Sun's supercongruence for two Apéry-like binomial sums at discriminant −20

Oleksiy Babanskyy

Abstract

Let $a_n = \sum_{j=0}^{n} \binom{n}{j}^2 \binom{2j}{j}$ and let $Q_n = \sum_{j=0}^{n} \binom{n}{j}(-8)^{n-j} \sum_{k=0}^{j} \binom{j}{k}^3$. We prove Sun's Conjecture 3.7: for every prime $p \neq 2, 5$, the two sums $(-1)^{(p-1)/2} \sum_{n<p} \binom{2n}{n} a_n 20^{-n}$ and $(-1)^{(p-1)/2} \sum_{n<p} \binom{2n}{n} Q_n (-16)^{-n}$ are congruent modulo p^2 to $4x^2 - 2p$ if $p = x^2 + 5y^2$, to $2x^2 - 2p$ if $2p = x^2 + 5y^2$, and to zero if $(-5/p) = -1$. For split primes, two modular periods at one complex multiplication point yield separate finite specializations of an integral Hecke polynomial. Its degree-p endpoint and the sign in the nonprincipal class are treated explicitly. For inert primes, a degree-five endomorphism with square $[-5]$ forces a Hasse polynomial to vanish; a finite quadratic differential invariant then lifts each original sum from modulo p to modulo p^2. Fixed algebraic certificates and their uniform specialization are included.

hexagon:2611.00551v1

1 The supercongruence and its two proof branches

For $n \geq 0$ define the Franel numbers and two Apéry-like sequences by

$$\begin{aligned} f_n &= \sum_{j=0}^{n} \binom{n}{j}^3, \qquad a_n = \sum_{j=0}^{n} \binom{n}{j}^2 \binom{2j}{j}, \\ Q_n &= \sum_{j=0}^{n} \binom{n}{j} (-8)^{n-j} f_j. \end{aligned} \tag{1}$$

Write

$$G_a(t) = \sum_{n \geq 0} \binom{2n}{n} a_n t^n, \qquad G_Q(t) = \sum_{n \geq 0} \binom{2n}{n} Q_n t^n. \tag{2}$$

Their truncations at degrees $0, \ldots, p-1$ are denoted by $G_{a,p}(t)$ and $G_{Q,p}(t)$. This convention for the subscript p will also be used for a generic series G. All congruences of p-integral rational numbers are interpreted in $\mathbb{Z}_p$.

Theorem 1.1. *For every prime $p \neq 2, 5$,*

$$\begin{aligned} (-1)^{(p-1)/2} G_{a,p}(1/20) &\equiv (-1)^{(p-1)/2} G_{Q,p}(-1/16) \\ &\equiv \begin{cases} 4x^2 - 2p, & p = x^2 + 5y^2, \quad p \equiv 1, 9 \pmod{20}, \\ 2x^2 - 2p, & 2p = x^2 + 5y^2, \quad p \equiv 3, 7 \pmod{20}, \\ 0, & p \equiv 11, 13, 17, 19 \pmod{20} \end{cases} \pmod{p^2}. \end{aligned} \tag{3}$$

This is Conjecture 3.7 of Zhi-Hong Sun [1, p. 2742]. The existence of the representations in the two split cases is proved in Lemma 6.2. The signs of x, y do not affect the displayed values.

The two sums are evaluated separately. For split primes we identify G_a, G_Q as modular periods, derive a finite polynomial congruence, and evaluate it at a common point of discriminant -20. Both ideal classes occur, giving matrices of determinant one and two. For inert primes we first reduce the sums modulo p to a square of a Legendre polynomial. An explicit endomorphism

of an elliptic curve forces that polynomial to vanish, and a differential invariant lifts the vanishing of each sum modulo p^2. Thus the equality of the two sums follows from their evaluations; it is not used as a bridge in either argument. The prime 3 is computed directly at the end of Section 8.

The finite invariant and integral Hecke specialization follow the organization of the author's treatments of Sun's Conjectures 3.5 and 3.6 [4, 5]. Their needed forms are established here; the two previous supercongruences are not assumptions of the proof.

The modular orbit argument uses Beukers's Lemma 3.7 [6]. The degree-p endpoint follows the coefficient comparison in the proof of his Theorem 6.1, whose stronger congruence has different hypotheses; the modulo-p^2 statement required here is proved in Theorem 5.3. The modulo-p Legendre and Franel antecedents are identified in Section 7; the classical Legendre square identity is derived here from its symmetric-square equation. The endomorphism is certified by polynomial identities before reduction. The appendices give exact arithmetic inputs and the bounds which make those finite computations sufficient.

2 A finite differential invariant and lifting

The three integral sequences a_n, Q_n, f_n satisfy [1, pp. 2729–2730]

$$(n+1)^2 u_{n+1} = (\alpha n(n+1) + \beta)u_n - \gamma n^2 u_{n-1}, \qquad u_0 = 1, \quad u_1 = \beta, \tag{4}$$

with parameters

u_n	α	β	γ
a_n	10	3	9
Q_n	−17	−6	72
f_n	7	2	−8

(5)

For any such sequence put $v_n = \binom{2n}{n} u_n$, $V(t) = \sum_{n\geq 0} v_n t^n$, $U(t) = V_p(t)$, and $\theta = t\, d/dt$. The central binomial factor converts (4) into $LV = 0$, where

$$L = \theta^3 - 2t(2\theta+1)(\alpha\theta^2 + \alpha\theta + \beta) + 4\gamma t^2(\theta+1)(2\theta+1)(2\theta+3). \tag{6}$$

Lemma 2.1. *Let $p > 3$ be prime, let $\alpha, \beta, \gamma \in \mathbb{Z}$, and let u_n be an integral sequence satisfying* (4)*. Define*

$$\begin{aligned} D(t) &= 1 - 4\alpha t + 16\gamma t^2, \\ I(Y) &= D\{2Y\theta^2 Y - (\theta Y)^2\} + (\theta D)Y\theta Y + 4t(-\beta + 3\gamma t)Y^2. \end{aligned} \tag{7}$$

Then $I(U) \equiv 0 \pmod{p^2}$ as a polynomial identity.

Proof. Leibniz's rule gives the universal identity

$$\theta I(Y) = 2YLY. \tag{8}$$

In characteristic zero this implies $I(V) = 0$, since its constant term is zero. The residual of the truncation is exactly

$$LU = -p^3 v_p t^p + 4\gamma p(2p-1)(2p+1)v_{p-1}t^{p+1}. \tag{9}$$

The factor $\binom{2p-2}{p-1}$ shows that $p \mid v_{p-1}$. Consequently $LU \equiv 0$ and $\theta I(U) \equiv 0 \pmod{p^2}$.

The latter congruence alone does not determine coefficients at degrees divisible by p. We have $\deg I(U) \leq 2p$ and constant term zero. Every coefficient at a degree not divisible by p is zero modulo p^2, because that degree is a unit in $\mathbb{Z}_p$. The two remaining coefficients, calculated before reduction, are

$$[t^p]I(U) = -2p^2 v_p, \qquad [t^{2p}]I(U) = 4\gamma(2p-1)(2p+1)v_{p-1}^2. \tag{10}$$

For the first equality compare with $I(V) = 0$: the first omitted term $v_p t^p$ contributes $2p^2 v_p$ at degree p. The second equality comes from the highest-degree term of U. Both are divisible by p^2, completing the coefficientwise proof. □

Lemma 2.2. *Under the hypotheses of Lemma 2.1, let $t_0 \in \mathbb{Z}_p$ with $t_0 D(t_0) \in \mathbb{Z}_p^\times$. If $U(t_0) \equiv 0 \pmod p$, then $U(t_0) \equiv 0 \pmod{p^2}$.*

Proof. Evaluate the invariant modulo p. It gives $\theta U(t_0) = 0$, so the reduction of U has a root of multiplicity at least two at the reduction of t_0. The multiplicity is exactly two. Indeed, $U(0) = 1$ and $\deg U < p$, so a higher multiplicity would satisfy $3 \le m < p$. The coefficient of the ordinary third derivative in L is $t^3 D(t)$. In the local expansion of LU at t_0, the term of degree $m-3$ then has nonzero coefficient proportional to

$$t_0^3 D(t_0) m(m-1)(m-2).$$

The lower derivatives cannot cancel it, contradicting (9) modulo p. Therefore $\theta^2 U(t_0)$ is a unit. In $I(U)(t_0)$ modulo p^2, the terms quadratic in $U(t_0)$ and $\theta U(t_0)$ vanish, leaving

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

Its coefficient of $U(t_0)$ is a unit, proving the assertion. □

For the three parameters used below,

$$D_a(1/20) = -\frac{16}{25}, \qquad D_Q(-1/16) = \frac{5}{4}, \qquad D_f(1/16) = -\frac{5}{4}. \tag{11}$$

All are units when $p > 5$. Here an ordinary point means a nonsingular point of the differential equation; it does not assert that an associated elliptic curve is ordinary.

3 Modular data and the two periods

3.1 Eta quotients and cusp divisors

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

$$\begin{aligned} h &= \frac{\eta_2 \eta_6^5}{\eta_1^5 \eta_3}, & z &= \frac{\eta_1^6 \eta_6}{\eta_2^3 \eta_3^2}, & J &= (\eta_1\eta_2\eta_3\eta_6)^2, \\ U_\eta &= z^2, & B_\eta &= h z^2, & V_\eta &= h^2 z^2, \\ R &= \frac{\eta_2^{12}\eta_3^{12}}{\eta_1^{12}\eta_6^{12}}, & v &= \frac{\eta_2^{24}}{\eta_1^{24}}, & S &= \left(\frac{\eta_2\eta_6}{\eta_1\eta_3}\right)^6. \end{aligned} \tag{12}$$

For the eta-quotient criteria and cusp-order formula we use [8, p. 2]. For the quotients listed in the following table (which uses z^2, not z), the exponent sums $\sum d r_d$ and $\sum (6/d) r_d$ are multiples of 24; the weights are even and $\prod d^{r_d}$ is a rational square. The character on $\Gamma_0(6)$ is therefore trivial. At the cusps $0, 1/2, 1/3, \infty$ the orders are as follows:

	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	$(-1,1,1,-1)$
v	-24	24	0	0	0	$(-3,3,-1,1)$
U_η	12	-6	-4	2	2	$(2,0,0,0)$
B_η	7	-5	-5	7	2	$(1,0,0,1)$
V_η	2	-4	-6	12	2	$(0,0,0,2)$
J	2	2	2	2	4	$(1,1,1,1)$
S	-6	6	-6	6	0	$(-1,1,-1,1)$

The eta function has no zeros in the upper half-plane. Since h has one simple pole on the compact curve $X_0(6)$, it is a global coordinate of degree one on that curve.

Lemma 3.1. *The following identities hold:*

$$R = h^{-1} + 17 + 72h = \frac{(1+8h)(1+9h)}{h}, \tag{13}$$

$$v(1+8h) = h(1+9h)^3, \qquad S = \frac{h(1+9h)}{1+8h}, \tag{14}$$

$$\Theta_a := U_\eta + 18B_\eta + 72V_\eta = \partial \log S, \tag{15}$$

$$\Theta_Q := U_\eta - 72V_\eta = -\partial \log R. \tag{16}$$

The forms Θ_a, Θ_Q are nonzero at every cusp.

Proof. The only poles of R are simple and lie at $h = 0, \infty$, so $R = a/h + b + ch$. The exact expansions

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

give $a = 1, b = 17, c = 72$.

The function $v(1+8h) - h(1+9h)^3$ has a pole of order at most four at the cusp 0, a pole of order at most one at $1/3$, and no other poles. Its coefficients through q^5 vanish by the finite expansion in Appendix A, so its zero at infinity has order at least six. Equality of the total orders of zeros and poles for a nonzero meromorphic function on a compact curve proves the first identity in (14).

By (13), the remaining two cusps have h-values $-1/8, -1/9$. At $1/3$ the pole of v forces $1 + 8h = 0$ in the preceding identity; hence $h(1/3) = -1/8$ and $h(1/2) = -1/9$. The rational function asserted for S has the same divisor as S and the same initial term q. Their ratio is therefore one.

Logarithmic derivatives of modular units are modular forms of weight two. They have no interior poles. At a cusp of width w, write the local expansion as $Q^r(c_0 + O(Q))$, with $c_0 \neq 0$. The transformed logarithmic derivative has constant term r/w. Here $r = \pm 1$ for both R, S, so this constant is nonzero. The differences in (15) and (16) belong to $M_2(\Gamma_0(6))$, and their coefficients q^0, q^1, q^2 vanish. The index of $\Gamma_0(6)$ in $\mathrm{SL}_2(\mathbb{Z})$ is 12; the valence bound is 2. Thus both differences vanish identically. □

3.2 Identities of weight eight

Lemma 3.2. *Take either $\Theta = \Theta_a$ and $(\alpha, \beta, \gamma) = (10, 3, 9)$, or $\Theta = \Theta_Q$ and $(\alpha, \beta, \gamma) = (-17, -6, 72)$. Set $W = \Theta\partial \log J - 2\partial\Theta$. Then*

$$W^2 - \Theta^4 + 4\alpha J\Theta^2 - 16\gamma J^2 = 0, \tag{17}$$

$$2\Theta\partial^2\Theta - 3(\partial\Theta)^2 - 4\beta J\Theta^2 + 12\gamma J^2 = 0. \tag{18}$$

Proof. We first show that the residuals are holomorphic modular forms of weight eight. For $M \in \Gamma_0(6)$, put $j = c\tau + d$ and $s_0 = c/(2\pi i)$. The chain rule gives

$$\begin{aligned}(\partial\Theta)(M\tau) &= j^4\partial\Theta + 2s_0 j^3\Theta,\\ (\partial^2\Theta)(M\tau) &= j^6\partial^2\Theta + 6s_0 j^5\partial\Theta + 6s_0^2 j^4\Theta,\\ (\partial \log J)(M\tau) &= j^2\partial \log J + 4s_0 j.\end{aligned}$$

The anomalous terms cancel: W has weight four, and $2\Theta\partial^2\Theta - 3(\partial\Theta)^2$ has weight eight. For a cusp representative σ, let $F_\sigma = \Theta|_2\sigma$ and $H_\sigma = J|_4\sigma$. The same cancellation gives

$$W|_4\sigma = F_\sigma \partial \log H_\sigma - 2\partial F_\sigma.$$

The transformed second expression is $2F_\sigma\partial^2 F_\sigma - 3(\partial F_\sigma)^2$. The series F_σ is holomorphic and $H_\sigma = Q^r$ times a unit, so $\partial \log H_\sigma$ is regular. Derivatives preserve nonnegative powers of the

local parameter. Thus the residuals are holomorphic at all cusps. There are no interior poles, because J does not vanish there.

For each of the four residuals the exact coefficients of $q^0, \dots, q^8$ are zero; Appendix A specifies the arithmetic calculation. The classical valence bound [10, Theorem 1.1(1)] is $8 \cdot 12/12 = 8$. Order at least nine therefore proves the identities. □

Proposition 3.3. *Define*

$$P(h) = h(1+8h)(1+9h), \quad C(h) = 1 + 18h + 72h^2, \quad K(h) = 1 - 72h^2.$$

The parameters and modular periods are

$$t_a = \frac{J}{\Theta_a^2} = \frac{P(h)}{C(h)^2}, \qquad t_Q = \frac{J}{\Theta_Q^2} = \frac{P(h)}{K(h)^2}, \tag{19}$$

$$G_a(t_a(q)) = \Theta_a(q), \qquad G_Q(t_Q(q)) = \Theta_Q(q). \tag{20}$$

Both parameters lie in $q + q^2\mathbb{Z}[[q]]$, and $t_Q = t_a/(1 - 36t_a)$.

Proof. Comparison of eta exponents gives $J = h^2Rz^4$, and (13) then yields the rational formulas. All series are integral, the constant terms of Θ_a, Θ_Q are one, and $J = q + O(q^2)$. The identity $C^2 - K^2 = 36P$ gives the relation between the parameters.

For either row put $e = \partial \log t = W/\Theta$, a formal unit. Equation (17) gives $e^2 = D(t)\Theta^2$. Substitute $\partial = e\theta$ into (18), using

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

It becomes $I(\Theta) = 0$. These divisions take place among formal units. By (8), $L\Theta = 0$. In characteristic zero the operator L determines the coefficient of degree $n \geq 1$ from the preceding ones by division by n^3. It consequently has a unique formal solution with constant term one. By (4), G_a, G_Q are those solutions. □

The rational relation between t_a and t_Q describes the parameters. No transformation of their truncations modulo p^2 is inferred from it.

4 Characters and pole orders

Use the determinant-normalized slash operator

$$(Y|_2M)(\tau) = \det(M)(c\tau + d)^{-2}Y(M\tau), \qquad W_2 = \begin{pmatrix} 2 & -1 \\ 6 & -2 \end{pmatrix}, \quad W_6 = \begin{pmatrix} 0 & -1 \\ 6 & 0 \end{pmatrix}.$$

Let $\Gamma = \Gamma_0(6) + \langle 2, 6\rangle$ denote the full Atkin–Lehner extension at level six; its projective quotient by $\Gamma_0(6)$ has order four [6, §3]. Scalar matrices act trivially under this slash convention.

Lemma 4.1. *The actions on h are*

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

Both t_a, t_Q are Γ-invariant. The characters of the forms, trivial on $\Gamma_0(6)$, satisfy

	W_2	W_6
Θ_a	-1	-1
Θ_Q	-1	$+1$

Proof. The matrices show that W_2 exchanges $\infty \leftrightarrow 1/3$ and $0 \leftrightarrow 1/2$, while W_6 exchanges $\infty \leftrightarrow 0$ and $1/2 \leftrightarrow 1/3$. Since h is a global coordinate, three values from $0, \infty, -1/9, -1/8$ determine each displayed action. Rational substitution gives

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

$$S(\phi_2(h))S(h) = S(\phi_6(h))S(h) = 1/64.$$

The same substitution proves invariance of both parameters. If $F(M\tau) = c_0 F(\tau)^e$, differentiation gives $(\partial \log F)|_2 M = e\partial \log F$. Apply this to (15) and (16). □

Proposition 4.2. *Each of t_a, t_Q is a Hauptmodul for Γ. On the base curve it has two double poles, and the corresponding Θ has a simple zero at each of those points and no cusp zeros. A Γ-invariant function with holomorphic numerators and at most m factors Θ^{-1} is a polynomial in t of degree at most $\lfloor m/2 \rfloor$.*

Proof. Each rational function in (19) has degree four without cancellation. Invariance and the projective index four give degree one on the quotient curve. The poles of t_a are $h = -1/6, -1/12$; those of t_Q are $h = \pm 1/\sqrt{72}$. They are double and distinct from all cusps. The corresponding forms are $C(h)z^2, K(h)z^2$, and z has no interior zeros. The factors C, K have simple zeros. The base group has no elliptic stabilizers: an order-two stabilizer is impossible modulo 3, and an order-three stabilizer is impossible modulo 2. Thus these are ordinary local coordinates on the base curve. Cusp nonvanishing was proved in Lemma 3.1.

On the quotient a meromorphic function whose only possible pole is at the pole of a Hauptmodul is a polynomial in that Hauptmodul. On the base cover its pole order is at most m, while a polynomial of degree d in t has pole order $2d$. Hence $2d \le m$. This calculation is on the base cover and requires no assignment of integral orders at orbifold points of the quotient. □

5 The integral Hecke polynomial and finite specialization

Lemma 5.1. *For every prime $p > 3$,*

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

The congruence $Q_p \equiv Q_1 = -6 \pmod{p^2}$ is known: it is the $n = 1$ consequence, after reduction modulo p^2, of Mao's stronger congruence for Q_{np} modulo p^3 [9, Theorem 1.4]. We give the alternative deduction from Straub below to make the sequence convention explicit.

Proof. We have

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

since $\sum_{k=1}^{p-1} k^{-1} \equiv 0 \pmod{p}$. Each interior term in a_p contains $\binom{p}{k}^2$, so $a_p \equiv 1 + \binom{2p}{p} \equiv 3 \pmod{p^2}$.

For Q_p the interior terms have only one factor $\binom{p}{k}$ and cannot be discarded. Straub's sequence [7, (10), Theorem 3.2] is

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

His theorem gives $A_F(p^r n) \equiv A_F(p^{r-1} n) \pmod{p^{2r}}$ for primes $p \ge 3$ and $n, r \ge 1$. Taking $n = r = 1$ gives $Q_p \equiv -6 \pmod{p^2}$. Multiplication by the central binomial coefficient proves the two assertions. This import concerns one coefficient and does not assume either sum in Theorem 1.1. □

Lemma 5.2. *For either pair (t, Θ) above and any prime $p > 3$, there is a polynomial*

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

with the exact identity

$$\begin{aligned} \mathscr{T}_p(X, t(\tau)) = {} & \left(1 - \frac{\Theta(p\tau)}{\Theta(\tau)} X\right) \\ & \cdot \prod_{k=0}^{p-1} \left(p^2 - \frac{\Theta((\tau + k)/p)}{\Theta(\tau)} X\right). \end{aligned} \tag{21}$$

Its coefficients satisfy

$$\deg C_m \le \lfloor m/2 \rfloor, \qquad \mathscr{T}_p \equiv C_p X^p + C_{p+1} X^{p+1} \pmod{p^2}, \qquad C_{p+1} \equiv 1 \pmod{p}. \tag{22}$$

Proof. Beukers's Lemma 3.7 [6, pp. 17–18] applies to weight two, a character trivial on the base group and defined on its Atkin–Lehner extension, and $p \nmid 6$. These hypotheses are supplied by Lemma 4.1. With representatives

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

the extended group permutes the ratios $(\Theta|_2 D)/\Theta$. The product in (21) is $p^{2p} \prod_D (1 - (\Theta|_2 D)/(p\Theta)X)$, so its coefficients are invariant.

The numerators are holomorphic in the interior and at cusps. For the cusp assertion, a rational matrix of positive determinant takes a rational cusp to a rational cusp. In local coordinates at the source and target it becomes triangular and replaces a local parameter by a positive power times a nonzero constant. It creates no negative powers. Since Θ does not vanish at any cusp, Proposition 4.2 gives polynomiality and the degree bound.

For integrality, form the product first in $\mathbb{Z}[\zeta_p][[s_1]]$, where $s_1 = q^{1/p}$. The denominators are units with constant term one. Invariance under $s_1 \mapsto \zeta_p s_1$ eliminates exponents not divisible by p; Galois invariance makes the remaining coefficients rational. They are algebraic integers and thus lie in $\mathbb{Z}[[q]]$. Since $t = q + q^2\mathbb{Z}[[q]]$, successive subtraction of its powers at the lowest nonzero degree shows $C_m \in \mathbb{Z}[t]$.

For $m < p$, every contribution to the coefficient of X^m contains at least one constant factor p^2. Dividing by p^2 before the integrality argument leaves the same symmetries and algebraic integrality. The quotient therefore belongs to $\mathbb{Z}[t]$. Since $p + 1$ is even,

$$C_{p+1} = \frac{\Theta(q^p) \prod_{k=0}^{p-1} \Theta(\zeta_p^k s_1)}{\Theta(q)^{p+1}}.$$

Reduce the numerator product modulo $1 - \zeta_p$: $\Theta(s_1)^p \equiv \Theta(q)$. Its coefficients are integers and $(1 - \zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = p\mathbb{Z}$. Also $\Theta(q^p) \equiv \Theta(q)^p \pmod{p}$. It follows that $C_{p+1} \equiv 1$ as a series, and by the same triangular argument as a polynomial. □

Theorem 5.3. *For every prime $p > 3$, let $G = G_a$ or G_Q and let t be its corresponding parameter. Then*

$$C_p(t) + C_{p+1}(t) G_p(t) \equiv 0 \pmod{p^2} \tag{23}$$

as a polynomial identity. If $t_0 \in \mathbb{Z}_p$ and ξ is an exact p-adic unit root of $\mathscr{T}_p(X, t_0)$, then $G_p(t_0) \equiv \xi \pmod{p^2}$.

Proof. The endpoint comparison follows the coefficient comparison in the proof of Beukers's Theorem 6.1 [6, p. 24]. His theorem has different hypotheses and proves a congruence modulo p^3. The case needed here modulo p^2, with pole-bound exponent $1/2$, is proved directly as follows.

The formal quotient $\mathcal{Q} = \Theta(q)/\Theta(q^p)$ is a unit root of (21). Dividing by $\mathcal{Q}^p$ in $\mathbb{Z}_p[[t]]$ gives $C_p + C_{p+1}\mathcal{Q} \equiv 0$. Write $C_{p+1} = 1 + pE$ with $E \in \mathbb{Z}[t]$. Then

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

The degree bound is p, so its last coefficient must be handled. The integral inverse $q = q(t)$ gives $t^\sigma = t(q(t)^p) = t^p + O(t^{p+1})$. By Proposition 3.3,

$$\mathcal{Q} = \frac{G(t)}{G(t^\sigma)} = G_p(t) + ([u^p]G(u) - [u]G(u))t^p + O(t^{p+1}).$$

Here $[u]G(u)$ is 6 for G_a and -12 for G_Q. Lemma 5.1 eliminates precisely this extra coefficient modulo p^2. All coefficients of the polynomial of degree at most p are now congruent to those of G_p. Multiplication by C_{p+1} proves (23), including every degree of its left side.

We now use only polynomials. From $\mathscr{T}_p(\xi, t_0) = 0$ and (22),

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

Divide by the unit ξ^p, subtract (23) evaluated at t_0, and divide by $C_{p+1}(t_0) \equiv 1 \pmod{p}$. This proves the specialization. No infinite series has been evaluated at a unit parameter. □

6 The common CM point and both split classes

Lemma 6.1. *Let $\delta = i\sqrt{5}$ and $\tau_0 = (1 + \delta)/6$. Then*

$$h(\tau_0) = \frac{\sqrt{5} - 2 + i(\sqrt{5} + 2)}{36}, \qquad t_a(\tau_0) = \frac{1}{20}, \qquad t_Q(\tau_0) = -\frac{1}{16}.$$

Neither Θ_a nor Θ_Q vanishes at τ_0.

Proof. We have $-1/\tau_0 = 6\tau_0 - 2$ and $-1/(2\tau_0) = 3\tau_0 - 1$. The eta transformations [11, §23.18, (23.18.5)–(23.18.7)]

$$\eta(\tau + 1) = e^{\pi i/12}\eta(\tau), \qquad \eta(-1/\tau) = \sqrt{-i\tau}\,\eta(\tau)$$

with their standard holomorphic square root give

$$\eta_6 = e^{\pi i/6}\sqrt{-i\tau_0}\,\eta_1, \qquad \eta_3 = e^{\pi i/12}\sqrt{-2i\tau_0}\,\eta_2.$$

The number $-i\tau_0$ lies in the right half-plane, so $\sqrt{-2i\tau_0} = \sqrt{2}\sqrt{-i\tau_0}$ with no extra sign. Hence

$$h(\tau_0) = e^{3\pi i/4}\frac{(-i\tau_0)^2}{\sqrt{2}} = \frac{1 - i}{2}\tau_0^2.$$

Expansion gives the displayed value of h. Substitution into (19) verifies $20P(h) = C(h)^2$, $16P(h) = -K(h)^2$, and $C(h)K(h) \neq 0$ at this point. Since z has no interior zeros, the forms are also nonzero there. □

Lemma 6.2. *For $p > 5$ with $(-5/p) = 1$, there are positive integers x, y such that either*

$$p = x^2 + 5y^2, \quad p \equiv 1, 9 \pmod{20},$$

or

$$2p = x^2 + 5y^2, \quad p \equiv 3, 7 \pmod{20}.$$

In the first case x, y have opposite parity; in the second both are odd. In both cases $\gcd(x, y) = 1$ and exactly one is divisible by 3.

Proof. Choose $r^2 \equiv -5 \pmod{p}$. The primitive positive form $[p, 2r, (r^2+5)/p]$ has discriminant -20 and represents p. Among its unimodular transforms choose a minimal leading coefficient a, then normalize $|b| \le a$. Minimality gives $a \le c$, whence $20 = 4ac - b^2 \ge 3a^2$ and $a \le 2$. The only reduced forms are $[1, 0, 5]$ and $[2, \pm 2, 3]$. In the latter case multiplication by two gives $(2u \pm v)^2 + 5v^2 = 2p$. Congruences modulo $4, 5, 8$ assign the stated residue classes and parities. Neither coordinate is zero; their signs may be chosen positive. A common square factor would divide p or $2p$; the parity conditions exclude a factor two, so the representation is primitive. Modulo three, two nonzero coordinates would give $x^2 + 5y^2 \equiv 0$, impossible for $p > 3$; two zero coordinates would give $9 \mid p$ or $9 \mid 2p$. Finally quadratic reciprocity gives $(-5/p) = 1$ precisely in the four classes $1, 3, 7, 9 \pmod{20}$. No uniqueness of the representation is needed below. □

Proposition 6.3. *Theorem 1.1 holds for every split prime $p > 5$.*

Proof. First let $p = x^2+5y^2$. The preceding parity and divisibility conditions give $\gcd(x+y, 6y) = 1$. Choose $a, b \in \mathbb{Z}$ with $a(x+y) + 6by = 1$, and set

$$M_1 = \begin{pmatrix} a & b \\ -6y & x+y \end{pmatrix} \in \Gamma_0(6), \qquad k = b(x-y) - ay.$$

The denominator at τ_0 is $x - y\delta$. Rationalizing gives

$$M_1\tau_0 = \frac{\tau_0 + k}{p}.$$

For either form its character on M_1 is one, so the transformation law exhibits the exact root

$$\xi_1 = p^2 \frac{\Theta(\tau_0)}{\Theta(M_1\tau_0)} = \frac{p^2}{(x-y\delta)^2} = (x+y\delta)^2 \tag{24}$$

of the specialized polynomial (21). Periodicity makes the representative k mod p legitimate.

Next let $2p = x^2 + 5y^2$, where x, y are odd. Here $\gcd(x+y, 3y) = 1$. Choose $a, b \in \mathbb{Z}$ with $a(x+y) + 3by = 1$, and put

$$M_2 = \begin{pmatrix} 2a & b \\ -6y & x+y \end{pmatrix}, \qquad k = \frac{b(x-y)}{2} - ay \in \mathbb{Z}.$$

Then $\det M_2 = 2$, $M_2\tau_0 = (\tau_0 + k)/p$, and

$$M_2 W_2^{-1} = \begin{pmatrix} -2a-3b & a+b \\ 3(y-x) & x-2y \end{pmatrix} \in \Gamma_0(6).$$

Both forms have character -1 on this class. In our normalization $\Theta(M\tau) = \chi(M)(c\tau + d)^2\Theta(\tau)/\det M$. Thus the exact root is

$$\xi_2 = -\frac{2p^2}{(x-y\delta)^2} = -\frac{(x+y\delta)^2}{2}. \tag{25}$$

This establishes the negative sign and the factor $1/2$ before any reduction.

These roots are algebraic identities in $\mathbb{Q}(\sqrt{-5})$. For a split prime choose its embedding in $\mathbb{Q}_p$ so that $x + y\delta$ is a unit. The two factors $x \pm y\delta$ cannot both vanish modulo p, by primitivity and $p > 5$, and their product is p or $2p$. Hence the other factor has valuation exactly one. The same embedding works for both forms, and Theorem 5.3 applies at $1/20, -1/16 \in \mathbb{Z}_p$.

In the principal case the trace of ξ_1 is $4x^2 - 2p$. In the nonprincipal case the trace of ξ_2 is $2p - 2x^2$. The nonunit conjugate root has valuation two and disappears modulo p^2, so either sum is congruent to the respective trace. Finally $(-1)^{(p-1)/2} = 1$ in the principal residue classes and $(-1)^{(p-1)/2} = -1$ in the nonprincipal classes. This proves the two signed values. □

7 Finite transport, Legendre polynomials and Hasse

The Hasse–Legendre relation below is already contained in Sun's [2, Theorem 2.1(ii) and equation (4.1)]; the latter also treats the parameter as a polynomial variable. His Theorem 4.2 gives the quartic reduction (33) at $m=-1024$. Sun also evaluates $F_{16,p}$ modulo p in the principal split classes [3, Theorem 2.10]. We retain local derivations of the identities needed here.

Lemma 7.1. *Let p be odd, $N=(p-1)/2$, and $c,t,u_0,\dots,u_{p-1}\in\mathbb{Z}_p$. Suppose $D_0=1-4ct$ is a unit, and define $b_n=\sum_{j=0}^{n}\binom{n}{j}c^{n-j}u_j$. Then*

$$\sum_{n<p}\binom{2n}{n}b_n t^n\equiv D_0^N\sum_{j<p}\binom{2j}{j}u_j(t/D_0)^j\pmod p. \tag{26}$$

Proof. For $n<p$ we have $\binom{2n}{n}\equiv(-4)^n\binom{N}{n}\pmod p$. Substitute this and reorder the finite sum. For $j\le N$, the coefficient of u_j is

$$\binom{N}{j}(-4t)^j\sum_{m=0}^{N-j}\binom{N-j}{m}(-4ct)^m=\binom{N}{j}(-4t)^jD_0^{N-j}.$$

For $j>N$ both coefficients vanish modulo p. All summands are p-integral and t/D_0 is p-integral, so the calculation gives (26). □

Sun's binomial identity [1, Lemma 3.1] is $a_n=\sum_j\binom{n}{j}f_j$. For Q_n the analogous transform is its definition. With

$$F_{16,p}=\sum_{n=0}^{p-1}\binom{2n}{n}f_n16^{-n},$$

the pairs $(c,t)=(1,1/20),(-8,-1/16)$ have $D_0=4/5,-1$. Consequently

$$G_{a,p}(1/20)\equiv\left(\frac{5}{p}\right)F_{16,p},\qquad G_{Q,p}(-1/16)\equiv(-1)^{(p-1)/2}F_{16,p}\pmod p. \tag{27}$$

These specializations also follow from [1, Theorem 3.4]. They are used only modulo p: even a modulo-p^2 vanishing of R_p does not pass through them without an additional argument.

Lemma 7.2. *For $p>5$,*

$$F_{16,p}\equiv(-1)^{(p-1)/2}R_p\pmod p,\qquad R_p=\sum_{j=0}^{p-1}\frac{(4j)!}{(j!)^4}(-1024)^{-j}. \tag{28}$$

Proof. Put $N=(p-1)/2$. Dixon's form of the Franel numbers, recorded in [1, p. 2729], is $f_n=\sum_k\binom{n}{k}^2\binom{2k}{n}$. Group the sum by k. Modulo p, all terms with $n>N$ vanish; when $n\le N$ we also have $k\le N$. Each group can be completed through $n=2k<p$, since the added terms have central binomial coefficient divisible by p. The exact identity for a completed group is

$$\begin{aligned}\sum_{n=k}^{2k}\binom{2n}{n}\binom{n}{k}^2\binom{2k}{n}16^{-n}&\\ =\frac{\binom{2k}{k}^2}{16^k}\sum_{j=0}^{k}\frac{(-k)_j(k+1/2)_j}{(j!)^2}(-1/4)^j.&\end{aligned}$$

At $n=k+r$, the ratio of successive summands is $(k-r)(2k+2r+1)/(8(r+1)^2)$; the initial term is $\binom{2k}{k}^2/16^k$. This proves the identity without evaluating an infinite hypergeometric series.

Modulo p, $k+1/2 \equiv k-N$ and $\binom{2k}{k}^2/16^k \equiv \binom{N}{k}^2$. On interchanging the sums, the inner sum is the integer identity

$$\sum_{k=0}^{N} \binom{N}{k}^2 \binom{k}{j}\binom{N-k}{j} = \binom{N}{j}^2 \binom{2N-2j}{N-2j}, \tag{29}$$

with right side zero if $2j > N$. Indeed the summand equals $\binom{N}{j}^2\binom{N-j}{k-j}\binom{N-j}{k}$, so Vandermonde's identity applies. For $2j \le N$,

$$\binom{2N-2j}{N-2j} \equiv (-1)^{(p-1)/2}\binom{N}{2j} \pmod{p},$$

and

$$\binom{N}{j}^2\binom{N}{2j}(-1/4)^j \equiv \frac{(1/4)_j(1/2)_j(3/4)_j}{(j!)^3}(-1/4)^j = \frac{(4j)!}{(j!)^4}(-1024)^{-j}.$$

For $j > \lfloor p/4 \rfloor$ the latter factorial quotient is divisible by p, with $j!$ a unit. This proves (28), including both boundaries of the sum. □

Let P_n be the Legendre polynomial normalized by $P_n(1) = 1$. For $p > 3$, $N = (p-1)/2$ and $d = \lfloor p/4 \rfloor$, define

$$f_u(X) = X^3 - \frac{3(3u+5)}{2}X + 9u + 7, \qquad \mathcal{H}_p(u) = [X^{p-1}]f_u(X)^N. \tag{30}$$

Lemma 7.3. *In* $\mathbb{F}_p[u]$,

$$\mathcal{H}_p(u) = \left(\frac{6}{p}\right) P_d(u). \tag{31}$$

Proof. The exact translation

$$f_u(Z+2) = Z\left(Z^2 + 6Z + \frac{9}{2}(1-u)\right)$$

preserves the coefficient at degree $p-1$ modulo p. Indeed the degree is at most $3N$, and the possible extra contributions contain $\binom{p-1+j}{p-1} \equiv 0 \pmod{p}$ for $1 \le j \le N$. Taking the coefficient of Z^N in the quadratic raised to N therefore gives

$$\mathcal{H}_p(u) = \sum_{j=0}^{d} \binom{N}{2j}\binom{2j}{j} 6^{N-2j}(9/2)^j(1-u)^j.$$

The number of quadratic and constant factors must both be j, which explains the entire support of this sum. Modulo p,

$$\binom{N}{2j}\binom{2j}{j} \equiv 4^j\frac{(1/4)_j(3/4)_j}{(j!)^2}, \qquad 6^N = \left(\frac{6}{p}\right), \qquad 6^{-2j}(9/2)^j = 8^{-j}.$$

The unordered pair $\{-d, d+1\}$ reduces to $\{1/4, 3/4\}$, depending on p mod 4. Rodrigues's formula gives

$$P_d(u) = \sum_{j=0}^{d} \frac{(-d)_j(d+1)_j}{(j!)^2}\left(\frac{1-u}{2}\right)^j,$$

which proves the polynomial identity. All factorial denominators are units modulo p. □

Lemma 7.4. *For every integer $n \geq 0$, the following identity holds in $\mathbb{Q}[u]$:*

$$P_n(u)^2 = \sum_{j=0}^{n} \binom{n}{j}\binom{n+j}{j}\binom{2j}{j}\left(\frac{u^2-1}{4}\right)^j. \tag{32}$$

Proof. Rodrigues's formula gives the Legendre equation $(1-u^2)y'' - 2uy' + \lambda y = 0$, where $\lambda = n(n+1)$, as well as $P_n(-u) = (-1)^n P_n(u)$ and $P_n(1) = 1$. For $W = y^2$, differentiation and substitution give

$$\begin{aligned}(1-u^2)^2 W''' - 6u(1-u^2)W'' \\ + \{6u^2 - 2 + 4\lambda(1-u^2)\}W' - 4\lambda u W = 0.\end{aligned}$$

Since P_n^2 is even, write it as $V(z)$ for $z = 1-u^2$. With $\vartheta = z\,d/dz$ the equation becomes

$$\{\vartheta^3 - z(\vartheta + 1/2)(\vartheta - n)(\vartheta + n + 1)\}V = 0.$$

This change is verified in $\mathbb{Q}(u)$; the new left side is $-(1-u^2)/(8u)$ times the preceding one. Clearing the intermediate denominator gives a polynomial identity. With $V(0) = 1$, its coefficient recursion uniquely yields

$$[z^j]V = \frac{(-n)_j (n+1)_j (1/2)_j}{(j!)^3}.$$

The coefficients terminate for $j > n$. Use $(-n)_j(n+1)_j/(j!)^2 = (-1)^j\binom{n}{j}\binom{n+j}{j}$ and $(1/2)_j/j! = 4^{-j}\binom{2j}{j}$ to obtain the result. □

Corollary 7.5. *For $p > 5$, $d = \lfloor p/4 \rfloor$ and either root $s^2 = 5$ in $\mathbb{F}_{p^2}$,*

$$R_p = P_d(s/2)^2 \quad \text{in } \mathbb{F}_{p^2}. \tag{33}$$

Proof. Set $n = d$ and $u = s/2$ in (32) and reduce modulo p. We have $1 - u^2 = -1/4$ and $\{-d, d+1\} = \{1/4, 3/4\}$ modulo p. The coefficient becomes $(4j)!(-1024)^{-j}/(j!)^4$. Its terms for $d < j < p$ vanish modulo p, giving exactly R_p. □

Both (31) and (32) are polynomial identities before any value is substituted. They remain valid in extension fields; no character sum over $\mathbb{F}_p$ has been reinterpreted as a character sum over $\mathbb{F}_{p^2}$.

8 An explicit endomorphism and the inert branch

8.1 The degree-five map

Let $s^2 = 5$ and $\delta^2 = -5$. These are distinct roles: s enters the coefficients of the curve, and δ enters the vertical coordinate of the map. Initially work in $\mathcal{R} = \mathbb{Z}[1/10, s]/(s^2 - 5)$, adjoining δ and its inverse when defining the map. Put

$$a = -\frac{30 + 9s}{4}, \qquad b = \frac{14 + 9s}{2}, \qquad f(X) = X^3 + aX + b, \qquad E_s:\ Y^2 = f(X). \tag{34}$$

Its Hasse coefficient is $\mathcal{H}_p(s/2)$. Define

$$k(X) = X^2 - \frac{5 + 3s}{2}X + \frac{65 + 42s}{20}, \tag{35}$$

$$\begin{aligned}n(X) = X^5 - (5 + 3s)X^4 + \frac{120 + 45s}{2}X^3 - \frac{1055 + 405s}{4}X^2 \\ + \frac{7045 + 3588s}{16}X - \frac{1395 + 540s}{4},\end{aligned} \tag{36}$$

and $A = -n$, $B = 5k^2$, $r = A/B$.

Theorem 8.1. *Over every field of characteristic $p > 5$ containing s, δ as above, the map*

$$\Phi(X,Y) = \left(r(X), \frac{Y r'(X)}{\delta}\right), \qquad \Phi(O) = O \tag{37}$$

defines a separable endomorphism of degree five of E_s and $\Phi^2 = [-5]$.

Proof. We use four fixed polynomial identities in $\mathcal{R}[X]$. Their explicit inputs and arithmetic verification are described in Appendix B. First, with $T = A'B - AB'$,

$$fT^2 + 5(A^3B + aAB^3 + bB^4) = 0. \tag{C0}$$

Dividing by $-5B^4$ gives $f(X)r'(X)^2/\delta^2 = f(r(X))$, so the map lands on the same curve.

To determine the composition including the sign of the second coordinate, use the classical division-polynomial normalization [13, §§5.5–5.6]. The required polynomials are

$$\begin{aligned}
\psi_3 &= 3X^4 + 6aX^2 + 12bX - a^2,\\
F_4 &= X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4abX - a^3 - 8b^2,\\
\psi_5 &= 32f^2F_4 - \psi_3^3,\\
m &= X\psi_5^2 - 8fF_4\psi_3(\psi_5 - 4F_4^2),\\
\psi_7 &= \psi_5\psi_3^3 - 128f^2F_4^3,\\
\Omega_5 &= 4\psi_7F_4^2 - \psi_3^3(\psi_5 - 4F_4^2)^2.
\end{aligned} \tag{38}$$

Reducing the multiplication formula with $Y^2 = f(X)$ gives

$$[5](X,Y) = \left(\frac{m}{\psi_5^2}, \frac{Y\Omega_5}{\psi_5^3}\right). \tag{39}$$

Here $\psi_4 = 4YF_4$ and $\Omega_5 = \omega_5/Y$ in that convention. For a polynomial F of degree at most five write $F^{[5]}(U,V) = V^5F(U/V)$. The other three certificates are

$$A^{[5]}(A,B) = m, \tag{C1}$$

$$B^{[5]}(A,B) = \psi_5^2, \tag{C2}$$

$$m'\psi_5 - 2m\psi_5' = 5\Omega_5. \tag{C3}$$

The first two give $r(r(X)) = m/\psi_5^2$. For the second coordinate the chain rule and (C3) give

$$(\Phi^2)_Y = \frac{Y}{\delta^2}(r\circ r)' = -\frac{Y}{5}\frac{m'\psi_5 - 2m\psi_5'}{\psi_5^3} = -\frac{Y\Omega_5}{\psi_5^3}.$$

Thus both coordinates agree with $[-5]$ in (39).

It remains to check reduction and extension at all points. Exact arithmetic gives

$$\begin{aligned}
\Delta(E_s) &= 729(s-2), & N(\Delta) &= -729^2,\\
\mathrm{Res}(n,k) &= \frac{3^{10}(25-11s)}{250}, & N(\mathrm{Res}(n,k)) &= \frac{3^{20}}{5^5},\\
\mathrm{Disc}(k) &= \frac{9}{10}(5-s), & N(\mathrm{Disc}(k)) &= \frac{81}{5}.
\end{aligned} \tag{40}$$

All coefficient denominators involve only 2 and 5. For $p > 5$ the discriminant and resultant are units for both choices of s: their norms have numerator a power of three. Hence the curve is smooth, n, k stay coprime, and r still has degree five. At infinity $r(X) \sim -X/5$ and $r'(X) \sim -1/5$, so the rational map is nonconstant and takes O to O.

A rational map between smooth projective curves extends at its omitted points, and a nonconstant morphism between elliptic curves preserving the origin is a group homomorphism [12, Theorem 4.15 and Definition 4.20]. The poles of r are therefore points mapped to O. From the diagram $X \circ \Phi = r \circ X$, and $\deg X = 2$, it follows that $\deg \Phi = 5$. Its differential is nonzero; more precisely

$$\Phi^* \left(\frac{dX}{2Y} \right) = \delta \frac{dX}{2Y}.$$

Thus Φ is separable. Identities (C0)–(C3) reduce from $\mathcal{R}$ at every $p > 5$, proving the theorem uniformly. □

8.2 Geometric torsion, Hasse vanishing and lifting

Proposition 8.2. *For $p > 5$ with $(-5/p) = -1$ and either root $s^2 = 5$ in $\mathbb{F}_{p^2}$, we have $\mathcal{H}_p(s/2) = 0$. Consequently $G_{a,p}(1/20) \equiv G_{Q,p}(-1/16) \equiv 0 \pmod{p^2}$.*

Proof. Theorem 8.1 constructs Φ directly in characteristic p, over a field containing s and δ. If E_s were ordinary, its group of geometric p-torsion points would be cyclic of order p [14, p. 1]. Every endomorphism acts on that group by a scalar $c \in \mathbb{F}_p$, even when the morphism is defined over an extension of $\mathbb{F}_p$. The relation $\Phi^2 = [-5]$ would force $c^2 = -5$, impossible for an inert prime. Thus E_s is supersingular.

The Deuring–Hasse criterion [15, p. 1] now gives $[X^{p-1}]f(X)^{(p-1)/2} = 0$, which is $\mathcal{H}_p(s/2) = 0$. If necessary one extends the finite field so that the smooth cubic splits. Ordinarity, supersingularity and vanishing of this coefficient are preserved under field extension. This argument applies to either choice of s.

Lemma 7.3, Corollary 7.5, Lemma 7.2, and (27) give

$$\mathcal{H}_p(s/2) = 0 \implies P_d(s/2) = 0 \implies R_p = F_{16,p} = 0 \pmod{p}.$$

Equation (27) then gives $G_{a,p}(1/20) \equiv G_{Q,p}(-1/16) \equiv 0 \pmod{p}$. Apply Lemma 2.2 separately to $G_{a,p}$ at $1/20$ and to $G_{Q,p}$ at $-1/16$. The unit conditions are exactly (11). This yields vanishing modulo p^2 of each original sum. □

Completion of Theorem 1.1. Propositions 6.3 and 8.2 cover every prime $p > 5$. For $p = 3$, the three summands in each of $G_{a,3}(1/20)$ and $G_{Q,3}(-1/16)$ are $(1, 3, 0)$ modulo nine, by their definitions. Each sum is therefore congruent to 4; multiplying by $(-1)^{(3-1)/2} = -1$ gives 5 modulo nine. The representation $2 \cdot 3 = 1^2 + 5 \cdot 1^2$ gives $2 \cdot 1^2 - 2 \cdot 3 \equiv 5 \pmod{9}$, as required. The primes $2, 5$ are excluded in the original statement. □

The supersingularity argument uses geometric p-torsion; it does not assert that the integer Frobenius trace over $\mathbb{F}_{p^2}$ is zero. No complex uniformization or reduction theorem for a characteristic-zero endomorphism enters this inert branch.

9 Two consequences

Corollary 9.1. *Let $p > 5$ and $d = \lfloor p/4 \rfloor$. In $\mathbb{F}_p[u]$,*

$$4u^2 - 5 \mid P_d(u) \quad \iff \quad (-5/p) = -1.$$

When the divisibility holds, both roots of $4u^2 - 5$ are simple roots of P_d over $\mathbb{F}_{p^2}$.

Proof. For an inert prime, Proposition 8.2 and Lemma 7.3 give vanishing at both distinct roots $u = \pm s/2$. At either point $1 - u^2 = -1/4$ is a unit. In the Legendre equation, a multiple root of multiplicity $2 \le m \le d < p$ would produce an uncancelled leading local term $m(m-1)(1-u^2)$. Thus the roots are simple.

Conversely, if $4u^2-5$ divides P_d, then Corollary 7.5, Lemma 7.2 and (27) give $G_{a,p}(1/20)\equiv 0 \pmod p$. At a split prime, Theorem 1.1 gives $(-1)^{(p-1)/2}G_{a,p}(1/20)\equiv 4x^2$ or $2x^2$ modulo p, which is nonzero by the primitive representation. Hence the prime is inert. This converse uses the already proved theorem and is not a premise of its proof. □

Corollary 9.2. *If $p>5$ is inert, then for every $r\in\mathbb{Z}_p$,*

$$G_{a,p}(1/20+pr)\equiv 0, \qquad G_{Q,p}(-1/16+pr)\equiv 0 \pmod{p^2}.$$

Proof. The values at the unshifted parameters vanish modulo p^2 by Proposition 8.2. In Lemma 2.2 their first derivatives vanish modulo p, since the parameters are units and $\theta U(t_0)\equiv 0$. Taylor expansion of the finite polynomials therefore proves the result. □

A Finite modular certificates

This appendix specifies the finite arithmetic underlying Lemmas 3.1 and 3.2. For an eta quotient with exponent vector $(r_d)_{d|6}$, write

$$\prod_d \eta_d^{r_d} = q^{\sum dr_d/24}\prod_{m\ge 1}(1-q^m)^{e_m}, \qquad e_m=\sum_{d|m} r_d.$$

To calculate through degree M, after removal of the initial power, retain only $m\le M$ and use the finite binomial expansion

$$(1-q^m)^{e_m}=\sum_{j=0}^{\lfloor M/m\rfloor}(-1)^j\binom{e_m}{j}q^{mj} \pmod{q^{M+1}}.$$

For negative exponents the binomial coefficient has its usual integer meaning $\binom{-e}{j}=(-1)^j\binom{e+j-1}{j}$. Multiply these finite polynomials, discarding degrees exceeding M after each step.

A second exact recurrence gives the same coefficients. If the initial power has been removed and the constant term is one, set

$$\ell_n=-\sum_{m|n} me_m, \qquad a_0=1, \qquad na_n=\sum_{j=1}^{n}\ell_j a_{n-j}.$$

This follows from the logarithmic derivative, so the divisions are exact. Differentiation of a series uses $\partial q^n=nq^n$; division by a series with unit constant term uses its triangular coefficient recurrence. For $\partial\log J$, remove its initial q and add the resulting constant one.

The following coefficients provide intermediate values:

	q^0	q^1	q^2	q^3	q^4
h	0	1	5	19	61
J	0	1	−2	−3	4
Θ_a	1	6	6	42	6
Θ_Q	1	−12	−12	−12	−12
t_a	0	1	−14	117	−884
t_Q	0	1	22	405	6820
v	0	1	24	300	2624
S	0	1	6	21	68

The two form vectors through degree eight are

$$([q^n]\Theta_a)_{n=0}^8=(1,6,6,42,6,36,42,48,6),$$

$$([q^n]\Theta_Q)_{n=0}^8=(1,-12,-12,-12,-12,-72,-12,-96,-12).$$

Apply the preceding finite arithmetic to the exponent vectors in Section 3. For the named residuals the complete required vectors are

Residual	degrees	vector
$v(1+8h)-h(1+9h)^3$	0–5	$(0,0,0,0,0,0)$
$\Theta_a-\partial\log S$	0–2	$(0,0,0)$
$\Theta_Q+\partial\log R$	0–2	$(0,0,0)$
Left side of (17), Θ_a	0–8	$\mathbf{0}_9$
Left side of (18), Θ_a	0–8	$\mathbf{0}_9$
Left side of (17), Θ_Q	0–8	$\mathbf{0}_9$
Left side of (18), Θ_Q	0–8	$\mathbf{0}_9$

Here $\mathbf{0}_9$ means nine zeros. These are 48 coefficients: six for a function with total pole order at most five, six for forms of weight two with valence bound two, and 36 for forms of weight eight with valence bound eight. The three initial coefficients used to determine R were given in Lemma 3.1. Holomorphy and the pole bounds were proved before these coefficients were used. Consequently each finite zero vector proves an identity, rather than merely testing a prefix of an unbounded series.

B Fixed algebraic certificates

The four identities (C0)–(C3) have only the fixed polynomials (34)–(36) and (38) as inputs. Their expansion can be performed without algebraic-number approximations. Represent a coefficient $u+vs$ by the pair $(u,v)\in\mathbb{Q}^2$, with rules

$$(u,v)+(u',v')=(u+u',v+v'),\qquad (u,v)(u',v')=(uu'+5vv',uv'+vu').$$

Represent a polynomial by its coefficient list in ascending order. Addition is componentwise, multiplication is finite convolution, and differentiation sends its ith coefficient to i times that coefficient in degree $i-1$. For homogenization use the finite sum

$$F^{[5]}(A,B)=\sum_{i=0}^{5}F_iA^iB^{5-i},$$

padding F with zeros to degree five. Thus every arithmetic operation in the certificates is explicitly determined over rational pairs.

Form the residuals

$$\begin{aligned}H_0&=f(A'B-AB')^2+5(A^3B+aAB^3+bB^4),\\H_1&=A^{[5]}(A,B)-m,\\H_2&=B^{[5]}(A,B)-\psi_5^2,\\H_3&=m'\psi_5-2m\psi_5'-5\Omega_5.\end{aligned}$$

Their degree bounds and full coefficient-pair vectors are

Residual	degree at most	pairs	coefficient-pair vector
H_0	19	20	$((0,0))_{i=0}^{19}$
H_1	25	26	$((0,0))_{i=0}^{25}$
H_2	24	25	$((0,0))_{i=0}^{24}$
H_3	36	37	$((0,0))_{i=0}^{36}$

There are 108 rational pairs, or 216 rational entries. The bounds follow directly from the input degrees: $\deg A=5$, $\deg B=4$, $\deg f=3$, $\deg\psi_5=12$, $\deg m\le 25$, and $\deg\Omega_5\le 36$. The pair arithmetic above gives the displayed zero vectors. The companion supplies all inputs, intermediate polynomials and exact expansion code; a separate symbolic expansion provides a second implementation of these equalities.

For completeness, the nondegeneracy data in (40) follow from the standard polynomial discriminant and resultant, with norm $N(u+vs) = u^2 - 5v^2$. The short Weierstrass discriminant is $-16(4a^3 + 27b^2)$, giving $729(s-2)$. These computations are again over $\mathbb{Q}^2$. No unlisted prime denominator is introduced.

The coefficients of the fixed polynomials belong to $\mathcal{R}$; their identities therefore hold after every specialization in characteristic $p > 5$. The unit resultant prevents cancellation of the map's numerator and denominator after reduction, and the unit curve discriminant ensures smoothness. This proves why the finite certificates imply a statement for all the primes in Theorem 8.1. A finite panel of point counts or supercongruence tests would not supply this implication.

C Companion and reproducibility

The companion repository for this manuscript, version 0.1.1, is

`https://github.com/aconsciousfractal/Sun-3-7-Supercongruence`.

It includes the standalone source, modular coefficient calculations, the algebraic certificates (C0)–(C3), the endpoint calculations, and finite checks of the original binomial definitions. Its deterministic evidence manifest is identified by SHA-256

`035baf66ce55e008c441b05e316c54b323ad6b2146f5bc6f23eeede99d3ea977`

The evidence digest binds the stated arithmetic outputs and their inputs; it does not certify novelty or mathematical correctness. The modular identities and fixed algebraic certificates are used with the sufficiency arguments in the preceding appendices. Numerical checks at individual primes serve as regressions and are not premises of the uniform theorem.

Acknowledgment. The author thanks Zhi-Hong Sun for comments on the presentation of the companion manuscripts and for pointing out Mao's result on Q_{np}.

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.

[2] Zhi-Hong Sun, *Congruences concerning Legendre polynomials II*, Journal of Number Theory **133** (2013), 1950–1976. doi:10.1016/j.jnt.2012.11.004. Theorem and equation numbers refer to arXiv:1012.3898v2.

[3] Zhi-Hong Sun, *Congruences for sums involving Franel numbers*, International Journal of Number Theory **14** (2018), 123–142. doi:10.1142/S1793042118500094.

[4] Oleksiy Babanskyy, *Sun's supercongruence for an Apéry-like sequence*. Manuscript and companion repository.

[5] Oleksiy Babanskyy, *Sun's supercongruence for two Apéry-like binomial sums*. Manuscript and companion repository.

[6] Frits Beukers, *Supercongruences using modular forms*, arXiv:2403.03301v3. Lemma 3.7 and Theorem 6.1.

[7] Armin Straub, *Gessel–Lucas congruences for sporadic sequences*, arXiv:2301.12248v1. Theorem 3.2.

[8] Jeremy Rouse and John J. Webb, *On spaces of modular forms spanned by eta-quotients*, arXiv:1311.1460v3.

[9] Guo-Shuai Mao, *Congruences involving Franel numbers and Apéry-like numbers*, preprint (2023), Theorem 1.4. doi:10.13140/RG.2.2.23378.73922. The cited author-uploaded full text is dated 8 January 2025 on ResearchGate.

[10] William Craig, *New Types of Sturm bounds via p-adic transfer methods*, arXiv:2602.10240v1. Theorem 1.1(1), the classical valence bound.

[11] NIST Digital Library of Mathematical Functions, Section 23.18, transformations of the Dedekind eta function.

[12] Andrew V. Sutherland, *18.783 Elliptic Curves, Lecture 4*, MIT, Fall 2023. `https://math.mit.edu/classes/18.783/2023/LectureNotes4.pdf`.

[13] Andrew V. Sutherland, *18.783 Elliptic Curves, Lecture 5*, MIT, Fall 2023. `https://math.mit.edu/classes/18.783/2023/LectureNotes5.pdf`.

[14] Andrew V. Sutherland, *18.783 Elliptic Curves, Lecture 13*, MIT, Fall 2023. `https://math.mit.edu/classes/18.783/2023/LectureNotes13.pdf`.

[15] Christophe Debry, *Beyond two criteria for supersingularity: coefficients of division polynomials*, arXiv:1303.5002v1. The Deuring criterion.