Letters to the Editor

Cryptography for Poets

Reading the translated article by Berold and Ye of Tianxin's "Mathematicians and poets", *Notices,* April 2011, 590–596, reminds one of the course often jokingly referred to as Math for Poets.

My premise is this: for a student to succeed in a university he or she should have some reasonable ability either in mathematics or language, coaches notwithstanding.

The first nine weeks of my course covered the traditional topics: logic, algebra, geometry, number theory, graph theory, statistics, and probability. Also student evaluations occurred here. The last week was devoted to cryptography. The final consisted of closed-book multiple choice over the entire course as well as an open-book hour exam about cryptography. Usually five out of a class of thirty wrote a perfect cryptographic exam, and knew it!

The majority of students did not do the last problem using translation rather than substitution cipher. They were told to merely comment about reaching it without solving it, for four out of ten points. (I prefer such admissions to lengthy work which both the student and I know is utter nonsense.)

The first half of this exam involved deciphering an encrypted message with word breaks; simple substitution; statistics of letters of the encrypted message; and in the clear, at least three appearances of "the", two of "and", and more "a" than "I". Then the keyword which constructed the cipher alphabet is found. Here, after duplicates are removed from the keyword, it is the first line of a matrix, then the balance of the alphabet in order fills this partial rectangle. Then column by column in order delivers the cipher alphabet. (Correct completion = sixty points.)

For fifteen points, encipher a short message using a given keyword for a polyalphabetic cipher. A couple of examples for solution involved mod 26 arithmetic while the rest used an included copy of the Vigenère Tableau.

For fifteen points decode a short message written in my private code: 0:D,O,Q; 1:I,J,T; 2:S,Z; 3:E,F; 4:X,Y; 5:U,V,W; 6:C,G; 7:L,M,N, 8:B,P,R; 9:A,H,K. In messages there is usually only one correct letter; however, 8983 yields several words.

In a semester course with more time one may study deciphering polyalphabet ciphers by a computer program, deciphering without word breaks, deciphering when clear in a foreign language. This I prefer to showing off how factoring creates trap-door ciphers. This last is very appropriate in a number theory course.

—Raymond Killgrove
Retired
2041 W. Vista Way, #245
Vista, CA 92083

(Received April 7, 2011)

Oswald Spengler's Philosophy

The discussion of mathematics and poetry in Cai Tianxin's essay (*Notices,* April 2011) is interesting and comports with the kinship between mathematicians and artists that Oswald Spengler notes in his magnum opus *Der Untergang des Abendlandes* (1918, 1922), a work which puts forth a philosophy of history that predates similar work by Arnold Toynbee—Toynbee is justly remembered as an eminent philosopher of history, while Spengler is unjustly forgotten. Spengler's theory, incidentally, provides an explanation for the difference in taste that he asserts exists between modern (Faustian) mathematics and classical (Apollonian) mathematics.

—Jim Tseng
Ohio State University
tseng@math.ohio-state.edu

(Received April 25, 2011)

A Call for Collaboration

I read the entire March issue's series on mathematics education with great appreciation, but also with bafflement that I live in such a different world. I hope someone can help me make sense of my world, and perhaps offer advice as to how to change it.

From 1988 to 1995 I won fourteen grants for helping elementary school teachers mathematically, reported in my February 2005 *Notices* article, "Racial equity requires teaching elementary school teachers more mathematics", at http://www.ams.org/notices/200502/fea-kenschaft.pdf. A combination of political events in New Jersey conspired to stop this very satisfying program that was having a measurable and immeasurable impact on nine northern New Jersey school districts, including those of Newark, Paterson, and Passaic.

Since then an informant has told me of fifth graders in a different nearby nice suburban district being drilled in adding fractions by adding across the numerators and then across the denominators.

After I realized how bad elementary teaching of mathematics is affecting Americans' entire lives, I tried to get at least one course for elementary school teachers relevant to the mathematics they are expected to teach introduced at the university where I was a full professor of mathematics, so I could reach the teachers before they damage or possibly destroy children's mathematical ability. The math educators encouraged and helped me, and the mathematicians regarded the effort with indulgent bemusement.

Fifteen years of struggle yielded no success. The education leadership was adamant that no such course should be offered.

…My efforts to get a requirement in New Jersey for pre-service elementary school teachers to take at least one appropriate mathematics course also seem to lead nowhere. I have been told that there are a dozen New Jersey deans of education adamantly opposed to such a proposal. An email list of over one hundred concerned New Jersey residents seems to have little, if any, access to the powers who decide the requirements for teacher certification.

How do mathematicians and mathematics educators elsewhere

obtain the privilege of teaching such courses?

How do they get the needed state requirements passed?

How do they gain access to the power brokers?

How do we focus the attention of national leaders on the importance of teacher knowledge preparation?

Almost all teachers I have known are educable and eager. But nobody can teach what we don't know. Testing, threats, and demeaning the profession will not undo that basic fact.

—Pat Kenschaft
Montclair State University
kenschaft@pegasus.montclair.edu

(Received April 11, 2011)

The Impact of Mathematics

Two articles caught my attention in the May issue of *Notices*—"Mathematical intimidation" and the review of the book "The Quants"—for their shared cautionary tale about the potential misuse of mathematics. As a Ph.D. in differential geometry and a member of Congress, I often see firsthand the impact that mathematics has in shaping our country's policies, both for better and for worse.

I deeply enjoyed my studies and professional applications of mathematics and understand how easy it is to be seduced by the beauty of our own craft. We must remember, however, that applications of mathematics have a powerful impact on the world around us. I urge all mathematicians to take note of how our tools—when misused—can have a devastating impact on real peoples' lives. With power and stature comes great responsibility.

—Jerry McNerney
Member of Congress
(California's 11th Congressional District)

(Received May 14, 2011)

Correction

Due to a program error while formatting the reference list for the article "How a medieval troubadour became a mathematical figure", by Michael P. Saclolo (May 2010 *Notices,* http://www.ams.org/notices/201105/rtx110500682p.pdf), four of the references were dropped from the list. The complete reference list is printed below.

—Sandy Frost

References

1. Emil Artin, *Collected Papers*, Addison-Wesley, 1965.
2. Jean Boutière, *Biographies des Troubadours*, Nizet, 1964.
3. Monique Bringer, Sur un problème de R. Queneau, *Mathèmatiques et Sciences Humaines* **27** (1969), 13–20.
4. F. J. A. Davidson, The origin of the sestina, *Modern Language Notes* **25** (1910), no. 1, 18–20.
5. Jean-Guillaume Dumas, Caractérisation des quenines et leur représentation spirale, *Mathématiques et Sciences Humaines* **184** (2008), 9–23.
6. Frederick Goldin, *Lyrics of the Troubadours and Trouvères*, Anchor Books, 1973.
7. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 2008.
8. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1994.
9. Saunders Mac Lane and Garrett Birkhoff, *Algebra*, AMS Chelsea, 1999.
10. Warren F. Motte (ed.), *Oulipo, a Primer of Potential Literature*, University of Nebraska Press, 1986.
11. M. Ram Murty, Artin's conjecture for primitive roots, *Mathematical Intelligencer* **10** (1988), no. 4, 59–67.
12. Georges Pérec, *La Disparition*, Gallimard, 1989.
13. Raymond Queneau, *Cent Mille Milliard de Poèmes*, Gallimard, 1961.
14. _____ , Note complémentaire sur la sextine, *Subsidia Pataphysica* **1** (1963), 79–80.
15. _____, *Batôns, Chiffres et Lettres*, Gallimard, 1965.
16. _____ , *Letters, Numbers, Forms: Essays 1928–1970*, University of Illinois Press, 2007.
17. Jacques Roubaud, Un problème combinatoire posé par la poésie lyrique des troubadours, *Mathématiques et Sciences Humaines* **27** (1969), 5–12.
18. _____ , N-ine autrement dit quenine (encore), *La Bibliothèque Oulipienne*, numéro 66, 1993.
19. Peter Stevenhagen, The correction factor in Artin's primitive root conjecture, *Journal de Théorie des Nombres de Bordeaux* **15** (2003), no. 1, 383–391.
20. A. Tavera, Arnaut Daniel et la spirale, *Subsidia Pataphysica* **1** (1963), 73–78.
21. James J. Wilhelm, *The Poetry of Arnaut Daniel*, Garland Publishing, 1981.