DISTRIBUTION OF IRREGULAR PRIMES

BY

HUGH L. MONTGOMERY[1]

1. Introduction and prerequisite results

In 1850 E. E. Kummer verified [5] (see [6]) the Fermat conjecture for all prime exponents of a certain type; he called these primes regular. The purpose of this paper is to outline our knowledge of the irregular primes and to obtain a new result about them, Theorem 3.1. To prove this result we will use several arithmetic properties of the Bernoulli numbers, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$, $B_5 = 0, \cdots$. The following five theorems state these properties; their proofs [1], [3], [11] are well known and will not be included.

THEOREM 1.1. *For all integers $n \geq 1$, $B_{2n+1} = 0$ and $\operatorname{sgn} B_{2n} = (-1)^{n-1}$.*

THEOREM 1.2 (von Staudt-Clausen). *For every positive integer n, there is an integer $G(n)$ such that*

$$B_{2n} = G(n) - (1/l_1 + 1/l_2 + \cdots + 1/l_r),$$

where $l_1, l_2, \cdots, l_r$ are precisely those distinct primes for which $l_i - 1$ divides $2n$, $1 \leq i \leq r$.

The theorems above make it clear that if we write $B_{2n} = N_{2n}/D_{2n}$ in lowest terms with $D_{2n} > 0$, then $D_{2n} = l_1 l_2 \cdots l_r$ and $\operatorname{sgn} N_{2n} = (-1)^{n-1}$.

THEOREM 1.3 (J. C. Adams). *If l is an odd prime, l^w divides n, and l does not appear in D_{2n}, that is, $l - 1$ does not divide $2n$, then l^w divides N_{2n}.*

The preceding theorems enable us to write $n = n_1 n_2$, where n_1 and n_2 are relatively prime, n_1 divides N_{2n}, and every prime in n_2 appears in D_{2n}.

THEOREM 1.4. *For any positive integers n and t*

$$N_{2n}\, t \equiv D_{2n}\, S_{2n}(t) \pmod{t^2},$$

where, by definition,

$$S_{2n}(t) = \textstyle\sum_{i=1}^{t-1} i^{2n}.$$

THEOREM 1.5 (E. E. Kummer). *If l is an odd prime, n_1 and n_2 are positive integers, and $2n_1 \equiv 2n_2 \not\equiv 0 \pmod{l-1}$, then*

$$B_{2n_1}/n_1 \equiv B_{2n_2}/n_2 \pmod{l}.$$

The connection between the Bernoulli numbers and the irregular primes is given by the following:

Received October 28, 1964.

[1] This work was supported by the National Science Foundation under the Undergraduate Research Participation Program at the University of Illinois.

DEFINITION. An odd prime l is *regular* if and only if l does not divide any of the numerators

$$N_2, N_4, N_6, \cdots, N_{l-3}. \tag{1}$$

2. Knowledge of irregular primes

At the time of Kummer's proof only a few irregular primes were known to exist, but by 1940 H. S. Vandiver [12] had abandoned his project of listing the irregular primes because he had begun to doubt the existence of an infinity of regular primes. He found that of the primes less than 4002 approximately 39% are irregular. The irregular primes less than 300 are 37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293. Fermat's conjecture has been verified for all irregular prime exponents having certain properties. In this manner the conjecture has been verified for all odd prime exponents less than 4002 [9].

It is not known whether there are infinitely many regular primes, but in 1915 K. L. Jensen showed [4] (see [12]) that there are infinitely many irregular primes of the form $4m + 3$, and in 1955 L. Carlitz gave a simpler proof [2] of the weaker assertion that there are infinitely many irregular primes. In 1963 I. Š. Slavŭtskiĭ asserted [10] that there is an infinity of irregular primes of the form $3m + 2$, but his proof by contradiction was the result of a mistake in signs: no contradiction is obtainable when the error is corrected. However, his assertion is contained in our Theorem 3.1.

After L. Carlitz [2] we will call an odd prime l which divides the numerator of N_{2n}/n a *proper* divisor of N_{2n}, and all other prime divisors of N_{2n} *improper*. In Lemma 1 we will show that an odd prime l is irregular if and only if l is a proper divisor of some Bernoulli number. Little is known about the highest power l^w of l in the numerator of N_{2n}/n, except that $w > 1$ is possible. F. Pollaczek noted [8] that 37^2 divides the numerator of $N_{284}/142$. Apparently it is not known whether l^2 can divide any of the numbers in (1).

3. Distribution of irregular primes

We begin by proving two lemmas to Theorem 3.1.

LEMMA 1. *An odd prime is irregular if and only if it is a proper divisor of some Bernoulli number.*

Proof. I. Suppose l is irregular. Then l divides N_{2k} for some k, $1 \leq k \leq (l - 3)/2$. But l and k are relatively prime, so l also divides the numerator of N_{2k}/k, and hence l is a proper divisor of N_{2k}.

II. Suppose l is a proper divisor of N_{2k}. Then $k \not\equiv 0 \pmod{(l - 1)/2}$ by Theorem 1.2, because we know that l does not appear in D_{2k}. Let k' be the least positive residue of k modulo $(l - 1)/2$, so

$$2k \equiv 2k' \not\equiv 0 \pmod{l - 1} \quad \text{and} \quad 2 \leq 2k' \leq l - 3.$$

By Theorem 1.5 l is also a proper divisor of $N_{2k'}$. Thus l divides $N_{2k'}$, which is in (1), so l is irregular.

Lemma 1 complements Theorem 1.3 in that if l is regular and l^w is the highest power of l in n and l does not appear in D_{2n}, then l^w is the highest power of l in N_{2n}.

The following lemma will be used in conjunction with Theorem 1.4 to determine congruence properties of N_{2Q} once those of D_{2Q} are known.

LEMMA 2. *If P is an odd prime and $k \equiv 1 \pmod{\phi(P^2)}$, then*

$$S_{2k}(P) \equiv P/6 \pmod{P^2}.$$

Proof.

$$\begin{aligned} S_{2k}(P) &= \textstyle\sum_{i=1}^{P-1} i^{2k} \\ &\equiv \textstyle\sum_{i=1}^{P-1} i^2 \pmod{P^2} \\ &= P^3/3 - P^2/2 + P/6 \\ &\equiv P/6 \pmod{P^2}. \end{aligned}$$

THEOREM 3.1. *If P is an odd prime then there are infinitely many irregular primes not of the form $mP + 1$.*

Remark. In the proof we will determine an integer $Q \equiv 1 \pmod P$ for which $|N_{2Q}|/Q \not\equiv 1 \pmod P$, so that N_{2Q} has at least one proper divisor not of the form $mP + 1$. If Q is chosen properly, it may be shown that this proper divisor is distinct from some original set of primes, $p_1, p_2, \cdots, p_s$.

Proof. Let $p_1, p_2, \cdots, p_s$ be s distinct primes with $p_i \geq 5$. Then we will show the existence of an irregular prime, p_{s+1}, distinct from $p_1, p_2, \cdots, p_s$, and not congruent to 1 modulo P.

Let l be a prime such that

$$(2) \qquad l \equiv -1 \pmod{12\phi(P^2)p_1(p_1 - 1)p_2(p_2 - 1) \cdots p_s(p_s - 1)}.$$

But l appears in $D_{2\mu}$ where $\mu = (l - 1)/2$; let $l' \geq 5$ be the least prime (other than 2 and 3) in $D_{2\mu}$ such that $l' \not\equiv 1 \pmod P$. If $\mu' = (l' - 1)/2$ then l' appears in $D_{2\mu'}$. Furthermore, μ' divides μ so the primes in $D_{2\mu'}$ are from among those primes $\leq l'$ in $D_{2\mu}$. Thus the only primes in $D_{2\mu'}$ which are not of the form $mP + 1$ are 2, 3, and l'.

We will now show the existence of an appropriate number, η, such that, if $\mu'\eta = Q$, then

$$D_{2Q} = D_{2\mu'} \quad \text{and} \quad Q \equiv 1 \pmod{6\phi(P^2)p_1(p_1 - 1)p_2(p_2 - 1) \cdots p_s(p_s - 1)}.$$

Let $d_1, d_2, \cdots, d_r$ be all divisors of μ', and let $l_1, l_2, \cdots, l_r$ be r distinct primes obeying

$$l_i > l' \cdot 6\phi(P^2)p_1(p_1 - 1)p_2(p_2 - 1) \cdots p_s(p_s - 1).$$

We consider the simultaneous congruences

$$\eta \equiv 1/\mu' \pmod{l'\cdot 6\phi(P^2)p_1(p_1 - 1)p_2(p_2 - 1) \cdots p_s(p_s - 1)}, \tag{3}$$
$$\eta \equiv -1/2d_i \pmod{l_i^2}, \qquad 1 \leq i \leq r.$$

We see that μ' is relatively prime to

$$l'\cdot 6\phi(P^2)p_1(p_1 - 1)p_2(p_2 - 1) \cdots p_s(p_s - 1)$$

because μ' divides μ and by (2)

$$\mu \equiv -1 \pmod{6\phi(P^2)p_1(p_1 - 1) \cdots p_s(p_s - 1)}.$$

Also, $2d_i$ is relatively prime to l_i because $2d_i < l' < l_i$ and l_i is prime. The moduli of (3) are pairwise relatively prime, so there is a solution to (3), which is unique modulo the product of the moduli. This solution is clearly relatively prime to each of the moduli, so by Dirichlet's theorem [6] we may choose η to be a prime satisfying (3). Set $Q = \mu'\eta$. First we show that $D_{2Q} = D_{2\mu'}$. The divisors of $2Q$ are

$$\begin{gathered} d_1, d_2, \cdots, d_r, \\ 2d_1, 2d_2, \cdots, 2d_r, \\ d_1\eta, d_2\eta, \cdots, d_r\eta, \\ 2d_1\eta, 2d_2\eta, \cdots, 2d_r\eta. \end{gathered} \tag{4}$$

When 1 is added to each member of (4), the primes appearing in the first two rows are precisely those of $D_{2\mu'}$. All members of the third row are even when 1 is added, and by (3) $2d_i\eta + 1$ is divisible by l_i^2. Therefore $D_{2Q} = D_{2\mu'}$, and hence $D_{2Q}/6 \equiv l' \pmod P$.

We turn now to consider N_{2Q}. We put $n = Q$ and $t = P$ in Theorem 1.4 and apply Lemma 2 to obtain

$$N_{2Q}P \equiv D_{2Q}S_{2Q}(P) \equiv D_{2Q}\cdot P/6 \pmod{P^2},$$

so that

$$N_{2Q} \equiv D_{2Q}/6 \equiv l' \pmod P. \tag{5}$$

As we noted earlier, we may write $Q = Q_1Q_2$ with Q_1 and Q_2 relatively prime, where Q_1 divides N_{2Q} and every prime in Q_2 appears in D_{2Q}. The only primes in D_{2Q} which are not of the form $mP + 1$ are 2, 3, and l', but (3) assures us that $Q \equiv 1 \pmod{6l'}$, so all primes in Q_2 are of the form $mP + 1$, and hence $Q_1 \equiv Q \equiv 1 \pmod P$. But the numerator of N_{2Q}/Q is precisely the integer $N_{2Q}/Q_1 \equiv l' \pmod P$. From relation (5) we see that $l' \not\equiv 0 \pmod P$, because N_{2Q} and D_{2Q} are relatively prime. Theorem 1.1 assures us that $N_{2Q} > 0$, so we have the positive integer $N_{2Q}/Q_1 \not\equiv 1, \not\equiv 0 \pmod P$. Thus there is at least one prime p_{s+1} in N_{2Q}/Q_1 which is not of the form $mP + 1$. If p_{s+1} is such a prime, then p_{s+1} is a proper divisor of N_{2Q}, so by Lemma 2 p_{s+1} is irregular.

It remains to show that p_{s+1} is distinct from $p_1, p_2, \cdots, p_s$. The congruence (3) affords us the hypotheses of Theorem 1.5, which yields

$$B_{2Q}/Q \equiv B_2/1 = \tfrac{1}{6} \not\equiv 0 \pmod{p_i}, \qquad 1 \leq i \leq s,$$

so p_{s+1} is distinct from $p_1, p_2, \cdots, p_s$, and the proof is complete.

The most general result we can state now is

THEOREM 3.2. *If T is an integer $T > 2$, then there are infinitely many irregular primes which are not of the form $mT + 1$.*

Proof. If T has an odd prime factor then the assertion is true on the strength of the previous theorem. On the other hand, if T is a power of 2, $T = 2^k$, $k \geq 2$, then the assertion follows from Jensen's result that there are infinitely many primes of the form $4m + 3$.

For certain values of T we may state our results more precisely. For $T = 3$, there are infinitely many primes of the form $3m + 2$. For $T = 4$ we have Jensen's result. For $T = 6$ we have a result equivalent to that for $T = 3$, because all primes of the form $3m + 2$ are also of the form $6m + 5$, with the single exception of the prime 2.

It might be expected from these results that if $T > 2$ then there is a deficiency of irregular primes of the form $mT + 1$. However, this is not borne out by the numerical evidence of J. L. Selfridge, C. A. Nicol, and H. S. Vandiver [9]. There are 334 regular primes less than 4002, and 216 irregular primes less than 4002. If we group the latter modulo 12, for example, we find that forty-nine are congruent to 1, sixty-six are congruent to 5, forty-three are congruent to 7, and fifty-eight are congruent to 11.

I wish to thank Professor Paul T. Bateman for his kind assistance in directing this research and his aid in the preparation of this paper. The author is also indebted to Professor Leonard Carlitz for his suggestions and for confirming the author's suspicions of Slavŭtskiĭ's proof.

REFERENCES

1. PAUL BACHMANN, *Niedere Zahlentheorie*, Leipzig, Druck und Verlang von B. G. Teubner, 1910.
2. L. CARLITZ, *Notes on irregular primes*, Proc. Amer. Math. Soc., vol. 5 (1954), pp. 329–331.
3. ———, *The Staudt-Clausen theorem*, Math. Mag., vol. 34 (1961), pp. 131–146.
4. KAJ LØCHTE JENSEN, *Om talteoretiske Egenskaber ved de Bernouliiske Tal*, Nyt Tidsskrift Für Mathematik, vol. 26 (1915), Afdeling B, pp. 73–83.
5. E. E. KUMMER, *Algemeiner Beweis der Fermatschen Satzes, dass die Gelichung $x^l + y^l + z^l$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten l, welche ungerade Primzahl sind und in der Zahlern der ersten $\tfrac{1}{2}(l - 3)$ Bernoullischen Zählen als Faktoren nicht vorkommen*, J. Reine Angew. Math., vol. 40 (1850), pp. 93–138.
6. WILLIAM LEVEQUE, *Topics in number theory*, vol. 2, Reading, Addison-Wesley, 1956.
7. N. NIELSEN, *Traité élémentaire des nombres de Bernoulli*, Paris, 1923.

8. F. Pollaczek, *Über die irregularen Kreiskorper der l*-ten und l^2-ten *Einheitswurzen*, Math. Zeitschrift, vol. 21 (1924), p. 31.
9. J. L. Selfridge, C. A. Nicol, and H. S. Vandiver, *Proof of Fermat's last theorem for prime exponents less than 4002*, Proc. Nat. Acad. Sci., vol. 41 (1955), pp. 970–973.
10. I. Š. Slavŭtskiĭ, *Ka Voprosu o prostikh irregulyarnikh Chislakh*, Acta Arith., vol. 8 (1963), pp. 123–125.
11. J. V. Uspensky and M. A. Heaslet, *Elementary number theory*, New York, McGraw-Hill, 1939.
12. H. S. Vandiver, *Is there an infinity of regular primes?*, Scripta Math., vol. 21 (1955), pp. 306–309.
13. ———, *Notes on the divisors of the numerators of Bernoulli's numbers*, Proc. Nat. Acad. Sci., vol. 18 (1932), p. 594.
14. ———, *On Bernoulli's numbers and Fermat's last theorem*, Duke Math. J., vol. 3 (1937), p. 576.

University of Illinois
Urbana, Illinois