THE SUM-PRODUCT ESTIMATE FOR LARGE SUBSETS OF PRIME FIELDS

M. Z. GARAEV

(Communicated by Ken Ono)

ABSTRACT. Let $\mathbb{F}_p$ be the field of prime order p . It is known that for any integer $N \in [1, p]$ one can construct a subset $A \subset \mathbb{F}_p$ with $|A| = N$ such that

$$\max\{|A + A|, |AA|\} \ll p^{1/2}|A|^{1/2}.$$

One of the results of the present paper implies that if $A \subset \mathbb{F}_p$ with $|A| > p^{2/3}$, then

$$\max\{|A + A|, |AA|\} \gg p^{1/2}|A|^{1/2}.$$

1. INTRODUCTION

Let $\mathbb{F}_p$ be the field of residue classes modulo a prime number p and let A be a nonempty subset of $\mathbb{F}_p$. Consider the sum set

$$A + A = \{a + b : a \in A, b \in A\}$$

and the product set

$$AA = \{ab : a \in A, b \in A\}.$$

From the work of Bourgain, Katz, Tao [5] and Bourgain, Glibichuk, Konyagin [4] it is known that if $|A| < p^{1-\delta}$, where $\delta > 0$, then one has the sum-product estimate

$$(1) \quad \max\{|A + A|, |AA|\} \gg |A|^{1+\varepsilon}$$

for some $\varepsilon = \varepsilon(\delta) > 0$. This result and its versions have found many important applications in various areas of mathematics.

In the corresponding problem for integers (i.e., if the field $\mathbb{F}_p$ is replaced by the set of integers) the conjecture of Erdős and Szemerédi [7] is that $\max\{|A + A|, |AA|\} \gg |A|^{2-\varepsilon}$ for any given $\varepsilon > 0$. At present the best known bound in the integer problem is $\max\{|A + A|, |AA|\} \gg |A|^{14/11}(\log |A|)^{-3/11}$ due to Solymosi [12].

Explicit versions of (1) have been obtained in [8]–[11]. For subsets with relatively small cardinalities (say, $|A| < p^{13/25}$), in [8] we proved the bound

$$\max\{|A + A|, |AA|\} \gg |A|^{15/14}(\log |A|)^{O(1)},$$

which was subsequently improved in [10] to

$$\max\{|A + A|, |AA|\} \gg |A|^{14/13}(\log |A|)^{O(1)}.$$

Received by the editors June 26, 2007.

2000 *Mathematics Subject Classification*. Primary 11B75, 11T23.

Key words and phrases. Sum-product estimates, prime field, number of solutions.

©2008 American Mathematical Society
 Reverts to public domain 28 years from publication

In [8] we also considered the case of subsets with larger cardinalities, which had been previously studied in [9]. We showed, for example, that

$$\max\{|A + A|, |AA|\} \gg \min\{|A|^{2/3}p^{1/3}, |A|^{5/3}p^{-1/3}\}(\log |A|)^{O(1)}.$$

One may conjecture that the estimate

$$\max\{|A + A|, |AA|\} \gg \min\{|A|^{2-\varepsilon}, |A|^{1/2}p^{1/2-\varepsilon}\}$$

holds for all subsets $A \subset \mathbb{F}_p$. The motivation for the quantity $|A|^{1/2}p^{1/2-\varepsilon}$ is clear from the constructions in [2, 6], which can be described as follows. Let g be a generator of $\mathbb{F}_p^*$. By the pigeon-hole principle, for any $N \in [1, p]$ and for any integer $M \approx p^{1/2}N^{1/2}$ (which we associate with $M \pmod{p}$), there exists L such that

$$|\{g^x : 1 \leq x \leq M\} \cap \{L + 1, L + 2, \dots, L + M\}| \gg M^2/p \gg N.$$

Obviously, any subset $A \subset \{g^x : 1 \leq x \leq M\} \cap \{L + 1, L + 2, \dots, L + M\}$ with $|A| \approx N$ satisfies $\max\{|A + A|, |AA|\} \ll p^{1/2}|A|^{1/2}$.

Thus, it follows that for any integer $N \in [1, p]$ there exists a subset $A \subset \mathbb{F}_p$ with $|A| = N$ such that

$$\max\{|A + A|, |AA|\} \ll p^{1/2}|A|^{1/2}.$$

In the present paper we prove the following statement.

Theorem 1. *Let $A \subset \mathbb{F}_p$. Then*

$$|A + A||AA| \gg \min\left\{p|A|, \frac{|A|^4}{p}\right\}.$$

In view of the foregoing discussion, in the range $|A| > p^{2/3}$ our result implies the optimal in the general setting bound

$$\max\{|A + A|, |AA|\} \gg p^{1/2}|A|^{1/2}.$$

In papers [1, 3] one can find deep results on sum-product estimates in $\mathbb{Z}_m$ with applications; here $\mathbb{Z}_m$ is the ring of residue classes modulo a positive integer m . In [14] an analogy of the sum-product estimate from [9] has been obtained for subsets of $\mathbb{Z}_m$. The following generalization of Theorem 1 improves the corresponding result from [14].

Theorem 2. *Let $A \subset \mathbb{Z}_m$, $m > 1$. Then*

$$|A + A||AA| \gg \min\left\{m|A|, \frac{|A|^4}{m} \left(\sum_{\substack{d|m \\ d < m}} d^{1/2}\right)^{-2}\right\}.$$

We remark that if $m = p^2$, $A = \{px : x \in \mathbb{Z}_m\}$, where p is a prime number, then $|A| = |A + A| = m^{1/2}$, $|AA| = 1$ and the left-hand side of the estimate of Theorem 2 is of the same order of magnitude as the right-hand side.

Below we use the abbreviation $e_k(z) = e^{2\pi iz/k}$. The residue classes, where it is needed, are associated with their integer representatives.

2. PROOF OF THEOREM 1

We can assume that $\{0\} \not\subset A$. Consider the equation

$$(2) \quad xa_1^{-1} + a_2 = y, \quad (x, a_1, a_2, y) \in (AA) \times A \times A \times (A + A).$$

For any triple $(a_1, a_2, a_3) \in A \times A \times A$ the quadruple

$$(a_1a_3, a_1, a_2, a_3 + a_2) \in (AA) \times A \times A \times (A + A)$$

is a solution of (2). To different triples $(a_1, a_2, a_3) \in A \times A \times A$ correspond different solutions $(a_1a_3, a_1, a_2, a_3 + a_2)$. Thus, the number J of solutions of the equation (2) satisfies $J \geq |A|^3$. Expressing J via additive characters and following the standard procedure, we obtain

$$\begin{aligned} |A|^3 &\leq J = \frac{1}{p} \sum_{n=0}^{p-1} \sum_{x \in AA} \sum_{a_1 \in A} \sum_{a_2 \in A} \sum_{y \in A+A} e_p(n(xa_1^{-1} + a_2 - y)) \\ &\leq \frac{|AA||A|^2|A+A|}{p} + \frac{1}{p} \sum_{n=1}^{p-1} \left| \sum_{x \in AA} \sum_{a_1 \in A} e_p(nxa_1^{-1}) \right| \left| \sum_{a_2 \in A} \sum_{y \in A+A} e_p(n(a_2 - y)) \right|. \end{aligned}$$

Since

$$\max_{(n,p)=1} \left| \sum_{x \in AA} \sum_{a_1 \in A} e_p(nxa_1^{-1}) \right| \leq \sqrt{p|AA||A|}$$

(see, for example, [13, Chapter VI]), we have

$$|A|^3 \leq \frac{|AA||A|^2|A+A|}{p} + \frac{\sqrt{p|AA||A|}}{p} \sum_{n=0}^{p-1} \left| \sum_{a_2 \in A} e_p(na_2) \right| \left| \sum_{y \in A+A} e_p(ny) \right|.$$

Applying the Cauchy-Schwarz inequality to the sum over n , we get

$$|A|^3 \leq \frac{|AA||A|^2|A+A|}{p} + \sqrt{p|AA||A|} \sqrt{|A||A+A|},$$

and the result follows.

Remark. The reader may note that the proof of Theorem 1 gives, more generally, the bound

$$|A+B||AC| \gg \min \left\{ p|A|, \frac{|A|^2|B||C|}{p} \right\}$$

for any nonempty subsets A, B, C of $\mathbb{F}_p^*$.

3. PROOF OF THEOREM 2

Let us first reduce the problem to the case $A \subset \mathbb{Z}_m^*$. Let

$$d_0 = \min \{ (a, m) : a \in A \}.$$

Since

$$[0, m) = \bigcup_{j=1}^{d_0} \left[(j-1) \frac{m}{d_0}, j \frac{m}{d_0} \right),$$

we have

$$|AA| \geq |d_0 A| \geq \frac{|A|}{d_0}.$$

If

$$|A|^2 \leq \frac{4m}{d_0} \left(\sum_{\substack{d|m \\ d < m}} d^{1/2} \right)^2,$$

then

$$\frac{|A|^4}{m} \left(\sum_{\substack{d|m \\ d < m}} d^{1/2} \right)^{-2} \leq \frac{4|A|^2}{d_0} \leq 4|A||AA| \leq 4|A + A||AA|,$$

and the statement becomes trivial in this case. Thus, we can assume that

$$|A|^2 > \frac{4m}{d_0} \left(\sum_{\substack{d|m \\ d < m}} d^{1/2} \right)^2.$$

But then we have that

$$\begin{aligned} \{a \in A : (a, m) > 1\} &= \{a \in A : (a, m) \geq \max\{d_0, 2\}\} \leq \sum_{\substack{d|m \\ d \geq \max\{d_0, 2\}}} \frac{m}{d} \\ &= \sum_{\substack{d|m \\ d \leq \min\{m/d_0, m/2\}}} d \leq \left(\frac{m}{d_0}\right)^{1/2} \sum_{\substack{d|m \\ d < m}} d^{1/2} < \frac{|A|}{2}. \end{aligned}$$

Hence, $|A \cap \mathbb{Z}_m^*| > |A|/2$. Denoting $A \cap \mathbb{Z}_m^*$ again by A we deduce that it suffices to deal with the case $A \subset \mathbb{Z}_m^*$.

We can also assume that $|A|^3 > 2|AA||A|^2|A + A|/m$, since otherwise we are done. Following the proof of Theorem 1, we obtain

$$|A|^3 \leq \frac{2}{m} \sum_{n=1}^{m-1} \left| \sum_{x \in AA} \sum_{a_1 \in A} e_m(nxa_1^{-1}) \right| \left| \sum_{a_2 \in A} \sum_{y \in A+A} e_m(n(a_2 - y)) \right|.$$

For a given divisor $d|m$ we collect together those n for which $(n, m) = d$. Thus, denoting n/d by n again, we get

$$|A|^3 \leq \frac{2}{m} \sum_{\substack{d|m \\ d < m}} \sum_{\substack{n=1 \\ (n, m/d)=1}}^{m/d} \left| \sum_{x \in AA} \sum_{a_1 \in A} e_{m/d}(nxa_1^{-1}) \right| \left| \sum_{a_2 \in A} \sum_{y \in A+A} e_{m/d}(n(a_2 - y)) \right|.$$

Since $(n, m/d) = 1$, we have

$$\left(\left| \sum_{x \in AA} \sum_{a_1 \in A} e_{m/d}(nxa_1^{-1}) \right| \right)^2 \leq |AA| \sum_{x=0}^{m-1} \left| \sum_{a_1 \in A} e_{m/d}(xa_1^{-1}) \right|^2 \leq dm|AA||A|.$$

Thus,

$$|A|^3 \leq \frac{2|A|^{1/2}|AA|^{1/2}}{m^{1/2}} \sum_{\substack{d|m \\ d < m}} d^{1/2} \sum_{n=1}^{m/d} \left| \sum_{a_2 \in A} e_{m/d}(na_2) \right| \left| \sum_{y \in A+A} e_{m/d}(ny) \right|.$$

Using the inequalities

$$\sum_{n=1}^{m/d} \left| \sum_{a_2 \in A} e_{m/d}(na_2) \right|^2 \leq m|A|, \quad \sum_{n=1}^{m/d} \left| \sum_{y \in A+A} e_{m/d}(ny) \right|^2 \leq m|A + A|,$$

we deduce that

$$|A|^3 \leq 2|A|^{1/2}|AA|^{1/2}m^{1/2}|A|^{1/2}|A+A|^{1/2} \sum_{\substack{d|m \\ d < m}} d^{1/2}.$$

This proves Theorem 2.

ACKNOWLEDGEMENTS

The author is grateful to A. Granville and S. V. Konyagin for very useful remarks. This work was supported by the Project PAPIIT IN 100307 from UNAM.

REFERENCES

- [1] J. Bourgain, *The sum-product theorem in Z_q with q arbitrary*, preprint.
- [2] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, Int. J. Number Theory **1** (2005), 1–32. MR2172328 (2006g:11041)
- [3] J. Bourgain and M.-C. Chang, *Exponential sum estimates over subgroups and almost subgroups of Z_Q^* , where Q is composite with few prime factors*, Geom. Funct. Anal. **16** (2006), 327–366. MR2231466 (2007d:11093)
- [4] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) **73** (2006), 380–398. MR2225493 (2007e:11092)
- [5] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), 27–57. MR2053599 (2005d:11028)
- [6] M.-C. Chang, *Some problems in combinatorial number theory*, preprint.
- [7] P. Erdős and E. Szemerédi, *On sums and products of integers. Studies in pure mathematics*, 213–218, Birkhäuser, Basel, 1983. MR820223 (86m:11011)
- [8] M. Z. Garaev, *An explicit sum-product estimate in F_p* , Int. Math. Res. Notices (2007), no. 11, Art. ID rnm035. MR2344270
- [9] D. Hart, A. Iosevich and J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Notices (2007), no. 5, Art. ID rnm007. MR2341599
- [10] N. H. Katz and Ch.-Y. Shen, *A slight improvement to Garaev’s sum product estimate*, preprint.
- [11] N. H. Katz and Ch.-Y. Shen, *Garaev’s inequality in fields not of prime order*, preprint.
- [12] J. Solymosi, *On the number of sums and products*, Bull. London Math. Soc. **37** (2005), 491–494. MR2143727 (2006c:11021)
- [13] I. M. Vinogradov, *An introduction to the theory of numbers*, Pergamon Press, London and New York, 1955. MR0070644 (17:13a)
- [14] V. Vu, *Sum-product estimates via directed expanders*, arXiv:0705.0715v1 [math.CO].

INSTITUTO DE MATEMÁTICAS, UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, CAMPUS MORELIA, APARTADO POSTAL 61-3 (XANGARI), C.P. 58089, MORELIA, MICHOACÁN, MÉXICO
E-mail address: garaev@matmor.unam.mx