MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 113–120

Irregular Primes and Cyclotomic Invariants

By Wells Johnson*

Dedicated to Professor Derrick H. Lehmer

Abstract. The table of irregular primes less than 30000 has been computed and deposited in the UMT file. The fraction of irregular primes in this range is 0.3924, close to the heuristic prediction of $1 - e^{-1/2}$. Fermat's Last Theorem has been verified for all prime exponents $p < 30000$, and the cyclotomic invariants μ_p, λ_p, and ν_p of Iwasawa have been completely determined for these primes. The computations show that for p in this range, $\mu_p = 0$ and the invariants λ_p and ν_p both equal the index of irregularity of p.

1. Historical Summary and Introduction. It has been roughly 125 years since Kummer proved his monumental theorem that the Fermat equation $x^p + y^p = z^p$ has no nontrivial integral solutions for regular prime exponents p. A prime p is called regular if it does not divide the numerator of any of the Bernoulli numbers $B_2, B_4, \cdots, B_{p-3}$. This condition is equivalent to the assumption that p does not divide the class number of the cyclotomic field obtained by adjoining a primitive pth root of unity to the rational field. A detailed exposition of these results appears in [1].

Kummer himself began the search for the primes to which his proof of the Fermat conjecture did not apply. By 1874 he had determined that exactly 8 of the 37 odd primes less than 165 are irregular, including the prime 157, the first prime which divides the numerators of *two* of the Bernoulli numbers in question. With the aid of desk calculators, Vandiver and his associates [23] continued the computations to 617 in the 1930's. By 1955, Vandiver, D. H. Lehmer, E. Lehmer, Selfridge and Nicol [12], [24], [17] had completed the computations to 4001 on the SWAC computer at Los Angeles. In 1963, D. H. Lehmer [11] reported statistical results to 10000, and in 1964 Selfridge and Pollack [18] announced completion of the table to 25000 on the IBM 7090 at UCLA. These latter tables have not appeared in print. In 1970, Kobelev [10] published the table to 5500 and this was extended to 8000 by the author [8] in 1973.

Received June 13, 1974.
AMS (MOS) subject classifications (1970). Primary 10A40, 12A35, 12A50.
Key words and phrases. Irregular primes, Bernoulli numbers, Fermat's Last Theorem, cyclotomic fields, class numbers, Γ-extensions, cyclotomic invariants.
*Assisted by a grant from the Faculty Research Fund, Bowdoin College.

We have now managed to complete the table of irregular primes to 30000. This entire table, together with several other important tables which depend upon it, has been deposited in the UMT file. These latter tables involve a test for Fermat's Last Theorem, an examination of the numerators of the Bernoulli numbers, and the determination of the cyclotomic invariants of Iwasawa.

We use the "even-index" notation for the sequence of Bernoulli numbers, B_n. If p is an irregular prime and p divides the numerator of the Bernoulli number B_{2k} for $0 < 2k < p - 1$, we shall refer to $(p, 2k)$ as an *irregular pair.* For a given prime p, the number of such pairs is called the *index of irregularity* of p.

2. Fermat's Last Theorem. Various numerical tests have been devised to verify Fermat's Last Theorem in the case of an irregular prime exponent. Kummer himself worked on the irregular case and claimed a proof of the Fermat conjecture for the three irregular primes < 100. His theoretical results were later questioned and corrected by Vandiver [20], [21], [22]. With the advent of digital computers, the work of Vandiver led to the following criteria for the irregular case:

THEOREM [12]. *Let p be an irregular prime, and suppose $P = rp + 1$ is a prime satisfying $P < p^2 - p$. Let t be any integer such that $t^r \not\equiv 1 \pmod{P}$. For an irregular pair $(p, 2k)$, form the product*

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

where $m = (p - 1)/2$ and $d = \Sigma_{n=1}^{m} n^{p-2k}$. If $Q_{2k}^r \not\equiv 1 \pmod{P}$ for all such irregular pairs, then Fermat's Last Theorem holds for exponent p.

We have used the theorem above to verify the Fermat conjecture for all prime exponents $p < 30000$.' The numerical results are included in the table deposited in the UMT file. In all cases, it was sufficient merely to use $t = 2$ and the minimal prime P with the required properties. While such primes P readily occur with values of r quite small compared to p, the existence of even one such P has not been proved.

Some interesting theorems proved in the nineteenth century give sufficient conditions for Fermat's Last Theorem in the first case, when p does not divide any of the integers x, y, z. According to Dickson [2, p. 742], in 1852 Genocchi used a theorem of Cauchy to prove that the first case is true for exponent p provided $(p, p - 3)$ is not an irregular pair. Kummer showed in 1857 that for the first case it is sufficient to establish that either $(p, p - 3)$ or $(p, p - 5)$ fails to be an irregular pair. In 1905 Mirimanoff extended the result still further to include the pairs $(p, p - 7)$ and $(p, p - 9)$.

Our most surprising discovery to date has been that $(p, p - 3)$ is in fact an irregular pair for $p = 16843$. This is the first and only time this occurs for $p < 30000$. In addition, we found in our range that $(p, p - 5)$ is an irregular pair for $p = 37$ only, $(p, p - 9)$ is an irregular pair for $p = 67$ and $p = 877$ only, while

there is no example of an irregular pair of the form $(p, p-7)$. It has been known for a long time that consecutive irregular pairs (those of the form $(p, 2k)$ and $(p, 2k+2)$) occur for $p = 491$ and 587. We found no other examples of this for $p < 30000$. Thus there are no known examples of three or more consecutive irregular pairs, a situation that must exist if the Fermat equation is to have a nontrivial solution in the first case.

3. The Distribution of Irregular Primes. Siegel [19], basing his argument on the assumption that the residues of the Bernoulli numbers are randomly distributed mod p, predicted that the ratio of irregular primes to primes approaches the limit $1 - e^{-1/2} = 0.3935$. This limit was also mentioned by Lehmer [11] in his report of the computations to 10000. We have found that 1273 (39.24%) of the 3244 odd primes less than 30000 are irregular. A generalization of Siegel's argument predicts that the irregular primes of index k satisfy the Poisson distribution $\lambda^k e^{-\lambda}/k!$ with $\lambda = \frac{1}{2}$. Assuming such a distribution we can calculate the expected number of primes of each index within our range. The table below compares the actual data with these predictions:

	Observed	Expected
Index = 0	1971	1967.59
Index = 1	974	983.79
Index = 2	254	245.95
Index $\geqslant 3$	45	46.67
Total	3244	3244.00

Testing this data for goodness of fit by the χ^2 statistic, we obtain the small value 0.4266.

Jensen proved in 1915 that there are infinitely many irregular primes of the form $4n + 3$ (cf. Vandiver [25]). It is still not known, however, if there are infinitely many regular primes, or whether the Fermat conjecture is true for infinitely many prime exponents.

We found only two primes, 12613 and 15737, which have index 4, and none with index $\geqslant 5$, confirming the report of Selfridge and Pollack [18]. It is likely that the index is unbounded over all primes p, although this has not been proved. One might hope to prove that there are infinitely many irregular primes of index $\geqslant 2$, but no proof of this is known either.

Montgomery [16], extending Jensen's theorem, proved that there are infinitely many irregular primes not congruent to 1 (mod N) for any modulus $N \geqslant 3$. No modulus $N \geqslant 3$ is known for which we are certain that the residue class of 1 (mod N) contains infinitely many irregular primes, although Metsänkylä [13] has shown that this is true for either $N = 3$ or $N = 4$. Metsänkylä [15] has also proved that for $N \geqslant 3$ there are infinitely many irregular primes not congruent

to $k \pmod N$, where k runs through a proper subgroup of the reduced residue classes $\pmod N$.

Our computations show that the irregular primes seem to be distributed quite evenly among the reduced residue classes of various moduli N. We found, for example, that within our range exactly 624 (38.73%) of the 1611 primes of the form $4n + 1$ are irregular, while 649 (39.74%) of the 1633 primes of the form $4n + 3$ are irregular. For $N = 60$, similar data ranges from a low of 66 (33.17%) of the 199 primes of the form $60n + 1$ to a high of 91 (43.75%) of the 208 primes of the form $60n + 17$.

We did not find an example of an irregular pair $(p, 2k)$ for which p^2 divides the numerator of the Bernoulli number B_{2k}. In fact, all of the properties of the Bernoulli numbers reported previously by the author [9] remain true for the irregular primes $p < 30000$. The table of [9], which is only partially presented there, has now been completed to 30000, and the results are included in our table deposited in the UMT file.

4. The Cyclotomic Invariants of Iwasawa. If p is an odd prime and F_n denotes the cyclotomic field of p^{n+1}th roots of unity over the rational field, we let $p^{e(n)}$ be the exact power of p which divides the class number h_n of F_n. Iwasawa [4] has shown that there exist integers $\mu_p \geqslant 0$, $\lambda_p \geqslant 0$ and ν_p such that

$$e(n) = \mu_p p^n + \lambda_p n + \nu_p$$

for all n sufficiently large. It is known that $\mu_p = \lambda_p = \nu_p = 0$ for a regular prime p. Iwasawa and Sims [7] computed the cyclotomic invariants μ_p, λ_p, and ν_p and completely determined the structure of the p-Sylow subgroup of the ideal class group of F_n for the irregular primes $p \leqslant 4001$. Their computations imply that $\mu_p = 0$, while λ_p and ν_p both equal the index of irregularity of p for all such primes p. We have now completed these computations to 30000, and the results of Iwasawa and Sims remain true for these primes. The complete numerical table of [7] for the irregular primes $p < 30000$ is included in our table deposited in the UMT file.

The theoretical results of [7] depend upon the assumption that the irregular prime p does not divide the second factor ${}^+h_0$ of the class number h_0 of F_0 (even though p divides h_0). It is pointed out in [17] that this assumption is true if the numerical test cited previously for Fermat's Last Theorem is satisfied. Our successful completion of this test for the irregular primes less than 30000 justifies the application of the theory of [7] to these primes.

We now describe some results which we used to extend the time-consuming computations of [7] to 30000. For $1 \leqslant a \leqslant p - 1$, let $v(a)$ denote the unique p-adic $(p - 1)$st root of unity such that $v(a) \equiv a \pmod p$. We denote the p-adic expansion of $v(a)$ by

$$v(a) = a + v(a)_1 p + v(a)_2 p^2 + \cdots, \qquad 0 \leqslant v(a)_n < p.$$

Following [7], we define for odd i, $1 \leqslant i \leqslant p-4$, the p-adic sums

$$A(p, i) = \sum_{a=1}^{p-1} a v(a)^i = a_0 + a_1 p + a_2 p^2 + \cdots, \qquad 0 \leqslant a_n < p,$$

and

$$B(p, i) = \sum_{a,b=1}^{p-1} C_{a,b} b v(a)^i = b_0 + b_1 p + b_2 p^2 + \cdots, \qquad 0 \leqslant b_n < p,$$

where $C_{a,b}$ is defined to be the smallest nonnegative residue of $v(a)_1 + ab \pmod p$. It is known that $a_0 = b_0 = 0$ and that $a_1 = 0$ if and only if $(p, i+1)$ is an irregular pair. The results of [7] follow once the values of a_2 and b_1 are shown to be nonzero.

The time for the calculations of a_2 and b_1 can be shortened by means of the symmetry which exists between the terms indexed by a and $p-a$ in the sums above. Since $v(a)$ is the unique $(p-1)$st root of unity satisfying $v(a) \equiv a \pmod p$, it follows that $v(p-a) = -v(a)$, and thus $v(a)_n + v(p-a)_n = p-1$ for $n \geqslant 1$. Letting $m = (p-1)/2$ and using the fact that i is odd, we obtain

$$A(p, i) = -\sum_{a=1}^{m} (p - 2a) v(a)^i.$$

Since

$$C_{a,b} = v(a)_1 + ab - p[(v(a)_1 + ab)/p],$$

we have

$$B(p, i) = \sum_{b=1}^{p-1} b \sum_{a=1}^{p-1} v(a)_1 v(a)^i + \sum_{b=1}^{p-1} b^2 \sum_{a=1}^{p-1} a v(a)^i - p \sum_{a,b=1}^{p-1} b \left[\frac{v(a)_1 + ab}{p}\right] v(a)^i.$$

But

$$\sum_{b=1}^{p-1} b \equiv \sum_{b=1}^{p-1} b^2 \equiv \sum_{a=1}^{p-1} a v(a)^i \equiv 0 \pmod p \quad \text{for } p > 3,$$

and a formula of Friedmann and Tamarkine [3] is equivalent to

$$\sum_{a=1}^{p-1} v(a)_1 v(a)^i \equiv -B_{i+1}/(i+1) \pmod p. \tag{1}$$

Hence, if $(p, i+1)$ is an irregular pair, it follows that

$$-B(p, i)/p \equiv \sum_{a,b=1}^{p-1} b \left[\frac{v(a)_1 + ab}{p}\right] v(a)^i \pmod p.$$

Now the fact that

$$\left[\frac{v(a)_1 + ab}{p}\right] + \left[\frac{v(p-a)_1 + (p-a)b}{p}\right] = b$$

implies

$$-b_1 \equiv 2\sum_{a=1}^{m}\sum_{b=1}^{p-1}\left[\frac{v(a)_1 + ab}{p}\right]ba^i \pmod{p}.$$

The highly efficient recursion formulas which appear in [7] were used to calculate the inner sums above indexed by b.

The fact that b_1 is nonzero for all the irregular pairs $(p, i+1)$ of our table implies that $\mu_p = 0$ for $p < 30000$. The author [8], [9] has previously shown that $\mu_p = 0$ for $p < 8000$ using other criteria. The tables of these papers have also been continued to 30000, giving us further verification that $\mu_p = 0$ for $p < 30000$. The complete results of these computations are included in the table deposited in the UMT file.

It should be noted that Iwasawa [5] and Metsänkylä [14] have shown that $\mu_p < (p-1)/2$ for the cyclotomic Γ-extensions defined above. Also, Iwasawa [6] has found a whole class of other Γ-extensions for which the corresponding invariants μ are not only positive but assume arbitrarily large values.

5. The Computations. All of the computations reported here were performed on the PDP-10 computer at Bowdoin College. Lengthy computations were done overnight when there was little demand on the time-sharing system. The programs were written in FORTRAN for the most part, but certain subroutines were rewritten in assembly language (MACRO) when it became clear that this could significantly reduce the execution time. For a single prime p near 30000, it took close to 22 minutes on the PDP-10 to test for irregularity and to determine all the irregular pairs $(p, 2k)$. For such an irregular pair, it took nearly two minutes to complete the calculation for Fermat's Last Theorem, one minute to perform the calculations of [9] (including a long check), and less than 3½ minutes to determine the values of a_2 and b_1.

We used the criteria of [12] to search for the irregular primes. Checks for irregularity were inserted wherever possible in later programs. In the computation of b_1, for example, we used Eq. (1) in the form

$$-B_{i+1}/(i+1) \equiv \sum_{a=1}^{m}(2v(a)_1 + 1)a^i \pmod{p}$$

to verify the irregularity of the pair $(p, i+1)$. Another check for irregularity is described in [9]. If we take $i = 1$ and $B_2 = 1/6$ in the equation above, we obtain the congruence

$$48\sum_{a=1}^{m} av(a)_1 \equiv 1 \pmod{p}.$$

This provides us with a check on the computation of the digits $v(a)_1$, $1 \leqslant a \leqslant m$. Also, if $(p, i+1)$ is an irregular pair, then it can be shown that

$$a_2 \equiv A_0 + i(A_1 - A_0) \pmod{p},$$

where A_0 and A_1 are defined by the congruences

$$B_{i+1}/(i+1) \equiv A_0 p \pmod{p^2} \quad \text{and} \quad B_{i+p}/(i+p) \equiv A_1 p \pmod{p^2}.$$

Since A_0 and A_1 are an essential part of the table of [9], their values became known and provided us with a check on the computation of a_2.

Note Added in Proof. As this manuscript was being submitted, the tables of [18] were made available to the author. The two tables of irregular pairs are in complete agreement up to 25000 (in fact, up to 26390). It was discovered, however, that the tables of [18] contain errors in the verification of Fermat's Last Theorem. These errors occur if and only if the value of P in the theorem of Section 2 exceeds $2^{18} = 262144$, the first case being for $p = 5227$.

Department of Mathematics
Bowdoin College
Brunswick, Maine 04011

1. Z. I. BOREVIČ & I. R. ŠAFAREVIČ, *Number Theory*, "Nauka", Moscow, 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966. MR **30** #1080; **33** #4001.

2. L. E. DICKSON, *History of the Theory of Numbers*. Vol. II, Carnegie Institution of Wash., Washington, D. C., 1920.

3. A. FRIEDMANN & J. TAMARKINE, "Quelques formules conçernant la théorie de la fonction $[x]$ et des nombres de Bernoulli," *J. Reine Angew. Math.*, v. 135, 1909, pp. 146–156.

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

5. K. IWASAWA, "On the μ-invariants of cyclotomic fields," *Acta Arith.*, v. 21, 1972, pp. 99–101. MR **46** #1750.

6. K. IWASAWA, *Lecture Notes of a Course at Princeton*, Fall semester, 1971.

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

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

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

10. V. V. KOBELEV, "Proof of Fermat's last theorem for all prime exponents less than 5500," *Dokl. Akad. Nauk SSSR*, v. 190, 1970, pp. 767–768 = *Soviet Math. Dokl.*, v. 11, 1970, pp. 188–190. MR **41** #3363.

11. D. H. LEHMER, "Automation and pure mathematics" in *Applications of Digital Computers*, W. F. Freiberger and W. Prager, editors, Ginn, Boston, Mass., 1963.

12. 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.

13. T. METSÄNKYLÄ, "Note on the distribution of irregular primes," *Ann. Acad. Sci. Fenn. Ser. A I*, No. 492, 1971, 7pp. MR **43** #168.

14. T. METSÄNKYLÄ, "Class numbers and μ-invariants of cyclotomic fields," *Proc. Amer. Math. Soc.*, v. 43, 1974, pp. 299–300.

15. T. METSÄNKYLÄ, "Distribution of irregular prime numbers," *J. Reine Angew. Math.* (To appear.)

16. H. L. MONTGOMERY, "Distribution of irregular primes," *Illinois J. Math.*, v. 9, 1965, pp. 553–558. MR **31** #5861.

17. J. L. SELFRIDGE, C. A. NICOL & H. S. VANDIVER, "Proof of Fermat's last theorem for all prime exponents less than 4002," *Proc. Nat. Acad. Sci. U.S.A.*, v. 41, 1955, pp. 970–973. MR **17**, 348.

18. 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.

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

20. H. S. VANDIVER, "On Kummer's memoir of 1857 concerning Fermat's last theorem," *Proc. Nat. Acad. Sci. U.S.A.*, v. 6, 1920, pp. 266–269.

21. H. S. VANDIVER, "On the class number of the field $\Omega(e^{2i\pi/p^n})$ and the second case of Fermat's last theorem," *Proc. Nat. Acad. Sci. U.S.A.*, v. 6, 1920, pp. 416–421.

22. H. S. VANDIVER, "On Fermat's last theorem," *Trans. Amer. Math. Soc.*, v. 31, 1929, pp. 613–642.

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

24. H. S. VANDIVER, "Examination of methods of attack on the second case of Fermat's last theorem," *Proc. Nat. Acad. Sci. U.S.A.*, v. 40, 1954, pp. 732–735. MR **16**, 13.

25. H. S. VANDIVER, "Is there an infinity of regular primes?," *Scripta Math.*, v. 21, 1955, pp. 306–309.