Submittee: Michael Jacobson, Jr.
Date Submitted: 2014-01-20 11:50
Title: Workshop on Curves and Applications
Event Type: Conference-Workshop

Location:
University of Calgary, Calgary, Alberta

Dates:
August 19-21, 2013

Topic:
This project-driven workshop on algebraic curves will bring together experts to further current research in the following areas: Mathematical aspects of algebraic curves, with emphasis on constructing curves with special properties, such as prescribed covering groups, torsion or with many rational points; /// Arithmetic infrastructure, with the additional goal of implementation in the computer algebra system SAGE; /// Applications, including cryptography.

Methodology:
Lectures in the morning (2 each), mentor-led problem/project sessions in the afternoons.

Organizers:
Bauer, Mark, Mathematics and Statistics, University of Calgary // Jacobson, Michael, Computer Science, University of Calgary // Scheidler, Renate, Mathematics and Statistics, University of Calgary

---

Speakers:
1. Jeff Acter (Colorado State University), Counting Abelian Surfaces. Abstract: Abelian varieties are smooth, projective group varieties; they are the higher-dimensional analogues of elliptic curves. In addition to their interest they provide, by the theory of the Jacobian, an essential tool for probing the arithmetic and geometry of algebraic curves. In the fi rst part of the talk, I review some of the fundamental structures used in studying abelian varieties. In the second part, I discuss a collection of questions concerning the distribution of abelian varieties over fi nite elds, with special emphasis on recent result for abelian surfaces. /// 2. Nils Bruin (Simon Fraser University), Computing with divisor classes on curves using global sections. Abstract: One can represent divisors on curves in many essentially equivalent ways. The one most explored from an explicit computational point of view is by representing them by ideals in fi nite extensions of univariate polynomial rings. This fixes a representation of the function fi eld of the curve as a fi nite extension of a rational function field. In this instructional exposition we will explore a di fferent way: Associated to a divisor is its Riemann-Roch space: the space of global sections of the line bundle associated to the divisor. For divisors of su fficiently high degree, this space determines the divisor uniquely. For such divisors, their arithmetic can be expressed in terms of straightforward linear algebra operations, which one

can use to compute with divisor classes. We will largely follow Kamal Khuri-Makdisi's approach. Our objective is to investigate the possible practical bene fits of using this approach to compute in the Picard groups of, say, smooth plane curves. /// 3. Craig Costello (Microsoft Research), The State-of-the-art in Hyperelliptic Curve Cryptography. Abstract: I will give a ground up talk on the use of algebraic curves in cryptography. I will focus mostly on genus 2 curves, because they are much more fun than elliptic curves. This talk contains joint work with Joppe Bos, Huseyin Hisil and Kristin Lauter. /// 4. David Jao (University of Waterloo), Isogeny-Based Cryptography on Mobile Platforms. Abstract: To protect against the possible development of large-scale quantum computers, the deployment of effi cient quantum-resistant cryptosystems designed for use on mobile devices is of the utmost importance. In 2011, De Feo, Jao and Plt proposed a candidate quantum-resistant public key cryptosystem based on isogenies between supersingular elliptic curves. We present C and assembly implementations of this cryptosystem suitable for use on mobile devices. Our implementation uses pre-computed parameters, with all time consuming computations offl oaded from the device. We demonstrate the performance of our library on iOS and An- droid devices, describe ongoing e fforts at optimization, and provide comparisons to other quantum-resistant public key cryptosystem candidates in the context of mobile applications. Our results indicate that isogeny-based cryptosystems are viable for post-quantum applications, with manageable running times and best-in-class key sizes. /// 5. Kumar Murty (University of Toronto), Splitting of Abelian Varieties. Abstract: It is possible for an irreducible polynomial with integer coefficients to become reducible modulo p for every prime p. We will consider a geometric variant of this phenomenon, where polynomials are replaced with Abelian varieties. The Galois theory that is used to understand the situation with polynomials is now largely replaced (or rather, supplemented) with Tate's theorem. /// 6. Ben Smith (INRIA), Explicit isogenies and endomorphisms of low-genus Jacobians: Theory and applications. Abstract: The last few decades have seen the development of many computational tools for algebraic curves and their Jacobians: algorithms for divisor class arithmetic, point counting and zeta functions, explicit Riemann{Roch spaces... On the other hand, algorithms for the mappings between these objects remain relatively underdeveloped. From a category-theoretic point of view: we've got a reasonably good handle on (most of) the objects in our diagrams, but we have a chronic shortage of e ffective arrows! In this talk, we consider some of the problems involved in computing with isogenies and endomorphisms of low-genus Jacobians, with a special focus on their applications in cryptography. For example: isogenies can be used to accelerate point counting, to relate ostensibly di fferent discrete logarithm problems, and to improve the e fficiency of cryptographic operations on elliptic and genus 2 curves. We will survey these constructions, consider their limitations, and give an idea of some open problems.

Links:
http://www.pims.math.ca/scientific-event/130819-wca
