

## 第 8 回「代数学と計算」研究集会

The 8th Symposium on Algebra and Computation (AC2009)

日本応用数学会正会員の方の AC2009 での発表論文は Jsiam Letters 誌への投稿機会が与えられます。詳しくは Jsiam Letters 誌についての web を御参照ください。

なおこの研究集会は、科学研究費補助金基盤研究 (C)「計算機による散在型単純群のモジュラー表現解析」(課題番号 19540004 代表 脇克志) および日本応用数学会「数論アルゴリズムとその応用」研究部会活動促進費から一部助成を受けております。

代数学と計算は、主に代数学と計算機科学との関わりを中心に幅広い分野から話題をとりあげ、普段独立して議論されることが多い各分野の交流を深めることを目的として始められた研究集会で今回で 8 回目になります。

<http://tnt.math.metro-u.ac.jp/ac/2009/>

主催者 中村 憲 (首都大学東京)  
脇 克志 (山形大学)  
津村 博文 (首都大学東京)  
内山 成憲 (首都大学東京)

### 記

日時：2007 年 12 月 2 日 (水) ~ 4 日 (金)

場所：首都大学東京 国際交流会館

東京都八王子市南大沢 1-1

## プログラム [Program]

12月2日(水)

9:55 - 10:00: Opening

10:00 - 10:20: 宋慧玲, 伊藤浩行 (広島大)

“巨大有限体の構成について”

10:20 - 10:40: 新谷誠 (静岡大)

“互いに素な シュタイナー系  $S(5,8,24)$  と  $5-(24,12,48)$  デザイン”

11:00 - 11:40: 松岡聡 (産業技術総合研究所)

“MLL プルーフネットの符号理論的研究”

13:30 - 14:20: [特別講演] 蓮尾一郎 (京大数理解析研究所/JST さきがけ)

“小宇宙原理とコンポーネント計算：計算機システムの基礎理論としての普遍代数・余代数をめぐって”

14:40 - 15:10: 知念宏司 (近畿大)

“一般 Hamming 符号から作られる不変式の Riemann 予想について”

15:10 - 15:40: 原田昌晃 (山形大/JST さきがけ)

“Extremal Type II  $\mathbb{Z}_{2k}$ -codes”

16:00 - 16:20: 三枝崎剛 (北海道大), 坂内英一 (九州大)

“ユークリッド空間における 2 次元整数格子のある性質”

16:20 - 16:50: 藤田育嗣 (日本大), 寺井伸浩 (足利工大)

“楕円曲線  $E: y^2 = x^3 - nx$  の生成元”

12月3日(木)

10:00-10:20: 森川良三 (首都大)

“ワーリングタイプの問題を探求する為の、いくつかの概念と方法 II”

10:20 - 10:50: 酒井祐貴子, 橋本喜一郎 (早稲田大)

“ $\sqrt{2}$  乗法をもつ曲線と Humbert のモジュラー方程式の一般化について”

11:10 - 11:40: 大石亮子 (高エネルギー加速器研究機構)

“トポグラフを用いた 3 次元粉末結晶の格子を決定するアルゴリズム”

13:30 - 14:20: [特別講演] 黒田茂 (首都大)

“多項式環をめぐるいくつかの話題”

14:35 - 15:10: 清野善裕, 吉田仁, 金田康正 (東大)

“Riemann zeta 関数の零点とその計算の基礎について”

15:10 - 15:40: 村田玲音 (明治学院大), 神谷諭一 (大東文化大)

“数論的関数とコード・システムのある関係について”

16:00 - 16:20: 谷口哲也 (東京理科大)

“非正則素数の高速計算”

16:20 - 16:40: 長谷川武博 (都留文科大), 犬塚美代子, 鈴木隆文

“関数体の塔に関する Elkies 予想の数値的証拠”

12月4日(金)

10:00 - 10:20: 小松尚夫 (弘前大), Chris K. Caldwell (University of Tennessee at Martin)

“Powers of Sierpinski numbers base  $b$ ”

10:20 - 10:40: 堀口直之 (千葉大)

“Hall-Janko 群で不変な rank 3 グラフと rank 4 グラフについて”

11:00 - 11:30: 平野貴人, 田中圭介 (東工大)

“1 のベキ乗根とその暗号への応用”

11:30 - 12:00: 佐々木義卓, 大野泰生, 山崎知佳 (近畿大)

“ある離散対数問題に関する古典アルゴリズムと量子アルゴリズムの比較について”

– JANT セッション 『格子と暗号の数理』 –

14:00 - 14:10: 小暮淳 (富士通研)

“格子と暗号の数理”

14:10 - 15:00: 島田伊知朗 (広島大)

“超特異  $K3$  曲面と格子理論”

15:20 - 16:10: 田中圭介 (東工大)

“イデアル格子を用いた Fully Homomorphic Encryption について”

16:10 - 17:00: 國廣昇 (東大)

“RSA 暗号に対する格子攻撃”

17:00 - 17:10: Closing