Discovery of a Lost Factoring Machine

Jeffrey Shallit
Department of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
shallit@graceland.uwaterloo.ca

The slides for this talk can be found on my home page:
http://math.uwaterloo.ca/~shallit/

Joint work with H. C. Williams (Manitoba) and F. Morain (École Polytechnique).

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
- 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:

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

- Could therefore potentially be used to factor numbers with as many as 21 decimal digits
- Displayed at the *Exposition Publique de Machines à Calculer* in Paris, 5–13 June 1920.
- Could examine 35–40 numbers per second
- But what happened to this machine?

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 2×10^8 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

Epilogue

- The Carissan machine found a new home at the Conservatoire National des Arts et Métiers in Paris in June 1994.

For Further Reading

1. Jeffrey Shallit, Hugh C. Williams, and François Morain, Discovery of a lost factoring machine, *Math. Intelligencer*, **17** (1995), 41–47.

2. R. F. Lukes, C. D. Patterson, and H. C. Williams, Numerical sieving devices: their history and some applications, *Nieuw Archief v. Wiskunde* **13** (1995), 113–139.