MATHEMATICS OF COMPUTATION, VOLUME 32, NUMBER 142
APRIL 1978, PAGES 617–629

Cyclotomic Invariants and E-Irregular Primes

By R. Ernvall and T. Metsänkylä

Abstract. We prove some general results about the Iwasawa invariants λ^- and μ^- of the $4p$th cyclotomic field (p an odd prime), and determine the values of these invariants for $p < 10^4$. The properties of λ^- and μ^- are closely connected with the E-irregularity (i.e. the irregularity with respect to the Euler numbers) of p. A list of all E-irregular primes less than 10^4, computed by the first author, is included and analyzed.

1. Introduction. Let p be an odd prime. For a natural number m prime to p, consider the p-class groups of the cyclotomic fields K_n of mp^{n+1}th roots of unity ($n = 0, 1, \ldots$). For all sufficiently large n, the orders of these groups equal $p^{e(n)}$ with $e(n) = \lambda n + \mu p^n + \nu$, where $\lambda = \lambda_{mp}$ and $\mu = \mu_{mp}$ are nonnegative integers that (as well as ν) do not depend on n. The same holds true when K_n is replaced by its maximal real subfield; let us denote then the corresponding invariants by λ^+ and μ^+. Put $\lambda = \lambda^- + \lambda^+$, $\mu = \mu^- + \mu^+$. Then the invariants $\lambda^- = \lambda^-_{mp}$ and $\mu^- = \mu^-_{mp}$ are related to the exact power of p dividing the first factor h_n^- of the class number of K_n.

Iwasawa [10] has conjectured that $\mu = 0$ for every choice of m. This has been proved only for $p = 3$ [5]. Note that $\lambda^+ \leqslant \lambda^-$, $\mu^+ \leqslant \mu^-$ (see e.g. [5, p. 63]) so that the results $\lambda = 0$ and $\mu = 0$ are implied by $\lambda^- = 0$ and $\mu^- = 0$, respectively. We also know that $\lambda^- = \mu^- = 0$ if and only if p does not divide h_1^-/h_0^- (see [9, p. 95], where λ^- and μ^- are denoted by λ and μ).

Suppose that $m = 1$. Then the condition $\lambda^- = \mu^- = 0$ is also equivalent to the fact that p is a *regular* prime [9, p. 96], i.e. $p \nmid h_0^-$ or, equivalently, p does not divide the numerator of any of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$. For irregular primes p, the invariants λ_p^- and μ_p^- (and λ_p, μ_p) have been determined with the help of computers up to $p < 125{,}000$ [11], [14], [23]. It has turned out that $\mu_p = 0$ for all these p.

In this paper we shall be concerned with the case $m = 4$. Although this case is rather similar to the case $m = 1$, some new features appear. We shall prove that $\mu_{4p}^- = \mu_p^-$ if p is *E-regular*, i.e. p does not divide any of the Euler numbers $E_2, E_4, \ldots, E_{p-3}$. Furthermore, using results obtained by computer, we shall show that $\mu_{4p}^- = 0$ for every prime $p < 10^4$, and determine the value of λ_{4p}^- for these p.

Received February 8, 1977; revised August 15, 1977.
AMS (MOS) subject classifications (1970). Primary 10A40, 12A35, 12A50; Secondary 10B15.
Key words and phrases. Class numbers, cyclotomic fields, Z_p-extensions, E-irregular primes, irregular primes, Euler numbers, Fermat's Last Theorem, Fermat quotients.

We note that the connection between the E-regularity of p and the divisibility by p of the class number of the $4p$th cyclotomic field was discovered by Gut [7] (see also [21]). Gut [6] has also found that the E-regularity of p is connected with the solvability of the diophantine equation $x^{2p} + y^{2p} = z^{2p}$.

The list of E-irregular primes produced by our computation procedure is also interesting in its own right. This list is included at the end of this paper and analyzed in Section 2. Among other things, it may be compared with the corresponding list of ordinary irregular primes (called *B-irregular* below).

Section 2, together with Section 7 containing a report of the computations, is due to the first author, who also prepared the computer programs. Sections 3–6 concerning λ_{4p}^- and μ_{4p}^- are work of the second author.

2. E-Irregular Primes. Euler numbers E_n ($n = 0, 1, \ldots$) can be defined by the symbolic equations

$$(E + 1)^n + (E - 1)^n = 2 \quad \text{for } n = 0,$$
$$= 0 \quad \text{for } n \geqslant 1$$

(see, e.g. [19, p. 25]). It follows that all the E_n are integers and those with an odd index equal zero. Moreover,

$$(1) \qquad (m + E + 1)^{2n} + (m + E - 1)^{2n} = 2m^{2n} \qquad (n \geqslant 1),$$

where m is an arbitrary integer. Take an odd k. Letting m run through odd integers from 1 to $2k - 1$, we get from (1)

$$(2) \qquad E_{2n} \equiv \sum_{a=1}^{2k} \theta(a) a^{2n} \pmod{k^2},$$

where θ is the unique Dirichlet character with conductor 4. Almost all the properties of Euler numbers needed in the sequel are based on this congruence.

We say that a prime $p \geqslant 5$ is *E-irregular* if there exists an even integer $2n$ such that $2 \leqslant 2n \leqslant p - 3$ and p divides E_{2n}. We then say that $(p, 2n)$ is an *E-irregular pair*. For each p, we call the number of such pairs the *index of E-irregularity* of p and denote it by i_E. Carlitz [3] has proved that there are infinitely many E-irregular primes. The first author [4] has shown that the number of the E-irregular primes $\not\equiv \pm 1 \pmod 8$ is infinite. It is not known whether there are infinitely many *E-regular* primes.

We used a computer to find all E-irregular pairs $(p, 2n)$ with $p < 10^4$. The table at the end of the paper lists all these pairs. There are 495 E-irregular primes in all. It should be noted that, as was to be expected, they are quite evenly distributed mod 8. Furthermore, $i_E = 2$ for 86 primes and $i_E = 3$ for 15 primes. The case $i_E = 4$ occurs for the primes 3673 and 8681 and the case $i_E = 5$ for 5783. No prime with $i_E \geqslant 6$ was found. (For these and the following results, compare the corresponding results concerning B-irregular primes [12], [14], [23].)

Gut [6] has proved that the condition $E_{p-3} \equiv E_{p-5} \equiv E_{p-7} \equiv E_{p-9} \equiv E_{p-11} \equiv 0 \pmod p$ is necessary for the equation $x^{2p} + y^{2p} = z^{2p}$ ($p \nmid xyz$) to be solvable. Vandiver [22] has given a proof of the fact that if $x^p + y^p = z^p$ ($p \nmid xyz$) is satisfied,

then $(p, p-3)$ is an E-irregular pair. In our range we found that $(p, p-3)$ is an E-irregular pair for $p = 149$ and 241, $(p, p-9)$ is such a pair for $p = 19$, 31, and 3701, and $(p, p-11)$ for $p = 139$ only, while there is no example of an E-irregular pair of the form $(p, p-5)$ or $(p, p-7)$. No consecutive E-irregular pairs (of the form $(p, 2n)$ and $(p, 2n+2)$) were found.

For each E-irregular pair $(p, 2n)$ we also computed $E_{2n} \bmod p^2$. It appeared that E_{2n} is never divisible by p^2 for $p < 10^4$ (cf. [13], [14], [23]).

Denote by $\pi_B(x)$, $\pi_E(x)$, and $\pi_{BE}(x)$ the number of those primes, not exceeding x, which are B-irregular, E-irregular, and both B- and E-irregular, respectively. Siegel [20] predicted that the ratio $\pi_B(x)/\pi(x)$ approaches the limit $1 - e^{-1/2} = 0.3934\ldots$ as $x \to \infty$. This result can be obtained by assuming that the numerators of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ are randomly distributed mod p. The same hypothesis on the Euler numbers $E_2, E_4, \ldots, E_{p-3}$ leads to the conjecture that $\pi_E(x)/\pi(x) \to 1 - e^{-1/2}$ and $\pi_{BE}(x)/\pi(x) \to 1 - 2e^{-1/2} + e^{-1} = 0.1548\ldots$ as $x \to \infty$. The information obtained from our computations seems to support these hypotheses, as is seen from the following table. (The values of π_B and π_B/π are appended in this table for the sake of comparison. In calculating π_B and π_{BE} we used the table computed by Johnson [14].)

x	π_B	π_E	π_{BE}	π_B/π	π_E/π	π_{BE}/π
2000	113	121	56	0.373	0.399	0.18
4000	213	218	91	0.387	0.396	0.17
6000	308	300	126	0.393	0.383	0.16
8000	397	400	169	0.394	0.397	0.17
10000	497	495	218	0.404	0.403	0.18

As in the case of B-irregular primes, one is also led to the conjecture that the E-irregular primes with index k satisfy the Poisson distribution $t^k e^{-t}/k!$ with $t = \frac{1}{2}$. The table below compares the actual number of primes of each index within our range with these predictions.

Index	0	1	2	3	$\geqslant 4$	Total
Observed	732	391	86	15	3	1227
Expected	744.2	372.1	93.0	15.5	2.2	1227.0

3. Preliminaries About the Iwasawa Invariants. We shall treat the invariants λ_{4p}^- and μ_{4p}^- on the basis of the theory of p-adic L-functions, due to Iwasawa [9, Section 6].

Denote by Z_p the ring of p-adic integers. For a rational integer a prime to p, let $\omega(a) \in Z_p$ be the p-adic limit of the sequence $\{a^{p^n}\}$. Then

$$\omega(a) \equiv a^{p^n} \pmod{p^{n+1}Z_p} \tag{3}$$

for all $n \geqslant 0$, and ω can be viewed, in a natural way, as a Dirichlet character that generates the character group mod p.

For each $n \geqslant 0$, let $\sigma_n(a)$ denote the residue class mod $4p^{n+1}$ determined by the integer a, and put

$$\Gamma_n = \{\sigma_n(a) \mid a \equiv 1 \pmod{4p}\},$$
$$\Delta_n = \{\sigma_n(a) \mid a \text{ odd and } a^{p-1} \equiv 1 \pmod{p^{n+1}}\}.$$

It is easy to verify that the multiplicative residue class group mod $4p^{n+1}$ is the direct product of its subgroups Γ_n and Δ_n. Denote by A_n the set of integers a with $1 \leqslant a < 4p^{n+1}$ and $(a, 4p) = 1$. Fix p^n (= the order of Γ_n) integers c_n so that $1 \leqslant c_n < 4p^{n+1}$ and, for each $a \in A_n$,

$$\sigma_n(a) = \sigma_n(c_n)\sigma_n(d_n), \qquad \sigma_n(c_n) \in \Gamma_n,\ \sigma_n(d_n) \in \Delta_n.$$

In the following χ will denote an even character whose conductor f_χ equals p or $4p$. Let R be the inverse limit of the group algebras $Z_p[\Gamma_n]$ with respect to the natural homomorphisms, induced by $\sigma_m(a) \mapsto \sigma_n(a)$ $(m \geqslant n)$. For $n \geqslant 0$, write

$$\xi_n = \xi_n(\chi) = -(8p^{n+1})^{-1} \sum_{a \in A_n} a\chi(a)\omega^{-1}(a)\sigma_n(c_n)^{-1}. \tag{4}$$

We know that $\xi_n \in Z_p[\Gamma_n]$ and that $\xi = \lim \xi_n$ is a well-defined element of R (see [9, pp. 72–76], where $\sigma_n(c_n)$ and $\sigma_n(d_n)$ are denoted by $\gamma_n(a)$ and $\delta_n(a)$, respectively). Moreover, there exists an isomorphism τ from R onto the formal power series algebra $Z_p[[x]]$ such that the image of ξ under τ, say

$$f(x; \chi) = \sum_{k=0}^{\infty} a_k x^k \in Z_p[[x]],$$

has the following connection with the p-adic L-function $L_p(s; \chi)$:

$$L_p(s; \chi) = 2f((1 + 4p)^s - 1; \chi)$$

for all $s \in Z_p$ (see [9, pp. 69, 77]). This implies, among other things, that $f(x; \chi)$ does not vanish identically. Consequently, there are unique nonnegative integers $\lambda(\chi)$ and $\mu(\chi)$ such that

$$f(x; \chi) = p^{\mu(\chi)} \sum_{k=0}^{\infty} b_k x^k \qquad (b_k \in Z_p)$$

with $b_k \equiv 0 \pmod{pZ_p}$ for $0 \leqslant k < \lambda(\chi)$ and $b_{\lambda(\chi)} \not\equiv 0 \pmod{pZ_p}$. Then

$$\lambda_{4p}^- = \sum_\chi \lambda(\chi), \qquad \mu_{4p}^- = \sum_\chi \mu(\chi), \tag{5}$$

where χ ranges over all even characters with $f_\chi = p$ or $4p$ [17, p. 65].

Let X stand for the set of all even characters with conductor $4p$, that is,

$$X = \{\theta\omega^{m+1} \mid m \text{ even and } 0 \leqslant m \leqslant p - 3\}.$$

We rewrite the equations (5) as

$$\lambda_{4p}^{-} = \lambda_{p}^{-} + \sum_{\chi \in X} \lambda(\chi), \qquad \mu_{4p}^{-} = \mu_{p}^{-} + \sum_{\chi \in X} \mu(\chi). \tag{6}$$

To obtain information about $\lambda(\chi)$ and $\mu(\chi)$ we have to investigate the divisibility by p of the coefficients $a_0, a_1, \ldots$ of $f(x; \chi)$. For this purpose we need a relationship between $f(x; \chi)$ and the generalized Bernoulli numbers (for the definition of these, see, e.g. [9, p. 9]). Indeed, for $n \geqslant 1$ and $\chi \in X$ we have

$$2f((1 + 4p)^{1-n} - 1; \chi) = -(1 - (\chi\omega^{-n})(p)p^{n-1})B_n(\chi\omega^{-n})/n, \tag{7}$$

where $B_n(\psi)$ denotes the nth generalized Bernoulli number belonging to the character ψ [9, p. 78]. Below we shall employ this formula for $n = 1$ and $n = 2$ only; then it will be useful to know that

$$B_1(\psi) = f^{-1} \sum_{a=1}^{f} \psi(a)a \qquad (\psi \text{ odd}), \tag{8}$$

$$B_2(\psi) = f^{-1} \sum_{a=1}^{f} \psi(a)a^2 \qquad (\psi \text{ even}), \tag{9}$$

where $f = f_\psi > 1$ ([9, p. 14] and [17, p. 67]).

In studying $\lambda(\chi)$ and $\mu(\chi)$ for $\chi = \theta\omega^{m+1} \in X$ we have to distinguish between the cases $m = 0$ and $m \neq 0$.

4. The Zero Case.

THEOREM 1. $\mu(\theta\omega) = 0$.

Proof. Write the formula (4), for $\chi = \theta\omega$, in the form

$$\xi_n = \sum_{c_n} S_n(c_n)\sigma_n(c_n)^{-1}, \qquad S_n(c_n) = -(8p^{n+1})^{-1} \sum_{a \in A_n(c_n)} a\theta(a),$$

where c_n ranges over all its p^n values and

$$A_n(c_n) = \{a \in A_n \mid \sigma_n(a) \in \sigma_n(c_n)\Delta_n\}.$$

Assume that $\mu(\theta\omega) > 0$. From a result proved in [17, p. 69], we then infer that

$$S_n(c_n) \equiv 0 \pmod{pZ_p}$$

for all $n \geqslant 0$ and all c_n.

Let $a \in A_n$ with $1 \leqslant a < 2p^{n+1}$. Then it is seen that $a \in A_n(c_n)$ if and only if $a + 2p^{n+1} \in A_n(c_n)$. Indeed, suppose that $a \in A_n(c_n)$; there is an integer d_n such that

$$a \equiv c_n d_n \pmod{4p^{n+1}}, \qquad \sigma_n(d_n) \in \Delta_n,$$

and then

$$a + 2p^{n+1} \equiv c_n(d_n + 2p^{n+1}) \pmod{4p^{n+1}},$$

where, furthermore, $\sigma_n(d_n + 2p^{n+1}) \in \Delta_n$. The converse is verified by a similar argument. Observing that $\theta(a + 2p^{n+1}) = -\theta(a)$ we thus obtain

$$S_n(c_n) = -(8p^{n+1})^{-1}\sum_a [a\theta(a) + (a + 2p^{n+1})\theta(a + 2p^{n+1})] = 4^{-1}\sum_a \theta(a),$$

where the sums are extended over those numbers $a \in A_n(c_n)$ for which $1 \leqslant a < 2p^{n+1}$. The last sum consists of $p - 1$ terms $\theta(a) = \pm 1$. Being divisible by p, it must therefore vanish. Consequently, $\xi_n = 0$ for all $n \geqslant 0$. This in turn implies that $\xi = 0$, and so $f(x; \theta\omega) = 0$, which is a contradiction.

THEOREM 2. *If* $p \equiv 3 \pmod 4$, *then* $\lambda(\theta\omega) = 0$. *If* $p \equiv 1 \pmod 4$, *then* $\lambda(\theta\omega) > 0$.

Proof. By setting $n = 1$ in (7) we get

$$a_0 = f(0; \theta\omega) = -(1 - \theta(p))B_1(\theta)/2.$$

It follows from (8) that $B_1(\theta) = -\frac{1}{2}$. Hence $a_0 = \frac{1}{2}$ if $p \equiv 3 \pmod 4$, and $a_0 = 0$ if $p \equiv 1 \pmod 4$. In view of Theorem 1 this proves our assertion.

The proof of Theorem 2 also gives an easier proof of Theorem 1 in the case $p \equiv 3 \pmod 4$. As a consequence of Theorem 2, one finds that $\lambda_{4p}^- > 0$ if $p \equiv 1 \pmod 4$. We remark that the weaker result $\lambda_{4p}^- + \mu_{4p}^- > 0$, for $p \equiv 1 \pmod 4$, follows also directly from [16, Satz 10] which concerns the divisibility by p of the first factor of the class number of the $3p^{n+1}$th and $4p^{n+1}$th cyclotomic fields.

THEOREM 3. *Let* $p \equiv 1 \pmod 4$. *Then* $\lambda(\theta\omega) > 1$ *if and only if the Euler number* E_{p-1} *is divisible by* p^2.

Proof. Since in this case $f(x; \theta\omega) = a_1 x + a_2 x^2 + \ldots$ and $\mu(\theta\omega) = 0$, the condition $\lambda(\theta\omega) > 1$ is equivalent to $p \mid a_1$. Put $\alpha = (1 + 4p)^{-1} - 1 = -4p(1 + 4p)^{-1}$. Equation (7) gives, for $n = 2$, the relation

$$4f(\alpha; \theta\omega) = -B_2(\theta\omega^{-1}).$$

Accordingly, $p \mid a_1$ if and only if $B_2(\theta\omega^{-1}) \equiv 0 \pmod{p^2 Z_p}$.

We shall show that

$$B_2(\theta\omega^{-1}) \equiv E_{p-1} \pmod{p^2 Z_p}; \tag{10}$$

by the above this proves the theorem. Using (9), we obtain

$$B_2(\theta\omega^{-1}) = (4p)^{-1}\sum_{a=1}^{4p} \theta(a)\omega^{-1}(a)a^2$$

$$= -\sum_{a=1}^{2p} \theta(a)\omega^{-1}(a)a - p\sum_{a=1}^{2p} \theta(a)\omega^{-1}(a).$$

The last sum here vanishes, as $\theta(2p - a) = \theta(a)$ and $\omega(2p - a) = -\omega(a)$. By (2) and (3) we, therefore, see that (10) is equivalent to

$$\sum_{a=1}^{2p} \theta(a)(\omega^{-1}(a)a + \omega(a)a^{-1}) \equiv 0 \pmod{p^2 Z_p}.$$

The validity of this congruence follows from the identity

$$\sum_{a=1}^{2p} \theta(a)\omega^{-1}(a)a(1-\omega(a)a^{-1})^2 \equiv 0 \pmod{p^2 Z_p}$$

on noting that $p \equiv 1 \pmod 4$ implies $\Sigma_{a=1}^{2p}\theta(a) = 0$. Hence, our theorem is proved.

Note that for $p \equiv 1 \pmod 4$, E_{p-1} is always divisible by p. This can be seen either from the preceding proof or, of course, directly from (2). – On checking by computer all primes p less than 10^4 and congruent to 1 (mod 4), we found that E_{p-1} was never divisible by p^2. Hence, we have the result: *if* $p \equiv 1 \pmod 4$, *then* $\lambda(\theta\omega) = 1$ *whenever* $p < 10^4$.

5. The Remaining Cases. In the following the statement $m \not\equiv 0$ will mean that m is even and $2 \leqslant m \leqslant p-3$, so that the character $\chi = \theta\omega^{m+1}$ belongs to X and is different from $\theta\omega$. It should be noted that the considerations in this section (as well as above in the proof of Theorem 3) are partly similar to those presented in [17, Section 6], where the case of the pth cyclotomic field was discussed.

THEOREM 4. *If* $\chi = \theta\omega^{m+1}$, $m \not\equiv 0$, *then* $\lambda(\chi) = \mu(\chi) = 0$ *if and only if the pair* (p, m) *is E-regular.*

Proof. The same arguments as before give now

$$4a_0 = -2B_1(\theta\omega^m) = -(2p)^{-1}\sum_{a=1}^{4p}\theta(a)\omega^m(a)a$$

$$= \sum_{a=1}^{2p}\theta(a)\omega^m(a) \equiv E_m \pmod{pZ_p}.$$

On the other hand, $p \nmid a_0$ if and only if $\lambda(\chi) = \mu(\chi) = 0$.

THEOREM 5. *Let* $\chi = \theta\omega^{m+1}$, $m \not\equiv 0$. *If the pair* (p, m) *is E-irregular and the congruence*

$$E_m \equiv E_{m+p-1} \pmod{p^2} \tag{11}$$

does not hold, then $\lambda(\chi) = 1$ *and* $\mu(\chi) = 0$.

Proof. By Theorem 4, it suffices to show that $p \mid a_1$ implies (11).

Let $p \mid a_1$ and choose α as in the proof of Theorem 3. Then

$$f(0; \theta\omega^{m+1}) \equiv f(\alpha; \theta\omega^{m+1}) \pmod{p^2 Z_p}.$$

Since

$$4f(\alpha; \theta\omega^{m+1}) = -B_2(\theta\omega^{m-1}) = \sum_{a=1}^{2p}\theta(a)\omega^{m-1}(a)a,$$

the above congruence can be written in the form

$$\sum_{a=1}^{2p}\theta(a)\omega^{m-1}(a)(\omega(a)-a) \equiv 0 \pmod{p^2 Z_p}.$$

This yields

$$\sum_{a=1}^{2p}\theta(a)a^{m-1}(a^p - a) \equiv 0 \pmod{p^2 Z_p},$$

and so the assertion (11) follows by virtue of (2).

Our computer search indicates that (11) does not hold for any E-irregular pair (p, m) with $p < 10^4$. Consequently, $\lambda(\theta\omega^{m+1}) = 1$ *and* $\mu(\theta\omega^{m+1}) = 0$ *whenever* $m \neq 0$ *and the pair* (p, m) *is E-irregular with* $p < 10^4$.

An inspection of the preceding proof shows that one can prove even more, namely that $p \mid a_1$ is equivalent to (11). Put

$$K_r(2n) = \sum_{i=0}^{r} (-1)^i \binom{r}{i} E_{2n+i(p-1)} \qquad (r = 0, 1, \ldots).$$

Then (11) can be written as $K_1(m) \equiv 0 \pmod{p^2}$. By Kummer's congruences [18, Chapter XIV], $K_r(2n) \equiv 0 \pmod{p^r}$ for $2n \geqslant r$, so that the preceding congruence is always true mod p.

If (11) did hold for some E-irregular pair (p, m), it would be rather easy to check whether $p \mid a_2$ or not. Indeed, the second author has proved that generally $a_0 \equiv a_1 \equiv \ldots \equiv a_k \equiv 0 \pmod{pZ_p}$ if and only if $K_r(m) \equiv 0 \pmod{p^{r+1}}$ for $r = 0, \ldots, k$, provided that $k \leqslant m$. The proof will appear elsewhere.

6. Summary of Results About the Iwasawa Invariants. Summarizing the results from Theorems 1–5 and from our computer search we may state, by (6), that

(i) $\mu_{4p}^- = \mu_p^-$ if either p is E-regular or p is E-irregular and less than 10^4;

(ii) $\lambda_{4p}^- = \lambda_p^-$ if $p \equiv 3 \pmod 4$ and p is E-regular;

(iii) $\lambda_{4p}^- = \lambda_p^- + i_E$ if $p \equiv 3 \pmod 4$ and $p < 10^4$;

(iv) $\lambda_{4p}^- = \lambda_p^- + 1$ if $p \equiv 1 \pmod 4$ and p is E-regular;

(v) $\lambda_{4p}^- = \lambda_p^- + i_E + 1$ if $p \equiv 1 \pmod 4$ and $p < 10^4$.

Note in this connection that, by known results, $\mu_p^- = \lambda_p^- = 0$ if and only if p is B-regular, and $\mu_p^- = 0$ and λ_p^- equals the index of B-irregularity of p for all B-irregular primes less than 125,000 (see [14], [23]).

7. The Computations. All the computations were performed on the UNIVAC 1108 computer at the University of Turku, and they took about 26 hours. Only integers and vectors consisting of integer components were used, and so the possibility of round-off errors was avoided.

We used the following criterion in order to find out the E-irregular pairs $(p, 2n)$. The powers of integers needed here were calculated by the aid of a primitive root g_p, which was computed first (the values of g_p were checked from a table).

THEOREM 6. *A necessary and sufficient condition for* $(p, 2n)$ *to be an E-irregular pair is that*

$$1^{2n} + 2^{2n} + \ldots + [p/4]^{2n} \equiv 0 \pmod{p}.$$

Proof. Put $s = (p-1)/2$. By (2),

$$\begin{aligned} E_{2n} &\equiv 2\{1^{2n} - 3^{2n} + - \ldots + (-1)^{s-1}(p-2)^{2n}\} \\ &\equiv (-1)^{s-1}2\{2^{2n} - 4^{2n} + - \ldots + (-1)^{s-1}(p-1)^{2n}\} \\ &\equiv (-1)^{s-1}2^{2n+1}\{1^{2n} - 2^{2n} + - \ldots + (-1)^{s-1}s^{2n}\} \pmod{p}. \end{aligned}$$

TABLE

E-irregular pairs $(p, 2n)$ *to* $p < 10^4$

p	2n	p	2n	p	2n	p	2n
19	10	761	104	1531	472	2203	606
31	22	769	246		848		1944
43	12	773	498	1559	1402	2213	572
47	14	811	726	1583	438		2030
61	6	821	622	1601	52	2221	558
67	26	877	286	1621	782	2239	1792
71	28	887	560	1637	590	2293	392
79	18	907	318	1663	1626	2341	72
101	62		818	1693	1600	2377	576
137	42	929	722	1697	606	2411	666
139	128	941	686	1723	592	2417	2360
149	146		804		1166	2459	916
193	74	967	12	1733	482	2473	2000
223	132	971	824	1759	1002	2477	104
241	210	983	556	1787	396	2531	1366
	238	1013	410		962	2543	160
251	126	1019	88	1801	868	2579	2344
263	212		288	1831	348	2591	164
277	8		500	1867	262	2609	904
307	90	1031	278	1873	1704	2617	950
	136	1039	292	1877	924	2633	2354
311	86	1049	342	1879	198	2659	10
	192	1051	360		422	2671	472
349	18	1069	544	1889	1612	2677	2078
	256		612	1901	1478	2687	1290
353	70	1151	114	1907	368		2310
359	124	1163	870	1931	1762	2699	282
373	162	1187	166	1933	1800	2711	1728
379	316		334	1951	256	2729	1472
419	158	1223	364	1987	932		1886
433	214	1229	930	1993	178	2731	1034
461	426	1231	766	1997	1730	2749	54
463	228	1277	480	2011	982	2797	1912
491	428	1279	508		1600	2803	1834
509	140	1283	1028	2039	68		1924
541	464	1291	674		852		2748
563	174	1307	1070		1698	2819	252
	260	1319	1186	2063	1976		2686
571	388	1361	440	2069	504	2843	1852
577	208	1381	608	2081	590	2879	1582
	426	1399	1114	2083	2028	2897	2030
587	44	1409	362	2099	1682	2917	2076
619	370	1423	652	2129	1548	2957	1372
	542	1427	1314	2131	2070	2963	1610
677	528		1410	2137	24	2971	2368
691	548	1429	626	2141	182	2999	520
709	492	1439	1192	2143	694		2472
739	494	1447	1080	2161	2082	3001	310
751	296	1453	322	2179	738	3061	304
	710	1523	264				1558

TABLE (*continued*)

p	2n	p	2n	p	2n	p	2n
3067	2294	3911	2106	4799	2302	5807	3408
3079	706	3917	3330	4813	1422		5454
3089	2604	3923	1312	4817	2136	5813	3168
3119	1492	3989	316	4861	2638	5827	3372
3121	358	4003	1876	4871	2662	5843	3734
3137	2070	4007	3136	4933	1094	5849	1202
3163	1308	4021	1576	4937	734	5857	2354
3167	1690		2908	4943	4194		4716
	2186	4051	3496	5009	2016	5867	2554
3169	1216	4057	2622	5101	1014	5879	2874
3187	418	4093	2918	5107	4870	5881	5374
	2298	4099	898	5113	310	6011	260
3217	696		3912	5147	682	6037	1438
	1700	4129	1000		1246	6043	124
3257	262	4133	1282		5108	6047	4960
	1054	4153	34	5153	3794	6053	3768
	2598		802		4542	6089	4570
3301	1748	4241	4108	5209	4270		5492
3313	650	4259	2426	5227	3994	6121	3712
3331	2352	4271	1386	5233	3602	6131	5028
3343	146		2684	5279	766	6211	5074
	166	4283	2824		3766	6229	1786
3449	2752	4289	1128	5303	56		3118
	3058		1446	5351	4088		3932
3467	1288	4337	356	5393	2296	6247	5812
3491	1512	4339	198		4128	6263	182
3517	2176	4349	292	5399	4328	6269	1340
3539	1266		2254		5084		5980
3541	318	4357	230	5413	4458	6271	2486
3547	2144	4373	3678	5521	5454	6301	5880
3571	780	4391	1542	5527	872	6329	976
	1106	4397	84	5531	604	6337	5722
3581	2288		1042	5557	1748	6359	3896
3623	2074	4421	2206		4984	6379	4778
3631	1086	4463	134	5563	42	6397	5456
3671	740	4481	978		1286		6072
3673	204		1568		3860	6421	2754
	382	4493	2740	5569	778		5524
	1650		4082	5591	580	6427	1326
	2740	4523	1606		656	6449	4528
3677	208	4549	3684	5623	208	6473	6456
	326	4591	4490	5639	50	6571	2944
3701	3692	4603	1526	5641	704	6577	1128
3727	416	4643	4054		2052	6607	3074
3733	1196	4657	2434	5659	5446	6619	1110
3761	3114	4673	4430	5689	5442	6653	3738
3793	204	4679	568	5711	5432	6659	5896
	2918	4691	3630	5783	1232	6691	1510
3797	1438	4703	2714		4630	6709	2680
3821	404	4721	4570		4892	6719	5142
3833	1380	4729	3608		5662	6737	2034
3847	3202	4733	3120		5704	6779	154
3851	2886	4789	404	5801	1808	6791	3866
3853	816		942			6793	6542

TABLE (*continued*)

p	2n	p	2n	p	2n	p	2n
6803	1406	7589	4002	8447	4546	9323	4046
6833	2542		4290		8226		6484
6863	62	7591	976	8501	6842		8802
	2438	7603	4352	8527	7446	9337	8942
6869	6356	7607	7258	8573	4332	9341	3784
6899	4164	7639	1928	8609	2310	9371	2060
6947	3050	7669	302		5208		4706
6971	6894		4280	8627	2084		5886
6977	3504	7681	7462	8629	176	9377	5652
6991	3598	7723	4510	8647	102	9391	938
6997	122	7727	7220		126		1798
7019	2904	7741	3460	8663	734	9397	744
	5826	7753	130	8669	5848	9403	556
7039	870	7757	1662		8244		3676
	5188	7789	2240	8681	1552	9413	2400
	6432	7853	1548		6406	9473	3308
7043	448		5836		7692	9491	9146
	516	7907	5684		8258	9511	2220
7069	6214	7937	1938	8689	3774	9539	8304
7079	4506	7949	1344	8693	3270	9547	7380
	6568	7993	5830	8713	3908		7532
7103	6622		7298		7362	9587	1600
7121	6992		7928	8719	2186	9601	1702
7129	6048	8039	436	8737	4098	9613	2372
7151	1906	8059	2172	8761	5886	9619	8332
7177	4920	8081	1862	8803	350	9623	4028
7193	596		5786		1840	9629	4310
7207	5052	8089	2864		5102	9631	498
7213	748		7062	8821	5206	9643	5218
7219	2256	8101	2608	8831	8394		9622
7229	3420	8111	6100	8837	4846	9677	5716
7243	5432	8117	4450	8839	8708	9689	6232
7297	710	8123	3456	8863	2296	9733	6850
7307	1664	8171	696		4442	9739	8766
7309	6074	8219	2898	8893	2848	9767	2144
7321	5350	8221	350	8923	626		3794
	5844	8231	268	8929	4736	9791	5122
7331	5426		790	9001	6954	9811	9106
7351	4644		3612	9011	3642	9817	2334
7393	4440	8233	3560	9049	4672	9883	5524
7411	356		4736	9067	3264		7982
7417	7336	8237	8116	9091	930		9150
7433	6414	8291	3958		3336	9887	278
7481	5896	8311	5462	9127	6026	9907	2774
7487	418		5868	9133	2098	9967	4522
7489	278	8329	6852		6980		5540
7507	2050	8377	1088	9137	6146		
7517	2672	8387	5000	9181	2944		
	6870	8389	2654	9187	580		
7529	2916	8423	3684		3332		
7541	4098		6696		7552		
7559	1586	8429	6554	9257	36		
7577	2006	8431	6464		3018		
	4064			9277	228		

On the other hand,

$$2\sum_{k=1}^{s} k^{2n} \equiv \sum_{k=1}^{p-1} k^{2n} \equiv 0 \pmod{p}.$$

Combining these congruences, we see that

$$E_{2n} \equiv (-1)^s 2^{4n+2}\{1^{2n} + 2^{2n} + \ldots + [p/4]^{2n}\} \pmod{p}.$$

This proves the theorem.

For each E-irregular pair $(p, 2n)$ we computed $E_{2n}/p \bmod p$ and $(E_{2n+p-1} - E_{2n})/p \bmod p$ on the basis of the congruence (2). Similarly, this congruence was employed to compute $E_{p-1}/p \bmod p$ for each $p \equiv 1 \pmod 4$. To write (2) in a more suitable form, observe first that the *Fermat quotient* of an integer u prime to p is defined as the least nonnegative integer q_u satisfying the congruence $u^{p-1} \equiv 1 + q_u p \pmod{p^2}$. It is easy to verify that $q_{2p-u} \equiv q_u + 2u^{p-2} \pmod p$. Hence (2) yields the following congruences which were actually used in the computations:

$$E_{2n}/p \equiv 2p^{-1}\sum_{k=1}^{s}(-1)^{k+1}(2k-1)^{2n} - 4n\sum_{k=1}^{s}(-1)^{k+1}(2k-1)^{2n-1} \pmod{p},$$

$$(E_{2n+p-1} - E_{2n})/p \equiv 2\sum_{k=1}^{s}(-1)^{k+1}\{(2k-1)^{2n}q_{2k-1} + (2k-1)^{2n-1}\} \pmod{p},$$

$$E_{p-1}/p \equiv 2\sum_{k=1}^{s}(-1)^{k+1}\{q_{2k-1} + (2k-1)^{p-2}\} \pmod{p} \quad (\text{for } p \equiv 1 \pmod 4).$$

As a check, we computed the value mod p of the expression

$$S = -6\sum_{k=1}^{s}(2k-1)^2 q_{2k-1}.$$

Indeed, it follows from the known congruence

$$B_2 + 2\sum_{k=1}^{p-1} k^2 q_k \equiv 0 \pmod{p}$$

(see, e.g. [15, p. 255]) that $S \equiv 1 \pmod p$. A further check was supplied by the value of q_2, which was also printed and then compared with Haussner [8]. Our value of q_2 was different from that of [8] for eleven primes, namely 2437, 4049, 4733, 4969, 5689, 6113, 6997, 7121, 7321, 8089, and 8093. A comparison with Beeger's tables [1], [2] showed that in these cases q_2 is incorrectly given in [8]. We note that there can be more errors in [8] (extended up to the prime 10 009), for we checked only the primes ($< 10^4$) which are either congruent to 1 (mod 4) or E-irregular.

A table including all the results of our computations has been deposited in the UMT file.

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

1. N. G. W. H. BEEGER, "On a new case of the congruence $2^{p-1} \equiv 1 \pmod{p^2}$," *Messenger of Math.*, v. 51, 1922, pp. 149–150. Jbuch **48**, 1154.

2. N. G. W. H. BEEGER, "On the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and Fermat's last theorem," *Messenger of Math.*, v. 55, 1925/1926, pp. 17–26. Jbuch **51**, 127.

3. L. CARLITZ, "Note on irregular primes," *Proc. Amer. Math. Soc.*, v. 5, 1954, pp. 329–331. MR **15**, 778.

4. R. ERNVALL, "On the distribution mod 8 of the E-irregular primes," *Ann. Acad. Sci. Fenn. Ser. A I Math.*, v. 1, 1975, pp. 195–198. MR **52** #5594.

5. B. E. FERRERO, *Iwasawa Invariants of Abelian Number Fields*, Thesis, Princeton Univ., 1975.

6. M. GUT, "Eulersche Zahlen und grosser Fermat'scher Satz," *Comment. Math. Helv.*, v. 24, 1950, pp. 73–99. MR 12, 243.

7. M. GUT, "Euler'sche Zahlen und Klassenanzahl des Körpers der $4l$-ten Einheitswurzeln," *Comment. Math. Helv.*, v. 25, 1951, pp. 43–63. MR 12, 806.

8. R. HAUSSNER, "Reste von $2^{p-1}-1$ nach dem Teiler p^2 für alle Primzahlen bis 10009," *Arch. Math. Natur.*, v. 39, no. 2, 1925, 17pp. Jbuch **51**, 128.

9. K. IWASAWA, *Lectures on p-Adic L-Functions*, Ann. of Math. Studies, No. 74, Princeton Univ. Press, Princeton, N. J., 1972. MR **50** #12974.

10. K. IWASAWA, "On the μ-invariants of Z_l-extensions," *Number Theory, Algebraic Geometry and Commutative Algebra*, in honor of Y. Akizuki, Kinokuniya, Tokyo, 1973, pp. 1–11. MR **50** #9839.

11. 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.

12. W. JOHNSON, "On the vanishing of the Iwasawa invariant μ_p for $p < 8000$," *Math. Comp.*, v. 27, 1973, pp. 387–396. MR **52** #5621.

13. W. JOHNSON, "Irregular prime divisors of the Bernoulli numbers," *Math. Comp.*, v. 28, 1974, pp. 653–657. MR **50** #229.

14. W. JOHNSON, "Irregular primes and cyclotomic invariants," *Math. Comp.*, v. 29, 1975, pp. 113–120. MR **51** #12781.

15. W. JOHNSON, "p-adic proofs of congruences for the Bernoulli numbers," *J. Number Theory*, v. 7, 1975, pp. 251–265. MR **51** #12687.

16. T. METSÄNKYLÄ, "Über den ersten Faktor der Klassenzahl des Kreiskörpers," *Ann. Acad. Sci. Fenn. Ser. A I Math.*, No. 416, 1967, 48 pp. MR 37 #4046.

17. T. METSÄNKYLÄ, "On the cyclotomic invariants of Iwasawa," *Math. Scand.*, v. 37, 1975, pp. 61–75. MR **52** #10677.

18. N. NIELSEN, *Traité Élémentaire des Nombres de Bernoulli*, Gauthier-Villars, Paris, 1923.

19. N. E. NÖRLUND, *Vorlesungen über Differenzenrechnung*, Verlag von Julius Springer, Berlin, 1924.

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

21. I. Š. SLAVUTSKIĬ, "Generalized Bernoulli numbers that belong to different characters, and an extension of Vandiver's theorem," *Učen. Zap. Leningrad. Gos. Ped. Inst.*, v. 496, part 1, 1972, pp. 61–68. (Russian) MR **46** #7194.

22. H. S. VANDIVER, "Note on Euler number criteria for the first case of Fermat's last theorem," *Amer. J. Math.*, v. 62, 1940, pp. 79–82. MR 1, 200.

23. S. S. WAGSTAFF, JR., "The irregular primes to 125000," *Math. Comp.*, v. 32, 1978, pp. 583–591.