MECHANIZED MATHEMATICS

D. H. LEHMER

It is indeed an honor to be invited to this platform. One has only to read the names of my distinguished predecessors to realize that, as the saying goes, I have thirty-seven acts that are hard to follow. As a mostly pure mathematician my concern is increased when I note that thirty-two of the lectures have dealt with applications of mathematics to other sciences. The true desperation of my predicament becomes apparent when I tell you that I plan to discuss the application of science to mathematics.

I am convinced, however, that if Professor Gibbs were with us today he would be among the first to endorse the application of mechanical devices to the better understanding of pure, as well as applied, mathematics. To support this conviction I should like to call your attention to a bit of mathematical history of the turn of the century, having to do with Gibb's discovery of the phenomenon that now bears his name. In 1898 Michelson and Stratton, at the University of Chicago, completed the construction of their big 80 term harmonic analyzer and published drawings of some of its output in Philos. Mag. One of these is a graph of the function

$$F_{80}(x) = 2\sum_{n=1}^{80}(-1)^{n+1}\frac{\sin nx}{n}.$$

As we all recall, the corresponding infinite series is the Fourier series of the sawtooth function

$$y = \begin{cases} x & \text{for } -\pi < x < \pi, \\ 0 & \text{for } x = \pi, \end{cases}$$
$$y(x + 2\pi) = y(x).$$

Michelson's graph of $F_{80}(x)$ showed a sort of fluttering as x approaches π resulting in a nine percent overshoot of the expected value. Michelson knew that his instrumentation was better than this and he must have felt that not mechanics but mathematics was to blame. At any rate he wrote a rather petulant letter to Nature (of October 6, 1898) about it. Gibbs made two replies published December 29 and April 27, 1899. Between these dates Gibbs must have taken a closer look at

The thirty-eighth Josiah Willard Gibbs lecture delivered before the Annual Meeting of the Society in Denver on Tuesday January 26, 1965.

the drawings, for in the second letter he corrects his first letter to confirm the overshoot phenomenon, the nine percent being precisely

$$\frac{1}{\pi}\int_0^{\pi}\frac{\sin u}{u}\,du - \frac{1}{2} = .0895.$$

Whatever else the Michelson analyzer may have contributed to the advancement of science, it served to call attention to an interesting anomaly in the theory of Fourier series. We now have a better understanding of this part of mathematics and are forewarned of this behavior elsewhere.

Mechanical aids to mathematics are as old as mathematics itself. The clay tablet of the Babylonians and the papyrus of the Egyptians were simply ancient memory devices used sometimes for computing and recording mathematical results. The sand box of Archimedes is not far behind the blackboard on which so much modern mathematics is created. Rather more mechanical were the ruler and compass, the analogue instruments of the Greeks, and the piles of pebbles and notched sticks, the digital equipment of the same age. With the coming of paper and printing to Europe also came graphics, nomograms, and the slide rule as further analogue equipment. The advent of the calculus (a word which ironically enough refers to pebbles) took most of mathematics down the primrose path of continuity. Nevertheless, one of the inventors of calculus, Leibniz, saw the need for mechanical aid to his newly discovered combinatorial analysis and accordingly invented and constructed a digital instrument, a sort of automatic abacus, which we now recognize as a desk calculator. Two centuries later such machines were to be mass produced, not for the mathematician but for the accountant. By the turn of this century some mathematicians had rediscovered the desk calculator. Tables of logarithms began to collect dust on their shelves while a host of new tables of special functions began to appear in print. The very existence of such tables provided the excuse for other mathematicians to leave their problems solved in terms of special functions. In this way many interesting properties of these functions were discovered, even though their original inspiration was based on some inaccurate little table prepared by what we now condescendingly call hand computing. We owe all this, then, to the accountant. To him and the census taker we owe also the punched card equipment of the early part of this century.

There were some inventions and even constructions of equipment for special mathematical use. On the analogue side one can mention

the planimeter and other integrators, the harmonic analyzer, such as Michelson's, already mentioned. Such mechanical analogue equipment culminated in the Bush differential analyser of 1930, whose components were then gradually replaced by electronic analogues. On the digital side the difference engine of Babbage stands as a forlorn monument to brilliant invention bogged down by the inadequate technology of the 1860's. Much had to be learned about physics before Babbage's ideas for helping mathematics could be realized. A little later Jevons invented a special purpose digital device for formal logic. As far as I know, this was not constructed. Even today we have no special equipment for this purpose.

Mention should be made of the number theory device invented more than 2000 years ago by Eratosthenes and called the sieve. This device appears to have been realized for the first time graphically by Hindenburg in 1776. Up to the early 20th century graphical sieves were used in varying forms for the construction of our large factor tables and for the solution of diophantine equations. The sieve became mechanized in 1927 and photoelectric in 1932.

By the end of the great depression the development of two industries, the telephone and punched card accounting, had advanced the technology of the electromechanical relay to a point where thousands of these devices could be counted upon to operate in harmony with tolerable reliability. It occurred to Aiken and Stibitz that here was a component on which to base a workable realization of Babbage's difference engine. Thus in 1945 emerged two tape driven monsters, the immediate forerunners of our present day electronic computers.

Also during the depression the problem of counting cosmic rays had led to the perfection of another bistable mechanism. This is the electronic flipflop or trigger circuit, used, incidentally, on the photoelectric sieve. Mauchley and Eckert realized that, by putting tens of thousands of such circuits together, they could have an extremely fast computing system with no moving parts. Thus was conceived the first electronic computer, the ENIAC. With its birth in 1947 came a new era to mechanized mathematics, as well as our whole social system. The prodigious speed of the ENIAC, a relatively slow machine by today's standards, made it necessary to abandon the idea of human control or even a punched paper tape control. Authority was surrendered to the machine itself. While this obvious policy was to bring chill to the thoughts of newspaper editors, it had two happy consequences for mathematics: (a) it provided for greater flexibility in the use of the machine, and (b) it made necessary the introduction of certain logical operations or instructions that turned out to be ex-

tremely useful to other branches of mathematics than the mere solution of differential equations.

The last two decades have witnessed, after a slow start, improvements in reliability and speed that are so great they are difficult to appreciate. Reliability, though less noticeable, has increased more than speed. With increased speed has come decreased cost per operation until now, on widely distributed machines, 10000 or more multiplications or 100000 or more decisions can be purchased for one cent. These machines are doing elementary rational and logical operations faster than humans by a factor variously estimated from 10^5 to 10^7. This factor is difficult to comprehend and has been achieved in no other branch of science. Hamming likes to point out that the fastest way one can go from Denver to New York is only about 100 times faster than a brisk walk. If one can do computing five or seven orders of magnitude faster by machine than by hand, it changes one's whole outlook on computing and even the reasons for doing it. Along with increased speed has come the larger sized memories needed to accommodate the larger amounts of internal data required for the solutions of the larger problems that now can be solved in a reasonable time. A modern machine also has a slightly larger repertory of commands than its ancestors of the early 1950's, but almost the same basic structure.

In spite of these remarkable developments and the consequent "computer revolution," the life of the average pure research mathematician goes on nearly undisturbed. There are exceptions however. Some of us are attempting to develop new ways of solving old problems. Back in 1948 Hartree predicted that a new mathematics would emerge from the electronic computer. Although this has hardly come to pass yet, there are a number of techniques in wide use, for example linear programming or Monte Carlo methods, that have now become feasible. However, the requirement of feasibility has never been much of a brake on the imagination of the pure mathematician. In point of fact, the methods used today are often the crudest of those originally proposed for hand computing, just because they are also the most economical.

In a way, Hartree was right: we do have new branches of mathematics whose devotees we can uncharitably call camp followers, since they don't actually use the computer. These branches have sprung up only because electronic computers exist. Branches like cybernetics, artificial intelligence, automata theory, etc. are interesting in their own right and could have been introduced in Babbage's time a century ago. That they are really branches of mathematics is evidenced,

for example, by the fact that an abstract automaton is an ordered quadruplet $[A, B, C, D]$. We observe also the tendency to pass on to the infinite case rather than come to grips with the finite case. But we are getting away from mechanized mathematics.

We were just pointing out that a small number of pure mathematicians have a positive attitude toward the computer. There are others whose attitude is negative. They feel that much of the computing that goes on is ill advised and that it would be better if more effort were spent in the search for new ideas, a point that is very often well taken. I experienced the ultimate in negativity some years ago as an editor of a small computing journal. I received a short paper for publication which contained a value of a fundamental constant computed to some 500 decimal places. In politely rejecting this contribution, I pointed out that a value to some 2000 places had already been published. In reply, the author called my attention to the fact that the earlier 2000 place value was obtained by machine whereas his value was more worthy of publication being a genuine handmade article.

I have already indicated that the average pure mathematician has an indifferent attitude towards the computer. I assume that a majority of those present are either pure mathematicians or have occasional moments of purity in their applied thinking. For this majority the above mentioned attitude needs no explanation. For the few others some words of comment may be needed. Why can't we mechanize most of the mathematics one finds in current periodicals? Why do so few mathematicians sign up for time at the computer center? It is not the language problem since even psychologists and linguists can learn to converse with their computer. It is mostly because the mathematical objects being operated upon are impossible, or nearly so, to explain in complete detail to the digital computer. Also the number of operations that need to be performed is small and quite within the capability of a human being. There is nothing to be gained by executing five logical steps at the rate of 15000 steps per second. To understand the first difficulty a little better, one has only to realize that a digital computer is a finite collection of circuits each capable of a finite number of stable states, usually two; at any clock pulse time there exists in the computer one of only a finite number of state configurations. Finally the computer runs for only a finite time interval, all too short usually, that is, for only a finite number of clock pulse times. All in all, the information content here is finite. But even a number like π contains an infinite amount of information. Hence the computer will never be able to understand com-

pletely such figments of the imagination as real numbers, continuity, derivatives, different kinds of integrals, cosines, areas, infinite products, or even the set of all fibre bundles of a C^* algebra. On the other hand the computer has no trouble with such things as finite geometries, finite fields or positive integers as long as its memory capacity and time allotment hold out. In short, nearly all the things that the mathematician holds dear can only be simulated on the computer. The mathematician is analogue minded and the digital computer is not. There are other difficulties implied by this. Even the basic operations of addition and multiplication on the machine are not what the mathematician is used to, because of the finite width of the arithmetic unit. Addition may give a surprising sum because of overflow. The associative law of multiplication may fail because of round off. The limit

$$\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$$

may be 1, not e, because of floating addition. Of course, such limitations have existed in the desk calculator for some time now. They are only compounded in the automatic version. The real difficulty lies in the fact that only a finite number of angels can dance on the head of a pin, whereas the mathematician is more apt to be interested in the infinite angel problem only.

Well, as every one knows, there is, for the applied mathematician, a way out of all these difficulties. He can try to live with a simulated real number system, a discretized geometry, and a finite difference calculus, fighting against truncation error and round off noise by taking more time and space. Hopefully the conclusions reached by the computer somehow correspond to the right answer to the ideal question with sufficient accuracy for all practical purposes.

But what if there are no practical purposes? What can be done with the function which is 0 when x is rational and 1 when x is irrational? If we are to deal with such matters there is but one way in which we can use the computer. We must compress our infinity of angels into one machine word. The computer can then perform in its finite restricted logic any reasonable finite number of operations on words that stand for infinite sets, just as the mathematician does by hand. Usually this will be inadequate. The mathematician will want the computer to take limits and infinite subsequences and to use the axiom of choice. In such cases he will have to move up in the hierarchy giving his machine words new meanings. All this may be just

too much trouble. Small wonder that most of us would rather be just left to our own devices.

In spite of this display of pessimism, the computer does have a number of roles to play in the development of mathematics. There are two kinds of activities in mathematical research: (a) the improvement of highways between the well-established parts of mathematics and the outposts of the realm, and (b) the establishment of new outposts. Taking up the second activity first, there appear to be two schools of thought on the question of how best to discover new outposts. The most popular school now-a-days favors the extension of existing methods of proof to more general situations. This procedure tends to weaken hypotheses rather than to strengthen conclusions. It favors the proliferation of existence theorems and is psychologically comforting in that one is less likely to run across theorems one cannot prove. Under this regime mathematics would become an expanding universe of generality and abstraction, spreading out over a multi-dimensional featureless landscape in which every stone becomes a nugget by definition.

Fortunately there is a second school of thought. This school favors exploration as a means of discovery, a method much used by such men as Euler and Gauss. By more or less elaborate expeditions into the dark mathematical world one sometimes glimpses outlines of what appear to be mountains and one tries to beat a new path in their direction. Sometimes the hoped for mountains turn out to be merely nearby boulders on an otherwise flat plain. Often the mountains are real enough but too much for us to conquer. New methods, not old ones are needed, but are wanting. Besides the frequent lack of success, the exploration procedure has other difficulties. One of these is distraction. One can find a small world of its own under every overturned stone. A systematic exploration of the world of mathematics would turn it into a classificatory science worse than biology. One has to make judgments about relative importance. One principle here is that a theorem that makes an assertion about an infinite class of mathematical objects is apt to be more important than a proposition about a finite class so that it can be verified in a finite number of cases. There are exceptions however. One of these is the counter example. Untold manhours of futile effort can be saved by a single counter example.

Computers have been fairly successful in the discovery of counter examples, especially in such disciplines as algebra, group theory and the theory of numbers. Once a counter example has been found it

makes no difference whence it came. Anyone can now verify that the proposed theorem is actually false. One can even be ungrateful and fail to mention the computer's contribution to the better understanding of part of mathematics.

Passing on from this example of minimum involvement of the computer, there is next the case in which no counter example is discovered, but instead a large number N of instances of the proposed theorem are verified by the computer. As N increases, the plausibility of the theorem increases, as Polya would say, usually nonlinearly. Although we cannot obtain a rigorous proof this way, there is always a possibility that a careful analysis of many special cases may reveal why the proposition is generally true. Under proper direction, the computer can sometimes be made to carry out this analysis itself. Thus the computer may well be the source of the idea that leads to the desired proof. Again, there is no real need to mention this assistance.

Alternatively, instead of a proposition whose truth value is desired, we may start with a set of mathematical objects such as, for example, division algebras of order 32, and ask the computer to examine them, and make a tabulated report. Most of the fundamental classical theorems of number theory were discovered from the inspection of tabular evidence. Today tables can be produced in such quantities as to render their publication or even, in some cases, their inspection economically impossible. In these latter cases it is a simple matter to ask the computer to do the inspection internally. From the computer's report one can make new conjectures which may have some interest and whose proof may not be too difficult. Again, in publishing our results we need not give credit where some credit is due.

Gibbs once said that algebra is the greatest labor saving device ever invented. Even so, it can be drudgery. Nonmathematicians know better than mathematicians that the digital computer is a powerful tool in dealing with nonnumerical data. This opens the possibility of having the computer do one's algebra for one. This has been going on sporadically since 1950. Codes have been written for carrying out the differentiation of the elementary functions, the manipulation of formal power series, the algebra of rational functions etc. New and more powerful codes for symbol manipulation are promised for the near future. The theory of algebraic invariants was largely abandoned early in the twentieth century because the symbol manipulation involved became humanly unbearable. This kind of drudgery is easy for the computer. With our new hardware and software, interest in parts of algebra may reawaken. In such applications

some credit must now be given to the computer because of its greater responsibility.

Increasing this responsibility still further, let us discuss briefly the subject of mechanical theorem proving. Here the newspaper editor has visions of the machine "taking over" and long lines of unemployed mathematicians. Just the opposite is true. In almost all theorem proving projects, so far, many manhours and a few machine minutes have been spent in getting proofs of a few well known propositions. The results are a triumph for the ingenuity of human beings.

One procedure is as follows. To prove a given proposition p, one introduces into the memory of the machine a set of axioms known to be sufficient for the proof of p, the hypotheses of the proposition, and finally the denial of its conclusion. It is now up to the computer to make logical deductions from this input until two such results are contradictory. It is not very clear what the exact ground rules of this game are. Clearly it is unfair to help the computer. But without some built in safeguards much valuable machine time may be lost. Suppose for example we are trying to get the machine to prove that every positive integer is the sum of 4 squares, so we introduce the well known Peano axioms for the natural numbers. One of these axioms states that whenever n is a natural number, so also is $n+1$. Since our allotted time is finite we must somehow prevent the machine from deducing that 2 is a natural number and hence 3 is a natural number and hence, and so on. Another question to consider is: what is a fair selection of axioms? If we deliberately introduce axioms that are not really needed in the proof of p we can delay the computer by distraction. On the other hand if we give it the bare minimum, assuming we know it, of axioms sufficient to prove p, will this not be too strong a hint? This interesting game begins to look less like mathematics and more like pedagogy. To illustrate what actually happens under adequate safeguards and suitable heuristics, I give an example from the 1964 literature. The proposition to be proved is: If the square of every element of a group is the identity element then the group is commutative. The machine proof takes fourteen steps of which the four essential ones, in our notation, are

$$ab = ab[(ba)(ba)] = a(bb)a(ba) = (aa)ba = ba.$$

The whole program is a beautiful piece of coding. Other theorem proving projects have dealt with parts of plane geometry and first order predicate calculus.

Another form of theorem proving, and one with which I have been associated, has rather different ground rules. We are dealing here

with a man-machine cooperative. The man furnishes to the machine the best information that he has about the proposed theorem and the sort of proof that he thinks is likely to succeed. From this you will infer correctly that the actual proof is unknown to the man. In fact he doesn't know whether the theorem is false, or, if true, whether the machine can prove it. The machine is asked to carry out the logical steps of the proof, if indeed it can, in the allotted time. You will infer from this that there are a great many steps and that they cannot be carried out by hand. Usually the steps are not only numerous but are connected in some complicated combinatorial way. Here we are exploiting not only the speed of the computer but also its logical circuitry that allows it to keep track of and to modify its own complicated program to a degree well beyond human capability. Theorems of this kind are not easy to find in those drab branches of mathematics where elaborate proofs are not the rule. However, there are infinitely many such theorems in number theory alone. A very simple example of such a theorem is the following: Every set of five consecutive odd numbers contains either a prime or else a composite number divisible by a prime greater than or equal to 37. This theorem is best possible. The proof contains 2048 steps and is much too difficult to follow in detail. The computer has found much more elaborate proofs of theorems having to do with the distribution of power residues with respect to a prime modulus. In such cases the proof tree may contain millions of tiny branches even though the machine is provided with heuristic safeguards and a whole memory full of instructions. These programs will make curious reading for the archeologist of the distant future. To add a touch of reality to my remarks I can give a specific theorem whose proof is not only well beyond the ability of a team of human beings, but also beyond those computers that one finds at the big universities. By this I mean that I expect the proof would cost several thousand dollars.

The theorem has to do with the distribution of the so called quintic residues of a prime p, that is, the numbers modulo p that are congruent to a fifth power of an integer. The theorem to be proved is the following: There exists a world constant C such that every prime $p>3331$ has three quintic residues that are consecutive integers $<C$. The proviso, $p>3331$, is necessary because the prime $p=3331$ has no such set of three quintic residues. We know that if C exists it must exceed 76613, but I would be surprised if it were less than a million.

To return for a moment to the first mentioned research activity, that of building of improved, or alternate, highways between well

established locations and the outposts of mathematics. The mechanization of this activity appears, at this time, to be very inefficient or too difficult. However, already in the case of Gelernter's pioneering work in plane geometry, one sees the possibility of producing different kinds of proofs by assigning different priorities to different heuristic strategies. In another two decades the state of the art may have advanced sufficiently to program the making of roads from A to B via specified points C and D, as one now does by hand every semester in planning a graduate course. By this time no doubt mechanical theorem proving will have advanced to mechanical theory building. Of course, the mathematician will be still further ahead of this.

For the more immediate future there are at least two interesting opportunities for furthering the mechanization of mathematics. One of these is the remote console, the on line, time sharing computing system. With language general enough to handle symbol manipulation as well as some simple-minded numerical work, such a system can provide a working atmosphere almost comparable to that with which the average mathematician is familiar. The instant turn-around time of this system allows the mathematician to concentrate on one problem at a time instead of the five or six that efficient operation otherwise requires.

Another opportunity that needs further consideration is the construction of special purpose hardware for doing special mathematical research. The economics of even a minor project of this sort seems, at first sight, to be dubious. However there are ways around this stumbling block. Every advance in electronic technology makes obsolete, and nearly worthless, components and equipment that were until recently the best that money could buy. Slave labor is available from the graduate school of the electrical engineering department. As an illustration I cite here the special purpose Delay Line Sieve built this way at the University of California for occasional use on large number theory problems. In spite of its relative simplicity it can perform thirty-one divisions, inspect the remainders, and decide what to do next, all in a millionth of a second.

In conclusion I should like to speculate briefly on the overall impact of mechanization upon mathematics of the not too distant future. Mechanization tends to emphasize practice rather than theory, deeds rather than words, explicit answers rather than existence statements, definitions that are formalized rather than behavioristic, local rather than global phenomena, the limited rather than the infinite, the concrete rather than the abstract, and one could almost say, the scientific rather than the artistic. Man's role in this symbiosis should be to

supply the imagination, the judgment, the criticism, and yes, the control, as necessary, to further the search for truth in mathematics. The computer is the instrument of our observatory, our window to the hard facts of the world of mathematics. It would be a pleasure to predict that, as time goes on, the use of the instrument will become widespread and the nature of mathematics will slowly change from the dangerously unstable fluid art that it is apparently approaching today to a more and more structured and explicit science.

There is an alternate prediction. Already we see, instead, a splitting from mathematics of a new branch commonly called computer science, which includes enough technology to frighten away your topologist or functional analyst. Soon disciplinary fences will be erected. It has been said that the invention of photography relieved the graphic artist of his obligation to depict nature and drove him into impressionism and finally to abstraction. This, it seems to me, is apt to be also the future of mathematics. Still we do have Ansel Adams. It will be interesting to hear what the seventy-sixth Gibbs Lecturer has to say about it.