Sun's supercongruence for two Apéry-like binomial sums

Oleksiy Babanskyy

Abstract

Let $f_n = \sum_{j=0}^{n} \binom{n}{j}^3$ and $Q_n = \sum_{k=0}^{n} \binom{n}{k}(-8)^{n-k} f_k$. We prove that, for every odd prime p, the two sums $\sum_{n=0}^{p-1} \binom{2n}{n} Q_n/(-32)^n$ and $\sum_{n=0}^{p-1} \binom{2n}{n} Q_n/64^n$ are congruent modulo p^2 to $4x^2 - 2p$ when $p = x^2 + 2y^2 \equiv 1, 3 \pmod 8$, and to zero when $p \equiv 5, 7 \pmod 8$. For inert primes a finite quadratic differential invariant gives ordinary and singular lifting results, including a formula for the defect at a simple singularity. For split primes we certify the modular period by identities of weight eight, construct an integral Hecke polynomial with an explicit degree bound, and specialize a finite polynomial identity at two complex multiplication points. The coefficient at degree p, both classes of complex multiplication matrices, and the primes 3 and 5 are treated explicitly.

hexagon:2611.00550v1

1 The supercongruence and the proof strategy

For $n \geq 0$ define

$$f_n = \sum_{j=0}^{n} \binom{n}{j}^3, \qquad Q_n = \sum_{k=0}^{n} \binom{n}{k}(-8)^{n-k} f_k. \tag{1}$$

The numbers f_n are the Franel numbers. Write

$$G(t) = \sum_{n \geq 0} \binom{2n}{n} Q_n t^n, \qquad G_p(t) = \sum_{n=0}^{p-1} \binom{2n}{n} Q_n t^n. \tag{2}$$

The denominators are units for every odd prime. Congruences between p-integral rational numbers are interpreted in $\mathbb{Z}_p$. The subscript p always denotes truncation at $p-1$.

Theorem 1.1. *For every odd prime p,*

$$G_p(-1/32) \equiv G_p(1/64) \equiv \begin{cases} 4x^2 - 2p, & p = x^2 + 2y^2 \equiv 1, 3 \pmod 8, \\ 0, & p \equiv 5, 7 \pmod 8 \end{cases} \pmod{p^2}. \tag{3}$$

This is Conjecture 3.6 of Zhi-Hong Sun [1, p. 2742]. The representation by $x^2 + 2y^2$ is unique up to the signs of x, y, which do not affect $4x^2 - 2p$. Its existence for $p \equiv 1, 3 \pmod 8$ follows from the norm-Euclidean ring $\mathbb{Z}[\sqrt{-2}]$ and quadratic reciprocity. Indeed, rounding both coordinates gives an error of norm at most $1/4 + 2/4 < 1$, so this ring is Euclidean. For these primes a root of $X^2 + 2$ modulo p gives a proper nontrivial factor of (p), and a generator of that factor has norm p.

The sequence in (1) satisfies the integral recurrence

$$(n+1)^2 Q_{n+1} = (-17n(n+1) - 6)Q_n - 72n^2 Q_{n-1}, \qquad Q_0 = 1, \quad Q_1 = -6, \tag{4}$$

as recorded in [1, pp. 2729–2730]. Sun's Theorem 3.7 on p. 2740 supplies the input

$$G_p(-1/32) \equiv G_p(1/64) \equiv 0 \pmod p \qquad (p > 5,\ p \equiv 5, 7 \pmod 8). \tag{5}$$

Although its printed statement includes $p > 3$, the proof uses a sum with denominator 100^n. We use it only for $p > 5$ and supply an autonomous argument for $p = 5$ in Section 3.

Section 2 proves the differential invariant and the local lifting results. Section 3 completes the inert branch. The endpoint congruence in Section 4 concerns individual coefficients and is independent of the sums in (3). Sections 5 and 6 certify the period, its character, its divisors and the two complex multiplication values. Section 7 proves the Hecke orbit and the integral polynomial construction, following [2, Lemma 3.7 and Section 5]. Section 8 derives the finite specialization, with the degree-p coefficient included. Section 9 gives the three required matrix constructions and completes the proof. All uses of finite modular certificates are accompanied by the holomorphy and valence argument that makes them sufficient.

2 The finite differential invariant and local lifting

We first work with an integral sequence u_n, parameters $a, b, c \in \mathbb{Z}$, and recurrence

$$u_0 = 1, \quad u_1 = b, \qquad (n+1)^2 u_{n+1} = (an(n+1) + b)u_n - cn^2 u_{n-1} \quad (n \geq 1). \tag{6}$$

Let $v_n = \binom{2n}{n} u_n$, $V(t) = \sum_{n \geq 0} v_n t^n$ and $\theta = t\, d/dt$. The ratios of consecutive central binomial coefficients give

$$n^3 v_n = 2(2n-1)(an(n-1) + b)v_{n-1} - 4c(n-1)(2n-3)(2n-1)v_{n-2} \quad (n \geq 1), \tag{7}$$

where $v_{-1} = 0$. Thus $LV = 0$, with

$$L = \theta^3 - 2t(2\theta + 1)(a\theta^2 + a\theta + b) + 4ct^2(\theta + 1)(2\theta + 1)(2\theta + 3). \tag{8}$$

Put $D(t) = 1 - 4at + 16ct^2$. With coefficients on the left,

$$\begin{aligned} L = D\theta^3 &+ (-6at + 48ct^2)\theta^2 \\ &+ (-2(a + 2b)t + 44ct^2)\theta - 2bt + 12ct^2. \end{aligned} \tag{9}$$

For a polynomial or formal series Y, define

$$I(Y) = D(2Y\theta^2 Y - (\theta Y)^2) + (\theta D)Y\theta Y + 4t(-b + 3ct)Y^2. \tag{10}$$

Lemma 2.1. *For every Y,*

$$\theta I(Y) = 2Y LY. \tag{11}$$

In particular $I(V) = 0$ in $\mathbb{Q}[[t]]$.

Proof. Set $E = 4t(-b + 3ct)$. The product rule gives

$$\theta I(Y) = 2DY\theta^3 Y + 3(\theta D)Y\theta^2 Y + (\theta^2 D + 2E)Y\theta Y + (\theta E)Y^2.$$

The coefficients agree with $2YLY$ in (9). Since $LV = 0$, $I(V)$ is constant in characteristic zero, and its constant term is zero. □

Proposition 2.2. *Under (6), suppose all u_n are integers. For every prime $p > 3$, the polynomial $U(t) = \sum_{n=0}^{p-1} v_n t^n$ satisfies*

$$I(U) \equiv 0 \pmod{p^2} \quad \text{in } \mathbb{Z}[t], \qquad \deg(U \bmod p) \leq \frac{p-1}{2}. \tag{12}$$

Proof. The exact residual of the truncation, from (7), is

$$LU = -p^3 v_p t^p + 4cp(2p-1)(2p+1)v_{p-1} t^{p+1}. \tag{13}$$

The omitted v_p supplies the first term, and the highest remaining degree is $p+1$. Since $p \mid \binom{2p-2}{p-1}$ and u_{p-1} is integral, $p \mid v_{p-1}$. Hence $LU \equiv 0 \pmod{p^2}$, and (11) gives $\theta I(U) \equiv 0 \pmod{p^2}$.

Here $\deg I(U) \le 2p$ and $[t^0]I(U) = 0$. For positive degrees other than $p, 2p$, division by the degree is division by a unit modulo p^2. The two remaining coefficients must be computed before reduction. As $V - U = v_p t^p + O(t^{p+1})$ and $I(V) = 0$,

$$[t^p]I(U) = -2p^2 v_p. \tag{14}$$

At this degree the only contribution of the omitted term pairs $V(0) = 1$ with $\theta^2(v_p t^p)$ in $2V\theta^2 V$; all other terms have an extra t or a derivative of the constant. At degree $2p$, only the highest coefficient of each factor U contributes. Its scalar multiplier is

$$16c(p-1)^2 + 32c(p-1) + 12c = 4c(2p-1)(2p+1),$$

so

$$[t^{2p}]I(U) = 4c(2p-1)(2p+1)v_{p-1}^2. \tag{15}$$

Both coefficients are divisible by p^2. This proves the polynomial congruence in every degree. Finally, $p \mid \binom{2n}{n}$ for $(p-1)/2 < n < p$, proving the degree bound after reduction modulo p. □

Remark 2.3. The half-degree bound in (12) holds modulo p. The polynomial U in the congruence modulo p^2 still includes every index $0 \le n < p$; its upper coefficients have not been discarded.

Lemma 2.4. *Let $\overline{U} \in \mathbb{F}_p[t]$ be the reduction of U in Proposition 2.2, and let $r \in \overline{\mathbb{F}_p}^\times$ be a zero of $\overline{U}$. If $D(r) \neq 0$, its multiplicity is exactly two. If $D(r) = 0$ and $D'(r) \neq 0$, its multiplicity is exactly one.*

Proof. At an ordinary zero the invariant modulo p implies $\theta\overline{U}(r) = 0$, so the multiplicity is at least two. The coefficients of the third and second ordinary derivatives in L are

$$A_3 = t^3 D, \qquad A_2 = 3t^2 D + \tfrac{3}{2} t^3 D'. \tag{16}$$

If the multiplicity were $3 \le m < p$, write the leading local term as $u(t-r)^m$, $u \neq 0$. At degree $m-3$, the term LU would have coefficient $ur^3 D(r)m(m-1)(m-2) \neq 0$; the other derivatives start in higher degrees. This contradicts $LU \equiv 0 \pmod p$. The nonzero polynomial $\overline{U}$ has degree less than p, so larger multiplicities cannot occur.

At a simple zero of D, suppose $m \ge 2$. By the half-degree bound, $m \le (p-1)/2$. In degree $m-2$, the combined leading coefficient of the third and second derivatives is

$$ur^3 D'(r)m(m-1)(m-\tfrac{1}{2}).$$

All remaining terms start at degree at least $m-1$. This coefficient is nonzero: the bound excludes the resonance $m = (p+1)/2$ as well as $m = 0, 1$. Hence the zero is simple. □

Theorem 2.5 (Ordinary lifting)**.** *In Proposition 2.2, let $t_0 \in \mathbb{Z}_p$ with $t_0 D(t_0) \in \mathbb{Z}_p^\times$. Then*

$$U(t_0) \equiv 0 \pmod p \quad \Longrightarrow \quad U(t_0) \equiv 0 \pmod{p^2}.$$

The conclusion holds for every p-integral lift of the same residue class.

Proof. Lemma 2.4 shows that the reduced zero is exactly double. Therefore $\theta U(t_0) \in p\mathbb{Z}_p$ and $\theta^2 U(t_0) \in \mathbb{Z}_p^\times$. In (12), all terms at t_0 except $2D(t_0)U(t_0)\theta^2 U(t_0)$ are divisible by p^2. Its coefficient of $U(t_0)$ is a unit, proving the result. The argument applies to every lift of the residue class. □

Theorem 2.6 (Lifting at an exact simple singularity)**.** *In Proposition 2.2, let $t_0 \in \mathbb{Z}_p^\times$ with $D(t_0) = 0$ exactly and $D'(t_0) \in \mathbb{Z}_p^\times$. Then $U(t_0) \equiv 0 \pmod p$ implies $U(t_0) \equiv 0 \pmod{p^2}$.*

Proof. Lemma 2.4 gives $U'(t_0) \in \mathbb{Z}_p^\times$. Since $D(t_0) = 0$, the invariant specializes to

$$U(t_0)\big[(\theta D)(t_0)\theta U(t_0) + 4t_0(-b + 3ct_0)U(t_0)\big] \equiv 0 \pmod{p^2}.$$

The bracket is a unit: its first term is a unit and the second is divisible by p. Division by this bracket proves the conclusion. □

Theorem 2.7 (The defect at a simple singularity)**.** *In Proposition 2.2, suppose $t_0 \in \mathbb{Z}_p^\times$, $D(t_0) \equiv U(t_0) \equiv 0 \pmod{p}$, and $D'(t_0) \in \mathbb{Z}_p^\times$. Then $U'(t_0)$ is a unit and*

$$U(t_0) \equiv D(t_0)\frac{U'(t_0)}{D'(t_0)} \pmod{p^2}. \tag{17}$$

Consequently $U(t_0) \equiv 0 \pmod{p^2}$ if and only if $D(t_0) \equiv 0 \pmod{p^2}$.

Proof. The unit assertion follows from Lemma 2.4. The terms containing $D(t_0)U(t_0)$ or $U(t_0)^2$ vanish modulo p^2 in the invariant. Thus

$$-D(t_0)(\theta U(t_0))^2 + (\theta D(t_0))U(t_0)\theta U(t_0) \equiv 0 \pmod{p^2}.$$

Both $\theta U(t_0) = t_0 U'(t_0)$ and $\theta D(t_0) = t_0 D'(t_0)$ are units. Dividing by them gives (17). The quotient $U'(t_0)/D'(t_0)$ is a unit, giving the equivalence. □

Corollary 2.8. *For a zero $r \in \mathbb{F}_p^\times$ of $\overline{U}$, if $D(r) \neq 0$, all p lifts modulo p^2 are zeros of U modulo p^2. If $D(r) = 0$ and $D'(r) \neq 0$, there is exactly one such lift; it is the unique zero of D modulo p^2 above r.*

Proof. The ordinary assertion is Theorem 2.5. In the singular case, Theorem 2.7 identifies the two sets of zeros. For any lift $\widetilde{r}$, the congruence

$$D(\widetilde{r} + ps) \equiv D(\widetilde{r}) + psD'(\widetilde{r}) \pmod{p^2}$$

has exactly one solution $s \in \mathbb{F}_p$. □

3 The inert primes, including the prime five

For the recurrence (4), the parameters are $(a, b, c) = (-17, -6, 72)$, and

$$D(t) = 1 + 68t + 1152t^2 = (1 + 32t)(1 + 36t). \tag{18}$$

At $t_- = -1/32$, one has $D(t_-) = 0$ exactly and $t_- D'(t_-) = 1/8$. Theorem 2.6 applies for every $p > 3$. At $t_+ = 1/64$,

$$D(t_+) = 75/32, \qquad D'(t_+) = 104. \tag{19}$$

For $p > 5$ this is an ordinary point, so Theorem 2.5 applies. The input (5) therefore gives $G_p(-1/32) \equiv G_p(1/64) \equiv 0 \pmod{p^2}$ for all inert $p > 5$.

For $p = 5$, the first three original coefficients are $Q_0 = 1, Q_1 = -6, Q_2 = 42$. The half-degree bound gives, directly,

$$G_5(t) \equiv 1 - 12t + 252t^2 \equiv 1 + 3t + 2t^2 \pmod{5}. \tag{20}$$

This vanishes at $-1/32 \equiv 2$ and $1/64 \equiv 4 \pmod{5}$. The first point is handled by the exact singular lifting theorem. For the second, (19) gives $D(t_+) \equiv 0 \pmod{25}$ and $D'(t_+) \not\equiv 0 \pmod{5}$; Theorem 2.7 gives $G_5(1/64) \equiv 0 \pmod{25}$. Equivalently,

$$\frac{1}{64} - \left(-\frac{1}{36}\right) = \frac{25}{576}$$

identifies this point modulo 25 with the other exact singularity. This calculation supplies the initial residue at five without using the denominator-100 step in the proof of Sun's theorem.

Remark 3.1. Exact singular lifting need not persist under arbitrary shifts by p. For example, direct evaluation at $p = 7$, $t_- = -1/32$, gives

$$G_7(t_-) \equiv 0 \pmod{49}, \qquad \theta G_7(t_-) \equiv 5 \pmod{7}, \qquad G_7(t_- + 7) \equiv 7 \pmod{49}.$$

The defect formula (17) describes the dependence on the lift.

4 The coefficient at degree p

The modular truncation will require $\binom{2p}{p} Q_p \equiv -12 \pmod{p^2}$. This known coefficient congruence is separate from Theorem 1.1. For $p > 3$, the congruence for Q_p below follows by setting $n = 1$ and reducing modulo p^2 in Mao's formula for Q_{np} modulo p^3 [3, p. 3, Theorem 1.4]. We retain the proof via Straub's theorem, which also covers $p = 3$, and the direct derivation from Gorodetsky's representation.

Lemma 4.1. *For every odd prime p,*

$$Q_p \equiv -6 \pmod{p^2}, \qquad \binom{2p}{p} Q_p \equiv -12 \pmod{p^2}. \tag{21}$$

Proof. The positive sequence F in Straub's notation is

$$A_F(n) = \sum_{k=0}^{n} (-1)^k 8^{n-k} \binom{n}{k} f_k = (-1)^n Q_n.$$

Straub [4, p. 5, (10), Theorem 3.2] proves $A_F(p^r n) \equiv A_F(p^{r-1} n) \pmod{p^{2r}}$ for $p \geq 3$ and $n, r \geq 1$. Setting $n = r = 1$ gives $Q_p = -A_F(p) \equiv -A_F(1) = -6 \pmod{p^2}$. Also

$$\binom{2p}{p} = 2 \prod_{k=1}^{p-1} (1 + p/k) \equiv 2 \pmod{p^2},$$

because $\sum_{k=1}^{p-1} k^{-1} = 0 \pmod{p}$ for every odd prime. Multiplication gives the second congruence. □

The required case can also be seen directly from the exact representation of Gorodetsky [5, p. 4, Proposition 1.2, (1.8)]:

$$A_F(n) = \sum_{(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d},\mathbf{e}) \in T(n)} (-1)^{a_1 + b_2 + c_3} \binom{n}{\mathbf{a}} \binom{n}{\mathbf{b}} \binom{n}{\mathbf{c}} \binom{n}{\mathbf{d}} \binom{n}{\mathbf{e}}. \tag{22}$$

Here each of the five rows is a nonnegative triple of sum n, and the three columns satisfy

$$a_i + b_i + c_i + d_i + 2e_i = 2n \qquad (i = 1, 2, 3).$$

At $n = p$, call a row pure if it is a permutation of $(p, 0, 0)$. Every non-pure row has its multinomial divisible by p and has a coordinate nonzero modulo p. If it were the only non-pure row, the corresponding column equation modulo p would be impossible: the pure rows contribute zero and the weight of this coordinate is 1 or 2, both invertible. Therefore every term with a non-pure row has at least two such rows and is divisible by p^2.

For the all-pure terms, division of every coordinate by p gives a bijection with $T(1)$. Their multinomials are 1, and their signs are preserved since p is odd. Their sum is $A_F(1) = 6$. Thus (22) proves the necessary endpoint as well. Straub's proof uses this representation; these are two presentations of the arithmetic step, with the representation itself attributed to Gorodetsky. Neither presentation uses a value of $G_p(-1/32)$ or $G_p(1/64)$.

5 An exact modular period

5.1 Eta products, divisors and the cusp constants

Let $q = e^{2\pi i\tau}$, $\eta_d = \eta(d\tau)$ and $\partial = q\,d/dq = (2\pi i)^{-1}d/d\tau$. Define

$$h = \frac{\eta_2\eta_6^5}{\eta_1^5\eta_3}, \qquad z = \frac{\eta_1^6\eta_6}{\eta_2^3\eta_3^2}, \qquad U_\eta = z^2, \qquad V_\eta = h^2z^2,$$
$$\Theta = U_\eta - 72V_\eta = (1-72h^2)z^2, \qquad J = (\eta_1\eta_2\eta_3\eta_6)^2,$$
$$R = \frac{\eta_2^{12}\eta_3^{12}}{\eta_1^{12}\eta_6^{12}}, \qquad H_2 = \frac{\eta_2^{24}}{\eta_1^{24}}. \tag{23}$$

The subscript in U_η distinguishes it from the finite polynomial U.

We use the eta-quotient criterion and cusp-order formula in [6, p. 2]. For an exponent vector $(r_d)_{d|6}$, the weight is $k = \frac{1}{2}\sum r_d$. The congruences

$$\sum_{d|6} dr_d \equiv \sum_{d|6}(6/d)r_d \equiv 0 \pmod{24}$$

and the condition that $\prod d^{r_d}$ is a rational square give trivial character here, since every weight in the table is even. For a cusp with denominator $c \mid 6$, its local order is

$$\frac{6}{24\gcd(c^2,6)}\sum_{d|6}\frac{\gcd(c,d)^2}{d}r_d. \tag{24}$$

The cusp representatives are $0, 1/2, 1/3, \infty$, of widths $6, 3, 2, 1$, respectively. The resulting data are

	r_1	r_2	r_3	r_6	weight	cusp orders
h	-5	1	-1	5	0	$(-1,0,0,1)$
R	-12	12	12	-12	0	$(-1,1,1,-1)$
H_2	-24	24	0	0	0	$(-3,3,-1,1)$
U_η	12	-6	-4	2	2	$(2,0,0,0)$
V_η	2	-4	-6	12	2	$(0,0,0,2)$
J	2	2	2	2	4	$(1,1,1,1)$

The nonnegative orders show that U_η, V_η, J are holomorphic modular forms. The other products are meromorphic modular functions. Eta has no zeros on $\mathfrak{H}$. Thus h has precisely one pole, simple, on the compact curve $X_0(6)$, so it is a global coordinate on that curve. This also establishes genus zero directly.

The exact phases, derived from the Dedekind transformation law in Appendix B, give

$$h(0) = \infty, \qquad h(1/2) = -1/9, \qquad h(1/3) = -1/8, \qquad h(\infty) = 0. \tag{25}$$

These agree with the data in [2, Section 8.10].

Lemma 5.1. *The following identities hold:*

$$R = h^{-1} + 17 + 72h = \frac{(1+8h)(1+9h)}{h}, \tag{26}$$
$$H_2 = \frac{h(1+9h)^3}{1+8h}, \tag{27}$$
$$\Theta = -\partial \log R. \tag{28}$$

Moreover, Θ is holomorphic of weight two with trivial character on $\Gamma_0(6)$, and is nonzero at every cusp.

Proof. In the coordinate h, R has only simple poles at 0 and ∞. Consequently it has the form $a/h + b + ch$. The exact expansions

$$h = q + 5q^2 + 19q^3 + O(q^4), \qquad R = q^{-1} + 12 + 78q + O(q^2)$$

determine $a = 1, b = 17, c = 72$. The three-dimensional rational function space justifies the sufficiency of this comparison.

By (25), the right side of (27) has the same divisor as H_2: its orders are $(-3, 3, -1, 1)$. There are no other zeros or poles, and both functions have leading term q at infinity. Their quotient is a holomorphic nonvanishing function on a compact curve, so it is the constant 1.

The logarithmic derivative $\partial \log R$ is modular of weight two on the base group. In the interior it is holomorphic since R has no zeros or poles there. At a cusp of width w, the transformed function has expansion $Q^r(c_0 + O(Q))$, with $Q = e^{2\pi i\tau/w}$, $r = \pm 1$ and $c_0 \neq 0$. Its logarithmic derivative has constant term r/w and no negative powers. Hence $\Theta + \partial \log R \in M_2(\Gamma_0(6))$. The first three coefficients vanish, because both sides of (28) begin $1 - 12q - 12q^2$.

The index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(6)] = 12$ gives valence bound 2 in weight two. A nonzero holomorphic form cannot have order greater than 2 at infinity; see [7, p. 2, Theorem 1.1(1)] for this classical bound. The difference has order at least 3 and is therefore zero. At each cusp the constant term of Θ is $-r/w \neq 0$. This proves its nonvanishing without assuming that the two summands U_η and $72V_\eta$ cannot cancel. □

5.2 Two identities of weight eight

Lemma 5.2. *Put* $W = \Theta\partial \log J - 2\partial\Theta$. *Then*

$$W^2 - \Theta^4 - 68J\Theta^2 - 1152J^2 = 0, \tag{29}$$

$$2\Theta\partial^2\Theta - 3(\partial\Theta)^2 + 24J\Theta^2 + 864J^2 = 0. \tag{30}$$

Proof. For $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(6)$, set $j = c\tau + d$ and $s = c/(2\pi i)$. The chain rule gives

$$\begin{aligned} (\partial\Theta)(M\tau) &= j^4\partial\Theta + 2sj^3\Theta, \\ (\partial^2\Theta)(M\tau) &= j^6\partial^2\Theta + 6sj^5\partial\Theta + 6s^2j^4\Theta, \\ (\partial \log J)(M\tau) &= j^2\partial \log J + 4sj. \end{aligned}$$

Therefore W has weight four, and $2\Theta\partial^2\Theta - 3(\partial\Theta)^2$ has weight eight. All derivative anomalies cancel exactly.

These covariant expressions are also holomorphic at the cusps. For a cusp matrix σ, the same chain-rule computation expresses their transforms in terms of the holomorphic expansions of $\Theta|_2\sigma$ and $J|_4\sigma$. Derivatives introduce no negative powers. The logarithmic derivative of $J|_4\sigma$ is holomorphic there, since its expansion begins with a nonzero constant times a power of the local parameter. In the interior J has no zeros. Thus both residuals really belong to $M_8(\Gamma_0(6))$ before any coefficient comparison is made.

Appendix A gives the exact expansions and an integer-product algorithm for the coefficients from q^0 to q^8 of both residuals. All eighteen coefficients are zero. The valence bound in weight eight is $8 \cdot 12/12 = 8$; each residual has order at least 9, so both vanish identically. Only the classical holomorphic-form bound is used. □

Proposition 5.3. *Let*

$$P(h) = h(1 + 8h)(1 + 9h), \qquad K(h) = (1 - 72h^2)^2.$$

Then

$$t = \frac{J}{\Theta^2} = \frac{P(h)}{K(h)} \in q + q^2\mathbb{Z}[[q]], \qquad G(t(q)) = \Theta(q). \tag{31}$$

Proof. Comparison of eta exponents gives $J = h^2Rz^4$. Equations (26) and (23) give the rational expression for t. The products have integral expansions and $\Theta(0) = 1$, so $t \in q + q^2\mathbb{Z}[[q]]$. This series has an integral formal inverse $q = q(t)$.

Let $e = \partial \log t = W/\Theta$, a unit formal series. The first certificate implies

$$e^2 = D(t)\Theta^2, \qquad D(t) = 1 + 68t + 1152t^2.$$

Regard $Y(t) = \Theta(q(t))$ as a series in t. Then $\partial = e\theta$, and logarithmic differentiation of the last identity gives

$$2\frac{\theta e}{e} = \frac{\theta D}{D} + 2\frac{\theta Y}{Y}.$$

Substituting $\partial = e\theta$ into (30), dividing by e^2, and using $J = tY^2$, gives

$$D\big(2Y\theta^2 Y - (\theta Y)^2\big) + (\theta D)Y\theta Y + (24t + 864t^2)Y^2 = 0.$$

This is $I(Y) = 0$ for $(a, b, c) = (-17, -6, 72)$. By (11) and the fact that Y is a unit, $LY = 0$ in characteristic zero. The recurrence (4) gives $LG = 0$ for the same operator. At each degree $n \geq 1$, the equation determines the new coefficient with multiplier $n^3 \neq 0$. The constant term 1 therefore determines a unique formal solution, proving $Y = G$. □

The period also corresponds to the level-6 parametrization of Chan–Cooper [9]. In their convention the recurrence parameter is $c = -72$, the negative of the $c = 72$ in (6). The proof above certifies the period directly and does not require that parametrization as an input.

6 Character, quotient geometry and complex multiplication values

For a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of positive determinant, use

$$(Y|_2 M)(\tau) = \det(M)(c\tau + d)^{-2} Y(M\tau). \tag{32}$$

Scalar matrices act trivially in this convention. Set

$$W_2 = \begin{pmatrix} 2 & -1 \\ 6 & -2 \end{pmatrix}, \qquad W_6 = \begin{pmatrix} 0 & -1 \\ 6 & 0 \end{pmatrix}, \qquad \Gamma = \Gamma_0(6) + \langle 2, 6\rangle. \tag{33}$$

We regard this full Atkin–Lehner extension projectively. The normalizer action on $X_0(6)$ has a quotient of order four. For completeness, the conjugation formulas in Section 7 show that both W_2, W_6 normalize the base group. Also $W_2^2 = -2I$, $W_6^2 = -6I$ and

$$W_2W_6(W_6W_2)^{-1} = \begin{pmatrix} 5 & 2 \\ 12 & 5 \end{pmatrix} \in \Gamma_0(6). \tag{34}$$

Thus the projective quotient has at most four elements. The determinant classes modulo squares in $\mathbb{Q}^\times$ are $1, 2, 3, 6$, so these four cosets are distinct. This is the standard extension used in [2, Section 3].

Lemma 6.1. *The actions on h are*

$$\phi_2(h) = -\frac{1 + 8h}{8(1 + 9h)}, \qquad \phi_6(h) = \frac{1}{72h}. \tag{35}$$

The form Θ has trivial character on $\Gamma_0(6)$ and

$$\Theta|_2 W_2 = -\Theta, \qquad \Theta|_2 W_6 = \Theta.$$

The parameter t is invariant under Γ.

Proof. Since h is a global coordinate, an automorphism acts on it by a Möbius transformation. Direct action on the cusp fractions shows that W_2 exchanges $\infty \leftrightarrow 1/3$ and $0 \leftrightarrow 1/2$, while W_6 exchanges $\infty \leftrightarrow 0$ and $1/2 \leftrightarrow 1/3$. The four values in (25) determine the two transformations in (35); three values suffice in each case. Exact rational substitution gives

$$R(\phi_2(h)) = R(h)^{-1}, \qquad R(\phi_6(h)) = R(h), \qquad t(\phi_2(h)) = t(\phi_6(h)) = t(h).$$

If $R(M\tau) = R(\tau)^{\varepsilon}$, the chain rule and $d(M\tau)/d\tau = \det(M)/(c\tau + d)^2$ imply

$$(-\partial \log R)|_2 M = \varepsilon(-\partial \log R).$$

Equation (28) proves the character assertions. The signs follow from the transformation law of R. □

Proposition 6.2. *The function t is a Hauptmodul for Γ. On $X_0(6)$ its two poles are double, and the zeros of Θ in the interior are simple and lie precisely above these poles. The form Θ has no zeros at the cusps. An invariant function with at most m factors Θ^{-1} in its denominator, holomorphic numerators and no other poles is a polynomial in t of degree at most $\lfloor m/2 \rfloor$.*

Proof. The polynomials P and K are coprime, and P/K has degree four as a map in the base coordinate h. Its invariance under the quotient of order four makes its degree on the quotient curve equal to one, proving the Hauptmodul assertion. Its base poles are $h = \pm 1/\sqrt{72}$, both double and both away from the cusps. The formula $\Theta = (1 - 72h^2)z^2$, with z nonzero in the interior, gives simple zeros precisely there. The base group has no elliptic torsion: trace zero is impossible modulo 3, and trace ± 1 is impossible modulo 2 for matrices of determinant one with lower-left entry divisible by 6. Thus h is an ordinary local coordinate at these points. Nonvanishing at the cusps was proved in Lemma 5.1.

The invariant function in the final assertion has no poles on the quotient except at $t = \infty$, so it is a polynomial in t. On the base curve its pole order is at most m. A polynomial of degree d in t has pole order $2d$ there. Hence $2d \le m$, as claimed. This calculation takes place on the base curve and does not require integral local orders on the orbifold quotient. □

Lemma 6.3. *For $\delta = \sqrt{-2}$ with positive imaginary part, set*

$$\beta = \delta/2, \qquad \gamma = (2 + \delta)/6. \tag{36}$$

Then

$$t(\beta) = 1/64, \qquad t(\gamma) = -1/32, \qquad \Theta(\beta)\Theta(\gamma) \neq 0. \tag{37}$$

Proof. Since $2\beta = -1/\beta$, the eta inversion formula [8, Section 23.18] gives $H_2(\beta) = (-i\beta)^{12} = 1/64$. Equation (27) therefore gives

$$64h(1 + 9h)^3 - (1 + 8h) = (72h^2 + 16h + 1)(648h^2 + 72h - 1) = 0.$$

All eta factors are positive on the imaginary axis, so $h(\beta) > 0$. It follows that $h(\beta) = (\sqrt{6} - 2)/36$, the positive root of the second factor. The identity

$$64P(h) - K(h) = -(8h^2 - 8h - 1)(648h^2 + 72h - 1)$$

proves $t(\beta) = 1/64$.

The equation $6\gamma^2 - 4\gamma + 1 = 0$ shows that $W_2\gamma = \gamma$. Its action on h gives $72h(\gamma)^2 + 16h(\gamma) + 1 = 0$. Now

$$32P(h) + K(h) = (72h^2 + 16h + 1)^2$$

proves $t(\gamma) = -1/32$. Neither of the two relevant quadratics has a common root with $1 - 72h^2$. Thus the rational denominators and Θ are nonzero at both points. These values follow from exact algebraic identities. □

7 The Hecke orbit and an integral polynomial

7.1 The orbit for a general prime

The following argument makes explicit the level-6 case of [2, Lemma 3.7]. It uses the weight-two transformation law and the trivial character on the base group. For $p > 3$, let

$$\mathcal{M}(6,p) = \{M \in M_2(\mathbb{Z}) : \det M = p,\ 6 \mid M_{21}\}.$$

Lemma 7.1. *The left classes modulo $\Gamma_0(6)$ in $\mathcal{M}(6,p)$ have representatives*

$$D_\infty = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \qquad D_k = \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix} \quad (0 \le k < p). \tag{38}$$

The group Γ permutes the ratios $r_D = (\Theta|_2 D)/\Theta$ for these $p+1$ representatives.

Proof. For $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}(6,p)$, put $r = \gcd(a,c) > 0$. Then $r \mid p$, so $r = 1$ or p, and $6 \mid c/r$ because $p \nmid 6$. Choose u, v with $ua + vc = r$. The matrix

$$L = \begin{pmatrix} u & v \\ -c/r & a/r \end{pmatrix} \in \Gamma_0(6) \quad \text{gives} \quad LM = \begin{pmatrix} r & b' \\ 0 & p/r \end{pmatrix}.$$

A left translation reduces b' modulo p/r. This gives D_∞ when $r = p$, and a D_k when $r = 1$. Unimodular row operations preserve r. In the latter case, $D_l D_k^{-1} = \begin{pmatrix} 1 & (l-k)/p \\ 0 & 1 \end{pmatrix}$ is integral if and only if $k \equiv l \pmod p$, proving distinctness.

Right multiplication and conjugation by base-group elements preserve $\mathcal{M}(6,p)$. For $M = \begin{pmatrix} a & b \\ 6c & d \end{pmatrix}$, direct multiplication gives

$$\begin{aligned} W_2^{-1} M W_2 &= \begin{pmatrix} -2a - 6b + 6c + 3d & a + 2b - 3c - d \\ -6a - 18b + 12c + 6d & 3a + 6b - 6c - 2d \end{pmatrix}, \\ W_6^{-1} M W_6 &= \begin{pmatrix} d & -c \\ -6b & a \end{pmatrix}. \end{aligned} \tag{39}$$

These matrices are integral with determinant p and lower-left entry divisible by 6. The operations are reversible and hence permute the left classes. The same formulas with determinant one also verify normalization of $\Gamma_0(6)$ as used above.

For a normalizer element w, using the slash convention (32) and its character $\chi(w)$ gives

$$r_D(w\tau) = \frac{\Theta|_2 Dw}{\Theta|_2 w} = \frac{\Theta|_2 w(w^{-1}Dw)}{\chi(w)\Theta} = \frac{\Theta|_2 (w^{-1}Dw)}{\Theta}.$$

Reduction of $w^{-1}Dw$ to a representative D_j uses a matrix on the left in $\Gamma_0(6)$, whose character is trivial. Thus these transformations permute the ratios. The same computation for the base group completes the assertion for the whole extension. □

7.2 Polynomiality, degree and integral descent

Proposition 7.2. *For every prime $p > 3$ there is a polynomial*

$$\mathcal{T}_p(X,t) = \sum_{m=0}^{p+1} C_m(t) X^m \in \mathbb{Z}[X,t]$$

such that

$$\mathcal{T}_p(X, t(\tau)) = \left(1 - \frac{\Theta(p\tau)}{\Theta(\tau)}X\right) \prod_{k=0}^{p-1} \left(p^2 - \frac{\Theta((\tau+k)/p)}{\Theta(\tau)}X\right). \tag{40}$$

Its coefficients satisfy

$$\deg C_m \le \lfloor m/2 \rfloor, \qquad \mathcal{T}_p \equiv C_p X^p + C_{p+1}X^{p+1} \pmod{p^2}, \qquad C_{p+1} \equiv 1 \pmod{p}. \tag{41}$$

Proof. The product in (40) equals

$$p^{2p} \prod_{[D]} \left(1 - \frac{\Theta|_2 D}{p\Theta}X\right),$$

since $r_{D_\infty} = p\Theta(p\tau)/\Theta(\tau)$ and $r_{D_k} = \Theta((\tau+k)/p)/(p\Theta(\tau))$. Lemma 7.1 proves invariance of its coefficients under Γ.

The numerators $\Theta|_2 D$ are holomorphic in the interior and at the cusps. To justify the latter assertion, let $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ represent a cusp, and choose $\sigma' \in \mathrm{SL}_2(\mathbb{Z})$ taking infinity to the rational cusp $D\sigma\infty$. Then $\sigma'^{-1}D\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $a/d > 0$. Up to a nonzero constant, the expansion of $(\Theta|_2 D)|_2\sigma$ is that of $\Theta|_2\sigma'$ evaluated at $(a\tau+b)/d$. Nonnegative exponents remain nonnegative; possible fractional local exponents cause no poles. The denominator Θ has nonzero constant term at every cusp. Thus the coefficients have no cusp poles, and their only possible interior poles lie above $t = \infty$. Proposition 6.2 makes them polynomials in t and gives the degree bound $\lfloor m/2 \rfloor$.

For integral descent, first work in $\mathbb{Z}[\zeta_p][[s]]$, where $s = q^{1/p}$ and ζ_p is a primitive pth root of unity. All coefficients of Θ are integers, and its constant term is 1, so its inverse has integral coefficients. The symmetry $s \mapsto \zeta_p s$ of the product eliminates powers of s not divisible by p. Galois substitutions $\zeta_p \mapsto \zeta_p^a$ permute the factors and make the resulting coefficients rational. They are also algebraic integers, and hence the coefficients lie in $\mathbb{Z}[[q]]$. Since $t = q + q^2\mathbb{Z}[[q]]$, successive elimination of the lowest coefficient of a polynomial in t gives $C_m \in \mathbb{Z}[t]$. More explicitly, the coefficient of q^j after removal of the terms of lower t-degree is exactly the coefficient of t^j, and is an integer.

For $m < p$, every term contributing to X^m contains at least one constant factor p^2 from the p finite factors. After division by p^2, the same symmetries and integral descent still apply. Thus $C_m \in p^2\mathbb{Z}[t]$ for $m < p$.

Since $p+1$ is even, the leading coefficient is

$$C_{p+1} = \frac{\Theta(q^p)\prod_{k=0}^{p-1}\Theta(\zeta_p^k s)}{\Theta(q)^{p+1}}. \tag{42}$$

The finite product in the numerator lies in $\mathbb{Z}[[q]]$. Modulo $1-\zeta_p$, it equals $\Theta(s)^p$, which in characteristic p equals $\Theta(q)$. On its already integral rational coefficients, $(1-\zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = p\mathbb{Z}$, so this is a congruence modulo p in $\mathbb{Z}[[q]]$. Also $\Theta(q^p) \equiv \Theta(q)^p \pmod{p}$. Equation (42) gives $C_{p+1} \equiv 1$ as a series, and triangular elimination gives the same congruence in $\mathbb{Z}[t]$. □

The ratio of a simple zero of Θ to a double pole of t is $1/2$. The proof of Proposition 7.2 uses exactly this bound and a modulus-p^2 product argument. It does not apply the general modulus-p^3 theorem in [2, Section 5], whose relevant stronger hypothesis is not satisfied here.

8 The finite specialization and its degree boundary

Theorem 8.1. *For every prime $p > 3$,*

$$C_p(t) + C_{p+1}(t)G_p(t) \equiv 0 \pmod{p^2} \quad \textit{in } \mathbb{Z}_p[t]. \tag{43}$$

If $t_0 \in \mathbb{Z}_p$ and α is an exact unit root in $\mathbb{Z}_p$ of $\mathcal{T}_p(X, t_0)$, then

$$G_p(t_0) \equiv \alpha \pmod{p^2}. \tag{44}$$

Proof. The formal unit $\mathcal{Q} = \Theta(q)/\Theta(q^p)$ is a root of (40). Work in $\mathbb{Z}_p[[t]]$ using the integral inverse $q = q(t)$. Reducing by (41) and dividing by $\mathcal{Q}^p$ gives

$$C_p + C_{p+1}\mathcal{Q} \equiv 0 \pmod{p^2}.$$

Write $C_{p+1} = 1 + pE$, with $E \in \mathbb{Z}[t]$. Then

$$\mathcal{Q} \equiv -(1 - pE)C_p \pmod{p^2}, \qquad \deg((1 - pE)C_p) \le \frac{p+1}{2} + \frac{p-1}{2} = p. \tag{45}$$

The comparison polynomial can have degree p. We use the coefficient comparison from the proof of Beukers' Theorem 6.1 [2], for ratio $1/3$ modulo p^3; here the ratio is $1/2$ modulo p^2.

Set $t^\sigma = t(q(t)^p)$. The initial term $t(q) = q + O(q^2)$ implies $t^\sigma = t^p + O(t^{p+1})$. The exact period identity (31) gives

$$\mathcal{Q} = \frac{G(t)}{G(t^\sigma)} = G_p(t) + \left(\binom{2p}{p} Q_p + 12\right) t^p + O(t^{p+1}). \tag{46}$$

Lemma 4.1 eliminates the degree-p coefficient modulo p^2. The polynomial in (45) and G_p therefore have congruent coefficients at every degree from 0 through p. Both have degree at most p, so they are congruent as polynomials. Consequently $\mathcal{Q} \equiv G_p$ as a formal series modulo p^2, which gives (43).

Now use only polynomials. The exact equation $\mathcal{T}_p(\alpha, t_0) = 0$ and (41) imply

$$\alpha^p(C_p(t_0) + C_{p+1}(t_0)\alpha) \equiv 0 \pmod{p^2}.$$

Divide by the unit α^p and subtract (43) evaluated at t_0. Since $C_{p+1}(t_0) \equiv 1 \pmod{p}$, it is a unit and (44) follows. No infinite series is evaluated at a p-adic unit parameter, and no division by $G_p(t_0)$ is needed. □

9 Complex multiplication matrices and the split primes

Let $p > 3$ be split, and write $p = x^2 + 2y^2$ with $x, y > 0$. Then x is odd, $\gcd(x, y) = 1$, and exactly one of x, y is divisible by 3. Indeed, if both were nonzero modulo 3, then $p \equiv 1 + 2 = 0 \pmod{3}$, and if both vanished then $9 \mid p$. Keep $\delta = \sqrt{-2}$ and the points (36).

9.1 The point γ

The integer $x + 2y$ is coprime to $6y$: it is odd, is coprime to y, and is nonzero modulo 3. Choose $A, B \in \mathbb{Z}$ satisfying $A(x + 2y) + 6By = 1$, and put

$$M_\gamma = \begin{pmatrix} A & B \\ -6y & x + 2y \end{pmatrix} \in \Gamma_0(6), \qquad k = B(x - 2y) - Ay. \tag{47}$$

The denominator of $M_\gamma\gamma$ is $x - y\delta$. Rationalization gives

$$M_\gamma\gamma = \frac{\gamma + k}{p}. \tag{48}$$

To check both coordinates, the coefficient of δ in the rationalized numerator is $\{A(x + 2y) + 6By\}/6 = 1/6$. The real part is $A(x - y)/3 + Bx = 1/3 + k$, by the same Bézout identity.

The weight-two law has trivial character on the base group, so

$$\alpha_\gamma = p^2 \frac{\Theta(\gamma)}{\Theta(M_\gamma\gamma)} = \frac{p^2}{(x - y\delta)^2} = (x + y\delta)^2 \tag{49}$$

is an exact root of $\mathcal{T}_p(X, -1/32)$. It comes from the factor indexed by $k \bmod p$ in (40); reduction of k is valid since $\Theta(\tau + 1) = \Theta(\tau)$.

9.2 The point β when $3 \mid y$

Choose $A, B \in \mathbb{Z}$ satisfying $Ax + 2By = 1$, and define

$$M_\beta = \begin{pmatrix} A & B \\ -2y & x \end{pmatrix} \in \Gamma_0(6), \qquad k = Bx - Ay. \tag{50}$$

The denominator is $x - y\delta$, and rationalization gives $M_\beta\beta = (\beta + k)/p$. For clarity, its real numerator is $Bx - Ay = k$, and its δ coefficient is $Ax/2 + By = 1/2$. Thus

$$\alpha_\beta = p^2 \frac{\Theta(\beta)}{\Theta(M_\beta\beta)} = (x + y\delta)^2 \tag{51}$$

is an exact root of $\mathcal{T}_p(X, 1/64)$.

9.3 The point β when $3 \mid x$

Choose $A, B \in \mathbb{Z}$ satisfying $2Ay + Bx = 1$, and define

$$M_\beta = \begin{pmatrix} 2A & B \\ -2x & 2y \end{pmatrix}, \qquad \det M_\beta = 2, \qquad k = By - Ax. \tag{52}$$

One has

$$M_\beta W_2^{-1} = \begin{pmatrix} -2A - 3B & A + B \\ 2x - 6y & -x + 2y \end{pmatrix} \in \Gamma_0(6),$$

where the lower-left entry is divisible by 6 because $3 \mid x$. Therefore $\chi(M_\beta) = -1$. The denominator is $2y - x\delta$, of norm $2p$. Rationalizing $(A\delta + B)/(2y - x\delta)$ gives real part $By - Ax = k$ and δ coefficient $(2Ay + Bx)/2 = 1/2$ after division by p. Hence again $M_\beta\beta = (\beta + k)/p$.

The transformation convention (32) gives

$$\Theta(M\tau) = \frac{\chi(M)}{\det M}(c\tau + d)^2\Theta(\tau).$$

In this case it yields the exact root

$$\alpha_\beta = p^2 \frac{\Theta(\beta)}{\Theta(M_\beta\beta)} = -\frac{2p^2}{(2y - x\delta)^2} = (x - y\delta)^2 \tag{53}$$

of $\mathcal{T}_p(X, 1/64)$. The last equality uses $2y - x\delta = -\delta(x + y\delta)$ and $\delta^2 = -2$. Both the negative character and the determinant factor are part of this computation.

9.4 Separate embeddings and the rational trace

Each root in (49), (51) and (53) has been constructed exactly in $\mathbb{Q}(\delta)$. Its polynomial equation has rational coefficients, so it remains valid under either embedding into $\mathbb{Q}_p$. Since $\left(\frac{-2}{p}\right) = 1$, there are two such embeddings. The two factors $x + y\delta$ and $x - y\delta$ have product p; they cannot both be divisible by p, since their sum is $2x$ and $p \nmid x$. Thus one is a unit and the other has valuation one. Choose the embedding in which the factor occurring in the required root is a unit. Its conjugate square is zero modulo p^2, and

$$(x + y\delta)^2 + (x - y\delta)^2 = 4x^2 - 2p \tag{54}$$

shows that the unit root is congruent to $4x^2 - 2p \pmod{p^2}$.

When $3 \mid x$, the roots constructed at γ and β are conjugates. They are not both units in a single embedding. For $G_p(-1/32)$ choose the embedding making (49) a unit; for $G_p(1/64)$

choose the other embedding making (53) a unit. The sums are rational p-integral numbers, and both embeddings give the same rational trace in (54). Theorem 8.1, applied separately to the two polynomial equations, proves

$$G_p(-1/32) \equiv G_p(1/64) \equiv 4x^2 - 2p \pmod{p^2} \qquad (p > 3,\ p \equiv 1, 3 \pmod 8).$$

Unit roots have therefore been obtained from the matrices and the norm before applying the congruence for the finite sums.

9.5 The prime three and completion of the proof

For $p = 3$, the definitions give $Q_0 = 1, Q_1 = -6, Q_2 = 42$. Both sums have addends $1, 6, 0$ modulo 9, and hence both equal 7 (mod 9). This is $4 - 2 \cdot 3$ for $3 = 1^2 + 2 \cdot 1^2$. As an additional direct check at five, the original addends are

sum	addends modulo 25	total
$G_5(-1/32)$	$1, 16, 23, 5, 5$	0
$G_5(1/64)$	$1, 17, 12, 15, 5$	0

Section 3 proved the inert case for every $p > 3$, and the preceding matrix argument proved the split case for $p > 3$. The direct evaluation at three completes Theorem 1.1.

10 Further consequences and the precision of the result

10.1 The squarefree part of a finite period

Proposition 10.1. *Under Proposition 2.2, suppose D mod p is separable. There are $S, V \in \mathbb{F}_p[t]$ such that*

$$\overline{U} = SV^2, \qquad S(0) = V(0) = 1, \qquad S \mid D, \qquad \gcd(S, V) = 1,$$

where S is squarefree. All ordinary zeros of $\overline{U}$ are double, and all its zeros on D are simple.

Proof. Lemma 2.4 determines the multiplicities over $\overline{\mathbb{F}_p}$. Zero is not a root, because $\overline{U}(0) = 1$. Let $g = \gcd(\overline{U}, \overline{U}')$ be monic in $\mathbb{F}_p[t]$. Each double root contributes exactly once to g, and a simple root contributes nothing. Thus $g(0) \neq 0$ and $V = g/g(0)$ lies in $\mathbb{F}_p[t]$ with constant term 1. The quotient $S = \overline{U}/V^2$ is a polynomial with constant term 1, whose roots are precisely the remaining simple roots. They are roots of D, so $S \mid D$. They are disjoint from the roots of V, proving the last assertions. □

For the sequence Q_n, $D = (1+32t)(1+36t)$ is separable for $p > 3$. An explicit form of S uses, in addition, Sun's classical *Theorem* 3.5 modulo p [1, p. 2739], which determines the vanishing of $G_p(-1/36)$ for $p > 5$. It is an auxiliary source input for the next corollary, not a premise of Theorem 1.1. It is distinct from Sun's *Conjecture* 3.5 modulo p^2.

Corollary 10.2. *For every prime $p > 3$, there is $V_p \in \mathbb{F}_p[t]$, $V_p(0) = 1$, such that*

$$G_p(t) \equiv (1 + 32t)^{e_2(p)}(1 + 36t)^{e_3(p)} V_p(t)^2 \pmod{p}, \tag{55}$$

where

$$e_2(p) = \frac{1 - \left(\frac{-2}{p}\right)}{2}, \qquad e_3(p) = \frac{1 - \left(\frac{-3}{p}\right)}{2}.$$

Proof. For $p > 5$, Sun's Theorem 3.7 determines whether $-1/32$ is a zero, and Theorem 3.5 determines whether $-1/36$ is a zero. In each case the inert residue is zero and the split residue is $4x^2$, nonzero modulo p, with its corresponding quadratic representation. Thus these zeros occur exactly when $\left(\frac{-2}{p}\right) = -1$ and $\left(\frac{-3}{p}\right) = -1$, respectively. Proposition 10.1 gives the factorization and its normalization at zero. For $p = 5$, (20) equals $D(t)$ modulo 5, and both characters are -1; take $V_5 = 1$. □

10.2 An exact Fourier trace and two Hecke coefficients

Proposition 10.3. *The Fourier expansion of the certified period is*

$$\Theta(q) = \sum_{n\geq 0} c_n q^n, \qquad c_0 = 1, \qquad c_n = -12 \sum_{\substack{d\mid n \\ (d,6)=1}} d \quad (n \geq 1). \tag{56}$$

For every prime $p > 3$,

$$p\Theta(q^p) + \frac{1}{p}\sum_{k=0}^{p-1} \Theta(\zeta_p^k q^{1/p}) = (p+1)\Theta(q). \tag{57}$$

For the polynomial normalization in (40)*,*

$$C_0 = p^{2p}, \qquad C_1 = -p^{2p-1}(p+1). \tag{58}$$

Proof. Logarithmic differentiation of the eta product R in (28) gives

$$c_n = -12\big(\sigma_1(n) - 2\sigma_1(n/2) - 3\sigma_1(n/3) + 6\sigma_1(n/6)\big),$$

with σ_1 set to zero on nonintegral arguments. Writing $n = 2^a 3^b m$, $(m, 6) = 1$, and using $\sigma_1(2^a) - 2\sigma_1(2^{a-1}) = 1$ and the analogous identity for 3, the bracket equals $\sigma_1(m)$. This proves (56) for every coefficient.

The root-of-unity filter makes the coefficient of q^n on the left of (57) equal to $pc_{n/p} + c_{pn}$, with $c_{n/p} = 0$ for $p \nmid n$. For $n > 0$, the geometric sum in the p-part of the divisor sum gives $pc_{n/p} + c_{pn} = (p+1)c_n$. For $n = 0$, both sides are $p + 1$. Finally, the product defining $\mathcal{T}_p$ gives $C_0 = p^{2p}$ and

$$C_1 = -p^{2p-2}\frac{p^2\Theta(q^p) + \sum_k \Theta(\zeta_p^k q^{1/p})}{\Theta(q)}.$$

The trace identity evaluates this as the constant in (58). □

This trace gives a second method of generating the period coefficients and checks the normalization of the Hecke product. The degree bound and the finite specialization still require the arguments of Sections 7 and 8.

10.3 The modulus cannot be raised uniformly to a cube

The corresponding equality and inert vanishing modulo p^3 fail already at $p = 7$. Direct calculation from (1) gives

$$G_7(-1/32) \equiv 294, \qquad G_7(1/64) \equiv 49 \pmod{343}. \tag{59}$$

Both are zero modulo 49, as Theorem 1.1 asserts; neither is zero modulo 343, and the two residues are distinct. This example fixes the scope of the stated supercongruence.

A Finite certificates for the modular identities

The certificate in Lemma 5.2 is an exact coefficient calculation coupled with the holomorphic valence bound. Let $\ell_J = \partial \log J$ and let A_8, B_8 denote the left sides of (29) and (30). The necessary coefficients are

n	$[q^n]h$	$[q^n]\Theta$	$[q^n]J$	$[q^n]\ell_J$	$[q^n]A_8$	$[q^n]B_8$
0	0	1	0	1	0	0
1	1	−12	1	−2	0	0
2	5	−12	−2	−10	0	0
3	19	−12	−3	−14	0	0
4	61	−12	4	−26	0	0
5	174	−72	6	−12	0	0
6	455	−12	6	−70	0	0
7	1112	−96	−16	−16	0	0
8	2573	−12	−8	−58	0	0

The weight-two comparison in Lemma 5.1 has

n	$[q^n]\Theta$	$[q^n](-\partial \log R)$	$[q^n](\Theta + \partial \log R)$
0	1	1	0
1	−12	−12	0
2	−12	−12	0

These tables can be recomputed entirely from the eta products. For an exponent vector (r_d) write

$$\prod_{d|6} \eta_d^{r_d} = q^{\sum dr_d/24} \prod_{d|6} \prod_{m\geq 1} (1-q^{dm})^{r_d}. \tag{60}$$

After accounting for the initial shift, only factors with $dm \leq K$ can affect coefficients through degree K. Expand each factor by the integral binomial series and multiply with truncation after every product. This is a finite exact algorithm.

Alternatively, put $A(q) = \prod_{d|6} \prod_{m\geq 1} (1-q^{dm})^{r_d}$, $A(0) = 1$. Its logarithmic derivative is

$$\frac{\partial A}{A} = \sum_{n\geq 1} \ell_n q^n, \qquad \ell_n = -\sum_{\substack{d|6 \\ d|n}} r_d d\, \sigma_1(n/d),$$

so its coefficients obey the exact recursion

$$nA_n = \sum_{j=1}^{n} \ell_j A_{n-j}. \tag{61}$$

For the logarithmic derivative required at degree eight, use directly

$$\ell_J = 1 - 2 \sum_{n\geq 1} \left(\sum_{\substack{d|6 \\ d|n}} d\, \sigma_1(n/d) \right) q^n. \tag{62}$$

In particular, the coefficient of degree eight of ℓ_J is not inferred from the displayed prefix of J alone. Ordinary sums, products and the rule $\partial q^n = nq^n$ now reproduce all residual entries. The table supplies the complete eighteen coefficients needed at weight eight, while the three weight-two coefficients suffice at its smaller bound.

B Exact eta phases at the two finite cusps

We derive the signs in (25) from the Dedekind eta law [8, 23.18.5–23.18.7]. For $c = 2, 3$, let $\sigma_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$. For $d = 1, 2, 3, 6$, put $g = \gcd(c, d)$, $a = d/g$, $c' = c/g$, and choose $e, b \in \mathbb{Z}$ with

$ae - bc' = 1$. The exact matrix decomposition is

$$\begin{pmatrix} d & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c' & e \end{pmatrix} \begin{pmatrix} g & -b \\ 0 & a \end{pmatrix}. \tag{63}$$

Let $s(u, v)$ be the Dedekind sum

$$s(u,v) = \sum_{j=1}^{v-1} \left(\frac{j}{v} - \frac{1}{2}\right)\left(\left\{\frac{uj}{v}\right\} - \frac{1}{2}\right) \quad (\gcd(u,v) = 1,\ v > 0),$$

where the empty sum for $v = 1$ is zero. All summands here have nonintegral uj/v. Along $\tau = iY$, $Y \to +\infty$, the eta law and its leading term give

$$\eta(d\sigma_c\tau) \sim \sqrt{\frac{g}{d}}\sqrt{-i(c\tau+1)}\, e^{\pi i \lambda_{c,d}} q^{g^2/(24d)}, \qquad \lambda_{c,d} = \frac{a+e}{12c'} + s(-e,c') - \frac{b}{12a}. \tag{64}$$

The roots are principal. The scale g/d is positive, and $-i(c\tau + 1)$ has positive real part along the stated path, so the factorization introduces no extra sign.

For h the exponents are $(r_1, r_2, r_3, r_6) = (-5, 1, -1, 5)$. The common square-root factor cancels because $\sum r_d = 0$, and the q exponent cancels because both cusp orders are zero. The following choices give all eight phases explicitly:

c	d	g	a	c'	e	b	$\lambda_{c,d}$
2	1	1	1	2	1	0	1/12
2	2	2	1	1	1	0	1/6
2	3	1	3	2	1	1	5/36
2	6	2	3	1	1	2	5/18
3	1	1	1	3	1	0	0
3	2	1	2	3	2	1	1/8
3	3	3	1	1	1	0	1/6
3	6	3	2	1	1	1	5/24

Consequently

c	$\sum_{d\mid 6} r_d \lambda_{c,d}$	$\prod_{d\mid 6} (\gcd(c,d)/d)^{r_d/2}$
2	1	1/9
3	1	1/8

In each case the total phase is $e^{\pi i} = -1$. Therefore $h(1/2) = -1/9$ and $h(1/3) = -1/8$, including their signs.

C Companion computations

The companion software, version 0.1.1, implements the original binomial definitions, finite invariants, local lift checks, eta products and modular residual calculations, and exact Hecke polynomial reconstruction. It also provides bounded regression checks of the sums and the complex multiplication matrices. Companion repository:

`https://github.com/aconsciousfractal/Sun-3-6-Supercongruence`

The repository README and `REPRODUCE.md` give the verification and build instructions. The coefficient algorithms in Appendix A and the exact phase tables in Appendix B specify the finite certificates used in the proof. Tests over bounded sets of primes serve as regression checks; the all-prime conclusion follows from the arguments above. The evidence inventory is `EVIDENCE_SHA256.txt`; its SHA-256 is

`72ee87724109900a536869bf5f5d61f8ccdaedf5c0f91ca2f0e1a014351d6c51`

The inventory identifies companion code, tests, configuration and exact evidence, excluding the manuscript and prose that quote the digest.

Acknowledgment. The author thanks Zhi-Hong Sun for helpful comments on the manuscript, including suggestions to simplify the notation and the reference to Mao's stronger coefficient congruence.

AI assistance and responsibility. AI assistance under the author's direction was used for mathematical exploration, proof criticism, source comparison, manuscript drafting, exact computation and repository preparation. OpenAI Codex and GPT-6.1 Sol assisted with consolidation and separate checks of the proof and companion. Research supplied through an external agent was also examined; its complete model provenance is not asserted. The systems had access to related arguments. Their checks are not independent human peer review, formal proof verification or a determination of priority. Individual proof steps are not attributed to particular systems. The author retains responsibility for the manuscript, attributions and decision to publish.

References

[1] Zhi-Hong Sun, *Supercongruences involving Apéry-like numbers and binomial coefficients*, AIMS Mathematics **7**(2) (2022), 2729–2781. doi:10.3934/math.2022153. Definitions and recurrence, pp. 2729–2730; Theorems 3.5 and 3.7, pp. 2739–2740; Conjecture 3.6, p. 2742.

[2] Frits Beukers, *Supercongruences using modular forms*, arXiv:2403.03301v3, 16 June 2025. `https://arxiv.org/abs/2403.03301v3`. Section 3, pp. 16–18, especially Lemma 3.7; Section 5, pp. 20–22; Theorem 6.1, p. 24; Section 8.10, p. 28.

[3] Guo-Shuai Mao, *Congruences involving Franel numbers and Apéry-like numbers*, preprint, 2023, ResearchGate. doi:10.13140/RG.2.2.23378.73922. Theorem 1.4, p. 3, in the author-uploaded text of 8 January 2025.

[4] Armin Straub, *Gessel–Lucas congruences for sporadic sequences*, arXiv:2301.12248v1, 28 January 2023. `https://arxiv.org/abs/2301.12248v1`. Equation (10) and Theorem 3.2, p. 5; proof, pp. 6–7. The positive sequence is $A_F(n) = (-1)^n Q_n$. Journal publication: Monatshefte für Mathematik **203** (2024), 883–898, doi:10.1007/s00605-023-01894-3. The proof locators refer to the specified arXiv version.

[5] Ofir Gorodetsky, *New representations for all sporadic Apéry-like sequences, with applications to congruences*, arXiv:2102.11839v2, 5 January 2025. `https://arxiv.org/abs/2102.11839v2`. Proposition 1.2, equation (1.8), p. 4; Proposition 3.3 and row F, p. 10; multinomial derivation, p. 12. Journal publication: Experimental Mathematics **32**(4) (2023), 641–656, doi:10.1080/10586458.2021.1982080. The locators above refer to the specified arXiv version.

[6] Jeremy Rouse and John J. Webb, *On spaces of modular forms spanned by eta-quotients*, arXiv:1311.1460v3, 14 November 2014. `https://arxiv.org/abs/1311.1460v3`. Eta-quotient criterion and cusp-order formula, p. 2. Journal publication: Advances in Mathematics **272** (2015), 200–224. doi:10.1016/j.aim.2014.12.002.

[7] William Craig, *New Types of Sturm bounds via p-adic transfer methods*, arXiv:2602.10240v1, 10 February 2026. `https://arxiv.org/abs/2602.10240v1`. Only the classical holomorphic-form bound in Theorem 1.1(1), p. 2, is used.

[8] NIST Digital Library of Mathematical Functions, Section 23.18, *Modular Transformations*, equations 23.18.5–23.18.7. `https://dlmf.nist.gov/23.18`.

[9] Heng Huat Chan and Shaun Cooper, *Rational analogues of Ramanujan's series for* $1/\pi$, Mathematical Proceedings of the Cambridge Philosophical Society **153**(2) (2012), 361–383. doi:10.1017/S0305004112000254. The level-6 parametrization is cited for comparison; it is not needed for the direct period certification.