平成 30 年度理学系研究科公開セミナー

計算アーキテクチャーと素因数分解

株式会社富士通研究所　伊豆哲也

期日：平成31年3月2日(土) 14:00～16:00
場所：大阪府立大学中百舌鳥キャンパス　A12 サイエンスホール

プログラム

13:30　開場
14:00　開会の挨拶
　　溝口　幸司（理学系研究科長）
14:10　「イントロダクション－素因数分解はなぜ重要なのか？暗号の視点から」
　　川添　充　（理学系研究科・教授）
14:40　「計算アーキテクチャーと素因数分解」
　　伊豆　哲也（株式会社富士通研究所）
15:50　質疑応答
16:00　閉会

セミナー概要

2019 を 3×673 という素数の積に分解する計算は素因数分解と呼ばれ、小学校の算数で学習するおなじみの問題です。2019 のような小さな自然数であれば暗算でも素因数分解できますが、20190302 (＝2×11×11×83481) や 2019030214 (＝2×18947×53281) のような大きな自然数に対しては、暗算は厳しくなり、計算機の出番となります。計算機を使うとどれくらい大きな数の素因数分解ができるのでしょうか。この問いは、数学として興味があるというだけでなく、暗号の安全性とも関係することから、現実の社会にとって重要な問題でもあります。本セミナーでは、計算機を使った場合のいくつかの素因数分解法や、どのような大きさの合成数が実際に素因数分解されているかの記録を紹介するとともに、このような素因数分解法を使ったとしても素因数分解ができないようなもっと大きな合成数について、計算機の計算ルールを変更し、新しい計算アーキテクチャーを利用することで、素因数分解が簡単に解けるようになるかもしれないことを紹介します。具体的には、量子ゲート計算機（いわゆる量子計算機）と、量子アニーリング計算機による素因数分解法と、それぞれの素因数分解法による記録を紹介します。

●事前の参加申し込み・参加費は不要です。

大阪府立大学
OSAKA PREFECTURE UNIVERSITY
高度研究型大学～世界に翔く地域の信頼拠点～

問い合わせ先
〒599-8531 大阪府堺市中区学園町１－１
大阪府立大学大学院理学系研究科支援室
TEL: 072-254-9161
主催：大阪府立大学大学院理学系研究科