Shkredov, Ilya D.
On some applications of GCD sums to arithmetic combinatorics. (English) Zbl 07419384
J. Number Theory 231, 433-450 (2022)

The paper at hand proves some new instances of the sum-product phenomenon over the integers. Theorems 1 and 12 provide an upper bound on the joint multiplicative energy of the (truncated) set of primes and an arbitrary set of integers (which holds under some technical conditions which we will not describe in this review). As a corollary, for example, the following is proven: if $S \subset \mathbb{Z}$ satisfies $|SS| \ll |S|$, then any arithmetic progression in $S$ which begins at zero must be of size at most $\ll \log |S| \cdot \log \log |S|$. Interestingly, this corollary may be viewed as obtaining an upper bound in an integer analogue of the well-studied (though still quite poorly understood) least quadratic non-residue problem in $\mathbb{Z}/p\mathbb{Z}$. Indeed, the set of squares in $\mathbb{Z}/p\mathbb{Z}$ is closed under multiplication, and an upper bound on the size of the largest arithmetic progression which starts at zero belonging to this set is clearly also an upper bound on the least quadratic non-residue. In fact, up to constant factors, the upper bound obtained here over the integers matches the best known (conditional on GRH) lower bound in $\mathbb{Z}/p\mathbb{Z}$. It is, however, unclear whether the same answer should be expected across contexts.

In a slightly different direction, given finite sets $A, S \subset \mathbb{Z}$ with control over the size of the sumset $|A + A|$ and under some other technical conditions which we will not describe, the author obtains in Theorem 2 a lower bound on the size of the set $|(A - a)S|$ for a particular $a \in A$ (one therefore also trivially obtains a lower bound on $|(A - A)S|$).

The proofs of the aforementioned results use the method of ‘GCD sums’. Loosely, one relates multiplicative energies to sums involving GCDs, which in turn may be bounded in terms of moments of a random zeta function like
\[
\zeta_X(\alpha) := \prod_p (1 - X_p/p^\alpha)^{-1},
\]
where the $X_p$ are i.i.d. uniformly distributed on $S^1$, for which upper bounds may be relatively directly obtained. We direct the reader to [M. Lewko and M. Radziwiłł, Adv. Math. 305, 280–297 (2017; Zbl 1375.11056)] for more on this connection and method.

Finally, the author proves in Theorem 4 upper bounds on the joint additive energy of a suitably convex set and an arbitrary set. The proof proceeds purely combinatorially and without recourse to the arithmetic of the integers; indeed, the results hold over $\mathbb{R}$.

Reviewer: Daniel Altman (Oxford)

MSC:
11B30 Arithmetic combinatorics; higher degree uniformity
11A05 Multiplicative structure; Euclidean algorithm; greatest common divisors

Keywords:
GCD sums; arithmetic combinatorics; sum-product

Full Text: DOI arXiv

References:
[1] Aistleitner, C.; El-Baz, D.; Munsch, M., A pair correlation problem, and counting lattice points with the zeta function (2020)
[2] Ankeny, N. C., The least quadratic non residue, Ann. Math. (2), 55, 65-72 (1952) · Zbl 0046.04006
[3] Balog, A.; Roche-Newton, O.; Zhelezov, D., Expanders with superquadratic growth, Electron. J. Comb., P3-P14 (2017) · Zbl 1373.52021
[4] Bloom, T. F.; Walker, A., GCD sums and sum-product estimates, Isr. J. Math., 235, 1, 1-11 (2020) · Zbl 1450.11094
[5] Bondarenko, A.; Seip, K., Large greatest common divisor sums and extreme values of the Riemann zeta function, Duke Math.
