

# SOME CONGRUENCES FOR PARTITIONS THAT ARE $p$ -CORES

FRANK G. GARVAN \*

Department of Mathematics  
Statistics & Computing Science  
Dalhousie University  
Halifax, Nova Scotia  
Canada B3H 3J5

October 18, 1991

ABSTRACT. A number of linear congruences modulo  $r$  are proved for the number of partitions that are  $p$ -cores where  $p$  is prime,  $5 \leq p \leq 23$ , and  $r$  is any prime divisor of  $(p-1)/2$ . Analogous results are derived for the number of irreducible  $p$ -modular representations of the symmetric group  $S_n$ . The congruences are proved using the theory of modular forms.

## 1. Introduction

A partition of  $n$  is a finite nonincreasing sequence of positive integers whose sum is  $n$ . It is well-known that  $p(n)$ , the number of partitions of  $n$ , is also the number of irreducible representations of the symmetric group  $S_n$ .  $p$ -cores are important in the study of  $p$ -modular representations of  $S_n$ . A  $p$ -core is a partition that has no hook numbers which are divisible by  $p$  [Ga-K-S]. We let  $a_p(n)$  denote the number of partitions of  $n$  that are

---

1980 *Mathematics Subject Classification* (1991 *Revision*) Primary 11P83, Secondary 05A17, 11B65, 11F11, 11F20, 11F33, 11F60, 20C20, 20C30

*Key words and phrases.* Partitions, congruences,  $p$ -cores,  $p$ -modular representations, Dedekind's eta function,  $q$ -series, modular forms, Eisenstein series, Hecke operators.

\*Research began at Macquarie University, NSW 2109, Australia, where the author was a Macquarie University Research Fellow. It was completed at the University of Florida, Gainesville FL 32611, and Dalhousie University where the author is an NSERC International Fellow. On leave (1991) from the University of Florida. Email: frank@cs.dal.ca, frank@math.ufl.edu

$p$ -cores. In [Ga-K-S] we gave a combinatorial proof of the following generating function identity:

$$(1.1) \quad \sum_{n \geq 0} a_p(n)q^n = \prod_{m=1}^{\infty} \frac{(1 - q^{pm})^p}{(1 - q^m)}, \quad (|q| < 1).$$

See [Ga-K-S, (2.1)]. See also [Kl] for a different combinatorial proof. Hence if  $p > 3$  is prime then  $\delta_p := (p^2 - 1)/24 \in \mathbb{Z}$  and

$$(1.2) \quad \sum_{n \geq \delta_p} a_p(n - \delta_p)q^n = \frac{\eta^p(p\tau)}{\eta(\tau)} =: X_p(\tau),$$

where  $q = e^{2\pi i\tau}$ ,  $\tau \in \mathcal{H}$  (the complex upper half-plane), and  $\eta(\tau)$  is Dedekind's well-known  $\eta$ -function

$$(1.3) \quad \eta(\tau) := e^{\pi i/12} \prod_{m=1}^{\infty} (1 - q^{2m\pi i\tau}).$$

When  $p$  is a prime  $> 3$ , Hecke has observed that the function  $X_p$  on the right side of (1.2) is a modular form of level  $p$ , weight  $(p-1)/2$  and character the Legendre symbol  $\left(\frac{\cdot}{p}\right)$ , for the congruence subgroup  $\Gamma_0(p)$ . See [O, p.28]. We may obtain good asymptotic estimates for  $a_p(n)$  by using known estimates for cusp forms and by noting that we obtain a cusp form from  $X_p$  by subtracting off a suitable multiple of an Eisenstein series. In this way it can be shown that for  $p$  prime  $> 3$  then

$$(1.4) \quad a_p(n - \delta_p) = \alpha_p u_p(n) + O(n^{(p-3)/4+\epsilon}) \quad \text{for any } \epsilon > 0,$$

where

$$u_p(n) = n^{(p-3)/2} \sum_{d|n} \frac{1}{d^{(p-3)/2}} \left(\frac{d}{p}\right),$$

and  $\alpha_p$  is some non-zero constant. This is a consequence of Deligne's proof of the Ramanujan-Petersson conjecture (see [Ka]). It follows that for two distinct primes  $3 < p_1 < p_2$  and  $n$  sufficiently large we have

$$(1.5) \quad a_{p_1}(n) \leq a_{p_2}(n).$$

Dennis Stanton has conjectured that this result holds for all  $3 < p_1 < p_2 < n$  with  $p_1, p_2$  not necessarily prime. It is also open whether  $a_p(n) > 0$  for all prime  $p > 3$  and all  $n \geq 0$ .

There is a general result of Serre's [Se2] that states that for a fixed integer  $m \geq 1$  almost all of the fourier coefficients of a modular form of positive integral weight on a congruence subgroup are divisible by  $m$ . Explicitly, let

$$f = \sum_{n=0}^{\infty} c_n e^{2\pi i n \tau / M}, \quad M \geq 1,$$

be such a modular form. We suppose the coefficients  $c_n$  are contained in some ring of integers  $\mathcal{O}_K$  of some algebraic number field  $K$ . If  $m$  is an integer  $\geq 1$  we write  $a \equiv 0 \pmod{m}$  if  $a \in m\mathcal{O}_K$ . We define  $E_{f,m}$  to be the set of integers  $n \in \mathbb{N}$  such that  $c_n \equiv 0 \pmod{m}$ . Serre's result is that  $E_{f,m}$  has density 1. Hence, in our case, we deduce that  $a_p(n) \equiv 0 \pmod{m}$  for almost all  $n$ , where  $m$  is any integer  $\geq 1$  and  $p$  is any prime  $> 3$ . In this paper we give some explicit subsets of  $E_{f,m}$  of positive density for certain  $f = X_p$  and certain  $m$ .

Ramanujan's [H-W, §19.12] congruences modulo 5, 7 and 11 for  $p(n)$  together with (1.1) easily yield the following congruences:

$$(1.6) \quad a_5(5n - 1) \equiv 0 \pmod{5},$$

$$(1.7) \quad a_7(7n - 2) \equiv 0 \pmod{7},$$

$$(1.8) \quad a_{11}(11n - 5) \equiv 0 \pmod{11}.$$

In [Ga-K-S] we were able to explain and prove (1.6)–(1.8) combinatorially. More general congruences hold

$$(1.9) \quad a_p(p^\alpha n - \delta_p) \equiv 0 \pmod{p^\alpha},$$

for all  $\alpha \geq 1$  and where  $p = 5, 7$  or  $11$ . The cases  $p = 5, 7$  were proved in [Ga-K-S]. The case  $p = 11$  is proved in §3. The congruences (1.6)–(1.9) come from the level of the relevant space of modular forms. It should also be noted that the proof of (1.9) is much easier than its analog for the partition function  $p(n)$ .

In this paper we are mainly concerned with congruences of a different sort. This time the modulus comes from the weight of the space of modular forms instead of the level. The weight here is  $(p-1)/2$  so we let  $r$  be any prime divisor of  $(p-1)/2$ . Then for each prime  $5 \leq p \leq 23$  there is an  $\epsilon_p$  ( $= 1$  or  $-1$ ) such that

$$(1.10) \quad a_p(n - \delta_p) \equiv 0 \pmod{r}, \quad \text{whenever } \left(\frac{n}{p}\right) = \epsilon_p \text{ and } n \not\equiv 0 \pmod{r}.$$

In particular,  $\epsilon_p = 1$  for  $p = 11, 13$  and  $\epsilon_p = -1$  for  $p = 5, 7, 17, 19, 23$ . For  $p = 17$  stronger congruences hold:

$$(1.11) \quad a_{17}(n-12) \equiv 0 \pmod{8} \quad \text{if } \left(\frac{n}{17}\right) = -1 \text{ and } n \not\equiv 0 \pmod{2},$$

and

$$(1.12) \quad a_{17}(n-12) \equiv 0 \pmod{2} \quad \text{if } \left(\frac{n}{17}\right) = -1 \text{ and } n \not\equiv 0 \pmod{4}.$$

These congruences are reminiscent of some congruences due to Kolberg [Kol2] for  $c_n$  the coefficients of the modular invariant  $j(\tau)$ . However, in Kolberg's case, the weight is 0 and the level is 1.

An easy consequence of (1.10)–(1.12) are analogous congruences for  $b_p(n)$ , the number of irreducible  $p$ -modular representations of  $S_n$ . It is well-known (see [An-O]) that

$$(1.13) \quad b_p(n) = \text{the number of partitions of } n \text{ in which no multiple of } p \text{ occurs as a part,}$$

so that

$$(1.14) \quad \begin{aligned} \sum_{n \geq 0} b_p(n)q^n &= \prod_{m=1}^{\infty} \frac{(1-q^{pm})}{(1-q^m)} \\ &= \frac{\sum_{n \geq 0} a_p(n)q^n}{\prod_{m=1}^{\infty} (1-q^{pm})^{p-1}}. \end{aligned}$$

Now as before let  $p$  be prime,  $5 \leq p \leq 23$ , and let  $r$  be any prime divisor of  $(p-1)/2$ . Then

$$\sum_{n \geq 0} b_p(n)q^n \equiv \frac{\sum_{n \geq 0} a_p(n)q^n}{\prod_{m=1}^{\infty} (1-q^{prm})^{(p-1)/r}} \pmod{r}.$$

It follows that  $b_p(n)$  satisfies the same congruence as  $a_p(n)$  given in (1.10). The results analogous to (1.11) and (1.12) also hold. These congruences have been observed independently by Gordon [Go]. The modular function on the right side of (1.14) and its powers has been previously studied by Newman [N5]. However, our congruences do not follow from Newman's identities.

Our proof depends on the classical Hecke theory of modular forms. We need a certain twist operator (see §2.3), the existence of special bases for cusp forms (see §2.4) and the

existence of certain  $r$ -th powers of modular forms (see §2.5). For the case  $p = 5, 7, 19, 23$  the problem is reduced to computing the constant term of a certain Eisenstein series (see Table I, §2.2). The remaining cases involve computing the first few terms of the  $q$ -expansion of certain modular forms.

The necessary preliminary results are set up in §2. The majority of the congruences are proved in §3 with the special congruence (1.11) being left until §4. The  $q$ -expansions were computed using the computer algebra package MAPLE.

It would be interesting to know if an elementary proof of the congruences could be found using the multidimensional theta function representation for the generating function for  $a_p(n)$  given in [Ga-K-S, (2.2)]. Klyachko [Kl] has observed that this representation follows from Macdonald's [M] identity for the root system  $A_{p-1}$ .

## 2. Preliminary Results

### 2.1 Definitions and Notation

Let  $\mathcal{H}$  denote the complex upper half plane.  $\mathrm{SL}_2(\mathbb{Z})$  acts transitively on  $\mathcal{H}$  by linear fractional transformations

$$(2.1.1) \quad \gamma\tau = \frac{a\tau + b}{c\tau + d}, \quad \text{where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Let  $N$  be a positive integer. We define

$$(2.1.2) \quad \Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{N}, \quad b \equiv c \equiv 0 \pmod{N} \right\},$$

so that  $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ . A subgroup of  $\Gamma(1)$  is called a *congruence subgroup of level  $N$*  if it contains  $\Gamma(N)$ . We will also be concerned with the following congruence subgroups:

$$(2.1.3) \quad \Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : c \equiv 0 \pmod{N} \right\},$$

$$(2.1.4) \quad \Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a \equiv 1 \pmod{N} \right\},$$

Now we consider functions  $f : \mathcal{H} \rightarrow \mathbb{C}$ . The notation  $f|[\gamma]_k$  is used to denote the function whose value at  $\tau$  is  $(c\tau + d)^{-k} f(\gamma\tau)$ . The value of  $f|[\gamma]_k$  at  $\tau$  is denoted by  $f(\tau)|[\gamma]_k$  so that

$$(2.1.5) \quad f(\tau)|[\gamma]_k := (c\tau + d)^{-k} f(\gamma\tau), \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1).$$

We define modular forms and cusp forms for a congruence subgroup  $\Gamma' \subset \Gamma(1)$  of level  $N$ . Let  $q_N$  denote  $e^{2\pi i\tau/N}$ . Let  $k \in \mathbb{Z}$ . A function  $f : \mathcal{H} \rightarrow \mathbb{C}$  is said to be a *modular form* of *weight*  $k$  for  $\Gamma'$  if it satisfies the following conditions:

- (i)  $f$  is holomorphic on  $\mathcal{H}$ ,
- (ii)  $f|[\gamma]_k = f$  for all  $\gamma \in \Gamma'$ ,
- (iii)  $f$  is holomorphic at the cusps  $\gamma(\infty)$  for  $\gamma \in \Gamma(1)$ ; i.e.  $f(\tau)|[\gamma]_k$  has the form  $\sum_{n \geq 0} a_n q_N^n$ .

We let  $M_k(\Gamma')$  denote the set of such modular forms. It turns out that  $M_k(\Gamma')$  is a finite dimensional  $\mathbb{C}$ -vector space. If  $a_0 = 0$  for all  $\gamma \in \Gamma(1)$  we say  $f$  is a *cusp form*. We let  $S_k(\Gamma')$  denote the subspace of cusp forms.

Now we define what it means for a function to be a modular form of weight  $k$  and character  $\chi$  for the group  $\Gamma_0(p)$  when  $p$  is prime. Let  $\chi$  be a Dirichlet character modulo  $p$

$$(2.1.6) \quad \chi : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}^\times, \quad \text{with } \chi(-1) = (-1)^k.$$

A function  $f : \mathcal{H} \rightarrow \mathbb{C}$  is said to be a *modular form* of *weight*  $k$  and *character*  $\chi$  for  $\Gamma_0(p)$  if it satisfies conditions (i)–(iii) above except (ii) is replaced by

$$(2.1.7) \quad f|[\gamma]_k = \chi(d)f \quad \text{for all } \gamma \in \Gamma_0(p).$$

In this case, condition (iii) amounts to the following two conditions:

$$(2.1.8a) \quad f(\tau) = \sum_{n=0}^{\infty} a_n q^n, \quad q = e^{2\pi i\tau}$$

and

$$(2.1.8b) \quad \tau^{-k} f(-1/p\tau) = \sum_{n=0}^{\infty} b_n q^n, \quad q = e^{2\pi i\tau}.$$

We call the Fourier series in (2.1.8a) the  $q$ -expansion of  $f$  at  $\infty$ , and we call (2.1.8b) the  $q$ -expansion at 0. We let  $M_k(p, \chi)$  denote the space of such modular forms. If  $a_0 = b_0 = 0$  in (2.1.8) above then  $f$  is a *cusp form*. We let  $S_k(p, \chi)$  denote the subspace of cusp forms. We have for  $k \geq 2$

$$M_k(p, \chi) = E_k(p, \chi) \oplus S_k(p, \chi),$$

where  $E_k(p, \chi)$  is a space of Eisenstein series of dimension 2 (the number of inequivalent cusps in this case).

We will be concerned with a number of characters modulo  $p$ . We let  $\chi_0$  denote the trivial character. For  $p$  an odd prime and  $d \mid \frac{1}{2}(p-1)$  we define

$$(2.1.9) \quad \chi_{p,d} : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times, \quad \text{by } \chi_{p,d}(g) = \exp(\pi i/d),$$

where  $g$  is the smallest primitive root modulo  $p$ . We note that

$$(2.1.10) \quad \chi_p := \chi_{p,1} = \left(\frac{\cdot}{p}\right) \quad (\text{the Legendre symbol}),$$

and

$$(2.1.11) \quad \chi_{p,d}^d = \chi_p = \left(\frac{\cdot}{p}\right).$$

## 2.2 Eisenstein Series and $\eta$ -Products

Kolberg [Kol3] has studied the Eisenstein series for  $\Gamma_0(p)$  and has shown how to derive certain Ramanujan-type identities that involve Eisenstein series and certain  $\eta$ -products. Let  $\chi$  be a Dirichlet character modulo  $p$ . We consider the Gauss sum

$$(2.2.1) \quad S_\chi(n) := \sum_{j=1}^{p-1} \chi(j) \exp(2\pi i j n / p).$$

Then

$$(2.2.2) \quad S_\chi(n) = \bar{\chi}(n) S_\chi(1).$$

We need the  $q$ -expansion of the two Eisenstein series for  $M_k(p, \chi)$ . We define

$$(2.2.3a) \quad V_{\chi,k} := A_k + \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \chi(n) n^{k-1} q^{mn} \quad \text{for } k \geq 1,$$

where

$$(2.2.3b) \quad A_k = A_{\chi,k} := -\frac{1}{2k} \sum_{j=0}^{k-1} \binom{k}{j} B_j p^{j-1} \sum_{n=1}^{p-1} \chi(n) n^{k-j},$$

and  $B_0 = 1$ ,  $B_1 = -1/2$ ,  $B_2 = 1/6$ ,  $B_3 = 0$ ,  $B_4 = -1/30, \dots$  are the Bernoulli numbers.

We define

$$(2.2.4) \quad U_{\chi,k} := \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \chi(m) n^{k-1} q^{mn} \quad \text{for } k \geq 2,$$

and

$$U_{\chi,1} := V_{\chi,1}.$$

**Proposition (2.2.5)**([Kol3]). *Let  $p$  be an integer  $> 1$ , let  $k$  be an integer  $\geq 1$ , and let  $\chi$  be a character modulo  $p$ . If  $\chi(-1) = (-1)^k$  and  $\chi \neq \chi_0$  then*

- (i)  $U_{\chi,k}, V_{\chi,k} \in M_k(p, \chi)$ ,
- (ii)  $V_{\chi,k}(-1/p\tau) = \frac{(p\tau)^k}{S_{\bar{\chi}}(1)} U_{\bar{\chi},k}(\tau)$ ,
- (iii)  $U_{\chi,k}(-1/p\tau) = \frac{p\tau^k}{S_{\bar{\chi}}(1)} V_{\bar{\chi},k}(\tau)$ .

We note that in the case that  $\chi$  is real and  $p$  is an odd prime (i.e.  $\chi = \chi_p$ ) then

$$(2.2.6) \quad S_{\bar{\chi}}(1) = S_{\chi}(1) = i^{(p-1)^2/4} \sqrt{p}.$$

We define

$$(2.2.7a) \quad U_{p,k} := U_{\chi_p,k},$$

$$(2.2.7b) \quad V_{p,k} := V_{\chi_p,k},$$

$$(2.2.7c) \quad A_{p,k} := A_{\chi_p,k}.$$

We now determine which  $\eta$ -products belong to  $M_k(p, \chi)$ . If we let  $\sqrt{\phantom{x}}$  denote the branch of the square root having nonnegative real part, then

$$(2.2.8) \quad \eta(-1/\tau) = \sqrt{\tau/i} \eta(\tau), \quad \text{for } \tau \in \mathcal{H}.$$

See [Kob, Prop.14 p.121].

**Proposition (2.2.9)**. *Let  $p$  be an odd prime and suppose  $k$  and  $m$  are integers satisfying*

$$(2.2.10a) \quad m \equiv 1 \pmod{2}, \quad (p+1)k \equiv 0 \pmod{12}, \quad (p-1)m \equiv 2k \pmod{24},$$

$$(2.2.10b) \quad -kp \leq \frac{(p-1)}{2}m \leq k.$$

Then

$$Y_{k,m} := \frac{\eta(\tau)^{2k+m}}{\eta(p\tau)^m} \in M_k(p, \chi_p).$$

Further, if there is strict inequality in (2.2.10b) then the  $\eta$ -product above is a cusp form.

*Remark:* Some  $\eta$ -products that are cusp forms are given below in Table II.

*Proof.* Let  $\gamma \in \Gamma_0(p)$ , and suppose that the conditions of the Proposition are satisfied. Kolberg [Kol3, Lemma 4 p.13] has shown that

$$(2.2.11) \quad Y_{k,m} | [\gamma]_k = \chi_p(d) Y_{k,m}.$$

It is clear from (1.3) that  $Y_{k,m}$  is holomorphic on  $\mathcal{H}$  and that it satisfies (2.1.8a). Condition (2.1.8b) follows by using (2.2.8). Hence  $Y_{k,m} \in M_k(p, \chi_p)$ .  $\square$

**Corollary (2.2.12).** *Let  $p > 3$  be prime. Then*

- (i)  $X_p := \frac{\eta^p(p\tau)}{\eta(\tau)} \in M_{\frac{1}{2}(p-1)}(p, \chi_p)$ ,
- (ii)  $c_p X_p - U_{p, \frac{1}{2}(p-1)} \in S_{\frac{1}{2}(p-1)}(p, \chi_p)$ , where  $c_p := pA_{p, \frac{1}{2}(p-1)} i^{\frac{1}{4}(p-1)(p-3)} \neq 0$ .

*Remark:* A table for some of the  $c_p$  is given below.

*Proof.* (i) follows immediately from Proposition (2.2.9). The  $q$ -expansion of  $X_p$  at  $\infty$  is

$$X_p = q^{r_p} + \dots,$$

where  $r_p = (p^2 - 1)/24 > 0$ . We choose  $c_p$  so that the constant term of the  $q$ -expansion at 0 of  $c_p X_p - U_{p, \frac{1}{2}(p-1)}$  is zero. Using (2.2.5)(iii), (2.2.6) and (2.2.8) we find

$$c_p := pA_{p, \frac{1}{2}(p-1)} i^{\frac{1}{4}(p-1)(p-3)},$$

which gives the desired result. Finally,  $c_p \neq 0$  follows from the fact that  $A_{p, \frac{1}{2}(p-1)}$  is a nonzero multiple ([Kol3, (2.26)]) of a Dirichlet  $L$ -series  $L(\frac{1}{2}(p-1), \chi_p)$  ([Se1, p.71]) which is nonzero.  $\square$

$p$	$c_p$
5	1
7	$8 = 2^3$
11	$1275 = 3 \cdot 5^2 \cdot 17$
13	$33463 = 109 \cdot 307$
17	$59901794 = 2 \cdot 19 \cdot 1576363$
19	$3708443635 = 5 \cdot 13 \cdot 67 \cdot 851537$
23	$27533989805352 = 2^3 \cdot 3 \cdot 63659 \cdot 18021797$

Table I.  $c_p$  of Corollary (2.2.12) (ii).

We need to calculate which  $\eta$ -products are cusp forms for  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$ ,  $5 \leq p \leq 23$ . For  $k = \frac{1}{2}(p-1)$  we need  $m \equiv 1 \pmod{2}$ ,  $(p-1)(m-1) \equiv 0 \pmod{24}$  and  $-(p-1) \leq m \leq 0$ . In this way we may calculate Table II below.

$p$	$\eta$ -product cusp forms
5	–
7	$\eta^3(\tau)\eta^3(7\tau)$
11	–
13	$\eta^{2n+1}(\tau)\eta^{11-2n}(13\tau)$ ( $0 \leq n \leq 5$ )
17	$\eta^5(\tau)\eta^{11}(17\tau), \eta^5(17\tau)\eta^{11}(\tau)$
19	$\eta^{4n+3}(\tau)\eta^{15-4n}(19\tau)$ ( $0 \leq n \leq 4$ )
23	$\eta^{11}(\tau)\eta^{11}(23\tau)$

Table II.  $\eta$ -products in  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$  for small  $p$ .

Klyachko [Kl, p.1883] has the following explicit formula

$$\dim S_{\frac{1}{2}(p-1)}(p, \chi_p) = \begin{cases} [(p-1)^2/24], & \text{if } p \not\equiv -1 \pmod{12}, \\ [(p-1)^2/24] - 1, & \text{if } p \equiv -1 \pmod{12}. \end{cases}$$

A table of these dimensions for small  $p$  is given below. We note that Proposition (2.4.13) below also gives these dimensions. For general  $k$  and  $\chi$ ,  $\dim S_k(p, \chi)$  may be calculated from [C-O, Thm 1].

$p$	$\dim S_{\frac{1}{2}(p-1)}(p, \chi_p)$
5	0
7	1
11	3
13	6
17	10
19	13
23	19
29	32

Table III. Dimension of certain spaces of cusp forms.

From this table we observe that

$$(2.2.13) \quad \dim S_{\frac{1}{2}(p-1)}(p, \chi_p) < p \quad \text{for } p \text{ prime, } 5 \leq p \leq 23.$$

Our proof of the congruences depends in part on this inequality. This explains to some extent why the congruences seem to stop at  $p = 23$ .

### 2.3 Operators

Let  $N > 1$  be an odd integer. Let  $f \in M_k(N, \chi)$  where  $\chi$  is a Dirichlet character modulo  $N$ . Suppose  $f(\tau) = \sum_{n \geq 0} a_n q^n$  ( $q = e^{2\pi i \tau}$ ). For  $p$  prime, the *Hecke operator*  $T_p$  is given by  $T_p(f(\tau)) = \sum_{n \geq 0} b_n q^n$  where

$$(2.3.1) \quad b_n = a_{pn} + \chi(p)p^{k-1}a_{n/p}.$$

Here we take  $\chi(p) = 0$  if  $p|N$  and take  $a_{n/p} = 0$  if  $n$  is not divisible by  $p$ . See [Kob, Prop.37 p.161]. The Hecke operators  $T_n$  may be defined for all  $n$  (see [Kob, (5.8) p.158]). The  $T_n$  preserve the spaces  $M_k(N, \chi)$  and  $S_k(N, \chi)$  [Kob, Prop.35 p.160]. For  $f, g \in S_k(\Gamma_1(N)) \supset S_k(N, \chi)$  we may define the *Petersson product* of  $f$  and  $g$  as

$$(2.3.2) \quad \langle f, g \rangle := \frac{1}{[\Gamma(1) : \Gamma_1(N)]} \int_{\Gamma_1(N) \backslash \mathcal{H}} f(\tau) \overline{g(\tau)} y^k \frac{dx dy}{y^2} \quad (\tau = x + iy).$$

We need

**Theorem (2.3.3).** (*Petersson*) Let  $T_n$  be a Hecke operator on  $S_k(N, \chi)$  with  $\gcd(n, N) = 1$ . If  $f, g \in S_k(N, \chi)$  then

$$\langle T_n f, g \rangle = \chi(n) \langle f, T_n g \rangle.$$

See [Kob, Prop.48 p.171] for a proof.

**Corollary (2.3.4).** ([Kob, Prop.51 p.173]) There exists a basis of the  $\mathbb{C}$ -vector space  $S_k(N, \chi)$  whose elements are eigenforms for all the Hecke operators  $T_n$  for which  $\gcd(n, N) = 1$ .

**Corollary (2.3.5).** Suppose  $\lambda_n$  is an eigenvalue of the Hecke operator  $T_n$  for  $S_k(p, \chi_p)$ . Then

- (i)  $\lambda_n$  is real if  $\left(\frac{n}{p}\right) = \chi_p(n) = 1$ ,
- (ii)  $\lambda_n$  is pure imaginary if  $\left(\frac{n}{p}\right) = \chi_p(n) = -1$ .

We now describe the needed *twist-operator* for  $S_k(p, \chi_p)$ . We follow [Z, p.36]. There is a natural involution on  $S_k(p, \chi_p)$  due to Hecke:

$$(2.3.6) \quad \rho' : S_k(p, \chi_p) \longrightarrow S_k(p, \chi_p), \quad f^{\rho'}(\tau) = \overline{f(-\bar{\tau})}.$$

If  $f(\tau) = \sum_{n \geq 1} a_n q^n$  then  $f^{\rho'}(\tau) = \sum_{n \geq 1} \overline{a_n} q^n$ . An eigenform for the Hecke operators  $T_n$  with  $\gcd(n, p) = 1$  is *normalized* if  $a_1 = 1$  in its  $q$ -expansion at  $\infty$ . In this case the

eigenvalues are  $\lambda_n = a_n$  ([Kob, Prop.40 p.163]). By Corollary (2.3.5) we have

$$(2.3.7) \quad a_n^{\rho'} = \chi_p(n)a_n = \binom{n}{p}a_n \quad \text{if } p \nmid n.$$

Since, by Corollary (2.3.4), the normalized Hecke eigenforms form a basis for  $S_k(p, \chi_p)$  we may extend the action of  $\rho'$  on the eigenforms by linearity to a linear operator on all of  $S_k(p, \chi_p)$

$$\rho : S_k(p, \chi_p) \longrightarrow S_k(p, \chi_p),$$

so that

$$(2.3.8) \quad a_n^\rho = \binom{n}{p}a_n \quad \text{if } p \nmid n,$$

where  $f(\tau) = \sum_{n \geq 1} a_n q^n$  is any  $f \in S_k(p, \chi_p)$ . We let

$$(2.3.9) \quad S_{k,p}^+ := \left\{ f \in S_k(p, \chi_p) : f(\tau) = \sum_{n \geq 1} a_n q^n, \quad a_n = 0 \quad \text{for } \binom{n}{p} = -1 \right\},$$

$$(2.3.10) \quad S_{k,p}^- := \left\{ f \in S_k(p, \chi_p) : f(\tau) = \sum_{n \geq 1} a_n q^n, \quad a_n = 0 \quad \text{for } \binom{n}{p} = +1 \right\}.$$

Clearly,

$$(2.3.11) \quad S_k(p, \chi_p) = S_{k,p}^+ + S_{k,p}^-,$$

since we may write any  $f \in S_k(p, \chi_p)$  as

$$(2.3.12) \quad f = \frac{1}{2}(f + f^\rho) + \frac{1}{2}(f - f^\rho).$$

A well-known lemma of Hecke ([O, p.32]) says that a nonzero cusp form of level  $p$  and character  $\chi \neq \chi_0$  can not have a development of the form  $\sum_{n \geq 1} a_n q^{pn}$ . It follows that  $S_{k,p}^+ \cap S_{k,p}^- = \{0\}$  so that

$$(2.3.13) \quad S_k(p, \chi_p) = S_{k,p}^+ \oplus S_{k,p}^-.$$

It is clear that the  $S_{k,p}^{\pm}$  are the  $(\pm 1)$ -eigenspaces of  $\rho$ .

Let  $p$  be a fixed prime,  $5 \leq p \leq 23$ . Let  $d := \dim S_{\frac{1}{2}(p-1)}(p, \chi_p)$ . Then, by (2.2.13),

$$(2.3.14) \quad d < p.$$

In §2.4 we will show that we may construct a basis  $\mathcal{B} = \{B_1, B_2, \dots, B_d\}$  for  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$  such that each  $B_j \in \mathbb{Z}[[q]]$  and

$$(2.3.15) \quad B_j = q^j + \dots \quad .$$

**Proposition (2.3.16).** *Let  $\epsilon = \pm 1$  be fixed. Suppose  $p$  is prime with  $7 \leq p \leq 23$ . Let  $d := \dim S_{\frac{1}{2}(p-1)}(p, \chi_p)$ . Suppose  $f \in S_{\frac{1}{2}(p-1)}(p, \chi_p)$  and  $f(\tau) = \sum_{n \geq 1} a_n q^n$ . If*

$$a_n = 0 \quad \text{for } \left(\frac{n}{p}\right) = \epsilon \text{ and } n \leq d,$$

then

$$a_n = 0 \quad \text{for all } n \text{ with } \left(\frac{n}{p}\right) = \epsilon.$$

*Remark:* A table for the  $d$ 's is given in Table III in §2.2.

*Proof.* Let  $g := f + \epsilon f^p = \sum_{n \geq 1} b_n q^n$ , so that  $g \in S_{\frac{1}{2}(p-1)}(p, \chi_p)$ . Then, by (2.3.14), we have

$$b_n = 2a_n = 0 \quad \text{for all } n \leq d.$$

Hence, by (2.3.15),  $g = 0$ ,  $f \in S_{\frac{1}{2}(p-1), p}^{-\epsilon}$  and the result follows.  $\square$

*Example.* For  $p = 7$ ,  $d = 1$  and a basis for  $S_3(7, \chi_7)$  is

$$\eta^3(\tau)\eta^3(7\tau) = q + \dots = \sum_{n \geq 1} a_n q^n.$$

Hence,  $a_n = 0$  for  $\left(\frac{n}{7}\right) = -1$ .

We note that there is an alternative approach to this problem. Instead of using the operator  $\rho$  we could have used the the Atkin-Lehner operator  $R_p^*$  ([At-L, p.155]). See also [Kob, Prop.17 p.127]. However this would have required working in the space  $S_{\frac{1}{2}(p-1)}(p^2, \chi_p)$  rather than  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$ . Clearly the smaller space  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$  and  $\rho$  are preferable.

The action of Hecke operators on Eisenstein series is easily calculated.

**Lemma (2.3.17).** *Let  $p$  be an odd prime and let  $r$  be prime. For the Hecke operator  $T_r$  on  $S_k(p, \chi_p)$  we have*

$$(i) \quad T_r(U_{p,k}) = (\chi_p(r) + p^{k-1})U_{p,k},$$

$$(ii) \quad T_r(V_{p,k}) = (1 + \chi_p(r)p^{k-1})V_{p,k}.$$

We now introduce some elementary operators that act on formal power series in  $\mathbb{Z}[[q]]$ . Let  $p$  be an odd prime. For  $\epsilon = +$  or  $-$  we define the operator  $\Psi_\epsilon = \Psi_{\epsilon,p}$  that acts on a series  $\sum_{n \geq 0} a_n q^n$  and picks out those terms in which  $\chi_p(n) = \epsilon$ ; i.e.

$$(2.3.18) \quad \Psi_\epsilon \left( \sum_{n \geq 0} a_n q^n \right) = \sum_{\substack{n \geq 1 \\ \chi_p(n) = \epsilon}} a_n q^n.$$

We note that  $\Psi_\epsilon$  does not necessarily preserve the space  $M_k(p, \chi_p)$ . However, the action of  $\Psi_\epsilon$  on Eisenstein series is nice.

**Lemma (2.3.19).** *Let  $p$  be an odd prime then for  $\epsilon = \pm$  we have*

$$(2.3.20) \quad \Psi_\epsilon(U_{p,k}) = \epsilon \Psi_\epsilon(V_{p,k}).$$

*Proof.* Let  $r$  be prime,  $r \neq p$ . Let  $u(n)$  ( $v(n)$  resp.) be the  $n$ -th coefficient in the  $q$ -expansion of  $U_{p,k}$  ( $V_{p,k}$  resp.) at  $\infty$ . An easy calculation gives

$$u(r^\alpha) = \chi_p(r^\alpha)v(r^\alpha).$$

So, by multiplicativity, we have

$$u(n) = \chi_p(n)v(n) \quad \text{for } p \nmid n,$$

and the result follows.  $\square$

Finally, for  $r > 1$  we define  $\Phi_r$  to be the operator that acts on a series  $\sum_{n \geq 0} a_n q^n$  and picks out those terms in which  $n \not\equiv 0 \pmod{r}$ ; i.e.

$$(2.3.21) \quad \Phi_r \left( \sum_{n \geq 0} a_n q^n \right) = \sum_{\substack{n \geq 1 \\ n \not\equiv 0 \pmod{r}}} a_n q^n.$$

We note that  $\Phi_r$  does not necessarily preserve the space  $M_k(p, \chi_p)$ . Let  $\mathcal{O}$  denote a ring of algebraic integers. For

$$W = \sum_{n \geq 0} a_n q^n \in \mathcal{O}[[q]]$$

we write  $W \equiv 0 \pmod{r}$  if and only if  $a_n \equiv 0 \pmod{r}$  in  $\mathcal{O}$  for all  $n \geq 0$ . In our applications we consider  $\mathcal{O} = \mathbb{Z}$  or  $\mathbb{Z}[\zeta]$ , where  $\zeta$  is some root of unity.

**Lemma (2.3.22).** *Let  $p$  be an odd prime and let  $r$  and  $s$  be two distinct primes. Let  $\mathcal{O}$  be a ring of algebraic integers. Suppose  $k > 1$ ,  $r \mid k$  and  $W \in M_{k/r}(p, \chi) \cap \mathcal{O}[[q]]$ , where  $\chi$  is a Dirichlet character modulo  $p$  such that  $\chi^r = \chi_p$ . Then*

- (i)  $\Phi_r(W^r) \equiv 0 \pmod{r}$ ,
- (ii)  $\Phi_r(T_s(W^r)) \equiv 0 \pmod{r}$ .

*Proof.* (i) is trivial. We have

$$W^r = \sum_{n \geq 0} a_n q^n \in M_k(p, \chi_p),$$

where  $a_n \in \mathbb{Z}$ , and  $a_n \equiv 0 \pmod{r}$  for  $n \not\equiv 0 \pmod{r}$ . Now

$$T_s(W^r) = \sum_{n \geq 0} b_n q^n,$$

where

$$b_n = a_{sn} + \chi_p(s) s^{k-1} a_{n/s}.$$

If  $n \not\equiv 0 \pmod{r}$  then  $sn \not\equiv 0 \pmod{r}$  and  $n/s \not\equiv 0 \pmod{r}$ , so that

$$b_n \equiv 0 \pmod{r},$$

which is (ii).  $\square$

There is an elementary congruence for Eisenstein series.

**Lemma (2.3.23).** *Let  $p$  be an odd prime and  $k \geq 1$ . If  $d$  is prime and  $d-1 \mid k-1$  then*

$$\Phi_d \circ \Psi_-(U_{p,k}) \equiv 0 \pmod{d}.$$

*Proof.* Let  $u(n)$  denote the  $n$ -th coefficient in the  $q$ -expansion of  $U_{p,k}$  at  $\tau = \infty$ . If  $\left(\frac{a}{p}\right) = -1$  and  $n \not\equiv 0 \pmod{d}$  then there is a prime  $q$ ,  $q \neq d$ , such that  $\left(\frac{q}{p}\right) = -1$  and  $q^\alpha \parallel n$  with  $\alpha$  odd. Now

$$q^{d-1} \equiv 1 \pmod{d} \quad \text{since } q \neq d.$$

Since  $d-1 \mid k-1$  we have

$$\begin{aligned} q^{k-1} &\equiv 1 \pmod{d} \\ u(q^\alpha) &= q^{\alpha(k-1)} - q^{(\alpha-1)(k-1)} + \dots - 1 \\ &\equiv 0 \pmod{d}, \end{aligned}$$

so that

$$u(n) \equiv 0 \pmod{d} \quad (\text{by multiplicativity}),$$

which is the result.  $\square$

#### 2.4 Construction of Bases

In this section we construct bases for  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$  for  $p$  prime,  $7 \leq p \leq 23$ . Let  $d := \dim S_{\frac{1}{2}(p-1)}(p, \chi_p)$  (see Table III, §2.2). We want to construct a basis,  $\mathcal{B} = \{B_1, B_2, \dots, B_d\}$  with the following properties:

For each  $j$ ,

$$(2.4.1a) \quad B_j \in \mathbb{Z}[[q]],$$

$$(2.4.1b) \quad B_j = q^j + \dots \quad .$$

We call such a basis *good*. To do this we first construct polynomial bases for certain sets of modular functions on  $\Gamma_0(p)$ . This problem has been studied previously by Kolberg [Kol3] and Newman [N3], [N4].

Let  $p$  be prime. A function  $f : \mathcal{H} \rightarrow \mathbb{C}$  is said to be a *modular function* on  $\Gamma_0(p)$  if it satisfies the following conditions:

- (i)  $f$  is meromorphic on  $\mathcal{H}$ ,
- (ii)  $f|[\gamma]_0 = f$  for all  $\gamma \in \Gamma_0(p)$ ,
- (iii)  $f$  is meromorphic at the cusps  $\gamma(\infty)$  for  $\gamma \in \Gamma(1)$ ; i.e.  $f(\tau)|[\gamma]_0$  has the form  $\sum_{n \geq \nu} a_n q_p^n$  for some  $\nu \in \mathbb{Z}$  where  $q_p = e^{2\pi i \tau / p}$ .

As in the case of modular forms, condition (iii) amounts to the following two conditions:

$$(2.4.2a) \quad f(\tau) = \sum_{n \geq \nu_\infty} a_n q^n, \quad q = e^{2\pi i \tau}, \quad \text{some } \nu_\infty \in \mathbb{Z}$$

and

$$(2.4.2b) \quad f(-1/p\tau) = \sum_{n \geq \nu_0} b_n q^n, \quad q = e^{2\pi i \tau}, \quad \text{some } \nu_0 \in \mathbb{Z}.$$

We say  $\nu_\infty$  is the *valence* of  $f$  at  $\tau = \infty$  and  $\nu_0$  is the *valence* at  $\tau = 0$ , when  $a_{\nu_\infty}, b_{\nu_0} \neq 0$ .

Let  $F_p$  denote the set of functions  $f$  with the following properties:

- (i)  $f$  is a modular function on  $\Gamma_0(p)$ ,
- (ii)  $f$  is holomorphic on  $\mathcal{H}$  and the only pole of  $f$  in the fundamental region of  $\Gamma_0(p)$  is at  $\tau = \infty$  (i.e.  $\nu_0 \geq 0$ ).

When  $p$  is a prime  $> 3$  the genus of  $\Gamma_0(p)$  is given by

$$(2.4.3) \quad g = \begin{cases} [p/12] - 1, & \text{if } p \equiv 1 \pmod{12}, \\ [p/12], & \text{if } p \equiv 5, 7 \pmod{12}, \\ [p/12] + 1, & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

This follows from [Sc, p.103]. For each prime  $5 \leq p \leq 23$  we will construct a polynomial basis for  $F_p$  consisting of  $g+1$  functions  $f_j$ , where  $f_j$  has valence  $-j$  for  $g+1 \leq j \leq 2g+1$  at  $\tau = \infty$ . It is an open problem as to whether this can be done for general  $p$ . Once we have constructed such a basis it is an easy matter to construct a (linear) basis for  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$ .

Following Kolberg [Kol1] we construct our polynomial bases out of  $\eta$ -products and Fine's  $W_k$ -functions [F]. Kolberg has constructed such bases however we require our bases to have two additional properties: For each  $j$ ,

$$(2.4.4) \text{ (i)}$$

$$f_j = q^{-j} + \dots \quad \text{with integral coefficients, and}$$

$$(2.4.4) \text{ (ii)}$$

$$f_j \text{ is zero at } \tau = 0 \text{ (i.e. } \nu_0 \geq 1).$$

We call such a basis *good*.

Let  $p > 3$  be prime. Following Fine [F] we define

$$(2.4.5) \quad W_k(\tau) = W_{k,p}(\tau) := q^{\frac{6k^2}{p} - k} \prod_{m \geq 1} \frac{(1 - q^{pm-4k})(1 - q^{pm+4k-p})}{(1 - q^{pm-2k})(1 - q^{pm+2k-p})},$$

for  $k \not\equiv 0 \pmod{p}$ . We note that  $W_k$  may be defined for all  $(p, 6) = 1$  with  $p$  not necessarily prime. Atkin and Swinnerton-Dyer [At-S, Lemma 6] observed that the  $W_k(p\tau)$  occur in the  $p$ -dissection of the modular function  $\eta(\tau)/\eta(p^2\tau)$ .

**Proposition (2.4.6)** ([F]). *Let  $p > 3$  be prime, and let  $k \in \mathbb{Z}$  with  $k \not\equiv 0 \pmod{p}$ . Then*

$$(i) \quad W_k = W_{-k} = W_{k+p},$$

$$(ii) \quad W_k | [\gamma]_0 = \exp(12\pi i k^2 ab/p) W_{ak}, \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p),$$

$$(iii) \quad W_k(-1/p\tau) = 2 \cos(2k\pi/p) + O(q).$$

From (i) there are  $\frac{1}{2}(p-1)$  distinct  $W_k$  namely  $W_1, W_2, \dots, W_{\frac{1}{2}(p-1)}$ . We say that a polynomial in the  $W_k$ 's is *cyclic* if it is invariant under  $k \mapsto ak$  for every  $a \not\equiv 0 \pmod{p}$ . Further, a polynomial in the  $W_k$ 's is called  $(p, 0)$ -*isobaric* if each term has weight  $\equiv 0 \pmod{p}$  provided that  $W_k$  is assigned weight  $k^2$ . Since each  $W_k$  is holomorphic on  $\mathcal{H}$  we have

**Corollary (2.4.7)** ([F, p.153]). *Let  $p > 3$  be prime. Then*

- (i) *Every cyclic  $(p, 0)$ -isobaric polynomial in the  $W_k$  ( $1 \leq k \leq \frac{1}{2}(p-1)$ ) is a modular function on  $\Gamma_0(p)$ . In fact, each such function belongs to  $F_p$ .*
- (ii) *The constant term (in the  $q$ -expansion at  $\tau = 0$ ) of any cyclic polynomial in the  $W_k$  with integral coefficients is a rational integer.*

*Proof.* (i) is immediate from Proposition (2.4.6). From (2.4.6) (iii) the constant term of  $W_k$  (in the  $q$ -expansion at  $\tau = 0$ ) is  $2 \cos(2k\pi/p)$  which is an algebraic integer in the field  $\mathbb{Q}(\zeta_p)$  where  $\zeta_p = \exp(2\pi i/p)$ . It follows that the constant term of a cyclic  $\mathbb{Z}$ -polynomial is a rational integer since it is invariant under all the  $\mathbb{Q}$ -automorphisms  $\zeta_p \mapsto \zeta_p^a$ ,  $a \not\equiv 0 \pmod{p}$ .  $\square$

Let  $p > 3$  be prime. Let  $\varrho$  be the least positive even integer such that  $(p-1)\varrho \equiv 0 \pmod{24}$ . We define

$$(2.4.8) \quad w_p(\tau) := \left( \frac{\eta(\tau)}{\eta(p\tau)} \right)^\varrho.$$

Then

$$(2.4.9) \quad w_p(\tau) = q^{-(p-1)\varrho/24} + \dots,$$

and by (2.2.8) we have

$$(2.4.10) \quad w_p(-1/p\tau) = p^{\varrho/2} q^{(p-1)\varrho/24} + \dots.$$

Newman [N4] has determined which  $\eta$ -products are modular functions on  $\Gamma_0(N)$ . From [N4, Thm1 p.375] we may obtain

**Proposition (2.4.11).** *Let  $p > 3$  be prime. Then*

$$w_p \in F_p.$$

We obtain the following result which is analogous to [Kol1, Lemma 4 p.6].

**Proposition (2.4.12).** *Let  $p > 3$  be prime. If  $p \leq 23$  then there exists a good polynomial basis for the set of modular functions  $F_p$ .*

*Remarks.* See (2.4.4) for the definition of good. This proposition is probably true for larger  $p$ .

*Proof.* Let  $5 \leq p \leq 23$  be prime. By utilising Corollary (2.4.7), and Proposition (2.4.11) we have constructed functions  $f_j$  ( $g+1 \leq j \leq 2g+1$ ) that satisfy (2.4.4):

$p = 5, \quad g = 0 :$

$$f_1 = w_5 = \left( \frac{\eta(\tau)}{\eta(5\tau)} \right)^6 = q^{-1} - 6 + 9q + 10q^2 - 30q^3 + 6q^4 - 25q^5 + \dots \quad .$$

$p = 7, \quad g = 0 :$

$$f_1 = w_7 = \left( \frac{\eta(\tau)}{\eta(7\tau)} \right)^4 = q^{-1} - 4 + 2q + 8q^2 - 5q^3 - 4q^4 - 10q^5 + \dots \quad .$$

$p = 11, \quad g = 1 :$

$$\begin{aligned} f_2 &= W_1^3 W_4 W_5 + W_2^3 W_3 W_1 + W_3^3 W_1 W_4 + W_4^3 W_5 W_2 + W_5^3 W_2 W_3 - 17 \\ &= q^{-2} + 2q^{-1} - 12 + 5q + 8q^2 + q^3 + 7q^4 + \dots, \end{aligned}$$

$$\begin{aligned} f_3 &= 2 - (W_1^6 W_4 + W_2^6 W_3 + W_3^6 W_1 + W_4^6 W_5 + W_5^6 W_2) \\ &= q^{-3} + q^{-1} - 12 + 2q + 2q^2 + 16q^3 + 16q^4 + \dots \quad . \end{aligned}$$

$p = 13, \quad g = 0 :$

$$f_1 = w_{13} = \left( \frac{\eta(\tau)}{\eta(13\tau)} \right)^2 = q^{-1} - 2 - q + 2q^2 + q^3 + 2q^4 - 2q^5 + \dots \quad .$$

$p = 17, \quad g = 1 :$

$$\begin{aligned} f_2 &= W_1 W_2^2 W_5 + W_2 W_4^2 W_7 + W_3 W_6^2 W_2 + W_4 W_8^2 W_3 + W_5 W_7^2 W_8 \\ &\quad + W_6 W_5^2 W_4 + W_7 W_3^2 W_1 + W_8 W_1^2 W_6 - 9 \\ &= q^{-2} + q^{-1} - 6 + q + 2q^2 + 2q^3 + 3q^4 + \dots, \end{aligned}$$

$$\begin{aligned} f_3 &= W_1^3 W_2 W_5 W_6 + W_2^3 W_4 W_7 W_5 + W_3^3 W_6 W_2 W_1 + W_4^3 W_8 W_3 W_7 \\ &\quad + W_5^3 W_7 W_8 W_4 + W_6^3 W_5 W_4 W_2 + W_7^3 W_3 W_1 W_8 + W_8^3 W_1 W_6 W_3 - 36 \\ &= q^{-3} + 3q^{-2} + 3q^{-1} - 24 + 5q + 8q^2 + 3q^3 + \dots \quad . \end{aligned}$$

$p = 19, \quad g = 1 :$

$$\begin{aligned} f_2 &= W_1 W_7 W_8 + W_2 W_5 W_3 + W_4 W_9 W_6 - 5 \\ &= q^{-2} - 4 + q + 2q^2 + 2q^3 - q^4 + \dots, \end{aligned}$$

$$f_3 = w_{19} = \left( \frac{\eta(\tau)}{\eta(19\tau)} \right)^4 = q^{-3} - 4q^{-2} + 2q^{-1} + 8 - 5q - 4q^2 - 10q^3 + \dots \quad .$$

$p = 23, \quad g = 2 :$

$$\begin{aligned}
f_3 &= -8 - (W_1^2 W_6 W_{10} + W_2^2 W_{11} W_3 + W_3^2 W_5 W_7 + W_4^2 W_1 W_6 + W_5^2 W_7 W_4 \\
&\quad + W_6^2 W_{10} W_9 + W_7^2 W_4 W_1 + W_8^2 W_2 W_{11} + W_9^2 W_8 W_2 + W_{10}^2 W_9 W_8 \\
&\quad + W_{11}^2 W_3 W_5) \\
&= q^{-3} + 2q^{-2} + q^{-1} - 12 + 2q + 2q^2 + 6q^4 + \dots, \\
f_4 &= 7 - (W_1^3 W_5 W_8 + W_2^3 W_{10} W_7 + W_3^3 W_8 W_1 + W_4^3 W_3 W_9 + W_5^3 W_2 W_6 \\
&\quad + W_6^3 W_7 W_2 + W_7^3 W_{11} W_{10} + W_8^3 W_6 W_5 + W_9^3 W_1 W_3 + W_{10}^3 W_4 W_{11} \\
&\quad + W_{11}^3 W_9 W_4) \\
&= q^{-4} - q^{-3} - q^{-2} + 2q^2 + 4q^3 - 6q^4 + \dots, \\
f_5 &= -32 - (W_1^4 W_6 W_{11} + W_2^4 W_{11} W_1 + W_3^4 W_5 W_{10} + W_4^4 W_1 W_2 + W_5^4 W_7 W_9 \\
&\quad + W_6^4 W_{10} W_3 + W_7^4 W_4 W_8 + W_8^4 W_2 W_4 + W_9^4 W_8 W_7 + W_{10}^4 W_9 W_5 \\
&\quad + W_{11}^4 W_3 W_6) \\
&= q^{-5} + q^{-4} + q^{-3} + q^{-2} + 2q^{-1} - 24 + 3q + \dots \quad .
\end{aligned}$$

The first few terms of each  $q$ -expansion above were obtained using the symbolic algebra package MAPLE. Now suppose  $f \in F_p$ . Then it is clear that there is a polynomial  $P$  with integral coefficients such that

$$\nu_\infty(f - P(f_{g+1}, \dots, f_{2g+1})) \geq -g.$$

It follows by the Weierstrass gap theorem [Sp, p.272] that

$$f = c + P(f_{g+1}, \dots, f_{2g+1})$$

for some constant  $c$ . Hence  $\{f_{g+1}, \dots, f_{2g+1}\}$  is a good polynomial basis for  $F_p$ .  $\square$

It is now a simple matter to construct a good (linear) basis for  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$  for  $p$  prime,  $7 \leq p \leq 23$ .

**Proposition (2.4.13).** *Let  $p > 5$  be prime. If  $p \leq 23$  then*

- (i)  $d := \dim S_{\frac{1}{2}(p-1)}(p, \chi_p) = r_p - g - 1$ , where  $r_p := (p^2 - 1)/24$  and  $g$  is the genus of  $\Gamma_0(p)$ ,
- (ii)  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$  has a good linear basis  $\mathcal{B} = \{B_1, B_2, \dots, B_d\}$  where

$$B_j = X_p f_{r_p - j}, \quad \text{if } d - g \leq j \leq d,$$

$$B_j = X_p f_{g+1}^{(t-1)} f_{s+g+1}, \quad \text{if } j < d - g,$$

$t := [(r_p - j)/(g + 1)]$ ,  $s := r_p - t(g + 1) - j$ , and  $\{f_{g+1}, \dots, f_{2g+1}\}$  form a good polynomial basis for  $F_p$  as given in the proof of Proposition (2.4.12).

*Remarks.* See (2.4.1) for the definition of good. This proposition is probably true for larger  $p$ .

*Proof.* Suppose there is an  $f \in M_{\frac{1}{2}(p-1)}(p, \chi_p)$  with  $\nu_\infty(f) > r_p - g - 1$ . Then  $f/X_p \in F_p$  since  $X_p \in M_{\frac{1}{2}(p-1)}(p, \chi_p)$  and has no zeros in  $\mathcal{H}$ . But now,  $\nu_\infty(f/X_p) \geq -g$  which contradicts our construction in Proposition (2.4.12) unless  $f = cX_p$  (for some constant  $c$ ). Since  $X_p$  is not a cusp form this means that if  $f \in S_{\frac{1}{2}(p-1)}(p, \chi_p)$  then  $\nu_\infty(f) \leq r_p - g - 1$ . We will show that for each  $1 \leq j \leq r_p - g - 1$  there is a  $B_j \in S_{\frac{1}{2}(p-1)}(p, \chi_p)$  that satisfies (2.4.1). Then the  $B_j$  form a basis and we have (i).

From the proof of Proposition (2.4.12) there are modular functions  $f_{g+1}, \dots, f_{2g+1}$  on  $\Gamma_0(p)$  that satisfy (2.4.4). For  $1 \leq j \leq r_p - g - 1$  we let  $m = m_j = r_p - j$  so that  $m \geq g + 1$ .

*Case (i).*  $m \leq 2g + 1$ . We take

$$B_j := X_p f_m \in S_{\frac{1}{2}(p-1)}(p, \chi_p),$$

since  $X_p \in M_{\frac{1}{2}(p-1)}(p, \chi_p)$ ,  $\nu_\infty(B_j) = r_p - m = j \geq 1$  and  $\nu_0(B_j) = \nu_0(X_p) + \nu_0(f_m) = \nu_0(f_m) \geq 1$ .

*Case (ii).*  $m > 2g + 1$ . We find  $t \geq 2$  and  $s \geq 0$  such that

$$m = t(g + 1) + s,$$

where  $0 \leq s < g + 1$ , so that

$$m = (t - 1)(g + 1) + (s + g + 1)$$

and

$$g + 1 \leq s + g + 1 \leq 2g + 1.$$

In this case we take

$$B_j := X_p f_{g+1}^{(t-1)} f_{s+g+1},$$

which has the desired properties.

Hence we have (i) and (ii) is the construction given above.  $\square$

The following result follows easily from Propositions (2.3.16) and (2.4.13).

**Corollary (2.4.14).** *Let  $p$  be prime,  $7 \leq p \leq 23$ , and  $d := \dim S_{\frac{1}{2}(p-1)}(p, \chi_p)$ . Then there exists a good basis  $\mathcal{C} = \{C_1, C_2, \dots, C_d\}$  for  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$  such that*

- (i)  $C_i = q^i + O(q^{d+1}) \quad (1 \leq i \leq d)$ ,
- (ii)  $\mathcal{C}^+ = \{C_i : \left(\frac{i}{p}\right) = 1\}$  is a good basis for  $S_{\frac{1}{2}(p-1), p}^+$ ,
- (iii)  $\mathcal{C}^- = \{C_i : \left(\frac{i}{p}\right) = -1\}$  is a good basis for  $S_{\frac{1}{2}(p-1), p}^-$ .

*Remark.* This result is not true for  $p > 23$  since for such  $p$  we have  $p > d$ .

### 2.5 Construction of $r$ -th powers

Let  $p$  be prime  $11 \leq p \leq 23$ , and let  $r$  be a prime divisor of  $\frac{1}{2}(p-1)$ . In this section we construct modular forms  $f$  of weight  $\frac{(p-1)}{2r}$  such that  $f^r \in M_{\frac{1}{2}(p-1)}(p, \chi_p)$ . Where possible we construct a cusp form  $f$  and where needed we calculate a superset of the coefficient set of  $f$ . If  $f = \sum_{n \geq 0} a_n q^n$  then the *coefficient set* of  $f$  is simply  $\{a_n : n \geq 0\}$ . If this superset is a ring of algebraic integers this construction yields a congruence modulo  $r$ .

$$p = 11$$

In this case  $r = \frac{1}{2}(p-1) = 5$ . Since  $11 \equiv 3 \pmod{4}$  we have, by Proposition (2.2.5),

$$(2.5.1) \quad W := 2V_{11,1} = 1 + 2 \sum_{m,n \geq 1} \binom{n}{11} q^{nm} \in M_1(11, \chi_{11}).$$

Hence

$$W^5 \in M_5(11, \chi_{11}).$$

If we define

$$(2.5.2) \quad V := 11V_{11,5} = 1275 + 11 \sum_{m,n \geq 1} \binom{n}{11} n^4 q^{nm}$$

and

$$(2.5.3) \quad U := U_{11,5} = \sum_{m,n \geq 1} \binom{n}{11} m^4 q^{nm},$$

then some combination of  $U$ ,  $V$  and  $W^5$  is a cusp form. We find

$$(2.5.4) \quad C := 11^3 U + V - 1275 W^5 \in S_5(11, \chi_{11}).$$

$$p = 13$$

In this case  $\frac{1}{2}(p-1) = 6$  so that  $r = 2$  or  $3$ .

*Case (i).*  $r = 3$ . We consider the character  $\chi_{13,3}$ , which is defined in (2.1.9) and has the property  $\chi_{13,3}^3 = \chi_{13} = \left(\frac{\cdot}{13}\right)$ . Let  $\omega = \exp(\pi i/3)$ . More explicitly we may define  $\chi_{13,3}$  by  $\chi_{13,3}(2) = \omega$ , since 2 is a primitive root modulo 13.

**Lemma (2.5.5).** *If  $\chi = \chi_{13,3}$  then*

- (i)  $\dim S_2(13, \chi) = 1$ ,
- (ii)  $C(\tau) := U_{\chi,2}[1 + (3 + 2\omega)\eta^2(13\tau)/\eta^2(\tau)]^{-1}$  is a cusp form with coefficient set in  $\mathbb{Z}[\omega]$ .

*Proof.* (i) follows from [C-O, Thm 1]. We provide a more elementary proof for fun. By Proposition (2.4.13), there is a good basis for  $S_6(13, \chi_{13})$  given by

$$(2.5.6) \quad B_j := \eta^{13-2j}(\tau)\eta^{2j-1}(13\tau) \quad (1 \leq j \leq 6).$$

Now suppose  $\dim S_2(13, \chi) > 1$ , then there is a cusp form  $F$  with  $q$ -expansion

$$F(\tau) = q^\nu + \dots$$

with  $\nu \geq 2$ . But  $F^3 \in S_6(13, \chi_{13})$  so that

$$F^3(\tau) = cB_6 = c\eta(\tau)\eta^{11}(13\tau)$$

for some constant  $c \neq 0$ . By (2.2.8) we have

$$[\tau^{-2}F(-1/13\tau)]^3 = c\sqrt{13}\eta(13\tau)\eta^{11}(\tau) = c\sqrt{13}q + \dots$$

This is impossible since  $\tau^{-2}F(-1/13\tau) \in S_2(13, \bar{\chi})$  by [Kob, Ex.15 p.145]. Hence,  $\dim S_2(13, \chi) \leq 1$  so we need only construct a nonzero cusp form.

By Proposition (2.2.5) and (2.2.8) we have

$$(2.5.7) \quad \begin{aligned} C(\tau) &:= \frac{13}{6 + 18\omega} \left\{ -A_{\chi,2} \frac{\eta^2(\tau)}{\eta^2(13\tau)} U_{\chi,2} + V_{\chi,2} \right\} \in S_2(13, \chi). \\ &= q - (1 + \omega)q^2 + 2(\omega - 1)q^3 + \omega q^4 + (1 - 2\omega)q^5 + 2(2 - \omega)q^6 + \dots \end{aligned}$$

Hence  $\dim S_2(13, \chi) = 1$  and  $C$  provides a basis. It appears that the coefficient set of  $C$  is in  $\mathbb{Z}[\omega]$ . To show this we find another representation for  $C$ . Clearly,  $C(\tau)\eta^2(13\tau)/\eta^2(\tau) \in M_2(13, \chi)$  and since  $\dim M_2(13, \chi) = 3$  we find

$$(3 + 2\omega)C(\tau) \frac{\eta^2(13\tau)}{\eta^2(\tau)} = U_{\chi,2} - C(\tau).$$

Hence

$$(2.5.8) \quad C(\tau) = U_{\chi,2} \left[ 1 + (3 + 2\omega) \frac{\eta^2(13\tau)}{\eta^2(\tau)} \right]^{-1},$$

which implies the coefficient set of  $C$  is in  $\mathbb{Z}[\omega]$ .  $\square$

*Case (ii).*  $r = 2$ . We consider the character  $\chi$  modulo 13 defined by  $\chi(2) = i$ , so that  $\chi^2 = \chi_{13} = \left(\frac{\cdot}{13}\right)$ . In the notation of (2.1.9)  $\chi = \chi_{13,2}$ .

**Lemma (2.5.9).** *If  $\chi = \chi_{13,2}$  then*

$$(2.5.10) \quad D(\tau) := \frac{1+i}{2} \left\{ (27+60i) \frac{\eta^2(\tau)}{\eta^2(13\tau)} U_{\chi,3} + 13V_{\chi,3} \right\} \in S_3(13, \chi)$$

and the coefficient set of  $D$  is in  $\mathbb{Z}[i]$ .

*Proof.* Noting that

$$A_{\chi,3} = - \left( \frac{27+60i}{13} \right),$$

the proof of (2.5.10) is analogous to that of (2.5.7) in the proof of Lemma (2.5.5). We show that the coefficient set is in  $\mathbb{Z}[i]$ . We define

$$D_1(\tau) := \left( \frac{2}{1+i} \right) D(\tau),$$

so that the coefficient set of  $D_1$  is in  $\mathbb{Z}[i]$ . A MAPLE calculation gives

$$(2.5.11) \quad D_1^2 = (2058i - 21560) B_2 + (66374i - 208852) B_3 \\ + (352600i - 761288) B_4 + (699296i - 1048944) B_5.$$

Hence in  $\mathbb{Z}[i]$  we have

$$D_1^2 \equiv \sum_{n \geq 1} d_n^2 q^{2n} \equiv 0 \pmod{2},$$

where  $D_1(\tau) = \sum_{n \geq 1} d_n q^n$ . Now for each  $n$ ,  $d_n = a_n + b_n i$  for some  $a_n, b_n \in \mathbb{Z}$ . We know  $d_n^2 \equiv 0 \pmod{2}$  which implies  $a_n \equiv b_n \pmod{2}$  so that  $\frac{1}{2}(1+i)d_n \in \mathbb{Z}[i]$  and the coefficient set of  $D$  is in  $\mathbb{Z}[i]$ .  $\square$

In this case  $\frac{1}{2}(p-1) = 8$ . We consider  $r = 8$  in view of the congruences (1.11) and (1.12). We consider the character  $\chi$  modulo 17 defined by  $\chi(3) = \omega_8 := \exp(\pi i/8)$ , so that  $\chi^8 = \chi_{17} = \left(\frac{\cdot}{17}\right)$ . In the notation of (2.1.9)  $\chi = \chi_{17,8}$ . It can be shown that  $\dim S_1(17, \chi) = 0$  so we can only consider Eisenstein series. By applying Proposition (2.2.5), we find

$$(2.5.12) \quad W := \frac{V_{\chi,1}}{A_{\chi,1}} = 1 + (\omega_8^2 - \omega_8^3 + \omega_8^5 - \omega_8^7) \sum_{m,n \geq 1} \chi(n) q^{nm} \in M_1(17, \chi).$$

Hence

$$W^8 \in M_8(17, \chi_8).$$

The coefficient set of  $W^8$  is in  $\mathbb{Z}[\omega_8]$ . However, it seems that all coefficients except the coefficient of  $q^0$  are even. Instead we consider

$$(2.5.13) \quad Y := \frac{W^8}{(1 - \omega_8)}.$$

Since

$$(2.5.14) \quad (\omega_8^2 - \omega_8^3 + \omega_8^5 - \omega_8^7) = (1 - \omega_8)(\omega_8^2 + \omega_8^5 + \omega_8^6)$$

it follows that, except for the first term, the coefficient set of  $Y$  is in  $\mathbb{Z}[\omega_8]$ . To simplify calculations we will construct an element of  $M_8(17, \chi_{17})$  from  $Y$  whose coefficient set lies in  $\mathbb{Z}$  except for the first term.

Let  $\text{Frob} := \text{Gal}(\mathbb{Q}[\omega_8]/\mathbb{Q})$ . Every element  $\alpha$  of  $\mathbb{Q}[\omega_8]$  can be uniquely written

$$\alpha = a_0 + a_1\omega_8 + \cdots + a_7\omega_8^7 \quad (a_i \in \mathbb{Q}).$$

We define a  $\mathbb{Q}$ -linear map  $\text{CT} : \mathbb{Q}[\omega_8] \rightarrow \mathbb{Q}$  by  $\text{CT}(\alpha) = a_0$ .  $\text{CT}$  stands for ‘‘constant term’’. Then

$$\text{CT}(\alpha) = \frac{1}{8} \sum_{\rho \in \text{Frob}} \alpha^\rho.$$

For  $\rho \in \text{Frob}$  we define  $W^\rho := \sum_{n \geq 0} a_n^\rho q^n$  where  $W = \sum_{n \geq 0} a_n q^n$ . It is clear that  $W^\rho \in M_1(17, \chi^\rho)$  and  $(\chi^\rho)^8 = \chi_{17} = \left(\frac{\cdot}{17}\right)$ . Hence

$$(2.5.15) \quad Z := \text{CT}(Y) = \text{CT}(W^8/(1 - \omega_8)) = \frac{1}{8} \sum_{\rho \in \text{Frob}} \frac{(W^8)^\rho}{(1 - \omega_8)^\rho} \in M_8(17, \chi_{17}).$$

Via MAPLE, we have

$$(2.5.16) \quad \begin{aligned} Z = & \frac{1}{2} + 8q^2 + 112q^3 - 552q^4 + 1344q^5 - 4108q^6 + 4104q^7 \\ & - 12577q^8 + 12544q^9 - 27536q^{10} - 39912q^{11} - 16730q^{12} \\ & - 112264q^{13} - 327000q^{14} - 493408q^{15} - 667184q^{16} - 937824q^{17} \\ & - 1361376q^{18} - 1649208q^{19} - 2705028q^{20} + \dots \end{aligned}$$

Some combination of  $U_{17,8}$ ,  $V_{17,8}$  and  $Z$  is a cusp form. We find

$$(2.5.17) \quad C := 262387 U_{17,8}/2 - 17 V_{17,8}/2 + 59901794 Z \in S_8(17, \chi_{17}).$$

Since the coefficients of  $Z$  are difficult to compute we express  $C$  as a combination of our basis  $\{B_1, B_2, \dots, B_{10}\}$  for  $S_8(17, \chi_{17})$ . A MAPLE calculation gives

$$(2.5.18) \quad \begin{aligned} C = & 131185 B_1 + 495087737 B_2 + 4024494968 B_3 - 52619639118 B_4 \\ & + 389220577648 B_5 - 2898533428798 B_6 + 6549413846776 B_7 \\ & - 39849989479818 B_8 + 31228607702837 B_9 - 169818268113767 B_{10}. \end{aligned}$$

$$p = 19$$

In this case  $\frac{1}{2}(p-1) = 9$  and  $r = 3$ . From Proposition (2.2.9) (or Table II, §2.2), we find two cubes in  $S_9(19, \chi_{19})$ :

$$(2.5.19) \quad [\eta(19\tau)\eta^5(\tau)]^3 = q^3 + \dots$$

and

$$(2.5.20) \quad [\eta(\tau)\eta^5(19\tau)]^3 = q^{12} + \dots$$

$$p = 23$$

In this case  $r = \frac{1}{2}(p-1) = 11$ . From Proposition (2.2.9) (or Table II §2.2), we find an 11-th power in  $S_{11}(23, \chi_{23})$ :

$$(2.5.21) \quad [\eta(\tau)\eta(23\tau)]^{11} = q^{11} + \dots$$

### 3. The Congruences

In this section we prove our main result (1.10) as well as (1.12). The proof of (1.11), the stronger congruence for  $p = 17$  is delayed until §4. We distinguish three cases.

$$p = 5, 7, 19, 23$$

Let  $r$  be a prime divisor of  $\frac{1}{2}(p-1)$ . In this first case  $\epsilon_p = -1$  and our goal is to prove

$$(3.1) \quad a_p(n - \delta_p) \equiv 0 \pmod{r} \quad \text{if} \quad \left(\frac{n}{p}\right) = -1 \quad \text{and} \quad n \not\equiv 0 \pmod{r},$$

$$\text{i.e.} \quad \Phi_r \circ \Psi_-(X_p) \equiv 0 \pmod{r}.$$

We recall from Corollary (2.2.12) that

$$(3.2) \quad C := c_p X_p - U_{p, \frac{1}{2}(p-1)} \in S_{\frac{1}{2}(p-1)}(p, \chi_p),$$

where  $c_p$  is some positive integer (given explicitly in Table I, §2.2). We observe that in this case we have

$$(3.3a) \quad \gcd(c_p, r) = 1,$$

$$(3.3b) \quad (r-1) \mid \left(\frac{1}{2}(p-1) - 1\right).$$

Hence, from Lemma (2.3.23), we have

$$(3.4) \quad \Phi_r \circ \Psi_-(U_{p, \frac{1}{2}(p-1)}) \equiv 0 \pmod{r}.$$

We need the existence of a special basis for  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$  which follows easily from Corollary (2.4.14) and the construction of our  $r$ -th powers from §2.5.

**Proposition (3.5).** *Suppose  $p = 7, 19, 23$ ,  $d := \dim S_{\frac{1}{2}(p-1)}(p, \chi_p)$ , and  $r$  is a prime divisor of  $\frac{1}{2}(p-1)$ . There is a good basis  $\mathcal{D} = \{D_1, D_2, \dots, D_d\}$  with the following properties:*

For  $1 \leq i \leq d$

- (i)  $D_i = q^i + \dots$ ,
- (ii) If  $\left(\frac{i}{p}\right) = 1$  then  $D_i \in S_{\frac{1}{2}(p-1), p}^+$ ,
- (iii) If  $\left(\frac{i}{p}\right) = -1$  and  $i \not\equiv 0 \pmod{r}$  then  $D_i \in S_{\frac{1}{2}(p-1), p}^-$ ,
- (iv) If  $\left(\frac{i}{p}\right) = -1$  and  $i \equiv 0 \pmod{r}$  then  $\Phi_r(D_i) \equiv 0 \pmod{r}$ .

*Proof.* Let  $\mathcal{C} = \{C_1, C_2, \dots, C_d\}$  be the good basis of Corollary (2.4.14). When  $p = 7$ ,  $d = 1$  and we take

$$D_1 = C_1 = \eta^3(\tau)\eta^3(7\tau).$$

For  $p = 19$ ,  $d = 13$  and  $r = 3$ . If  $1 \leq i \leq 13$ ,  $\left(\frac{i}{19}\right) = 1$  or  $i \not\equiv 0 \pmod{3}$  we take  $D_i := C_i$ . Otherwise,  $i = 3$  or  $12$ . In this case we use our cubes (2.5.19), (2.5.20):

$$\begin{aligned} D_3 &:= [\eta(19\tau)\eta^5(\tau)]^3, \\ D_{12} &:= [\eta(\tau)\eta^5(19\tau)]^3. \end{aligned}$$

These clearly satisfy (iv).

The case  $p = 23$  is similar. Here  $d = 19$  and  $r = 11$ . If  $1 \leq i \leq 19$  and  $i \neq 11$  we take  $D_i := C_i$ . Otherwise, we use our 11-th power (2.5.21):

$$D_{11} := [\eta(\tau)\eta(23\tau)]^{11},$$

which satisfies (iv).  $\square$

We now complete the proof of (3.1). Now

$$(3.6) \quad C := c_p X_p - U_{p, \frac{1}{2}(p-1)} = \sum_{i=1}^d \alpha_i D_i$$

for some  $\alpha_i \in \mathbb{Z}$ . We note that in the case  $p = 5$  we interpret this to say  $C = 0$  since  $d = 0$ . Since  $\nu_\infty(X_p) = \delta_p > d$  and (3.4) holds we have (by Proposition (3.5))

$$(3.7) \quad \alpha_i \equiv 0 \pmod{r} \quad \text{if} \quad \left(\frac{i}{p}\right) = -1 \quad \text{and} \quad i \not\equiv 0 \pmod{r}.$$

Hence, since  $\Psi_-$  annihilates  $S^+$ , we have

$$\Phi_r \circ \Psi_-(C) \equiv 0 \pmod{r}.$$

Now (3.3a) and (3.4) imply

$$\Phi_r \circ \Psi_-(X_p) \equiv 0 \pmod{r},$$

which is our result (3.1).

$$p = 13$$

In this case  $r = 2$  or  $3$  and  $\epsilon_p = 1$ . Our goal is to prove

(3.8a)

$$a_{13}(n-7) \equiv 0 \pmod{2} \quad \text{if } \left(\frac{n}{13}\right) = 1 \quad \text{and } n \text{ is odd,}$$

(3.8b)

$$a_{13}(n-7) \equiv 0 \pmod{3} \quad \text{if } \left(\frac{n}{13}\right) = 1 \quad \text{and } n \not\equiv 0 \pmod{3};$$

i.e.  $\Phi_r \circ \Psi_+(X_{13}) \equiv 0 \pmod{r}$  for  $r = 2$  or  $3$ .

Recall, by Proposition (2.4.13), that the

$$B_j := \eta^{13-2j}(\tau)\eta^{2j-1}(13\tau) \quad (1 \leq j \leq 6)$$

provide a good basis for  $S_6(13, \chi_{13})$ . Let  $C$  be as in Lemma (2.5.5). Then  $C^3 \in S_6(13, \chi_{13})$  and a calculation shows that

$$(3.9) \quad C^3 = B_3 + (4 - 3\omega)B_4.$$

It follows that

$$(3.10) \quad X_{13} + B_6 = \frac{\eta^6(13\tau)}{\eta^6(\tau)}(B_3 + B_4) \equiv \left[ \frac{\eta^2(13\tau)}{\eta^2(\tau)} C(\tau) \right]^3 \pmod{3}.$$

Hence, since the coefficient set of  $C$  is in  $\mathbb{Z}[\omega]$ , we have

$$(3.11) \quad \Phi_3(X_{13}) + \Phi_3(B_6) \equiv 0 \pmod{3}.$$

Since  $\nu_\infty(B_6) = \dim S_6(13, \chi_{13}) = 6$  we have

$$(3.12) \quad \Psi_+(B_6) = 0, \quad (\text{by Proposition (2.3.16)})$$

which together with (3.11) and the fact that the operators  $\Phi_3$  and  $\Psi_+$  commute yields the result (3.8b). We note that an elementary proof of (3.12) may be obtained using Jacobi's identity for  $\eta^3(\tau)$  ([H-W, Thm 357]).

The proof of (3.8a) is analogous. Let  $D$  be as in Lemma (2.5.9). Then  $D^2 \in S_6(13, \chi_{13})$ . A calculation shows

$$(3.13) \quad \begin{aligned} -D^2 = & (1029 + 10780i) B_2 + (33187 + 104426i) B_3 \\ & + (176300 + 380644i) B_4 + (349648 + 524472i) B_5, \end{aligned}$$

so that

$$(3.14) \quad D^2 \equiv B_2 + B_3 \pmod{2}.$$

But

$$(3.15) \quad X_{13} + B_6 = \frac{\eta^8(13\tau)}{\eta^8(\tau)}(B_2 + B_3) \equiv \left[ \frac{\eta^4(13\tau)}{\eta^4(\tau)} D(\tau) \right]^2 \pmod{2},$$

so that

$$(3.16) \quad \Phi_2(X_{13}) + \Phi_2(B_6) \equiv 0 \pmod{2},$$

and the result (3.8a) follows from (3.12). It is interesting to note that (3.11) and (3.16) combine to give the following result.

**Curious Result.** *If*

$$\sum_{n \geq 0} b_n q^n = \prod_{m=1}^{\infty} \frac{(1 - q^m)}{(1 - q^{13m})} + q \prod_{m=1}^{\infty} \frac{(1 - q^{13m})}{(1 - q^m)},$$

and  $r = 2$  or  $3$  then

$$b_n \equiv 0 \pmod{r} \quad \text{if } n \not\equiv 0 \pmod{r}.$$

$$p = 11, 17$$

For  $p = 11$ ,  $r = 5$  and  $\epsilon_p = 1$ , and our goal is to prove

$$(3.17) \quad a_{11}(n - 5) \equiv 0 \pmod{5} \quad \text{if } \left( \frac{n}{11} \right) = 1 \quad \text{and } n \not\equiv 0 \pmod{5}.$$

We first observed (3.17) in [Ga-K-S, Thm 8, p.16] where the proof was omitted. Here we provide the details. We also give a proof of the  $p = 11$  case of (1.10) which was omitted from [Ga-K-S].

For the case  $p = 17$  we have  $r = 4$  and  $\epsilon_p = -1$ , and our goal is the proof of (1.12) which is a stronger version of (1.10) and which we restate below.

$$(3.18) \quad a_{17}(n - 12) \equiv 0 \pmod{2} \quad \text{if } \left( \frac{n}{17} \right) = -1 \quad \text{and } n \not\equiv 0 \pmod{4}.$$

We delay the proof of (1.11) until §4. Our proofs of (3.17) and (3.18) are similar and involve Hecke operators.

In both cases we consider an Eisenstein series  $W \in M_1(p, \chi)$  where  $\chi^{(p-1)/2} = \chi_p = \left(\frac{\cdot}{p}\right)$  for some Dirichlet character  $\chi$ , so that  $W^{(p-1)/2} \in M_{\frac{1}{2}(p-1)}(p, \chi_p)$ . For the case  $p = 11$  we take  $Z := W^5$ . To simplify computations for the  $p = 17$  case we take  $Z := \text{CT}(W^8/(1 - \omega_8))$  instead of  $W^8$ . The details of this construction are given in §2.5. Now let

$$(3.19) \quad d_\epsilon := \dim S_{\frac{1}{2}(p-1), p}^{\epsilon_p},$$

$$(3.20) \quad d := \dim S_{\frac{1}{2}(p-1)}(p, \chi_p).$$

We can easily calculate  $d_\epsilon$  using Corollary (2.4.14).

$p$	$\epsilon_p$	$d_\epsilon$	$d$
11	1	2	3
17	-1	5	10

We build a cusp form  $C$  out of  $Z$  (see (2.5.4) and (2.5.17)). Now we use Hecke operators  $T_p$  (with  $\gcd(p, r) = 1$ ) to build a subspace  $S'$  of  $S_{\frac{1}{2}(p-1)}(p, \chi_p)$  so that

$$(3.21) \quad S_{\frac{1}{2}(p-1)}(p, \chi_p) = S' \oplus S_{\frac{1}{2}(p-1), p}^{-\epsilon_p}.$$

We describe  $S'$  in terms of a basis  $\mathcal{C}$ . For  $p = 11$  we take  $\mathcal{C} := \{C, T_2(C)\}$ . For  $p = 17$  we take  $\mathcal{C} := \{C, T_3(C), T_5(C), T_7(C), T_{11}(C)\}$ . In each case we need to show that  $\mathcal{C}$  is linearly independent and that the  $S'$  that  $\mathcal{C}$  generates satisfies  $S' \cap S_{\frac{1}{2}(p-1), p}^{-\epsilon_p} = \{0\}$ . This can be done by showing the  $\Psi_{\epsilon_p}(\mathcal{C})$  is linearly independent. For  $p = 11$  this could (in principle) be done by hand. We give some details. We find

$$(3.22) \quad C = 16(-713q - 1950q^2 - 1091q^3 + 292q^4 + 3737q^5 + 5850q^6 + \dots),$$

and

$$(3.23) \quad T_2(C) = 2^5 \cdot 3 \cdot 5^2 \cdot 13(-q + 6q^2 + 3q^3 + 14q^4 + \dots).$$

Hence

$$(3.24) \quad \Psi_+(C) = -16(713q + 1091q^3 + \dots),$$

$$(3.25) \quad \Psi_+(T_2(C)) = 2^5 \cdot 3 \cdot 5^2 \cdot 13(-q + 3q^3 + \dots),$$

which are clearly linearly independent. Since  $\Psi_+$  annihilates  $S_{5,11}^-$ ,  $\Psi_+(X_{11})$  is some linear combination of  $\Psi_+(U_{11,5})$ ,  $\Psi_+(Z)$ , and  $\Psi_+(T_2(Z))$ , by (3.21) and Lemmas (2.3.17) and (2.3.19). With the help of MAPLE we find

$$(3.26) \quad 15808 \Psi_+(X_{11}) = -26 \Psi_+(Z) + 9 \Psi_+(T_2(Z)) - 100 \Psi_+(U_{11,5}),$$

and our result (3.17) follows by Lemma (2.3.22). We have checked the identity (3.26) to order  $O(q^{100})$ .

We now include the proof of the  $p = 11$  case of (1.10) since its proof also involves Hecke operators. By Corollary (2.2.12), we have

$$(3.27) \quad F := 1275 X_{11} - U_{11,5} \in S_5(11, \chi_{11}).$$

Since  $\dim S_5(11, \chi_{11}) = 3$  it can be shown that  $\{F, T_2(F), T_3(F)\}$  forms a basis of cusp forms. We find

$$(3.28) \quad T_{11}(F) = 11(T_3 - 2T_2 + 4)(F).$$

Since the Hecke operators commute we have

$$(3.29) \quad T_{11}^\alpha(F) = 11^\alpha(T_3 - 2T_2 + 4)^\alpha(F)$$

and

$$(3.30) \quad T_{11}^\alpha(F) \equiv 0 \pmod{11^\alpha}.$$

From Lemma (2.3.17) we have

$$(3.31) \quad T_{11}^\alpha(U_{11,5}) \equiv 0 \pmod{11^{4\alpha}}$$

and the result follows.

The proof of the case  $p = 17$  with  $r = 4$  is analogous. Now the problem of verifying that  $\Psi_-(\mathcal{C})$  is linearly independent is a tedious calculation but one that is easily performed by MAPLE. For example, in order to compute  $T_{11}(C)$  up to  $q^{10}$  it is necessary to compute  $C$  up to  $q^{110}$ . Here  $Z$  and  $C$  are defined in (2.5.15) and (2.5.17) respectively. We omit most details. The reader who wishes to carry out these calculations will find (2.5.18), the alternative expression for  $C$ , helpful. Using MAPLE we have shown that  $\Psi_-(\mathcal{C})$  is linearly independent so that, analogous to the  $p = 11$  case,  $\Psi_-(X_{11})$  is some linear combination of  $\Psi_-(U_{17,8})$ ,  $\Psi_-(Z)$ ,  $\Psi_-(T_3(Z))$ ,  $\Psi_-(T_5(Z))$ ,  $\Psi_-(T_7(Z))$ , and  $\Psi_-(T_{11}(Z))$ . We have found

this linear combination in MAPLE but since the coefficients are huge we give a version that is reduced modulo 8.

$$(3.32) \quad 2\Psi_-(X_{17}) \equiv 6\Psi_-(Z) + 2\Psi_-(T_3(Z)) + 5\Psi_-(T_5(Z)) + 5\Psi_-(T_{11}(Z)) \pmod{8}.$$

We have checked (3.32) directly to order  $O(q^{15})$  and by an indirect method to order  $O(q^{100})$ . It follows that

$$(3.33) \quad \Phi_4 \circ \Psi_-(X_{17}) \equiv 0 \pmod{2} \quad (\text{which is the desired result (3.18)}),$$

and

$$(3.34) \quad \Phi_2 \circ \Psi_-(X_{17}) \equiv 0 \pmod{4}.$$

However a stronger result than (3.34) holds, namely

$$(3.35) \quad \Phi_2 \circ \Psi_-(X_{17}) \equiv 0 \pmod{8}.$$

We attack this stronger result in the next section. The methods of this section seem inadequate.

#### 4. The Proof of (1.11)

In this section we prove

$$(4.1) \quad a_{17}(n-12) \equiv 0 \pmod{8} \quad \text{if } \left(\frac{n}{17}\right) = -1 \text{ and } n \not\equiv 0 \pmod{2}.$$

Our solution to this problem is mildly computational. It turns out that the problem can be reduced to verifying (4.1) for the first 7 values of  $n$  (i.e.  $n = 23, 27, 29, 31, 37, 39, 41$ ) and computing the first 14 coefficients of a certain modular form in  $M_8(17, \chi_{17})$ .

First we show how (4.1) is equivalent to a certain congruence (see (4.7) below) in  $S_{20}(17, \chi_{17})$ . We have

$$(4.2) \quad B(\tau) = \sum_{n \geq 29} b_n q^n := \frac{\eta^{41}(17\tau)}{\eta(\tau)} \in S_{20}(17, \chi_{17})$$

by Proposition (2.2.9). Now

$$(4.3) \quad \begin{aligned} B(\tau) &= \eta^{24}(\tau) \frac{\eta^{17}(17\tau)}{\eta(\tau)} \\ &= q^{17} \prod_{m=1}^{\infty} (1 - q^{17m})^{24} \sum_{n \geq 12} a_{17}(n-12) q^n \\ &\equiv \prod_{m=1}^{\infty} (1 - q^{34m})^{12} \sum_{n \geq 12} a_{17}(n-12) q^{n+17} \pmod{8}, \end{aligned}$$

since  $(1-x)^{24} \equiv (1-x^2)^{12} \pmod{8}$ . It follows that (4.1) is equivalent to

$$(4.4) \quad b_n \equiv 0 \pmod{8} \quad \text{if } \left(\frac{n}{17}\right) = -1 \text{ and } n \equiv 0 \pmod{2},$$

i.e.

$$(4.5) \quad b_{2n} \equiv 0 \pmod{8} \quad \text{if } \left(\frac{n}{17}\right) = -1,$$

since  $\left(\frac{2}{17}\right) = 1$ . Now we consider the Hecke operator  $T_2$  on  $S_{20}(17, \chi_{17})$ . Then

$$(4.6) \quad T_2(B) = \sum_{n \geq 15} c_n q^n \equiv \sum_{n \geq 15} b_{2n} q^n \pmod{2^{19}},$$

since  $c_n = b_{2n} + \left(\frac{n}{17}\right) 2^{19} b_{n/2}$ . Hence (4.1) is equivalent to

$$(4.7) \quad \Psi_-(T_2(B)) \equiv 0 \pmod{8}.$$

We now show the existence of certain special bases for  $S_{20,17}^+$  and  $S_{20,17}^-$  (defined in (2.3.9) and (2.3.10)). We let  $\{B_1, B_2, \dots, B_{10}\}$  be our good basis for  $S_8(17, \chi_{17})$  constructed in Proposition (2.4.13). We may complete this to a good basis  $\{B_0, B_1, \dots, B_{10}, B_{12}\}$  for  $M_8(17, \chi_{17})$  by defining

$$(4.8) \quad B_0 := \frac{\eta^{17}(\tau)}{\eta(17\tau)} = 1 + \dots,$$

$$(4.9) \quad B_{12} := X_{17} = \frac{\eta^{17}(17\tau)}{\eta(\tau)} = q^{12} + \dots$$

We note that there is no form in  $M_8(17, \chi_{17})$  with a  $q$ -expansion of the form

$$q^{11} + \dots,$$

since  $\dim M_8(17, \chi_{17}) = 10 + 2 = 12$ . It is clear from this construction that there is a modular form  $D \in M_8(17, \chi_{17})$  with integral coefficients and a  $q$ -expansion of the form

$$(4.10) \quad D = 1 + \gamma q^{11} + O(q^{13}),$$

for some  $\gamma \in \mathbb{Z}$ . Using MAPLE we have computed

$$(4.11) \quad D = 1 + 34q^{13} + 102q^{15} + 170q^{16} + \dots \quad .$$

From (4.17) and Proposition (4.19) below it follows that  $\Psi_-(D) = 0$ . As a check on our taylor expansion we have confirmed this to order  $O(q^{100})$ .

We show that there is a basis  $\mathcal{C} = \{C_1, C_2, \dots, C_{27}, C_{29}\}$  for  $S_{20}(17, \chi_{17})$  such that

$$(4.12a) \quad C_j \in \mathbb{Z}[[q]] \quad (\text{for each } j),$$

$$(4.12b) \quad C_j = q^j + \beta_j q^{28} + O(q^{30}) \quad (\text{for } 1 \leq j \leq 27 \text{ and } \beta_j \in \mathbb{Z}),$$

$$(4.12c) \quad C_{29} = q^{29} + O(q^{30}).$$

We define

$$(4.13) \quad \Delta(\tau) := \eta^{24}(\tau) = q + \dots \quad .$$

As is well-known  $\Delta \in S_{12}(\Gamma(1))$ . It follows, from [Kob, Prop. 17 p.127], that

$$(4.14) \quad \Delta_{17} := \Delta(17\tau) = q^{17} + \dots \in S_{12}(17, \chi_0).$$

In addition  $\Delta_{17}$  has no zeros in  $\mathcal{H}$ . If  $C \in S_{20}(17, \chi_{17})$  and  $\nu_\infty(C) \geq 17$  then  $\Delta_{17}^{-1}C \in M_8(17, \chi_{17})$ . It follows that there is no cusp form in  $S_{20}(17, \chi_{17})$  with  $\nu_\infty(C) = 17+11 = 28$  and that for  $C \in S_{20}(17, \chi_{17})$ ,  $C \neq 0$ , we have

$$(4.15) \quad \nu_\infty(C) \leq 29.$$

We take

$$(4.16) \quad C_{29} := B = \frac{\eta^{41}(17\tau)}{\eta(\tau)},$$

$$(4.17) \quad C_{17} := \Delta_{17}D,$$

where  $D$  is the form in  $M_8(17, \chi_{17})$  described before so that

$$(4.18) \quad C_{17} = q^{17} + 34q^{30} + 102q^{32} + 170q^{33} + \dots \quad .$$

We next construct  $C'_i \in S_{20}(17, \chi_{17})$ ,  $1 \leq i \leq 27$   $i \neq 17$ , with

$$C'_i = q^i + \dots \in \mathbb{Z}[[q]],$$

as in Proposition (2.4.13). We simply set

$$C'_i = C_{29}f_2^k f_3^\ell,$$

where  $f_2, f_3$  are given in the proof of Proposition (2.4.12) with  $p = 17$ , and  $k \geq 0, \ell \geq 0$  are chosen such that  $29 - 2k - 3\ell = i$ . Now the remaining  $C_j$  may be easily constructed from the  $C'_i, C_{17}, C_{29}$ .

We now use the twist operator  $\rho$  described in §2.3. We have

$$\rho(C_{17}) = \gamma q^{17} + 34q^{30} + \dots,$$

for some  $\gamma \in \mathbb{C}$ . Hence

$$\rho(C_{17}) - \gamma C_{17} = O(q^{30}) \in S_{20}(17, \chi_{17}).$$

From (4.15) it follows that

$$\rho(C_{17}) = \gamma C_{17} = C_{17}$$

and  $C_{17} \in S_{20,17}^+$ .

**Proposition (4.19).**

(a)  $\{C_j : 1 \leq j \leq 26 \text{ and } \left(\frac{j}{17}\right) = 1 \text{ or } j = 17\}$  is a basis for  $S_{20,17}^+$ .

(b) For certain constants  $\gamma_j$ ,

$$\{C_j - \gamma_j C_{17} : 3 \leq j \leq 29, j \neq 28 \text{ and } \left(\frac{j}{17}\right) = -1\} \text{ is}$$

a basis for  $S_{20,8}^-$ .

*Proof.* Suppose  $1 \leq j \leq 26$  and  $\left(\frac{j}{17}\right) = 1$ . We know

$$C_j = q^j + \beta_j q^{28} + O(q^{30})$$

for some  $\beta_j \in \mathbb{Z}$ , so that

$$\rho(C_j) = q^j + 2\gamma_j q^{17} - \beta_j q^{28} + O(q^{30})$$

for some  $\gamma_j \in \mathbb{C}$ . We have

$$\rho(C_j) - C_j - 2\gamma_j C_{17} = -2\beta_j q^{28} + O(q^{30}).$$

It follows that  $\beta_j = 0$ , and

$$\rho(C_j) = C_j + 2\gamma_j C_{17},$$

so that

$$\rho^2(C_j) = C_j + 4\gamma_j C_{17}, \quad (\text{since } C_{17} \in S_{20,17}^+).$$

But  $\rho^2(C_j) = C_j$  which means that  $\gamma_j = 0$  and  $C_j \in S_{20,17}^+$ .

Now suppose  $3 \leq j \leq 29$ ,  $j \neq 28$  and  $\binom{j}{17} = -1$ . Then

$$\rho(C_j) = -q^j + 2\gamma_j q^{17} - \beta_j q^{28} + O(q^{30})$$

for certain  $\gamma_j, \beta_j \in \mathbb{C}$ . Arguing as before we deduce

$$\rho(C_j) = -C_j + 2\gamma_j C_{17}.$$

Hence

$$\rho(C_j - \gamma_j C_{17}) = -C_j + \gamma_j C_{17},$$

so that

$$C_j - \gamma_j C_{17} \in S_{20,17}^-.$$

The result follows from (2.3.13) since  $\dim S_{20}(17, \chi_{17}) = 28$ .  $\square$

We need to verify (4.1) for  $n \leq 41$  (i.e.  $n = 23, 27, 29, 31, 37, 39, 41$ ). Via MAPLE we have

$$\begin{aligned} (4.20) \quad X_{17} &:= q^{12} + q^{13} + 2q^{14} + 3q^{15} + 5q^{16} + 7q^{17} + 11q^{18} + 15q^{19} + 22q^{20} + 30q^{21} \\ &\quad + 42q^{22} + 56q^{23} + 77q^{24} + 101q^{25} + 135q^{26} + 176q^{27} + 231q^{28} + 280q^{29} \\ &\quad + 368q^{30} + 456q^{31} + 576q^{32} + 707q^{33} + 883q^{34} + 1068q^{35} + 1320q^{36} \\ &\quad + 1584q^{37} + 1926q^{38} + 2296q^{39} + 2766q^{40} + 3256q^{41} + 3887q^{42} \\ &\quad + 4547q^{43} + 5357q^{44} + 6216q^{45} + 7380q^{46} + \dots \\ &\equiv q^{12} + q^{13} + 2q^{14} + 3q^{15} + 5q^{16} + 7q^{17} + 3q^{18} + 7q^{19} + 6q^{20} + 6q^{21} \\ &\quad + 2q^{22} + 5q^{24} + 5q^{25} + 7q^{26} + 7q^{28} + 3q^{33} + 3q^{34} + 4q^{35} \\ &\quad + 6q^{38} + 6q^{40} + 7q^{42} + 3q^{43} + 5q^{44} + 4q^{46} + \dots \pmod{8}. \end{aligned}$$

We complete the proof of (4.7). Since  $\mathcal{C}$  is a basis that satisfies (4.12), there are  $\alpha_j \in \mathbb{Z}$  such that

$$(4.21) \quad T_2(B) = \sum_{\substack{j=15 \\ j \neq 28}}^{29} \alpha_j C_j.$$

By Proposition (4.19) we have

$$(4.22) \quad \Psi_-(T_2(B)) = \sum_{\substack{j=20 \\ \binom{j}{17}=-1 \\ j \neq 28}}^{29} \alpha_j \Psi_-(C_j).$$

Let  $20 \leq j \leq 29$ ,  $\binom{j}{17} = -1$  and  $j \neq 28$ . From (4.3), (4.6), (4.12) and (4.20) it follows that  $\alpha_j \equiv 0 \pmod{8}$  and we have (4.7) as required.  $\square$

### 5. Further results

There are some congruences for  $b_p(n)$ , defined in (1.13), due to Morris Newman. If  $n$  is a nonnegative integer, define  $p_s(n)$  as the coefficient of  $q^n$  in

$$(5.1) \quad \prod_{n=1}^{\infty} (1 - q^n)^s;$$

otherwise define  $p_s(n)$  as 0. Newman [N1], [N2] has shown the following result:

Suppose that  $s$  is even,  $0 < s \leq 24$ . Let  $r$  be a prime such that  $\delta := s(r-1)/24$  is an integer. Then for all integral  $n$

$$(5.2) \quad p_s(rn + \delta) = p_s(n)p_s(\delta) - r^{\frac{1}{2}s-1}p_s((n-\delta)/r).$$

For  $p$  prime we have  $b_p(n) \equiv p_{p-1}(n) \pmod{p}$ . Hence we have the following result:

Suppose  $p$  is prime,  $3 \leq p \leq 23$ . Let  $r$  be a prime such that  $\theta := (p-1)(r-1)/24$  is an integer. Then for all integral  $n$

$$(5.3) \quad b_p(rn + \theta) \equiv b_p(n)b_p(\theta) - r^{(p-3)/2}b_p((n-\theta)/r) \pmod{p}.$$

A nice instance is when  $p = r = 13$ .

$$(5.4) \quad b_{13}(13n + 6) \equiv 11b_{13}(n) \pmod{13}.$$

We have found a weak analog of (5.3) for  $a_p(n)$ . It seems that the following holds:

Suppose  $p$  is prime with  $5 \leq p \leq 23$ , and let  $r$  be any prime. Then for all integral  $n$

$$(5.5) \quad a_p(prn - \delta_p) + \delta_p a_p(pr - \delta_p) a_p(pn - \delta_p) + r^{(p-2)} a_p(p(n/r) - \delta_p) \equiv 0 \pmod{p}.$$

We note that for  $5 \leq p \leq 11$  (5.5) follows trivially from (1.6)–(1.8). Although we have not carried out the details, it would seem likely that  $T_p(X_p)$  is congruent to a Hecke eigenform modulo  $p$ . A nice consequence of (5.5) is

For  $p$  prime,  $5 \leq p \leq 23$  and all integral  $n$

$$(5.6) \quad a_p(p^2n - \delta_p) \equiv -\delta_p a_p(p^2 - \delta_p) a_p(pn - \delta_p) \pmod{p}.$$

#### *Acknowledgments*

I would like to thank the following for helpful discussions: Oliver Atkin, Winfried Kohnen, Morris Newman, J.B. Olsson and S.S. Rangachari.

#### **References**

- [An-O] G.E. Andrews and J.B. Olsson, Partition identities with an application to group representation theory, *J. Reine Angew. Math.* **413** (1991), 198–212.
- [At-L] A.O.L. Atkin and J. Lehner, Hecke operators on  $\Gamma_0(m)$ , *Math. Ann.* **185** (1970), 134–160.
- [At-S] A.O.L. Atkin and H.P.F. Swinnerton-Dyer, Some properties of partitions, *Proc. London Math. Soc.* (3) **4** (1954), 84–106.
- [C-O] H. Cohen and J. Oesterlé, Dimensions des espaces de formes modulaires, “Modular Functions in One Variable VI,” International Summer School of Modular Functions, Bonn 1976, Springer Lecture Notes in Math., **627**, Springer, New York, 1976, pp.69–78.
- [F] N.J. Fine, On a system of modular functions connected with Ramanujan identities, *Tôhoku Math. J.* (2) **8** (1956), 149–164.
- [Ga-K-S] F.G. Garvan, D. Kim and D. Stanton, Cranks and  $t$ -cores, *Inventiones math.* **101** (1990), 1–17.
- [Go] B. Gordon, private communication.
- [H-W] G.H. Hardy and E.M. Wright, “An Introduction to the Theory of Numbers,” Oxford Univ. Press, London, 1979.
- [Ka] N. Katz, An overview of Deligne’s proof of the Riemann hypothesis for varieties over finite fields, *Amer. Math. Soc. Proc. Symp. Pure Math.* **28** (1976), 275–305.
- [Kl] A.A. Klyachko, Modular forms and representations of symmetric groups, *J. Soviet Math.* **26** (1984), 1879–1887.
- [Kob] N. Koblitz, “Introduction to Elliptic Curves and Modular Forms,” Springer, New York, 1984.

- [**Kol1**] O. Kolberg, Congruences involving the partition function for the moduli 17, 19 and 23, *Universitet i Bergen Årbok, Naturvitenskapelig rekke*, Nr.15, 1959.
- [**Kol2**] O. Kolberg, Congruences for the coefficients of the modular invariant  $j(\tau)$ , *Math. Scand.* **10** (1962), 173–181.
- [**Kol3**] O. Kolberg, Note on the Eisenstein series of  $\Gamma_0(p)$ , *Årbok for Universitet i Bergen Mat.-Naturv. Series*, No.6, 1968.
- [**N1**] Morris Newman, Remarks on some modular identities, *Trans. Amer. Math. Soc.* **73** (1952), 313–320.
- [**N2**] Morris Newman, The coefficients of certain infinite products, *Proc. Amer. Math. Soc.* **4** (1953), 435–439.
- [**N3**] Morris Newman, Construction and application of a class of modular functions, *Proc. London Math. Soc.* (3) **7** (1957), 334–350.
- [**N4**] Morris Newman, Construction and application of a class of modular functions (II), *Proc. London Math. Soc.* (3) **9** (1959), 373–387.
- [**N5**] Morris Newman, Weighted restricted partitions, *Acta Arithmetica* **X** (1959), 371–380.
- [**M**] I.G. Macdonald, Affine root systems and Dedekind's  $\eta$ -function, *Invent. Math.* **15** (1972), 91–143.
- [**O**] A. Ogg, Survey of modular functions of one variable, “Modular Functions in One Variable I,” Springer Lecture Notes in Math., **320**, Springer, New York, 1973, pp.1–36.
- [**Sc**] B. Schoeneberg, “Elliptic Modular Functions,” Springer, New York, 1974.
- [**Se1**] J.-P. Serre, “A Course in Arithmetic,” Springer, New York, 1973.
- [**Se2**] J.-P. Serre, Divisibilité des coefficients des formes modulaires de poids entier, *C.R. Acad. Sci. Paris* **279** (1974), série A, 679–682.
- [**Sp**] G. Springer, “Introduction to Riemann Surfaces,” Addison-Wesley, Reading, Mass., 1957.
- [**Z**] D. Zagier, Modular forms associated to real quadratic fields, *Inventiones math.* **30** (1975) 1–46.