BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 39, Number 2, Pages 293–297
S 0273-0979(02)00937-0
Article electronically published on January 2, 2002

Character sums with exponential functions and their applications, by S. Konyagin and I. Shparlinski, Cambridge Univ. Press, New York, 1999, viii+163 pp., $49.95, ISBN 0-521-64263-9

The book *Character sums with exponential functions and their applications* by S. Konyagin and I. Shparlinski is a welcome addition to the theory of exponential and character sums, a classical topic from analyic number theory. It includes a number of timely applications in algebraic number theory, function fields, complexity theory, pseudo-random number generation, cryptography, and coding theory. This is an advanced monograph which will likely be of interest mostly to specialists and advanced students. In fact, a number of open research questions are outlined in the course of presentation. In order to place this work in a broader context, I will first provide a brief review of one classical set of ideas to which it contributes. Then I will turn to the topic at hand. Although it is somewhat specialized, it is also quite extensive, so my aim here will be only to provide a brief glimpse.

1. Background

The realization of the finite field $\mathbf{F}_p$ as $\mathbf{Z}/p\mathbf{Z}$ gives rise to a number of classical problems of analytic number theory. Among these are the problems of bounding the smallest quadratic non-residue (non-square) and the smallest primitive root (generator of $\mathbf{F}_p^*$) modulo p. More generally, one is interested in the distribution of subsets of $\mathbf{Z}/p\mathbf{Z}$ defined by algebraic conditions from $\mathbf{F}_p$ for large values of the prime p.

The usual tool for studying these examples is the character sum

$$S_\chi(x) = \sum_{1 \le n \le x} \chi(n)$$

or a suitably smoothed version, where χ is a Dirichlet character modulo p, that is a character of the multiplicative group of $\mathbf{F}_p$ pulled back naturally to $\mathbf{Z}$. For example, if $p > 2$ and

$$\chi(n) = (\frac{n}{p})$$

is the Legendre symbol,[1] then one detects the smallest quadratic non-residue by finding the smallest positive integer x in terms of p so that $S_\chi(x) < x$.

The primitive root problem needs all characters. It is an exercise in finite harmonic analysis to prove the following formula for the characteristic function $g(n)$ of the primitive roots modulo p for n not divisible by p:

$$g(n) = \frac{\phi(p-1)}{p-1} \sum_{d|(p-1)} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(n) \tag{1}$$

where the outer sum is over square-free integers d and the inner sum is over all characters χ_d modulo p of order d. Here $\phi(n)$ is the Euler totient function and $\mu(n)$

2000 *Mathematics Subject Classification.* Primary 11Lxx, 11Txx.

[1] $(\frac{n}{p})$ is 0 if $p|n$, while for $p \not| n$ it is 1 if n is a square modulo p and -1 otherwise.

is the Möbius function. This formula leads one once again to finding bounds for $S_{\chi_d}(x)$.

The Pólya-Vinogradov inequality (see [Dav]) gives the bound

$$|S_\chi(x)| \le \sqrt{p}\log p$$

for non-trivial χ which is, remarkably, independent of x. Thus it gives a non-trivial bound for $S_\chi(x)$ provided $x > \sqrt{p}\log p$. If N_p is the smallest quadratic non-residue, then this leads immediately to the bound[2] $N_p \ll p^{1/2+\varepsilon}$ for any $\varepsilon > 0$ and, using an elementary trick this was improved by Vinogradov (see [Mon]) to give

$$N_p \ll p^{\frac{1}{2\sqrt{e}}+\varepsilon}. \tag{2}$$

Similarly (1) leads to the bound

$$M_p \ll p^{1/2+\varepsilon} \tag{3}$$

for any $\varepsilon > 0$ for the smallest primitive root modulo p. In 1962 Burgess [Bur] succeeded in obtaining a non-trivial bound for $S_\chi(x)$ for smaller p relative to x by using A. Weil's proof of the Riemann hypothesis for curves. This led to the exponent $\frac{1}{4\sqrt{e}} + \varepsilon$ in (2) and $1/4 + \varepsilon$ in (3).

Deeper properties of the sum $S_\chi(x)$ are hidden in those of the Dirichlet L-function

$$L(s,\chi) = \sum_{n\ge 1} \chi(n) n^{-s}.$$

This function is entire (when χ is nontrivial; otherwise it has a simple pole at $s = 1$) and satisfies a functional equation relating s to $1 - s$ and χ to $\bar{\chi}$. Using classical complex analysis to relate the sum $S_\chi(x)$ to an integral involving $L(s,\chi)$, the question ultimately becomes one of bounding $L(s,\chi)$ for s on the critical line $Re(s) = 1/2$ in terms of p. From the functional equation and the convexity principle of Phragmén-Lindelöf it follows that

$$L(s,\chi) \ll p^{1/4+\varepsilon}$$

for $Re(s) = 1/2$, the implied constant now depending on s and ϵ. This leads to essentially the same result as the Polya-Vinogradov inequality, while the work of Burgess "breaks convexity". If one assumes the Generalized Riemann Hypothesis (GRH) for $L(s,\chi)$, that the nontrivial zeros of $L(s,\chi)$ lie on the critical line, then one may replace the 1/4 by 0, which is called the Lindelöf hypothesis in the level aspect. In fact, using the primes in a refinement allowed by the GRH, one may show, assuming its truth, that (see [Mon])

$$N_p \ll (\log p)^2. \tag{4}$$

Of course the GRH is unsolved! This problem was one of the motivations which brought Linnik to create the large sieve as a substitute for the Riemann hypothesis. His idea was to estimate the number of possible exceptions to a bound such as (4)

[2] Here we use notation $f \ll g$ to mean that there is a constant c, depending only on ε, such that $|f| \le cg$.

and conclude that the expected consequence of the GRH holds *almost always*. In analytic form the large-sieve inequality (see [Bom]) states

$$\sum_{q \leq Q} \sideset{}{^*}\sum_{\chi \bmod q} \Big| \sum_{n \leq N} c_n \chi(n) \Big|^2 \leq (N + Q^2) \sum_{n \leq N} |c_n|^2, \tag{5}$$

where the starred sum is over all primitive Dirichlet characters modulo q and the coefficients c_n are arbitrary complex numbers. Inequalities such as this, when enough flexibility in parameters is allowed, permit one to obtain results as strong, or even stronger than, the GRH would imply. After Iwaniec, the state of the art is to go backwards and obtain individual bounds from correctly positioned averages. The literature here is extensive; a recent advance leading to an improvement of the Burgess bound for $L(s, \chi)$ is given in [C-I].

2. The distribution of powers modulo p

The book of Konyagin and Shparlinski gives a detailed study of problems around the distribution of the powers g^x in $\mathbf{Z}/p\mathbf{Z}$ for some g not divisible by p. Clearly this topic belongs to the classical tradition outlined above, although mostly additive character sums (exponential sums) are employed in its treatment.

More exactly, the following problems are considered. For $(a, p) = 1$, $1 \leq N \leq t$, $0 \leq M < p$ and $1 \leq H \leq p$ let $T_a(N, M, H)$ denote the number of solutions in x of the equation

$$ag^x \equiv M + u \pmod{p} \tag{6}$$

where $1 \leq x \leq N$ and $1 \leq u \leq H$.
This book addresses the following questions:
i) What is the largest value of $|T_a(N, M, H) - NH/p|$ over all a and M?
ii) What are the restrictions on N and H under which $T_a(N, M, H) > 0$ for every M?
iii) For how many integers i up to $p/(H - 1)$ is $T_a(N, iH, H) > 0$?
iv) In terms of N what is the largest value of H for which $T_a(N, M, H) = 0$ for some M?
v) In terms of N what is the smallest value of H for which $T_a(N, M, H) = N$ for some M?
The role of the parameter a varies, and depending on the problem they obtain appropriate results for all a, a single special a, almost all a or even at least one "good" a. Similar questions are posed over algebraic number fields.

An example of an exponential sum that arises from (6) is

$$\sum_{x \leq t} e(ag^x/p)$$

where $e(z) = \exp(2\pi i z)$. Bounds are given for this sum both uniformly in a and for almost all moduli with various constraints.

Since many questions about the distribution of g^x modulo p are equivalent to similar ones about x^n modulo p where $n = (p-1)/t$, they are naturally led to Gauss sums of the type

$$S_n(a, q) = \sum_{1 \leq x \leq q} e(ax^n/q).$$

Here some new results are obtained for

$$A(n) = \sup_{q \geq 1} \frac{G_n(q)}{q^{1-1/n}}$$

where

$$G_n(q) = \operatorname*{Max}_{gcd(a,q)=1} |S_n(a,q)|.$$

For example, it is shown in Theorem 6.7 that

$$A(n) = 1 + O(n^{-1}\tau(n)\ln n)$$

where $\tau(n)$ is the divisor function. Mostly the techniques used are elementary yet sophisticated. In fact, the bulk of the book is devoted to a variety of applications. Some of these are enumerated by the authors and include:

1. Egami's question about the smallest norm representatives of the residue classes modulo **q** and Euclid's algorithm.
2. Prediction of the $1/M$-pseudo-random number generator of Blum, Blum and Shub and the linear congruential generator.
3. Girstmair's problem about the relative class number of subfields of cyclotomic fields and Myerson's problem about Gaussian periods.
4. Kodama's question about supersingular hyperelliptic curves.
5. Tompa's question about lower bounds for the QuickSort algorithm.
6. Lenstra's constants modulo **q** and Győry's arithmetical graphs.
7. Estimating the dimension of BCH codes.
8. Robinson's question about small m-th roots modulo p.
9. Hastad, Lagarius and Odlyzko's question about the average value of smallest elements in multiplicative translations of sets modulo p.
10. Niedereiter's problem about the multiplier of linear congruential pseudo-random number generators.
11. Stechkin's question about the constant in the estimate of Gaussian sums.
12. Odlyzko and Stanley's problem about 0,1-solutions of a certain congruence modulo p.

References for these questions are provided on p. 5, and other applications are given as well. It is perhaps surprising that such a diverse collection of problems may be unified under one theme. This book should serve as a useful reference for mathematicians interested in such problems as well as a valuable source of open questions for research projects.

References

[Bom] Bombieri, E., Le grand crible dans la théorie analytique des nombres. (French) [The large sieve in analytic number theory] Second edition. Astérisque No. 18 (1987). MR **88g:**11064

[Bur] Burgess, D.A., On character sums and primitive roots, Proc. London Math. Soc. III, 12, 179–192 (1962). MR **24:**A2569

[C-I] Conrey, J. B.; Iwaniec, H., The cubic moment of central values of automorphic L-functions. Ann. of Math. (2) 151 (2000), no. 3, 1175–1216 MR **2001g:**11070

[Dav] Davenport, H., Multiplicative number theory. Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000 MR **2001f:**11001

[Mon] Montgomery, H.L., Topics in Multiplicative Number Theory, Lecture Notes in Math. vol. 227, Springer-Verlag (1971). MR **49:**2616

W. Duke
University of California, Los Angeles
E-mail address: `wdduke@ucla.edu`