Abstract:
In SCIS 2017, M. Shirase proposed a new factoring algorithm for integers by combining elliptic curve method (ECM) with complex multiplication method which is one of generating methods of elliptic curves. This algorithm works in polynomial time for a composite having a prime factor of special form which is related to the complex multiplication theory. However, the range of application of this algorithm is limited. We give a generalization and extend the range of application. In this talk, firstly I will give a brief explanation of ECM and complex multiplication theory. After that, I will explain the generalized algorithm. This is a joint work with K. Nuida and M. Shirase.