MATHEMATICS OF COMPUTATION, VOLUME 32, NUMBER 142
APRIL 1978, PAGES 583–591

The Irregular Primes to 125000

By Samuel S. Wagstaff, Jr.

Abstract. We have determined the irregular primes below 125000 and tabulated their distribution. Two primes of index five of irregularity were found, namely 78233 and 94693. Fermat's Last Theorem has been verified for all exponents up to 125000. We computed the cyclotomic invariants μ_p, λ_p, ν_p, and found that $\mu_p = 0$ for all $p < 125000$. The complete factorizations of the numerators of the Bernoulli numbers B_{2k} for $2k \leqslant 60$ and of the Euler numbers E_{2k} for $2k \leqslant 42$ are given.

1. Introduction. A pair $(p, 2k)$ is called *irregular* if the prime p divides the numerator of the Bernoulli number B_{2k} and $2k$ is an even integer between 1 and $p - 2$. We use the even index notation for the Bernoulli numbers. The *index of irregularity* of a prime p is the number of $2k$'s for which $(p, 2k)$ is irregular. The prime p is called *regular* when this index vanishes and *irregular* otherwise. Regularity plays an important role in proving Fermat's "Last Theorem" for the exponent p, as will be explained in Section 4. We have verified that Fermat's conjecture is correct for all exponents up to 125000.

Two tables of irregular prime pairs and other information were deposited by the author in the UMT files. They cover the ranges $p < 100000$ and $100000 < p < 125000$, and extend Johnson's table [10] of 1975 which gives practically the same information for $p < 30000$. Our most exciting result was the discovery of two primes of index 5 of irregularity, namely 78233 and 94693. Selfridge and Pollack [16] found two primes of index 4 below 25000; we found 14 more of them. Table 1 gives the known primes of index 4 and 5. No primes of index greater than 5 were discovered.

To Johnson's historical summary of work on irregular primes in [10] we add that in 1976, Hideo Wada [20] found the irregular pairs with $p < 32768$. His work agrees completely with Johnson's results and ours to that limit.

In Section 2, we tell how the irregular pairs were found. The next section describes the distribution of the pairs. The connection with Fermat's "Last Theorem" and the Iwasawa invariants is discussed in Section 4 and Section 5. Section 6 presents work of Selfridge, Wunderlich and the author in factoring the first few Bernoulli and Euler numbers. The last section deals with computational details.

2. Determination of the Irregular Pairs. The congruences listed below were used in finding the irregular pairs. Let $c(x, y, z) = x^{p-2k} + y^{p-2k} - z^{p-2k} - 1$. Then, at least for primes $p > 8$ and $2 \leqslant 2k \leqslant p - 3$, we have

Received April 21, 1977; revised August 19, 1977.
AMS (MOS) subject classifications (1970). Primary 10A40, 12A35, 12A50.
Key words and phrases. Bernoulli numbers, Euler numbers, irregular primes, Fermat's Last Theorem, cyclotomic invariants.

$$c(3, 4, 6)B_{2k}/4k \equiv \sum_{p/6<s<p/4} s^{2k-1} \pmod{p}, \tag{1}$$

$$c(2, 3, 4)B_{2k}/4k \equiv \sum_{p/4<s<p/3} s^{2k-1} \pmod{p}, \tag{2}$$

$$c(4, 5, 8)B_{2k}/4k \equiv \sum_{p/8<s<p/5} s^{2k-1} + \sum_{3p/8<s<2p/5} s^{2k-1} \pmod{p}, \tag{3}$$

$$c(2, 5, 6)B_{2k}/4k \equiv (2^{2k-1} + 1) \sum_{p/6<s<p/5} s^{2k-1} - 2^{2k-1} \sum_{3p/10<s<p/3} s^{2k-1} \pmod{p}, \tag{4}$$

$$(2^{2k-1} + 3^{2k-1} + 6^{2k-1} - 1)B_{2k}/4k \equiv \sum_{0<s<p/6} (p - 6s)^{2k-1} \pmod{p^2}. \tag{5}$$

A proof of (4) may be found in [19, p. 574], while (5) is due to E. Lehmer [12]; the first three are well-known corollaries of Voronoi's congruence. Note that the sums in (1) and (2) have about $p/12$ terms each, while those in (3) and (4) have a total of about $p/10$ and $p/15$ terms, respectively.

In the early stages of this work (p from 30000 to about 46000) we began by computing the sum in (1). If it vanished (mod p), we evaluated $c(3, 4, 6)$. If this coefficient was nonzero (mod p), we had shown that $(p, 2k)$ was irregular. Otherwise, we computed the coefficients in (2) and (3) to seek a definitive test for regularity. In case both coefficients vanished we used (5), which was always decisive.

When we learned of (4) from Johnson, we modified the program to use it first. If it did not decide the regularity of the pair, then we tried the other four congruences in the order shown. This procedure was used for $46000 < p < 125000$.

It is remarkable that for any irregular pair $(p, 2k)$ with $p < 125000$, at most one of the coefficients in congruences (1)–(4) vanishes (mod p), so that any two of them are sufficient to prove the irregularity of $(p, 2k)$. Furthermore, the regularity of any regular pair $(p, 2k)$ with $30000 < p < 125000$ can be proved using only the five congruences. The other congruences of E. Lehmer [12] were not needed.

It is clear that congruences like (1) to (4) with fewer terms in the sums would provide a swifter test for regularity. At the beginning of this work we searched for congruences like (1) to (3) with sums taken over as many as four intervals on s whose endpoints were integer multiples of $1/n$ with $n \leqslant 120$, as well as some larger n, but found nothing better than (1) and (2). We did not try multiplying the sums by coefficients and thus did not discover (4). Perhaps one could prove that no congruence of the form

$$c(p - 2k)B_{2k}/4k \equiv \sum_{ap/n<s<bp/n} s^{2k-1} + \cdots + \sum_{ep/n<s<fp/n} s^{2k-1} \pmod{p},$$

with $0 \leqslant a < b < \cdots < e < f \leqslant n$, which holds for $2 \leqslant 2k \leqslant p - 3$ and all sufficiently large primes p, can have fewer than a total of about $p/12$ terms in the sums.

TABLE 1

Irregular primes of index $\geqslant 4$

p	Values of 2k for which p divides B_{2k}				
12613	308	502	9400	10536	
15737	6352	7454	12486	13078	
43189	9454	14464	26380	35578	
56263	10770	21958	52530	55200	
72337	2346	15858	44354	68030	
76289	11860	25284	26406	72266	
77783	5590	52114	52246	73092	
78233	10400	32084	46620	47364	64628
84067	16322	43722	44246	44794	
94693	11636	54754	76326	80650	84726
102559	6076	50092	54402	66162	
108179	9344	15048	56432	78964	
109789	10734	44536	44836	105520	
109843	16464	25396	27844	84202	
109891	36552	56682	69590	103212	
115727	36360	71962	101956	112830	
115901	33582	68462	90922	95722	
120557	42760	93110	95380	101758	

Two series of programs were run to determine the irregular pairs. The first implemented the first four congruences. It printed and punched on cards the pairs $(p, 2k)$ which it could not prove regular. A second program decided the regularity of each pair by evaluating the four $c(x, y, z)$'s and then using (5) if necessary. Many pairs of the form $(p, (p \pm 1)/2)$ were punched by the first program, but all of these were found to be regular by the second program. For $p \equiv 3 \pmod 4$, it follows from Voronoi's congruence that $(p, (p + 1)/2)$ is regular. When $p \equiv 1 \pmod 4$, however, the question of whether $(p, (p - 1)/2)$ can be irregular is related to an important question about the fundamental unit in $\mathbf{Q}(\sqrt{p})$. (See [1] and the references there.) Apparently, the question is still unsettled, but we note that $(p, (p - 1)/2)$ is regular for $p < 125000$. Occasionally, an irregular pair $(p, 2k)$ satisfies $p \equiv \pm 1 \pmod{2k}$. We found that among the irregular pairs in the range $p < 125000$ we have $p \equiv 1 \pmod{2k}$ exactly for the pairs (3617,16), (5479,1826), (43867,18) and (90247,6942); while $p \equiv -1 \pmod{2k}$ for (131,22), (593,22), (9433,178), (9539,1060) and (60353,6706).

3. The Regularities of the Irregular Primes. C. L. Siegel [18] gave a heuristic argument showing that the ratio of the number of irregular primes to regular primes below a given limit tends to $e^{1/2} - 1 = 0.6487\ldots$. His assumption was that the numerators of the B_{2k} are uniformly distributed modulo q for all odd primes q. As Johnson remarked [10], the same hypothesis predicts that the index of irregularity of primes satisfies a Poisson distribution with mean 1/2. This means that the fraction of primes below a given limit with index s of irregularity should be approximately $e^{-1/2}/s!2^s$. Wooldridge [21] has given the details of this heuristic reasoning (independently of Johnson). For $s \geqslant 0$ let $\pi_s(x)$ denote the number of primes not exceeding x with index s of irregularity. Let $\pi(x)$ be the number of *odd* primes below x and $u_s(x) = \pi_s(x)/\pi(x)$. In the table below we give $\pi_s(x)$ and $u_s(x)$ for $x = 125000$, and $0 \leqslant s \leqslant 5$. The column headed "Poisson" gives the heuristic limiting values. There are 11733 odd primes below 125000.

s	$\pi_s(x)$	$u_s(x)$	Poisson
0	7128	.60752	.60653
1	3559	.30333	.30327
2	875	.07458	.07582
3	153	.01304	.01264
4	16	.00136	.00158
5	2	.00017	.00016

The data support the hypothesis very well, especially since a change of 1 in $\pi(x)$ (to include 2 or discard 3, say) would alter the fourth significant figure of $u_s(x)$, and a change of 1 in $\pi_s(x)$ would alter the fourth decimal place of $u_s(x)$. For $x = 125000$ the computed fractions $u_s(x)$ agree with the Poisson values to within 1 in the third decimal place.

For each multiple x of 1000 to 125000 we used our data to compute the χ^2 statistic as in [10] for the irregular primes below x. It fluctuated usually between 0.1 and 1.0 and had the value 0.29 at $x = 125000$. It was 0.03 at $x = 8000$.

There are 1473 twin prime pairs below 125000. According to Siegel's heuristic reasoning, about $1473(1 - e^{-1/2})^2$ or 228 of these should have both primes irregular. In fact, there are 207 such pairs below 125000.

It has been conjectured, but never proved, that there are primes of arbitrarily high index of irregularity. One might guess that the first prime p of index s would be one for which $\pi(p)e^{-1/2}/s!2^s$ is approximately 1. This prediction is nearly correct for $s = 3$ and $s = 5$, while the least primes of index 1, 2, and 4 are more than twice as large as would be expected. The first primes of index 1, 2, 3, 4, 5 are 37, 157, 491, 12613, and 78233, respectively. The first prime of index 6 is expected near 1000000. Compare these results with those for E-irregular primes [4], which have a similar theory.

Another conjecture is that the irregular primes are distributed uniformly among the possible residue classes to every modulus. The best theorem in this direction is

due to Metsänkylä [13]: For $m \geqslant 3$ there are infinitely many irregular primes outside of each subgroup of the group of reduced residue classes modulo m. (See also [23] and [7].) In particular, there are infinitely many irregular primes. Whether there are infinitely many regular primes is unknown. Johnson [10] found that the irregular primes below 30000 are distributed quite evenly among the reduced residue classes of various moduli. Wooldridge [21] tabulated the distribution of irregular primes below 30000 in residue classes modulo m for $3 \leqslant m \leqslant 36$. We extended his count to 125000 and added the first three irregular primes, 37, 59, and 67 as moduli. The results strongly suggest that the irregular primes are asymptotically distributed equally among the $\phi(m)$ reduced residue classes modulo m for every m. We give the data for $m = 3, 4$, and 5 below. The heuristic ratio of irregular primes to odd primes is $1 - e^{-1/2} = .39347$. Similar results were obtained when the primes were counted with multiplicity equal to the index of irregularity.

m	Residue Class	Irregular primes to 125000	Odd Primes to 125000	Ratio
3	1	2282	5842	.3906
	2	2323	5890	.3944
4	1	2283	5838	.3911
	3	2322	5895	.3939
5	1	1114	2928	.3805
	2	1193	2942	.4055
	3	1149	2947	.3899
	4	1149	2915	.3942

Wooldridge [21] studied the distribution of the numbers $2k/p$ for which $(p, 2k)$ is an irregular pair with $p < 30000$. The data led to his conjecture that these numbers have a uniform distribution in the unit interval (0, 1). The additional data for all $p < 125000$ further support this conjecture. The mean of these 5842 fractions is .4983 and their standard deviation is .2898. The theoretical standard deviation for the uniform distribution on (0, 1) is $1/\sqrt{12} = .2887$. When they are arranged in increasing order in (0, 1) the largest gap between consecutive fractions is .001492, and the least gap is .0000000056.

The largest known block of consecutive primes which are all regular is the set of 27 primes beginning with 17881. The largest known block of irregular primes contains 11 primes, the first being 8597.

4. The Proof of Fermat's "Last Theorem" to 125000. Kummer proved that Fermat's "Last Theorem" (FLT) holds for all regular prime exponents. We have verified FLT for each irregular prime exponent below 125000 by using this criterion of Vandiver [11]:

THEOREM. *Let p be an irregular prime. Suppose $P = rp + 1$ is a prime less than $p(p-1)$. Let t be a positive integer such that $t^r \not\equiv 1 \pmod{P}$. For each irregular pair $(p, 2k)$ let*

$$Q_{2k} = t^{-rd/2} \prod_{b=1}^{m} (t^{rb} - 1)^{b^{p-1-2k}},$$

where $m = (p-1)/2$ *and* $d = \sum_{j=1}^{m} j^{p-2k}$. *If* $Q_{2k}^r \not\equiv 1 \pmod{P}$ *for each irregular pair* $(p, 2k)$, *then FLT holds for the exponent* p.

Thus, irregular pairs may be considered as obstructions to proving FLT, which are removable if $Q_{2k}^r \not\equiv 1 \pmod{P}$ holds.

For every p, the choices $t = 2$ and the least possible prime P always led to a successful application of the criterion. The value of P was frequently about $p \log p$, as one would expect, and r was always much smaller than p. The tables deposited in the UMT files give P, r, $d \pmod{P-1}$, $Q_{2k} \pmod{P}$, and $Q_{2k}^r \pmod{P}$ for each irregular pair. Our values of Q_{2k} differ from those in [11] because we computed d modulo $P-1$ rather than modulo p. Since Q_{2k}^r is never 1 modulo P in our table, Vandiver's theorem proves FLT for all exponents below 125000.

There are several simple conditions which imply the first case of FLT: For some small odd positive $m > 2$, if $(p, p-m)$ is not an irregular pair, then the equation $x^p + y^p = z^p$ has no nontrivial solution with p relatively prime to xyz. The odd m, with $2 < m < 30$, for which an irregular pair $(p, p-m)$ is known to exist are 3, 5, 9, 11, 15, 17, 19, 21, 29. Those who would prove the first case of FLT in general by showing that for some particular m, $(p, p-m)$ is never irregular, should not select one of these values of m.

5. Computation of the Iwasawa Invariants. For an odd prime p and $n \geq 0$, let $p^{e(n)}$ be the highest power of p which divides the class number of the cyclotomic field of p^{n+1}st roots of unity over the rationals. Iwasawa [5] showed that $e(n) = \lambda_p n + \mu_p p^n + \nu_p$ for all sufficiently large integers n, where the integers λ_p, μ_p, ν_p depend only on p.

The tables we deposited in the UMT file extend to 125000 the tables of Johnson [8]–[10] and Iwasawa and Sims [6]. For each irregular pair, we give the numbers t_0, a_1, and t of [9], the numbers a_2 and b_1 defined in [6] and [10] and the values of "terms" and "sum" of [8]. All the results concerning Bernoulli numbers, FLT, and the Iwasawa invariants which are stated in these four papers and in [22] hold true to 125000, for example, $\mu_p = 0$ while λ_p and ν_p each equal the index of irregularity of p.

6. Factorization of Some Bernoulli and Euler Numbers. As a result of the search for irregular primes described in Section 2, 5842 prime divisors $p \geq 2k+3$ are now known for the numerators P_{2k} of 5301 different Bernoulli numbers B_{2k}. J. C. Adams' theorem and Kummer's congruences provide several thousand more prime divisors p of P_{2k} with $p < 2k+3 \leq 125000$. These results together give all prime factors $p < 125000$ of P_{2k} with $2k \leq 125000$. The only other prime divisors of Bernoulli numerators which we know are those of P_{2k} with $2k \leq 60$, which were factored completely by Selfridge and Wunderlich [17]. They used the Morrison-Brillhart [14] method for factoring and the Proth-Lehmer theorem and their "combined" theorem to prove primality of large cofactors. With their kind permission we include the factorizations, which have never been published, as Table 2. The numer-

TABLE 2

Prime factorization of Bernoulli numerators

2k	Prime factors of P_{2k}
20	283.617
22	11.131.593
24	103.2294797
26	13.657931
28	7.9349.362903
30	5.1721.1001259881
32	37.683.305065927
34	17.151628697551
36	26315271553053477373
38	19.154210205991661
40	137616929.1897170067619
42	1520097643918070802691
44	11.59.8089.2947939.1798482437
46	23.383799511.67568238839737
48	653.56039.153289748932447906241
50	5.5.417202699.47464429777438199
52	13.577.58741.401029177.4534045619429
54	39409.660183281.1120412849144121779
56	7.113161.163979.19088082706840550550313
58	29.67.186707.6235242049.37349583369104129
60	2003.5549927.109317926249509865773025015237911

ators before P_{20} are either prime or unity, and so are omitted. Table 2 is the first extensive one of its kind, although others have factored the first few. M. Ohm [15] reported on an early attempt to factor some Bernoulli numerators. J. Bertrand [2] has factored them as far as P_{34}.

We decided to prepare a factor table of the closely related Euler numbers E_{2k} at the same time. (See Ernvall and Metsänkylä [4].) We found the small prime factors in Table 3, while Selfridge and Wunderlich determined the large ones. The Euler numbers before E_8 are prime or unity. Both the Bernoulli numerators and the Euler numbers may be found in unfactored form in [3].

7. General Details of the Computations. The search for the irregular primes consumed about 90% of the computer time used in this project, which was done over two years. The first program of Section 2 had a running time proportional to p^2 and took about 80 minutes per prime on an IBM 360/75 for primes near 125000. The second program described in Section 2 took hardly any time at all. A third program proved FLT and a fourth one found the Iwasawa invariants.

TABLE 3

Prime factorization of Euler numbers

2k	Prime factors of E_{2k}
8	5.277
10	19.2659
12	5.13.43.967
14	47.4241723
16	5.17.228135437
18	79.349.87224971
20	5.5.41737.354957173
22	31.1567103.1427513357
24	5.13.2137.111691689741601
26	67.61001082228255580483
28	5.19.29.71.30211.2717447.77980901
30	15669721.28178159218598921101
32	5.17.930157.42737921.52536026741617
34	4153.8429689.2305820097576334676593
36	5.13.37.9257.73026287.25355088490684770871
38	234895805270431082520178285761989477 41
40	5.5.41.763601.52778129.359513962188687126618793
42	137.5563.135995291275641748195493390306196519 71

Four IBM computers at the University of Illinois were used in the project. Most jobs were run during vacations and on weekends. The first program was written entirely in 360 assembler language. The other three had FORTRAN main programs and one or more assembler subroutines.

All of the jobs for the primes between 107000 and 108000 were repeated because we suspected (wrongly) that the computer which did them the first time might have had memory read errors. The first program for about another 100 primes was also run twice for a variety of reasons: output misplaced and later found, only printed or punched output was obtained, etc. In every case when we got legible output for two runs for the same prime, the results were identical.

The author thanks the staff of the Computing Services Office for their assistance and tolerance, and the Research Board of the University of Illinois for granting him so much computer time. He thanks W. Johnson for some helpful conversations and correspondence. He is grateful to the referee for uncovering several oversights in the original manuscript.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

1. N. C. ANKENY & S. CHOWLA, "A further note on the class number of real quadratic fields," *Acta Arith.*, v. 7, 1962, pp. 271–272.

2. J. BERTRAND, Personal communication.

3. H. T. DAVIS, *Tables of the Mathematical Functions*, v. II, The Principia Press, San Antonio, 1935.

4. R. ERNVALL & T. METSÄNKYLÄ, "Cyclotomic invariants and E-irregular primes," *Math. Comp.*, v. 32, 1978, pp. later.

5. K. IWASAWA, "On Γ-extensions of algebraic number fields," *Bull. Amer. Math. Soc.*, v. 65, 1959, pp. 183–226. MR **23** #A1630.

6. K. IWASAWA & C. C. SIMS, "Computation of invariants in the theory of cyclotomic fields," *J. Math. Soc. Japan*, v. 18, 1966, pp. 86–96. MR **34** #2560.

7. J. JOHNSEN, "On the distribution of irregular primes," *J. Number Theory*, v. 8, 1976, pp. 434–437.

8. W. JOHNSON, "On the vanishing of the Iwasawa invariant μ_p for $p < 8000$," *Math. Comp.*, v. 27, 1973, pp. 387–396. MR **52** #5621.

9. W. JOHNSON, "Irregular prime divisors of the Bernoulli numbers," *Math. Comp.*, v. 28, 1974, pp. 653–657. MR **50** #229.

10. W. JOHNSON, "Irregular primes and cyclotomic invariants," *Math. Comp.*, v. 29, 1975, pp. 113–120. MR **51** #12781.

11. D. H. LEHMER, E. LEHMER & H. S. VANDIVER, "An application of high-speed computing to Fermat's last theorem," *Proc. Nat. Acad. Sci. U.S.A.*, v. 40, 1954, pp. 25–33. MR **15**, 778.

12. E. LEHMER, "On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson," *Ann. of Math.*, v. 39, 1938, pp. 350–360.

13. T. METSÄNKYLÄ, "Distribution of irregular prime numbers," *J. Reine Angew. Math.*, v. 282, 1976, pp. 126–130.

14. M. A. MORRISON & J. BRILLHART, "A method of factoring and the factorization of F_7," *Math. Comp.*, v. 29, 1975, pp. 183–205.

15. M. OHM, "Etwas über die Bernoullischen Zahlen," *J. Reine Angew. Math.*, v. 20, 1840, pp. 11–12.

16. J. L. SELFRIDGE & B. W. POLLACK, "Fermat's last theorem is true for any exponent up to 25,000," *Notices Amer. Math. Soc.*, v. 11, 1964, p. 97. Abstract #608–138.

17. J. L. SELFRIDGE & M. WUNDERLICH, Personal communication.

18. C. L. SIEGEL, "Zu zwei Bemerkungen Kummers," *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II*, Nr. 6, 1964, pp. 51–57. MR **29** #1198; Also in *Gesammelte Abhandlungen*, v. III, Springer-Verlag, Berlin and New York, 1966, pp. 436–442.

19. H. S. VANDIVER, "On Bernoulli's numbers and Fermat's last theorem," *Duke Math. J.*, v. 3, 1937, pp. 569–584.

20. H. WADA, Personal communication.

21. K. WOOLDRIDGE, *Some Results in Arithmetical Functions Similar to Euler's Phi-Function*, Ph.D. thesis, University of Illinois at Urbana-Champaign, 1975.

22. I. YAMAGUCHI, "On a Bernoulli numbers conjecture," *J. Reine Angew. Math.*, v. 288, 1976, pp. 168–175.

23. H. YOKOI, "On the distribution of irregular primes," *J. Number Theory*, v. 7, 1975, pp. 71–76.