Doing Mathematics on the ENIAC. Von Neumann's and Lehmer's different visions.

Liesbeth De Mol

Doing Mathematics on the ENIAC. Von Neumann's and Lehmer's different visions.*

Liesbeth De Mol
Center for Logic and Philosophy of Science
University of Ghent, Blandijnberg 2, 9000 Gent, Belgium
elizabeth.demol@ugent.be

Abstract

In this paper we will study the impact of the computer on mathematics and its practice from a historical point of view. We will look at what kind of mathematical problems were implemented on early electronic computing machines and how these implementations were perceived. By doing so, we want to stress that the computer was in fact, from its very beginning, conceived as a mathematical instrument per se, thus situating the contemporary usage of the computer in mathematics in its proper historical background. We will focus on the work by two computer pioneers: Derrick H. Lehmer and John von Neumann. They were both involved with the ENIAC and had strong opinions about how these new machines might influence (theoretical and applied) mathematics.

1 Introduction

The impact of the computer on society can hardly be underestimated: it affects almost every aspect of our lives. This influence is not restricted to everyday activities like booking a hotel or corresponding with friends. Science has been changed dramatically by the computer – both in its form and in

*The author is currently a postdoctoral research fellow of the Fund for Scientific Research – Flanders (FWO) and a fellow of the Kunsthochschule für Medien, Köln.

its content. Also mathematics did not escape this influence of the computer. In fact, the first computer applications were mathematical in nature, i.e., the first electronic general-purpose computing machines were used to solve or study certain mathematical (applied as well as theoretical) problems.
The financial force behind the first electronic digital computers was the military establishment. The ENIAC, the first electronic general-purpose digital computer, presented to the public on February 15, 1946 at Penn University, was financed with U.S. army money. The original idea of building this electronic machine came from John W. Mauchly. He had always had a keen interest in weather prediction. The available mechanical computers at that time however were not fast enough to his idea, so he thought about building an electronic computer using vacuum tubes (See e.g.[32]). In 1941, Mauchly met Presper J. Eckert at the Moore School at Penn University. Eckert "*was willing and agreeable to talk about the possibility of electronic computers [...] Nobody else really wanted to give it a second thought* [32, p. 43]". Mauchly then wrote a memo proposing to build a very fast electronic digital computer using vacuum tubes. Because of its speed, this new computer would be very suitable to compute firing tables,[1] an at that time attractive application for the planned machine since the world was at war. The memo caught the attention of Lieutenant Herman Goldstine, the contact between the U.S. Army and the Moore school. He asked Mauchly to write a formal proposal to apply for money with the army. The U.S. Army provided the money (the contract was signed in 1943) and a team of engineers, under the direction of Eckert, could start to build their computing machine now known as the Electronic Numerical Integrator and Computer, the ENIAC.[2]

[1]The following quote, explains what fire tables were used for: "*The army used its lush fields and rolling hills to test artillery guns and other weapons. Since a gunner often couldn't see his target over a hill, he relied on a booklet of firing tables to aim the artillery gun. How far the shell travelled depended on a host of variables, from the wind speed and direction to the humidity and temperature and elevation above sea level. Even the temperature of the gunpowder mattered. A gun such as the 155-millimeter "Long Tom" required a firing table with five hundred different sets of conditions. Each new gun, and each new shell, had to have new firing tables , and the calculations were done at Aberdeen based on test-firings and mathematical formulas.*" [30, p. 53]

[2]It should be noted that computing firing tables was not the sole purpose of the ENIAC. As is recounted by Eckert: "*Unfortunately, it is often said that the ENIAC was built just for preparing firing tables. Cunningham and others at BRL all supported us in making the ENIAC as generally useful as we could contrive to make it within the limited time that conditions of war demanded. Yes, BRL wanted firing tables, but they also wanted to be*

The ENIAC was primarily used for military purposes. However, these military applications were in fact applied mathematics (like the computation of the solution of non-linear differential equations describing the path of bullets and missiles) and even had certain side-results (as will be illustrated in Sec. 3.2) which can hardly be regarded as applied. But also more theoretical problems were implemented on the ENIAC, problems that had no connection at all with the military purposes the ENIAC was built for (See Sec. 3.3). [3]
The fact that the first electronic digital computers were used to do mathematics (applied or non-applied) is remarkable, especially in the light of the present-day usage of computers within mathematics. The purpose of this paper is to study the impact of the computer on mathematics and its practice from a historical point of view. I will look at what kind of mathematical problems were implemented on early electronic computing machines (focusing on the ENIAC) and how these implementations were perceived by two computer pioneers and mathematicians. In doing so, attention is given to the fact that the electronic general-purpose computer was in fact, from its very beginning, conceived as a mathematical instrument per se. The contemporary usage of the electronic general-purpose computer in mathematics will thus be situated in its proper historical context.
We will focus on the work by two computer pioneers: Derrick H. Lehmer and John von Neumann. They were both involved with the ENIAC and formulated clear opinions about how these new machines might be used in and have an impact on (theoretical and applied) mathematics. We will describe four of the computer implementations they were involved with (three on the ENIAC, one on more "modern" machines, see Sec. 3) and discuss and contrast their surprisingly contemporary visions on the use of the computer in and its impact on mathematics.

---

able to do "interior" ballistics, and all kinds of data reduction, and they went on and on with examples of what they would hope to be able to do with a truly flexible computer. We wince a little when we hear the ENIAC referred to as a special-purpose computer; it was not. The name "ENIAC," where the "I" stands for "integrator," was devised to help sell the Pentagon that what the BRL was getting would compute firing tables, which were, in 1943, the greatest need of Ordnance. But there was a flexibility of control far beyond the implications of the name." [10, p. 526]

[3] A detailed list of the problems implemented on the ENIAC can be found in [12, pp. 42–45].

2 How Lehmer and von Neumann got involved with computers

Von Neumann and Lehmer were two mathematicians who were very enthusiastic about the idea of using the computer in their domain, each of them having his own motivations for this enthusiasm. When they got the opportunity to get involved with the ENIAC, the first U.S. electronic computer, they grabbed this opportunity with both hands. In this section we will discuss why Lehmer and von Neumann got interested in computers.

2.1 The case of Lehmer. Number-crunching in number theory

Derrick H. Lehmer (1905-1991) was born into number theory. His father, Derrick N. Lehmer, was a number-theorist, known for his factor table up to 10,000,000 and his stencil sheets to find factors of large numbers. But it was not only the profession itself D.H. learned from his father [24, p. 3]:

> My father did many things to make me realize at an early age that mathematics, and especially number theory, is an experimental science. If one examines the collected works of Euler, Gauss, Legendre, to name but three, one finds them shamelessly and laboriously computing examples of empirical discoveries. Often these efforts led to the establishment of important theorems. Some of these discoveries remain to this day without logical links to Peano's axioms. Exploring in discrete variable mathematics is generally simpler than in continuum mathematics. One can see the input and the resulting experimental output with absolute clarity. For the same reason a digital or discrete variable computer is a better aid to discovery than an analog machine.[...] We should regard the digital computer system as an instrument to assist the exploratory mind of the number theorist in investigating the global and local properties of this, the natural numbers and their algebraic expansions.

Throughout Lehmer's papers one finds numerous statements about the experimental character of mathematics and more specifically number theory, which he regarded as a kind of observational science. It is exactly in this

context that one should understand Lehmer's interest in computers. He regarded them as instruments to experimentally study mathematics (See Sec. 4.2 for more details). Already as a young boy, Lehmer began to design and build small special-purpose machines, known as sieves, to assist him in his number-theoretical work.

A sieve process is known to solve sieve problems. Following Lehmer [21] the general problem can be stated as follows. Let $m_1, m_2, ..., m_k$ (the moduli) be a set of k (the width) positive integers. For each m_i we consider n_i distinct arithmetical progressions denoted by:

$$P_{ij}(x) = m_i x + a_{ij} \begin{cases} i = 1, 2, ..., k \\ j = 1, 2, ..., n_i \end{cases}$$

We assume that for i fixed, the a_{ij} are distinct non-negative integers less than m_i. The problem is then to find all integers N between given limits A and B such that each N belongs to k arithmetical progressions. An example of such a sieve problem is the problem to find the least positive integer of the form:

$$\begin{cases} 3x + 1 \text{ or } 2 \\ 7x + 3 \text{ or } 5 \end{cases}$$

One famous example of a sieve is the sieve of Erasthotenes to compute prime numbers.

Lehmer was made familiar with sieves through his father, who used a sieve technique called the stencil method to construct his factor table [25]. However, this method was still quite slow and cumbersome and this is why Lehmer started wondering about building machines that could do the work for him. His first sieve, dated 1926, was an electro-mechanical sieve built with bicycle chains. It eliminated values X at the rate of 60 per second and had a width k of 16. As Lehmer notes about this machine: "*It was a genuine parallel machine*" [25, p. 447]. Ten years later, Lehmer built another electromechanical sieve using 16 mm film, where the values a_{ij} were little round holes in the main tape. Four years before, in 1932, Lehmer had also built a photoelectric sieve, using a beam of light that "*entered on one side and tried to run the gauntlet of the holes to reach a photocell and find the first answer*" [25, p. 448–449]. It ran at 5000 counts per second, and was thus faster than the electro-mechnanical ones. The next sieve Lehmer was to "build" was an implementation on the ENIAC (See Sec. 3.3).

When World War II began, Lehmer "*got involved into war work mostly having to do with the analysis of bombing* [28, p. 3]". He built a special-purpose

machine, a "*bombing analyzer [which] was a combination of the digital and the analog device. [...] I demonstrated it in Washington one time at the Pentagon. [...] This thing was Army Ordnance, I guess.* [31, pp. 16–17]".
Just after the war Lehmer was called upon by the Ballistic Research Laboratories (Aberdeen Proving Ground) to become a member of the 'Computations Committee', which was assembled to prepare for utilizing the ENIAC after its completion [1, p. 693]. The ENIAC was to be extensively test-run during its first months by members of this committee. Besides Lehmer, the committee included Haskell B. Curry, Leland B. Cunningham and Franz Alt. They implemented non-military problems of which some were pure theoretical ones. The at that time revolutionary fast and highly parallel ENIAC, doing no less than 5000 additions per second, must have been very appealing to Lehmer. He already had a keen interest in computing machines, especially parallel ones for building sieves, and was very well aware that this kind of increase in computational speed could be invaluable to solve or study certain mathematical problems.
After his experience with the ENIAC, Lehmer remained in computing and worked on several of the early post-war American computers like the SWAC, exploring the universe of numbers in ways that had been impossible before.

2.2 The case of von Neumann: Number-crunching in Physics

John von Neumann is far more famous than D.H. Lehmer, not in the least because the hardware of computers nowadays is still referred to as 'the von Neumann architecture'.[4] He was a mathematician by education and made

[4]This however should not be taken for granted. One of the basic reasons for von Neumann's name being connected to the invention of the modern computer has to do with the fact that it is his name and none other that is associated with the *First draft of a Report on the EDVAC* [40] – the EDVAC being identified with the von Neumann architecture. The history of who really invented the first electronic digital general-purpose and (!) stored-program computer is still a matter of debate. Many people believe von Neumann is the inventor of the stored-program computer but, as far as my knowledge goes, there is no real convincing and/or definite evidence proving that it was really von Neumann who deserves all the credit. Eckert and Mauchly, and with them several other people who were involved, like Jean Bartik one of the ENIAC programmers and employee of the Eckert-Mauchly computer cooperation, have contradicted this. Moreover, one should not neglect the fact that Besides the adjective stored-program, modern computers are also electric and general-purpose, two features the ENIAC already had and which are at least

major contributions in many different fields, including: mathematical logic, set theory, economics and game theory, quantum mechanics, hydrodynamics, computer science,...

Von Neumann's acquaintance with the field of mathematical logic had a major influence on his work on computers. He had been there in 1930 at the conference in Königsberg where Gödel announced his now famous incompleteness results for the first time. He was also fully aware of Turing's seminal paper [37] that not only contained a negative solution to the Entscheidungsproblem, but also an "algorithmic" description of the universal Turing machine, a theoretical machine that can be regarded as the theoretical version of the stored-program computer.[5] After Gödel's results von Neumann wanted to stay far away from logic. But then he got involved with the ENIAC project, and with "real" computing. In this context von Neumann's logical background would prove very useful.

It was not his interest in logic, however, that triggered his interest in the subject. In [39], Ulam explains why von Neumann got interested in computers (pp. 93–94):

> It must have been in 1938 that I first had discussions with von Neumann about problems in mathematical physics, and the first I remember were when he was very curious about the problem of mathematical treatment of turbulence in hydrodynamics. [...] He was fascinated by the role of Reynolds number, a dimensionless number, a pure number because it is the ratio of two forces, the inertial one and the viscous [...] [von Neumann] [...] wanted to find an explanation or at least a way to understand this very puzzling large number. [...] 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

as fundamental as the stored-program idea (not in the least because stored-program only makes sense if one already has a general-purpose computer). This paper however is not the proper place to discuss these matters. For more information, the reader is referred to some of the existing literature [5, 6, 10, 13, 29, 30] to form his/her opinion on the matter. In any way, one must be very careful in these matters.

[5] As is argued in [15] and [8], based on a letter by Ulam to Hodges ([15], p. 145) (available on-line through Andrew Hodges website on Turing: http://www.turing.org.uk/sources/vonneumann.html) von Neumann must have read Turing's paper before the outbreak of the war.

> 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. Proceeding by "brute force" is considered by some to be more lowbrow. [...] I remember also discussions about the possibilities of predicting the weather at first only locally, and soon after that, about how to calculate the circulation of meteorological phenomena around the globe.

Von Neumann got particularly interested in computers for doing numerical calculations in the context of theoretical physics and thus understood, quite early, that fast computing machines could be very useful in the context of applied mathematics.

In 1943, during World War II, von Neumann was invited to join the Manhattan project – the project to develop the atomic bomb – because of his work on fluid dynamics. He soon realized that the problems he was working on involved a lot of computational work which might take years to complete. He submitted a request for help, and in 1944 he was presented a list of people he could visit. He visited Howard Aiken and saw his Harvard Mark I (ASCC) calculator. He knew about the electromechanical relay computers of George Stibitz, and about the work by Jan Schilt at the Watson Scientific Computing Laboratory at Columbia University. These machines however were still relatively slow to solve the problems von Neumann was working on. But then he accidentally met Herman Goldstine at Aberdeen railwaystation. While waiting for their train on the platform, Goldstine told him about the top-secret ENIAC project at the Moore school [13]. Von Neumann got very excited, and Goldstine made arrangements (providing the necessary clearance document) so that von Neumann could visit the ENIAC. As is recounted by Eckert, "*his first visit could not have been before 7 September 1944. In my own records, which also became a court document, is confirmation that Eckert and I had a commitment to meet von Neumann about 7 September. I believe that was our first meeting with him.* [10]" After this first visit, he was a frequent visitor of the ENIAC.

He became one of the major contributors to the design of what is known as the first electronic, general-purpose *stored-program* computer, the EDVAC (See footnote 4). The main design ideas for the EDVAC were described by von Neumann in the first draft of this machine [40]. Even though it is not completely clear who contributed what to the design, the emphasis on the logical aspects of the EDVAC must be credited to von Neumann. He also

made important contributions to the rewiring of the ENIAC at Aberdeen, since the permanent set of instructions to be internalized were chosen with von Neumann's consultation.[6] As was the case for Lehmer, von Neumann never really left the domain of computers once he got involved with them. He laid the foundations for several research topics within computer science that are up until today very much alive, like research on cellular automata –which he co-invented.
Von Neumann died in 1957 of bone cancer, possibly caused by exposure to radiation during (one of) the A-bomb tests at the Bikini islands.

3 Four Examples of Early mathematical (applied and theoretical) computations.

As is clear from Sec. 2, von Neumann and Lehmer each had their own motives to be interested in computers: Lehmer wanted to use computers mainly to study and solve theoretical problems in number theory, while von Neumann wanted to use them in applied mathematics, like fluid dynamics. In this section, we will describe four examples of early mathematical computations in which von Neumann and Lehmer were involved. The difference between their interests is also apparent from these examples, a difference that converges with their views on the use of computers within mathematics to be discussed in Sec. 4.

3.1 The Monte Carlo method and the H-bomb

The ENIAC was built with army money and thus had to devote its "official" time to military computations. At the time von Neumann got involved with the ENIAC, he was already a consultant to Los Alamos. It was he who first

[6]Neukom's paper [35] gives a detailed description of "the ENIAC's second life". It should also be noted here that while the usual account on the rewiring of the ENIAC is that von Neumann suggested the idea and Clippinger detailed out the design, Metropolis tells us a slightly different story: "*In the meantime Richard Clippinger, a staff member at Aberdeen, had suggested that the ENIAC had sufficient flexibility to permit is controls to be reorganized into a more convenient (albeit static) stored-program mode of operation. [...] Although implementing the new approach is an interesting story, suffice it to say that Johnny's wife, Klari, and I designed the new controls in about two months and completed the implementation in a fortnight.*" ([33], p. 128).

suggested to prepare "a preliminary computational model of a thermonuclear reaction for the ENIAC." As is recounted by Metropolis [33, p. 126]:

> For a whole host of reaons [von Neumann] had become seriously interested in the thermonuclear problem being pawned at that time in Los Alamos by a friendly fellow-Hungarian scientist, Edward Teller, and his groups. Johnny (as he was affectionally called) let it be known that construction of the ENIAC was nearing completion, and he wondered whether Stan Frankel and I would be interested in preparing a preliminary computational model of a thermonuclear reaction for the ENIAC. He felt he could convince the authorities at Abeerdeen that our problem could provide a more exhaustive test of the computer than mere firing-table computations. [...] Our response to von Neumann's suggestion was enthusiastic, and his heuristic arguments were accepted by the authorities at Aberdeen.

After von Neumann, Frankel and Metropolis had visited the ENIAC, Frankel and Metropolis began to work on a model that was realistically calculable and the computations were then implemented on the ENIAC. In the spring of 1946, a review of the ENIAC results was held at Los Alamos. Among the people present was also Stan Ulam. He was very much impressed by the speed and versatility 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.[7] As Ulam recounts (Remark dated 1983, quoted in [11, p. 131]):

> 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

[7] In fact the name "Monte Carlo" goes back to a story about Ulam's uncle, who would borrow money from relatives because "he just had to go to Monte Carlo" [33].

> 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. Later [in 1946, I] described the idea to John von Neumann and we began to plan actual calculations.

After having heard about the ENIAC's possibilities, Ulam discussed his ideas on using the Monte Carlo method for tackling problems in nuclear physics, and the possibility of implementing it on the ENIAC, with von Neumann. He immediately understood the significance of Ulam's suggestion. In March 1947 he wrote a letter to Robert Richtmyer, at that time the Theoretical Division leader at Los Alamos, explaining why the statistical approach suggested by Ulam was very well suited for a digital treatment.
The Monte Carlo method can be used as a way to explore the behavior of various physical and mathematical systems, in order to make certain predictions about these systems. It was particularly well-suited for exploring the behavior of neutron chain reactions in fission devices. The basic idea 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 his letter to Richtmyer, as follows [33, p.127]:

> 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.

In 1947, after the ENIAC was rewired and moved to its permanent home at the Ballistics Research Lab in Maryland (see footnote 6), the first ambitious

test of the Monte Carlo method was implemented [33, p.128]:

> Nine problems were computed corresponding to various configurations of materials, initial distributions of neutrons and running times. [...] The neutron histories were subjected to a variety of statistical analyses and comparisons with other approaches. Conclusions about the efficacy of the method were quite favorable. It seemed as though Monte Carlo was here to stay.

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 to be successful, the computer must first have 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.

3.2 Are π and e random?

Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin. [42]

Von Neumann's interest in the statistical properties of numbers like π and e should, most probably, be understood in the context of the use of the Monte Carlo method on the ENIAC. In 1949 he suggested to use the ENIAC to compute the first 2000 decimal values of π and e in order to get an idea about their statistical distribution ([36, p. 11]):

> Early in June, 1949, Professor John von Neumann expressed an interest in the possibility that the ENIAC might sometime be employed to determine the value of π and e to many decimal places with a view toward obtaining a statistical measure of the randomness of distribution of the digits [...]

The computations for e were finished in July 1949, those for π during Labor-Day weekend, in September 1949.[8] In [34] and [36] set-up and results are

[8] As was the case for several more theoretical computations done on the ENIAC, these were all done outside the "official time", during holidays. As Reitwiesner [36] explains, four members of the ENIAC staff and Reitwiesner himself did 8-hours shifts to keep the ENIAC operating continuously throughout the Labor-day weekend.

discussed: the first 2000 decimal digits of both numbers were computed. A statistical analysis (by hand) of the data led to the conclusion that "*the material has failed to disclose any significant deviations from randomness for π, but is has indicated quite serious ones for e.*" ([34], p. 109).[9]

3.3 The first extensive number-theoretical computation on the ENIAC

On the Friday of the 4th of July week-end in 1946, the Lehmer family – Derrick, Emma and two teenage kids – arrived at the Moore school where they met John Mauchly. He helped them set up the ENIAC for the implementation of an interesting number-theoretical problem and stayed on as an operator through the week-end [25, p. 451]. As is explained by Franz Alt, what made the problem particularly interesting [17, p. 40]:

> [...] 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 – something as sophisticated in number theory – and produce useful results. There were many people who speculated about this – von Neumann among them – but to actually do it, to demonstrate it, was, I think, important to the post-war reputation of electronic computers among mathematicians.

The problem concerned the converse of Fermat's little theorem which states:

Theorem 1 *If $a^{p-1} \equiv 1 \bmod p$ than p is prime*

This converse gives a good (read fast) test for primality. Unfortunately this converse is not true in general: there are certain p for which $a^{p-1} \equiv 1 \bmod p$ with p not a prime number. If one wants to use this primality test, one needs a list of exceptions to the theorem. This is exactly what Lehmer wanted to

[9] It is interesting to point out that part of the research on the random character of the digits in π is still situated in a more heuristic research context. Recently, an important paper was published in the journal *Experimental Mathematics* on this topic [2], in which it is shown that the statistical randomness of several constants, including π, depends on an hypothesis concerning the distribution of the iterates of certain dynamical maps, and is thus situated in a branch of mathematics, characterized by the numerous computer experiments underlying it, i.e., chaos theory.

do.
Taking a equal to 2 (which is computationally the most advantageous choice), one way to compute the composite p's for which $2^{p-1} \equiv 1 \bmod p$ is to use a table of exponents e of 2 modulo the prime p, e being the least value n such that $2^n \equiv 1 \bmod p$ and e is some divisor of $p-1 = ef$.[10] Kraïtchik published such an exponent table in 1924 for $p < 300000$, but it contained quite some errors [18]. Lehmer now proposed to use the ENIAC to compute a table of exponents correcting and extending Kraïtchik's table to $p < 4.5 \cdot 10^6$. The results of Lehmer's calculation on the ENIAC were published as a list of corrigenda to Kraïtchik's table in 1947 (MTAC 2 (19) p. 313). In 1949 an article discussing some computational details of setting up this 'program' on the ENIAC appeared [19]. It was exactly for this problem that Lehmer implemented his first sieve on an electronic general-purpose computer.
As Lehmer remarks right at the beginning of his description of the ENIAC set-up: "*The method used by the ENIAC to find the exponent of 2 modulo p differs greatly from the one used by human computer*" [19, p. 301]. The exponent e of 2 modulo a prime p should either be a divisor of or equal to $p-1$, and one can thus restrict oneself to doing trial divisions with suitable divisors of $p-1$ only. On the ENIAC however, it was more expeditive to compute 2^t for all $t < p-1$. This 'idiot approach' takes, in the worst case, "*less than 2.4 seconds, less time than it takes to copy down the value of p*", whereas the sophisticated method requires "*much outside information via punched cards [...] to be prepared by hand in advance.*" [19, p. 302]. We will not discuss the details of the implementation here. For more information the reader is referred to [9].

3.4 One of the first machine proofs. A result on cubic residues.

In 1962 a paper titled *Machine Proof of a Theorem on Cubic Residues* [26] appeared by D.H. Lehmer, Emma Lehmer, W.H. Mills and J.L. Selfridge, containing a description of what can be considered as one of the first real machine proofs, i.e., the proof of a theorem that has not (and cannot) be proven by a human being. Other, far more famous (but younger) examples, are of course the machine proof of the four color theorem by Appel and Haken

[10] More details about how to use these exponents to find composite numbers can be found in [18].

and the still not completely accepted proof of the sphere packing problem by Thomas Hales. The machines used were the IBM 701, 704, 709 and 7090. To understand the theorem it is important to first explain the notion of cubic residues. If p is a prime of the form $6m + 1$ the numbers

$$1^3, 2^3, ..., (p-1)^3$$

when reduced modulo p consist of only $(p-1)/3 = 2m$ distinct numbers between 1 and $p-1$. These $2m$ numbers are the *cubic residues* of p. For example, the cubic residues of 13 are 1, 5, 8 and 12. A prime $p = 6m + 1$ is called *exceptional* if it does not have a triplet of cubic residues, where a triplet is any set of three consecutive positive integers. It had already been proven by Brauer in 1928 that all "sufficiently large" primes have a triplet of cubic residues. Thus there are only a finite number of exceptional primes. However, as Lehmer notes "*[b]y using machine methods we have proved much more* [26, p. 407]". Indeed, the theorem that was proven by the IBM machines is:

Theorem 2

(a) *The only exceptional primes are:*

$$2, 3, 7, 13, 19, 31, 37, 43, 61, 67, 79, 127, 283$$

(b) *Every non-exceptional prime has a triplet of cubic residues that does not exceed:*

$$(23532, 23533, 23534) \tag{1}$$

(c) *There are infinitely many primes whose smallest triplet of cubic residues is* (2). *Hence, result* (b) *is the best possible.*

Initially they were unsure about the outcome of the machines, because nobody could know in advance whether the proof tree that had to be constructed would come to a halt. The limit of 55 "stories" for each branch of the proof tree was determined by the machine. Furthermore, the "world constant" 23532 , as Lehmer called it, was found by the machine, independent of the method of proof.

We cannot discuss the details of the set-up and proof here. Still it is important to point out some important features of this machine proof, as they were emphasized by Lehmer. First of all to obtain (a), (b) and (c) an infinite number of cases was reduced to a finite number of cases by the computer which makes the theorem a genuine theorem according to Lehmer: "*a genuine theorem should be a statement about an infinite class or should make an infinite number of statements in its conclusion.* [22]". Secondly, Lehmer emphasizes the significance of man-computer interaction for the result [26, pp. 407–408]:

> In our work, instead of starting with axioms, we did not hesitate to use any device or previously known result that might be useful. In particular, the authors aided and abetted the machine in its search for a theorem and its proof. Nevertheless, all three results (a), (b), and (c) are due to the machine. Even the verification of these results using data supplied by the machine would be far too long and hazardous a calculation to do by hand.

Last, because the proof is humanly impractical " *no one has all the details. The machine was asked to make progress reports from time to time and studying these reports we can follow the proof in broad outline only.* [22]"

4 Lehmer's and von Neumann's different visions on mathematics and the computer.

It is interesting to see how von Neumann's and Lehmer's particular interests (See Sec. 2) got them involved with quite different examples of early computations. The Monte Carlo method and its use for the H-bomb computations is (very clearly) to be situated within the field of applied mathematics. The question on the random character of π and e is quite theoretical, but, von Neumann's interest in the problem was not that innocent: there was a definite reason for being interested in randomness generated by simple mathematical functions. The computations done by Lehmer are very different from these first two: they are number-theoretical problems that did not have any immediate application at their time and might even be called "exotic".
This kind of difference between applied and theoretical mathematics can also in part be found in von Neumann's and Lehmer's thoughts on mathematics

and how (certain parts of) it could be studied with the help of the computer. However, there are also some very clear similarities between their points of view, not in the least because they both situated the mathematical use of the computer within an experimental setting.

4.1 Von Neumann's point of view.

In a talk entitled *The Mathematician* [41] von Neumann formulated the following view on mathematics:

> I think that it is a relatively good approximation to truth [...] that mathematical ideas originate in empirics, although the genealogy is sometimes long and obscure. But, once they are so conceived, the subject begins to live a peculiar life of its own and is better compared to a creative one, governed by almost entirely aesthetical motivations, than to anything else and, in particular, to an empirical science. [...] As a mathematical discipline travels far from its empirical source, or still more, if it is a second and third generation only indirectly inspired by ideas coming from "reality", it is beset with very grave dangers. It becomes more and more purely aestheticizing, more and more purely *l'art pour l'art*. [...] there is a grave danger that the subject will develop along the line of least resistance, that the stream, so far from its source, will separate into a multitude of insignificant branches, and that the discipline will become a disorganized mass of details and complexities. In other words, at a great distance from its empirical source, or after much "abstract" inbreeding, a mathematical subject is in danger of degeneration. At the inception the style is usually classical; when it shows signs of becoming baroque, then the danger signal is up. It would be easy to give examples, to trace specific evolutions into the baroque and the very high baroque, but this, again, would be too technical. In any event, whenever this stage is reached, the only remedy seems to me to be the rejuvenating return to the source: the reinjection of more or less directly empirical ideas. I am convinced that this was a necessary condition to conserve the freshness and the vitality of the subject and that this will remain equally true in the future.

For von Neumann mathematical ideas originate in an empirical reality. If these empirical roots get obscured, mathematics is in danger of degeneration. His interest in connecting mathematics with more empirical sciences like physics, thus has a clear motivation: it prevents mathematics from becoming highly baroque, or, maybe even worse, 'l'art pour l'art'. Von Neumann's interest in connecting empirical with more theoretical ideas form the proper background for understanding his interest in computers.

But what kind of role did he exactly have in mind for these new computing machines in the context of mathematics? In Sec. 2 we already mentioned that according to Ulam, von Neumann got interested in computers, due to the realization that some of the usual methods of mathematics were not enough to study certain problems in mathematical physics. Number-crunching seemed a good alternative to these methods. However, once von Neumann realized the full potentiality of the new computing machines, he understood that although any computer is essentially nothing more but a "number-cruncher", it can play a much more important role in mathematics and, more generally, science.

That von Neumann assigned an important role to computers within those parts of science that can be tackled from a more mathematically oriented approach, is apparent when one goes through some of his later works. We will not discuss these in any details here, but we should at least mention von Neumann's work on natural and artificial automata. One of the texts he wrote in this context, *The computer and the brain* [43], which is a published version of the prestigious Silliman lectures and the last text written by von Neumann, contains clear statements about the significance of a complete theory of artificial automata for the development of a complete theory of the nervous system.

Besides discussing the possibilities of using computers within other domains like physics or biology – thus providing a mathematical approach to study problems in more "down-to-earth" domains (see e.g. the introduction of [43]) – he also made some explicit remarks about *how* the computer should be used within mathematics, and what kind of things it should produce. Most interesting here are the five lectures he gave at Illinois University in 1949, published as a series of annotated texts by Burks [45].

First of all, he was convinced that computers should not be used to produce vast amounts of data [45, pp. 38–39]:

> [...] let me point out that we will probably not want to produce

> vast amounts of numerical material with computing machines, for example, enormous tables of functions. The reason for using fast computing machines is not that you want to produce a lot of information. After all, the mere fact that you want some information means that you somehow imagine that you can absorb it, and, therefore, wherever there may be bottlenecks in the automatic arrangement which produces and processes this information, there is a worse bottleneck at the human intellect into which the information ultimately seeps. The really difficult problems are of such a nature that the number of data which enter is quite small. All you may want to know is a few numbers, which give a rough curve, or one number. All you may want in fact is a "yes" or a "no," the answer as to whether something is or is not stable, or whether turbulence has or has not set in.

According to von Neumann, computers should indeed not be used to produce (or store) large tables of information to be studied or used by man, because we simply cannot cope with so much information. Rather, a computer should provide definite and not too long answers after a program has been executed. As we will see in Sec. 4.2, this stands to some extent in contrast with the significance Lehmer attached to the production and inspection of tables by computers.
Secondly and more importantly, von Neumann became convinced that the computer could be used to solve certain problems for which both mere physical experimentation as well as theoretical considerations fail. For him, the computer could be the means to build up an intuition of such problems, and thus to get better heuristic ideas ([45], pp. 33–35):

> In pure mathematics the really powerful methods are only effective when one already has some intuitive connection with the subject, when one already has, before a proof has been carried out, some intuitive insight, some expectation which, in a majority of cases, proves to be right. In this case one is already ahead of the game and suspects the direction in which the result lies. A very great difficulty in any new kind of mathematics is that there is a vicious circle: you are at a terrible disadvantage in applying the proper pure mathematical methods unless you already have a reasonably intuitive heuristic relation to the subject and unless

> you have had some substantive mathematical successes in it already [...] progress has an autocatalytic feature. Almost all of the correct mathematical surmises in [the area of the non-linear sciences] have come in a very hybrid manner from experimentation. If one could calculate solutions in certain critical situations [...] one would probably get much better heuristic ideas. [...] there are large areas in pure mathematics where we are blocked by a peculiar inter-relation of rigor and intuitive insight, each of which is needed for the other, and where the unmathematical process of experimentation with physical problems has produced almost the only progress which has been made. Computing, which is not too mathematical either in the traditional sense but is still closer to the central area of mathematics than this sort of experimentation is, might be a more flexible and more adequate tool in these areas than experimentation.

To von Neumann, the computer was a means to "de-block" certain areas of mathematics for further exploration, allowing to build up an intuition of a certain problem. By e.g. solving certain special cases of a given set of equations numerically, which is easily obtained by varying the parameters, one can "*get a feeling for such phenomena as turbulence and shock waves, and with this qualitative orientation [can] pick out further critical cases to solve numerically, eventually developing a satisfactory theory.* ([4] pp. 2–3)" Although the task the computer has to perform seems quite inessential – in the end, it "merely" computes faster than we can, and, in the meantime, stores and processes more information than we can – it has shown itself an indispensable tool in several branches of science in the way von Neumann believed they would be useful. To give just one example, the area of fractal geometry and chaos theory would probably have remained "blocked" were it not for the computer. The best way to explore this domain is to do computing and visualizations of the numbers computed. The role "computer experiments" have played in this domain can hardly be overestimated, i.e., most results and conjectures go back to such "experiments".

4.2 A number theorist's point of view

While von Neumann believed that it was fundamental for, if not inherent to, mathematics to be rooted in the "real world", this was never really the issue

for Lehmer. He was a number-theorist and could sometimes even get quite annoyed with the fact that more and more money and computer time was being invested in applications.[11]
As we know from Sec. 2.1, Lehmer learned from his father that mathematics and more specifically number theory is an experimental science. This view shaped his understanding of computers within mathematics: for him, they were instruments to explore aspects of the universe of mathematics [20, p. 146]:

> There is no doubt that these new machines are creating new service jobs for mathematicians, young and old. However, it seems to me, 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

These are quite remarkable words by Lehmer: he was convinced that the computer would make it possible for the mathematician to explore objects existing in the "world" of mathematics, which were quite inaccessible before. This position stands in contrast with Von Neumann's: for Lehmer mathematics is a world worth exploring for its own sake. Despite this fundamental difference, they both situated the use of computers in mathematics in an experimental or heuristic context.

[11] This is e.g. very clear from the following quote: "*In fact, it is sometimes a little exasperating for the number theorist to assist the applied mathematician in juggling round-off errors, truncating errors and a flitting decimal point in order to adapt a problem in fluid mechanics to a discrete-variable machine when all the time the machine, being digital, is all ready to work on clear-cut problems involving whole numbers. However, I realize that this exasperation is shared by very few present. Most of you will be relieved to know that, to the best of my knowledge, very little valuable time on large-scale computing has been spent on such unprofitable problems.* [20]"

Von Neumann had a very articulated view on how to use the computer in mathematics, as is clear from what he did in and wrote on the subject. The same goes for Lehmer, but there are far more explicit statements by Lehmer on the computer's role in mathematics. In a paper, titled *Computer Technology applied to the Theory of Numbers* [23] he sums up the different possibilities for using the computer in number theory "*in order of increasing machine involvement*", answering the question "*Why might a number theorist want to add pulse circuitry to pencil and paper?*"
First of all, the machine can be used in the search for counterexamples [23, p. 118]:

> By using a machine, one's ability to explore is enormously enhanced and so one may be fortunate enough to discover at least one value of n for which the statement is patently false. This settles the question of the truth value of the statement, once and for all.

By searching for counter examples, important conjectures might be disproved. If no counter example is found, this kind of computational work is still very useful, since the truth of the conjecture tested is experimentally supported. One of the earliest examples of this method on an electronic computer was implemented by Turing in June 1950 on the Manchester University Mark I. It concerned the search for non-trivial zeros of the Riemann-zeta function for which the real part is different from 1/2, i.e., finding counter examples to the Riemann hypothesis [38, p. 99]. This approach is still used today for several different mathematical conjectures, including the Riemann hypothesis. Other famous examples are the Collatz problem and Goldbach's conjecture.
Unsuccessful searches for counter examples, or, put more positively, testing a large number of cases to verify the truth of a given conjecture, can also be used to come to a better understanding of why a given conjecture seems to be true [23]:

> Although we cannot obtain a proof by this device, there is the possibility that a careful analysis of many cases will reveal "why" the proposition is generally true and thus the machine has helped by leading to the idea of the proof. If properly directed, the machine itself can undertake this analysis.

This kind of use of the computer in mathematics is comparable to von Neumann's view on the use of the computer to build up an intuition of a given problem: by analyzing several special cases, one may come to a better understanding of a given problem and/or get better heuristic ideas to solve the problem.
Another important usage of the computer mentioned by Lehmer is the production and inspection of tables by computers [23, p. 118]:

> Most of the important classical theorems in number theory were discovered as a by-product of the production and inspection of tables. These were constructed by hand. The modern machine can produce tables with speed and reliability many orders of magnitude greater than what is humanly possible. Not only is the publication of such tables impossible; even the inspection is well beyond human capability. It soon becomes apparent that it should be the machine's responsibility to make this inspection, with, of course, a little sound advise of the programmer.

Lehmer's interest in the production and inspection of tables by computers should not be surprising. He learned from his father that they were basic tools for doing number theory. The production of tables with the aid of computers was one very early use of the electronic digital computer, as is clear from examples 2 and 3 (Sec. 3). In Sec. 4.1 we saw that von Neumann did not see any use in producing vast amounts of data by the computer, because man is not capable of processing large data sets. Also Lehmer understands this: from a given order of magnitude onward, man is no longer capable of inspecting large tables. However, this did not imply for Lehmer that computers should not be used to produce tables. If the size of the tables becomes humanly impractical, the task of inspecting tables should simply be "outsourced" to the computer itself. However, this 'automated' inspection cannot be done without the help of the programmer: he has to instruct the machine what kind of inspection it must perform. In this sense, the programmer himself must know the tables produced to some extent.[12] This kind of interaction

[12]It is interesting to point out that because of the computer, huge amounts of data have indeed become available (one only has to think of the internet). In order to handle this amount of information, one has to invent certain techniques, techniques that are in their turn internalized into the computer. Recently a new journal called *Internet Mathematics* has been founded, that is devoted to fundamental problems that occur in dealing with large complex information networks such as the Internet.

between man and machine, each making a significant contribution to the solution or study of a given mathematical problem, has been emphasized quite frequently by Lehmer (See also example 4, Sec. 3.4).
One further step in the order of increasing machine involvement is the use of the computer to verify the truth of a large but finite number of different statements. As Lehmer notes, also this kind of problem is not very suitable for humans [23, p. 119]:

> This kind of activity is not well suited to humans, not only because of the large number of different things to do, but also because of the complexities of the relationships or arrangements of the things themselves. Fortunately, the modern digital computer is not only very fast but also very adroit in handling combinatorial complexities when carefully programmed.

This kind of computer usage has had many applications. A less well-known but nonetheless equally "important" example, is the use of such methods for computing busy beaver functions $\Sigma(n, m)$, i.e., the maximum number of 1's that can be produced by a Turing machine with m states and n symbols, when started on a blank tape (See e.g. [27]). Brady, who solved one of the cases with the help of the computer, described this approach as follows [3, p. 647]:

> The four-state case has previously been reduced to solving the blank input tape halting problem of only 5820 individual machines. In this final stage of the $k = 4$ case, one appears to move into a heuristic level of higher order where it is necessary to treat each machine as representing a distinct theorem. [...] The proof techniques, embodied in programs, are entirely heuristic, while the inductive proofs, once established by the computer, are completely rigorous and become the key to the proof of [a] new and original mathematical results.

A more famous example of this method, is the verification of a huge number of cases by an IBM 370, implemented by Appel and Haken to prove the four-color theorem. Also Lehmer used this method for his machine proof on cubic residues (See Sec. 3.4). This approach is indeed an important technique in machine proofs, which are the last class of things mentioned by Lehmer, for which a computer can be used within mathematics ([23, p.119]):

> It is but a simple step from the preceding instance [exhaustive search] to one kind of mechanical "theorem proving." This is not the kind of machine proof with a "look, no hands!" point of view in which the machine starts from the postulates and proves a well known elementary theorem, *simulating* [m.i.] well established heuristic procedures in its search for a proof. Rather it is a man-machine cooperative endeavor in which the man furnishes the best information he has as to the kind of proof most likely to succeed and the machine attempts to carry out all the steps by exhaustive search.

As is clear, Lehmer was very much aware of the different ways the computer can be used in mathematics, anticipating the many ways the computer is still used today within this context. Besides pointing out the different opportunities for the mathematician offered by the computer, Lehmer made some explicit critical remarks about how and in what kind of situations the computer should be used. We already know that he attached a great value to a 'balanced' man-computer interaction. The following remark can also be situated in this context [28, p. 23]:

> A lot of the people around here know a machine, the computing machine is a place where you leave the deck and then there is a place where you pick up the paper. That's what a computing machine is. [...] And they are fighting this machine, trying to get it to respond to their demands, finally succeeding; that's what a machine is to them. They really don't have any – I guess the way we say it today: they don't have a sense of identity with the machine. We used to have, when we had "hands on" policies, you know.

The way Lehmer saw computers is very different from the way most people nowadays see and use their computers. The distance between man and his computer has only grown even more since Lehmer made this remark: It is a long way from wiring a computation on the ENIAC to mathematics software packages like Mathematica or Maple. To Lehmer, the kind of (growing) distance between man and machine he already observed in his days (as compared to the way e.g. the ENIAC was used) is connected with the fact that people take too much for granted what the machine is doing, i.e., how it works.

Another important point made by Lehmer, is his recurring emphasis on using computers for problems that are 'humanly impractical' or unfeasible. Only then it is possible to e.g. prove really new theorems, theorems that could not have been proven or even been stated by a human being. In this context, it is very important that the outcome has a certain sense of unpredictability [22, 141–142]:

> I would like to speak briefly of some theorem proving programs that we have been running in which the human is completely outclassed in what, I think you will agree, are fair contests. [...] The novelty of the theorems is guaranteed by the fact that the proofs are humanly impractical. [...] In casting about for genuine theorems the proofs of which will tax the powers of a human being, we want to exploit the speed of the machine. This means that the proof must involve many thousands of steps all sufficiently different so that the outcome cannot be forecast. We must also exploit those features of the logical system of the machine that permit it to supervise and organize its own program. We should make it proceed in an unpredictable way by laying its own track ahead of it like a caterpillar tractor. At the same time it should keep a record of where it has been, so that it can return at a previous point and branch out along another path whenever it decides that this is necessary. Humans find this kind of work difficult even when it occurs in only moderate amounts.

Maybe, one of the most important lessons to be learned from Lehmer's emphasis on man-computer interaction, the significance of using computers for problems and questions that cannot be tackled by mere human means, as well as the unpredictability involved in using the computer for such problems, is that the machine confronts the mathematician with his own mathematical shortcomings, making it necessary for him to have a little faith in what the machine has done or can do (to some extent) [23]:

> At the end of the run, the machine announces, in words introduced in advance by the programmer, that all cases have been considered and verified. Having entrusted the machine with this much responsibility, one must have faith that it performed all its instructions correctly. Those of little faith will ask: Is this really mathematics since it cannot be done at the blackboard?

Indeed, if the machine really produces a result we cannot 'produce', one is faced with the question whether the thing the computer can, but we cannot, is still mathematics. In this sense, if one is not too skeptical about using the computer for solving mathematical problems we cannot solve, the computer has not only changed the way mathematics is practiced but maybe also the way it is perceived.

5 Conclusion

How can a mere quantitative increase in computing speed give rise to a qualitative change in mathematics? Although von Neumann and Lehmer had different motivations to use the computer within mathematics, it is clear that these computer pioneers were convinced that the new electronic computer and its computational speed could be used to tackle mathematical problems in ways that would not have been possible before.
For von Neumann mathematics originates in empirics. To forget about these empirical roots leads to the degeneration of mathematics into a "disorganized mass of details and complexities". Von Neumann's interest in using computers for doing mathematics can be understood from this point of view: they allow for an experimental study of intricate mathematical problems within physics and other more down-to-earth sciences, like the phenomenon of turbulence. The computer can help to build up an intuition of problems for which the usual methods of mathematics and physics fall short. This can e.g. be done by simulating the behaviour of certain mathematical functions corresponding to some physical phenomenon, that is hard to study within an experimental physical context and asks for a high computational speed when studied in a more mathematical-theoretical setting.
Von Neumann's point of view on mathematics and the use of the computer to study it, can be contrasted to some extent with Lehmer's. According to Lehmer mathematics is in and by itself an experimental science. Connecting it with e.g. physics or biology was not his main concern, as mathematics is a universe worth to be explored for its own sake, in a way similar to the physician studying the "real" world. The computer can help the mathematician in exploring the universe of numbers: through its speed it allows the mathematician to really see and observe "the objects at close range". But Lehmer goes even further than that: the computer not only gives a more direct access to certain mathematical objects that are already known to the

mathematician, be it in an abstract way, but it might even disclose new ideas, objects and theorems within mathematics that could not have been "discovered" without the help of the computer.
Nowadays it has become more common (but not very common) to talk about mathematics as an experimental science, witness the increase in the number of books and papers on the subject and the foundation of a new journal called "Experimental Mathematics" in recent years. In this sense, the computer has really changed mathematics: not only has it given rise to new ideas and results, but it has also changed our understanding of mathematics itself on a more philosophical level. Indeed, the fact that more and more people accept that certain parts of mathematics beg for a more experimental approach is mostly due to the computer: most results discussed are results that were found with the aid of the computer's speed.
In this paper we have situated the modern use of the computer within mathematics in its proper historical context, showing that already the first electronic general-purpose digital computer, the ENIAC, was conceived as the perfect instrument to study certain (applied and theoretical) mathematical problems. Although Lehmer and von Neumann were interested in different problems and applications of the computer, they both emphasized the significance of empirical and experimental aspects of mathematics and the fact that the computer could be used within this context. It is significant to point out that, if one takes both views together, one gets a relatively complete picture of the way the computer is nowadays still used within mathematics.[13]
This kind of usage of the computer gives rise to a whole range of interesting philosophical questions that beg for more research:

- How different is mathematics from other sciences like physics?
- Has the practice of the mathematician really changed through the computer?
- Can a computer really outrun the mathematician for certain problems and what does this imply for the (philosophical) notion of proof.

[13]Of course, the actual implementations and methods used are quite different from the first ENIAC implementations, given the software and hardware development over the last 60 years. One important we want to mention, and that was not foreseen by Lehmer nor von Neumann, is the use of computer visualizations, like plots and graphs. These allow man to observe and study vast amounts of data, because they have been "summarized" in a form that can be easily accessed by humans.

I.e.what if some computer would prove a long-standing important conjecture, but nobody would really understand the proof.

- How should man-computer interaction be understood within the context of doing computer experiments?
- ...

There are several different approaches to study these related questions. In our view, one useful way to tackle these questions is the historical approach. By studying original papers and technical reports from the forties and fifties, reconstructing original computer programs and analyzing and comparing the different applications of the older electronic and general-purpose computers within mathematics, one is able to understand if and how mathematics *as it was and is practiced* has really changed through the rise of the computer.[14]

However, in the back of one's mind there should be some gratitude for the machine that has opened our eyes to a new situation in the complex universe of the integers.
Derrick H. Lehmer, 1969

References

[1] Franz L. Alt, *Archaeology of computers – reminiscences, 1945–1947*, Communications of the ACM **15** (1972), no. 7, 693–694.

[2] David H. Bailey and Richard E. Crandall, *On the random character of fundamental constant expansions*, Experimental Mathematics **10** (2001), no. 2, 175–190.

[3] Allen H. Brady, *The determination of the value of rado's noncomputable function σ for four-state turing machines*, Mathematics of Computation **40** (1983), no. 162, 647–665.

[4] Arthur W. Burks, *Preface*, 1966, in [45], 1–28.

[14] Of course before the first electronic general-purpose computers there were other computing devices in use, i.e., analogue and/or special purpose, which also deserve attention within this context.

[5] ———, *From eniac to the stored-program computer: The revolutions in computers*, 1980.

[6] Arthur W. Burks and Alice R. Burks, *The eniac: First general-purpose electronic computer*, IEEE Annals of the History of Computing **3** (1981), no. 4, 310–399.

[7] Martin Davis, *The undecidable. Basic papers on undecidable propositions, unsolvable problems and computable functions*, Raven Press, New York, 1965, Corrected republication (2004), Dover publications, New York.

[8] ———, *Mathematical logic and the origin of modern computers*, 1987, Reprinted in [14], 149–174, pp. 137–165.

[9] Liesbeth De Mol and Maarten Bullynck, *A week-end off. The first extensive number-theoretical computation on the ENIAC*, Logic and Theory of Algorithms, Fourth Conference on Computability in Europe, CiE 2008, Athens, Greece, June 2008 (Berlin) (Costas Dimitracopoulos Arnold Beckmann and Benedikt Löwe, eds.), Lecture Notes in Computer Science, Springer Verlag, 2008, Accepted for Publication.

[10] John Presper Eckert, *The eniac*, 1980, in: [16], 525–540.

[11] Roger Eckhardt, *Stan ulam, john von neumann and the monte carlo method*, Los Alamos Science (Special Issue, Stanislaw Ulam 1909-1984) **15** (1987), 131–137.

[12] W. Barkley Fritz, *Eniac – a problem solver*, Annals of the History of Computing IEEE **16** (1994), no. 1, 25–45.

[13] Herman H. Goldstine, *The computer from pascal to von neumann*, Princeton University Press, Princeton, 1972.

[14] Rolf Herken (ed.), *The Universal Turing machine*, Oxford University Press, Oxford, 1988, Republication (1994), Springer Verlag, New York.

[15] Andrew Hodges, *Alan m. turing. the enigma*, Burnett Books, London, 1983, Republication (1992), 2nd edition, Vintage, London.

[16] John Howlett, Nicolas Metropolis, and Gian-Carlo Rota (eds.), *A history of computing in the twentieth century*, Academia Press, New York, 1980, Proceeding of the International Research Conference on the History of Computing, Los Alamos, 1976.

[17] Atsushi Akera (interviewer), *Franz alt interview: January 23 and feburary 2, 2006*, ACM Oral History interviews (2006), no. 1.

[18] Derrick H. Lehmer, *On the converse of fermat's theorem*, American Mathematical Monthly **43** (1936), no. 6, 347–354.

[19] ———, *On the converse of fermat's theorem ii*, American Mathematical Monthly **56** (1949), no. 5, 300–309.

[20] ———, *Mathematical methods in large scale computing units*, Proceedings of Second Symposium on Large-Scale Digital Calculating Machinery, 1949 (Cambridge, Massachussetts), Harvard University Press, 1951, pp. 141–146.

[21] ———, *The sieve problem for all-purpose computers*, Mathematical Tabels and Other Aids to Computation **7** (1953), no. 41, 6–14.

[22] ———, *Some high-speed logic*, Experimental Arithmetic, High Speed Computing and MAthematics, Proceedings of Symposia in Applied Mathematics, vol. 15, 1963, pp. 141–376.

[23] ———, *Computer technology applied to the theory of numbers*, Studies in Number Theory (W.J. Leveque, ed.), Studies in Mathematics, vol. 6, 1969, pp. 117–151.

[24] ———, *The influence of computing on research in number theory*, The Influence of Computing on Mathematical Research and Education (J. P. LaSalle, ed.), Proceedings of Symposia in Applied Mathematics, vol. 20, 1974, pp. 3–12.

[25] ———, *A history of the sieve process*, 1980, in: [16], 445–456.

[26] Derrick H. Lehmer, Emma Lehmer, W.H. Mills, and John L. Selfridge, *Machine proof of a theorem on cubic residues*, Mathematics of computation **16** (1962), no. 80, 407–415.

[27] Shen Lin and Tibor Rádo, *Computer studies of turing machine problems*, Journal of the ACM **12** (1965), no. 2, 196–212.

[28] Robina Mapstone, *Derrick h. lehmer interview: April 18, 1973*, Computer Oral History Collection, Archives Center, National Museum of American History (Washington, DC, USA), Archives Center, National Museum of American History, 1973, p. 27.

[29] John W. Mauchly, *The eniac*, 1980, in: [16], 541–550.

[30] Scott McCartney, *Eniac: The triumphs and tragedies of the world's first computer*, Walker & Co, New York, 1999.

[31] Uta Merzbach, *Derrick h. lehmer interview: October 8, 1969*, Computer Oral History Collection, Archives Center, National Museum of American History (Washington, DC, USA), Archives Center, National Museum of American History, 1969, p. 20.

[32] Uta C. Merzbach, *John w. mauchly (1907-1980) interview: June 22, 1970*, Computer Oral History Collection (Washington, DC, USA), Archives Center, National Museum of American History, Smithsonian Institution Press, 1999, p. 58.

[33] Nicholas Metropolis, *The beginning of the monte carlo method*, Los Alamos Science (Special Issue, Stanislaw Ulam 1909-1984) **15** (1987), 125–130.

[34] 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*, Mathematical tables and other aids to Computations **4** (1950), no. 30, 109–112, Also published in [44].

[35] Hans Neukom, *The second life of eniac (+ web extras)*, IEEE Annals of the history of computing **28** (2006), no. 2, 4–16.

[36] George W. Reitwiesner, *An eniac determination of pi and e to more than 2000 decimal places*, Mathematical Tables and Other Aids to Computation **4** (1950), no. 29, 11–15.

[37] Alan M. Turing, *On computable numbers with an application to the entscheidungsproblem*, Proceedings of the London Mathematical Society (1936–37), no. 42, 230–265, A correction to the paper was published in the same journal, vol. 43, 1937, 544–546. Both were published in [7], 116–151.

[38] _____, *Some calculations of the riemann-zeta function*, Proceedings of the London Mathematical Society **3** (1953), no. 3, 99–117.

[39] Stanislaw M. Ulam, *von neumann: The interaction of mathematics and computing*, 1980, in: [16], 93–99.

[40] John von Neumann, *First draft of a report on the edvac, contract no. w-670-ord-492, moore school of electrical engineering, univiversity of pennsilvania, philadelphia.*, 1945, Also published in IEEE Annals of the History of Computing, Vol. 15, No. 4, 27-75, 1993.

[41] _____, *The mathematician*, The works of the Mind (Chicago) (R.B. Heywood, ed.), University of Chicago Press, 1947, pp. 180–196.

[42] _____, *Various techniques used in connection with random digits*, J. Resources of the National Bureau of Standards - Applied Mathematics Series **12** (1951), 36–38, Lecture given at the "Symposium on 'Monte Carlo Method"', held June-July 1949 in Los Angeles. Also published in [44], 768-770.

[43] _____, *The computer and the brain*, Yale University Press, Yale, 1958.

[44] _____, *The Collected Works V. design of computers, theory of automata and numerical analysis.*, Pergamon Press, Oxford, 1963.

[45] _____, *The general and logical theory of automata*, University of Illinois Press, Urbana, London, 1966.