MATHEMATICS THROUGH MAN-COMPUTER INTERACTION. A STUDY OF THE EARLY YEARS OF COMPUTING.

Liesbeth De Mol[1]

Centre for Logic and Philosophy of Science, Ghent University.

1. INTRODUCTION

With the rise of the electronic, digital general-purpose computer a new tool became available to the mathematician, one that helps the mathematician to "*disclose the universe of discourse of mathematics"* to put it in Derrick H. Lehmer's words.[2] Until now, the true impact of the computer on mathematics has not been properly researched, even though the machine was originally conceived as an instrument for doing mathematics, be it, initially, some very raw form of mathematics.

In this note we will look at some of the early typical mathematical problems that were investigated with the computer as well as summarize the views of two computer pioneers, Derrick H. Lehmer and John von Neumann, on the impact of the computer on mathematics. The main focus will be on the ENIAC since it was the first American electronic digital and (basically) general-purpose computer.

2. WHY WOULD A MATHEMATICIAN GET INTERESTED IN COMPUTERS?

When the first electronic computers were built, the world was at war. It was the military establishment that sponsored the construction of the first electronic computers, including ENIAC. As a consequence, the main task of these computers was to compute for purposes of war like e.g. computing firing tables. Of course, to compute firing tables is not very appealing to the mathematically oriented mind. However, mathematicians like von Neumann and Lehmer immediately understood that the brute force of these electronic computers could be used for far more interesting things.

D. H. Lehmer was a number theorist whose father D. N. Lehmer, also a number theorist, made "[Lehmer] realize at an early age that mathematics, and especially number theory, is an

---

[1] Postdoctoral Fellow of the Research Foundation - Flanders (FWO).

[2] D.H. Lehmer, Mathematical methods in large scale computing units, in: Proceedings of Second Symposium on Large-Scale Digital Calculating Machinery, 1949 (Cambridge, Massachussetts), Harvard University Press, 1951, pp. 141-146.

experimental science."[3] Given this experimental attitude towards number theory, the idea of a computing machine to "assist the exploratory mind of the number theorist in investigating the global and local properties of the natural numbers" must have been very appealing to Lehmer. It should thus not come as a surprise that, long before the ENIAC was built, Lehmer had already built several analogue special-purpose machines to assist him in his research. In 1946 Lehmer was appointed as one of the members of the ENIAC's computation committee. His task was to test the mathematical possibilities of ENIAC.

As is recounted by Ulam, already in 1938 von Neumann expressed a clear interest in computers to tackle certain problems in mathematical physics like turbulence and the dynamics of shock waves:

> I remember that in our discussions von Neumann realized that the known analytical methods, the method of mathematical analysis, even in their most advanced forms, were not powerful enough to give any hope of obtaining solutions in closed form. This was perhaps one of the origins of his desire to try to devise methods of very fast numerical computations, a more humble way of proceeding.[4]

Von Neumann thus understood quite early that the computer could be useful in the context of applied mathematics. In 1944, von Neumann accidentally met lieutenant Hermann Goldstine, who was involved with the ENIAC project. At that time, von Neumann was already a consultant for the Los Alamos project. Goldstine most probably knew about this and told von Neumann about the top-secret project at the Moore school, i.e., the development of the ENIAC. Soon after this meeting, von Neumann got the necessary security clearance and became a frequent visitor of the machine.

3. FOUR (TYPICAL) EXAMPLES OF EARLY MAN-COMPUTER INTERACTIONS

The Monte Carlo method and the H-bomb

One of the most important applications of ENIAC were its computations for the H-bomb. As was explained in Sec. 2, von Neumann was already a consultant for the Los Alamos project when he became involved with ENIAC. It was "Johnny" who first suggested to implement a preliminary computational model of a thermonuclear reaction for the ENIAC. He was convinced (and could convince others) that:

> [...] it could provide a more exhaustive test of the computer than mere firing-table computations. [...] his heuristic arguments were accepted by the authorities at Aberdeen.[5]

Among the people who were present at the meeting where the results from these preliminary tests were reviewed was Stanislaw Ulam. Ulam was very much impressed by the speed and versatility

---

[3] D..H. Lehmer, The influence of computing on research in number theory, The Influence of Computing on Mathematical Research and Education (J. P. LaSalle, ed.), in: Proceedings of Symposia in Applied Mathematics, vol. 20, 1974, pp. 3-12.

[4] Stanislaw M. Ulam, Von Neumann: The interaction of mathematics and computing, in: John Howlett, Nicolas Metropolis, and Gian-Carlo Rota (eds.), in: A history of computing in the twentieth century, Academia Press, New York, 1980, 93-99.

[5] Nicholas Metropolis, The beginning of the Monte Carlo method, in: Los Alamos Science (Special Issue, Stanislaw Ulam 1909-1984) 15 (1987), 125-130.

of the ENIAC and understood that this machine could be just the thing needed to implement an idea he had been pondering about for some time, i.e., the use of what is now known as the Monte Carlo method for thermonuclear computations:

> The first thoughts and attempts I made to practice [the Monte Carlo Method] were suggested by a question which occurred to me in 1946 as I was convalescing from an illness and playing solitaires. The question was: what are the chances that a Canfield solitaire laid out with 52 cards will come out successfully? After spending a lot of time trying to estimate them by pure combinatorial calculations, I wondered whether a more practical method than "abstract thinking" might not be to lay it out say one hundred times and simply observe and count the number of successful plays. This was already possible to envisage with the beginning of the new era of fast computers, and I immediately thought of problems of neutron diffusion and other questions of mathematical physics, and more generally how to change processes described by certain differential equations into an equivalent form interpretable as a succession of random operations.[6,7]

Ulam suggested this idea to von Neumann and some months later the first tests using the Monte Carlo method were done on the ENIAC. The basic idea behind the method is to use a randomly distributed sample, and look at what happens to the sample, or to make certain random decisions that determine the future behaviour of the sample. Metropolis explained how the method could be used, describing an example from von Neumann in a letter to Richtmeyer, as follows:

> Consider a spherical core of fissionable material surrounded by a shell of tamper material. Assume some initial distribution of neutrons in space and in velocity but ignore radiative and hydrodynamic effects. The idea is to now follow the development of a large number of individual neutron chains as a consequence of scattering, absorption, fission and escape. [...] [A] genealogical history of an individual neutron is developed. The process is repeated for other neutrons until a statistically valid picture is generated. [...] How are the various decisions made? To start with, the computer must have a source of uniformly distributed pseudo-random numbers.[8]

The first tests were successful, and the Monte Carlo method became a standard method for doing computations on problems connected to the H-bomb design. However, in order for the Monte Carlo method to be successful, the computer needed a source of random numbers. It occurred to von Neumann that the computer could be programmed to generate its own random numbers and so he became interested in sequences of computable random numbers, sequences that are nowadays known as pseudo-random. The idea of generating random numbers through computation was new at that time and its significance, also from a more philosophical point of view, should not be underestimated.

Are π and e random?

> Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin. (John von Neumann, 1951)

---

[6] Roger Eckhardt, Stan Ulam, John von Neumann and the Monte Carlo method, in: Los Alamos Science (Special Issue, Stanislaw Ulam 1909-1984) 15 (1987), 131-137.

[7] The fact that Ulam prefers brute force over more "intelligent" approaches illustrates one fundamental aspect of the use of the computer within mathematics: even though the brute force method seems less "intelligent" it is often the most effective in computer mathematics, leading to interesting new results within mathematics.

[8] Nicholas Metropolis, The beginning of the Monte Carlo method, in: Los Alamos Science (Special Issue, Stanislaw Ulam 1909-1984) 15 (1987), 125-130.

In the light of the significance of the computer being capable of generating its own random numbers for successful tests of the Monte Carlo method, it should not come as a surprise that von Neumann suggested to do tests on the statistical distribution of the digits of π and *e*. To do so, the first 1000 digits of π and *e* were generated with the ENIAC, the results were then analysed by hand. The conclusion was that the distribution of the digits of π did not show any significant deviation from statistical randomness, *e* however did.[9]

The digits of π were, probably, never used for the H-bomb computations. Most probably it was von Neumann's middle square method, a generator that is known to perform very badly in general but performs quite well when started with the proper initial seed. In order to know which generator was actually used, we will have to wait until the U.S. Army decides to declassify the documents on the H-bomb computations.

The first extensive number-theoretical computation on the ENIAC

During the 4th of July week-end of 1946 Lehmer and his wife set-up a very nice problem on the ENIAC in order to test its mathematical capabilities. The problem was to compute a list of exponents *e* mod *p*, i.e., the least value *n* such that $2^n = 1 \bmod p$ and that *e* is some divisor of $p - 1$. These exponents could be used to compute the exceptions to the valid converse of Fermat's little theorem, first proven by Lucas.[10] What made this problem particularly interesting:

> [...] was that this was a difficult enough problem that it attracted the attention of some mathematicians who could say, yes, an electronic computer could actually do an interesting problem in number theory [...]to actually do it, to demonstrate it, was, I think, important to the post-war reputation of electronic computers among mathematicians.[11]

These kind of computations, i.e., automate the generation of mathematical tables, is a very typical example of how the computer has replaced humans. Nowadays, computers are still used within this context. It can be argued that mathematical tables have changed with the rise of the computer, both on the level of their use as well as on the level of their generation. For example, the inspection of large mathematical tables is now usually done through the interaction of man and computer, many aspects of this inspection being internalized in the machine.

One of the first computer proofs. A result on cubic residues.

Probably one of the most discussed "contributions" of the computer to mathematics is its capability to prove certain theorems *that cannot or have so far not been proven by a human mathematician.* One of the more famous such "computer proofs" is the proof of the four-color theorem by Appel and Haken from 1977. Much less known is that Lehmer, together with several other researchers had already found a computer proof in 1962 of a certain theorem in number

---

[9] For more details see: Nicholas Metropolis, George Reitwiesner, and John von Neumann, Statistical treatment of values of first 2000 decimal digits of *e* and of π calculated on the ENIAC, in: Mathematical tables and other aids to Computations (1950), no. 30, 109-112.

[10] For more details see: L. De Mol and M. Bullynck, A week-end off. The first extensive number-theoretical computation on the ENIAC, in: Logic and Theory of Algorithms, (C. Dimitracopoulos, A. Beckmann and Benedikt Löwe, eds.), Lecture Notes in Computer Science, vol.. 5028, Springer Verlag, 2008, 158-167.

[11] A. Akera (interviewer), Franz Alt interview: January 23 and February 2, 2006, ACM Oral History interviews (2006), no. 1.

theory.[12] Lehmer pointed out several fundamental features of the proof. First of all, he noted that the theorem is a genuine theorem because it involves the reduction of an infinite to a finite number of cases. Secondly, he emphasized the significance of man-computer interaction for the proof, each "player" having made its own contribution to the actual proof. Finally, and this is the point where Lehmer differentiated genuine computer proofs from, what he called, simulations, the proof is humanly impractical.

4. EARLY VISIONS ON MAN-COMPUTER INTERACTIONS WITHIN MATHEMATICS

Both Lehmer and von Neumann were involved with very different applications of the computer within mathematics, a difference that can, in part, be explained by their different views on mathematics.

For von Neumann, mathematical ideas ultimately originate in "empirics", i.e., physical reality. When mathematics becomes too far removed from this empirical source it becomes too much "l'art pour l'art" and it should be reinjected with empirical ideas.[13] Lehmer on the other hand was convinced that mathematics, and especially number theory, is by its very nature an experimental science. He considered the universe of the numbers as a world in itself to be explored for its own sake and not because it is connected to some physical problem.

From these backgrounds both computer pioneers formulated their own views on the significance of the computer for mathematics. Probably the most important aspect of von Neumann's view is the fact that he considered it as a means to build up an intuition, to get a feeling, for certain mathematical problems like e.g. the dynamics of shock waves. Nowadays the computer is still often used in this way.[14]

Lehmer was more explicit about the possibilities of these new computing machines.[15] Most important is that for Lehmer:

> [...] the most important influence of the machines on mathematics and mathematicians should lie in the opportunities that exist for applying the experimental method to mathematics. Much of modern mathematics is being developed in terms of what can be proved by general methods rather than in terms of what really exists in the universe of discourse. Many a young Ph.D. Student in mathematics has written his dissertation about a class of objects without ever having seen one of the objects at close range. There exists a distinct possibility that the new machines will be used in some cases to explore the terrain that has been staked out so freely and that something worth proving will be discovered in the rapidly expanding universe of mathematics.[16]

---

[12] For more detail see: D. H. Lehmer, E. Lehmer, W.H. Mills, and J. L. Selfridge, Machine proof of a theorem on cubic residues, in: Mathematics of computation 16 (1962), no. 80, 407-415.

[13] Annotation from: J. von Neuman, The mathematician, in: The works of the Mind (Chicago) (R.B.Heywood, ed.), University of Chicago Press, 1947, pp. 180-196.

[14] See for example: L. De Mol, On the boundaries of solvability and unsolvability in tag systems. Theoretical and experimental results, in: Proceedings of the International workshop on the complexity of simple programs (Cork) (T. Neary, T.Seda D. Woods, eds.) Cork University Press, forthcoming.

[15] Von Neumann died of bone cancer at a time that the computer was only starting to develop.

[16] D.H. Lehmer, Mathematical methods in large scale computing units, idem.

Lehmer was also quite explicit about computer proofs. He emphasized on several occasions that the only genuine computer proofs are those that are humanly impractical, i.e., proofs that cannot be found by a human being. As a consequence, the mathematician can never know all the details of the proof and he must thus have faith in what the machine has done. As such, the mathematician is confronted with the unpredictability of his own discipline, being outcasted by a machine that produces humanly unpredictable outcomes. Lehmer correctly pointed out that this characteristic might lead those mathematicians of little faith to the question: Is this really mathematics since it cannot be done at the blackboard?[17]

5. CONCLUDING

Nowadays probably every mathematician has one or more computers. In this sense, his work is already influenced by the computer. The several available text editors like LaTeX, mathematical software like Maple or Mathematica, the several tools to generate mathematical graphics like GnuPlot, the possibility to directly communicate with colleagues through mail, the direct availability of thousands of old and new papers in ones domain,.... All these kind of applications have changed the way mathematics is practised on a day-to-day basis. The kind of computer applications people like von Neumann and Lehmer were involved with, however, have affected certain parts of mathematics in a more profound way.

Computer proofs are still quite rare, although more emerge with time. One recent important example is Hales' proof of the sphere packing problem. Large networks of computers are still used to compute large prime numbers and the question of whether π is random or not is still an open question, investigated within the context of what is now known as experimental mathematics.[18] In general, computers are often used to generate, store or inspect mathematical tables. Some more recent examples are Wolfram's classification of a certain type of cellular automata and Sloane's on-line encyclopedia of integer sequences. Computers are also very often used in the context of computer experiments. One famous example is the use of the computer to investigate the Riemann hypothesis. Besides this, it is clear that the computer has given rise to new branches in mathematics like e.g. theoretical computer science or fractal geometry, these new domains frequently making use of computer experiments and proofs.

In this sense, few will deny that the computer has (had) an important influence on mathematics. Notwithstanding this fact, it still remains unclear whether this influence has led or will lead to a fundamental *change* of the whole of mathematics or whether this will remain restricted to some isolated cases. A detailed historical analysis of the way the computer has been and is still used within mathematics can help to tackle this problem.

[17] D.H. Lehmer, The influence of computing on research in number theory, idem.

[18] See for example: David H. Bailey and Richard E. Crandall, On the random character of fundamental constant expansions, in: Experimental Mathematics 10 (2001), no. 2, 175-190.