

Centre de recherches mathématiques
Université de Montréal

Atelier «Comptage de points : théorie, algorithmes et pratique»
Du 19 au 23 avril 2010

Workshop on Counting Points: Theory, Algorithms and Practice
April 19-23, 2010

HORAIRE / *PROGRAM*

Conférences : salle 6214

Pauses-café : salle 6245

Lectures: Room 6214

Coffee Breaks: Room 6245

Le lundi 19 avril 2010 / Monday, April 19, 2010

10:30 - 11:30 Inscription (salle 5345) et café-croissants (salle 6245) / *Registration (Room 5345) and Coffee & Croissants (Room 6245)*

11:30 - 12:30 **Kristin E. Lauter** (Microsoft Research)
“Constructing genus 2 curves with a given number of points”

12:30 - 14:30 Pause-déjeuner / *Lunch break*

14:30 - 15:30 **Daniel J. Bernstein** (University of Illinois at Chicago)
“Counting points as a video game”

15:30 - 16:00 Pause-café / *Coffee break*
(Salle / *Room 6245*)

16:00 - 16:45 **Christiane Peters** (Technische Universiteit Eindhoven)
“Algebraic construction of the Elkies factor”

16:45 Réception de bienvenue (6245) / *Welcoming Reception (6245)*

Le mardi 20 avril 2010 / *Tuesday, April 20, 2010*

09:00 - 10:00 Café croissants (6245) / *Coffee & Croissants (6245)*

10:00 - 11:00 **Igor Shparlinski** (Macquarie University)
“Group Structures of Elliptic Curves over Finite Fields”

11:00 - 11:30 Pause-café / *Coffee break*
(Salle / Room 6245)

11:30 - 12:30 **Christophe Ritzenthaler** (Université de la Méditerranée)
“From the curve to its Jacobian and back”

12:30 - 14:30 Pause-déjeuner / *Lunch break*

14:30 - 15:30 **Pierrick Gaudry** (LORIA - Bât. A)
“Point counting on genus 2 curves with real multiplication”

15:30 - 16:00 Pause-café / *Coffee break*
(Salle / Room 6245)

16:00 - 16:45 **David Roe** (Harvard University)
“Computing zeta functions using p -adic cohomology”

17:00 - 17:30 Session de travail / *Open Problems Session*

Le mercredi 21 avril 2010 / *Wednesday, April 21, 2010*

09:00 - 10:00 Café croissants (6245) / *Coffee & Croissants (6245)*

10:00 - 11:00 **Andrew V. Sutherland** (Massachusetts Institute of Technology)
“Genus 1 point counting in essentially quartic time and quadratic space”

11:00 - 11:30 Pause-café / *Coffee break*
(Salle / *Room* 6245)

11:30 - 12:30 **John Voight** (University of Vermont)
“Computing zeta functions for sparse hypersurfaces using Dwork cohomology”

12:30 Pause-déjeuner et après-midi libre / *Lunch Break and Free Afternoon*

Le jeudi 22 avril 2010 / *Thursday, April 22, 2010*

09:00 - 10:00 Café croissants (6245) / *Coffee & Croissants (6245)*

10:00 - 11:00 **David Harvey** (New York University)
“Computing zeta functions of projective hypersurfaces in large characteristic”

11:00 - 11:30 Pause-café / *Coffee break*
(Salle / Room 6245)

11:30 - 12:30 **Luis Finotti** (University of Tennessee)
“Lifting the j -Invariant and Computations with Witt Vectors”

12:30 - 14:30 Pause-déjeuner / *Lunch break*

14:30 - 15:30 **Reynald Lercier** (DGA & Université de Rennes 1)
“Fast p -adic arithmetic for (hyper)elliptic AGM point counting algorithms”

15:30 - 16:00 Pause-café / *Coffee break*
(Salle / Room 6245)

16:00 - 16:30 **Benjamin Smith** (INRIA Saclay - Île-de-France)
“Families of curves amenable to RM-accelerated point counting”

16:30 - 17:15 **Nick Alexander** (University of California, Irvine)
“Point counting on reductions of CM abelian surfaces”

Le vendredi 23 avril 2010 / *Friday, April 23, 2010*

09:00 - 10:00 Café croissants (6245) / *Coffee & Croissants (6245)*

10:00 - 11:00 **Daqing Wan** (University of California, Irvine)
“Improving the Weil bound for Artin-Schreier curves”

11:00 - 11:30 Pause-café / *Coffee break*
(Salle / Room 6245)

11:30 - 12:00 **Adriana Salerno** (Bates College)
“Rational Points and Hypergeometric Functions”

12:30 Fin de l’atelier / *Closure of the workshop*