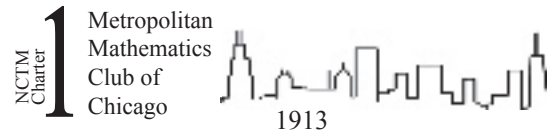


POINTS AND ANGLES

Newsletter of the Metropolitan
Mathematics Club of Chicago



Volume XL

October 2005

No. 2

The Changing Face of Mathematical Literacy: Statistics

By RICH RUKIN

Numbers, numbers everywhere – the world in which we live is becoming increasingly a society that quantifies everything from ranking and rating schools to reporting the chance of a risk for using a given medical treatment to the measurements necessary to orchestrate and plot the path of a space vehicle. Whether it is called numeracy, quantitative literacy, mathematical literacy or even statistics, the message is clear that to be a functional citizen in the world of today and tomorrow students have to be able to use mathematical skills in ways much different from those in the past. What is the relationship of this “new math” to the traditional curriculum? What effect will this have on the mathematics many of us hold dear? What role does statistical literacy play in this new era – and just how are statistics and mathematics related anyway? At our October meeting, Gail Burrill will look at some questions, hypothesize about some possible answers, and consider the implications for the mathematics curriculum we currently teach at the secondary and post-secondary levels.

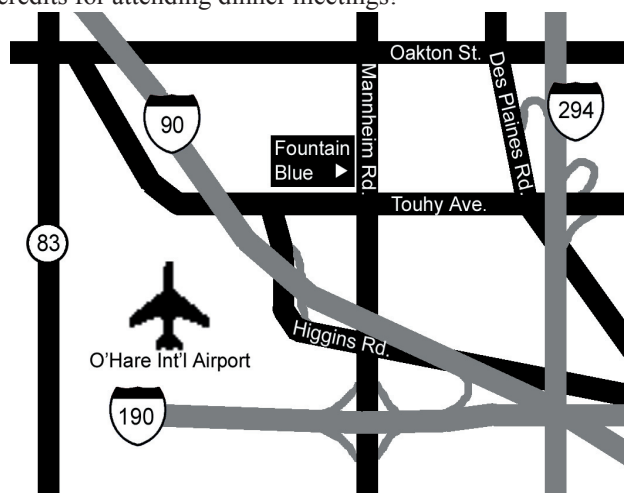
Gail Burrill was a secondary teacher and department chair in suburban Milwaukee, Wisconsin for over 25 years and spent time as an associate researcher at the University of Wisconsin-Madison. While on leave from the University of Wisconsin, she served as President of the National Council of Teachers of Mathematics (NCTM) and as Director of the Mathematical Sciences Education Board. As an instructor for Teachers Teaching with Technology, she does workshops around the country on using technology in the classroom. Her honors include the Presidential Award for Excellence in Teaching Mathematics and the Wisconsin Distinguished Educator Award. She was elected a fellow of the American Statistical Association and was awarded an honorary doctorate degree from Rose-Hulman Institute of Technology. She is currently the NCTM International Representative, directs the Secondary School Teachers Program for the Institute of Advanced Study’s Park City Mathematics Institute and serves on numerous boards and committees in an advisory capacity. Burrill has written many books and articles on teaching and learning statistics. She has spoken nationally and internationally on issues in teaching and learning mathematics. Her research interests are statistics education, the use of technology in teaching secondary mathematics, and issues related to teaching mathematics.

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

Date: Friday, October 28, 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, October 24th, by noon,
please!

To RESERVE:
Call Evanston Math Department at
(847) 424-7600 or
email: reservations@mmchicago.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...	
Points from the Interior	2
September Talk Summary	3
ByLaws	4
NCTM Regional Meeting	5

Can You Keep a Secret? Cryptography and Inverse Functions

BY RICH KICK

“Can You Keep A Secret?” It is likely that the “secrets” shared by Ray Barton at the MMC presentation September 30 will quickly spread through the Chicago area mathematics community. At this meeting, Ray revealed some of the mathematical details associated with a variety of encryption algorithms. His examples ranged from simple algorithms that can be shared with Algebra I students through sophisticated algorithms involving number theory that are used in secure computer systems today.

Ray motivated the need for computer encryption techniques by reminding us of the unpredictable and insecure routing of email messages on the internet, and the increasing frequency of identity theft through electronic means. He described the commonly used technique of associating letters of the alphabet “A” through “Z” with integers, called Unicode values (also known as ASCII values). The letter “A” is paired with the value 65, “B” is paired with 66, and so on until you reach “Z”, which is paired with 90. Ray described the “Caesar Cipher” that involves an arbitrary integer that is added to or subtracted from each integer assigned to the letters, wrapping any values that are mapped outside the 65 to 90 range. A video clip was played showing a scene from “A Christmas Story”, where a little boy (Ray speculated that it was John Diehl) uses his Little Orphan Annie decoder badge to decode a radio broadcast message. The badge consisted of two rotating discs which were attached at their centers. The first disc had the letters “A” through “Z” printed on its edge, and the second disc had the numbers 1 through 26 printed on its edge. By rotating the numerical disc by a given amount, secret codes in the form of a cipher could be decoded by transforming the code numbers into letters as indicated on the decoder badge.

A more sophisticated technique of encoding and decoding messages was made available to Algebra I students by using linear functions that were presented by Ray. His first example used the function $y = 3x + 11$ as an encoding function. This function encodes the letter “A”, numerically represented by 65, as the number $3 \cdot 65 + 11$, or 206. The letter “B” is encoded as 209, and the letter “Z” is encoded as $3 \cdot 90 + 11$, or 281. The decoding function is simply the inverse of the encoding function $y = (x - 11) / 3$. The decoding function transforms the value 206 into $(206 - 11) / 3$, or 65, as expected. Ray used the power of Computer Algebra Systems (CAS) to encode and decode complete lists of numbers rather than individually processing each value.

While this technique is easily accessible to your algebra students, it is fairly easy to “crack the code” by using frequency analysis (predicting which letters are associated with which numbers by examining the frequency of use of each code number). A relatively simple technique that helps to further obscure the original message is grouping. Ray used the word “MATHEMATICS” to illustrate the grouping technique. The Unicode representation of “MATHEMATICS” is 77 65 84 72 69 77 65 84 73 67 83. Rather than applying a linear function to the individual Unicode numbers, Ray suggested that the numbers can be paired to form four digit integers before applying the linear function. Because there are an odd number of letters in the word “MATHEMATICS”, ray added the space character to the end

of the word whose Unicode value is 32. The values created from the pairing process are 7765 8472 6977 6584 7367 8332. Applying the linear encoding function $y = 4x - 215$ to the newly created integers results in the coded message 30845 33673 27693 26121 29253 33113. Once again, the decoding function is the inverse of the encoding function $y = (x + 215) / 4$. Applying the decoding function to the encoded message, the original paired integer values are obtained.

Ray included an example of a quadratic function that could also be used as encoding functions provided the quadratic function is one-to-one over the set of integer message values. Ray’s example used the encoding function $y = 3x^2 + 6x + 15$, defined over the limited domain, and he provided the encoded message shown below.

186283212 32235864 191184879 144199479 210170712 138027279
146370687 208316679

We can be certain that Ray would like all of us and our students to take the decoded version of this message to heart.

The next form of encoding presented involved modular division in order to provide a mathematical method for scrambling the order of the message symbols. Using $y \equiv x^3 \pmod{p}$, where p is prime and $(p-1)$ is not divisible by 3, Ray encoded messages and decoded them using $y \equiv x(2p - 1)/3 \pmod{p}$.

Ray ended his presentation with a discussion of the RSA encryption technique that was invented by three computer scientists from MIT, each of whom began their post-high school education with a degree in mathematics. The combination of modular arithmetic and products of prime number helps to create a simple to use, yet very secure encryption technique. Public keys made from the product of very large prime numbers are exchanged and used with private keys that allow people exchanging messages to verify both the sender and content of messages. Ray noted that there is money to be made by mathematicians that can find ways to factor very large numbers that are the product of two prime numbers.

So, the secret is out. Encryption is an exciting, mathematically rich topic that can be shared with your students. Ray Barton’s ability to present interesting mathematics that will motivate both students and educators is also no longer a secret; at least not among MMC members.

POINTS AND ANGLES

Volume XL, Number 2, October 2005

Points and Angles, published nine times per school year, is the official publication of the Metropolitan Mathematics Club of Chicago. Founded in 1913, the Metropolitan Mathematics Club is the National Council of Teachers of Mathematics’ first affiliate.

The official club website: <http://www.mmccchicago.org/>

Correspondence may be directed to the editor:

Kristen Clegg
517 Wildflower Way
Streamwood, IL 60107
kristenclegg@comcast.net

ByLaws

At the August meeting, the MMC Board approved submitting the following By-Law revisions to the membership for a vote in January. The full text of the By-Laws, including the suggested revisions, can be found on the MMC website. Copies will also be available at MMC meetings through December. At those meetings, board members will be available from 6:00 – 6:30 to answer any questions about the suggested By-Law revisions.

Suggested Revision	Rationale
<p>Under ARTICLE VIII- Elections</p> <p>The nominations committee shall nominate for the position of elected Director any person who has been a member of the Club for at least two full years, and for the office of President-Elect any person who has been a member for at least three full years. <i>The Board of Directors shall approve the slate for officers and Board members prior to the announcement of the slate to the membership.</i></p> <p>Ballots shall be mailed to all current members. The election shall be conducted <i>Ballots may be returned by mail or in person</i> and the persons with a plurality of the votes shall be elected.</p>	<p>It is common practice in organizations for the Board of Directors and/or membership to approve either the nominating committee or the slate. Due to the time constraints on appointing a membership committee, it would be more appropriate for the board to approve the slate. This is partially a courtesy to the Board, but also allows for additional input on the slate.</p> <p>This change will allow for ballots to be brought to a meeting. Although this has been the practice, the current wording does not allow for ballot return other than by mail.</p>
<p>Under ARTICLE IX- Officers</p> <p>The officers of the Club shall be President, President-Elect, Past-President, Secretary, and Treasurer. However, other officers, such as <i>membership chair</i>, historian, editor or committee chairpersons, may be established as the Board of Directors deems necessary to carry out the functions of the Club <i>or as required by NCTM for affiliate groups. Officers shall meet the requirements established by NCTM for affiliate groups.</i></p> <p>The Secretary shall see that keep membership records are kept of all members and their addresses and of <i>shall keep records of all</i> proceedings of the Club and the Board of Directors.</p> <p>The Treasurer shall receive all dues and other income, pay all bills as directed by the Board, see that all income is deposited and that all bills are paid, and <i>shall keep records of all financial transactions.</i></p>	<p>The position of membership chair is vital to the organization, as it is important for the Board to ensure that accurate membership records are kept. As an affiliate member organization of NCTM, MMC is also responsible for making sure that we meet all of the requirements to maintain our status as an affiliate.</p> <p>While it is important that accurate records are kept, income is deposited, and bills are paid, it is not always possible that the Secretary and/or Treasurer do these tasks personally.</p>
<p>ARTICLE XI- Finances and Contracts</p> <p>All funds shall be deposited by the Treasurer in a depository depositories which is are insured by the Federal Government. The title of the accounts shall be the same as <i>include</i> the name of the Club. Disposition of funds shall be approved by the Board of Directors. The Board of Directors shall approve those persons authorized as signatories on Club accounts. The Treasurer Those persons authorized as signatories on accounts shall be bonded to an amount equal to the anticipated funds for the fiscal year.</p> <p><i>The Board of Directors and/or Executive Committee has the authority to enter into contracts on behalf of the organization.</i></p>	<p>Current wording requires that all funds be held in a single account. This change would allow greater flexibility. It is also not always reasonable to expect that the Board approve all individual expenditures, as currently required. It also requires the Board to approve those who are authorized to sign checks and enter into contracts. There is no current designation as to who may act on behalf of the organization in signing contracts.</p>
<p>ARTICLE XV- Amendments to By-Laws</p> <p>These By-Laws may be amended by a majority of the members voting at any time, provided notice of the proposed amendment shall have been sent by mail to every member, and during one meeting of members sufficient time has been provided for a discussion of the proposed amendment. The vote shall be conducted by mail. Ballots shall be mailed to all current members. Ballots may be returned by mail or in person.</p>	<p>Similar to the change regarding elections, this would allow for voting either by returning the ballot by mail, or bringing it in person to a meeting.</p>

MMC Problems for October
2.1 Arithmetic

This year solutions to the problems will be provided. However, I would like for readers to send in their solutions, for (a) they might provide insights that I do not know, and (b) I might not be able to solve the problems and need assistance. The best solution (my judgment) will be given during future issues of Points and Angles.

The topic this month is arithmetical simplifications. The objective is to write the answer in the simplest form. Radicals within radicals should be changed if possible to radicals. No radicals in the denominator.

- (1) $\sqrt{4\sqrt{2} + 2\sqrt{6}}$ (2) $\sqrt[3]{9\sqrt{3} - 11\sqrt{2}}$
- (3) $\frac{2 + \sqrt{6}}{2\sqrt{2} + 2\sqrt{3} - \sqrt{6} - 2}$ (4) $\sqrt[3]{5\sqrt{2} + 7} - \sqrt[3]{5\sqrt{2} - 7}$
- (5) $\frac{\sqrt{5 - 2\sqrt{6}}(5 + 2\sqrt{6})(49 - 20\sqrt{6})}{\sqrt{27} - 3\sqrt{18} + 3\sqrt{12} - \sqrt{6}}$

Michael Keyton
IMSA
keyton@imsa.edu

NCTM Central Regional Conference
Experience the Winds of Change in Mathematics Education!
Chicago, Illinois
September 20-September 22, 2006
(Wednesday, Thursday, Friday)

- Featuring a CAS (Computer Algebra Systems) Strand
- Located at the Hyatt Regency McCormick Place
- This will take the place of the 2006 ICTM Conference



MMC Membership and Change of Address Form

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

Make check payable to MMC.

Please use a different form for each person.

Name _____

Address _____

Phone _____

School _____

Address _____

Phone _____

E-Mail _____

Check preferred mailing address above.

Change of Address

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

MEECAS Upcoming Meetings
 Saturdays
 9 a.m. to 12 noon
 Continental Breakfast provided

- * October 29, 2005 "CAS Camp for CAS Novices"
 Glenbrook South High School
 4000 W. Lake Avenue, Glenview, IL 60026
- * December 3, 2005 "Proof and CAS"
 Glenbrook South High School
 4000 W. Lake Avenue, Glenview, IL 60026

For questions, more information, or to RSVP,
 contact Michelle Kolet at 847-755-4600 or mkolet@d211.org

MEECAS is a consortium for mathematics educators who are exploring, or are interested in exploring, the use of computer algebra systems (CAS) in mathematics classrooms.

<http://gbs.glenbrook.k12.il.us/Academics/gbsmat/meecas/home.htm>

GET INVOLVED IN MMC!

We will be forming an Elections Committee to determine the slate for MMC Board positions. If interested, please notify Gwen Zimmermann (gzimmerm@hinsdale86.org or 630.570.8420). The Committee's first meeting will take place at Fountain Blue immediately preceding the October

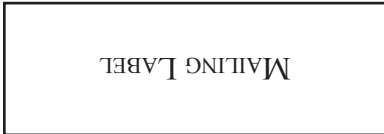
WE NEED YOU! VOLUNTEER!!

Volunteer to help at the NCTM Regional Meeting in Chicago September 20-22, 2006

It takes great people like you to make the conference a success! Contact either Gwen Zimmermann (gzimmerm@hinsdale86.org) or Laura DiMarco (ldimarco@hinsdale86.org) for more information. (or phone 630.570.8421)

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.



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

