POINTS AND ANGLES

Newsletter of the Metropolitan Mathematics Club of Chicago

NCTM Charter 1 Metropolitan Mathematics Club of Chicago 1913

Volume XXXIX June 2005 No. 9

Can You Keep a Secret? Cryptography and Inverse Functions

BY RICH RUKIN

An enormous amount of information is exchanged each day in the form of digital transmissions such as bank transactions, e-mail, internet orders, telephone calls and many other forms of communication. The need to prevent unwanted third parties from viewing or interfering with these exchanges has created a significant need for practical and reliable cryptography. Powerful and convenient new cryptographic methods have been developed to meet security needs. These new methods, however, have resulted in controversy regarding the proper balance between individual privacy rights and the government's ability to protect the public from criminals and terrorists. The mathematics involved in these cryptographic methods is well within the grasp of high school students: functions and their inverses, modular division, and prime factorization. Many students will find these topics motivational as they study modern cryptography because they are accessible and relevant.

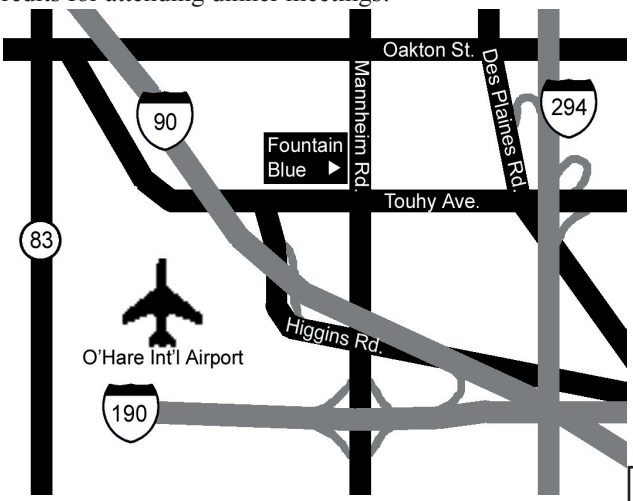
Our September speaker, Ray Barton, teaches at Olympus High School in Salt Lake City. he is also an instructor for TI's Teaching Teacher with Technology (T3) program. He is the author of several articles, curriculum, and books, and is a frequent speaker at institutes. We look forward to an outstanding presentation in September of 2005.

REMEMBER!! You can earn CPDU credits for attending dinner meetings!

Date: Friday, September 30, 2005
Time: 5:30 p.m. Doors Open
6:00 p.m. Social Hour
7:00 p.m. Dinner and Talk
Place: Fountain Blue Banquets & Convention Center
2300 Mannheim Rd.
Des Plaines, IL
(847) 298-3636
Cost: Members $31
Nonmembers $37

RESERVATION DEADLINE
Monday, September 26th, by noon, please!

TO RESERVE:
Call Lee Ann Swanson at
(630) 570-8421 or
email: lswanson@hinsdale86.org
Requests for special meals must be made in advance.



From Southbound I-294 & Eastbound I-290:
Exit at I-190 West to O'Hare; Exit onto North Mannheim Rd.; Take Mannheim Rd. North 2.25 miles.
From Northbound I-294:
Exit at West Touhy Ave.; Take Touhy Ave. to Mannheim Rd.; Turn right on Mannheim Rd.
Public Transit:
Take the CTA Blue Line to the Rosemont Bus Terminal; Take Pace Bus #223; Exit at Touhy Ave. & Lee Rd.; Walk East on Touhy to Mannheim Rd.

INSIDE...

Unfolding the Mathematical Mysteries Within a Sheet of Paper

BY BILL ROLOFF

On May 13 Edward Burger from Williams College proved to be a very entertaining and enjoyable speaker to close out the year. His topic was "Unfolding the Mathematical Mysteries within a Sheet of Paper." The basic premise was that simple things could lead to complex and fantastic discoveries.

He started out having us take a strip of paper and fold it in half as many times as we could. Most people could do it five or six times. When unfolded, there was a series of ridges and valleys and the challenge was to find if a pattern existed and if so, what it was. The sequence of ridges and valleys seemed to be very chaotic, and our challenge was to break the code and determine the structure of those ridges and valleys.

Like any good math teacher, he had us simplify the problem by folding it in half once and seeing that there is one valley. Fold that in half again, and when it was opened up, there were two valleys and a ridge: ˅˅^. Three folds made this sequence: ˅˅^˅˅^. Four folds made this sequence: ˅˅^˅˅^^˅˅^˅^^. The pattern? Look closely at each generation. The initial fold is always in the middle of each generation. Take any generation, put a valley at the end of it, then rotate the characters for that generation over the valley and you have the rest of the next generation. So we can repeat this as long as we want and know what the pattern will be for any number of folds. The fact that it is physically impossible to do more than seven folds on any sheet of paper does not matter as mathematics allows us to transcend what we can physically do.

Dr. Burger had us look at it another way. Put the initial ˅ in the center of your paper. Then on each side of it put a valley and a ridge: ˅˅^. Now spread out those symbols and starting before the first valley, begin with a valley, and between each symbol alternate ridges and valleys. The original generation: ˅ ˅ ^. Now alternate valleys and ridges (the original three symbols are underlined): ˅˅^˅˅^^

At this point we had two different ways of building the sequence of valleys and ridges. The problem was that to get any generation, you had to know the previous generation. So the question became how can we get any generation. If we let any valley equal a 1 and any ridge equal a 0, then the third generation can be written as 1101100. The fourth generation is 110110011100100.

He then showed us some simple Turing machines. The idea is that when a number is read, other numbers are added to the end of the sequence. As an example, if we read a 1, we could write at the end 212, read a 2, write 130, read a 3, write 0. So if we start out with a 1, then the sequence becomes: 1/212/130/212/130/212/0. At this point the machine is in a holding pattern, because it reads a 0, and doesn't know what to do. A second example he gave us was this:

Read	Write
0	01
1	32
2	42
3	31
4	41

So beginning with one, the sequence is: 1/32/31/42/31/32/41/42/3 1/32/31/42/41, etc. This machine will never enter a holding pattern because every output leads to an input, unlike the first example. Now change every odd number to a 1 and every even number to a 0, and the sequence becomes 1101100111001001110110001…, which is exactly the paper folding sequence of ridges and valleys. So now we have a method to generate the sequence of valleys and ridges for any number of folds we desire.

He paused to show a picture of a fractal and made it seem that there was no connection to what he had been doing prior to that. He had us fold our paper as before, but open it into a right angle, and continue with a second fold, opening it into right angles and so on. The sequence continued out infinitely led to that fractal he showed us.

Dr. Burger ended his talk by pointing out that we do not need to do complicated things to create something infinitely complicated. What he led us through with the paper folding was very simple, but it quickly became complicated when we tried to find the patterns.

His presentation was humorous, lively and extremely interesting. It was an excellent way to end the 2004-2005 year of talks.

Later this summer a book written by Edward Burger and Michael Starbird called "Coincidences, Chaos and All that Jazz" is coming out that explores this topic even deeper.

Board Report
Meeting of 26 May 2005

The Board of Directors held its fourth meeting of the 2004-2005 academic year on 26 May 2005. Gwen Zimmerman led the meeting until she passed the gavel to John Diehl, the new president.

The Board members expressed their gratitude for the excellent work done by the departing Board members, Bill Roloff and Sam Urbain. Bill ably chaired the Scholarship Committee in recent years, and Sam initiated significant changes during her role as president.

Mary Wiltjer reported a club membership of 504, of whom 10 are first year members, 48 are retired members, 5 are student members, and 2 are life members.

Ron Vavrinek submitted a treasurer's report indicating that the club is in good financial shape; the Board approved his report unanimously.

Carol Nenne presented a draft of revisions to the By-Laws. Board members suggested other changes that Carol will add to the document. During the next academic year the proposed revisions will be presented to the membership for conversation and a vote.

The next meeting of the Board is scheduled for 24 August 2005 at White Eagle Banquets and Restaurant at 6839 N. Milwaukee Ave. in Niles at 6:00 PM. Members of the club are welcome to attend any Board meeting, but please contact John Diehl at jdiehl@hinsdale.86.org before 15 August if you plan to attend this meeting. Because this is a dinner meeting, you would be expected to pay for your meal.

2005 Scholarship Winners

MMC Scholarship Recipient:

Emily Jacobson is currently taking Multivariable Calculus and Linear Algebra, and doing quite well. She has been a member of the ETHS math team for three years and has emerged as one of the leaders of the team. She intends to attend Grinnell next fall and become a high schoolmathematics teacher. She has done quite a bit of tutoring during her ETHS career and has distinguished herself as an able substitute teacher. When John Benson is gone for professional leave, Emily has been his stand in in BC Calculus. She has done an admirable job. She is also one of the students who makes excellent suggestions about improving instruction.

The Dennis Filliman Scholarship Recipients:

Katherine Evans from St. Charles North H.S.
She is a spirited and enthusiastic advocate of mathematics and has encouraged many other math students to become active on the math team. While tutoring with the National Honor Society program, she discovered a valuable life long truth; that by teaching and helping others you are continually learning yourself.

Stacy Pancratz from St. Charles North.
Stacy's key words are fun and enjoyment in the teaching and learning of mathematics. She doesn't think she will find a class in college for teaching how enjoyable learning can be. She thinks that is inherent in the teacher themselves, an infectious characteristic shown by their own enjoyment and love of mathematics and learning.

Whitney Rutherford from Evanston Township H. S.
She exhibits great enthusiasm and is in love with math. As our family members read the applications, they chuckled with her expressions and excitement with mathematics. She has also learned a valuable lesson from tutoring younger students, realizing the value of the problem solving process and a thoughtful approach not only the speed with which answers are given.

MMC Membership and Change of Address Form

Mail to: MMC
415 S. Ridgeland Ave. #2
Oak Park, IL 60302

Name _____

Address ☐ _____

_____

Phone _____

School _____

Address ☐ _____

_____

Phone _____

E-Mail _____

Check preferred mailing address above.

☐ Change of Address

Make check payable to MMC.

Please use a different form for each person.

Membership: ☐ New ☐ Renewal

Choose one:

☐ 1 year ($20) _____

☐ 2 year ($35) _____

☐ 3 year ($50) _____

☐ 1st year teacher ☐
☐ retired ☐ ($10) _____
☐ student ☐

Donations:

Scholarship Fund _____

Speaker Fund _____

Total amount of check: _____

NOTICES & REMINDERS

2005 – 2006 MMC Program of Speakers

September 30, 2005	Ray Barton
October 28, 2005	Gail Burrill
November 18, 2005	Beth Chance
December 9, 2005	Phil Mallinson
January 13, 2006	Terry Piercante
February 10, 2006	Kristen Clegg
March 10, 2006	John Jensen
May 5, 2006	Zal Usiskin

Experience the Winds of Change in Mathematics Education!
NCTM regional meeting in Chicago, Sept 2006

(Taking the place of the ICTM conference in 2006)

* Featuring a CAS (Computer Algebra Systems) Conference within a Conference
* Located at the Hyatt Regency McCormick Place on Lake Michi gan in the South Loop. Easy access to the Museum Campus, Navy Pier, Magnificent Mile, the NEW Millennium Park, and world-class shopping, theaters, and dining.
* Speaker proposal form available at http://www.nctm.org/meet ings/speak_reg.htm

*Deadline is July 11, 2005.

MMC Dinner Coupon

$5 off a dinner for New Attendees

— or —

$7 off a dinner for New Attendees who join MMC

_____ name

_____ date used

Valid only at the MMC Meetings on September 30, October 28, November 18, and December 9, 2005.
Limit one (1) coupon per person. Not for use with other discounts.

If you would like a notice or reminder to appear in POINTS AND ANGLES, please email the text you would like to appear to kristenclegg@comcast.net no later than the date of the MMC meeting preceding the issue in which you would like it to appear. All notices are subject to editing.

Your membership renewal date appears in the upper right corner of the label.

MAILING LABEL

METROPOLITAN MATHEMATICS CLUB OF CHICAGO
c/o MMC
415 S. Ridgeland Ave. #2
Oak Park, IL 60302

STAMP