慶應義塾大学　21世紀COEプログラム
「統合数理科学：現象解明を通した数学の発展」

Pathways Lecture Series in Mathematics, Keio

Speaker ： Prof. Hyungju Park
(Korean Institute for Advanced Study)

Date: March 13, Monday
Place: Bldg14, 2F Room 204, Yagami Campus

Lecture 1 **11:00-12:30** Combinatorial study of algebro-geometric objects via monomial ideals

Computational methods in commutative algebra and algebraic geometry has relatively short history. At the turn of the 20th century, mathematicians like Macaulay demonstrated constructive spirit. But their work has been largely forgotten during mostof the 20th century, and only recently their influence is being rediscovered in several contexts.

Most significant contribution in this line of work is Buchberger‘s introduction of Grobner basis in 60s. It took many years fort his concept to be accepted by main-stream mathematicians. With the ever-growing power of computers, it is now viewed as a universal Engine behind algebraic or symbolic computation.

In this short survey, we will try to explain what makes computations possible in commutative algebra and algebraic geometry without going into full detail. Our theme would be the deformation of a given ideal to a monomial ideal on which many difficult problems become fairly simple combinatorial problems.

Date: Mach 14, Tuesday, 2006
Place:Bldg14, 2F Room 204, Yagami Campus

Lecture 2 **13:00-14:30** Combinatorial-Algebraic Cryptosystems and Polynomial-based Cryptography

In early 90's, Koblitz and Fellows reputed the common place view thatNP-problems can not be used to construct good cryptosystems. Since NP-problems can be converted to polynomial system solving problems, they called this line of approach Combinatorial-Algebraic (CA). While not many developments have been made in CA Cryptogragraphy for the most of 90's, several noticeable results started appearing recently. In the mean time,another cryptosystems called HFE became popular whose security is also based on the difficulty of solving multivariate polynomial systems. So far, themost successful attack on these polynomial-based cryptosystems is known tobe based on Grobner bases. We will outline the research issues in this lineof approach to cryptography.

Lecture 3 **15:00-16:30** Algebraic approach to multidimensional systems theory

Multidimensional signal processing is an area of growing interest due to the emergence of images and other multimedia signals as important data format.However, many well-understood problems in audio processing are considerablyharder in higher dimensions, and the digital nature of the underlying signals and systems makes algebraic methods a natural fit.

問合わせ先：慶應義塾大学21世紀COEプログラム　統合数理科学 渉外担当
横浜市港北区日吉3－14－1
Tel: 045-566-1442 Fax: 045-566-1768 e-mail: coe-admin@math.keio.ac.jp
URL: http://coe.math.keio.ac.jp