# Algorithmic Number Theory Before Computers

Jeffrey Shallit
Department of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
shallit@graceland.uwaterloo.ca
http://www.math.uwaterloo.ca/~shallit

# Introduction

What is Algorithmic Number Theory?

- The design and analysis of algorithms for problems from the theory of numbers, e.g.,
  - primality testing
  - integer factorization
- The marriage of an ancient subject, number theory, with a modern one, the theory of computational complexity
- The title of a book with Eric Bach (MIT Press, 1996) that you should all go out and buy

# Algorithmic Number Theory Firsts

Algorithmic number theory can claim many "firsts":

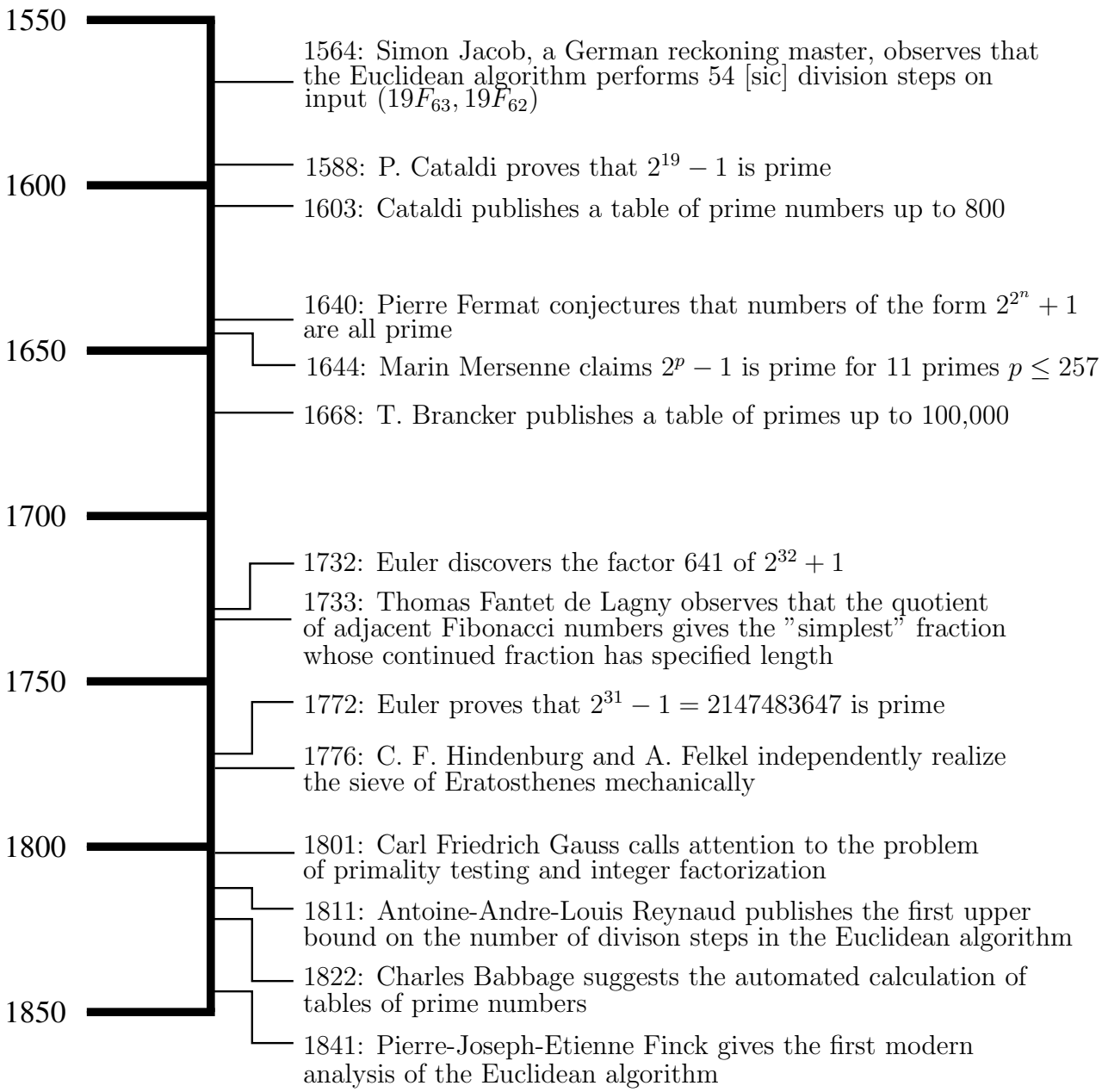
- The "first" algorithm
  - The Euclidean algorithm for computing the greatest common divisor (c. 300 B. C. E.)
- The "first" analysis of an algorithm
  - Simon Jacob (1564)
  - de Lagny (1733)
  - Reynaud (1811)
  - Léger (1837)
  - Finck (1841)
  - Lamé (1844)

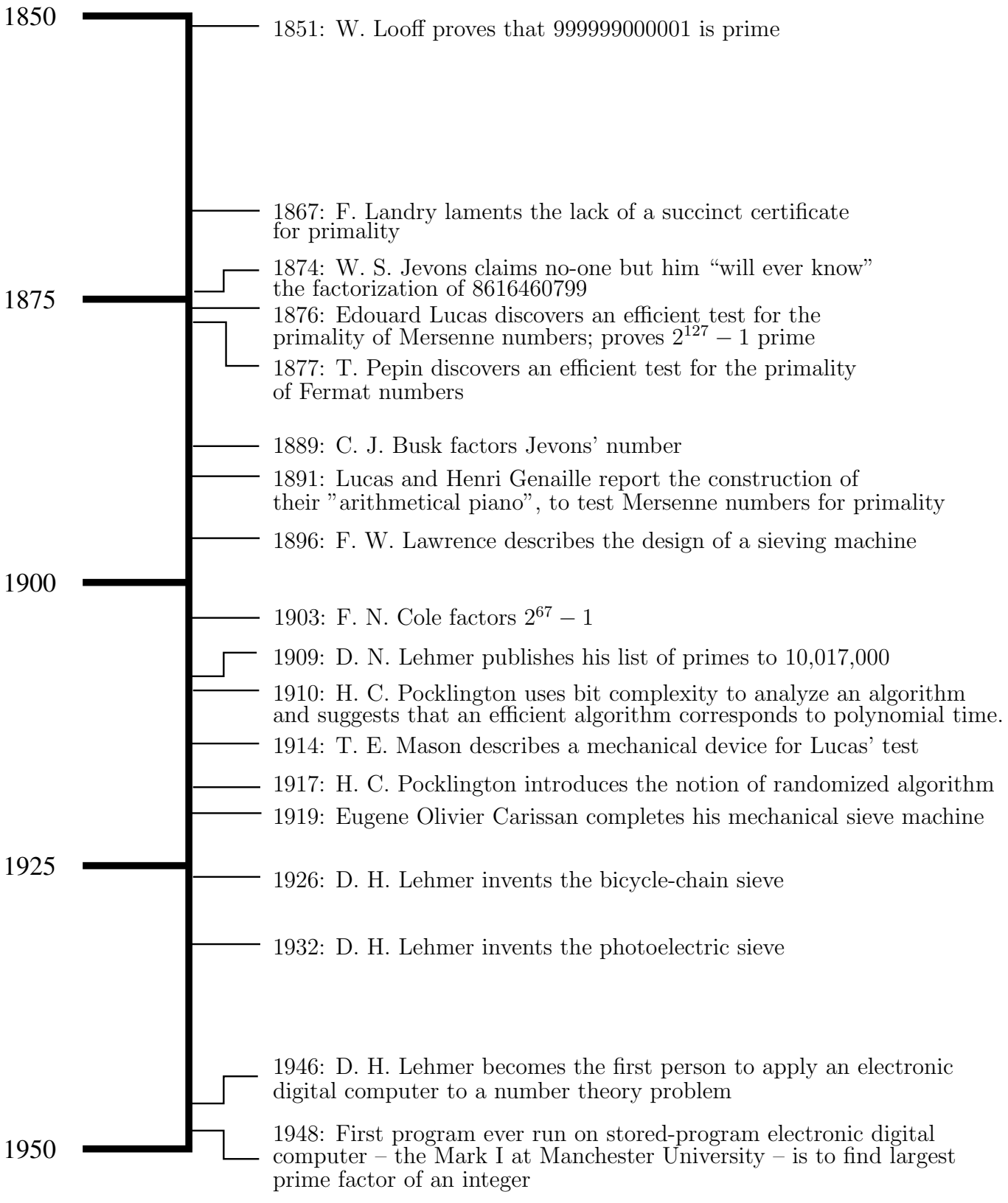
# Algorithmic Number Theory Firsts

- Recognition of the need for short certificates of membership (the class NP)
- Invention of the randomized algorithm (the class RP)
- Polynomial time as representing "efficient" algorithms (the class P)

Algorithmic number theorists have used "computers" for over two hundred years.

# Algorithmic Number Theory Before Computers: A Timeline






Prepared by Jeffrey Shallit for talk at Microsoft Research
July 13, 2001

# Algorithmic Number Theory: The Earliest Days

- Euclid's algorithm for the greatest common divisor of two integers (c. 300 B.C.E.)
- The sieve of Eratosthenes (c. 250 B.C.E.) for making a list of prime numbers (known through works of Nicomachus)
- The "extended Euclidean algorithm", which finds integers $a, b$ such that $ax+by = 1$ (when $\gcd(x, y) = 1$) was given by Arhyabhata in the Sanskrit astronomical work *Aryabhatiya*, c. 450 C.E.
- Leonardo Pisano (Fibonacci) observed c. 1200 C.E. that to tell whether a number $n$ is a prime, it suffices to divide by the integers $\leq \sqrt{n}$

# Felkel and Hindenburg

- Tables of prime numbers and factor tables were constructed starting with Fibonacci in 1202
- In 1776, both C. F. Hindenburg and A. Felkel devised machines for automating the construction of factor tables
- Brief descriptions are given in the letters of J. H. Lambert
- Felkel's machines were even offered for sale to the general public

Lambert to Rosenthal, c. February 1776:

*I obtained the enclosed paper from its author in Vienna. This gentleman [Felkel] is planning to create a machine for simplified discovery of divisors as well as a table that covers the numbers 1 to 144,000.*

# Felkel and Hindenburg

Felkel to Lambert, January 15 1776:

*After examining certain mathematical rules I have come to the conclusion that it would be important to find an apparatus that computes the factors of the numbers...*

*My computations were initially carried out according to a particular standard which could be eventually transformed into a machine. With a small movement this machine would not only show all the numbers that are divisible by a particular factor but also all the other factors of a number. After completion of the work I see that I could have easily finished everything within a month. It took me 2 months to finish the project.*

# Carl Friedrich Gauss

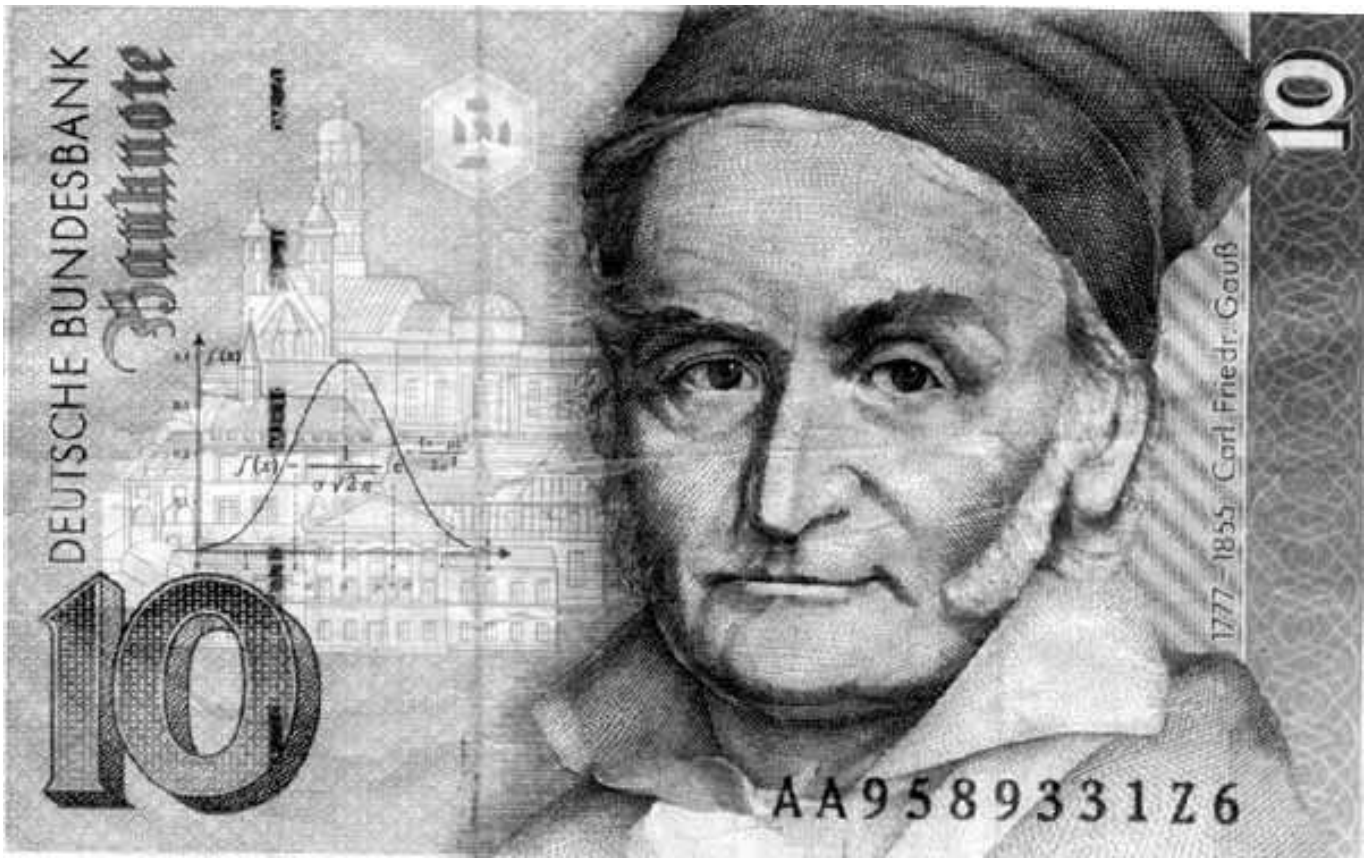



Figure 1: Carl Friedrich Gauss (1777–1855)

# Carl Friedrich Gauss

*The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length.*

*Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that even for numbers that do not exceed the limits of tables constructed by estimable men, i.e. for numbers that do not yield to artificial methods, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers.*

# Carl Friedrich Gauss

*Even though the tables, which are available to everyone and which we hope will continue to be extended, are indeed sufficient for most ordinary cases, it frequently happens that the trained calculator will be sufficiently rewarded by reducing large numbers to their factors so that it will compensate for the time spent.*

*Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.*

# Charles Babbage: the Irascible Genius

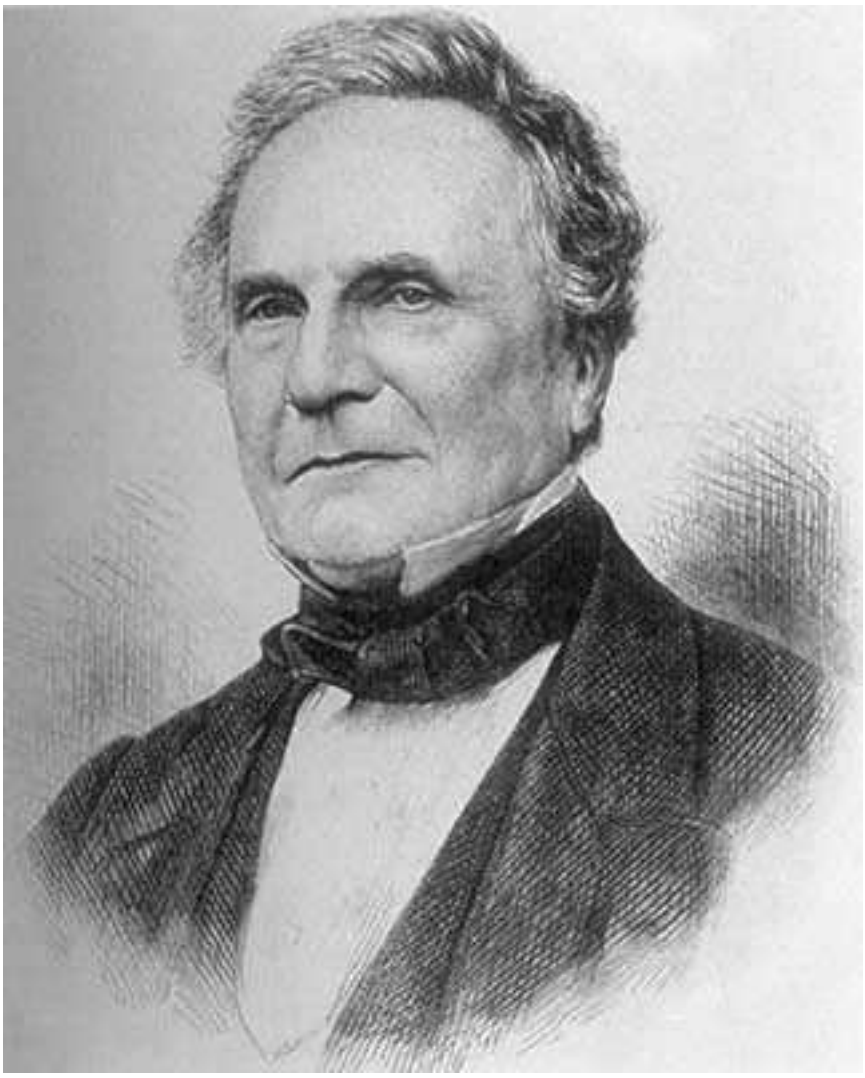


Figure 2: Charles Babbage (1791–1871)

## Charles Babbage: the Irascible Genius

Charles Babbage, letter to the Astronomical Society of London, June 2, 1822:

*I have taken the method of differences as the principle on which my machinery is founded; and in the engine which is just finished I have limited myself to two orders of differences. With this machine I have repeatedly constructed tables of squares and triangular numbers, as well as a table from the singular formula* $x^2 + x + 41$, *which comprises amongst its terms so many prime numbers.*

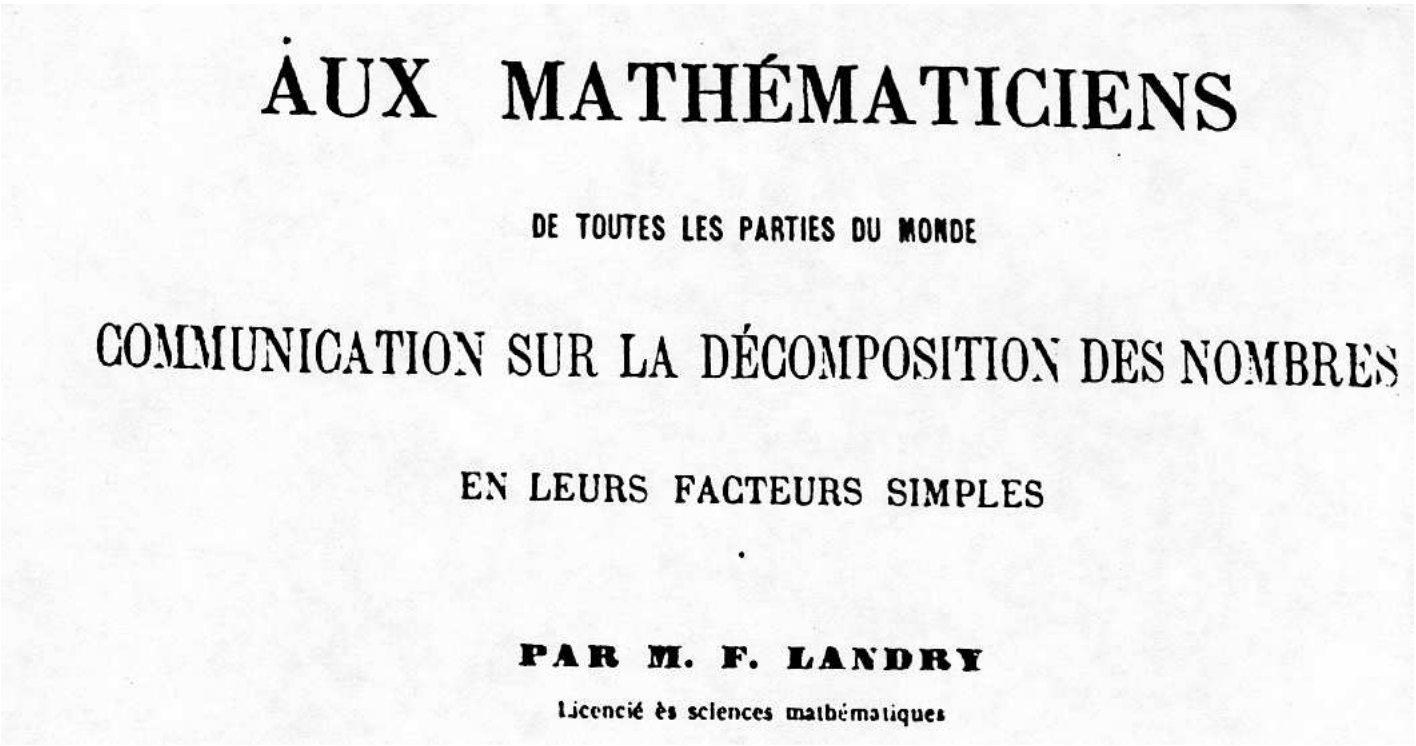
## Charles Babbage: the Irascible Genius

Charles Babbage, letter to Sir Humphry Davy, July 3, 1822:

*The computed table is presented to the eye at two opposite sides of the machine; and a friend having undertaken to write down the numbers as they appeared, it proceeded to make a table from the formula* $x^2 + x + 41$. *In the earlier numbers my friend, in writing quickly, rather more than kept pace with the engine; but as soon as four figures were required, the machine was at least equal in speed to the writer...*

*I have also certain principles by which, if it should be desirable, a table of prime numbers might be made, extending from 0 to ten millions.*

# Fortuné Landry



AUX MATHÉMATICIENS

DE TOUTES LES PARTIES DU MONDE

COMMUNICATION SUR LA DÉCOMPOSITION DES NOMBRES

EN LEURS FACTEURS SIMPLES

PAR M. F. LANDRY

Licencié ès sciences mathématiques

*At this point we are, if not uneasy, then at least somewhat embarrassed.*

*Indeed, when one has succeeded in factoring a number, and has given its factors, this can be verified immediately. But it is a different matter when the methods used fail to discover any factor, and one then asserts that the number is prime. How could one then transmit to another such a totally personal conviction? Who*

*would be convinced, without having redone all the calculations, and without having understood the principles on which those calculations were based?*

*We understand well that our claim is valid only as an assertion, worthwhile until someone proves the contrary, or until we make known our methods and enable others to apply them.*

# William Stanley Jevons

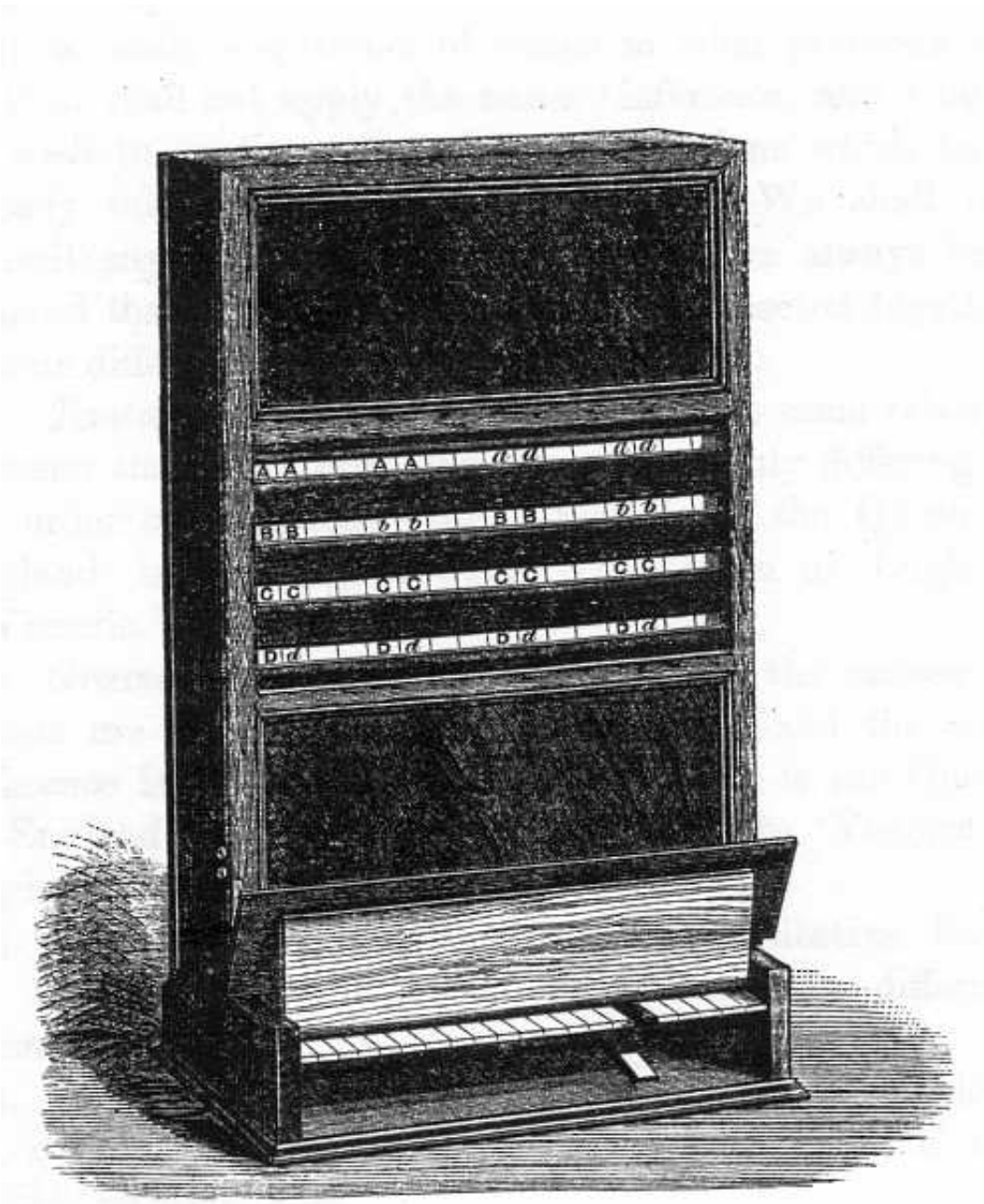
Figure 3: William Stanley Jevons (1835–1882)

# William Stanley Jevons

From his book *The Principles of Science*, 1874:

Given any two numbers, we may by a simple and infallible process obtain their product, but it is quite another matter when a large number is given to determine its factors. Can the reader say what two numbers multiplied together will produce the number 8,616,460,799? I think it unlikely that any one but myself will ever know; for they are two large prime numbers, and can only be rediscovered by trying in succession a long series of prime divisors until the right one be fallen upon. The work would probably occupy a good computer for many weeks, but it did not occupy me many minutes to multiply the two factors together. Similarly there is no direct process for discovering whether any number is a prime or not; it is only by exhaustingly trying all inferior numbers which could be divisors, that we can show there is none...

# William Stanley Jevons



THE LOGICAL MACHINE.

Figure 4: The logical machine of Jevons

# Edouard Lucas

Figure 5: Edouard Lucas (1842–1891)

## Lucas' Primality Test for Mersenne Numbers

To test $n = 2^p - 1$ for primality:

Set

$$\begin{aligned} a_1 &= 4 \\ a_{k+1} &= a_k^2 - 2 \pmod{n} \end{aligned}$$

Then $n$ is prime if and only if $a_{p-1} \equiv 0 \pmod{n}$.

Example.

$n = 2^5 - 1 = 31$

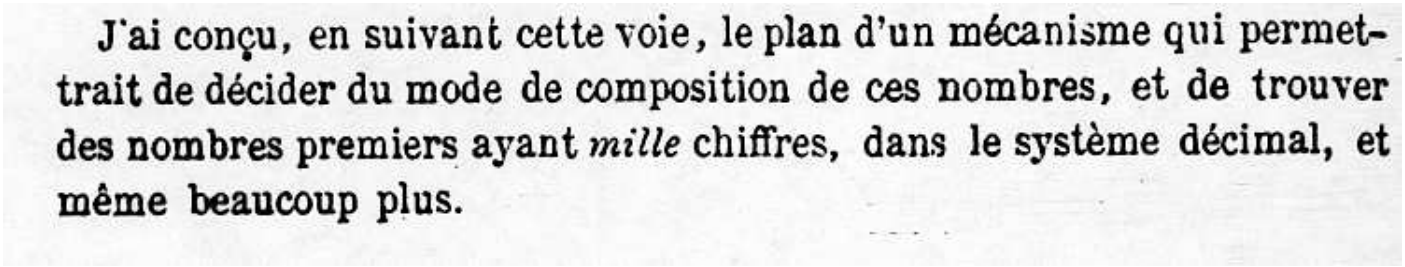
$$\begin{aligned} a_1 &= 4 \\ a_2 &= a_1^2 - 2 = 14 \\ a_3 &= a_2^2 - 2 = 194 \equiv 8 \pmod{31} \\ a_4 &= a_3^2 - 2 = 62 \equiv 0 \pmod{31} \end{aligned}$$

Therefore $n$ is prime.

# Lucas and Machines

Lucas made many remarks about automating his test.

From *Assoc. Française pour l'Avancement des Sciences; Comptes Rendus*", 1876:



J'ai conçu, en suivant cette voie, le plan d'un mécanisme qui permettrait de décider du mode de composition de ces nombres, et de trouver des nombres premiers ayant *mille* chiffres, dans le système décimal, et même beaucoup plus.

*I have conceived, in following this path, the plan of a mechanism which will permit one to discover whether these numbers are prime or composite, and to find prime numbers having one thousand digits, in the decimal system, and even much larger.*

# Lucas and Machines

From *Bull. Biblio. Storia Sci. Mat. Fis.* **10** (1877):

*I will only observe for the moment that I have created the plan of a mechanism which will permit one to decide almost instantaneously if the assertions of Father Mersenne and Baron Plana, mentioned in this note, on the numbers*

$$2^{53}-1, \quad 2^{67}-1, \quad 2^{127}-1, \quad 2^{257}-1$$

*which they believed to be primes, are correct.*

# Lucas and Henri Genaille

From *Assoc. Française pour l'Avancement des Sciences; Comptes Rendus*", 1891:

*Arithmetical piano for the verification of large prime numbers. — The arithmetical piano allows one to give a practical follow-up to the method formulated by Mr. E. Lucas, at the Clermont-Ferrand conference, for the verification of large prime numbers. By the simple movement of some pegs, the verification of prime numbers of the form* $2^n - 1$ *is reduced in the majority of cases to several hours' work. This machine, which may automatically perform the most important calculations, will one day realize the goal of a calculating machine which peforms arithmetic operations by itself.*

# Thomas E. Mason

In 1914, Mason (1883–1939) published a brief article in which he suggested building a machine for Lucas' test:

*It would be possible to construct a machine which would have two parallel bars in which could be set pins for the places where* $1$ *occurs in the number. The pins on one bar would be in reverse order. The bars could be turned over and the number of pins striking could be recorded automatically...*

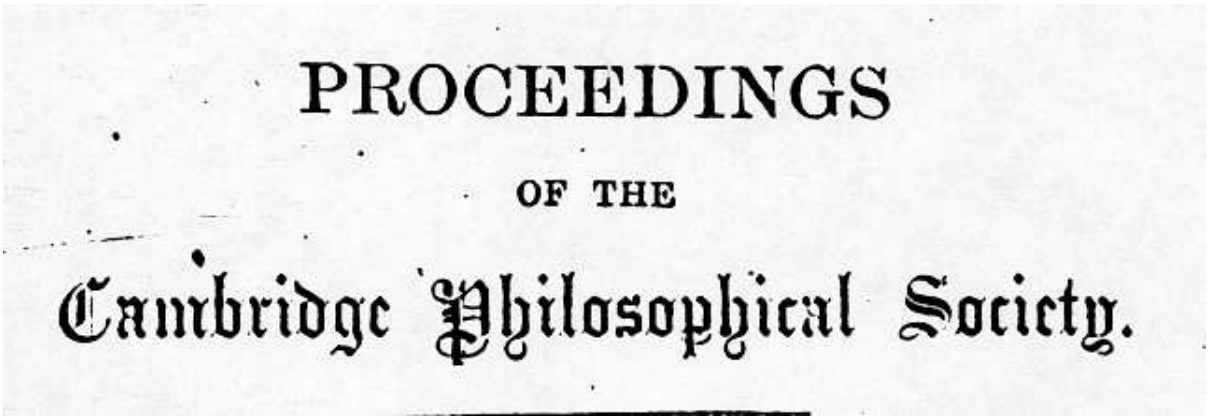
# Henry C. Pocklington

From *Proc. Cambridge Philosophical Soc.* **18** (1914):

*This method has the disadvantage that we only (excepting in rare cases) determine whether N is is prime or composite and that we may require to factorize* $N-1$ *in part at least. The advantage lies in the fact that the labour increases approximately as* $(\log N)^3$*, not as* $\sqrt{N}$*, which makes it a much easier method than that of the Idoneals if* $N$ *is large. It is also well adapted for use with the arithmometer.*

# Henry C. Pocklington

From *Proc. Cambridge Philosophical Soc.* **19** (1917):



PROCEEDINGS

OF THE

Cambridge Philosophical Society.

1. The solution of congruences by exclusion methods, although easy enough when the modulus is moderately large, becomes impracticable for large moduli because the labour varies as the modulus or its square root. In a direct method the labour varies roughly as the cube of the number of digits in the modulus, and so remains moderate for large moduli. The object of this paper is to develop the direct method. We take $x^2 \equiv a$, mod. $p$, first, discussing the cases where $p = 4m + 3$ and $p = 8m + 5$ in § 2 and that where $p = 8m + 1$ in § 3. We next take $x^2 \equiv a$ and discuss the cases where $p = 3m + 2$, $p = 9m + 4$ and $p = 9m + 7$ in § 4 and that where $p = 9m + 1$ in § 5.

* We have to do this by trial, using the Law of Quadratic Reciprocity, which is a defect in the method. But as for each value of $u$ half the values of $t$ are suitable, there should be no difficulty in finding one.

# Factoring by Sieving

Suppose we want to factor the number $N = 611$. One way to do this is to express $N$ as the difference of two squares

$$N = x^2 - y^2 = (x - y)(x + y).$$

Now any perfect square must be congruent to either $0$, $1$, or $4$ (modulo $8$), and $611 \equiv 3 \pmod 8$. Therefore, we can only have $x^2 \equiv 4 \pmod 8$ and $y^2 \equiv 1 \pmod 8$. It follows that $x \equiv 2 \pmod 4$.

Similarly, since any perfect square can only be congruent to $0$ or $1$ (modulo $3$), and $611 \equiv 2 \pmod 3$, we must have $x^2 \equiv 0 \pmod 3$, and $y^2 \equiv 1 \pmod 3$. Hence $x \equiv 0 \pmod 3$.

# Factoring by Sieving (Continued)

Continuing in this way, we find that $x$ must satisfy the following system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 0, 1, 4 \pmod 5 \\ x &\equiv 2, 3, 4, 5 \pmod 7 \end{aligned}$$

The least solution to this system is $x = 30$, and for this value we find $y = 17$. Hence

$$N = 611 = (x - y)(x + y) = 13 \cdot 47.$$

# Mechanical Sieving

- Apparently first proposed by in 1896 by Frederick William Lawrence; but he did not actually construct a sieve
- André Gérardin published a French translation of Lawrence's paper in his review, *Sphinx-Oedipe*
- This inspired Russian engineer Maurice Kraitchik to construct a sieve model in 1912, made of wood
- Gérardin himself built a sieve prototype in 1912 out of paper loops

# The Work of Pierre and Eugène Carissan

- Pierre Carissan, a French high-school mathematics teacher, designed a sieve prototype in 1912, which was built by his brother Eugène Olivier Carissan, but it also was ineffective
- In 1913–1914, Eugène Olivier Carissan, at the time a lieutenant in the French infantry, began his development of a 2nd automatic numerical sieving device
- But the work was halted due to the outbreak of World War I, and the machine was not completed until 1919

# Carissan's Sieve Machine

- Built by the Paris firm of Chateau Frères
- Dimensions: 27cm $\times$ 33cm $\times$ 12cm
- Used 14 congruence rings (circular rings made of brass)
- The moduli were:

  $19, 21, 23, 26, 29, 31, 34, 37, 41, 43, 47, 53, 55, 59$

- Displayed at the *Exposition Publique de Machines à Calculer* in Paris, 5–13 June 1920.
- Could examine 35–40 numbers per second
- It could factor

  $225058681 = 229 \cdot 982789$ in 3 mins.

  $3450315521 = 1409 \cdot 2418769$ in 2 mins.

  $3570537526921 = 841249 \cdot 4244329$ in 18 mins.

  (note $841249 = 277 \cdot 3037$)

# Sieve Developments

- D. H. Lehmer (1905–1991) built many sieves, starting in 1927
- His DLS-127 and DLS-157 achieved $10^6$ trials/sec
- Sieving was the most efficient way to factor large numbers until about 1970
- H. C. Williams and co-workers have achieved $2 \times 10^8$ trials/sec.
- Bronson and Buell have achieved $10^9$ trials/sec
- Sieving is still used for calculations in number theory; e.g., determination of pseudosquares