ISSN 1881-6193

RIMS Kôkyûroku Bessatsu B90

Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties

edited by Shushi Harashita, Momonari Kudo, Katsuyuki Takashima

June, 2022
Research Institute for Mathematical Sciences
Kyoto University

RIMS ***Kôkyûroku Bessatsu*** *B90*

Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties

October 13 ∼ 15, 2020

edited by Shushi Harashita, Momonari Kudo, Katsuyuki Takashima

June, 2022

Research Institute for Mathematical Sciences

Kyoto University, Kyoto, Japan

Preface

This volume is the proceedings of the conference “Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties”, held from October 13th to 15th, 2020. This conference is supported by the joint research program of the Research Institute for Mathematical Sciences (RIMS) of Kyoto University and was planned to be held at RIMS, but unfortunately was held online (Zoom) due to the covid-19 epidemic.

We had two aims of this conference. The first was to follow the international conference Supersingular Abelian Varieties and Related Arithmetic held at Nagoya in 2019. The second was to include, in a single conference, topics not only on the theory of supersingular curves and supersingular abelian varieties but also on its applications such as post-quantum cryptography using supersingular isogenies, hoping that the conference would give fruitful contribution to interaction between theoretical aspect and practical one on supersingular things.

In this conference, we have 16 lectures and 128 participants (the affiliated institutions of 64 among them are outside Japan). The organizers thank all the lectures and all the participants for their kind cooperation and their active discussions in this conference.

June, 2022
Shushi Harashita, Momonari Kudo, Katsuyuki Takashima

Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties

October 13th - 15th, 2020

RIMS Conference

PROGRAM

All times are given in Japan standard time JST (UTC+09:00).

Tuesday, October 13th (UTC+09:00)

09:40 – 09:50	Opening

Morning session

09:50 – 10:50	**Shushi Harashita** Supersingular abelian varieties and curves, and their moduli spaces
11:10 – 12:10	**Tomoyoshi Ibukiyama** Supersingular loci of low dimensions and parahoric subgroups

Afternoon session

14:00 – 15:00	**Chia-Fu Yu** Polarized simple superspecial abelian surfaces with real Weil numbers
15:20 – 16:20	**Jean-Stefan Koskivirta** Abelian varieties and stacks of G-zips
16:40 – 17:40	**Toshiyuki Katsura** On the classification of Enriques surfaces with finite automorphism group

Wednesday, October 14th (UTC+09:00)

Morning session

09:50 – 10:50	**Everett W. Howe** Constructions for supersingular and superspecial curves
11:10 – 12:10	**Momonari Kudo** Counting the isomorphism classes of superspecial curves

Afternoon session

14:00 – 15:00	**Yusuke Aikawa** Post-quantum cryptography from supersingular isogenies
15:20 – 16:20	**Hiroshi Onuki** OSIDH and SiGamal: cryptosystems from supersingular elliptic curves
16:40 – 17:40	**Jana Sotáková** Elliptic curves over finite fields and their endomorphism rings

Thursday, October 15th (UTC+09:00)

Morning session

08:30 – 09:30 **Bruce W. Jordan**
Isogeny graphs of superspecial abelian varieties

09:50 – 10:50 **Yevgeny Zaytman**
Proving connectedness of isogeny graphs with strong approximation

11:10 – 12:10 **Hyungrok Jo**
On generalized LPS Ramanujan graphs and Bruhat-Tits trees

Afternoon session

14:00 – 15:00 **Masaya Yasuda and Kazuhiro Yokoyama**
Introduction to algebraic approaches for solving isogeny path-finding problems

15:20 – 16:20 **Katsuyuki Takashima**
Counting superspecial Richelot isogenies by reduced automorphism groups

16:40 – 17:40 **Benjamin Smith**
Special structures and cryptosystems in the superspecial Richelot isogeny graph

Contents

Preface i

Program ii

Contents iv

Supersingular abelian varieties and curves, and their moduli spaces, with a remark on the dimension of the moduli of supersingular curves of genus 4
Shushi Harashita 1

Supersingular abelian varieties and quaternion hermitian lattices
Tomoyoshi Ibukiyama 17

Polarized superspecial simple abelian surfaces with real Weil numbers: a survey
Jiangwei Xue and Chia-Fu Yu 39

Vector bundles on the stack of G-zips and partial Hasse invariants
Jean-Stefan Koskivirta 59

Counting isomorphism classes of superspecial curves
Momonari Kudo 77

Post-quantum cryptography from supersingular isogenies
Yusuke Aikawa 97

OSIDH and SiGamal: cryptosystems from supersingular elliptic curves
Hiroshi Onuki 117

Isogeny graphs of superspecial abelian varieties
Bruce W. Jordan 131

Proving connectedness of isogeny graphs with strong approximation
Yevgeny Zaytman 145

Generalized LPS Ramanujan graphs
Hyungrok Jo 153

Introduction to algebraic approaches for solving isogeny path-finding problems
Ryoya Fukasaku, Yasuhiko Ikematsu, Momonari Kudo, Masaya Yasuda and Kazuhiro Yokoyama 169

Counting superspecial Richelot isogenies by reduced automorphism groups
Katsuyuki Takashima 185

An atlas of the Richelot isogeny graph
Enric Florit and Benjamin Smith 195

RIMS Kôkyûroku Bessatsu

Ｂ７５ New development of microlocal analysis and singular perturbation theory

Ｂ７６ On the examination and further development of inter-universal Teichmüller theory

Ｂ７７ Algebraic Number Theory and Related Topics 2016

Ｂ７８ Mathematical structures of integrable systems and their applications

Ｂ７９ Stochastic Analysis on Large Scale Interacting Systems

Ｂ８０ Regularity, singularity and long time behavior for partial differential equations with conservation law

Ｂ８１ Study of the History of Mathematics 2019

Ｂ８２ Regularity and Asymptotic Analysis for Critical Cases of Partial Differential Equations

Ｂ８３ Algebraic Number Theory and Related Topics 2017

Ｂ８４ Inter-universal Teichmüller Theory Summit 2016

Ｂ８５ Study of the History of Mathematics 2020

Ｂ８６ Algebraic Number Theory and Related Topics 2018

Ｂ８７ Mathematical structures of integrable systems, its deepening and expansion

Ｂ８８ Harmonic Analysis and Nonlinear Partial Differential Equations

Ｂ８９ Study of the History of Mathematics 2021

RIMS Kôkyûroku Bessatsu
Vol. B90

2022年6月発行

発行所　京都大学数理解析研究所
印刷所　明文舎印刷株式会社