MATHEMATICS OF COMPUTATION
VOLUME 43, NUMBER 167
JULY 1984, PAGES 273-288

Generalized Bernoulli Numbers and m-Regular Primes

By Fred H. Hao and Charles J. Parry

Abstract. A prime p is defined to be m-regular if p does not divide the class number of a certain abelian number field. Several different characterizations are given for a prime to be m-regular, including a description in terms of the generalized Bernoulli numbers. A summary is given of two computations which determine the m-regularity or m-irregularity of primes p for certain values of m and p.

In an earlier article [3], we defined m-regular primes and showed under certain simple congruence conditions that the Fermat equation of exponent p has no solutions in the field $Q(\sqrt{m})$ when p is an m-regular prime. In this note we give several equivalent conditions for a prime to be m-regular. In particular, it is possible to describe m-regularity by means of the generalized Bernoulli numbers.

The following notation will be used throughout this article.

Q: the field of rational numbers.
Z: ring of rational integers.
m: a square-free integer, $m \neq 1$.
p: an odd prime.
ζ: a primitive pth root of unity.
$k = Q(\sqrt{m})$: quadratic number field.
$L = Q(\zeta + \zeta^{-1})$.
$K = Q(\zeta, \sqrt{m})$.
K_1: the maximal real subfield of K.
$K_3 = Q(\zeta)$: the pth cyclotomic field.
K_2: the totally imaginary quadratic extension of L contained in K with $K_2 \neq K_3$.
$h(\ )$: the class number of the field ( ).
$(\hat{\ })$: the character group of the field ( ).
χ: a character in $\hat{K}$.
$f(\chi)$: the conductor of χ.
$d = |m|$ or $4|m|$: the conductor of k.

The prime p is defined to be m-regular if p does not divide $h(K)$. Since m may be replaced with the square-free kernel of $(-1)^{(p-1)/2} \cdot pm$, we may assume that $(m, p) = 1$.

Received January 17, 1983; revised August 4, 1983 and October 11, 1983.
1980 *Mathematics Subject Classification*. Primary 12A50, 12A35, 12A15.

Theorems 1 and 2 of Parry [6] show that a regular prime p is m-irregular if and only if $p \mid h(K_2)$ and Hasse [4, p. 12] shows that $p \mid h(K_2)$ if and only if $p \mid h^*$ where

$$h^* = Q^*\omega \prod_{\substack{\chi \in \hat{K}_2 \\ \chi(-1)=-1}} \frac{1}{2f(\chi)} \sum_{t=1}^{f(\chi)} (-\chi(t)t).$$

Here Q^* is the index of the unit group of L in the unit group of K_2 and ω is the number of roots of unity in K_2. Now Q^* is easily seen to be a power of 2 and since K_3 is not a subfield of K_2, p does not divide ω. Thus $(p, Q^*\omega) = 1$ and $p \mid h^*$ if and only if

$$\prod_{\substack{\chi \in \hat{K}_2 \\ \chi(-1)=-1}} G_\chi \equiv 0 \pmod{p}$$

as a p-adic integer where

$$G_\chi = \frac{1}{f(\chi)} \sum_{t=1}^{f(\chi)} \chi(t)t = B_{1,\chi}$$

by Iwasawa [5, p. 14] where $B_{1,\chi}$ is the first generalized Bernoulli number.

If χ_1 is the generator of $\hat{K}_3$, then $\hat{L} = \langle \chi_1^2 \rangle$. If χ_2 is a generator of $\hat{k}$, we will describe $\hat{K}_2$ in terms of χ_1 and χ_2. When $m < 0$, $K_2 = Lk$ with $L \cap k = Q$. Therefore, $\hat{K}_2 = \hat{L} \times \hat{k}$, and so

$$\hat{K}_2 = \left\{ \chi_1^{2j}\chi_2^l \,\middle|\, 0 \leqslant j \leqslant (p-3)/2, 0 \leqslant l \leqslant 1 \right\}.$$

If $m > 0$, then $K = K_3k$ with $K_3 \cap k = Q$, so $\hat{K} \simeq \hat{K}_3 \times \hat{k}$. Because $[\hat{K} : \hat{K}_2] = 2$ and $\hat{K}_1 = \hat{L} \times \hat{k}$, $\hat{K}_3 = \langle \chi_1 \rangle$, it follows that

$$\hat{K}_2 = \left\{ \chi_1^{2j}, \chi_1^{2j+1}\chi_2 \,\middle|\, 0 \leqslant j \leqslant (p-3)/2 \right\}.$$

Since χ_1 is odd and χ_2 is odd exactly when $m < 0$, the odd characters of $\hat{K}_2$ have the form $\chi_1^n\chi_2$, where $0 \leqslant n \leqslant p-2$ and n is odd or even according as m is positive or negative. Note that when $m < 0$ and $n = 0$, $f(\chi_2) = d$ and

$$G_{\chi_2} = \frac{1}{d} \sum_{t=1}^{d} \chi_2(t)t = -h(k).$$

Moreover, for $n > 0$, $f(\chi_1^n\chi_2) = pd$.

THEOREM 1. *Let p be a prime with $(p, m) = 1$ and $\chi_2(a) = (D/a)$ be the Kronecker symbol where D is the discriminant of $Q(\sqrt{m})$. Then p is m-regular if and only if*

(i) *p is regular and*

(ii) *none of the numerators B_{n+1,χ_2} is divisible by p where B_{n+1,χ_2} is the $(n+1)$st generalized Bernoulli number and $0 \leqslant n \leqslant p-2$ with n odd or even according as m is positive or negative.*

Proof. See Section 2 of Iwasawa [5] or Washington [9, pp. 30–31] for definitions and basic properties of generalized Bernoulli numbers. If p is irregular, then class field theory shows p is m-irregular. If p is regular, then the above remarks show p is m-irregular if and only if $B_{1,\chi} \equiv 0 \pmod{p}$ for some character $\chi = \chi_1^n\chi_2$ with n as described in (ii). Exercise 7.5 of Washington [9, p. 141] shows that $B_{n+1,\chi_2}/(n+1) \equiv B_{1,\chi} \pmod p$. Since $p \nmid (n+1)$, the theorem follows immediately.

COROLLARY. *Let p be an odd regular prime with $(p, m) = 1$ and $\chi = \chi_2$ be the nontrivial character of the field k. Then p is m-irregular if and only if there exists a natural number n with $n = 1$ or $n \not\equiv 1 \pmod{(p-1)}$ for $n > 1$ and $n \equiv \delta_\chi \pmod 2$ such that $B_{n,\chi}/n \equiv 0 \pmod p$, where $\delta_\chi = 0$ or 1 according as m is positive or negative.*

Proof. If p is m-irregular, the above theorem shows there exists n with $1 \leqslant n \leqslant p-1$ and $n \equiv \delta_\chi \pmod 2$ such that

$$B_{n,\chi} \equiv 0 \pmod p, \quad \text{so} \quad B_{n,\chi}/n \equiv 0 \pmod p.$$

Conversely, assume $B_{n,\chi}/n \equiv 0 \pmod p$ for some natural number n satisfying our hypothesis. If $n = 1$, then as seen in the proof of the theorem,

$$G_\chi \equiv B_{1,\chi} \equiv 0 \pmod p$$

and p is m-irregular. Otherwise, $n \not\equiv 1 \pmod{(p-1)}$, and so there exists an integer l with $2 \leqslant l \leqslant p-1$ such that $n \equiv l \pmod{(p-1)}$. Theorem 5 of Carlitz [1] shows that

$$B_{n,\chi}/n \equiv B_{l,\chi}/l \pmod p,$$

and so $B_{l,\chi} \equiv 0 \pmod p$. Since $p-1$ is even, $l \equiv n \equiv \delta_\chi \pmod 2$ and our theorem shows p is m-irregular.

Remark. The hypothesis that $n \not\equiv 1 \pmod{(p-1)}$ for $n > 1$ in the above corollary can be dropped when $m > 0$ or when $m < 0$ and $\chi(p) = (D/p) = -1$.

Proof. When m is positive, δ_χ is 0 and hence n must be even. Hence $n \not\equiv 1 \pmod{(p-1)}$ is automatically satisfied.

Suppose now m is negative, Theorem 6 of Carlitz [1] shows for $n \equiv 1 \pmod{(p-1)}$ that

$$B_{n,\chi}/n \equiv (1 - \chi(p))B_{1,\chi} \pmod p.$$

Thus, if $\chi(p) = -1$, then $B_{n,\chi}/n \equiv 0 \pmod p$ if and only if $B_{1,\chi} \equiv 0 \pmod p$, which implies that p is m-irregular.

Let g be a primitive root modulo p chosen so that $g^{p-1} \equiv 1 \pmod{p^2}$. Moreover, let η be a primitive $(p-1)$st root of unity such that $\chi_1(g) = \eta$. The following result is easily proved using standard techniques of algebraic number theory.

LEMMA 1. *There exists a prime divisor P of p in $Q(\eta)$ such that $g \equiv \eta \pmod{P^2}$.*

Assume now that $p \nmid h(k)$. Then $p \mid \prod_{\chi \in \hat{K}_2; \chi \text{ odd}} G_\chi$ if and only if there exists n with $0 < n < p-1$ with n odd or even according as m is positive or negative and $\chi = \chi_1^n \chi_2$ such that $G_\chi \equiv 0 \pmod P$ for the prime divisor P of p in $Q(\eta)$.

LEMMA 2. *If $0 < n < p-1$, $\chi = \chi_1^n\chi_2$ and P is the prime ideal defined above, then*

$$G_\chi \equiv 0 \pmod P \quad \textit{iff} \quad \sum_{t=1}^{d-1} \chi_2(t) \sum_{u=0}^{ct-1} u^n \equiv 0 \pmod p,$$

where $cd \equiv 1 \pmod p$.

Proof. Let B_i ($i \geqslant 0$) denote the ordinary Bernoulli numbers and

$$B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}$$

denote the nth Bernoulli polynomial. Exercise 4.1 of Washington [9, p. 45] shows that

$$\sum_{u=0}^{ct-1} u^n = \left(\frac{1}{n+1}\right)\left[B_{n+1}(ct) - B_{n+1}(0)\right].$$

Since $1 < n+1 < p$, the von Staudt-Clausen Theorem shows that none of $B_0, B_1, \ldots, B_n$ has denominators divisible by p. Thus

$$B_{n+1}(ct) - B_{n+1}(0) \equiv B_{n+1}(t/d) - B_{n+1}(0) \pmod{p}.$$

Hence

$$\begin{aligned}
\sum_{t=1}^{d-1} \chi_2(t) \sum_{u=0}^{ct-1} u^n &\equiv \left(\frac{1}{n+1}\right) \sum_{t=1}^{d-1} \chi_2(t)\left[B_{n+1}(t/d) - B_{n+1}(0)\right] \pmod{p} \\
&\equiv \left(\frac{1}{n+1}\right) \sum_{t=1}^{d-1} \chi_2(t) B_{n+1}(t/d) \pmod{p} \\
&\equiv \frac{d^{-n}}{n+1} B_{n+1,\chi_2} \equiv \frac{1}{d^n} B_{1,\chi} \equiv \frac{1}{d^n} G_\chi \pmod{p}.
\end{aligned}$$

The final three congruences follow from Proposition 4.1 of Washington [9, p. 31] and arguments used in the proof of Theorem 1. Since $p \nmid d$, the lemma follows immediately.

THEOREM 2. *Let p be an odd regular prime and $\chi = \chi_2$ be the nontrivial character of the field $k = Q(\sqrt{m})$ with conductor $f = d$ where $(m, p) = 1$. Then p is m-regular if and only if*

$$\sum_{j=1}^{p} S_n(j) A_{jk} \not\equiv 0 \pmod{p}$$

for all n with $1 \leqslant n \leqslant p-1$ and $n \equiv 1 + \delta_\chi \pmod{2}$. Here

$$S_n(j) = \sum_{u=0}^{j-1} u^n \quad \textit{and} \quad A_n = \sum_{\substack{t=1 \\ t \equiv n \,(\mathrm{mod}\, p)}}^{f} \chi(t).$$

Proof. The remarks preceding Theorem 1 combined with Lemma 2 show that p is m-regular if and only if

$$p \nmid h(k) \quad \text{for } m \text{ negative}$$

and

$$\sum_{t=1}^{f} \chi(t) \sum_{u=0}^{ct-1} u^n \not\equiv 0 \pmod{p}$$

for all n with $1 \leqslant n \leqslant p-2$ and $n \equiv 1 + \delta_\chi \pmod{2}$. Here $c \equiv f^{-1} \pmod{p}$.

Recall $S_n(p) = \sum_{u=0}^{p-1} u^n \equiv 0 \pmod{p}$ if n is not divisible by $p-1$. Hence, for such n, $i \equiv j \pmod{p}$ implies

$$S_n(i) \equiv S_n(j) \pmod{p}.$$

Moreover, $t \equiv jf \pmod p$ implies $ct - 1 \equiv cjf - 1 \equiv j - 1 \pmod p$. Thus

$$\sum_{t=1}^{f} \chi(t) \sum_{u=0}^{ct-1} u^n = \sum_{j=1}^{p} \left(\sum_{\substack{t=1 \\ t \equiv jf \pmod p}}^{f} \chi(t) \sum_{u=0}^{ct-1} u^n \right)$$

$$\equiv \sum_{j=1}^{p} \left(\sum_{\substack{t=1 \\ t \equiv jf \pmod p}}^{f} \chi(t) \sum_{u=0}^{j-1} u^n \right) \equiv \sum_{j=1}^{p} S_n(j) A_{jf} \pmod p.$$

When $m < 0$, the additional condition $p \nmid h(k)$ is equivalent to

$$\frac{1}{f} \sum_{t=1}^{f} \chi(t) t \not\equiv 0 \pmod p.$$

Since

$$S_{p-1}(j) = \sum_{u=0}^{j-1} u^{p-1} \equiv j - 1 \pmod p \quad \text{and} \quad \sum_{j=1}^{p} A_{jf} = \sum_{a=1}^{f} \chi(a) = 0,$$

it follows that

$$\frac{1}{f} \sum_{t=1}^{f} \chi(t) t \equiv \sum_{j=1}^{p} (j) A_{jf} \pmod p$$

$$\equiv \sum_{j=1}^{p} (j-1) A_{jf} \equiv \sum_{j=1}^{p} S_{p-1}(j) A_{jf} \pmod p.$$

The following result is easily verified.

LEMMA 3. *For any* n, $A_{f-n} = \chi(-1) A_n$.

LEMMA 4. *If* $f = pg + i$ *with* $1 \leqslant i \leqslant p - 1$, *then*

$$A_0 = \chi(p) \sum_{t=0}^{g} \chi(t)$$

and

$$A_{p-i} = \chi(p) \sum_{t=g+1}^{2g+j} \chi(t) \quad \text{where } j = \begin{cases} 0 & \text{if } 2i < p, \\ 1 & \text{if } 2i > p. \end{cases}$$

When $2i < p$,

$$A_{p-2i} = \chi(p) \sum_{t=2g+1}^{3g+l} \chi(t), \quad \text{where } l = \begin{cases} 0 & \text{if } 3i \leqslant p, \\ 1 & \text{if } 3i > p, \end{cases}$$

and when $2i > p$,

$$A_{2p-2i} = \chi(p) \sum_{t=2g+2}^{3g+s+1} \chi(t), \quad \text{where } s = \begin{cases} 0 & \text{if } \frac{3}{2}i \leqslant p, \\ 1 & \text{if } \frac{3}{2}i > p. \end{cases}$$

Proof. For any integer n with $0 \leqslant n < p$, set

$$b = b(n, i) = \begin{cases} 0 & \text{if } n \geqslant i, \\ 1 & \text{if } n < i. \end{cases}$$

Then

$$A_n = \sum_{\substack{t=1 \\ t \equiv n \pmod p}}^{f} \chi(t) = \sum_{a=0}^{g-1+b} \chi(pa + n)$$

$$= \chi(p) \sum_{a=0}^{g-1+b} \chi(a + p^{-1}n) = \chi(p) \sum_{t=p^{-1}n}^{p^{-1}n+g-1+b} \chi(t),$$

where p^{-1} denotes $p^{-1} \pmod f$. Thus

$$A_0 = \chi(p) \sum_{t=0}^{g} \chi(t).$$

Since $i \equiv -pg \pmod f$,

$$p^{-1}(p - i) \equiv p^{-1}(p + pg) \equiv 1 + g \pmod f,$$

so it follows that

$$A_{p-i} = \chi(p) \sum_{t=g+1}^{2g+j} \chi(t).$$

If $2i < p$, then $1 \leqslant p - 2i < p$ and

$$p^{-1}(p - 2i) \equiv p^{-1}(p + 2pg) \equiv 2g + 1 \pmod f.$$

Thus

$$A_{p-2i} = \chi(p) \sum_{t=2g+1}^{3g+l} \chi(t).$$

If $2i > p$, then $1 < 2(p - i) < p$ and

$$2(p - i)p^{-1} \equiv 2(p + pg)p^{-1} \equiv 2g + 2 \pmod f.$$

Thus

$$A_{2(p-i)} = \chi(p) \sum_{t=2g+2}^{3g+s+1} \chi(t).$$

THEOREM 3. *Explicit conditions for each of the primes $p = 3, 5$ and 7 to be m-regular for $(m, p) = 1$ are*:

(a) $p = 3$ *if and only if* $A_0 \not\equiv 0 \pmod 3$.

(b) $p = 5$ *and* $m < 0$ *if and only if*

$$A_{4f}(A_0 + 3A_{4f}) \not\equiv 0 \pmod 5.$$

(c) $p = 5$ *and* $m > 0$ *if and only if*

$$(A_0 - A_{4f})(A_0 + 2A_{4f}) \not\equiv 0 \pmod 5.$$

(d) $p = 7$ *and* $m < 0$ *if and only if*

$$(A_{5f} + 3A_{6f})(A_{5f} - 2A_{6f})(A_0 - 2A_{5f} + 3A_{6f}) \not\equiv 0 \pmod 7.$$

(e) $p = 7$ *and* $m > 0$ *if and only if*

$$(A_0 - 3A_{5f} + 2A_{6f})(A_0 - A_{5f})(A_0 - 3A_{5f} + 3A_{6f}) \not\equiv 0 \pmod 7.$$

Proof. Since the proof of each of the five parts is similar, we shall prove only part (e). Lemma 3 shows that $A_0 = A_f$, $A_{2f} = A_{6f}$ and $A_{3f} = A_{5f}$, and since

$$\sum_{j=0}^{6} A_{jf} = \sum_{t=1}^{f} \chi(t) = 0,$$

then

$$A_{4f} = -2(A_0 + A_{5f} + A_{6f}).$$

Applying Theorem 2 with $n = 1$, 3 and 5 shows that 7 is m-regular if and only if

$$A_{2f} + 3A_{3f} + 6A_{4f} + 3A_{5f} + A_{6f} \not\equiv 0 \pmod 7,$$
$$A_{2f} + 2A_{3f} + A_{4f} + 2A_{5f} + A_{6f} \not\equiv 0 \pmod 7,$$
$$A_{2f} + 5A_{3f} + 3A_{4f} + 5A_{5f} + A_{6f} \not\equiv 0 \pmod 7.$$

Using the relations on the A's given above, the last three congruences reduce to the condition stated in (e).

Remarks. (1) The A's in Theorem 3 can easily be computed using Lemma 4.

(2) When $p = 3$, K is a bicyclic, biquadratic field, and the Dirichlet class number relation shows that 3 is m-regular if and only if each of the quadratic subfields has class number not divisible by 3. A result of Scholz [8] shows that the latter condition is satisfied if and only if the imaginary quadratic subfield $Q(\sqrt{m})$ or $Q(\sqrt{-3m})$ of K has class number relatively prime to 3. C. Queen [7] has shown the latter condition is equivalent to part (a) of Theorem 3 under the hypothesis that $m \equiv 1 \pmod 4$ and m is a positive prime.

For any real number x, let $[x]$ and $\{x\}$ denote the greatest integer less than or equal to x and the least integer greater than or equal to x, respectively. Define

$$S_n(x) = S_n(\{x\}) = \sum_{u=0}^{\{x\}-1} u^n.$$

THEOREM 4. *Let p be an odd regular prime and χ the nontrivial character of the field $k = Q(\sqrt{m})$ with conductor f where $(m, p) = 1$. If $p > f$, then p is m-regular if and only if*

$$\sum_{j=1}^{[(f-1)/2]} \left(S_n\left(\frac{jp}{f}\right) - E\right)\chi(j) \not\equiv 0 \pmod p$$

for all n with $1 \leqslant n \leqslant p-1$ and $n \equiv 1 + \delta_\chi \pmod 2$. Here $E = (p-1)/2$ or 0 according as $n = p - 1$ or not.

Proof. According to Theorem 2, p is m-regular if and only if

$$\sum_{j=1}^{p} S_n(j) A_{jf} \not\equiv 0 \pmod p$$

for all n with $1 \leqslant n \leqslant p-1$ and $n \equiv 1 + \delta_\chi \pmod 2$. If $jf \equiv f_j \pmod p$ with $0 \leqslant f_j < p$, then since $f < p$,

$$A_{jf} = \sum_{\substack{t=1 \\ t \equiv jf \pmod p}}^{f} \chi(t) = \begin{cases} \chi(f_j) & \text{if } f_j < f, \\ 0 & \text{if } f_j \geqslant f. \end{cases}$$

If $f_j = k$, then $j \equiv f^{-1}k \equiv k_f \pmod p$, where $0 \leqslant k_f < p$. Thus

$$\sum_{j=1}^{p} S_n(j) A_{jf} = \sum_{k=1}^{f-1} S_n(k_f)\chi(k).$$

Now if $j_k \equiv -p^{-1}k \pmod f$ with $0 < j_k < f$, then $(j_k p + k)/f$ is an integer less than p and $(j_k p + k)/f \equiv f^{-1}k \pmod p$. Thus $k_f = (j_k p + k)/f$ and so

$$\begin{aligned}\sum_{j=1}^{p} S_n(j) A_{jf} &= \sum_{k=1}^{f-1} S_n\left(\frac{j_k p + k}{f}\right)\chi(k) = \sum_{k=1}^{f-1} S_n\left(\frac{j_k p}{f}\right)\chi(k) \\ &= \sum_{j=1}^{f-1} S_n\left(\frac{jp}{f}\right)\chi(-pj) = \chi(-p)\sum_{j=1}^{f-1} S_n\left(\frac{jp}{f}\right)\chi(j) \\ &= \chi(-p)\sum_{j=1}^{[(f-1)/2]}\left[S_n\left(\frac{jp}{f}\right) + \chi(-1) S_n\left(\frac{(f-j)p}{f}\right)\right]\chi(j).\end{aligned}$$

Since $\sum_{u=1}^{p-1} u^n \equiv C \pmod p$, where $C = -1$ or 0 according as $n = p-1$ or not,

$$\begin{aligned}\chi(-1) S_n\left(\frac{(f-j)p}{f}\right) &\equiv -\chi(-1)\left(-C + \sum_{u=\{(f-j)p/f\}}^{p-1} u^n\right) \\ &\equiv -\chi(-1)\left(-C + \sum_{u=1}^{[jp/f]} (-u)^n\right) \equiv -C + \sum_{u=1}^{[jp/f]} u^n \\ &\equiv -C + S_n\left(\frac{jp}{f}\right) \pmod p,\end{aligned}$$

because χ and n have opposite parity. Hence

$$\sum_{j=1}^{p} S_n(j) A_{jf} \equiv \chi(-p) \sum_{j=1}^{[(f-1)/2]} \left(2S_n\left(\frac{jp}{f}\right) - C\right)\chi(j) \pmod p,$$

and the desired result follows immediately from Theorem 2.

COROLLARY. *Explicit conditions for a regular prime $p > 7$ to be m-regular for $m = -1, \pm 2, -3, 5$ and -7 are*:

(a) $m = -1$:

$$\sum_{0<u<p/4} u^n \not\equiv 0 \pmod p,$$

(b) $m = 2$:

$$\sum_{p/8<u<3p/8} u^n \not\equiv 0 \pmod p,$$

(c) $m = -2$:

$$\sum_{0<u<p/8} u^n - \sum_{3p/8<u<p/2} u^n \not\equiv 0 \pmod p,$$

(d) $m = -3$:

$$\sum_{0<u<p/3} u^n \not\equiv 0 \pmod{p},$$

(e) $m = 5$:

$$\sum_{p/5<u<2p/5} u^n \not\equiv 0 \pmod{p},$$

(f) $m = -7$:

$$\sum_{0<u<p/7} u^n - \sum_{2p/7<u<3p/7} u^n \not\equiv 0 \pmod{p},$$

where $1 \leqslant n \leqslant p-2$ and n is even or odd according as m is negative or positive.

Proof. As the proof of each part is similar, we shall prove only part (f). From Theorem 4, p is -7-regular if and only if

$$\sum_{j=1}^{3}\left(S_n\left(\frac{jp}{7}\right) - E\right)\chi(j) \not\equiv 0 \pmod{p}$$

for all even n with $1 \leqslant n \leqslant p-1$. As seen in the proof of Theorem 2, the condition for $n = p-1$ is equivalent to the fact that $h(Q(\sqrt{-7})) = 1$ is not divisible by p. Thus we may assume $n < p-1$ and so $E = 0$. The above condition becomes

$$S_n\left(\frac{p}{7}\right) + S_n\left(\frac{2p}{7}\right) - S_n\left(\frac{3p}{7}\right) \not\equiv 0 \pmod{p}$$

for all even n with $1 < n < p-2$. Since

$$S_n\left(\frac{2p}{7}\right) - S_n\left(\frac{3p}{7}\right) = -\sum_{2p/7<u<3p/7} u^n,$$

the proof of part (f) is complete.

Using Fortran programs, we did two different types of calculations. First, using the results of Theorem 3, we computed all values of m with $m = n$ or $2n$ and $|n| < 10{,}000$ for which the primes $p = 3$, 5 or 7 are m-irregular. A summary of these results appears in Table 1. Next we determine which primes $p < 5025$ satisfy the hypothesis of the corollary to Theorem 4 for each $m = -3, -1, -7, -2, 5$ and 2. This computation gives exactly those primes p for which $h^* = h^*(p, m)$ is divisible by p. Since any irregular prime is, by our definition, always m-irregular, a complete list of m-irregular primes can be obtained by including those irregular primes $p < 5025$ which do not appear in Table 2. In [2], Ernvall and Metsänkylä have studied m-regular primes with $m = -1$. It is reassuring that there are no discrepancies between their table and ours.

TABLE 1: *$m = n$ or $2n$ with $|n| < 10{,}000$*

p	3	5	7
Number values m	12169	13515	14193
Number m-irregular	4474	5202	5548
Percent m-irregular	36.8	38.5	39.1

TABLE 2: *m-irregular primes* $p \leqslant 5025$

p\m -3	-1	-7	-2	5	2
23	19	29	19	17	11
47	31	47	23	19	13
53	43	53	59	41	19
67	47	59	73	61	31
103	61	73	83	67	37
113	67	83	89	73	59
139	71	109	113	107	71
197	79	113	131	127	79
199	101	137	137	131	89
241	137	139	139	137	107
257	139	149	149	139	127
263	149	157	173	149	149
271	193	173	179	151	151
281	223	181	197	163	173
317	241	191	223	167	179
331	251	193	227	191	199
337	263	223	229	239	229
347	277	233	233	251	293
353	307	263	241	281	307
401	311	281	263	293	347
409	349	307	269	313	359
419	353	313	307	331	367
421	359	317	317	347	379
457	373	349	347	349	383
467	379	353	353	383	397
491	419	359	379	389	409
521	433	373	397	401	439
547	461	379	449	409	443
577	463	383	457	439	479
601	491	401	461	443	491
617	509	421	463	449	499
631	541	463	487	457	521
643	563	467	523	499	541
661	571	479	547	503	569
673	577	499	601	547	571
677	587	503	607	557	587
683	619	521	613	569	593
691	677	541	641	601	607
809	691	547	643	617	617
811	709	563	647	641	659

TABLE 2 (*continued*)

p\m	-3	-1	-7	-2	5	2
	821	739	587	653	653	691
	859	751	593	661	659	709
	863	761	607	673	661	739
	877	769	653	677	673	761
	887	773	659	683	677	787
	919	811	661	691	683	797
	997	821	691	739	701	809
	1009	877	701	757	769	821
	1013	887	709	811	787	823
	1039	907	751	823	821	853
	1049	929	787	853	839	859
	1061	941	797	857	863	911
	1091	967	823	883	941	919
	1093	971	827	953	953	929
	1097	983	863	977	977	937
	1151	1013	877	983	1009	953
	1153	1019	911	997	1019	977
	1171	1031	919	1019	1039	983
	1187	1039	947	1031	1051	991
	1193	1049	967	1033	1063	1013
	1201	1051	977	1063	1087	1019
	1213	1069	997	1069	1093	1087
	1217	1151	1009	1087	1109	1091
	1237	1163	1031	1093	1129	1093
	1249	1187	1051	1097	1151	1097
	1283	1223	1061	1129	1181	1103
	1297	1229	1087	1151	1201	1129
	1303	1231	1097	1163	1213	1151
	1319	1277	1117	1181	1237	1187
	1409	1279	1129	1187	1249	1193
	1453	1283	1153	1213	1277	1217
	1523	1291	1171	1291	1283	1223
	1567	1307	1201	1303	1289	1229
	1579	1319	1231	1319	1291	1289
	1583	1361	1283	1327	1303	1291
	1607	1381	1409	1361	1327	1307
	1613	1399	1439	1381	1433	1321
	1621	1409	1451	1427	1447	1381
	1663	1423	1453	1429	1511	1423
	1667	1427	1459	1439	1523	1427

TABLE 2 (*continued*)

p\m -3	-1	-7	-2	5	2
1669	1429	1471	1447	1543	1433
1697	1439	1481	1451	1601	1439
1699	1447	1483	1453	1607	1453
1709	1453	1523	1489	1619	1481
1733	1523	1531	1499	1627	1483
1759	1531	1549	1511	1637	1489
1777	1559	1553	1549	1693	1493
1823	1583	1559	1567	1733	1499
1847	1601	1597	1571	1741	1559
1867	1621	1607	1579	1747	1567
1871	1637	1627	1583	1783	1571
1901	1663	1657	1601	1823	1579
1913	1693	1667	1607	1867	1607
1951	1697	1669	1609	1873	1609
1973	1723	1699	1613	1879	1637
1979	1733	1723	1619	1931	1667
1993	1759	1783	1637	1933	1669
2011	1787	1787	1657	1973	1693
2063	1801	1801	1667	1987	1697
2069	1831	1811	1669	1999	1721
2083	1867	1823	1697	2003	1759
2089	1873	1831	1699	2017	1777
2099	1877	1871	1721	2029	1783
2131	1879	1877	1753	2053	1787
2161	1889	1879	1823	2063	1823
2203	1901	1907	1861	2081	1867
2207	1907	1913	1873	2087	1873
2221	1931	1931	1907	2111	1889
2239	1933	1933	1949	2137	1931
2269	1951	1993	1979	2141	1993
2281	1987	1999	1987	2143	2003
2293	1993	2003	1997	2161	2011
2309	1997	2017	2003	2179	2053
2347	2011	2027	2011	2207	2063
2351	2039	2029	2017	2239	2087
2441	2063	2053	2039	2243	2141
2473	2069	2063	2069	2267	2143
2477	2081	2069	2081	2287	2221
2531	2083	2081	2089	2297	2239
2539	2099	2111	2111	2339	2243

TABLE 2 (*continued*)

p\m -3	-1	-7	-2	5	2
2549	2129	2203	2129	2341	2251
2557	2131	2221	2137	2351	2267
2609	2137	2237	2153	2371	2273
2621	2141	2269	2203	2381	2287
2647	2143	2281	2243	2383	2339
2663	2161	2309	2251	2423	2347
2671	2179	2377	2281	2441	2371
2693	2203	2381	2297	2467	2399
2699	2213	2383	2333	2477	2411
2707	2221	2389	2339	2503	2417
2749	2239	2393	2341	2521	2447
2767	2293	2399	2371	2531	2459
2797	2341	2423	2393	2543	2473
2803	2377	2441	2399	2551	2521
2819	2411	2473	2411	2609	2549
2833	2417	2521	2441	2617	2579
2843	2459	2531	2467	2621	2591
2851	2473	2549	2477	2663	2617
2879	2477	2579	2503	2711	2621
2903	2531	2591	2521	2713	2633
2939	2543	2609	2539	2749	2663
2963	2579	2633	2579	2753	2671
2969	2591	2647	2647	2791	2677
2971	2609	2677	2659	2819	2689
2999	2617	2687	2671	2833	2699
3011	2633	2711	2741	2837	2741
3023	2659	2731	2753	2843	2753
3041	2671	2767	2767	2851	2801
3049	2677	2777	2789	2879	2803
3061	2687	2801	2791	2897	2843
3067	2699	2861	2833	2903	2879
3083	2711	2897	2857	2927	2887
3089	*2729*	*2909*	2861	2957	2903
3121	2731	2917	2887	2969	2909
3181	2749	2927	2917	2999	2917
3217	2797	2971	2927	3011	2957
3229	2803	3001	2939	3049	2963
3251	2819	3011	2953	3061	2971
3259	2843	3019	2999	3067	3001
3301	2879	3023	3019	3083	3041

TABLE 2 (*continued*)

p\m -3	-1	-7	-2	5	2
3319	2897	3037	3037	3109	3049
3329	2917	3083	3041	3181	3061
3343	2957	3121	3119	3209	3067
3361	2963	3137	3121	3251	3167
3373	2971	3203	3191	3253	3209
3407	2999	3271	3217	3257	3217
3413	3001	3299	3221	3271	3229
3461	3061	3301	3251	3307	3253
3463	3067	3331	3253	3313	3271
3499	3079	3347	3259	3319	3301
3533	3089	3359	3271	3329	3313
3539	3119	3361	3313	3347	3343
3541	3121	3391	3323	3359	3347
3581	3137	3407	3331	3371	3361
3583	3163	3449	3343	3407	3389
3631	3167	3469	3361	3461	3391
3637	3169	3499	3391	3467	3457
3643	3187	3529	3407	3469	3469
3659	3217	3533	3433	3511	3499
3673	3257	3547	3449	3517	3511
3677	3301	3559	3511	3529	3529
3691	3313	3571	3557	3559	3533
3727	3331	3583	3559	3607	3559
3733	3343	3593	3571	3613	3581
3761	3449	3613	3581	3617	3613
3797	3467	3631	3607	3643	3623
3821	3491	3637	3623	3673	3659
3823	3517	3709	3643	3677	3671
3833	3539	3727	3659	3691	3673
3853	3541	3779	3673	3697	3677
3907	3547	3821	3719	3701	3691
3931	3571	3833	3761	3719	3697
3947	3581	3851	3767	3727	3709
3967	3623	3853	3769	3733	3727
4007	3631	3863	3779	3761	3739
4013	3671	3911	3821	3779	3767
4021	3673	3929	3851	3803	3779
4027	3677	3943	3863	3821	3793
4093	3701	3967	3881	3853	3797
4127	3727	4007	3917	3881	3821

TABLE 2 (*continued*)

p\m -3	-1	-7	-2	5	2
4153	3733	4019	3919	3889	3863
4157	3761	4021	3931	3911	3889
4219	3793	4027	3943	3917	3907
4231	3797	4057	4003	3919	3919
4259	3821	4073	4021	3943	3947
4261	3833	4091	4051	3947	3967
4297	3847	4111	4079	3967	4007
4337	3851	4129	4099	3989	4019
4357	3853	4133	4111	4013	4073
4441	3911	4159	4133	4019	4093
4447	3917	4231	4219	4027	4099
4451	3923	4241	4231	4051	4111
4481	3989	4259	4241	4093	4129
4483	4003	4261	4243	4099	4153
4493	4007	4339	4253	4153	4159
4517	4021	4349	4261	4211	4177
4519	4051	4363	4273	4241	4201
4523	4057	4373	4289	4253	4217
4547	4093	4441	4357	4283	4241
4567	4099	4447	4423	4327	4271
4583	4129	4451	4447	4337	4297
4597	4133	4463	4481	4357	4339
4643	4153	4481	4483	4373	4397
4649	4241	4493	4493	4451	4421
4651	4259	4513	4507	4457	4423
4657	4271	4517	4519	4463	4447
4813	4283	4547	4549	4481	4493
4831	4289	4583	4561	4519	4507
4903	4337	4597	4567	4523	4523
4919	4339	4621	4583	4549	4561
4969	4349	4639	4597	4643	4591
4993	4357	4663	4621	4649	4597
5003	4373	4679	4637	4651	4603
5009	4391	4783	4639	4703	4639
5021	4397	4787	4643	4723	4657
	4421	4831	4663	4789	4729
	4463	4861	4679	4793	4787
	4481	4903	4691	4861	4789
	4493	4931	4721	4871	4793
	4523	4933	4733	4903	4801

TABLE 2 (*continued*)

p\m	-3	-1	-7	-2	5	2
		4549	4943	4751	4919	4817
		4591	4993	4759	4931	4861
		4603	5003	4789	4937	4871
		4643	5011	4889	4943	4889
		4657	5023	4931	4957	4919
		4673		4951	4967	4931
		4679		4969	5009	4937
		4691		4973	5011	4967
		4703		4993		4993
		4721		5009		5021
		4729		5011		
		4733		5021		
		4789		5023		
		4799				
		4813				
		4817				
		4861				
		4871				
		4933				
		4937				
		4943				
		5009				

Department of Mathematics
Valparaiso University
Valparaiso, Indiana 46383

Department of Mathematics
Virginia Polytechnic Institute and State University
Blacksburg, Virginia 24061

1. L. CARLITZ, "Arithmetic properties of generalized Bernoulli numbers," *J. Reine Angew. Math.*, v. 202, 1959, pp. 174–182.

2. R. ERNVALL & T. METSÄNKYLÄ, "Cyclotomic invariants and *E*-irregular primes," *Math. Comp.*, v. 32, 1978, pp. 617–629.

3. F. HAO & C. PARRY, "The Fermat equation over quadratic fields," *J. Number Theory*. (To appear.)

4. H. HASSE, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.

5. K. IWASAWA, *Lectures on p-Adic L-Functions*, Princeton Univ. Press, Princeton, N. J., 1972.

6. C. PARRY, "On the class numbers of relative quadratic fields," *Math. Comp.*, v. 32, 1978, pp. 1261–1270.

7. C. QUEEN, "A note on class numbers of imaginary quadratic number fields," *Arch. Math.* (*Basel*), v. 27, 1976, pp. 295–298.

8. A. SCHOLZ, "Über die Beziehung der Klassenzahlen quadratischer Körper zueinander," *J. Reine Angew. Math.*, v. 166, 1932, pp. 201–203.

9. L. WASHINGTON, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, Heidelberg, Berlin, 1982.