Applications of additive combinatorics methods to some multiplicative problems

Rafał Bystrzycki

The main aim of this dissertation is the study of different ways in which additive combinatorics may be used to tackle some problems arising in multiplicative number theory. Specific problems studied here concern computational complexity of calculating values of number-theoretic functions, sums of dilates and exponential sums.

The main part of the thesis deals with the following problem: Suppose that for some natural number n and some prime number p we are given the set of residues mod p of all its divisors and we would like to know which of those residues correspond to prime factors of n. An algorithm which approximately solves this problem for p and n satisfying some natural conditions is presented and it is proved that there are plenty of such numbers. One interesting feature of the proof is that it relies on additive combinatorics. The proposed algorithm consists of two algorithms, which performed one after another lead to the solution. Failure of the first part implies the structural properties captured by the notion of additive energy of the set which are then used by the second, more intricate part based on techniques from Fourier analysis.

The main theorem of this part states that for a squarefree integer n satisfying some constraints and a prime number p satisfying some other technical conditions if we are given the set of residues modulo p of all divisors of n (denoted A_p), there exists an efficient deterministic algorithm which finds a set B such that $\Gamma_p \subset B \subset A_p$ (where Γ_p denote the set of residues of prime divisors of n) and $|B| < \epsilon |A_p|$.

All conditions appearing in the assumptions are very weak and in fact occur for almost every squarefree number n and for enough primes p in order to be practical. In this way, we show that for all but $o(x)$ squarefree numbers less than x and a suitable p (dependent only on x, not on n), the set B from theorem can be found. We also give an application of this result to the algorithm which finds factorization of a given number using an oracle for values of functions $\sigma_k(n)$. In fact, the search for deterministic reductions of factorization to some other number-theoretic problems was our original motivation to study this problem.

In the next part of the thesis the problem concerning exponential sums is studied. More specifically the following expression

$$s(a/q) = \sum_{r=1}^{\tau} e\left(\frac{a2^r}{q}\right),$$

where $e(x) := \exp(2\pi i x)$ and τ is multiplicative order of an element corresponding to number 2, is considered. Absolute value of this sum is estimated. The results we obtained in this line of research are the following. We give an upperbound with a better constant than previously known (given by Kaczorowski and Molteni) and provide some new examples where this bound is close to being tight.

In the last part of the thesis bounds for the size of sums of dilates are considered. Sums of dilates are sets of the form

$$\lambda_1 \cdot A + \cdots + \lambda_h \cdot A,$$

where for any scalar λ and any sets of integers A, B we take the notation $\lambda \cdot A = \{\lambda a : a \in A\}$ and $A + B = \{a + b : a \in A, b \in B\}$. Series of results giving upperbounds on the size of this set is proved under the small doubling condition, namely A satisfies $|A + A| < K|A|$ for some constant K.

The most general bound obtained here has the form $K^{O\left(\frac{rh}{\log(h)} + h\log(h)\right)}|A|$, where r denotes the maximal number of bits of coefficients and h is the number of summands. It consists an improvement over the result of Bukh.

Our next theorem applies to the case when K is much smaller than h. It shows that then the dependence on h becomes polynomial under those assumptions. Hence it improves on a previous theorem in such circumstances.

Our last theorem considers the case when Λ - the set of λ_i coefficients - has some additive structure. In such a setting a spectacular improvement is possible. If we denote by L the doubling constant of Λ, then the bound takes the form $K^{O((h+r)L\log L)}|A|$.

Rafał Bystrzycki