Idempotents and number theory

Štefan Porubský

Idempotents (elements satisfying the identity $e \cdot e = e$) represent an important structural element in semigroups (algebraic structure endowed with an associative binary operation). Existence of idempotents is actually equivalent with the existence of subgroups in a given semigroup. More precisely, every identity elements of a subgroup is an idempotent, and conversely around every idempotents these lives at least one sub(semi)group of the given semigroup (e.g. the cyclic (semi)group generated by an element a power of which is the given idempotent). Though the complex of such subgroups and subsemigroups could be rich and mirrors arithmetic properties of connected algebraic structures, their role was studied very sporadically hitherto. For instance, in the semigroup of residue classes modulo n we have 2^r distinct idempotents and connected complexes of subgroups and subsemigroups, where r is the number of distinct prime divisors of n. Besides the well-known group of the reduced residue classes connected with idempotent 1 and the semigroup of nilpotent residue classes around 0, there are additional ones provided $r > 1$. A typical demonstration example of their presence is the analysis of the classical Euler-Fermat theorem, Bauer identical congruence or Wilson Theorem given by Štefan Schwarz and enabling him to deduce many variants of these important elementary results in multiplicative semigroups of various matrix structures, of power sets of a finite set or of binary relations on a finite set. His approach is capable of a wide generalization giving a way to extend these results to more general commutative rings appearing in number theory as it was done by the author of this talk and M. Laššák. In this survey talk we show some of these applications as well some new ones, e.g. in a solution of a simple linear congruence $ax \equiv b \pmod{n}$.