Hecke eigenvalues in level 1 modulo powers of 2 and 3: Hatada's question (1981) and the Coleman–Stein conjecture

David Niedbala Giraudin
ORCID 0009-0009-1526-1178

hexagon:2611.00035v1

Abstract

Let f be a normalized Hecke eigenform of level 1 and weight k, with eigenvalues $a_n(f)$. In 1981 Hatada asked whether $a_p(f) \equiv 1 + p \pmod{2^a}$ whenever $p \equiv \pm 1 \pmod{2^{a-1}}$ and $6 \le a \le 13$. Rustom's congruence modulo 128 answers this for $a \le 7$. We show that the answer is affirmative for $a \le 10$ and negative for $a = 11$, 12 and 13, the counterexamples coming from weight 16 and $p = 12289$. The proof combines Rustom's theorem with a certificate for T_5 modulo 512 on period polynomials, a 2-adic Galois law (for instance $a_p \equiv 1 + p^{k-1} \pmod{2^{10}}$ for every $p \equiv 1 \pmod 8$), and a reduction to a computation in a finite group. As a consequence, $a_p(f) = 0$ implies $p \equiv -1 \pmod{2^{11}}$. At the prime 3 we show that, on Hatada's lattice of period polynomials, $T_2^2 \equiv 9(k-1)^2 \pmod{27}$, with refinements modulo 81. This gives an independent proof of Conjecture 9.1 of Rustom without any ramification hypothesis and of the level 1 case of the Coleman–Stein conjecture, both of which also follow from Rustom's recent classification modulo 81. We also prove that $a_n(f) \equiv \sigma_{k-1}(n) \pmod{81}$ for every $n \equiv 1 \pmod 3$, and a 3-adic Galois law modulo 243 on the Galois group of $\mathbb{Q}(\sqrt{-3})$, which gives congruences modulo 243 and 729 for suitable split primes and a bilinear law for primes $\ell \equiv 2 \pmod 3$. Beyond 729, for every prime $\ell \equiv 2 \pmod 3$ we prove $a_\ell^2 \equiv \sigma_{k-1}(\ell)^2 \pmod{3^{\min(2j+2,10)}}$, where $j = v_3(\ell+1)$; the exponent $2j+2$ is attained for $j \le 4$ and fails for $j = 5$. Each statement is marked as proved, known, verified or open. The finite computations are certified by seven Python scripts, provided as ancillary files.

1 The question

For even k, let S_k be the space of cusp forms of weight k for $\mathrm{SL}_2(\mathbb{Z})$, and let λ_p be an eigenvalue of the Hecke operator $T_k(p)$, p an odd prime. Hatada proved that $\lambda_p \equiv 1 + p \pmod 8$ for every odd p [9], and then that

$$\lambda_p \equiv 1 + p \pmod{16} \text{ if } p \equiv \pm 1 \pmod 8, \qquad \lambda_p \equiv 1 + p \pmod{32} \text{ if } p \equiv \pm 1 \pmod{16}$$

[10, p. 305]. He then asks the following question [10, p. 306]:

> *Is it true that* $\lambda_p \equiv 1 + p \pmod{2^a}$ *if* $p \equiv \pm 1 \pmod{2^{a-1}}$ *and* $6 \le a \le 13$ *?*

together with a stronger version concerning the lattice L^-_{w+2} of forms whose odd periods are integers (stability of L^-_{w+2} under $(T_{w+2}(p) - 1 - p)/2^a$), which implies the former. In his Remark 1, Hatada points out that for $a \ge 14$ the congruence may fail when $p \equiv -1 \pmod{2^a}$, after Swinnerton-Dyer [22]. According to Rustom [17], the question was asked at Serre's suggestion. Rustom proved $\lambda_p \equiv 1 + p^{k-1} \pmod{128}$ for every odd p and every k [17, Thm 8.1], which gives the affirmative answer for $a \le 7$[1].

In residue characteristic 3, Hatada proved $\lambda_p \equiv 1 + p \pmod 3$ for $p \neq 3$, $\lambda_3 \equiv 0 \pmod 9$, and $\lambda_3 \equiv 0 \pmod{27}$ if $3 \nmid k$ [9, congruences (5) to (7)]. Coleman and Stein [6] conjectured that there are only five residue classes modulo 9 of eigenforms (levels 1, 3, 9), and checked it up to

[1] Rustom states it for $a < 7$; the case $a = 7$ follows, since $p \equiv \pm 1 \pmod{2^6}$ implies $p^2 \equiv 1 \pmod{2^7}$, hence $p^{k-1} \equiv p \pmod{2^7}$.

weight 74 in level 1. Rustom [17, Thm 9.2] states that finiteness modulo 9 in level 1 follows from the following statement.

Conjecture 9.1 of [17] (Conjecture 1.1 of [4]; Rustom writes the weight as $w+2$). *For every eigenform f of level* 1 *and weight k, one has $a_2(f) \equiv 3$ or $6 \pmod{9\overline{\mathbb{Z}}_3}$ if $k \equiv 0, 2 \pmod 6$, and $a_2(f) \equiv 0 \pmod{9\overline{\mathbb{Z}}_3}$ if $k \equiv 4 \pmod 6$.*

Chiriac [4] proved unconditionally that $a_2 \equiv 0 \pmod{9\overline{\mathbb{Z}}_3}$ implies $k \equiv 4 \pmod 6$ [4, Thm 1.2], and the whole of Conjecture 9.1 when 3 is unramified in the coefficient field [4, Cor. 1.3]; since Rustom checked this non-ramification for $k \le 1000$ [17], Conjecture 9.1 is proved for $k \le 1000$.

Related work. The recent preprint [18] of Rustom classifies, in every weight, the prime-to-p Hecke eigensystems of level 1 modulo 2^8, 3^4, 5^3 and 7^2, by Hecke-equivariant transfer maps between modular-symbol modules. At $p = 3$, [18, Thm 1.5] gives in particular the literal congruence modulo 27 of every prime-to-3 eigensystem with an Eisenstein twist; this implies Conjecture 9.1 of [17] without any ramification hypothesis, and the level 1 case of the Coleman–Stein conjecture. Our Corollary L and Theorem M were obtained independently, by a different route (explicit certificates on Hatada's lattice), and [18] has priority for these two statements. At $p = 2$, [18, Thm 1.4] is a classification modulo 2^8 in the valuative sense ($v_2(a_\ell - \alpha) > 7$); it does not address Hatada's question, and for $p \equiv \pm 1 \pmod{2^7}$ it gives the valuative form of the case $a = 8$. The congruences modulo 2^9 and 2^{10} of §8, the negative answer for $a = 11, 12, 13$, and the 3-adic results beyond 81 of §§7–9 are not covered by [18]. Earlier, Calegari and Emerton [3, Lemma 3.3] had proved $a_\ell \equiv 1 + \ell \pmod 9$ for $\ell \equiv \pm 1 \pmod 9$.

The main results of this paper are the following. We first give again (Theorem F, §4), on Hatada's lattice, his congruences $a_3(f) \equiv 0 \pmod 9$, and $\pmod{27}$ if $3 \nmid k$ [9]. Next (§5), *on Hatada's lattice,* $T_2^2 \equiv 9(k-1)^2 \pmod{27}$, and, more precisely, modulo 81, $T_2^2 \equiv \sigma_{k-1}(2)^2$ if $k \equiv 0, 2 \pmod 6$ and $T_2^2 + 9T_2 \equiv 0$ if $k \equiv 4 \pmod 6$ (Theorems I and K). It follows that Conjecture 9.1 of [17] holds for every eigenform of level 1, without any ramification hypothesis (this also follows from [18, Thm 1.5], see above), and even that $a_2(f) \equiv \pm\sigma_{k-1}(2) \pmod{27}$ when $k \equiv 0, 2 \pmod 6$ (Corollary L). Together with [17], we obtain the level 1 case of the Coleman–Stein conjecture (Theorem M). Next, §6 extends these congruences to the operators T_ℓ, $\ell \le 19$, and deduces, with the structure theorem for the 3-adic Hecke algebra of [17], a law valid in every weight: *for every eigenform f of level* 1 *and every $n \equiv 1 \pmod 3$, $a_n(f) \equiv \sigma_{k-1}(n) \pmod{81}$*, and, if $k \not\equiv 4 \pmod 6$, $a_n(f) \equiv \psi(n)\sigma_{k-1}(n) \pmod{27}$ for every n prime to 3, with ψ trivial or equal to the character of conductor 3 (Theorem O). Section 7 derives a Galois law: *on the Galois group of $\mathbb{Q}(\sqrt{-3})$,* $\operatorname{tr}\rho_f \equiv 1 + \chi^{k-1} + (a_2^2 - \sigma_{k-1}(2)^2)\,u^2 \pmod{243}$, where u measures the action on ζ_9 (Theorem P); hence $a_\ell \equiv \sigma_{k-1}(\ell) \pmod{243}$ if $\ell \equiv 1 \pmod 9$, a congruence modulo 729 for the ℓ that split completely in $\mathbb{Q}(\zeta_9, \sqrt[3]{3})$ (Theorem R), a bilinear law for $\ell, \ell' \equiv 2 \pmod 3$ (Theorem S), and, if $k \not\equiv 4 \pmod 6$, the determination of all a_n, $3 \nmid n$, modulo 81 by a_2 modulo 81 (Corollary T). Then §8 establishes a 2-adic Galois law (Theorem U), from the modulo 128 theorem of [17] and a certificate for T_5 modulo 512: $a_p \equiv 1 + p^{k-1} \pmod{2^{10}}$ *for every $p \equiv 1 \pmod 8$*, and explicit laws on the other classes; with a reduction to a computation in a finite group (Theorem W), Hatada's question is completely answered: affirmatively for $a \le 10$, negatively for $a = 11, 12, 13$ (Corollary X), and $a_p(f) = 0$ implies $p \equiv -1 \pmod{2^{11}}$ for every eigenform of level 1 (Corollary Y). Finally, §9 extends the 3-adic Galois law beyond 729: *for every prime $\ell \equiv 2 \pmod 3$, $a_\ell^2 \equiv \sigma_{k-1}(\ell)^2 \pmod{3^{\min(2j+2,10)}}$, where $j = v_3(\ell+1)$* (Theorem R′); the exponent $2j+2$ is attained for $j \le 4$ and no longer holds for $j = 5$. It follows that $v_3(a_\ell) = v_3(\ell+1)$ if $v_3(\ell+1) \le 4$ and $k \not\equiv 4 \pmod 6$, and that, for such k, $a_\ell(f) = 0$ implies $\ell \equiv -1 \pmod{2^{11} \cdot 3^5}$ (Corollary Y′). For $\ell \equiv 1 \pmod{27}$ with 3 a cube modulo ℓ, $a_\ell \equiv \sigma_{k-1}(\ell) \pmod{3^7}$, and $\pmod{3^8}$ if $k \equiv 4 \pmod 6$ and $\ell = X^2 + XY + 547Y^2$ (Theorem R″).

Each statement carries a status: **PROVED** (complete proof, possibly resting on a finite exact computation whose certificate is checked by an ancillary script), **KNOWN** (a result of the literature, given again or checked independently), **VERIFIED** (checked by computation on the stated range only) or **OPEN**.

2 2-adic results

For $k \in \{12, 16, 18, 20, 22, 26\}$, let $\Delta_k = \sum_{n\geq 1} a_k(n) q^n$ be the unique normalised eigenform in S_k (thus $\Delta_{12} = \Delta$ and $a_{12}(n) = \tau(n)$). One has $\Delta_k = E_{k-12}\,\Delta$.

Theorem A (negative answer for $a = 11, 12, 13$)**.** *The answer to Hatada's question is negative for $a = 11$, $a = 12$ and $a = 13$. The prime $p = 12289 = 3 \cdot 2^{12} + 1$ provides witnesses at the three levels:*

	Δ_{12}	Δ_{16}	Δ_{18}	Δ_{20}	Δ_{22}	Δ_{26}
$a_k(p) \bmod 2^{16}$	*18434*	*3074*	*11266*	*49154*	*40962*	*25602*
$v_2\big(a_k(p) - 1 - p\big)$	*11*	*10*	*10*	*12*	*12*	*10*
failing levels a	*12, 13*	*11, 12, 13*	*11, 12, 13*	*13*	*13*	*11, 12, 13*

In particular, for Ramanujan's function,

$$\tau(12289) = 13\,297\,575\,938\,818\,018\,265\,090, \qquad v_2\big(\tau(12289) - 12290\big) = 11,$$

whereas $12289 \equiv 1 \pmod{2^{12}}$: the requested congruence fails modulo 2^{12} and modulo 2^{13}. A second witness at level $a = 11$ is $p = 13313 = 13 \cdot 2^{10} + 1$, for which $v_2(a_k(p) - 1 - p) = 10$ if $k = 16, 18, 26$.

Status: **PROVED**. Finite exact computation. All values were obtained by two independent methods which agree: PARI/GP [16] (`ramanujantau`; `mfinit`, `mfeigenbasis`, `mfcoef`) and a computation modulo 2^{23} by products of the η function and Eisenstein series. The "lattice" version of the question therefore also fails for these three values of a.

Proposition B (class congruences)**.** *For n odd and $n \equiv r \pmod 8$,*

$$a_k(n) \equiv c_{k,r}\,\sigma_{k-1}(n) \pmod{2^{A_{k,r}}},$$

with the following pairs $(A_{k,r},\, c_{k,r})$ (for $r = 3, 5, 7$, the value given is a representative of the constant):

k	$r = 1$	$r = 3$	$r = 5$	$r = 7$
12	(11, 1)	(13, 1217)	(12, 1537)	(14, 705)
16	(10, 1)	(12, 609)	(11, 769)	(13, 353)
18	(10, 1)	(12, 97)	(11, 769)	(13, 865)
20	(12, 1)	(14, 3969)	(13, 3073)	(15, 2945)
22	(12, 1)	(14, 897)	(13, 3073)	(15, 3969)
26	(10, 1)	(12, 289)	(11, 257)	(13, 545)

For $k = 12$, these are Kolberg's congruences [12]. The exponents are optimal: no constant works modulo $2^{A_{k,r}+1}$.

Status: **PROVED**. For odd r, the restriction $f_r = \sum_{n\equiv r\,(8)} a(n) q^n$ of a form f of level 1 is a linear combination of the twists of f by the Dirichlet characters modulo 8, all of which lie in $M_k(\Gamma_0(64))$ with trivial character (these characters being quadratic). With $G_k = -\frac{B_k}{2k} + \sum_{n\geq 1} \sigma_{k-1}(n) q^n$, the form $g = (\Delta_k)_r - c_{k,r}(G_k)_r$ therefore belongs to $M_k(\Gamma_0(64)) \cap \mathbb{Z}[[q]]$. By Sturm's theorem [21], applied successively to g, $g/2$, $g/4, \ldots$, it suffices to check divisibility by $2^{A_{k,r}}$ of the coefficients of index $n \leq \frac{k}{12}\,[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(64)] = 8k \leq 208$. Checked for all odd $n \leq 2000$, for the six forms and the four classes (24 congruences); optimality is witnessed by some $n \leq 2000$ in each case.

Theorem C (exact threshold for the six rational forms)**.** *Let $k \in \{12, 16, 18, 20, 22, 26\}$ and $6 \le a \le 13$. Hatada's question has an affirmative answer for Δ_k if and only if $a \le a_k$, where*

$$a_{12} = 11, \qquad a_{16} = a_{18} = a_{26} = 10, \qquad a_{20} = a_{22} = 12.$$

More precisely, the requested congruence holds for every $a \le 13$ when $p \equiv -1 \pmod{2^{a-1}}$; when $p \equiv +1 \pmod{2^{a-1}}$, it holds exactly for $a \le a_k = A_{k,1}$.

Proof. Let $p \equiv \pm 1 \pmod{2^{a-1}}$ with $6 \le a \le 13$. Then $p \equiv \pm 1 \pmod 8$ and $p^2 \equiv 1 \pmod{2^a}$, whence $p^{k-1} \equiv p \pmod{2^a}$ since $k-2$ is even.

If $p \equiv -1 \pmod{2^{a-1}}$, Proposition B (class $r = 7$, $A_{k,7} \ge 13 \ge a$) gives $a_k(p) \equiv c\,(1 + p^{k-1}) \pmod{2^a}$ with c odd. As $1 + p^{k-1} = (1+p)(1 - p + \cdots + p^{k-2})$, the second factor being a sum of an odd number of odd terms, one has $v_2(1+p^{k-1}) = v_2(1+p) \ge a-1$, hence $(c-1)(1+p^{k-1}) \equiv 0 \pmod{2^a}$, and $a_k(p) \equiv 1 + p^{k-1} \equiv 1 + p \pmod{2^a}$.

If $p \equiv 1 \pmod{2^{a-1}}$ and $a \le A_{k,1}$, Proposition B (class $r = 1$, $c_{k,1} = 1$) gives directly $a_k(p) \equiv 1 + p^{k-1} \equiv 1 + p \pmod{2^a}$.

Finally, if $A_{k,1} < a \le 13$, the prime $p = 12289$, which satisfies $p \equiv 1 \pmod{2^{12}}$, is a counterexample (Theorem A). □

Status: **PROVED**.

Corollary D (non-vanishing)**.** *For each of the six forms, if p is an odd prime and $v_2(p+1) < A_{k,r}$ with $r \equiv p \pmod 8$, then $v_2\big(a_k(p)\big) = v_2(p+1)$; in particular $a_k(p) \ne 0$. Consequently $a_k(p) = 0$ implies*

$$p \equiv -1 \pmod{2^{A_{k,7}}}, \qquad 2^{A_{k,7}} = 2^{14},\ 2^{13},\ 2^{13},\ 2^{15},\ 2^{15},\ 2^{13} \quad \text{for } k = 12, 16, 18, 20, 22, 26.$$

Proof. By Proposition B, $a_k(p) \equiv c\,(1+p^{k-1}) \pmod{2^{A_{k,r}}}$ with c odd, and $v_2(1+p^{k-1}) = v_2(1+p)$. If $p \not\equiv 7 \pmod 8$, then $v_2(p+1) \le 2 < A_{k,r}$. □

Status: **PROVED**.

Remark (Tian–Qin bounds). The five bounds B_k ($k = 16, 18, 20, 22, 26$) of [23, Prop. 5.2], taken from the arXiv version 1504.07381v3, are primes satisfying the congruence conditions of [23], but $v_2(B_k+1) = 1, 3, 1, 6, 2$ respectively. By Corollary D, $a_{B_k}(\Delta_k) \ne 0$ and $v_2\big(a_{B_k}(\Delta_k)\big) = v_2(B_k+1)$. Four of them were already excluded by [9, 10], which force $p \equiv -1 \pmod{32}$ for a zero, and all five by [17], which forces $p \equiv -1 \pmod{128}$. The values of the published version of [23] were not consulted.

3 The threshold in all weights ≤ 100

For even k, $12 \le k \le 100$, $k \ne 14$, and for each prime $p \le 13313$ with $p \equiv \pm 1 \pmod{2^7}$ (48 primes), we compute the minimal valuation $s(k,p) = \min_\lambda v_2(\lambda - 1 - p)$, where λ runs over the eigenvalues of T_p on S_k (all eigenforms, including those with irrational coefficients; dimension up to 8). The computation is exact modulo 2^{128} in a Miller basis; every valuation ≤ 14 obtained is guaranteed.

Theorem E (failures in all weights ≤ 100)**.** *For every $k \le 100$ with $k \equiv 0$ or $2 \pmod 8$ and $k \ge 16$, there is an eigenvalue λ of T_{12289} on S_k with $v_2(\lambda - 12290) = 10$; Hatada's question therefore fails at level 11 in each of these weights. For $k \equiv 4$ or $6 \pmod 8$, $k \in \{12\} \cup [28, 100]$, there is one with $v_2(\lambda - 12290) = 11$, hence a failure at level 12.*

Status: **PROVED**. Finite exact computation: for each such k, the Newton polygon at 2 of the characteristic polynomial of $T_{12289} - 12290$ on S_k (PARI/GP, see §11).

weight k	first failing level a observed
$k \equiv 0, 2 \pmod 8$, $16 \le k \le 98$	11
$k \equiv 4, 6 \pmod 8$, $k = 12$ and $28 \le k \le 100$	12
$k = 20,\ 22$	13

The failure at the stated level is proved (Theorems A and E); the absence of failure at lower levels is checked on the range of Statement V.

Statement V. For every eigenform of weight $12 \le k \le 100$, every $6 \le a \le 10$ and every prime $p \le 13313$ with $p \equiv \pm 1 \pmod{2^{a-1}}$, one has $\lambda_p \equiv 1 + p \pmod{2^a}$. The same holds for $24 \le k \le 54$ and all primes $p \le 60000$ (183 primes $p \equiv \pm 1 \pmod{2^7}$, 48 of which satisfy $p \equiv \pm 1 \pmod{2^9}$). Level 10 is attained with equality: for example $v_2\big(\tau(7681) - 7682\big) = 10$, where $7681 \equiv 1 \pmod{2^9}$.

Status: **VERIFIED**. Exhaustive check on the stated range; the first failing levels of the table above are unchanged when passing from $p \le 13313$ to $p \le 60000$.

Statement V′ ("lattice" form). For $12 \le k \le 100$ and each of the 194 primes $p \le 13313$ such that $p \equiv \pm 1 \pmod{32}$, the lattice L^-_{w+2} of [10] is stable under $(T_{w+2}(p) - 1 - p)/2^a$ for every $a \le 10$ such that $p \equiv \pm 1 \pmod{2^{a-1}}$ (ten of these primes reach $a = 10$). The first failing level of the lattice form is 11, 12 or 13 according to k; it is strictly smaller than that of the eigenvalues (11 against 12) for $k \in \{36, 52, 60, 68, 76, 84, 92, 100\}$.

Status: **VERIFIED**. Exact computation on a basis of L^-_{w+2}.

Remark (conjecture). The data suggest that Hatada's question has an affirmative answer exactly for $a \le 10$, including in its "lattice" form: the congruence $\lambda_p \equiv 1 + p \pmod{2^a}$ for $p \equiv \pm 1 \pmod{2^{a-1}}$ would hold for every eigenform of level 1 as soon as $a \le 10$, and it fails for $a = 11$. Section 8 proves the affirmative answer for $a \le 10$ (Corollary X); the "lattice" form remains only verified.

4 3-adic results

Notation. Let $k \ge 12$ be even and $w = k-2$. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ with non-zero determinant and $P \in \mathbb{Q}[X]$ of degree $\le w$, put $(P|\gamma)(X) = (cX + d)^w P\big(\frac{aX+b}{cX+d}\big)$. With $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $U = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, let W^- be the space of odd polynomials P such that $P|(1+S) = P|(1+U+U^2) = 0$. The map sending f to the odd part of $\int_0^{i\infty} f(z)(X - z)^w\, dz$ identifies $S_k(\mathbb{R})$ with $W^- \otimes \mathbb{R}$ and transforms T_n into $P \mapsto P|\widetilde{T}_n$, where $\widetilde{T}_n = \sum_{M \in \mathcal{M}_n} M$ and $\mathcal{M}_n$ is the set of integer matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $ad - bc = n$, $a > c \ge 0$ and $d > b \ge 0$ [14, 24]. For f with real coefficients, this odd part is the real part of the integral; since $\widetilde{T}_n$ is a sum of integer matrices, it commutes with taking real parts, and W^- is therefore stable under $\widetilde{T}_n$.

The coefficient of X^{w-j} in $\int_0^{i\infty} f(z)(X - z)^w\, dz$ is $(-1)^j \binom{w}{j} r_j(f)$, with $r_j(f) = \int_0^{i\infty} f(z) z^j\, dz$. Hatada's lattice L^-_{w+2}, formed by the forms whose odd periods $r_j(f)$ are integers [10, p. 305], therefore corresponds to

$$L_k = \Big\{ P = \sum_j \tbinom{w}{j} m_j X^j \in W^- \ :\ m_j \in \mathbb{Z} \Big\}.$$

The polynomials $\sum_j \binom{w}{j} m_j X^j$, $m_j \in \mathbb{Z}$, form a module B_w stable under $P \mapsto P|\gamma$ for every $\gamma \in M_2(\mathbb{Z})$, by virtue of the identity $\binom{w}{j}\binom{j}{s}\binom{w-j}{l-s} = \binom{w}{l}\binom{l}{s}\binom{w-l}{j-s}$. Thus $L_k = W^- \cap B_w$ is a lattice of rank $\dim S_k$, saturated in B_w, stable under each $\widetilde{T}_n$, whose eigenvalues are the $a_n(f)$.

For $P \in L_k$, we write μ_P for the $\mathbb{Z}$-linear form on the space $\mathbb{Z}[x, y]_w$ of integral binary forms of degree w defined by $\mu_P(x^j y^{w-j}) = m_j$. Then $P(X) = \mu_P\big((xX + y)^w\big)$ and

$$\mu_{P|\gamma}(F) = \mu_P\big(F(ax + cy,\, bx + dy)\big).$$

Lemma 1 (period identities)**.** *For every $P \in W^-$:*

(a) $m_j = 0$ for even j, $m_j = m_{w-j}$ for every j, and $\mu_P\big(F(y,x)\big) = \mu_P(F)$;

(b) $P(1) = P'(1) = 0$, $P(\frac{1}{2}) = 0$ and $P(\frac{1}{3}) + P(\frac{2}{3}) = 0$;

(c) $\mu_P\big((x+y)^w\big) = \mu_P\big(x(x+y)^{w-1}\big) = \mu_P\big(y(x+y)^{w-1}\big) = 0$ and $\mu_P\big(x^2(x+y)^{w-2}\big) = \mu_P\big(y^2(x+y)^{w-2}\big) = -2m_1$, $\mu_P\big(xy(x+y)^{w-2}\big) = 2m_1$; the same identities hold with $x+y$ replaced by $y-x$, with the values $0,0,0$ and $2m_1, 2m_1, 2m_1$.

Proof. (a) P is odd; the relation $X^w P(-1/X) = -P(X)$ gives $m_j = m_{w-j}$. (b) The relations for U (at the point $1+t$) and for S (at the point t) give the three-term relation $P(1+t) = P(t) - (1+t)^w P\big(\frac{t}{1+t}\big)$. At $t=0$: $P(1) = 0$; differentiating at $t=0$: $P'(1) = -wP(0) = 0$; at $t=1$, with the relation for S at the point 2 and oddness: $P(2) = -2^w P(\frac{1}{2}) = 2^w P(\frac{1}{2})$, whence $P(\frac{1}{2}) = 0$; at $t = -\frac{1}{3}$: $P(\frac{2}{3}) = P(-\frac{1}{3}) - (\frac{2}{3})^w P(-\frac{1}{2}) = -P(\frac{1}{3})$. (c) One has $P(1) = \mu_P((x+y)^w)$ and $P'(1) = w\,\mu_P(x(x+y)^{w-1})$. The relation for U applied to $F = x^2y^{w-2}$ reads $\mu_P(F) + \mu_P\big(x^{w-2}(x+y)^2\big) + \mu_P\big(y^2(x+y)^{w-2}\big) = 0$, that is $0 + 2m_1 + \mu_P(y^2(x+y)^{w-2}) = 0$; the other values follow by (a) and by writing $y = (x+y) - x$. The passage to $y-x$ is made by the substitution $x \mapsto -x$, which changes μ_P into $-\mu_P$. □

Lemma 2 (T_3 modulo 27)**.** *For every $P \in L_k$ and every form $F \in \mathbb{Z}[x,y]_w$,*

$$\mu_{P|\widetilde{T}_3}(F) \equiv m_1(P)\Big[\,3\sum_{t=0}^{2}\big(\partial_y F(1,t) + \partial_x F(t,1)\big) + 18\,\big(\tfrac{1}{2}\partial_x^2 + \partial_x\partial_y + \tfrac{1}{2}\partial_y^2\big)F(1,-1)\Big] \pmod{27}.$$

In particular $\mu_{P|\widetilde{T}_3}(F) \equiv 0 \pmod 9$ if $3 \mid m_1(P)$, and $\mu_{P|\widetilde{T}_3}(F) \equiv 0 \pmod{27}$ if $9 \mid m_1(P)$.

Proof. The seven elements of $\mathcal{M}_3$ give the following substitutions $(x,y) \mapsto (ax+cy, bx+dy)$, written in the form $\lambda(x,y)\,u + 3h(x,y)$:

$$\begin{array}{lll}(x,3y) = x\,(1,0) + 3(0,y), & (x,x+3y) = x\,(1,1) + 3(0,y), & (x,2x+3y) = x\,(1,2) + 3(0,y),\\ (3x,y) = y\,(0,1) + 3(x,0), & (3x+y,y) = y\,(1,1) + 3(x,0), & (3x+2y,y) = y\,(2,1) + 3(x,0),\\ (2x+y,\,x+2y) = (y-x)\,(1,-1) + 3(x,y).\end{array}$$

Since the divided derivatives of an integral form are integral, Taylor's formula gives, modulo 27, $F(\lambda u + 3h) \equiv \lambda^w F(u) + 3\lambda^{w-1}\sum_i h_i\,\partial_i F(u) + 9\lambda^{w-2}\sum_{i\le i'} h_i h_{i'}\,\partial^{[i,i']}F(u)$, with $\partial^{[i,i]} = \frac{1}{2}\partial_i^2$ and $\partial^{[1,2]} = \partial_1\partial_2$. Apply μ_P. By Lemma 1, $\mu_P(\lambda^w) = 0$ for $\lambda \in \{x, y, y-x\}$; $\mu_P(x^{w-1}y) = \mu_P(y^{w-1}x) = m_1$, $\mu_P(x^w) = \mu_P(y^w) = 0$, $\mu_P\big((y-x)^{w-1}g\big) = 0$ for linear g; at second order, $\mu_P(x^{w-2}y^2) = m_{w-2} = 0$, $\mu_P(y^{w-2}x^2) = m_2 = 0$ and $\mu_P\big((y-x)^{w-2}q\big) = 2q(1,1)\,m_1$ for quadratic q. Collecting the terms gives the stated formula. □

Lemma 3 (the first period)**.** *For every $P \in L_k$, $3 \mid m_1(P)$; if moreover $6 \nmid k$, then $9 \mid m_1(P)$.*

Proof. By Lemma 1(b), $3^w\big(P(\frac{1}{3}) + P(\frac{2}{3})\big) = 0$, that is $\sum_j \binom{w}{j} 3^{w-j}(1+2^j)m_j = 0$. Putting $i = w-j$ and using $m_{w-i} = m_i$, we get

$$\sum_{i \text{ odd}} c_i\, m_i = 0, \qquad c_i = 3^i\tbinom{w}{i}\big(1 + 2^{w-i}\big).$$

The terms $i=1$ and $i=w-1$ both carry m_1. For odd n, $v_3(1+2^n) = 1 + v_3(n)$ (lifting the exponent). Thus $v_3(c_1) = 2 + v_3(w) + v_3(w-1)$ and, for odd $i \ge 3$, with $\binom{w}{i} = \frac{w}{i}\binom{w-1}{i-1}$,

$$\delta_i := v_3(c_i) - v_3(c_1) = (i-1) - v_3(i) + v_3\tbinom{w-1}{i-1} + v_3(w-i) - v_3(w-1).$$

Let $e = v_3(w-1)$. If $v_3(i-1) < e$, the addition in base 3 of $i-1$ and $w-i$, with sum $w - 1 \equiv 0 \pmod{3^e}$, has a carry at each position from $v_3(i-1)$ to $e-1$; by Kummer's theorem

$v_3\binom{w-1}{i-1} \geq e - v_3(i-1)$, whence $\delta_i \geq (i-1) - v_3(i) - v_3(i-1) \geq 1$, since at most one of the two consecutive integers $i-1, i$ is divisible by 3, with valuation at most $\log_3 i$. If $v_3(i-1) \geq e$ and $e = 0$, then $\delta_i \geq (i-1) - v_3(i) \geq 1$. If $v_3(i-1) \geq e \geq 1$, then $3 \nmid i$, $i - 1 \geq 3^e$ and $\delta_i \geq (i-1) - e \geq 2$. Hence $\delta_i \geq 1$ for every odd $i \geq 3$; in particular $v_3(c_1 + c_{w-1}) = v_3(c_1)$, and the relation gives $v_3(c_1) + v_3(m_1) \geq v_3(c_1) + \min_{3 \leq i \leq w-3} \delta_i$, that is $v_3(m_1) \geq 1$.

If $6 \nmid k$, then $w \not\equiv 1 \pmod 3$, hence $e = 0$. For $i \geq 5$, $\delta_i \geq (i-1) - v_3(i) \geq 2$; for $i = 3$, $\delta_3 = 1 + v_3(w-2) + v_3(w-3) \geq 2$, since 3 divides w or $w-2$. Hence $v_3(m_1) \geq 2$. □

Theorem F (a_3 modulo 9 and 27; Hatada)**.** *For every even $k \geq 12$, $\widetilde{T}_3(L_k) \subset 9L_k$, and $\widetilde{T}_3(L_k) \subset 27L_k$ if $6 \nmid k$. Consequently, for every eigenform f of level 1 and weight k, $a_3(f)/9$ is an algebraic integer, and so is $a_3(f)/27$ when $6 \nmid k$. These bounds are optimal: $\tau(3) = 2^2 \cdot 3^2 \cdot 7$ ($k = 12$) and $a_3(\Delta_{16}) = -2^2 \cdot 3^3 \cdot 31$ ($k = 16$).*

Proof. Let $P \in L_k$. By Lemmas 2 and 3, $\mu_{P|\widetilde{T}_3}(F)$ is divisible by 9 (by 27 if $6 \nmid k$) for every $F \in \mathbb{Z}[x,y]_w$, hence $P|\widetilde{T}_3 \in 9B_w$ (resp. $27B_w$). Since $P|\widetilde{T}_3 \in W^-$ and $L_k = W^- \cap B_w$ is saturated in B_w, we get $P|\widetilde{T}_3 \in 9L_k$ (resp. $27L_k$). The operator $\widetilde{T}_3/9$ (resp. $\widetilde{T}_3/27$) is therefore an endomorphism of the $\mathbb{Z}$-module L_k; its characteristic polynomial is monic with integer coefficients and its roots are the $a_3(f)/9$ (resp. $a_3(f)/27$). □

Status: **KNOWN**. These are congruences (6) and (7) of [9], proved by Hatada on the same lattice, from the first period [9, §8]; the proof above is a write-up of it. Checks (`VERIF_A3.py`): the inequality $\delta_i \geq 1$ (and ≥ 2 if $w \not\equiv 1 \pmod 3$) for all even $w \leq 3000$; the identity of Lemma 3, the divisibility of m_1 and the inclusion $\widetilde{T}_3(L_k) \subset 9L_k$ (resp. $27L_k$) on a basis of $L_k \otimes \mathbb{Z}_{(3)}$ for $12 \leq k \leq 100$; eigenvalues recovered for the six rational forms. With PARI/GP, for every $k \leq 400$, the smallest 3-adic slope of the characteristic polynomial of T_3 on S_k is 2 if $6 \mid k$; if $6 \nmid k$, it is 3, except for $k \equiv 10, 14 \pmod{18}$, where it lies between 4 and 6 (**VERIFIED**).

Theorem G (Conjecture 9.1 up to weight 1000; Chiriac)**.** *For every even weight $12 \leq k \leq 1000$, $k \neq 14$, every eigenform of level 1 and weight k satisfies Conjecture 9.1 of [17].*

Status: **KNOWN**. [4, Cor. 1.3] together with [17]. Independent check, which does not use the non-ramification hypothesis (494 spaces, all eigenforms). Certificate: let P be the characteristic polynomial of T_2 on S_k, of degree d, computed exactly modulo 3^{2d+2}. If $k \equiv 4 \pmod 6$, the Newton polygon of P at 3 has all its d slopes ≥ 2. If $k \equiv 0, 2 \pmod 6$, the number of slopes ≥ 2 of the Newton polygon of $P(x+3)$, plus that of $P(x+6)$, is d; since $v_3\big((\lambda-3)-(\lambda-6)\big) = 1$, no root can be counted twice, so that every eigenvalue satisfies $\lambda \equiv 3$ or $6 \pmod{9\overline{\mathbb{Z}}_3}$. At precision 3^{2d+2}, the slopes < 2 are determined exactly.

Theorem H (level 1 case of the Coleman–Stein conjecture)**.** *Let f be an eigenform of level 1 and weight k. If $k \leq 1000$, or if 3 is unramified in the coefficient field of f, then $a_3(f) \equiv 0 \pmod{9\overline{\mathbb{Z}}_3}$ and f is congruent modulo $9\overline{\mathbb{Z}}_3$, coefficient by coefficient, to one of the five eigenforms of the table of [6] (weights 12, 16, 20, 24, 32). The five classes are distinct and all attained.*

Proof. For $k \geq 3$, one has $a_{3n}(f) = a_3(f)a_n(f) - 3^{k-1}a_{n/3}(f) \equiv a_3(f)a_n(f) \pmod 9$: the reduction of f modulo 9 is an eigenvector of the operator U, with eigenvalue $a_3(f)$, and of $t_\Lambda = [1+3]$, with eigenvalue 4^k. By [17, Thm 7.2(ii)], the Hecke algebra $\mathbb{T}(3, \mathbb{Z}_3)$ is generated by U, T_2, $1+T_7$ and t_Λ; all the coefficients of f modulo $9\overline{\mathbb{Z}}_3$ are therefore determined by $(a_2, a_3, a_7, 4^k)$ mod $9\overline{\mathbb{Z}}_3$. One has $a_3 \equiv 0$ ([9]; Theorem F); by [17, Prop. 9.3], $a_7 \equiv 5, 8, 2 \pmod{9\overline{\mathbb{Z}}_3}$ according as $k \equiv 0, 2, 4 \pmod 6$, and $4^k \bmod 9$ depends only on $k \bmod 3$; finally a_2 satisfies Conjecture 9.1 (Theorem G if $k \leq 1000$, [4, Cor. 1.3] under the non-ramification hypothesis). At most five tuples remain: two for $k \equiv 0 \pmod 6$ ($a_2 \equiv 3$ or 6), two for $k \equiv 2 \pmod 6$, one for $k \equiv 4 \pmod 6$ ($a_2 \equiv 0$). They are realised by the weights 12 and 24, 32 and 20, and 16 respectively. □

Status: **PROVED**. A consequence of [17, Thm 7.2, Prop. 9.3], of [4], of Theorem G and of [9] (Theorem F). Coleman and Stein had checked their conjecture up to weight 74 in level 1.

Remark. In the proof of [17, Thm 9.2], each $a_n(f)$ modulo 9 is a polynomial with coefficients in $\mathbb{Z}/9\mathbb{Z}$ in $a_2(f)$, $a_3(f)$, $a_7(f)$ and the eigenvalue of t_Λ; Conjecture 9.1 controls $a_2(f)$, [17, Prop. 9.3] controls $a_7(f)$, the eigenvalue of t_Λ is 4^k, and $a_3(f) \equiv 0 \pmod{9\overline{\mathbb{Z}}_3}$ is taken there from [9]. Only Conjecture 9.1 therefore remained; it is proved in §5.

5 The eigenvalue a_2 modulo 9 and 27

We keep the notation of §4. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with non-zero determinant and $F \in \mathbb{Z}[x,y]_w$, put $\sigma_\gamma F(x,y) = F(ax+cy,\, bx+dy)$; thus $\mu_{P|\gamma} = \mu_P \circ \sigma_\gamma$, $\sigma_\gamma\sigma_\delta = \sigma_{\gamma\delta}$, and $\sigma_{-\gamma} = \sigma_\gamma$ since w is even. We extend $\gamma \mapsto \sigma_\gamma$ by linearity to the ring $\mathbb{Z}[\mathcal{M}]$ of the monoid $\mathcal{M} = M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})$. We write $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $T' = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, $\varepsilon = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, F_x, F_y for the partial derivatives, and $s = \sigma_{k-1}(2) = 1 + 2^{k-1}$. Since $2^n = (3-1)^n \equiv -1 + 3n \pmod 9$ for odd n,

$$s \equiv 3(k-1) \pmod 9.$$

Let $P \in W^-$. By definition, $P|(1+S) = P|(1+U+U^2) = P|(1+\varepsilon) = 0$; since $T = US^{-1}$ and $T' = -U^2S$, we deduce the three-term relation $P = P|T + P|T'$ (the one in the proof of Lemma 1(b)). Thus, for every form H,

$$\mu_P(H + \sigma_\varepsilon H) = \mu_P(H + \sigma_S H) = \mu_P(H - \sigma_T H - \sigma_{T'} H) = 0. \tag{R}$$

Applying the last one to $\sigma_\varepsilon H$ ($T\varepsilon = \varepsilon T^{-1}$, $T'\varepsilon = \varepsilon T'^{-1}$), we also get $\mu_P(H - \sigma_{T^{-1}}H - \sigma_{T'^{-1}}H) = 0$. More generally, let $\mathcal{I}$ be the right ideal of $\mathbb{Z}[\mathcal{M}]$ generated by $1+S$, $1+U+U^2$ and $1+\varepsilon$: one has $\mu_P \circ \sigma_\zeta = 0$ for every $\zeta \in \mathcal{I}$.

5.1 Modulo 27

Theorem I (T_2 modulo 27)**.** *For every even $k \geq 12$, $\widetilde{T}_2(L_k) \subset 3L_k$ and, for every $P \in L_k$,*

$$P|\widetilde{T}_2^2 \equiv 9(k-1)^2\, P \pmod{27L_k}.$$

Corollary J. *For every eigenform f of level 1 and weight k, $a_2(f) \equiv 0 \pmod{3\overline{\mathbb{Z}}_3}$ and $a_2(f)^2 \equiv 9(k-1)^2 \pmod{27\overline{\mathbb{Z}}_3}$. If $k \equiv 0, 2 \pmod 6$, then $a_2(f) \equiv 3$ or $6 \pmod{9\overline{\mathbb{Z}}_3}$, without any ramification hypothesis. If $k \equiv 4 \pmod 6$, then $v_3\big(a_2(f)\big) \geq 3/2$.*

Proof. Let $\lambda = a_2(f)$. The operator $\widetilde{T}_2$ is an endomorphism of the $\mathbb{Z}$-module L_k, with eigenvalues the $a_2(f)$; let $v \in L_k \otimes \overline{\mathbb{Z}}_3$ be an eigenvector for λ at least one of whose coordinates is a unit ($\overline{\mathbb{Z}}_3$ is a valuation ring). By Theorem I, $\lambda v \in 3(L_k \otimes \overline{\mathbb{Z}}_3)$ and $\big(\lambda^2 - 9(k-1)^2\big)v \in 27(L_k \otimes \overline{\mathbb{Z}}_3)$; reading a unit coordinate, $\lambda = 3\nu$ with $\nu \in \overline{\mathbb{Z}}_3$ and $\nu^2 \equiv (k-1)^2 \pmod{3\overline{\mathbb{Z}}_3}$. If $k \not\equiv 1 \pmod 3$, then $(k-1)^2 \equiv 1$. The two factors of $(\nu-1)(\nu+1) \in 3\overline{\mathbb{Z}}_3$ are not both in the maximal ideal, since their difference 2 is a unit; one of them is therefore a unit, and the other lies in $3\overline{\mathbb{Z}}_3$. Hence $\nu \equiv \pm 1$ and $\lambda \equiv \pm 3 \pmod{9\overline{\mathbb{Z}}_3}$. If $k \equiv 1 \pmod 3$, then $\nu^2 \in 3\overline{\mathbb{Z}}_3$, that is $v_3(\lambda) \geq 3/2$. □

Status: **PROVED**. For $k \equiv 0, 2 \pmod 6$, one also has $a_2(f) \equiv \pm s \pmod{9\overline{\mathbb{Z}}_3}$, since $s \equiv 3(k-1) \pmod 9$. The case $k \equiv 4 \pmod 6$ is treated in §5.2.

The proof of Theorem I occupies the rest of this subsection.

Lemma 4 (expansion of T_2)**.** *For $F \in \mathbb{Z}[x,y]_w$, put*

$$A^*F = y\,F_y(x,-y) + y\,F_y(x,x-y) + x\,F_x(-x,y) + x\,F_x(y-x,y).$$

There is a $\mathbb{Z}$-linear endomorphism B^* of $\mathbb{Z}[x,y]_w$ such that, for every $P \in L_k$ and every F,

$$\mu_{P|\widetilde{T}_2}(F) \equiv -3\mu_P(F) + 3\mu_P(A^*F) + 9\mu_P(B^*F) \pmod{27}.$$

Proof. With $2 = -1 + 3$, the four substitutions of $\mathcal{M}_2$ read

$$(x, 2y) = (x, -y) + 3(0, y), \quad (x, x + 2y) = (x, x - y) + 3(0, y),$$
$$(2x, y) = (-x, y) + 3(x, 0), \quad (2x + y, y) = (y - x, y) + 3(x, 0).$$

In other words, each $M \in \mathcal{M}_2$ is written $M = N + 3H$, where N runs over $N_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $N_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$, $N_3 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $N_4 = \left(\begin{smallmatrix} -1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Taylor's formula, whose divided derivatives are integral, gives $\sum_M \sigma_M F \equiv \sum_i \sigma_{N_i} F + 3A^*F + 9B^*F \pmod{27}$, the first-order term being A^*F. Finally $\sigma_{N_1} = \sigma_{N_3} = \sigma_\varepsilon$, $\sigma_{N_2} = \sigma_\varepsilon \sigma_T$ and $\sigma_{N_4} = \sigma_\varepsilon \sigma_{T'}$ (since $N_2 = N_1 T$ and $N_4 = N_3 T'$); by (R), $\mu_P\big(\sum_i \sigma_{N_i} F\big) = -2\mu_P(F) - \mu_P(\sigma_T F + \sigma_{T'} F) = -3\mu_P(F)$. □

Lemma 5 (an identity in characteristic 3)**.** *Let μ be a linear form on $\mathbb{Z}[x, y]_w$, with values in $\mathbb{F}_3$, which satisfies the relations (R) modulo 3. For every F,*

$$\mu\big(A^*A^*F + A^*F\big) = w(w + 2)\,\mu(F) - w\,\mu\big(y\,\partial_x[(\sigma_T - 1)^2 F]\big).$$

Proof. Write $E = \partial_x + \partial_y$; steps (i) to (iii) are exact identities.

(i) One has $A^*F = -\sigma_{N_1}(yF_y) + \sigma_{N_2}\big((x - y)F_y\big) - \sigma_{N_3}(xF_x) + \sigma_{N_4}\big((y - x)F_x\big)$. With the equalities of the proof of Lemma 4 and $xF_x + yF_y = wF$, we get $A^* = \sigma_\varepsilon \circ (\Phi - w)$, where $\Phi F = \sigma_T\big((x - y)F_y\big) - \sigma_{T'}\big((x - y)F_x\big)$.

(ii) Since $x - y = -\sigma_\varepsilon(x + y)$, $\partial_y \sigma_\varepsilon = \sigma_\varepsilon \partial_y$, $\partial_x \sigma_\varepsilon = -\sigma_\varepsilon \partial_x$, $T\varepsilon = \varepsilon T^{-1}$ and $T'\varepsilon = \varepsilon T'^{-1}$, one has, for every H, $\Phi(\sigma_\varepsilon H) = -\sigma_\varepsilon X_H$ with $X_H = \sigma_{T^{-1}}\big((x + y)H_y\big) + \sigma_{T'^{-1}}\big((x + y)H_x\big)$. With $G = \Phi F$, we get $A^*A^*F + A^*F = -X_{G - wF} - w(G - wF) + \sigma_\varepsilon(G - wF)$, then, by (R),

$$\mu(A^*A^*F + A^*F) = -\mu(X_G + G) - w\,\mu(G) + w\,\mu(X_F) + w(w + 1)\,\mu(F).$$

(iii) Put $K_1 = (x - y)F_y$ and $K_2 = (x - y)F_x$, so that $G = \sigma_T K_1 - \sigma_{T'} K_2$. The rules $\partial_x \sigma_T = \sigma_T E$, $\partial_y \sigma_T = \sigma_T \partial_y$, $\partial_x \sigma_{T'} = \sigma_{T'} \partial_x$, $\partial_y \sigma_{T'} = \sigma_{T'} E$, $(x+y)\,\sigma_T Y = \sigma_T(yY)$, $(x+y)\,\sigma_{T'} Y = \sigma_{T'}(xY)$, $T^{-1}T' = ST$ and $T'^{-1}T = -ST'$ give

$$X_G = y\,\partial_y K_1 - x\,\partial_x K_2 - \sigma_S \sigma_T(xEK_2) + \sigma_S \sigma_{T'}(yEK_1).$$

Put $Z_1 = xEK_2 + K_1$ and $Z_2 = yEK_1 + K_2$. Euler's identities $xF_{xx} + yF_{xy} = (w - 1)F_x$ and $xF_{xy} + yF_{yy} = (w-1)F_y$ give $Z_1 + Z_2 = w(x-y)EF$ and $y\,\partial_y K_1 - x\,\partial_x K_2 - Z_2 = -wF - w(x-y)F_x$. By (R), $\mu \circ \sigma_S = -\mu$ and $\mu \circ \sigma_{T'} = \mu - \mu \circ \sigma_T$; hence

$$\mu(X_G + G) = \mu\big(y\,\partial_y K_1 - x\,\partial_x K_2 - Z_2\big) + \mu\big(\sigma_T(Z_1 + Z_2)\big) = w\,\mu\big(-F - (x-y)F_x + \sigma_T((x-y)EF)\big).$$

(iv) Substituting into (ii), using again $\mu \circ \sigma_{T'} = \mu - \mu \circ \sigma_T$ and $\mu \circ \sigma_{T'^{-1}} = \mu - \mu \circ \sigma_{T^{-1}}$, together with $\sigma_T\big((x - y)EF\big) = -y\,\partial_x(\sigma_T F)$ and $\sigma_{T^{-1}}\big((x + y)(F_x - F_y)\big) = y\,\partial_x(\sigma_{T^{-1}} F)$, we obtain the exact identity

$$\mu(A^*A^*F + A^*F) = w(w + 2)\,\mu(F) + 3w\,\mu(xF_x) - w\,\mu\big(y\,\partial_x[(1 - 2\sigma_T + \sigma_{T^{-1}})F]\big).$$

Modulo 3, the term $3w\,\mu(xF_x)$ vanishes, $\sigma_{T^{-1}} = \sigma_{T^2}$ (since $T^3 \equiv I$) and $1 - 2\sigma_T + \sigma_{T^2} \equiv 1 + \sigma_T + \sigma_{T^2} \equiv (\sigma_T - 1)^2$. □

Lemma 6 (information modulo 9)**.** *For every $P \in L_k$ and every $F \in \mathbb{Z}[x, y]_w$, $\mu_P\big(y\,\partial_x[(\sigma_T - 1)^2 F]\big) \equiv 0 \pmod 3$.*

Proof. Let $\mathcal{G}$ be the group of matrices in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ of determinant ± 1, modulo $\pm I$; it has 648 elements, and the action $F \mapsto \sigma_\gamma F$ on $\mathbb{Z}[x, y]_w/9$ factors through $\mathcal{G}$, whence an action of the ring $\mathcal{R} = (\mathbb{Z}/9\mathbb{Z})[\mathcal{G}]$. Let $\mathcal{I}_9$ be the image of $\mathcal{I}$ in $\mathcal{R}$, and $\mathcal{C} \subset \mathcal{R}$ the two-sided ideal generated by 3 and the $\kappa - 1$, $\kappa \equiv \pm I \pmod 3$. A finite exact computation in $\mathcal{R}$ (an explicit combination of 290 terms, redone by `VERIF_A2.py`) shows that

$$\xi := T\,(1 + T' + T'^2)(1 + T + T^2) \in \mathcal{I}_9 + \mathcal{C}^2.$$

The elements of $\mathcal{I}_9$ annihilate μ_P modulo 9. Each σ_κ, $\kappa \equiv \pm I \pmod 3$, is congruent to the identity modulo 3; every element of $\mathcal{C}$ therefore acts by an operator vanishing modulo 3, and $\mathcal{C}^2$ acts by 0 modulo 9. Thus $\mu_P(\sigma_\xi F) \equiv 0 \pmod 9$. On the other hand, multiplying on the right the relation $P = P|T + P|T'$ by T'^j $(j = 0, 1, 2)$ and summing, we get $P|T(1 + T' + T'^2) = P - P|T'^3$; with $H = (1 + \sigma_T + \sigma_{T^2})F$ and $\sigma_{T'^3} H(x, y) = H(x + 3y, y)$, Taylor's formula gives

$$\mu_P(\sigma_\xi F) = \mu_P(H) - \mu_P(\sigma_{T'^3} H) \equiv -3\,\mu_P(y\,\partial_x H) \pmod 9.$$

Hence $\mu_P(y\,\partial_x H) \equiv 0 \pmod 3$, and one concludes with $1 + \sigma_T + \sigma_{T^2} = (\sigma_T - 1)^2 + 3\sigma_T$. □

Proof of Theorem I. Let $P \in L_k$. By Lemma 4, $\mu_{P|\widetilde{T}_2}(F) \equiv 0 \pmod 3$ for every F, hence $P|\widetilde{T}_2 \in 3B_w \cap W^- = 3L_k$. Put $Q = P|\widetilde{T}_2$. Lemma 4 gives $\mu_Q(G) \equiv 3\mu_P(A^*G - G) \pmod 9$ for every G, and, applied to Q, $\mu_{Q|\widetilde{T}_2}(F) \equiv 3\mu_Q(A^*F - F) + 9\mu_Q(B^*F) \equiv 9\mu_P\big((A^* - 1)^2 F\big) \pmod{27}$, since $\mu_Q \equiv 0 \pmod 3$. Modulo 3, $(A^* - 1)^2 \equiv A^*A^* + A^* + 1$; Lemmas 5 and 6, applied to the reduction of μ_P, give $\mu_P\big((A^* - 1)^2 F\big) \equiv \big(1 + w(w + 2)\big)\mu_P(F) = (k - 1)^2 \mu_P(F) \pmod 3$. Thus $P|\widetilde{T}_2^2 - 9(k - 1)^2 P \in 27B_w \cap W^- = 27L_k$. □

STATUS: **PROVED**. Lemma 6 rests on a finite exact computation, whose certificate is checked by `VERIF_A2.py`. Checks: the congruence of Theorem I checked directly on L_k for $12 \le k \le 290$ (PARI/GP); the identity of Lemma 5 on all solutions modulo 3 of the relations, and the condition of Lemma 6 on L_k, for $k \le 40$ (`VERIF_A2.py`).

5.2 Modulo 81

Theorem K (T_2 modulo 81)**.** *Let $k \ge 12$ be even and $P \in L_k$. Then*

$$\begin{aligned} &P|\widetilde{T}_2^2 \equiv s^2 P \pmod{81L_k} && \text{if } k \equiv 0, 2 \pmod 6,\\ &P|\widetilde{T}_2^2 + 9\,P|\widetilde{T}_2 \equiv 0 \pmod{81L_k} && \text{if } k \equiv 4 \pmod 6. \end{aligned}$$

Corollary L. *Let f be an eigenform of level 1 and weight k. If $k \equiv 0, 2 \pmod 6$, then $a_2(f) \equiv \pm\sigma_{k-1}(2) \pmod{27\overline{\mathbb{Z}}_3}$. If $k \equiv 4 \pmod 6$, then $a_2(f) \equiv 0 \pmod{9\overline{\mathbb{Z}}_3}$. In particular, Conjecture 9.1 of [17] holds for every eigenform of level 1.*

Proof. Let $\lambda = a_2(f)$. As in the proof of Corollary J, Theorem K gives $\lambda^2 - s^2 \in 81\overline{\mathbb{Z}}_3$ if $k \equiv 0, 2 \pmod 6$, and $\lambda^2 + 9\lambda \in 81\overline{\mathbb{Z}}_3$ if $k \equiv 4 \pmod 6$.

If $k \equiv 4 \pmod 6$ and $v_3(\lambda) < 2$, then $v_3(\lambda + 9) = v_3(\lambda)$ and $v_3(\lambda^2 + 9\lambda) = 2v_3(\lambda) < 4$, which is excluded; hence $\lambda \in 9\overline{\mathbb{Z}}_3$.

If $k \equiv 0, 2 \pmod 6$, then $3 \nmid k - 1$, hence $s \equiv 3(k - 1) \equiv \pm 3 \pmod 9$ and $v_3(s) = 1$. From $\lambda^2 \equiv s^2 \pmod{81}$ we get $v_3(\lambda) = 1$. The elements $\lambda - s$ and $\lambda + s$ lie in $3\overline{\mathbb{Z}}_3$, and their sum 2λ has valuation 1: one of the two has valuation exactly 1, and the other, whose product with the first lies in $81\overline{\mathbb{Z}}_3$, has valuation ≥ 3. Hence $\lambda \equiv \pm s \pmod{27\overline{\mathbb{Z}}_3}$; reducing modulo 9, $\lambda \equiv 3$ or $6 \pmod{9\overline{\mathbb{Z}}_3}$. □

STATUS: **PROVED**. From Theorem K, whose proof is completed below (Lemma 8). The same consequences follow from [18, Thm 1.5], obtained independently by another method.

Lemma 7 (a vanishing criterion)**.** *Let $n \ge 1$ and $r \in \{0, 1, 2\}$. Let $\mathcal{H}$ be a system of integral representatives of $\mathrm{GL}_2(\mathbb{F}_3)/\{\pm 1\}$, and let $X = \sum_g c_g\, g$ be a finite combination, with integer coefficients, of integer matrices g with determinant prime to 3. Write $g \equiv \pm h_g \kappa_g \pmod{3^n}$ with $h_g \in \mathcal{H}$ and $\kappa_g = \left(\begin{smallmatrix} p & q \\ u & v \end{smallmatrix}\right) \equiv I \pmod 3$. For $\delta \in \mathbb{Z}$ and $A, B \ge 0$, put*

$$c_{\delta,A,B}(\kappa_g) = \sum u^a\, q^b\, (p - 1)^m\, (v - 1)^{m'} \tbinom{A}{a} \tbinom{B}{b},$$

the sum running over the $a, b, m, m' \geq 0$ such that $b - a = \delta$, $a + m = A$ and $b + m' = B$; and, for $h \in \mathcal{H}$,

$$f_{h,\delta}(i,t) = \sum_{h_g = h} c_g \sum_{A+B<n} c_{\delta,A,B}(\kappa_g) \tbinom{i}{A} \tbinom{3t+r-i}{B},$$

where $\binom{z}{B} = z(z-1)\cdots(z-B+1)/B!$. If, for all h, δ and $A + B < n$, the finite difference $\Delta_i^A \Delta_t^B f_{h,\delta}(0,0)$ is divisible by 3^n, then $\sigma_X(\mathbb{Z}[x,y]_w) \subset 3^n \mathbb{Z}[x,y]_w$ for every even w such that $w \equiv r \pmod 3$.

Proof. Let w be even, $w = 3t + r$. The operator σ_g modulo 3^n depends only on g modulo 3^n, and $\sigma_{-g} = \sigma_g$; hence $\sigma_g \equiv \sigma_{h_g} \sigma_{\kappa_g}$. For $\kappa = \left(\begin{smallmatrix} p & q \\ u & v \end{smallmatrix}\right)$ and $i + j = w$,

$$\sigma_\kappa(x^i y^j) = (px + uy)^i (qx + vy)^j = \sum_{a,b} \tbinom{i}{a} \tbinom{j}{b} p^{i-a} u^a \, q^b v^{j-b} \, x^{i-a+b} y^{j+a-b}.$$

Expand $p^{i-a} = \sum_m \binom{i-a}{m} (p-1)^m$ and $v^{j-b} = \sum_{m'} \binom{j-b}{m'} (v-1)^{m'}$, and use $\binom{i}{a}\binom{i-a}{m} = \binom{i}{a+m}\binom{a+m}{a}$. The terms with $a + b + m + m' \geq n$ are divisible by 3^n, since u, q, $p - 1$ and $v - 1$ are divisible by 3. We get

$$\sigma_X(x^i y^{w-i}) \equiv \sum_{h \in \mathcal{H}} \sigma_h \Big(\sum_\delta f_{h,\delta}(i,t) \, x^{i+\delta} y^{w-i-\delta} \Big) \pmod{3^n}.$$

The polynomial $f_{h,\delta}$ has total degree $< n$ and takes integer values on $\mathbb{Z}^2$; by Newton's formula, $f_{h,\delta}(i,t) = \sum_{A+B<n} \Delta_i^A \Delta_t^B f_{h,\delta}(0,0) \binom{i}{A}\binom{t}{B}$. Under the hypothesis, all its values are divisible by 3^n, and $\sigma_X(x^i y^{w-i}) \in 3^n \mathbb{Z}[x,y]_w$ for every i. □

Lemma 8 (three certificates)**.** *Let $\mathcal{T} = \sum_{M \in \mathcal{M}_2} M$ and $\Lambda_2 = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, and put $\Xi_\sigma = \mathcal{T}^2 - (1 + 2\Lambda_2)^2$ and $\Xi_4 = \mathcal{T}^2 + 9\mathcal{T}$. There are explicit elements $\zeta_0, \zeta_1, \zeta_2 \in \mathcal{I}$, sums of 977, 1005 and 1079 terms, such that $\Xi_\sigma - \zeta_0$, $\Xi_\sigma - \zeta_1$ and $\Xi_4 - \zeta_2$ satisfy the hypothesis of Lemma 7 with $n = 4$ and $r = 0$, 1, 2 respectively.*

Proof. Each term has the form $c\,\gamma\,h\,(\kappa_1 - 1)^{\alpha_1}(\kappa_2 - 1)^{\alpha_2}(\kappa_3 - 1)^{\alpha_3}(\kappa_4 - 1)^{\alpha_4}$, with c an integer, $\gamma \in \{1 + S, 1 + U + U^2, 1 + \varepsilon\}$, $h \in \mathcal{H}$, $\kappa_1 = \left(\begin{smallmatrix} 4 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\kappa_2 = \left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right)$, $\kappa_3 = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)$, $\kappa_4 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ and $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \leq 3$; it belongs to $\mathcal{I}$, which is a right ideal. Checking the hypothesis of Lemma 7 is a finite exact computation: one expands $\Xi - \zeta_r$ as a combination of matrices modulo 81, then computes the finite differences. This computation, and the three certificates, are in `VERIF_A2.py`. □

Proof of Theorem K. Let $P \in L_k$, $w = k - 2$ and $r \in \{0, 1, 2\}$ such that $w \equiv r \pmod 3$: $r = 0$ if $k \equiv 2 \pmod 6$, $r = 1$ if $k \equiv 0 \pmod 6$ and $r = 2$ if $k \equiv 4 \pmod 6$. Let $\Xi = \Xi_\sigma$ if $r \leq 1$, $\Xi = \Xi_4$ if $r = 2$, and $\zeta = \zeta_r$. Since $\mu_{P|\gamma} = \mu_P \circ \sigma_\gamma$ and Λ_2 acts on $\mathbb{Z}[x,y]_w$ by 2^w, the form $\mu_P \circ \sigma_\Xi$ is that of $P|\widetilde{T}_2^2 - s^2 P$ if $r \leq 1$, of $P|\widetilde{T}_2^2 + 9\,P|\widetilde{T}_2$ if $r = 2$. One has $\mu_P \circ \sigma_\zeta = 0$ since $\zeta \in \mathcal{I}$, and, by Lemmas 7 and 8, $\sigma_{\Xi - \zeta}(F) \in 81\mathbb{Z}[x,y]_w$ for every F. Since μ_P takes integer values on $\mathbb{Z}[x,y]_w$, we get $\mu_P(\sigma_\Xi F) \equiv 0 \pmod{81}$ for every F: the polynomial under consideration lies in $81 B_w \cap W^- = 81 L_k$. □

Status: **PROVED**. Finite exact computation (Lemma 8), checked by `VERIF_A2.py` (part E). Checks: direct action of the remainders $\Xi - \zeta_r$ on $\mathbb{Z}[x,y]_w$ modulo 81 for all even $w \leq 60$ in the relevant class (part G); congruences of Theorem K checked directly on L_k for $12 \leq k \leq 290$ and, if $k \equiv 4 \pmod 6$, up to $k = 334$ (PARI/GP). For $k \equiv 0, 2 \pmod 6$, an operator congruence of the same kind for T_2^2 modulo 81, on a lattice of even modular symbols, appears independently in [18, §5.2.2].

Remark. Theorem K implies Theorem I, given $\widetilde{T}_2(L_k) \subset 3L_k$ (Lemma 4). For $k \equiv 4 \pmod 6$, one does not have $\widetilde{T}_2(L_k) \subset 9L_k$ in general (for example for $k = 40$): the quadratic congruence of Theorem K is the natural form of the statement. Corollaries J and L contain [4, Thm 1.2 and

Cor. 1.3]; the difference is that the congruences of Theorems I and K concern the operator $\widetilde{T}_2$ acting on the whole lattice L_k, and therefore pass to all eigenvalues, whatever the coefficient field. For the rational forms of weights 12, 18, 20 and 26, one has $a_2 = -24$, -528, 456, -48, and even $a_2 \equiv -s \pmod{27}$; for example $\tau(2) = -24 \equiv -2049 \pmod{27}$. For $k = 16$ and 22, $a_2 = 216$ and -288 are divisible by 9.

Theorem M (level 1 case of the Coleman–Stein conjecture)**.** *Let f be an eigenform of level* 1 *and weight k. Then $a_3(f) \equiv 0 \pmod{9\overline{\mathbb{Z}}_3}$, and f is congruent modulo $9\overline{\mathbb{Z}}_3$, coefficient by coefficient, to one of the five eigenforms of the table of [6]: the one of weight* 16 *if $k \equiv 4 \pmod 6$; the one of weight* 12 *or the one of weight* 24 *if $k \equiv 0 \pmod 6$, and the one of weight* 32 *or the one of weight* 20 *if $k \equiv 2 \pmod 6$, according as $a_2(f) \equiv 3$ or $6 \pmod{9\overline{\mathbb{Z}}_3}$.*

Proof. This is the proof of Theorem H, with Corollaries J and L in place of Conjecture 9.1. □

STATUS: **PROVED**. A consequence of [17, Thm 7.2, Prop. 9.3], of [9] (Theorem F) and of Corollaries J and L, without any hypothesis on k or on the coefficient field. This statement also follows from [18, Thm 1.5], obtained independently by another method.

6 An Eisenstein law modulo 81

We write χ for the Dirichlet character of conductor 3 ($\chi(n) = 1$ if $n \equiv 1$, -1 if $n \equiv 2 \pmod 3$), $\mathbf{1}_3$ for the principal character modulo 3, $\sigma(n) = \sigma_{k-1}(n)$ and, for a prime $\ell \neq 3$, $s_\ell = \sigma_{k-1}(\ell) = 1 + \ell^{k-1}$. If $\ell \equiv 2 \pmod 3$, $v_3(s_\ell) = v_3(\ell+1) + v_3(k-1)$; for $\ell \not\equiv -1 \pmod 9$ (for example $\ell = 2, 5, 11$), this equals 1 if $k \not\equiv 4 \pmod 6$ and is at least 2 otherwise.

6.1 Other operators T_ℓ

Theorem K extends to other primes by the same method: $\widetilde{T}_\ell = \sum_{M \in \mathcal{M}_\ell} M$ replaces $\widetilde{T}_2$ ($|\mathcal{M}_\ell| =$ 15, 25, 54, 77, 93, 109 for $\ell = 5, 7, 11, 13, 17, 19$), $\Lambda_\ell = \left(\begin{smallmatrix} \ell & 0 \\ 0 & \ell \end{smallmatrix}\right)$, which acts on $\mathbb{Z}[x,y]_w$ by ℓ^w, replaces Λ_2, and Lemma 7 applies with any modulus 3^n.

Theorem N (T_ℓ modulo 81 and 243, $\ell \leq 19$)**.** *Let $k \geq 12$ be even and $P \in L_k$.*

(a) For $\ell \in \{7, 13\}$: $P|\widetilde{T}_\ell \equiv s_\ell P \pmod{81 L_k}$ if $k \not\equiv 4 \pmod 6$, and $\pmod{27 L_k}$ if $k \equiv 4 \pmod 6$. For $\ell = 19$: the same congruences modulo $243 L_k$ and $81 L_k$ respectively.

(a′) If $k \equiv 4 \pmod 6$: $P|\widetilde{T}_7 - s_7 P - 18\, P|\widetilde{T}_2 \equiv 0 \pmod{81 L_k}$.

(a″) If $k \equiv 4 \pmod 6$: $P|\widetilde{T}_{19} - s_{19} P - 54\, P|\widetilde{T}_2 \equiv 0 \pmod{243 L_k}$.

(b) For $\ell \in \{5, 11\}$ and $k \not\equiv 4 \pmod 6$: $P|\widetilde{T}_\ell^2 \equiv s_\ell^2 P \pmod{81 L_k}$; for $\ell = 17$, modulo $243 L_k$.

(c) For $\ell \in \{5, 11\}$ and $k \equiv 4 \pmod 6$: there are explicit polynomials $a_\ell, b_\ell \in (\mathbb{Z}/81\mathbb{Z})[X]$ of degree 5, with $b_\ell(\ell^w) \equiv 0$ and $a_\ell(\ell^w) \equiv 0 \pmod 9$ for every even $w \equiv 2 \pmod 3$, such that $P|\widetilde{T}_\ell^2 + a_\ell(\ell^w)\, P|\widetilde{T}_\ell + b_\ell(\ell^w) P \equiv 0 \pmod{81 L_k}$.

In particular, for every eigenform f of level 1 *and weight k, $a_7(f) \equiv s_7 \pmod{81\overline{\mathbb{Z}}_3}$ and $a_{19}(f) \equiv s_{19} \pmod{243\overline{\mathbb{Z}}_3}$ whatever k.*

Proof. Each congruence on L_k is established by a certificate $\zeta \in \mathcal{I}$ and the criterion of Lemma 7, exactly as in Lemma 8: nineteen certificates (from 229 to 1600 terms), all checked by `VERIF_EISENSTEIN.py`, which also checks, for (c), the two conditions on $a_\ell(\ell^w)$ and $b_\ell(\ell^w)$ (they depend only on ℓ^w modulo 81, which takes 27 values). For the last assertion, if $k \equiv 4 \pmod 6$, (a′) gives $a_7 - s_7 \equiv 18\, a_2 \pmod{81}$ and (a″) gives $a_{19} - s_{19} \equiv 54\, a_2 \pmod{243}$, and $9 \mid a_2$ (Corollary L). □

STATUS: **PROVED**. Finite exact computation. For $\ell = 7$, the congruence modulo 9 is [17, Prop. 9.3]; the congruence $a_7 \equiv s_7$ modulo 81 in the valuative sense is also in [18, (5.5)].

6.2 The law

We use the full Hecke algebra $\mathbb{T} = \mathbb{T}(3, \mathbb{Z}_3)$ of [17]: it acts on the space $D(3, \cdot)$ of divided congruences (Katz) of cusp forms of level 3, is generated by the T_n, $3 \nmid n$, and by U, and contains the operator $t = [1+3]$ of the action of $\mathbb{Z}_3^\times$, which acts by x^k on forms of weight k, so that t acts by $t_k = 4^k$. Let V^{par} be the space of cuspidal 3-adic modular functions of tame level 1 (in Katz's sense: vanishing at all cusps of the Igusa tower), and $V \supset V^{\mathrm{par}}$ that of all 3-adic modular functions of tame level 1. For every finite quotient R of the ring of integers O of a finite extension of $\mathbb{Q}_3$, one has $D(3,R) = D(3,O) \otimes R = V^{\mathrm{par}}(O) \otimes R$ [17, Prop. 2.1 and Lemma 3.1]. We use three of its properties.

(F1) [17, Thm 7.2(ii)]: $\mathbb{T}$ is local, with residue field $\mathbb{F}_3$, and the set $\mathcal{S} = \{U, T_2, 1+T_7, t-1\}$ generates it as a $\mathbb{Z}_3$-algebra (by Nakayama's lemma: $\mathfrak{m} = (3, \mathcal{S}) + \mathfrak{m}^2$). By induction, $\mathbb{T} = \mathbb{Z}_3[\mathcal{S}] + \mathfrak{m}^N$ for every N; since every finite quotient of $\mathbb{T}$ is local Artinian, hence killed by a power of $\mathfrak{m}$, the image of $\mathbb{T}$ in every finite quotient is that of $\mathbb{Z}_3[\mathcal{S}]$.

(F2) [17, Thm 2.2, Prop. 3.3] (Katz): the q-expansion is injective on $V^{\mathrm{par}}(O)$. If $F \in V^{\mathrm{par}}(O)$ satisfies $a_1(F) = 1$ and is an eigenvector of the T_n ($3 \nmid n$) and of U, its reduction modulo 81 is an element of $D(3, O/81) = V^{\mathrm{par}}(O) \otimes O/81$ which is an eigenvector of $\mathbb{T}$, and $\tau \mapsto a_1(\tau F)$ defines a character $\varphi_F : \mathbb{T} \to O/81O$, with $\varphi_F(T_n) = a_n(F)$ for $3 \nmid n$ (since $a_1(T_n G) = a_n(G)$). Moreover $V^{\mathrm{par}}(O)$ is saturated in $O[[q]]$: if the expansion of $F \in V^{\mathrm{par}}(O)$ lies in $3\,O[[q]]$, then $F \in 3V^{\mathrm{par}}(O)$, since $D(3, O/3) = V^{\mathrm{par}}(O) \otimes O/3$ injects into $(O/3)[[q]]$.

(F3) If $G \in V(O)$ is an eigenvector of weight k of the T_ℓ ($\ell \neq 3$), with eigenvalues λ_ℓ, the series $\theta^j G = \sum n^j a_n(G) q^n$, $\theta = q\,d/dq$, is a 3-adic modular form in Serre's sense [19], a limit of forms of level 1 with coefficients in O, hence an element of $V(O)$ [13]; it has weight $k + 2j$ (the action of $x \in \mathbb{Z}_3^\times$ is multiplied by x^{2j}), and is an eigenvector with eigenvalues $\ell^j \lambda_\ell$. Since x acts by a scalar, the constant term of $\theta^j G$, which vanishes at the cusp ∞, vanishes at all cusps: $\theta^j G \in V^{\mathrm{par}}(O)$. For $j = 2 \cdot 3^m$ (resp. $j = 3^m$), n^j tends, as $m \to \infty$, to $\mathbf{1}_3(n)$ (resp. $\chi(n)$), uniformly in n. The limits $G \otimes \mathbf{1}_3 = \sum_{3 \nmid n} a_n(G) q^n$ and $G \otimes \chi$ are therefore in $V^{\mathrm{par}}(O)$, eigenvectors of the T_ℓ with eigenvalues λ_ℓ and $\chi(\ell)\lambda_\ell$, killed by U, and t acts on them by the same scalar as on G (since $4^{2j} \to 1$).

Theorem O (Eisenstein law modulo 81)**.** *Let f be a normalised cuspidal eigenform of level* 1 *and weight k, and fix an embedding of its coefficient field into $\overline{\mathbb{Q}}_3$.*

(i) For every $n \equiv 1 \pmod 3$: $a_n(f) \equiv \sigma_{k-1}(n) \pmod{81\overline{\mathbb{Z}}_3}$.

(ii) If $k \not\equiv 4 \pmod 6$, let $\psi = \mathbf{1}_3$ if $a_2(f) \equiv s_2 \pmod{27}$ and $\psi = \chi$ if $a_2(f) \equiv -s_2 \pmod{27}$ (Corollary L); then $a_n(f) \equiv \psi(n)\,\sigma_{k-1}(n) \pmod{27\overline{\mathbb{Z}}_3}$ for every n prime to 3.

(iii) If $k \equiv 4 \pmod 6$: $a_n(f) \equiv \sigma_{k-1}(n) \pmod{9\overline{\mathbb{Z}}_3}$ for every n prime to 3.

Proof. Let O be the ring of integers of a finite extension of $\mathbb{Q}_3$ containing the coefficients of f, and $R = O/81O$. The weight k being fixed, let $E = -\frac{2k}{B_k} G_k$, where $G_k = -\frac{B_k}{2k} + \sum \sigma(n) q^n$; by von Staudt–Clausen, $v_3(B_k) = -1$, hence $c = -2k/B_k$ satisfies $v_3(c) = 1 + v_3(k) \geq 1$, and $E = 1 + c\sum \sigma(n) q^n$ is a form of level 1 with coefficients in $\mathbb{Z}_3$, hence an element of $V(\mathbb{Z}_3)$. By (F3), applied to f and to E, then the saturation (F2) (to divide by c), the four series

$$f \otimes \mathbf{1}_3, \qquad f \otimes \chi, \qquad E^{\mathbf{1}} = \sum_{3 \nmid n} \sigma(n) q^n, \qquad E^{\chi} = \sum_{3 \nmid n} \chi(n)\sigma(n) q^n$$

lie in $V^{\mathrm{par}}(O)$, with $a_1 = 1$, are eigenvectors of the T_ℓ, are killed by U, and t acts on them by t_k. By (F2), they define four characters $\varphi, \varphi^\chi, \varphi_E, \varphi_E^\chi : \mathbb{T} \to R$. On the generators of (F1), they take the values

$$U \mapsto 0, \qquad t \mapsto t_k, \qquad T_2 \mapsto a_2,\ -a_2,\ s_2,\ -s_2, \qquad 1+T_7 \mapsto 1+a_7,\ 1+a_7,\ 1+s_7,\ 1+s_7,$$

and $a_7 \equiv s_7 \pmod{81}$ (Theorem N). Let n be prime to 3. The image of $\mathbb{T}$ in R^4 is finite; (F1) therefore provides a polynomial P with coefficients in $\mathbb{Z}_3$ such that T_n and $P(U, T_2, 1+T_7, t)$ have the same image under the four characters. Put $Q(x) = P(0, x, 1+s_7, t_k) \in R[x]$. Then

$$a_n(f) \equiv Q(a_2), \quad \chi(n)a_n(f) \equiv Q(-a_2), \quad \sigma(n) \equiv Q(s_2), \quad \chi(n)\sigma(n) \equiv Q(-s_2) \pmod{81}.$$

(i) If $n \equiv 1 \pmod 3$, write $Q(x) = Q_0(x^2) + xQ_1(x^2)$. From $Q(a_2) \equiv Q(-a_2)$ we get $2a_2Q_1(a_2^2) \equiv 0$, and likewise for s_2; hence $a_n(f) \equiv Q_0(a_2^2)$ and $\sigma(n) \equiv Q_0(s_2^2)$. Now $a_2^2 \equiv s_2^2 \pmod{81}$: this is Theorem K if $k \not\equiv 4 \pmod 6$; if $k \equiv 4 \pmod 6$, one has $a_2^2 \equiv 0$ and $s_2^2 \equiv 0 \pmod{81}$, since $9 \mid a_2$ (Corollary L) and $9 \mid s_2$. Hence $a_n(f) \equiv \sigma(n) \pmod{81}$.

(ii) If $\psi(2)s_2 \equiv a_2 \pmod{27}$, then $Q(a_2) \equiv Q(\psi(2)s_2) \pmod{27}$, that is, $a_n(f) \equiv \psi(n)\sigma(n) \pmod{27}$.

(iii) If $k \equiv 4 \pmod 6$, $a_2 \equiv s_2 \equiv 0 \pmod 9$, hence $a_n(f) \equiv Q(a_2) \equiv Q(s_2) \equiv \sigma(n) \pmod 9$. □

Status: **PROVED**. From [17, Prop. 2.1, Thm 2.2, Lemma 3.1, Prop. 3.3, Thm 7.2(ii)], from the theory of 3-adic modular forms [19, 13] and from Theorems K and N. The principle — $a_n(f)$ is a polynomial in the eigenvalues of the generators of $\mathbb{T}$ — is that of the proof of Theorem 8.1 of [17] ($a_\ell \equiv 1 + \ell^{k-1} \pmod{128}$ for odd ℓ, at $p = 2$). Statements (ii) and (iii) can also be read off from the literal classification modulo 27 of [18, Thm 1.5]. Independent check, by Sturm's theorem: the series $\sum_{n\equiv 1(3)}(a_n(f) - \sigma(n))q^n = \frac{1}{2}\big((f - E') \otimes \mathbf{1}_3 + (f - E') \otimes \chi\big)$, where $E' = \sum_{n\geq 1}\sigma(n)q^n$, lies in $M_k(\Gamma_0(9))$ (the constant term of G_k disappears under twisting), and the index of $\Gamma_0(9)$ is 12; it therefore suffices to check (i) for $n \leq k$. This check was made for every $k \leq 212$ (Newton polygons of charpoly$(T_n - \sigma(n))$ on S_k, PARI/GP), and (ii) for $k \leq 140$ on an eigenbasis embedded in $\overline{\mathbb{Q}}_3$; part C of `VERIF_EISENSTEIN.py` redoes (i) for $k \leq 44$ on the lattice L_k.

Remark. (1) Statement (i) is equivalent, by multiplicativity, by Chebotarev's theorem and by the identity $\operatorname{tr} g \operatorname{tr} h = \operatorname{tr} gh + \det g \operatorname{tr} g^{-1}h$ (which reduces $a_\ell a_{\ell'}$, $\ell \equiv \ell' \equiv 2 \pmod 3$, to traces on the subgroup of index 2), to: $\operatorname{tr}\rho_f(g) \equiv 1 + \chi_{\mathrm{cyc}}^{k-1}(g) \pmod{81}$ for every g in the absolute Galois group of $\mathbb{Q}(\sqrt{-3})$, where ρ_f is the 3-adic representation of f. For $\ell \equiv 2 \pmod 3$, it gives $a_\ell^2 \equiv s_\ell^2 \pmod{81}$ (via $a_{\ell^2} = a_\ell^2 - \ell^{k-1}$), hence $a_\ell \equiv \pm s_\ell \pmod{27}$ if $v_3(s_\ell) = 1$ (that is, $\ell \not\equiv -1 \pmod 9$ and $k \not\equiv 4 \pmod 6$), and $a_\ell \equiv 0 \pmod 9$ otherwise: Theorem O contains Conjecture 9.1 of [17] and, modulo 9, its analogue for every prime $\ell \equiv 2 \pmod 3$.

(2) For Δ, (i) and (ii) are contained in Swinnerton-Dyer's theorem $\tau(n) \equiv n^{-610}\sigma_{1231}(n) \pmod{3^6}$ for $3 \nmid n$ [22]: since $(\mathbb{Z}/81\mathbb{Z})^\times$ is cyclic of order 54, one has $n^{27} \equiv \chi(n) \pmod{81}$; for $de = n$, $n^{-610}d^{1231} \equiv d^{27}e^{38} \equiv \chi(n)\, e^{11} \pmod{81}$, whence $\tau(n) \equiv \chi(n)\,\sigma_{11}(n) \pmod{81}$ for $3 \nmid n$. Modulo 3, (i) to (iii) give back Hatada's theorem $a_\ell \equiv 1 + \ell \pmod 3$ [9]. Modulo 9, (ii), (iii) and $a_3 \equiv 0 \pmod 9$ give exactly the five classes of [6]: two for $k \equiv 0$ and two for $k \equiv 2 \pmod 6$ (according to ψ), one for $k \equiv 4 \pmod 6$.

(3) The statements are optimal: (ii) is false modulo 81 (for $k = 18$, $a_2 + s_2 = -528 + 131073 = 27\cdot 4835$, $3 \nmid 4835$), and for $k \equiv 4 \pmod 6$ nothing survives beyond $a_\ell \equiv 0 \pmod 9$, $\ell \equiv 2 \pmod 3$ (for $k = 40$, the three values of $a_2/9$ modulo 3 are 0, 1 and 2).

(4) The depth of (i) increases by one when $\ell \equiv \pm 1 \pmod 9$: this is Corollary Q of §7, which also describes the other classes modulo 243, and Theorem R gives depth 6 when ℓ splits completely in $\mathbb{Q}(\zeta_9, \sqrt[3]{3})$ or $\ell \equiv -1 \pmod 9$.

7 A Galois law modulo 243 and 729

Let f be a normalised cuspidal eigenform of level 1 and weight k, O the ring of integers of a finite extension of $\mathbb{Q}_3$ containing its coefficients, and $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(O)$ its 3-adic representation [7]: it is unramified outside 3, $\operatorname{tr}\rho_f(\mathrm{Frob}_\ell) = a_\ell$ and $\det\rho_f = \chi^{k-1}$, where χ is the 3-adic cyclotomic character. We put $T = \operatorname{tr}\rho_f$, $D = \chi^{k-1}$, $T_E = 1 + \chi^{k-1}$ (trace of $\mathbf{1} \oplus \chi^{k-1}$), $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$

and $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. On G_K, $\chi \equiv 1 \pmod 3$; we define two homomorphisms $u, v : G_K \to \mathbb{Z}/3\mathbb{Z}$ by

$$\chi(g) \equiv 1 + 3u(g) \pmod 9, \qquad g(\sqrt[3]{3}) = \zeta_3^{v(g)} \sqrt[3]{3}.$$

Thus $u(\mathrm{Frob}_\mathfrak{l}) = 0$ if and only if $\ell \equiv 1 \pmod 9$, and $v(\mathrm{Frob}_\mathfrak{l}) = 0$ if and only if 3 is a cube modulo ℓ ($\mathfrak{l} \mid \ell$, $\ell \equiv 1 \pmod 3$); $\ker u \cap \ker v = G_{\mathbb{Q}(\zeta_9, \sqrt[3]{3})}$.

Lemma 9 (Fricke reduction)**.** *Let Γ be a group, A a commutative ring, $D : \Gamma \to A^\times$ a homomorphism and $T : \Gamma \to A$ a function such that $T(1) = 2$, $T(gh) = T(hg)$ and*

$$T(gh) + D(g)\,T(g^{-1}h) = T(g)\,T(h) \qquad (g, h \in \Gamma). \tag{1}$$

For every word W in the free group on two letters, there is a polynomial $P_W \in \mathbb{Z}[t_1, t_2, t_3, d_1^{\pm 1}, d_2^{\pm 1}]$, depending only on W, such that $T(W(x,y)) = P_W(T(x), T(y), T(xy), D(x), D(y))$ for all Γ, A, D, T as above and all $x, y \in \Gamma$.

Proof. For $a, b, z \in \Gamma$, (1) with $(g, h) = (z, zba)$ and invariance under conjugation give

$$\text{(R1)}\quad T(az^2b) = T(z)T(azb) - D(z)T(ab), \qquad \text{(R2)}\quad T(az^{-1}b) = D(z)^{-1}\big(T(z)T(ab) - T(azb)\big),$$

(R2) being obtained by applying (R1) to (az^{-1}, z, b). We argue by induction on the pair (length of W, number of negative exponents), ordered lexicographically, W being taken cyclically reduced (which does not change T). If a syllable of W has an exponent ≥ 2, (R1) reduces to shorter words; if a syllable has a negative exponent, (R2) reduces to a shorter word and to a word of the same length with one negative exponent fewer; otherwise W is 1, x, y, or conjugate to $(xy)^m$, $m \geq 1$, and (R1) with $z = xy$ gives $T((xy)^m) = T(xy)T((xy)^{m-1}) - D(x)D(y)T((xy)^{m-2})$. The algorithm depends only on W. □

For traces of 2×2 matrices, this is the classical theorem of Fricke and Vogt [8]; (1) holds for $T = \mathrm{tr}\,\rho$, $D = \det\rho$, by Cayley–Hamilton ($g + \det(g)g^{-1} = \mathrm{tr}(g)$).

Lemma 10 (the group)**.** *Let E be the maximal pro-3-extension of K unramified outside 3 and $\widehat{G} = \mathrm{Gal}(E/K)$.*

(a) The cyclic extensions of degree 3 of K unramified outside 3 are the subfields of degree 3 of $K(\zeta_9, \sqrt[3]{3})$; u and v factor through $\widehat{G}$ and $(u, v) : \widehat{G} \to (\mathbb{Z}/3\mathbb{Z})^2$ is surjective.

(b) Two elements $x, y \in \widehat{G}$ such that $(u, v)(x) = (1, 0)$ and $(u, v)(y) = (0, 1)$ topologically generate $\widehat{G}$.

(c) T, D and T_E, restricted to G_K, factor through $\widehat{G}$.

Proof. (a) K contains μ_3 and has class number one; by Kummer theory, such an extension is $K(\sqrt[3]{a})$ with $a \in O_K[1/3]^\times$, and $O_K[1/3]^\times/(O_K[1/3]^\times)^3$ has dimension 2, generated by ζ_3 and $1 - \zeta_3$, or equally by ζ_3 and $3 = -\zeta_3^2(1 - \zeta_3)^2$; and $K(\sqrt[3]{\zeta_3}) = K(\zeta_9)$. (b) $\widehat{G}$ is a pro-3-group and $\mathrm{Hom}(\widehat{G}, \mathbb{Z}/3\mathbb{Z})$ is generated by u, v; this is Burnside's basis theorem [11]. (c) By Chebotarev and Hatada's congruence $a_\ell \equiv 1 + \ell^{k-1} \pmod 3$ [9], $T \equiv 2$ and $D \equiv 1 \pmod 3$ on G_K: every $\rho_f(g)$, $g \in G_K$, has characteristic polynomial $(X - 1)^2$ modulo the maximal ideal, so the image of $\rho_f(G_K)$ in GL_2 of the residue field consists of unipotents and is a 3-group; the kernel of the reduction being a pro-3-group, $\rho_f(G_K)$ is a pro-3-group, and ρ_f being unramified outside 3, $\rho_f|_{G_K}$ factors through $\widehat{G}$. Likewise for $\chi|_{G_K}$, with values in $1 + 3\mathbb{Z}_3$. □

By Shafarevich [20], $\widehat{G}$ is even free on two generators; this fact is used only in §9. This group, and the two conditions "ℓ modulo 9" and "3 a cube modulo ℓ", also govern the structure of the Hecke algebra of level 1 *modulo* 3 [1, 15]; the statements below concern the eigenvalues in characteristic 0.

Lemma 11 (a quadratic form)**.** *Let O' be the ring of integers of a finite extension of $\mathbb{Q}_3$, and $T_1, T_2 : \widehat{G} \to O'$ two continuous functions satisfying the hypotheses of Lemma 9 with the same D, where $D \equiv 1$ and $T_2 \equiv 2 \pmod 3$. If $T_1 - T_2 \in 3^n O'$ with $n \geq 1$, there are $\alpha, \beta, \gamma \in O'/3O'$ such that*

$$T_1(g) - T_2(g) \equiv 3^n\big(\alpha\, u(g)^2 + \beta\, u(g)v(g) + \gamma\, v(g)^2\big) \pmod{3^{n+1}O'} \qquad (g \in \widehat{G}).$$

If moreover T_1 and T_2 are invariant under an automorphism σ of $\widehat{G}$ such that $u \circ \sigma = u$ and $v \circ \sigma = -v$, then $\beta = 0$.

Proof. Let x, y be as in Lemma 10(b), $x_1 = x$, $x_2 = y$, $x_3 = xy$, and $\varepsilon = (T_1 - T_2)/3^n$ modulo 3. For a word W, Lemma 9 and Taylor's formula (the two points differ only in the first three coordinates, by at most 3^n, and $2n \geq n + 1$) give $\varepsilon(W) = \sum_j c_j(W)\varepsilon(x_j)$ with $c_j(W) = \partial_j P_W(2, 2, 2, 1, 1) \bmod 3$, since $T_2 \equiv 2$ and $D \equiv 1 \pmod 3$. For a quadratic form $Q = \alpha u^2 + \beta uv + \gamma v^2$ with coefficients in $O'/3$, the function $T_Q = 2 + \delta Q$, with values in $(O'/3)[\delta]/(\delta^2)$, with $D = 1$, satisfies the hypotheses of Lemma 9: this is the parallelogram identity $Q(a + b) + Q(b - a) = 2Q(a) + 2Q(b)$. Since $P_W(2, 2, 2, 1, 1) = 2$ (constant function $T = 2$, $D = 1$), we also have $Q(W) = \sum_j c_j(W)Q(x_j)$. Choose $\alpha = \varepsilon(x)$, $\gamma = \varepsilon(y)$, $\beta = \varepsilon(xy) - \alpha - \gamma$: then $\varepsilon = Q$ on the subgroup generated by x, y, which is dense by Lemma 10(b), hence everywhere by continuity. Finally, if σ exists, $\varepsilon \circ \sigma = \varepsilon$ gives $Q(a, -b) = Q(a, b)$, whence $2\beta = 0$ and $\beta = 0$. □

Conjugation by a complex conjugation c provides such a σ: E is Galois over $\mathbb{Q}$, $\chi(cgc^{-1}) = \chi(g)$, and, c fixing the real $\sqrt[3]{3}$ and sending ζ_3 to ζ_3^{-1}, $v(cgc^{-1}) = -v(g)$; T, D, T_E are class functions on $G_{\mathbb{Q}}$.

Theorem P (Galois law modulo 243)**.** *For every $g \in G_K$,*

$$\operatorname{tr} \rho_f(g) \equiv 1 + \chi(g)^{k-1} + \big(a_2^2 - s_2^2\big)\, u(g)^2 \pmod{243\, O}.$$

Proof. By Theorem O(i) and Chebotarev (the $\mathrm{Frob}_\mathfrak{l}$, $\mathfrak{l}$ of degree 1, are dense in G_K), $T - T_E \in 81O$ on G_K. Lemma 11 ($n = 4$, $T_1 = T$, $T_2 = T_E$, σ conjugation by c) gives $T - T_E \equiv 81(\alpha u^2 + \gamma v^2) \pmod{243}$. For the Frobenius element g_1 of the prime ideal $2O_K$ (inert, residue field $\mathbb{F}_4$), $g_1 = \mathrm{Frob}_2^2$, $\chi(g_1) = 4$, hence $u(g_1) = 1$, and $v(g_1) = 0$ since $3 = 1$ is a cube in $\mathbb{F}_4$; $T(g_1) = a_2^2 - 2 \cdot 2^{k-1}$, $T_E(g_1) = 1 + 4^{k-1}$, whence $81\alpha \equiv a_2^2 - s_2^2$. For $g_2 = \mathrm{Frob}_\mathfrak{l}$, $\mathfrak{l} \mid 19$: $u(g_2) = 0$ since $19 \equiv 1 \pmod 9$, $v(g_2) \neq 0$ since $3^6 \equiv 7 \pmod{19}$, whence $81\gamma \equiv a_{19} - s_{19} \equiv 0 \pmod{243}$ by Theorem N: (a) if $k \not\equiv 4 \pmod 6$, (a″) if $k \equiv 4 \pmod 6$. □

STATUS: **PROVED**. From Theorem O, hence from [17], and from Theorem N.

Corollary Q (primes)**.** *Let $\ell \neq 3$ be prime.*

(i) If $\ell \equiv 1 \pmod 3$: $a_\ell \equiv s_\ell \pmod{243}$ if $\ell \equiv 1 \pmod 9$, and $a_\ell \equiv s_\ell + a_2^2 - s_2^2 \pmod{243}$ if $\ell \equiv 4, 7 \pmod 9$.

(ii) If $\ell \equiv 2 \pmod 3$: $a_\ell^2 \equiv s_\ell^2 \pmod{243}$ if $\ell \equiv -1 \pmod 9$, and $a_\ell^2 \equiv s_\ell^2 + a_2^2 - s_2^2 \pmod{243}$ if $\ell \equiv 2, 5 \pmod 9$.

Proof. (i) $g = \mathrm{Frob}_\mathfrak{l}$. (ii) $g = \mathrm{Frob}_\ell^2$, the Frobenius of the inert ideal ℓO_K: $T(g) = a_\ell^2 - 2\ell^{k-1}$, $T_E(g) = 1 + \ell^{2k-2}$, $\chi(g) = \ell^2$, and $u(g) = 0$ if and only if $\ell \equiv \pm 1 \pmod 9$. □

In particular, the depth of the Eisenstein law increases by one for every $\ell \equiv \pm 1 \pmod 9$, in every weight. The correction $a_2^2 - s_2^2$ is necessary: without it, the congruence fails modulo 243 for $\ell = 7$, 31 and $\ell^2 = 25$ in all the weights $12 \leq k \leq 70$ examined except $k = 12$ and $k = 22$, where $a_2^2 \equiv s_2^2 \pmod{243}$.

Theorem R (modulo 729)**.** *For every* $g \in G_{\mathbb{Q}(\zeta_9,\sqrt[3]{3})}$, $\operatorname{tr}\rho_f(g) \equiv 1+\chi(g)^{k-1} \pmod{729\,O}$. *In particular* $a_\ell \equiv s_\ell \pmod{729}$ *if* $\ell \equiv 1 \pmod 9$ *and* 3 *is a cube modulo* ℓ*, and* $a_\ell^2 \equiv s_\ell^2 \pmod{729}$ *if* $\ell \equiv -1 \pmod 9$.

Proof. Put $\kappa = k-1$ and, for $g \in G_K$, $\lambda(g) = \frac{1}{3}\log_3\chi(g) \in \mathbb{Z}_3$; λ is a continuous homomorphism and $\lambda \equiv u \pmod 3$. For s in the ring of integers O' of a finite extension of $\mathbb{Q}_3$ containing O, let $\psi_s = \exp(3s\lambda)$, a continuous character of G_K with values in $O'^\times$, and $M_s = \psi_s + \chi^\kappa\psi_s^{-1}$, the trace of $\psi_s \oplus \chi^\kappa\psi_s^{-1}$; M_s satisfies (1) with the same D, is invariant under σ, and

$$M_s - T_E = -(e^A-1)(e^B-1), \qquad A = 3s\lambda, \quad B = 3(\kappa-s)\lambda.$$

Let $\alpha \in O/3$ be defined by $81\alpha \equiv a_2^2 - s_2^2 \pmod{243}$. If $3 \nmid \kappa$, take $s = 9t$ with $t \equiv -\alpha\kappa^{-1} \pmod 3$: $v_3(A) \ge 3$, $v_3(B) \ge 1$, and $M_s - T_E \equiv -AB \equiv -81t\kappa\lambda^2 \equiv 81\alpha u^2 \pmod{243}$ (the other terms of the expansion have valuation ≥ 5). If $3 \mid \kappa$ ($k \equiv 4 \pmod 6$), take $s = 3t$, where $t \in O'$ is a root of $X^2 - \frac{\kappa}{3}X - \tilde\alpha$ ($\tilde\alpha \in O$ lifting α): $v_3(A), v_3(B) \ge 2$ and $M_s - T_E \equiv -81t(\frac{\kappa}{3}-t)\lambda^2 \equiv 81\alpha u^2 \pmod{243}$. In both cases, Theorem P gives $T \equiv M_s \pmod{243O'}$ on G_K, and Lemma 11 ($n=5$, $T_1 = T$, $T_2 = M_s$) gives $T - M_s \equiv 243\,Q'(u,v) \pmod{729}$ for a quadratic form Q', which vanishes if $u = v = 0$. Finally, if $u(g) = 0$, then $3 \mid \lambda(g)$, hence $v_3(A) + v_3(B) \ge 6$ in both cases, and $v_3(M_s(g) - T_E(g)) = v_3(A) + v_3(B) \ge 6$. For the Frobenius of ℓO_K, $\ell \equiv -1 \pmod 9$, one has $u = 0$, and $v = 0$ since 3 is a cube in $\mathbb{F}_\ell^\times$, hence in $\mathbb{F}_{\ell^2}$. □

Status: **PROVED**. From Theorem P.

Theorem S (bilinear law)**.** *For a prime* $\ell \equiv 2 \pmod 3$*, let* $\tilde u(\ell) = -1,\ 1,\ 0$ *according as* $\ell \equiv 2,\ 5,\ 8 \pmod 9$*. For all primes* $\ell, \ell' \equiv 2 \pmod 3$*,*

$$a_\ell\, a_{\ell'} \equiv s_\ell\, s_{\ell'} + \tilde u(\ell)\tilde u(\ell')\big(a_2^2 - s_2^2\big) \pmod{243}.$$

Proof. Let g, g' be Frobenius elements at ℓ, ℓ'; gg' and $g^{-1}g'$ lie in G_K, and $T(g)T(g') = T(gg') + D(g)T(g^{-1}g')$, likewise for T_E. One has $-\ell \equiv 1 + 3\tilde u(\ell) \pmod 9$, hence $u(gg') = \tilde u(\ell) + \tilde u(\ell')$ and $u(g^{-1}g') = \tilde u(\ell') - \tilde u(\ell)$. By Theorem P, and $D(g) \equiv -1 \pmod 3$, $a_\ell a_{\ell'} - s_\ell s_{\ell'} \equiv (a_2^2 - s_2^2)\big((\tilde u + \tilde u')^2 - (\tilde u' - \tilde u)^2\big) = 4\tilde u\tilde u'(a_2^2 - s_2^2) \pmod{243}$, and $4 \equiv 1 \pmod 3$. □

Status: **PROVED**.

Corollary T (law modulo 81)**.** *If* $k \not\equiv 4 \pmod 6$*, for every prime* $\ell \equiv 2 \pmod 3$*,*

$$a_\ell \equiv \frac{s_2\, s_\ell - \tilde u(\ell)\,(a_2^2 - s_2^2)}{a_2} \pmod{81\overline{\mathbb{Z}}_3},$$

and, for every n *prime to* 3*,* $a_n(f)$ *modulo* 81 *depends only on* k *and on* $a_2(f)$ *modulo* 81*.*

Proof. Take $\ell' = 2$ in Theorem S ($\tilde u(2) = -1$) and divide by a_2, which has valuation 1 (Corollary L). The numerator modulo 243 and the quotient modulo 81 do not change if a_2 is replaced by $a_2 + 81e$. For $\ell \equiv 1 \pmod 3$, use Corollary Q(i), then multiplicativity and $a_{\ell^{r+1}} = a_\ell a_{\ell^r} - \ell^{k-1}a_{\ell^{r-1}}$. □

Modulo 27, this formula gives back Theorem O(ii) for $\ell \equiv 2 \pmod 3$; the corollary is the analogue modulo 81 of the classification of [6]. If $k \equiv 4 \pmod 6$ and $9 \parallel a_2$, the same division determines a_ℓ modulo 27 for $\ell \equiv 2 \pmod 3$: a_2 obeys no uniform law modulo 27 (Remark (3) of §6), but it governs the others.

Remark. **VERIFIED** (PARI/GP, exact Newton polygons on S_k). Theorem P for all primes $\ell < 200$ and $12 \le k \le 70$; Theorem S for 1836 pairs ($\ell, \ell' < 110$, $12 \le k \le 80$); $a_{19} \equiv s_{19} \pmod{243}$ for all $k \equiv 4 \pmod 6$, $k \le 298$. Minimal depth $\min v_3$ observed for $12 \le k \le 100$ (for $\ell \equiv -1 \pmod 9$, on $a_\ell^2 - s_\ell^2$): 5 for $\ell = 19, 37, 109, 127, 163, 181, 199$ (3 not a cube); 6 for $\ell = 73$ and for $\ell = 17, 71, 89, 179, 197, 233, 251$; 8 for $\ell = 53, 107, 269$ ($\ell \equiv -1 \pmod{27}$) and for $\ell = 271$ ($\equiv 1 \pmod{27}$, 3 a cube) if $k \not\equiv 4 \pmod 6$, 7 for $\ell = 271$ if $k \equiv 4 \pmod 6$. Theorems P and R explain exactly the depths 5 and 6; the depths 7 and 8 are treated in §9 (Theorems R′ and R″).

8 A 2-adic Galois law and the answer to Hatada's question

8.1 A 2-adic certificate

Lemma 7 holds, with the same proof, with 3 replaced by 2:

Lemma 12 (vanishing criterion, $p = 2$)**.** *Let $n \geq 1$, $\mathcal{H}_2$ a system of integral representatives of $\mathrm{GL}_2(\mathbb{F}_2)$, and $X = \sum_g c_g\, g$ a finite combination, with integer coefficients, of integer matrices with odd determinant. Write $g \equiv h_g \kappa_g \pmod{2^n}$ with $h_g \in \mathcal{H}_2$ and $\kappa_g \equiv I \pmod 2$, define $c_{\delta,A,B}$ as in Lemma 7, and then $f_{h,\delta}(i,t) = \sum_{h_g = h} c_g \sum_{A+B<n} c_{\delta,A,B}(\kappa_g)\binom{i}{A}\binom{2t-i}{B}$. If all the finite differences $\Delta_i^A \Delta_t^B f_{h,\delta}(0,0)$, $A + B < n$, are divisible by 2^n, then $\sigma_X(\mathbb{Z}[x,y]_w) \subset 2^n\mathbb{Z}[x,y]_w$ for every even w.*

Proof. That of Lemma 7: u, q, $p-1$, $v-1$ are divisible by 2, so the terms with $a+b+m+m' \geq n$ are divisible by 2^n, and $w = 2t$. □

Lemma 13 (a_5 modulo 512)**.** *There is an explicit element $\zeta \in \mathcal{I}$, a sum of 190 terms $c\,\gamma\, h\,(\kappa_1' - 1)^{\alpha_1} \cdots (\kappa_4' - 1)^{\alpha_4}$, with $\gamma \in \{1 + S, 1 + U + U^2, 1 + \varepsilon\}$, $h \in \mathcal{H}_2$, $\kappa_1' = \left(\begin{smallmatrix}3&0\\0&1\end{smallmatrix}\right)$, $\kappa_2' = \left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right)$, $\kappa_3' = \left(\begin{smallmatrix}1&0\\2&1\end{smallmatrix}\right)$, $\kappa_4' = \left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right)$ and $\sum \alpha_i \leq 8$, such that $\widetilde{T}_5 - (1 + 5\Lambda_5) - \zeta$ satisfies the hypothesis of Lemma 12 with $n = 9$. Consequently $P|\widetilde{T}_5 \equiv s_5 P \pmod{512 L_k}$ for every k and every $P \in L_k$, and $a_5(f) \equiv 1 + 5^{k-1} \pmod{512\overline{\mathbb{Z}}_2}$ for every eigenform f of level 1.*

Proof. Finite exact computation (`VERIF_HATADA2.py`, parts A and B); the conclusion is drawn as in the proof of Theorem K. □

Status: **PROVED**.

8.2 The law

Let f be an eigenform of level 1 and weight k, O the ring of integers of a finite extension of $\mathbb{Q}_2$ containing its coefficients, $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(O)$ its 2-adic representation, $T = \operatorname{tr}\rho_f$, $D = \chi^{k-1}$ (χ the 2-adic cyclotomic character), $T_E = 1 + \chi^{k-1}$, $\Delta = T - T_E$, and $s_p = 1 + p^{k-1}$, $d_3 = a_3 - s_3$. Let L be the maximal pro-2-extension of $\mathbb{Q}$ unramified outside $\{2, \infty\}$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. We call the *class* of $g \in G$ the class of $\chi(g)$ modulo 8.

(G1) Since $a_\ell \equiv 1 + \ell \pmod 8$ [9], $T \equiv 0$ and $D \equiv 1 \pmod 2$; the residual image is unipotent, $\rho_f(G_{\mathbb{Q}})$ is a pro-2-group, and T, D, T_E factor through G. By [17, Thm 8.1] and Chebotarev, $\Delta(G) \subset 2^7 O$.

(G2) The quadratic extensions of $\mathbb{Q}$ unramified outside 2 are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$: $\Phi(G)$ is the set of elements of class 1, and $G/\Phi(G) \simeq (\mathbb{Z}/8\mathbb{Z})^\times$ via the class.

(G3) For a complex conjugation c, $T(c) = T_E(c) = 0$ (ρ_f is odd).

(G4) If $\chi(g) \equiv 1 \pmod 4$, $v_2(T_E(g)) = 1$; if $\chi(g) \equiv 3 \pmod 4$, $v_2(T_E(g)) = v_2(1 + \chi(g))$, since $k - 1$ is odd. As $T \equiv T_E \pmod{2^7}$, T has the same valuation as long as it is < 7.

(G5) $H = \{g : \chi(g) \equiv \pm 1 \pmod 8\} = \mathrm{Gal}(L/\mathbb{Q}(\sqrt{2}))$ and $N = \Phi(G) = \mathrm{Gal}(L/\mathbb{Q}(\zeta_8))$; L is also the maximal pro-2-extension of $\mathbb{Q}(\sqrt{2})$ and of $\mathbb{Q}(\zeta_8)$ unramified outside 2 and ∞ (that extension is Galois over $\mathbb{Q}$, with group an extension of a finite 2-group by a pro-2-group, hence a pro-2-extension of $\mathbb{Q}$ unramified outside $\{2, \infty\}$, contained in L). These fields have class number one, and Kummer theory gives isomorphisms $H/\Phi(H) \simeq (\mathbb{Z}/2)^3$ via $(\theta_{-1}, \theta_{1+\sqrt{2}}, \theta_{\sqrt{2}})$ and $N/\Phi(N) \simeq (\mathbb{Z}/2)^3$ via $(\theta_{\zeta_8}, \theta_{1+\sqrt{2}}, \theta_{1-\zeta_8})$, where $\theta_x(g) \in \mathbb{Z}/2$ is defined by $g(\sqrt{x}) = (-1)^{\theta_x(g)}\sqrt{x}$; and $\theta_x(s^{-1}as) = \theta_{s(x)}(a)$.

Lemma 14 (parity)**.** *Let $n \geq 1$ and $g, h \in G$ be such that $\Delta(gh), \Delta(g^{-1}h) \in 2^n O$ and $\Delta(g)T(h) + T_E(g)\Delta(h) \in 2^{n+1}O$. Then $\Delta(gh) \equiv \Delta(g^{-1}h) \pmod{2^{n+1}}$. In particular, if $\Delta(K) \subset 2^n O$ for a closed subgroup K of G, the function $\Delta/2^n \bmod 2$ is constant on the classes of K modulo $\Phi(K)$, and vanishes on $\Phi(K)$.*

Proof. Subtracting (1) for T_E from (1) for T: $\Delta(gh)+D(g)\Delta(g^{-1}h) = \Delta(g)T(h)+T_E(g)\Delta(h)$, and $D(g)$ is odd. If $g, h \in K$, the hypothesis is satisfied since T and T_E are even; with (g, gh) instead of (g, h), we get invariance under left multiplication by squares, which topologically generate $\Phi(K)$. □

Theorem U (2-adic law)**.** *For every odd prime p:*

$$a_p \equiv s_p \ (2^{10}) \text{ if } p \equiv 1 \ (8); \quad a_p \equiv s_p \ (2^8) \text{ if } p \equiv 5 \ (8); \quad a_p - s_p \equiv d_3 \ (2^8) \text{ if } p \equiv 3 \ (8);$$

$$a_p - s_p \equiv 2d_3 \ (2^9) \text{ if } p \equiv 7 \ (16); \qquad a_p \equiv s_p \ (2^9) \text{ if } p \equiv 15 \ (16).$$

Proof. Step 1 (modulo 2^8). By (G1) and Lemma 14 ($K = G$, $n = 7$), $\varepsilon = \Delta/2^7 \bmod 2$ depends only on the class, and $\varepsilon = 0$ on class 1. On class 7, $\varepsilon(c) = 0$ by (G3). On class 5, $\varepsilon(\mathrm{Frob}_5) = 0$ by Lemma 13. On class 3, $\Delta \equiv \Delta(\mathrm{Frob}_3) = d_3 \pmod{2^8}$.

Step 2 (modulo 2^9 on H). By step 1, $\Delta(H) \subset 2^8 O$; by Lemma 14, $\varepsilon_2 = \Delta/2^8 \bmod 2$ is a function on $V = H/\Phi(H) \simeq (\mathbb{Z}/2)^3$, vanishing at 0 and at $\bar{c}$. Let s be of class 3 or 5 and $a, b \in N$; for $g = sa$, $h = sb$, of the same class, the hypothesis of Lemma 14 ($n = 8$) is satisfied by (G4) and step 1, and $gh = s^2(s^{-1}as)b$, $g^{-1}h = a^{-1}b$. Since $s(1+\sqrt{2}) = -(1+\sqrt{2})^{-1}$, $s(\sqrt{2}) = -\sqrt{2}$ and $\theta_{-1}(a) = 0$, one has $\overline{s^{-1}as} = \bar{a}$, whence $\varepsilon_2(\overline{s^2} + w) = \varepsilon_2(w)$ for every $w \in V_N = \{\theta_{-1} = 0\}$, the image of N. By Euler's criterion in $\mathbb{F}_9$ and $\mathbb{F}_{25}$ (`VERIF_HATADA2.py`, part C), $\overline{\mathrm{Frob}_3^2} = (0, 1, 0)$ and $\overline{\mathrm{Frob}_5^2} = (0, 0, 1)$, which generate V_N: hence $\varepsilon_2 = 0$ on V_N, that is, $a_p \equiv s_p \pmod{2^9}$ if $p \equiv 1 \pmod 8$. For g of class 3 and h of class 5 (or the reverse), gh and $g^{-1}h$ are of class 7, and (G4) and step 1 give $\Delta(g)T(h) + T_E(g)\Delta(h) \equiv 2^8\varepsilon(3) \pmod{2^9}$, whence $\varepsilon_2(gh) + \varepsilon_2(g^{-1}h) = \varepsilon(3)$; with $g = \mathrm{Frob}_3 a$, $h = \mathrm{Frob}_5 b$, we get $\varepsilon_2(z + \overline{\mathrm{Frob}_3^2}) = \varepsilon_2(z) + \varepsilon(3)$ for every z in the image V_7 of class 7, and likewise with Frob_5^2. Since $2 + \sqrt{2} = \sqrt{2}\,(1 + \sqrt{2})$, one has $\theta_{2+\sqrt{2}} = \theta_{1+\sqrt{2}} + \theta_{\sqrt{2}}$, which takes the value 1 at Frob_3^2 and at Frob_5^2 (part C). Since $\varepsilon_2(\bar{c}) = 0$, $\varepsilon_2(g) = \varepsilon(3)\,\theta_{2+\sqrt{2}}(g)$ on class 7 ($2 + \sqrt{2}$ is totally positive, so $\theta_{2+\sqrt{2}}(c) = 0$). Now $\theta_{2+\sqrt{2}}(g) = 0$ if and only if g fixes $\mathbb{Q}(\zeta_{16})^+ = \mathbb{Q}(\sqrt{2+\sqrt{2}})$, that is, $\chi(g) \equiv 15 \pmod{16}$ for g of class 7; and $2^8\varepsilon(3) \equiv 2d_3 \pmod{2^9}$.

Step 3 (modulo 2^{10} on N). By step 2, $\Delta(N) \subset 2^9 O$, and $\varepsilon_3 = \Delta/2^9 \bmod 2$ is a function on $V' = N/\Phi(N) \simeq (\mathbb{Z}/2)^3$, vanishing at 0. (i) For $g = ca$, $h = cb$ ($a, b \in N$), of class 7, $\Delta(g), \Delta(h) \in 2^8 O$ and $v_2(T(h)), v_2(T_E(g)) \geq 3$: Lemma 14 ($n = 9$) gives $\varepsilon_3(\overline{cac^{-1}} + \bar{b}) = \varepsilon_3(\bar{a} + \bar{b})$. Since $\zeta_8\, c(\zeta_8) = 1$, $(1 + \sqrt{2})\, c(1 + \sqrt{2}) = (1 + \sqrt{2})^2$ and $(1 - \zeta_8)\, c(1 - \zeta_8) = -\zeta_8^{-1}(1 - \zeta_8)^2$, the element $\overline{cac^{-1}} + \bar{a}$ equals $(0, 0, \theta_{\zeta_8}(a))$: ε_3 is invariant under $e_3 = (0, 0, 1)$. (ii) For $g = \mathrm{Frob}_3 a$, $h = \mathrm{Frob}_3 b$: $\Delta(g) \equiv \Delta(h) \equiv d_3 \pmod{2^8}$, $T(h) = 4u$, $T_E(g) = 4u'$; here $u' = T_E(g)/4$ lies in $\mathbb{Z}_2^\times$, and $u \equiv T_E(h)/4 \pmod{2^5}$ with $T_E(h)/4 \in \mathbb{Z}_2^\times$, so that $u, u' \in \mathbb{Z}_2^\times + 2^5 O$ and $u + u' \in 2O$; hence $\Delta(g)T(h)+T_E(g)\Delta(h) \equiv 4(u+u')d_3 \equiv 0 \pmod{2^{10}}$. Here $\zeta_8\, \zeta_8^3$ and $(1+\sqrt{2})(1-\sqrt{2})$ are squares, so $\overline{s^{-1}as} + \bar{a} \in \langle e_3 \rangle$, and ε_3 is invariant under $\overline{\mathrm{Frob}_3^2}$, whose first two coordinates are $(1, 1)$ (part C). Thus $\varepsilon_3 = \beta\,(\theta_{\zeta_8} + \theta_{1+\sqrt{2}})$ for some $\beta \in O/2$. (iii) For g of class 5, $g^2 \in N$ has first two coordinates $(1, 0)$ (part C, and the same computation as in (ii)), and $\Delta(g^2) = \Delta(g)\big(T(g) + T_E(g)\big)$, since $T(g^2) = T(g)^2 - 2D(g)$; now $\Delta(g) \in 2^8 O$ (step 1) and $v_2(T(g) + T_E(g)) = v_2(2T_E(g) + \Delta(g)) = 2$, hence $\Delta(g^2) \in 2^{10} O$ and $\beta = \varepsilon_3(g^2) = 0$. □

Status: **PROVED**. From [17, Thm 8.1] and Lemma 13.

Corollary V (Hatada's question, $a = 8$ and 9)**.** *For every eigenform of level 1 and every weight, Hatada's question has an affirmative answer for $a = 8$ and for $a = 9$; for $a = 10$, the requested congruence holds for every $p \equiv 1 \pmod{2^9}$.*

Proof. If $p \equiv \pm 1 \pmod{2^{a-1}}$ and $a \geq 4$, then $p^2 \equiv 1 \pmod{2^a}$ and $p^{k-1} \equiv p \pmod{2^a}$. If $p \equiv 1 \pmod{2^{a-1}}$, then $p \equiv 1 \pmod 8$ and Theorem U gives the congruence modulo 2^{10}. If $p \equiv -1 \pmod{2^{a-1}}$ and $a \in \{8, 9\}$, then $p \equiv 15 \pmod{16}$, and Theorem U gives the congruence modulo 2^9. □

STATUS: **PROVED**.

8.3 The case $p \equiv -1$ and the complete answer

Let $t \in G$ be a Frobenius element at 5: $\chi(t) = 5$, and the images of t and of c generate $G/\Phi(G) \simeq (\mathbb{Z}/8\mathbb{Z})^\times$, so c and t topologically generate G. Put $x = \Delta(t) = a_5 - s_5$ and $y = \Delta(ct)$: by Lemma 13, $x \in 2^9 O$; ct is of class 3, so $y \in 2^7 O$. Let $D = 5^{k-1}$ and, in $\mathrm{GL}_2(\mathbb{Z}_2[\eta]/(\eta^2))$,

$$\mathcal{C} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \qquad \mathcal{T}_X = \left(\begin{smallmatrix} 1 & 1 \\ 0 & D \end{smallmatrix}\right) + \eta \left(\begin{smallmatrix} 1 & 0 \\ D+1 & 1 \end{smallmatrix}\right), \qquad \mathcal{T}_Y = \left(\begin{smallmatrix} 1 & 1 \\ 0 & D \end{smallmatrix}\right) + \eta \left(\begin{smallmatrix} 1 & 0 \\ D-1 & -1 \end{smallmatrix}\right).$$

For a word W in two letters, let $\tau_X(W)$ (resp. $\tau_Y(W)$) be the coefficient of η in the trace of $W(\mathcal{C}, \mathcal{T}_X)$ (resp. $W(\mathcal{C}, \mathcal{T}_Y)$), and $\chi(W) = (-1)^a 5^b$ if W contains a letters c and b letters t (with sign).

Lemma 15 (universal family)**.** *For every word W,*

$$\Delta(W(c,t)) \equiv 2^7 \frac{x}{2^8}\, \tau_X(W) + 2^6 \frac{y}{2^7}\, \tau_Y(W) \pmod{2^{14} O}.$$

Proof. For indeterminates u, v, let $\rho_{u,v}$ be the representation of the free group on c, t given by $c \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $t \mapsto \left(\begin{smallmatrix} \alpha & 1 \\ \gamma & \delta \end{smallmatrix}\right)$ with $\alpha = 1 + \frac{u+v}{2}$, $\delta = D + \frac{u-v}{2}$, $\gamma = \alpha\delta - D$: its trace at t is $1 + D + u = T_E(t) + u$, at ct it is $1 - D + v = T_E(ct) + v$, its determinant at c is -1 and at t is D. By Lemma 9, applied on the one hand to T on G (with $T(c) = 0$, $D(c) = -1$) and on the other hand to $\rho_{u,v}$, $T(W(c,t)) = P_W(0, T_E(t) + x, T_E(ct) + y, -1, D) = \operatorname{tr} \rho_{x,y}(W)$. The polynomial P_W has integer coefficients; the Taylor expansion at $(u, v) = (0, 0)$ therefore has terms of order ≥ 2 in $(x, y)^2 O \subset 2^{14} O$, the constant term $T_E(W)$, and first-order terms equal to the coefficients of η computed with the derivatives $\partial_u \rho(t) = \frac{1}{2}\left(\begin{smallmatrix} 1 & 0 \\ D+1 & 1 \end{smallmatrix}\right)$ and $\partial_v \rho(t) = \frac{1}{2}\left(\begin{smallmatrix} 1 & 0 \\ D-1 & -1 \end{smallmatrix}\right)$, whence the formula with $x = 2^8 \cdot \frac{x}{2^8}$ and $y = 2^7 \cdot \frac{y}{2^7}$. □

Theorem W (depth on the class of -1)**.** *Let $g \in G$. If $\chi(g) \equiv 1 \pmod 8$, then $\Delta(g) \in 2^{10} O$; if $\chi(g) \equiv 5 \pmod 8$, then $\Delta(g) \in 2^9 O$. If $v_2(1 + \chi(g)) = m \geq 2$, then $\Delta(g) \in 2^{\min(m+5,\,11)} O$. In particular, for every prime $p \equiv -1 \pmod{32}$, $a_p \equiv 1 + p^{k-1} \pmod{2^{10}}$.*

Proof. For powers of two N and N', the map $W \mapsto \big(W(\mathcal{C}, \mathcal{T}) \bmod N,\ \chi(W) \bmod N'\big)$ is a morphism to a finite group, which depends on k only through $D \bmod N$, hence through $k - 1$ modulo $N/4$ (the order of 5 modulo N). For $(N, N') = (16, 64)$ and then $(32, 512)$, and for all these classes of $k - 1$, `VERIF_HATADA2.py` (part E) enumerates these images (512 to 32 768 elements) and checks that $\tau_X \equiv 0 \pmod 8$ and $\tau_Y \equiv 0 \pmod{16}$ when $\chi \equiv 1 \pmod 8$ or $\chi \equiv -1 \pmod{32}$, and that $2^7 \tau_X$ and $2^6 \tau_Y$ are divisible by $2^{\min(m+5,11)}$ when $v_2(1 + \chi) = m \geq 2$ (each of these assertions is tested by the script); finally that $\tau_X \equiv 0 \pmod 2$ and $\tau_Y \equiv 0 \pmod 8$ when $\chi \equiv 5 \pmod 8$, which, with $x \in 2^9 O$, gives $2^9 \mid \Delta$ on class 5. By Lemma 15, the conclusion holds for every word $W(c, t)$. For arbitrary $g \in G$, T modulo 2^{11} and χ modulo 2^{12} factor through a finite quotient of G, in which the image of the dense subgroup generated by c and t is everything: there is a word W such that $T(W) \equiv T(g) \pmod{2^{11}}$ and $\chi(W) \equiv \chi(g) \pmod{2^{12}}$, hence $T_E(W) \equiv T_E(g) \pmod{2^{11}}$. □

STATUS: **PROVED**. Finite exact computation, from [17, Thm 8.1] and Lemma 13. This computation also gives back, by a route independent of Kummer theory, the congruence modulo 2^{10} of Theorem U for $p \equiv 1 \pmod 8$.

Corollary X (complete answer to Hatada's question)**.** *Hatada's question has an affirmative answer for* $6 \le a \le 10$*, for every eigenform of level* 1 *and every weight, and a negative answer for* $a = 11$*,* 12 *and* 13*.*

Proof. For $a = 6, 7$, this is [17, Thm 8.1] (Section 1 and its footnote); for $a = 8, 9$, it is Corollary V; for $a = 10$, $p \equiv 1 \pmod{2^9}$ falls under Corollary V and $p \equiv -1 \pmod{2^9}$ under Theorem W. For $a \in \{11, 12, 13\}$, Theorem A gives counterexamples (Δ_{16} and $p = 12289$). □

Status: **PROVED**.

Corollary Y (non-vanishing)**.** *For every eigenform* f *of level* 1 *and every odd prime* p *such that* $v_2(p+1) \le 10$*, one has* $v_2(a_p(f)) = v_2(p+1)$*. In particular,* $a_p(f) = 0$ *implies* $p \equiv -1 \pmod{2^{11}}$*, and even* $p \equiv -1 \pmod{2^{11} \cdot 27}$ *if* $k \not\equiv 4 \pmod 6$*.*

Proof. One has $v_2(s_p) = v_2(1 + p)$: if $p \equiv 1 \pmod 4$, both equal 1; otherwise, $k - 1$ being odd, $1 + p^{k-1} = (1 + p)(1 - p + \cdots + p^{k-2})$ with an odd second factor. If $p \equiv 1 \pmod 4$, $a_p \equiv s_p \pmod{2^8}$ (Theorem U), hence $v_2(a_p) = 1$. If $v_2(p + 1) = m \in [2, 10]$, Theorem W gives $a_p - s_p \in 2^{\min(m+5,11)}O$ and $\min(m + 5, 11) > m$, hence $v_2(a_p) = m$. If $k \not\equiv 4 \pmod 6$, $v_3(k - 1) = 0$, and Theorem O gives $a_p \equiv s_p \not\equiv 0 \pmod 3$ if $p \equiv 1 \pmod 3$, and $a_p \equiv \pm s_p \pmod{27}$ with $v_3(s_p) = v_3(p + 1)$ if $p \equiv 2 \pmod 3$; hence $a_p = 0$ implies $p \equiv -1 \pmod{27}$. □

Status: **PROVED**.

Status: **PROVED by the optional part F of the script, disabled by default**. With $(N, N') = (64, 2048)$ (about 500 000 elements), the same computation gives $\Delta(g) \in 2^{12}O$ as soon as $v_2(1 + \chi(g)) \ge 7$, whence $p \equiv -1 \pmod{2^{12}}$. This sieve is effective but concerns only p; for fixed p, the (non-effective) finiteness of the set of forms of level 1 such that $a_p(f) = 0$ is due to Calegari and Sardari [2].

Remark. **VERIFIED** (PARI/GP, $12 \le k \le 80$, $p < 300$): the minimal depths observed are 10 for $p \equiv 1 \pmod 8$ (optimal, Theorem E), 7 for $p \equiv 3 \pmod 8$, 9 for $p \equiv 5 \pmod 8$, and 8, 9, 10 for $p \equiv 7 \pmod{16}$, 15 (mod 32), 31 (mod 32), in accordance with Theorems U and W. The laws of Theorem U were checked in 1247 cases ($k \le 70$, $p < 200$) without failure; the correction $2d_3$ is necessary in 84 of them. The depth 9 on class 5 (Theorem W) is therefore optimal.

9 Beyond 729: the law of inert primes

Notation of §7; $\kappa = k - 1$ and $s_\ell = 1 + \ell^\kappa$. We still write σ for the automorphism of $\widehat{G}$ induced by conjugation by a complex conjugation c. Let $x \in \widehat{G}$ be the Frobenius element of a prime ideal of O_K above 7, and $y = \sigma(x)$. Since $7 \equiv 7 \pmod 9$ and 3 is not a cube modulo 7, one has $u(y) = u(x) \ne 0$ and $v(y) = -v(x) \ne 0$; the images of x and y in $(\mathbb{Z}/3\mathbb{Z})^2$ form a basis, so x and y topologically generate $\widehat{G}$ (Burnside's basis theorem).

The anticyclotomic character. The group $\widehat{G}$ is free on two generators [20], so $\mathrm{Hom}(\widehat{G}, \mathbb{Z}_3)$ is free of rank 2; σ acts on it as an involution, and its $+1$ and -1 eigenparts, of rank 1, reduce modulo 3 onto $\langle u \rangle$ and $\langle v \rangle$. The $+1$ part is generated by $\lambda = \frac{1}{3}\log_3 \chi$ (proof of Theorem R); we fix a generator μ of the -1 part. Then (λ, μ) is a basis of $\mathrm{Hom}(\widehat{G}, \mathbb{Z}_3)$, and $\mathrm{Hom}(\widehat{G}, A) = A\lambda \oplus A\mu$ for every finite $\mathbb{Z}_3$-module A. The fixed field of $\ker(\mu \bmod 9)$ is therefore the unique cyclic extension of degree 9 of K, unramified outside 3, on whose Galois group c acts by -1. The ring class field H_{27} of the order $\mathbb{Z} + 27O_K$, of discriminant -2187, has these properties: it is unramified outside 3, c acts by -1 on $\mathrm{Gal}(H_{27}/K)$ [5, §9], and this group, isomorphic to the Picard group of the order, is cyclic of order 9. For a prime $\ell \equiv 1 \pmod 3$ and $\mathfrak{l} \mid \ell$, one therefore has $\mu(\mathrm{Frob}_\mathfrak{l}) \in 9\mathbb{Z}_3$ if and only if ℓ splits completely in H_{27}, that is [5, §9], if and only if $\ell = X^2 + XY + 547Y^2$ with $X, Y \in \mathbb{Z}$. Likewise, $v(\mathrm{Frob}_\mathfrak{l}) = 0$ if and only if $\ell = X^2 + XY + 61Y^2$.

The base point. Let $s \in O'$ be as in the proof of Theorem R ($s = 9t$ if $3 \nmid \kappa$, $s = 3t$ if $3 \mid \kappa$; in the latter case, changing the lift $\tilde{\alpha}$ if necessary, we assume $2s \neq \kappa$, which ensures $w < \infty$ and $\Delta \neq 0$ in Lemma 17). Put $\psi_1 = \psi_s$, $\psi_2 = \chi^\kappa \psi_s^{-1}$, $\theta = \psi_1/\psi_2 = \exp\bigl(3(2s-\kappa)\lambda\bigr)$ and $w = v_3(2s-\kappa)$: $w = 0$ if $3 \nmid \kappa$, $w \geq 1$ if $3 \mid \kappa$. Thus $M_s = \psi_1 + \psi_2$, and, by the proof of Theorem R, $T \equiv M_s \pmod{243\,O'}$ on G_K. The functions $\psi_1, \psi_2, \theta, \lambda$ are invariant under σ, and $\theta \equiv 1 \pmod 3$ on $\widehat{G}$.

Lemma 16 (an irreducible tangent)**.** *There are continuous functions $\beta, \gamma, z : \widehat{G} \to O'$ such that, for $h, h' \in \widehat{G}$,*

$$\beta(hh') = \beta(h) + \theta(h)\beta(h'), \quad \gamma(hh') = \gamma(h) + \theta(h)^{-1}\gamma(h'), \quad z(hh') = z(h) + z(h') + \theta(h)\gamma(h)\beta(h'),$$

$\beta(x) = \gamma(x) = 1$, $z(x) = 0$, $\beta \circ \sigma = -\beta$, $\gamma \circ \sigma = -\gamma$, $z \circ \sigma = z$, and such that the function $e = \psi_2\bigl((1-\theta)z + \theta\beta\gamma\bigr)$ satisfies $e(1) = 0$, $e(hh') = e(h'h)$, $e \circ \sigma = e$ and, with $D = \chi^\kappa$,

$$e(hh') + D(h)\, e(h^{-1}h') = e(h)M_s(h') + M_s(h)e(h') \qquad (h, h' \in \widehat{G}). \tag{2}$$

Moreover:

(a) for every $h \in \widehat{G}$, $e(\sigma(h)h) = 2\psi_2(h)^2\bigl(1-\theta(h)\bigr)F(h)$, where $F = (1+\theta)z - \theta\beta\gamma$;

(b) $\beta \equiv \gamma \equiv v/v(x) \pmod{3O'}$, and there is $a \in O'$ such that $F \equiv a\,u \pmod{3O'}$;

(c) if $w \geq 1$, there are $b, b' \in O'$ such that $\beta \equiv b\mu$ and $\gamma \equiv b'\mu \pmod{9O'}$.

Proof. Let ε be such that $\varepsilon^2 = 0$, $C = \mathrm{diag}(1,-1)$, and Γ_1 the subgroup of $\mathrm{GL}_2(O'[\varepsilon])$ formed by the matrices congruent, modulo the ideal generated by the maximal ideal of O' and ε, to an upper unipotent matrix; it is a pro-3-group. The matrices

$$R = \left(\begin{smallmatrix} \psi_1(x) & \psi_2(x) \\ 0 & \psi_2(x) \end{smallmatrix}\right)\left(1 + \varepsilon \left(\begin{smallmatrix} 0 & 0 \\ \theta(x) & 0 \end{smallmatrix}\right)\right) \quad \text{and} \quad CRC$$

lie in Γ_1. Since $\widehat{G}$ is a free pro-3-group of rank 2 [20] generated by x and y, the pair (x, y) is a basis of it (a free pro-3-group of finite rank is Hopfian [11]), and there is a continuous homomorphism $\rho : \widehat{G} \to \Gamma_1$ such that $\rho(x) = R$ and $\rho(y) = CRC$; one has $\rho \circ \sigma = C\rho C$, the two sides agreeing at x and y. Write $\rho = \rho_0(1 + \varepsilon Z)$, where ρ_0 is the reduction of ρ modulo ε. Then ρ_0 is upper triangular, with diagonal (ψ_1, ψ_2) (two characters which agree with ψ_1, ψ_2 at x and at y), $Z(hh') = \rho_0(h')^{-1}Z(h)\rho_0(h') + Z(h')$, and $\mathrm{tr}\, Z$ is a homomorphism vanishing at x and y, hence zero; thus $\det\rho = \det\rho_0 = D$. Put $\beta = (\rho_0)_{12}/\psi_2$, $\gamma = Z_{21}/\theta$ and $z = Z_{22}$: the three relations are obtained by reading these identities coefficient by coefficient, and $\mathrm{tr}\,\rho = M_s + \varepsilon e$. The function $\mathrm{tr}\,\rho$ satisfies (1) over $O'[\varepsilon]$ with the same D, so e satisfies (2); the symmetries come from $\rho \circ \sigma = C\rho C$, which also gives $\beta(y) = \gamma(y) = -1$ and $z(y) = 0$.

(a) The relations give $\beta(\sigma(h)h) = (\theta(h)-1)\beta(h)$, $\gamma(\sigma(h)h) = (\theta(h)^{-1}-1)\gamma(h)$, $z(\sigma(h)h) = 2z(h) - \theta(h)\gamma(h)\beta(h)$, and $\theta(\sigma(h)h) = \theta(h)^2$, $\psi_2(\sigma(h)h) = \psi_2(h)^2$. With $t = \theta(h)$ and $P = \beta(h)\gamma(h)$,

$$\frac{e(\sigma(h)h)}{\psi_2(h)^2} = (1-t^2)\bigl(2z(h) - tP\bigr) - t(1-t)^2P = 2(1-t)\bigl((1+t)z(h) - tP\bigr).$$

(b) Since $\theta \equiv 1 \pmod 3$, β and γ are, modulo 3, homomorphisms $\widehat{G} \to O'/3$ negated by σ and equal to 1 at x: they are multiples of v, equal to $v/v(x)$. Then $z - \frac{1}{2}\beta\gamma$ is, modulo 3, a homomorphism (the term $\gamma(h)\beta(h') - \frac{1}{2}(\beta(h)\gamma(h') + \beta(h')\gamma(h))$ vanishes modulo 3 since $\beta \equiv \gamma$) invariant under σ, hence a multiple $a'u$ of u, and $F \equiv 2z - \beta\gamma \equiv 2a'u \pmod 3$. (c) If $w \geq 1$, then $\theta \equiv 1 \pmod 9$ on $\widehat{G}$; β and γ are, modulo 9, homomorphisms negated by σ, hence lie in $(O'/9)\mu$. □

Lemma 17 (expansion at the point M_s)**.** *There are A', B' in the fraction field of O', with $v_3(A') \geq 4 - w$ and $v_3(B') \geq 5$, such that, for every $h \in \widehat{G}$,*

$$T(h) - M_s(h) \equiv A'\,\lambda(h)\bigl(\psi_1(h) - \psi_2(h)\bigr) + B'\,e(h) \pmod{3^{10}O'}.$$

Proof. Let $e_r = \lambda(\psi_1 - \psi_2)$; it is the ε-part of the trace of $\psi_1 e^{\varepsilon\lambda} \oplus \psi_2 e^{-\varepsilon\lambda}$, which has determinant D, so e_r satisfies (2); it is central and invariant under σ. One has $e(x) = \psi_1(x)$, a unit; $e_r(x) = \lambda(x)\psi_2(x)(\theta(x) - 1)$, of valuation $1 + w$ ($\lambda(x)$ is a unit since $u(x) \neq 0$); $xy = \sigma(y)y$ and $F(y) = -\theta(y)$, hence, by Lemma 16(a), $e(xy) = -2\psi_2(x)^2\theta(x)(1 - \theta(x))$, of valuation $1 + w$; finally $e_r(xy) = 2\lambda(x)\psi_2(x)^2(\theta(x)^2 - 1)$, of valuation $1+w$. The determinant $\Delta = e_r(x)e(xy) - e(x)e_r(xy)$ therefore has valuation exactly $1 + w$. Let $\delta = T - M_s$, with values in $3^5 O'$ on $\widehat{G}$, and A', B' defined by $A'e_r + B'e = \delta$ at x and at xy; Cramer's formulas give $v_3(A') \geq 5 - (1+w)$ and $v_3(B') \geq (5 + 1 + w) - (1 + w)$. The function $L = A'e_r + B'e$ satisfies (2) and $L(y) = L(x) = \delta(x) = \delta(y)$ (σ-invariance). Apply Lemma 9 to the pseudo-representation $M_s + \varepsilon L$ (over $\mathrm{Frac}(O')[\varepsilon]$) and to T, M_s, with $x_1 = x$, $x_2 = y$, $x_3 = xy$ and $m = (M_s(x), M_s(y), M_s(xy), D(x), D(y))$: for every word W, $L(W) = \sum_j \partial_j P_W(m)\, \delta(x_j)$ and

$$\begin{aligned} T(W) - M_s(W) &= P_W\big(m + (\delta(x_1), \delta(x_2), \delta(x_3), 0, 0)\big) - P_W(m) \\ &\equiv \sum_j \partial_j P_W(m)\, \delta(x_j) \pmod{3^{10} O'}, \end{aligned}$$

since P_W has integer coefficients, $D(x)$, $D(y)$ are units, and the Taylor coefficients of order ≥ 2 of P_W at m therefore lie in O', while $\delta(x_j) \in 3^5 O'$. One concludes by density of the subgroup generated by x and y. □

Theorem R′ (law of inert primes)**.** *Let $\ell \equiv 2 \pmod 3$ be prime and $j = v_3(\ell + 1)$. For every eigenform f of level 1 and weight k,*

$$a_\ell^2 \equiv s_\ell^2 \pmod{3^{\min(2j+2,\,10)} O}.$$

In particular $a_\ell^2 \equiv s_\ell^2 \pmod{3^8}$ if $\ell \equiv -1 \pmod{27}$, and $\pmod{3^{10}}$ if $\ell \equiv -1 \pmod{81}$.

Proof. Let f_ℓ be a Frobenius element at ℓ and $h = cf_\ell \in G_K$; then $f_\ell^2 = chch = \sigma(h)h$, $\chi(h) = -\ell$, and $T(f_\ell^2) - T_E(f_\ell^2) = a_\ell^2 - 2\ell^\kappa - (1 + \ell^{2\kappa}) = a_\ell^2 - s_\ell^2$. One has $v_3(\lambda(h)) = v_3(\log_3(-\ell)) - 1 = j - 1$, hence $v_3(\theta(h) - 1) = j + w$, $v_3(\lambda(f_\ell^2)) = j - 1$ and $v_3(\theta(f_\ell^2) - 1) = j + w$; finally $u(h) = 0$ if and only if $j \geq 2$. Write $T - T_E = (M_s - T_E) + (T - M_s)$ at f_ℓ^2 and estimate the terms. (i) $M_s - T_E = -(\psi_s - 1)(\chi^\kappa \psi_s^{-1} - 1)$ has valuation at least $(j + v_3(s)) + (j + v_3(\kappa - s)) \geq 2j + 2$, since $v_3(s) \geq 2$ if $3 \nmid \kappa$, and $v_3(s), v_3(\kappa - s) \geq 1$ if $3 \mid \kappa$. (ii) $A'e_r(f_\ell^2)$ has valuation at least $(4 - w) + (j - 1) + (j + w) = 2j + 3$. (iii) By Lemma 16(a), $B'e(f_\ell^2) = 2B'\psi_2(h)^2(1 - \theta(h))F(h)$ has valuation at least $5 + j + w + v_3(F(h))$, and $v_3(F(h)) \geq 1$ if $j \geq 2$ by Lemma 16(b): hence at least $j + 6 \geq \min(2j + 2, 10)$ if $j \geq 2$, and at least 6 if $j = 1$. Lemma 17 concludes. □

Status: **PROVED**. From Theorem R. For $j = 1$ and $j = 2$, one recovers $a_\ell^2 \equiv s_\ell^2$ modulo 81 and modulo 729 (Theorems O and R).

Corollary Y′ (non-vanishing, 3-adic)**.** *If $k \not\equiv 4 \pmod 6$ and if $\ell \equiv 2 \pmod 3$ is a prime with $v_3(\ell + 1) \leq 4$, then $v_3(a_\ell(f)) = v_3(\ell + 1)$. Consequently, if $k \not\equiv 4 \pmod 6$, $a_\ell(f) = 0$ implies $\ell \equiv -1 \pmod{2^{11} \cdot 3^5}$.*

Proof. If $3 \nmid \kappa$, $v_3(s_\ell) = v_3(\ell+1) + v_3(\kappa) = j$, and Theorem R′ gives $a_\ell^2 \equiv s_\ell^2 \pmod{3^{2j+2}}$ for $j \leq 4$, whence $v_3(a_\ell^2) = 2j$. If $a_\ell = 0$, then $\ell \neq 2$ (Corollary L), $\ell \neq 3$ (Corollary Y), $\ell \not\equiv 1 \pmod 3$ ($a_\ell \equiv s_\ell \equiv 2 \pmod 3$), and, by what precedes, $j \geq 5$; one concludes with Corollary Y. □

Status: **PROVED**.

Theorem R″ (split primes)**.** *Let $\ell \equiv 1 \pmod{27}$ be a prime such that 3 is a cube modulo ℓ. For every eigenform f of level 1 and weight k, $a_\ell \equiv s_\ell \pmod{3^7 O}$. If moreover $k \equiv 4 \pmod 6$ and $\ell = X^2 + XY + 547Y^2$ ($X, Y \in \mathbb{Z}$), then $a_\ell \equiv s_\ell \pmod{3^8 O}$, and $\pmod{3^9 O}$ if $\ell \equiv 1 \pmod{81}$.*

Proof. Let $h = \mathrm{Frob}_{\mathfrak{l}}$, $\mathfrak{l} \mid \ell$, and $n = v_3(\lambda(h)) = v_3(\ell-1) - 1 \geq 2$; $v(h) = 0$, so $\beta(h), \gamma(h) \in 3O'$ (Lemma 16(b)). (i) $M_s(h) - T_E(h)$ has valuation at least $(1 + v_3(s) + n) + (1 + v_3(\kappa - s) + n) \geq 2n + 4$. (ii) $A'e_r(h)$ has valuation at least $(4 - w) + n + (1 + w + n) = 2n + 5$. (iii) $e(h) = \psi_2(h)\big((1 - \theta(h))z(h) + \theta(h)\beta(h)\gamma(h)\big)$ has valuation at least $\min(1 + w + n, 2) = 2$, so $B'e(h)$ has valuation at least 7. Lemma 17 gives the first assertion. If $k \equiv 4 \pmod 6$, then $w \geq 1$; if moreover $\ell = X^2 + XY + 547Y^2$, then $\mu(h) \in 9\mathbb{Z}_3$, so $\beta(h), \gamma(h) \in 9O'$ by Lemma 16(c), and $e(h)$ has valuation at least $\min(2 + n, 4)$; the minimum of $2n + 4$, $2n + 5$, $5 + \min(2 + n, 4)$ and 10 is 8 if $n = 2$ and 9 if $n \geq 3$. □

Status: **PROVED**. From Theorem R.

Remark. **VERIFIED** (PARI/GP, exact Newton polygons on S_k). *Inert primes*, $12 \leq k \leq 94$: the minimal depth of $a_\ell^2 - s_\ell^2$ is exactly 8 for the eight primes $\ell \equiv -1 \pmod{27}$, $\ell \not\equiv -1 \pmod{81}$, $\ell < 1200$ $(53, 107, 269, 431, 593, 701, 863, 1187)$, and 10 for $\ell = 647$ and 809 ($j = 4$), except for $k = 12$ and $k = 22$, where it is 9 and 11: the exponent $2j + 2$ is attained for $j \leq 4$. For $\ell = 971$ ($j = 5$), it is 11 if $k \not\equiv 4 \pmod 6$ (12 for $k = 12$) and 12 if $k \equiv 4 \pmod 6$ (13 for $k = 22$): the exponent $2j + 2$ does not hold for $j = 5$, which corresponds to term (iii) of the proof. *Split primes*, $12 \leq k \leq 78$, for the seven primes $\ell \equiv 1 \pmod{27}$, $\ell < 3000$, such that 3 is a cube modulo ℓ $(271, 757, 919, 1621, 1783, 2269, 2971)$: if $k \equiv 4 \pmod 6$, the minimal depth of $a_\ell - s_\ell$ is 7 for $271, 919, 1621, 1783$, which are not of the form $X^2 + XY + 547Y^2$, 8 for 757 and 2971, and 9 for 2269 (except $k = 22$, where it is larger); if $k \not\equiv 4 \pmod 6$, it is 7 for 757 and 2971, and at least 8 for the other five. The depth 8 for $\ell \equiv 1 \pmod{27}$ when $k \not\equiv 4 \pmod 6$ remains **OPEN**: modulo 3^8, only the term $B'\psi_2\theta\beta\gamma$ of the proof can obstruct it, and $\beta/3$, $\gamma/3$ are then characters of $\mathrm{Gal}(E/K(\sqrt[3]{3}))$ which, unlike the case $3 \mid \kappa$ (Lemma 16(c)), do not factor through $\mathrm{Gal}(H_{27}/K)$ (script `VERIF_INERTES.py`, part A).

10 What remains open

- Hatada's question: **SOLVED** (Corollary X): affirmative answer for $6 \leq a \leq 10$, negative for $a = 11, 12, 13$. "Lattice" form for $a \leq 10$: verified (Statement V′), not proved.
- Gain in depth for $\ell \equiv \pm 1 \pmod 9$: **PROVED** in every weight (Corollary Q, Theorem R). Beyond: **PROVED** for inert primes up to 3^{10}, with the optimal exponent $2v_3(\ell + 1) + 2$ for $v_3(\ell + 1) \leq 4$ (Theorem R′), and, for $\ell \equiv 1 \pmod{27}$ with 3 a cube, up to 3^7, or 3^8 and 3^9 if $k \equiv 4 \pmod 6$ and $\ell = X^2 + XY + 547Y^2$ (Theorem R″). **OPEN**: the depth 8 for $\ell \equiv 1 \pmod{27}$ when $k \not\equiv 4 \pmod 6$ (Remark of §9), and the depths beyond 3^{10}.
- Value of $a_2(f)$ modulo 27 when $k \equiv 4 \pmod 6$: there is no uniform law (Remark (3) of §6), but a_2 determines the other a_ℓ, $\ell \equiv 2 \pmod 3$, by Theorem S; the possible values of $a_2(f)$ modulo 81 (valuative sense) are listed, by class of k modulo 54, in [18, Thm 1.5 and Table 3].
- Coleman–Stein conjecture in levels 3 and 9: **OPEN** (checked by Coleman and Stein up to weight 40).

11 Verification

- PARI/GP:
  `ramanujantau(12289)`
  `F = mfeigenbasis(mfinit([1,16],1))[1]; mfcoef(F,13313)`
  `charpoly(mfheckemat(mfinit([1,k],1),3))` (3-adic slopes of T_3)
  In Sage: `pari('ramanujantau(12289)')`.

- Script `VERIF_HATADA.py` (Python, numpy only, a few seconds): self-test on known values and on the exact value of $\tau(12289)$; the 24 class congruences for all odd $n \leq 2000$; the two witnesses; a scan of all primes $p \leq 13313$, which shows that the smallest witness at each failing level is 12289, and that no $a \leq 10$ fails for the six forms.

- Script `VERIF_MOD9.py` (Python only): the criteria of Theorems G and H (T_2 and T_3), for increasing weights until a time budget set in the file is exhausted, with self-test. With the values set in the file it covers $12 \leq k \leq 400$ in a few minutes; the range $k \leq 1000$ of Theorem G (494 spaces) was covered by the same certificate computed independently with FLINT and PARI/GP (Miller basis, characteristic polynomials of T_2 and T_3, Newton polygons at 3), in about forty minutes.

- Script `VERIF_A3.py` (Python only, a few minutes at most): the checks of Theorem F described above, with self-test on the period of Δ, proportional to $(48, -25, 20, -25, 48)$, and on $\tau(3) = 252$.

- Script `VERIF_A2.py` (Python only, under a minute): the certificate of Lemma 6 in $(\mathbb{Z}/9\mathbb{Z})[\mathcal{G}]$ (290 terms); the three certificates of Lemma 8 and the criterion of Lemma 7, which prove Theorem K; direct check of Theorems I and K on L_k for $12 \leq k \leq 100$; the identity of Lemma 5 on all solutions modulo 3 of the relations, and the condition of Lemma 6 on L_k, for $k \leq 40$; direct action of the remainders of Lemma 8 on $\mathbb{Z}[x, y]_w$ for $w \leq 60$, with out-of-class witnesses; self-test on the period of Δ and on $\tau(2) = -24$.

- Script `VERIF_EISENSTEIN.py` (Python only, about two minutes): the nineteen certificates of Theorem N (criterion of Lemma 7, moduli 27, 81, 243), their check by direct action on $\mathbb{Z}[x, y]_w$, statement (i) of Theorem O for $k \leq 44$ (characteristic polynomials of T_n on L_k, $n \equiv 1 \pmod 3$, $n \leq k$), and Theorems P, R, S for $k \leq 40$ and $\ell \leq 43$, $\ell = 73$, on L_k, with witnesses where the correction term is necessary; self-test on $\tau(2)$ and $\tau(7)$.

- Script `VERIF_HATADA2.py` (Python only, under a minute): the certificate of Lemma 13 (190 terms, criterion of Lemma 12 modulo 512), the direct action of the remainder on $\mathbb{Z}[x, y]_w$ for $w \leq 40$ (witnesses of odd degree), the Kummer symbols in the proof of Theorem U, the five laws of that theorem on L_k for $k \leq 40$, and the enumeration of the finite groups of Theorem W (part E; part F, heavier, is optional); self-test on $\tau(3)$ and $\tau(5)$.

- Script `VERIF_INERTES.py` (Python only, under a minute): the identities of Lemma 16 and the valuations of the system of Lemma 17 in the dual-number representation, on random words modulo 3^{14}, with witnesses; Theorem R′ and Corollary Y′ on L_k for $k \leq 40$ and $\ell \in \{5, 11, 17, 53, 71, 107\}$, the exponent being attained for each ℓ; Theorems R′, R″ and Corollary Y′ for the six weights of dimension 1 and all primes $\ell < 3000$ (1332 inert cases, 42 split cases), with the witnesses $v_3(a_{971}^2 - s_{971}^2) = 11$ for $k = 18$ and $v_3(a_{271} - s_{271}) = 7$ for $k = 16$; finally the cyclicity of the Picard groups of the orders of conductor 9 and 27 in $\mathbb{Z}[\zeta_3]$ and their consistency with the forms $X^2 + XY + 61Y^2$, $X^2 + XY + 547Y^2$ and the cube criterion for $\ell < 20\,000$; self-test on $\tau(n)$, $n \leq 11$.

- Theorem E (PARI/GP): for $12 \leq k \leq 100$, $k \neq 14$,
  `P = charpoly(mfheckemat(mfinit([1,k],1),12289));`
  `newtonpoly(subst(P,x,x+12290),2)`
  contains the slope 10 if $k \equiv 0, 2 \pmod 8$ ($k \geq 16$) and the slope 11 if $k \equiv 4, 6 \pmod 8$ and $k \in \{12\} \cup [28, 100]$.

- Check of Theorem O by Sturm's theorem (PARI/GP): Newton polygons of charpoly$(T_n - \sigma_{k-1}(n))$ on S_k for $n \equiv 1 \pmod 3$, $n \leq k$, $12 \leq k \leq 212$; statement (ii) on an eigenbasis embedded in $\overline{\mathbb{Q}}_3$ for $k \leq 140$.

Acknowledgements

Technical assistance: Claude (Anthropic).

References

[1] J. Bellaïche, C. Khare, *Level 1 Hecke algebras of modular forms modulo p*, Compos. Math. **151** (2015), 397–415, doi:10.1112/S0010437X1400774X.

[2] F. Calegari, N. T. Sardari, *Vanishing Fourier coefficients of Hecke eigenforms*, Math. Ann. **381** (2021), 1197–1215, doi:10.1007/s00208-021-02178-7 (arXiv:2003.07570).

[3] F. Calegari, M. Emerton, *The Hecke algebra T_k has large index*, Math. Res. Lett. **11** (2004), 125–137, doi:10.4310/MRL.2004.v11.n1.a12.

[4] L. Chiriac, *Congruences for Hecke eigenvalues via period polynomials*, Bull. Aust. Math. Soc., online first, published online 21 September 2026, doi:10.1017/S0004972726101889.

[5] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, 2nd ed., Wiley, Hoboken (2013).

[6] R. F. Coleman, W. A. Stein, *Approximation of eigenforms of infinite slope by eigenforms of finite slope*, Geometric aspects of Dwork theory, vol. I, de Gruyter, Berlin (2004), 437–449.

[7] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki 1968/69, exp. 355, Lecture Notes in Math. **179**, Springer (1971), 139–172.

[8] W. M. Goldman, *Trace coordinates on Fricke spaces of some simple hyperbolic surfaces*, Handbook of Teichmüller theory, vol. II, IRMA Lect. Math. Theor. Phys. **13**, EMS (2009), 611–684.

[9] K. Hatada, *Eigenvalues of Hecke operators on* $\mathrm{SL}(2,\mathbb{Z})$, Math. Ann. **239** (1979), 75–96.

[10] K. Hatada, *Congruences for eigenvalues of Hecke operators on* $\mathrm{SL}_2(\mathbb{Z})$, Manuscripta Math. **34** (1981), 305–326.

[11] H. Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer, 2002.

[12] O. Kolberg, *Congruences for Ramanujan's function $\tau(n)$*, Årbok Univ. Bergen Mat.-Natur. Ser. 1962, no. 11.

[13] N. M. Katz, *Higher congruences between modular forms*, Ann. of Math. (2) **101** (1975), 332–367.

[14] Yu. I. Manin, *Periods of parabolic forms and p-adic Hecke series*, Mat. Sb. (N.S.) **92(134)** (1973), 378–401; Math. USSR-Sb. **21** (1973), 371–393.

[15] A. Medvedovsky, *An explicit Galois representation on the mod-3 Hecke algebra*, manuscript, 23 December 2016, `https://people.mpim-bonn.mpg.de/medved/Mathwriting/Mod3galoisrep.pdf`.

[16] The PARI Group, *PARI/GP*, version 2.17.2, Univ. Bordeaux, `https://pari.math.u-bordeaux.fr`.

[17] N. Rustom, *Congruences modulo prime powers of Hecke eigenvalues in level 1*, Res. Number Theory **5** (2019), Paper 10, doi:10.1007/s40993-018-0147-5 (arXiv:1710.00928).

[18] N. Rustom, *Prime-power congruences for level-one eigenforms*, preprint (2026), arXiv:2609.16750.

[19] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, in *Modular Functions of One Variable III*, Lecture Notes in Math. **350**, Springer, 1973, 191–268.

[20] I. R. Shafarevich, *Extensions with given points of ramification*, Publ. Math. IHÉS **18** (1963), 71–92 (in Russian).

[21] J. Sturm, *On the congruence of modular forms*, Lecture Notes in Math. **1240**, Springer (1987), 275–280.

[22] H. P. F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Lecture Notes in Math. **350**, Springer (1973), 1–55.

[23] P. Tian, H. Qin, *Non-vanishing Fourier coefficients of Δ_k*, Appl. Math. Comput. **339** (2018), 507–515, doi:10.1016/j.amc.2018.07.022 (arXiv:1504.07381, under the title *Non-vanishing Fourier coefficients of modular forms*).

[24] D. Zagier, *Hecke operators and periods of modular forms*, Israel Math. Conf. Proc. **3** (1990), 321–336.