congruences discusses the

problem of deciding, efficiently, whether or not a number has square roots modulo some modulus. The Legendre function and its properties are explained, to the extent that the existence of square roots can be determined. Complete proofs are given for these properties.

Diophantine equations are equations where we want to find integer solutions, if there are any. The most famous of these is Fermat's Last Theorem, involving the Diophantine equation $x^n + y^n = z^n$. For $n > 2$ this has no positive solutions. Although Fermat was convinced of the truth of this statement in the 17^{th} century it has taken till the end of the 20^{th} century for a proof to be found, a proof moreover that requires tools beyond the borders of Number Theory itself.

CONTENTS

1. DIVISIBILITY

2. LINEAR CONGRUENCES

3. QUADRATIC CONGRUENCES

4. SUMS OF SQUARES

5. DISTRIBUTION OF PRIMES

6. POWER CONGRUENCES

7. MERSENNE AND FERMAT PRIMES

8. MULTIPLICATIVE FUNCTIONS