MATHEMATICAL SCIENCES RESEARCH INSTITUTE

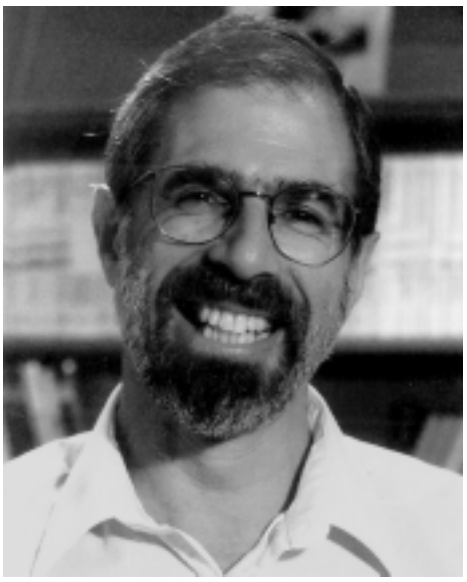
EMISSARY

JANUARY 2001

WWW.MSRI.ORG

Notes from the Director

David Eisenbud



MSRI is in full swing with the characteristic sounds of a busy autumn semester. The Institute is thriving, with major programs this year on Algorithmic Number Theory, Operator Algebras, and Spectral Invariants of Manifolds, and a microprogram on Minimal Surfaces. On the applied mathematics side, MSRI is conducting workshops on Cryptography, Combinatorial Designs, Nonlinear Estimation, and Random Methods in Financial Mathematics.

(continued on page 12)

Inside This Issue

Operator Algebras 2000-2001

Edward G. Effros
Program Chair, Operator Algebras

When I completed my dissertation in 1961, there were only a handful of operator algebraists in the world. By contrast, even though more than two hundred mathematicians will participate in the current program, there are at least another one hundred who *should* have been invited. Owing to the enormous growth of the subject and the limited space at MSRI, it was necessary for the organizers to restrict the sessions to certain areas that are currently undergoing rapid expansion. In addition to an introductory workshop, the schedule has been organized around four double workshops (described below). These link topics that have had particularly fruitful interactions. After a brief summary of the subject, I have sketched the topics covered by the workshops. I am indebted to Dietmar Bisch and Dmitri Shlyakhtenko for their contributions to this task.

Operator Algebras

In a nutshell, operator algebraists study the mathematics of quantum physics. Heisenberg postulated that the "variables" or "observables" of physics should be thought of as matrices, or more precisely self-adjoint Hilbert space operators, rather than real-valued functions. For simplicity we restrict our attention to bounded functions and operators. By contrast with functions, operators incorporate the highly specific uncertainty properties of quantum physics. As Heisenberg discovered, these properties flow from the fact that matrices need not commute.

The first question that will occur to the novice is *how can one think of a self-adjoint matrix as a "generalized function"*? This is more easily understood if one goes in the reverse direction. Given a real n-tuple $(\lambda_1, \ldots, \lambda_n)$ (i.e., a real function on $\{1, \ldots, n\}$), we may associate with it the self-adjoint matrix

$$T = \begin{bmatrix} \lambda_1 & 0 & & 0 \\ 0 & \lambda_2 & & 0 \\ & & \ddots & \\ 0 & 0 & & \lambda_n \end{bmatrix}$$

On the other hand if T is an arbitrary self-ajdoint $n \times n$ matrix, then T has the above form with respect to an orthonormal basis of eigenvectors. In this sense, every self-adjoint matrix is a "function", but these functions can be "incommensurable" in the sense that they cannot be simultaneously diagonalized.

Operator algebras provide the key to understanding quantum variables. In the formulation given by Gelfand and Naimark, we can view an operator algebra as the most natural

(continued on page 4)

Special Events

Each year MSRI sponsors mathematical events of interest to the general public. In the Fall of 2000, these events were:

DNA Computing, Molecular Biology and String Theory: Mathematics Across the Sciences
Saturday. September 16, 2000, 1-5 pm

This event was part of the three-day Panorama of Mathematics Conference, September 14-16, 2000, in honor of MSRI's founding director Shiing-Shen Chern.

The first talk was given by Leonard Adleman of Stanford University whose contributions to the theory of computation and cryptography include co-developing the now widely used RSA system for data encryption. He is given credit as the first scientist to actually solve a mathematical problem using DNA and he spoke on "DNA Computation."

Richard Karp of UC Berkeley gave the second talk, "Mathematical Challenges from Genomics and Molecular Biology". Professor Karp has done pioneering research on combinatorial algorithms, including early work on what has become one of the Clay Institute's million-dollar problems: Does P=NP?

The third talk was given by Brian Greene of Columbia University, who is known for both his research on superstring theory and his enormously successful popular book, "The Elegant Universe." The title of his talk was: "String Theory and the Fabric of Spacetime." Introductory remarks were given by John Gage, Director of the Science Office at Sun Microsystems.

Code Breaking in WWII:
The Enigma, The Colossus and Bletchley Park
Thursday, October 19, 2000, 8pm

This talk by Anthony E. Sale, Hon. FBCS, described the enormous impact of the Allied cryptographers in Bletchley Park on WWII. Sale began by describing how the German Enigma cipher was broken, first by the Poles and then by the code breakers in Bletchley Park using remarkable contributions by Alan Turing. He then discussed the breaking of the German Lorenz code with the Colossus, the world's first large electronic computer. He related some of the many anecdotes about life in Bletchley Park, which had 250 people in 1939 but exploded to 12,000 people by the end of the war.

Tony Sale has had careers in electronics, intelligence (with MI5) and (since 1963) in computers. He started Bletchley Park Museums and the rebuild of the Colossus in 1993, and was Museums Director until 1999. He has lectured and written widely on the history of cryptography and computers, and served as a consultant for "Breaking the Code" and the soon-to-be-released film version of Robert Harris's book "Enigma".

Why Voting Procedures Can Create a Mess:
A Mathematician Looks at Elections
Wednesday, November 29, 2000, 7:30pm

This talk by Don Saari looked at the question: Was this year's Presidential election mess really due to bad chad, poorly designed ballots, -- or subtle flaws of our election procedure? He described, for a general audience, how a mathematical analysis of this question reveals some unexpected and paradoxical results and described some of the insights that one can attain, and the lessons we can apply to prevent future elections from falling into the electoral morass of Y2K.

Donald Saari is a UCI Distinguished Professor of Mathematics and Economics at UC Irvine. Much of Professor Saari's research has emphasized dynamical systems and their applications to physics (mainly the Newtonian N-body problem) and to issues generated by the social sciences (such as voting procedures and economics). He is the author of the book "The Geometry of Voting" and numerous papers including "The likelihood of dubious election outcomes."

Musical Canons
Wednesday, December 6, 2000, 4:30pm

Mathematician, composer and pianist Noam D. Elkies discussed the ubiquitous musical form of the canon - a form occuring in simple rounds like "Three Blind Mice" as well as in the compendium of canons Bach compiled in his Musical Offering, and of continuing interest to contemporary composers and performers. Elkies brought both a mathematician's and musician's point of view to this subject, which he illustrated with both abstract diagrams and specific examples.

Noam Elkies is Professor of Mathematics at Harvard. His work on elliptic curves, lattices and other aspects of the theory of numbers has been recognized by such prizes and awards as the Presidential Young Investigator Award of the National Science Foundation and the Prix Peccot of the College de France. In addition, he has been composing and playing the piano since the age of three. He has recently performed with the Boston Youth Symphony, the Metamorphosen Chamber Orchestra and the Harvard-Radcliffe Chorus, and has premiered piano pieces by many composers, including all of his own. His compositions have won two BMI awards and have been performed on three continents.

Anthony E. Sale, founder of the Bletchley Park Museums

Cramer-Shoup Encryption

Joe Buhler
Program Chair, Algorithmic Number Theory

The second workshop in the fall-semester Algorithmic Number Theory program (see sidebar) was "Number-Theoretic Cryptography." During the last twenty-five years the role and visibility of mathematics, especially number theory, in cryptography has grown enormously. More recently, there have been a number of results in the direction of providing rigorous foundations for cryptography.

One of the central goals of the workshop was to bring together people working in these two directions. To this end, the workshop was preceded by a two-day "short course" taught by Cynthia Dwork and Moni Naor. The aim of the short course (whose lectures can be viewed on the MSRI web site, www.msri.org) was to introduce mathematicians, and others, to ideas about the foundations of cryptography that have arisen the last 10 or 20 years out of computational complexity.

Cryptography has any number of well-known fault lines. The conflicting interests of government agencies and academic researchers were well-publicized in the 1980's, and more recently the varied commercial forces in cryptography, the growth of the Internet, and the rapid pace of academic research have created an explosion of conflicting interests. One specific example of diverging perspectives, perhaps less well known than it should be among mathematicians, is the difference between the newer "theoretical" views of the foundations of the subject (arising out of computer science as least as much as mathematics), and the more "practical" views, both inside and outside the academic world. Mathematicians can be found all over the map on this issue, despite the fact that the desire for rigorous definitions and proofs is a more traditional "mathematical" approach.

The goal of this article is to give an overview of a recent cryptosystem, discovered by Ronald Cramer and Victor Shoup, that was discussed during the short course and workshop, and has several interesting features that narrow the gap between theory and practice. The covert goal is to shed at least a little light on the aforementioned fault line.

Algorithmic Number Theory Workshops

Clay Mathematics Institute
Introductory Workshop in Algorithmic Number Theory,
August 14-23, 2000

Organizers: David Bailey, Joe Buhler (chair), Cynthia Dwork, Hendrik Lenstra, Jr., Andrew Odlyzko, Bjorn Poonen, William Velez, Noriko Yui

Number-Theoretic Cryptography, October 16-20, 2000

Organizers: Eric Bach, Dan Boneh, Cynthia Dwork (chair), Shafi Goldwasser, Kevin McCurley, Carl Pomerance

Arithmetic Geometry,
December 11-15, 2000

Organizers: Noam Elkies, William McCallum, Jean-Francois Mestre, Bjorn Poonen (chair), René Schoof

Public-Key Cryptography

The first public discussion of public-key cryptography was in a paper in 1976 by Whitfield Diffie and Martin Hellman that described, among other things, the now famous Diffie-Hellman key exchange. This was followed, in 1977, with the vital contribution of Ronald Rivest, Adi Shamir, and Leonard Adleman describing their cryptosystem in Martin Gardner's Mathematical Games column in *Scientific American*.

Over the years there were hints that these ideas had been discovered within the US or UK national security communities, and in the last few years, it has become publicly known that three employees of the GCHQ (the British analogue of the NSA) discovered these same ideas. The idea that public-key cryptography might be possible was due to James Ellis in 1969; by 1975 Ellis, Malcolm Williamson, and Clifford Cocks had discovered the DH and RSA schemes.

Before the 1970's all systems for allowing two parties to securely send and receive messages required agreed-upon hidden information ("keys") that were exchanged beforehand. In some contexts where secret communications are desired, the problem of distributing those keys is onerous or almost impossible.

This state of affairs was dramatically altered by the invention of public-key cryptography in the 1970's. The basic premise is very counterintuitive: two parties can send and receive secret messages without having exchanged any information beforehand, in such a way that an eavesdropper can obtain no information about the transmitted messages.

This sounds impossible (and from the point of view of information theory, it is!). However, in the real world computational power is limited, and this is the crucial fact that makes public key cryptography a realistic possibility. The history of public-key cryptography is curious (see sidebar).

The basic public-key idea for sending a message is as follows. Suppose that Alice wants to send Bob a message m from a large finite set M of messages. She starts by looking up Bob's "public key" k in a trusted publicly accessible directory. She then uses a public encryption function

$$m \to E_k(m)$$

to convert a plaintext message m into cipher text $E_k(m)$.

Of course, if Alice wants to send a longer message she can break her message up into blocks, each of which can be identified with an element of M. Bob decrypts the message by applying the inverse transformation $m \to D_k(m)$; the function D_k is of course kept secret. The crux of the secrecy is that it should be easy to generate the

(continued on page 7)

Operator Algebras 2000-2001

(continued from page 1)

generalization of the (one-dimensional) algebra of complex numbers $\mathbf{C}$. A C^*- algebra is just a Banach algebra A with an involution and a norm satisfying $\|a^*a\| = \|a\|^2$. Our model for a quantum variable is an element of A_{sa}, the self-adjoint elements in a C^*-algebra A.

If we let $A = \mathbf{C}$ with the * -operation $\alpha^* = \overline{\alpha}$, and the norm $\|\alpha\| = |\alpha|$, this is just the identity $|\alpha\overline{\alpha}| = |\alpha|^2$. More generally, we have the C^*-algebra $C_0(\Omega)$ (respectively, unital C^*- algebra $C(\Omega)$) of continuous complex functions $f : \Omega \to \mathbf{C}$ on a locally compact (respectively compact) Hausdorff space Ω with the usual algebraic operations, the *-operation $f^* = \overline{f}$, and the norm $\| f \|_\infty = \sup \{|f(\omega)| : \omega \in \Omega\}$. If $\Omega = \{1, \ldots, n\}$, we obtain the C^*- algebra of n-tuples $\mathbf{C}^n$.

Perhaps the simplest non-commutative example is the C^*- algebra $B(H)$ of bounded linear operators T on a Hilbert space H with the usual *-algebraic operations, and the operator norm $\|T\| = \sup\{\|T\xi\| : \xi \in H, \|\xi\| = 1\}$. If $H = \mathbf{C}^n$, this is the C^*- algebra of $n \times n$ matrices M_n.

These examples are universal. Any commutative C^*- algebra is of the form $C_0(\Omega)$, and any C^*- algebra can be identified with a closed C^*-subalgebra of $B(H)$ for some Hilbert space H. The spectral theorem provides a key illustration of these ideas. If T is a self-adjoint operator on a Hilbert space H, then the unital C^*- algebra $C^*(T)$ generated by T and the identity operator is commutative, and thus must have the form $C(\Omega)$. It follows from the spectral theorem that the mapping $f \to f(T)$ determines an isometric * -isomorphism $C(\mathrm{sp}T) \cong C^*(T)$.

Turning to another important special case, if μ is a Borel measure on a compact space Ω, then $R = L^\infty(\Omega, \mu)$ with the usual operations is a unital commutative C^*- algebra. It follows that R may be identified with $C(\widetilde{\Omega})$ for some space $\widetilde{\Omega}$. R is also the dual of the Banach space $L^1(\Omega, \mu)$. In general we say that a C^*- algebra A is a *von Neumann algebra* if it is the dual of a Banach space (which must then be essentially unique). These are the algebras that von Neumann introduced in his development of "quantized integration theory".

There is a natural extension of *probability theory* to the context of operator algebras. A simple example of a probability space is a compact Hausdorff space Ω together with a probability measure μ on Ω, or equivalently a positive linear functional μ on $C(\Omega)$ for which $\mu(1)=1$. The corresponding notion of a C^*-*probability space* is a pair (A, μ), where A is a unital C^*- algebra and μ is a linear functional on A which is a *state*, i.e., it is positive in the sense that $\mu(a^*a) \geq 0$ for all a in A and $\mu(1) = 1$. Perhaps the simplest non-commutative example of a C^*-probability space is (M_n, tr) , where tr is the normalized trace functional.

We may regard the self-adjoint elements of a C^*-probability space (A, μ) as *non-commuting random variables*, or in the terminology of physics, the *observables* of a given physical system. Given $a \in A_{sa}$, we may identify $C(\mathrm{sp}\ a)$ with the unital $C^*(a)$ generated by a , and μ then restricts to a state μ_a on $C(\mathrm{sp}\ a)$, or equivalently, a probability measure on sp a. If $A = C(\Omega)$, then μ_a is just the usual distribution measure on sp $a = a(\Omega)$. We interpret $\mu(a)$ as the expectation of the random variable a. It coincides with the expectation of μ_a.

Simple C*-algebras and Dynamical Systems

Since one has an essential (contravariant) equivalence between the categories of locally compact spaces and commutative C^*-algebras, operator algebraists have regarded C^*- algebra theory as the study of "quantized locally compact topological spaces". From this point of view, the possibility of *classifying* C^*- algebras would seem to be hopeless since in the commutative case this would amount to classifying the locally compact spaces. It came as a bombshell in the early 1980's that the introduction of non-commutativity completely alters this situation.

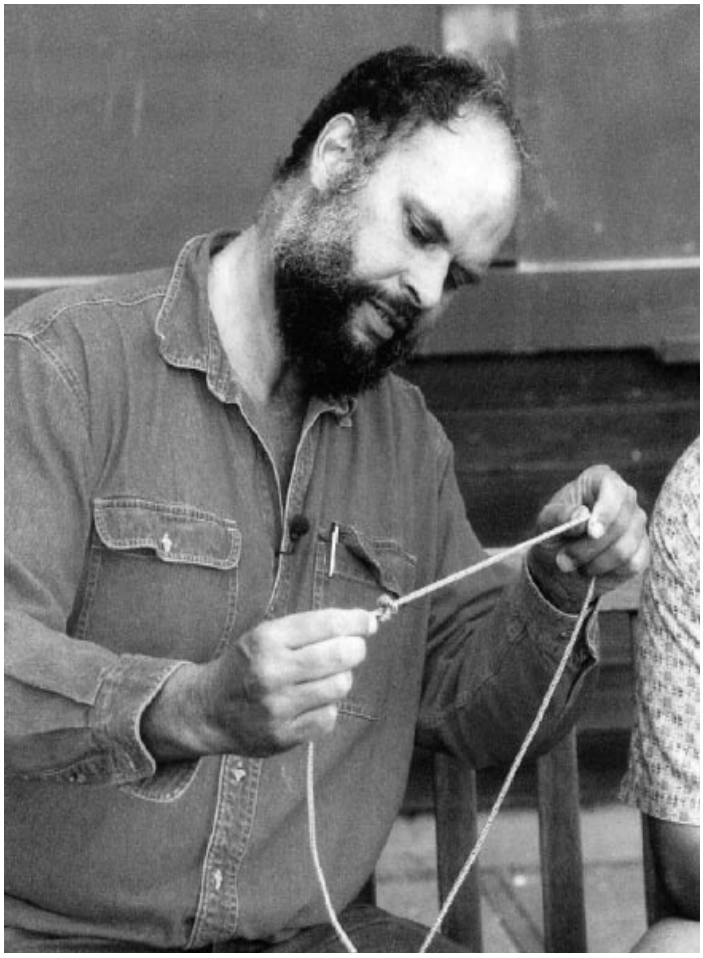
For some years operator algebraists had sought C^*-algebraic analogues of the invariants of algebraic topology. This was a very discouraging affair, since only K -theory and its variants seemed to have a meaning in this context. What shocked everyone was George Elliott's crazy but inspired guess that non-commutativity (in the form of simplicity) *simplifies* the underlying topology. More explicitly he conjectured that simple C^*-algebras could be classfied by their K -theory. This was regarded as ridiculous by many (including myself), and we waited for the counter-examples to appear. We are still waiting. It seems that a large class of simple C^*-algebras can indeed be classified by various K-theoretic invariants. These developments have required the efforts of some of the top operator algebraists.

Since one can associate natural operator algebras with dynamical systems, these results have had a significant impact on the classification of dynamical systems. In addition, the context of operator algebras enables one to study actions of groups on operator algebras. The interaction between these fields has proved to be quite beautiful.

Subfactors and Quantum Field Theory

This theory essentially began with Vaughan Jones' study of the *position* of a subalgebra N in a von Neumann algebra M. For simplicity it is better to consider inclusions $N \subseteq M$ of finite factors, i.e., algebras with a unique trace functional, and for which the centers consist of the scalar multiples of the identity. For instance, given a group of outer automorphisms G of the finite factor M, the algebra of invariants M^G is an example of such an inclusion. In general we shall call N a *subfactor* of M.

The study of subfactors $N \subseteq M$ is in a sense analogous to Galois theory, which is devoted to the analysis of group actions of fields. Murray and von Neumann proved in the 30's that the representation theory of an infinite dimensional finite factor is labelled by a continuous parameter, measuring the "dimension" of the representation. Given a subfactor $N \subseteq M$, the "dimension" of N in



Vaughan Jones thinks about a knot.

its natural representation on M is called the *Jones index* $[M : N]$ of N in M. *A priori* any real number greater than or equal to 1 could occur as the index of some subfractor. However, Jones discovered that the index is *quantized*, namely $[M : N] \in \{4\cos^2 \frac{\pi}{n} : n = 2, 3, \ldots\} \cup [4, \infty]$. Furthermore he showed that every number in this set is achieved. The key idea in his proof led to a new braid group representation which Jones used to construct his invariant for knots and links, the *Jones polynomial*.

But Jones' discovery was only the tip of the iceberg. Just as Galois theory led to the theory of groups, it can be argued that subfactors provide the best framework for studying symmetries of quantized systems. This includes group symmetries and symmetries captured by quantum groups. There is a vast algebraic-combinatorial structure underlying subfactor theory which is closely related to a wide range of topics including low-dimensional topology, loop groups, statistical mechanics, and quantum field theory. In addition to its importance in knot theory, it has led to completely new invariants for 3-manifolds. This is a very active field that has attracted the attention of such individuals as Atiyah and Witten.

Free Probability

The notion of *independent* random variables has a simple interpretation for C^*-probability spaces. Given two such systems (A_i, μ_i), we have a corresponding space $(A_1 \otimes A_2, \mu_i \otimes \mu_2)$ where we use the "minimal" C^* -algebraic tensor product. Given $a_1 \in (A_i)_{sa}$, the operators $b_1 = a_1 \otimes 1$ and $b_2 = 1 \otimes a_2$ are the prototypical examples of independent random variables. As in the classical case, one finds that if $\mu = \mu_i \otimes \mu_2$, then $\mu(b_1^k b_2^l) = \mu(b_1)^k \mu(b_2)^l$ for $k, l \in \boldsymbol{N}$.

There is also canonical state $\mu = \mu_1 * \mu_2$ on the *free product* C^*-algebra $A = A_1 * A_2$. This operation has no direct classical analogue since the free product is necessarily non-commutative. An amazing idea of Vociulescu was to nevertheless imitate the classical theory of independence. He regarded random variables $a_1 \in A_1 \subseteq A_1 * A_2$ and $a_2 \in A_2 \subseteq A_1 * A_2$ as being *freely independent* in $A = A_1 * A_2$.

The *free probability theory* deveoped by Voiculescu and his colleagues has remarkable parallels with the classical theory. In particular, there are free analogues of the central limit theorem, stable laws, and Brownian motion, as well as information-theoretic quantities such as entropy.

Very large random matrices tend to behave like freely independent random variables, and this has turned out to be one of the most powerful techniques in the subject. The theory is closely related to the asymptotic theory of large matrices, and this has led to remarkable new results in the classification of free product von Neumann algebras.

Operator Spaces

In recent years, operator algebraists have discovered that there is a natural quantized analogue for Banach space theory. If E is a Banach space, then we can realize E as a *function space*, i.e. a closed subspace of $l^\infty(S)$ for some set S. This suggests that it would be similarly useful to define a (complete) operator space V to be a closed subspace of $B(H)$ for some Hilbert space H. One might think that since V isn't assumed closed under multiplication, all that V inherits is the norm from $B(H)$. That, however, is not the case. $B(H)$ has a hidden structure which is of great importance.

If E is a Banach space, there is a natural "supremum norm" on the n-tuple space E^n given by $\|(x_1, \ldots, x_n)\| = max\{\|x_j\|\}$. Equivalently, we have a natural embedding $E^n \subseteq l^\infty(nS)$ where nS is the disjoint union of n copies of S. Turning to operator spaces, it is only natural to look for operator norms on the matrix space $M_n(V)$ of $n \times n$ matrices $v = [v_{ij}]$, $(v_{ij} \in V)$. We have a corresponding embedding $M_n(V) \subseteq B(H^n)$, where we let a matrix of operators $b = [b_{ij}]$ act on H^n by matrix multiplication. However, there is no simple formula for $\|b\|$ in terms of the $\|b_{ij}\|$. The matrix norms on the $M_n(V)$ very much depend upon the embedding $V \subseteq B(H)$, and they constitute an essential part of the structure of an operator space.

Turning to the natural mappings of the operator spaces, we must take the matrix norms into consideration. A linear mapping of operator spaces $\varphi : V \to W$ determines mappings $\varphi_n : M_n(V) \to M_n(W)$, where $\varphi_n([v_{ij}]) = [\varphi(v_{ij})]$. We say that φ is *completely isometric* if each mapping φ_n is isometric, and that it is *completely*

(continued on page 6)

Operator Algebras 2000-2001

(continued from page 5)

bounded if $\| \varphi \|_{cb} = \sup \{\| \varphi_n \|\} < \infty$.

Operator space theory is the the study of these matrix normed spaces together with their completely bounded mappings. An axiomatic (representation-free) characterization was given by Ruan. It is now understood that the subject very much parallels classical Banach space theory. Perhaps the most intriguing new phenomenon is the fact that such simple linear notions as the operator space analogues of local reflexivity and finite-dimensional approximation provide some of the deepest invariants in the study of operator algebras. It is also of great interest that they provide a new approach to studying the duals of C^*-algebras and more general operator spaces which naturally arise in non-commutative functional analysis.

Quantization and Noncommutative Geometry

In some sense these subjects represent the heart of what operator algebraists would like to achieve in the new century. Both modern geometry and quantum physics lead one to the inescapable conclusion that quantized forms of geometry must exist and that they will have a far-reaching impact on both subjects. Connes is the leading figure in this area and he has gone a long way to formulating a framework for these investigations.

One of the very early goals of non-commutative geometry was to find the appropriate setting for equivariant forms of the Atiyah-Singer index theorem. Connes has shown how this may be accomplished, and he has also succeeded in finding non-commutative versions of the theory of differential forms and Riemannian geometry.

Non-commutative geometry has proved to be one of the most powerful tools for studying the Novikov conjecture. Considerable progress has been made on the Baum-Connes conjecture, a far-reaching generalization of that problem. A wide range of quantization problems in physics provides important examples of non-commutative geometrical spaces. On the other hand, Connes has constructed an intriguing non-commutative model of four-dimensional space-time that reproduces the standard model of elementary particles from very general considerations.

It is impossible to convey the many facets of operator algebra theory in this note. Those interested in obtaining a more comprehensive view of this area may wish to consult Connes' monograph *Non-commutative Geometry*, Academic Press 1994.

YOUR OTHER COUNTRY

Remember, years ago, a woman on a N.Y, train
turned on two young men talking math
non-stop —You foreigners, she fumed,

either speak English or go back to your own country!
We thought it sad and funny, her discomfort
with math carried to xenophobic heights.

And I a young bride married to one of those!
But in truth I, too, found math forbidding.
It took years of living with you to see

your day in day out affair as close kin
to my passion as a poet. You'd work in a tent,
on a beach or train. All you needed

was pen and paper. In a pinch you'd do
with less, perfecting the skill of easing in
and out of solitude. Our daughters understood.

If you showed up early to drive them home
from parties, they'd say 'Not yet Dad,
you won't mind, just sit in the car and think!'

Then the way you push the limits of the known.
For days, months, you play with a hunch,
let a premise lead you, without forcing it,

towards the as yet unseen, unheard . . . Face flushed,
you look for me in the house to say
you've got it and it's beautiful! By morning

you see flaws, try to simplify, make it elegant;
you, like a poet, speaking in metaphor.
Numbers intertwine like arms, legs, hearts;

a theory tilts, perhaps at risk; loci, sadly,
are of the degenerate kind; ideals tainted
by duplicity; and quivers can be infinite.

In-finite qui-vers— that titillates
my tongue. I'm not surprised you spawned
good work along those lines.

At a conference in your honor you summed up
your life in math: I'm a man,
you smiled, of unresolved resolutions.

Colleagues laughed, aware of problems
you hope to solve in the field of resolutions.
But I liked your deft way of saying

you're an ongoing paradox;
true, I might add, of our long marriage—
deeply familiar, yet strangely tantalizing.

Betty S. Buchsbaum

Cramer-Shoup Encryption

(continued from page 3)

public key k and the decryption function, that the encryption function should be easy to compute knowing k, and that it should be computationally infeasible to calculate D_k knowing k.

The most famous example is the RSA cipher due to Rivest, Adleman, and Shamir. In this case, the message set M is the set of positive integers up to n that are relatively prime to n, where $n = pq$ is a product of two large distinct primes. The public key is a pair $k = (n, e)$ and the encryption function is

$$E_k(m) = m^e \bmod n.$$

The inverse permutation is $D_k(m) = m^e \bmod n$ where

$$ed \equiv 1 \bmod (p\text{-}1)(q\text{-}1).$$

It is easy to generate an exponent e and two large primes p and q, and then find the inverse exponent d. Moreover, the encryption and decryption functions can be computed efficiently. However, no one has any ideas on how to find D_k without factoring n, and factoring large enough integers appears, at the moment, to be computationally infeasible.

The naive RSA scheme described above is completely unsatisfactory in the real world for several reasons. For example, suppose that an eavesdropper Eve knows that the message m will come from a small finite collection of messages. All that Eve then has to do is to compute the encryptions $E_k(m)$ of each possible message and see which encryption is transmitted. Thus the scheme can very definitely leak information about a message.

An active adversary, who can not only eavesdrop on messages but also send malicious messages, makes the situation even worse. A particularly simple example for the RSA system is as follows (e.g., as in [DDN]). Suppose that Eve knows that the message m is an offer on a house in the Bay Area, and suppose that Eve wants to make a slightly higher offer, independent of m. It seems plausible that a purchase price would be divisible by \$100, so Eve can overbid by 1 percent by intercepting $E_k(m)$, multiplying by $E_k(101/100)$, and transmitting the result under her own signature. The receiver will see

$$E_k(m)E_k(101/100) \equiv m^e(101/100)^e \equiv (101m/100)^e \equiv E_k(101m/100) \bmod n.$$

Thus the multiplicativity of the RSA encryption allows Eve to modify the message so that she can make a small overbid, without knowing the original message. A system in which messages can be usefully modified by an active adversary is said to be "malleable."

Another more potent attack arises from the possibility that Eve might be able to trick Bob into providing decryptions. Eve could intercept $y = E_k(m)$ and ask for a decryption of the apparently unrelated message $y' = y\ E_k(m') = E_k(mm')$, for an arbitrary m'. From $mm' = D_k(y')$ Eve immediately calculates $m = D_k(y')/m'$. This is an example of a "chosen ciphertext" attack in which the adversary chooses a ciphertext, related to the original message, and obtains a decryption.

Note that none of these attacks requires the ability to factor the large integer n.

These are serious concerns. However, practical, if ad hoc, modifications to the concept are well-known, and the RSA system is a cornerstone of real-world cryptography. Indeed, many of the cryptosystems in everyday use in the financial world or on the Internet use the RSA idea in crucial ways. Current belief is that in practice moduli n larger than 2^{1024} are safe.

Other public-key cryptosystems have been proposed in the last 25 years. Many have been shown to be flawed, but another one that has stood the test of time is due to El Gamal, and is basically a modification of a key exchange protocol due to Diffie and Hellman. Since the Cramer-Shoup system is itself a variant of the El Gamal system, we describe the El Gamal system briefly.

Let G be a cyclic group of prime order p and let g be a generator; both G and g are publicly known. We will write the group additively here, so that if n is an integer then ng is the result of adding g to itself n times. The "discrete logarithm" problem (DLP) is to find n, knowing g and ng. (The terminology comes from the case in which G is a subgroup of the multiplicative group $(\boldsymbol{Z}/q\boldsymbol{Z})^*$ of integers modulo a prime.) For some groups it seems reasonable to assume that the DLP is computationally infeasible, and this is related to the security of the system. For a discussion of this, and a discussion of why there can be "different" groups of order p, and a discussion of the phases of the El Gamal system, see the sidebars.

The kinds of breaks described earlier against the naive RSA should certainly impel us to think about the safety of any cryptosystem. In the case of El Gamal this means that we should think about whether the system could be insecure even if the DLP is hard.

(continued on page 10)

El Gamal Cryptosystem

Key Generation: Choose a cyclic group $(G, +)$ of prime order p and a generator g. Choose a secret random integer s in the range $1 < s < p$. The public key consists of $K = (G, g, h)$ where $h = sg$.

Encryption: Choose a random r, $1 < r < p$. The encryption of a message m is

$$E_k(m) = (x, y) := (rg, m + rh).$$

Decryption: $D_k(x, y) = y - sx$.

Remarks: It is easy to verify that D_k is inverse to E_k. The inclusion of the random information r prevents the "information leakage" described for the naive RSA. Note that if the *DLP* is easy for G, then the system is trivially breakable: from rg one could find r and hence $m = (m + rh) - rh$ from the ciphertext $m + rh$ and the public key.

Panorama of Mathematics Conference

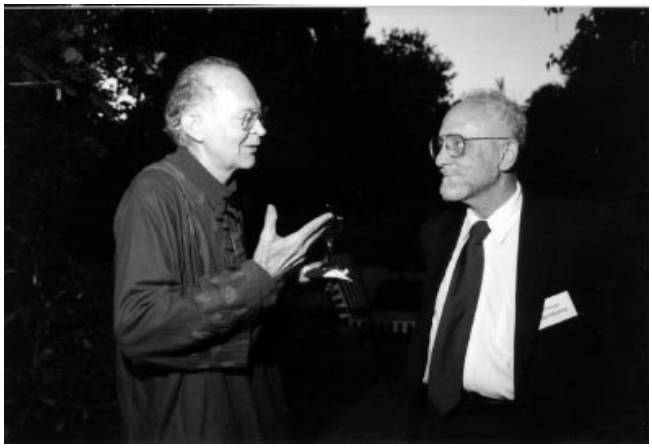
MSRI Honors Geometer S.-S. Chern

Professor Chern in his room while pursuing sudies in Hamburg, 1935.

MSRI hosted its Panorama of Mathematics conference on September 13th-16th with a series of well-attended lectures and heartfelt tribute celebrations honoring Professor Shiing-Shen Chern, one of MSRI's founding directors. It was both an edifying and festive week!

On Thursday and Friday afternoons, MSRI Trustee Robert Bryant, Harvard's S.T. Yau, Institute for Advanced Studies' Director Phillip Griffiths, and MIT's I.M. Singer delivered talks on a wide range of topics related to the work of renowned geometer S.-S. Chern. On Friday morning, Jeremy Gray surveyed the last century of mathematics via the history of the Hilbert problems, and Tom Leighton, the MIT applied mathematician who founded the company Akamai, described his company and some of the mathematical problems on which its success is based. The conference culminated on Saturday with three fascinating public lectures by cryptographer Leonard Adleman, computer scientist Richard Karp, and physicist Brian Greene; these lectures were to a packed house at Berkeley's Andersen Auditorium.

Several social events enhanced the week's activities. Trustees and Academic Sponsors were treated to a dinner honoring Professor Chern at the home of China's Consul General Wang Yunxiang in San Francisco. The next evening, MSRI friends Ed and Rosemary Baker hosted an elegant dinner — with Chern once again the guest of honor — for board members and friends of MSRI at their home in Piedmont to kick off the board phase of MSRI's anticipated capital campaign for a new lecture hall and expanded library.



Donald Knuth (left) and Elwyn Berlekamp (right) discuss the lectures presented earlier that day at the conference.

At Ed and Rosemary Baker's home, Professor Shiing-Shen Chern greets guests Nathaniel and Laura Simons (son and daughter-in-law of trustee Jim Simons) who extend their congratulations on the success of the "Panorama of Mathematics" conference.

At home, August 2000.

Physicist Paul Chu (left) and National Science Foundation Director of the Division of Mathematical Sciences Philippe Tondeur (right) discuss the future of mathematics and MSRI.

Professor Chern lecturing in China, 1987.

(Left to right) MSRI Deputy Director Joe Buhler, Consul General Wang Yunxiang, MSRI Director David Eisenbud, and Hendrik Lenstra.

China's General Consul Wang Yunxiang presents Professor Chern with a plaque to commemorate his return to that nation and his continuing support of Chinese mathematicians.

Hostess Rosemary Baker (left) engaged in conversation with dinner guests Johnson Cha, Acting Deputy Director Michael Singer and Leilani Grinold.

MSRI's Board Chair Dusa McDuff is welcomed by Friend of MSRI and host Ed Baker.

Cramer-Shoup Encryption

(continued from page 7)

Cyclic groups

It may sound silly to talk about choosing a cyclic group of order p, since there is only one such group up to isomorphism. However, for algorithmic purposes, group elements must be represented as bit strings. The choice of this representation, and the difficulty of the algorithm for the group operation, can be crucial. This can be illustrated by the following three instances of a group, together with a representation of group elements by bit strings and a group operation algorithm.

Suppose that the group G is the group $\boldsymbol{Z}/p\boldsymbol{Z}$, where the elements are represented as the standard binary representations of the integers $\{0,1, \ldots, p\text{-}1\}$. Addition is done modulo p in the usual way. The DLP is easy to solve in this group: if G is an arbitrary generator then it easy to use Euclid's algorithm to determine n (modulo p) from ng and g.

Let q be a prime and let G be a cyclic subgroup of order p of the multiplicative group $(\boldsymbol{Z}/q\boldsymbol{Z})^*$. (For instance, if $p = (q\text{-}1)/2$ is prime, we can take the subgroup of index 2.) Elements of the group are represented as binary expansions of integers x, $1 \le x < q$. The DLP is now a standard example of a hard problem for which no polynomial time algorithm is known; the DLP is currently judged to be intractable if p has several hundred decimal digits. For reasons not fully understood, the DLP for this group seems to be similar in difficulty to the problem of factoring numbers of approximately the size of p. Sub-exponential algorithms are known, but none are polynomial time.

Finally, G might be a subgroup of the group of points on an elliptic curve over a finite field. In this case the group operation is particularly opaque and no sub-exponential algorithm for the DLP is known. The theory is that security equivalent to the multiplicative group for primes of several hundred digits can be obtained with elliptic curve cryptosystems over fields whose size is between 50 and 80 digits.

This may sound like a daunting task, but we could conceivably hope for a relative proof of security: **if** the system is breakable then an underlying number-theoretic problem is easy.

This is an ambitious goal. In order to prove something like this, we first need definitions! We have to specify what it means to break a system, what computational power we allow the attacker, and what access will be allowed to the system.

First, we limit the attacker's computational power by assuming that a problem is "infeasible" for a realistic attack if it cannot be solved in polynomial time. Of course, if we allow the adversary unlimited computations, then any public-key system can be broken.

Second, we will consider here only "chosen ciphertext attacks" (CCA). Roughly speaking, this means that after the attacker intercepts a message $y = E_k(m)$ she is then allowed to obtain the decryption of many ciphertexts y' subject only to the proviso that $y' \neq y$. This is sometimes said to be an "adaptive" attack since the y' can be chosen after the attacker has seen y.

Finally, we say that an attacker has broken the system if she can say anything non-trivial about the encrypted messages! For instance, if she could guess whether m was the all-zero message with probability significantly different from one-half. Or if she could distinguish between $E_k(m_0)$ and $E_k(m_1)$ with probability significantly different from one-half.

This is a remarkably strong notion of security, widely thought to be as strong as is necessary in the real world. It incorporates all known attacks and vulnerabilities. For instance, it has been proved that a system secure against CCA does not leak any information about messages, and is non-malleable.

The system due to Cramer and Shoup has two properties not possessed by any previous cryptosystem: it is reasonably efficient (not only in the theoretical sense of requiring polynomial time, but also in practical terms), and it allows one to prove that if a certain number-theoretic problem is hard then the system is secure against adaptive chosen ciphertext attacks.

The number theory problem is a somewhat easier problem than the DLP, namely the Decisional Diffie-Hellman problem (DDH). Roughly speaking, the problem is: given ng, $n'g$, and $n''g$, determine whether $nn' \equiv n'' \bmod p$. (As above, G is a group of prime order p, and g is a generator of G; n, n', and n'' are integers.) If one can solve the DLP then one can solve the DDH, but possibly not conversely. Thus, assuming that the DDH is hard is stronger than assuming that the DLP is hard. However, for suitable groups no attack is known for either problem.

The Cramer-Shoup system is given in a sidebar. It is an extension of the El Gamal system. Basically, the extension allows ciphertexts to contain an embedded authentication; the idea is that useful CCA attacks have to modify ciphertexts in useful ways, and the embedded authentication should make it infeasible to modify the ciphertext without knowing the original plaintext. The proof that this is the case shows how to use an assumed break of the system to solve instances of the DDH problem, and one key component of this is that the authentication information in the ciphertext limits what can be learned from decryptions.

Several other schemes have been proposed that have some of the features of the Cramer-Shoup system. For instance, there are proposals in [DDN] that provide security against CCA, but are impractical. Several other schemes have been proposed that have potential resilience against CCA, but no proof of security is known.

Does the Cramer-Shoup system solve all our cryptographic problems? Not really.

From a theoretical point of view, there is the nagging fact that the security proof is relative --- we need to assume that the DDH is hard. This is annoying, but seems to be unavoidable at the moment since no one has any ideas on how to prove lower bounds on the difficulty of the number theory problems that are involved. For instance, it is quite conceivable that efficient algorithms will be discovered for factoring, or for solving the DDH or DLP. It is also conceivable that the DDH will be easy for some groups even if the DLP is hard. In any event, the difficulty in proving lower bounds

on time required for any algorithm for a given problem is notorious, and is illustrated by our famous inability to prove that $NP \neq P$. It should also be noted that several of the number-theoretic problems here are definitely not *NP*-complete if $NP \neq P$ so that, whether or not they can be solved in polynomial time, they are not likely to be as hard as *NP*-complete problems.

From a practical point of view, some would complain even more vigorously. It is arguable that nothing has been gained. The Cramer-Shoup system takes about twice the time of the El Gamal system, which is already a little less efficient than RSA-based systems. In addition, the key sizes and message sizes are significantly larger. It is quite possible that the chance that the Cramer-Shoup system is truly stronger than the El Gamal system is less than the chance that the DLP and the DDH are easy and both systems are weak.

From these points of view, the amount of practical security that has been obtained is not entirely clear.

One counterargument to this is that an apparently strong practical system, called PKCS#1 and based on the RSA system, was unexpectedly shown to be vulnerable to a CCA [Bl], without any corresponding attack on the RSA system. It was easy to devise a fix to the system, but this vulnerability is a sobering reminder about the difficulty of providing security in the real world. This particular difficulty would have been avoided by a system that was proved to be secure against CCA.

Cramer-Shoup Cryptosystem

Key Generation: Choose p and G as in the El Gamal system, and choose generators g and g'. Choose a collision-resistant hash function (see below) H that is maps bit strings to integers between 0 and p. Choose random integers (s, t, t', u, u') between 1 and p. The public key is $K = (G, g, g', h, k, k')$ where $h = sg, \quad k = tg + t'g', \quad k' = ug + u'g'$.

Encryption: To encrypt a message m, choose a random r; calculate $n = H(S)$ where S is the concatenation of the bit strings representing rg, rg', and $m + rh$. Set

$$E_k(m) = (x, y, z, w) := (rg, rg', m + rh, rk + (rn)k').$$

Decryption: To decrypt (x, y, z, w) calculate $n = H(S)$ where S is the concatnation of x, y and z, and check that $(t = nu)x + (t' + nu')y = w$.

If this is true, output $D_k(x, y, z, w) = z - sx$.

Remarks: The verification that decryption inverts encryption is more involved here, but is mechanical. The "certification" step prevents an attacker from sending arbitrary ciphertext for decryption. The hash or "message digest" function $H(x)$ maps arbitrary bit strings to bit strings of a fixed size. It suffices to assume that it is "collision-resistant" in the sense that it is infeasible to find two inputs with the same output. As explained in [CS] use of a hash function can be removed at the cost of complicating the scheme.

In any event, cryptography is a wide-open field at the moment. The connections between number theory and cryptography will continue to grow, and it seem plausible to hope that the narrowing between theory and practice illustrated by Cramer-Shoup might continue; in any case, there will be much work in the near future, and continuing tension between all sorts of views.

Remarks:

The original Cramer-Shoup system is given in [CS]; improvements (using a weaker number-theoretic assumption) are given in [Sh2]. An expository account is given in [Sh1]. Non-malleability was first defined, and achieved, in [DDN]. More recent work of Shoup, [Sh3], shows unanticipated weaknesses in security proofs. Historical and political discussions of cryptography can be found in [Kahn], [Bauer], [Singh], [DL]. Book-length treatments of aspects of theoretical cryptography can be found in [Luby] and [Goldreich]. Numerous practical aspects of cryptography are covered in [Schneier]. I have profited from useful comments on earlier drafts of this article from Danalee Buhler, Cynthia Dwork, David Eisenbud, Arjen Lenstra, Michael Singer, and Victor Shoup, even when I (obtusely) chose to ignore them.

References:

[Bauer] Friedrich Bauer, *Decrypted Secrets*, Springer Verlag, 1997.

[Bl] Daniel Bleichenbacher, *Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1*, in Springer Verlag LNCS vol.1462, Eurocrypt 1998, 1-12.

[CS] Ronald Cramer and Victor Shoup, *A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack*, in Springer LNCS vol.1462, Eurocrypt 1998, 13-15.

[DDN] Danny Dolev, Cynthia Dwork, and Moni Naor, *Non-malleable cryptography*, in 23rd Annual STOC, 1991, 542-555, and the final version in SIAM J. Comput., v. 30, 391-437, 2000.

[DL] Whitfield Diffie and Susan Landau, *Privacy on the Line. The Politics of Wiretapping and Encryption*, MIT Press, 1998.

[DN] Cynthia Dwork and Moni Naor, Streaming video of a Short course on the foundations of cryptography, October 14-15, 2000; http:/www.msri.org

[Goldreich] Oded Goldreich, *Foundations of Cryptography: Basic Tools*, to appear.

[Kahn] David Kahn, *The Codebreakers*, revised edition, Scribners, 1996.

[Luby] Michael Luby, *Pseudorandomness and Cryptographic Applications*, Princeton University Press, 1996.

[Schneier] Bruce Schneier, *Applied Cryptography*, John Wiley & Sons, 1996.

[Sh1] Victor Shoup, *Why Chosen Ciphertext Security Matters*, IBM Research Report RZ 3076, November, 1998.

[Sh2] Victor Shoup, *Using Hash Functions as a Hedge against Chosen Ciphertext Attack*, in Springer LNCS vol.1806, Eurocrypt 2000, 275-288.

[Singh] Simon Singh, *The Code Book*, Random House, New York, 1999.

Notes from the Director

(continued from page 1)

A special feature this fall was that the two Introductory Workshops were run as Clay Mathematics Institute events, and completely funded by CMI. The generous funding allowed us to add features that are unusual in our programs, to say the least: we rented the Monterey Aquarium for a dinner for Algorithmic Number Theory, while the Operator Algebra folks enjoyed a cruise on the Bay. There were plenty of students at these programs, the level of the talks seemed perfect, and the participants seemed both to learn a lot and to have a good time.

Early in September, just after the dust of the Introductory Workshops had settled, we hosted a three-day event called "The Panorama of Mathematics", in honor of our founding director, Shiing Shen Chern. The range of talks was very wide; you can get a sense of it from the program on our web site. A special Saturday event, "Mathematics Across The Sciences," reached beyond the mathematical community to a much broader audience. Leonard Adleman (the "A" in "RSA") spoke on DNA computing and the adventures and misadventures in his lab ("If the DNA computer doesn't do what it should, try throwing in a handful of salt"); Richard Karp surveyed the tremendous mathematical challenges that remain in dealing with our burgeoning knowledge of the genome; and Brian Greene wowed a packed house with his amazing blend of showmanship and genuine education. (As usual, you can find most of the conference in streaming video on our website.)

Chern has now returned to the Nankai Institute of Mathematics, which he also founded. I recently visited him there during a conference he organized in memory of the Chinese mathematicians Chow and Chen. I had never had the opportunity of meeting Chow, and his name is used so often in Algebraic Geometry (Chow forms, Chow varieties, Chow groups, ...) that I had come to think of “Chow” as an adjective rather than a proper noun. My own mathematical work lately has had a lot to do with Chow forms, but it took a moment for me to bridge the gap from name to man, and realize that I had a perfect subject for a talk in this conference! A highlight of the conference was an audience with China's President, Jiang Zemin, that Chern arranged for some of the participants.

Gang Tian and David Eisenbud standing behind Shiing-Shen Chern and Chinese President Jiang Zemin (photo taken from a Chinese television broadcast).

I'm truly delighted to finish a story whose progress I've reported in every Emissary since I became Director, three and a half years ago: MSRI HAS SIGNED ITS COOPERATIVE AGREEMENT WITH THE NSF! This agreement is the final step of the recompetition. It secures our major operational funding for the next five years, after which, if all goes well, there may be a non-competitive renewal. This victory was made possible by the support of the mathematics community---you---expressed in innumerable ways. I'm proud of this vote of confidence, from the community and from the NSF, in the work being done by MSRI.

As for future renewals, there is a significant expectation: the NSF requires that MSRI demonstrate serious progress toward identifying new sources of funding, and toward decreased dependence on the NSF. With this mandate the Board of Trustees and I have focused on exploring ways in which MSRI can increase its individual, corporate and foundation support.

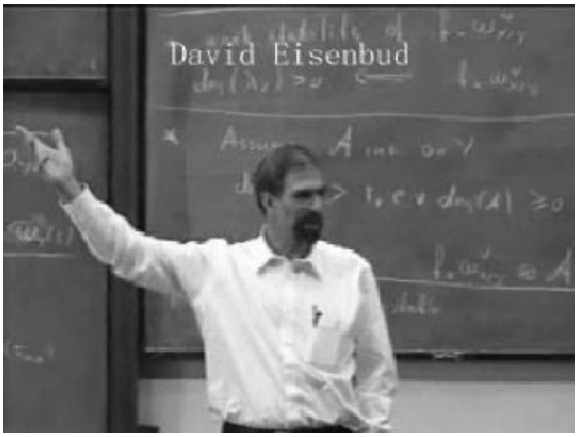
I firmly believe that a wider base of support for MSRI will strengthen the Institute, nurture its growth, and ensure its leadership position in the mathematical community. The NSF has been a steadfast and generous patron, and I believe it will continue to be. However, in the long run, heavy dependence on a single source of funding would not allow the Institute to grow and develop in accordance with the needs of the mathematical community. MSRI has already gone from 100% dependence on the NSF core grant in its early days, to now receiving about 30% of its funding from other sources.

Many valued things that MSRI does for the mathematical community are not eligible for support from our NSF core grant. Funding from private sources allows us the freedom to launch such important activities as our Journalist-in-Residence program and the events we offer to inform the public about the value of mathematics to society at large. Nongovernmental funding also supports this newsletter and, not by any means least, our much-anticipated (and scientifically indispensable!) daily teas. On a larger scale, the NSF has made it clear that the necessary major improvements to our building must come from private sources. To ensure all these programs central to our mission of supporting mathematics, we need to continue to develop a wide range of private support.

I am confident that we will be able to satisfy the funding expectation set forth by the NSF. A number of elements are already in place:

- This summer, we received a [matching] gift of $2.5 million from the Simons Foundation, in anticipation of a campaign that will allow us to improve our building, double the size of our library, and add a world-class lecture hall. Stay tuned for a future Emissary article outlining the building plans.

- Significant individual gifts have also been made to a separate Investment Fund, which currently stands at about $3 million. This fund will one day become MSRI's permanent endowment, whose interest income will contribute to the Institute's ongoing programs.



David Eisenbud lecturing at the Nankai Institute of Mathematics in China (photo taken from a Chinese television broadcast).

• MSRI currently has 14 Corporate Affiliates who make significant contributions to the Institute. This corporate support has grown rapidly in the last three years, and I am confident that it will continue to do so.

•Now that our Board of Trustees has approved a major development program, the Institute is ready to seek increased individual and foundation support. We are excited about the increasing number of MSRI's friends who are contributing to our efforts. Their support demonstrates wonderful commitment to MSRI's goals, and we are enormously grateful to them.

If you have supported MSRI in the past, we thank you! I hope that you will consider continuing your support this year. If you would like to support the activities of the Institute but have not yet done so, I hope you will! In either case, I would like to direct you to the envelope in the center of this newsletter and ask you to consider joining the growing number of contributors who will make such a difference in what MSRI is able to do this year.

Hearty thanks for your interest and best wishes of the season!

Loving a Mathematician

for Sherman

The ether, or whatever's up there--
some infinite glassy staircase--
crackles for you
with truth, with beauty--and I
have never followed you even to
the second rung. I used to think Pi
was just a way of measuring circles.
You tell me now that Pi dwells
in gaseous, in liquid universes
where there are no circles, where rings
couldn't form if I dropped a pebble.
For there are no pebbles either--
no discs no balls no equators,
only pure structure.
It's true, you say,
that Pi always turns up,
like an old irrational uncle
who's been traveling round the country
doing card tricks. But circles
are only one of his arts:
Pi rolls his thumb through the ink
of odd numbers; from his hiding place in
square roots under square roots like
a wagonload of deviant potatoes
Pi shines traces beyond
the galaxies mathematicians map,
haunts the void between electrons,
stalks black holes and red shifts.
Inching like a growing crystal
into cosmic chinks, Pi waits
for thought to close in, waits
to be pounced on with a pencil
as his secrets repercuss
into patient, searching minds.
I ask you this: does Pi buckle
the whole universe together?
Can Pi be God?

For the first time I believe
I could follow you up and up--

Hannah Stein

This poem, dedicated to the author's husband Sherman Stein, appears in her collection of poetry Earthlight, *La Questa Press, 2000, © Hannah Stein.*

MSRI thanks former Cartoonist-in-Residence Larry Gonick for the artwork on page 13 and on the back cover.

Problem Corner

Elwyn Berlekamp (berlek@math.berkeley.edu)
Joe Buhler (jpb@msri.org)

One of the fun parts of doing mathematics is standing around and talking to colleagues about puzzles and conundrums. Here are some problems that were discussed at MSRI this fall.

1. (a) A unit cube is cut in half by a saw cut that is perpendicular to its long diagonal. What is the shape of the cross section of the cut?

(b) Generalize to n dimensions.

Comment: The question came up recently in connection with a problem in the geometry of numbers; the 3-dimensional case is well-known.

2. You owe your friend 62 cents, but have only a (fair) dollar coin. Devise a sequence of coin flips which has the property that he wins the dollar coin exactly 62% of the time.

Comment: John Conway described a practical and elegant scheme to solve this problem, which can come up in practice in settling a bill at a restaurant when no one has change.

3. Suppose that n players shoot at bins labeled 1, 2, 3, ... and hit bin k with probability 2^{-k}. Let p_n be the probability that there is a unique shot in the highest numbered bin that was hit. Prove that p_n is not a monotone function of n and that in fact the limit

$$\lim_{n\to\infty} p_n$$

does not exist.

Comment: This problem was suggested by Carl Pomerance; generalizations are discussed in a paper by undergraduate authors in a new online journal: Integers: Electronic Journal of Combinatorial Number Theory, volume 0, *Number Theory, Balls in Boxes, and the Asymptotic Uniqueness of Maximal Discrete Order Statistics*, by Jayadev S. Athreya and Lukasz M. Fidkowski.

4. Let $a(n)$ be the number of digits in 2^n, in its usual decimal expansion, that are bigger than or equal to 5. Evaluate

$$\sum_{n=1}^{\infty} \frac{a(n)}{2^n}.$$

Comment: The problem was given to us by Hendrik Lenstra, who tells us that it is a well-known conundrum with a surprisingly nice answer.

5. A mathemagician has an audience select five numbers from the set $\{1, 2, \ldots, n\}$. (The case of $n = 52$ is of course of special interest.) The mathemagician thinks carefully about the five numbers and then names four numbers, and asks an audience member to write those four numbers, in that order, on a blackboard. (The audience contains no shills, i.e., people who collude with the mathemagician.)

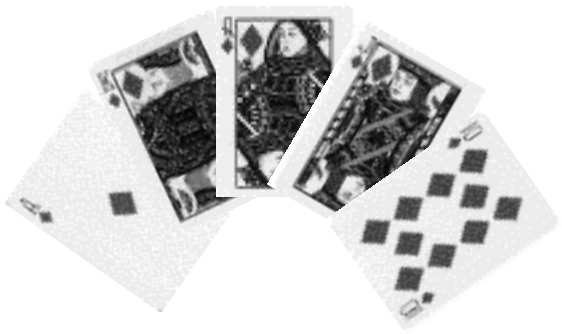
The mathemagician then leaves the room and a partner, who has been oblivious to the proceedings so far, is summoned to enter the room through a different door. After announcing that "numbers naturally come in sets of five, so that the outlier can be determined from the remaining four," she studies the four numbers on the board and correctly announces the fifth number in the original collection.

How can this be done when $n = 52$?

What is the maximum value of n for which this is possible, no matter what 5-element subset is chosen?

Devise practical algorithms for the two mathematicians so that this trick could actually be performed.

Comment: This has been discussed in several forums in recent years; there are several known solutions for $n = 52$, and those have been applied in the real world. Considerable ingenuity is required to come up with a practical scheme for the maximum value of n, and the only known solution requires some practice if your goal is to perform the trick.



Semester and Year-long Programs

Fall 2000-Spring 2001	**Operator Algebras**
Fall 2000	**Algorithmic Number Theory**
Spring 2001	**Spectral Invariants**
Summer 2001	**The Global Theory of Minimal Surfaces**
Fall 2001	**Integral Geometry**
Fall 2001	**Inverse Problems**
Spring 2002	**Infinite-Dimensional Algebras and Mathematical Physics**
Spring 2002	**Algebraic Stacks, Intersection Theory, and Non-Abelian Hodge Theory**

2000-2001 Events

August 14-23	**Clay Mathematics Institute Introductory Workshop in Algorithmic Number Theory**
August 24-September 1	**Clay Mathematics Institute Introductory Workshop in Operator Algebras**
September 14-16	**The Panorama Of Mathematics** (see Special Events)
September 25-29	**NATO Advanced Research Workshop: Simple C*-Algebras and Non-Commutative Dynamical Systems**
October 14-20	**Number-Theoretic Cryptography**
October 19	**Code Breaking in World War II, the Enigma, the Colossus, and Bletchley Park** (see Special Events)
November 5-10	**Emerging Applications of Combinatorial Design**
December 4-8	**Subfactors and Algebraic Aspects of Quantum Field Theory**
December 11-15	**Arithmetic Geometry**
January 22-26	**Free Probability and Non-Commutative Banach Spaces**
Feb 9-11	**The Preparation of Math Majors in the First Two Years: A Curriculum Policy Workshop**
March 1-3	**Analysis, Models and Methods: A Conference in Memory of Fred Howes**
March 12-16	**Geometric Aspects of Spectral Theory**
March 19-29	**Nonlinear Estimation and Classification**
March 30-April 1	**Randomized Algorithms in Finance**
April 23-May 2	**Quantization and Non-Commutative Geometry**
May 7-11	**Geometric Scattering Theory and Elliptic Theory on Noncompact and Singular Spaces**
May 29-June 1	**The Continuum Hypothesis**
June 4-15	**Summer Graduate Program I: The Mathematics of Modern Signal Processing**
June 25-July 28	**Summer Graduate Program II and Microprogram: The Global Theory of Minimal Surfaces**

Governance Committees

In 2000, the Board of Trustees elected six new trustees: **Johnson M. D. Cha** *(C. M. Capital Corporation)*, **David Hodges** *(UC Berkeley)*, **Barry Mazur** (*Harvard*) **Robert Megginson** *(University of Michigan)*, **Sandor Straus** *(Merfin LLC)*, and **Chang-Lin Tien** *(UC Berkeley)*.

The Board elected **James Donaldson** (*Howard University*) and **Carolyn Mahoney** *(Elizabeth State University)* to the Human Resources Advisory Committee (HRAC).

Finally the Board elected **Stuart Geman** (*Brown University*), **Michael Hopkins** *(Massachusetts Institute of Technology)* and **Richard Stanley** *(Massachusetts Institute of Technology)* to the Scientific Advisory Committee (SAC).

Corporate Partners

Cylink
Hewlett-Packard Laboratories
Microsoft
Pfizer Corporation

Corporate Affiliates

Affymetrix
Bell Labs/LucentTechnologies
Crabtree Ventures
Fair, Isaac
The Mathworks
Pacific Journal of Mathematics
Sun Microsystems
Waterloo Maple
Wells Fargo
Wolfram Research

Mathematical Sciences Research Institute
1000 Centennial Drive, Berkeley CA 94720-5070
510.642.0143 • FAX 510.642.8609
www.msri.org

Address Correction Requested

Come to the reception at the January 2001 AMS meeting.
Wednesday, Jan. 10, 2001
5:30 - 7:30 pm
Waterbury Room,
Sheraton New Orleans

Mathematical Sciences Research Institute