H. G. Kolsky
Date ?
probably
1961
or
earlier

COMPUTER APPLICATIONS IN THE FIELD OF NUMBER THEORY

by

H. M. McAndrew

International Business Machines Corporation
Thomas J. Watson Research Center
Yorktown Heights, New York

1. INTRODUCTION

Recent number-theoretic work using computers has been of mainly two types. Firstly, there have been calculations of specific numbers or sequences which are of interest for their own sakes; examples include the sequence of primes, particular large primes, Mersenne primes and perfect numbers. Secondly, there have been attempts to disprove various outstanding conjectures or at least to produce sufficient numerical evidence to suggest whether or not the conjecture is true; examples of this kind include the work on Fermat's Last Theorem and the Riemann hypothesis. Yet another use for a computer, with even greater potential value, is as a conjecture-generator rather than a conjecture-prover. The computer can produce rapidly a large amount of data in which, by a combination of human ingenuity and machine processing, one can hope to recognize patterns. Most conjectures, of course, arise in this way. The mathematician observes a pattern valid on a limited possibly finite range of systems, hypothesises that this pattern holds over a wider range and then attempts to prove that this is so. To use a computer in this process requires a suitable mixture of luck and mathematical insight; supported hopefully, by a greater understanding of the general problem of pattern recognition, both how humans do it and how we can program machines to do it.

2. SPECIFIC PROBLEMS

The following is a description of some outstanding Number-Theoretic problems and conjectures for which a computer may serve as a useful tool. The list is by no means exhaustive, but reflects the interest of the author.

(i) The Riemann hypothesis.

"The non-trivial zeros of the Riemann zeta-function $\zeta(s)$ lie on the line $\mathrm{Re}(s) = 1/2$". As early as 1935 a series of calculations was made by Titchmarsh (1) who showed the hypothesis to be true for the first 195 zeros. Later calculations (2, 3, 4, 12) have verified the conjecture for the first 35,337 zeros. At first sight this appears overwhelming evidence for the truth of the hypothesis, however, as pointed out in (4), there is an observed tendency for the zeta function to behave more capriciously as $t = \mathrm{Im}(s)$ increases. For example, Gram's Law, the truth of which would have implied the truth of the Riemann Hypothesis, is almost universally true for small t but is broken with increasing frequency as t increases. This and other effects are connected with the nature of the asymptotic series generally used to approximate $\zeta(s)$ in the region $0 < \mathrm{Re}(s) < 1$. Each term of the series is a "smooth" function of s and only $O(t^{1/2})$ terms are required to approximate $\zeta(s)$ to the required accuracy. The large

initial terms contribute the sort of regular behaviour to $\zeta(s)$ which would make the Riemann Hypothesis true. When, if ever, the hypothesis breaks down it must be where contributions from a large number of smaller terms mutually reinforce and outweigh the larger terms. On rough heuristic arguments of this type one expects the hypothesis to be valid up to fairly large values of t so that the numerical evidence already available still leaves open a reasonable possibility that the hypothesis is false. Further numerical work could be designed to either increase the present known range of validity or to look in suitably chosen intervals **far** along the line $\mathrm{Re}(s) = 1/2$.

(ii) Fermat's Last Theorem.

"There are no non-trivial integral solutions of $x^n + y^n = z^n$ for $n > 2$". This, probably the most familiar unsolved problem in the whole of mathematics, has been the subject of much numerical work since the advent of fast computers. It is sufficient to restrict one's attention to the case of n prime; now the problem splits naturally into two cases $n \nmid xyz$ and $n \mid xyz$. Results of computations (5, 6, 7, 8) have shown that the hypothesis is true in the first case for $n < 253,747,889$ and in the second case for $n < 4002$. (9, 10, 11.) Here the numerical evidence overwhelmingly suggests the truth of the conjecture; future nu-

merical work should probably wait on new theoretical methods for increasing the range of validity more rapidly.

A stronger form of Fermat's Last Theorem was conjectured by Euler, namely, that for no integral $x_1, x_2, \ldots, x_k$ with $k > 2$,

$$\sum_{i=1}^{k-1} x_i^k = x_k^k.$$

Little numerical work has been carried out in an attempt to disprove this conjecture.

(iii) Fermat Primes.

Fermat conjectured that all $F_n = 2^{2^n} + 1$ are prime and verified this for $n = 1,2,3,4$. Euler, however, found in 1732 that F_5 is composite. It is now known that F_7, F_8, F_9, F_{10}, F_{11}, F_{12}, F_{13} and several larger F_n are composite. Fermat's conjecture was singularly unfortunate in that not one case of F_n prime has been found other than the first four. It is now of interest to ask whether there are any further Fermat primes or whether F_1, F_2, F_3, F_4 form the complete set.

(iv) Mersenne Primes and Perfect Numbers.

A perfect number is a number n the sum of whose divisors, including 1 but excluding n, is n. A Mersenne prime is a prime

of form 2^p-1. It is known that an even perfect number must be of the form $2^{p-1}(2^p-1)$, where 2^p-1 is a Mersenne prime; whether or not there exists an odd perfect number is an unsolved problem. Several authors (13, 14, 15, 16, 17, 18) have extended the list of Mersenne primes by using computers and also listed factors of the composite Mersenne numbers 2^p-1. The present count of Mersenne primes, and hence the count of perfect numbers, stands at 20, all candidates up to $2^{5000}-1$ having been tested.

(v) Goldbach's Conjecture.

"Every even number > 2 is the sum of two primes". The truth or falsity of this conjecture is still an open question. Since numerical evidence and probabilistic argument suggest strongly that the conjecture is true, a computer might well be used in a search for a stronger form of the conjecture, such as "every even number $n > 2$ is the sum of two primes each greater than $n/2 - f(n)$" for some $f(n)$. On arguments of probabilistic type, which usually give the correct order of magnitude in problems of this type, the best possible $f(n)$ should be $0(\log^2 n)$.

(vi) Kummer's Conjecture.

Kummer (19) showed that

$$x_p = 1 + 2 \sum_{\nu=1}^{\frac{p-1}{2}} \cos \left(\frac{2\pi\nu^3}{p}\right)$$

for all $p \equiv 1 \pmod 3$ satisfies

$$f(x) \equiv x^3 - 3px - pA = 0,$$

where A is uniquely determined by

$$4p = A^2 + 2 > B^2, \quad A \equiv 1 \pmod 3.$$

f(x) has three real roots for each p. Kummer classified the primes $p \equiv 1 \pmod 3$ according as x_p is the largest, middle or smallest zero of f(x) and conjectured that the asymptotic frequencies for these classes are 1/2, 1/3, 1/6. Kummer tested this conjecture by evaluating the first 45 of the x_p and finding densities of .5333, .3111, .1556. A later computation (20) indicated a departure from the conjectured densities and a trend toward randomness. However, only the first 611 x_p were calculated; a more extensive calculation could now be performed on high speed machines and would give more significant evidence as to the truth or falsity of the conjecture.

(vii) Ramanujan's Function $\tau(n)$.

This is defined by $\prod_{\nu=1}^{\infty} (1 - x^{\nu})^{24} = \sum_{n=1}^{\infty} \tau(n)\, x^{n-1}$. It was noted by Ramanujan that $\tau(n)$ is multiplicative; that is, $\tau(m)\tau(n) = \tau(mn)$ for coprime integers m, n. There is also a recurrence relation (21) connecting $\tau(p)$, $\tau(p^{\alpha})$ and $\tau(p^{\alpha+1})$. Hence $\tau(n)$ may be found readily once $\tau(p)$ is known for all p. As to $\tau(p)$, no explicit formula for it has yet been discovered.

Ramanujan conjectured that $|\tau(p)| < p^{11/2}$ and regarded the truth of this as "highly probable" though he verified only the first ten cases. Lehmer (22) verified the conjecture for the first 46 primes.

A further interesting question connected with $\tau(n)$ is whether or not $\tau(n) = 0$ for any n. In (23) it is shown that $\tau(n) \neq 0$ for $n < 3,316,799$.

(viii) The Series of Primes.

Conjectures connected with the distribution of primes are legion. It is known (Dirichlet) that any arithmetic sequence which does not exclude primes trivially contains infinitely many primes; very little is known of the distribution of primes in a quadratic sequence (29).

A conjecture of a purely numerical nature still outstanding is the point at which $\pi(x) - \ell i(x)$ first changes signs, where $\pi(x)$ is the number of primes less than or equal to x and $\ell i(x) = \int_0^x \frac{dt}{\log t}$. It is known that $\pi(x) - \ell i(x)$ changes sign infinitely often and it has been computed (24) for x as large as 10^{10}, no sign change having been found yet. An upper bound for the first sign change was deduced in (25) and is the rather discouraging figure of $10^{10^{10^{10^3}}}$. The actual point is certainly much lower than this and may well be within the range of this or the next generation of

computers.

(ix) Wilson's Theorem and Fermat's Theorem.

Wilson's Theorem states that $(p-1)! \equiv -1 \pmod{p}$; Fermat's Theorem states that, for $p \nmid a$, $a^{p-1} \equiv +1 \pmod{p}$. It is natural to ask for what values of a,p can $(p-1)! \equiv -1 \pmod{p^2}$ or $a^{p-1} \equiv 1 \pmod{p^2}$. The second possibility has applications to the first case of Fermat's Last Theorem. It is know that $4! \equiv -1 \pmod{5^2}$ and $12! \equiv -1 \pmod{13^2}$. Goldberg (26) computed Wilson Remainders for all $p < 10^4$ and found just one further example, $562! \equiv -1 \pmod{563^2}$. Fröberg (27) found no further example in $10^4 < p < 3.10^4$. In the latter paper all solutions of $2^{p-1} \equiv -1 \pmod{p^2}$ in $p < 5.10^4$ were computed; there are two such, 1093 and 3511. Kravitz (28) found no further example in $p < 10^5$.

References

(1) Titchmarsh, E. C., "The Zeros of the Riemann Zeta-Function", Proc. Roy. Soc. A. 151, (1935) pp. 234-255.

(2) Titchmarsh, E. C., "The Zeros of the Riemann Zeta-Function", Proc. Roy. Soc. A. 157, (1936) pp. 261-263.

(3) Turing, A. M., "Some Calculations of the Riemann Zeta-Function", Proc. Lond. Math. Soc. (3) 3, (1953) pp. 99-116.

(4) Lehmer, D. H., "On the Roots of the Riemann Zeta-Function", Acta. Math. 95, (1956) pp. 291-297.

(5) Meissner, W., "Uber die Tielbarkeit von $2^p - 2$ durch das Quadrat der Primzahl p = 1093", Akad. d. Wiss, Berlin, Sitzungsb., 35, (1913), pp. 663-667.

(6) Beeger, N.G.W.H., Messenger Math., 51, (1922) pp. 149-150.

(7) Western, A. W., (unpublished).

(8) Lehmer, D. H., and Lehmer, Emma, "On the First Case of Fermat's Last Theorem", Bull. Amer. Math. Soc. 47, (1941) pp. 139-142.

(9) Lehmer, D. H., Lehmer, Emma, and Vandiver, H. S., "An Application of High-Speed Computing to Fermat's Last Theorem", Proc. Nat. Acad. Sci. 40, (1954) pp. 25-33.

(10) Vandiver, H. S., "Examination of Methods of Attack on the Second Case of Fermat's Last Theorem", Proc. Nat. Acad. Sci. 40, (1954) pp. 732-735.

(11) Selfridge, J. L., Nicol, C. A., and Vandiver, H. S., "Proof of Fermat's Last Theorem for all Prime Exponents Less than 4002", Proc. Nat. Acad. Sci. 41, (1955) pp. 970-973.

(12) Meller, N. A., "Computations Connected with the Check of the Riemann Hypothesis", Dokl. Akad. Nauk. SSSR 123, (1958) pp. 246-248.

(13) Riesel, H., "Mersenne Numbers", M.T.A.C. 12, (1958) pp. 207-213.

(14) Scheffler, D., and Ondrejka, R., "The Numerical Evaluation of the Eighteenth Perfect Number", Math. Comp. 14, (1960) p. 199.

(15) Brillhart, J., and Johnson, G. D., "On the Factors of Certain Mersenne Numbers", Math. Comp. 14, (1960), pp. 365-369.

(16) Kravitz, S., "Divisors of Mersenne Numbers, $10,000 < p < 15,000$", Math. Comp. 15, (1961) pp. 292-293.

(17) Karst, E., "New Factors of Mersenne Numbers", Math. Comp. 15, (1961) p. 51.

(18) Selfridge, J. L., (unpublished).

(19) Kummer, E. E., "De Residuis Cubicis Disquisitiones Nannullae Analyticae", J. fur reine angew math. 32, (1846) pp. 341-345.

(20) von Neumann, J., and Goldstine, H. H., "A Numerical Study of a Conjecture of Kummer", M.T.A.C. 7, (1953) pp. 133-134.

(21) Mordell, L. J., "On Mr. Ramanujan's Emperical Expansion of Modular Functions", Proc. Camb. Phil. Soc. 19, (1917) pp. 117-124.

(22) Lehmer, D. H., "Ramanujan's Function $\tau(n)$", Duke Math. J. 10, (1943) pp. 483-492.

(23) Lehmer, D. H., "The Vanishing of Ramanujan's Function $\tau(n)$", Duke Math. J. 14, (1947) pp. 429-433.

(24) Lehmer, D. H., "On the Exact Number of Primes Less than a Given Limit", Ill. J. Math. 3, (1959) pp. 381-388.

(25) Skewes, S., "On the Difference $\pi(x) - \ell i(x)$ II", Proc. Lond. Math. Soc. 5, (1955) pp. 48-70.

(26) Goldberg, K., "A Table of Wilson Quotients and the Third Wilson Prime", J. Lond. Math. Soc. 28, (1953) pp. 252-256.

(27) Fröberg, Carl-Erik, "Some Computations of Wilson and Fermat Remainders", M.T.A.C. 12, (1958) p. 281.

(28) Kravitz, S., "The Congruence $2^{p-1} \equiv 1 \pmod{p^2}$ for $p < 100,000$", M.T.A.C. 14, (1960) p. 378.

(29) Shanks, D., "On the Conjecture of Hardy and Littlewood Concerning the Number of Primes of the Form $n^2 + a$", Math. Comp. 14, (1960) pp. 321-322.