Abstracts for the Computational Number Theory Workshop @ FOCM 2011

Jennifer Balakrishnan: ***Computations with Coleman integrals***

The Coleman integral is a p-adic line integral that can encapsulate valuable information about the arithmetic and geometry of curves and abelian varieties. For example, certain integrals allow us to find rational points or torsion points; certain others give us p-adic height pairings. I'll present a brief overview of the theory, describe algorithms to calculate some of these integrals, and illustrate these techniques with numerical examples computed using Sage.

Martin Bright: ***Rational points on surfaces***

Much effort has been spent over the last century understanding the arithmetic of curves; attention has turned more recently to surfaces. Although we are far from being able to algorithmically find rational points on anything but the simplest of surfaces, computational techniques have been very useful in investigating the existence and distribution of rational points. I will briefly describe some approaches.

Claus Diem: ***The discrete logarithm problem in elliptic curves***

It is well known that the classical discrete logarithm problem (the problem to compute indices modulo prime numbers) can be solved in subexponential expected time.

In contrast, it is not known whether the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields (the elliptic curve discrete logarithm problem) can be solved in subexponential expected time. Indeed, it was the lack of an obvious algorithm for this computational

problem which was faster than "generic" algorithms which lead Miller and Koblitz to suggest the use of the problem for cryptographic applications.

In 2004 Gaudry gave a randomized algorithm with which one can - under some heuristic assumptions - solve the elliptic curve discrete logarithm problem over all finite fields with a fixed extension degree at least 3 faster than with generic algorithms. By using a similar algorithm, I have shown that there exists a sequence of finite fields (of strictly increasing cardinality) over which the elliptic curve discrete logarithm problem can be solved in subexponential time.

Recently, I have been able to extend the result in such a way that now for more families of finite fields the elliptic curve disctrete logarithm problem can be solved in subexponential expented time. A corresponding algorithm and its analysis will be outlined in the talk.

Tim Dokchitser: ***Frobenius elements in Galois groups***

I will discuss a method of computing Frobenius elements in arbitrary Galois extensions of global fields, which may be seen as a generalisation of Euler's criterion. It is a part of the general question how to compare splitting fields and identify conjugacy classes in Galois groups.

This is joint work with Vladimir Dokchitser.

David Mandell Freeman: ***Cryptography from Hard Problems in Number Fields***

Most public key cryptographic protocols in use today base their security on the difficulty of one of two computational problems: factoring large composite integers or computing discrete logarithms in certain alegbraic groups (such as F_q^* or the group of points on an elliptic curve over a finite field). Recently, some systems have been proposed whose security is based on hard problems on integer lattices (e.g., closest vector and shortest vector problems). When the lattices in question are embeddings of ideals in number fields, we can create cryptosystems with functionalities that cannot currently be produced using factoring or discrete-log techniques. In particular, Gentry (2009) used "ideal lattices" to create a *fully homomorphic encryption scheme*, which allows users to perform computations on encrypted data.

We will describe another new application of "ideal lattices," a *homomorphic signature scheme*. This scheme allows users to perform computations

on authenticated data so that the output of the computation can be verified even without knowing the inputs. The security of our scheme is based on the difficulty of finding a small element in an ideal, where "small" refers to the length of the corresponding vector in the canonical embedding.

This is joint work with Dan Boneh.

David Holmes: ***Computations on the Jacobians of high-genus curves***

Let J be the Jacobian of a curve of genus $g > 1$ over a number field. If $g = 2$ then we have explicit projective models for J which are very useful for effective computation; for example we can determine the Mordell-Weil group of J by descent followed by a saturation process using the Neron-Tate height. However, g is greater than 2 it is no longer practical to write down a projective model of J. A lot of effective computation is still possible, for example descent has been applied to determining finite index subgroups of the Mordell-Weil group. As yet it has not been possible to perform saturation to find the whole Mordell-Weil group; I will describe recent work towards a resolution of this problem building on work of Neron, Arakelov, Faltings and Hriljac, including the effective computation of Neron-Tate heights on Jacobians of curves of genus up to 9.

Filip Najman: ***Mordell-Weil groups of elliptic curves over number fields of small degree***

I will talk about various recent results about elliptic curves over number fields of degree 2, 3 and 4, focusing on the interplay of the torsion group and the rank over a fixed number field. It will be shown that what happens is quite different than over the rationals. I will also discuss how these results can be applied to choosing good elliptic curves for factoring.

Sebastian Pancratz: ***Point counting on hypersurfaces over finite fields***

Bjorn Poonen: ***Descent for Jacobians of genus 3 curves***

I will present an update on ongoing work with Nils Bruin and Michael

Stoll on explicit descent on Jacobians of genus 3 curves.

Soma Purkait: ***Eigenforms of half-integral weight and some applications***

Let f be a modular form of half-integral weight $k/2$, k odd and level N. The fundamental theorem of Shimura associates to f a modular form $Sh_t(f)$ of integer weight $k-1$; the modular form $Sh_t(f)$ is called the Shimura lift of f. This Shimura correspondence commutes with the action of the Hecke operators of integral and half-integral weight. We will discuss our algorithm for computing eigenforms of half-integral weight and hence inverse Shimura lifts of newforms of integral weight, if these exist. Once we have inverse Shimura lifts, we will explore Waldspurger's theorem by looking at some examples and will obtain explicit formulae for the critical values of the L-functions of twists of elliptic curves in those cases in terms of the coeficients of corresponding modular forms of half integral weight.

Lanos Rónyai: ***Splitting full matrix algebras over number fields***

Samir Siksek: ***The generalized Fermat equation*** $x^3 + y^4 + z^5 = 0$

This talk is based on joint work with Michael Stoll (Bayreuth). The equation of the title was suggested by Zagier as the next case of the Generalized Fermat Conjecture. Work of Edwards reduces this equation to the determination of rational points on 49 hyperelliptic curves of genus 14. Standard methods for determining the rational points fail on many of these curves. We describe a new technique which we call 'partial descent' that succeeds in completing the determination of rational points on these curves. We deduce that the only solutions in coprime integers x, y, z satisfy $xyz = 0$.

Andrew Sutherland: ***Genus 1 point counting in quadratic space and essentially quartic time***

The Schoof-Elkies-Atkin (SEA) algorithm is the method of choice for counting points on an elliptic curve modulo a prime p. Its main limitation is the size of the modular polynomials it requires. The largest of these uses on the order of $n^3 \log n$ bits of storage, where $n = \log p$, and their aggregate

size is quartic in n.

I will describe a modified version of the SEA algorithm that requires only quadratic space, based on a method for directly computing instantiated modular polynomials via an explicit form of the Chinese remainder theorem. This algorithm is not only able to handle much larger problem sizes, its reduced space complexity also yields a better running time. These results have led to a new point counting record, modulo a prime p with more than 5000 decimal digits. Time permitting, I will discuss how the same techniques may be applied to some other problems in computational number theory.
