NOTE ON IRREGULAR PRIMES

L. CARLITZ

1. We recall that a prime p is *irregular* if it divides the numerator of at least one of the numbers

$$(1.1)\qquad B_2, B_4, \cdots, B_{p-3},$$

where B_m denotes a Bernoulli number in the even-suffix notation. Jensen has proved that there exist infinitely many irregular primes of the form $4n+3$ (for the proof see [**3**, p. 82]; see also [**4**]).

In this note we give a simple proof of the weaker result that the number of irregular primes is infinite. We also prove a like result corresponding to the prime divisors of the Euler numbers.

The letter p will always denote a prime >2.

2. We shall make use of the following well known properties of Bernoulli numbers. For proofs see [**2**, Chaps. 13, 14].

$$(2.1)\qquad B_m \equiv 0 \pmod{p^r} \qquad (p^r \mid m,\ p-1 \nmid m).$$

$$(2.2)\qquad pB_m \equiv -1 \pmod{p} \qquad (p-1 \mid m).$$

$$(2.3)\qquad \frac{B_{m+r(p-1)}}{m+r(p-1)} \equiv \frac{B_m}{m} \pmod{p} \qquad (p-1 \nmid m).$$

(2.2) is contained in the Staudt-Clausen theorem, while (2.3) is a special case of Kummer's congruence for the Bernoulli numbers. Note that both members of (2.3) are integral (mod p).

A prime divisor of the numerator of B_m/m may be called a *proper* divisor of B_m; this is not quite the terminology of [**4**].

It follows from (2.3) that if p is a proper divisor of B_m then it is also a divisor of B_s, where

$$m \equiv s \pmod{p-1} \qquad (0 < s < p-1);$$

that $s \neq 0$ is a consequence of (2.2). Thus a proper divisor of any B_m is certainly irregular. Now assume that there are only a finite number of irregular primes $p_1, \cdots, p_k$, and consider the number B_M, where

$$(2.4)\qquad M = 2t\prod_{i=1}^{k}(p_i - 1).$$

If we put

Received by the editors August 23, 1953.

(2.5) $$B_M/M = N_M/D_M \qquad ((N_M, D_M) = 1),$$

it follows from the above and (2.2) that $N_M = \pm 1$. For, as already remarked, a prime divisor of N_M is a proper divisor of B_M and therefore irregular; but by (2.2) and (2.4) the irregular primes $p_1, \cdots, p_k$ occur in the denominator of B_M. On the other hand it is clear from

$$\frac{B_{2m}}{2m} = (-1)^{m-1} \frac{2(2m-1)!}{(2\pi)^{2m}} \sum_{r=1}^{\infty} \frac{1}{r^{2m}}$$

that $|B_{2m}/2m| \to \infty$ as $m \to \infty$. Since t in (2.4) is at our disposal, it is evident that this contradicts $|N_M| = 1$.

3. Some criteria in terms of Euler numbers for the first case of Fermat's last theorem have been given. Vandiver [**5**] has proved that if

$$x^p + y^p = z^p \qquad (p \nmid xyz)$$

is satisfied, then

(3.1) $$E_{p-3} \equiv 0 \pmod{p}.$$

Gut [**1**] has proved that if

$$x^{2p} + y^{2p} = z^{2p} \qquad (p \nmid xyz)$$

is satisfied, then

(3.2) $$E_{p-3} \equiv E_{p-5} \equiv E_{p-7} \equiv E_{p-9} \equiv E_{p-11} \equiv 0 \pmod{p}.$$

Here the E_m denote Euler numbers in the even suffix notation.

We accordingly define a prime p as irregular with respect to the Euler numbers if it divides at least one of the numbers

(3.3) $$E_2, E_4, \cdots, E_{p-3}.$$

We shall prove that the number of such primes is infinite.

Analogous to (2.3) we now have [**2**, Chap. 14]

(3.4) $$E_{m+r(p-1)} \equiv E_m \pmod{p} \qquad (m \geqq 1).$$

We have also the property [**2**, p. 273]: if $p-1 \mid m$,

(3.5) $$E_m \equiv \begin{cases} 0 \pmod{p} & (p \equiv 1 \pmod{4}) \\ 2 \pmod{p} & (p \equiv 3 \pmod{4}). \end{cases}$$

We shall say that p is a proper divisor of E_m provided $p \mid E_m$ and $p-1 \nmid m$; clearly in view of (3.5) only primes of the form $4n+1$ can be improper divisors.

It follows from (3.4) that if p is a proper divisor of E_m then it is also a divisor of E_s, where

$$m \equiv s \pmod{p-1} \qquad (0 < s < p-1).$$

Let us now assume that there are only a finite number of irregular primes (relative to the Euler numbers) $p_1, \cdots, p_k$, and consider the number E_M, where

$$M = 4t \prod (p_i - 1) + 2. \tag{3.6}$$

By (3.4)

$$E_M \equiv E_2 \equiv -1 \pmod{p_i} \qquad (i = 1, \cdots, k).$$

Thus

$$(E_M, p_1 p_2 \cdots p_k) = 1;$$

also since $M \equiv 2 \pmod 4$, it is clear that E_M has no improper divisors. Consequently $E_M = \pm 1$. But since

$$E_{2m} = (-1)^m \frac{4(2m)!2^{2m}}{\pi^{2m+1}} \sum_{r=0}^{\infty} \frac{(-1)^r}{r^{2m+1}},$$

it is evident that $|E_M| \to \infty$.

References

1. M. Gut, *Eulersche Zahlen und grosser Fermat'scher Satz*, Comment. Math. Helv. vol. 24 (1950) pp. 73–99.

2. N. Nielsen, *Traité élémentaire des nombres de Bernoulli*, Paris, 1923.

3. H. S. Vandiver and G. E. Wahlin, *Algebraic numbers* II, Bulletin of the National Research Council, no. 62, 1928.

4. H. S. Vandiver, *Note on the divisors of the numerators of Bernoulli's numbers*, Proc. Nat. Acad. Sci. U. S. A. vol. 18 (1932) pp. 594–597.

5. ———, *Note on Euler number criteria for the first case of Fermat's last theorem*, Amer. J. Math. vol. 62 (1940) pp. 79–82.

Duke University