A CERTIFIED CENSUS OF THE SUPERSPECIAL GENERALIZED HOWE CURVES OF GENUS 4, 5 AND 6, AND THE CELL $(g, p) = (6, 13)$

KOREA SUPERINTELLIGENCE LABS

Abstract. A recent preprint of Ohashi (arXiv:2604.18074) constructs, in every characteristic $p > 5$, three explicit families of curves of genus 4, 5 and 6 whose Jacobians are completely decomposable, and reduces the question of whether a member is superspecial to whether three elliptic curves are supersingular — that is, to the vanishing of an explicit polynomial (Deuring's for genus 4, the Ibukiyama–Katsura–Oort polynomials for genus 5 and 6) at points of $\mathbb{F}_{p^2}$. We take that finite core as the object of study. For every prime $7 \le p \le 157$ ($7 \le p \le 113$ in genus 4) we compute, and certify with a proof assistant, the cardinalities of the root sets of the three polynomials in $\mathbb{F}_{p^2}$ and the exact numbers $N_4(p)$, $N_5(p)$, $N_6(p)$ of ordered parameter pairs that pass the criterion — numbers the preprint never prints, since its algorithms stop at the first witness. The zero sets reproduce the preprint's exception lists for genus 4 and genus 5 exactly. In genus 6 they reproduce the part of its list that lies in range, with one difference: the genus-6 family contains no superspecial member in characteristic 13, whereas the preprint's Theorem 6.4 asserts one for every prime $11 < p < 10^5$ outside a list that does not contain 13, and nothing else in the preprint covers $p = 13$. The author's own public computation log records the same failure at $p = 13$, so the discrepancy is a transcription slip in the exception list, and $(g, p) = (6, 13)$ joins $(5, 13)$ and $(6, 7)$ as a cell the preprint leaves open. We also observe that the genus-6 count is a solution count, $N_6(p) = \#\{(x, y, z) \in \mathcal{T}_6(p)^3 : xyz = 1\}$, which carries an action of a group of order 12 that the preprint's algorithm does not use, and that $6 \mid N_6(p)$ at every prime in range. Every statement about $\mathbb{F}_{p^2}$ is machine-checked in Lean 4; the statements about $p = 13$ are checked by the kernel alone.

1. Introduction

A curve over a field of characteristic $p > 0$ is *superspecial* when its Jacobian is isomorphic to a product of supersingular elliptic curves. In genus 1, 2 and 3 the answer is known in every characteristic (Table 1 of the preprint discussed below records existence for all p in genus 1, for $p \ge 5$ in genus 2 and for $p \ge 3$ in genus 3); for genus $g \ge 4$ the question is open in general. The preprint [11] — R. Ohashi, *Generalized Howe curves of genus 4, 5, and 6 with completely decomposable Jacobians*, arXiv:2604.18074, version 3 — attacks genus 4, 5 and 6 through three explicit two-parameter families, and its Theorems 1.1, 1.2 and 1.3 read, verbatim:[1]

> **Theorem 1.1.** For every prime p with $7 < p < 10^6$ and $p \neq 13, 19, 73$, there exists a superspecial curve $X_{s,t}$ of genus 4 in characteristic p.
>
> **Theorem 1.2.** For every prime p with $7 \le p < 10^5$ and $p \neq 13$, there exists a superspecial curve of genus 5 in characteristic p.
>
> **Theorem 1.3.** For every prime p with $7 < p < 10^5$, there exists a superspecial curve of genus 6 in characteristic p.

Its Table 1 summarises existence by a circle and non-existence by a cross for $p \in \{2, 3, 5, 7, 11, 13\}$ and "$\cdots$", prints "??" at $(g, p) = (5, 13)$ and $(6, 7)$, and is followed by the sentence "It remains open whether superspecial curves exist for $(g, p) = (5, 13)$ and $(6, 7)$." At $(6, 13)$ Table 1 prints a circle. The preprint

[1] Every theorem, proposition, algorithm, lemma, equation, table and appendix number of [11] used in this paper is the number of the *compiled* e-print of version 3 (the arXiv source compiled with tectonic, numbers read from the `.aux` file; the first two pages were additionally read from the compiled PDF). The raw LaTeX source carries unresolved cross-references and was used only for wording. The single exception is Lemma 3.3, which carries no label and so has no `.aux` entry; see the footnote in §2.3.

adds that, combined with the result of Kudo, Harashita and Howe [6], Theorem 1.1 gives superspecial genus-4 curves for all $7 < p < 10^6$, and that its genus-4 algorithm is a speed-up of theirs.

The three families and their finite core. The families are the desingularised fibre products $X_{s,t}$, $Y_{s,t}$, $Z_{s,t}$ of

$$\begin{aligned} &E_1 : y^2 = (x-1)(x-s)(x-t), && E_2 : y^2 = (x+1)(x+s)(x+t) && \text{(genus 4; [11], §3)},\\ &C_1 : y^2 = x(x^2-1)(x^2-s^2), && C_2 : y^2 = x(x^2-1)(x^2-t^2) && \text{(genus 5; [11], §4)},\\ &C_1 : y^2 = (x^3-1)(x^3-s^6), && C_2 : y^2 = (x^3-1)(x^3-t^6) && \text{(genus 6; [11], §5)}, \end{aligned}$$

with $s, t \notin \{0, \pm 1\}$, $s^2 \neq t^2$ in genus 4 and 5, and $s, t \neq 0$ with $1, s^6, t^6$ pairwise distinct in genus 6. Their Jacobians are completely decomposable, and Propositions 3.1, 4.1 and 5.2 of [11] say that a member is superspecial if and only if three associated elliptic curves are supersingular. Each of those supersingularity conditions is the vanishing of a classical polynomial: Deuring's H_p for a Legendre curve, and the polynomials g_p and h_p of Ibukiyama, Katsura and Oort [4] for the genus-2 curves $y^2 = (x^3-1)(x^3-\alpha)$ and $y^2 = x(x^2-1)(x^2-\beta)$. The upshot, which [11] turns into its Algorithms 3.4, 4.2 and 5.3, is that existence of a superspecial member in characteristic p is a statement about roots of explicit polynomials in $\mathbb{F}_{p^2}$: for instance (Algorithm 5.3 of [11]), with $\mathcal{T}$ the set of roots $\alpha \neq 0, 1$ of g_p,

$$\text{a superspecial } Z_{s,t} \text{ exists in characteristic } p \iff \exists\, \alpha_1 \neq \alpha_2 \in \mathcal{T} \text{ with } \alpha_1/\alpha_2 \in \mathcal{T}.$$

The preprint proves its theorems by running these searches (in a j-invariant reformulation, its Algorithms 4.3 and 5.4) in Magma, stopping at the first witness, and reports the outcome as an exception list: Theorem 6.3 for genus 5 ($19 < p < 10^5$, $p \neq 37, 53, 89, 97, 101, 137$) and Theorem 6.4 for genus 6 ($11 < p < 10^5$ outside a 19-element list). The primes the searches miss are then handled by individually constructed curves in its Appendices A and B. The implementation and the complete per-prime logs are public [12].

What this paper does. We take the finite core — the polynomials, their root sets in $\mathbb{F}_{p^2}$, and the three membership tests — as the object, and we certify it. Everything we prove is a statement about $\mathbb{F}_{p^2}$; no curve, Jacobian or isogeny occurs in any of our theorems. The passage from a theorem here to a statement about superspecial curves is always the quoted equivalence of [11] together with the quoted classical criterion, and we display it separately, as a *reading*, wherever we use it. Concretely:

(i) For every prime $7 \leq p \leq 157$ (genus 4: $7 \leq p \leq 113$) we certify the cardinalities $|\mathcal{T}_4| = (p-1)/2$, $|\mathcal{T}_5| = \lfloor p/4 \rfloor$, $|\mathcal{T}_6| = \lfloor p/3 \rfloor$ that [11] quotes from [13] and [4], and the exact numbers $N_4(p)$, $N_5(p)$, $N_6(p)$ of ordered parameter pairs passing the criterion (Theorem 6.1). The preprint prints no such count anywhere; its logs print one witness or `false` per prime.

(ii) The zero sets of N_4 and N_5 are exactly the preprint's exception lists (plus the primes below the ranges of its theorems). For genus 5 the certified range covers the whole exception list of Theorem 6.3.

(iii) The genus-6 family is empty in characteristic 13: $N_6(13) = 0$ (Theorem 4.1). Theorem 6.4 of [11] asserts the opposite, Appendix B of [11] does not cover $p = 13$, and so Theorem 1.3 and the circle at $(6, 13)$ in Table 1 have no support in the preprint. The author's own log prints `false` at $p = 13$ [12]; the omission of 13 from the exception list is a transcription slip, and $(6, 13)$ is a third cell the preprint leaves open. This part is checked by the Lean kernel alone, with no native evaluation.

(iv) The genus-6 count is a solution count: $N_6(p) = \#\{(x, y, z) \in \mathcal{T}_6^3 : xyz = 1\}$ (Proposition 5.2, Theorem 5.3). The right-hand side carries an action of $S_3 \times \langle \text{inversion} \rangle$, of order 12, which the double loop of Algorithm 5.3 does not use; $6 \mid N_6(p)$ holds at every prime $7 \leq p \leq 157$, and is recorded as a checked fact rather than a theorem, because the action is not free.

(v) Inside the preprint's own families, its two open cells are empty: $N_5(13) = 0$ and $N_6(7) = 0$ (Propositions 3.6 and 3.8). This does not close either cell — a superspecial curve could lie outside the family — it says the preprint's construction cannot close them.

We stress what (iii) does and does not show. It shows that the preprint's family $Z_{s,t}$ has no superspecial member in characteristic 13 and that the preprint supplies no other construction there. It does not show that no superspecial curve of genus 6 exists in characteristic 13.

Verification. All statements about $\mathbb{F}_{p^2}$ are formalised and checked in Lean 4 with Mathlib (Section 8, Appendix A). The field $\mathbb{F}_{p^2}$ is built by hand as $\mathbb{F}_p[w]/(w^2-n)$ for a quadratic non-residue n, because that representation reduces inside the kernel; the ring axioms of the model are proved for every p and n, and the field property is checked at the characteristics where the kernel is used. Every statement about $p = 13$ is discharged by kernel evaluation (`decide +kernel`) and depends on no axiom beyond `propext` and `Quot.sound`; the eight sweeps over all primes to 157 use compiled evaluation (`native_decide`) and carry its axiom.

2. The finite core

Throughout, $p > 5$ is prime and $m = (p-1)/2$.

2.1. **The field.** Fix a quadratic non-residue n modulo p. We represent $\mathbb{F}_{p^2} = \mathbb{F}_p[w]/(w^2-n)$ as pairs $(a,b) \in \mathbb{F}_p^2$ standing for $a + bw$, with componentwise addition and

$$(a,b)\cdot(c,d) = (ac + n\,bd,\ ad + bc).$$

In every statement below the non-residue is the least one, $n = 2$ for $p \in \{11, 13, 19, 37\}$, $n = 3$ for $p \in \{7, 17\}$, $n = 5$ for $p = 23$, and in general the least $n \geq 2$ that is not a square modulo p; the sweeps over ranges of primes compute it. A root $a + bw$ is printed below as $a + bw$ with $0 \leq a, b < p$.

2.2. **Three polynomials and their root sets.**

Definition 2.1. For $p > 5$ put

$$H_p(\lambda) = \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i,$$

$$h_p(\beta) = \sum_{i=0}^{\lfloor p/4 \rfloor} \binom{m}{\lfloor (p+1)/4 \rfloor + i} \binom{m}{i} \beta^i,$$

$$g_p(\alpha) = \sum_{i=0}^{\lfloor p/3 \rfloor} \binom{m}{\lfloor (p+1)/6 \rfloor + i} \binom{m}{i} \alpha^i,$$

as polynomials over $\mathbb{F}_p$, and let $\mathcal{T}_4(p)$, $\mathcal{T}_5(p)$, $\mathcal{T}_6(p) \subset \mathbb{F}_{p^2}$ be the sets of roots of H_p, h_p, g_p in $\mathbb{F}_{p^2}$ different from 0 and 1.

H_p is Deuring's polynomial [3], in the form of [13, Theorem V.4.1(b)]: the Legendre curve $y^2 = x(x-1)(x-\lambda)$ is supersingular if and only if $H_p(\lambda) = 0$. The polynomials g_p and h_p are, verbatim, Definitions 1.6 and 1.7 of [4, p. 135], whose Propositions 1.8 and 1.9 (p. 135) state that the genus-2 curve $C_\alpha : y^2 = (x^3-1)(x^3-\alpha)$ ($\alpha \neq 0, 1$) is supersingular if and only if $g_p(\alpha) = 0$, and $C_\beta : y^2 = x(x^2-1)(x^2-\beta)$ ($\beta \neq 0, 1$) is supersingular if and only if $h_p(\beta) = 0$; these two curves are their Classes (a) and (b) (p. 132), and their Proposition 1.14 (p. 138) states that the zeros of g_p and of h_p are simple. Two remarks on these citations. First, [4] say *supersingular* where [11] says *superspecial*; for exactly the curves in question the two agree by [4, Proposition 1.10] (p. 136: for a genus-2 curve in their Classes (2)–(5), $J(C)$ is a supersingular abelian surface if and only if it is isomorphic to a product of two supersingular elliptic curves), which covers Classes (a) and (b) because a curve in Class (a) (resp. (b)) is isomorphic to one in Class (2), (4) or (5) (resp. (3), (4) or (5)) [4, p. 133]. Second, the cardinalities we use are stated in neither [4] nor [13]. [11] cites Proposition 1.14 of [4] for $|\mathcal{T}_5| = \lfloor p/4 \rfloor$ and $|\mathcal{T}_6| = \lfloor p/3 \rfloor$, and Theorem V.4.1 of [13] for $|\mathcal{T}_4| = m$; but Proposition 1.14 gives simplicity of the zeros only, and so does [13, Theorem V.4.1(c)], which says that H_p has distinct roots and not how many. Each count also needs the degree — $\deg H_p = m$, $\deg h_p = \lfloor p/4 \rfloor$, $\deg g_p = \lfloor p/3 \rfloor$ (the leading coefficients are products of binomial coefficients $\binom{m}{k}$ with $m < p$, hence non-zero modulo p) — that 0 and 1 are not

roots ($H_p(0) = 1$ and $H_p(1) = \binom{p-1}{m} \equiv (-1)^m$, and likewise for h_p, g_p), and the fact that every root lies in $\mathbb{F}_{p^2}$. All of these are among the facts certified below (Proposition 3.3 and Propositions 3.2, 3.4–3.9).

2.3. **The three membership tests and the counts.** For $u, v \in \mathbb{F}_{p^2}$ write

$$\widetilde{H}_p(u, v) = \sum_{i=0}^{m} \binom{m}{i}^2 u^i v^{m-i}$$

for the homogenised Deuring polynomial, so that for $v \neq 0$ one has $\widetilde{H}_p(u, v) = 0$ if and only if $H_p(u/v) = 0$. Every test below is stated without division, which is what keeps kernel evaluation affordable and explains the shape of the statements in Appendix A.

Definition 2.2. *Genus* 4. For $(\lambda_1, \lambda_3) \in \mathcal{T}_4(p)^2$ put

$$c_1 = \lambda_1 - \lambda_3, \quad c_2 = \lambda_1^2 - \lambda_3, \quad c_3 = \lambda_1^2 - 2\lambda_1 + \lambda_3, \quad c_4 = 2\lambda_1\lambda_3 - \lambda_1^2 - \lambda_3.$$

The pair *passes* when $c_1c_2c_3c_4 \neq 0$ and $\widetilde{H}_p(\lambda_3 c_3^2, c_4^2) = 0$, i.e. $H_p(\lambda_4) = 0$ for $\lambda_4 = \lambda_3 c_3^2/c_4^2$. $N_4(p)$ is the number of ordered pairs that pass.

Genus 5. For $(\beta_1, \beta_2) \in \mathcal{T}_5(p)^2$ the pair passes when $\beta_1 \neq \beta_2$ and $\widetilde{H}_p(\beta_2, \beta_1) = 0$. $N_5(p)$ is the number of ordered pairs that pass.

Genus 6. For $(\alpha_1, \alpha_2) \in \mathcal{T}_6(p)^2$ the pair passes when $\alpha_1 \neq \alpha_2$ and there is $\alpha_3 \in \mathcal{T}_6(p)$ with $\alpha_2\alpha_3 = \alpha_1$, i.e. $\alpha_1/\alpha_2 \in \mathcal{T}_6(p)$. $N_6(p)$ is the number of ordered pairs that pass.

These are Step 2 of Algorithms 3.4, 4.2 and 5.3 of [11] respectively, with the following bookkeeping. In genus 4, $\lambda_1 = (t-s)/(1-s)$ and $\lambda_3 = (t^2-s^2)/(1-s^2)$ are the Legendre parameters of the elliptic curves E_1 and E_3 of [11], the four conditions $c_i \neq 0$ are the conditions (3.2) of [11], equation (3.3) of [11] recovers $s = c_2/c_3$ and $t = c_4/c_3$, and $\lambda_4 = (t^2-s^2)/(t^2(1-s^2)) = \lambda_3/t^2$ is the Legendre parameter of E_4 (equation (3.1) of [11]); the lemma following (3.3) in [11] shows that every (λ_1, λ_3) with $\lambda_i \neq 0, 1$ satisfying (3.2) comes from an admissible (s, t) in this way.[2] In genus 6, $(\alpha_1, \alpha_2) = (s^6, t^6)$ and $\alpha_1/\alpha_2 = s^6/t^6$. In genus 5, $(\beta_1, \beta_2) = (s^2, t^2)$ and Step 2 of Algorithm 4.2 asks whether the elliptic curve $E_3 : y^2 = (x^2 - \beta_1)(x^2 - \beta_2)$ is supersingular; [11] decides this through the j-invariant of E_3, and we use instead:

Lemma 2.3 (not formalised)**.** *Let $\beta_1, \beta_2 \in \mathbb{F}_{p^2}$ be distinct and non-zero. The elliptic curve $E_3 : y^2 = (x^2 - \beta_1)(x^2 - \beta_2)$ is supersingular if and only if $\widetilde{H}_p(\beta_2, \beta_1) = 0$, i.e. if and only if $H_p(\beta_2/\beta_1) = 0$.*

Proof. Let k be a perfect field of odd characteristic p and $y^2 = f(x)$ a curve with $f \in k[x]$ square-free of degree $2g+1$ or $2g+2$. Writing $f(x)^m = \sum_i c_i x^i$, the matrix of the Cartier operator on $H^0(\Omega^1)$ in the basis $\{x^{i-1}\,dx/y\}_{1 \le i \le g}$ is $(c_{ip-j}^{1/p})_{1 \le i,j \le g}$ [1, §3.1], a computation that nowhere uses $g \geq 2$; and the Cartier operator vanishes if and only if the Jacobian is isomorphic to a product of supersingular elliptic curves [9, Theorem 4.1]. Our $f = (x^2 - \beta_1)(x^2 - \beta_2)$ is square-free of degree $4 = 2g + 2$ with $g = 1$, the matrix is the single entry $c_{p-1}^{1/p}$, which vanishes exactly when c_{p-1} does, and the Jacobian is the curve; so E_3 is supersingular if and only if the coefficient of x^{p-1} in $f(x)^m$ is zero. (The odd-degree form of this is [13, Theorem V.4.1(a)], whose proof uses $\deg f = 3$; [1] is a note warning that the even-degree case, and the difference between the Hasse–Witt and the Cartier–Manin matrix, have been a source of published errors. Only the vanishing is used here, and the two matrices vanish together.) Now $f(x)^m = (x^2 - \beta_1)^m (x^2 - \beta_2)^m$, and the coefficient of $x^{p-1} = x^{2m}$ is

$$\sum_{a+b=m} \binom{m}{a} (-\beta_1)^{m-a} \binom{m}{b} (-\beta_2)^{m-b} = (-1)^m \sum_{a=0}^{m} \binom{m}{a}^2 \beta_1^{m-a} \beta_2^a = (-1)^m\, \widetilde{H}_p(\beta_2, \beta_1),$$

which is $(-1)^m \beta_1^m H_p(\beta_2/\beta_1)$. □

[2] That lemma carries no `\label` in the source and so has no entry in its `.aux`; since [11] runs one counter through all its theorem environments and its neighbours are Proposition 3.1, Corollary 3.2 and Algorithm 3.4, it prints as Lemma 3.3. Equation (3.3) inverts $(s, t) \mapsto (\lambda_1, \lambda_3)$, and we checked exhaustively over $\mathbb{F}_p$ for $p \in \{11, 13, 17, 19, 23\}$ that the two maps are mutually inverse on admissible pairs.

The lemma is used only to identify our genus-5 test with Step 2 of Algorithm 4.2; the formal statements use $\widetilde{H}_p(\beta_2, \beta_1) = 0$ as the definition. As a check, the two tests were also compared numerically (a Legendre-form j-invariant test against $\widetilde{H}_p$) at every prime $7 \le p \le 157$, with agreement at every pair.

2.4. **The reading.** Putting the quoted statements together:

- $X_{s,t}$ is superspecial $\iff$ E_1, E_3, E_4 are supersingular ([11], Proposition 3.1) $\iff$ $H_p(\lambda_1) = H_p(\lambda_3) = H_p(\lambda_4) = 0$ [13, V.4.1(b)];
- $Y_{s,t}$ is superspecial $\iff$ E_1, E_2, E_3 are supersingular ([11], Proposition 4.1) $\iff$ $h_p(s^2) = h_p(t^2) = 0$ and $\widetilde{H}_p(t^2, s^2) = 0$: the first two conditions are the sentence [11] draws from [4, Prop. 1.9] just after its (4.3), since $J(C_i)$ is isogenous to E_i^2; the third is Lemma 2.3;
- $Z_{s,t}$ is superspecial $\iff$ $g_p(s^6) = g_p(t^6) = g_p(s^6/t^6) = 0$ ([11], Proposition 5.2 and the sentence following (5.2), with [4, Prop. 1.8, 1.10]).

Hence, *reading through these equivalences*, $N_g(p) = 0$ says exactly that the genus-g family has no superspecial member in characteristic p, and $N_g(p)$ counts the ordered parameter pairs — (λ_1, λ_3), (s^2, t^2), (s^6, t^6) — of superspecial members. One point needs care: our root sets are taken in $\mathbb{F}_{p^2}$, whereas the parameters s, t range over $\overline{\mathbb{F}}_p$. The sweeps are nevertheless exhaustive, for two independent reasons. [11] itself proves or cites that the relevant parameters lie in $\mathbb{F}_{p^2}$: $\mathcal{T}_4 \subset \mathbb{F}_{p^2}$ by Auer–Top [2, Proposition 2.2], $s, t \in \mathbb{F}_{p^2}$ for superspecial $Y_{s,t}$ by [10, Main Theorem A], and $s, t \in \mathbb{F}_{p^2}$ for superspecial $Z_{s,t}$ by Lemma 5.1 of [11]. Independently, at every prime we treat, the number of distinct roots found in $\mathbb{F}_{p^2}$ equals the degree of the polynomial (Proposition 3.3 and the small-p statements), so each polynomial splits completely over $\mathbb{F}_{p^2}$ and the root set computed there is its full root set in $\overline{\mathbb{F}}_p$.

3. The model, the reproduced record, and the controls

The results of this section are the published facts the rest of the paper stands on, reproduced from the definitions and certified, together with the controls without which an exhaustive search proves nothing; the counts appearing in the controls are, like those of Section 6, values the preprint does not print. Their statements in the proof assistant are listed in Appendix A.

3.1. **The model.**

Proposition 3.1. (a) *For every p and every $n \in \mathbb{Z}/p\mathbb{Z}$, the addition and multiplication of §2.1 on $(\mathbb{Z}/p\mathbb{Z})^2$ are commutative and associative, multiplication distributes over addition, and $(0,0)$, $(1,0)$ are the units.*

(b) *2 is a quadratic non-residue modulo 11, 13 and 19; 3 is one modulo 7 and 17; and the least non-residue is $3, 2, 2, 3, 2$ at $p = 7, 11, 13, 17, 19$.*

(c) *With $p = 13$ and $n = 2$, every one of the 168 non-zero elements has a multiplicative inverse.*

(d) *With $p = 13$ and $n = 3$ instead ($3 = 4^2$ is a square modulo 13), exactly 24 non-zero elements have no inverse.*

Proof. (a) is a polynomial identity in the components and is proved by `ring`, for all p and n at once; (b)–(d) are finite checks evaluated by the kernel. (d) is the negative control that the non-residue hypothesis is not idle: $3 = 4^2$ in $\mathbb{F}_{13}$, so $w^2 - 3 = (w-4)(w+4)$, and the 24 elements are the zero divisors $a(4 \pm w)$, $a \neq 0$. □

3.2. **The three polynomials at $p = 13$.**

Proposition 3.2. (a) $H_{13}(\lambda) = 1 + 10\lambda + 4\lambda^2 + 10\lambda^3 + 4\lambda^4 + 10\lambda^5 + \lambda^6$ *over* $\mathbb{F}_{13}$, *and* $|\mathcal{T}_4(13)| = 6 = (13-1)/2$.

(b) $h_{13}(\beta) = 7 + 12\beta + 12\beta^2 + 7\beta^3$, *and* $\mathcal{T}_5(13) = \{8 + 5w,\ 8 + 8w,\ 12\}$ *in* $\mathbb{F}_{13}[w]/(w^2 - 2)$; *so* $|\mathcal{T}_5(13)| = 3 = \lfloor 13/4 \rfloor = \deg h_{13}$.

(c) $g_{13}(\alpha) = 2 + 3\alpha + 4\alpha^2 + 3\alpha^3 + 2\alpha^4$, *and* $\mathcal{T}_6(13) = \{5,\ 8,\ 9 + w,\ 9 + 12w\}$; *so* $|\mathcal{T}_6(13)| = 4 = \lfloor 13/3 \rfloor = \deg g_{13}$, *and g_{13} splits completely over* $\mathbb{F}_{13^2}$.

Proof. Kernel evaluation of the definitions; the coefficient lists are computed from the binomial formulas of Definition 2.1. For (c) by hand: g_{13} is palindromic, and with $u = \alpha + \alpha^{-1}$ one has $g_{13}(\alpha) = 2\alpha^2\, u\,(u+8)$; $u = 0$ gives $\alpha^2 = -1$, $\alpha \in \{5, 8\}$, and $u = 5$ gives $\alpha^2 - 5\alpha + 1 = 0$ with discriminant $21 \equiv 8$, a non-residue, hence the conjugate pair $9 \pm w$. □

3.3. **Cardinalities over the whole range.**

Proposition 3.3. *For every prime $7 \le p \le 157$: $|\mathcal{T}_5(p)| = \lfloor p/4 \rfloor$ and $|\mathcal{T}_6(p)| = \lfloor p/3 \rfloor$, and the coefficient lists of h_p and g_p have lengths $\lfloor p/4 \rfloor + 1$ and $\lfloor p/3 \rfloor + 1$. For every prime $7 \le p \le 113$: $|\mathcal{T}_4(p)| = (p-1)/2$ and the coefficient list of H_p has length $(p-1)/2 + 1$.*

Proof. Three sweeps by compiled evaluation. The leading coefficients are non-zero modulo p (§2.2), so the list lengths are the degrees plus one, and the count of distinct roots in $\mathbb{F}_{p^2}$ equals the degree in each case. □

These are the cardinalities [11] quotes from Silverman and from [4, Proposition 1.14]; as noted in §2.2, both citations supply simplicity of the roots only, and the degree supplies the rest.

3.4. **Genus 4.**

Proposition 3.4. *$N_4(7) = N_4(13) = N_4(19) = 0$; moreover $|\mathcal{T}_4(7)| = 3$ and $|\mathcal{T}_4(19)| = 9$.*

Proposition 3.5 (controls)**.** *$|\mathcal{T}_4(11)| = 5$ and $N_4(11) = 8$. At $p = 11$ the four conditions $c_i \neq 0$ reject exactly 5 of the 25 ordered pairs $(\lambda_1, \lambda_3) \in \mathcal{T}_4(11)^2$.*

Both are kernel evaluations. Reading through §2.4: the genus-4 family has no superspecial member at $p = 7$, 13, 19 — 13 and 19 are two of the three exceptions of Theorem 1.1 of [11], whose Section 6.1 says its "algorithm failed to output a superspecial genus-4 curve for $p \in \{13, 19, 73\}$", and at $p = 7$ no superspecial genus-4 curve exists at all by Kudo–Harashita [5] — while at $p = 11$ it has eight members counted by (λ_1, λ_3). The second half of Proposition 3.5 shows that the conditions (3.2) are not carried along inertly (the five rejected pairs are the diagonal $\lambda_1 = \lambda_3$).

3.5. **Genus 5.**

Proposition 3.6. *$N_5(13) = 0$, and $N_5(7) = N_5(11) = N_5(17) = N_5(19) = 0$.*

Proposition 3.7 (controls)**.** *$|\mathcal{T}_5(23)| = 5$ and $N_5(23) = 6$; $|\mathcal{T}_5(37)| = 9$ and $N_5(37) = 0$.*

Kernel evaluations, with the test of Definition 2.2 (Lemma 2.3). Reading: the genus-5 family is empty at $p = 13$ — the preprint's own open cell $(5, 13)$, where Section 6.2 of [11] says "For the remaining primes p (except for $p = 13$), we individually constructed superspecial generalized Howe curves of genus 5" — and at the four primes $7, 11, 17, 19$ below the range of its Theorem 6.3, for which its Appendix A supplies curves by a different construction. It is not always empty ($p = 23$), and 19 is not the last failure ($p = 37$, the first exception of Theorem 6.3).

3.6. **Genus 6.**

Proposition 3.8. *$g_7(\alpha) = 3 + 2\alpha + 3\alpha^2$, $|\mathcal{T}_6(7)| = 2$ and $N_6(7) = 0$; $|\mathcal{T}_6(11)| = 3$ and $N_6(11) = 0$.*

Proposition 3.9 (controls)**.** *At $p = 17$ (with $n = 3$): $4, 13, 16 \in \mathcal{T}_6(17)$, $13 \cdot 16 = 4$ in $\mathbb{F}_{17}$, and $N_6(17) = 6$. At $p = 19$: $|\mathcal{T}_6(19)| = 6$ and $N_6(19) = 0$.*

Kernel evaluations. Reading: the genus-6 family is empty at $p = 7$ — the preprint's other open cell, $(6, 7)$ — and at $p = 11$, the prime below the range of Theorem 6.4 that Appendix B of [11] supplies; it is not always empty ($p = 17$, with the explicit witness $(\alpha_1, \alpha_2) = (4, 13)$, $\alpha_1/\alpha_2 = 16$); and 13, the subject of the next section, is not the last failure ($p = 19$, the first exception of Theorem 6.4).

Remark 3.10. Propositions 3.6 and 3.8 say that the two cells the preprint declares open cannot be closed by the preprint's own families. They say nothing about curves outside those families.

4. The cell $(g, p) = (6, 13)$

Theorem 6.4 of [11] (compiled e-print, p. 11) reads, verbatim:

> For every prime p with $11 < p < 10^5$ and
>
> $$p \neq 19, 37, 43, 61, 67, 79, 97, 109, 127, 151, 157, 223, 229, 283, 313, 331, 337, 373, 571,$$
>
> there exists a superspecial curve $Z_{s,t}$ of genus 6 in characteristic p.

The prime 13 satisfies $11 < 13 < 10^5$ and is not in the list. Appendix B of [11] (p. 14) states its own scope verbatim as "examples of superspecial generalized Howe curves of genus 6 for characteristic p with $p \in \{11, 19, 37, 43, 61, 67, 79, 97, 109, 127, 151, 157, 223, 229, 283, 313, 331, 337, 373, 571\}$"; 13 is absent there too. Theorem 6.4 and Appendix B are between them the whole of the preprint's genus-6 argument: its §6.3 says, of the primes Theorem 6.4 leaves out, "For the remaining primes p with $p > 7$, we individually constructed superspecial generalized Howe curves of genus 6", and those constructions are Appendix B's list. So the only support in the preprint for existence at $p = 13$ — for Theorem 1.3 and for the circle at $(6, 13)$ in Table 1 — is Theorem 6.4.

Theorem 4.1. *Let $\mathcal{T} = \mathcal{T}_6(13) = \{5, 8, 9 + w, 9 + 12w\} \subset \mathbb{F}_{13}[w]/(w^2 - 2)$.*

(a) *There are no $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{T}$ with $\alpha_1 \neq \alpha_2$ and $\alpha_2\alpha_3 = \alpha_1$. Equivalently, no two distinct roots of g_{13} have a quotient that is again a root.*
(b) $N_6(13) = 0$.
(c) *The search in (a) is not vacuous: $\mathcal{T}^2$ contains exactly 12 ordered pairs with distinct entries, so the quantifier in (a) ranges over $12 \cdot |\mathcal{T}| = 48$ triples.*

Proof. All three are kernel evaluations over the four-element set of Proposition 3.2(c); they depend on no axiom beyond `propext` and `Quot.sound`. By hand: $5 \cdot 8 = 40 \equiv 1$, so $5/8 = 8/5 = 12 \notin \mathcal{T}$; and for the conjugate pair $r = 9 + w$, $\bar{r} = 9 + 12w = 9 - w$ one has $r\bar{r} = 81 - 2 = 79 \equiv 1$, so $\bar{r} = r^{-1}$, $r/\bar{r} = r^2 = 5r - 1 \notin \mathbb{F}_{13}$ and $r^2 \neq r, r^{-1}$, while $5/r = 5\bar{r}$, $8/r = 8\bar{r}$, $r/5 = 8r$, $r/8 = 5r$ are the elements $6 + 8w$, $7 + 5w$, $7 + 8w$, $6 + 5w$, none of which is a root. The search is exhaustive because g_{13} splits completely over $\mathbb{F}_{13^2}$ (Proposition 3.2(c)), and independently by Lemma 5.1 of [11]. □

Corollary 4.2 (reading)**.** *No member of the genus-6 family $Z_{s,t}$ of* [11] *is superspecial in characteristic* 13*. Consequently Theorem 6.4 of* [11]*, as printed, is false at $p = 13$. Theorem 1.3 of* [11] *and the circle at* $(6, 13)$ *in its Table 1 are then unsupported by anything in the preprint, and* $(6, 13)$ *is a third cell, beside* $(5, 13)$ *and* $(6, 7)$*, in which the preprint does not settle existence. We do not claim the rest of the exception list is wrong: the author's logs record a failure at exactly the printed primes together with* 7*,* 11 *and* 13 *(Remark 4.3), so what his computation supports is the printed list with* 13 *added; but that is a reading of his log files, whereas what is certified here is the range $7 \leq p \leq 157$.*

Proof. Theorem 4.1 and the reading of §2.4 (Proposition 5.2 of [11] with [4, Prop. 1.8, 1.10]). □

The author's own computation. The Magma implementation of [11] and its complete per-prime logs are public [12]. The genus-6 driver (`g=6/main.m`, lines 17–19) runs `FindSSpGenus6Howe` first over $\mathbb{F}_p$, assigns the result to a flag, and on failure runs it again over $\mathbb{F}_{p^2}$ as a bare expression, whose value Magma prints; a block therefore contains a lone line `false` exactly when both passes failed. The file `g=6/00007-10000.log`, lines 11–14, reads verbatim:

```
In characteristic p = 13.
Time: 0.000
false
Time: 0.000
```

So the author's own search found no superspecial $Z_{s,t}$ at $p = 13$, in agreement with Theorem 4.1, and the omission of 13 from the exception list of Theorem 6.4 is a transcription slip, not a disagreement about the computation. All file and line references to [12] are to commit `f44b8cd627e866d189ef7688b7c5e5acf7cad703` (17 May 2026), the head of its `main` branch on 7 September 2026.

Remark 4.3 (a computation outside the formal development). Parsing every block of the logs of [12] — 39 231 primes for genus 4, 8 665 for genus 5, 9 589 for genus 6 — gives the sets of primes at which both passes print `false`:

genus 4 : $\{7, 13, 19, 73\}$,

genus 5 : $\{7, 11, 13, 17, 19, 37, 53, 89, 97, 101, 137\}$,

genus 6 : $\{7, 11, 13, 19, 37, 43, 61, 67, 79, 97, 109, 127, 151, 157, 223, 229, 283, 313, 331, 337, 373, 571\}$.

The genus-4 set is the exception list of Theorem 1.1 plus 7; the genus-5 set is the exception list of Theorem 6.3 plus the primes $7, 11, 13, 17, 19$ below its range; the genus-6 set is the exception list of Theorem 6.4 plus 7, 11 *and* 13. The first two agree with the preprint exactly; in the third, 7 and 11 are outside the range of Theorem 6.4 (11 being covered by Appendix B), and 13 is the slip. These sets are parsed from text files and are not part of the formal development; what is certified is Theorem 6.1 below, which reproduces the three sets on $7 \le p \le 157$ (genus 4: ≤ 113) from the criterion itself.

One observation about the genus-6 logs, which does not touch the `false` lines used above. Where a block prints a witness, the printed pair is a pair of roots of g_p — an $(\alpha_1, \alpha_2) = (s^6, t^6)$ pair in the sense of Algorithm 5.3 — and not the pair (s^3, t^3) that the committed `g=6/main.m` returns, a solution of equation (5.3) of [11] for a supersingular j, which is also what the repository's README describes as the genus-6 output. At $p = 17$ the log prints `[ 4, 16 ]`: both entries lie in $\mathcal{T}_6(17)$ and $4/16 = 13$ does too, whereas a re-implementation of the committed driver returns $(s^3, t^3) = (2, 4)$, whose squares are 4 and 16 — and 16 solves (5.3) over $\mathbb{F}_{17}$ for neither of the two supersingular j-invariants there, $j = 0$ and $j = 8$. At each of $p = 17$, 29, 41, 53, 59, 71, 83 we checked that both printed entries lie in $\mathcal{T}_6(p)$ and that the printed pair passes the test of Definition 2.2. Logs and committed driver therefore differ in output convention, not in what was searched.

Remark 4.4. Nothing in this section shows that no superspecial curve of genus 6 exists in characteristic 13. Settling the cell would require a search over all genus-6 curves in characteristic 13, not over a two-parameter family, and is not attempted here.

5. The genus-6 count is a solution count of $xyz = 1$

Remark 5.1 (inversion-closure). Each of H_p, h_p, g_p is palindromic. For H_p this is $\binom{m}{i} = \binom{m}{m-i}$. For g_p, with $a = \lfloor (p+1)/6 \rfloor$ and $d = \lfloor p/3 \rfloor$ one has $a + d = m$ (both residues of p modulo 6), so the coefficient of α^{d-i} is $\binom{m}{a+d-i}\binom{m}{d-i} = \binom{m}{m-i}\binom{m}{a+i}$, the coefficient of α^i; for h_p the same holds with $a = \lfloor (p+1)/4 \rfloor$, $d = \lfloor p/4 \rfloor$, $a + d = m$. Hence $\alpha \neq 0$ is a root if and only if α^{-1} is, and each of $\mathcal{T}_4(p)$, $\mathcal{T}_5(p)$, $\mathcal{T}_6(p)$ is closed under inversion. For $\mathcal{T}_6$ and $\mathcal{T}_5$ this is also the geometric statement of [4, Lemma 1.5, p. 133]: C_α is isomorphic to $C_{\alpha'}$ if and only if $\alpha = \alpha'$ or $\alpha = 1/\alpha'$ (and likewise for C_β), so that supersingularity, an isomorphism invariant, is shared by α and α^{-1}. The argument from palindromicity is ours, and is what the formal statements use: it needs no geometry.

Proposition 5.2 (proved here; checked prime by prime in the formal development)**.** *For every prime $p > 5$,*

$$N_6(p) = \#\{(x, y, z) \in \mathcal{T}_6(p)^3 : xyz = 1\}.$$

Proof. Write $\mathcal{T} = \mathcal{T}_6(p)$; it is closed under inversion (Remark 5.1) and $1 \notin \mathcal{T}$ by definition. Send a passing pair (α_1, α_2) to $(\alpha_1, \alpha_2^{-1}, \alpha_2/\alpha_1)$: all three entries lie in $\mathcal{T}$ (α_2/α_1 because $\alpha_1/\alpha_2 \in \mathcal{T}$ and $\mathcal{T}$ is inversion-closed) and their product is 1. Send a solution (x, y, z) back to (x, y^{-1}): $y^{-1} \in \mathcal{T}$; $x \neq y^{-1}$, since $x = y^{-1}$ would force $z = (xy)^{-1} = 1 \notin \mathcal{T}$; and $x/y^{-1} = xy = z^{-1} \in \mathcal{T}$, so the pair passes. The two maps are mutually inverse. □

The right-hand side is invariant under the symmetric group S_3 permuting (x, y, z) and under simultaneous inversion $(x, y, z) \mapsto (x^{-1}, y^{-1}, z^{-1})$, which commute; a group of order 12 acts on the solution set. Neither the left-hand side nor Algorithm 5.3 of [11] — a double loop over $\mathcal{T}^2$ with a membership test — displays this symmetry. The action is not free: at $p = 17$ the triple $(4, 4, 16)$ is a solution ($4 \cdot 4 \cdot 16 = 256 \equiv 1$) whose S_3-orbit has three elements, paired by inversion with $(13, 13, 16)$.

Theorem 5.3. *For every prime $7 \le p \le 157$, $N_6(p) = \#\{(x,y,z) \in \mathcal{T}_6(p)^3 : xyz = 1\}$ and $6 \mid N_6(p)$.*

Proof. For the eight primes $7 \le p \le 31$ both statements are evaluated by the kernel; for all 34 primes $7 \le p \le 157$ they are evaluated by compiled code. The identity is also Proposition 5.2; the divisibility is a checked fact only. □

We do not claim $6 \mid N_6(p)$ for all p. It would follow from an orbit count if every orbit of the order-12 action had size divisible by 6; the example above shows that orbits of size 6 occur, and ruling out sizes $1, 2, 3, 4$ in general is not attempted here.

Theorem 5.4. (a) *For every prime $7 \le p \le 31$, each of $\mathcal{T}_4(p)$, $\mathcal{T}_5(p)$, $\mathcal{T}_6(p)$ is closed under inversion, in the division-free form: every element x of the set has a partner y in the set with $xy = 1$. In particular $\mathcal{T}_6(13)$ is, with $5 \cdot 8 = 1$ and $(9+w)(9+12w) = 1$.*

(b) *For every prime $7 \le p \le 157$, $2 \mid N_5(p)$.*

Proof. (a) by the kernel; (b) by compiled evaluation. (b) has a general proof: $\widetilde{H}_p(u,v) = \widetilde{H}_p(v,u)$ since $\binom{m}{i}^2 = \binom{m}{m-i}^2$, so (β_1, β_2) passes the genus-5 test if and only if (β_2, β_1) does, and the swap has no fixed passing pair because $\beta_1 \ne \beta_2$ is required. As with $6 \mid N_6$, the formal statement is the checked range. □

6. The certified tables

Theorem 6.1. (a) *For every prime $7 \le p \le 113$, $N_4(p)$ is as in Table 1. Its zero set is $\{7, 13, 19, 73\}$.*

(b) *For every prime $7 \le p \le 157$, $N_5(p)$ is as in Table 1. Its zero set is*

$$\{7, 11, 13, 17, 19, 37, 53, 89, 97, 101, 137\}.$$

(c) *For every prime $7 \le p \le 157$, $N_6(p)$ is as in Table 1. Its zero set is*

$$\{7, 11, 13, 19, 37, 43, 61, 67, 79, 97, 109, 127, 151, 157\}.$$

Proof. Three sweeps by compiled evaluation, one module each, of the counts of Definition 2.2 with the root sets of Definition 2.1; the coefficient list and the root set are computed once per prime and passed to the pair loop. Each sweep is exhaustive by Proposition 3.3. □

Table 1. The certified counts $N_4(p)$ $(7 \le p \le 113)$, $N_5(p)$ and $N_6(p)$ $(7 \le p \le 157)$; a dash means outside the certified range.

p	7	11	13	17	19	23	29	31	37	41	43	47
N_4	0	8	0	8	0	32	26	36	12	56	12	80
N_5	0	0	0	0	0	6	8	4	0	4	8	24
N_6	0	0	0	6	0	6	6	24	0	30	0	24
p	53	59	61	67	71	73	79	83	89	97	101	103
N_4	38	110	30	24	242	0	54	110	122	36	224	24
N_5	0	16	16	16	32	16	10	24	0	0	0	34
N_6	12	30	0	0	48	24	0	42	36	0	48	24
p	107	109	113	127	131	137	139	149	151	157		
N_4	116	84	116	–	–	–	–	–	–	–		
N_5	32	16	16	40	36	0	12	8	60	8		
N_6	24	0	60	0	72	6	24	18	0	0		

Against the preprint: the zero set of N_4 on $7 \le p \le 113$ is the exception list $\{13, 19, 73\}$ of Theorem 1.1 of [11] together with 7 (below its range); the zero set of N_5 on $7 \le p \le 157$ is the *complete* exception list $\{37, 53, 89, 97, 101, 137\}$ of Theorem 6.3 together with every prime below its range $19 < p$, so the certified range covers the whole of that list; and the zero set of N_6 on $7 \le p \le 157$ is the initial segment

$\{19, 37, 43, 61, 67, 79, 97, 109, 127, 151, 157\}$ of the exception list of Theorem 6.4, together with 7 and 11 below its range, and 13 (Section 4). The remaining exceptions $223, \dots, 571$ of Theorem 6.4 lie outside the certified range.

The counts themselves are new data: [11] prints no count, its logs print at most one witness per prime (Remark 4.3), and none of the three sequences is in the OEIS (searched 7 September 2026, by the full lists, by sub-runs of them and by keyword; no entry of the OEIS matches even a five-term run of any of the three). Reading through §2.4, $N_g(p)$ is the number of superspecial members of the genus-g family counted by ordered parameter pairs; note that each count is at least the number of members up to the obvious relabellings, and that in genus 6 the parameters (s^6, t^6) identify 36 pairs (s, t) at once.

7. What is not settled, and its price

(1) The genus-6 table stops at 157. A sweep costs $\Theta(p^3)$ field operations (a p^2-element root search against a degree-$\lfloor p/3 \rfloor$ polynomial); the eight remaining exceptions of Theorem 6.4, namely 223, 229, 283, 313, 331, 337, 373 and 571, have $\sum p^3 \approx 3.9 \cdot 10^8$ against $3.1 \cdot 10^7$ for the whole table to 157, which took about four minutes of compiled evaluation, so certifying them is affordable and is left for a sequel; every prime to 571 is not.

(2) Proposition 5.2 is proved on paper for all p but checked in the proof assistant only for $p \le 157$; a general formal proof is a bijection argument on finite lists and is not compute-bound. Whether $6 \mid N_6(p)$ for all p is open; an orbit count on the order-12 action would need to exclude orbits of size 1, 2, 3, 4.

(3) The cells $(5, 13)$, $(6, 7)$ and now $(6, 13)$: the families of [11] are empty there (Propositions 3.6, 3.8, Theorem 4.1); closing any of them needs a search beyond the families.

8. Verification

Every numbered statement of Sections 3–6 except Corollary 4.2, Proposition 5.2 and the remarks — and, in Section 2, except Lemma 2.3 — is checked in Lean 4 (toolchain v4.32.0) with Mathlib [7, 8]; the statements are reproduced verbatim in Appendix A. The development is eight modules and 49 theorem declarations (one module of definitions with one theorem, then 16, 10, 11, 5, 2, 2, 2). The field $\mathbb{F}_{p^2}$ is the hand-built model of §2.1 on `ZMod` $p \times$ `ZMod` p, chosen because Mathlib's `GaloisField` does not reduce inside the kernel; its ring axioms are proved by `ring` for all p and n (Proposition 3.1(a)). Two tactics discharge the finite statements. Kernel evaluation, `decide +kernel`, is used for every statement at a single prime $p \le 37$ and for the $p \le 31$ halves of Theorems 5.3 and 5.4; these depend on the axioms `propext` and `Quot.sound` only, and in particular every statement about $p = 13$ — Proposition 3.2, Theorem 4.1 — is kernel-checked with no native evaluation. Compiled evaluation, `native_decide`, is used for the eight sweeps over all primes to 157 (Proposition 3.3 and Theorems 5.3, 5.4(b), 6.1), each of which records its own native-evaluation axiom; these sweeps require `set_option maxHeartbeats 0`, and the three table sweeps are kept in separate modules so that each is re-checkable on its own. No declaration uses `Classical.choice` or `sorry`. The lemma

$$\texttt{fastChoose}\ n\ k = \binom{n}{k} \quad \text{for all } n, k, \qquad \text{where}$$

$$\texttt{fastChoose}\ n\ 0 = 1, \qquad \texttt{fastChoose}\ n\ (k+1) = \left\lfloor \frac{\texttt{fastChoose}\ n\ k \cdot (n-k)}{k+1} \right\rfloor,$$

is proved from Mathlib's `Nat.choose_succ_right_eq` and is what makes the coefficient lists evaluable: Lean core's `Nat.choose` is the unmemoised Pascal recursion, costing $\Theta(\binom{n}{k})$ additions, and $\binom{78}{39} \approx 10^{22}$ (the Deuring polynomial at $p = 157$) is out of reach of kernel and interpreter alike — a first sweep built on it did not finish in eight minutes, and finished in 243 s after the substitution. Measured cost of the whole development, on one core: about 1.3 CPU-hours in total, the three table modules taking 187–243 s each and the symmetry module 617 s, with a peak resident set of 10.4 GB (of which 6.6–6.9 GB is the baseline of importing Mathlib). Independently of the formal development, all counts were first computed by a pure-Python re-implementation of the criteria and, for genus 6 at $p \le 71$, by a

re-implementation of the j-invariant route of Algorithm 5.4 of [11], with agreement on the zero/non-zero pattern at every prime. Repository reference to be added at submission.

Appendix A. The formal statements

The Lean statements corresponding to the results above, verbatim (statements only; proofs, docstrings and attributes omitted), preceded by the definitions they use. `Fq p` is the pair model of $\mathbb{F}_{p^2}$ of §2.1 with the non-residue `n` passed to `fmul`; `elems p` lists its p^2 elements; `homEval n cs u v` is $\sum_i c_i u^i v^{m-i}$ for the coefficient list `cs` and `polyEval` the plain evaluation; `T4`, `T5`, `T6` are $\mathcal{T}_4$, $\mathcal{T}_5$, $\mathcal{T}_6$; `genus4Hit`, `genus5Hit`, `genus6Hit` are the three tests of Definition 2.2; `genus`g`Pairs` lists the passing ordered pairs and `N4`, `N5`, `N6` are their lengths; `unitTriples p n` is $\#\{(x,y,z) \in \mathcal{T}_6^3 : xyz = 1\}$. An element $a + bw$ is the pair `(a, b)`. Natural-number subtraction and division in `fastChoose` are Lean's truncated operations. The correspondence with the text: Proposition 3.1 is `Model.lean`; Proposition 3.2 is `deuring_13`, `ikoH_13`, `ikoG_13`, `T6_13_eq`, `T6_13_card`; Theorem 4.1 is `no_superspecial_genus6_at_13`, `N6_13`, `sweep_13_nonvacuous`; Propositions 3.4–3.9 are the remaining statements of `Genus45.lean` and `Genus6.lean`; Theorems 5.3 and 5.4 are `Symmetry.lean`; Proposition 3.3 is the three `genus`g`_root_count` and Theorem 6.1 the three `genus`g`_table`.

`Criterion.lean (definitions)`

```
abbrev Fq (p : ℕ) := ZMod p × ZMod p
def fzero (p : ℕ) : Fq p := (0, 0)
def fone (p : ℕ) : Fq p := (1, 0)
def fadd {p : ℕ} (x y : Fq p) : Fq p := (x.1 + y.1, x.2 + y.2)
def fsub {p : ℕ} (x y : Fq p) : Fq p := (x.1 - y.1, x.2 - y.2)
def fmul {p : ℕ} (n : ZMod p) (x y : Fq p) : Fq p :=
  (x.1 * y.1 + n * (x.2 * y.2), x.1 * y.2 + x.2 * y.1)
def fnat {p : ℕ} (k : ℕ) : Fq p := ((k : ZMod p), 0)
def elems (p : ℕ) : List (Fq p) :=
  (List.range p).flatMap fun a => (List.range p).map fun b => ((a : ZMod p), (b : ZMod p))
def isNonResidue (p : ℕ) (n : ZMod p) : Bool :=
  (List.range p).all fun a => ((a : ZMod p) * (a : ZMod p)) != n
def leastNR (p : ℕ) : ZMod p :=
  ((((List.range p).drop 2).find? fun n : ℕ => isNonResidue p (n : ZMod p)).getD 0 : ℕ)
def homEval {p : ℕ} (n : ZMod p) (cs : List (ZMod p)) (u v : Fq p) : Fq p :=
  (cs.foldl (fun st c => (fadd (fmul n st.1 v) (fmul n ((c : ZMod p), 0) st.2), fmul n st.2 u))
    ((fzero p, fone p) : Fq p × Fq p)).1
def polyEval {p : ℕ} (n : ZMod p) (cs : List (ZMod p)) (x : Fq p) : Fq p :=
  cs.foldr (fun c acc => fadd (fmul n acc x) ((c, 0) : Fq p)) (fzero p)
def fastChoose (n : ℕ) : ℕ → ℕ
  | 0 => 1
  | k + 1 => fastChoose n k * (n - k) / (k + 1)
def deuringCoeffs (p : ℕ) : List (ZMod p) :=
  (List.range ((p - 1) / 2 + 1)).map fun i => ((fastChoose ((p - 1) / 2) i ^ 2 : ℕ) : ZMod p)
def ikoHCoeffs (p : ℕ) : List (ZMod p) :=
  (List.range (p / 4 + 1)).map fun i =>
    ((fastChoose ((p - 1) / 2) ((p + 1) / 4 + i) * fastChoose ((p - 1) / 2) i : ℕ) : ZMod p)
def ikoGCoeffs (p : ℕ) : List (ZMod p) :=
  (List.range (p / 3 + 1)).map fun i =>
    ((fastChoose ((p - 1) / 2) ((p + 1) / 6 + i) * fastChoose ((p - 1) / 2) i : ℕ) : ZMod p)
def rootSet (p : ℕ) (n : ZMod p) (cs : List (ZMod p)) : List (Fq p) :=
  (elems p).filter fun x => polyEval n cs x == fzero p && x != fzero p && x != fone p
def T4 (p : ℕ) (n : ZMod p) : List (Fq p) := rootSet p n (deuringCoeffs p)
def T5 (p : ℕ) (n : ZMod p) : List (Fq p) := rootSet p n (ikoHCoeffs p)
def T6 (p : ℕ) (n : ZMod p) : List (Fq p) := rootSet p n (ikoGCoeffs p)
def genus4Hit (p : ℕ) (n : ZMod p) (cs : List (ZMod p)) (l1 l3 : Fq p) : Bool :=
  let two : Fq p := fnat 2
  let l1sq := fmul n l1 l1
  let c1 := fsub l1 l3
  let c2 := fsub l1sq l3
  let c3 := fadd (fsub l1sq (fmul n two l1)) l3
  let c4 := fsub (fsub (fmul n two (fmul n l1 l3)) l1sq) l3
  c1 != fzero p && c2 != fzero p && c3 != fzero p && c4 != fzero p &&
    homEval n cs (fmul n l3 (fmul n c3 c3)) (fmul n c4 c4) == fzero p
def genus5Hit (p : ℕ) (n : ZMod p) (cs : List (ZMod p)) (b1 b2 : Fq p) : Bool :=
  b1 != b2 && homEval n cs b2 b1 == fzero p
def genus6Hit (p : ℕ) (n : ZMod p) (T : List (Fq p)) (a1 a2 : Fq p) : Bool :=
  a1 != a2 && T.any fun a3 => fmul n a2 a3 == a1
def genus4Pairs (p : ℕ) (n : ZMod p) : List (Fq p × Fq p) :=
  let cs := deuringCoeffs p
  let T := rootSet p n cs
```

```
  (T.flatMap fun l1 => T.map fun l3 => (l1, l3)).filter fun q => genus4Hit p n cs q.1 q.2
def genus5Pairs (p : ℕ) (n : ZMod p) : List (Fq p × Fq p) :=
  let cs := deuringCoeffs p
  let T := rootSet p n (ikoHCoeffs p)
  (T.flatMap fun b1 => T.map fun b2 => (b1, b2)).filter fun q => genus5Hit p n cs q.1 q.2
def genus6Pairs (p : ℕ) (n : ZMod p) : List (Fq p × Fq p) :=
  let T := rootSet p n (ikoGCoeffs p)
  (T.flatMap fun a1 => T.map fun a2 => (a1, a2)).filter fun q => genus6Hit p n T q.1 q.2
def N4 (p : ℕ) (n : ZMod p) : ℕ := (genus4Pairs p n).length
def N5 (p : ℕ) (n : ZMod p) : ℕ := (genus5Pairs p n).length
def N6 (p : ℕ) (n : ZMod p) : ℕ := (genus6Pairs p n).length
```

Criterion.lean

```
theorem fastChoose_eq (n : ℕ) : ∀ k, fastChoose n k = Nat.choose n k
```

Model.lean

```
theorem elems_card_13 : (elems 13).length = 169 ∧ (elems 13).Nodup :=
theorem nonResidue_13 : isNonResidue 13 2 = true :=
theorem nonResidue_7 : isNonResidue 7 3 = true :=
theorem nonResidue_11 : isNonResidue 11 2 = true :=
theorem nonResidue_17 : isNonResidue 17 3 = true :=
theorem nonResidue_19 : isNonResidue 19 2 = true :=
theorem leastNR_values :
    leastNR 7 = 3 ∧ leastNR 11 = 2 ∧ leastNR 13 = 2 ∧ leastNR 17 = 3 ∧ leastNR 19 = 2 :=
theorem nonResidue_13_negative : isNonResidue 13 3 = false :=
theorem fadd_comm {p : ℕ} (x y : Fq p) : fadd x y = fadd y x :=
theorem fadd_assoc {p : ℕ} (x y z : Fq p) : fadd (fadd x y) z = fadd x (fadd y z) :=
theorem fmul_comm {p : ℕ} (n : ZMod p) (x y : Fq p) : fmul n x y = fmul n y x :=
theorem fmul_assoc {p : ℕ} (n : ZMod p) (x y z : Fq p) :
    fmul n (fmul n x y) z = fmul n x (fmul n y z) :=
theorem fmul_fadd {p : ℕ} (n : ZMod p) (x y z : Fq p) :
    fmul n x (fadd y z) = fadd (fmul n x y) (fmul n x z) :=
theorem fmul_one {p : ℕ} (n : ZMod p) (x : Fq p) :
    fmul n x (fone p) = x ∧ fadd x (fzero p) = x :=
theorem fq13_field :
    ((elems 13).filter fun x => x != fzero 13 &&
      !((elems 13).any fun y => fmul 2 x y == fone 13)).length = 0 :=
theorem fq13_not_field_at_square :
    ((elems 13).filter fun x => x != fzero 13 &&
      !((elems 13).any fun y => fmul 2 x y == fone 13)).length = 0 ∧
    ((elems 13).filter fun x => x != fzero 13 &&
      !((elems 13).any fun y => fmul 3 x y == fone 13)).length = 24 :=
```

Genus6.lean

```
theorem ikoG_13 : ikoGCoeffs 13 = [2, 3, 4, 3, 2] :=
theorem T6_13_eq : T6 13 2 = [(5, 0), (8, 0), (9, 1), (9, 12)] :=
theorem T6_13_card : (T6 13 2).length = 4 ∧ (ikoGCoeffs 13).length = 5 :=
theorem no_superspecial_genus6_at_13 :
    ((T6 13 2).filter fun a => (T6 13 2).any fun b => (T6 13 2).any fun c =>
      a != b && fmul 2 b c == a).length = 0 :=
theorem N6_13 : genus6Pairs 13 2 = [] :=
theorem sweep_13_nonvacuous :
    (((T6 13 2).flatMap fun a => (T6 13 2).map fun b => (a, b)).filter
      fun q => q.1 != q.2).length = 12 :=
theorem no_superspecial_genus6_at_7 :
    ikoGCoeffs 7 = [3, 2, 3] ∧ (T6 7 3).length = 2 ∧ genus6Pairs 7 3 = [] :=
theorem no_superspecial_genus6_at_11 :
    (T6 11 2).length = 3 ∧ genus6Pairs 11 2 = [] :=
theorem superspecial_genus6_at_17 :
    ((4 : ZMod 17), (0 : ZMod 17)) ∈ T6 17 3 ∧
    ((13 : ZMod 17), (0 : ZMod 17)) ∈ T6 17 3 ∧
    ((16 : ZMod 17), (0 : ZMod 17)) ∈ T6 17 3 ∧
    fmul 3 ((13 : ZMod 17), (0 : ZMod 17)) ((16 : ZMod 17), (0 : ZMod 17))
      = ((4 : ZMod 17), (0 : ZMod 17)) ∧
    (genus6Pairs 17 3).length = 6 :=
theorem no_superspecial_genus6_at_19 :
    (T6 19 2).length = 6 ∧ genus6Pairs 19 2 = [] :=
```

Genus45.lean

```
theorem deuring_13 :
    deuringCoeffs 13 = [1, 10, 4, 10, 4, 10, 1] ∧ (T4 13 2).length = 6 :=
theorem no_superspecial_genus4_at_13 : genus4Pairs 13 2 = [] :=
theorem no_superspecial_genus4_at_19 :
    (T4 19 2).length = 9 ∧ genus4Pairs 19 2 = [] :=
theorem no_superspecial_genus4_at_7 :
    (T4 7 3).length = 3 ∧ genus4Pairs 7 3 = [] :=
```

```
theorem superspecial_genus4_at_11 :
    (T4 11 2).length = 5 ∧ (genus4Pairs 11 2).length = 8 :=
theorem genus4_conditions_nonvacuous :
    ((((T4 11 2).flatMap fun l1 => (T4 11 2).map fun l3 => (l1, l3)).filter fun q =>
      let l1sq := fmul 2 q.1 q.1
      !(fsub q.1 q.2 != fzero 11 && fsub l1sq q.2 != fzero 11 &&
        fadd (fsub l1sq (fmul 2 (fnat 2) q.1)) q.2 != fzero 11 &&
        fsub (fsub (fmul 2 (fnat 2) (fmul 2 q.1 q.2)) l1sq) q.2 != fzero 11)).length = 5) :=
theorem ikoH_13 :
    ikoHCoeffs 13 = [7, 12, 12, 7] ∧ T5 13 2 = [(8, 5), (8, 8), (12, 0)] :=
theorem no_superspecial_genus5_at_13 : genus5Pairs 13 2 = [] :=
theorem no_superspecial_genus5_small :
    genus5Pairs 7 3 = [] ∧ genus5Pairs 11 2 = [] ∧ genus5Pairs 17 3 = [] ∧
    genus5Pairs 19 2 = [] :=
theorem superspecial_genus5_at_23 :
    (T5 23 5).length = 5 ∧ (genus5Pairs 23 5).length = 6 :=
theorem no_superspecial_genus5_at_37 :
    (T5 37 2).length = 9 ∧ genus5Pairs 37 2 = [] :=
```

Symmetry.lean

```
def sweepPrimesSym : List ℕ :=
  [7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,
   101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157]
def unitTriples (p : ℕ) (n : ZMod p) : ℕ :=
  let T := T6 p n
  (T.flatMap fun x => T.flatMap fun y =>
    T.filter fun z => fmul n (fmul n x y) z == fone p).length
theorem T6_13_inv_closed :
    ((T6 13 2).all fun x => (T6 13 2).any fun y => fmul 2 x y == fone 13) = true :=
theorem rootSets_inv_closed_small :
    (([7, 11, 13, 17, 19, 23, 29, 31] : List ℕ).all fun p =>
      ((T4 p (leastNR p)).all fun x => (T4 p (leastNR p)).any fun y =>
        fmul (leastNR p) x y == fone p) &&
      ((T5 p (leastNR p)).all fun x => (T5 p (leastNR p)).any fun y =>
        fmul (leastNR p) x y == fone p) &&
      ((T6 p (leastNR p)).all fun x => (T6 p (leastNR p)).any fun y =>
        fmul (leastNR p) x y == fone p)) = true :=
theorem census_eq_unitTriples_small :
    (([7, 11, 13, 17, 19, 23, 29, 31] : List ℕ).all fun p =>
      (N6 p (leastNR p) == unitTriples p (leastNR p)) &&
      (N6 p (leastNR p) % 6 == 0)) = true :=
theorem census_eq_unitTriples :
    (sweepPrimesSym.all fun p =>
      (N6 p (leastNR p) == unitTriples p (leastNR p)) &&
      (N6 p (leastNR p) % 6 == 0)) = true :=
theorem genus5_even :
    (sweepPrimesSym.all fun p => N5 p (leastNR p) % 2 == 0) = true :=
```

TableGenus4.lean

```
def primes113 : List ℕ :=
  [7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,
   101, 103, 107, 109, 113]
theorem genus4_table :
    (primes113.map fun p => (p, N4 p (leastNR p))) =
      [(7, 0), (11, 8), (13, 0), (17, 8), (19, 0), (23, 32), (29, 26), (31, 36), (37, 12),
       (41, 56), (43, 12), (47, 80), (53, 38), (59, 110), (61, 30), (67, 24), (71, 242),
       (73, 0), (79, 54), (83, 110), (89, 122), (97, 36), (101, 224), (103, 24), (107, 116),
       (109, 84), (113, 116)] :=
theorem genus4_root_count :
    (primes113.all fun p =>
      ((T4 p (leastNR p)).length == (p - 1) / 2) &&
      ((deuringCoeffs p).length == (p - 1) / 2 + 1)) = true :=
```

TableGenus5.lean

```
def primes157g5 : List ℕ :=
  [7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,
   101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157]
theorem genus5_table :
    (primes157g5.map fun p => (p, N5 p (leastNR p))) =
      [(7, 0), (11, 0), (13, 0), (17, 0), (19, 0), (23, 6), (29, 8), (31, 4), (37, 0),
       (41, 4), (43, 8), (47, 24), (53, 0), (59, 16), (61, 16), (67, 16), (71, 32), (73, 16),
       (79, 10), (83, 24), (89, 0), (97, 0), (101, 0), (103, 34), (107, 32), (109, 16),
       (113, 16), (127, 40), (131, 36), (137, 0), (139, 12), (149, 8), (151, 60),
       (157, 8)] :=
theorem genus5_root_count :
    (primes157g5.all fun p =>
```

```
      ((T5 p (leastNR p)).length == p / 4) && ((ikoHCoeffs p).length == p / 4 + 1)) = true :=
```

`TableGenus6.lean`

```
def primes157 : List ℕ :=
  [7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,
   101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157]
theorem genus6_table :
    (primes157.map fun p => (p, N6 p (leastNR p))) =
      [(7, 0), (11, 0), (13, 0), (17, 6), (19, 0), (23, 6), (29, 6), (31, 24), (37, 0),
       (41, 30), (43, 0), (47, 24), (53, 12), (59, 30), (61, 0), (67, 0), (71, 48), (73, 24),
       (79, 0), (83, 42), (89, 36), (97, 0), (101, 48), (103, 24), (107, 24), (109, 0),
       (113, 60), (127, 0), (131, 72), (137, 6), (139, 24), (149, 18), (151, 0), (157, 0)] :=
theorem genus6_root_count :
    (primes157.all fun p =>
      ((T6 p (leastNR p)).length == p / 3) && ((ikoGCoeffs p).length == p / 3 + 1)) = true :=
```

References

[1] J. D. Achter and E. W. Howe, *Hasse–Witt and Cartier–Manin matrices: a warning and a request*, in: Arithmetic Geometry: Computation and Applications, Contemporary Mathematics **722**, American Mathematical Society, 2019, 1–18; DOI 10.1090/conm/722/14534; arXiv:1710.10726. The section number cited above is that of the arXiv version (v5, the corrected version, 7 February 2020).

[2] R. Auer and J. Top, *Legendre elliptic curves over finite fields*, J. Number Theory **95** (2002), no. 2, 303–312; DOI 10.1006/jnth.2001.2760.

[3] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272; DOI 10.1007/BF02940746.

[4] T. Ibukiyama, T. Katsura and F. Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no. 2, 127–152. Read from the NUMDAM scan, item `CM_1986__57_2_127_0`; the page numbers cited above are the journal's.

[5] M. Kudo and S. Harashita, *Superspecial curves of genus 4 in small characteristic*, Finite Fields Appl. **45** (2017), 131–169; DOI 10.1016/j.ffa.2016.12.001; arXiv:1607.01114.

[6] M. Kudo, S. Harashita and E. W. Howe, *Algorithms to enumerate superspecial Howe curves of genus 4*, in: ANTS XIV, Open Book Ser. **4** (2020), no. 1, 301–316; DOI 10.2140/obs.2020.4.301; arXiv:2006.11499.

[7] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction – CADE 28, Lecture Notes in Computer Science **12699**, Springer, 2021, 625–635; DOI 10.1007/978-3-030-79876-5_37.

[8] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), 367–381; DOI 10.1145/3372885.3373824.

[9] N. O. Nygaard, *Slopes of powers of Frobenius on crystalline cohomology*, Ann. Sci. École Norm. Sup. (4) **14** (1981), 369–401. Read from the NUMDAM scan, item `ASENS_1981_4_14_4_369_0`; Theorem 4.1 is on p. 388.

[10] R. Ohashi, *On the Rosenhain forms of superspecial curves of genus two*, Finite Fields Appl. **97** (2024), article 102445; DOI 10.1016/j.ffa.2024.102445.

[11] R. Ohashi, *Generalized Howe curves of genus 4, 5, and 6 with completely decomposable Jacobians*, preprint, arXiv:2604.18074v3 (v1 20 April 2026, v2 28 April 2026, v3 3 June 2026, the current version on 7 September 2026; no journal reference). All numbered references to [11] in this paper are to the compiled e-print of v3.

[12] R. Ohashi, *FindSSpGenHowe*: the Magma implementation of the algorithms of [11] with per-prime logs, `https://github.com/Ryo-Ohashi/FindSSpGenHowe`, commit `f44b8cd627e866d189ef7688b7c5e5acf7cad703` (17 May 2026), the head of the `main` branch on 7 September 2026.

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, 2009; DOI 10.1007/978-0-387-09494-6. Theorem V.4.1 is on pp. 148–149 of this edition. [11] cites the 1986 first edition; the preface to the second states that the numbering of the first was preserved.