<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Time</th>
<th>Place</th>
<th>Speaker</th>
<th>Title</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, September 27</td>
<td>Discrete Mathematics Seminar</td>
<td>3:30 p.m. – 4:30 p.m.</td>
<td>Jeffery 115</td>
<td>Chris Godsil, University of Waterloo</td>
<td>State Transfer on Graphs</td>
<td>Attached</td>
</tr>
<tr>
<td>Wednesday, September 28</td>
<td>Curves Seminar</td>
<td>3:30 p.m. – 5:00 p.m.</td>
<td>Jeffery 319</td>
<td>Tony Geramita</td>
<td>Will continue his series of lectures on Waring’s problem for Forms</td>
<td></td>
</tr>
<tr>
<td>Friday, September 30</td>
<td>Number Theory Seminar</td>
<td>11:30 a.m. – 12:20 p.m.</td>
<td>Jeffery 422</td>
<td>Ramarathnam Venkatesan, Microsoft and University of Toronto</td>
<td>Non Abelian Analogues of Lattice Rounding</td>
<td>Attached</td>
</tr>
<tr>
<td>Friday, September 30</td>
<td>Department Colloquium</td>
<td>2:30 p.m.</td>
<td>Jeffery 234</td>
<td>Ramarathnam Venkatesan, Microsoft and University of Toronto</td>
<td>Random Continued fractions and new attacks on small exponent RSA</td>
<td>Attached</td>
</tr>
<tr>
<td>Monday, October 3</td>
<td>Algebraic Geometry Seminar</td>
<td>4:30 p.m. – 5:30 p.m.</td>
<td>Jeffery 319</td>
<td>Eric Katz, Waterloo</td>
<td>Log concavity of characteristic polynomials and tropical intersection theory</td>
<td>Attached</td>
</tr>
<tr>
<td>Wednesday, October 5</td>
<td>Department Meeting</td>
<td>3:30 p.m.</td>
<td>Jeffery 234</td>
<td>Dr. Alistair MacLean and Dr. Cynthia Fekken</td>
<td>Visit during the departmental meeting time. Time permitting the normal department meeting will start immediately following the visit.</td>
<td></td>
</tr>
</tbody>
</table>

Items for the Info Sheet should reach Anne (burnsa@mast.queensu.ca) by noon on Monday. The Info Sheet is published every Tuesday.

**Tuesday, September 27, 3:30 p.m. Jeffery 115**

Speaker: Chris Godsil  
Title: State Transfer on Graphs

**Abstract:** If A is the adjacency matrix of a graph, we define the transition operator \( H(t) \) by \( H(t) = \exp(itA) \). This a symmetric, unitary matrix that defines what physicists call a continuous quantum walk. The basic problem is to relate the properties of the systems modelled by \( H(t) \) to the structure of the underlying graph. I will discuss how standard tools from algebraic graph theory yield useful information, and also introduce some of the interesting problems that remain.
Number Theory Seminar

Friday, September 30, 11:30 a.m. Jeffery 422
Speaker: Ramarathnam Venkatesan
Title: Non Abelian Analogues of Lattice Rounding

Abstract: Given a point y in R^n and a lattice (by its basis), the closest vector problem asks one to compute a lattice point closest to y. Classic LLL Lattice Reduction algorithm can be used to efficiently compute an approximation within a factor depending only on n (namely, \(2^{O(n)}\)). In this talk, we study the analogue in matrix groups where a discrete subgroup of generators we show that there is no similar such approximation depending on dimensions only, is possible. We also show that under a mild condition on the generators (separation of first and second Lyapunov exponents) one can decompose a random word on generators efficiently back to a product of generators.

This is joint work with Steve Miller (Rutgers) and Evgeny Begelfor (Hebrew University)

Department Colloquium

Friday, September 30, 2:30 p.m. Jeffery 234
Speaker: Ramarathnam Venkatesan,
Title: Random Continued fractions and new attacks on small exponent RSA

Abstract: We describe a new algorithm to attack small exponent RSA using continued fractions. We show that lattice reduction algorithms can be used to improve the attack on RSA for secret exponents of size up to \(n^{0.32}\), if the system of polynomials produced by the reduction stage are algebraically independent (usually assumed heuristically). We discuss our experimental results.

Joint work with
Bhargav Narayanan (IIT Madras-> Trinity college, Cambridge)
Stephen Miller (Rutgers)
C. Pandurangan (IIT Madras)

Algebraic Geometry Seminar

Monday, October 3, 4:30 p.m. Jeffery 319
Speaker: Eric Katz
Title: Log concavity of characteristic polynomials and tropical intersection theory

Abstract: In a recent joint work with June Huh, we proved the log concavity of the characteristic polynomial of a realizable matroid by relating its coefficients to intersection numbers on an algebraic variety and applying an algebraic geometric inequality. This extended earlier work of Huh which resolved a conjecture in graph theory. In this talk, we rephrase the problem in terms of more familiar algebraic geometry, outline the proof, and discuss an approach to extending this proof to all matroids. Our approach suggests a general theory of positivity in tropical geometry.