Banff International Research Station
for Mathematical Innovation and Discovery

Polynomials over Finite Fields and Applications
November 18-23, 2006

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). Hours: 6 am–12 midnight. LCD projector, overhead projectors and blackboards are available for presentations. *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

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

Sunday

7:00–8:45	Breakfast
8:45–9:00	Introduction and Welcome to BIRS by BIRS Station Manager, Max Bell 159
9:00	M. Car: "Ternary quadratic forms that represent 0, the function field case"
10:00	S. Huczynska: "The strong primitive normal basis theorem"
10:30	Coffee Break, 2nd floor lounge, Corbett Hall
11:00	I. Shparlinski: "On the Sato-Tate conjecture on average"
12:00–13:30	Lunch
13:30	J. von zur Gathen: "Counting bivariate polynomials: reducible, exceptional, and singular ones"
14:30	M. Moisio: "Kloosterman curves, their fibre products, and explicit enumeration of irreducible polynomials with two coefficients prescribed, I"
15:00	H. Ranto: "Kloosterman curves, their fibre products, and explicit enumeration of irreducible polynomials with two coefficients prescribed, II"
15:30–16:00	Coffee Break, 2nd floor lounge, Corbett Hall
16:00	F. Ruskey: "Exhaustive generation of irreducible polynomials over small finite fields"
17:00	D. Bernstein: "Faster factorization into coprimes"
17:30	J. Dillon: "APN polynomials and related codes"
18:00–19:30	Dinner

Monday

7:00–9:00	Breakfast
9:00	A. Enge: "Asymptotically optimal computation of modular polynomials"
10:00	F. Voloch: "Symmetric cryptography and algebraic curves"
10:30	Coffee Break, 2nd floor lounge, Corbett Hall
11:00	S. Gao: "Primary decomposition of zero-dimensional ideals over finite fields"
12:00–13:30	Lunch
13:00–13:55	Guided Tour of The Banff Centre; meet in the 2nd floor lounge, Corbett Hall
13:55	Group Photo; meet on the front steps of Corbett Hall
14:00	W. Li: "Characterizations of pseudo-codewords of a parity-check code"
15:00	H. Tapia Recillas: "The simplex code over finite chain rings"
15:30	Coffee Break, 2nd floor lounge, Corbett Hall
16:00	H. Lenstra: "Constructing finite fields"
16:30	I. Semaev: "On solving sparse algebraic equations over finite fields"
17:00	M. Zieve: "Polynomial decomposition"
18:00–19:30	Dinner
19:30–20:30	Open Problem Session

Tuesday

7:00–9:00	Breakfast
9:00	G. Gong: "Two-level autocorrelation sequences, polynomials, and exponential sum equalities"
10:00	Q. Wang: "Permutation polynomials and sequences over finite fields"
10:30	Coffee Break, 2nd floor lounge, Corbett Hall
11:00	P. Lisonek: "Caps and highly nonlinear functions on finite fields"
11:30	A. Bluher: "Hyperquadratic elements of degree 4"
12:00–13:30	Lunch
	Free Afternoon
18:00–19:30	Dinner

Wednesday

7:00–9:00	Breakfast
9:00	D. Wan: "Counting rational points on varieties over finite fields"
10:00	M. Presern: "Completing the Hansen-Mullen primitivity conjecture"
10:30	Coffee Break, 2nd floor lounge, Corbett Hall
11:00	J. Park: "Monomial dynamics over finite fields"
11:30	G. Mullen: "A polynomial analogue of the $3n + 1$ problem"
12:00–13:30	Lunch
13:30	J. Yucas: "Generalized reciprocals and factors of Dickson polynomials"
14:30	O. Ahmadi: "Quadratic transformation of irreducible polynomials over finite fields"
15:15	A. Masuda: "Permutation binomials over $\mathbb{F}_{2^k p+1}$ where p and $2^k p + 1$ are primes"
15:30	Coffee Break, 2nd floor lounge, Corbett Hall
16:00	A. Garcia: "Some Artin-Schreier towers are easy"
17:00	J. Hirschfeld: "Non-isomorphic maximal curves over a finite field"
17:30	M. Dewar: "When do pentanomials divide trinomials over $\mathbb{F}_2$?"
17:45	L. Gallardo: "Sums of biquadrates in $\mathbb{F}_q[t]$"
18:00–19:30	Dinner

Thursday

7:00–9:00	Breakfast
9:00	Lectures (if desired)
	Informal discussions, as many participants must catch early flights
10:30	Coffee Break, 2nd floor lounge, Corbett Hall
11:30–13:30	Lunch

Checkout by 12 noon.

** 5-day workshops are welcome to use the BIRS facilities (2nd Floor Lounge, Max Bell Meeting Rooms, Reading Room) until 3 pm on Thursday, although participants are still required to checkout of the guest rooms by 12 noon. **

Polynomials over Finite Fields and Applications
November 18-23, 2006

ABSTRACTS
(in alphabetic order by speaker surname)

Speaker: **Omran Ahmadi** (University of Toronto)
Title: *Quadratic transformation of irreducible polynomials over finite fields*
Abstract: Self-reciprocal irreducible monic (srim) polynomials over finite fields have been studied in the past. These polynomials can be studied in the context of quadratic transformation of irreducible polynomials over finite fields. In this talk we present the generalization of some of the results known about srim polynomials to polynomials obtained by quadratic transformation of irreducible polynomials over finite fields.

Speaker: **Dan Bernstein** (University of Illinois at Chicago)
Title: *Faster factorization into coprimes*
Abstract: How quickly can we factor a set of univariate polynomials into coprimes? See `http://cr.yp.to/coprimes.html` for examples and applications. Bach, Driscoll, and Shallit achieved time $n^{(2+o(1))}$ in 1990, where n is the number of input coefficients; I achieved time $n(\lg n)^{(O(1))}$ in 1995; much more recently I achieved time $n(\lg n)^{(4+o(1))}$.

Speaker: **Antonia Bluher** (National Security Agency)
Title: *Hyperquadratic elements of degree 4*
Abstract:

I will describe joint work with Alain Lasjaunias about the construction of degree-4 polynomials over fields K of char. p whose roots α have a Frobenius property:

$$\alpha^q = \frac{A\alpha + B}{C\alpha + D},$$

where $A, B, C, D \in K$, $AD - BC$ is nonzero, and q is a power of p.

The case of interest is when K is a function field and α has a Laurent series expansion. It is conjectured that in such a case, α might have interesting patterns in its continued fraction expansion, such as those found by Buck and Robbins for a root of the polynomial $X^4 + X^2 - TX + 1 \in \mathbb{F}_13(T)[X]$.

Speaker: **Mireille Car** (Universite Paul Cezanne (Aix-Marseille III))
Title: *Ternary Quadratic forms that represent 0, the function field case*
Abstract: Let K be a global function field with field of constants a finite field k with q elements and odd characteristic. Let S be a finite set of $s > 0$ places of K and let R_S denote the set of S-integers of K. For s-tuples of rational integers $\mathbf{m} = (m_v)_{v\in S}$ and $\mathbf{n} = (n_v)_{v\in S}$, let $Q_S(\mathbf{m}, \mathbf{n})$ denote the number of pairs (a, b) of integers of R_S such that $v(a) = m_v, v(b) = n_v$ for all $v \in S$, and such that the quadratic form

$(f_{a,b})$ $$X^2 - aY^2 - bZ^2$$

represents 0 over the field K. We give an asymptotic estimate for the number $Q_S(\mathbf{m},\mathbf{n})$ for s-tuples $\mathbf{m}$ and $\mathbf{n}$ such that the numbers

$$\|\mathbf{m}\| = -\sum_{v\in S} f_v m_v, \qquad \|\mathbf{n}\| = -\sum_{v\in S} f_v n_v$$

tend to $+\infty$, f_v denoting the degree of the place v.

In a previous work, we dealt with these questions in the case of a rational function-field. (Indeed, if $K = k(T)$, the rational function field, the polynomial ring $k[T]$ is the ring $R_{\{\infty\}}$ with ∞ the $\frac{1}{T}$-place, and if m and n are positive integers, if $(\mathbf{m},\mathbf{n}) = ((-m),(-n))$, the number $Q_{\{\infty\}}(\mathbf{m},\mathbf{n})$ is equal to the number $H(m,n)$ of polynomials a and b in $k[T]$ of degree m and n respectively, such that the quadratic form $(f_{a,b})$ represents 0 over the field $k(T)$.) The case of the rational function-field was a polynomial analogue of questions asked by Serre and solved by Hooley and Guo about the size of the number $H(x)$ of pairs $(a,b) \in \mathbb{Z}^2$, such that $|a| \le x$, $|b| \le x$ and such that the ternary quadratic form

$$X^2 + aY^2 + bZ^2$$

represents 0 over the field $\mathbb{Q}$. Presently now, no number field analogue of the theorems proved in what follows is known.

Speaker: **Michael Dewar** (University of Illinois, Urbana-Champaign)
Title: *When do pentanomials divide trinomials over $\mathbb{F}_2$?*
Abstract: Over $\mathbb{F}_2$, up to reciprocals, no pentanomial of degree m divides a trinomial of degree at most $2m$ except for 25 specific exceptions, all with degree $m < 14$, and one infinite family of pentanomials. A careful case analysis reveals that for large degree the coefficients cancel in a "staircase"-like manner. This divisibility property allows the construction of orthogonal arrays of strength 3.

[This is a joint work with L. Moura, D. Panario, B. Stevens and Q. Wang.]

Speaker: **John Dillon** (National Security Agency)
Title: *APN polynomials and related codes*
Abstract: A map $f : \mathrm{GF}(2^m) \to \mathrm{GF}(2^m)$ is APN (*almost perfect nonlinear*) if $x \mapsto f(x+a)-f(x)$ is 2-to-1 for all nonzero a in $\mathrm{GF}(2^m)$. Equivalently, the binary code of length $2^m - 1$ with parity-check matrix

$$H := \begin{bmatrix} \cdots & \omega^j & \cdots \\ \cdots & f(\omega^j) & \cdots \end{bmatrix}$$

is double-error-correcting, where ω is primitive in $\mathrm{GF}(2^m)$ and we may, without loss of generality, assume that $f(0) = 0$.

We give a brief review of these maps and their polynomials; and we present some new examples along with some related codes and designs which serve as invariants for their equivalence classes.

Speaker: **Andreas Enge** (Ecole polytechnique, Paris)
Title: *Asymptotically optimal computation of modular polynomials*
Abstract: Modular polynomials play an essential role in the Schoof-Elkies-Atkin algorithm for point counting on elliptic curves over finite fields, and they occur in several algorithms for constructing elliptic curves with prescribed complex multiplication. I present an algorithm based on floating point evaluation and interpolation that computes several flavours of modular polynomials in essentially linear time in the output size, and that has enabled us to set the recent records for elliptic curve point counting.

Speaker: **Luis H. Gallardo** (L'Universite de Bretagne Occidentale)
Title: *Sums of biquadrates in $\mathbb{F}_q[t]$*
Abstract: For most q's, it is known that every polynomial $P \in \mathbb{F}_q[t]$ that is a sum of biquadrates in $\mathbb{F}_q[t]$ is a strict sum, (i.e., if $P = A^4 + \ldots$ then $\deg(A^4) < \deg(P) + 4$), of 16 biquadrates.

Here we explain how we may reduce this to 11 biquadrates. Essentially this is done by using a new formula (that was discovered recently) to write t as a sum of 4 biquadrates when -1 is not a biquadrate in $\mathbb{F}_q$. (Its proof uses Jacobi sums).

[This is joint work with Mireille Car.]

Speaker: **Shuhong Gao** (Clemson University)
Title: *Primary decomposition of zero-dimensional ideals over finite fields*
Abstract: A new algorithm is presented for computing primary decomposition of zero-dimensional ideals over finite fields. Like Berlekamp's algorithm for univariate polynomials, the new method is based on the kernel of the Frobenius map acting on the quotient algebra. The dimension of the kernel equals the number of primary components, and a basis of the kernel yields a complete decomposition. Unlike previous approaches for multivariate polynomial systems, the new method needs no generic projections but reduces the problem directly to root finding of univariate polynomials over the ground field. If time permits, we shall show how Gröbner basis structure can be used to get partial primary components without root finding.

[Joint work with Daqing Wan and Mingsheng Wang.]

Speaker: **Arnaldo Garcia** (IMPA)
Title: *Some Artin-Schreier towers are easy*
Abstract: Towers of function fields (resp. of algebraic curves) over finite fields with positive limit, for the ratios of numbers of rational places over the genera, provide examples of curves with large genus having many rational points over a finite field. It is in general a difficult task to calculate the limit of a tower. In this talk we present a simple method how to calculate the genus of certain Artin-Schreier towers. As an illustration of our method we obtain a very simple and unified proof for the limits of some towers which attain the Drinfeld-Vladut bound or the Zink bound.The limits of their Galois closures can also be obtained similarly. The method computes the limit of certain towers avoiding the hard computations envolved in the determination of the individual genus of each function field in the tower.

Speaker: **Joachim von zur Gathen** (University of Bonn)
Title: *Counting bivariate polynomials: reducible, exceptional, and singular ones*
Abstract: Among the bivariate polynomials over a finite field, most are irreducible. We count some classes of special polynomials, namely the reducible ones, those with a square factor, the "exceptional" ones which are irreducible but factor over an extension field, and the singular ones, which have a root at which both partial derivatives vanish.

Speaker: **Guang Gong** (University of Waterloo)
Title: *Two-level Autocorrelation Sequences, Polynomials, and Exponential Sum Equalities*
Abstract: In this presentation, first, I will provide a survey of all the known constructions of (ideal) 2-level autocorrelation sequences with period $p^n - 1$ over a finite field $GF(p)$ where p is a prime and n is a positive integer. These sequences have important applications in code division multiple access (CDMA) communications. Any sequence over $GF(p)$ with period dividing $p^n - 1$ can be represented by a sum of multiple trace terms, which corresponds to a polynomial function from $GF(p^n)$ to $GF(p)$. Then I will present some conjectures on ternary sequences with 2-level autocorrelation, their trace representations, and some extremely surprising exponential sum equalities obtaining by iteratively applying the two operations of decimation and Hadamard transform.

Speaker: **James Hirschfeld** (University of Sussex)
Title: *Non-isomorphic maximal curves over a finite field*
Abstract: A *maximal curve* $\mathcal{F}$ over the finite field $\mathbf{F}_q$ is an algebraic curve attaining the Hasse–Weil upper bound,

$$q + 1 + 2g\sqrt{q},$$

where g is the genus of $\mathcal{F}$ and q is necessarily a square.

The genus of $\mathcal{F}$ satisfies the inequality,

$$g \leq \tfrac{1}{2}(q - \sqrt{q}),$$

where equality is achieved if and only if $\mathcal{F}$ is isomorphic to the Hermitian curve $\mathcal{H}_q$, given by the form,

$$X_0^{\sqrt{q}+1} + X_1^{\sqrt{q}+1} + X_2^{\sqrt{q}+1}.$$

If a curve is a quotient of $\mathcal{H}_q$, then it is maximal. It is conjectured that every maximal curve is a quotient of $\mathcal{H}_q$.

A family of quotient curves of $\mathcal{H}_q$ with genus $\sqrt{q} - 1$ is considered. The members of the family have many similar properties but provide many non-isomorphic maximal curves.

[Joint work with M. Giulietti, G. Korchmáros and F. Torres.]

Speaker: **Sophie Huczynska** (University of St Andrews)
Title: *The Strong Primitive Normal Basis Theorem*
Abstract: An element α of the extension E of degree n over the finite field $F = GF(q)$ is called free over F if $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a (normal) basis for E/F. The Primitive Normal Basis, first established in full by Lenstra and Schoof (1987), asserts that for any such extension E/F, there exists an element $\alpha \in E$ which is simultaneously primitive (generates the multiplicative group of E) and free over F (equivalently, there exists a primitive free polynomial). in this talk, I will discuss the following strengthening of this theorem: aside from four specific extensions E/F, there exists an element $\alpha \in E$ such that both α and α^{-1} are simultaneously primitive and free over F (equivalent to the existence of a pair of reciprocal primitive free polynomials).

[This is joint work with S.D.Cohen (Glasgow).]

Speaker: **Hendrik W. Lenstra** (University of Leiden)
Title: *Constructing finite fields*
Abstract: We shall describe an algorithm that, given a prime number p and an integer D with $D > (\log p)^{46/25}$, produces an irreducible polynomial f over $\mathbf{Z}/p\mathbf{Z}$ with $D \leq \deg f < 4D$. It is a particularly attractive feature of the algorithm that its run time is essentially linear in terms of the length of the output; that is, it runs in time at most $(d \log p) \cdot (2 + \log d + \log\log p)^c$, where c is some universal constant. The algorithm was developed jointly with Carl Pomerance, as a byproduct of a new primality test.

Speaker: **Winnie Li** (Pennsylvania State University)
Title: *Characterizations of pseudo-codewords of a parity-check code*
Abstract: In this survey talk we shall explain how pseudo-codewords of a parity-check code arise, the role they play in the fast decoding algorithms, and give two ways to characterize them.

Speaker: **Petr Lisonek** (Simon Fraser University)
Title: *Caps and highly nonlinear functions on finite fields*
Abstract: We consider functions on binary vector spaces which are far from linear functions in different senses. Three well studied classes of such functions are crooked (CR) functions, almost bent (AB) functions and almost perfect nonlinear (APN) functions. In the binary case all known constructions of such functions arise from certain monomial functions on GF(2^n). In 2003 van Dam and Fon-Der-Flaass obtained a combinatorial characterization of all AB functions in terms of the number of solutions to a certain system of equations. We study a similar characterization for certain classes of APN functions. We discuss an application of this characterization in the study of caps in the finite projective spaces over GF(2).

Speaker: **Ariane Masuda** (Carleton University)
Title: *Permutation binomials over $\mathbb{F}_{2^k p+1}$ where p and $2^k p + 1$ are primes*

Abstract: In this talk we present results on the characterization of permutation binomials over $\mathbb{F}_{2^k p+1}$ where $k \geq 1$, p and $2^k p + 1$ are primes. We also give a formula for the number of permutation binomials of degree smaller than $q-1$ when $k = 1$ and 2.

[This is joint work with Daniel Panario and Steven Wang.]

Speaker: **Marko Moisio** (University of Vaasa)
Title: *Kloosterman curves, their fibre products, and explicit enumeration of irreducible polynomials with two coefficients prescribed, I*
Abstract: Let $\mathbb{F}_q$ be a finite field with $q = p^r$ and let $c \in \mathbb{F}_q$. In this talk some preliminaries for an explicit enumeration of the irreducible polynomials

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$$

with $a_{m-1} = 0$ and $a_1 = c$, are given.

First, for $a, b \in \mathbb{F}_q^*$ $(a \neq b)$, the number of rational places of the function field $\mathbb{F}_{q^m}(x, y, z)$ with $y^q - y = x + ax^{-1}$, $z^q - z = x + bx^{-1}$, is given in terms of moments of Kloosterman sums over $\mathbb{F}_q$. Secondly, evaluation of moments in cases $p = 2, 3$ is considered. More precisely, the moments are connected by Pless's power moment identity to the weight distribution of Melas codes, which opens up a possibility to evaluate moments by using explicit weight formulae obtained by Schoof, van der Vlugt, and van der Geer.

We illustrate the method by giving explicitely the number of rational places of $\mathbb{F}_{q^m}(x, y, z)$ for $m = 1, \ldots, 10$.

Speaker: **Gary Mullen** (Pennsylvania State University)
Title: *A polynomial analogue of the* $3n + 1$ *problem*
Abstract: The integer $3n+1$ problem is a well studied but still open problem. In particular, if n is an even positive integer, then one divides by 2 while if n is odd, one calculates $3n+1$. The process is repeated and the $3n + 1$ problem conjectures that after a finite number of iterations, one always ends at the value 1.

I will discuss a polynomial analogue of this problem which was first motivated by considering polynomials over the binary field $\mathbb{F}_2$. We will consider an even more general version over any field. The interesting point is that after a finite number of iterations, our algorithm for monic polynomials over a field always ends at 1. We will also discuss several related open problems which arise in the case of the binary field $\mathbb{F}_2$.

Speaker: **Jang-Woo Park** (Clemson University)
Title: *Monomial dynamics over finite fields*
Abstract: Let k be a finite field and $f : k^n \to k^n$ a map defined by polynomials. It is an important problem to study the dynamics of f, particularly its fixed points and cycles of various lengths. This problem is well understood for linear functions, but wide open for nonlinear funtions. In this talk, we present our recent work on dynamics defined by monomials.

Speaker: **Mateja Presern** (Univeristy of Glasgow)
Title: *Completing the Hansen-Mullen primitivity conjecture*
Abstract: The Hansen-Mullen Primitivity Conjecture (1992) is that, generally, there exists a primitive polynomial of degree n over a finite field $\mathbb{F}_q$ with any coefficient arbitrarily prescribed. This was proved by S. D. Cohen for $n \leq 3$ and $n \geq 9$ and S. D. Cohen and M. Prešern for $n = 4$. We present refinements of these ideas which yield the facts that the 3rd or 4th (or $(n-3)$rd or $(n-4)$th) coefficient can be prescribed, thus completing the proof of the Hansen-Mullen Primitivity Conjecture. We particularly focus on primitive polynomials of degree 8. A very small amount of computation is needed.

[This is joint work with S. D. Cohen.]

Speaker: **Kalle Ranto** (University of Turku)
Title: *Kloosterman curves, their fibre products, and explicit enumeration of irreducible polynomials with two coefficients prescribed, II*

Abstract: Let $\mathbb{F}_q$ be a finite field with $q = p^r$ and let $c \in \mathbb{F}_q$. We show how the number of irreducible polynomials $x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$ with $a_{m-1} = 0$ and $a_1 = c$ is connected to the number of rational places of the function field $\mathbb{F}_{q^m}(x, y, z)$ with $y^q - y = x + ax^{-1}$, $z^q - z = x + bx^{-1}$, $a, b \in \mathbb{F}_q^*$, and $a \neq b$. The number of these rational places in cases $p = 2, 3$ were recently obtained by Marko Moisio, and this enables us to give the number of irreducible polynomials in question when $m = 1, ..., 10$.

Speaker: **Frank Ruskey** (University of Victoria)
Title: *Exhaustive generation of irreducible polynomials over small finite fields*
Abstract: We have exhaustively generated all irreducible polynomials over GF(2), GF(3), GF(4), GF(5), GF(7), and GF(8) for "reasonable" values of n. Reasonable means that they will fit on a single CD after compression. For example, over GF(3) we generate up to degree $n = 20$, and there are 174,342,216 such polynomials. We also generate one million primitive polynomials for each degree $n \leq 64$. The basic technique is to generate Lyndon strings and convert each string to a polynomial using a shift and add technique on computer words. The optimization of the crucial add routine leads to interesting questions in circuit optimization that are addressed in the latest drafts of Knuth Volume IV.

Using the data we have produced tables computing various statistics of the polynomials and will present several conjectures based on those statistics.

[This research done together with my Ph.D. student Gilbert Lee.]

Speaker: **Igor Semaev** (University of Bergen)
Title: *On solving sparse algebraic equations over finite fields*
Abstract: A system of algebraic equations over a finite field is called sparse if each equation depends on a small number of variables. In this talk new deterministic algorithms for solving such equations are presented. The mathematical expectation of their running time is derived. These estimates are at present the best theoretical bounds on the complexity of solving average instances of the above problem.

Speaker: **Igor Shparlinski** (Macquarie University)
Title: *On the Sato-Tate conjecture on average*
Abstract: We obtain asymptotic formulae for the number elliptic curves $E_{a,b} : Y^2 = X^3 + aX + b$ over a field $\mathbb{F}_p$ where p is prime, satisfying certain "natural" properties. We consider the cases when:

- a and b are fixed but p is chosen at random with $p \leq x$,
- p is fixed but a and b are chosen at random with $|a| \leq A$ and $|b| \leq B$,
- a, b and p are chosen at random with $|a| \leq A$, $|b| \leq B$ and $p \leq x$.

Specifically, we investigate the behavior of such curves with respect to the Sato-Tate conjecture, cyclicity and divisibility of the number of points by a fixed integer m.

[Joint work with Bill Banks.]

Speaker: **Horacio Tapia-Recillas** (Universidad Autonoma Metropolitana-Iztapalapa)
Title: *The simplex code over finite chain rings*
Abstract: Codes over finite rings have been studied since the early seventies, particularly over the ring $\mathbb{Z}_m$ of integer modulo m. Recently the ring $\mathbb{Z}_4$ has been of particular interest after the work of Nechaev and later, Hammond et al. These authors show that certain non-linear binary codes with good parameters, including the Kerdock and Preparata codes, are the image of $\mathbb{Z}_4$ linear codes under the Gray isometry between $(\mathbb{Z}_4^n, d_L)$ and $(\mathbb{Z}_2^{2n}, d_H)$, (here d_L and d_H are the Lee and Hamming distance respectively). This result has motivated the study of several types of codes over finite rings and their image under the (generalized) Gray isometry. These rings include $\mathbb{Z}_{p^s}$ where p is a prime and s a positive integer, Galois rings, finite chain rings and Frobenious rings, to mention some of them. Recently the simplex code over the ring $\mathbb{Z}_{2^s}$ has been introduced and some of its properties studied. Since this ring, and, more generally, the ring $\mathbb{Z}_{p^s}$ where p is a prime and s a positive integer, is a particular case of a Galois ring and the latter is an example

of a finite chain ring, it is natural to ask if it is possible to extend some of the results previously given for the (linear) simplex code over the ring $\mathbb{Z}_{2^s}$ to the case of finite chain rings. Also, the Gray isometry for codes over a finite chain ring has been introduced; thus, one can ask if the image under the Gray isometry of the (linear) simplex code defined over a finite chain ring is still linear. In this talk the simplex code over a finite chain ring is defined and its homogeneous weight distribution is determined. Furthermore, it is shown with an example that the image of this simplex code under the Gray isometry is not linear in general.

Speaker: **Felipe Voloch** (University of Texas at Austin)
Title: *Symmetric Cryptography and Algebraic Curves*
Abstract: The S-boxes of symmetric cryptography can be viewed as polynomials over finite fields (of characteristic two). Their non-linearity properties, which are important for their use in cryptography, translate into properties of certain algebraic curves. I will explain these facts and present some results obtained along these lines.

Speaker: **Daqing Wan** (University of Calirfornia, Irvine)
Title: *Counting rational points on varieties over finite fields*
Abstract: This is an expository lecture on both complexity and algorithms for counting the number of rational points on a hypersurface over a finite field, with an emphasis on modular reduction via p-adic methods.

Speaker: **Qiang (Steven) Wang** (Carleton University)
Title: *Permutation polynomials and sequences over finite fields*
Abstract: A polynomial over a finite field is called a permutation polynomial if it induces a bijective map from the finite field to itself. Permutation polynomials were first investigated by Hermite, and since then, many studies concerning them have been devoted. Recently there has been a revival in the interest for permutation polynomials, in part due to their applications in coding theory, combinatorics, and cryptography. In this talk I will describe some new classes of permutation polynomials of finite fields in terms of sequences over finite fields. I will also explain the tight connections between permutation behaviors of binomials and the periodicity of certain class of sequences.

Speaker: **Joseph L. Yucas** (Southern Illinois University)
Title: *Generalized reciprocals and factors of Dickson polynomials*
Abstract: We discuss recent results on Dickson polynomials. In particular we give new descriptions of the factors of Dickson polynomials over finite fields in terms of cyclotomic factors. To do this generalized reciprocal polynomials are introduced and characterized.

[This is joint work with Robert W. Fitzgerald.]

Speaker: **Michael Zieve** (IDA Center for Communications Research)
Title: *Polynomial decomposition*
Abstract: Consider the operation of composition on polynomials over a field K, namely $(f \circ g)(x) = f(g(x))$. A polynomial of degree at least 2 is called indecomposable if it cannot be written as the composition of polynomials of strictly lower degree. Every polynomial f of degree at least 2 can be written as the composition of indecomposable polynomials, but this decomposition need not be unique. However, if K has characteristic zero, then results of Ritt, Levi, Engstrom, and Schinzel provide a complete theory of polynomial decomposition – for instance, any two decompositions of f must have the same length, and it is known how to produce all decompositions of f from any single decomposition.

I will present several results and examples about the analogous problem in fields of positive characteristic. Along the way I will present new examples of indecomposable polynomials which decompose over an extension field; new types of reducible 'variables separated' polynomials $f(x) - g(y)$; and various results on computing the intersection of two subfields of $K(x)$.