SIMON KUTTNER, Carleton University

Applications of the subset sum problem over finite abelian groups

Given a finite abelian group G, a finite set D, and a mapping $f : D \to G$, we find the number of r-subsets $S \subseteq D$ where for $b \in G$,

$$\sum_{x \in S} f(x) = b.$$

We obtain simple exact expressions when f is an abelian group homomorphism. When $G = \mathbb{F}_q$, we extend known results when $D \in \{\mathbb{F}_q, \mathbb{F}_q^*\}$ and $f(x) = x^N$, which include quadratic and semiprimitive cases. We count degree n monic polynomials over $\mathbb{F}_q$ with r distinct roots in a set $D \subseteq \mathbb{F}_q$ when the leading terms of degree at least $n - \ell$ are fixed. We obtain new formulas for $\ell = 1$ when D is a multiplicative subgroup of $\mathbb{F}_q^*$, and for $\ell = 2$ when D is an arbitrary subfield of $\mathbb{F}_q$ with q odd.