Journal of Combinatorial Theory, Series A **92**, 138–157 (2000)
doi:10.1006/jcta.2000.3057, available online at http://www.idealibrary.com on IDEAL®

The 2-Adic Behavior of the Number of Partitions into Distinct Parts

Ken Ono[1]

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802; and Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail: ono@math.psu.edu, ono@math.wisc.edu

and

David Penniston

Pennsylvania 16802
E-mail: dkp@math.psu.edu

Communicated by George Andrews

Received November 3, 1999

Let $Q(n)$ denote the number of partitions of an integer n into distinct parts. For positive integers j, the first author and B. Gordon proved that $Q(n)$ is a multiple of 2^j for every non-negative integer n outside a set with density zero. Here we show that if $i \not\equiv 0 \pmod{2^j}$, then

$$\#\{0 \leqslant n \leqslant X : Q(n) \equiv i \pmod{2^j}\} \gg_j \sqrt{X}/\log X.$$

In particular, $Q(n)$ lies in every residue class modulo 2^j infinitely often. In addition, we examine the behavior of $Q(n) \pmod 8$ in detail, and we obtain a simple "closed formula" using the arithmetic of the ring $\mathbb{Z}[\sqrt{-6}]$. © 2000 Academic Press

1. INTRODUCTION AND STATEMENT OF RESULTS

A *partition* of a non-negative integer n is any non-increasing sequence of positive integers whose sum is n. In this paper we examine $Q(n)$, the

[1] The first author is supported by an NSF Early Career Award, an Alfred P. Sloan Foundation Research Fellowship, and a David and Lucile Packard Foundation Fellowship.

0097-3165/00 $35.00

number of partitions of n into distinct parts. The generating function for $Q(n)$ is given by the infinite product

$$\sum_{n=0}^{\infty} Q(n)\, q^n := \prod_{n=1}^{\infty} (1+q^n) = 1+q+q^2+2q^3+2q^4+3q^5+4q^6+5q^7+\cdots. \tag{1.1}$$

In some recent papers, Alladi [A1, A2, A3] has studied the 2-adic behavior of $Q(n)$ using combinatorial methods. In particular, Alladi has obtained the following striking formula for $Q(n)$;

$$Q(n) = \sum_k g_3(n, k)\, 2^k,$$

where $g_3(n, k) := \sum_v g_3(n; v, k)$ and $g_3(n; v, k)$ denotes the number of partitions of n into v parts of the form

$$n = b_1 + \cdots + b_v$$

with minimal difference three with the additional property that there are precisely k gaps $b_\ell - b_{\ell+1} \geqslant 4$. (Note. The convention is made that $b_{v+1} = -1$.) Alladi examines the residue of $Q(n) \pmod{2^j}$ for small j by studying the combinatorics associated to his $g_3(n, k)$ functions.

Here we study the behavior of $Q(n)$ from a "modular" perspective modulo every power of 2. In particular, we employ certain facts about modular forms with complex multiplication, and the general theory of modular Galois representations to study $Q(n)$. Before proceeding, we point out an important preprint by Lovejoy [Lo] regarding the behavior of $Q(n)$ modulo odd primes p. His results clearly indicate that $Q(n)$ behaves very differently modulo odd primes p. In particular, he provides overwhelming evidence that Theorem 1 below is not true for any prime other than $p=2$.

We begin with an elementary fact. By Euler's Pentagonal Number Theorem [An, Cor. 1.7], it is easy to see that

$$\sum_{n=0}^{\infty} Q(n)\, q^n = \prod_{n=1}^{\infty} (1+q^n) \equiv \prod_{n=1}^{\infty} (1-q^n) \equiv \sum_{k=-\infty}^{\infty} q^{(3k^2+k)/2} \pmod{2}.$$

In particular, we have that

$$Q(n) \equiv \begin{cases} 1 \pmod{2} & \text{if } \; n = \dfrac{3k^2+k}{2} \text{ for some integer } k, \\ 0 \pmod{2} & \text{otherwise,} \end{cases}$$

and so it is simple to see that

$$\#\{0 \leqslant n \leqslant X : Q(n) \equiv 1 \pmod 2\} \sim \sqrt{\frac{8X}{3}}. \tag{1.2}$$

Obviously, $Q(n)$ is "almost always" even. It turns out that this simple observation is the first case of a much more general phenomenon. In a recent paper, the first author and Gordon proved the following theorem [G-O, Thm. 1]:

THEOREM 1 (Gordon–Ono). *If j is a positive integer, then*

$$Q(n) \equiv 0 \pmod{2^j}$$

for a subset of non-negative integers n with arithmetic density one.

In view of Theorem 1, it is natural to consider the following question.

QUESTION. *If j is a positive integer and $i \not\equiv 0 \pmod{2^j}$, are there infinitely many integers n for which*

$$Q(n) \equiv i \pmod{2^j}?$$

Using an observation due to Serre on the behavior of modular forms modulo m, we solve this question by proving the following general result.

THEOREM 2. *If j is a positive integer and $1 \leqslant i \leqslant 2^j - 1$, then*

$$\#\{0 \leqslant n \leqslant X : Q(n) \equiv i \pmod{2^j}\} \gg_{i,j} \sqrt{X}/\log X.$$

In view of (1.2), it is clear that it would be difficult to improve on Theorem 2 for odd i. However, for even i one can typically make a substantial improvement.

THEOREM 3. *If j is a positive integer and $2 \leqslant i < 2^j$ is an even integer for which there is a positive integer n such that*

(i) $24n + 1$ *is square-free and*

(ii) $Q(n) \equiv i \pmod{2^j}$,

then

$$\#\{0 \leqslant n \leqslant X : Q(n) \equiv i \pmod{2^j}\} \gg_{i,j} X/\log X.$$

Since almost every $Q(n)$ is a multiple of 2^j, it is clear that one cannot substantially improve the estimate in Theorem 3.

EXAMPLE. Since $Q(n)$ attains the values $2, 4, 6, 8, 10$, and 12 with positive integers n with $24n+1$ square-free, Theorem 3 implies that if $i \in \{2, 4, 6, 8, 10, 12\}$ and j is any positive integer, then

$$\#\{0 \leqslant n \leqslant X : Q(n) \equiv i \pmod{2^j}\} \gg_{i,j} X/\log X.$$

An examination of the proof of Theorem 3 illustrates, for every positive integer j, that there is indeed a formula for $Q(n) \pmod{2^j}$. In general, these formulae are finite linear combinations of multiplicative functions arising from certain explicit 2-adic Galois representations.

It seems that the last palatable formula occurs with modulus 8. Before we state this formula, we need to define an auxilary character χ. Let $K := \mathbb{Q}(\sqrt{-6})$ and let $\mathscr{F}$ be the ideal in $\mathcal{O}_K$ given by

$$\mathscr{F} := (12, 4\sqrt{-6}). \tag{1.3}$$

It turns out that $(\mathcal{O}_K/\mathscr{F})^*$ has order 16 and is generated by the residue classes 5, 7, and $\beta := 1 + \sqrt{-6}$ (which have orders 2, 2, and 4, respectively). Define the character χ on $(\mathcal{O}_K/\mathscr{F})^*$ by

$$\chi(5) = -1, \qquad \chi(7) = 1, \qquad \text{and} \qquad \chi(\beta) = i. \tag{1.4}$$

Throughout this paper p shall denote a prime.

THEOREM 4. *If n is non-negative, then let N and M be the unique positive integers for which*

$$24n + 1 = N^2 M$$

with M squarefree. Moreover, define integers $\gamma, \delta_5, \delta_{11}, \delta_{13}, \delta_{17}$ and δ_{19} by

$$\gamma := \prod_{p \nmid M \text{ and } p \equiv 1 \pmod{24}} (2\,\mathrm{ord}_p(N) + 1),$$

$$\delta_i := \begin{cases} \#\{p \equiv 5 \pmod{24} : \mathrm{ord}_p(N) \equiv 2, 3 \pmod 4 \text{ and } p \nmid M\} & \text{if } \quad i = 5, \\ \#\{p \equiv i \pmod{24} : \mathrm{ord}_p(N) \text{ is odd and } p \nmid M\} & \text{otherwise.} \end{cases}$$

With these quantities, define the integer ε by

$$\varepsilon := \gamma 5^{\delta_5} 3^{\delta_{11}} 5^{\delta_{13}} 7^{\delta_{17}} 3^{\delta_{19}}.$$

The residue of $Q(n) \pmod 8$ is determined by the following rules.

(1) *If $M = 1$, then $Q(n) \equiv \varepsilon \pmod 8$.*

(2) *Suppose that* $M=p$ *is prime, and* $\operatorname{ord}_p(24n+1)\equiv 1, 3$ or $5 \pmod 8$. *If* u *and* v *are integers for which* $u^2+6v^2=p$, *then*

$$Q(n)\equiv \varepsilon u\cdot(\operatorname{ord}_p(24n+1)+1)\,\chi(u+v\sqrt{-6}) \pmod 8.$$

(3) *Suppose that* $M=p_1p_2$ *where* $p_1\equiv p_2\equiv i \pmod{24}$ *are distinct primes with* $i\in\{1,5\}$ *and* $\operatorname{ord}_{p_1}(24n+1)\equiv \operatorname{ord}_{p_2}(24n+1)\equiv 1 \pmod 4$. *Then*

$$Q(n)\equiv 4 \pmod 8.$$

(4) *In all other cases we have that*

$$Q(n)\equiv 0 \pmod 8.$$

Corollary 5. *If* n *is non-negative integer, then let* N *and* M *be the unique positive integers for which*

$$24n+1=N^2M$$

with M *squarefree. Then the following are true*:

(1) *If* $M=1$, *then* $Q(n)$ *is odd.*

(2) *If* $M=p$ *is prime and* $\operatorname{ord}_p(24n+1)\equiv 1 \pmod 4$, *then* $Q(n)\equiv 2 \pmod 4$.

(3) *If* $M=p$ *is prime and* $\operatorname{ord}_p(24n+1)\equiv 3 \pmod 8$, *then* $Q(n)\equiv 4 \pmod 8$.

(4) *If* $M=p_1p_2$ *where* $p_1\equiv p_2\equiv i \pmod{24}$ *are distinct primes with* $i\in\{1,5\}$ *and* $\operatorname{ord}_{p_1}(24n+1)\equiv \operatorname{ord}_{p_2}(24n+1)\equiv 1 \pmod 4$, *then*

$$Q(n)\equiv 4 \pmod 8.$$

(5) *In all other cases we have that*

$$Q(n)\equiv 0 \pmod 8.$$

In Section 2 we prove Theorems 2 and 3, and in Section 3 we obtain Theorem 4 using the arithmetic of the ring $\mathbb{Z}[\sqrt{-6}]$.

2. PRELIMINARIES AND THE PROOFS OF THEOREMS 2 AND 3

As usual, let $\eta(z)$ denote Dedekind's eta-function, given by the infinite product

$$\eta(z):=q^{1/24}\prod_{n=1}^{\infty}(1-q^n).$$

(Note. $q := e^{2\pi i z}$ throughout.) We shall assume that the reader is familiar with basic facts from the theory of modular forms (see [K, M]).

Proposition 6. *If j is a positive integer, then*

$$\left(\frac{\eta^2(24z)}{\eta(48z)}\right)^{2^{j-1}} \equiv 1 \pmod{2^j}.$$

Proof. Since $(1-X)^2 \equiv 1 - X^2 \pmod 2$, it is easy to see that

$$\frac{\eta^2(24z)}{\eta(48z)} = \prod_{n=1}^{\infty} \frac{(1-q^{24n})^2}{(1-q^{48n})} \equiv 1 \pmod 2.$$

Therefore

$$\frac{\eta^2(24z)}{\eta(48z)} = 1 + 2 \sum_{n=1}^{\infty} a(n)\, q^n = 1 + 2g(z),$$

where the coefficients $a(n)$ are integers. It is easy to see that

$$\left(\frac{\eta^2(24z)}{\eta(48z)}\right)^2 = \left[1 + 2 \sum_{n=1}^{\infty} a(n)\, q^n\right]^2 = [1 + 2g(z)]^2$$
$$= 1 + 4g(z) + 4g^2(z) \equiv 1 \pmod 4.$$

The claim now follows immediately by induction. ▮

Using (1.1), it is easy to see that

$$\sum_{n=0}^{\infty} Q(n)\, q^{24n+1} = \frac{\eta(48z)}{\eta(24z)}. \tag{2.1}$$

This function is a modular function with respect to the congruence subgroup $\Gamma_0(1152)$. Although the distribution of the Fourier coefficients of modular functions modulo m is typically difficult to determine, it turns out that these coefficients modulo powers of 2 are determined by the coefficients of integer weight cusp forms, and so are determined by Galois representations. This follows from the next result, which is also proved in [G-O].

Theorem 7. *Let $j \geqslant 3$ be a positive integer. Then*

$$F_j(z) = \sum_{n=1}^{\infty} a_j(n)\, q^n := \frac{\eta(48z)}{\eta(24z)} \cdot \left(\frac{\eta^2(24z)}{\eta(48z)}\right)^{2^{j-1}}$$

is a cusp form in the space $S_{2^j-2}(\Gamma_0(1152), \chi_2)$, *and it satisfies the following congruence*:

$$F_j(z) = \sum_{n=1}^{\infty} a_j(n)\, q^n \equiv \sum_{n=0}^{\infty} Q(n)\, q^{24n+1} \pmod{2^j}.$$

(*Note. Here* χ_2 *denotes the Kronecker character for the quadratic field* $\mathbb{Q}(\sqrt{2})$.)

Proof. That the function $F_j(z)$ satisfies the desired congruence follows immediately from Proposition 6. It suffices to prove that $F_j(z)$ is a cusp form with respect to the congruence subgroup $\Gamma_0(1152)$ with Nebentypus character χ_2.

Let us briefly recall certain facts about eta-products of the form

$$f(z) := \prod_{\delta \mid N} \eta^{r(\delta)}(\delta z), \tag{2.2}$$

which may be found in [Bi, L]. If N is a positive integer for which

(i) $\sum_{\delta \mid N} \delta r(\delta) \equiv 0 \pmod{24}$ and
(ii) $\sum_{\delta \mid N} \frac{N r(\delta)}{\delta} \equiv 0 \pmod{24}$;

then

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z)$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, where the weight k and Nebentypus character χ are given by

$$k := \frac{1}{2} \sum_{\delta \mid N} r(\delta),$$

$$\chi(d) := \left(\frac{(-1)^k D}{d}\right),$$

with $D := \prod_{\delta \mid N} \delta^{r(\delta)}$. Using these facts, it is simple to deduce that $F_j(z)$ satisfies the desired transformation properties.

Since the eta-function is non-zero on the upper half of the complex plane, the zeros and poles of $F_j(z)$ are supported at the cusps. However, the order of an eta-product $f(z)$ of the form (2.2) at a cusp c/d with $d \mid N$ is given by the formula

$$\frac{N}{24 d (d, N/d)} \sum_{\delta \mid N} \frac{(d, \delta)^2 r(\delta)}{\delta}.$$

A simple calculation verifies that these orders are always positive for $F_j(z)$, and so $F_j(z)$ is a cusp form. ▮

Remarks. The function $F_j(z)$ is also a cusp form for $j=1$ and 2. If $j=1$, then $F_j(z)=\eta(24z)$, a weight 1/2 cusp form, and for $j=2$, $F_j(z)$ is the weight 1 form $\eta^3(24z)/\eta(48z)$ with character χ_{-2}.

Proof of Theorem 2. Suppose that $F(z)=\sum_{n=1}^{\infty} a(n)\, q^n$ is an integer weight cusp form with coefficients in $\mathbb{Z}$. If m is a fixed positive integer, then Serre [S, 6.4] proved that there is a set of primes, say S_m, of positive density with the property that

$$a(np^r) \equiv (r+1)\, a(n) \pmod{m}$$

whenever $p \in S_m$, r is a positive integer, and n is coprime to p.

Therefore, for each $j \geqslant 3$ there is a set of primes $\mathfrak{S}_j$ with positive density for which

$$a_j(np^r) \equiv (r+1)\, a_j(n) \pmod{2^j} \tag{2.3}$$

whenever $p \in \mathfrak{S}_j$, r is a positive integer, and n is coprime to p. Since $a_j(1) \equiv 1 \pmod{2^j}$, let p_0 be any fixed prime in $\mathfrak{S}_j$, and for each integer $1 \leqslant i \leqslant 2^j$, let n_i be the positive integer

$$n_i := p_0^i\,.$$

By Theorem 7 and (2.3) we have that

$$Q\left(\frac{n_i-1}{24}\right) \equiv a_j(n_i) \equiv i+1 \pmod{2^j}.$$

Obviously, these 2^j values cover the residue classes modulo 2^j.

By Theorem 7 and (2.3) again, for all but finitely primes $p \in \mathfrak{S}_j$ we have that

$$Q\left(\frac{n_i p^2-1}{24}\right) \equiv a_j(n_i p^2) \equiv 3(i+1) \pmod{2^j}.$$

In particular, for each such p the 2^j numbers $a_j(n_i p^2)$ cover all the residue classes modulo 2^j. Since $\mathfrak{S}_j$ contains a positive proportion of the primes, it now follows for each i that

$$\#\{0 \leqslant n \leqslant X : Q(n) \equiv i \pmod{2^j}\} \gg_{i,\,j} \pi(\sqrt{X}) \sim 2\sqrt{X}/\log X. \quad ▮$$

Now we turn to the proof of Theorem 3. If $F(z) := \sum_{n=1}^{\infty} a(n) q^n \in S_k(\Gamma_0(M), \chi)$ is a newform with Nebentypus character χ, then the Fourier coefficients $a(n)$ are algebraic integers which generate a finite extension of $\mathbb{Q}$, say L_F. If L is any finite extension of $\mathbb{Q}$ containing L_F, and if $\mathcal{O}_v$ is the completion of the ring of integers of L at any finite place v with residue characteristic, say ℓ, then by the work of Shimura, Deligne, and Serre [Sh; D; D–S] there is a continuous representation

$$\rho_{F,v}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_v)$$

for which

$$\operatorname{trace} \rho_{F,v}(\mathrm{frob}_p) = a(p) \qquad \text{for all} \quad \text{primes } p \nmid M\ell. \tag{2.4}$$

Here frob_p denotes any Frobenius element for the prime p. Theorem 3 essentially follows from the existence of these representations.

Proof of Theorem 3. Assume that $j \geqslant 3$ is an integer and that n_0 is a positive integer for which $24n_0 + 1$ is square-free and

$$Q(n_0) \equiv a_j(24n_0+1) \equiv i \qquad (\mathrm{mod}\ 2^j).$$

By Theorem 7, $F_j(z)$ is a cusp form of integer weight on $\Gamma_0(1152)$, and so by the theory of newforms has a unique decomposition as

$$F_j(z) = F_j^{\mathrm{new}}(z) + F_j^{\mathrm{old}}(z)$$

with

$$F_j^{\mathrm{new}}(z) = \sum_{k=1}^{h} \alpha_k f_k(z),$$

$$F_j^{\mathrm{old}}(z) = \sum_{r=1}^{g} \beta_r h_r(\delta_r z),$$

where each $f_k(z) = \sum_{n=1}^{\infty} b_k(n) q^n$ and $h_r(z)$ is a newform with level dividing 1152 and each $\delta_r > 1$ is an integer dividing 1152. Moreover, each α_k and β_r is algebraic. Since $a_j(24n_0+1) \equiv i \not\equiv 0 \pmod{2^j}$ and $(24n_0+1, 1152) = 1$, it must be that $F_j^{\mathrm{new}}(z)$ is not identically zero. Therefore, if $(n, 24) = 1$, then

$$a_j(n) = \sum_{k=1}^{h} \alpha_k b_k(n). \tag{2.5}$$

Let L be a finite extension of $\mathbb{Q}$ containing the Fourier coefficients of each $f_k(z)$ and the α_k's. Let w be a place of L over 2 with ramification index e. Moreover, let $\mathcal{O}_w$ be the completion of the ring of integers of L at the place w, and let λ be a uniformizer for $\mathcal{O}_w$. Let E be the positive integer defined by

$$E := \max_{1 \leqslant k \leqslant h} |\mathrm{ord}_w(\alpha_k)|, \tag{2.6}$$

and consider the Galois representations associated to the newforms $f_k(z)$, which we denote

$$\rho_{f_k, w} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_w).$$

Now let ρ be the product Galois representation defined by

$$\rho = \bigoplus_{k=1}^{h} \rho_{f_k, w} \qquad \mathrm{mod}\ \lambda^{E+ej+1}.$$

If the prime factorization of $24n_0+1$ is

$$24n_0+1 = p_1 \cdots p_r,$$

then the Chebotarev Density Theorem implies, for each $1 \leqslant d \leqslant r$, that there are $\gg X/\log X$ primes q less than X for which $\rho(\mathrm{frob}_q) = \rho(\mathrm{frob}_{p_d})$. By (2.4), for such primes we have that

$$b_k(q) \equiv b_k(p_d) \qquad \mathrm{mod}\ \lambda^{E+ej+1}$$

for all k. It follows from these observations and the multiplicativity of the Fourier coefficients of newforms that there are $\gg \frac{X}{\log X} (\log \log X)^{r-1}$ square-free integers $m = q_1 \cdots q_r$, $m < X$, such that

$$b_k(m) \equiv b_k(24n_0+1) \qquad \mathrm{mod}\ \lambda^{E+ej+1}.$$

For any such m, it follows from (2.5) and (2.6) that $a_j(m) \equiv a_j(24n_0+1)$ mod λ^{ej+1}, and so has the property that

$$a_j(m) \equiv i \qquad (\mathrm{mod}\ 2^j). \quad \blacksquare$$

3. THE PROOF OF THEOREM 4

Let K, $\mathcal{F}$, and χ be as defined in the introduction (see (1.3) and (1.4)). Denote also by χ the extension of this character to the subgroup of K^* consisting of all elements prime to $\mathcal{F}$. Now we define a Hecke character c

of exponent 1 on the group $I_K(\mathscr{F})$ of fractional ideals of K prime to $\mathscr{F}$ as follows: on principal ideals (α), set

$$c((\alpha)) = \chi(\alpha)\,\alpha. \tag{3.1}$$

There are two ways to extend this to $I_K(\mathscr{F})$ (since $\mathbb{Z}[\sqrt{-6}]$ has class number 2); we fix c once and for all by defining it to be

$$c(\mathscr{P}) = \sqrt{2} + \sqrt{-3} \tag{3.2}$$

on the nonprincipal ideal $\mathscr{P} = (5, \sqrt{-6} + 2)$.

THEOREM 8. *Let $F_3(z) = \sum_{n=1}^{\infty} a_3(n)\,q^n$ be defined as in Theorem 7, and let $\phi(z)$ be the newform with complex multiplication in $S_2(\Gamma_0(384), \chi_2)$ defined by*

$$\phi(z) = \sum_{n=1}^{\infty} b(n)\,q^n := \sum_{(\mathscr{I}, \mathscr{F})=1} c(\mathscr{I})\,q^{N(\mathscr{I})}$$
$$= q + 2\sqrt{-3}\,q^5 - 2\sqrt{6}\,q^7 - 4\sqrt{-2}\,q^{11} - 7q^{25} - 6\sqrt{-3}\,q^{29} + \cdots,$$

where the sum is over all integral ideals of $\mathcal{O}_K$ prime to $\mathscr{F}$. Then

$$a_3(n) = \begin{cases} b(n) & \text{if } \; n \equiv 1 \pmod{24}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By definition, it is easy to see that

$$b(n) \neq 0 \Rightarrow n \equiv 1, 5, 7, 11 \pmod{24}.$$

Let $\phi_1(z) = \sum_{n=1}^{\infty} b_1(n)\,q^n$ be the modular form defined by

$$\phi_1(z) = \sum_{n=1}^{\infty} b_1(n)\,q^n := \frac{1}{2} \sum_{n=1}^{\infty} \left(b(n) + \left(\frac{n}{3}\right) b(n) \right) q^n. \tag{3.3}$$

By [Ko, p. 127], it turns out that $\phi_1(z)$ is in the space $S_2(\Gamma_0(3456), \chi_2)$. Similarly, let $\phi_2(z) = \sum_{n=1}^{\infty} b_2(n)\,q^n$ be the modular form

$$\phi_2(z) = \sum_{n=1}^{\infty} b_2(n)\,q^n := \frac{1}{2} \sum_{n=1}^{\infty} (b_1(n) + \chi_{-1}(n)\,b_1(n))\,q^n. \tag{3.4}$$

By [Ko, p. 127] again, we have that $\phi_2(z)$ is in the space $S_2(\Gamma_0(55296), \chi_2)$, and by (3.3) and (3.4) has the additional property that

$$b_2(n) = \begin{cases} b(n) & \text{if } \; n \equiv 1 \pmod{24}, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, Theorem 8 is equivalent to the assertion that

$$\phi_2(z) = F_3(z).$$

This follows by checking that $a_3(n) = b_2(n)$ for all $n \leqslant 18432$ (see for instance [Mu]). ∎

In view of Theorems 7 and 8, Theorem 4 boils down to a computation of $b(n) \pmod 8$ for all $n \equiv 1 \pmod{24}$. To this end, we recall two essential properties of the $b(n)$. Since $\phi(z)$ is an eigenform of the Hecke operators, we have that

$$b(n)\, b(m) = b(nm) \qquad \text{if} \quad \gcd(n, m) = 1, \tag{3.5}$$

and

$$b(p^{k+1}) = b(p)\, b(p^k) - \chi_2(p)\, b(p^{k-1})\, p \qquad \text{if} \quad p \geqslant 5 \text{ is prime and } k \geqslant 0. \tag{3.6}$$

In view of (3.5) and (3.6), we begin by obtaining 2-adic information about $b(p)$ when p is prime. For convenience, we list all the values of χ on $(\mathcal{O}_K/\mathcal{F})^*$ (recall that $\mathcal{F} = (12, 4\sqrt{-6})$ and $(\mathcal{O}_K/\mathcal{F})^*$ is generated by the classes of 5, 7, and $\beta = 1 + \sqrt{-6}$).

Values of χ

$\chi(5^0 7^0 \beta^0) = \chi(1) = 1$	$\chi(5^1 7^0 \beta^0) = \chi(5) = -1$
$\chi(5^0 7^1 \beta^0) = \chi(7) = 1$	$\chi(5^1 7^1 \beta^0) = \chi(11) = -1$
$\chi(5^0 7^0 \beta^1) = \chi(1 + \sqrt{-6}) = i$	$\chi(5^1 7^0 \beta^1) = \chi(5 + \sqrt{-6}) = -i$
$\chi(5^0 7^1 \beta^1) = \chi(7 + 3\sqrt{-6}) = i$	$\chi(5^1 7^1 \beta^1) = \chi(11 + 3\sqrt{-6}) = -i$
$\chi(5^0 7^0 \beta^2) = \chi(7 + 2\sqrt{-6}) = -1$	$\chi(5^1 7^0 \beta^2) = \chi(11 + 2\sqrt{-6}) = 1$
$\chi(5^0 7^1 \beta^2) = \chi(1 + 2\sqrt{-6}) = -1$	$\chi(5^1 7^1 \beta^2) = \chi(5 + 2\sqrt{-6}) = 1$
$\chi(5^0 7^0 \beta^3) = \chi(7 + \sqrt{-6}) = -i$	$\chi(5^1 7^0 \beta^3) = \chi(11 + \sqrt{-6}) = i$
$\chi(5^0 7^1 \beta^3) = \chi(1 + 3\sqrt{-6}) = -i$	$\chi(5^1 7^1 \beta^3) = \chi(5 + 3\sqrt{-6}) = i$

PROPOSITION 9. *Let p be a prime.*

(1) *If $p \equiv 13, 17, 19$ or $23 \pmod{24}$, then*

$$b(p) = 0.$$

(2) *If* $p \equiv 1 \pmod{24}$ *and* $p = u^2 + 6v^2$ *where* u *and* v *are integers, then*

$$b(p) = 2\chi(u + v\sqrt{-6})\, u.$$

(3) *If* $p \equiv 7 \pmod{24}$ *and* $p = u^2 + 6v^2$ *where* u *and* v *are integers, then*

$$b(p) = 2\chi(u + v\sqrt{-6})\, v\sqrt{-6}.$$

Proof. (1) If $p \equiv 13, 17, 19$ or $23 \pmod{24}$, then $(\frac{-6}{p}) = -1$, and so p is inert in $\mathcal{O}_K$. Hence $\mathcal{O}_K$ has no ideals of norm p, and $b(p) = 0$.

(2) Suppose $p \equiv 1 \pmod{24}$. Since $p \equiv 1 \pmod{6}$, there exist integers u and v such that $p = u^2 + 6v^2$ (note that u is odd and v is even). Therefore we have the factorization

$$p\mathcal{O}_K = (u + v\sqrt{-6})(u - v\sqrt{-6}),$$

where both principal ideals have norm p. Hence

$$b(p) = \chi(u + v\sqrt{-6})(u + v\sqrt{-6}) + \chi(u - v\sqrt{-6})(u - v\sqrt{-6}).$$

Since v is even, the table of values of χ indicates that $\chi(u \pm v\sqrt{-6}) \in \{-1, 1\}$. Moreover, $\chi(u + v\sqrt{-6})\, \chi(u - v\sqrt{-6}) = \chi(p) = \chi(1) = 1$. Thus $\chi(u + v\sqrt{-6}) = \chi(u - v\sqrt{-6})$, and so $b(p) = 2\chi(u + v\sqrt{-6})\, u$.

(3) Suppose $p \equiv 7 \pmod{24}$. As in (2) there exist integers u and v with $p = u^2 + 6v^2$ (note that here u and v are both odd). Since v is odd, $\chi(u \pm v\sqrt{-6}) \in \{-i, i\}$. Also, $\chi(u + v\sqrt{-6})\, \chi(u - v\sqrt{-6}) = \chi(p) = \chi(7) = 1$. Thus $\chi(u + v\sqrt{-6}) = -\chi(u - v\sqrt{-6})$, and $b(p) = 2\chi(u + v\sqrt{-6})\, v\sqrt{-6}$. ∎

Corollary 10. *Let* p *be a prime and let* $T := \mathbb{Z}[\sqrt{6}]$.

(1) *If* $p \equiv 13, 17, 19$ *or* $23 \pmod{24}$, *then* $b(p) \equiv 0 \pmod{8}$.

(2) *If* $p \equiv 1 \pmod{24}$, *then* $b(p) \equiv 2 \pmod{4}$.

(3) *If* $p \equiv 7 \pmod{24}$, *then* $b(p) \equiv 2\sqrt{6} \pmod{4T}$.

Proof. For (2) and (3) recall that in the proof of Proposition 9, we showed that if $p = u^2 + 6v^2$, then $\chi(u + v\sqrt{-6}) \in \{-1, 1\}$ when $p \equiv 1 \pmod{24}$ and $\chi(u + v\sqrt{-6}) \in \{-i, i\}$ when $p \equiv 7 \pmod{24}$. ∎

We now consider the $b(p)$ for primes $p \equiv 5, 11 \pmod{24}$. To study these cases, we require the following result which is interesting on its own.

THEOREM 11. *Let $p \equiv 5$ or $11 \pmod{24}$ be prime. There are integers x and y for which*

$$x^2 + 24y^2 = p^2.$$

Moreover, there are integers x and y for which

$$x^2 + 96y^2 = p^2$$

if and only if $p \equiv 11 \pmod{24}$.

Proof. Since $(\frac{-6}{p}) = 1$, we have that

$$p\mathcal{O}_K = \mathcal{P}_1 \mathcal{P}_2.$$

Since $p \equiv 5 \pmod 6$, it is easy to see that p is not represented by $x^2 + 6y^2$, and so the $\mathcal{P}_i$ are not principal. Now, $\mathbb{Z}[\sqrt{-6}\,]$ has class number 2, so $\mathcal{P}_i^2$ is principal. Hence there exist nonzero integers u and v with $\mathcal{P}_1^2 = (u + v\sqrt{-6})$ and $\mathcal{P}_2^2 = (u - v\sqrt{-6})$, i.e., $p^2 = u^2 + 6v^2$. Since $p^2 \equiv 1 \pmod{24}$, v is even and $p^2 = u^2 + 24(v/2)^2$.

Let M be the ring class field of the order $\mathbb{Z}[\sqrt{-96}\,]$, which has conductor 4 in the maximal order $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}\,]$. Then $[M:K] = h(-384) = 8$, and $M = K(j(\sqrt{-96}))$. Furthermore, M contains $L = K(\sqrt{2}, \sqrt{3})$, the ring class field of $\mathbb{Z}[\sqrt{-24}\,]$. Let $\mathcal{Q}$ be a prime ideal of $\mathcal{O}_M$ above p, write $k := \mathcal{O}_M/\mathcal{Q}$ for the residue field, and let $f_p := [k : \mathbb{F}_p]$ be the residue degree (recall that this degree is independent of the choice of $\mathcal{Q}$, since $M/\mathbb{Q}$ is Galois). Denote the Artin map $[\frac{M/K}{\cdot}] : H(-384) \to \mathrm{Gal}(M/K)$.

Since $(\frac{2}{p}) = -1$ and $\sqrt{2} \in M$, we have that $2 \mid f_p$. Moreover, since $\sqrt{3}$, $\sqrt{-6} \in \mathbb{F}_{p^2}$ and M is a quadratic extension of $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{-6})$, it follows that $f_p = 2$ or 4. Furthermore,

$$p^2 \text{ is represented by } x^2 + 96y^2 \Leftrightarrow \left[\frac{M/K}{\mathcal{Q}}\right]^2 = 1 \Leftrightarrow f_p = 2. \tag{3.7}$$

Thus we must study the quadratic extension $M = L(j(\sqrt{-96}))/L$.

If $f_1(z) := \eta(z/2)/\eta(z)$ is the usual Weber function, then

$$j(\sqrt{-96}) = \left(\frac{f_1(\sqrt{-96})^{24} + 16}{f_1(\sqrt{-96})^8}\right)^3$$

(see, for example, [C, p. 257]). Write

$$(a; q)_\infty = \prod_{i=0}^{\infty} (1 - aq^i),$$

and for a positive rational number n define

$$G_n := 2^{-1/4} q_n^{-1/24} (-q_n; q_n^2)_\infty \qquad \text{and} \qquad g_n := 2^{-1/4} q_n^{-1/24} (q_n; q_n^2)_\infty,$$

where $q_n := \exp(-\pi \sqrt{n})$. By [Be, pp. 183 and 187] we have

$$f_1(\sqrt{-24}) = 2^{1/4} g_{24}, \qquad f_1(\sqrt{-96}) = 2^{1/4} g_{96},$$

as well as

$$(g_{24} G_{24})^8 \, (G_{24}^8 - g_{24}^8) = 1/4$$

and

$$g_{96} = 2^{1/4} g_{24} G_{24}.$$

Using these relations we find that

$$M = L(j(\sqrt{-96})) = L(f_1(\sqrt{-24})^{12} \sqrt{f_1(\sqrt{-24})^{24} + 64}\,).$$

Using Weber's [W, p. 722] evaluation

$$f_1(\sqrt{-24})^{24} = 2^9 (1 + \sqrt{2})^2 \, (2 + \sqrt{3})^3 \, (\sqrt{2} + \sqrt{3})^3,$$

we find that

$$M = L(\sqrt{(2+\sqrt{3})(\sqrt{2}+\sqrt{3})(8(1+\sqrt{2})^2 \, (2+\sqrt{3})^3 \, (\sqrt{2}+\sqrt{3})^3 + 1)}\,).$$

We are studying $f_p = [k : \mathbb{F}_p]$, so let us work in the residue field $k = \mathcal{O}_M / \mathcal{Q}$. We know that $\mathbb{F}_{p^2} \subset k$. We will use the fact that

$$\gamma \in \mathbb{F}_{p^2} \text{ is a square in } \mathbb{F}_{p^2} \Leftrightarrow N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\gamma) \text{ is a square in } \mathbb{F}_p.$$

First consider $2 + \sqrt{3}$. If $p \equiv 5 \pmod{24}$, then $(\frac{3}{p}) = -1$, and so

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(2 + \sqrt{3}) = (2 + \sqrt{3})(2 - \sqrt{3}) = 1.$$

If $p \equiv 11 \pmod{24}$, then $(\frac{3}{p}) = 1$, and so

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(2 + \sqrt{3}) = (2 + \sqrt{3})^2.$$

In either case, $2 + \sqrt{3}$ is a square in $\mathbb{F}_{p^2}$.

Now consider

$$\begin{aligned} \delta &:= 8(1+\sqrt{2})^2 \, (2+\sqrt{3})^3 \, (\sqrt{2}+\sqrt{3})^3 + 1 \\ &= 18873 + 13344\sqrt{2} + 10896\sqrt{3} + 7704\sqrt{6}\,. \end{aligned}$$

If $p \equiv 5 \pmod{24}$, then $(\frac{2}{p}) = (\frac{3}{p}) = -1$. Hence

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\delta) = (18873 + 13344\sqrt{2} + 10896\sqrt{3} + 7704\sqrt{6}) \times (18873 - 13344\sqrt{2} - 10896\sqrt{3} + 7704\sqrt{6}) = 6705 + 2736\sqrt{6} = (57 + 24\sqrt{6})^2.$$

If $p \equiv 11 \pmod{24}$, we similarly find that

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\delta) = 124209 + 71712\sqrt{3} = (249 + 144\sqrt{3})^2.$$

So δ is a square in $\mathbb{F}_{p^2}$ in either case.

Finally, consider $\sqrt{2} + \sqrt{3}$. If $p \equiv 5 \pmod{24}$, then as above,

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\sqrt{2} + \sqrt{3}) = -(\sqrt{2} + \sqrt{3})^2.$$

Since $\sqrt{2} + \sqrt{3} \notin \mathbb{F}_p$ and $(\frac{-1}{p}) = 1$, it follows that $\sqrt{2} + \sqrt{3}$ is not a square in $\mathbb{F}_{p^2}$. If $p \equiv 11 \pmod{24}$, then

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\sqrt{2} + \sqrt{3}) = (\sqrt{2} + \sqrt{3})(-\sqrt{2} + \sqrt{3}) = 1,$$

and therefore $\sqrt{2} + \sqrt{3}$ is a square in $\mathbb{F}_{p^2}$.

We have shown that $(2 + \sqrt{3})(\sqrt{2} + \sqrt{3})\,\delta$ is a square in $\mathbb{F}_{p^2}$ exactly when $p \equiv 11 \pmod{24}$. Thus $f_p = 2$ if and only if $p \equiv 11 \pmod{24}$. This completes the proof by (3.7). ▮

Using Theorem 11 we prove:

PROPOSITION 12. *If $p \equiv 5$ or $11 \pmod{24}$ is prime and u and v are integers for which*

$$p^2 = u^2 + 6v^2,$$

then

$$b(p)^2 = 2(\chi(u + v\sqrt{-6})\,u - p).$$

Proof. Retain the notation from the proof of Theorem 11, so we have $p\mathcal{O}_K = \mathcal{P}_1 \mathcal{P}_2$, and nonzero integers u and v such that $\mathcal{P}_1^2 = (u + v\sqrt{-6})$, $\mathcal{P}_2^2 = (u - v\sqrt{-6})$. Then $\mathcal{O}_K$ has three ideals of norm p^2, namely $\mathcal{P}_1^2$, $\mathcal{P}_2^2$ and (p). Hence

$$b(p^2) = \chi(u + v\sqrt{-6})(u + v\sqrt{-6}) + \chi(u - v\sqrt{-6})(u - v\sqrt{-6}) + \chi(p)\,p.$$

Recall that v is even, which implies (using the table of values of χ) that $\chi(u \pm v\sqrt{-6}) \in \{-1, 1\}$. Furthermore

$$\chi(u+v\sqrt{-6})\,\chi(u-v\sqrt{-6}) = \chi(p^2) = \chi(1) = 1.$$

Thus $\chi(u+v\sqrt{-6}) = \chi(u-v\sqrt{-6})$, and so

$$b(p^2) = 2\chi(u+v\sqrt{-6})\,u + \chi(p)\,p.$$

Then by (3.6),

$$\begin{aligned} b(p)^2 &= b(p^2) + \chi_2(p)\,p = 2\chi(u+v\sqrt{-6})\,u + \chi(p)\,p + \chi_2(p)\,p \\ &= 2(\chi(u+v\sqrt{-6})\,u - p). \quad \blacksquare \end{aligned}$$

Using Proposition 12 we obtain the following result.

PROPOSITION 13. *Let* $p \equiv 5, 11 \pmod{24}$ *be prime.*

(1) *If* $p \equiv 5 \pmod{24}$, *then*

$$b(p) = 2t\sqrt{-3}$$

for some integer t *coprime to* 6.

(2) *If* $p \equiv 11 \pmod{24}$, *then*

$$b(p) = 4t\sqrt{-2}$$

for some integer t *not divisible by* 3.

Proof. Retain the notation from the proof of Proposition 12. Recall that v is even. Since $6v^2 = (p-u)(p+u)$ and the greatest common divisor of $p-u$ and $p+u$ is 2, it follows that either

$$\{p-u, p+u\} = \{6r^2, s^2\} \qquad \text{with } r \text{ odd, } s \text{ even and not divisible by 3,} \tag{3.8}$$

or

$$\{p-u, p+u\} = \{3r^2, 2s^2\} \qquad \text{with } r \text{ even and } s \text{ coprime to 6.} \tag{3.9}$$

Suppose $p \equiv 5 \pmod{24}$. We claim that $u \equiv 1$or $11 \pmod{12}$. To see this, note that if $u \equiv 5 \pmod{12}$, then $p+u \equiv 10 \pmod{12}$, and if $u \equiv 7 \pmod{12}$, then $p-u \equiv 10 \pmod{12}$; but none of the numbers in the sets in (3.8) and (3.9) can be congruent to 10 modulo 12. Next, by Theorem 11, v is not divisible by 4. Combining these facts with the table of values of χ, we find that $\chi(u+v\sqrt{-6})\,u \equiv 11 \pmod{12}$, and hence $p-\chi(u+v\sqrt{-6})\,u \equiv 6 \pmod{12}$. Recalling that $\chi(u+v\sqrt{-6}) \in \{-1, 1\}$, we have that $p-\chi(u+v\sqrt{-6})\,u$ is equal to one of $p-u$, $p+u$. By inspection of (3.8) and (3.9) we conclude that $\chi(u+v\sqrt{-6})\,u-p=-6r^2$ for some r coprime to 6. Then by Proposition 12, $b(p)^2=-12r^2$ and we have our result.

Now suppose $p \equiv 11 \pmod{24}$. Again using that neither $p-u$ nor $p+u$ is congruent to 10 modulo 12, we get that $u \equiv 5$or $7 \pmod{12}$. By Theorem 11, $4 \mid v$. We find that $\chi(u+v\sqrt{-6})\,u \equiv 7 \pmod{12}$, and hence $p-\chi(u+v\sqrt{-6})\,u \equiv 4 \pmod{12}$. Recalling that $\chi(u+v\sqrt{-6}) \in \{-1, 1\}$, we have that $p-\chi(u+v\sqrt{-6})$ is equal to $p-u$ or $p+u$. Inspection of (3.8) and (3.9) gives us that $\chi(u+v\sqrt{-6})\,u-p=-s^2$, where s is even and not divisible by 3. Now we claim that $u \equiv 3$ or $5 \pmod 8$. To see this, note that if $u \equiv 1 \pmod 8$, then $\mathrm{ord}_2(6v^2)=\mathrm{ord}_2(p-u)+\mathrm{ord}_2(p+u)=3$, which is false since $4 \mid v$; by a similar argument u is not congruent to 7 modulo 8. It follows from the table of values of χ that $\chi(u+v\sqrt{-6})\,u \equiv 3 \pmod 8$. Hence $\chi(u+v\sqrt{-6})\,u-p \equiv 0 \pmod 8$, which implies that s is divisible by 4. Since $b(p)^2=-2s^2$ by Proposition 12, we have our result. ▮

By combining (3.6) with Propositions 9, 12, and 13 and Corollary 10, it is straightforward but tedious to obtain the following result.

THEOREM 14. *Let* $R=\mathbb{Z}[\sqrt{-2}]$, $S=\mathbb{Z}[\sqrt{-3}]$, $T=\mathbb{Z}[\sqrt{6}]$, *and let* $p \geqslant 5$ *be prime.*

(1) *If* $p \equiv 1 \pmod{24}$, *then*

$$b(p^k) \equiv \begin{cases} k+1 \pmod 8 & \textit{if } k \textit{ is even or } b(p) \equiv 2 \pmod 8, \\ -(k+1) \pmod 8 & \textit{otherwise.} \end{cases}$$

(2) *If* $p \equiv 5 \pmod{24}$, *then*

$$b(p^k) = \begin{cases} 1 \pmod 8 & \textit{if } k \equiv 0, 2 \pmod 8, \\ 5 \pmod 8 & \textit{if } k \equiv 4, 6 \pmod 8, \\ (k+1)\sqrt{-3} \pmod{4S} & \textit{if } k \text{ is odd.} \end{cases}$$

(3) *If* $p \equiv 7 \pmod{24}$, *then*

$$b(p^k) \equiv \begin{cases} 1 \pmod 8 & \textit{if } k \textit{ is even}, \\ (k+1)\sqrt{6} \pmod{4T} & \textit{if } k \textit{ is odd.} \end{cases}$$

(4) *If* $p \equiv 11 \pmod{24}$, *then*

$$b(p^k) \equiv \begin{cases} 3^{k/2} \pmod 8 \\ \qquad \text{if} \quad k \text{ is even}, \\ 2(k+1)\sqrt{-2} \pmod{8R} \\ \qquad \text{if} \quad k \text{ is odd and } b(p) \equiv 4\sqrt{-2} \pmod{8R}, \\ 0 \pmod{8R} \\ \qquad \text{if} \quad k \text{ is odd and } b(p) \equiv 0 \pmod{8R}. \end{cases}$$

(5) *If* $p \equiv 13 \pmod{24}$, *then*

$$b(p^k) \equiv \begin{cases} 5^{k/2} \pmod 8 & \text{if} \quad k \text{ is even}, \\ 0 \pmod 8 & \text{if} \quad k \text{ is odd}. \end{cases}$$

(6) *If* $p \equiv 17 \pmod{24}$, *then*

$$b(p^k) \equiv \begin{cases} 7^{k/2} \pmod 8 & \text{if} \quad k \text{ is even}, \\ 0 \pmod 8 & \text{if} \quad k \text{ is odd}. \end{cases}$$

(7) *If* $p \equiv 19 \pmod{24}$, *then*

$$b(p^k) \equiv \begin{cases} 3^{k/2} \pmod 8 & \text{if} \quad k \text{ is even}, \\ 0 \pmod 8 & \text{if} \quad k \text{ is odd}. \end{cases}$$

(8) *If* $p \equiv 23 \pmod{24}$, *then*

$$b(p^k) \equiv \begin{cases} 1 \pmod 8 & \text{if} \quad k \text{ is even}, \\ 0 \pmod 8 & \text{if} \quad k \text{ is odd}. \end{cases}$$

Using (3.5) and Theorems 7, 8, and 14, Theorem 4 follows immediately.

ACKNOWLEDGMENTS

The authors thank K. Alladi for sharing his reprints. The authors also thank B. Berndt and K. Williams for their valuable assistance pertaining to the material in Section 3.

REFERENCES

[A1] K. Alladi, A combinatorial correspondence related to Göllnitz' (BIG) partition theorem and applications, *Trans. Amer. Math. Soc.* **349** (1997), 2721–2735.

[A2] K. Alladi, Partition identities involving gaps and weights, *Trans. Amer. Math. Soc.* **349** (1997), 5001–5019.

[A3] K. Alladi, Weighted partition identities and applications, *in* "Analytic Number Theory, I," pp. 1–15, Progr. Math., Vol. 138, Birkhäuser, Boston, 1996.
[An] G. E. Andrews, "The Theory of Partitions," Cambridge Univ. Press, Cambridge, 1998.
[Be] B. Berndt, "Ramanujan's Notebooks Part V," Springer, New York, 1998.
[Bi] A. Biagioli, The construction of modular forms as products of transforms of the Dedekind eta-function, *Acta Arith.* **54** (1990), 273–300.
[C] D. A. Cox, "Primes of the form x^2+ny^2," Wiley, New York, 1989.
[D] P. Deligne, Formes modulaires et repŕesentations ℓ-adiques, *Sem. Bourbaki* **355** (1969).
[D-S] P. Deligne and J.-P. Serre, Formes modulaires de poids 1, *Ann. Sci. École Norm. Sup. (4)* **7** (1974).
[G-O] B. Gordon and K. Ono, Divisibility of certain partition functions by powers of primes, *Ramanujan J.* **1** (1997), 25–34.
[K] A. Knapp, "Elliptic Curves," Princeton Univ. Press, Princeton, 1992.
[Ko] N. Koblitz, "Introduction to Elliptic Curves and Modular Forms," Springer-Verlag, New York, 1984.
[L] G. Ligozat, Courbes modulaires de genre 1, *Bull. Soc. Math. France* **43** (1972), 1–80.
[Lo] J. Lovejoy, Divisibility and distribution of $Q(n)$, preprint.
[M] T. Miyake, "Modular Forms," Springer-Verlag, New York, 1989.
[Mu] M. R. Murty, Congruences between modular forms, *in* "Analytic Number Theory," pp. 309–320, London Math. Soc. Lect. Note Ser., Vol. 247, London Math. Soc., London, 1997.
[S] J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, *Enseign. Math.* **22** (1976), 227–260.
[Sh] G. Shimura, "Introduction to the Arithmetic Theory of Automorphic Functions," Iwanami Shoten/Princeton Univ. Press, Tokyo/Princeton, 1971.
[W] H. Weber, "Lehrbuch der Algebra," dritter Band, Chelsea, 1961.