Annales Academiæ Scientiarum Fennicæ
Series A. I. Mathematica
Volumen 1, 1975, 195 – 198

ON THE DISTRIBUTION mod 8 OF THE E-IRREGULAR PRIMES

REIJO ERNVALL

1. A prime p is called *irregular* if it divides the numerator of at least one of the Bernoulli numbers B_2, B_4,..., B_{p-3} (in the even suffix notation); see e.g. [1, pp. 367 – 389]. Carlitz [2] has given the simplest proof of the fact that the number of irregular primes is infinite. Metsänkylä [5] has proved that for $N \geq 3$ there are infinitely many irregular primes not congruent to k (mod N), where k runs through a subgroup of the reduced residue classes (mod N). (See also [4] and [6].)

D e f i n i t i o n . A prime p is *irregular with respect to the Euler numbers*, shortly *E-irregular*, if it divides at least one of the Euler numbers E_2, E_4,..., E_{p-3}.

Here Euler numbers E_m ($m = 0, 1, 2, ...$) are defined by the symbolic equation $(E + 1)^m + (E - 1)^m = 0$, where $E_0 = 1$ and $m \geq 1$. It is easy to see that all Euler numbers are integers and that those with an odd index equal zero. The first few non-vanishing Euler numbers are $1, -1, 5, -61, 1385$.

The list of E-irregular primes begins as follows: 19, 31, 43, 47, 61, 67, 71, 79, 101. Carlitz [2] has proved that the number of E-irregular primes is infinite. The proof is similar to the corresponding proof mentioned above. One might therefore expect that it would also be easy to obtain results on the distribution of E-irregular primes, by modifying suitable methods used in connection with the ordinary irregular primes. It seems, however, that this is not the case, and so one has to look for new methods when dealing with this problem. We have found one such method which allows us to prove the following theorem.

T h e o r e m . *There are infinitely many E-irregular primes* $\not\equiv \pm 1$ (mod 8).

2. The letter p will always denote a prime > 2. By s we mean the number $(p-1)/2$.

doi:10.5186/aasfm.1975.0102

It is known (see [3, p. 297], [7, p. 269]) that, for any polynomial f and integer n, the symbolic equation

$$f(n + E + 1) + f(n + E - 1) = 2f(n) \tag{1}$$

holds. Take an odd l and an even $m > 0$. If we choose $f(x) = x^m$ and let n run odd integers from 1 to $2l-1$, we get as a consequence of (1)

$$E_m \equiv 1^m - 3^m + 5^m - + \ldots + (2l-1)^m \pmod{l^2}. \tag{2}$$

This gives us the Kummer congruence

$$E_{m+p-1} \equiv E_m \pmod{p}.$$

In case $p-1 \mid m$, (2) yields the known result

$$\begin{aligned} E_m &\equiv 0 \pmod{p} \quad \text{for } p \equiv 1 \pmod 4, \\ &\equiv 2 \pmod{p} \quad \text{for } p \equiv 3 \pmod 4. \end{aligned} \tag{3}$$

(Compare with [7, p. 269].)

3. Before we can prove the theorem, we need two lemmas.

L e m m a 1. *If* $m \equiv 6 \pmod 8$, *then* $E_m \equiv 3 \pmod 8$.

Proof. Substituting in (1) $f(x) = x^m$ and $n = 1$ we have

$$E^m + (E + 2)^m = 2.$$

Using the fact that all Euler numbers with an odd index equal zero, we get

$$2E_m + \binom{m}{2} 4E_{m-2} \equiv 2 \pmod{16}$$

or

$$E_m \equiv 1 - m(m-1)E_{m-2} \pmod 8.$$

Hence

$$\begin{aligned} E_m &\equiv 1 \pmod 8 \quad \text{for } m \equiv 0 \pmod 8, \\ &\equiv 7 \pmod 8 \quad \text{for } m \equiv 2 \pmod 8, \\ &\equiv 5 \pmod 8 \quad \text{for } m \equiv 4 \pmod 8, \\ &\equiv 3 \pmod 8 \quad \text{for } m \equiv 6 \pmod 8. \end{aligned}$$

L e m m a 2. *If* $p \equiv 5 \pmod 8$, *then* E_s *is not divisible by* p.

Proof. We use (2) to get

$$\begin{aligned} E_s &\equiv 1^s - 3^s + 5^s - + \ldots + (2p-1)^s \\ &\equiv 2[1^s - 3^s + 5^s - + \ldots - (p-2)^s] \\ &\equiv 2[1^s - 2^s - 3^s + 4^s + 5^s - - + + \ldots + + + - s^s] \pmod p. \end{aligned}$$

Thus it follows from the Euler criterion concerning Legendre symbols that

$$E_s \equiv 2\left[\left(\frac{1}{p}\right) - \left(\frac{2}{p}\right) - \left(\frac{3}{p}\right) + + - - \ldots + + - \left(\frac{s}{p}\right)\right] \pmod{p}.$$

For brevity we shall denote by A the expression in the square brackets. As $-p < A < p$, we must show that $A \neq 0$. Because the number of the quadratic residues of p is equal to the number of the quadratic non-residues of p, and because i and $p-i$ are simultaneously either residues or non-residues (as $p \equiv 1 \pmod 4$), we have

$$\sum_{i=1}^{s} \left(\frac{i}{p}\right) = 0.$$

Combining this with the definition of A we find that A may be put in the form $2B$, where $B \equiv (p-1)/4 \not\equiv 0 \pmod 2$. Hence the assertion follows.

4. We shall now prove our theorem.

Suppose that $q_1 \ (= 19), q_2, \ldots, q_k$ are the E-irregular primes $\not\equiv \pm 1 \pmod 8$. Let

$$M' = 2 \prod_{i=1}^{k} (q_i - 1)/2^{\alpha(i)},$$

where $\alpha(i) = 1$ or 2 $(i = 1, 2, \ldots, k)$ depending on, whether 2 or 4 exactly divides $q_i - 1$. Because M' is divisible by 2 but not by 4, we can choose $K = 1$ or 3, such that $M = K M' \equiv 6 \pmod 8$.

We next show that q_i does not divide E_M, for $i = 1, \ldots, k$. If $q_i \equiv 3 \pmod 4$, we have $q_i - 1 \mid M$ so that (3) gives $E_M \equiv 2 \not\equiv 0 \pmod{q_i}$. In case $q_i \equiv 5 \pmod 8$, we get $M \equiv (q_i - 1)/2 \pmod{q_i - 1}$. Then, by Kummer's congruence and Lemma 2, q_i does not divide E_M.

As $M \equiv 6 \pmod 8$, Lemma 1 gives $E_M \equiv 3 \pmod 8$. Therefore there exists an odd prime $q \not\equiv \pm 1 \pmod 8$ dividing E_M.

We shall show that q is E-irregular, and this is the contradiction. Because of Kummer's congruence we need only prove that M is not divisible by $q-1$. Suppose $q-1 \mid M$. If now $q \equiv 1 \pmod 4$, we have $4 \mid M$. If $q \equiv 3 \pmod 4$, we have $E_M \equiv 2 \pmod q$ (this follows from (3)). But these are both impossible.

References

[1] Borevich, Z. I., and I. R. Shafarevich: Number Theory. - Academic Press, New York — London, 1966.

[2] CARLITZ, L.: Note on irregular primes. - Proc. Amer. Math. Soc. 5, 1954, 329—331.
[3] CESÀRO, E.: Elementares Lehrbuch der algebraischen Analysis und der Infinitesimalrechnung. - B. G. Teubner, Leipzig, 1904.
[4] METSÄNKYLÄ, T.: Note on the distribution of irregular primes. - Ann. Acad. Sci. Fenn. Ser. A I 492, 1971, 1—7.
[5] METSÄNKYLÄ, T.: Distribution of irregular prime numbers. - J. Reine Angew. Math. (to appear).
[6] MONTGOMERY, H. L.: Distribution of irregular primes. - Illinois J. Math. 9, 1965, 553—558.
[7] USPENSKY, J. V., and M. A. HEASLET: Elementary Number Theory. - Mc Graw—Hill Book Company, New York — London, 1939.

University of Turku
Department of Mathematics
SF-20500 Turku 50
Finland

Received 3 February 1975