THE LEAST QUADRATIC NONRESIDUE AND VINOGRADOV'S HYPOTHESIS.

Abdunabiyev Jamshid Olimjon o'g'li
TerDU matematika yo'nalishi
1-kurs magistranti

Abstract: *Let α_m and β_n be two sequences of real numbers supported on [M,2M] and [N,2N] with M = $X^{1/2-\delta}$ and N = $X^{1/2+\delta}$. We show that there exists a $\delta_0 > 0$ such that the multiplicative convolution of α_m and β_n has exponent of distribution $\frac{1}{2} + \delta - \varepsilon$ (in a weak sense) as long as $0 \le \delta < \delta_0$, the sequence β_n is Siegel-Walfisz and both sequences α_m and β_n are bounded above by divisor functions. Our result is thus a general dispersion estimate for "narrow" type-II sums. The proof relies crucially on Linnik's dispersion method and recent bounds for trilinear forms in Kloosterman fractions due to Bettin-Chandee. We highlight an application related to the Titchmarsh divisor problem.*

Keywords: *equidistribution in arithmetic progressions, dispersion method.*

Introduction

Let p be an odd prime. We denote $\mathbf{e}(z) = \exp(2\pi iz/p)$ and use χ to denote a non-principal multiplicative character modulo p. An enormous number of number theoretic (and not only) results depend on bounds of exponential and character sums

$S(N;f) = {}^{X}\mathbf{e}(f(n))$and $\quad T(N;f) = {}^{X}\chi(f(n))$

$1 \le n \le N \qquad 1 \le n \le N$

with a polynomial f with integer coefficients of degree $n \ge 1$, see [7, 8, 9, 10, 11, 12, 13] and references there in. The celebrated *Weil bound* asserts that for $N = p$, that is, for *complete sums* we have

$|S(p;f)| \le (n-1)p^{1/2}$and $\quad |T(p;f)| \le (n-1)p^{1/2} \qquad (1)$

unless there is "an obvious" reason why this cannot be true. In the case of the sums $S(N;f)$ this reason is simply the fact that f is a constant polynomial modulo p, In the case of the sums $T(N;f)$ this reason is simply the fact that f is a kth power of another polynomial modulo p, where k is the order of the character χ. Under a similar conditions one has bounds for *incomplete sums*

$|S(N;f)| = O(np^{1/2}\log p) \qquad$ and $\qquad |T(N;f)| = O(np^{1/2}\log p) \qquad (2)$

96 Igor E. Shparlinski

for every $N \le p$.

Polynomials of large degree

One immediately remarks that the bounds (1) are useless if $n > p^{1/2}$. Despite a half a century history of attempts to obtain a general nontrivial result beyond the square-root bound, we still do not know any such result. However, in some special cases, very ingenious methods have been invented, see [1, 2, 5, 6, 4], which may be a good indication (and even a way to go) that sich a non-trivial general bound exists. Proving such a bound or showing that it does not exist would have a tantalasing effect on a vast number of areas such as number theory, algebraic geometry, coding theory, theoretic computer science and cryptography.

Short sums

Even if n is small (for example $n = 2$) the bounds (2) are also useless for "short" sums with $N \le p^{1/2}$ and generally the situation seems to be a mirror reflection of the situation with polynomials of large degree. However, here there is one important exception for linear polynomials. Namely, the celebrated *Burgess bound* [3] asserts that if for any $\varepsilon > 0$ there is $\delta > 0$ such that if $N \ge p^{1/4+\varepsilon}$ then

$$\left|\sum_{n=1}^{N} \chi(n+a)\right| = O(Np^{-\delta}) \qquad (3)$$

for any integer a, see also [7, 10]. Curiously enough, all know proofs of this bound are based on the Weil bound (1).

This naturally leads to two questions:

• *What about even shorter sums? For example with $N \ge p^{\varepsilon}$?*

This question seems to be extremely hard, such a bound does not even follow from the Extended Riemann Hypothesis (at least not in a obvious way, unless $a = 0$). Moreover it would immediately imply the famous Vinogradov's conjectures about the smallest quadratic non-residue and primitive root modulo p (both are believed to be of order $O(p^{\varepsilon})$. Thus it would probably be too ambitious to believe that we will be able to prove a nontrivial bound for N of order p^{ε}. However, moving beyond $1/4 + \varepsilon$ could be a much easier but still enormosuly important achievement.

• *What about extending the Burgess bound* (3) *to polynomials of higher degree? For example $n = 2$?*

Again, it seems that even the Extended Riemann Hypothesis is of no help here. Besides being a very natural number theoretic problem, such a bound would have a number of applications, including better analysis of a polynomial factorisation algorithm over finite fields, see Section 1.1 (and Problem 1.3 in particular) in [11]. Even the special case of quadratic polynomials of the form $f(X) = (X + a)(X + b)$ (the only one needed for the aforementioned purpose) seems to be hard (however, it is not infeasible to hope for some progress in the nearest future).

REFERENCES:

[1] J. Bourgain, *Mordell type exponential sum estimates in fields of prime order*, Comptes Rendus Mathematique **339** (2004), 321–325.

[2] J. Bourgain, *Mordell's exponential sum estimate revisited*, Preprint, 2004.

[3] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika **4** (1957), 106– 112.

The 10th problem 97

[4] T. Cochrane, J. Coffelt and C. G. Pinner, *A further refinement of Mordell's bound on exponential sums*, Acta Arith. **116** (2005), 35–41.

[5] T. Cochrane and C. G. Pinner, *Stepanov's method applied to binomial exponential sums*, Quart J. Math. **54** (2003), 243–255.

[6] T. Cochrane and C. G. Pinner, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. **133** (2005), 313–320.

[7] H. Iwaniec and E. Kowalski, *Analytic number theory*, (Amer. Math. Soc. Providence 2004).

[8] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, (Cambridge Univ. Press Cambridge 1999).

[9] N. M. Korobov, *Exponential sums and their applications*, (Kluwer Acad. Publ. Dordrecht 1992).

[10] R. Lidl and H. Niederreiter, *Finite fields*, (Cambridge University Press Cambridge 1997).

[11] I. E. Shparlinski, *Finite fields: Theory and computation*, (Kluwer Acad. Publ. Dordrecht 1999).

[12] I. E. Shparlinski, *Cryptographic applications of analytic number theory*, (Birkhauser 2003). [13] R. C. Vaughan, *The Hardy–Littlewood method*, (Cambridge Univ. Press Cambridge 1981).