The University of Montana

Department of Mathematical Sciences

A Newsletter for Alumni, Faculty, Staff, and Friends Spring 2007

Math Ph.D. Student Wins University Teaching Award

by Greg St. George

Seth Braver, a graduate student in the Department of Mathematical Sciences, has won the University's 2006-2007 Graduate Assistant Teaching Award. This award was recently established by the UM Center for Teaching Excellence, the Graduate School and the Provost's Office to honor outstanding teaching by a graduate teaching assistant. Only one is awarded each year, and winners receive $1,000 and a trophy.

Seth, who is a doctoral student, taught an experimental version of the Math 107 course last spring and again during the spring 2007 semester. The students largely come from non-scientific majors and have very limited mathematical background knowledge. Seth introduced these students to the Elements, a book by Euclid dating from about 300 BCE. Although high school geometry courses used to be based on this material, this is no longer the case, and so for many of the students this was their first exposure to the abstract logical development of plane geometry. The glowing reviews that the course received are testament to Seth's success teaching this difficult material.

Seth has an undergraduate degree, summa cum laude, from San Francisco State University, and a master’s degree from the University of California at Santa Cruz. Seth is finishing a thesis regarding the famous Russian geometer Nikolai Lobachevski's “Theory of Parallels”, under the direction of Professors Karel Stroethoff and Greg St. George, which he defended this spring.

In This Issue:

And quite a bit more!

The addition to the math building has just been completed – see our website for more photos; we will tell you more about it in the next newsletter. **The official inauguration of the addition is planned for September – we hope you will be able to join us for this celebration!** Details will be posted on our web site.

Cryptography

by Jenny McNulty

As long as there have been secrets, there have been ways to encode (or encrypt) these messages. For example, Caesar used a simple shift of the alphabet to encode messages of military importance to his troops. This is one of the first recorded uses of ciphers. Mary Queen of Scots was put to death after her secret message was intercepted and decoded. Since this time, codes (encryption) have come a long way. Did you know every time you purchase something on-line you are using mathematics to encrypt your information? All basic data encryptions (including those used on the internet) are based on the mathematical principles of number theory. In this article we explore the mathematics behind internet encryption, in particular we will investigate the RSA system of public key cryptography.

Before we introduce the mathematics, let’s consider the Caesar cipher and make a few general observations. The Caesar cipher is a shift of length 3. To encode a message we simply shift the letters (to the right) by 3. Thus, A becomes D, B becomes E, etc. with Z being encrypted as C. A few things to note, (1) the shift involves “wrap-around”, (2) to decrypt we shift letters to the left by 3, (3) this code is easy to crack, and (4) these ideas apply to numbers as well as letters.

(Continued on page 6 - “Cryptography”)

Notes from the Chair

As the spring semester comes to a close, I am excited to report that the Math Building addition is finally done. There were some construction delays which pushed back the finish date from early in the semester to nearly the end, but it was all worth it. It is beautiful! The exterior matches the old building and is connected to the new building by all-glass hallways. In addition to the elevator, we now have modern bathrooms on every floor and seven new offices with lots of windows. While the official dedication will be in September, I invite you to stop by any weekday (including the summer) to take a look for yourself. I guarantee you that you'll be impressed.

Three members of our department received major University awards this past year – one faculty member (Jim Hirstein, Faculty Service Award), one staff member (Michelle Johnsen, Outstanding Staff Award for Excellence in Job Performance) and one graduate student (Seth Braver, Graduate Assistant Teaching Award). That's a remarkable record for one year, but indicative of the quality of the faculty, staff and students in the department.

Twenty-one students will receive degrees in the mathematical sciences this spring (page 7). I would like to especially recognize our two Ph.D. recipients – Seth Braver and Kathy Gray. Seth completed our Option II program for those intending to become college teachers and was an ideal student for that program. His dissertation, under co-advisors Karel Stroethoff and Greg St. George, entitled "Lobachevski Illuminated: Content, Methods, and Context of the Theory of Parallels," is a new English translation of Lobachevski's work (in German) on the theory of parallels, with extensive mathematical, historical and philosophical commentary. Anyone who has heard Seth give a talk about geometry or any of his other mathematical interests, knows why he was selected as the University's outstanding teaching assistant this year (story on page 1). Seth will teach in our department next year as an adjunct assistant professor. Kathy received a Bachelor's degree in Wildlife Biology from UM 11 years ago. She then decided to get a second Bachelor's in our department with an emphasis in statistics. I doubt she suspected then that she would continue on to an M.A., a Ph.D. and, starting this fall, a tenure-track assistant professor position in statistics at Cal State – Chico. Along the way, she has been an outstanding T.A. – so good, in fact, that we asked her to teach the large lecture introductory statistics course as a full-time adjunct this past year. She also worked part-time at the Forest Service Fire Lab on a variety of projects combining her interests in biology and statistics. As her co-advisor (with Brian Steele) for her dissertation on trend detection in time series data with applications to bird and animal populations, I am very proud of Kathy's accomplishments, but also sad to see her go.

New Ph.D.'s Seth Braver and Kathy Gray in front of the entrance to the Math Building addition.

Finally, I would like to thank those of you who donated money to the department this past year. Our list of donors may not be as long as those of the professional schools like Business and Pharmacy, but I am impressed by the number of you who donate every year. Your continuing support of our scholarships and programs is very gratifying.

Best wishes for the summer,

Dave Patterson

Faculty:
David Patterson, *Chair*
Jenny McNulty, *Associate Chair-Graduate Program*
Nikolaus Vonessen, *Associate Chair-Undergraduate Program and Newsletter Editor*

John Bardsley, *Applied Mathematics*
Rick Billstein, *Mathematics Education*
Lauren Fern, *Lecturer*
Jon Graham, *Statistics*
Jennifer Halfpap, *Analysis*
Solomon Harrar, *Statistics*
Jim Hirstein, *Mathematics Education*
Leonid Kalachev, *Applied Mathematics*
Mark Kayll, *Combinatorics*
Libby Knott, *Mathematics Education*
Jenny McNulty, *Combinatorics*
George McRae, *Optimization*
Adam Nyman, *Algebra*
David Patterson, *Statistics*
Jakayla Robbins, *Combinatorics*
Matt Roscoe, *Lecturer*
Greg St. George, *Analysis*
Regina Souza, *Lecturer*
Bharath Sriraman, *Education*
Brian Steele, *Statistics*
Emily Stone, *Applied Mathematics*
Karel Stroethoff, *Analysis*
Thomas Tonev, *Analysis*
Carol Ulsafer, *Lecturer*
Nikolaus Vonessen, *Algebra*

Staff:
Michelle Johnsen, *Office Manager*
Linda Azure, *Administrative Associate*
Brenda Brown, *Administrative Associate*
Guy Shepard, *Computer Systems Administrator*

Faculty Emeriti:
William Ballard
Mary Jean Brod
Charles Bryan
Bill Derrick
Rudy Gideon
Stanley Grossman
Gloria Hewitt
Don Loftsgaarden
Johnny Lott
Merle Manis
Robert McKelvey
William Myers
Howard Reinhardt
George Votruba
Keith Yale

James Hirstein wins Faculty Service Award

by Nikolaus Vonessen

In recognition of his long and distinguished service record, Jim Hirstein, Professor of Mathematics and past chair of the Department of Mathematical Sciences, received this year's *Montana Faculty Service Award* at the Charter Day 2007 ceremonies.

Jim joined the department in 1989, and has since been involved in teaching, research and service at many levels. From the Department's point of view, his most important service contribution were his six years as chair, from 1999 to 2005. Under his leadership, the department weathered several storms and made important advances. Throughout, Jim always treated people fairly and humanely, while upholding department and university policies and standards. One of Jim's outstanding qualities is that he is very approachable; he is always willing to listen, to give advice, and most importantly, to do something about the issue at hand. In our department, chairs typically serve only three years. But we didn't let him get away with it, and – in a rare event – elected him for a second term.

Jim's service was not restricted to the department. He served on many of the most important university committees, and chaired two of them, including the university's *Strategic Planning and Budget Committee*. He also served on various state committees such as the *Committee to Write the State Mathematics Standards for K-12*, which produced important documents regarding the education of students in Montana. At the national level, he served on various committees and was involved in several large grants.

His exceptional service contributions were also recognized by the administration. To quote from an evaluation of Jim's performance by James Flightner, a former dean of the College of Arts and Sciences: "[Jim is] chair of UM's most demanding committee…, chair of a large, complex department with UM's largest service role, and a 'No fuss, can do, do do' approach to each… enough said, this service contribution is stellar." Enough said, indeed. **Congratulations, Jim! You deserve it!**

Outstanding Staff Award goes to Michelle Johnsen

by David Patterson

The UM Staff Senate awarded the 2006-7 UM *Outstanding Staff Award for Excellence in Job Performance* to our own Michelle Johnsen, the office manager for the Department. Michelle was presented with her award (including a check for $1,500) by UM President George Dennison at the University Awards Ceremony on April 25. Those of you who know Michelle won't be surprised by this award; she has been a dedicated, helpful, and always cheerful member of our staff since 1993. She started out as one of the two secretaries under then-office manager Valerie Crepeau and moved into Valerie's position when Valerie moved to Information Technology in 2000. When I solicited supporting statements for Michelle's nomination for the award this spring, many students and faculty responded. Here are just a couple of those statements: "Michelle has always been so kind and hard working. She makes the office a comfortable place to be and seems to have the answer to every question" (from a graduate student) and "When I was interviewing at Montana, I was delighted to see how organized Michelle is. Michelle's work prior to, during, and after my interview is one of the reasons I felt comfortable accepting the job" (from a new faculty member). As the current Department Chair and a former Associate Chair, I know that Michelle is indispensable to the smooth operation of the department. She does many things well, including being a top notch organizer of events like our annual awards ceremony and departmental picnic and softball game. **Congratulations, Michelle!**

Student Profile: Hallie Torrey

by James Hirstein

Hallie Torrey is a senior in applied mathematics from Salmon, Idaho. She came to The University of Montana in the fall of 2003 on a Western Undergraduate Exchange Scholarship, along with scholarship awards from Backstage Dance Studio and Kiwanis for Leadership.

Here at UM, Hallie has been a member of the Davidson Honors College and the Golden Key International Honor Society. She received a Department of Mathematical Sciences Tutorial Scholarship, working with Dr. Robbins in Calculus and with Dr. McRae in the Introduction to Abstract Mathematics course. She has been a member and an officer of the Math Club, President of the UM Honors Student Association, and a member of Pi Mu Epsilon (the mathematics honor society). In the spring of 2007, Hallie presented "The Dynamics of Money: Linking Physics and Finance" at the Western Regional Honors Conference in Anaheim, CA. She is a three-year volunteer in Missoula's after-school Flagship Program. She tutored students in mathematics and science at Meadow Hill Middle School and was recently honored for her work there as the recipient of the 2007 Outstanding Student Volunteer Award.

Hallie will graduate with honors this May. She will receive a B.A. with an emphasis in Applied Mathematics. She will also wear the medallion of the President's Senior Recognition Award, selected by Pi Mu Epsilon. In the fall, Hallie plans to attend the University of Washington to begin work on a master's degree in applied mathematics.

Greetings from Helsinki

by John Bardsley

The University of Montana offers its faculty a remarkable opportunity through its Faculty Exchange Program: six months to a year abroad with full pay and no sabbatical penalty. When I found out about it during my first year in the Department of Mathematical Sciences, I knew that I would apply at some point. As it has turned out, I applied in my third year and am now, as I write, almost eight months into my stay at the University of Helsinki in Finland. With me are my wife Jennifer, son Alex, and daughter Elli.

A question that I've gotten many times, both from Americans before I left the U.S. and from Finns while I've been here, is, "Why Finland?" My choice was originally determined by the facts that the University of Helsinki is one of a small list of host universities offered by the Exchange Program and that Finland is a hot bed for the type of applied mathematics that I study, namely, Inverse Problems. However, having spent nearly three quarters of a year here, I've come to believe that a much more appropriate answer to this question, and the one that I now use, is, "Why not?" Finland is a great country.

I have been fortunate to have been able to travel widely within Finland. This has been thanks, in large part, to spring semester 2006 UM Visiting Professor Heikki Haario, who has sponsored my travel to a number of research meetings because of my work on one of his group's research projects. In my travels, I have visited all of the main Finnish cities as well as the skiing towns of Luosto and Koli and have been struck by the fact that even the smaller cities have a cosmopolitan feel. But it is the subtle natural beauty of Finland that has made the deepest impression on me. The most dramatically beautiful region that I have visited is the fell (small mountain) region of Lapland near Luosto, where there are real mountains; where the forests are old; where the sky is big; and where in winter the snow is deep and the cross country skiing outstanding.

Helsinki, where we live, is a great city, with good museums, cafes and an edgy (in a good way) feel, but with its vast trail system, accessible forest and placement on the Baltic Sea, outdoor play opportunities are plentiful. It is a particularly beautiful place to be in the summer, but is a gem in any season.

It is true that winters in Finland are long and dark, but one can easily survive by doing what the locals do: winter sports (cross country skiing and ice skating are Finnish favorites), sauna, and the consumption of the occasional beer (or so I've been told). Given the close proximity of our flat to Helsinki's main cross country ski tracks, we have done a lot of cross country skiing during this year's short winter. We also downhill skied as a family in Lapland, and I was fortunate to be able to take part in a long distance trek known as the Rajalta Rajalle-hiihto, translated "from border to border-cross country ski", in which participants skied over 400 kilometers in a seven day period, from the Russian to the Swedish borders across Finland.*

My impression of Finland has been colored, in large part, by the fact that I am here with my family; so that rather than being able to comment on the quality of Helsinki's night life and restaurants, I can say something about my kids' experience with the school system. You may know that the Finnish education system is considered one of the best in the world, but such a general statement and particular experience don't always go hand in hand, particularly for foreign students who only spend one year in school.

My ten year old son Alex has spent the year in a public international school, where instruction is in English. Overcrowded classes, insufficient funds for school supplies, and a very inexperienced teacher quickly make one realize that many of the problems faced by American schools are also faced here. On the positive side, Alex's classmates are from all over the world – Africa, Iran, U.S.A., and Indonesia to name a few – and he has made some great friends. So even if his scholastic experience has been only adequate (at least we hope), the social experience has been priceless.

Our daughter Elli has had a very different experience due to the fact that we chose to enroll her in our neighborhood school, where all instruction is in Finnish. The effort that it has required for her to gain fluency in her interactions with friends – which began to occur only in the seventh month of our stay – has required so much effort on her part that it has monopolized her scholastic experience. My wife has had to work with her outside of school to keep her up to speed so that she'll be ready to reenter Missoula's public schools.

Professionally, the opportunity to focus on research has been a great experience for me. I feel that I have reached a higher level of maturation as a mathematician. I will return to Missoula more confident in my abilities as a researcher than when I left. The time has been very productive, both in terms of my own work as well as in my collaborations with others here in Finland. I have to thank the Faculty Exchange Program, the University of Helsinki, and, most of all, my colleagues in the Department of Mathematical Sciences, for making this exchange possible.

I have found it very valuable to spend time in another country. I have come to greatly appreciate Finnish culture and society; things run so smoothly here. But I have also gained a deeper appreciation of American culture. Also, it has been great to be in a place where we have no roots, because it has required us to depend more on each other. As a result, we are closer as a family. It has been good for Jen too, because she has had more time to do her art. However, we all anxiously await our return to the U.S. and to Missoula, and I look forward to returning to the Department of Mathematical Sciences.

Professor Bardsley and his family will return to Missoula on July 31, 2007.

*John Bardsley wrote an article for the Missoulian about this amazing trip, see http://www.missoulian.com/articles/2007/04/05/outdoors/out19.txt.

2007 Scholarship and Award Winners

Joseph Hashisaki
Memorial Scholarship
Erin Mondloch

Mac Johnson Family Scholarships
Katharine Banner
Jade Roskam
Kristen Waarvik

Undergraduate Teaching Scholars
Tamatha Abell Katharine Banner
Nicole Crouch Clark Kogan
Stephen Schutten Tricia Vanetta
Kristen Waarvik

John A. Peterson Awards
for Math Education
Natalie Creamer
Shannon Johnson

Pi Mu Epsilon New Members
Katharine Banner Hamza Haffari
Scott Lambert Erica Miller
Erin Mondloch Nick Paterno
Stephen Schutten Tricia Vannatta
Kristen Waarvik

President's Senior
Recognition Awards
Jeff Arends (Pure Mathematics)
Anita Sindelar Bohlert (Applied Math)
Beth Hegland (Statistics)
Shannon Johnson (Mathematics Educ.)
Mandy McCoughey (BA in Math Sci.)
Hallie Torrey (Pi Mu Epsilon)

Graduate Student
Distinguished Teaching Awards
Scott Lambert
Rebekah Yates

Graduate Student
Summer Research Awards
Michael Gilliam
Scott Lambert
N'Djekornom Dara Laobeul

Bertha Morton Scholarships
(from UM's Graduate School)
Scott Lambert
N'Djekornom Dara Laobeul

Graduate Assistant Teaching Award
(University Award)
Seth Braver

Honor Roll of Donors

William and Lee Ballard
Linda Baugher
Ruth Brocklebank
Rodney and Mary Jean Brod
Arthur and Shirley Clarkson
Lauren Doyle
Mark and Terry Eastman
Frank L. Gilfeather
Gary Glaze
Francis T. Hannick
Mary Hashisaki
Gloria C. Hewitt
William and Barbara Irlbeck
Stephen Johnson
Gary and Daryl Little
Lynne Loerzel
Nenette and Don Loftsgaarden
Sandra and Bruce Mueller
Todd Oberg
Harvey Odgen
David Patterson
Jeffery Pagdett and Catherine Stewart
Betty B. Remington
David Sherry and Jeanne Ambruster
Gregory and Jan St. George
Nikolaus Vonessen and Regina Souza
Carla and Richard Welter
David Winkler

Department News

After retiring from the math department, Emeritus Professor **Johnny Lott** served part-time as director of UM's Center for Teaching Excellence. But retirement did not fit him – this February he accepted a new challenge: he is now (full-time) director of the Center for Excellence in Teaching and Learning at the University of Mississippi (another "UM"), and a professor of both Mathematics and Education. Good Luck, Johnny – we miss you!

The 9th edition of the bestselling textbook *A Problem Solving Approach to Mathematics for Elementary School Teachers* (2007) by Professor **Rick Billstein**, Professor Shlomo Libeskind (University of Oregon) and Emeritus Professor **Johnny Lott** was recently published by Addison Wesley Longman Publishing Co. The 1095-page tome also appeared as an instructor's edition, and is accompanied by many ancillaries.

Professor **Thomas Tonev** published a new advanced monograph with the renowned mathematical publishing company Birkhäuser. He coauthored the book, *Shift-invariant Uniform Algebras on Groups*, with Suren Grigoryan, a professor at Kazan State University in Russia, who has visited UM several times over the past years.

Professor **Jenny McNulty** and Assistant Professor **Jakayla Robbins** organized last fall the three-day *Montana Matroid Workshop*. The conference was attended by students and faculty from UM and around the country. The two invited speakers were Thomas Brylawski (University of North Carolina) and Talmage James Reid (University of Mississippi). In addition to the invited talks, there were talks by faculty, a mini-course about matroids for students, and a problem session for faculty and more advanced graduate students.

You may know Associate Professor **Bharath Sriraman** as the editor of the online journal *The Montana Mathematics Enthusiast* (see page 7 of our Fall 2006 newsletter). He just published the first TMME monograph, *International Perspectives on Social Justice in Mathematics Education*, which contains a collection of articles with authors from nine different countries. It is available both online at http://www.montanamath.org/TMME/ and as a print edition.

First-year master's student **Demitri Plessas** won the *Best Graduate Oral Presentation Award* for a talk he presented at the annual meeting of the Montana Academy of Sciences this April. In his talk, titled *Simple Loopless Graphs with Strong Morphisms is an Impoverished Category*, he reported on work done under the supervision of his advisor, Professor **George McRae**.

Lecturer **Matt Roscoe** (M.Ed. 2000) who also serves as the Director of our Mathematics Learning Center, decided to go over to the other side, and be once again a student: Come fall, he will be enrolled in our Ph.D. program in Mathematics Education, while working for the department as a teaching assistant. For most of the spring semester he had us worried that he might study at our arch rival MSU. But he finally came to his senses and decided to pursue his doctoral work at UM! ☺

Cryptography *- Continued from page 1*

We use the concept of modular arithmetic, to formalize the idea "wrap-around". Let m be a positive integer, then for any integers a, b, we say $a \equiv b \bmod m$ (read "a is congruent to b mod m") if m divides $(a – b)$ or equivalently if a and b have the same remainder upon division by m. For example, $28 \equiv 2 \bmod 26$. If we think of the letters A-Z as the numbers 00-25, then the Caesar shift can be thought of as addition of 3 mod 26. (Z is 25, add 3 to get 28, reduce mod 26 to get 2, 2 is C.) Thus, decryption is just the inverse operation, that is subtraction by 3 mod 26.

The RSA system is an exponential cipher, that is to say encryption involves exponentiation mod m, and decryption uses logarithms mod m. (This is called the discrete logarithm problem.) As we will see, one of the differences between the Caesar cipher and the RSA system, is that while it is easy to compute the inverse operation of the shift cipher it is not so for the exponential cipher.

In 1640, Pierre de Fermat, a French lawyer, sent a letter to a friend stating: "p divides $a^{p-1} – 1$ whenever p is prime and a is relatively prime to p." (Two positive integers are relatively prime if their greatest common factor is 1.) This statement (which Fermat stated without proof – yes this is the Fermat of the famous "Fermat's Last Theorem") has become known as Fermat's Little Theorem; it can be stated more modernly in terms of congruences.

Fermat's Little Theorem: Let p be a prime and a a positive integer relatively prime to p, then $a^{p-1} \equiv 1 \bmod p$.

In 1707 (300 years ago), Leonhard Euler was born. Euler was an incredible mathematician and made contributions to many fields. Of interest for us, is that he both provided a proof of Fermat's Little Theorem and generalized the theorem to any modulus. We state here a special case of Euler's Theorem.

Special Case of Euler's Theorem: Let p and q be distinct prime numbers and a a positive integer relatively prime to both p and q, then $a^{(p-1)(q-1)} \equiv 1 \bmod pq$.

In an exponential cipher, we are given the modular base m and the encryption exponent e and we encrypt message x as y where $y \equiv x^e \bmod m$. This encryption process is called modular exponentiation; it is a task that is relatively easy for a computer to perform. To decrypt, we need to solve the congruence $y \equiv x^e \bmod m$ for x (given y and m). If we know that $(x^e)^d \equiv x \bmod m$, then we can decrypt by computing $y^d \bmod m$ (since $y^d \equiv (x^e)^d \equiv x \bmod m$). This is where our old friends Euler and Fermat can help us out. We need one more fact from number theory that follows from the Euclidean Algorithm (due to Euclid circa 300 BCE).

Euclid's Theorem: If e and f are relatively prime positive integers, then there exist integers r and s so that $er + fs = 1$.

We note that r can be thought of as the inverse of $e \bmod f$ since, $er \equiv er + fs \equiv 1 \bmod f$. Back to the exponential cipher with modular base m and encryption exponent e. Let's first consider the case in which m is a prime p. For technical reasons (as we will see), we choose e to be relatively prime to $(p – 1)$ and assume the message x (thought of as a number) is smaller than p. Since e and $p–1$ are relatively prime, Euclid's Theorem tells us $er + (p – 1)s = 1$ for some r and s. Now, $x = x^1 = x^{er + (p-1)s} = x^{er} * x^{(p-1)s} = x^{er} * (x^{p-1})^s$. By Fermat's Little Theorem, $x^{p-1} \equiv 1 \bmod p$, and so $(x^{p-1})^s \equiv 1^s \equiv 1 \bmod p$. Thus, $x \equiv x^{er + (p-1)s} \equiv x^{er} \bmod p$. This says that r is the decryption exponent and $y^r \equiv x \bmod p$!!!!

The RSA system was created in 1971 by Rivest, Shamir, and Adleman, who at the time were researchers at MIT. It is an exponential cipher in which the modular base m is the product of two (large) primes, say p and q, and in which both the base m and the encryption exponent e are known to the public. This is an example of Public Key cryptography since anyone can use the key to encrypt messages. To find the decryption exponent, we need to find the inverse r of e modulo $(p – 1)(q – 1)$. (We assume here e is relatively prime to both $p – 1$ and $q – 1$ and $x < m$). By Euclid's Theorem there exist integers r, s so that $er + (p – 1)(q – 1)\, s = 1$. By Euler's Theorem, $x \equiv x^{er + (p-1)(q-1)s} \equiv x^{er} \bmod m$. Again, r is the decryption exponent. You may ask, why is this system secure since we can find the inverse r of e modulo $(p – 1)(q – 1)$ easily? While it is true that the inverse of e modulo $(p – 1)(q – 1)$ is easily found, we don't know what p and q are, only their product m. Thus, to find the decryption exponent, we first have to factor m into the product of primes, which is not an easy task.

Cryptography is a fascinating area that mixes ancient ideas with cutting edge technology. Most secure sites on the internet (which includes all e-commerce) use a form of the RSA cryptosystem. The next time you are using a web browser, you might investigate the type of encryption that is currently being used by your computer. For example, find the "certificate for encrypted connections" of a "trusted root certification authority" – this is sometimes found under internet options. If you view the details of the certificate, you can actually see the RSA Public Key that this authority uses. If your interest is more in cracking codes, you may wish to try some of the RSA challenges available at http://www.rsa.com/rsalabs/. This web site is also a good reference for further details on cryptography (see Crypto FAQ) currently in use. It will be interesting to see what directions cryptography takes in future years with advances in both technology and theoretical mathematics.

Wintersession Courses— January 2008

The Math Department plans to offer the following special-topics courses during the two-week period January 7-18, 2008. (Math 395, 1 credit each):

Topic	*Instructor*	*Days*
Cryptography	Jenny McNulty	TWR
Exploring Mathematics with Maple	Richard Lane	TWR
LaTeX Document Preparation	Karel Stroethoff	Daily

What's new in Graduate Education at UM?

by Jenny McNulty

The Department of Mathematical Sciences has a long history of training a wide variety of graduate students at both the Master's and PhD levels. Over the years some unique changes have been made in the program. While the department offers "traditional" MA and PhD degrees with concentrations in Algebra, Analysis, Applied Mathematics, Combinatorics & Optimization, Mathematics Education and Statistics, we also offer several "non-traditional" options. For example, in the early 70's an option of training teachers of 4-year colleges was developed in response to the shortage of professors trained to teach a broad spectrum of courses. This option is known as our "non-traditional" Option II PhD; it differs in many ways from the traditional Option I PhD, requiring more coursework, a teaching internship and an expository lecture. In 1998, the Master of Arts in Teaching (MAT) was changed to an MA in Mathematics with an Option in Mathematics Education, our Option II MA. This summer program, for middle and high school teachers, has recently been transformed so that each course includes an on-line component (most will still involve one week of face-to-face instruction). In 2006, a combined degree in Mathematics and Computer Science was developed, fueled by the need for computational scientists in academics and industry. Currently, many faculty and graduate students are part of the NSF-funded interdisciplinary Montana Ecology of Infectious Disease Program.

If you have ever thought about taking another mathematics course or getting an advanced degree, you might want to check out our offerings. Please feel free to e-mail or call me (contact information below) to find out more about our program. We would also like to hear from the graduates of our program; please let us know what you are doing.

Contact Information: http://www.math.umt.edu/graduate, *gradmath@umontana.edu,* or (406) 243-2473

Alumni News

After **Renee Fite** (BA 2005) earned her degree, she took a year off before joining Blue Cross Blue Shield of Montana in May 2006. She first worked as a Decision Support Analyst, before joining their Actuarial Department. Now she plans on taking the actuarial exams – we wish you success! On a more personal note, Renee writes: "My daughter, Kinzie is just finishing up kindergarten and doing amazingly well. My son, Karson is now three and in full throttle from dawn to dusk. My fiancé and I are getting married in July and are currently looking to buy a house. Helena is growing on all of us, and I think we will be here for a long time."

Tiffany Horsch (BA 2002, MA 2005) is in the final weeks of a five-month world trip with her fiancé, John Bulger. In total, they will have seen parts of 16 countries, including the areas of South East Asia, India, Nepal, and Europe. Currently in Europe, she has been working on minimal-cost train transportation.

Congratulations are due to **Dave Perkins** (PhD 2005), an associate professor at Houghton College, a liberal arts school in western New York: he just earned tenure! Because his department is small, he gets to teach a wide variety of classes. This fall he will be teaching a special topics course on the constants φ, π, *e* and *i* – that sounds like a very interesting class.

Beth Robinson (MA 2006) is teaching at Coastal Carolina Community College in Jacksonville, NC, where her fiancé Chad is stationed at Camp Lejeune. She writes: "I'm teaching a Survey of Math course and Calc II. I teach a night class on base, where most of my students are active duty Marines. I absolutely love my job – the people I work with are great – especially my boss. The first semester was crazy, but it's getting a little easier." Thanks for the news, Beth – please keep in touch.

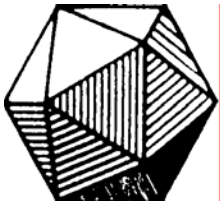
We heard from **Yong Zhao** (MA 1998, MS Computer Science 1999), who has been writing computer code for Microsoft Corporation for eight years as a software design engineer. He adds: "Now with a wife and two young kids, I am finding my spare time interest in a new kind of math problem, *Mathematics of Marriage* by John Gottman." I am impressed – when I had young kids, my spare time was not occupied reading scholarly math books!

*Please send in your news; we're always glad to hear from you, and **your classmates will enjoy reading about you** in this column.*

CLASS OF 2007

Name	*Degree*	*Hometown*
Jeffrey James Arends	BA	Missoula, MT
Pierre Robert Blouin	BA	
Anita L. Bohlert	BA	
Karin Christine Chimo	BA	
Natalie Ann Creamer	BA	Homer, AK
Beth Delaney Hegland	BA	Billings, MT
Vanessa Elizabeth Johnston	BA	Billings, MT
Mandy Rae McCaughey	BA	Belgrade, MT
Sarah Marie Nicol	BA	Oceanside, CA
William James Polk	BA	Browning, MT
Benjamin D. Smith	BA	
Hallie M. Torrey	BA	Salmon, ID
David Russell Winkler	BA	Plains, MT
Prof. Randall Skelton, Anthropology Dept.	BS *Combined CS/Math*	Missoula, MT

Name	*Degree*	*Advisor*
Rebecca Jane Burkala	MA	Nikolaus Vonessen
John Abraham Goldes	MA	John Bardsley
Nicholas Fitzgerald McClure	MA	Leonid Kalachev
Sharon Beth O'Hare	MA	Libby Knott
Seth Philip Braver	PhD	Greg St. George & Karel Stroethoff
Katharine Lynn Gray	PhD	Brian Steele



Math Club Corner

http://www.math.umt.edu/mathclub/

by Nikolaus Vonessen

The Math Club had an eventful spring semester. One of the highlights was our recent trip to the Missoula Fire Sciences Lab of the US Forest Service. UM Alumna **Patricia Andrews** (MA 1973, PhD in Forestry 2005), one of the research scientists, showed us around, arranged for several presentations about how advanced math is involved in the work done at the Fire Lab, and generally took great care of us. Thanks, Patricia!

Continuing a long tradition, we celebrated π-Day by, quite appropriately, selling pies generously donated by UM Food Services! And April brought our 8th Math Film Festival, which took place in the UC Theater. We had a great schedule – check it out at http://www.math.umt.edu/mathclub/filmsched07.pdf. Do watch *The Great Pi/e Debate* if you can – parts of it are really hilarious (if you cannot find it at a library, it is available from http://www.maa.org). And Hans Rosling's talk *Myths About the Developing World* contains amazing graphical representations of statistical data – you can watch it online at http://video.google.com. Unfortunately, this year we could not show any blockbuster Hollywood movie. Although we do not charge admission, we would have had to pay nearly $400 to show such a movie, and that does not seem to be an appropriate use of money for the Math Club (nor for the Math Department).

There is an update on **lockers** for undergraduate students! The department generously agreed to match the Math Club's $1,000 for the purchase of 24 half-high lockers. They will be located in the basement of the math building, in the hallway leading to the new elevator addition. If all goes well, they will be available at the beginning of the fall semester. And if demand exceeds supply (as we expect), we will hopefully be able to add more lockers next year.

The Math Club is always looking for outside speakers, especially alumnae and alumni, to talk about their professional lives, and how they use mathematics or statistics in their careers. Please let me know if you can help out! (406-243-6222 or nikolaus.vonessen@umontana.edu)

MATHEMATICAL SCIENCES
The University of Montana

The University of Montana

Department of Mathematical Sciences (MMAI01)
Mathematics Building
Missoula, MT 59812-0864
Phone: 406-243-5311
Website: www.umt.edu/math