ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

492

NOTE ON THE DISTRIBUTION OF IRREGULAR PRIMES

BY

TAUNO METSÄNKYLÄ

HELSINKI 1971
SUOMALAINEN TIEDEAKATEMIA

doi:10.5186/aasfm.1971.492

Communicated 15 January 1971 by K. A. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1971

Note on the distribution of irregular primes

1. Introduction. A prime p is said to be *irregular* if it divides the numerator of at least one of the Bernoulli numbers B_2, $B_4, \ldots, B_{p-3}$ (in the even suffix notation). The simplest proof for the known fact that the number of irregular primes is infinite was given by CARLITZ [1]. JENSEN [2] proved the stronger result that there is an infinity of irregular primes $\equiv -1 \pmod 4$, and MONTGOMERY [3] generalized this as follows: for every integer $T > 2$, there are infinitely many irregular primes $\not\equiv 1 \pmod T$. This result also contains the proposition asserted by SLAVUTSKIĬ [5], namely, that the number of irregular primes $\equiv -1 \pmod 3$ is infinite.

SLAVUTSKIĬ remarked that some of the known irregular primes $\equiv -1 \pmod 3$ are $\equiv 1 \pmod 4$. According to MONTGOMERY, the first 216 irregular primes, grouped modulo 12, split into groups of 49, 66, 43, and 58 primes. More generally, as noted in [3], numerical results indicate that there is no deficiency of irregular primes in the residue class $1 \pmod T$, if $T > 2$.

In this note we shall show that there are infinitely many irregular primes $\equiv \pm 5 \pmod{12}$, so that the following theorem holds true:

Theorem 1. *At least one of the residue classes* $1 \pmod 3$ *and* $1 \pmod 4$ *contains an infinite number of irregular primes.*

In addition, using ideas from [3], we shall generalize this result by proving

Theorem 2. *For every integer* $T > 4$, $T \neq 6$, *there are infinitely many irregular primes* $\not\equiv \pm 1 \pmod T$.

We also wish to mention the connexion between the questions about the distribution of irregular primes and the number of *regular* primes. This number has been conjectured to be infinite ([4], cf. also [7]). The conjecture is proved if, for some integer T, there exists a residue class (mod T) prime to T containing only a finite number of irregular primes. However, in view of our present knowledge about irregular primes, the existence of such a residue class seems improbable.

2. Preliminary results. Write the Bernoulli numbers in the form

$$B_{2k} = N_{2k}/D_{2k}$$

(in lowest terms) with $D_{2k} > 0$. Then, by the known Staudt-Clausen theorem, D_{2k} is the product of those distinct primes l for which $l - 1$ divides $2k$. Furthermore, by setting

$$S_{2k}(t) = 1^{2k} + 2^{2k} + \ldots + (t-1)^{2k}$$

we can state that N_{2k} is connected with D_{2k} by the congruences

$$t\,N_{2k} \equiv D_{2k} S_{2k}(t) \pmod{t^2}, \tag{1}$$

valid for each positive integer t [6, p. 260].

Those prime divisors of N_{2k} which divide the numerator of N_{2k}/k are called *proper*. As is known (see, e.g., [3]), every prime which is a proper divisor of some N_{2k} is irregular.

To be able to use (1), we shall need some information about $S_{2k}(t)$. If P denotes an arbitrary odd prime, we have [3, p. 555]

$$S_{2k}(P) \equiv P/6 \pmod{P^2} \text{ for } k \equiv 1 \pmod{P(P-1)}. \tag{2}$$

Moreover, assuming that $k > 1$ the following congruences can be easily established:

$$S_{2k}(8) \equiv -12 \pmod{32} \text{ for } k \equiv 1 \pmod{4}, \tag{3}$$

$$S_{2k}(9) \equiv -3 \pmod{27} \text{ for } k \equiv 1 \pmod{9}, \tag{4}$$

$$S_{2k}(12) \equiv -10 \pmod{24}. \tag{5}$$

3. Proof of theorem 1. Let us suppose that there exists only a finite set of irregular primes $\equiv \pm 5 \pmod{12}$, say, $p_1, \ldots, p_s$. Put

$$A = (p_1 - 1)\ldots(p_s - 1)$$

and consider B_{2q} with a prime $q \equiv 1 \pmod{12A}$.

It is seen that $D_{2q} = 6$. Hence, by (1),

$$12N_{2q} \equiv 6S_{2q}(12) \pmod{12^2}, \tag{6}$$

which combined with (5) yields

$$N_{2q} \equiv -5 \pmod{12}.$$

From this congruence it follows that N_{2q} must contain a prime factor $p \not\equiv \pm 1 \pmod{12}$. Since $p \neq q$, we conclude that p is a proper divisor of N_{2q} and thus irregular. By our assumption, p then appears in the above set of primes.

Now, because N_{2q} contains a prime p_i $(1 \leqq i \leqq s)$ as a factor, the congruence

$$B_{2q}/q \equiv 0 \pmod{p_i}$$

holds true. On the other hand, by virtue of $q \equiv 1 \pmod{p_i - 1}$, the so-called Kummer's congruence gives us

$$B_{2q}/q \equiv B_2/1 = 1/6 \pmod{p_i},$$

and we have a contradiction.

4. Proof of theorem 2. It is sufficient to prove, that the number of irregular primes $\not\equiv \pm 1 \pmod{t}$ is infinite for $t = 8, 9, 12,$ and P (an arbitrary prime > 3). Indeed, every integer $T > 4$, $T \neq 6$, is divisible by at least one of these numbers t.

For $t = 12$, the proof was carried out above. The case $t = 9$ can be treated analogously by choosing $q \equiv 1 \pmod{18A}$, whereupon (6) is replaced by

$$9\, N_{2q} \equiv 6\, S_{2q}(9) \pmod{9^2}$$

which gives, by (4), the congruence

$$N_{2q} \equiv -2 \pmod{9}.$$

The remaining cases are more complicated. In the first place, let P be a prime > 3 and suppose, contrary to our assertion, that $p_1, \ldots, p_s$ are the irregular primes $\not\equiv \pm 1 \pmod{P}$.

We put

$$M = 6P(P-1)(p_1 - 1) \ldots (p_s - 1) = P^h M_1, \tag{7}$$

where M_1 is not divisible by P, and choose a prime l satisfying

$$l \equiv -1 \pmod{2M_1}, \qquad l \equiv 3 \pmod{P^h}. \tag{8}$$

Then $l \not\equiv \pm 1 \pmod{P}$, and we can find a factor n of $\frac{1}{2}(l-1)$ such that D_{2n}, the denominator of B_{2n}, is of the form $6al'$ where $a \equiv \pm 1 \pmod{P}$ and l' $(= 2n + 1)$ is a prime $\not\equiv \pm 1 \pmod{P}$. (See [3], proof of theorem 3.1, where n is denoted by μ'.)

Note that l is chosen such that $(\frac{1}{2}(l-1), M) = 1$. Consequently, $(n, l'M) = 1$ and the congruence

$$nq \equiv 1 \pmod{l'M} \tag{9}$$

is solvable for q. Moreover, one can assume q to be a prime satisfying simultaneously with (9) also

(10) $$2d_jq \equiv -1 \pmod{l_j^2} \qquad (i = 1, \ldots, r),$$

where $d_1, \ldots, d_r$ are the divisors of n and $l_1, \ldots, l_r$ are distinct primes $> l'M$.

Consider B_{2Q} with $Q = nq \equiv 1 \pmod{l'M}$. Then (10) assures us that D_{2Q} has no other prime factors than those of D_{2n}, that is,

(11) $$D_{2Q} = D_{2n} = 6\,a\,l', \qquad a \equiv \pm 1 \pmod{P}.$$

Applying this with (2) to the congruence

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

we get

(13) $$N_{2Q} \equiv \pm\, l' \pmod{P}.$$

To eliminate the improper divisors of N_{2Q}, we must write $Q = Q_1Q_2$ with $(Q_1, Q_2) = 1$ and Q_2 containing exactly those primes of Q that divide D_{2Q}. Then Q_1 divides N_{2Q} (see, e.g., [6, p. 261]) and thus the numerator of N_{2Q}/Q equals N_{2Q}/Q_1. Now, because $Q \equiv 1 \pmod{6l'}$, none of the prime factors 2, 3, and l' of D_{2Q} appears in Q_2 so that, by (11), $Q_2 \equiv \pm 1 \pmod{P}$, and we have $Q_1 \equiv \pm\, Q \equiv \pm\, 1 \pmod{P}$. Together with (13) this yields

$$N_{2Q}/Q_1 \equiv \pm\, l' \pmod{P}.$$

Hence N_{2Q} contains a proper prime factor $\not\equiv \pm\, 1 \pmod{P}$ and the proof can be finished similarly as in the above cases.

As for the case $t = 8$, one has to modify slightly the preceding proof. In fact, the formulas (7), (8), and (12) are replaced by

(7′) $$M = 24(p_1 - 1)\ldots(p_s - 1) = 2^h M_1 \qquad (M_1 \text{ odd}),$$

(8′) $$l \equiv -1 \pmod{M_1}, \qquad l \equiv 3 \pmod{2^h},$$

(12′) $$8\,N_{2Q} \equiv D_{2Q}S_{2Q}(8) \pmod{8^2},$$

the last of which then gives, by (3), the crucial congruence

$$N_{2Q} \equiv \pm\, l' \pmod{8}.$$

University of Jyväskylä
and
University of Turku
Finland

References

[1] CARLITZ, L.: Note on irregular primes. - Proc. Amer. Math. Soc. 5 (1954), 329—331.

[2] JENSEN, K. L.: Om talteoretiske Egenskaber ved de Bernoulliske Tal. - Nyt Tidsskrift for Matematik 26, Afd. B (1915), 73—83.

[3] MONTGOMERY, H. L.: Distribution of irregular primes. - Illinois J. of Math. 9 (1965), 553—558.

[4] SIEGEL, C. L.: Zu zwei Bemerkungen Kummers. - Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II Nr. 6 (1964), 51—57.

[5] SLAVUTSKIĬ, I. Š. [И. Ш. Славутский]: К вопросу о простых иррегулярных числах. - Acta Arith. 8 (1963), 123—125.

[6] USPENSKY, J. V., and HEASLET, M. A.: Elementary number theory. New York (1939).

[7] VANDIVER, H. S.: Is there an infinity of regular primes? - Scripta Math. 21 (1955), 306—309.

Printed March 1971