

Extremal Modular Forms Modulo p and a Conjecture of Bannai, Koike, Shinohara and Tagami

Alper Ferudun*

October 1, 2026

Abstract

For even $k \geq 4$ let $f_k = 1 + O(q^{\dim M_k})$ be the extremal modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$. Bannai, Koike, Shinohara and Tagami conjectured that if $k = 12\mu$ and $f_k \bmod p$ is a nonconstant power series in q^p (their Case (2)), then $f_k(\tau) \equiv g(p^r \tau) \pmod{p}$ for an extremal modular form g of smaller weight and some $r \geq 1$. We observe that this is a corollary of the classical theory of modular forms modulo p : the key input is the equality $w(h^p) = pw(h)$ for the filtration of a p -th power, which follows from Swinnerton-Dyer's structure theorem and underlies the theorem of Serre and Katz on the kernel of θ . For every even $k \geq 4$ and every prime p in Case (2) we get $f_k(\tau) \equiv f_{k'}(p\tau) \pmod{p}$ with $k' = w(f_k \bmod p)/p$, where $4 \leq k' \leq k/p$ and $k' \equiv k \pmod{p-1}$. So the conjecture holds with $r = 1$, and by iteration also with the largest possible r . For $k = 12\mu$ every prime in Case (2) satisfies $11 \leq p \leq 3\mu$ and $p \neq 13$, and Case (2) is decided by a finite test. Exact computations for all weights $12\mu \leq 7200$ and all even $k \leq 2400$, covering 9433 pairs (k, p) in Case (2), agree with these statements. This is an unrefereed note.

1 Introduction

Let M_k be the space of modular forms of weight k for $\mathrm{SL}_2(\mathbb{Z})$, let $q = e^{2\pi i\tau}$, and let $a_n(F)$ be the n -th coefficient of F . For even $k \geq 4$ write $k = 12\mu + k_0$ with $k_0 \in \{0, 4, 6, 8, 10, 14\}$. Then $\dim M_k = \mu + 1$, and there is a unique $f_k \in M_k$ with $f_k = 1 + O(q^{\mu+1})$, the *extremal modular form* of weight k ; its coefficients are integers (Lemma 2.1). For instance $f_k = E_k$ for $k \in \{4, 6, 8, 10, 14\}$, and $f_{12} = \Theta_{\Lambda_{24}}$ is the theta series of the Leech lattice; the theta series of an extremal even unimodular lattice of rank $2k$ is f_k . Motivated by spherical designs, Bannai, Koike, Shinohara and Tagami [Ban05b, Ban05a, BKST06] studied $a_n = a_n(f_k)$ modulo a prime p and distinguished three cases: (1) $p \mid a_n$ for all $n \geq 1$; (2) $p \mid a_n$ for all $n \geq 1$ with $p \nmid n$, and $p \nmid a_j$ for some $j \geq 1$; (3) $p \nmid a_j$ for some $j \geq 1$ with $p \nmid j$. So Case (2) says that $f_k \bmod p$ is a nonconstant power series in q^p . In both printings of the extended abstract, [Ban05b, p. 13] and [Ban05a, p. 3], the first condition of Case (2) is printed as “ $p \nmid a_i$ ”. Read literally, Case (2) would be empty for $k = 12\mu$ (as $a_1 = 0$) and the conjecture below vacuous. The abstract of the journal version [BKST06] has $p \mid a_i$, which is also the only reading under which exactly one case holds for every pair (k, p) ; we use it. The authors show that Case (1) holds if and only if $(p-1) \mid k$, give sufficient conditions for Case (2), and propose the following conjecture [Ban05b, p. 14], [Ban05a, p. 4], paraphrased here.

Conjecture 1.1 (Bannai, Koike, Shinohara and Tagami). *Let $k = 12\mu$ and let p be a prime in Case (2) for f_k . (i) Then $f_k(\tau) \equiv g(p\tau) \pmod{p}$ for a modular form g of smaller weight. (ii) Moreover, there are an extremal modular form g of smaller weight and a natural number r with $f_k(\tau) \equiv g(p^r \tau) \pmod{p}$.*

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: <https://github.com/AlperTheKing>.
Unrefereed preprint. CC BY 4.0.

They report proofs in many cases, including all $\mu \leq 150$; by its abstract, the journal version [BKST06] also ends with a conjecture meant to characterize Case (2). The conjecture is record OWR-782-001 of the UnsolvedMath dataset [ula26]; record OWR-782-002 is a duplicate that asks for an extremal g already in (i). Congruences between q -series are coefficientwise, and $w(h)$ is the filtration of a modular form h modulo p , the least weight in which it occurs (Section 2).

Theorem 1.2. *Let $k \geq 4$ be even and let p be a prime in Case (2) for f_k . Then $p \geq 5$, $(p-1) \nmid k$, and $w(f_k \bmod p) = pk'$ for an even k' with $4 \leq k' \leq k/p$ and $k' \equiv k \pmod{p-1}$. Moreover $f_k(\tau) \equiv f_{k'}(p\tau) \pmod{p}$, that is, $a_{pn}(f_k) \equiv a_n(f_{k'})$ for all n and $a_n(f_k) \equiv 0$ for $p \nmid n$.*

Corollary 1.3. *Let $k \geq 4$ be even and p in Case (2) for f_k . Put $k_0 = k$ and, while p is in Case (2) for f_{k_i} , $k_{i+1} = w(f_{k_i} \bmod p)/p$. This stops after $R \geq 1$ steps, with $k = k_0 > k_1 > \dots > k_R \geq 4$, and: (a) $f_k(\tau) \equiv f_{k_i}(p^i \tau) \pmod{p}$ for $0 \leq i \leq R$; (b) p is in Case (3) for f_{k_R} ; (c) if $f_k(\tau) \equiv h(p^r \tau) \pmod{p}$ with $r \geq 1$ and $h \in \mathbb{Z}_{(p)}[[q]]$, then $r \leq R$ and $h \equiv f_{k_r} \pmod{p}$. In particular Conjecture 1.1 is true: (i) and (ii) hold with $r = 1$ and $g = f_{k_1}$; for $r \geq 1$, (ii) holds exactly when $r \leq R$, and then g is unique modulo p , namely $g \equiv f_{k_r} \pmod{p}$; for $r = R$ the form g is not a power series in q^p modulo p .*

Corollary 1.4. *Let $k \geq 4$ be even, $d = \dim M_k$ and p prime. (a) p is in Case (1) if and only if $(p-1) \mid k$ [Ban05b]. (b) If $(p-1) \nmid k$, then p is in Case (2) if and only if some even k' with $4 \leq k' \leq k/p$ and $k' \equiv k \pmod{p-1}$ satisfies $f_{k'} \equiv 1 + O(q^{\lfloor (d-1)/p \rfloor + 1}) \pmod{p}$; the least such k' is $w(f_k \bmod p)/p$. (c) In Case (2), $p \leq k/4$; if $k = 12\mu$, then $11 \leq p \leq 3\mu$ and $p \neq 13$.*

The only nonelementary input is Swinnerton-Dyer's theory of modular forms modulo p [SD73], in Serre's formulation [Ser73a]: the structure theorem and the fact that the polynomial expressing E_{p-1} in E_4, E_6 has no repeated factor modulo p . They give $w(h^p) = pw(h)$, an equality that Serre uses in [Ser73a, §2.2]. The same mechanism gives the classical theorem that forms modulo p annihilated by $\theta = qd/dq$ have filtration divisible by p (Serre [Ser73a, Ser73c] in level one, Katz [Kat77] in general; see [BKT18, §1]), and Case (2) means $\theta(f_k \bmod p) = 0$, $f_k \not\equiv 1$. So our results are corollaries of the classical theory, and specialists may regard them as an exercise; we have not found them in print (Section 4). Weights $k \not\equiv 0 \pmod{12}$ are needed for the reading of Conjecture 1.1 with the largest r , since the chain leaves the multiples of 12 (Table 1).

2 Preliminaries

Let $E_4 = 1 + 240 \sum \sigma_3(n)q^n$, $E_6 = 1 - 504 \sum \sigma_5(n)q^n$ and $\Delta = q \prod (1 - q^n)^{24} = (E_4^3 - E_6^2)/1728$, all in $\mathbb{Z}[[q]]$. For even $w \geq 0$, $w \neq 2$, fix $a, b \geq 0$ with $4a + 6b = w$ and put $E_w^* = E_4^a E_6^b$. For even $k \geq 0$ let $d_k = \dim M_k$, which is $\lfloor k/12 \rfloor$ if $k \equiv 2 \pmod{12}$ and $\lfloor k/12 \rfloor + 1$ otherwise. Then M_k has the basis $b_{k,j} = E_{k-12j}^* \Delta^j$, $0 \leq j < d_k$ [Ser73b, Ch. VII], and $b_{k,j} = q^j + O(q^{j+1})$ lies in $\mathbb{Z}[[q]]$. For $B \subset \mathbb{Q}$ put $M_k(B) = M_k \cap B[[q]]$; $\mathbb{Z}_{(p)}$ is the ring of fractions with denominator prime to p , and a bar denotes reduction modulo p . Note that $G^p = G(q^p)$ for $G \in \mathbb{F}_p[[q]]$.

Lemma 2.1. *Let $k \geq 4$ be even and $d = d_k$. (a) There are $g_{k,j} \in M_k(\mathbb{Z})$, $0 \leq j < d$, with $g_{k,j} = q^j + O(q^d)$. (b) Every $F \in M_k$ equals $\sum_{j < d} a_j(F) g_{k,j}$. Hence $f_k = g_{k,0} \in M_k(\mathbb{Z})$, and if $F \in M_k(\mathbb{Z}_{(p)})$ has $a_j(F) \equiv 0 \pmod{p}$ for all $j < d$, then $F \equiv 0 \pmod{p}$.*

Proof. (a) Put $g_{k,d-1} = b_{k,d-1}$ and, for $j = d-2, \dots, 0$, $g_{k,j} = b_{k,j} - \sum_{i > j} a_i(b_{k,j}) g_{k,i}$. (b) The form $F - \sum_{j < d} a_j(F) g_{k,j}$ is $O(q^d)$; its first nonzero coordinate c_j in the basis $(b_{k,j})$, if any, would give a term $c_j q^j$ with $j < d$. So it vanishes, and the rest is clear. $\square$

The $g_{k,j}$ form the Victor Miller basis. From now on let $p \geq 5$. Since $1728 \in \mathbb{Z}_{(p)}^\times$, Lemma 2.1 shows that $M_k(\mathbb{Z}_{(p)})$ consists of the weight- k polynomials in E_4, E_6 over $\mathbb{Z}_{(p)}$ [Ser73a, §1.2]. By von Staudt–Clausen, $E_{p-1} \in M_{p-1}(\mathbb{Z}_{(p)})$ and $E_{p-1} \equiv 1$. Let X, Y have weights 4, 6, let $S_k \subset \mathbb{F}_p[X, Y]$ be the isobaric polynomials of weight k , and let $\rho: \mathbb{F}_p[X, Y] \rightarrow \mathbb{F}_p[[q]]$ be the ring map with $\rho(X) = \bar{E}_4$, $\rho(Y) = \bar{E}_6$. Then $\widetilde{M}_k := \{\bar{F} : F \in M_k(\mathbb{Z}_{(p)})\} = \rho(S_k)$. Let $\tilde{A} \in S_{p-1}$ reduce the polynomial A with $A(E_4, E_6) = E_{p-1}$; then $\rho(\tilde{A}) = 1$ and $\widetilde{M}_k \subset \widetilde{M}_{k+p-1}$. For $0 \neq h \in \bigcup_k \widetilde{M}_k$ the filtration $w(h)$ is the least k with $h \in \widetilde{M}_k$ [Ser73a, §1.4]; $F \in S_k$ with $\rho(F) = h$ represents h in weight k .

Theorem 2.2 (Swinerton-Dyer [SD73]; see [Ser73a, §1]). *Let $p \geq 5$. (i) $\ker \rho = (\tilde{A} - 1)$ [Ser73a, Th. 1]. (ii) If $0 \neq h \in \widetilde{M}_{k_1} \cap \widetilde{M}_{k_2}$, then $k_1 \equiv k_2 \pmod{p-1}$ [Ser73a, Th. 2]. (iii) $\tilde{A}$ has no repeated irreducible factor in $\mathbb{F}_p[X, Y]$ [Ser73a, Cor. 1 to Th. 3 and Cor. 1 to Th. 5].*

Serre attributes (i) and his Th. 5 to an unpublished 1971 manuscript of Swinerton-Dyer and deduces (ii) from (i); his other proof of (iii) uses Deligne’s identification of $\tilde{A}$ with the Hasse invariant.

Lemma 2.3. *Let $p \geq 5$ and $0 \neq h \in \bigcup_k \widetilde{M}_k$. (a) ρ is injective on each S_k . (b) If $F_i \in S_{k_i}$ represent h and $k_1 \leq k_2$, then $F_2 = \tilde{A}^t F_1$ with $t = (k_2 - k_1)/(p-1) \in \mathbb{Z}$. (c) A representative $F \in S_k$ of h has $k = w(h)$ if and only if $\tilde{A} \nmid F$. (d) $w(h^p) = pw(h)$.*

Proof. Parts (a) and (c) are in [Ser73a, §§1.2, 1.4], and (d) is the argument of [Ser73a, §2.2]. (a) The d_k polynomials $E_{k-12j}^*(X, Y)((X^3 - Y^2)/1728)^j$ lie in S_k , and their images $\bar{b}_{k,j}$ are linearly independent. As the monomials of weight k give a basis of M_k [Ser73b, Ch. VII], $\dim S_k = d_k$, so these polynomials form a basis of S_k that ρ maps to an independent family. (b) $t \in \mathbb{Z}$ by Theorem 2.2(ii); $\tilde{A}^t F_1$ and F_2 lie in S_{k_2} and have the same image, so they are equal by (a). (c) If $F = \tilde{A} F'$, then F' represents h in weight $k - p + 1$. If $w(h) < k$, then (b) gives $\tilde{A} \mid F$. (d) Let F represent h in weight $w = w(h)$, so $\tilde{A} \nmid F$, and F^p represents h^p in weight pw . If $\tilde{A} \mid F^p$, every irreducible factor of $\tilde{A}$ divides F ; by Theorem 2.2(iii) they are pairwise non-associate, so $\tilde{A} \mid F$ in the factorial ring $\mathbb{F}_p[X, Y]$, a contradiction. So $w(h^p) = pw$ by (c). $\square$

3 Proofs

Lemma 3.1. *For even $k \geq 4$ and p prime, $f_k \equiv 1 \pmod{p}$ if and only if $(p-1) \mid k$.*

Proof. Let $d = d_k$. For $p \in \{2, 3\}$ we have $(p-1) \mid k$, and $E_4 \equiv E_6 \equiv 1$, as p divides 240 and 504. Write $f_k = \sum_{j < d} c_j \bar{b}_{k,j}$ with $c_j \in \mathbb{Z}$ (the basis is unitriangular); then $f_k \equiv \sum_{j < d} c_j \Delta^j$, and comparing coefficients of $q^0, \dots, q^{d-1}$ gives $c_0 \equiv 1$ and $c_j \equiv 0$ for $j \geq 1$. Let $p \geq 5$. If $(p-1) \mid k$, then $f_k - E_{p-1}^{k/(p-1)} \in M_k(\mathbb{Z}_{(p)})$ has its first d coefficients $\equiv 0$, so $f_k \equiv 1$ by Lemma 2.1(b). If $f_k \equiv 1$, then $1 \in \widetilde{M}_0 \cap \widetilde{M}_k$, so $(p-1) \mid k$ by Theorem 2.2(ii). $\square$

Lemma 3.2. *Let $k \geq 4$ be even, $p \geq 5$, $d = d_k$ and $L = \lfloor (d-1)/p \rfloor + 1$. If k' is even, $4 \leq k' \leq k/p$, $k' \equiv k \pmod{p-1}$ and $f_{k'} \equiv 1 + O(q^L) \pmod{p}$, then $f_k(\tau) \equiv f_{k'}(p\tau) \pmod{p}$.*

Proof. Here $m = (k - pk')/(p-1)$ is a nonnegative integer, as $k - pk' \equiv k - k' \equiv 0 \pmod{p-1}$. The form $H = f_{k'}^p E_{p-1}^m \in M_k(\mathbb{Z}_{(p)})$ has $\bar{H} = \bar{f}_{k'}(q^p) = 1 + O(q^{pL})$ and $pL \geq d$, so $f_k \equiv H$ by Lemma 2.1(b). $\square$

Proof of Theorem 1.2. Let $d = d_k$, $a_n = a_n(f_k)$, $\bar{f} = \bar{f}_k$ and $L = \lfloor (d-1)/p \rfloor + 1$.

Step 1. In Case (2), $\bar{f} \neq 1$, so $(p-1) \nmid k$ by Lemma 3.1, and $p \geq 5$.

Step 2. The Hecke operator T_p preserves M_k , and $a_n(T_p f_k) = a_{pn} + p^{k-1} a_{n/p}$, with $a_{n/p} = 0$ for $p \nmid n$ [Ser73b, Ch. VII]. So $G := \overline{T_p f_k} = \sum_n \bar{a}_{pn} q^n$ lies in $\widetilde{M}_k$, and $\bar{f} = G(q^p) = G^p$, as $\bar{a}_n = 0$ for $p \nmid n$. Since $\bar{f}$ is not constant, neither is G .

Step 3. Let $k' = w(G)$. As $\widetilde{M}_0 = \mathbb{F}_p$ and $\widetilde{M}_2$ and the $\widetilde{M}_k$ with odd k vanish, k' is even and $k' \geq 4$. By Lemma 2.3(d), $w(\bar{f}) = pk'$, so $pk' \leq k$; and $k' \equiv k \pmod{p-1}$ by Theorem 2.2(ii), since $G \in \widetilde{M}_{k'} \cap \widetilde{M}_k$.

Step 4. For $1 \leq n < L$ we have $pn \leq d-1$, so $a_{pn} = 0$; hence $G = 1 + O(q^L)$.

Step 5. We show $d_{k'} \leq L$. Always $d_{k'} - 1 \leq \lfloor k'/12 \rfloor \leq \lfloor k/(12p) \rfloor$. If $k \not\equiv 2 \pmod{12}$, then $\lfloor k/(12p) \rfloor = \lfloor \lfloor k/12 \rfloor / p \rfloor = L-1$. If $k = 12M+2$, then $d-1 = M-1$ and $\lfloor k/(12p) \rfloor = \lfloor M/p+1/(6p) \rfloor = \lfloor M/p \rfloor$, which is $L-1$ unless $p \mid M$. If $p \mid M$ and $d_{k'} > L$, then $d_{k'} - 1 = \lfloor k'/12 \rfloor = M/p$, so $k' \not\equiv 2 \pmod{12}$ and $12M/p \leq k' \leq (12M+2)/p < 12M/p+1$. Hence $k' = 12M/p$ and $k = pk' + 2 \equiv k' + 2 \pmod{p-1}$, and $k' \equiv k$ gives $(p-1) \mid 2$, which is absurd.

Step 6. Lifting a representative of G of weight k' to $\mathbb{Z}$ and evaluating at (E_4, E_6) gives $\hat{G} \in M_{k'}(\mathbb{Z})$ with $\hat{G} = G$. By Steps 4 and 5 its first $d_{k'}$ coefficients are $\equiv 1, 0, \dots, 0$, so $\hat{G} \equiv g_{k',0} = f_{k'}$ by Lemma 2.1(b). Thus $G = \bar{f}_{k'}$ and $\bar{f} = \bar{f}_{k'}(q^p)$. $\square$

Proof of Corollary 1.3. By Theorem 1.2, while p is in Case (2) for f_{k_i} , k_{i+1} is even with $4 \leq k_{i+1} \leq k_i/p$ and $f_{k_i}(\tau) \equiv f_{k_{i+1}}(p\tau)$. So the process stops, and (a) holds. As $\bar{f}_k = \bar{f}_{k_R}(q^{p^R})$ is not constant, p is not in Case (1) for f_{k_R} , nor, by the definition of R , in Case (2). For (c): $\bar{f}_k = \bar{h}(q^{p^r})$ lies in $\mathbb{F}_p[[q^{p^r}]]$, but $\bar{f}_k = \bar{f}_{k_R}(q^{p^R}) \notin \mathbb{F}_p[[q^{p^{R+1}}]]$ because $\bar{f}_{k_R} \notin \mathbb{F}_p[[q^p]]$. So $r \leq R$, and $\bar{h}(q^{p^r}) = \bar{f}_{k_r}(q^{p^r})$ gives $\bar{h} = \bar{f}_{k_r}$. $\square$

Proof of Corollary 1.4. (a) is Lemma 3.1. (b) If such a k' exists, Lemma 3.2 gives $f_k(\tau) \equiv f_{k'}(p\tau)$, and p is not in Case (1) by (a). Conversely, in Case (2), $k' = w(\bar{f}_k)/p$ qualifies, since $\bar{f}_{k'} = G = 1 + O(q^L)$ (Steps 4 and 6). If k'' qualifies, then $\bar{f}_k = \bar{f}_{k''}(q^p)$ by Lemma 3.2, so $G = \bar{f}_{k''} \in \widetilde{M}_{k''}$ and $k'' \geq w(G) = k'$. (c) follows from $4 \leq k' \leq k/p$ and, for $k = 12\mu$, from (a): $p-1$ divides 12 for $p = 2, 3, 5, 7, 13$. $\square$

4 Examples and remarks

k	p	chain $k_0 > k_1 > \dots > k_R$	congruence modulo p
84	11	$84 > 4$	$f_{84} \equiv E_4(q^{11})$
84	17	$84 > 4$	$f_{84} \equiv E_4(q^{17})$
96	11	$96 > 6$	$f_{96} \equiv E_6(q^{11})$
132	11	$132 > 12$	$f_{132} \equiv \Theta_{\Lambda_{24}}(q^{11})$
252	11	$252 > 12$	$f_{252} \equiv \Theta_{\Lambda_{24}}(q^{11})$
504	11	$504 > 44 > 4$	$f_{504} \equiv f_{44}(q^{11}) \equiv E_4(q^{121})$
5544	11	$5544 > 484 > 44 > 4$	$f_{5544} \equiv f_{484}(q^{11}) \equiv f_{44}(q^{121}) \equiv E_4(q^{1331})$
5544	1109	$5544 > 4$	$f_{5544} \equiv E_4(q^{1109})$

Table 1: Some pairs (k, p) in Case (2) with $12 \mid k$ and the chain of Corollary 1.3. For $(504, 11)$ and $(5544, 11)$, part (ii) of Conjecture 1.1 holds exactly for $r \leq 2$ and $r \leq 3$.

Table 1 lists examples; in our computations the least weight 12μ with a prime in Case (2) is 84. Since $k_R \geq 4$ and $k_{i+1} \leq k_i/p$, we have $k \geq 4p^R$; for $12 \mid k$ the least possible p is 11, so $R \geq 3$ needs $k \geq 5324$, and the first instance is $(5364, 11)$. Among the 4040 pairs $(12\mu, p)$ in Case (2) with $\mu \leq 600$, $R = 1, 2, 3$ occur 3306, 703 and 31 times. So the power p^r in Conjecture 1.1 is natural, although $r = 1$ always works. Only the reduction of g is determined, not g or its weight: for $(252, 11)$ both $k' = 12$ and $k' = 22$ pass the test of Corollary 1.4(b), and indeed $f_{22} \equiv f_{12} \pmod{11}$, since both lie in $\widetilde{M}_{22}$ and begin with $1 + 0 \cdot q$; for $(5544, 11)$ the weights 484, 494 and 504 pass it.

Remark 4.1 (Theorems 2 and 3 of [Ban05b, Ban05a]). This refers to the text of the extended abstract. Its Theorem 2 gives $f_k(\tau) \equiv f_{k_2}(p\tau) \pmod{p}$, where $k_2 \equiv k \pmod{p-1}$ is least with $\dim M_{k_2} \geq \lfloor (\mu+1)/p \rfloor + 1$, provided $k \geq pk_2$ (in its notation, $r_2 \geq k_2$). This is the case of Lemma 3.2 in which $f_{k_2} \equiv 1 + O(q^L)$ holds for dimension reasons. Of the 1631 pairs $(12\mu, p)$ in Case (2) with $\mu \leq 300$, 240 fail $k \geq pk_2$, the first being $(252, 11)$ with $k_2 = 32$ (Table 1); so Conjecture 1.1 did not follow from Theorem 2 alone. Its Theorem 3 says that for $k = 12\mu$ every prime $p \geq 13$ dividing $2k(2k+2)(2k+4)(2k+6)(2k+8)(2k+12)$ is in Case (2) and divides $a_{\mu+1}$. As printed, it does not exclude primes with $(p-1) \mid k$, which are in Case (1): for $k = 12$, $p = 13$ divides $2k+2$. With $(p-1) \nmid k$ added, it agrees with our computations for $\mu \leq 600$. The journal version [BKST06], which we have not seen, may contain this hypothesis.

Verification. The proofs are complete; the computations only check them.

1. The author's program `bkst_verify.py` (exact integer arithmetic) computes f_k as $E_{k_0}^* \Delta^\mu P(j)$, with j the modular invariant and P a polynomial of degree at most μ , for $k = 12\mu$, $\mu \leq 300$, and all even $k \leq 1200$; it checks this against the basis of Lemma 2.1 for $k \leq 240$ and against theta series of the Leech lattice and of extremal lattices of rank 32, 40, 48, 72. For every such k and every prime p it certifies the case of p : Case (1) by Corollary 1.4(a), Case (3) by a coefficient, Case (2) by a weight as in Corollary 1.4(b) and a nonzero coefficient; large primes are excluded by a gcd argument. It finds 1631 pairs in Case (2) with $12 \mid k$ and 2191 with $12 \nmid k$, none unresolved, and for each it checks $f_k \equiv f_{k'}(q^p)$ on all computed coefficients and $w(f_k \bmod p) = pk'$, and computes R . `spot_check.py` (elimination modulo p) and `sd_check.py` (Theorem 2.2(iii) for $5 \leq p \leq 900$) add further checks.
2. An independent verification run, which was AI-assisted, checked every step of the argument and the sources, re-ran these programs with identical results apart from timings, and wrote the separate program `indep_verify.py`. It computes f_k by expanding in $t = \Delta/E_4^3$ via $E_4 = H^4$, $E_6 = H^6(1 - 1728t)^{1/2}$, $H = {}_2F_1(\frac{1}{12}, \frac{5}{12}; 1; 1728t)$ (checked up to q^{60}), and detects Case (2) without using the results of this note: $\theta(f_k \bmod p) \in \widetilde{M}_{k+p+1}$ [Ser73a, Cor. 2 to Th. 5] vanishes if its coefficients up to $q^{\lfloor (k+p+1)/12 \rfloor}$ do (Lemma 2.1(b)). It then tests Theorem 1.2 and Corollaries 1.3 and 1.4, with filtrations computed by a separate implementation modulo p . For $\mu \leq 300$ and $k \leq 1200$ it finds the same 3822 pairs with the same k' and R ; it extends the range to $k = 12\mu$ with $\mu \leq 600$ (4040 pairs) and to even $k \leq 2400$ with $12 \nmid k$ (5393 pairs), with no failure. Its `spot_r3.py` checks $f_{5544} \equiv E_4(q^{1331}) \pmod{11}$ below q^{2700} .
3. A second independent verification run, also AI-assisted, checked the proofs, the statements cited from [Ser73a] and both printings of the extended abstract, and wrote its own programs (`independent_run_2/`). They compute f_k exactly by elimination in the basis of Lemma 2.1, with Δ from Jacobi's identity for $\prod(1 - q^n)^3$, decide the case of every prime by the θ test and a gcd argument, and compute filtrations from extremal forms alone: for $p \geq 5$ and $4 \leq w \leq k$ with $w \equiv k \pmod{p-1}$, $f_k \bmod p$ lies in $\widetilde{M}_w$ if and only if $f_w \equiv 1 + O(q^{d_k}) \pmod{p}$. For all weights $12\mu \leq 7200$, all even $k \leq 2400$ and all primes they find the same 9433 pairs in Case (2) with the same k' and R , and for each pair they confirm Theorem 1.2, including $w(f_k \bmod p) = pw(f_{k'} \bmod p)$, the chain of Corollary 1.3 and the least weight of Corollary 1.4(b). They also confirm Table 1, the counts in Remark 4.1 and Theorem 2.2(iii) for $5 \leq p \leq 1000$. This run also re-ran all programs above from the released source archive, with identical results apart from timings.
4. All programs were run again for this note, with the same results apart from timings; `paper_numbers.py` extracts the numbers quoted here from the outputs.

Scope and priority. Corollary 1.3 proves Conjecture 4 of [Ban05b, Ban05a], with Case (2) read as in Section 1, for both readings of (ii) (with $r = 1$ and with the largest r); it settles records OWR-782-001 and OWR-782-002 of [ula26]. We read the Oberwolfach printing [Ban05b] and the RIMS printing [Ban05a], which reprints the same extended abstract after a Japanese preface. We could not read the full text of the journal version [BKST06] (paywalled); by its abstract the question was open there too, but we could not compare its wording or check it for further partial results. zbMATH lists 14 documents citing [BKST06], Math-Net.Ru 16 and Semantic Scholar 26; by title and venue they concern designs, codes, Assmus–Mattson type theorems, Lehmer’s conjecture and similar topics, and none of those we read addresses Conjecture 1.1. Koike [Koi09] treats congruences modulo powers of 2 and 3 only. Searches of arXiv, Crossref, OpenAlex, zbMATH and CiNii and web searches found no proof or disproof. The argument uses only classical results and may be known to experts; we claim only that we found no written account. We read [Ser73a] and cite its numbering; we have not seen [SD73], [Ser73c] or [Kat77] and cite them for attribution, following [Ser73a, BKT18]. This negative search is not a proof of priority.

AI-assisted tools were used to search the problem corpus and the literature, to find the arguments, to write and run the verification programs, and to help prepare this manuscript. The author has reviewed the proofs, the computations and the sources and is responsible for all claims. The note has not been peer reviewed.

References

- [Ban05a] E. Bannai. Spherical designs attached to extremal lattices and the modulo p properties of the Fourier coefficients of extremal modular forms. *RIMS Kôkyûroku*, 1440:1–4, 2005. Joint work with M. Koike, M. Shinohara and M. Tagami. Japanese title and preface (English title as given there), followed by the English extended abstract, which is headed by all four authors. hdl:2433/47528.
- [Ban05b] E. Bannai. Spherical designs, extremal lattices and the Fourier coefficients modulo p of the extremal modular forms. *Oberwolfach Reports*, 2(1):12–15, 2005. Joint work with M. Koike, M. Shinohara and M. Tagami. Report 1/2005, *Gitter und Anwendungen*. doi:10.4171/OWR/2005/01.
- [BKST06] E. Bannai, M. Koike, M. Shinohara, and M. Tagami. Spherical designs attached to extremal lattices and the modulo p property of Fourier coefficients of extremal modular forms. *Moscow Mathematical Journal*, 6(2):225–264, 2006. doi:10.17323/1609-4514-2006-6-2-225-264.
- [BKT18] S. Böcherer, T. Kikuta, and S. Takemori. Weights of the mod p kernels of theta operators. *Canadian Journal of Mathematics*, 70(2):241–264, 2018. arXiv:1606.06390. doi:10.4153/CJM-2017-014-0.
- [Kat77] N. M. Katz. A result on modular forms in characteristic p . In *Modular Functions of One Variable V (Proc. Second Internat. Conf., Univ. Bonn, 1976)*, volume 601 of *Lecture Notes in Mathematics*, pages 53–61. Springer, Berlin, 1977. doi:10.1007/BFb0063944.
- [Koi09] M. Koike. Congruences between extremal modular forms and theta series of special types modulo powers of 2 and 3. *Kyushu Journal of Mathematics*, 63(1):123–132, 2009. doi:10.2206/kyushujm.63.123.
- [SD73] H. P. F. Swinnerton-Dyer. On ℓ -adic representations and congruences for coefficients of modular forms. In *Modular Functions of One Variable III (Proc. Internat. Summer School,*

- Univ. Antwerp, 1972*), volume 350 of *Lecture Notes in Mathematics*, pages 1–55. Springer, Berlin, 1973. doi:10.1007/978-3-540-37802-0_1.
- [Ser73a] J.-P. Serre. Congruences et formes modulaires [d’après H. P. F. Swinnerton-Dyer]. In *Séminaire Bourbaki, vol. 1971/72, Exposés 400–417*, volume 317 of *Lecture Notes in Mathematics*, pages 319–338. Springer, Berlin, 1973. Exposé no. 416. doi:10.1007/BFb0069289.
- [Ser73b] J.-P. Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer, New York, 1973. doi:10.1007/978-1-4684-9884-4.
- [Ser73c] J.-P. Serre. Formes modulaires et fonctions zêta p -adiques. In *Modular Functions of One Variable III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, volume 350 of *Lecture Notes in Mathematics*, pages 191–268. Springer, Berlin, 1973. doi:10.1007/978-3-540-37802-0_4.
- [ula26] ulamai. UnsolvedMath. Hugging Face dataset, <https://huggingface.co/datasets/ulamai/UnsolvedMath>, 2026. Version 1.6.0; records OWR-782-001 and OWR-782-002.