Previous research

Takanori Ayano

The theory of elliptic functions was the main subject of research in the 19th century and the concrete theory of elliptic functions was constructed. It is applied to many fields in mathematics and science. As the technology advances, there are movements to apply the Abelian functions, which are generalizations of the elliptic functions to many variables, to many fields in mathematics and science. Via the Abel–Jacobi map, the algebraic functions on algebraic curves correspond to the Abelian functions. My purpose of research is to construct the concrete theory of the Abelian functions and apply it to cryptography, number theory, and integrable systems.

The elliptic sigma functions $\sigma(u)$ and the elliptic functions $\wp(u)$, which are defined and studied by Weierstrass, are generalized to the multivariable sigma functions and the Abelian functions associated with the hyperelliptic curves by F. Klein and H. F. Baker about 100 years ago. In the 1990s, V. M. Buchstaber, V. Z. Enolski, and D. V. Leykin generalized the theory of the hyperelliptic sigma functions and the hyperelliptic Abelian functions to a plane curve called (n, s) curve. I extended the theory of the sigma functions and the Abelian functions for the (n, s) curves to telescopic curves, which are studied in coding theory. The telescopic curves include the (n, s) curves. I think that this result will give the great progress in the theory of the Abelian functions.

The Abelian function associated with a hyperelliptic curve of genus g is a meromorphic function on $\mathbb{C}^g$ that satisfy $2g$ periodicity conditions on $\mathbb{C}^g$. Baker, Buchstaber, Enolski, and Leykin proved that the Abelian functions associated with hyperelliptic curves satisfy the KdV–equations. For hyperelliptic curves of genus 3, I constructed the theory of the meromorphic functions that satisfy 6 periodicity conditions on the zero set of the sigma functions and derived the partial differential equations integrable by these functions, which is a joint work with V. M. Buchstaber. These partial differential equations are two parametric deformations of the KdV–equations.

In the 19th century, many mathematicians such as Jacobi, Kowalewski, Königsberger, and Bolza gave many examples of hyperelliptic integrals that can be reduced to elliptic integrals. This problem is closely related to the coverings of algebraic curves, split Jacobians, the automorphism groups of algebraic curves, and Humbert varieties. This knowledge is applied to the isogeny based cryptography. In [Enolski and Salerno 1996], when a hyperelliptic curve of genus 2 admits a morphism of degree 2 to an elliptic curve, the relationships between the hyperelliptic functions of genus 2 and the Jacobi elliptic functions are derived. I derived the relationships between the hyperelliptic functions of genus 2 and the Weierstrass elliptic functions under the same conditions as [Enolski and Salerno 1996], which is a joint work with V. M. Buchstaber. In integrable systems and mathematical physics, when solutions of differential equations are expressed in terms of the Abelian functions associated with an algebraic curve, it is important to express them in terms of the Abelian functions associated with algebraic curves of lower genus. In cryptography, it is important to reduce computations on algebraic curves to those on algebraic curves of lower genus. Our results can be applied to integrable systems and cryptography.