1. Record Nr. UNINA9910777087703321

Autore	Koniagin S. V (Sergei Vladimirovich)
Titolo	Character sums with exponential functions and their applications / / Sergei V. Konyagin, Igor E. Shparlinski [[electronic resource]]
Pubbl/distr/stampa	Cambridge : , : Cambridge University Press, , 1999
ISBN	1-107-12817-X 1-280-43245-4 9786610432455 0-511-17763-1 0-511-04036-9 0-511-14804-6 0-511-33017-0 0-511-54293-3 0-511-05179-4
Descrizione fisica	1 online resource (viii, 163 pages) : digital, PDF file(s)
Collana	Cambridge tracts in mathematics ; ; 136
Disciplina	512/.73
Soggetti	Exponential sums
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Title from publisher's bibliographic system (viewed on 05 Oct 2015).
Nota di bibliografia	Includes bibliographical references (p. 157-161) and index.
Nota di contenuto	pt. 1. Preliminaries -- 1. Introduction -- 2. Notation and Auxiliary Results -- pt. 2. Bounds of Character Sums -- 3. Bounds of Long Character Sums -- 4. Bounds of Short Character Sums -- 5. Bounds of Character Sums for Almost All Moduli -- 6. Bounds of Gaussian Sums -- pt. 3. Multiplicative Translations of Sets -- 7. Multiplicative Translations of Subgroups of F*[subscript p] -- 8. Multiplicative Translations of Arbitrary Sets Modulo p -- pt. 4. Applications to Algebraic Number Fields -- 9. Representatives of Residue Classes -- 10. Cyclotomic Fields and Gaussian Periods -- pt. 5. Applications to Pseudo-Random Number Generators -- 11. Prediction of Pseudo-Random Number Generators -- 12. Congruential Pseudo-Random Number Generators -- pt. 6. Applications to Finite Fields -- 13. Small mth Roots Modulo p -- 14. Supersingular Hyperelliptic Curves -- 15. Distribution of Powers of Primitive Roots -- pt. 7. Applications to Coding Theory and Combinatorics -- 16. Difference Sets in V[subscript

p] -- 17. Dimension of BCH Codes -- 18. An Enumeration Problem in Finite Fields.

Sommario/riassunto

The theme of this book is the study of the distribution of integer powers modulo a prime number. It provides numerous new, sometimes quite unexpected, links between number theory and computer science as well as to other areas of mathematics. Possible applications include (but are not limited to) complexity theory, random number generation, cryptography, and coding theory. The main method discussed is based on bounds of exponential sums. Accordingly, the book contains many estimates of such sums, including new estimates of classical Gaussian sums. It also contains many open questions and proposals for further research.