September 1990 Issue 53

NOESIS

THE MONTHLY JOURNAL OF THE ONE-IN-A-MILLION SOCIETY

Contents

Publisher & Editor

Ronald K. Hoeflin
P. O. Box 7430
New York, NY 10116

Editor's Page

Membership: As of October 29, 1990, we have 14 members and 12 non-member subscribers. The members are:

(1) Anthony J. Bruni (Houston, Texas)
(2) Chris Cole (Newport Beach, California)
(3) Eric Erlandson (Lincoln, Nebraska)
(4) Kjeld Hvatum (Sharon, Massachusetts)
(5) James Hajicek (Burlington, Wisconsin)
(6) Dean Inada (El Toro, California)
(7) Christopher M. Langan (Speonk, New York)
(8) Richard May (Buffalo, New York)
(9) Richard Sterman (Encino, California)
(10) Cedric Stratton (Savannah, Georgia)
(11) Marilyn vos Savant (New York, New York)
(12) Jeff Ward (San Diego, California)
(13) Ray Wise (Harwinton, Connecticut)
(14) Jeff Wright (Holmen, Wisconsin)

The seven members who have not renewed yet are as follows:

(1) Geraldine Brady (Chicago, Illinois)
(2) H. W. "Bill" Corley (Arlington, Texas)
(3) George W. Dicks, Jr. (New Haven, Indiana)
(4) Eric Hart (Miller Place, New York)
(5) Johann Oldhoff (Solna, Sweden)
(6) Keith Raniere (Clifton Park, New York)
(7) Karl G. Wikman (Askloster, Sweden)

The twelve subscribers are as follows:

(1) Arval Bohn (Austin, Texas)
(2) Henry P. Donnon (Moorestown, New Jersey)
(3) Marshall Fox (Atlanta, Georgia)
(4) Fred Galvin (Lawrence, Kansas)
(5) LeRoy C. Kottke (Ann Arbor, Michigan)
(6) Celia Manolesco (Santa Monica, California)
(7) Rick L. Marriott (Longmont, Colorado)
(8) Robert D. Russell (Grapevine, Texas)
(9) Creath S. Thorne (St. Joseph, Missouri)
(10) Sam Woolsey (Houston, Texas)
(11) Hans Badstuebner (Stayton, Oregon)
(12) Dirk E. Skinner (Vineland, New Jersey)

Material in this issue: I shall include a dialogue that appeared on Richard Weatherwax's computer bulletin board, "Synapse BBS," for high-IQ societies, sent to me by James Hajicek, concerning a puzzle that was addressed by Marilyn vos Savant in one of her *Parade* magazine columns dated May 13, 1990.

Letters to the Editor

To the Editor:

Just to clarify, I did not mean to suggest that I believed Richard Sterman's asymmetric solution was wrong. But when I was asked if I could verify it, the most I could confidently say was "I don't know." If it had any errors, they were certainly more subtle than the error in the symmetric case, and I did not catch any in my initial examination. In fact, his solution corrects an error I made in some of my initial attempts at an asymmetric solution. So I wouldn't consider my failure to verify it as a "refutation" so much as an admission that my analysis was inadequate to fairly evaluate it.

Dean Inada

To the Editor:

Sorry to take so long to reply. I've been moving and studying for Jeopardy, the game show, on which I finished a disappointing but not humiliating second. Rather than guaranteeing victory, frenzied studying seemed to prevent a lackluster third-place finish.

I'd like to meet other L.A. area members, if it isn't already too late.

I still don't think my solution to the spheres/tetrahedron problem is an unsuccessful attempt, though I haven't done any more work on it. I think that my chain of reasoning, which leads to a naive and wildly wrong symmetrical solution, ends at the correct asymmetrical answer, which was what I was pursuing, flawed intermediate solutions notwithstanding.

Richard Sterman

To the Editor:

The data from the Titan Test was most interesting. I calculated a Kuder-Richardson formula 21 reliability of .9381413 for the Omni data. As you probably know, I regard the Kuder-Richardson formula 20--for formula 21, but 20--as the only mathematically justifiable method for estimating a test's reliability. However, it generally turns out that the value found by using the uder-Richardson formula 20 is equal to or greater than that found with the KR-21. Since I regard a KR-20 of .85 to be the lowest possible acceptable reliability for an intelligence test, and the KR-21 I calculated greatly exceeds that, it follows that the KR-20 will almost certainly exceed it as well.

Looks like you've got a winner.

Grady M. Towers

The Chicken & Egg Problem

My father-in law loves to ask this question, which usually ends in an argument. Can you settle it? If a hen and a half can lay an egg and a half in a day and a half, how many hens does it take to lay six eggs in six days?

Kristen Hedberg (Medford Oregon)

My father loved this one, too, but I didn't get it then, and I don't get it now. What's the problem? Is "one hen" too obvious? If a hen and a half can lay an egg and a half, etc., that means a hen can lay an egg in a day. And if just one hen lays one egg a day for six days, we'd have six eggs right there, wouldn't we? (I'm afraid I'm missing something, like a terrible pun about scrambled eggs.)

Marilyn vos Savant (New York, NY)

Computer Bulletin Board Commentary

There is a fairly well known problem which asks: If a chicken and a half can lay an egg and a half in a day and a half, how many chickens does it take to lay six eggs in six days. Post your solution, then I'll tell you why I've mentioned it.

Kevin Langdon

To Mr. Langdon:
With regard to the chicken and egg problem:

Let C = number of chickens
T = time allowed for egg laying
R = egg laying rate
E = number of eggs

It seems to me that the appropriate formula is:

$$E = C\ T\ R$$

If a chicken and a half can lay an egg and a half in a day and a half, then for this data point:

$$1.5 \text{ eggs} = (1.5 \text{ chickens})\ (1.5 \text{ days})\ R$$

$$R = 2/3 \text{ egg/chicken-day}$$

Then for six eggs in six days, to determine the number of chickens required:

$$6 \text{ eggs} = C\ (6 \text{ days})\ (2/3 \text{ eggs/chicken-day})$$

$$C = 1.5 \text{ chickens}$$

I believe I know why you are asking this question. Let me say that if I had a reputation to maintain, and if I were going to make a public announcement about my solution to this problem, I would do the following things:

1. Solve the problem very carefully, as above.
2. Solve the problem several different ways.

3. Have another high-IQ person check my answer.

4. Not be arrogant in public about my answer.

You are clearly on the right track.

James Hajicek

To Mr. Langdon:

I noticed a subtle difference in your version of the problem. Whenever I ask it, I ask how many eggs will x number of chickens lay in y number of days. But you are asking for the number of chickens, for x eggs in x days, making it simple. I will let others give their answer.

Sysop

To Mr. Langdon:

First determine the daily egg unit production rate per chicken. This will be determined by one-and-one-half eggs divided by one-and-one-half days divided by one-and-one-half chickens, yielding 2/3 eggs produced per day per chicken. At that daily production rate per chicken, nine chickens would be required to produce six eggs in one day. Since six days are allotted, one-and-one-half chickens would produce six eggs in six days. It seems intuition provides the same answer. In other words, if X chickens produce Y eggs in Y days, then X cnickens will produce six eggs in six days.

Gregory Cline

To Mr. Cline:

Of course, those of you who have given an answer to the chickens and eggs problem are correct. I mentioned it because Marilyn vos Savant gave the incorrect answer, one chicken, in her column in Parade Magazine. A genius can't be too careful these days.

Kevin Langdon

To Mr. Langdon:

Since half a chicken is useless for laying eggs, and it is impossible to lay 1.5 eggs without laying two eggs, then the problem as stated must mean that one chicken can lay two eggs in 1.5 days. Then the answer to the puzzle must be one.

On another subject, I cannot agree that methodology but not content can be silly. Anyone who watches federal research grants knows that content can be very silly indeed. Of course, silliness is relative; any item of research has the potential to be useful to someone at some time--even assessments of the relative intelligence of races. Nevertheless, it seems likely that the pernicious effects of such research overwhelm any marginal scientific benefits.

Mark Stegeman

Editor's comment:

It did not seem to me that Marilyn's solution to this puzzle smacked of arrogance. It seemed quite modest and lighthearted to me.

Ron Hoeflin

THE NEW YORK TIMES, SUNDAY, JUNE 18, 1989

A Program That Makes Conjectures

By GINA KOLATA

SUPPOSE a computer program could give artists their ideas for what to paint. Or what if a computer program churned out possible story ideas for novelists? Would anyone want to use them?

Mathematicians, many of whom consider themselves more artists than scientists, have had to consider exactly this problem. A researcher has devised a program that spews out conjectures in a field of mathematics known as graph theory.

A conjecture is to a mathematician what a hypothesis is to a scientist: an educated guess to be tested for possible canonization into the realm of truth.

"Finding a good conjecture is definitely half of the job," said Siemion Fajtlowicz, the University of Houston mathematics professor who wrote the program, called Graffiti. The program can easily generate tens of thousands of conjectures, he said. Although some mathematicians have been happy to work on proving the conjectures true or false, others seem to resent the computer, Dr. Fajtlowicz said. "I've run into quite a few Luddites," he said.

Although Dr. Fatjtlowicz has been promoting his program at math meetings, throwing out conjectures and hoping that his colleagues or students would become interested in trying to prove them, most mathematicians, even graph theorists, have still not heard of it. It remains a somewhat bizarre source of mathematical inspiration and an irritant to some researchers.

One mathematician told Dr. Fajtlowicz he was furious that the computer had chanced upon a mathematical truth that he himself had discovered. Another mathematician wrote to Dr. Fajtlowicz, only half in jest, that Graffiti was putting him out of a job.

Seeking Truths

Dr. Fajtlowicz said his computer program starts with a collection of graphs, which are groups of points connected by lines. A highway road map is a graph, for example. The program looks for relationships that seem to hold true for the graphs in its collection and then proposes them as more general truths.

In a way, it is like the story of the monkeys banging away at typewriters. Sooner or later, one will type "Hamlet." And sooner or later, Graffiti will find important mathematical truths by randomly trying many different relationships. But the challenge, Dr. Fajtlowicz said, is to find that mathematical work of art when it appears. "The difficult thing is to discard everything else but 'Hamlet,' " he said.

So Dr. Fajtlowicz had to decide what made a good conjecture. He said he could not simply ask the program to spit out every conjecture it could find because he would soon be buried in a pile of mostly uninteresting ones. One round of Graffiti results in 3,000 to 8,000 conjectures.

The trick was to find a way to automate a mathematician's instinctive feeling that some possibilities are more worthy of study than others. But mathematicians describe the act of research as highly creative and say they are guided by an intuitive sense of what is significant and what is not. They often describe a theorem they like as beautiful and a particularly striking proof as elegant.

"I asked everybody in sight, 'How do you know if a conjecture is interesting?' " Dr. Fajtlowicz said. "Nobody seemed to know."

Looking for Beauty

He eventually chose four criteria. A conjecture would have to be surprising, judged by how different it was from conjectures the computer had made before. It could not be a logical consequence of another conjecture. It should not be overly specific. And if a conjecture compared two quantities, the quantities should be close in size. Using these standards, he was able to eliminate all but 20 to 50 of the proposals produced by a run of the program.

Dr. Fajtlowicz said that at least 20 mathematicians have worked on proving conjectures generated by the program and that he knows of five papers proving Graffiti conjectures that have either been published or accepted for publication by mathematics journals.

Fan Chung, who directs research in mathematics and communications at Bell Communications Research in Morristown, N.J., has worked on a Graffiti conjecture. She described it as a statement about two properties of a graph. One is the average distance between pairs of points. The other is a quantity called the independence number, which has to do with how many areas of the graph are not adjacent to one another. The conjecture said that if the average distance is large, so is the independence number.

"What attracted me to the conjecture was its simplicity," Dr. Chung said. "It was a very clean relationship. But it was harder to prove than it first looked."

Dr. Chung said that given a choice, she would rather work on her own conjectures or on those that have gained a certain fame or notoriety in mathematics because they have been so difficult to verify. But, she added, "it doesn't bother me," to work on a problem suggested by a machine.

Dr. Fajtlowicz said that the more he has worked with Graffiti, the more he appreciates its abilities. "I think Graffiti is good at generating problems," he said. "In fact, I think now it is better than me."

THE NEW YORK TIMES WEDNESDAY, AUGUST 22, 1990

4 Honored With Fields Medal in Mathematics

By MALCOLM W. BROWNE

Fields Medals, the most prestigious international awards in mathematics, were bestowed yesterday upon two mathematicians from the United States and one each from Japan and the Soviet Union.

The Americans, honored at a ceremony in Kyoto, Japan, were Dr. Vaughan F. R. Jones, a professor of mathematics at the University of California, Berkeley, and Dr. Edward Witten, a professor of mathematics and theoretical physics at the Institute for Advanced Studies in Princeton, N.J.

Medals were also awarded to Dr. Vladimir G. Drinfeld, a senior fellow of the Institute for Low Temperature Physics and Engineering, Kharkov, U.S.S.R., and Dr. Shigefumi Mori, a faculty member of the Research Institute of Mathematical Sciences at Kyoto University, Japan.

Held Equivalent to Nobels

The Fields Medal, which carries no monetary award, is regarded by mathematicians as equivalent to the Nobel Prizes in the sciences. There is no Nobel Prize in mathematics. Fields Medals are awarded once every four years by the International Congress of Mathematicians, which was convened this year in Kyoto.

The medal was conceived by John Charles Fields, a Canadian mathematician, "in recognition of work already done and as an encouragement for further achievements on the part of the recipient." Since 1936, when the medal was first awarded, judges have interpreted the terms of Dr. Fields's trust fund to mean that the award should usually be limited to mathematicians under 40 years old.

Dr. Jones, 37 years old and a native of New Zealand, and Dr. Witten, 38, have worked on clósely related problems. Dr. Jones is best known for his contributions to a branch of topology known as knot theory, while Dr. Witten's work has focused on string theory. Their work goes far beyond the scope of pure mathematics; it lays the groundwork for some revolutionary theories that could help to explain the fundamental building blocks of the universe and the genetic code of life.

Dr. Jones's most famous discovery, which he made in 1984, was a polynomial equation enabling a mathematician to tell whether two seemingly different knots are genuinely different or are merely variations of the same underlying pattern.

Practical Applications

This discovery, which had long eluded mathematicians, found quick practical applications, especially in the science of molecular biology. DNA, the complex helical molecule that makes up the genes of living organisms, takes the form of complex knots, and the Jones polynomial enabled biologists to begin sorting out these knots according to type. This, in turn, made it possible to determine the sequence of changes DNA undergoes as it participates in the processes of life.

Dr. Witten is one of the principal authors of a theory that the fundamental particles that make up the universe may take the form of almost infinitessimally small strings closed into tiny loops. Dr. Witten and many other theorists believe that the mathematics describing these strings could one day prove to be the key to one of the main enigmas of physics: the relationship of gravity to the other known natural forces.

Few scientists believe that string theory can be tested in any practical wav in the foreseeable future, but it is at least a mathematical tool physicists might be able to use in explaining not only gravity but also the origin of matter and everything else in the universe; it is sometimes called "the theory of everything."

Dr. Drinfeld's work is also connected with physics. His most recent contributions have been to the theory of quantum groups, a branch of theoretical physics. His citation also mentioned his "profound contributions" to algebraic geometry, number theory and the theory of automorphic forms.

Dr. Mori was cited for developing a classical theory of algebraic surfaces in such a way as to extend the theory to three dimensions. His medal was awarded for "deep and beautiful work on the classification of complex algebraic varieties of dimension bigger than two."

THE NEW YORK TIMES WEDNESDAY, JUNE 20, 1990

Giant Leap in Math: 155 Divided to 0

By GINA KOLATA

In a mathematical feat that seemed impossible a year ago, a group of several hundred researchers using about 1,000 computers has broken a 155-digit number down into three smaller numbers that cannot be further divided.

The number is about 50 digits longer than any that mathematicians have reported being able to break down in the same way, an unusually long leap in this area of mathematics.

The latest finding could be the first serious threat to systems used by banks and other organizations to encode secret data before transmission, cryptography experts said yesterday.

These systems are based on huge numbers that cannot be easily factored, or broken down into numbers that cannot be divided further.

First Break in the System

This is the first time that mathematicians have factored a number of the size used in these coding systems, said Dr. Arjen Lenstra, director the project who is at Bellcore Inc., in Morristown, N.J., the research arm of the Bell operating companies.

To break the huge number into three smaller numbers, which are 7, 49 and 99 digits long, the mathematicians had to find a new method because the one used in recent years was not up to the job. If someone had asked him to break up a 155-digit number a year ago, Dr. Lenstra said, "I would have said it was impossible,"

Dr. Andrew Odlyzko, a mathematician at the American Telephone and Telegraph Bell Laboratories in Murray Hill, N.J., said: "This is a great achievement. From the standpoint of computational number theory, it represents a breakthrough."

The number itself was famous among mathematicians as a factoring challenge. In October 1988, mathematicians reported the factoring of a 100-digit number. It is a rule of thumb in mathematics that for every 10-digit increase in the size of a number, the amount of computing needed to factor it increases 10 fold. Until now, factoring advances had come in increments of 10 digits or less.

Secrets Are at Stake

But the practical importance of the result, experts said, is what it might mean to cryptography. In 1977, a group of three mathematicians devised a way of making secret codes that involves scrambling messages according to a mathematical formula based on factoring. Now, such codes are used in banking, for secure telephone lines and by the Defense Department.

In this system, each letter is replaced by a pair of digits, with each line of the message being considered one number. That number is multiplied by itself many times. Then it is divided by a large number whose factors are secret. The remainder of that division — the amount left over — is the coded message.

In making these codes, engineers have to strike a delicate balance when they select the numbers used to scramble messages. If they choose a number that is easy to factor, the code can be broken. If they make the number much larger, and much harder to factor, it takes much longer for the calculations used to scramble a message.

For most applications outside the realm of national security, cryptographers have settled on numbers that are about 150 digits long, said Dr. Gus Simmons, a senior fellow at Sandia National Laboratories in Albuquerque, N.M., who advises the Defense Department on how to make coding secure.

Broader Application Seen

Dr. Lenstra, who also led in the breaking of the previous 100-digit number, said: "For the first time, we have gotten into the realm of what is being used in cryptography. It means it is impossible to gurantee security."

Although the number the group factored had a special mathematical structure, Dr. Lenstra and his colleagues say the factoring method can be modified so it would have broad application.

Mixed blessing: an advance that could imperil secrets.

Others are more circumspect. Dr. Simmons said that although he agrees that the method is generally applicable, he is waiting to see whether it can break down other numbers quickly enough to be practical. The method, he said, "may become of concern to cryptographers, but that depends on how efficiently it can be implemented."

Nonetheless, Dr. Simmons said, he would not feel comfortable advising the use of a 150-digit number to maintain security. "If national security were hidden behind a 150-digit number, we're getting very close to a situation where it would be feasible to factor that," he said. "Do I advise the Government to use bigger numbers? You bet."

The newly factored number was the largest number on a list mathematicians keep of the 10 Most Wanted Numbers, which are large numbers that are set up as a challenge to factoring experts. And it is so large that it is inconceivable to even think of factoring it without special mathematical tricks.

Dr. Mark Manasse of the Digital Equipment Corporation's Systems Research Center in Palo Alto, Calif., calculates that if a computer could perform a billion divisions a second, it would take 10 to the 60th years, or 10 with 59 zeros after it, to factor the number simply by trying out every smaller number that might divide into it easily. But with a newly discovered factoring method and with a world-wide collaborative effort, the number was cracked in a few months.

The new factoring method was discovered last year by John Pollard of Reading, England, and Dr. Hendrik Lenstra Jr. of the University of California at Berkeley, the brother of Dr. Arjen Lenstra. The two mathematicians found a shortcut to factoring numbers of a particular form that happened to fit the form of many large numbers that were purposely derived so as to be difficult to factor.

Then Dr. Manasse and Dr. Arjen Lenstra recruited computer scientists and mathematicians from around the world to help in the factoring effort. Each person who agreed to help got programs sent electronically to their computers and a piece of the problem to work on.

Like a Jigsaw Puzzle

It was like solving a giant, and twisted, jigsaw puzzle, Dr. Manasse said. Each computer was set to work doing the mathematical equivalent of sorting through a box with about 50 million pieces "including all sorts of useless stuff that look like jigsaw pieces that are not," Dr. Manasse said, adding: "Each person has to find the real piecs in the box. Some boxes don't have any and some have just one or two."

After about a month, the researchers got back the equivalent of about two and a half million pieces of the puzzle. To speed up the search and the final putting together of the pieces that would allow them to factor the number, the researchers used a powerful computer at the Universtiy of Florida that finished the job for them in three hours.

The current factoring landmark is the latest in a series of what to mathematicians have been breathtaking feats. In 1971, mathematicians scored a coup by factoring a 40-digit number. Ten years ago, a 50-digit number was thought to be all but impossible to factor. Then, with advances in research that led to unexpected shortcuts, 60-, 70- and 80-digit numbers fell. A year and a half ago, the 100-digit number was cracked.

Factoring a 155-Digit Number: The Problem Solved

13,407,807,929,942,597,099,574,024,998,205,846,127,
479,365,820,592,393,377,723,561,443,721,764,030,073,
546,976,801,874,298,166,903,427,690,031,858,186,486,
050,853,753,882,811,946,569,946,433,649,006,084,097

equals

2,424,833

times

7,455,602,825,647,884,208,337,395,736,200,454,918,
783,366,342,657

times

741,640,062,627,530,801,524,787,141,901,937,474,059,
940,781,097,519,023,905,821,316,144,415,759,504,705,
008,092,818,711,693,940,737

Source: Mark Manasse, Ph.D.

THE **ACHIEVER REPOSITORY**

14120 MAGNOLIA BOULEVARD . SHERMAN OAKS, CALIFORNIA 91423

October 3, 1990

One-In-A-Million Society
G.P.O Box 7430
New York, NY 10116

Dear Sirs:

May I request additional information regarding your organizaion with particular reference to the selection techniques used for your membership. Do you publish a news letter and, if so, are discreet inserts or advertisements allowed in your publication?

We are an international organization that searches for men who are high achievers and who have a personal desire to contribute a superior genome to future generations.

I look for forward to your reply.

Sincerely yours,

Dean L Moyer

Dean L. Moyer, M.D.
Medical Driector

DLM/llr

Ronald K. Hoeflin
P. O. Box 7430
New York, NY 10116

First Class
Mail