Computability, Complexity, and Effectivity in Number Theory

Gisbert Wüstholz (Eidgenössische Technische Hochschule Zürich and University of Zürich)

Finding solutions of algebraic equations in rational numbers is a central question in number theory with applications also in other parts of natural sciences. This already begins with linear equations like the famous abc-conjecture.

One of the very significant areas in mathematics is cryptography, which uses the full strength of mathematical research. The well-known Rivest–Shamir–Adleman (RSA) cryptosystem is conceptually an almost trivial application of elementary number theory. However, in reality a big amount of highly non-trivial number theory comes together. Conceptually much less trivial are the elliptic cryptosystems, where non-linear equations, so-called elliptic curves, play the key role. They depend on parameters and consequently have much higher flexibility. Here, very deep concepts of arithmetic have to be used and have led to very difficult problems of the existence and computability of solutions of relatively simply looking algebraic equations. This has an enormous impact in particular on cryptography. We shall try to give a glance onto the beautiful parts of modern arithmetic with emphasis on computability and complexity. Of course, in the background one finds everywhere algorithms.