Unlikely intersections

CIRM Workshop 3–7 February 2014

Organizers: Igor Shparlinski

An amazingly large number of problems in number theory and cryptography lead to the following generic question : given two sets $\mathcal{A}$ and $\mathcal{B}$ defined by two seemingly unrelated conditions, prove that the intersection $\mathcal{A} \cap \mathcal{B}$ is sparse. The term "unlikely intersections" for problems of this type was introduced by Bombieri, Masser and Zannier [3], see also [4]. Out of all problems of this type the most commonly occurring in number theory and cryptography is the case when these sets $\mathcal{A}$ and $\mathcal{B}$ are taken to be one of the following types

- an arithmetic progression $\mathcal{I} = \{ai + b \ : \ i = 1, \ldots, h\}$ of length h,
- a multiplicative subgroup $\mathcal{G}$,
- an algebraic variety $\mathcal{V}$.

In particular, a variety of estimates on $\#(\mathcal{I} \cup \mathcal{G})$ have been given in [2, 10, 11, 21, 26].

Furthermore, let integers a and g satisfy $\gcd(ag, p) = 1$. Given two intervals $\mathcal{I}$ and $\mathcal{J}$, we denote by $R_{a,g,p}(\mathcal{I}, \mathcal{J})$ the number of solutions of the congruence

$$x \equiv ag^z \pmod{p}, \quad (x, z) \in \mathcal{I} \times \mathcal{J}. \tag{1}$$

Investigation of $R_{a,g,p}(\mathcal{I}, \mathcal{J})$ is heavily based on the methods of additive combinatorics. For example, let $H_{g,p}(N)$ be the largest H such that $R_{a,g,p}(\mathcal{I}, \mathcal{J}) = 0$ for some a with $\gcd(a, p) = 1$ and intervals $\mathcal{I}$ and $\mathcal{J}$ of lengths H and N, respectively.

In the case where the length of $\mathcal{J}$ is equal to the multiplicative order t modulo p of g, Bourgain, Konyagin & Shparlinski [10, Theorem 7] have given the following estimate of $H_{g,p}(t)$ (improving that of Konyagin & Shparlinski [23, Theorem 7.10]) :

Theorem 4.1. *For any element $g \in \mathbf{F}_p^*$ of multiplicative order $t \geq p^{1/2}$ we have*

$$H_{g,p}(t) \leq p^{463/504 + o(1)}$$

as $p \to \infty$.

It is easy to see that using the new bound of Shkredov [26] in the argument of [10] one can improve Theorem 4.1.

Theorem 4.1 and other results of [10] have found several more number theoretic applications. These applications include a series of results on Fermat quotients [5, 13, 25, 28, 29], pseudopowers [9] and the distribution of digits in g-ary expansions of rational fractions [30].

Recent results of Shkredov [26, 27] immediately lead to improvements of the estimates from [5, 9, 13, 25, 28, 29] and probably have many other applications (the results of [30] are already based on [26]).

Combining the ideas from [6] and [10], Konyagin & Shparlinski [24, Theorem 2] obtained the following result.

Theorem 4.2. *Let $\nu \geq 1$ be a fixed integer. Then for any primitive root $g \in \mathbf{F}_p$ and $p > N > p^{1/2}$ the following bound holds :*

$$H_{g,p}(N) \leq N^{-47/72 + (2\nu+1)/6\nu(\nu+1) + o(1)} p^{95/72 - 1/6(\nu+1)} + N^{-47/96 + 1/4\nu + o(1)} p^{119/96 - 1/4\nu}$$

as $p \to \infty$.

In particular, in the most interesting case of $N = p^{1/2+o(1)}$, the optimal value of ν is $\nu = 72$; thus

$$H_{g,p}(p^{1/2+o(1)}) \le p^{62635/63072+o(1)} = p^{0.9930714...}.$$

In the symmetric case, when both $\mathcal{I}, \mathcal{J}$ are of the same length h, Chan & Shparlinski [12] have noticed that classical sum-product theorem of Bourgain, Katz & Tao [8] gives a nontrivial estimate on $R_{a,g,p}(\mathcal{I}, \mathcal{J})$ for any h. Stronger upper bounds on $R_{a,g,p}(\mathcal{I}, \mathcal{J})$, that are given by Bourgain, Garaev, Konyagin & Shparlinski [7] and Cilleruelo & Garaev [17], are also based on the ideas that stem from the methods of additive combinatorics.

Some of the above results can be presented in a more general setting of almost arithmetic and geometric progressions. We say that sets $\mathcal{I} \subseteq \mathbf{F}_p$ and $\mathcal{G} \subseteq \mathbf{F}_p$ are an *almost arithmetic progression* and an *almost geometric progression* if for every fixed positive integer k we have

$$\#(k\mathcal{I}) = \#\mathcal{I}p^{o(1)} \qquad \text{and} \qquad \#\left(\mathcal{G}^k\right) = \#\mathcal{G}p^{o(1)},$$

as $p \to \infty$. Upper bounds on

$$\#(\mathcal{I} \cap \mathcal{G}) \qquad \text{and} \qquad \#\left(\mathcal{I} \cap \mathcal{J}^{-1}\right)$$

have been given in [1].

Besides upper bounds on intersections between small groups and intervals, Bourgain [2] have also found applications of methods of additive combinatorics to studying the distribution of products xu where $x \in \mathcal{I}$ is take from a small interval $\mathcal{I}$ and $u \in \mathcal{G}$ is taken from a small subgroup $\mathcal{G} \subseteq \mathbf{F}_p^*$, see [2]. Hegyvári & Hennecart [21] have considered more general products $f(x)u$ with a polynomial f.

Studying intersections of zero sets of varieties with cartesian products of intervals and multiplicative subgroups is also a very challenging and important direction, see [15, 16, 18, 19, 20, 22].

These questions can also be considered over the complex or real numbers, residue ring $\mathbf{Z}/m\mathbf{Z}$, matrix rings and other algebraic domains.