MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 151–153

IRREGULAR PRIMES AND CYCLOTOMIC INVARIANTS TO FOUR MILLION

J. BUHLER, R. CRANDALL, R. ERNVALL, AND T. METSÄNKYLÄ

Dedicated to the computational genius of Derrick Lehmer

ABSTRACT. Recent computations of irregular primes, and associated cyclotomic invariants, were extended to all primes below four million using an enhanced multisectioning/convolution method. Fermat's "Last Theorem" and Vandiver's conjecture were found to be true for those primes, and the cyclotomic invariants behaved as expected. There is exactly one prime less than four million whose index of irregularity is equal to seven.

An irregular pair (p, t) consists of an odd prime p and an even integer t such that $0 < t < p-1$ and p divides (the numerator of) the Bernoulli number B_t. The index of irregularity r_p for a prime p is the number of irregular pairs for p.

Kummer computed the irregular pairs for odd primes p less than 165 by 1874. In the 1920s and 1930s, H. S. Vandiver used desk calculators and graduate students to find the irregular primes for $p < 620$, and used these computations to verify Fermat's "Last Theorem" (FLT) for those primes. Derrick and Emma Lehmer, together with H. S. Vandiver, used a computer in 1954 [7] to make the same computations for $p < 2000$ "in a few hours." They indicated an awareness of the importance of these computations independent of FLT: "Irrespective of whether Fermat's Last Theorem is proved or disproved, the contents of the table... constitute a permanent addition to our knowledge of cyclotomic fields."

The wisdom of this remark is clear, for instance, from Iwasawa's subsequent theory of the structure of cyclotomic class groups. The enduring interest of these calculations is also evident from the fact that a sequence of papers in this journal over the last thirty years has progressively extended the upper limit; one paper [5] appeared in the volume celebrating Derrick Lehmer's seventieth birthday.

Our goal here is to extend this sequence by announcing that the computations of irregular pairs, and verification of the usual conjectures, have been completed for all primes p between one and four million. The notation, and details of the underlying algorithms, can be found in [1] and [4] (or their predecessors), which describe the calculations for p less than one million. The most immediate applications are to FLT, Vandiver's conjecture, and cyclotomic invariants.

Received by the editor October 29, 1992 and, in revised form, December 14, 1992.

1991 *Mathematics Subject Classification.* Primary 11B68, 11D41, 11R23, 11Y40; Secondary 65T20, 11R18, 11R29.

The first author was partially supported by National Science Foundation Grant DMS-9012989.

For each p in the stated range we find that FLT is true. We also find that Vandiver's conjecture is true, i.e., that the class number of the real cyclotomic field $\mathbf{Q}(\cos(2\pi/p))$ is prime to p. Finally, by computing the cyclotomic invariants as in [4] we find that the behavior of the p-part of the cyclotomic class groups is exactly as observed before: the numerators of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ are never divisible by p^2 and for each $n \geq 0$

$$A_n \cong (\mathbf{Z}/p^{n+1}\mathbf{Z})^{r_p},$$

where A_n is the p-Sylow part of the class group of the cyclotomic field of p^{n+1}th roots of unity.

The techniques of [1] and [4] sufficed, except that it was necessary to further speed the polynomial multiplication routines. This was done by multisectioning by 12 rather than 8 (see [1]) and by incorporating Nussbaumer's convolution algorithm ([6, p. 654] and [2]). In this algorithm many smaller convolutions are computed, whose length is approximately the square root of the overall run length. These convolutions, typically of length 512 or 1024, were computed with reduced run length discrete weighted transforms as described in [3]. This enabled us to use significantly less memory and enabled us to carry the computations to four million using the "free" machine time on the network of NeXT workstations as described in [1].

The distribution of the indices of irregularity is given in Table 1. It has been conjectured that the density of primes of index r is $(2^r r!\sqrt{e})^{-1}$, so that number is also included in the table. In that table, $\pi(n)$ is the number of odd primes less than n, and $\pi_r(n)$ is the number of primes less than n with index of irregularity equal to r, and all decimals are rounded. The largest observed index of irregularity for $p < 4{,}000{,}000$ is seven and is attained for the prime $p = 3{,}238{,}481$. The conjectures on the distribution of the indices might lead one to guess that the smallest prime of index seven should be about $16{,}500{,}000$, so the observed prime is, in some sense, significantly smaller than expected.

Two other exceptional events occurred for p between one and four million. The pair $(p, p-3)$ is irregular for $p = 2{,}124{,}679$. No other instances of $(p, p-3)$ or $(p, p-5)$ being irregular were observed. (For $p < 1{,}000{,}000$, $(p, p-3)$ is irregular for $p = 16843$ and $(p, p-5)$ is irregular for $p = 37$.) For irregular pairs (p, t) for which $2^t \equiv 1 \bmod p$, the easiest formulas of [4] for verifying the behavior of the cyclotomic invariants must be replaced with alternate formulas; this was necessary only for $p = 2{,}010{,}401$ and $t = 1{,}234{,}960$. (For $p < 1{,}000{,}000$ this was necessary for $p = 130{,}811$ and $p = 599{,}479$.)

This project involved the accumulation of a large amount of data. The calculations were done over the course of several months, using the spare time on about one hundred NeXT workstations. We estimate that the computations represent about 10^{15} arithmetic operations that would have taken about 10 years on one of those machines. In these circumstances, it is natural to inquire about the reliability of the data. In the calculation of the irregular pairs, we used the stringent check sum described in [1]. In addition, each irregular pair (p, t) was separately checked for irregularity by using the sums described in [8]. Thus, we have a very high degree of confidence in our tabulated list of irregular pairs. The reliability of the calculations required to verify FLT, Vandiver's conjecture, and the expected behavior of the cyclotomic invariants is harder to

TABLE 1. Irregularity index densities

r	$\pi_r(4 \cdot 10^6)$	$\pi_r(4 \cdot 10^6)/\pi(4 \cdot 10^6)$	$e^{-1/2}/(2^r r!)$
0	171548	.60586411	.60653066
1	86037	.30386091	.30326533
2	21523	.07601379	.07581633
3	3533	.01247766	.01263605
4	441	.00155750	.00157951
5	55	.00019425	.00015795
6	7	.00002472	.00001316
7	1	.00000353	.00000094

estimate. In each case the output would be "special" (i.e., equal to 0 or 1) if something unusual happened. The output was, perhaps not surprisingly, never special. Our belief in the validity of the output is high, but not nearly as high as it is for the irregular pairs. Our confidence, such as it is, relies on the fact that several entirely different programs written at different times by different programmers were used to check the data.

ACKNOWLEDGMENTS

The authors are indebted to Joshua Doenias, NeXT Computer, Inc., for his support in implementing the software that performed, via network distribution, most of our calculations, and to NeXT Computer, Inc. and Reed College for donating the "spare cycles" on many of their workstations.

BIBLIOGRAPHY

1. J. Buhler, R. Crandall, and R. Sompolski, *Irregular primes to one million*, Math. Comp. **59** (1992), 717–722.
2. D. Bernstein, *Multidigit multiplication, the FFT, and Nussbaumer's algorithm*, manuscript.
3. R. Crandall and B. Fagin, *Discrete weighted transforms and large-integer arithmetic*, Math. Comp. (1994) (to appear).
4. R. Ernvall and T. Metsänkylä, *Cyclotomic invariants for primes to one million*, Math. Comp. **59** (1992), 249-250.
5. W. Johnson, *Irregular primes and cyclotomic invariants*, Math. Comp. **29** (1975), 113-20.
6. D. Knuth, *The art of computer programming,* vol. 2, Addison-Wesley, Reading, MA, 1981.
7. D. H. Lehmer, E. Lehmer, and H. S. Vandiver, *An application of high-speed computing to Fermat's Last Theorem*, Proc. Nat. Acad. Sci. U.S.A. **40** (1954), 25-33.
8. J.W. Tanner and S.S. Wagstaff, Jr., *New congruences for the Bernoulli numbers*, Math. Comp. **48** (1987), 341-350.

DEPARTMENT OF MATHEMATICS, REED COLLEGE, PORTLAND, OREGON 97202
E-mail address: jpb@reed.edu

SCIENTIFIC COMPUTATION GROUP, NEXT COMPUTER, INC., 900 CHESAPEAKE DRIVE, REDWOOD CITY, CALIFORNIA 94063
E-mail address: Richard_Crandall@next.com

FORSSA INSTITUTE OF TECHNOLOGY, SAKSANKATU 46, SF-30100 FORSSA, FINLAND

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TURKU, SF-20500 TURKU, FINLAND
E-mail address: taumets@sara.cc.utu.fi