MORE CONGRUENCES FOR THE COEFFICIENTS OF QUOTIENTS OF EISENSTEIN SERIES

KARL MAHLBURG

Abstract. Berndt and Yee [1] recently proved congruences for the coefficients of certain quotients of Eisenstein series. In each case, they showed that an arithmetic progression of coefficients is identically zero modulo a small power of 3 or 7. The present paper extends these results by proving that there are infinite classes of odd primes for which the set of coefficients that are zero modulo an arbitrary prime power is a set of arithmetic density one. A new family of explicit congruences modulo arbitrary powers of 2 is also found.

1. Introduction and Statement of Results

The Eisenstein series have been of interest to number theorists since the earliest work in modular forms. Before defining these series, first recall the standard s-th divisor function on positive integers,

$$\sigma_s(n) := \sum_{d|n,\ d>0} d^s.$$

We will also need the Bernoulli numbers, B_n, which are determined by the Fourier expansion

$$\sum_{n=0}^{\infty} \frac{B_n x^n}{n!} := \frac{x}{e^x - 1}.$$

Then for each positive, even integer k, the Eisenstein series E_k is defined for any complex z in the upper half plane (i.e., $z \in \mathcal{H} = \{z \mid \mathrm{Im}(z) > 0\}$) by

$$E_k(q) := 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \tag{1.1}$$

where $q = e^{2\pi i z}$ is the standard complex power series variable. For more background on divisor functions, Bernoulli numbers, and the Eisenstein series, see [3].

Ramanujan and Hardy [2] paid particular attention to studying the coefficients of the first three Eisenstein series, and their notation is adopted here:

$$\begin{aligned} P(q) &:= E_2(q) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n, \\ Q(q) &:= E_4(q) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n, \\ R(q) &:= E_6(q) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n. \end{aligned} \tag{1.2}$$

Date: February 18, 2004.

The author thanks the support of an NSF Graduate Research Fellowship.

In a recent paper, Berndt and Yee [1] proved congruences modulo small powers of 3 and 7 for seven different quotients of these Eisenstein series.

Their results are summarized in Table 1, where the first two columns define the functions $F_i(q)$ for $i = 1, \dots, 7$, whose coefficients are denoted by

$$F_i(q) =: \sum_{n=0}^{\infty} a_i(n) q^n. \tag{1.3}$$

The final two columns of the table describe the arithmetic progressions of n values for which congruences in $a_i(n)$ hold.

i	F_i	$n \equiv 2 \pmod 3$	$n \equiv 4 \pmod 8$
1	$1/P(q)$	$a_1(n) \equiv 0 \pmod{3^4}$	
2	$1/Q(q)$	$a_2(n) \equiv 0 \pmod{3^2}$	
3	$1/R(q)$	$a_3(n) \equiv 0 \pmod{3^3}$	$a_3(n) \equiv 0 \pmod{7^2}$
4	$P(q)/Q(q)$	$a_4(n) \equiv 0 \pmod{3^3}$	
5	$P(q)/R(q)$	$a_5(n) \equiv 0 \pmod{3^2}$	
6	$Q(q)/R(q)$	$a_6(n) \equiv 0 \pmod{3^3}$	
7	$P^2(q)/R(q)$	$a_7(n) \equiv 0 \pmod{3^5}$	$a_7(n) \equiv 0 \pmod 7$

Table 1. Berndt and Yee's congruences

Their method of proof relies on the fact that each of the series in (1.2) has the form

$$F(q) = 1 + M \sum_{n=1}^{\infty} a(n) q^n, \tag{1.4}$$

where M is some rational number. Setting $G(q) := 1/F(q)$ and observing that $G(q)F(q) = 1$ leads to a simple functional equation for the power series of $G(q)$, namely

$$G(q) = 1 - G(q) \left(M \sum_{n=1}^{\infty} a(n) q^n \right), \tag{1.5}$$

which when iterated gives the formula

$$\begin{aligned} G(q) &= 1 - M \sum_{n_1=1}^{\infty} a(n_1) q^{n_1} + M^2 \sum_{n_1=1}^{\infty} \sum_{n_2=1}^{\infty} a(n_1) a(n_2) q^{n_1+n_2} + \dots \\ &= 1 + \sum_{k=1}^{\infty} (-1)^k M^k \sum_{n_1,\dots,n_k=1}^{\infty} a(n_1) \cdots a(n_k) q^{n_1+\dots+n_k}. \end{aligned} \tag{1.6}$$

Note that if M is prime, then this is actually the M-adic expansion of $1/F(q)$ (see [5] for an example). In more generality, the formula in (1.4) provides expressions for $1/F(q)$ modulo powers of p for any prime p that divides M. In the specific cases examined by Berndt and Yee, the value of M is always divisible by 3 in the expansion of $1/P(q)$, $1/Q(q)$, and $1/R(q)$, and is additionally divisible by 7 in the case of $1/R(q)$. By using both new and known identities involving divisor functions, they obtained the stated congruences.

The first theorem of this paper shows that the types of congruences in Table 1 are actually quite common, as there are infinite classes of primes for which almost every coefficient is divisible by arbitrary prime powers.

Theorem 1.1. *Let the coefficients $a_i(n)$ be defined as above.*

(1) *If l is any positive integer, then the set of non-negative integers n satisfying*

$$a_1(n) \equiv 0 \pmod{3^l}$$

has arithmetic density 1.

(2) *If $i \in \{2, 4\}$, the prime p is in the set $\{3\} \cup \{s \equiv 5 \text{ or } 11 \pmod{12}\}$, and l is any positive integer, then the set of non-negative integers n satisfying*

$$a_i(n) \equiv 0 \pmod{p^l}$$

has arithmetic density 1.

(3) *If $i \in \{3, 5, 6, 7\}$, the prime p is in the set $\{3\} \cup \{s \equiv 7 \text{ or } 11 \pmod{12}\}$, and l is any positive integer, then the set of non-negative integers n satisfying*

$$a_i(n) \equiv 0 \pmod{p^l}$$

has arithmetic density 1.

Remark. In each of the cases in Theorem 1.1, there are infinitely many arithmetic progressions of coefficients that satisfy congruences as in the original work of Berndt and Yee. To find them, one merely needs to amplify the statement of Theorem 2.4 with the theory of Hecke operators. In this way, Berndt and Yee's congruences are all accounted for, along with many others.

The proof of Theorem 1.1 is postponed to Section 2, and is preceded by a review of certain properties of the coefficients of modular forms and specific congruences satisfied by the Eisenstein series.

The case of $p = 2$ was not addressed in [1], but the following theorem shows that all of the coefficients $a_i(n)$ also satisfy explicit congruences modulo arbitrary powers of 2.

Theorem 1.2. *If $1 \le i \le 7$ and l is a positive integer, then the set of non-negative integers n satisfying*

$$a_i(n) \equiv 0 \pmod{2^l}$$

has arithmetic density 1. *Furthermore, there exists some integer w such that*

$$a_i(mn') \equiv 0 \pmod{2^l}$$

whenever m is a square-free odd integer that is the product of at least $w \cdot l$ odd prime factors, with $(m, n') = 1$.

The second part of the above theorem actually implies that there are numerous specific arithmetic sequences for which congruences hold, as in the remark after Theorem 1.1. For example, we will see later how to construct many congruences such as

$$a_3(1334025n + 1155) \equiv 0 \pmod{2^4}. \tag{1.7}$$

The proof of this theorem follows from the nilpotency of the integral weight Hecke operators modulo 2, and appears in Section 3.

2. The Coefficients of Modular Forms

To begin this section, recall the basic definitions of integer weight modular forms, as found in [4] or any other standard text. Let $\Gamma = SL_2(\mathbb{Z})$ be the modular group.

Definition 2.1. A holomorphic function f on the complex upper half plane is a *modular form of weight* k if it has the following properties.

(1) $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ whenever $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

(2) f has a Fourier expansion in q of the form

$$f(z) = \sum_{n=0}^{\infty} c(n) q^n.$$

The space of modular forms of weight k is denoted by M_k, and is a complex vector space of dimension at most $\frac{k}{12} + 1$.

In the current context, the most important examples of modular forms are the Eisenstein series of (1.1). In particular, it is well known that $E_k \in M_k$ for any even $k \geq 4$.

For a holomorphic function f, let $\mathrm{ord}_z(f)$ denote the order of zero of f at z. The definitions of modular forms and holomorphicity then imply a useful result.

Lemma 2.2. *If two modular forms $f \in M_k$ and $f' \in M_{k'}$ satisfy*

$$\mathrm{ord}_z(f) \geq \mathrm{ord}_z(f')$$

for all $z \in \mathcal{H}$, then $\frac{f}{f'} \in M_{k-k'}$.

The following basic facts are useful in understanding the divisors and congruence properties of Eisenstein series. For notational convenience, let $\omega = (-1 + i\sqrt{3})/2$ be the unique cube root of unity in the upper half plane.

Lemma 2.3. *Suppose that $k \geq 2$ is even. Then the following hold:*

(1) $E_k(z) \equiv 1 \pmod{24}$ *for all k.*
(2) *If p is prime and $(p-1) \mid k$, then $E_k(z) \equiv 1 \pmod{p^{\mathrm{ord}_p(2k)+1}}$.*
(3) *If $k \geq 4$ and $k \not\equiv 0 \pmod 6$, then $E_k(\omega) = 0$. In particular, E_4 has a simple zero at ω.*
(4) *If $k \geq 4$ and $k \not\equiv 0 \pmod 4$, then $E_k(i) = 0$. In particular, E_6 has a simple zero at i.*

The proof of this Lemma follows from the definitions of modular forms and the Eisenstein series, and from classical congruences for the denominators of Bernoulli numbers (see [3], [6])

The proof of Theorem 1.1 will ultimately depend on the invocation of a powerful theorem of Serre [8], which describes the nature of the coefficients of modular forms, i.e., that almost every coefficient is divisible by any chosen integer.

Theorem 2.4 (Serre)**.** *Let $f(z)$ be a holomorphic modular form of positive integer weight k, with Fourier expansion*

$$f(z) = \sum_{n=0}^{\infty} a(n) q^n, \tag{2.1}$$

where $a(n)$ are algebraic integers in some number field. If M is a positive integer, then there exists a positive constant α such that there are $O\left(\frac{x}{log^{\alpha}x}\right)$ integers $n \leq x$ where the $a(n)$ are not divisible by M.

Thus Theorem 1.1 would be proven if each $F_i(q)$ were a modular form of positive integer weight. However, these functions are not even holomorphic, so we must use a more specialized argument. By Lemmas 2.2 and 2.3, it will follow that for the primes p specified in Theorem 1.1 and any exponent l, $F_i(q)$ is congruent modulo p^l to a modular form of positive integer weight. Serre's theorem will then apply and give the desired conclusion.

One final difficulty that must be addressed before proceeding with the proof is the fact that E_2 is not quite a modular form over Γ. Fortunately, this trouble is remedied through Serre's study of p-adic modular forms [9]. Just as $\mathbb{Q}_p$ may be understood as the inverse limit of finite field extensions of $\mathbb{Q}$, the space of p-adic modular forms is the inverse limit of spaces of modular forms, where the p-adic metric on power series is used. Here modular forms are identified by their q-expansions, and a sequence of power series converges p-adically only if the coefficients converge uniformly. For the present purposes, the following definition will suffice.

Definition 2.5. Let p be a prime number. A *p-adic modular form* is a function $f = \sum_{n\geq 0} a(n)q^n$, with coefficients $a(n) \in \mathbb{Q}_p$ for which there exists a sequence $\{f_i\}_{i\geq 1}$ of modular forms with rational coefficients that satisfy

$$\lim_{i\to\infty} f_i = f.$$

If each f_i in the above sequence has weight k_i, then the weight of f is defined as $k = \lim_{i\to\infty} k_i$. A key fact is that the value of k does not depend on the f_i, and thus the weight of a p-adic modular form is well-defined.

With these preliminaries, we may now state and employ a useful result [9].

Proposition 2.6. *For all positive, even integers k, and for any prime p, the Eisenstein series E_k is a p-adic modular form of weight k.*

This implies that modulo p^l, an Eisenstein series E_k may always be replaced by a modular form of integral weight.

The Proof of Theorem 1.1. We now present the proof of each case of the theorem.

(1) Suppose that $i = 1$, and consider the function $F_1(q) = 1/P(q)$. By Proposition 2.6, P is a 3-adic modular form of weight 2. By Definition 2.5 and the definition of uniformly convergent power series, this implies that for any positive l, there is some modular form $P_l^*(q)$ of positive weight $k \equiv 2 \pmod{3^l}$ with the property that

$$P_l^*(q) \equiv P(q) \pmod{3^l}.$$

From equation (1.2), it is clear that $P(q) \equiv 1 \pmod 3$, and thus

$$P(q)^{3^{l-1}} \equiv 1 \pmod{3^l}.$$

To complete this section of the proof, apply Theorem 2.4 to

$$\frac{1}{P(q)} \equiv \frac{1}{P(q)} \cdot (P(q))^{3^{l-1}} \equiv (P(q))^{3^{l-1}-1} \equiv (P_l^*(q))^{3^{l-1}-1} \pmod{3^l} \tag{2.2}$$

(2) Now suppose that $i \in \{2,4\}$, so that the function $F_i(q)$ has the form $G(q)/Q(q)$ for some G. First, we dispense with the case $p = 3$. Once again, equation (1.2) shows that $Q(q) \equiv 1 \pmod 3$. For any l, define $G_l^*(q) \equiv G(q) \pmod{3^l}$ so that $G_l^*(q)$ is a modular form with rational coefficients (as above, we are replacing $P(q)$ by a modular form when necessary). Then Serre's Theorem applies to

$$\frac{G(q)}{Q(q)} \equiv \frac{G_l^*(q)}{Q(q)} \cdot (Q(q))^{3^{l-1}} \equiv G_l^*(q) \cdot (Q(q))^{3^{l-1}-1} \pmod{3^l}, \tag{2.3}$$

The remaining cases are when $p \equiv 5$ or $11 \pmod{12}$. As before, define a modular form $G_l^*(q) \equiv G(q) \pmod{p^l}$ for every l. By Lemma 2.3,

$$E_{(p-1)p^{l-1}}(q) \equiv 1 \pmod{p^l}, \tag{2.4}$$

and therefore

$$\frac{G(q)}{Q(q)} \equiv \frac{G_l^*(q)}{Q(q)} \cdot E_{(p-1)p^{l-1}}(q) \equiv G_l^*(q) \cdot \frac{E_{(p-1)p^{l-1}}(q)}{Q(q)} \pmod{p^l}. \tag{2.5}$$

A simple calculation shows that

$$(p-1)p^{l-1} \equiv \begin{cases} 4 \cdot 5^{l-1} \pmod{12} & \text{if } \quad p \equiv 5 \pmod{12} \\ 10 \cdot (-1)^{l-1} \pmod{12} & \text{if } \quad p \equiv 11 \pmod{12}. \end{cases}$$

In both cases, $(p-1)p^{l-1} \not\equiv 0 \pmod 6$, and therefore by Lemmas 2.2 and 2.3, we conclude that $E_{(p-1)p^{l-1}}/Q$ is a modular form of weight $(p-1)p^{l-1} - 4$. This is a positive value unless $p = 5$ and $l = 1$, but in this case the quotient becomes $E_4/Q = 1$, and the congruences in the statement of the Theorem hold trivially.

(3) Finally, consider the cases where $i \in \{3,5,6,7\}$. Here the functions $F_i(q)$ all have the form $G(q)/R(q)$, and as $R(q) \equiv 1 \pmod 3$, an equation similar to (2.3) holds, which proves the Theorem for $p = 3$.

Now suppose that $p \equiv 7$ or $11 \pmod{12}$. Define once more a modular form $G_l^*(q) \equiv G(q) \pmod{p^l}$ for every l, so that a direct analog to equation (2.5) holds. In order to apply Serre's Theorem, it must be verified that $E_{(p-1)p^{l-1}}/R$ is a modular form of integer weight. We have that

$$(p-1)p^{l-1} \equiv \begin{cases} 6 \cdot 7^{l-1} \pmod{12} & \text{if } \quad p \equiv 7 \pmod{12} \\ 10 \cdot (-1)^{l-1} \pmod{12} & \text{if } \quad p \equiv 11 \pmod{12}, \end{cases}$$

and in either case, $(p-1)p^{l-1} \not\equiv 0 \pmod 4$. Lemmas 2.2 and 2.3 again imply that $E_{(p-1)p^{l-1}}/R$ is a modular form of positive weight, with a single exception when $p = 7$ and $l = 1$, which is the trivial case $E_6/R = 1$.

□

3. The Case $p = 2$

In this section, the integral weight Hecke operators are defined, and then their behavior modulo 2 is used to prove Theorem 1.2. To begin, we review the operators (as in [6]).

Definition 3.1. If $f(q) = \sum_{n=0}^{\infty} a(n)q^n \in M_k$, then for any prime p define the p-th Hecke operator by

$$f(q) \mid T(p) := \sum_{n=0}^{\infty} \left(a(pn) + p^{k-1} a\left(\frac{n}{p}\right)\right) q^n. \tag{3.1}$$

Furthermore, it is known [6] that the Hecke operators preserve spaces of modular forms, so that $f(q) \mid T(p) \in M_k$.

Following conjectures of Serre, Tate proved [10] that the action of the Hecke operators is locally nilpotent modulo 2. In other words, if $f \in M_k$, there exists an $w \leq \dim M_k \leq \frac{k}{12} + 1$ such that for any collection of distinct odd primes $p_1, \ldots, p_w$,

$$f \mid T(p_1) \mid \cdots \mid T(p_w) \equiv 0 \pmod 2.$$

Combined with (3.1), this leads to the following fact.

Lemma 3.2. *If $f = \sum_{n=0}^{\infty} a(n) q^n$ is a modular form of integral weight, and $p_1, \ldots, p_w$ are distinct odd primes such that*

$$f \mid T(p_1) \mid \cdots \mid T(p_w) \equiv 0 \pmod 2,$$

then $a(np_1 \cdots p_w) \equiv 0 \pmod 2$ for any n that is coprime to $p_1 p_2 \cdots p_w$.

Proof. By induction on Definition 3.1 (as in [6]), we obtain

$$f(q) \mid T(p_1) \mid \cdots \mid T(p_w) \equiv \sum_{n=0}^{\infty} q^n \sum_{d \mid m} a\left(\frac{nm}{d^2}\right) \pmod 2, \tag{3.2}$$

where $m = p_1 \cdots p_w$. The conclusion follows, as $a(nm)$ is the only non-zero term in the coefficient of q^n whenever n is coprime to m. □

The Proof of Theorem 1.2. For any i, the series $F_i(q)$ has the form $F(q)/G(q)$, and we are interested in the coefficients modulo 2^l for some exponent l. By the discussion of p-adic modular forms in Section 2, both F and G may be replaced by integer weight modular forms $F_l^*(q) \equiv F(q) \pmod{2^l}$ and $G_l^*(q) \equiv G(q) \pmod{2^l}$. Also, $G(q) \equiv 1 \pmod 8$ in all cases by (1.2), and hence we may write

$$\frac{F(q)}{G(q)} \equiv \frac{F(q)}{G(q)} \cdot (G(q))^{2^{l-3}} \equiv F_l^*(q) \cdot (G_l^*(q))^{2^{l-3}-1} \pmod{2^l}, \tag{3.3}$$

where the final term is a modular form of integral weight k for some k. This modular form is denoted by

$$H_0(q) := \sum_{n=0}^{\infty} b(n) q^n = F_l^*(q) G_l^*(q)^{2^{l-3}-1}. \tag{3.4}$$

Theorem 2.4 then immediately implies the desired density result.

To prove the specific congruence claims, observe that by the earlier discussion, H_0 has some degree of nilpotency that is bounded by $w = \left[\frac{k}{12}\right] + 1$, which also bounds the degree of nilpotency of the image of H_0 under any Hecke operator. Let $p_1, \ldots, p_w$ be distinct odd primes, and define

$$H_1'(q) := H_0(q) \mid T(p_1) \mid \cdots \mid T(p_w). \tag{3.5}$$

By the definition of nilpotency, $H_1'(q) \equiv 0 \pmod 2$, so we may set $H_1(q) := H_1'(q)/2$, which is again a modular form of weight k with integer coefficients.

Now iterate the above process to construct $H_i(q)$ for each $1 \leq i \leq l-1$. For each i, choose primes $p_{wi+1}, \ldots, p_{w(i+1)}$ that are coprime to $p_1, \ldots, p_{wi}$, and then define

$$H_{i+1}(q) := \frac{1}{2}\Big[H_i(q) \mid T(p_{wi+1}) \mid \cdots \mid T(p_{w(i+1)})\Big]. \tag{3.6}$$

The end result of this is the function $H_l(q)$, which is a modular form with integer coefficients. Expanding (3.5) and (3.6), this means that

$$2H_l(q) = \frac{1}{2^{l-1}}\Big[H_0(q) \mid T(p_1) \mid \cdots \mid T(p_{wl})\Big] \equiv 0 \pmod 2. \tag{3.7}$$

By Lemma 3.2, we conclude that

$$\frac{b(n)}{2^{l-1}} \equiv 0 \pmod 2$$

for any n that is coprime to $p_1 \cdots p_{wl}$, which completes the proof, as the above arguments hold for every set of distinct primes.

□

It bears noting that in the cases $i = 2, 3, 6$, neither $F(q)$ nor $G(q)$ are equal to $P(q)$, and thus $F_l^*(q) = F(q)$ and $G_l^*(q) = G(q)$. We can thus calculate the weight of $H_0(q)$ explicitly to obtain bounds on the weights of the modular forms in (3.3), which in turn gives bounds on the nilpotency degree w in the statement of Theorem 1.2.

For example, if $i = 3$, then $F_3(q) = 1/R(q)$ and we have

$$H_0(q) = \frac{1}{R(q)} \equiv \frac{1}{R(q)} \cdot (R(q))^{2^{l-3}} \equiv (R(q))^{2^{l-3}-1} \pmod{2^l}.$$

This has weight $6(2^{l-3} - 1) = 12 \cdot 2^{l-4} - 6$, and thus the nilpotency degree w is at most 2^{l-4}. Let m be the product of the first $l \cdot 2^{l-4}$ primes; then since $mn + 1$ is prime to m for any integer n,

$$a_3(m^2 n + m) \equiv 0 \pmod{2^l}. \tag{3.8}$$

In particular, when $l = 4$ and 5, then m is the product of the first 4 and 10 primes, respectively, and (3.8) becomes

$$a_3\left((3 \cdot 5 \cdot 7 \cdot 11)^2 n + 3 \cdot 5 \cdot 7 \cdot 11\right) \equiv 0 \pmod{2^4}$$
$$a_3\left((3 \cdot 5 \cdots 31)^2 n + (3 \cdot 5 \cdots 31)\right) \equiv 0 \pmod{2^5}.$$

This verifies (1.7).

4. Concluding Remarks

In this paper, simple congruence and divisor properties of modular forms were used to prove congruences for quotients of Eisenstein series. We found infinite classes of primes for which congruences hold modulo arbitrary powers, and used the nilpotency of the Hecke operators modulo 2 to obtain specific congruences. Furthermore, the proofs in Sections 2 and 3 suggest that there are no such pervasive congruences for any other moduli, for Lemma 2.3 completely characterizes the Eisenstein series modulo prime powers (as shown by Serre [7]).

It should also be remarked that the techniques of this paper are not limited to quotients where the denominator has the form of equation (1.4). For example, consider the modular j-function, $j(z) = q^{-1} + 744 + 196884q + \ldots$, which is clearly not of this form [4]. Nonetheless, the coefficients of $1/j(z)$ can still be shown to satisfy all of the properties stated in Theorem 1.1, part (2), as we can write

$$\frac{1}{j(z)} = \frac{(Q(q))^3 - (R(q))^2}{1728(Q(q))^3} \equiv \frac{(Q(q))^3 - (R(q))^2}{1728(Q(q))^3} \cdot (E_{(p-1)p^l}(q))^3 \pmod{p^l}.$$

The arguments of section 2 show that the appropriate holomorphicity and modularity conditions are met, so the asserted congruences hold.

References

[1] Berndt, B., and Yee, A., *Congruences for the coefficients of quotients of Eisenstein series*, Acta Arithmetica **104** (2002) 297–308.

[2] Hardy, G., *Ramanujan*, Cambridge University Press, London, 1940.

[3] Ireland, K., and Rosen, M., *A Classical introduction to modern number theory*, Graduate Texts in Mathematics 84, Springer-Verlag, New York, 1990.

[4] Koblitz, N., *Introduction to elliptic curves and modular forms*, Springer-Verlag, New York, 1984.

[5] Mahlburg, K., *The overpartition function modulo small powers of 2*, to appear in Discrete Mathematics.

[6] Ono, K., *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS Regional Conference Series in Mathematics 102, American Mathematical Society, 2004.

[7] Serre, J.-P., *Congruences et formes modulaires* , Séminaire Bourbaki Exp. No. 416 (1971/1972), pp. 319–338. Lecture Notes in Math. 317, Springer, Berlin, 1973.

[8] Serre, J.-P., *Divisibilité des coefficients des formes modulaires de poids entier*, C.R. Acad. Sci. Paris (A) **279** (1974), 679–82.

[9] Serre, J.-P., *Formes modulaires et fonctions zêta p-adiques*, Springer Lect. Notes **350** (1973), 191-268.

[10] Tate, J., *The non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside 2*, Arithmetic Geometry (Tempe, Az., 1993), Contemp. Math. **174**, Amer. Math. Soc., Providence, RI., (1994), 153-156.

University of Wisconsin-Madison
E-mail address: mahlburg@math.wisc.edu