Advertise!*

Richard EHRENBORG

These days it is not enough to teach interesting courses. We also have to attract students to take our courses. Even more so, we have to attract and retain students in the sciences and in mathematics.

I have been teaching a junior level course called *Applicable Algebra* at the University of Kentucky. The course begins with elementary number theory in order to cover topics including RSA, primality testing and factoring large integers. The course then continues to discuss polynomials in order to introduce finite fields and turn the attention to error correcting codes, such as BCH codes. The course focus is on the applications and how the mathematics supports them.

The course aims to make mathematics appealing to the students. The goal is twofold: First, to encourage students to major in mathematics. Second, to attract students from other majors, such as computer science, to double major in mathematics.

How does one get the word out to potential students? Advertise! Inspired by the NSA advertising campaign to hire mathematicians, I made a collection of posters. I handed them out to interested students and posted them around campus.

Here are the posters and some short explanations and references.

Shuffle a deck of cards eight times. Do it perfectly each time. Then you are back to where you started. Nice card trick. Why does it work? If you are curious, take CS 340/Math 340 Spring 2006.

The perfect shuffles mentioned here are out-shuffles, that is, the top card stays on the top. For a deck with an even number n cards, label the positions 0 through $n-1$. Now a perfect out-shuffle brings the card in position x to position $2x \bmod n-1$. So what we need to verify is that 2^8 is congruent to 1 mod 51.

How do pineapples relate to the greatest common divisor? If you are curious...

Two consecutive Fibonacci numbers are the worst case scenario for Euclid's algorithm. Consecutive Fibonacci numbers also appear when counting spirals on pineapples and pine cones.

*FOCUS **26** (2006) August/September issue, number 6, pages 28–29.

What do
cicadas
know
about
prime
numbers?

Assume that the cicadas appear every n years. A predator that appears every k years, where k is a divisor of n, can happily eat away. Hence the fewer divisors the period n has, the more likely the cicada population will survive. Prime numbers provide the minimum. See the article by Meredith Greer in the February 2006 issue of FOCUS.

Fermat
thought
4294967297
was
prime.
He
was
wrong.

The number in question is $2^{2^5}+1$. Euler showed that 641 is a prime factor. There is a nice way to do this using that $641 = 2^7 \cdot 5 + 1 = 5^4 + 2^4$.

How
did
the
twin primes
824633702441
and
824633702443
improve
your
Pentium chip?

In the computation of Brun's constant, Tom Nicely discovered that the Pentium chip could not divide. See the nice article by Barry Cipra in *What is Happening in the Mathematical Sciences 1995–1996,* pages 38–47.

Why
is
the inequality
$|\ln(\mathrm{lcm}(1,2,...,n)) - n| \leq 2\sqrt{n}(\ln(n))^2$
for $n \geq 100$
worth
$1,000,000?

This inequality is equivalent to the Riemann zeta hypothesis, something that we all should care about.

How are
an old Greek,
a French lawyer and
a Swiss man
involved in
you sending
your credit card number
over
the internet?

Fermat's little theorem and Euler's theorem are the basis of RSA, the first public key crypto system. Euclid also belongs since his algorithm allows us to find the decoding exponent from the encoding exponent and the secret factorization. I recommend the original article of R. L. Rivest, A. Shamir and L. Adelman, A method for obtaining digital signatures and public-key cryptosystems *Communications of the Association for Computing Machinery,* **21** (1978), no. 2, 120–126.

Your friend(?)
claims that
34034065601122854197959819122215174693
is a prime number.
How do you
prove her/him
wrong?

Primality testing is important when you need primes for your own RSA crypto system.

What is the probability
that two people
in this room
have the same
birthday?
What does this
have to do
with
factoring
LARGE numbers?

For a year with P days and about $\sqrt{\ln(4) \cdot P}$ persons, the probability is about fifty-fifty. The Pollard Rho factoring method uses this fact to run in $O(P^{1/2}) \leq O(N^{1/4})$ time to factor N, where P is the smallest prime factor of N.

How come
your cat
can scratch
your favorite cd
and
still
it
sounds
great?

And:

How do you send
pictures
from Mars
over
noisy channels
and still
get
a clear picture
to give
to CNN?

The answer to both of these questions is error correcting codes. It is amazing that your cd-player can lose 2.5mm of track and you will not hear the difference. Also note that NASA put high resolution cameras on the two Mars rovers in order to make both scientific observations and good PR for themselves.

The
NEW
engineering
MATH:
error correcting codes
and
public key cryptography.

These topics are what we mathematicians should be teaching our computer science and engineering students.

There are three people.
On each person we put either
a blue or red hat.
Each person can see
the color of the hats of the other two.
At the same time they have to guess
the color of their own hats.
Each of them says red, blue or pass.
If one of them is wrong, they lose.
If at least one of them is right they win
$1,000,000.
What is their best strategy?

This hat problem is related to Hamming codes, the first known class of error correcting codes. See Mira Bernstein's article in the November 2001 issue of FOCUS or the article by Joe Buhler, "Hat Tricks," in the Fall 2002 issue of *The Mathematical Intelligencer.*

Fun and interesting advertising is one way to attract more students to our classes. Finally, recall what Oscar Wilde wrote in *The Portrait of Dorian Gray*: There is only one thing in the world worse than being talked about, and that is not being talked about.

R. Ehrenborg, Department of Mathematics, University of Kentucky, Lexington, KY 40506, jrge@ms.uky.edu