CURRICULUM INSPIRATIONS: www.maa.org/ci

Innovative Online Courses: www.gdaymath.com
Tanton Tidbits: www.jamestanton.com

WHAT COOL MATH!

CURIOUS MATHEMATICS FOR FUN AND JOY

August 2016

THIS MONTH'S PUZZLER:
I have a dozen warring, but mathematics-loving, relatives who never get together. And I have a fortune amassed and stored in my safe. I am willing to give away the three-digit code to the safe and thus all 12 gold bars in it, one per relative, if all will come together, finally, for once, to meet and cooperate on a task. Actually, I will settle for just ten or eleven coming together, each taking a bar, and using the remaining bars to cover the costs of a blow-out party.

How could I send each of my relatives a clue to the safe number so that only if some subset of ten of them come together they will have, as a group, enough information to deduce that number?

ZERO KNOWLEDGE

It often happens in mathematics that one can prove certain numbers or objects exist, but be unable to give the slightest clue as to what they actually are or how you might go about finding them.

Two classic examples immediately come to my mind.

There exist two non-bald people in New York City each with exactly the same number of hairs on their heads.

Proof: According to Google, the average number of hairs on a human head is about 100,000. So I can safely assume that no New Yorker has a million or more head hairs. But there are more than a million non-bald New Yorkers and they can't all have a different number of hairs. Thus there must exist at least two New Yorkers with exactly the same head hair count.

Challenge: Find two New Yorkers with the same number of hairs on their heads.

It is possible to raise an irrational number to an irrational power to have a rational answer result.

Proof: $\sqrt{2}$ is an irrational number. Now consider $\left(\sqrt{2}\right)^{\sqrt{2}}$. I know nothing about this number.

But if $\left(\sqrt{2}\right)^{\sqrt{2}}$ happens to be rational, then we have found an example of what we seek. If, on the hand, $\left(\sqrt{2}\right)^{\sqrt{2}}$ is an irrational number, then $\left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}}$ is an example of what we seek since $\left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\times\sqrt{2}} = \left(\sqrt{2}\right)^{2} = 2$, a rational value.

So either $\sqrt{2}^{\sqrt{2}}$ or $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$ is an example of an irrational number raised to an irrational power with a rational answer. I just don't know which one is it.

Challenge: Is there a way to figure out which is it? (The *Gelfond-Schneider Theorem* has something to say about this.)

Another "zero-knowledge" challenge might come from mathematical coyness. Suppose I want to convince you that I know the solution to a problem, but I don't want to give you any clue as to what the solution is. (These sorts of matters often arise in the study of cryptography. The field of "zero-knowledge protocols" was established in 1985 by S. Goldwasser, S. Micali, and C. Rackoff.)

Such actions can often be done. Here's a simple example.

In the game of "Where's Waldo?" one is presented with a very complicated picture of a crowd scene, with hundreds of different figures drawn throughout the page. Your job is to find the one figure – Waldo  – wearing a distinctive red and white striped shirt and hat.

[By the way, outside of the U.S. Waldo is known as "Wally".]

Here's a picture.

I know where Waldo is in this picture. And I could prove to you that I know and not give you a hint as to where he is as I prove to you I have this knowledge. Here's how.

I'll take a big sheet of paper and cut a small hole in it, just the size of Waldo. Then you can watch me take a copy of the picture,

slide it under the sheet and arrange it so that Waldo's image appears through the hole. You can verify that I have indeed shown you Waldo, but you can't see where on this picture that image lies. Voila!

COIN FLIPPING

The zero-knowledge proofs and protocols developed the last few decades generally allow for a certain, negligibly small, level of uncertainty.

Suppose I want to convince you I can predict the tosses of a coin. To do this I could, for example, write on a piece of paper - and thus commit to - a sequence of ten Hs and Ts. I place that sheet in front of you and then have you toss a coin ten times in a row. As you observe the results as you toss you will then be thoroughly gob-smacked by my coin-predicting abilities.

Of course, with ten tosses of a coin there is a $\frac{1}{1024} \approx 0.1\%$ chance I could have just guessed correctly. If you think this was the result of luck, then we could do the experiment again (there is a $\frac{1}{2^{20}} \approx 0.001\%$ I'd, by chance, be right 20 times in a row) and again ($\frac{1}{2^{30}} \approx 0.00001\%$) and again, as many times as you want, until the odds of me being right just by guessing are so extraordinarily low that you would indeed be convinced I am a coin reader.

A TERRIBLE SCAM (which I in no way endorse, but am going to write about anyway):

Suppose you have some lousy investment scheme and you want to con some people into joining it. Here's what you can do.

At 4:05 p.m. this afternoon, email 3200 of your closest "friends" today's value of the Dow Jones Index along with a statement about the value of the Index at close end of day tomorrow. Tell half your friends that it will be higher, the other half that it will be lower.

Tomorrow at 4:05 p.m., of the 1600 friends for whom your "prediction" happened to be correct, do this again; telling half of them that the next day the stock market will close higher, the other half, lower.

Keep doing this, say five times in a row, halving the number of folk you email each evening, emailing only those whose predictions happened to be right.

You now have 100 people who have received five emails in a row from you, apparently predicting the close of the stock correctly each and every time. Now ask them to join your investment scheme.

Often zero-knowledge protocols rely on computing-tasks that are infeasible to conduct. For instance, computers are very swift at computing the product of two large prime numbers. But if given a number understood to be a product of two large primes, the computing time needed to factor the number to find those two primes typically runs into the hundreds or thousands of years. (Most of our modern-day computer encryption methods rely on this fact.)

Consider a coin-tossing problem Alberto and Beatrice face.

Long-Distance Coin Tossing: *Alberto lives on the east coast of the U.S., Beatrice on the west coast. During a telephone conversation they decide they need to toss a coin in order to decide who is going to follow through on a fun and exciting task. Alberto says he'll toss a coin and if it comes up heads, he wins, if it comes up tails, Beatrice wins.*

Beatrice, of course, objects to this plan, as she will not be able to see the coin toss and verify that Alberto is telling the truth about the result. So Beatrice offers this plan: She will first write on a piece of paper either "heads" or "tails" and commit to the choice. Then Alberto will toss the coin and announce the result. If Beatrice's prediction matches the toss, she wins, if it does not, Alberto wins. Now Alberto has no incentive to lie about the coin toss, but will object to this process as he has no way of telling if Beatrice lies about the prediction she made.

So how could Alberto and Beatrice possibly conduct the action of a long-distance coin toss and feel confident that the other person was not lying at any stage of the process?

Answer: Forget the coin and try this instead.

Alberto thinks of two large prime numbers p and q, one that is 1 more than a multiple of four and the other 3 more than a multiple of four. He then computes $N = pq$, their product, and shares that product with Beatrice over the phone. Alberto is thus committed to that number.

Because it is computationally infeasible to factor N, Beatrice cannot tell what the two primes are. Beatrice will then say out loud either the statement "The smaller of the two primes is the one that is 1 more than a multiple of four" or the statement ""The larger of the two primes is the one that is 1 more than a multiple of four." She commits to that statement.

Alberto now reveals the two primes p and q and both can verify that they are indeed primes (this is computationally feasible), have the required remainder properties, that their product is N, and whether or not Beatrice's guess was right or wrong to win or lose this virtual coin toss.

COIN TOSSES AND PERSONAL INFORMATION

The mathematics department at a college is wondering just how rampant cheating on math exams is across campus. What percentage of students cheat?

They would like to conduct a survey asking students "Have you cheated on a math exam this past year?" but know full well no one is going to honestly answer YES when faced with this question and nothing more. So how could the department garner the percentage of students that cheat by still asking this question, but assuring the students that in no way a "YES, I have cheated" answer can possibly be held as evidence against them for cheating?

One sets up the following protocol.

Have student toss a coin. Those that toss heads are to answer the question honestly. Those that toss tails are to flip a coin again and answer YES to the question if this second toss lands heads and NO if it lands tails.

Even if Cecile's name is mistakenly released with her answer to the question, one cannot hold her YES answer to cheating against her: she could well have been one of the 25% of the people instructed to answer YES because of the second toss of a coin. Similarly, Dilbert might well be an

incessant cheater, but could be one of the 25% of the people instructed to answer NO by the random process. His cheating habits will remain unnoticed.

So does this mean that survey results are of no use to the Mathematics Department?

Imagine there are 2000 students on campus and the department received 620 answers of YES and 1380 answers of NO.

Of those 2000 students, they expect close to a 1000 students answered the question honestly and 1000 to answer with the flip of a coin. In that second group, about 500 students answered YES and about 500 NO. Thus the department concludes that, among the 1000 students who answered honestly, about 120 answered YES, 880 answered NO. The percentage of students that have cheated is about 12%. (And yet, even if names are released with the survey results, the department still cannot identify a single cheater.)

Question: Are techniques like these used by internet data gatherers? Do they introduce a random element into a proportion of answers logged? Is our personal information actually private after all?

THE OPENING PUZZLER

To finish off, let's solve the opening puzzler.

Here we have a situation of wanting large groups to have full knowledge of some piece of content, but all smaller groups to have zero knowledge. It is surprising that we can create such knowledge structure.

Here's one way to do this for our example due to Israeli mathematician Adi Shamir.

Shamir's Secret Sharing: It is well known that two points in the plane determine a unique line, three points a unique quadratic, and so on. In general, N points in the plane determine a unique polynomial of degree $N-1$ (provided no two of those points have the same x-coordinate).

So what I can do is write down some degree nine polynomial P with y-intercept the code number to my safe and then send each relative a letter explaining what I have done and include, to the ith relative, the value of $P(i)$. (Here i ranges from 1 to 12, though any set of twelve distinct non-zero values for i will do.) Only when ten or more relatives are together will they have ten data points to determine the polynomial, and hence its y-intercept.

RESEARCH CORNER

The field of zero-knowledge proofs and zero-knowledge protocols is, to this day, very active. Learn more about this work on the internet and join in on the research action!

Also, learn about privacy protocols on data gathering. (Is our data safe?)

tanton.math@gmail.com