Arithmetic Geometry: Deep Theory, Efficient Algorithms and Surprising Applications

Gerhard Frey, University of Duisburg-Essen

One of the most astonishing success stories in recent mathematics is arithmetic geometry, which unifies methods from classical number theory with algebraic geometry ("schemes"). In particular, the extremely important role of the Galois groups of base schemes like rings of integers of number fields or curves over finite fields as algebraic equivalent of the topological fundamental group and its representations induced by the action on divisor class groups of varieties over these domains yielded spectacular results like Serre's Conjecture for two-dimensional representations of the Galois group of $\mathbb{Q}$, which implies for example the modularity of elliptic curves over $\mathbb{Q}$ and so Fermat's Last Theorem (and much more).

At the same time the algorithmic aspect of arithmetical objects like lattices and class groups of global fields became more and more important and accessible, stimulated by and stimulating itself the advances in theory.

Both aspects are used for the very surprising transformation of one of the purest parts of mathematics to an applied science: data security, at least depends crucially on results and methods of arithmetical geometry.

A first and very important example is ***coding*** theory using both the theory of lattices and of vector spaces over finite fields attached to Riemann-Roch spaces of curves.
Going further in this direction and applying the whole arsenal of algorithms and theory of arithmetic geometry one can deal with divisor class groups of curves over finite field in a very efficient way and then these groups can be used for public key ***crypto*** systems based on the problem of discrete logarithms in finite groups. But one has to be very careful since the obtained insights play a constructive and destructive role for the security of the systems. Algorithms for fast scalar multiplication and point counting make it possible to use such divisor classes in cryptographically relevant instances but, at the same time, yield algorithms for the computation of discrete logarithms that are in many cases "too fast" for security. The good news is that there is a narrow but (hopefully) not empty range of candidates usable for public key cryptography at least for attacks based on ***conventional*** computer algorithms.

In the lecture we shall try to give an overview on the methods and results obtained in the area described above. In addition, we shall discuss recent results and ideas emerging because of the better understanding of isogenies. Again, we have negative implications for security but also new ideas for public key protocols that generalize the Diffie-Hellman key exchange, and there is a vague hope that such protocols could be resistant against ***quantum*** computers.