CWI Quarterly

Volume 7 (4) 1994, pp. 281 – 283

Introduction to the Special Issue on Computational Number Theory

H.J.J. te Riele

CWI, Department of Numerical Mathematics,
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
e-mail: herman@cwi.nl

The numbers by which we count and the rational numbers have always been the subject of intensive study by amateur and professional number-theorists. The ancient Greeks already knew perfect numbers (which are equal to the sum of their proper divisors, like 28) and amicable pairs. The invention of electronic digital computers has stimulated many new developments in number theory: the discovery, in 1978, of cryptographic systems which are based on the difficulty of decomposing large numbers into their prime factors, provided an elegant application of number theory in cryptography and raised new interest in the classical problems of factorization and primality testing. Many other applications of number theory (e.g., in acoustics, long-range signal transmission, crystallography) are described in [1, 6, 9]. The increasing role of computers in number theory has stimulated the development of a new field of science now known as *Computational (or Algorithmic) Number Theory.* On the one hand, the computer is used here as an experimental tool to generate and test number-theoretic hypotheses; on the other hand, the computer has stimulated the need for ever more efficient number-theoretic algorithms, and has led to several new deep mathematical results [2, 5, 7, 8].

One of the pioneers in the science of computing, and in the field of computational number theory was Derrick Henry Lehmer, who passed away on May 21, 1991. Already before the era of digital computers he built his own special-purpose hardware for solving so-called sieve problems [4] (to which various number-theoretic problems can be reduced). Together with Raymond Clare Archibald, he was the founder, in 1943, of the journal "Mathematical Tables and other Aids to Computation"; in 1960, the name of the journal was changed into "Mathematics of Computation". For the larger part it is devoted to numerical algorithms and their mathematical analysis and computer implementation, but traditionally another substantial part of the journal covers

subjects from computational number theory [3]. A special issue (Volume 61, Number 203, July 1993) has honoured D.H. Lehmer and illustrated his great merits for computational number theory.

This special issue of CWI Quarterly contains three contributions. The first, by H.J.J. te Riele and J. van de Lune, describes the main computational number theory research at CWI conducted by the two authors in the period 1970 – 1994. Highlights were the numerical verification of the Riemann hypothesis for the first 1.5×10^9 complex zeros of the Riemann zeta function, where for the first time a massive amount of (otherwise idle) supercomputer time was used, and the disproof of the Mertens conjecture, also with the help of a supercomputer (joint work of A.M. Odlyzko and H.J.J. te Riele). Both results have stimulated a growing belief among experts in the truth of the Riemann hypothesis. In the second paper, P.L. Montgomery presents a survey of modern integer factorization algorithms. He was a visiting researcher at CWI and Leiden University in 1993 – 1994[1]. The present state-of-the-art of factorization could not have been reached without his algorithmic and implementational contributions. The third paper is a contribution by T.J. Dekker on the calculation of prime numbers in quadratic fields having the unique factorization property. These primes can be represented naturally in the plane, and several nice pictures of prime patterns are displayed which undoubtedly will evoke some aesthetical pleasure to the reader. At the occasion of the 1954 International Congress of Mathematicians in Amsterdam, a table-cover containing one of these prime number patterns (the so-called Gauss ring $[\sqrt{-1}]$) was distributed by the Mathematical Centre (presently CWI); probably, these covers now are collector's items.

References

1. S.A. Burr, editor (1992). *The Unreasonable Effectiveness of Number Theory*, volume 46 of *Proceedings of Symposia in Applied Mathematics*, American Mathematical Society, Providence, RI.
2. H. Cohen (1993). *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, Berlin.
3. W. Gautschi editor (1994). *Mathematics of Computation 1943–1993: a Half-Century of Computational Mathematics*, volume 48 of *Proceedings of Symposia in Applied Mathematics*, American Mathematical Society, Providence, RI.
4. R.F. Lukes, C. Patterson, and H. Williams (1995). Numerical Sieving Devices: Their History and Some Applications. *Nieuw Archief voor Wiskunde*, **13**(1):113–139.
5. M. Pohst and H. Zassenhaus (1989). *Algorithmic algebraic number theory*. Encyclopedia of Mathematics and Applications. Cambridge University Press, Cambridge etc.

[1] This visit was funded by the Thomas Stieltjes Institute for Mathematics (Leiden) and by CWI.

6. M. SCHROEDER (1984). *Number Theory in Science and Communication.* Springer-Verlag, Berlin etc..
7. R. D. SILVERMAN (1991). A Perspective on Computational Number Theory. *Notices of the Amer. Math. Soc.*, **38**(6):562–568.
8. R. S. VARGA (1990). *Scientific computation on mathematical problems and conjectures.* SIAM, Philadelphia, Pennsylvania.
9. M. WALDSCHMIDT, P. MOUSSA, J.-M. LUCK and C. ITZYKSON, editors (1992). *From Number Theory to Physics*, Berlin etc. Springer–Verlag, Berlin, etc.