Explicit Methods in Number Theory
November 13 – 18, 2004

MEALS

Breakfast (Continental): 7:00 – 9:00 am, 2nd floor lounge, Corbett Hall, Sunday – Thursday
***Lunch** (Buffet): 11:30 am – 1:30 pm, Donald Cameron Hall, Sunday – Thursday
***Dinner** (Buffet): 5:30 – 7:30 pm, Donald Cameron Hall, Saturday – Wednesday
Coffee Breaks: As per daily schedule, 2nd floor lounge, Corbett Hall
***Please remember to scan your meal card at the host/hostess station in the dining room for each lunch and dinner.**

MEETING ROOMS

All lectures will be held in Max Bell 159 (Max Bell Building accessible by bridge on 2nd floor of Corbett Hall). LCD projector, overhead projectors and blackboards are available for presentations. Hours: 6 am – 12 midnight. *Please note that the meeting space designated for BIRS is the lower level of Max Bell, Rooms 155-159. Please respect that all other space has been contracted to other Banff Centre guests, including any Food and Beverage in those areas.*

SCHEDULE

Saturday, November 13

16:00 Check-in begins (Front Desk – Professional Development Centre - open 24 hours)
17:30-19:30 Buffet Dinner, Donald Cameron Hall
20:00 Informal gathering in 2nd floor lounge, Corbett Hall
Beverages and small assortment of snacks available on a cash honour-system basis.

Sunday, November 14

7:00-9:00 Breakfast, 2nd floor lounge, Corbett Hall
9:15-9:30 Introduction and Welcome to BIRS by BIRS Station Manager, Max Bell 159
9:30 Ed Schaefer, Computing the Selmer group for an isogeny between abelian vars

Abstract: Selmer groups are of interest for bounding Mordell-Weil ranks and studying Shafarevich-Tate groups. The Selmer group for an isogeny from an abelian variety to a Jacobian can often be computed in a straightforward manner using functions on the curve. The Selmer group for an isogeny between two arbitrary abelian varieties can sometimes be computed by exploiting the idea above. In this talk, we will describe both methods and use them to find all of the rational points on the genus 3 curve $x^4+(y^2+1)(x+y)=0$.

10:20-10:40 Coffee, 2nd floor lounge, Corbett Hall
10:40-11:10 David Boyd, Computing A-polynomials using Puiseux expansions

Abstract: The A-polynomial of a hyperbolic manifold is computed by elimination of variables from a large system. Standard methods fail to work on many interesting examples. We discuss a method that depends on computing one or more Puiseux expansions and then using linear algebra. This can handle many examples that are otherwise inaccessible.

11:10-11:30 Coffee
11:30 Nils Bruin, Explicit visualisation for Abelian Surfaces

Abstract: We consider the problem of bounding the Mordell-Weil rank of Jacobians of hyperelliptic curves. A first step is to compute the 2-Selmer group of the Jacobian. We concentrate on the situation where this does not provide a sharp bound. We use a construction first proposed by Cremona and Mazur, which is referred to as "visualisation" and involves considering the Abelian surface as a subvariety of an Abelian variety of higher dimension.

Contrary to the case of elliptic curves, the corresponding principal homogeneous spaces have quotients that still have interesting geometry. We show that in the case of genus 2 curves with a rational Weierstrass point, the homogeneous spaces cover a Del-Pezzo surface, for which it may be possible to show it violates the Hasse-principle. This provides another way of exhibiting non-trivial elements in the Shafarevich-Tate group.

As an example, we derive an explicit parametrised infinite family of genus 2 curve whose Jacobians have nontrivial members of the Shafarevich-Tate

12-1:30 Lunch

1:00-2:00 Guided Tour of The Banff Centre; meet in the 2nd floor lounge, Corbett Hall

2:00 William Stein, Some New Data About Ranks of Elliptic Curves

Abstract: In this talk I will show many graphs of average ranks (and other information) as a function of the conductor. The data is surprising! For example, the average rank of these curves appears to be about 1, rather than 1/2, which the folklore conjectures suggest.

2:40-3:00 Coffee
3:00 Catherine O'Neil, Arithmetic Dimension

Abstract: The arithmetic dimension is a measurement of the complexity of a functor with respect to a base field. For example, if the functor is representable, then the arithmetic dimension is just the dimension of the representing scheme. In general the arithmetic dimension gives us some idea of the number of parameters necessary for, say, a computer search for certain types of objects such as genus one curves with additional structure. I will also compare this definition with other related ones.

3:40 -- 4:00 Coffee
4:00 -- 4:30 Renate Scheidler Approximation in Cubic Function Fields

A common way of computing the order h of the Jacobian Jac(F_q) of an algebraic function field K over a finite field F_q is to determine an interval]E-L,E+L[that is known to contain h and then search this interval using a baby step giant step technique or Pollard's kangaroo method. In the case where K/F_q(x) is a cubic extension, we use approximations via truncated Euler products to explicitly compute suitable values of E and L, thereby giving an algorithm for finding h that has complexity O (q^{(2g-1)/5}) where g is the genus of K/F_q. This is joint work with A. Stein of the University of Wyoming.

Monday, November 15

9:30 Ronald van Luijk, K3 surfaces with Picard number one and infinitely many rational points.

Abstract: Not much is known about the arithmetic of K3 surfaces in general. Once the Picard number, which is the rank of the Neron-Severi group, is high enough, more structure is known and more can be said. But still we don't know of a single K3 surface whose set of rational points has been proved to be neither empty, nor Zariski dense.

Also, until recently, not even a single K3 surface was known with Neron-Severi rank 1 and infinitely many rational points. We will give an explicit example of such a surface over $\mathbb{Q}$, where the Neron-Severi group in question is taken to be the one over $\mathbb{Q}$

10:15 Coffee

10:30 David Kohel, Igusa class invariants and the AGM

Abstract: The AGM algorithm, for elliptic curves or for higher genus, is a recursive algorithm for construction of p-adic canonical lifts of an abelian varieties over a finite field. This lifting algorithm been exploited for the explicit determination of zeta functions. In recent work with Christophe Ritzenthaler, we exploit the same algorithm for the construction of the Igusa invariants of genus 2 curves with complex multiplication. This provides a p-adic alternative to the complex analytic approach.

11:15 Kristin Lauter, Class invariants of quartic CM fields

Abstract: Motivated by Gross and Zagier's factorization formulae for differences of CM values of the modular j function, we obtain a bound on (and a characterization of) the primes appearing in the denominators of CM values of certain Siegel modular functions. Our bound is explicit and is related to the discriminant of the CM field. In particular our result gives a bound on the primes appearing in the denominators of the Igusa class polynomials arising in the construction of genus 2 curves with CM. Furthermore, in the context of Stark's conjectures, a generalization of elliptic units to the case of quartic CM fields is desired. We provide a proof that the construction of DeShalit-Goren yields S-units in abelian extensions of quartic CM fields, where S is the explicit set of primes described above. This is joint work with Eyal Goren, McGill University.

12-1:30 Lunch
12:00 Group photo; meet on the front steps of Corbett Hall
2:00 Dan Bernstein, Three algorithms related to the number-field sieve

Abstract: 1. The number-field sieve tries to factor an integer n by inspecting values of the homogeneous form of a polynomial related to n. What is the size distribution of those values? I'll explain a fast algorithm to evaluate the relevant superelliptic integral. 2. How long does it take to find a polynomial of, say, degree 6, whose values are B times smaller than typical? The best method in the literature is conjectured to search about B^3.6 polynomials. I'll explain an algorithm, using four-dimensional lattice reduction, that is conjectured to search only about B^2.4 polynomials. 3. The bottleneck in the fastest known method to inspect values is computing a large integer modulo many small integers. How long does this take? I'll explain an algorithm that's 2.6+o(1) times faster than the previous record.

3:00 Coffee
3:15 Siguna Mueller, Pseudo-Prime-Powers and Primality Testing

Abstract: It has been known since the 1930s that so-called pseudosquares yield a very powerful machinery for the primality testing of large integers $N$. In fact, assuming reasonable heuristics (which have been confirmed for numbers to $2^{80}$) this gives a deterministic primality test in time $O((\lg N)^{3+o(1)})$, which many believe to be best possible.

In the 1980s D.H. Lehmer posed a question tantamount to whether this could be extended to pseudo $r$th powers. Very recently, this was accomplished for $r=3$ by Berrizbeitia et.al. In fact, the results obtained indicate that $r=3$ might lead to an even more powerful algorithm than $r=2$. This naturally leads to the challenge if and how anything can be achieved for $r>3$.

The extension from $r = 2$ to $r = 3$ relied on properties of the arithmetic of the Eisenstein ring of integers $Z[\zeta_3]$, including the Law of Cubic Reciprocity. In this paper we present a generalization of our result for any odd prime $r$. The generalization is obtained by studying the properties of Gaussian and Jacobi sums in cyclotomic ring of integers, which are tools from which the $r$-th power Einsenstein Reciprocity Law is derived, rather than from the Law itself. Our theory includes a remark which allows some minor practical enhancement to any APRCL routine. While $r=3$ seems to lead to a more efficient algorithm than $r=2$, we show that extending to any $r>3$ does not appear to lead to any further improvements.

3:45 Coffee
4:00 Juergen Klueners, Factoring Polynomials

Abstract: It is well known that factorization of polynomials over the integers is in polynomial time. Unfortunately this algorithm was not useful in practice. Recently Mark van Hoeij found a new factorization algorithm which works very well in practice. We present the ideas of his algorithm and extend this algorithm to an algorithm for factoring polynomials in F[t][x], where F is a finite field. Using a new approach the presentation is much easier. Furthermore it is possible to prove that the new algorithm runs in polynomial time.

Remainder of Schedule for Explicit Methods in Number Theory

Tuesday, November 16

9:30-10:20 Manjul Bhargava, Gauss composition and exceptional groups

10:30-11:10 Sergei Krutelevich, Higher composition laws, Jordan algebras, and exceptional groups

Abstract: Higher composition laws were discovered by M. Bhargava several years ago as a way of generalizing Gauss's law of composition of binary quadratic forms. M. Bhargava also discovered a mysterious connection between higher composition laws and exceptional Lie groups.

In our talk we will describe an unexpected relation between higher composition laws and cubic Jordan algebras. We will show how this relation can be used to shed additional light on existing composition laws, as well as provide new examples of spaces with similar properties.

11:10-11:30 Coffee

11:30-12:00 Gabor Wiese, Mod p modular symbols

Abstract: In the talk I will discuss conditions under which parabolic cohomology resp. modular symbols over F_p provide faithful modules for the Hecke algebra of (Katz) cusp forms over F_p for Gamma_1(N) with and without character.

12-12:30 John Cremona, Solving conics over function fields

Abstract: I will report on recent joint work with Mark van Hoeij and David Roberts concerning algorithms for solving conics over F(T) where F is an arbitrary field of characteristic not two. The algorithm is an adaptation of similar algorithms for solving conics over Q, using a combination of classical algorithms of Legendre and Gauss combined with more recent methods of Denis Simon.

Free Afternoon

Wednesday, November 17

9:30-10:00 Michael Stoll - Covers and rational points

Abstract: We consider restrictions on the set of rational points on a curve that come from etale covers. For example, the Brauer-Manin obstruction for a curve is related to abelian etale covers. We look at more general covers and discuss the `functoriality' of the property that the set of rational points is exactly given by the adelic points that lift to to some twist of every etale cover.

10:05-10:35 Martine Girard, Maximality of the Weierstrass subgroup.

Abstract: The group generated by the Weierstrass points of a curve in its Jacobian, the Weierstrass subgroup, is a geometric invariant of the curve. We show that the Weierstrass subgroup of the generic curve of genus $g \geq 3$ is a free abelian group of rank $g(g^2-1)-1$.

This is joint work with David Kohel (Sydney) and Christophe Ritzenthaler
(Barcelona).

10:35-11:00 Coffee

11:00-11:30 Idris Mercer, Norms of Zero-One Polynomials and Ubiquity of Sidon Sets

Abstract: There is a rich literature on the theme of finding a polynomial with integer coefficients and

small norm. One natural restriction on the coefficients of our polynomial is to require them to be zero or one. Given this restriction, we can ask: What is the expected norm of such a polynomial? In this talk, we show that for some natural ways to interpret this question, the answer can be calculated explicitly. As a surprising corollary, we get a new proof of the following known result:
If m = o(n^{1/4}), then `most' m-subsets of {1,2,...,n} are Sidon, in a certain well-defined sense. (A Sidon set is one where all differences of pairs of elements are distinct.)

11:30-12:00 Richard Pinch, Carmichael numbers: theory and practice

Abstract: We discuss the recent result of Harman that the number of Carmichael numbers up to x, C(x) >> x^{0.332}, and report on some computations, especially of Carmichael numbers of small index (the ratio of n-1 to lambda(n)) and applications to Lehmer's problem of finding numbers with phi(n) dividing n-1.

12:30-2:00 Lunch

2:00-2:45 Frank Calegari, Irrationality of some p-adic periods for small p

Abstract: We prove that zeta_p(3) is irrational for p=2,3, where zeta_p is the Kubota-Leopoldt p-adic zeta function.

2:50-3:35 Lassina Dembele - Computing Hilbert modular forms

Abstract: I will present a new algorithm that can be used to compute Hilbert modular forms in a very efficient. This is an important step as it allows numerical experimentation on such forms as was never done before. I will illustrate the presentation with some numerical examples. I will also explain how one can determine some of the geometric objects corresponding to some of the forms.

3:35-4:00 Coffee

4:00-4:30 Mike Mossinghoff, Mahler's measure of Littlewood polynomials

Abstract: We discuss Lehmer's question on the existence of integer polynomials with small Mahler's measure for some special classes of polynomials, including the Littlewood polynomials, which have all ±1 coefficients. We also consider some related problems, like the conjecture of Schinzel and Zassenhaus, for these polynomials. This is joint work with P.Borwein, E.Dobrowolski, and A.Dubickas.

4:30-5:00 Edlyn Teske, Cryptographic implications of Hess' generalized GHS Weil descent attack on the elliptic curve discrete logarithm problem

Abstract: A finite field K is said to be weak for elliptic curve cryptography if all instances of the discrete logarithm problem for all elliptic curves over K can be solved in significantly less time than it takes Pollard's rho method to solve the hardest instances. We have examined characteristic two finite fields for weakness under the Gaudry-Hess-Smart (GHS) Weil descent attack and Hess' generalization of it. This talk summarizes our results with the example GF(2^{210}).

Joint work with Alfred Menezes

Thursday, November 18

9:30-10:20 Rene Schoof, Infrastructure

Abstract: In 1972 Daniel Shanks observed that the quadratic forms in the principal cycle of reduced binary quadratic forms of positive discriminant exhibit a group-like behavior. This was a surprising phenomenon, because the principal cycle itself constitutes the trivial class of the class group. Shanks called this group-like structure `inside' the neutral element of the class group the "infrastructure". He exploited it by designing an efficient algorithm to compute regulators of real quadratic number fields. In this talk we present a natural setting for the infrastructure phenomenon. It is provided by Arakelov theory and applies to arbitrary number fields.

10:20-10:40 Coffee

10:40-11:25 Henri Cohen, Experimentation with the Doubly-Exponential Integration Method

Abstract: In 1974, Takashi and Mori introduced a revolutionary new integration method enabling the computation of definite integrals in a few seconds. Very few papers have appeared since. The goal of this talk is to present a Pari/GP implementation, many examples, and experiments showing that the known heuristic explanations are completely unsatisfactory.

11:30-12:00 Bart de Smit, Computing Artin constants

For any number field K, and x in K, I will show how to find the density of the set of primes p of K for which x mod p is a primitive element of the residue field of p.

12:00-1:30 Lunch

Checkout by 12 noon.