参加報告

首都大学東京 田中 覚

2008年7月5日 JANT 18

ANTS VIII 基本情報

- 期日 5/17～5/22 (5/17: opening reception)
- 会場 Banff Centre, Banff, Canada
- 講演数: 32 (うち招待講演 4)
- ポスター数: 14
- 参加者数: 137
  - 国分布:USA>>CAN>FRA>GBR>NLD>DEU>JPN(6)
- Awards
  - Selfridge Prizes:
    Computing Hilbert class polynomials
    (by Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter)
  - Poster Award:
    Genus 2 Curves With Split Jacobians
    (by Kevin Doerksen)


CATERPILLAR

5/18: First Day

- Invited Talk: Andrew Granville
  Running time predictions for square products and large prime variations
- Morning(3): Point Counting
- Afternoon(4): Number Fields

5/18 Program

- 9:00 Andrew Granville(Invited),
  Running time predictions for square products and large prime variations
- 10:30 Wouter Castryck,
  Computing zeta functions in families of $C_{a,b}$ curves using deformation
- 11:00 Andrew V. Sutherland,
  Computing L-series of hyperelliptic curves
- 11:30 Remke Kloosterman,
  Point counting on singular hypersurfaces
- 14:30 John Voight,
  Enumeration of totally real number fields of bounded root discriminant
- 15:00 David P. Roberts,
  Number fields ramified at one prime
- 16:00 Brett A. Tangedal,
  Functorial properties of Stark units
- 16:30 Pieter Rozenhart,
  Tabulation of cubic function fields with imaginary and unusual Hessian

5/19: Second Day

- Invited Talk: Francois Morain,
  A survey on algorithms for computing isogenies on low genus curves
- 1st Poster Session
- Morning(3): Arithmetic of Elliptic Curves
- Afternoon(4): Number Theory, Cryptography
  - Alain Togbé,
    On the Diophantine equation $x^2 + 2^{\alpha}5^{\beta}13^{\gamma} = y^n$
- Last minute research announcements

5/19 Program

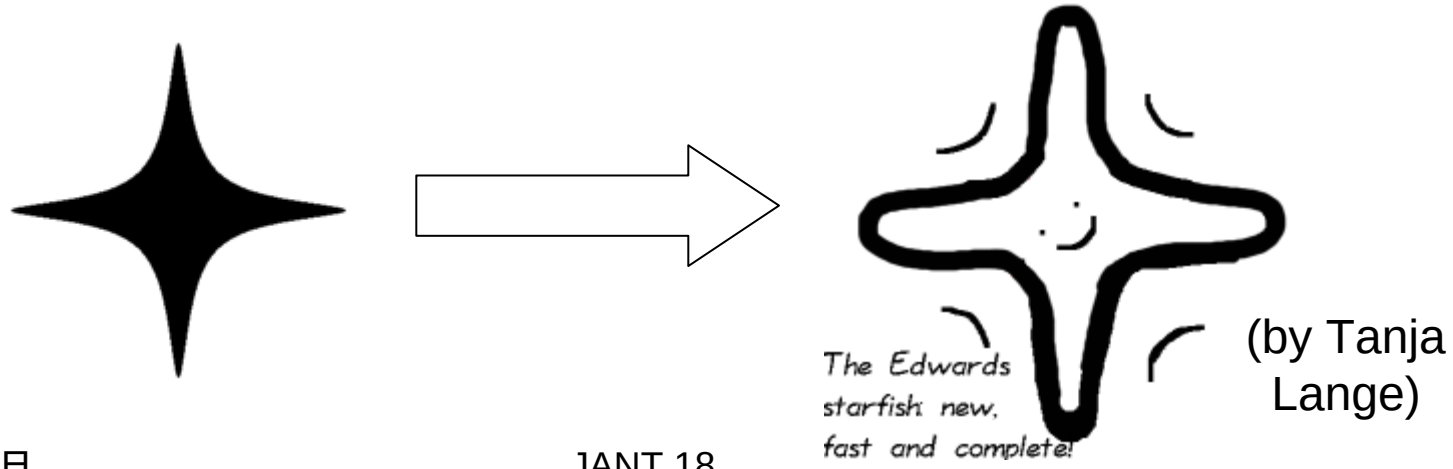
- 9:00 Francois Morain(Invited),
  A survey on algorithms for computing isogenies on low genus curves
- 10:00 1st Poster Session
- 10:30 Tom Fisher,
  Some improvements to 4-descent on an elliptic curve
- 11:00 Thotsaphon Thongjunthug,
  Computing a lower bound for the canonical height on elliptic curves over totally real number fields
- 11:30 John E Cremona,
  Computing in component groups of elliptic curves
- 14:00 Alain Togbé,
  On the Diophantine equation $x^2 + 2^{\alpha}5^{\beta}13^{\gamma} = y^n$
- 14:30 Sami Omar,
  Non-vanishing of Dirichlet L-functions at the central point
- 15:30 Andrew Shallue,
  An improved multi-set algorithm for the dense subset sum problem
- 16:00 Prasad Tetali,
  Birthday paradox for Markov chains, with an optimal bound for collision in the Pollard rho algorithm for discrete logarithm
- 16:40 Last minute research announcements

5/19 Last minute research announcements

- Steven Galbraith,
  Faster ECC using an efficient endomorphism for general curves
- Daniel J. Bernstein and Tanja Lange,
  The elliptic curve zoo: a study of curve shapes
- Igor Shparlinski,
  Fermat quotients
- Henri Cohen,
  Counting cubic extensions with given quadratic resolvent
- Noam Elkies,
  The smallest "congruent number" curves of rank 5

Elliptic zoo?

- The computational cost of elliptic-curve addition in Explicit Formulas Database (http://www.hyperelliptic.org/EFD/), nowadays the fastest form is Edwards. http://cr.yp.to/talks/2008.05.12/zoo.html



(by Tanja Lange)

5/20: The Middle Day

- Invited Talk: Johannes A. Buchmann
  Lattices in cryptography
- Morning(4): Elliptic Curve Cryptography and Generalizations
  - **Takashima,**
    Efficiently Computable Distortion Maps for Supersingular Curves

    …Coming Soon


Efficiently Computable Distortion Maps
for Supersingular Curves
ANTS 2008
2008 / 5 / 20
Katsuyuki Takashima
Mitsubishi Electric

5/20 Program

- 9:00 Johannes A. Buchmann(Invited),
  Lattices in cryptography
- 10:30 Takashima,
  Efficiently computable distortion maps for supersingular curves
- 11:00 Koray Karabina,
  On prime-order elliptic curves with embedding degrees k = 3, 4 and 6
- 11:30 Marco Streng,
  Ordinary Abelian varieties with prescribed embedding degree

5/21: The Fourth day

- Invited Talk: Hugh C. Williams,
  A new look at an old equation
- 2nd Poster Session
- Morning: Factorization, Multiplication
- Afternoon: Modular Form, CM Curves
  - Reinier Bröker
    Computing Hilbert class polynomials

5/21 Program

- 9:00 Hugh C. Williams(Invited),
  A new look at an old equation
- 10:00 2nd Poster Session
- 10:45 Alexander Kruppa,
  Improved stage 2 to P±1 factoring algorithms
- 11:15 Emmanuel Thomé,
  Faster multiplication in GF(2)[x]
- 11:45 Willemien Ekkelkamp,
  Predicting the sieving effort for the Number Field Sieve
- 14:00 Dan Yasaki,
  Hecke operators and Hilbert modular forms
- 14:30 Lassina Dembélé,
  Computing Hilbert modular forms over fields with nontrivial class group
- 15:30 Jorge Jimenez Urroz,
  Almost prime orders of CM elliptic curves modulo p
- 16:00 [Selfridge Prizes] Reinier Bröker,
  Computing Hilbert class polynomials

5/22: The final

- Morning:
  K3 surfaces, Hyperelliptic arithmetic
  - David J. Mireles Morales,
    Efficient hyperelliptic arithmetic using balanced representation for divisors

5/22 Program

- 9:00 Andreas-Stephan Elsenhans,
  K3 surfaces of Picard rank one and degree two
- 9:30 Noam D. Elkies,
  Shimura curve computations via K3 surfaces of Neron-Severi rank at least 19
- 10:00 David J. Mireles Morales,
  Efficient hyperelliptic arithmetic using balanced representation for divisors

Column

- 代数曲線関連の話題が毎日出現
  - 日本からの講演/ポスターも代数曲線絡み
    - Masaya Yasuda,
      The discrete logarithm problem on elliptic curves defined over Q
  - 両方のPrizeも非常に関連性が深い
- 次回はNancy, France
  http://www.lix.polytechnique.fr/Labo/Francois.Morain/ANTS9/