New findings on conjectures used in number theory with significance in cryptography on the cards

Interesting new findings on theoretical speculations in number theory may soon emerge from India. Scientists are working on new cases of Stark conjectures, hypothetical information about the leading terms of L-functions in number theory. These conjectures have direct applications to Hilbert’s 12th problem, one of the central problems in algebraic number theory, this theory has significance in cryptography, for instance, for generating elliptic curves for use in cryptosystems.

Number theory concerns the study of integer solutions to polynomial equations with integer coefficients. Solving such equations, in general, is challenging. They are studied by attaching various invariants—function, quantity, or property, which remains unchanged when a specific transformation is applied.

A very classical, fruitful, and much-studied invariant is the L-function (function on the complex plane, associated to one out of several categories of mathematical objects). Some of the deepest problems in modern number theory are concerned with proving exact formulae for the values of L-functions at integer points in terms of purely arithmetic objects. Professor Mahesh Kakde from the Department of Mathematics at the Indian Institute of Science, Bengaluru, one of the recipients of this year’s SwarnaJayanti fellowship instituted by the Department of Science & Technology, Government of India, concentrates on proving such exact formulae using various methods, including algebra, K-theory and the theory of modular forms.

Prof. Kakde’s recent work concentrates on proving conjectures made in the 1970s by the American mathematician Harold Stark postulating the existence of special elements related to leading terms of L-functions. With support from the SwarnaJayanti fellowship, Prof. Kakde will use a completely novel method to prove deep relationships between different Stark elements. Such relationships have hitherto been only proven in very special cases, and in these cases, Stark conjectures are already known. He intends to turn this on its head and use results from their research along with the results on conjectures by mathematicians’ Armand Brumer, Benedict Gross, and Harold Stark called the Brumer—Stark conjecture and the Gross—Stark conjectures to prove new cases of Stark conjectures.

For more details, Professor Mahesh Kakde (maheshkakde@iisc.ac.in) can be contacted.