SUPERSPECIAL POINTS ON HUMBERT SURFACES AND THE PROBABILITY OF (N, N)-SPLITTING

T. SHASKA

Abstract. Let $p \equiv 3 \pmod 4$ be a prime and let $N \geq 2$ be an integer. We determine, to first order in $1/p$ and with an explicit error bound, the proportion of superspecial principally polarized abelian surfaces over $\overline{\mathbb{F}}_p$ that are optimally (N, N)-split. The surfaces are weighted by the reciprocals of their automorphism orders, which is the stationary measure of the Richelot random walk. The main theorem states that for $p \nmid N$ the expected number of optimal (N, N)-splittings of a surface is exactly $5NJ_2(N)(p-1)/(p^2+1)$, where J_2 is Jordan's totient; that for $p > 2N^2$ the second factorial moment is $c_N/(p^2+1)$ with c_N independent of p; and consequently that, for fixed N, the proportion of split surfaces is $5NJ_2(N)/p + O_N(p^{-2})$. The constants c_N are determined explicitly for $2 \leq N \leq 7$. This proportion is the stationary target density of the splitting-detection attack on the superspecial isogeny problem in dimension two. It was previously known only from experiments or from a one-sided bound. The method is to show that the superspecial surfaces sample the genus of their refined Humbert invariants with Siegel's weights, which makes Siegel's theorem on genus averages available. The same method gives the first moment of primitive representations of every discriminant prime to p, mixed moments for several levels, an exact probability at level 2, and a proof that the geometric upper bound of earlier work has the correct leading term. All results are proved; the enumerations enter only through the values of c_N, and every formula was additionally confirmed by exact computation at twelve primes.

1. Introduction

This paper answers a counting question about abelian surfaces in characteristic p. Let $p \equiv 3 \pmod 4$ be a prime. A principally polarized abelian surface over $\overline{\mathbb{F}}_p$ is superspecial if it is isomorphic, as an abelian variety without polarization, to a product of two supersingular elliptic curves. There are finitely many such surfaces, about $p^3/2880$ of them. Some of them are optimally (N, N)-split. For a Jacobian this means that the curve has two complementary elliptic subcovers of degree N which are maximal, that is, which do not factor through an isogeny of elliptic curves of degree greater than one. The question is this. If a superspecial surface is chosen at random, what is the probability that it is optimally (N, N)-split? We give the answer in closed form, to first order in $1/p$, with an explicit bound on the error.

The question comes from cryptography. The superspecial isogeny problem in dimension two asks for an isogeny between two given superspecial surfaces. The best known classical algorithm, due to Costello and Smith [6], walks the Richelot isogeny graph until it reaches a product of elliptic curves, and this takes about p steps. Corte-Real Santos, Costello and Frengley [4, 5] shorten the walk by enlarging the set of targets. They stop at any node whose surface is optimally (N, N)-split, because such a node can be recognised without computing an isogeny. The gain from this idea depends on one number: the proportion of nodes that are optimally (N, N)-split. Until now this number was known only from experiments, or from a one-sided bound. In [27] the proportion was bounded above by $k(H_{N^2})(p-1)/(p^2+1)$, where $k(H_{N^2})$ is the weight of a Siegel modular form attached to the Humbert surface H_{N^2}. That bound came from an intersection number and gave no lower bound.

The random choice has to be made with the right weights. A long random walk on the Richelot graph does not visit all nodes equally often. It visits each node with frequency proportional to the reciprocal of the order

Date: October 17, 2026.

2020 *Mathematics Subject Classification.* Primary 94A60, 14G50; Secondary 11G10, 11E41, 11Y16.

Key words and phrases. isogeny-based cryptography, superspecial isogeny problem, Richelot isogeny graph, splitting detection, superspecial abelian surfaces, refined Humbert invariant, Siegel mass formula, Humbert surfaces.

Department of Computer Science and Engineering, Oakland University, Rochester, MI 48309, USA. Email: shaska@oakland.edu.

of its automorphism group, by a theorem of Florit and Smith [8]. All probabilities in this paper are taken with these weights. We also compare them with the uniform weights, and we show that the two agree to first order for $N \geq 3$ but not for $N = 2$.

Our method rests on a quadratic form. Kani [14, 15] attached to every principally polarized abelian surface (A, θ) its refined Humbert invariant q_θ, which is a positive definite quadratic form on the quotient of the Néron–Severi group by the class of θ. For a superspecial surface this form has rank five. The surface is optimally (N, N)-split exactly when q_θ represents N^2 by a primitive vector, and it has real multiplication by the quadratic order $\mathcal{O}_\Delta$ of discriminant Δ, in the optimal sense that $\mathcal{O}_\Delta$ is the full ring of Rosati-symmetric endomorphisms in its fraction field, exactly when q_θ represents Δ by a primitive vector. The word optimal cannot be dropped. If $\mathcal{O}_\Delta$ acts then so does its suborder $\mathcal{O}_{\Delta f^2}$, but q_θ need not represent Δf^2 primitively. We give an explicit example in Section 9. Kırımlı and Korpal [17, 18] observed that all the forms q_θ of superspecial surfaces lie in one genus, and they used this to detect splittings by solving representation problems. Their counts were obtained by enumeration.

The main structural fact of this paper is that the superspecial surfaces sample this genus with Siegel's weights. More precisely, the map which sends (A, θ) to the class of q_θ is onto the classes of the genus, and the total weight of the surfaces lying over a class M is exactly $2/\#O(M)$, where $O(M)$ is the automorphism group of the form. This is proved by reconstructing the Néron–Severi lattice from the quadratic form and applying a uniqueness theorem of Nikulin. Once this is known, Siegel's theorem on the genus average of representation numbers applies. The average number of primitive representations of any integer t prime to p by q_θ becomes a product of local densities, and we compute every local density. The answer involves the coefficients of Cohen's Eisenstein series of weight $5/2$. For $t = N^2$ the coefficient is $5NJ_2(N)$, where J_2 is Jordan's totient function, and this gives the expected number of splittings.

An expected number is not a probability. A surface can split in several ways, and then it is counted several times. To pass from the expectation to the probability we need the second factorial moment $\mathbb{E}[s_N(s_N - 1)]$, which counts ordered pairs of distinct splittings. Siegel's theorem also applies to representations of binary forms by the quinary form, and this expresses the second factorial moment through a finite sum of genus averages. We do not evaluate all the local densities that enter these averages. We prove instead that the only dependence on p is through a factor $1/(p^2 + 1)$, so that the second factorial moment is $c_N/(p^2 + 1)$ with c_N a constant. This is enough to show that the probability of being split is $5NJ_2(N)/p$ up to an error of order $1/p^2$, and it is enough to determine c_N for $N \leq 7$ from two enumerated genera. The same argument gives the mixed moments for two different levels, which are needed when a detector tests several levels at once.

These results have several consequences, and we work them out. The constant $5NJ_2(N)$ equals the Humbert weight $k(H_{N^2})$ for every $N \geq 3$, by a theorem of van der Geer. So the upper bound of [27] has the correct leading term, and the second factorial moment bounds its excess. On the product locus the mixed moment is sixty times the degree of the intersection curve $H_{N^2} \cap H_1$, which was computed in [26]. At level $N = 2$ the classification of automorphism groups of superspecial genus-two curves gives the probability exactly. For a detector that tests a finite set of levels we give two-sided bounds on its target probability and a criterion for adding a level. For non-square discriminants we obtain the first moment of the number of real-multiplication relations, which replaces a heuristic density in [18] by an exact expectation.

Every formula in the paper was checked against complete enumerations of the genus at twelve primes, by exact rational arithmetic. The first-moment formula was checked in 2313 cases, and the second and mixed moments at every prime where the theorems apply. The scripts, the enumerated genera and a single driver which reproduces all checks are available from the author on request.

The paper is organised as follows. Section 2 sets up the objects, fixes what is counted, and states the main theorem. Section 3 proves that the superspecial surfaces sample the genus with Siegel's weights. Section 4 computes the local densities and proves the first-moment formula for every discriminant. Section 5 specialises to squares, gives an elementary second proof of the first moment, and identifies the constant with the Humbert weight. Section 6 proves the second and mixed moment theorems and completes the proof of the main theorem. Section 7 treats the exact case $N = 2$ and compares the walk measure with the uniform measure. Section 8 draws the consequences for splitting detection. Section 9 treats real multiplication, and Section 10 lists open problems.

2. The setting and the main theorem

In this section we fix the objects of the paper and the conventions for counting them. We first recall the description of superspecial surfaces by hermitian matrices over a quaternion order, which is the form in which we shall compute. We then define the number s_N of splittings of a surface and explain how this count differs from earlier counts of elliptic subcovers. Next we fix the probability measure, which is the stationary measure of the Richelot walk. With these conventions in place we state the main theorem and say where each part is proved.

2.1. **Superspecial surfaces.** Throughout, $p \equiv 3 \pmod 4$ is a prime and k is an algebraically closed field of characteristic p. Let $B = (-1,-p)_{\mathbb{Q}}$ be the quaternion algebra with basis $1, i, j, ij$ and relations $i^2 = -1$, $j^2 = -p$. Let $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+ij}{2}$. This is a maximal order of B. The curve $E_0 \colon y^2 = x^3 - x$ is supersingular over k and $\mathrm{End}(E_0) \cong \mathcal{O}$. Every superspecial abelian surface over k is isomorphic to E_0^2, by a theorem of Deligne, Ogus and Shioda [29, Theorem 3.5]; see also the discussion before [13, Corollary 2.12].

The Néron–Severi lattice of E_0^2 is

$$\Lambda = \mathrm{Her}_2(\mathcal{O}) = \left\{ X = \begin{pmatrix} a & \beta \\ \bar{\beta} & d \end{pmatrix} : a, d \in \mathbb{Z},\ \beta \in \mathcal{O} \right\}, \qquad \langle X, Y \rangle = ad' + a'd - \mathrm{tr}(\beta\bar{\beta}'),$$

so that $\langle X, X \rangle = 2 \det X$ with $\det X = ad - \mathrm{nrd}\,\beta$ [13, 17]. The lattice Λ is even, of rank 6 and signature $(1,5)$. Its discriminant group is $\Lambda^\vee/\Lambda \cong \mathcal{O}^\vee/\mathcal{O} \cong \mathcal{O}/P \cong \mathbb{F}_{p^2}$. Here $\mathcal{O}^\vee$ is the dual of $\mathcal{O}$ for the pairing $\mathrm{tr}(x\bar{y})$ and P is the maximal ideal above p. As a group the discriminant group is $(\mathbb{Z}/p)^2$, and $\Lambda \otimes \mathbb{Z}_2$ is unimodular. The principal polarizations of E_0^2 are the positive definite $X \in \Lambda$ with $\det X = 1$. The group $\mathrm{GL}_2(\mathcal{O}) = \mathrm{Aut}(E_0^2)$ acts on Λ by $X \mapsto g^* X g$, where g^* is the conjugate transpose. This is a right action, which does not matter for orbits and stabilizers. Two polarizations give isomorphic principally polarized surfaces exactly when they lie in one orbit, and $\mathrm{Aut}(E_0^2, X) = U(X) = \{g : g^* X g = X\}$. This is a finite group containing -1. The mass of the superspecial principally polarized surfaces is

$$M_p = \sum_{(A,\theta)} \frac{1}{\#\,\mathrm{Aut}(A,\theta)} = \frac{(p-1)(p^2+1)}{5760}, \tag{1}$$

by Hashimoto and Ibukiyama [11]; see also [31, Theorem 1.1]. Eichler's mass formula is $\sum_E 1/\#\,\mathrm{Aut}\,E = (p-1)/24$, the sum over supersingular elliptic curves.

The mass formula (1) is the normalising constant of every average in this paper. Eichler's formula will be used whenever we count elliptic curves.

2.2. **Elliptic subgroups and splittings.** An elliptic subgroup of A is an elliptic curve $E \subset A$ through the origin. Its class $[E] \in \mathrm{NS}(A)$ is primitive and satisfies $[E]^2 = 0$. By Kani [14] every primitive class D with $D^2 = 0$ and $D \cdot \theta > 0$ is the class of exactly one elliptic subgroup. Let $A = J(C)$ be a Jacobian. An elliptic subgroup of degree $E \cdot \theta = N$ corresponds to a maximal elliptic subcover $C \to E'$ of degree N. Such subgroups come in complementary pairs E, E' with $[E] + [E'] = N\theta$ and $E \cdot E' = N^2$. A pair is the same thing as an isogeny $E_1 \times E_2 \to J(C)$ of type (N,N) whose kernel is the graph of an anti-isometry $E_1[N] \to E_2[N]$; here E_1, E_2 are the elliptic curves covered by C, and the splitting isogeny $J(C) \to E_1 \times E_2$ is the polarized dual. When such a pair exists we say that $J(C)$ is optimally (N,N)-split. Optimality means that the subcovers $C \to E_i$ are maximal. It is not a condition on the order of the kernel, which is always N^2.

Let $s_N(A,\theta)$ be the number of complementary pairs $\{E, E'\}$ of elliptic subgroups of degree N. For a Jacobian this is the number of optimal (N,N)-splittings. For a product $E_1 \times E_2$ with the product polarization the same definition applies, and $s_1 = 1$.

Elliptic subcovers of genus-two curves have been counted in several ways in the literature. In [28] degree-two elliptic subfields of a genus-two function field correspond to its non-hyperelliptic involutions. In [24] degree-three elliptic subfields are counted up to the automorphism group of the field, and the number of such classes is 0, 1, 2 or 4. In [25] curves with subcovers of degrees 2 and 3 at the same time are classified. Our count is different. The number s_N counts complementary pairs with no identification under $\mathrm{Aut}(A,\theta)$. An orbit of m pairs contributes m. The elliptic subgroups of degree N number $2s_N$. The primitive vectors of the refined Humbert invariant with value N^2 also number $2s_N$ (Lemma 5.1). The orbits of pairs under $\mathrm{Aut}(A,\theta)$ are

fewer when some pair has a proper stabilizer. This is why the automorphism strata enter the exact formula at $N = 2$ (Theorem 7.1) and the comparison of measures (Proposition 7.3).

2.3. **The walk and its measure.** The random choice in the main theorem has to be specified. We take the measure that the attack samples. The Richelot graph has as vertices the isomorphism classes of superspecial principally polarized surfaces. Its edges are the $(2,2)$-isogenies, one for each of the 15 maximal isotropic subgroups of $A[2]$. A random walk that chooses one of the 15 kernels uniformly has stationary distribution proportional to $1/\#\operatorname{Aut}(A,\theta)$, by Florit and Smith [8, Theorem 4.9]. All averages in this paper are taken with the weights $1/\#\operatorname{Aut}(A,\theta)$, normalised by M_p. We write $\mathbb{E}[f]$ for the average of a function f of the node, and $\mathbb{P}$ for the corresponding probability. A statement about this measure describes what a long walk sees in the limit. The expected number of steps to the first success needs, in addition, control of the dependence between consecutive steps. We do not address that question.

2.4. **Notation for the main theorem.** Jordan's totient is $J_2(N) = N^2 \prod_{\ell \mid N}(1-\ell^{-2})$. For $N \geq 1$ and a prime $p \nmid N$ we put

$$\mu_N(p) = \mathbb{E}[s_N], \qquad B_N(p) = \mathbb{E}[s_N(s_N-1)], \qquad \delta_N(p) = \mathbb{P}(s_N \geq 1).$$

So μ_N is the expected number of splittings, B_N is the second factorial moment, and δ_N is the weighted proportion of nodes that are optimally (N,N)-split. We can now state the main theorem. It has three parts. The first gives the expected number of splittings exactly. The second says that the second factorial moment has a simple shape. The third converts the two moments into a two-sided bound for the probability.

Theorem 2.1 (Main theorem)**.** *Let $N \geq 2$ be an integer.*

(1) *For every prime $p \equiv 3 \pmod 4$ with $p \nmid N$,*

$$\mu_N(p) = 5NJ_2(N)\,\frac{p-1}{p^2+1}.$$

(2) *There is a constant c_N, depending only on N, such that for every prime $p \equiv 3 \pmod 4$ with $p > 2N^2$,*

$$B_N(p) = \frac{c_N}{p^2+1}.$$

For $N = 2, \dots, 7$ the constants are $c_N = 660$, 12600, 53520, 343320, 501840, 2754960.

(3) *For every prime $p \equiv 3 \pmod 4$ with $p > 2N^2$,*

$$\mu_N(p) - \frac{c_N}{2(p^2+1)} \;\leq\; \delta_N(p) \;\leq\; \mu_N(p), \qquad \text{and therefore} \qquad \delta_N(p) = \frac{5NJ_2(N)}{p} + O_N\!\left(\frac{1}{p^2}\right).$$

Part (1) is proved in Section 5 as Theorem 5.2. Part (2) is proved in Section 6 as Theorem 6.3. Part (3) follows from (1) and (2) by an elementary inequality, and the proof is completed in Section 6. The constant $5NJ_2(N)$ equals the Humbert weight $k(H_{N^2})$ of [26, 27] for every $N \geq 3$ (Proposition 5.5). So the main theorem says that the geometric upper bound of [27] has the correct leading term, and it quantifies the excess of that bound. At $N = 2$ the probability δ_2 is given exactly in Theorem 7.1.

3. The refined Humbert invariant and its genus

The main theorem is about the random variable s_N on the finite set of superspecial nodes. Our strategy is to replace the nodes by quadratic forms. In this section we introduce the refined Humbert invariant q_θ of a node, which is a positive definite quinary form, and we prove the fact on which everything else rests: the nodes, counted with the walk measure, sample the genus of q_θ exactly with Siegel's weights $1/\#O(M)$ (Theorem 3.4). The proof has three steps. Lemma 3.2 shows that the Néron–Severi lattice together with its polarization can be rebuilt from q_θ. Lemma 3.3 uses this reconstruction and a uniqueness theorem of Nikulin to show that the map from polarizations to forms is onto the genus, and to identify its fibres and stabilizers. The theorem then follows from a double-coset count.

We begin with Kani's definition.

Definition 3.1. Let $X \in \Lambda$ be a principal polarization. The refined Humbert invariant of X is the quadratic form

$$q_X(D) = \langle D, X\rangle^2 - 2\langle D, D\rangle$$

on $\Lambda/\mathbb{Z}X$. Its bilinear form is $b_X(D, D') = \langle D, X\rangle\langle D', X\rangle - 2\langle D, D'\rangle$, so that $b_X(D, D) = q_X(D)$.

The form q_X is well defined and integral. It is positive definite of rank 5. To see this, write $D = \frac{1}{2}\langle D, X\rangle X + D^\perp$. Then $q_X(D) = -2\langle D^\perp, D^\perp\rangle$, and $X^\perp$ is negative definite. This is Kani's invariant [14, 15]. Two congruences follow from the definition, because Λ is even: $q_X(w) \equiv 0, 1 \pmod 4$ and $b_X(w, w') \equiv q_X(w)q_X(w') \pmod 2$. Kani's dictionary says the following. The form q_θ primitively represents N^2 if and only if A is optimally (N, N)-split. The form q_θ primitively represents a non-square discriminant Δ if and only if (A, θ) lies on the Humbert surface H_Δ.

The dictionary turns the counting of splittings into a representation problem for q_θ. The next observation is that all the forms q_θ belong to one genus, so that Siegel's theory of genus averages becomes available.

Kırımlı and Korpal [17, Section 3] show that all the forms q_X lie in the genus $\mathcal{G}_p$ of

$$q_5(x) = x_0^2 + 4x_1^2 + 4x_1x_3 + 4x_2^2 + 4x_2x_4 + (p+1)x_3^2 + (p+1)x_4^2. \tag{2}$$

Its Gram matrix G, defined by $q_5(x) = x^tGx$, has determinant $16p^2$. The statement that all q_X lie in one genus also follows from Lemma 3.2 below. A local isometry of Λ_ℓ that carries X to X' induces a local isometry from q_X to $q_{X'}$. Such a local isometry exists at every prime; see [17, Section 3].

The first lemma says that nothing is lost in passing from the pair (Λ, X) to the form q_X. The pair can be rebuilt from the form. We call this the gluing lemma.

Lemma 3.2. *Let M be a positive definite integral quadratic lattice with form q and bilinear form b. Suppose that $q(w) \equiv 0, 1 \pmod 4$ and $b(w, w') \equiv q(w)q(w') \pmod 2$ for all $w, w' \in M$. Put*

$$\Lambda(M) = \{(w, s) \in M \times \mathbb{Z} : s \equiv q(w) \pmod 2\}, \qquad X_M = (0, 2), \qquad \langle (w, s), (w', s')\rangle = \tfrac{1}{2}\big(ss' - b(w, w')\big).$$

Then $\Lambda(M)$ is an even lattice of signature $(1, \operatorname{rank} M)$, $\langle X_M, X_M\rangle = 2$, and the refined Humbert invariant of X_M is isometric to M. Conversely, let $X \in \Lambda$ be a principal polarization. Then the map $D \mapsto (D \bmod \mathbb{Z}X, \langle D, X\rangle)$ is an isometry $\Lambda \to \Lambda(\Lambda/\mathbb{Z}X, q_X)$ carrying X to X_M.

Proof. The set $\Lambda(M)$ is a subgroup, since $q(w + w') \equiv q(w) + q(w') \pmod 2$. The pairing is integral because

$$ss' \equiv q(w)q(w') \equiv b(w, w') \pmod 2,$$

and it is even because

$$\langle (w, s), (w, s)\rangle = \tfrac{1}{2}\big(s^2 - q(w)\big) \qquad \text{and} \qquad s^2 \equiv q(w) \pmod 4.$$

We have $\langle (w, s), X_M\rangle = s$. So the refined form of X_M is $s^2 - (s^2 - q(w)) = q(w)$, and $(w, s) \equiv (w', s')$ modulo $\mathbb{Z}X_M$ exactly when $w = w'$. The signature is read off from the decomposition $\mathbb{Q}X_M \oplus (M \otimes \mathbb{Q})$.

For the converse put $w = D \bmod \mathbb{Z}X$ and $s = \langle D, X\rangle$. Then

$$q_X(w) = s^2 - 2\langle D, D\rangle \equiv s^2 \pmod 4,$$

so the pair (w, s) lies in $\Lambda(M)$. If $w = 0$ then $D = mX$ and $s = 2m$, so $s = 0$ forces $D = 0$. Hence the map is injective. It is onto because $\langle D + mX, X\rangle = s + 2m$ runs through the whole class of s modulo 2. It is an isometry by Definition 3.1. □

The gluing lemma turns questions about forms into questions about polarizations of the single lattice Λ. The next lemma collects the consequences.

Lemma 3.3. *Let $X, X' \in \Lambda$ be principal polarizations, and let $O^+(\Lambda)$ be the group of isometries of Λ preserving the positive cone.*

1. *Restriction to $\Lambda/\mathbb{Z}X$ is an isomorphism $\operatorname{Stab}_{O(\Lambda)}(X) \to O(q_X)$.*
2. *$q_X \cong q_{X'}$ if and only if $X' = \phi(X)$ for some $\phi \in O^+(\Lambda)$.*
3. *Every class of $\mathcal{G}_p$ is q_X for some principal polarization X.*

Proof. (1) An isometry fixing X preserves $\mathbb{Z}X$ and q_X. By Lemma 3.2 an isometry ψ of q_X induces the map $(w, s) \mapsto (\psi w, s)$ on Λ. This map fixes X and restricts to ψ. An isometry fixing X is determined by its restriction.

(2) An isometry $q_X \to q_{X'}$ induces an isometry of Λ carrying X to X'. It preserves the positive cone because X and X' both lie in the positive definite component.

(3) The hypotheses of Lemma 3.2 are local conditions. They hold for q_X, hence for every $M \in \mathcal{G}_p$. The construction $M \mapsto \Lambda(M)$ commutes with completion, so $\Lambda(M)$ lies in the genus of Λ. Now Λ is even and indefinite of rank 6, with $\Lambda^\vee/\Lambda \cong (\mathbb{Z}/p)^2$ of length 2, and Λ_2 is unimodular. Nikulin's theorem [22, Theorem 1.14.2] states that an even indefinite lattice T has a single class in its genus provided

$$\operatorname{rank} T \;\geq\; \ell(A_{T_q}) + 2 \qquad \text{for every prime } q,$$

where ℓ denotes the minimal number of generators of the discriminant group. Here $6 \geq 2 + 2$ at $q = p$ and $6 \geq 0 + 2$ at $q = 2$. So there is an isometry $\Lambda(M) \to \Lambda$. The image of $\pm X_M$, with the sign that lands in the positive definite component, is a principal polarization X with $q_X \cong M$. □

We must now compare two groups acting on Λ. The isomorphism classes of surfaces are the orbits of $\mathrm{Aut}(E_0^2) = \mathrm{GL}_2(\mathcal{O})$, whereas the classes of forms are the orbits of the full group $O^+(\Lambda)$. The following paragraph shows that the first group has finite index in the second, which is what the counting argument needs.

Let $\Gamma \subset O(\Lambda)$ be the image of $\mathrm{GL}_2(\mathcal{O})$. For $g \in \mathrm{GL}_2(B)$ one has

$$\det(g^* X g) = \mathrm{nrd}(g) \det X,$$

where nrd is the reduced norm of $M_2(B)$. The reduced norm is positive on $\mathrm{GL}_2(B \otimes \mathbb{R}) = \mathrm{GL}_2(\mathbb{H})$. For $g \in \mathrm{GL}_2(\mathcal{O})$ it is a positive integer with integral inverse, so $\mathrm{nrd}(g) = 1$. Hence $g^* X g$ is positive definite together with X, so $\Gamma \subset O^+(\Lambda)$, and $\mathrm{GL}_2(\mathcal{O}) = \mathrm{SL}_2(\mathcal{O}) := \{g \in M_2(\mathcal{O}) : \mathrm{nrd}(g) = 1\}$. We write $\mathrm{SL}_2(B) = \mathrm{SL}_1(M_2(B))$ for the elements of reduced norm 1 in $\mathrm{GL}_2(B)$. The kernel of $\mathrm{GL}_2(\mathcal{O}) \to \Gamma$ consists of the g with $g^* X g = X$ for all X, which forces g to be a central unit, so the kernel is $\{\pm 1\}$.

We use the inverse to turn the right action into a left action. The map

$$g \longmapsto \big(X \mapsto (g^{-1})^* X g^{-1}\big), \qquad \mathrm{SL}_2(B) \longrightarrow \mathrm{SO}(\Lambda \otimes \mathbb{Q}),$$

is the isogeny of $\mathbb{Q}$-groups which expresses the exceptional isomorphism $D_3 = A_3$. Indeed, the involution $g \mapsto g^*$ of $M_2(B)$ is symplectic, $\mathrm{Her}_2(B)$ is its space of symmetric elements, and det is the Pfaffian norm of the involution; under these identifications $\mathrm{SL}_2(B)$ is the spin group of the quadratic space $(\mathrm{Her}_2(B), \det)$ [21, Section 15.C]. The group $\mathrm{SL}_2(\mathcal{O})$ is an arithmetic subgroup of the source, and the image of an arithmetic subgroup under an isogeny is arithmetic [1]. So Γ has finite index in $O^+(\Lambda)$.

We can now prove the theorem that transfers the walk measure to the genus.

Theorem 3.4 (Measure transfer)**.** *Put $c_p = \frac{1}{2}[O^+(\Lambda) : \Gamma]$. For every class M of $\mathcal{G}_p$,*

$$\sum_{(A,\theta):\, q_\theta \cong M} \frac{1}{\#\,\mathrm{Aut}(A, \theta)} = \frac{c_p}{\#O(M)},$$

the sum over isomorphism classes of superspecial principally polarized surfaces. In particular every class of $\mathcal{G}_p$ occurs. Hence $M_p = c_p\, m(\mathcal{G}_p)$, where $m(\mathcal{G}_p) = \sum_M 1/\#O(M)$ is the mass of the genus, and for every function f on classes the weighted average of $f(q_\theta)$ over superspecial nodes equals the Siegel average of f over $\mathcal{G}_p$.

Proof. Fix M and choose X_0 with $q_{X_0} \cong M$, which exists by Lemma 3.3(3). By Lemma 3.3(2) the polarizations X with $q_X \cong M$ form the orbit GX_0 with $G = O^+(\Lambda)$. Put $S = \mathrm{Stab}_G(X_0)$. Then $S \cong O(M)$ by Lemma 3.3(1).

The isomorphism classes of (E_0^2, X) with X in the orbit are the Γ-orbits on G/S, that is, the double cosets $\Gamma g S$. The surface (E_0^2, gX_0) has automorphism group of order $2\#(\Gamma \cap gSg^{-1})$, the factor 2 coming from the kernel $\{\pm 1\}$. So the left side of the formula is

$$\sum_{\Gamma g S} \frac{1}{2\#(\Gamma \cap gSg^{-1})}.$$

The group S acts on the finite set $\Gamma\backslash G$ by right multiplication. Its orbits are the double cosets, and the stabilizer of Γg is $S\cap g^{-1}\Gamma g$, which is conjugate to $\Gamma\cap gSg^{-1}$ and has the same order. Counting $\Gamma\backslash G$ by orbits gives

$$\sum_{\Gamma gS}\frac{\#S}{\#(\Gamma\cap gSg^{-1})}=[G:\Gamma].$$

Dividing by $2\#S=2\#O(M)$ gives the formula. Summing over M gives $M_p=c_p\,m(\mathcal{G}_p)$, and the statement about averages follows. □

The constant c_p cancels in every normalised average, so the moment formulas of the later sections do not depend on its value. It can nevertheless be determined. Let $\theta\colon O(\Lambda\otimes\mathbb{Q})\to\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ be the spinor norm, normalised so that a reflection in a vector v has spinor norm $\langle v,v\rangle/2$, and let $O'(\Lambda)=\ker\theta\cap\mathrm{SO}^+(\Lambda)$ be the spinor kernel, where $\mathrm{SO}^+(\Lambda)=\mathrm{SO}(\Lambda)\cap O^+(\Lambda)$.

Proposition 3.5. *For every prime $p\equiv 3 \pmod 4$ the group Γ is the spinor kernel $O'(\Lambda)$, the index $[O^+(\Lambda):\Gamma]$ is 4, and $c_p=2$. Hence, for every class M of $\mathcal{G}_p$,*

$$\sum_{(A,\theta)\colon q_\theta\cong M}\frac{1}{\#\operatorname{Aut}(A,\theta)}=\frac{2}{\#O(M)},\qquad\text{and}\qquad m(\mathcal{G}_p)=\frac{M_p}{2}=\frac{(p-1)(p^2+1)}{11520}.$$

Proof. Step 1: $\Gamma=O'(\Lambda)$. The map $\mathrm{SL}_2(B)\to\mathrm{SO}(V)$, $V=\Lambda\otimes\mathbb{Q}$, is the spin covering of $(V,\det)$, as recalled above. For a spin covering over a field the image of the rational points is the kernel of the spinor norm on $\mathrm{SO}(V)$. An element with trivial rational spinor norm has positive real spinor norm, and in signature $(1,5)$ the elements of $\mathrm{SO}(V\otimes\mathbb{R})$ with positive spinor norm are those preserving the positive cone. So $\ker\theta\cap\mathrm{SO}(\Lambda)=O'(\Lambda)$. Since Γ is the image of a subgroup of $\mathrm{SL}_2(B)$, we get $\Gamma\subset O'(\Lambda)$, and $O'(\Lambda)$ is the image of the stabilizer

$$\mathrm{Stab}_{\mathrm{SL}_2(B)}(\Lambda)=\{g\in\mathrm{SL}_2(B):g^*\Lambda g=\Lambda\}.$$

It remains to show that this stabilizer is $\mathrm{SL}_2(\mathcal{O})$. Let g be in it. Then $g^*\Lambda_\ell g=\Lambda_\ell$ for every prime ℓ, where $\Lambda_\ell=\mathrm{Her}_2(\mathcal{O}_\ell)$. We show that $g\in\mathrm{GL}_2(\mathcal{O}_\ell)$ for every ℓ; then g has entries in $B\cap\bigcap_\ell\mathcal{O}_\ell=\mathcal{O}$, so $g\in\mathrm{SL}_2(\mathcal{O})$.

Let $\ell\neq p$. Then $B_\ell\cong M_2(\mathbb{Q}_\ell)$ and $\mathcal{O}_\ell\cong M_2(\mathbb{Z}_\ell)$, with the involution $x\mapsto\bar{x}=\mathrm{adj}(x)$, and $\mathrm{GL}_2(\mathcal{O}_\ell)=\mathrm{GL}_4(\mathbb{Z}_\ell)$. The Cartan decomposition of $\mathrm{GL}_4(\mathbb{Q}_\ell)$ gives $g=k_1dk_2$ with $k_i\in\mathrm{GL}_2(\mathcal{O}_\ell)$ and $d=\mathrm{diag}(d_1,d_2)$, $d_i=\mathrm{diag}(\ell^{a_i},\ell^{b_i})\in M_2(\mathbb{Q}_\ell)$. The group $\mathrm{GL}_2(\mathcal{O}_\ell)$ stabilizes Λ_ℓ, so d does. Write the entries of $X\in\Lambda_\ell$ as $X=\left(\begin{smallmatrix}a&\beta\\ \bar\beta&c\end{smallmatrix}\right)$, with c in place of the earlier d. Then

$$d^*Xd=\begin{pmatrix}\ell^{a_1+b_1}a & \bar d_1\beta d_2\\ \bar d_2\bar\beta d_1 & \ell^{a_2+b_2}c\end{pmatrix},$$

since $\bar d_1d_1=\mathrm{nrd}(d_1)=\ell^{a_1+b_1}$. The diagonal entries must run through $\mathbb{Z}_\ell$, so $a_1+b_1=a_2+b_2=0$. The map $\beta\mapsto\bar d_1\beta d_2$ multiplies the four entries of $\beta\in M_2(\mathbb{Z}_\ell)$ by $\ell^{b_1+a_2},\ell^{b_1+b_2},\ell^{a_1+a_2},\ell^{a_1+b_2}$, and it must be a bijection of $M_2(\mathbb{Z}_\ell)$, since every $\beta\in\mathcal{O}_\ell$ is the $(1,2)$ entry of some $X\in\Lambda_\ell$. So all four exponents vanish, $d=1$, and $g\in\mathrm{GL}_2(\mathcal{O}_\ell)$.

Let $\ell=p$. Then B_p is a division algebra, $\mathcal{O}_p$ is its valuation ring, and $\pi=j$ is a uniformizer with $\bar\pi\pi=p$. The Cartan decomposition $\mathrm{GL}_2(B_p)=\mathrm{GL}_2(\mathcal{O}_p)\,\{\mathrm{diag}(\pi^m,\pi^n)\}\,\mathrm{GL}_2(\mathcal{O}_p)$ gives, as before, that $d=\mathrm{diag}(\pi^m,\pi^n)$ stabilizes Λ_p. Its effect on the diagonal entries is $a\mapsto p^ma$ and $c\mapsto p^nc$, so $m=n=0$ and $g\in\mathrm{GL}_2(\mathcal{O}_p)$.

Step 2: $[O^+(\Lambda):O'(\Lambda)]=4$. The vector $u=\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$ has $\langle u,u\rangle=-2$. The reflection r_u is integral, has determinant -1, and preserves the positive cone because u has negative norm. So $[O^+(\Lambda):\mathrm{SO}^+(\Lambda)]=2$. Next, the spinor norm is trivial on $\mathrm{SO}^+(\Lambda)$ at the real place, since SO^+ is the identity component of $\mathrm{SO}(V\otimes\mathbb{R})$. For $\ell\neq p$ the lattice Λ_ℓ is unimodular, and at $\ell=2$ it is even, that is, its norm ideal is $2\mathbb{Z}_2$. For such lattices the spinor norms of the integral rotations are units times squares: for odd ℓ see [19] or [2, Chapter 11], and for $\ell=2$ see [19] and [7, Theorem 3.8]. The evenness at 2 is essential here. Hence $\theta(\mathrm{SO}^+(\Lambda))$ is contained in the positive square classes that are units at every $\ell\neq p$, namely $\{1,p\}$, and $[\mathrm{SO}^+(\Lambda):O'(\Lambda)]\le 2$. The class p occurs. Let $v=\left(\begin{smallmatrix}0&-j\\ j&0\end{smallmatrix}\right)$. Then $\langle v,v\rangle=-2p$, and $\langle X,v\rangle=-\operatorname{tr}(\beta j)\in p\mathbb{Z}$ for every $X\in\Lambda$, because $\operatorname{tr}(\beta j)=-pz$ for $\beta=x+yi+z\frac{1+j}{2}+w\frac{i+ij}{2}$. So $r_v(x)=x+\langle x,v\rangle v/p$ is integral. The product r_ur_v lies in $\mathrm{SO}^+(\Lambda)$ and has spinor norm $(-1)(-p)=p$. Therefore $[\mathrm{SO}^+(\Lambda):O'(\Lambda)]=2$ and $[O^+(\Lambda):O'(\Lambda)]=4$.

Combining the two steps, $[O^+(\Lambda):\Gamma]=4$ and $c_p=2$. The displayed formulas follow from Theorem 3.4 and (1). □

The last formula is a mass formula for the genus of the refined Humbert invariant. It is confirmed by the complete enumerations of Section 6.3 at twelve primes.

Remark 3.6. Frobenius preserves intersection numbers and the polarization, so $q_\theta \cong q_{\theta^{(p)}}$, and each fibre of the map $(A,\theta)\mapsto q_\theta$ is a union of Frobenius orbits. Neither this invariance nor Proposition 3.5 shows that each fibre is a single orbit. Identifying the individual fibres is a separate problem, related to [16].

The next remark compares our genus with a quinary genus in the literature.

Remark 3.7. Ibukiyama [12, Theorem 4.5] relates type numbers of quaternion hermitian lattices to class numbers of quinary lattices. The integral normalisation can be compared with ours. For his principal genus, with $D_1=p$ and $D_2=1$, the lattice in [12, Section 4, equation (1)] is

$$L^{\mathrm{Ib}}=\mathbb{Z}\oplus\mathcal{O},\qquad Q(a,\beta)=a^2+\operatorname{nrd}\beta.$$

Under $(a,\beta)\mapsto(a,2\beta)$ our base lattice (2) becomes the sublattice $\mathbb{Z}\oplus 2\mathcal{O}$ of L^{Ib}, which has index 16. So the rational quadratic spaces and the completions at odd primes agree, while the integral lattices differ at 2. The polar bilinear forms have determinants $2p^2$ and $512p^2$ respectively. This comparison does not identify the class sets or their weights. Theorem 3.4 supplies the weighted statement for the genus of the refined Humbert invariant, which is what the averaging argument needs.

4. Siegel's theorem and the local densities

Having identified node averages with genus averages, we can bring in Siegel's theorem, which expresses the genus average of a representation number as a product of local densities. In this section we recall the theorem in the form we need, compute every local density of the base form q_5, and deduce a closed formula for the expected number of representations of any integer t prime to p (Theorem 4.2). The answer is expressed through Cohen's numbers $H(2,t)$, the coefficients of the Eisenstein series of weight $5/2$. The calculation at the prime 2 is the only laborious part of the section.

Let $L=(\mathbb{Z}^5,q_5)$. For a prime ℓ and $t\in\mathbb{Z}_\ell$ the local density is

$$\alpha_\ell(t)=\lim_{k\to\infty}\ell^{-4k}\,\#\{x\in(\mathbb{Z}/\ell^k)^5 : q_5(x)\equiv t\}.$$

It depends only on the genus. For a form q let $r_q(t)$ be the number of vectors x with $q(x)=t$, and let $r_q^*(t)$ be the number of primitive such vectors. Siegel's theorem [30] for a positive definite quinary form representing a number states

$$\frac{1}{m(\mathcal{G}_p)}\sum_{M\in\mathcal{G}_p}\frac{r_M(t)}{\#O(M)}=\frac{\pi^{5/2}}{\Gamma(5/2)}t^{3/2}(\det G)^{-1/2}\prod_\ell\alpha_\ell(t)=\frac{\pi^2t^{3/2}}{3p}\prod_\ell\alpha_\ell(t). \tag{3}$$

Let $H(2,t)$ be Cohen's numbers [3], the coefficients of the Eisenstein series of weight $5/2$. For $t\equiv 0,1 \pmod 4$ write $t=Df^2$, where D is a fundamental discriminant or $D=1$, and let χ_D be its character. Then

$$H(2,t)=L(-1,\chi_D)\sum_{d\mid f}\mu(d)\chi_D(d)\,d\,\sigma_3(f/d),$$

and $H(2,t)=0$ for $t\equiv 2,3 \pmod 4$. We put

$$H^*(2,t)=\sum_{f^2\mid t}\mu(f)H(2,t/f^2),\qquad C(t)=-60\,H^*(2,t).$$

For a prime ℓ with $\ell^b\parallel f$ put

$$e_\ell(t)=\ell^{-3b}\big(\sigma_3(\ell^b)-\chi_D(\ell)\,\ell\,\sigma_3(\ell^{b-1})\big),$$

where the second term is omitted when $b=0$. Then $\prod_\ell e_\ell(t)=f^{-3}\sum_{d\mid f}\mu(d)\chi_D(d)d\sigma_3(f/d)$.

We now compute the local densities. The lemma also records the local structure of L, which will be used again in Section 6.

Lemma 4.1. *The completions of L are $L_\ell \cong \langle 1,1,1,1,1\rangle$ for $\ell \nmid 2p$, $L_p \cong \langle 1,1,1\rangle \perp p\langle 1,1\rangle$, and $L_2 \cong \langle 1\rangle \perp 4(U \perp U)$ with $U(x,y) = xy$. In particular L_ℓ for $\ell \neq p$ does not depend on p. For $t \equiv 0,1 \pmod 4$,*

$$\alpha_\ell(t) = \frac{1-\ell^{-4}}{1-\chi_D(\ell)\ell^{-2}}\, e_\ell(t) \qquad (\ell \nmid 2p),$$
$$\alpha_p(t) = 1 - \frac{\chi_D(p)}{p} \qquad (p \nmid t),$$
$$\alpha_2(t) = 2\,\frac{1-2^{-4}}{1-\chi_D(2)2^{-2}}\, e_2(t),$$

and $\alpha_2(t) = 0$ for $t \equiv 2,3 \pmod 4$.

Proof. Local structure. The form is

$$q_5 = \langle 1\rangle \perp \beta \perp \beta, \qquad \beta = 4x^2 + 4xy + (p+1)y^2, \qquad \det\beta = 4p.$$

For $\ell \nmid 2p$ all summands are unimodular and $16p^2$ is a square, which determines L_ℓ. Over $\mathbb{Z}_p$ we have $\beta \cong \langle 4\rangle \perp \langle p\rangle$. Over $\mathbb{Z}_2$ we have $\beta = 4\beta_0$ with

$$\beta_0 = x^2 + xy + \tfrac{p+1}{4}y^2, \qquad \text{polar Gram matrix } \begin{pmatrix} 2 & 1 \\ 1 & (p+1)/2 \end{pmatrix} \text{ of determinant } p.$$

So β_0 is a unimodular quadratic $\mathbb{Z}_2$-lattice, and $\beta_0 \perp \beta_0 \cong U \perp U$, because two copies of a binary unimodular quadratic lattice have Arf invariant 0. This holds whether β_0 is isotropic, which happens for $p \equiv 7 \pmod 8$, or not.

Odd $\ell \neq p$. This is the density of t by a sum of five squares. The stated formula is classical [30].

$\ell = p$. Write $x = (y,z)$ with $y \in \mathbb{Z}_p^3$ in the unimodular part $Q_3 = \langle 1,1,1\rangle$. Since $p \nmid t$, the congruence $Q_3(y) + pQ_2(z) \equiv t \pmod p$ constrains only y. Its solutions in five variables are non-singular, with p^4 lifts at each step. The number of $y \in \mathbb{F}_p^3$ with $Q_3(y) = t$ is $p^2 + p\,\eta(-t)$, where η is the quadratic character of $\mathbb{F}_p$. Hence

$$\alpha_p(t) = \frac{p^2\cdot p^2 + p\,\eta(-t)\cdot p^2}{p^4} = 1 + \frac{\eta(-t)}{p} = 1 - \frac{\chi_D(p)}{p},$$

because $\eta(-1) = -1$ and $\eta(t) = \chi_D(p)$, the latter since $p \nmid f$.

$\ell = 2$. Let $H = x_1x_3 + x_2x_4$ and $\delta_H(c) = \lim_k 2^{-3k}\#\{x \in (\mathbb{Z}/2^k)^4 : H(x) \equiv c\}$. For $c \neq 0$ with $v = v_2(c)$,

$$\delta_H(c) = \tfrac{3}{4}\big(2 - 2^{-v}\big). \tag{4}$$

Indeed the number of solutions of $x_1x_3 + x_2x_4 \equiv c \pmod{2^k}$ is $2^{3k}(2-2^{-v})\cdot\frac{3}{4}$ for $k > v$. One sees this by counting the pairs (x_1,x_3) with $x_1x_3 \equiv c'$ for each c' and summing. Since $q_5 \cong x_0^2 + 4H$, counting modulo 2^k and letting $k \to \infty$ gives

$$\alpha_2(t) = 4\int_{\mathbb{Z}_2} \mathbf{1}\big[x_0^2 \equiv t \ (4)\big]\,\delta_H\big((t-x_0^2)/4\big)\,dx_0.$$

This vanishes unless $t \equiv 0,1 \pmod 4$. Put

$$\Phi(s) = \int_{\mathbb{Z}_2} \delta_H(s-y^2)\,dy, \qquad \Psi(u) = \int_{\mathbb{Z}_2} 2^{-v_2(u-y^2)}\,dy.$$

The case t odd. Then x_0 is odd, $x_0^2 \equiv 1 \pmod 8$ and f is odd, so $D \equiv t \pmod 8$ and $b = 0$. If $t \equiv 5 \pmod 8$ then $(t-x_0^2)/4$ is odd for every odd x_0, so

$$\alpha_2(t) = 4\cdot\tfrac{1}{2}\cdot\delta_H(\text{odd}) = 4\cdot\tfrac{1}{2}\cdot\tfrac{3}{4} = \tfrac{3}{2}.$$

If $t \equiv 1 \pmod 8$ then $t = s^2$ with $s \in \mathbb{Z}_2^\times$. For odd x_0 exactly one of $s \pm x_0$ is $\equiv 2 \pmod 4$, so $v_2(t-x_0^2) = j \geq 3$ on a set of x_0 of measure 2^{1-j}. Hence

$$\alpha_2(t) = 4\sum_{j\geq 3} 2^{1-j}\cdot\tfrac{3}{4}(2-2^{2-j}) = 3\Big(\sum_{j\geq 2} 2^{2-j} - \sum_{j\geq 3} 2^{3-2j}\Big) = 3\big(1-\tfrac{1}{6}\big) = \tfrac{5}{2}.$$

These are the stated values $2\cdot\frac{15}{16}/(1+\frac{1}{4}) = \frac{3}{2}$ and $2\cdot\frac{15}{16}/(1-\frac{1}{4}) = \frac{5}{2}$.

The case $4 \mid t$. Then $x_0 = 2y$ is even, the even x_0 have measure $\frac{1}{2}$, and $(t - x_0^2)/4 = t/4 - y^2$. So

$$\alpha_2(t) = 2\,\Phi(s), \qquad s = t/4.$$

We first compute $\Phi(s)$ for $4 \nmid s$ by splitting y into even and odd and using (4).

- For $s \equiv 2, 3 \pmod 4$, one of $s - y^2$ for y even and y odd has valuation 0 and the other has valuation 1, so
$$\Phi(s) = \tfrac{1}{2} \cdot \tfrac{3}{4} + \tfrac{1}{2} \cdot \tfrac{9}{8} = \tfrac{15}{16}.$$
- For $s \equiv 5 \pmod 8$, even y give valuation 0 and odd y give valuation exactly 2, so
$$\Phi(s) = \tfrac{1}{2} \cdot \tfrac{3}{4} + \tfrac{1}{2} \cdot \tfrac{21}{16} = \tfrac{33}{32}.$$
- For $s \equiv 1 \pmod 8$, even y give valuation 0, and for odd y the valuation is $j \geq 3$ on a set of measure 2^{1-j}, as in the odd case. So
$$\Phi(s) = \tfrac{3}{8} + \sum_{j \geq 3} 2^{1-j} \cdot \tfrac{3}{4}\big(2 - 2^{-j}\big) = \tfrac{3}{8} + \tfrac{3}{4}\Big(1 - \tfrac{1}{24}\Big) = \tfrac{35}{32}.$$

These base values agree with the formula. The case $s \equiv 2, 3 \pmod 4$ is D even and $b = 0$, where $\chi_D(2) = 0$, $e_2 = 1$ and the formula gives $2 \cdot \frac{15}{16} = \frac{15}{8} = 2\Phi(s)$. The cases $s \equiv 5, 1 \pmod 8$ are D odd and $b = 1$, where $e_2 = (9 - 2\chi_D(2))/8$, and the formula gives

$$2 \cdot \tfrac{15}{16} \cdot \frac{11/8}{1 + 1/4} = \tfrac{33}{16} \quad (\chi_D(2) = -1), \qquad 2 \cdot \tfrac{15}{16} \cdot \frac{7/8}{1 - 1/4} = \tfrac{35}{16} \quad (\chi_D(2) = 1).$$

For $4 \mid s$ we argue by induction on b. The identity $\delta_H(4c) = \delta_H(c) + \frac{9}{16} 2^{-v_2(c)}$, which follows from (4), gives the recursions

$$\Phi(s) = \tfrac{3}{8} + \tfrac{1}{2}\Phi(s/4) + \tfrac{9}{32}\Psi(s/4) \quad (4 \mid s), \qquad \Psi(u) = \tfrac{1}{2} + \tfrac{1}{8}\Psi(u/4) \quad (4 \mid u),$$

with the base values

$$\Psi(u) = \tfrac{3}{4} \ (u \equiv 2, 3 \bmod 4), \qquad \Psi(u) = \tfrac{5}{8} \ (u \equiv 5 \bmod 8), \qquad \Psi(u) = \tfrac{13}{24} \ (u \equiv 1 \bmod 8).$$

In terms of α_2, the first recursion reads

$$\alpha_2(t) = \tfrac{3}{4} + \tfrac{1}{2}\alpha_2(t/4) + \tfrac{9}{16}\Psi(t/16) \qquad (16 \mid t). \tag{5}$$

On the other side, write $\chi = \chi_D(2)$ and let

$$A(t) = K\,e_2(t), \qquad K = \frac{15/8}{1 - \chi/4},$$

be the right side of the formula to be proved. Since $\sigma_3(2^b) - 8\sigma_3(2^{b-1}) = 1$, the definition of e_2 gives

$$e_2(t) = e_2(t/4) + (1 - 2\chi)\,8^{-b}, \qquad \text{hence} \qquad A(t) = A(t/4) + K(1 - 2\chi)\,8^{-b} \qquad (b \geq 1). \tag{6}$$

Assume $\alpha_2(t/4) = A(t/4)$. By (5) and (6), the claim $\alpha_2(t) = A(t)$ is equivalent to

$$\tfrac{1}{2}A(t/4) + K(1 - 2\chi)\,8^{-b} \;=\; \tfrac{3}{4} + \tfrac{9}{16}\Psi(t/16). \tag{7}$$

We evaluate both sides. Unwinding the recursion for Ψ, with $a = b - 2$ steps when D is odd and $a = b - 1$ steps when D is even, gives

$$\Psi(t/16) = \tfrac{4}{7}\big(1 - 8^{-a}\big) + 8^{-a}\,\Psi_0, \qquad \Psi_0 = \tfrac{13}{24},\ \tfrac{5}{8},\ \tfrac{3}{4} \ \text{ according as } \chi = 1, -1, 0,$$

and summing the geometric series in the definition of e_2 gives

$$e_2(t/4) = \tfrac{8}{7}\big(1 - 8^{-b}\big) - \tfrac{2\chi}{7}\big(1 - 8^{1-b}\big).$$

Substituting, both sides of (7) equal

$$\tfrac{15}{14} - \tfrac{15}{14}\,8^{-b} \quad (\chi = 1), \qquad \tfrac{15}{14} + \tfrac{27}{14}\,8^{-b} \quad (\chi = -1), \qquad \tfrac{15}{14} + \tfrac{45}{56}\,8^{-b} \quad (\chi = 0).$$

So (7) holds, the dependence on D is through $\chi_D(2)$ alone, and $\alpha_2(t) = A(t)$ for all t.

All three formulas were also compared with direct counts modulo prime powers. □

We assemble the local densities into the first-moment formula. The formula is stated both as an average and as an absolute weighted sum.

Theorem 4.2 (First moments)**.** *Let $p \equiv 3 \pmod 4$, let $t \geq 1$ with $p \nmid t$, and put $\chi = (t/p)$. Then*

$$\mathbb{E}\big[r^*_{q_\theta}(t)\big] = 2\,C(t)\,\frac{p-\chi}{p^2+\chi}, \qquad \sum_{(A,\theta)} \frac{r^*_{q_\theta}(t)}{\#\operatorname{Aut}(A,\theta)} = \frac{C(t)\,(p-1)(p-\chi)(p^2+1)}{2880\,(p^2+\chi)}.$$

The same holds with r and $-60H(2,t)$ in place of r^* and $C(t)$.

Proof. By Theorem 3.4 the weighted node average of $r_{q_\theta}(t)$ is the left side of (3). For $t \equiv 2, 3 \pmod 4$ both sides vanish. Otherwise Lemma 4.1 with $\chi = \chi_D(p) = (t/p)$ and $e_p(t) = 1$ gives

$$\prod_\ell \alpha_\ell(t) = \frac{2L(2,\chi_D)}{\zeta(4)} \cdot \frac{p(p-\chi)}{p^2+\chi} \cdot \prod_\ell e_\ell(t).$$

The factor at p is $(1-\chi/p)(1-\chi p^{-2})/(1-p^{-4}) = p(p-\chi)/(p^2+\chi)$. Since $t^{3/2} = D^{3/2} f^3$, we have

$$t^{3/2} \prod_\ell e_\ell(t) = D^{3/2} \sum_{d \mid f} \mu(d)\chi_D(d) d\sigma_3(f/d).$$

The functional equation of the even character χ_D gives $D^{3/2}L(2,\chi_D) = -2\pi^2 L(-1,\chi_D)$. With $\zeta(4) = \pi^4/90$, equation (3) becomes

$$\mathbb{E}[r_{q_\theta}(t)] = \frac{\pi^2}{3p} \cdot \frac{180}{\pi^4} \cdot \frac{p(p-\chi)}{p^2+\chi} \cdot (-2\pi^2) H(2,t) = -120 H(2,t) \frac{p-\chi}{p^2+\chi}.$$

Since $r^*_q(t) = \sum_{f^2 \mid t} \mu(f) r_q(t/f^2)$ and $(t/f^2\,/\,p) = (t/p)$, Möbius inversion gives the primitive version. Multiplying by M_p gives the absolute form. □

The constant $C(t)$ has a geometric meaning, which we explain now and prove in Section 5.2.

Remark 4.3. The notation $C(t)$ is chosen for the following reason. By van der Geer [9, Chapter IX], the class of the Humbert surface H_Δ in $\operatorname{Pic}(\mathcal{A}_2) \otimes \mathbb{Q}$ is a multiple of the Hodge class, and the multiple is given by the coefficients of the Eisenstein series of weight $5/2$. In our normalisation this reads $[H_\Delta] = C(\Delta)\lambda_1$. It agrees with $[H_1] = 5\lambda_1$ and $[H_4] = 30\lambda_1$, the divisor of χ_{35} being $H_1 + H_4$. The identification is proved in Section 5.2 from the recurrence of van der Geer. Nothing in this section or in the proof of Theorem 5.2 uses it.

5. First moments of splittings and the Humbert weight

In this section we specialise the first-moment formula to squares $t = N^2$ and prove part (1) of the main theorem. We first check that primitive vectors of value N^2 are the same as elliptic subgroups of degree N (Lemma 5.1), so that the first moment of s_N is a representation number. We then evaluate the Cohen number at a square. We also give a second, elementary proof of the same formula by gluing two elliptic curves along their N-torsion. That proof does not use the genus, so it confirms this consequence of the measure transfer theorem independently. In the second half of the section we show that the constant $5NJ_2(N)$ is the Humbert weight $k(H_{N^2})$ of [26, 27]. This connects the main theorem with the geometric bound of those papers.

5.1. Splittings and primitive vectors.

Lemma 5.1. *Let (A,θ) be superspecial and $N \geq 1$. The map $E \mapsto [E] \bmod \mathbb{Z}\theta$ is a bijection from the set of elliptic subgroups $E \subset A$ with $E \cdot \theta = N$ onto the set of primitive $w \in \mathrm{NS}(A)/\mathbb{Z}\theta$ with $q_\theta(w) = N^2$. Complementary subgroups map to opposite vectors. Hence $r^*_{q_\theta}(N^2) = 2s_N(A,\theta)$.*

Proof. Let E be an elliptic subgroup of degree N. Since $[E]^2 = 0$,

$$q_\theta([E]) = (E \cdot \theta)^2 - 2[E]^2 = N^2.$$

Its image w is primitive. Indeed, suppose $w = kw'$ with $k \geq 2$. Then $q_\theta(w') = (N/k)^2$, so $k \mid N$. Since $q_\theta(w') \equiv N/k \pmod 2$, Lemma 3.2 gives a lift D' of w' with $D' \cdot \theta = N/k$. Then kD' and $[E]$ have the same

image and the same degree, so $[E] = kD'$, which contradicts primitivity. The map is injective: if $[E] \equiv [F]$ with $E \cdot \theta = F \cdot \theta = N$, then $[E] - [F] = m\theta$ with $2m = 0$, so $E = F$.

Conversely let w be primitive with $q_\theta(w) = N^2$. By Lemma 3.2 it has a lift D with $D \cdot \theta = N$, and then

$$D^2 = \tfrac{1}{2}\big(N^2 - q_\theta(w)\big) = 0.$$

The class D is primitive since w is. So $D = [E]$ for an elliptic subgroup E, by Kani's theorem. Finally $[E] + [E'] = N\theta$ gives $[E'] \equiv -[E]$. □

We can now prove part (1) of the main theorem.

Theorem 5.2. *Let $p \equiv 3 \pmod 4$ and $p \nmid N$. Then*

$$\mu_N(p) = \mathbb{E}[s_N] = 5NJ_2(N)\,\frac{p-1}{p^2+1}.$$

Proof. By Lemma 5.1 and Theorem 4.2 with $t = N^2$ and $\chi = 1$ we have $\mathbb{E}[s_N] = C(N^2)(p-1)/(p^2+1)$. It remains to compute $C(N^2)$. Here $D = 1$ and $L(-1, \chi_1) = -\frac{1}{12}$. So $H(2, N^2) = -\frac{1}{12}g(N)$ with $g(N) = \sum_{d|N} \mu(d)\, d\, \sigma_3(N/d)$, and $H^*(2, N^2) = -\frac{1}{12}(\mu * g)(N)$. Both g and $\mu * g$ are multiplicative, and for $a \geq 1$

$$(\mu * g)(\ell^a) = \big(\sigma_3(\ell^a) - \sigma_3(\ell^{a-1})\big) - \ell\big(\sigma_3(\ell^{a-1}) - \sigma_3(\ell^{a-2})\big) = \ell^{3a} - \ell^{3a-2},$$

where the last bracket is read as 1 when $a = 1$. Hence $(\mu * g)(N) = NJ_2(N)$ and $C(N^2) = 5NJ_2(N)$. □

The case $N = 1$ is a useful check, because the answer is known by a direct count.

Example 5.3. For $t = 1$, Theorem 4.2 gives $\mathbb{E}[r^*(1)] = 10(p-1)/(p^2+1)$. A vector of q_θ-value 1 is the class of an elliptic subgroup of degree 1. Such a subgroup exists exactly when (A, θ) is a product $E_1 \times E_2$ with the product polarization, and then $r^*(1) = 2$. So the weighted proportion of product nodes is $5(p-1)/(p^2+1)$. This can be checked independently. The products contribute

$$\frac{1}{2}\Big(\sum_E \frac{1}{\#\operatorname{Aut} E}\Big)^2 = \frac{(p-1)^2}{1152}$$

to the mass, and dividing by (1) gives $5(p-1)/(p^2+1)$ again. This is the proportion $5/p$ of product nodes in the random walk given in [5, Section 2.2]. The unweighted proportion of isomorphism classes is $10/p + O(p^{-2})$, since products have $\#\operatorname{Aut} \geq 4$.

The formula for μ_N can also be obtained without quadratic forms. We include this second proof because it tests Theorem 3.4 from outside the theory of the genus.

Remark 5.4 (An elementary proof of Theorem 5.2)**.** By Kani [14], an optimal (N, N)-splitting of (A, θ) is the same as a triple (E, E', ψ), where E, E' are elliptic curves and $\psi\colon E[N] \to E'[N]$ is an anti-isometry for the Weil pairings. Here $A = (E \times E')/\operatorname{graph}(\psi)$ and θ is the descended polarization. This is an equivalence of groupoids, and the automorphisms of a triple are the elements of $\operatorname{Aut} E \times \operatorname{Aut} E'$ compatible with ψ. For $p \nmid N$ the anti-isometries form a torsor under $\mathrm{SL}_2(\mathbb{Z}/N)$, which has order $NJ_2(N)$, and A is superspecial if and only if E and E' are supersingular. We count with groupoid weights. The triples (E, E', ψ) and (E', E, ψ^{-1}) give the same unordered pair of complementary subgroups, so

$$\sum_{(A,\theta)} \frac{s_N(A,\theta)}{\#\operatorname{Aut}(A,\theta)} = \frac{1}{2}\sum_{(E,E')} \frac{NJ_2(N)}{\#\operatorname{Aut} E\,\#\operatorname{Aut} E'} = \frac{NJ_2(N)}{2}\Big(\frac{p-1}{24}\Big)^2$$

by Eichler's formula. Dividing by (1) gives $\mu_N = 5NJ_2(N)(p-1)/(p^2+1)$. This proof uses neither the genus $\mathcal{G}_p$ nor Siegel's theorem. So it is an independent confirmation of the consequence of Theorem 3.4 at every square $t = N^2$. It does not extend to non-square t or to second moments, where the refined Humbert invariant is needed.

5.2. **The Humbert weight.** The main theorem says that the expected number of splittings is $5NJ_2(N)(p-1)/(p^2+1)$. The earlier paper [27] bounded the proportion of split nodes above by $k(H_{N^2})(p-1)/(p^2+1)$, where $k(H_{N^2})$ was obtained from intersection theory on the moduli space. We now show that the two constants agree for all $N \geq 3$. This identifies the first moment with a geometric degree, and it will allow us to say in Section 8 exactly how much the geometric bound overestimates the probability. We first recall the quantities of [26]. In [26] the weight of the Siegel modular form with divisor H_{N^2} is shown to be $k(H_{N^2}) = 12\nu(N) + 12\widetilde{R}(N)$ for $N \geq 3$. Here $\nu(N) = \deg(X_1(N) \to X(1))$, which equals $\frac{1}{2}\varphi(N)\psi(N) = \frac{1}{2}J_2(N)$ for $N \geq 3$ and 3 for $N = 2$, and

$$\widetilde{R}(N) = \sum_{\substack{x \in \mathbb{Z},\ |x|<N \\ x \equiv N \ (2)}} \ \sum_{\substack{u \geq 1,\ (u,x)=1 \\ u^2 \mid (N^2-x^2)/4}} \psi\Big(\frac{N^2-x^2}{4u^2}\Big),$$

which is the degree of the intersection curve $H_{N^2} \cap H_1$. The weighted degree of the equation F_N of the locus of genus-two curves with a maximal degree-N elliptic subcover is $\deg_w F_N = k(H_{N^2}) - 10\nu(N)$.

We distinguish the reduced divisor class from the weight convention of [26, 27]. Write $[H_\Delta] = \kappa_\Delta \lambda_1$ for the class of the reduced Humbert divisor on the moduli stack. Put $v(1) = v(4) = \frac{1}{2}$ and $v(\Delta) = 1$ otherwise. In the convention of those papers,

$$\kappa_\Delta = v(\Delta) k(H_\Delta).$$

The factor v accounts for the extra generic involution at discriminants 1 and 4. It is not the reciprocal of the full generic automorphism order, which also includes ± 1. Concretely, $\operatorname{div}(\chi_{10}) = 2H_1$ and $\operatorname{div}(\chi_{35}) = H_1 + H_4$, so $\operatorname{div}(\chi_{35}^2/\chi_{10}) = 2H_4$. Thus $\kappa_1 = 5$ and $\kappa_4 = 30$, whereas $k(H_1) = 10$ and $k(H_4) = 60$. Interpreting κ_Δ as a rational divisor-class coefficient avoids the need for a modular form with trivial character and multiplicity-one divisor at these two discriminants.

The recurrence of van der Geer [9], stated in [10, Theorem 5.1], reads in Cohen's normalisation

$$\sum_{x^2 \mid \Delta} v(\Delta/x^2)\, k(H_{\Delta/x^2}) = -60 H(2, \Delta), \tag{8}$$

with $k(H_t) = 0$ when t is not a discriminant. The sign reflects that Cohen's coefficients $H(2,t)$ are negative for positive discriminants, while the divisor degrees are positive. At $\Delta = 1, 4, 9$ the recurrence gives $k(H_1) = 10$, $k(H_4) = 60$ and $k(H_9) = 120$, which are the weights of χ_{10}, of χ_{35}^2/χ_{10}, and of the form of [26] with divisor H_9. Möbius inversion over the squares dividing Δ gives

$$\kappa_\Delta = v(\Delta) k(H_\Delta) = -60 H^*(2, \Delta) = C(\Delta),$$

which proves the identification of Remark 4.3.

Proposition 5.5. *For every $N \geq 3$ we have $k(H_{N^2}) = 5NJ_2(N) = C(N^2)$, $\widetilde{R}(N) = J_2(N)(5N-6)/12$, and $\deg_w F_N = 10(N-1)\nu(N)$. The degree formula also holds at $N = 2$, where $k(H_4) = 60$, $\nu(2) = 3$ and $\deg_w F_2 = 30$. Hence for all $N \geq 3$ the bound $k(H_{N^2})(p-1)/(p^2+1)$ of* [27, Theorem 3] *equals $\mu_N(p)$.*

Proof. For $N \geq 3$ we have $v(N^2) = 1$, and (8) inverted gives $k(H_{N^2}) = C(N^2) = 5NJ_2(N)$ by the proof of Theorem 5.2. Then

$$12\widetilde{R}(N) = k(H_{N^2}) - 12\nu(N) = 5NJ_2(N) - 6J_2(N), \qquad \deg_w F_N = k(H_{N^2}) - 10\nu(N) = 10(N-1)\nu(N).$$

At $N = 2$ the value $k(H_4) = 60$ was computed above, and $60 - 10 \cdot 3 = 30$. The divisor sum $\widetilde{R}(N)$ was also checked directly from its definition for $3 \leq N \leq 120$, and the weights agree with the values 120, 240, 600, 720, 1680, 3240 and 6600 tabulated in [27] for $N = 3, 4, 5, 6, 7, 9, 11$. These checks pin down the normalisation of (8). The last claim is Theorem 5.2. □

We close the section with a comment on the proof in [27], which explains why that paper obtained only an upper bound.

The proof of [27, Theorem 3] computes the intersection number $[H_{N^2}] \cdot [S_2]$ with the supersingular locus and discards the non-superspecial intersection points. For $p \nmid N$ there are none, because an optimally (N,N)-split supersingular surface is a quotient of a product by a subgroup of order prime to p, and such a quotient is

superspecial. Whether the remaining lower bound on local multiplicities is attained depends on an identification of the local branches of H_{N^2} at a superspecial point with its splittings. We have not checked this.

6. Second moments and the proof of the main theorem

The first moment of s_N does not give the probability that $s_N \geq 1$, because a node may split in several ways. In this section we compute the second factorial moment $\mathbb{E}[s_N(s_N-1)]$, which controls this multiplicity, and we complete the proof of the main theorem. The idea is the same as in Section 4. By Theorem 3.4 the node average of a pair count is a genus average, and Siegel's theorem applies to the representation of a binary form by the quinary form. We do not compute all the local densities of this binary problem. Instead we show that the only dependence on p comes from the prime p itself, where the density can be computed, so that $(p^2+1)\mathbb{E}[s_N(s_N-1)]$ does not depend on p. The same argument gives the mixed moments $\mathbb{E}[s_M s_N]$. We then prove the main theorem, treat the product locus, and derive bounds for detectors that test several levels at once.

6.1. **Bounds from two moments.** We first record the elementary inequalities that turn two moments into bounds for a probability.

Lemma 6.1. *Let X be a nonnegative integer-valued random variable with $\mu = \mathbb{E}[X]$, $B = \mathbb{E}[X(X-1)]$ and $\delta = \mathbb{P}(X>0)$. Then*

$$\max\Big\{0,\ \mu - \tfrac{B}{2},\ \frac{\mu^2}{\mu+B}\Big\} \ \leq\ \delta \ \leq\ \min\{1,\mu\}, \tag{9}$$

where the quotient is read as 0 when $\mu = B = 0$.

Proof. The upper bound is Markov's inequality. For the first lower bound,

$$\mu - \delta = \mathbb{E}\big[(X-1)\mathbf{1}_{X\geq 2}\big] \leq \tfrac{1}{2}\mathbb{E}\big[X(X-1)\big] = \tfrac{B}{2},$$

since $X - 1 \leq \frac{1}{2}X(X-1)$ for $X \geq 2$. For the second, Cauchy–Schwarz gives

$$\mu^2 = \mathbb{E}\big[X\mathbf{1}_{X>0}\big]^2 \leq \mathbb{E}[X^2]\,\delta = (\mu+B)\,\delta.$$

□

Two moments do not determine δ. They confine it to an interval of length at most $B/2$.

6.2. **The second factorial moment for general N.** To count ordered pairs of splittings we need representation numbers of binary forms. We set up the notation. Let T be a positive definite binary form, written as a symmetric matrix $\left(\begin{smallmatrix} a & m \\ m & c \end{smallmatrix}\right)$ with $a, c, m \in \mathbb{Z}$. For a quadratic lattice M with bilinear form b let $R_M(T)$ be the number of pairs $(x_1, x_2) \in M^2$ with $q(x_1) = a$, $q(x_2) = c$ and $b(x_1, x_2) = m$. Let $R^*_M(T)$ be the number of such pairs with x_1 and x_2 each primitive. For $d_1, d_2 \geq 1$ let

$$T[d_1, d_2] = \begin{pmatrix} a/d_1^2 & m/d_1 d_2 \\ m/d_1 d_2 & c/d_2^2 \end{pmatrix}$$

whenever this matrix is integral. If $x_i = d_i y_i$ with y_i primitive, then the Gram matrix of (y_1, y_2) is $T[d_1, d_2]$. Hence

$$R^*_M(T) = \sum_{d_1, d_2} \mu(d_1)\mu(d_2) R_M(T[d_1, d_2]), \tag{10}$$

where the sum runs over the pairs for which $T[d_1, d_2]$ is integral.

Of the local densities of this binary problem we shall need only those at the primes that do not divide $2 \det T$, and in particular the one at p.

Lemma 6.2. *Let T be a positive definite binary form and ℓ a prime with $\ell \nmid 2 \det T$. The ℓ-adic density of T by $\langle 1,1,1,1,1\rangle$ is $1 - \ell^{-4}$. For $\ell = p$, the p-adic density of T by $L_p = \langle 1,1,1\rangle \perp p\langle 1,1\rangle$ is $1 - p^{-2}$.*

Proof. The density is $\lim_k \ell^{-7k}\#\{X \in M_{5\times 2}(\mathbb{Z}/\ell^k) : X^tGX \equiv T\}$. Since T is nondegenerate modulo ℓ, every solution modulo ℓ is non-singular and lifts to $\ell^{7(k-1)}$ solutions modulo ℓ^k. So the density is ℓ^{-7} times the count over $\mathbb{F}_\ell$. By Witt's theorem the embeddings of a nondegenerate binary space into a nondegenerate n-dimensional space V over $\mathbb{F}_\ell$ number $\#O(V)/\#O(T^\perp)$, provided one embedding exists, which is the case when $n \geq 3$. For $n = 5$ this is

$$\frac{\#O_5(\mathbb{F}_\ell)}{\#O_3(\mathbb{F}_\ell)} = \frac{2\ell^4(\ell^2-1)(\ell^4-1)}{2\ell(\ell^2-1)} = \ell^3(\ell^4-1),$$

giving the density $\ell^{-7}\cdot\ell^3(\ell^4-1) = 1-\ell^{-4}$. For L_p write $X = (Y, Z)$ with $Y \in M_{3\times 2}$. Modulo p the condition is $Y^tQ_3Y \equiv T$ and Z is free, so the count is

$$p^4 \cdot \frac{\#O(Q_3)}{\#O(T^\perp)} = p^4 \cdot \frac{2p(p^2-1)}{2} = p^5(p^2-1),$$

giving the density $1-p^{-2}$. □

We now prove part (2) of the main theorem.

Theorem 6.3. *Let $N \geq 2$. There is a constant c_N such that for every prime $p \equiv 3 \pmod 4$ with $p > 2N^2$,*

$$B_N(p) = \mathbb{E}\big[s_N(s_N-1)\big] = \frac{c_N}{p^2+1}.$$

For $N \leq 7$ the constants are $c_N = 660,\ 12600,\ 53520,\ 343320,\ 501840,\ 2754960$.

Proof. By Lemma 5.1, $s_N(s_N-1)$ is one quarter of the number of ordered pairs (w_1, w_2) of primitive vectors of q_θ-value N^2 with $w_2 \neq \pm w_1$. Such w_1, w_2 are linearly independent. So their Gram matrix is

$$T_m = \begin{pmatrix} N^2 & m \\ m & N^2 \end{pmatrix}, \qquad m = b(w_1,w_2), \quad |m| < N^2.$$

Hence

$$s_N(s_N-1) = \tfrac{1}{4}\sum_{|m|<N^2} R^*_{q_\theta}(T_m) = \tfrac{1}{4}\sum_{|m|<N^2}\sum_{d_1,d_2}\mu(d_1)\mu(d_2)R_{q_\theta}(T_m[d_1,d_2]).$$

This is a finite combination of representation numbers of positive definite binary forms T' with $\det T' \mid N^4-m^2$, with coefficients independent of p. By Theorem 3.4 the node average of $R_{q_\theta}(T')$ is the Siegel average over $\mathcal{G}_p$. Siegel's theorem for a quinary form representing a binary form gives

$$\mathbb{E}_p[R(T')] = \frac{\pi^{9/2}}{\Gamma(5/2)\Gamma(2)}\,\det(T')\,(\det G)^{-1}\prod_\ell \alpha_\ell(L,T'),$$

with $\det G = 16p^2$ and $\kappa = \pi^{9/2}/(\Gamma(5/2)\Gamma(2))$; here the rank 5 of L exceeds $2+1$, so the factor ε of Siegel's theorem is 1.

We now compare two primes. Let p, p' be primes $\equiv 3 \pmod 4$ with $p, p' > 2N^2$, and write L_p and $L_{p'}$ for the two base lattices. Then $p, p' \nmid 2N\det T'$, because

$$\det T' \;\big|\; N^4 - m^2 = (N^2-m)(N^2+m)$$

and both factors lie in $[1, 2N^2-1]$. By Lemma 4.1 the completions of L_p and $L_{p'}$ coincide at every prime $\ell \notin \{p, p'\}$. At the primes p and p' themselves, Lemma 6.2 gives

$$\alpha_p(L_p,T') = 1-p^{-2}, \qquad \alpha_p(L_{p'},T') = 1-p^{-4}, \qquad \alpha_{p'}(L_{p'},T') = 1-p'^{-2}, \qquad \alpha_{p'}(L_p,T') = 1-p'^{-4},$$

since $L_{p'}\otimes\mathbb{Z}_p \cong \langle 1,1,1,1,1\rangle$ and symmetrically. Write

$$P(T') = \prod_{\ell\notin\{p,p'\}} \alpha_\ell(L,T'),$$

which is the same for both lattices. It may vanish, when T' is not represented locally at 2, and then both sides below are 0. Otherwise

$$(p^2+1)\,\mathbb{E}_p[R(T')] = \kappa\,\det(T')\,P(T')\,\frac{(p^2+1)(1-p^{-2})(1-p'^{-4})}{16p^2}$$
$$= \kappa\,\det(T')\,P(T')\,\frac{(p^4-1)(p'^4-1)}{16p^4p'^4} = (p'^2+1)\,\mathbb{E}_{p'}[R(T')],$$

because the middle expression is symmetric in p and p'. Summing over m, d_1, d_2 with the fixed coefficients gives

$$B_N(p)\,(p^2+1) = B_N(p')\,(p'^2+1).$$

The values of c_N for $N \le 7$ are read off from the enumerations at $p = 131$ and $p = 167$, which both exceed $2 \cdot 49$; see Section 6.3. □

6.3. **Determination of the constants.** The proof of Theorem 6.3 shows that $B_N(p)(p^2+1)$ does not depend on p once $p > 2N^2$, but it does not evaluate the constant. The values of c_N for $N \le 7$, and the mixed constants of Section 6.4 below, were read off from complete enumerations of the genus $\mathcal{G}_p$ at $p = 131$ and $p = 167$. For these values to be part of the theorems, the enumerations must be provably complete. The enumeration uses Kneser's neighbour method, which produces the whole genus only when the genus consists of a single spinor genus and the neighbour prime is suitable. The next lemma verifies both conditions.

Lemma 6.4. *Let $p \equiv 3 \pmod 4$ with $p \neq 3$. Every class of $\mathcal{G}_p$ is obtained from q_5 by a finite chain of Kneser 3-neighbours.*

Proof. Kneser's neighbour method connects the classes in a spinor genus when the rational quadratic space is isotropic at the neighbour prime [20, 2]. Here $3 \nmid 2\det G$, and $L \otimes \mathbb{Q}_3$ is isotropic because the nondegenerate rank-5 reduction modulo 3 has a nonzero isotropic vector, which lifts.

It remains to show that the genus has a single spinor genus. A sufficient criterion is that for every finite prime ℓ the spinor norms of the proper integral isometries of L_ℓ contain $\mathbb{Z}_\ell^\times(\mathbb{Q}_\ell^\times)^2$ [2, Chapter 11]. For odd ℓ, Lemma 4.1 gives a unimodular sublattice of rank at least 3, which represents every unit. Reflections in vectors of unit norm are integral. Composing one of norm u with one of norm 1 gives a proper isometry of spinor norm u modulo squares.

At $\ell = 2$, the lattice L_2 contains the orthogonal summand $4U$ with $q(x_1, x_2) = 4x_1x_2$. In the convention $b(x,x) = q(x)$, the reflection in a vector v is

$$x \longmapsto x - \frac{2b(x,v)}{q(v)}\,v.$$

For $v = (u, 1)$ with $u \in \mathbb{Z}_2^\times$ we have $q(v) = 4u$ and $2b(x,v) = 4(x_1 + ux_2)$. So the reflection is integral on $4U$ and fixes its orthogonal complement. Its product with the reflection in $(1,1)$ is proper and has spinor norm $16u \equiv u$ modulo squares. This proves the criterion and the claim. □

The genera were enumerated by 3-neighbours with PARI/GP [23], testing isometry with `qfisom` after hashing by theta coefficients, for the twelve primes $p = 7$, 11, 19, 23, 31, 43, 47, 59, 67, 71, 131, 167. By Lemma 6.4 each enumeration is complete. The class numbers are 2, 5, 9, 15, 22, 37, 58, 95, 98, 144, 621, 1152, and in every case $\sum_M 1/\#O(M) = M_p/2$, as Proposition 3.5 requires. The constants c_N in Theorem 6.3 are the values of $B_N(p)(p^2+1)$ at $p = 131$ and $p = 167$, which agree; the enumerations at the smaller primes show that the identity $B_N(p)(p^2+1) = c_N$ also holds for some primes below $2N^2$, but not for all. The enumerated genera, the scripts and a driver that reproduces every computation in the paper are available from the author on request.

Remark 6.5. The proof shows that $c(T') = (p^2+1)\mathbb{E}_p[R(T')]$ does not depend on p for $p > 2N^2$, and that $c_N = \frac{1}{4}\sum_{|m|<N^2}\sum_{d_1,d_2}\mu(d_1)\mu(d_2)\,c(T_m[d_1,d_2])$. Each $c(T')$ is determined by the local densities of T' at the primes dividing $2\det T'$, hence at primes $\ell \mid 2N(N^4-m^2)$, and we have not evaluated these in closed form. At $N = 3$ and $p = 7$, for instance, $B_3(p)(p^2+1) = 10080$, not 12600.

6.4. **Mixed moments.** A detector that tests several levels at once needs the mixed moment $\mathbb{E}[s_M s_N]$, which together with the first moments gives the covariance of s_M and s_N. It does not give the joint distribution, and in particular it does not give $\mathbb{P}(s_M > 0, s_N > 0)$. The argument of Theorem 6.3 gives the mixed moment with no extra work.

Theorem 6.6. *Let $1 \le M < N$. There is a constant $c_{M,N}$ such that for every prime $p \equiv 3 \pmod 4$ with $p > 2MN$,*

$$\mathbb{E}[s_M s_N] = \frac{c_{M,N}}{p^2+1}.$$

Proof. By Lemma 5.1, $s_M s_N$ is one quarter of the number of ordered pairs (w_1, w_2) of primitive vectors with $q_\theta(w_1) = M^2$ and $q_\theta(w_2) = N^2$. Primitive vectors of different norms are never proportional. So (w_1, w_2) is linearly independent, with Gram matrix

$$\begin{pmatrix} M^2 & m \\ m & N^2 \end{pmatrix}, \qquad |m| < MN.$$

Its determinant $(MN-m)(MN+m)$ has both factors in $[1, 2MN-1]$. The proof of Theorem 6.3 now applies without change. □

TABLE 1. The constants $c_{M,N} = \mathbb{E}[s_M s_N](p^2+1)$ for $p > 2MN$, from the complete enumerations at $p = 131$ and $p = 167$ (Section 6.3), which agree. The diagonal is $c_N = \mathbb{E}[s_N(s_N-1)](p^2+1)$.

$M\backslash N$	1	2	3	4	5	6	7
1	0	60	360	840	2280	2880	6960
2		660	2880	6120	15840	19440	46080
3			12600	25920	66240	80640	190080
4				53520	135360	164160	385920
5					343320	414720	973440
6						501840	1175040
7							2754960

6.5. **Proof of the main theorem.** All ingredients of the main theorem are now in place.

Proof of Theorem 2.1. Part (1) is Theorem 5.2. Part (2) is Theorem 6.3. For part (3) apply Lemma 6.1 to $X = s_N$. The bound $\mu - B/2 \le \delta \le \mu$ with the values from (1) and (2) is the displayed inequality. Finally $\mu_N(p) = 5NJ_2(N)/p + O_N(p^{-2})$ and $c_N/(2(p^2+1)) = O_N(p^{-2})$. □

6.6. **The product locus.** The mixed moments with $M = 1$ concern products of elliptic curves. For these we can compute the constant in closed form by counting isogenies instead of applying Siegel's theorem, and the answer is an intersection number. Recall that $\widetilde{R}(N)$, defined in Section 5.2, is the degree of the curve $H_{N^2} \cap H_1$.

Proposition 6.7. *Let $N \ge 2$ and $p \equiv 3 \pmod 4$ with $p > N^2/4$. Then*

$$\mathbb{E}[s_1 s_N] = \frac{60\,\widetilde{R}(N)}{p^2+1} = \frac{5J_2(N)(5N-6)}{p^2+1}.$$

Proof. The number s_1 is 1 on products with the product polarization and 0 elsewhere. So

$$\mathbb{E}[s_1 s_N]\, M_p = \sum_{\{E_1, E_2\}} \frac{s_N(E_1 \times E_2)}{\#\operatorname{Aut}(E_1 \times E_2, \theta)},$$

the sum over unordered pairs of supersingular curves. We compute s_N of a product. For the product polarization

$$q_\theta \cong \langle 1 \rangle \perp 4\deg \qquad \text{on } \mathbb{Z} \oplus \operatorname{Hom}(E_1, E_2)$$

[17, Section 3]. So by Lemma 5.1, $2s_N$ is the number of primitive pairs (x,φ) with $x^2+4\deg\varphi = N^2$. Every isogeny φ occurring here has degree at most $N^2/4 < p$, so it is separable. Its kernel has elementary divisors (u, uv), so it factors uniquely as $\varphi = [u]\circ\varphi_0$ with $u \geq 1$ and φ_0 cyclic. Equivalently u is the largest positive integer dividing φ in $\mathrm{Hom}(E_1, E_2)$. Then

$$x \equiv N \pmod 2, \qquad |x| < N, \qquad u^2 \mid d_x := \frac{N^2-x^2}{4}, \qquad \deg\varphi_0 = \frac{d_x}{u^2},$$

and (x,φ) is primitive exactly when $(u,x)=1$.

Next we count cyclic isogenies. Let $d \leq N^2/4$. Then $p \nmid d$, and a supersingular E_1 has $\psi(d)$ cyclic subgroups of order d. Each is the kernel of $\#\operatorname{Aut}(E_2)$ cyclic isogenies onto the representative E_2 of its quotient. So

$$\sum_{E_2} \frac{\#\{\varphi_0 \colon E_1 \to E_2 \text{ cyclic of degree } d\}}{\#\operatorname{Aut}(E_2)} = \psi(d).$$

Summing over ordered pairs with weights $1/(\#\operatorname{Aut} E_1 \#\operatorname{Aut} E_2)$ and using Eichler's formula gives

$$\sum_{(E_1,E_2)} \frac{2s_N(E_1\times E_2)}{\#\operatorname{Aut} E_1 \#\operatorname{Aut} E_2} = \frac{p-1}{24} \sum_{\substack{|x|<N \\ x\equiv N\,(2)}} \sum_{\substack{u^2\mid d_x \\ (u,x)=1}} \psi(d_x/u^2) = \frac{p-1}{24}\widetilde{R}(N).$$

Now $\#\operatorname{Aut}(E_1\times E_2,\theta) = \#\operatorname{Aut} E_1 \#\operatorname{Aut} E_2$ for $E_1 \not\cong E_2$, and it is $2\#\operatorname{Aut}(E)^2$ for $E_1 = E_2 = E$. So the sum over ordered pairs is twice the sum over nodes, and

$$\mathbb{E}[s_1 s_N]\, M_p = \frac{(p-1)\widetilde{R}(N)}{96}.$$

Dividing by (1) gives the first expression. The second expression is Proposition 5.5 for $N \geq 3$. At $N=2$ one has $\widetilde{R}(2)=1$ and $5J_2(2)(5\cdot 2-6) = 60$. □

The values $c_{1,N} = 60\widetilde{R}(N)$ in Table 1 are 60 times $1, 6, 14, 38, 48, 116$, which are the degrees of $H_{N^2}\cap H_1$ tabulated in [27].

6.7. **Several levels.** We now combine the moments into statements about a detector that tests a finite set S of levels. The relevant random variable is $\sum_{N\in S} s_N$, and its first two moments are sums of the constants computed above.

Corollary 6.8 (Detection at several levels)**.** *Let S be a nonempty finite set of positive integers. Write $\delta_S(p) = \mathbb{P}(\sum_{N\in S} s_N > 0)$ and put*

$$a_N = 5NJ_2(N), \qquad A_S = \sum_{N\in S} a_N, \qquad C_S = \sum_{N\in S} c_N + 2\sum_{\substack{M<N \\ M,N\in S}} c_{M,N},$$

where $c_1 = 0$. Let $p \equiv 3 \pmod 4$ with $p > 2(\max S)^2$, and set

$$\mu_S = \frac{A_S(p-1)}{p^2+1}, \qquad B_S = \frac{C_S}{p^2+1}.$$

Then

$$L_S := \max\left\{0,\ \mu_S - \frac{B_S}{2},\ \frac{\mu_S^2}{\mu_S+B_S}\right\} \ \leq\ \delta_S(p)\ \leq\ U_S := \min\{1,\mu_S\}. \tag{11}$$

In particular

$$0 \leq 1 - \frac{\delta_S}{\mu_S} \leq \frac{C_S}{2A_S(p-1)}, \qquad \delta_S(p) = \frac{A_S}{p} + O_S(p^{-2}).$$

The level 1 means success at a product with the product polarization.

Proof. Take $X_S = \sum_{N\in S} s_N$. Its first moment is μ_S by Theorem 5.2. Expanding $X_S(X_S-1)$ and applying Theorems 6.3 and 6.6 gives $\mathbb{E}[X_S(X_S-1)] = B_S$. The diagonal term for $N=1$ vanishes because s_1 is an indicator. Now apply Lemma 6.1. Dividing $0 \leq \mu_S - \delta_S \leq B_S/2$ by μ_S gives the relative bound. □

We illustrate with the levels that appear in [5, 27].

Example 6.9. For $S = \{4, 6\}$, Table 1 gives $A_S = 960$ and $C_S = 883680$. Hence, for $p > 72$,

$$\frac{960(p-1) - 441840}{p^2+1} \le \delta_{\{4,6\}}(p) \le \min\left\{1, \frac{960(p-1)}{p^2+1}\right\}.$$

The nonnegative and Cauchy–Schwarz lower bounds in (11) remain useful when the displayed lower bound is negative. Including products gives $A_{\{1,4,6\}} = 965$ and $C_{\{1,4,6\}} = 891120$. So the common policy of stopping at either a product or a detected split surface is covered by the same formula.

A practical question is whether adding a level to a detector is worth its cost. The following bound isolates the gain in target probability.

Corollary 6.10 (Adding one level)**.** *Let S be as in Corollary 6.8, let $N \notin S$, and let $p > 2(\max(S \cup \{N\}))^2$. With $c_{M,N} = c_{N,M}$ when $M > N$,*

$$\max\left\{0,\ \mu_N - \frac{c_N/2 + \sum_{M\in S} c_{M,N}}{p^2+1}\right\} \le \delta_{S\cup\{N\}} - \delta_S \le \min\{1, \mu_N\}.$$

For fixed S and N the gain is $a_N/p + O_{S,N}(p^{-2})$.

Proof. The gain equals $\mathbb{P}(s_N > 0 \text{ and } s_M = 0 \text{ for all } M \in S)$. This is $\mathbb{P}(s_N > 0)$ minus at most

$$\sum_{M\in S} \mathbb{P}(s_M > 0,\ s_N > 0) \ \le\ \sum_{M\in S} \mathbb{E}[s_M s_N].$$

Now use Lemma 6.1 for s_N. □

The mixed moment counts simultaneous witnesses, not just membership in an intersection. This makes the connection with [25] precise. Over $\mathbb{C}$, that paper classifies three rational families of genus-two curves with elliptic subcovers of degrees 2 and 3. Here

$$\mathbb{E}[s_2 s_3] = \frac{2880}{p^2+1} \qquad (p > 12)$$

is the total arithmetic incidence count, with automorphism weights and splitting multiplicities included. Distributing this number among the reductions of those families requires identifying the reductions, the exceptional primes and the multiplicities, and accounting separately for products. The characteristic-zero classification alone does not supply that distribution.

7. The exact case $N = 2$ and the two measures

The main theorem applies at $N = 2$, but at this level we can do better than a two-sided bound. A $(2, 2)$-splitting of a Jacobian is the same as a pair $\{\sigma, \iota\sigma\}$ of non-hyperelliptic involutions of the curve, where ι is the hyperelliptic involution, so the number of non-hyperelliptic involutions is $2s_2$. The superspecial curves with extra automorphisms were counted by Ibukiyama, Katsura and Oort. In this section we use their counts to give δ_2 exactly. The same case shows that the choice of measure matters. The walk measure and the uniform measure on isomorphism classes give different first-order answers at $N = 2$. We then prove that they agree to first order for every $N \ge 3$.

Theorem 7.1. *Let $p \ge 7$ with $p \equiv 3 \pmod 4$, and let $\varepsilon_d = 1 - (-d/p)$ for $d = 2, 3$. Then*

$$\delta_2(p) = \frac{10(3p-28)}{p^2+1} + \frac{360\varepsilon_2 + 240\varepsilon_3}{(p-1)(p^2+1)}, \qquad B_2(p) = \frac{660}{p^2+1}.$$

Consequently $\delta_2(p) = 30/p + O(p^{-2})$ and $\mu_2 - \delta_2 = O(p^{-2})$.

Proof. A superspecial node with $s_2 \ge 1$ is either a Jacobian whose curve has a non-hyperelliptic involution, or a product $E \times E$. Indeed, for a product $E_1 \times E_2$ an elliptic subgroup of degree 2 has projections of degrees 1 and 1, so it is the graph of an isomorphism $E_1 \to E_2$. The products $E \times E$ have $\#\operatorname{Aut} = 2\#\operatorname{Aut}(E)^2$

and $s_2 = \#\operatorname{Aut}(E)/2$, since the graphs of automorphisms come in complementary pairs $\alpha, -\alpha$. By Eichler's formula, with $\varepsilon_1 = 1 - (-1/p) = 2$, their weighted mass is

$$W_P = \sum_E \frac{1}{2\#\operatorname{Aut}(E)^2} = \frac{p-1}{96} - \frac{\varepsilon_1}{64} - \frac{\varepsilon_3}{72},$$

and their contribution to B_2 is $\sum_E s_2(s_2-1)/(2\#\operatorname{Aut}(E)^2)$. Now we turn to Jacobians. For $p \geq 7$ the genus-two curves with a non-hyperelliptic involution are those with reduced automorphism group C_2, $C_2 \times C_2$, S_3, D_6 or S_4, where D_6 is the dihedral group of order 12. Their automorphism groups and splitting numbers are

reduced group	C_2	$C_2 \times C_2$	S_3	D_6	S_4
$\#\operatorname{Aut}(C)$	4	8	12	24	48
s_2	1	2	3	4	6

The numbers of superspecial curves of each type are given by Ibukiyama, Katsura and Oort [13, Theorem 3.3]. Write n_g for the number of superspecial curves with $\#\operatorname{Aut}(C) = g$ among these five types. Specialising that theorem to $p \equiv 3 \pmod 4$, where $\varepsilon_1 = 2$, gives

$$n_4 = \frac{p^2 - 18p + 29}{48} + \frac{\varepsilon_2 + \varepsilon_3}{2}, \qquad n_8 = \frac{p-3}{8} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{2},$$
$$n_{12} = \frac{p-1}{6} - \frac{\varepsilon_2}{2} - \frac{\varepsilon_3}{3}, \qquad n_{24} = \frac{\varepsilon_3}{2}, \qquad n_{48} = \frac{\varepsilon_2}{2}.$$

These are classification formulas, and they were checked independently against the enumerated genera of Section 6.3. Summing n_g/g gives

$$W_J = \frac{(p-1)(3p-34)}{576} + \frac{\varepsilon_1}{64} + \frac{\varepsilon_2}{16} + \frac{\varepsilon_3}{18}.$$

Then

$$\delta_2 = \frac{W_J + W_P}{M_p}$$

is the stated formula, and the ε_1 terms cancel. Weighting the same counts by $s_2(s_2-1)$, together with the products, gives

$$B_2\, M_p = \frac{11(p-1)}{96}, \qquad \text{that is,} \qquad B_2 = \frac{660}{p^2+1}.$$

The quantities W_J, W_P, δ_2 and B_2 were each verified against the enumerations at all twelve primes. □

Remark 7.2. The weights matter at $N = 2$. A generic $(2,2)$-split Jacobian has $\#\operatorname{Aut} = 4$, while a generic node has $\#\operatorname{Aut} = 2$. So the uniform measure on isomorphism classes gives the split nodes twice the weight. For the walk measure $\mathbb{E}[s_2] \sim 30/p$, and for the uniform measure on classes $\mathbb{E}[s_2] \sim 60/p$; the same holds for the two probabilities. For $N \geq 3$ the two measures agree to first order. This needs an argument, because the locus of nodes with extra automorphisms has mass of the same order $1/p$ as the target. The argument is given next, with the help of the mixed moments.

Proposition 7.3. *Let $N \geq 3$ and $p \equiv 3 \pmod 4$ with $p > 2N^2$. Let $\delta_N^u(p)$ be the proportion of isomorphism classes of superspecial principally polarized surfaces that are optimally (N,N)-split. Then $\delta_N^u(p) = \delta_N(p) + O_N(p^{-2})$. The hypothesis $N \geq 3$ is used through Theorem 6.6 with $M = 2 < N$.*

Proof. Write X for the set of isomorphism classes and $X_N \subset X$ for the split ones. Let $Y \subset X$ be the set of classes with $\#\operatorname{Aut} > 2$, and write $\operatorname{mass}(Z) = \sum_Z 1/\#\operatorname{Aut}$ for $Z \subset X$. Then

$$\#X = \sum_X \frac{\#\operatorname{Aut}}{\#\operatorname{Aut}} = 2M_p + \sum_Y \frac{\#\operatorname{Aut} - 2}{\#\operatorname{Aut}},$$

and $\#\operatorname{Aut} \leq 72$. So $\#X = 2M_p + O(\operatorname{mass}(Y))$, and in the same way $\#X_N = 2M_p\delta_N + O(\operatorname{mass}(X_N \cap Y))$. For $p \geq 7$ the genus-two curves with a non-trivial reduced automorphism group have reduced group C_2, $C_2 \times C_2$, S_3, D_6, S_4 or C_5 [13, Section 1.2]. By that classification the first five types have a non-hyperelliptic involution. So a Jacobian in Y either has $s_2 \geq 1$ or is one of the finitely many curves with reduced group C_5. The other

elements of Y are products, where $s_1 = 1$. Hence, by Example 5.3 and Theorem 5.2 and by Theorem 6.6 and Proposition 6.7,

$$\frac{\mathrm{mass}(Y)}{M_p} \le \mathbb{E}[s_1] + \mathbb{E}[s_2] + O(p^{-3}) = O(1/p), \qquad \frac{\mathrm{mass}(X_N \cap Y)}{M_p} \le \mathbb{E}[s_1 s_N] + \mathbb{E}[s_2 s_N] + O(p^{-3}) = O_N(p^{-2}).$$

Therefore

$$\delta_N^u = \frac{\#X_N}{\#X} = \frac{2M_p\delta_N + O(M_p p^{-2})}{2M_p(1+O(1/p))} = \delta_N + O(p^{-2}),$$

using $\delta_N = O(1/p)$. □

8. Consequences for splitting detection

In this section we spell out what the main theorem says for the splitting-detection attack. We first compare the probability with the geometric bound of [27]. We then explain how the bounds of Section 6 enter a cost estimate for a detector, and what such an estimate assumes.

8.1. The geometric bound is sharp to first order.

Corollary 8.1. *For $N \ge 3$ and $p \equiv 3 \pmod 4$ with $p > 2N^2$,*

$$0 \;\le\; k(H_{N^2})\frac{p-1}{p^2+1} - \delta_N(p) \;\le\; \frac{c_N}{2(p^2+1)}.$$

For $N = 6$ and $p > 72$ this reads $0 \le 720(p-1)/(p^2+1) - \delta_6(p) \le 250920/(p^2+1)$.

Proof. By Proposition 5.5, $k(H_{N^2}) = 5NJ_2(N)$, so the first expression is μ_N. Now apply Theorem 2.1(3). □

So the intersection-theoretic bound of [27, Theorem 3] has the correct leading constant. It overestimates the probability because it counts each split node with the multiplicity of its splittings. The excess is exactly

$$\mu_N - \delta_N = \mathbb{E}\big[(s_N - 1)\mathbf{1}_{\{s_N>0\}}\big],$$

and the corollary bounds this excess by half the second factorial moment.

8.2. Target probabilities and cost.

For a fixed level set S, Corollary 6.8 gives both the leading target proportion A_S/p and a bound on the error at a finite prime. If the probability δ_S is replaced by its first moment μ_S, the error $\mu_S - \delta_S$ is at most $C_S/(2(p^2+1))$. Normalised by the first moment this is

$$\frac{\mu_S - \delta_S}{\mu_S} \le \frac{C_S}{2A_S(p-1)},$$

and normalised by the probability itself it is

$$\frac{\mu_S - \delta_S}{\delta_S} \le \frac{C_S}{2A_S(p-1) - C_S} \qquad \text{when } 2A_S(p-1) > C_S.$$

For example, at $S = \{3\}$ and $p = 131$ the enumeration gives $(\mu_3 - \delta_3)/\delta_3 = 11013/22787 \approx 0.483$, while the two bounds are $21/52 \approx 0.404$ and $21/31 \approx 0.677$. So the usefulness of the approximation depends on C_S/A_S as well as on the size of p. At the small primes of Table 2 many first moments exceed 1. There the clipped bounds in (11) should be used directly.

We now state a cost model. Assume that successive examined nodes are independent samples from the stationary measure. Let $K_S(p) > 0$ be the expected cost of obtaining and testing one such sample, including any walk, invariant-evaluation and detector costs charged to that sample. Costs must be expressed per sampled node. Shared computations and early stopping within a test contribute to K_S. Let T_S be the total cost up to and including the first successful sample. The renewal identity $\mathbb{E}[T_S] = K_S + (1-\delta_S)\mathbb{E}[T_S]$ gives

$$\frac{K_S}{U_S} \le \mathbb{E}[T_S] = \frac{K_S}{\delta_S} \le \frac{K_S}{L_S}, \qquad \mathbb{E}[T_S] = \frac{pK_S}{A_S}\big(1 + O_S(p^{-1})\big). \tag{12}$$

The interval uses the computable quantities of (11). The model allows the cost of a trial to depend on whether that trial succeeds. It needs independence between successive trials.

For example, suppose that testing level 6 alone costs K_6 per sampled node, and that adding level 4 increases that cost by d_4. The leading costs are $pK_6/720$ and $p(K_6+d_4)/960$. So adding level 4 is advantageous to first order exactly when

$$d_4 < K_6/3. \tag{13}$$

For a given finite prime, (12) gives intervals with which to certify a comparison. The leading-term criterion alone need not decide a near tie. Independently of costs, Corollary 6.10 bounds the extra target proportion for $p > 72$ by

$$\max\left\{0, \frac{240(p-1)-190920}{p^2+1}\right\} \le \delta_{\{4,6\}} - \delta_{\{6\}} \le \min\left\{1, \frac{240(p-1)}{p^2+1}\right\}.$$

These formulas give a concrete way to combine the level-6 detector of [27] with other tests. The benchmarks in [5, 27] amortise one evaluation over several revealed neighbours. They need a common sampling and cost convention before they can be inserted into (12). In particular, a cost quoted per revealed node cannot automatically be treated as the cost per independent sampled node.

An implementation must also distinguish recognition from construction. Reaching a node in H_{N^2} certifies that a splitting exists. Recovering the elliptic factors and the maps is a further task. Explicit constructions of the elliptic subcovers in superspecial characteristic, with their cost, would connect the present target statistics to an end-to-end algorithm. Finally, (12) is an independent-sampling calculation. The stationary measure alone does not give the first-hitting cost for a Richelot walk whose successive nodes are correlated.

TABLE 2. First moment μ_N, split proportion δ_N and second factorial moment B_N in the enumerated genera, multiplied by p or p^2. The last column in each group is p times the lower bound $\max\{0, \mu-\frac{B}{2}, \mu^2/(\mu+B)\}$ of (9). All entries are exact rationals rounded to one decimal.

	$N=2$				$N=3$				$N=4$			
p	$p\mu$	$p\delta$	p^2B	bound	$p\mu$	$p\delta$	p^2B	bound	$p\mu$	$p\delta$	p^2B	bound
47	29.3	24.6	659.7	22.3	117.4	41.5	12594.3	35.8	234.8	45.5	53495.8	40.1
71	29.6	26.3	659.9	24.9	118.3	57.4	12597.5	47.3	236.6	67.7	53509.4	56.5
131	29.8	27.9	660.0	27.3	119.1	80.3	12599.3	71.0	238.2	109.8	53516.9	87.7
167	29.8	28.4	660.0	27.8	119.3	86.6	12599.5	81.6	238.6	129.3	53518.1	101.8

9. Real multiplication

The first-moment formula of Theorem 4.2 holds for every t prime to p, not only for squares. In this short section we record what it says for non-square discriminants, where the representation problem corresponds to real multiplication rather than to splitting. We first make precise which real multiplication is counted.

Let $\Delta > 1$ be a non-square discriminant with $p \nmid \Delta$. The polarization identifies $\mathrm{NS}(A)$ with the Rosati-symmetric endomorphisms of A, and θ with the identity. So a vector $w \in \mathrm{NS}(A)/\mathbb{Z}\theta$ is the class of a symmetric endomorphism α modulo the scalars $\mathbb{Z}$. Under this identification

$$q_\theta(w) = \operatorname{disc}\mathbb{Z}[\alpha],$$

which does not change under $\alpha \mapsto \alpha + n$. We say that $\mathbb{Z}[\alpha]$ is optimally embedded if $\mathbb{Z}[\alpha] = \mathbb{Q}(\alpha) \cap \mathrm{End}^{\mathrm{sym}}(A)$. The vector w is primitive exactly when $\mathbb{Z}[\alpha]$ is optimally embedded. Indeed, $w = kw'$ with $k \ge 2$ means $\alpha = k\beta + n$ for a symmetric β, and then $\mathbb{Z}[\alpha] \subsetneq \mathbb{Z}[\beta]$. Conversely, if $\mathbb{Z}[\alpha]$ has index $f > 1$ in the larger order $\mathbb{Z}[\beta] = \mathbb{Q}(\alpha) \cap \mathrm{End}^{\mathrm{sym}}(A)$, then $\alpha = n \pm f\beta$ for some $n \in \mathbb{Z}$, so $w = \pm f\, w'$ with w' the class of β, and w is not primitive. So Kani's dictionary reads as follows. The surface (A, θ) lies on H_Δ, that is, it has real multiplication by $\mathcal{O}_\Delta$ in the optimal sense, exactly when q_θ primitively represents Δ. The pairs $\pm w$ of primitive vectors with $q_\theta(w) = \Delta$ correspond to the optimally embedded orders of discriminant Δ, each counted once for α and its conjugate $-\alpha$ modulo scalars. Theorem 4.2 applies without change.

Example 9.1. Optimality cannot be dropped. Let $p = 43$ and let $A = E_0^2$ with the product polarization, so that q_θ is (2) with $p + 1 = 44$. The symmetric endomorphism

$$\alpha = \begin{pmatrix} 0 & 1+i \\ 1-i & 0 \end{pmatrix}, \qquad \alpha^2 = 2,$$

embeds $\mathbb{Z}[\sqrt{2}]$, of discriminant 8, and indeed q_θ represents 8 primitively, for instance at $(0, 1, 1, 0, 0)$. The suborder $\mathbb{Z}[2\sqrt{2}] = \mathbb{Z}[2\alpha]$, of discriminant 32, also acts. But q_θ does not represent 32 primitively. A representation of 32 forces $x_3 = x_4 = 0$, hence $x_0^2 + 4x_1^2 + 4x_2^2 = 32$, so $x_0 = 2a$ with $a^2 + x_1^2 + x_2^2 = 8$, and every solution of the last equation has all three coordinates even. So (A, θ) has real multiplication by $\mathcal{O}_{32}$ but does not lie on H_{32}, and Corollary 9.2 counts only the optimal order $\mathcal{O}_8$ here.

Corollary 9.2. *Let Δ be as above and $\chi = (\Delta/p)$. The expected number of pairs $\pm w$ of primitive vectors with $q_\theta(w) = \Delta$ is $C(\Delta)(p - \chi)/(p^2 + \chi)$. In particular, the weighted proportion of superspecial nodes lying on H_Δ is at most $C(\Delta)/(p - 1)$ if p is inert in $\mathbb{Q}(\sqrt{\Delta})$, and at most $C(\Delta)(p - 1)/(p^2 + 1)$ if p splits in $\mathbb{Q}(\sqrt{\Delta})$.*

This is a first moment and an upper bound. The heuristic density of [18, Section 4.2] is replaced by an exact expectation, not by an exact probability. An analogue of the binary-representation calculation of Section 6 would provide second moments and probability bounds. We have not carried it out, and two moments alone would still not give an exact probability. The ratio $(p^2 + 1)/(p - 1)^2$ between the inert and the split case is a ratio of expectations. Table 3 lists $C(t)$ for small t.

TABLE 3. The constants $C(t) = -60H^*(2, t)$.

t	5	8	12	13	17	21	24	28	29	33	37
$C(t)$	24	60	120	120	240	240	360	480	360	720	600
N	1	2	3	4	5	6	7	8	9	10	11
$C(N^2) = 5NJ_2(N)$	5	30	120	240	600	720	1680	1920	3240	3600	6600

10. Conclusion

The measure transfer theorem makes Siegel's genus averages applicable to superspecial surfaces. It gives exact first moments for primitive Humbert representations. For fixed splitting levels and p in the stated range it gives factorial second moments and mixed moments of the form $c/(p^2 + 1)$. These yield the main theorem, explicit error bounds for individual and combined detectors, an exact probability at level 2, and a cost criterion once a sampling model and compatible per-sample costs are specified.

Several questions remain. Closed formulas for c_N and $c_{M,N}$ require the binary local densities at the bad primes. Distributing $c_{2,3}$ among the families of [25] would connect the aggregate incidence count with explicit subcover geometry. Higher joint moments would require a further analysis of singular configurations and of representation formulas beyond the binary case. Extending the results to $p \equiv 1 \pmod 4$ requires a suitable base order and a new check of the local and global lattice arguments. For cryptographic applications a further step is to combine the stationary bounds with the dependence of the walk, with compatible detector benchmarks, and with the reconstruction of splittings.

Finally, a word on verification. Every formula in the paper was checked, in exact rational arithmetic, against the complete enumerations of Section 6.3: the first-moment formula in 2313 cases, the local densities against direct counts modulo prime powers, the second, mixed and level-2 formulas at every enumerated prime in their range, and the probability bounds of Corollaries 6.8 and 6.10 against the enumerated distributions for 402 level sets and 1192 increments. The scripts assert each of these checks and stop at the first failure.

References

[1] A. Borel, *Introduction aux groupes arithmétiques*, Hermann, Paris, 1969.
[2] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, 1978.

[3] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. **217** (1975), 271–285.
[4] M. Corte-Real Santos, C. Costello and S. Frengley, *An algorithm for efficient detection of (N, N)-splittings and its application to the isogeny problem in dimension 2*, PKC 2024, LNCS 14603, Springer, 157–189.
[5] M. Corte-Real Santos, C. Costello and S. Frengley, *Efficient algorithms for the detection of (N, N)-splittings and endomorphisms*, J. Cryptology **39** (2026), Paper No. 2.
[6] C. Costello and B. Smith, *The supersingular isogeny problem in genus 2 and beyond*, PQCrypto 2020, LNCS 12100, Springer, 151–168.
[7] A. G. Earnest and J. S. Hsia, *Spinor norms of local integral rotations II*, Pacific J. Math. **61** (1975), 71–86.
[8] E. Florit and B. Smith, *Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph*, Arithmetic, Geometry, Cryptography, and Coding Theory 2021, Contemp. Math. **779**, Amer. Math. Soc., 2022, 103–132.
[9] G. van der Geer, *Hilbert Modular Surfaces*, Ergeb. Math. Grenzgeb. (3) **16**, Springer, 1988.
[10] D. Gruenewald, *Computing Humbert surfaces and applications*, Arithmetic, Geometry, Cryptography and Coding Theory 2009, Contemp. Math. **521**, Amer. Math. Soc., 2010, 59–69.
[11] K. Hashimoto and T. Ibukiyama, *On class numbers of positive definite binary quaternion hermitian forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **27** (1980), 549–601.
[12] T. Ibukiyama, *Quinary lattices and binary quaternion hermitian lattices*, Tohoku Math. J. **71** (2019), 207–220.
[13] T. Ibukiyama, T. Katsura and F. Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), 127–152.
[14] E. Kani, *Elliptic curves on abelian surfaces*, Manuscripta Math. **84** (1994), 199–223.
[15] E. Kani, *The moduli spaces of Jacobians isomorphic to a product of two elliptic curves*, Collect. Math. **67** (2016), 21–54.
[16] E. Kani and H. Kir, *The number of curves of genus 2 with a given refined Humbert invariant*, arXiv:2608.24122, 2026.
[17] E. Kırımlı and G. Korpal, *Refined Humbert invariants in supersingular isogeny degree analysis*, arXiv:2607.25552, 2026.
[18] E. Kırımlı and G. Korpal, *Detecting split surfaces, RM surfaces, and minimum walks on isogeny graphs*, IACR ePrint 2026/2088; arXiv:2609.23941.
[19] M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen*, Arch. Math. **7** (1956), 323–332.
[20] M. Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. **8** (1957), 241–250.
[21] M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The Book of Involutions*, Amer. Math. Soc. Colloq. Publ. **44**, 1998.
[22] V. V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR-Izv. **14** (1980), 103–167.
[23] The PARI Group, *PARI/GP version 2.17.2*, Univ. Bordeaux, 2025.
[24] T. Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), 263–280.
[25] T. Shaska, *Genus two curves with many elliptic subcovers*, Comm. Algebra **44** (2016), 4450–4466.
[26] T. Shaska, *Degrees of genus-two split-Jacobian loci and Humbert-form reconstruction*, arXiv:2608.16426, 2026.
[27] T. Shaska, *The Humbert form of discriminant 36, and what it says about splitting detection*, IACR ePrint 2026/2327.
[28] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, Arithmetic and Geometry with Applications, Springer, 2004, 703–723.
[29] T. Shioda, *Supersingular K3 surfaces*, Algebraic Geometry (Copenhagen, 1978), Lecture Notes in Math. **732**, Springer, 1979, 564–591.
[30] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. **36** (1935), 527–606.
[31] C.-F. Yu and J.-D. Yu, *Mass formula for supersingular abelian surfaces*, arXiv:0902.0244, 2009.

Department of Computer Science and Engineering, Oakland University, Rochester, MI 48309, USA
Email address: shaska@oakland.edu