Extension: 56419   Email: yfyang@math.nctu.edu.tw

Prof. Yi-Fan Yang / Department of Applied Mathematics

Number Theory, modular forms

Number theory is one of the oldest branches of mathematics. It is mainly concerned with properties and relations among rational numbers, integers, and their generalizations. For example, Fermat’s last theorem, which asserts that if is an integer greater than 2 and is an integer solution of the equation , then one of the three integers must be 0, is one of the most famous problems in number theory. In order to solve problems in number theory, mathematicians used ideas and tools from other areas of mathematics, such as algebra, geometry, differential equations, complex analysis, and discrete mathematics, to name a few. This in turn stimulates the development of other areas of mathematics.

In the past, number theory has been considered as a branch of pure mathematics, but in the past three decades, this has changed and mathematicians have found applications of number theory in cryptography and coding theory. For example, the RSA cryptosystem and the elliptic curve cryptosystem, which are commonly used in e-commerce and other security-related situations nowadays, are both based on theories from number theory.

Our research is mainly focused on construction and applications of modular forms and related problems about modular curves and Shimura curves. In short, a modular form is an analytic function with many symmetries. Naturally, we would expect that a function satisfying such special requirement must have lots of interesting properties. Indeed, mathematicians have found that a modular form carries a lot of arithmetic information and can be used to solve problems in number theory. For example, the proof of Fermat’s Last Theorem given by Andrew Wiles is in fact a proof of a certain connection between arithmetic properties of elliptic curves and those of modular forms. Nowadays, it is well-established that modular forms lies at the cross road of representation theory, arithmetic geometry, string theory, quantum field theory, and many others. Even though modular forms have been studied for one and half a centuries, there are still many open problems that need to be solved. Also, their higher-rank generalizations remain significant challenges to mathematicians.