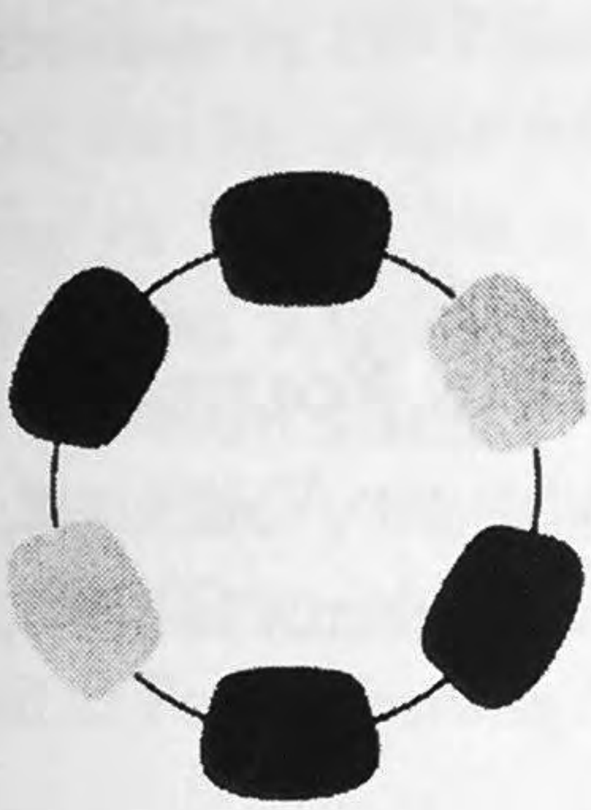
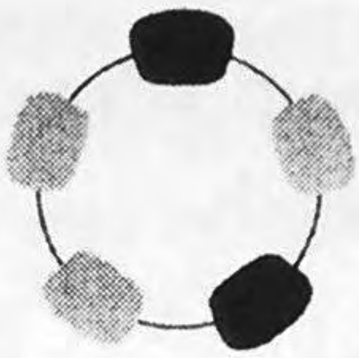
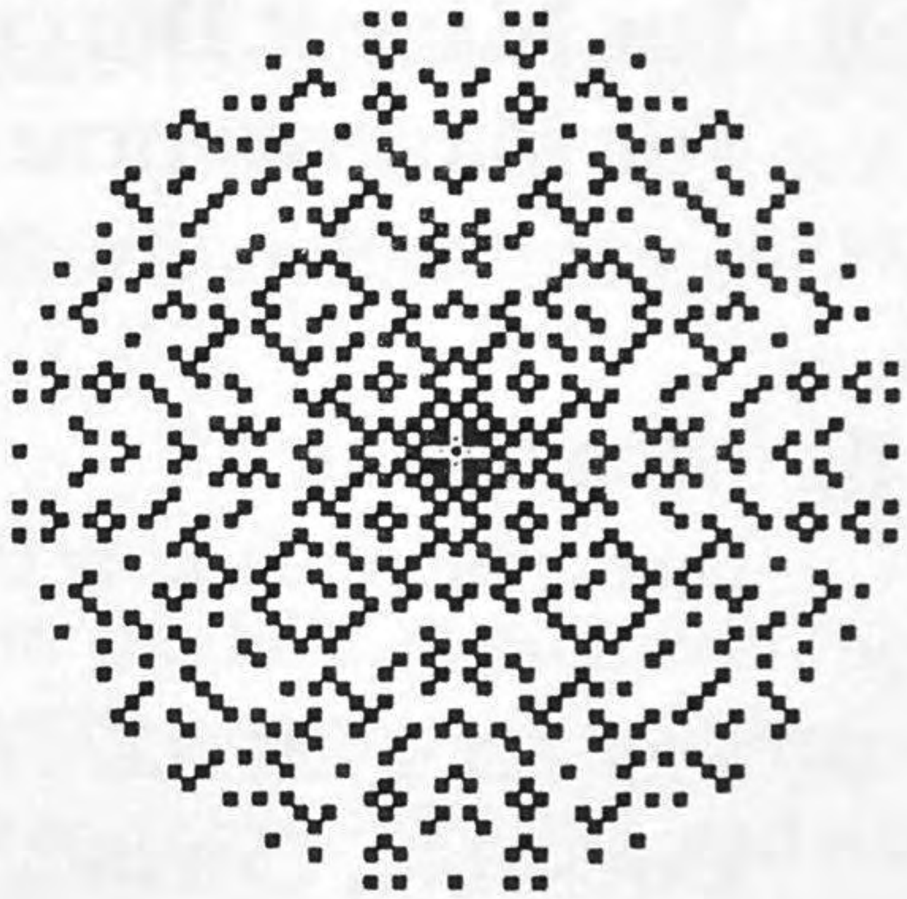
NUMBERS IN ACTION*

***A Mary P. Dolciani Halloran Foundation Mathematics Program**





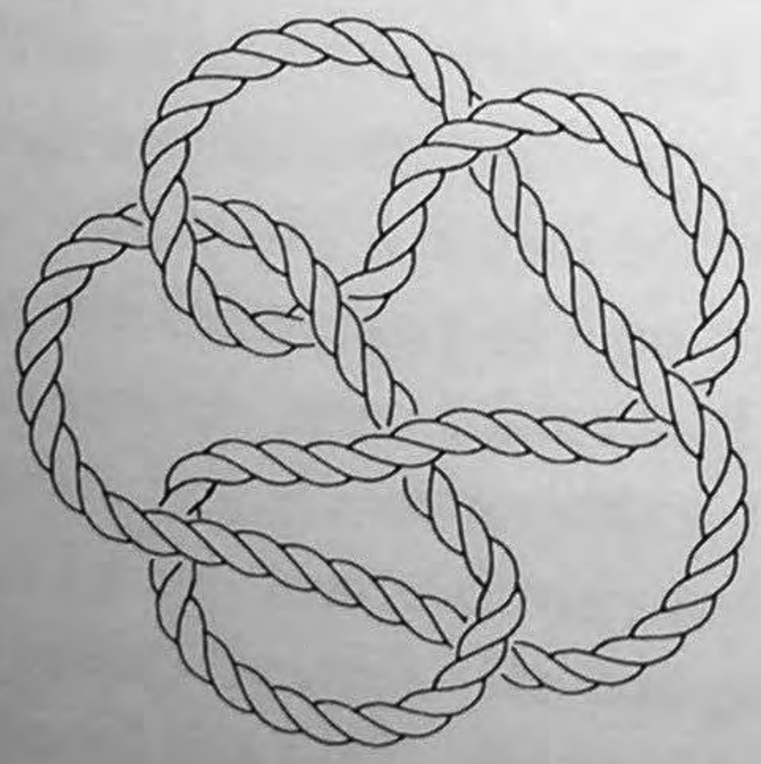


Sponsored by the

Mary P. Dolciani Halloran Foundation
and the Mathematical Association of America

Presented by the

Mathematical Sciences Research Institute



2050 Valley Life Sciences Building
University of California, Berkeley
Monday, December 4, 1995
4-6 p.m.

The Program

I. **Introduction and Welcome**
Robert Osserman, MSRI

II. **The Mary P. Dolciani Halloran Foundation**
The Mathematical Association of America
Donald J. Albers, Associate Executive Director of MAA

III. **Moderator**
Lenore Blum, Deputy Director, MSRI

IV. **Fermat's Little Theorem:**
Counting, Coding, and Computing
Hendrik Lenstra, UC Berkeley

V. **Prime Time**
Ellen Gethner, MSRI

VI. **Numbers and Knots**
John Conway, Princeton University

VII. **Question and Answer Period**
Lenore Blum

VIII. **Closing Remarks**
Robert Osserman

The Speakers

Hendrik W. Lenstra, Jr.

Hendrik W. Lenstra, Jr. is a Professor of Mathematics at UC Berkeley. Lenstra received his Ph.D. in Mathematics from the University of Amsterdam in 1977, immediately joined its faculty as Assistant Professor, and became a full Professor in 1978. He joined the Berkeley faculty in 1986. He is a member of the Royal Dutch Academy of Science and a recipient of the 1993-94 Miller Research Professorship in Mathematics. Lenstra is known for his work in algebraic number theory and algorithms. In 1985 he was awarded the Fulkerson Prize of the American Mathematical Society and the Mathematical Programming Society.

Ellen Gethner

Ellen Gethner received her Ph.D. in the field of Number Theory from Ohio State University in 1992. She was an Assistant Professor of Mathematics at Swarthmore College from 1992-1994, and is currently a Postdoctoral Fellow at the Mathematical Sciences Research Institute. She enjoys being a "communicator of mathematics."

John Conway

John Conway was born in Liverpool, England, on December 26, 1937.

He is currently the John Von Neumann Professor of Mathematics at Princeton University and was a Fellow of Gonville and Caius College and a former fellow of Sidney Sussex College, Cambridge. He is a Fellow of the Royal Society and was a Reader in Pure Mathematics at the University of Cambridge. He has held visiting professorships at several universities and has made original contributions to many branches of mathematics, notably in transfinite arithmetic, the theory of knots, many-dimensional geometry, and the theory of symmetry (group theory). He has published three books, *Regular Algebra and Finite Machines, On Numbers and Games, and Winning Ways*.

More Action

Write a program for your computer that computes the remainder of a^m upon division by k, when a, m and k are positive integers.

Use the program to verify that 2^{341} leaves remainder 2 upon division by *341*, even though *341* is not prime.

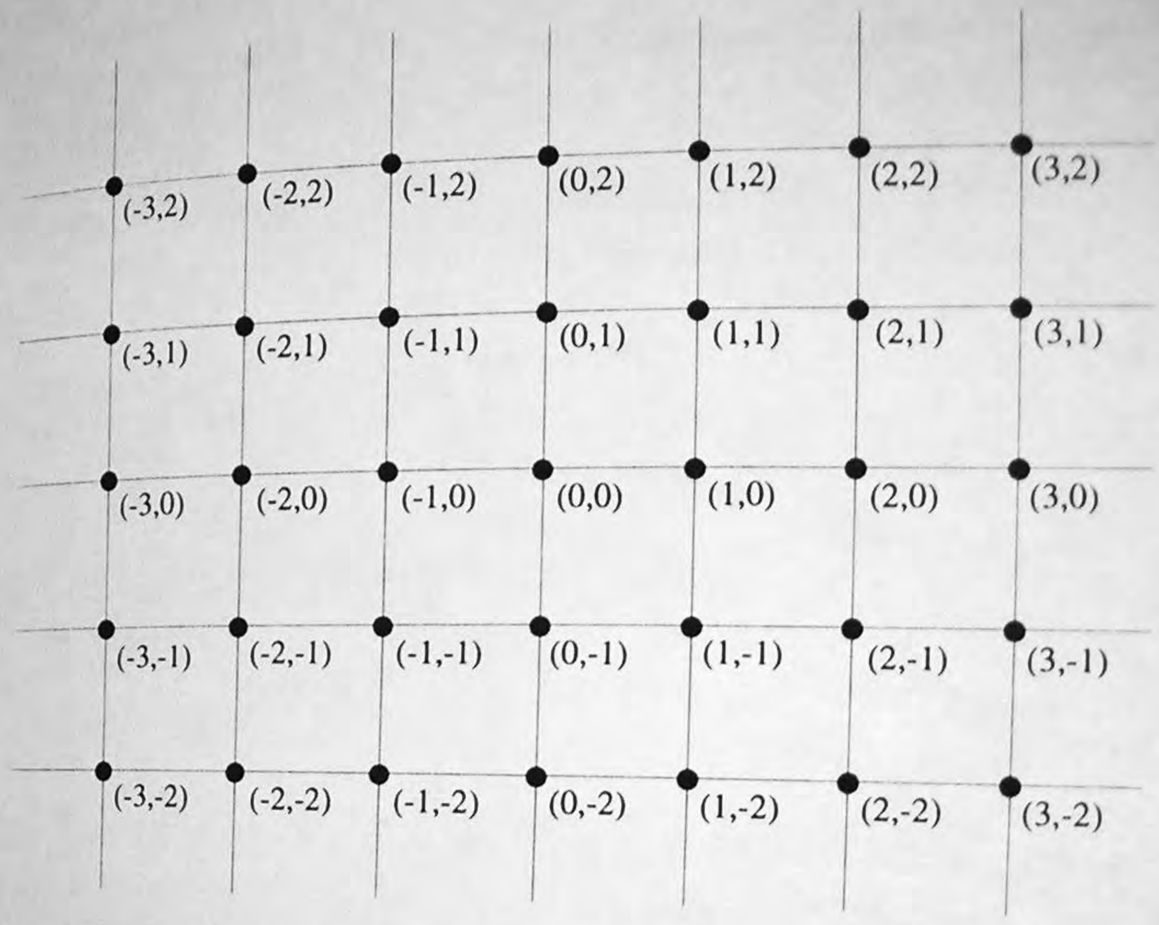
For more on coding, see the books *Cryptology* by Albrecht Beutelspacher, MAA 1994, and *A Course in Number Theory and Cryptography* by Neal Koblitz, Springer-Verlag 1994.

The counting numbers, sometimes known as natural or whole numbers, are 1,2,3,4,5,... and so on, forever. An interesting subset of the whole numbers is the set of prime numbers. What is a prime number? A prime number (or just "prime" for short) is a number which is divisible only by 1 and itself, like 2,3,5,7,11,13,..., and so on, forever (why forever!?). Another way of describing a prime number is to say that a number is prime if it can't be written as the product of smaller whole numbers.

Problem 1: Two primes are twins if they only differ by 2, like 3 and 5, 5 and 7, 11 and 13, 17 and 19, *etc.* Can you explain why no prime except 5 is twins with two different primes?

The "integers" are the whole numbers together with zero and the negative numbers, -1,-2,-3,-4,-5,... and so on, forever.

Now let us take a broader perspective on the idea of "number" and of "integer" as Carl Friedrich Gauss did 200 years ago. Gauss's numbers, called "Gaussian Integers" are pairs of integers like (7,12), (-2,7),(13,6),(-206,10027),..., and so on, forever. The picture of all of the Gaussian integers is too large to fit on this page (there are infinitely many Gaussian integers!), but a small portion of the picture is shown on the next page, and is a grid made up of many small squares.



Another way of describing the Gaussian integers (and this is what Gauss himself did) is to write, for example, (2,3) as 2+3i and (1,4) as 1+4i where $i^2=-1$. Then multiplying Gaussian integers is just as you think it should be. That is, (2,3) ¥ (1,4) is

$$(2+3i) ¥ (1+4i)=2+8i+3i+12i^2=-10+11i$$

(or (-10,11)). The general method for multiplying two Gaussian integers, say (a,b) and(c,d), is the same as above:

$$(a+bi) ¥ (c+di)=ac+adi+bci+bdi^2=ac-bd+(ad+bc)i$$

(or (ac-bd,ad+bc)). Once we have this method, it makes sense to talk about Gaussian primes. That is, a Gaussian integer is a Gaussian prime exactly when it can't be written as a product of "smaller" Gaussian integers, where "smaller" means closer to the origin, (0,0). (This amounts to the condition that (a,b) is smaller than (c,d) if $a^2+b^2<c^2+d^2$).

There is a nice trick for determining exactly when a Gaussian integer is prime. Suppose someone hands you the Gaussian integer (5,2) and wants to know if this number is a Gaussian prime. What to do? You first compute $5^2 + 2^2 = 25 + 4 = 29$, and check to see if the result is a (regular) prime. In this case, 29 is prime, so you're in luck—(5,2) is a Gaussian prime. This trick works on all Gaussian integers (a,b) as long as neither one of a nor b is zero. That is, given a Gaussian integer (a,b), compute a^2+b^2. The result is a (regular) prime precisely when (a,b) is a Gaussian prime.

Problem 2: Which of the following Gaussian integers are Gaussian primes?

a) (2,-3) b) (5,10) c) (-1,1) d) (3,1) e) (-10,1)

Problem 3: If (a,b) is a Gaussian prime satisfying $a^2 + b^2 = p$, explain why one of a or b must be even, and the other odd (as long as p is not 2).

Problem 4: If (a,b) is a Gaussian prime satisfying $a^2 + b^2 = p$, explain why the prime p is exactly 1 greater than a number which is divisible by 4 (as long as p is not 2).

Problem 5: Find as many Gaussian primes (a,b) as you can such that

a) $a^2 + b^2 = 17$ b) $a^2 + b^2 = 101$ c) $a^2 + b^2 = 809$ d) $a^2 + b^2 = 3229$

Explain why if you've found one Gaussian prime, you can find seven more provided that neither a nor b is 0. Does your answer to a)-d) lead you to any guesses about what might be true in general for Gaussian primes?