Contents

Preface — *page* vii

Acknowledgement — viii

Part one: Preliminaries — 1

1 Introduction — 3

2 Notation and Auxiliary Results — 8

Part two: Bounds of Character Sums — 11

3 Bounds of Long Character Sums — 13

4 Bounds of Short Character Sums — 26

5 Bounds of Character Sums for Almost All Moduli — 31

6 Bounds of Gaussian Sums — 37

Part three: Multiplicative Translations of Sets — 47

7 Multiplicative Translations of Subgroups of $\mathbb{F}_p^*$ — 49

8 Multiplicative Translations of Arbitrary Sets Modulo p — 59

Part four: Applications to Algebraic Number Fields — 63

9 Representatives of Residue Classes — 65

10 Cyclotomic Fields and Gaussian Periods — 76

Part five: Applications to Pseudo-Random Number Generators — 89

11 Prediction of Pseudo-Random Number Generators — 91

12 Congruential Pseudo-Random Number Generators — 99

Part six: Applications to Finite Fields — 107

13 Small mth Roots Modulo p — 109

14 Supersingular Hyperelliptic Curves — 115

15 Distribution of Powers of Primitive Roots — 131

Part seven: Applications to Coding Theory and Combinatorics — 141

16 Difference Sets in V_{p} — 143

17 Dimension of BCH Codes — 148

18 An Enumeration Problem in Finite Fields — 154

Bibliography — 157

Index — 163