Graphs, Digits, and Cryptography

WED/P1
11:00–11:40

Clemens Heuberger (TU Graz)

Non-standard digital expansions occur in a natural way in the solution of some problems in Graph theory as well as in the efficient implementation of public key cryptosystems.

One of the topological indices of interest in mathematical chemistry is the Merrifield-Simmons index, i.e., the number of independent subsets of a graph. If the maximum degree is fixed (which is a reasonable assumption in the context of chemistry), there is a unique tree maximising the Merrifield-Simmons index, and it is described by a digital system with non-standard digits. I report on joint work with S. Wagner on these trees as well as the related digital system.

A frequent operation in public key cryptography is scalar multiplication in Abelian groups, e.g., the point group of an elliptic curve over a finite field. One way to speed up the computations is the use of an appropriate digital expansion of the scalar. I briefly review some of the well-known ideas and will focus on my own contributions jointly achieved with R. Avanzi, J. Muir and H. Prodinger. One of the problems is to find optimal expansions given a certain set of digits. This can be formulated as a graph theoretical problem, and methods from combinatorial optimisation lead to “automatic” proofs.