Teichmüller Curves in Genus Two: Discriminant and Spin

Citation
McMullen, Curtis T. 2005. Teichmüller curves in genus two: Discriminant and spin. Mathematische Annalen 333(1): 87-130. Revised 2009.

Published Version
doi:10.1007/s00208-005-0666-y

Permanent link
http://nrs.harvard.edu/urn-3:HUL.InstRepos:3446004

Teichmüller curves in genus two: Discriminant and spin

Curtis T. McMullen[*]

9 April, 2004

Contents

1 Introduction

Let $\mathcal{M}_g$ denote the moduli space of Riemann surfaces of genus g, and $\Omega\mathcal{M}_g \to \mathcal{M}_g$ the bundle of Abelian differentials. A point in $\Omega\mathcal{M}_g$ is specified by a pair (X, ω), where $X \in \mathcal{M}_g$ and where $\omega \in \Omega(X)$ is a nonzero, holomorphic 1-form on X.

The bundle $\Omega\mathcal{M}_g$ admits a natural action of $\mathrm{SL}_2(\mathbb{R})$, and the projection of any orbit gives a holomorphic *Teichmüller disk* $f : \mathbb{H} \to \mathcal{M}_g$. If the stabilizer $\mathrm{SL}(X, \omega)$ of a form of genus g is a lattice in $\mathrm{SL}_2(\mathbb{R})$, then the disk generated by (X, ω) descends to a *Teichmüller curve*

$$f : V = \mathbb{H}/\,\mathrm{SL}(X, \omega) \to \mathcal{M}_g,$$

whose image is isometrically embedded for the Teichmüller metric.

In this paper we discuss the infinite family of Teichmüller curves generated by forms of genus two with double zeros. We show each such curve is uniquely determined by two invariants: its *discriminant* D and, when $D \equiv 1 \bmod 8$, its *spin invariant* $\epsilon \in \mathbb{Z}/2$. The proof is based on elementary moves that relate the cusps of V, and combinatorial number theory.

[*] Research partially supported by the NSF.

Conjecturally, this family accounts for all but one of the primitive Teichmüller curves in genus two.

Hilbert modular surfaces. In genus two, any Teichmüller curve as above lies on a unique *Hilbert modular surface* H_D, where $D > 0$ is a real quadratic discriminant [Mc1]. More precisely, we have a commutative diagram

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d] & \mathcal{M}_2 \arrow[d] \\ H_D \arrow[r] & \mathcal{A}_2, \end{tikzcd}$$

where $H_D = (\mathbb{H} \times \mathbb{H})/\operatorname{SL}_2(\mathcal{O}_D)$ parameterizes the locus of Abelian surfaces $A \in \mathcal{A}_2$ with real multiplication by the quadratic order $\mathcal{O}_D \cong \mathbb{Z}[x]/(x^2+bx+c)$, $D = b^2 - 4c$. We refer to D as the *discriminant* of the Teichmüller curve $f : V \to \mathcal{M}_2$.

The *Weierstrass curve* W_D is the locus of those Riemann surfaces $X \in \mathcal{M}_2$ such that

(i) $\operatorname{Jac}(X)$ admits real multiplication by $\mathcal{O}_D$, and

(ii) X carries an eigenform ω with a double zero at one of the six Weierstrass points of X.

(Here $\omega \in \Omega(X)$ is an *eigenform* if $\mathcal{O}_D \cdot \omega \subset \mathbb{C} \cdot \omega$.)

Every irreducible component of W_D is a Teichmüller curve of discriminant D. When $D \equiv 1 \bmod 8$, one can also define a *spin invariant* $\epsilon(X, \omega) \in \mathbb{Z}/2$, which is constant along the components of W_D. Our main result shows that eigenforms with double zeros have no other discrete invariants.

Theorem 1.1 *For any integer $D \geq 5$ with $D \equiv 0$ or $1 \bmod 4$, either:*

- *The Weierstrass curve W_D is irreducible, or*
- *We have $D \equiv 1 \bmod 8$ and $D \neq 9$, in which case $W_D = W_D^0 \sqcup W_D^1$ has exactly two components, distinguished by their spin invariants.*

(Note: $W_D = \emptyset$ for $D \leq 4$.)

Corollary 1.2 *Every Teichmüller curve generated by a form $(X, \omega) \in \Omega\mathcal{M}_2(2)$ is determined up to isomorphism by its discriminant D and, if $D \equiv 1 \bmod 8$, by its spin invariant $\epsilon(X, \omega) \in \mathbb{Z}/2$.*

Here $\Omega\mathcal{M}_2(2)$ denotes the space of forms of genus two with double zeros.

Billiards. To relate the discussion to billiards, let $P \subset \mathbb{C}$ be a polygon with angles in $\pi\mathbb{Q}$. Via an unfolding construction, (P, dz) determines a holomorphic form $(X, \omega) \in \Omega\mathcal{M}_g$, such that billiard trajectories in P go over to geodesics on the singular flat surface $(X, |\omega|)$. If (X, ω) generates a Teichmüller curve, we say P is a *lattice polygon.*

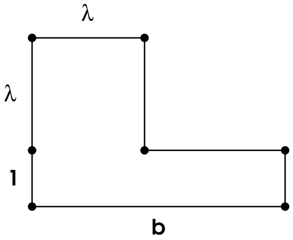

Figure 1. The billiard table $L(b,e)$, with $\lambda = (e+\sqrt{e^2+4b})/2$.

Veech showed that the billiard flow in a lattice polygon has optimal dynamical properties: for example, every trajectory is either periodic or uniformly distributed [V1].

Now let $L(b,e)$ be the polygon obtained by stacking a $\lambda \times \lambda$ square atop a $1 \times b$ rectangle, where $\lambda = (e+\sqrt{e^2+4b})/2$ and $b, e \in \mathbb{Z}$ (Figure 1). Let us say $L(b,e)$ is *admissible* if $e = -1, 0$ or 1, $e+1 < b$, and if $e = 1$ then b is even. (The condition $e+1 < b$ just insures $\lambda < b$.) It can be checked that $L(b,e)$ generates a Teichmüller curve with discriminant $D = e^2 + 4b$ and, when $D \equiv 1 \bmod 8$, with spin invariant $\epsilon = \pm 1$ depending on the sign of e (cf. Theorem 5.3 below). Since every possible (D, ϵ) occurs exactly once, we have:

Corollary 1.3 *Every Teichmüller curve generated by a form of genus two with a double zero is also generated by a unique admissible billiard table $L(b,e)$.*

For example, by applying the algorithm from [Mc1] to the tables $L(4, \pm 1)$, one can obtain explicit presentations for the two components of W_{17} as quotients of the upper halfplane (Figure 2).

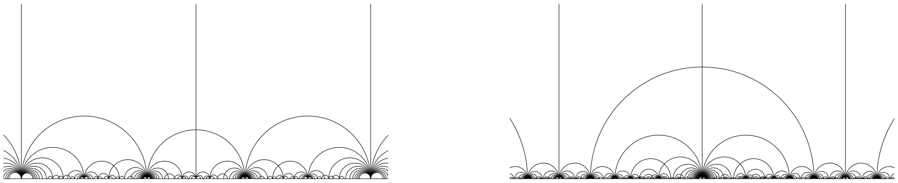

Figure 2. Uniformizations of the curves W^0_{17} and W^1_{17}.

Primitivity. A Teichmüller curve in $\mathcal{M}_g$ is *primitive* if it does not arise from a curve in $\mathcal{M}_h$, $h < g$, via a branched covering construction. We suspect that the billiard tables above account for all but one of the primitive Teichmüller curves in genus two.

Conjecture 1.4 *The regular decagon gives the only primitive Teichmüller curve $V \to \mathcal{M}_2$ generated by a form with simple zeros.*

Added in proof: This Conjecture is established in [Mc3].

Topology of branched covers. The case $D = d^2$ of Theorem 1.1 has the following purely topological consequence.

Let Σ_g denote a closed oriented surface of genus g. Let us say two mappings $f, g : \Sigma_2 \to \Sigma_1$ have the *same type* if there exist orientation-preserving homeomorphisms h_1, h_2 such that the diagram

$$\begin{tikzcd}
\Sigma_2 \arrow[r, "h_2"] \arrow[d, "f"'] & \Sigma_2 \arrow[d, "g"'] \\
\Sigma_1 \arrow[r, "h_1"] & \Sigma_1
\end{tikzcd}$$

commutes.

Every eigenform (X, ω) for $\mathcal{O}_{d^2}$ is the pullback, by a degree d map to an elliptic curve, of a form of genus one. Thus the components of W_{d^2} are labeled by types of branched covers. More precisely, Theorem 1.1 implies:

Corollary 1.5 *For $d = 3$, or any even $d \geq 4$, there is only one type of degree d covering*

$$f : \Sigma_2 \to \Sigma_1$$

branched over just one point and surjective on π_1. For odd $d \geq 5$, there are exactly two types of such branched coverings.

(For $d = 1$ or 2 there are no such branched coverings at all.)

D	5	8	9	12	13	16	17	20	21	24	25	28	29	32	33	36	37	40	41	44	45	48	49	52
$\lvert C(W_D)\rvert$	1	2	2+0	3	3	3	3+3	5	4	6	5+3	7	5	7	6+6	8	9	12	7+7	9	8	11	10+8	15

Table 3. The number of cusps of the Weierstrass curve, broken down as $|C(W_D^0)| + |C(W_D^1)|$ when $D \equiv 1 \bmod 8$.

Cusps. In the course of studying the components of W_D, we develop a combinatorial enumeration of its two-cylinder cusps (§4). To complete the picture, in the Appendix we discuss the remaining cusps of W_D and how they are partitioned by spin. For example, we show that W_D^0 and W_D^1 have the same number of cusps when $D \equiv 1 \bmod 8$ is not a square. Table 3 lists the number of cusps of each component of W_D for $D \leq 52$.

Square-tiled surfaces. Hubert and Lelièvre showed that W_{d^2} has at least two components when $d > 3$ is odd, and exactly two when $d = p$ is prime [HL]. They also showed the genus of W_{p^2} tends to infinity.

The components of W_{d^2} are distinguished in [HL] by counting the number of integral Weierstrass points on square-tiled surfaces. In §6 we show this count can be viewed as a special case of the spin invariant. In the Appendix we also prove that every square-tiled surface of genus two has a one-cylinder direction, generalizing [HL, Theorem 5.1].

By counting square-tiled surfaces, Eskin, Masur and Schmoll show that the orbifold Euler characteristic of the Weierstrass curve satisfies

$$\chi(W_{d^2}) = -\frac{1}{16}d^2(d-2)\sum_{r|d}\frac{\mu(r)}{r^2},$$

where μ is the Möbius function [EMS, §4.2]. It would be interesting to obtain a similar formula for $\chi(W_D)$, valid for all D.

Spin, elementary moves, and components of $\boldsymbol{W_D}$. We conclude with a sketch of the proof of Theorem 1.1.

1. *Spin structures.* The 2^{2g} spin structures on a surface X of genus g correspond topologically to quadratic forms

   $$q : H_1(X,\mathbb{Z}/2) \to \mathbb{Z}/2.$$

   The parity of a spin structure agrees with *Arf invariant* of q, given by

   $$\mathrm{Arf}(q) = \sum q(a_i)q(b_i) \in \mathbb{Z}/2$$

   with respect to a symplectic basis for $H_1(X,\mathbb{Z}/2)$.

   Any surface of genus two admits six odd spin structures, which correspond naturally to its six Weierstrass points.

2. *The spin invariant.* Let $\Omega W_D \to W_D$ denote the bundle of eigenforms (X,ω) with double zeros. Then the Weierstrass point at which ω vanishes determines a spin structure on X, and hence a quadratic form $q : H_1(X,\mathbb{Z}/2) \to \mathbb{Z}/2$.

   Now suppose $D \equiv 1 \bmod 8$. Write $D = Ef^2$ where E is square-free and $f > 0$. To extract the spin invariant of (X,ω), choose a generator T for $\mathcal{O}_D$, normalized so that

   $$T^*(\omega) \quad = \quad \frac{f+\sqrt{D}}{2}\omega.$$

   Then T gives an endomorphism of $H_1(X,\mathbb{Z}/2)$, whose image is a rank two symplectic subspace, say with basis $\langle a,b\rangle$.

   The *spin invariant* of (X,ω) is then defined by

   $$\epsilon(X,\omega) = \mathrm{Arf}(q|\,\mathrm{Im}(T)) = q(a)q(b) \in \mathbb{Z}/2.$$

   The eigenforms with even and odd spin invariant form $\mathbb{C}^*$-bundles over subsurfaces W_D^0 and W_D^1 of W_D. For $D \geq 17$ both spins occur, and thus W_D has at least two components (§5).

3. *A model for W_D.* The spin invariant provides a lower bound on the number of components of W_D. To obtain an upper bound, we analyze a combinatorial model for W_D given by

   $$S_D = \{e \equiv D \bmod 2 \ : \ e^2 < D \text{ and } (e+2)^2 < D\},$$

   equipped with the equivalence relation generated by

   $$e \sim e' = -e - 2q \ \text{ whenenever } e' \in S_D \text{ and } \gcd(b,q) = 1. \tag{1.1}$$

   Here $q > 0$ and $b = (D - e^2)/4$ is determined by the condition $e^2 + 4b = D$. We refer to the equivalence classes of S_D as its *components*.

4. *Elementary moves.* In §8 we show the number of components of S_D is an upper bound for the number of components of W_D.

   To prove this, we show each integer $e \in S_D$ labels a cusp of W_D, and the cusps so labeled meet every component W_D. Using an elementary *butterfly move* on connected sum decompositions of eigenforms (§7), we then show that cusps labeled by equivalent elements of S_D belong to the same component of W_D.

5. *Relative primes.* Relatively prime numbers play a central role in the structure of S_D, due to the condition $\gcd(b,q) = 1$ in (1.1) above.

   To show S_D is highly connected, in §9 we develop bounds for the smallest $x > 1$ relatively prime to a given integer n, as well as for the smallest relative prime in an arithmetic progression. These bounds are succinctly expressed in terms of *Jacobsthal's function* $J(n)$, defined as the largest gap between consecutive integers relatively prime to n.

6. *Combinatorial connectivity.* In §10 we show that, apart from five exceptional cases, the space S_D has exactly two components when $D \equiv 1 \bmod 8$, and otherwise just one.

   This agrees with the lower bound given by the spin invariant, and establishes our main result except for $D = 9, 49, 73, 121$ and 169. A short argument treats these cases as well (§11).

7. *Stabilization.* Due to irregularities in the distribution of prime numbers, our number-theoretic analysis of the connectivity of S_D applies only in the 'stable regime', when D is sufficiently large (e.g. $D \geq 2000$). The remaining values of D are treated by inspection, revealing the five exceptional cases above.

Notes and references. This paper is a sequel to [Mc1], as well as a complement to the classification of orbit closures and invariant measures for the action of $\mathrm{SL}_2(\mathbb{R})$ on $\Omega\mathcal{M}_2$ given in [Mc4].

The curves W_5 and W_8 come from billiards in a regular pentagon and a regular octagon, and were studied in [V1]. Kontsevich and Zorich used spin structures to determine the components of the strata $\Omega\mathcal{M}_g(p_1,\ldots,p_k)$ of holomorphic 1-forms with zeros of prescribed multiplicity [KZ]. Corresponding results for quadratic differentials are announced in [La]. See [EMS] and [HL] for additional results on the curves W_{d^2}, and [V1], [V2], [Vo], [Wa], [KS], [Pu], [GJ], [EO], and [Ca] for more on Teichmüller curves. I would like to thank D. Thurston for useful conversations.

2 Real multiplication

In this section we describe when a product of two elliptic curves, $E_1 \times E_2$, admits real multiplication by $\mathcal{O}_D$. In §3 we will see that such products, interpreted as Jacobians of stable curves, arise from cusps of W_D.

The space of lattices. Let $\mathcal{M}_1 \cong \mathbb{H}/\operatorname{SL}_2(\mathbb{Z})$ denote the moduli space of elliptic curves. Let $\Omega\mathcal{M}_1 \to \mathcal{M}_1$ denote the bundle of pairs (E,ω), where $E \in \mathcal{M}_1$ and $\omega \in \Omega(E)$ is a nonzero holomorphic 1-form on E.

We can identify $\Omega\mathcal{M}_1$ with the space of lattices $\Lambda \subset \mathbb{C}$ via the correspondence

$$\Lambda \leftrightarrow (\mathbb{C}/\Lambda, dz) = (E,\omega).$$

We can also view $\Omega\mathcal{M}_1$ as the homogeneous space $\operatorname{GL}_2^+(\mathbb{R})/\operatorname{SL}_2(\mathbb{Z})$; then $\mathbb{C}^* \cong \mathbb{R}_+ \cdot \operatorname{SO}_2(\mathbb{R})$ acts on the left with quotient $\mathcal{M}_1$.

Isogeny. Given $E_1, E_2 \in \mathcal{M}_1$, an *isogeny* $p : E_1 \to E_2$ is a surjective holomorphic group homomorphism. Its degree is given by $\deg(p) = |\operatorname{Ker}(p)|$. The *dual isogeny* $\overline{p} : E_2 \to E_1$ is defined by

$$\overline{p}(z_2) = \sum_{p(z_1)=z_2} z_1,$$

and satisfies $\overline{p}(p(z_1)) = \deg(p) z_1$. An isogeny is *primitive* if $\operatorname{Ker}(p) \cong \mathbb{Z}/\deg(p)$. Any isogeny can be factored as $p(z) = p_0(\ell z)$ where p_0 is primitive.

Typically $q(z) = -p(z)$ is the only other isogeny between E_1 and E_2 with $\deg(q) = \deg(p)$; more are possible if p factors through an elliptic curve with extra automorphisms.

The *Hecke correspondence of level* m is the curve $T_m \subset \mathcal{M}_1 \times \mathcal{M}_1$ defined by:

$$T_m = \{(E_1,E_2) \;:\; \text{there exists an isogeny } p : E_1 \to E_2 \text{ of degree } m\}.$$

If we impose the additional requirement that p is primitive, we obtain an irreducible curve $F_m \subset \mathcal{M}_1 \times \mathcal{M}_1$, and we have

$$T_m = \bigcup_{\ell^2 | m} F_{m/\ell^2}.$$

A point $(E_1,E_2) \in F_m$ is determined by the pair $(E_1, \operatorname{Ker}(p))$, and thus the normalization of F_m is given by

$$\widetilde{F_m} \cong \mathbb{H}/\Gamma_0(m) = \mathbb{H}/\{g \in \operatorname{SL}_2(\mathbb{Z}) \;:\; g \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod m\}.$$

The points of $\widetilde{F_m}$ correspond to pairs (E_1, E_2) with a *choice* of a primitive degree m isogeny $p : E_1 \to E_2$, up to sign.

Real multiplication. A *real quadratic discriminant* is an integer $D > 0$ satisfying $D \equiv 0$ or $1 \bmod 4$. The corresponding *real quadratic order* is the ring $\mathcal{O}_D \cong \mathbb{Z}[x]/(x^2 + bx + c)$, $b^2 - 4c = D$. We have

$$\mathcal{O}_D \otimes \mathbb{Q} \cong \begin{cases} \mathbb{Q} \times \mathbb{Q} & \text{if } D = d^2 \text{ is a square,} \\ \mathbb{Q}(\sqrt{D}) & \text{otherwise.} \end{cases}$$

Let $A = \mathbb{C}^2/L$ be a principally polarized Abelian surface. The polarization is given by a unimodular symplectic form $x \cdot y$ on $H_1(A, \mathbb{Z}) \cong L$. Let $\operatorname{End}(A)$ denote the endomorphism ring of A as a complex Lie group. A subring $R \subset \operatorname{End}(A)$ is *proper* if $(nT \in R, n \neq 0) \implies T \in R$, and an element $T \in \operatorname{End}(A)$ is *self-adjoint* if

$$(Tx) \cdot y = x \cdot (Ty)$$

for all $x, y \in H_1(A, \mathbb{Z})$.

We say A admits *real multiplication* by $\mathcal{O}_D$ if there is a self-adjoint endomorphism $T : A \to A$ generating a proper subring $\mathbb{Z}[T] \cong \mathcal{O}_D$ in $\operatorname{End}(A)$. In this case the space of 1-forms splits into eigenspaces

$$\Omega(A) = S_1 \oplus S_2$$

for the action of $\mathcal{O}_D$; the nonzero elements of $S_1 \cup S_2$ are *eigenforms.*

The moduli space of Abelian surfaces equipped with real multiplication by $\mathcal{O}_D$ can be identified with the Hilbert modular surface $H_D = (\mathbb{H} \times \mathbb{H}) / \operatorname{SL}_2(\mathcal{O}_D)$.

Products of elliptic curves. Now consider the case of an Abelian surface which is a product of elliptic curves, $A = E_1 \times E_2$. For any such A we have a natural isomorphism

$$\Omega(A) = \Omega(E_1) \oplus \Omega(E_2),$$

and a product polarization of coming from the isomorphism

$$H_1(A, \mathbb{Z}) \cong H_1(E_1, \mathbb{Z}) \oplus H_1(E_2, \mathbb{Z}).$$

The moduli space of holomorphic 1-forms

$$(A, \omega) = (E_1 \times E_2, \omega_1 + \omega_2)$$

on products of elliptic curves (with both $\omega_i \neq 0$) is naturally identified with $\Omega\mathcal{M}_1 \times \Omega\mathcal{M}_1$. The group $\operatorname{GL}_2^+(\mathbb{R})$ acts diagonally on the product. Within this moduli space we wish to describe the locus

$$\Omega Q_D = \{(E_1 \times E_2, \omega) \,:\, \omega \text{ is an eigenform for real multiplication by } \mathcal{O}_D\}.$$

Prototypes. Let us say a triple of integers (e, ℓ, m) is a *prototype* for real multiplication, with discriminant D, if

$$D = e^2 + 4\ell^2 m, \quad \ell, m > 0, \quad \text{and} \quad \gcd(e, \ell) = 1.$$

We begin by associating a prototype (e, ℓ, m) to each pair

$$(A, \omega) = (E_1 \times E_2, \omega_1 + \omega_2) \in \Omega Q_D.$$

Let $T \in \operatorname{End}(A)$ generate the unique action of $\mathcal{O}_D$ with ω as an eigenform. Then in terms of the product structure $A = E_1 \times E_2$, we can write

$$T(z_1, z_2) = \begin{pmatrix} e \cdot I & \overline{p} \\ p & f \cdot I \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}. \tag{2.1}$$

The fact that T is self-adjoint with respect to the polarization insures the on-diagonal blocks are multiples of the identity, and the off-diagonals are dual isogenies (cf. [Mc4, Theorem 8.3]).

There is a unique choice of generator $T \in \mathcal{O}_D$ such that $f = 0$ and such that $T^*\omega = \lambda\omega$ with $\lambda > 0$. By fixing this choice, p and e become invariants of $(E_1 \times E_2, \omega)$. Moreover p is a multiple of a primitive isogeny of degree m, giving a natural factorization

$$\deg(p) = \ell^2 m, \quad \ell, m > 0.$$

Since $\mathbb{Z}[T]$ is a proper subring of $\operatorname{End}(A)$, we have $\gcd(e, \ell) = 1$. The fact that $p\overline{p} = \deg(p) = \ell^2 m$ implies

$$T^2 = eT + \ell^2 m,$$

and therefore $D = e^2 + 4\ell^2 m$. Thus (e, ℓ, m) is a prototype for real multiplication by $\mathcal{O}_D$.

Theorem 2.1 *The space of all eigenforms $(E_1 \times E_2, \omega)$ for real multiplication by $\mathcal{O}_D$ decomposes into a finite union*

$$\Omega Q_D = \bigcup \Omega Q_D(e, \ell, m)$$

of closed $\mathrm{GL}_2^+(\mathbb{R})$ orbits, one for each prototype (e, ℓ, m). Each orbit projects to a Hecke curve $F_m \subset \mathcal{M}_1 \times \mathcal{M}_1$, with generic fiber $\mathbb{C}^*$.

Proof. The possible choices for (E_1, E_2) and $p : E_1 \to E_2$ in (2.1) are parameterized by $\widetilde{F_m}$. Thus the space of eigenforms with a given prototype (e, ℓ, m) is a connected set of the form $\Omega Q_D(e, \ell, m) \cong \mathrm{GL}_2^+(\mathbb{R})/\Gamma_0(m)$. ■

Corollary 2.2 *The product $E_1 \times E_2$ admits real multiplication by $\mathcal{O}_D$ iff we have $(E_1, E_2) \in F_m$ and there exists an integral solution to the equation $e^2 + 4m\ell^2 = D$ with $\ell > 0$ and $\gcd(e, \ell) = 1$.*

Examples. We conclude with an example of an eigenform for each prototype (e, ℓ, m).

Let $\lambda > 0$ be the unique positive root of the equation $\lambda^2 = e\lambda + \ell^2 m$. Define a pair of lattices in $\mathbb{C} \cong \mathbb{R}^2$ by

$$\Lambda_1 = \mathbb{Z}(\lambda, 0) \oplus \mathbb{Z}(0, \lambda), \quad \Lambda_2 = \mathbb{Z}(\ell m, 0) \oplus \mathbb{Z}(0, \ell).$$

Let $(E_i, \omega_i) = (\mathbb{C}/\Lambda_i, dz)$ be the corresponding forms of genus one, and let

$$(A, \omega) = (E_1 \times E_2, \omega_1 + \omega_2).$$

Then by construction, we have a pair of dual isogenies between E_1 and E_2 of the form

$$p(z_2) = \lambda z_2, \quad \overline{p}(z_1) = (\ell^2 m/\lambda) z_1.$$

These isogenies have degree $\ell^2 m$, and they are built from primitive isogenies of degree m. Defining T by (2.1) (with $f = 0$), we find $T^*(\omega) = \lambda\omega$; therefore (A, ω) is an eigenform with invariants (e, ℓ, m). We refer to (A, ω) as the *prototypical example* of type (e, ℓ, m).

Corollary 2.3 *Every eigenform* $(E_1 \times E_2, \omega)$ *is equivalent, under the action of* $\mathrm{GL}_2^+(\mathbb{R})$*, to a unique prototypical example.*

Notes. For more details on elliptic curves and isogeny, see e.g. [Ser, Ch. VII], [Kn], [Lang] and [GK]. Abelian varieties with real multiplication and their moduli are discussed in [vG], [Ru], [BL] and [Mc4, §4].

One can regard Corollary 2.2 as a description of the intersection $H_D \cap H_1$ of two Humbert surfaces in $\mathcal{A}_2$: they meet along the divisor $\sum a_m F_m$, where a_m is the number of integral points (e, ℓ) on the ellipse $e^2 + 4m\ell^2 = D$ satisfying $\gcd(e, \ell) = 1$ and $\ell > 0$. This locus consists of Abelian surfaces admitting an action (by endomorphisms) of a quaternion ring generated by $\mathcal{O}_1$ and $\mathcal{O}_D$.

It would be interesting to investigate more general intersections $H_D \cap H_E$ in the spirit of [HZ] and [GK].

3 Prototypical splittings

Every eigenform $(X, \omega) \in \Omega W_D$ splits, in infinitely many ways, as a *connected sum*

$$(X, \omega) = (E_1, \omega_1) \underset{I}{\#} (E_2, \omega_2)$$

of forms of genus one. In this section we determine the components of the covering space

$$\Omega W_D^s \to \Omega W_D$$

whose fibers encode all possible splittings of a given form.

Bundles over moduli space. We begin by recalling material from [Mc4].

Let $\Omega\mathcal{M}_g \to \mathcal{M}_g$ denote the bundle of holomorphic 1-forms (X, ω), $\omega \neq 0$, over the moduli space of Riemann surfaces of genus g. The periods of ω will be denoted by

$$\mathrm{Per}(\omega) = \left\{ \int_C \omega \ : \ C \in H_1(X, \mathbb{Z}) \right\} \subset \mathbb{C} \cong \mathbb{R}^2.$$

There is a natural action of $\mathrm{GL}_2^+(\mathbb{R})$ on $\Omega\mathcal{M}_g$, and we will denote the stabilizer of a given form by $\mathrm{SL}(X,\omega)$.

Within the space of forms of genus two, we let

- $\Omega\mathcal{M}_2(2)$ denote the forms with double zeros;
- ΩE_D, the eigenforms for real multiplication by $\mathcal{O}_D$; and
- $\Omega W_D = \Omega E_D \cap \Omega\mathcal{M}_2(2)$, the eigenforms with double zeros.

Each space above is also invariant under the natural action of $\mathrm{GL}_2^+(\mathbb{R})$.

The locus ΩW_D is a $\mathbb{C}^*$-bundle over the finite-volume (but possibly disconnected) hyperbolic surface

$$W_D = \mathbb{C}^* \backslash \Omega W_D.$$

We refer to W_D as the *Weierstrass curve* of discriminant D, because ΩE_D parameterizes the eigenforms (X,ω) that vanish at a Weierstrass point of X.

For any $(X,\omega) \in \Omega W_D$, the group

$$\mathrm{SL}(X,\omega) \subset \mathrm{SL}_2(\mathbb{R})$$

is a lattice with trace field $\mathbb{Q}(\sqrt{D})$, and the corresponding component V of W_D is isomorphic to $\mathbb{H}/\,\mathrm{SL}(X,\omega)$. The natural projection $V \to \mathcal{M}_2$ gives a *Teichmüller curve*, i.e. an isometrically immersed algebraic curve in moduli space [Mc4, Cor. 5.11].

Connected sums. Let $I = [0,v] = [0,1]\cdot v$ be the segment from 0 to $v \neq 0$ in $\mathbb{C}$, and let $(E_i,\omega_i) = (\mathbb{C}/\Lambda_i, dz) \in \Omega\mathcal{M}_1$ be a pair of forms of genus one. Suppose I maps to an embedded arc under each projection $\mathbb{C} \to E_i$. Then by slitting along these arcs and gluing corresponding edges, we can form the *connected sum*

$$(X,\omega) = (E_1,\omega_1) \underset{I}{\#} (E_2,\omega_2) \in \Omega\mathcal{M}_2.$$

The connected sum is a form of genus two, with a pair of simple zeros coming from the endpoints of I.

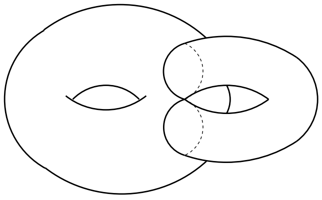

Figure 4. A connected sum resulting in a double zero.

Figure eights. To produce forms with double zeros, we extend the connected sum operation in a natural way to include the case where

$$[0,v] \cap \Lambda_1 = \{0,v\} \quad \text{and} \quad [0,v] \cap \Lambda_2 = \{0\}$$

or vice-versa. In this case I maps to a loop in E_1 and remains embedded in E_2. The connected sum then results in a double zero for ω, lying on a figure eight $L \subset X$ coming from the slits on E_1 and E_2 (see Figure 4). That is, we can describe X as the disjoint union

$$X = L \cup (E_2 - I) \cup (E_1 - I).$$

Theorem 3.1 *Let* $(X, \omega) = (E_1, \omega_1) \underset{I}{\#} (E_2, \omega_2)$. *Then:*

(i) ω *is an eigenform for real multiplication by* $\mathcal{O}_D$ *on* $\mathrm{Jac}(X) \iff$

(ii) $\omega_1 + \omega_2$ *is an eigenform for real multiplication by* $\mathcal{O}_D$ *on* $E_1 \times E_2$.

Proof. The property of being an eigenform depends only on the absolute periods of ω [Mc4, Cor 5.6], so it is preserved as I varies. In the limit as $I \to 0$ the connected sum yields the form $\omega_1 + \omega_2$ on the stable curve $E_1 \vee E_2$ with Jacobian $E_1 \times E_2$. ■

Splittings. Every form of genus two can be presented as a connected sum

$$(X, \omega) = (E_1, \omega_1) \underset{I}{\#} (E_2, \omega_2) \tag{3.1}$$

in infinitely many ways [Mc4, Theorem 1.7], each of which we regard as a *splitting* of (X, ω). To give a criterion for splitting, let $\eta : X \to X$ denote the hyperelliptic involution and $Z(\omega) \subset X$ the zeros of ω. Then by [Mc4, Thm. 7.3] we have:

Theorem 3.2 *Let* $L_0 \supset Z(\omega)$ *be a saddle connection such that* $L_0 \neq L_1 = \eta(L_0)$. *Then* (X, ω) *splits along* $L = L_0 \cup L_1$ *as a connected sum of tori.*

(Here a *saddle connection* is a geodesic segment for the metric $|\omega|$, joining a pair of zeros but with no zeros in its interior.)

The space of splittings. For $(X, \omega) \in \Omega W_D$, we adopt the convention that I maps to a loop in E_1, while it embeds in E_2; then the splitting (3.1) is uniquely determined by I.

Let ΩW_D^s denote the *splitting space*, consisting of triples (X, ω, I) such that $(X, \omega) \in \Omega W_D$ splits along I as in (3.1). There is a natural action of $\mathrm{GL}_2^+(\mathbb{R})$ on ΩW_D^s, and an equivariant projection

$$\Omega W_D^s \to \Omega \mathcal{M}_1 \times \Omega \mathcal{M}_1, \tag{3.2}$$

which records the summands (E_i, ω_i) in (3.1). By Theorem 3.1, this projection sends ΩW_D^s by a covering map to the locus of eigenforms ΩQ_D.

Prototypes. Let us say a quadruple of integers (a, b, c, e) is a *splitting prototype*, of discriminant D, if it satisfies the conditions

$$\begin{array}{lll} D = e^2 + 4bc, & 0 \le a < \gcd(b, c), & c + e < b, \\ 0 < b, & 0 < c, \quad \text{and} & \gcd(a, b, c, e) = 1. \end{array}$$

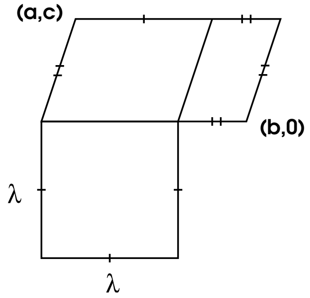

Figure 5. Prototypical splitting of type (a,b,c,e). Parallel edges are identified as shown to obtain a surface $X = E_1 \underset{I}{\#} E_2$ of genus two.

We denote the set of all such prototypes by P_D. For instance, we have:

$$P_{17} \;=\; \left\{ \begin{array}{lll} (0,2,2,-1), & (0,4,1,-1), & (0,1,2,-3), \\ (1,2,2,-1), & (0,4,1,1), & (0,2,1,-3) \end{array} \right\}.$$

Prototypical splittings. The *prototypical splitting* of type (a,b,c,e) is given by (3.1) with $I=[0,\lambda]$ and $(E_i,\omega_i) = (\mathbb{C}/\Lambda_i, dz)$, where

$$\Lambda_1 = \mathbb{Z}(\lambda,0)\oplus\mathbb{Z}(0,\lambda), \quad \Lambda_2 = \mathbb{Z}(b,0)\oplus\mathbb{Z}(a,c),$$

and $\lambda = (e+\sqrt{D})/2$ is the positive root of the equation $\lambda^2 = e\lambda + bc$. Note that I projects to a loop in E_1 since λ is a period of ω_1.

The resulting connected sum can be expressed in geometric terms as

$$(X,\omega) = (P,dz)/\sim,$$

where $P\subset\mathbb{C}$ is a polygon built from the period parallelograms for Λ_1 and Λ_2 as shown in Figure 5. The equivalence relation identifies parallel edges of P. The vertices of P are all equivalent, and correspond to the unique zero of ω on X.

The condition $c+e<b$ in the definition of a prototype is equivalent to $\lambda<b$, which insures that I projects an embedded arc in E_2.

Orbits. The stabilizer in $\mathrm{GL}_2^+(\mathbb{R})$ of the splitting above is the parabolic subgroup

$$N(n\mathbb{Z}) = \{\left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right) \,:\, t\in n\mathbb{Z}\}, \quad n = b/\gcd(b,c).$$

Indeed, the stabilizer of $I=[0,\lambda]$ is $N(\mathbb{R})$; the stabilizer of (I,Λ_1) is $N(\mathbb{Z})$; the stabilizer of (I,Λ_2) is $N((b/c)\mathbb{Z})$; and the intersection of all three is $N(n\mathbb{Z})$.

Thus the orbit of the prototypical splitting of type (a,b,c,e) is given by

$$\Omega W_D^s(a,b,c,e) \cong GL_2^+(\mathbb{R})/N(n\mathbb{Z}) \subset \Omega W_D^s,$$

a $\mathbb{C}^*$-bundle over the punctured disk $W_D^s(a,b,c,e)\cong\mathbb{H}/N(n\mathbb{Z})\cong\Delta^*$.

Theorem 3.3 *The splitting space ΩW_D^s is a finite union of closed, disjoint $\mathrm{GL}_2^+(\mathbb{R})$ orbits, one containing each prototypical splitting.*

Proof. Let (X, ω, I) be an element of the splitting space, corresponding to connected summands $(E_i, \omega_i) = (\mathbb{C}/\Lambda_i, \omega_i)$, $i = 1, 2$. Then

$$(A, \omega) = (E_1 \times E_2, \omega_1 + \omega_2)$$

is an eigenform for real multiplication by $\mathcal{O}_D$, say with prototype (e, ℓ, m).

Let $\lambda = (e + \sqrt{D})/2)$. By Theorem 2.1, we can normalize by the action of $\mathrm{GL}_2^+(\mathbb{R})$ so that

$$I = [0, \lambda], \ \ \Lambda_1 = \lambda \mathbb{Z}^2, \ \ \Lambda_2 \subset \mathbb{Z}^2 \ \text{ and } \ [\mathbb{Z}^2 : \Lambda_2] = d$$

where $d = \ell^2 m$. This normalization is unique up to the action of $N(\mathbb{Z})$. In these coordinates we can write

$$\Lambda_2 = \mathbb{Z}(b, 0) \oplus \mathbb{Z}(a, c)$$

with $b, c > 0$. The basis element $(b, 0)$ is canonical: it is the positive generator of $\Lambda_2 \cap I \cdot \mathbb{R}$. The second basis element, however, is determined only up to adding a multiple of the first: $(a + nb, c)$ would work as well. Moreover (a, c) is not fixed by $N(\mathbb{Z})$; its orbit is $(a + nc, c)$, $n \in \mathbb{Z}$. Thus there is a normalized basis of Λ_2 such that $0 \le a < \gcd(b, c)$.

By construction we have $D = e^2 + 4d = e^2 + 4bc$ and $0 < b, c$. By properness of the action of $\mathcal{O}_D$, we have $\gcd(a, b, c, e) = 1$. Since I embeds in E_2, we have $\lambda < b$ and therefore $c + e < b$. Thus the result of these normalizations is the unique prototypical splitting in the orbit of (X, ω, I). ■

Corollary 3.4 *The Weierstrass curve W_D is nonempty iff $D \ge 5$.*

Proof. For any discriminant $D \ge 5$ there is always at least one splitting prototype, namely $(a, b, c, e) = (0, (D - e)/4, 1, e)$, where $e = 0$ or 1 is chosen so $e \equiv D \bmod 4$. For $D = 1, 4$ there are none. ■

Relation of prototypes. It is easy to see that the projection (3.2) sends $\Omega W_D^s(a, b, c, e)$ to $\Omega Q_D(e, \ell, m)$ with $\ell = \gcd(a, b, c)$ and $\ell^2 m = bc$. Due to the ordering of E_1 and E_2, some components of ΩQ_D may fail to be in the image of ΩW_D^s; for example, $\Omega Q_5(1, 1, 1)$ is omitted.

4 Cusps

In this section we will establish:

Theorem 4.1 *There are natural bijections between:*

1. *The set of two-cylinder cusps $x \in C(W_D)$;*

2. *The set of components of the splitting space W_D^s; and*

3. *The set P_D of prototypes (a, b, c, e) of discriminant D.*

Cusps. Let $V = \mathbb{H}/\Gamma$ be a hyperbolic surface. A *cusp of* Γ is a point $x \in \partial\mathbb{H}$ fixed by a parabolic element $\gamma \in \Gamma$. The orbit of x under Γ is a *cusp of* V.

The cusps of V correspond bijectively to the finite-volume ends of V, and will be denoted $C(V)$. If $V = \bigcup V_i$ has more than one component, we define $C(V) = \bigcup C(V_i)$. When V has finite volume, its cusps can be adjoined to obtain a closed surface $\overline{V} = V \cup C(V)$.

Each cusp x determines a connected covering space $\widetilde{V}(x) \to V$, isomorphic to a punctured disk, with $\pi_1(\widetilde{V}(x)) \cong \mathbb{Z}$ generated by a small loop around x. A point $\widetilde{p} \in \widetilde{V}(x)$ corresponds to a point $p \in V$ with a chosen homotopy class of path from p to x.

Cylinders. Let $(X, \omega) \in \Omega\mathcal{M}_g$ be a holomorphic 1-form of genus $g \geq 2$. Then for each $s \in \mathbb{P}^1(\mathbb{R})$, we have a foliation $\mathcal{F}_s$ of $(X, |\omega|)$ by geodesics of slope s. The foliation $\mathcal{F}_s$ is tangent to $\operatorname{Ker}(\rho)$, where ρ is the closed 1-form $\operatorname{Re}(x + iy)\omega$, $s = x/y$.

The foliation $\mathcal{F}_s$ is *periodic* if every leaf is closed. In this case we define the *spine* of $\mathcal{F}_s$ to be the finite graph $S \subset X$ consisting of leaves through the zeros of ω. The components of $X - S$ form a finite set of open *cylinders* $C_1, \dots, C_n$, swept out by circular leaves of $\mathcal{F}_s$.

A central result from [V1, 2.4,2.11] is:

Theorem 4.2 (Veech dichotomy) *Suppose* $\operatorname{SL}(X, \omega)$ *is a lattice. Then for any slope s, either*

- *the foliation $\mathcal{F}_s$ is uniquely ergodic, or*

- *$\mathcal{F}_s$ is periodic with $n \geq 1$ cylinders, and $1/s$ is a parabolic fixed-point of* $\operatorname{SL}(X, \omega)$.

Thus the cusps of $V = \mathbb{H}/\operatorname{SL}(X, \omega)$ can be classified according to the number of cylinders of the corresponding periodic foliation $\mathcal{F}_s$.

Genus two. Recall that $\operatorname{SL}(X, \omega)$ is a lattice for any form in ΩW_D, so the Veech dichotomy applies.

Theorem 4.3 *Let s be a periodic slope for $(X, \omega) \in \Omega W_D$. Then either:*

- *$\mathcal{F}_s$ has one cylinder, and D is a square; or*

- *$\mathcal{F}_s$ has two cylinders, and (X, ω) splits as a connected sum of tori foliated by leaves of $\mathcal{F}_s$.*

Conversely, every splitting of (X, ω) comes from a periodic foliation $\mathcal{F}_s$ with two cylinders.

Proof. Let s be a periodic slope, let $S \subset X$ denote the spine of $\mathcal{F}_s$, and let $X - S = C_1 \cup \cdots \cup C_n$ be the complementary cylinders.

Let $\eta : X \to X$ denote the hyperelliptic involution. Then η fixes the 6 Weierstrass points of X, one of which is the double zero z_0 of ω. We have $\eta(C_i) = C_i$ for every i, and thus each cylinder contains 2 Weierstrass points. On the other hand, S is a bouquet of 3 circles joined at z_0, so $\bigcup C_i$ contains at most 4 Weierstrass points, and thus $n = 1$ or 2.

If $n = 2$, then S contains exactly one Weierstrass point p other than z_0. Therefore $S = L_0 \cup L_1 \cup K$ is a union of 3 loops meeting at z_0, with $p \in K$, $\eta(K) = K$ and $\eta(L_i) = L_{1-i}$). It follows from Theorem 3.2 that (X, ω) splits along $L_0 \cup L_1$ as a connected sum of tori.

The case $n = 1$ cannot arise when $\sqrt{D}$ is irrational, by [Mc2, Thm. 9.2].

Finally, let $(X, \omega) = (E_1, \omega_1) \underset{I}{\#} (E_2, \omega_2)$ be a splitting where I has slope s. Since I represents a closed loop on E_1, the foliation $\mathcal{F}_s | E_1$ is periodic; by isogeny, $\mathcal{F}_s | E_2$ is also periodic, so $\mathcal{F}_s$ gives a two-cylinder decomposition of X. ■

Cusps and prototypes. Since every (X, ω) has at least one splitting, we have:

Corollary 4.4 *Every component of W_D has a two-cylinder cusp.*

Proof of Theorem 4.1. A splitting $(X, \omega, I) \in \Omega W_D^s$, where I has slope s, picks out a parabolic point $1/s$ for $\mathrm{SL}(X, \omega)$ and hence a path from $[(X, \omega)] \in W_D$ to a two-cylinder cusp. Thus the splitting space can be described as:

$$W_D^s = \bigcup \widetilde{W_D}(x),$$

where the union is over the two-cylinder cusps $x \in C(W_D)$. On the other hand, we also have

$$W_D^s = \bigcup W_D^s(a, b, c, e),$$

where the union is over the splitting prototypes of discriminant D. By matching components, we obtain a canonical labeling of the cusps x by components of W_D^s, which are in turn labeled by prototypes. ■

Corollary 4.5 *When D is not a square, W_D has only two-cylinder cusps. In particular, $|C(W_D)| = |P_D|$.*

The one-cylinder cusps of W_{d^2} are studied in the Appendix.

5 Spin

In this section we introduce the *spin invariant* $\epsilon : \Omega W_D \to \mathbb{Z}/2$, and use it to prove:

Theorem 5.1 *The curve W_D has at least two components whenever $D \equiv 1 \bmod 8$ and $D > 9$.*

Spin structures. We begin with a brief discussion of spin structures on surfaces; for more details, see [At], [Jo] and [KZ].

Let V be a symplectic vector space of dimension $2g$ over the field $\mathbb{F}_2 \cong \mathbb{Z}/2$. A *quadratic form* on V is a function $q : V \to \mathbb{Z}/2$ satisfying

$$q(x + y) = q(x) + q(y) + x \cdot y, \tag{5.1}$$

where $x \cdot y$ is the symplectic form on V. The difference $q_1 - q_0$ of any two quadratic forms is a linear form; thus the number of quadratic forms on V is 2^{2g}. The *Arf invariant* of q is given by

$$\mathrm{Arf}(q) = \sum_1^g q(a_i)q(b_i) \in \mathbb{Z}/2,$$

where (a_i, b_i) is a symplectic basis for $H_1(X, \mathbb{Z})$; it is independent of the choice of basis. We say q is *even* or *odd* depending on the parity of $\mathrm{Arf}(q)$. There are 2^g more even forms than odd forms.

Now let $X \in \mathcal{M}_g$ be a compact Riemann surface. A *spin structure* $L \to X$ is the choice of a square-root of the canonical line bundle $K \to X$, up to isomorphism over X.

The spin structures on X correspond naturally to quadratic forms on $H_1(X, \mathbb{Z}/2)$. The quadratic form q_L associated to $L \to X$ can be defined as follows. Let $C : \mathbb{R}/\mathbb{Z} \to X$ be a smooth embedded loop, representing a class in $H_1(X, \mathbb{Z}/2)$. Let $\omega : C \to K$ be a smooth 1-form such that $\omega(C'(t)) = 1$ for all t. Then $q_L(C) = 1$ if and only if there is a section $\eta : C \to L$ such that $\eta^2 = \omega$.

A spin structure L is said to be *even* or *odd* depending on the value of $\mathrm{Arf}(q_L)$. The parity of L can also be described using the holomorphic structure of X: it is equal to $\dim H^0(X, L) \bmod 2$.

Spin from 1-forms. Any holomorphic 1-form $\omega \neq 0$ on X whose zeros have even order determines a spin structure, by taking $L = \mathcal{O}(D)$ where $2D = (\omega)$ is the divisor of ω.

In this case q_L can be computed as follows. Let $C : \mathbb{R}/\mathbb{Z} \to X$ be a smooth embedded loop avoiding the zeros of ω. The 1-form ω determines a *Gauss map* $G : S^1 \to S^1$ by

$$G = \frac{\omega(C'(t))}{|\omega(C'(t))|},$$

and we define $\deg(C, \omega) = \deg(G)$; then

$$q_L(C) = 1 + \deg(C, \omega) \bmod 2. \tag{5.2}$$

Note that the value of $\deg(C, \omega)$ changes by an even number if we slide C over a zero of ω.

When X has genus $g = 2$, each Weierstrass point $p \in X$ determines a spin structure on X, namely $L = \mathcal{O}(p)$. The six Weierstrass points correspond bijectively to the six odd spin structures on X.

Eigenforms. Now let (X,ω) be a form in ΩW_D, $D \equiv 1 \bmod 8$. Since ω has a double zero, it determines a canonical odd spin structure on X.

This spin structure is one ingredient in the definition of the spin invariant $\epsilon(X,\omega)$. The other ingredient comes from the action of real multiplication.

Theorem 5.2 *Let $(X,\omega) \in \Omega W_D$ be an eigenform for real multiplication by $\mathcal{O}_D = \mathbb{Z}[T]$, where $D \equiv 1 \bmod 8$. Then*

$$V = \operatorname{Im} T \subset H_1(X,\mathbb{Z}/2)$$

is a symplectic subspace isomorphic to $(\mathbb{Z}/2)^2$.

Proof. In $\mathcal{O}_D$ we have $T^2 + aT + b = 0$ where $D = a^2 + 4b$. Since $D \equiv 1 \bmod 8$, a is odd and b is even; thus $T^2 + T = 0 \bmod 2$.

Recall that the action of $\mathcal{O}_D$ on $H_1(X,\mathbb{Z})$ is self-adjoint. Thus the action of T on $H_1(X,\mathbb{Z}/2)$ is also self-adjoint. Since $T(T+1) = 0 \bmod 2$, the homology decomposes as a direct sum of symplectic eigenspaces

$$H_1(X,\mathbb{Z}/2) = V_0 \oplus V_1,$$

where $V_\lambda = \operatorname{Ker}(T - \lambda I)$.

Since $\mathcal{O}_D$ is a proper subring of $\operatorname{End}(\operatorname{Jac}(X))$, neither eigenspace can be trivial. For example, if V_1 is trivial, then V_0 is the whole space, which implies T is even and thus $(1/2)T \in \operatorname{End}(\operatorname{Jac}(X))$, contradicting properness. Thus both V_0 and $V = V_1$ are nontrivial symplectic subspaces of $H_1(X,\mathbb{Z}/2)$, so both have rank 2. ■

The virtual elliptic curve. The subspace V above has a simple geometric interpretation when $D = d^2$, d odd. In this case (X,ω) is an *elliptic differential*; that is, the periods of ω form a lattice $\Lambda \subset \mathbb{C}$, and the associated elliptic curve $E = \mathbb{C}/\Lambda$ is a factor of $\operatorname{Jac}(X)$. By integrating ω along paths based at its unique zero, we obtain a canonical degree d holomorphic map

$$p : X \to E.$$

Passing to cohomology, we obtain a map

$$p^* : H^1(E,\mathbb{Z}/2) \to H^1(X,\mathbb{Z}/2),$$

whose image is Poincaré dual to $\operatorname{Im}(T)$ for a suitable generator $T \in \mathcal{O}_D$.

When $D \equiv 1 \bmod 8$ is not a square, we lack the full geometry of E, but nevertheless the projection $X \to E$ persists on the level of mod 2 homology.

The conductor. The *conductor* f of $\mathcal{O}_D$ is the index of $\mathcal{O}_D$ in the maximal order of $K = \mathcal{O}_D \otimes \mathbb{Q}$.

When D is odd, we have $D = Ef^2$ with E square-free. A convenient choice of generator for $\mathcal{O}_D \subset \mathbb{R}$ is then given by

$$T_f = (f + \sqrt{D})/2 = f(1 + \sqrt{E})/2,$$

since this is a multiple of a generator for the maximal order $\mathcal{O}_E$.

The spin invariant. We can now complete the definition of the spin invariant. Let (X,ω) be an eigenform in ΩW_D with $D \equiv 1 \bmod 8$. Let $L \to X$ be the spin structure determined by ω, with quadratic form

$$q_L : H_1(X,\mathbb{Z}/2) \to \mathbb{Z}/2.$$

Let f be the conductor of $\mathcal{O}_D$, and let $\mathcal{O}_D = \mathbb{Z}[T_f]$ where

$$T_f^*(\omega) \quad = \quad \frac{f+\sqrt{D}}{2}\,\omega.$$

Then the *spin invariant* is defined by

$$\epsilon(X,\omega) = \operatorname{Arf}(q_L | \operatorname{Im} T_f).$$

When $D = d^2$ is an odd square, the conditions above do not quite uniquely determine $T_f \in \mathcal{O}_D$, since $2d - T_f$ satisfies the same conditions. The spin invariant is still well-defined, however, because $T_f = 2d - T_f \bmod 2$.

The spin ideal. Since $T^2 = T \bmod 2$ for any generator T of $\mathcal{O}_D$, we have

$$1 + \operatorname{Arf}(q_L | \operatorname{Im} T) = \operatorname{Arf}(q_L | \operatorname{Ker} T) = \operatorname{Arf}(q_L | \operatorname{Im}(T+1)). \qquad (5.3)$$

In particular, the map $\sigma : \mathcal{O}_D \to \mathbb{Z}/2$ given by

$$\sigma(U) = \operatorname{Arf}(q_L | \operatorname{Im} U)$$

is a ring homomorphism. A more functorial version of the spin invariant is provided by the *spin ideal*

$$I(X,\omega) = \operatorname{Ker}(\sigma) \subset \mathcal{O}_D\,.$$

The condition $D \equiv 1 \bmod 8$ is equivalent to the condition that $2\,\mathcal{O}_D$ factors as a product of distinct prime ideals $P_1 P_2$ in $\mathcal{O}_D$, and $I(X,\omega)$ coincides with one of these primes.

The invariant $\epsilon(X,\omega) = \sigma(T_f)$ is simply the image in $\mathcal{O}_D\,/I(X,\omega)$ of a convenient generator of $\mathcal{O}_D$; it also determines the spin ideal.

Even and odd eigenforms. For $D \equiv 1 \bmod 8$, we define the spaces of even and odd eigenforms by

$$\Omega W_D^i = \{(X,\omega) \in \Omega W_D \ : \ \epsilon(X,\omega) = i\}, \quad i \in \mathbb{Z}/2.$$

These spaces are $\mathrm{GL}_2^+(\mathbb{R})$-invariant $\mathbb{C}^*$-bundles over the even and odd subvarieties W_D^0, W_D^1 of the Weierstrass curve W_D.

Spin and prototypes. We say a *cusp* x of W_D has spin invariant ϵ if x belongs to $\overline{W_D^\epsilon}$. Similarly, a splitting prototype (a,b,c,e) has spin invariant ϵ if the connected set $\Omega W_D^s(a,b,c,e)$ projects into ΩW_D^ϵ. The parity of a prototype is the same as the parity of the cusp it labels.

Theorem 5.3 *The spin invariant of a splitting prototype (a, b, c, e) of discriminant $D \equiv 1 \bmod 8$ is given by*

$$\epsilon = \frac{e-f}{2} + (c+1)(a+b+ab) \bmod 2,$$

where f is the conductor of $\mathcal{O}_D$.

Proof. From the definitions the spin invariant of (a, b, c, e) is given by $\epsilon(X, \omega)$, where

$$(X, \omega) = (E_1, \omega_1) \underset{I}{\#} (E_2, \omega_2)$$

is the prototypical splitting of type (a, b, c, e). Using the identifications

$$H_1(X, \mathbb{Z}) = H_1(E_1, \mathbb{Z}) \oplus H_1(E_2, \mathbb{Z}) = \Lambda_1 \oplus \Lambda_2,$$

$\Lambda_i = \mathrm{Per}(\omega_i)$, we have a symplectic basis (a_i, b_i) for $H_1(X, \mathbb{Z})$ given by

$$\begin{array}{rclcll} \Lambda_1 & = & \mathbb{Z}(\lambda, 0) \oplus \mathbb{Z}(0, \lambda) & = & \mathbb{Z}a_1 \oplus \mathbb{Z}b_1 & \text{and} \\ \Lambda_2 & = & \mathbb{Z}(b, 0) \oplus \mathbb{Z}(a, c) & = & \mathbb{Z}a_2 \oplus \mathbb{Z}b_2, & \end{array}$$

where $\lambda = (e + \sqrt{D})/2$.

Let $q : H_1(X, \mathbb{Z}/2) \to \mathbb{Z}/2$ be the quadratic form associated to the spin structure determined by ω. It is easy to see that the homology class a_1 is represented by a loop $C : \mathbb{R}/\mathbb{Z} \to X$, avoiding the zero of ω and satisfying

$$\omega(C'(t)) = \int_{a_1} \omega = \lambda.$$

This loop can be taken as a closed geodesic on $(E_1 - I, |\omega_1|)$, or equivalently as a horizontal line through the middle of the $\lambda \times \lambda$ square in Figure 5 of §3. Since the direction of C is constant, its Gauss map has degree zero and thus

$$q(a_1) = 1 + \deg(\omega, C) = 1$$

by equation (5.2). Similarly $q(a_2) = q(b_2) = q(b_1 + b_2) = 1$, and thus $q(b_1) = 0$ by (5.1).

Now let $\mathcal{O}_D = \mathbb{Z}[T_e]$, where $T_e^*(\omega) = \lambda\omega$. Then $\int_{T_e(C)} \omega = \lambda \int_C \omega$ for any cycle $C \in H_1(X, \mathbb{Z})$. Using the periods given above, we find the corresponding endomorphism of $H_1(X, \mathbb{Z}/2)$ is given with respect to the basis (a_1, b_1, a_2, b_2) by

$$T_e = \begin{pmatrix} e & 0 & b & a \\ 0 & e & 0 & c \\ c & -a & 0 & 0 \\ 0 & b & 0 & 0 \end{pmatrix} \bmod 2.$$

Since $D \equiv 1 \bmod 8$, we have $e \equiv 1 \bmod 2$, and thus a symplectic basis for $V = \operatorname{Im} T_e$ is given by the first two columns (A_1, B_1) above. Using the values of q already obtained and the rule (5.1), we find

$$\begin{aligned} q(A_1) &= q(a_1 + cb_1) &=& \ 1 + c, \\ q(B_1) &= q(b_1 + aa_2 + bb_2) &=& \ a + b + ab. \end{aligned}$$

Therefore

$$\operatorname{Arf}(q|\operatorname{Im} T_e) = q(A_1)q(B_1) = (1 + c)(a + b + ab);$$

since $T_e = T_f + (e - f)/2$, this implies

$$\epsilon(X, \omega) = \operatorname{Arf}(q|\operatorname{Im} T_f) = \frac{(e - f)}{2} + (1 + c)(a + b + ab)$$

by (5.3). ■

Proof of Theorem 5.1. For any $D \equiv 1 \bmod 8$ with $D > 9$, we have a pair of splitting prototypes

$$(a, b, c, e) = (0, (D - 1)/4, 1, \pm 1)$$

of discriminant D with opposite spin invariants. Thus ΩW_D contains both even and odd eigenforms, and therefore W_D has at least two components. ■

6 Square-tiled surfaces

In this section we show that for $D = d^2$, the spin invariant carries the same information as the number of integral Weierstrass points, an invariant introduced by Hubert and Lelièvre in [HL].

A *square-tiled surface* is a form $(X, \omega) \in \Omega\mathcal{M}_2(2)$ such that $\operatorname{Per}(\omega) \subset \mathbb{Z}^2 \subset \mathbb{R}^2 = \mathbb{C}$. For such a surface, integration of ω gives a holomorphic map

$$p : X \to E = \mathbb{C}/\mathbb{Z}^2,$$

which can be normalized so it is branched only over $z = 0$. The $d = \deg(p)$ preimages of the square $[0, 1] \times [0, 1]$ provide a tiling of X. We say (X, ω) is *primitive* if $\operatorname{Per}(\omega) = \mathbb{Z}^2$; in this case, (X, ω) belongs to ΩW_{d^2}. Conversely, every $\mathrm{GL}_2^+(\mathbb{R})$-orbit in ΩW_{d^2} contains finitely many square-tiled surfaces.

A Weierstrass point $x \in X$ is *integral* if it lies at the vertex of a tile; in other words, if $p(x) = 0$.

Theorem 6.1 *Let $(X, \omega) \in \Omega W_{d^2}$ be a primitive square-tiled surface, with d odd. Then the number of integral Weierstrass points on X is given by*

$$N = \begin{cases} 1 & \textit{if } \epsilon(X, \omega) = 0, \textit{ and} \\ 3 & \textit{if } \epsilon(X, \omega) = 1. \end{cases}$$

Proof. The degree d projection $p : X \to E$ determines a natural symplectic splitting
$$H_1(X, \mathbb{Z}/2) = S_0 \oplus S_1,$$
where $S_0 = \mathrm{Ker}(p_*)$ and $S_1 \cong H_1(E, \mathbb{Z}/2)$.

Let $q : H_1(X, \mathbb{Z}/2) \to \mathbb{Z}/2$ denote the odd quadratic form coming from the spin structure associated to ω. Recall that the six Weierstrass points of X correspond naturally to the six odd quadratic forms on $H_1(X, \mathbb{Z}/2)$. A Weierstrass point is integral iff the correspond form satisfies $q'|S_1 = q|S_1$, in which case we have
$$\mathrm{Arf}(q'|S_0) = 1 + \mathrm{Arf}(q'|S_1) = 1 + \mathrm{Arf}(q|S_1)$$
since q' is odd. Conversely, the number of integral Weierstrass points agrees with the number of quadratic forms $q'|S_0$ satisfying the parity condition above.

To bring the spin invariant into play, let us write $\mathcal{O}_{d^2} = \mathbb{Z}[T_d]$ where $T_d^*(\omega) = d\omega$. Then $S_1 = \mathrm{Im}\, T_d$. Since $d = f$ is also the conduction of $\mathcal{O}_{d^2}$, we have
$$\mathrm{Arf}(q|S_1) = \mathrm{Arf}(q|\,\mathrm{Im}\, T_f) = \epsilon(X, \omega).$$

Thus $q'|S_0$ has the same parity as $1 + \epsilon(X, \omega)$. Since S_0 carries three even forms and one odd form, the Theorem follows. ■

Remark. The simple formulation of the preceding result is the reason we have used the conductor of $\mathcal{O}_D$ in the definition of $\epsilon(X, \omega)$.

Example: $D = 9$. The L-shaped surface $(X, \omega) \in \Omega W_9$ with $d = 3$ square tiles has a unique integral Weierstrass point; thus $N = 1$. For $D = 9$ there is a unique splitting prototype, namely $(a, b, c, e) = (0, 2, 1, -1)$, and the conductor of $\mathcal{O}_D$ is $f = 3$. Thus by Theorem 5.3 we have $\epsilon(X, \omega) = (-1 - 3)/2 \bmod 2 = 0$, in agreement with the Theorem above.

7 Butterfly moves

In this section we introduce an elementary move on splittings that yields a criterion for two cusps of W_D to belong to the same component.

Pairs of splittings. Let $(X, \omega) \in \Omega\mathcal{M}_2(2)$ be a form of genus two with a double zero, equipped with a splitting
$$(X, \omega) = (E_1, \omega_1) \underset{I}{\#} (E_2, \omega_2), \tag{7.1}$$
where $(E_i, \omega_i) = (\mathbb{C}/\Lambda_i, dz)$ and $I = [0, v]$. Recall that I maps to an embedded arc under the projection $\pi : \mathbb{C} \to E_2$, by our conventional ordering of the summands. The hyperelliptic involution η of X, when restricted to $E_2 - I$, has the form
$$\eta(z) = (v/2) - z. \tag{7.2}$$

Let $J = [0, w] \subset \mathbb{C}$ be a segment such that $\pi(J) \subset E_2$ is a simple loop. (This means $\pi|J$ identifies the endpoints of J but is otherwise injective.) Suppose in addition that

$$\pi(J) \cap \pi(I) = \{0\} \subset E_2.$$

Then $\pi(J)$ represents a saddle connection L_0 on X, satisfying $L_0 \neq L_1 = \eta(L_0)$ by (7.2). Thus by Theorem 3.2 we have a second splitting

$$(X, \omega) = (F_1, \eta_1) \underset{J}{\#} (F_2, \eta_2) \tag{7.3}$$

where, following our convention, J projects to a closed loop on F_1.

We say the splittings (X, ω, I) and (X, ω, J) are related by a *butterfly move*, because I and J give a pair of linked figure eights on the surface X (Figure 6).

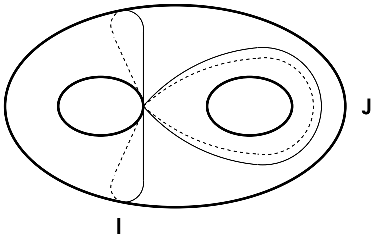

Figure 6. Butterfly move.

The geometric splitting (7.1) determines an algebraic splitting

$$H_1(X, \mathbb{Z}) = H_1(E_1, \mathbb{Z}) \oplus H_1(E_2, \mathbb{Z}),$$

while the oriented arcs I and J determine homology classes $[I] \in H_1(E_1, \mathbb{Z})$ and $[J] \in H_1(E_2, \mathbb{Z})$. The next result describes how this algebraic splitting changes under a butterfly move.

Theorem 7.1 *Let (a_i, b_i) be symplectic bases for $H_1(E_i, \mathbb{Z})$, $i = 1, 2$, with $[I] = a_1$ and $[J] = b_2$. Then we have*

$$\begin{aligned} H_1(F_1, \mathbb{Z}) &= \mathbb{Z}(a_2 - a_1) \oplus \mathbb{Z}b_2 \quad \textit{and} \\ H_1(F_2, \mathbb{Z}) &= \mathbb{Z}a_1 \oplus \mathbb{Z}(b_1 + b_2). \end{aligned}$$

(By a *symplectic basis* we mean the intersection numbers satisfy $a_i \cdot b_i = 1$.)

Proof. The parallel loops J and $\eta(J)$ cut $E_2 - I$ into two pieces. One is an $I \times J$ rectangle R, and the other an open cylinder identified with $F_1 - J$. The remainder of X is also an open cylinder, identified with $E_1 - I$; that is, we have:

$$X = (E_1 - I) \cup \overline{R} \cup (F_1 - J).$$

In this symmetric description, the two different splittings are obtained by allotting R to one side or the other. That is, $F_2 - J$ is obtained by gluing R to $E_1 - I$, while $E_2 - I$ is obtained gluing R to $F_1 - J$.

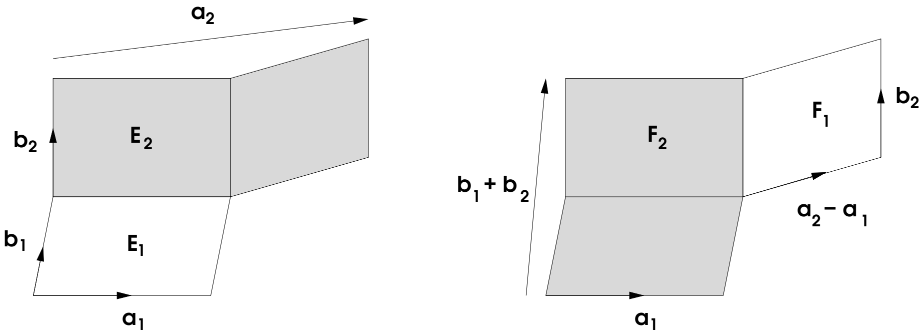

Figure 7. The surface X splits in two different ways:
as $E_1 \# E_2$ (left) and $F_1 \# F_2$ (right). The tori E_2 and F_2 are shaded.

The interchange of splittings is shown in Figure 7. Here (X, ω) is presented as the quotient $(P, dz)/\sim$ of an L-shaped polygon in $\mathbb{C}$ with parallel sides identified. The corner rectangle of P corresponds to R, and the two parallelograms, to E_1 and F_1.

As seen at the left, the edges of R represent the homology classes $a_1 = [I]$ and $b_2 = [J]$, and the edges of the lower parallelogram give the homology basis (a_1, b_1) for $H_1(E_1, \mathbb{Z})$. The edges of the shaded region formed by R and the parallelogram to its right give the homology basis (a_2, b_2) for $H_1(E_2, \mathbb{Z})$.

After performing a butterfly move, we obtain the splitting of X displayed at the right. Here R and E_1 have been combined to form F_2 (shaded), and the remaining parallelogram at the right represents F_1. As shown, $(a_2 - a_1, b_2)$ is then a symplectic basis for $H_1(F_1, \mathbb{Z})$, and $(a_1, b_1 + b_2)$ is a symplectic basis for $H_1(F_2, \mathbb{Z})$. ∎

Next we examine how different prototypes are related by butterfly moves.

Admissibility. Recall P_D denotes the finite set of splitting prototypes of discriminant D. Given $p = (a, b, c, e)$ in P_D, let

$$(X, \omega) = (E_1, \omega_1) \underset{I}{\#} (E_2, \omega_2)$$

be the corresponding prototypical splitting (§3). Using the identifications $H_1(E_i, \mathbb{Z}) = \mathrm{Per}(\omega_i) = \Lambda_i$, we have symplectic bases

$$\begin{aligned} \Lambda_1 &= \mathbb{Z}(\lambda, 0) \oplus \mathbb{Z}(0, \lambda) &&= \mathbb{Z}A_1 \oplus \mathbb{Z}B_1 \quad \text{and} \\ \Lambda_2 &= \mathbb{Z}(b, 0) \oplus \mathbb{Z}(a, c) &&= \mathbb{Z}A_2 \oplus \mathbb{Z}B_2 \end{aligned}$$

for the homology of E_1 and E_2. We also have $I = [0, \lambda]$, where $\lambda = (e + \sqrt{D})/2 > 0$. The projection of I to E_1 represents the class

$$[I] = A_1 \in H_1(E_1, \mathbb{Z}).$$

Now given an integer $q > 0$, let $J_q = [0, (a,c) + q(b,0)] \subset \mathbb{C}$; then J_q maps to a loop representing the class

$$[J_q] = A_2 + qB_2 \in H_1(E_2, \mathbb{Z}).$$

Similarly, we define $J_\infty = [0, (b,0)]$; then $[J_\infty] = B_2$. In both cases, q records the homological slope of J_q.

We say q is *admissible* for $p = (a,b,c,e)$ if, under the projection $\pi : \mathbb{C} \to E_2$, we have $\pi(J_q) \cap \pi(I) = \{0\}$. It is easy to see that $q = 1$ and $q = \infty$ are admissible for every prototype p.

Theorem 7.2 *The following conditions are equivalent:*

1. *The integer $q > 0$ is admissible for $(a,b,c,e) \in P_D$.*
2. *$|I| = \lambda = (e + \sqrt{D})/2$ is strictly less than b/q.*
3. *We have $(e + 2qc)^2 < D$.*

Proof. The loop $\pi(J_q)$ cuts $L = \mathbb{R}/\mathbb{Z}(b,0) \subset E_2$ into intervals of length b/q, and I is a subarc of L abutting J_q. Thus the first two conditions are equivalent. To see the last equivalence, note that $e + qc < \sqrt{D}$ is equivalent to

$$4qc\lambda < (\sqrt{D} - e)(\sqrt{D} + e) = 4bc,$$

and thus to $\lambda < b/q$; and $-\sqrt{D} < e + qc$ is automatic, because $e^2 < D$. ■

Butterfly maps. Let $P_D(q)$ denote the set of prototypes for which q is admissible.

When q is admissible for $p = (a,b,c,e)$, it defines a second splitting (X, ω, J_q) related to (X, ω, I) by a butterfly move. We have $(X, \omega, J_q) \in \Omega W_D^s(p')$, for a unique prototype p', and we define the *butterfly map*

$$B_q : P_D(q) \to P_D$$

by $B_q(p) = p'$.

Theorem 7.3 *For finite values of q, the butterfly map*

$$B_q(a,b,c,e) = (a', b', c', e')$$

satisfies $c' = \gcd(qc, b + qa)$ and $e' = -e - 2qc$.

Note: for our applications we will not need to keep track of the value of a', and b' is determined by the condition $D = (e')^2 + 4b'c'$.

Proof of Theorem 7.3. Let $(a_1, b_1) = (A_1, B_1)$ and $(a_2, b_2) = (-B_2, A_2 + qB_2)$ be symplectic bases for $H_1(E_i, \mathbb{Z})$, $i = 1, 2$, satisfying $[I] = a_1$ and $[J_q] = b_2$.

Then Theorem 7.1 provides a new splitting along J_q. The summands $(F_i, \eta_i) = (\mathbb{C}/\Lambda_i')$ of the new splitting satisfy $\Lambda_i' = M_i(\mathbb{Z}^2)$, where

$$M_1 = \begin{pmatrix} b+qa & \lambda + a \\ qc & c \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} \lambda & b+qa \\ 0 & \lambda + qc \end{pmatrix}$$

correspond to the symplectic bases $(b_2, a_1 - a_2)$ and $(a_1, b_1 + b_2)$ for $H_1(F_1, \mathbb{Z})$ and $H_1(F_2, \mathbb{Z})$ respectively.

Following the proof of Theorem 3.3, we can now locate the unique prototypical splitting in the $\mathrm{GL}_2^+(\mathbb{R})$-orbit of (X, ω, J_q). To this end, let $e' = -e - 2qc$, let $\lambda' = (e' + \sqrt{D})/2$, and let $g = \lambda' M_1^{-1} \in \mathrm{GL}_2^+(\mathbb{R})$. Note that $\lambda' > 0$ by the admissibility of q. Then we have

$$g(J_q) = [0, \lambda'], \quad g(\Lambda_1') = \lambda' \mathbb{Z}^2, \quad \text{and} \quad g(\Lambda_2') = N(\mathbb{Z}^2),$$

where

$$N = gM_2 = \begin{pmatrix} c & -a-e-qc \\ -qc & b+qa \end{pmatrix}.$$

Clearly the projection of $N(\mathbb{Z}^2) \subset \mathbb{R}^2$ to the y-axis is the subgroup $c'\mathbb{Z} \subset \mathbb{R}$, where $c' = \gcd(qc, b+qa)$. Therefore we have

$$N(\mathbb{Z}^2) = \mathbb{Z}(a', c') \oplus \mathbb{Z}(b', 0)$$

for suitable integers $a', b' > 0$ with a' reduced mod b'. Moreover, we have

$$\begin{gathered} (e')^2 + 4b'c' = (e+2qc)^2 + 4\det(N) = e^2 + 4bc = D, \\ \gcd(a', b', c', e') = \gcd(e', N_{ij}) = \gcd(a, b, c, e) = 1, \\ \text{and } c' + e' < b' \end{gathered}$$

because $\lambda' < b'$.

Replacing g with $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \cdot g$ for suitable n, we can further normalize so that $0 \le a' < \gcd(b', c')$. Then (a', b', c', e') is a prototype of discriminant D, and $g \cdot (X, \omega, J_q)$ is the corresponding prototypical splitting. In particular, (X, ω, J_q) belongs to $\Omega W_D^s(a', b', c', e')$ with $c' = \gcd(qc, b+qa)$ and $e' = -e - 2qc$. ■

Corollary 7.4 *If* $\gcd(b, qc) = 1$*, then*

$$B_q(0, b, c, e) = (0, b - qce - q^2c^2, 1, -e - 2qc).$$

Proof. Let $B_q(0, b, c, e) = (a', b', c', e')$. Then $e' = -e - 2c$ and $c' = 1$ by the preceding result; the condition $(e')^2 + 4b'c' = e^2 + 4bc$ determines b'; and $a' = 0$ since it is reduced $\bmod \gcd(b', c') = 1$. ■

A similar calculation establishes:

Theorem 7.5 *The butterfly map* $B_\infty(a, b, c, e) = (a', b', c', e')$ *satisfies* $c' = \gcd(a, c)$ *and* $e' = -e - 2c$.

8 From cusps to combinatorics

In this section we reduce the study of the geometric connectivity of W_D to a combinatorial problem, which we will solve in the next two sections.

Connecting prototypes. Let P_D be the set of splitting prototypes of discriminant D. Let $p \sim p'$ denote the equivalence relation on P_D generated by

$$p \sim B_q(p) \text{ whenever } q \in \{1, 2, 3, \ldots, \infty\} \text{ is admissible for } p. \tag{8.1}$$

We say p and p' are *connected* if they are equivalent, and we regard each equivalence class as a *component* of P_D. (This terminology refers to the topology on P_D whose open sets are unions of equivalence classes.)

Theorem 8.1 *The number of components of P_D is an upper bound for the number of components of the Weierstrass curve W_D.*

Proof. Recall there is a natural bijection

$$f : P_D \to C(W_D),$$

identifying the set of prototypes with the two-cylinder cusps of W_D (Corollary 4.4).

We claim that if p is connected to p' in P_D, then $f(p)$ and $f(p')$ belong to the same component of W_D. Since the equivalence relation on P_D is generated by (8.1), it suffices to establish the claim when $p' = B_q(p)$. But in this case there is a form (X, ω) admitting splittings $(X, \omega, I) \in \Omega W^s_D(p)$ and $(X, \omega, J_q) \in W^s_D(q)$. This implies $W^s_D(p)$ and $W^s_D(p')$ cover the same component of W_D, and hence $f(p)$ and $f(p')$ also belong to the same component.

By Corollary 4.4, every component of W_D has a two-cylinder cusp, and thus every component of W_D contains the image of a component of P_D. ∎

Reduced prototypes. Let us say a prototype $p = (a, b, c, e) \in P_D$ is *reduced* if $c = 1$; equivalently, if it has the form $p = (0, b, 1, e)$, where $e^2 + 4b = D$.

Theorem 8.2 *Every component of P_D contains a reduced prototype.*

Proof. Let $(a, b, c, e) = p$ be a prototype that minimizes the value of c among all $p' \sim p$. We will show p is reduced.

We begin by showing $a = 0$ and $c|b$. To see this, recall that $q = 1$ and $q = \infty$ are admissible for all p. By Theorem 7.5, $p \sim B_\infty(p) = (a', b', c', e')$ with $c' = \gcd(a, c)$. Since $c' \geq c > a \geq 0$, we have $a = 0$.

Similarly, let

$$p' = (a', b', c', e') = B_1(a, b, c, e) \sim p.$$

By Theorem 7.3, $c' = \gcd(b, c) \leq c$; but c is minimal, so $c = c'$ and $b|c$. Since $c' = c$, the same reasoning shows $a' = 0$ and $c|b'$. By Theorem 7.3 again, we have $e' = -e - 2c$. We also know

$$(e')^2 + 4b'c' = e^2 + 4bc = D,$$

and therefore $b' = b - c - e$. Since $c|b$ and $c|b'$, we have $c|e$. But then $c = \gcd(a, b, c, e) = 1$ by the definition of a splitting prototype, and therefore the prototype p is reduced. ∎

Combinatorial connectivity. To parameterize the reduced prototypes, let

$$S_D = \{e \in \mathbb{Z} \,:\, e \equiv D \bmod 2 \text{ and } e^2, (e+2)^2 < D\},$$

and define $\rho_D : S_D \to P_D$ by

$$\rho_D(e) = (0, (D - e^2)/4, 1, e).$$

Then ρ_D maps S_D bijectively to the set of reduced prototypes in P_D. For example, we have

$$S_{16} = \{-3, -1, 1\} \quad \text{and} \quad \rho_D(S_{16}) = \{(0, 3, 2, -1), (0, 6, 1, -1), (0, 6, 1, 1)\}.$$

Let $e \sim e'$ be the equivalence relation on S_D generated by

$$e \sim e' = -e - 2q \text{ whenenever } e' \in S_D \text{ and } \gcd(b, q) = 1, \tag{8.2}$$

where $q > 0$ and $b = (D - e^2)/4$ is determined by the condition $e^2 + 4b = D$. This relation describes the action of butterfly moves on reduced prototypes since, by Corollary 7.4, we have

$$B_q(\rho_D(e)) = B_q(0, b, 1, e) = (0, b - qe - q^2, 1, -e - 2q) = \rho_D(-e - 2q)$$

whenever q is admissible for e. In particular, the relation $e \sim e'$ implies $\rho_D(e) \sim \rho_D(e')$. Together with Theorem 8.2, this implies

Theorem 8.3 *The number of components of S_D is an upper bound for the number of components of P_D.*

Note that we do not need the action of B_∞, since $B_\infty(p) = B_1(p)$ when p is reduced.

Examples.

***D* = 4.** Here $S_D = \emptyset$, so W_4 is empty. (A surface of genus one admits no degree two cover branched over exactly one point.)

***D* = 5, 9.** Here $S_D = \{-1\}$, so W_D is connected.

***D* = 8, 12.** Here $S_D = \{-2, 0\}$; taking $q = 1$ in (8.2), we see S_D and W_D are connected in this case as well.

***D* = 13, 17.** Here $S_D = \{-3, -1, 1\}$. Taking $q = 1$ in (8.2), we see $-3 \sim 1$, so S_D has at most two components. When $D = 13$ we also have $-3 \sim 1$ (by taking $q = 2$), so W_{13} is connected; but W_{17} has exactly two components, because of the spin invariant (Theorem 5.1).

9 Relative primes

This section presents estimates for the smallest $x > 1$ relatively prime to n, and the smallest relative prime in an arithmetic progression. These results will be applied in the next section, to determine the number of components of S_D.

The smallest relative prime. Let $(\mathbb{Z}/n)^* \subset \mathbb{Z}/n$ denote the multiplicative group of integers $x \bmod n$ with $\gcd(x, n) = 1$. Its order is given by the Euler function

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product is taken over all primes dividing n. Since $\sum_{p \le x} 1/p = O(\log\log x)$, we have

$$\phi(n) \gg \frac{n}{\log\log n}$$

when n is large. In particular, there are many more relative primes than absolute primes ($\phi(n) \gg \pi(n) \sim n/\log n$). We begin by bounding the size of the smallest x relatively prime to n.

Theorem 9.1 *For any $n > 1$, there is an integer x relatively prime to n with*

$$1 < x \le \frac{3 \log n}{\log 2} \cdot$$

Note that the bound above is sharp for $n = 2$.

Proof. For a given n, the optimal choice for x is the smallest prime q not dividing n. Similarly, the smallest value of n demanding a particular prime q is the product of all primes less than q. Thus the Theorem is equivalent to the assertion

$$\frac{p_{k+1}}{\log(p_1 \cdot p_2 \cdots p_k)} \le \frac{3}{\log 2} \approx 4.328 \tag{9.1}$$

for all $k > 0$, where $p_1, p_2, p_3, \ldots = 2, 3, 5 \ldots$ is the sequence of primes.

Following Hardy and Wright [HW, Ch. XXII], let $\vartheta(x) = \sum_{p \le x} \log p$ and let $\psi(x) = \sum_{p^m \le x} \log p$. It is well-known that $\vartheta(x) \sim \psi(x) \sim x$ and $p_{k+1}/p_k \sim 1$, which implies

$$\frac{p_{k+1}}{\log(p_1 \cdot p_2 \cdots p_k)} = \frac{p_{k+1}}{\vartheta(p_k)} \sim \frac{p_{k+1}}{p_k} \sim 1$$

as $p_k \to \infty$. Consequently (9.1) holds whenever p_k is sufficiently large.

To make this an effective estimate, we will show that

$$\vartheta(x) \ge 19x/40$$

for all $x \ge 10^4$. Indeed, by [HW, p.342], we have

$$\psi(x) \ge \log \frac{(2y)!}{(y!)^2}$$

where $y = [x/2]$. By induction, the right-hand side is $\geq y$ for $y \geq 4$, and thus $\psi(x) \geq [x/2]$ for $x \geq 8$. On the other hand, we have

$$\vartheta(x) = \psi(x) - \sum_{m=2}^{\log x/\log 2} \vartheta(x^{1/m})$$

and $\vartheta(x) \leq 2x \log 2$, by [HW, p. 341]. It is straightforward to check that

$$2 \log 2 \sum_{m=2}^{\log x/\log 2} x^{1/m} < x/40$$

for all $x \geq 10^4$; combining these bounds, we obtain

$$\vartheta(x) \geq \psi(x) - x/40 \geq 19x/40$$

as claimed.

Now recall that $p_{k+1} \leq 2p_k$ for all k (Bertrand's postulate, [HW, p.343]). Thus for $p_k \geq 10^4$ we have

$$\frac{p_{k+1}}{\vartheta(p_k)} \leq \frac{2p_k}{19p_k/40} = \frac{80}{19} \approx 4.21 < \frac{3}{\log 2} \cdot$$

The proof is completed by verifying that (9.1) also holds for the 1229 primes satisfying $p_k < 10^4$. ■

Remark. The least $x > 1$ relatively prime to n also satisfies the lower bound $x > (1 - \epsilon) \log n$ infinitely often, since $\vartheta(x) \sim x$.

Gaps between relative primes. *Jacobsthal's function* $J(n)$ is defined to be the largest gap between consecutive integers relatively prime to n [Ja]; for example, $J(6) = 5 - 1 = 4$. A convenient estimate for $J(n)$ is provided by [Kan, Satz 4]:

Theorem 9.2 (Kanold) *For all $n \geq 1$, we have*

$$J(n) \leq 2^{\omega(n)},$$

where $\omega(n)$ is the number of distinct primes dividing n.

This result easily implies $J(n) \leq C_\epsilon n^\epsilon$, as well as:

Corollary 9.3 *If none of the first k primes $p_1 < p_2 < \ldots < p_k$ divide n, then we have*

$$J(n) \leq n^\alpha, \quad \alpha = \frac{\log(2)}{\log(p_{k+1})} \cdot$$

Proof. Each prime $p|n$ contributes a factor of at least $p^\alpha \geq 2$ to n^α, so $n^\alpha \geq 2^{\omega(n)} \geq J(n)$. ■

See [Er] and [St] for additional estimates on $J(n)$.

Relative primes in arithmetic progressions. Our second result bounds the smallest x relatively prime to n satisfying a given congruence condition.

To state this bound, let $a//b$ denote the largest divisor of a which is relatively prime to b. The quotient $a//b$ is obtained by removing from a all primes that divide b; for example, $20//6 = 5$. We then have:

Theorem 9.4 *For any $a, b, n \geq 1$ with $\gcd(a, b) = 1$, there is a positive integer $x \leq bJ(n//b)$ such that*

$$x \equiv a \bmod b \quad \textit{and} \quad \gcd(x, n) = 1.$$

Proof. We may assume $1 \leq a \leq b$. Let us write $x = a + by$, so the congruence $x \equiv a \bmod b$ is automatic. Then $\gcd(x, b) = 1$, so $\gcd(x, n) = \gcd(x, m)$ where $m = n//b$.

Since $\gcd(b, m) = 1$, b is invertible in $(\mathbb{Z}/m)^*$; that is, $bc \equiv 1 \bmod m$ for some c. By the definition of Jacobsthal's function we can find an integer y, $0 \leq y < J(m)$, such that $\gcd(ac + y, m) = 1$. Then we have

$$cx \equiv ac + bcy \equiv ae + y \bmod m,$$

which implies $\gcd(x, n) = \gcd(x, m) = \gcd(cx, m) = 1$; and by construction, we have $1 \leq x \leq b(y + 1) \leq bJ(m) = bJ(n//b)$. ■

10 Combinatorial connectivity

We have seen that the space S_D is a combinatorial caricature of the Weierstrass curve W_D, with at least as many components as W_D itself. In this section we will establish:

Theorem 10.1 *Assume $D \geq 5$ and $D \neq 9, 49, 73, 121$ or 169. Then S_D has exactly two components when $D \equiv 1 \bmod 8$, and otherwise just one.*

Small D. Recall from §8 that the space of reduced prototypes of discriminant D is parameterized by

$$S_D = \{e \equiv D \bmod 2 \;:\; e^2 < D \text{ and } (e + 2)^2 < D\},$$

equipped with the equivalence relation generated by

$$e \sim e' = -e - 2q \;\text{ whenenever } e' \in S_D \text{ and } \gcd(b, q) = 1. \tag{10.1}$$

Here $q > 0$ and $b = (D - e^2)/4$ is determined by the condition $e^2 + 4b = D$.

It is feasible to compute the number of components of S_D when D is reasonably small. For example, the number of components is one for $D = 9$ and three for $D = 49, 73, 121$ and 169, and one can verify:

Lemma 10.2 *Theorem 10.1 holds for all $D \le 2000$.*

Spin invariant. There is a simple congruence condition, equivalent to the spin invariant, that explains why S_D has (at least) two components when $D \equiv 1 \bmod 8$.

Theorem 10.3 *If $e \sim f$ in S_D and $D \equiv 1 \bmod 8$, then $e \equiv f \bmod 4$.*

Proof. The condition $D \equiv 1 \bmod 8$ implies $b = (D - e^2)/4$ is even, and hence q relatively prime to b is odd. Since e is also odd, we have $e \equiv -e - 2q \bmod 4$. ■

Small primes. To determine the components of S_D for general D, we begin by showing that the relations coming from $q = 1, 3, 5$ and 7 already connect large parts of S_D.

First note that by taking $q = 1$ in (10.1), we have $e \sim -e - 2$ for every $e \in S_D$. That is, every component of S_D is symmetric under reflection through $e = -1$. In particular, every component contains an element $e \le -1$.

Next consider $q \ge 2$. Let $b = (D - e^2)/4$ as before, and suppose

$$F_q(e) = e + 2(q - 1)$$

also belongs to S_D. Then we have

$$e \sim F_q(e) \quad \text{whenever} \quad \gcd(b, q) = 1,$$

because $e \sim -e - 2q \sim -(-e - 2q) - 2 = F_q(e)$.

In the case where $q = p$ is an odd prime, we have $\gcd(b, p) = \gcd(D - e^2)$, and therefore

$$e \sim F_p(e) \quad \text{whenever} \quad D \not\equiv e^2 \bmod p. \tag{10.2}$$

Since the equivalence relation is symmetric, we also have

$$e \sim F_{-p}(e) = e - 2(p - 1) \quad \text{whenever} \quad D \not\equiv (e + 2)^2 \bmod p. \tag{10.3}$$

We say $\pm p$ is *admissible* for (D, e) if the corresponding congruence inequality in (10.2) or (10.3) is satisfied. Clearly admissibility depends only on the value of $(D, e) \bmod p$.

Theorem 10.4 *Suppose $e - 12$ and $e + 16$ belong to S_D. Then*

- *$e \sim e + 4$, or*
- *(D, e) is congruent to $(1, -4)$ or $(1, -1)$ when reduced modulo $105 = 3{\cdot}5{\cdot}7$.*

Proof. The Theorem is immediate when $D \equiv 2 \bmod 3$, or more generally whenever $D \not\equiv e^2 \bmod 3$. Indeed, in this case F_3 is admissible for (D, e), and therefore $e \sim F_3(e) = e{+}4$. This argument covers two-thirds of the 105^2 possible values for $(D, e) \bmod 105$, or 7350 cases.

More generally, to prove $e \sim e+4$, it is sufficient to exhibit sequences

$$\begin{aligned} (p_1, \ldots, p_k) \quad &\text{in} \quad P = \{\pm 3, \pm 5, \pm 7\} \;\text{ and} \\ (e_1, \ldots e_{k+1}) \quad &\text{in} \quad E \equiv e + \{-12, -8, -4, 0, 4, 8, 12, 16\} \subset (\mathbb{Z}/105) \end{aligned}$$

such that $e \equiv e_1$, $e+4 \equiv e_{k+1}$, p_i is admissible for (D, e_i) and $e_{i+1} = F_{p_i}(e_i)$. We refer to $(p_1, \ldots, p_k)$ as a *strategy* for (D, e).

For example, if $(D, e) \equiv (16, 59) \bmod 105$, we can use the strategy $(-7, 5, 5)$ to move e along the sequence $(59, 47, 55, 63)$ to reach $e + 4 \equiv 63$. To check the admissibility of a given transition $F_{p_i}(e_i) = e_{i+1}$, such as $F_{-7}(59) = 47$, one need only check that (D, e_i) satisfies the corresponding congruence inequality, in this case

$$D \equiv 16 \equiv 2 \not\equiv (e_i + 2)^2 \equiv (59 + 2)^2 \equiv 4 \bmod 7.$$

It is straightforward to verify that a strategy as above exists for every pair $(D, e) \bmod 105$ with the two exceptions stated in the Theorem. In fact, each of these $105^2 - 2 = 11023$ cases can be handled by one of the 12 strategies listed in Table 8. ■

Remarks. When $(D, e) = (1, -1) \bmod 105$ we have

$$D \equiv e^2 \equiv (e+2)^2 \bmod p$$

for $p = 3, 5$ and 7, and therefore no $p \in P$ is admissible for (D, e). A similar difficulty would arise for any finite set of primes P.

$(p_1, \ldots, p_k)$	Cases	$(p_1, \ldots, p_k)$	Cases
(3)	7350	$(-5, 3, 5)$	9
$(5, -3)$	1960	$(5, 5, -7)$	6
$(7, -5)$	1176	$(-7, 5, 5)$	6
$(-3, 5)$	378	$(-3, 7, -3)$	1
$(-5, 7)$	126	$(-5, 3, 7, -3)$	1
$(5, 3, -5)$	9	$(-3, 7, 3, -5)$	1

Table 8. Connection strategies and the number of cases they handle.

Edge effects. Next we account for e close to the ends of the range S_D. Let

$$T_D = \{e \in S_D \; : \; e - 12, e + 16 \in S_D\}.$$

Then we have:

Theorem 10.5 *For $D > 900$, any $f \in S_D$ is equivalent to an $e \in T_D$.*

Proof. We may assume $f \le -1$ since $f \sim -f-2$. If $f-12 \in S_D$ we can simply take $e=f$; otherwise, we have

$$f^2 < D \le (f-12)^2$$

by the definition of S_D. It suffices now to show that $f \sim e$ with $f < e$ and $e+16 \in S_D$, since by repeatedly increasing f we can also obtain $e-12 \in S_D$, and thereby $e \in T_D$. In fact it suffices to obtain an e with

$$f < e < e+18 < \sqrt{D},$$

since for $e > f$ we have $e+16 \in S_D \iff e+18 < \sqrt{D}$.

The inequality $30^2 < D \le (f-12)^2$ implies $f \le -20$ and

$$b = (D-f^2)/4 \le 6(6-f).$$

Now if $\gcd(b,p)=1$ for some prime $p \le 13$, we have

$$f \sim e = F_p(f) = f + 2(p-1) > f,$$

and at the same time

$$e+18 = 18+f+2(p-1) \le 18-20+24 = 22 < \sqrt{D},$$

as desired.

It remains to handle the case where b is divisible by all primes $p \le 13$. In this case we have $D \ge 4b \ge 10^6$. By Theorem 9.1, there is an integer q relatively prime to b with

$$1 < q < \frac{3\log b}{\log 2} \le 5\log(D),$$

and hence an $e \sim f$ with

$$f < e = f + 2(q-1) \le 10\log(D).$$

Since $10\log(D)+18 < \sqrt{D}$ for all $D \ge 10^6$, we have $e+18 < \sqrt{D}$, completing the proof. ■

Corollary 10.6 *Theorem 10.1 holds for all $D \not\equiv 1 \bmod 105$.*

Proof. By Lemma 10.2, we may assume $D \ge 900$; then by Theorem 10.5, every component of S_D meets T_D.

Consider the partition $T_D = T_D^0 \sqcup T_D^1$, where

$$T_D^i = \{e \in T_D \,:\, e \equiv D + 2i \bmod 4\}.$$

By Theorem 10.4 we have $e \sim e+4$ whenever e and $e+4$ are both in T_D. Therefore all elements of T_D^0 are equivalent, as are all elements of T_D^1. This shows S_D has at most two components.

Since D is a quadratic discriminant, we have $D \equiv 0, 1, 4$ or $5 \bmod 8$. To complete the proof, we analyze each of these possibilities in turn.

If $D \equiv 0$ or $4 \bmod 8$, then we have $e = 0 \sim -e - 2 = -2 \not\equiv e \bmod 4$. This shows $0 \in T^0_D$ is joined to $i - 2 \in T^1_D$ and therefore S_D is connected.

If $D \equiv 5 \bmod 8$, then $b = (D - e^2)/4$ is odd when $e = 1$. Therefore $\gcd(b, q) = 1$ when $q = 2$, and therefore $1 \sim -1 - 2q = -5 \not\equiv 1 \bmod 4$. Thus S_D is connected in this case as well.

Finally if $D \equiv 1 \bmod 8$, then S_D has at least two components by Theorem 10.3. ■

The exceptional case. To complete the proof, we will use Theorem 9.4 on relative primes in an arithmetic progression to give an argument that works even if $D \equiv 1 \bmod 105$.

Let

$$U_D = \{e \in T_D \ : \ e \not\equiv -1 \bmod 105\},$$

and consider the partition $U_D = U^0_D \cup U^1_D$, where $U^i_D = U_D \cap T^i_D$.

Lemma 10.7 *For $D > 900$, the sets U^0_D and U^1_D are each contained in a single component of S_D.*

Proof. By Theorem 10.4 we have $e \sim e + 4$ whenever both lie in U_D. This almost shows that all elements of U^i_D are equivalent; however, a gap arises because we have excluded those $e \equiv -1 \bmod 5$. To bridge this gap, we simply note that if $e \equiv -5 \bmod 105$, then $e \sim e + 8 = F_5(3)$, since

$$e^2 \equiv 0 \not\equiv D \equiv 1 \bmod 5.$$

Thus all the elements of U^i_D are equivalent in S_D. ■

Lemma 10.8 *For $D > 2000$, any $e \in S_D$ is equivalent to an $f \in U_D$.*

Proof. By Theorem 10.5, we can assume $e \in T_D$. We can also assume $e \leq -1$, since $e \sim -e - 2$; and $e \equiv -1 \bmod 105$, since otherwise $e \in U_D$.

Suppose we can find an integer $q \geq 1$ such that

$$\gcd(b, q) = 1, q \not\equiv 1 \bmod 105 \text{ and } 2q + 15 < \sqrt{D}. \tag{10.4}$$

Let $f = F_q(e) = e + 2(q - 1)$. Then, since $e \leq -1$, we have

$$f + 18 = e + 2q + 16 \leq 2q + 15 < \sqrt{D}$$

and therefore $f \in T_D$. In fact $f \in U_D$, because $f - e = 2(q - 1) \not\equiv 0 \bmod 105$; and $e \sim f$, because $\gcd(b, q) = 1$. Thus to complete the proof, it suffices to find q satisfying (10.4).

Since $D > 2000$, we have $\sqrt{D} > 44$ and hence the last two conditions of (10.4) are automatic for $q = 2, 3, 5, 7, 11$ and 13. Thus we are done unless b is divisible $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$.

So assume $30030|b$; then we have $\sqrt{D} \geq \sqrt{4b} > 346$. In this case the last two conditions of (10.4) are automatic for all primes $p \leq 165$. Again we are done unless b is divisible by all these primes, in which case we have $b \geq 10^{63}$.

Now pick any integer a with $1 < a < 105$. Then by Theorem 9.4, there is a positive integer $q \leq 210J(b//210)$ with $\gcd(b, q) = 1$ and $q \equiv a \neq 1 \bmod 105$. Since no prime smaller than 11 divides $b//210$, and $2^3 < 11$, Corollary 9.3 gives

$$q \leq 210J(b//210) \leq 210b^{1/3}.$$

But $b > 10^{63}$, so we have

$$2q + 15 \leq 420b^{1/3} + 15 \lll b^{1/2} < D^{1/2}.$$

Thus q satisfies (10.4), and therefore $e \sim f \in U_D$. ■

Proof of Theorem 10.1. By Lemma 10.2 we can assume $D > 2000$. Then the preceding Lemmas imply S_D has at most two components: one containing U_D^0 and another containing U_D^1. When $D \equiv 1 \bmod 8$, there are exactly two components by Theorem 10.3; otherwise, U_D^0 and U_D^1 are connected to each other by the same argument used in the proof of Corollary 10.6. ■

11 Geometric connectivity

We can now complete the proof of our main result.

Theorem 11.1 *The Weierstrass curve W_D is connected unless $D \equiv 1 \bmod 8$ and $D \neq 9$, in which case it has exactly two components.*

Lemma 11.2 *For $D = 49, 73, 121$ and 169, the space of prototypes P_D has exactly two components, while for $D = 9$ it has just one.*

Proof. The space P_9 consists of a single prototype, namely $(a, b, c, e) = (0, 2, 1, -1)$, so it is connected. For the other values of D, P_D has at least two components because $D \equiv 1 \bmod 8$.

For $D = 49$ it is straightforward to check that $S_{49} = \{-5, -3, -1, 1, 3\}$ has 3 components, namely $\{-5, 3\}$, $\{-3, 1\}$ and $\{-1\}$. Consequently every $p \in P_{49}$ is connected to at least one of the reduced prototypes $\rho_D(-1), \rho_D(-3)$ or $\rho_D(-5)$.

But in fact $\rho_D(-1) \sim \rho_D(-5)$. To see this, recall from Corollary 7.4 that

$$B_q(0, b, c, e) = \rho_D(-e - 2qc)$$

whenever $\gcd(b, qc) = 1$. Applying B_q to the prototype $p = (0, 5, 2, -3)$ in S_{49} with $q = 1, 2$, we find

$$\rho_D(-1) = B_1(0, 5, 2, -3) \sim B_2(0, 5, 2, -3) = \rho_D(-3).$$

Thus P_{49} has at most two components, and hence exactly two.

Similarly S_{73} has 3 components, represented by $e \in \{-1, 1, 3\}$, but

$$\rho_D(3) = B_1(0, 3, 2, -7) \sim B_2(0, 3, 2, -7) = \rho_D(-1),$$

so P_{73} itself has only two components. For S_{121} we have 3 components, represented by $e \in \{1, 3, 5\}$, but again P_{121} has just 2 components, because

$$\rho_D(3) = B_1(0, 9, 2, -7) \sim B_2(0, 9, 2, -7) = \rho_D(-1).$$

Finally the components of S_{169} are represented by $e \in \{1, 3, 5\}$, while

$$\rho_D(5) = B_1(0, 11, 2, -9) \sim B_2(0, 11, 2, -9) = \rho_D(-1),$$

so P_{169} has exactly 2 components as well. ■

Proof of Theorem 11.1. Let $n_D = 2$ if $D > 9$ is congruent to $1 \bmod 8$, and let $n_D = 1$ otherwise. Let p_D and s_D denote the number of components of P_D and S_D respectively. Then for every $D \geq 5$ we have

$$n_D \leq (\text{the number of components of } W_D) \leq p_D \leq s_D.$$

(The lower bound comes from Corollary 3.4 and Theorem 5.1, while the upper bounds come from Theorems 8.1 and 8.3.) By Theorem 10.1, $s_D = n_D$ except when $D = 9, 49, 73, 121, 169$; but then $n_D = p_D$ by the Lemma above. Therefore n_D gives the number of components of W_D for every $D \geq 5$. ■

The proof also shows:

Corollary 11.3 *The space of splitting prototypes P_D and the Weierstrass curve W_D have the same number of components for every D.*

A Appendix: One-cylinder cusps

In this appendix we briefly describe the one-cylinder cusps of W_D, and how the two types of cusps are partitioned between W_D^0 and W_D^1 when $D \equiv 1 \bmod 8$. For more on the cusps of W_{d^2}, see [HL] and [EMS].

One-cylinder cusps. As for the case of two cylinders, it is useful to organize the one-cylinder cusps by prototypes.

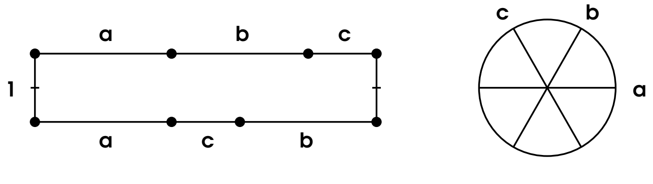

Figure 9. One-cylinder prototype.

Let $\langle a,b,c\rangle$ denote a cyclically ordered set of integers. We say $\langle a,b,c\rangle$ is a *one-cylinder prototype* for discriminant D if:

$$D = (a+b+c)^2, \quad a,b,c > 0, \quad \text{and} \quad \gcd(a,b,c) = 1.$$

We let R_D denote the set of all one-cylinder prototypes of discriminant D.

Theorem A.1 *Let $D = d^2 > 0$. Then the one-cylinder cusps of W_D are labeled by the one-cylinder prototypes $\langle a,b,c\rangle$ of discriminant D, with spin invariant*

$$\epsilon \equiv 1 + abc \bmod 2 \tag{A.1}$$

when $D \equiv 1 \bmod 8$.

Proof. By the results of §4, the one-cylinder cusps of W_D correspond to $\mathrm{GL}_2^+(\mathbb{R})$-orbits of pairs

$$((X,\omega),s) \in \Omega W_D \times \mathbb{P}^1(\mathbb{R}),$$

such that the foliation $\mathcal{F}_s$ of $(X,|\omega|)$ by geodesics with slope s is periodic with one cylinder C. Since $D = d^2$, every orbit has a representative where $s = 0$ and (X,ω) is a primitive square-tiled surface. Then ∂C consists of 3 saddle connections, with integral lengths (a,b,c). Since $\mathrm{Per}(\omega) = \mathbb{Z}^2$, the cylinder C must have height one and circumference $d = a+b+c$, with $\gcd(a,b,c) = 1$. Thus, after adjusting by the action of $N(\mathbb{Z}) = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\}$, we can put (X,ω) into the form $(P,dz)/\sim$, where P is the polygon shown in Figure 9. The ordering of the leaves of $\mathcal{F}_0$ around the zero of ω (shown at the right) gives a natural cyclic ordering to the lengths (a,b,c), yielding a complete invariant for the corresponding cusp of W_D.

The number of integral Weierstrass points of (X,ω) is one iff $abc \equiv 1 \bmod 2$, in which case $\epsilon = 0$ by Theorem 6.1. Otherwise, there are additional integral Weierstrass points at the mid-points of the saddle connections of even length, so $\epsilon = 1$. ■

Compare [HL, 5.1.1], [EMS, eq. (11)].

Corollary A.2

1. *The number of cusps of W_D is given by $|P_D| + |R_D|$.*
2. *When $D = d^2$, every component of W_D contains a one-cylinder cusp.*
3. *Every square-tiled surface has a one-cylinder direction.*

Proof. Since every cusp of W_D has one or two cylinders (Theorem 4.3), the first assertion is immediate from Theorem 4.1 and the preceding result. The second follows from the classification of the components of W_D (Theorem 1.1), upon noting that the prototypes $\langle 1, 1, d-2\rangle$ and $\langle 1, 2, d-3\rangle$ represent one-cylinder cusps of W_D, with opposite spin when d is odd. The third assertion is equivalent to the second. ■

Counting cusps by spin. Next we compare the number of even and odd cusps.

Theorem A.3 *When $D \equiv 1 \bmod 8$ is not a square, W_D^0 and W_D^1 have the same number of cusps.*

Proof. By the results of §4, W_D has only two-cylinder cusps, each labeled by a splitting prototype. Let $(a, b, c, e) \in P_D$ be a prototype of discriminant D. Then $D = e^2 + 4bc \equiv 1 \bmod 8$, so bc is even.

We define a bijection $F : P_D \to P_D$ as follows. For $(b, c) \equiv (0, 0) \bmod 2$, let

$$F(a, b, c, e) = (a + 1, b, c, e)$$

where $a + 1$ is taken modulo $\gcd(b, c)$. Otherwise, let

$$F(a, b, c, e) = \begin{cases} (a, c, b, e) & \text{if } b + e < c, \text{ and} \\ (a, b, c, -e) & \text{if } b + e > c. \end{cases}$$

(Note that the case $b+e = c$ does not occur, because it would imply $D = (b+c)^2$.)

By Theorem 5.3, the spin invariant of the prototype (a, b, c, e) is given by

$$\epsilon = \frac{e-f}{2} + (c + 1)(a + b + ab) \bmod 2,$$

where f is the conductor of $\mathcal{O}_D$. Thus F exchanges even and odd prototypes, so they must be equal in number. ■

Example. The reducible curve W_{17} has six cusps, paired off as follows:

$$\begin{array}{llll} W_{17}^0: & (0,2,2,1) & (0,4,1,-1) & (0,2,1,-3) \\ W_{17}^1: & (1,2,2,1) & (0,4,1,1) & (0,1,2,-3). \end{array}$$

Square discriminant. When $D = d^2$ is an odd square, each component W_D^i of W_D has both one- and two-cylinder cusps, labeled by the prototypes R_D^i and P_D^i with spin invariant i. We conclude with two formulas that allow $|P_D^i|$ and $|R_D^i|$ to be efficiently computed from $|P_D|$ and $|R_D|$.

Theorem A.4 *Let $D = d^2$ be an odd square. Then the number of even and odd cusps of W_D with two cylinders are related by*

$$|P_D^0| - |P_D^1| \;=\; \sum_{b+c=d, 0<c<b} \phi(\gcd(b,c)). \tag{A.2}$$

For one cylinder we have the relation

$$3|R_D^0| - |R_D^1| \;=\; \phi(d)/2, \tag{A.3}$$

provided $d > 3$.

Proof. The two-cylinder case follows the same lines as the proof of Theorem A.3, except that now prototypes (a,b,c,e) with $e^2 + 4bc = (b+c)^2 = D$ can occur. However these prototypes always have the form $(a,b,c,c-b)$ with $c < b$, by the relation $c + e < b$. Thus the number of such prototypes is given by the sum in (A.2). Noting that $f = d$ is the conductor of $\mathcal{O}_D$, we find the splittings with $b + c = d$ all have spin 0, because

$$\frac{e-f}{2} + (c+1)(a+b+ab) \equiv \frac{c-b-f}{2} + b \equiv \frac{d-f}{2} \equiv 0 \bmod 2,$$

so they account exactly for the difference $|P_D^0| - |P_D^1|$.

To prove (A.3), for $k = 0,1$ consider the set of *ordered* triples

$$\begin{aligned} A_k \;=\; & \{(a,b,c) \,:\, (a,b,c) \equiv (1,k,k) \bmod 2,\;\; a+b+c = d, \\ & a,b,c > 0 \;\text{ and }\; \gcd(a,b,c) = 1\}. \end{aligned}$$

By Theorem A.1, a prototype in R_D^0 contains three odd integers, while a prototype in R_D^1 contains just one. Thus $|A_0| = |R_D^1|$ and $|A_1| = 3|R_D^0|$. Now let

$$A_2 = \{(a,0,d-a) \,:\, 0 < a < d,\ a \text{ is odd and } \gcd(a,d) = 1\}.$$

Clearly $|A_2| = \phi(d)/2$. Let F be the unique permutation of $A_0 \cup A_1 \cup A_2$ satisfying

$$F(a,b,c) = (a,b',c') \;\text{ with } b' \equiv b + \gcd(a,d) \bmod (d-a).$$

Since a and d are odd, so is $\gcd(a,d)$; therefore b' and b have opposite parity. This implies $F(A_1) = A_0 \cup A_2$, and therefore

$$|A_1| = 3|R_D^0| = |A_0| + |A_2| = |R_D^1| + \phi(d)/2.$$

■

Examples. For $D = d^2$ with $d = 5$, we have

$$\begin{aligned} R_D^0 &= \{\langle 1,1,3\rangle\}, \quad R_D^1 \;=\; \{\langle 1,2,2\rangle\}, \\ P_D^0 &= \{(0,3,2,-1),(0,6,1,1),(0,2,2,-3),(0,4,1,-3)\} \quad \text{and} \\ P_D^1 &= \{(0,6,1,-1),(1,2,2,-3)\}. \end{aligned}$$

Thus W_D^0 has $|R_D^0| + |P_D^0| = 5$ cusps, while W_D^1 has 3. The numbers of cusps for other small values of d appear in Table 10.

d	3	5	7	9	11	13	15	17
$\lvert C(W^0_{d^2})\rvert$	1+1	1+4	2+8	3+13	5+21	7+30	8+34	12+48
$\lvert C(W^1_{d^2})\rvert$	0+0	1+2	3+5	6+8	10+16	15+24	20+22	28+40

Table 10. The number of (one-cylinder)+(two-cylinder) cusps of the components of the Weierstrass curve.

References

[At] M. F. Atiyah. Riemann surfaces and spin structures. *Ann. scient. Éc. Norm. Sup.* **4**(1971), 47–62.

[BL] C. Birkenhake and H. Lange. *Complex Abelian Varieties.* Springer-Verlag, 1992.

[Ca] K. Calta. Veech surfaces and complete periodicity in genus 2. *J. Amer. Math. Soc.* **17**(2004), 871–908.

[Er] P. Erdös. On the integers relatively prime to n and on a number-theoretic function considered by Jacobsthal. *Math. Scand.* **10**(1962), 163–170.

[EMS] A. Eskin, H. Masur, and M. Schmoll. Billiards in rectangles with barriers. *Duke Math. J.* **118**(2003), 427–463.

[EO] A. Eskin and A. Okounkov. Asymptotics of numbers of branched coverings of a torus and volumes of moduli spaces of holomorphic differentials. *Invent. math.* **145**(2001), 59–103.

[vG] G. van der Geer. *Hilbert Modular Surfaces.* Springer-Verlag, 1987.

[GK] B. H. Gross and K. Keating. On the intersection of modular correspondences. *Invent. math.* **112**(1993), 225–245.

[GJ] E. Gutkin and C. Judge. Affine mappings of translation surfaces: geometry and arithmetic. *Duke Math. J.* **103**(2000), 191–213.

[HW] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 1979.

[HZ] F. Hirzebruch and D. Zagier. Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus. *Invent. math.* **36**(1976), 57–113.

[HL] P. Hubert and S. Lelièvre. Square-tiled surfaces in $\mathcal{H}(2)$. *Preprint, 2004.*

[Ja] E. Jacobsthal. Über Sequenzen ganzer Zahlen, von denen keine zu n teilerfremd ist. I, II, III. *Norke Vid. Selsk. Forh. Trondheim* **33**(1961), 117–124, 125–131, 132–139.

[Jo] D. Johnson. Spin structures and quadratic forms on surfaces. *J. London Math. Soc.* **22**(1980), 365–373.

[Kan] H.-J. Kanold. Über eine zahlentheoretische Funktion von Jacobsthal. *Math. Ann.* **170**(1967), 314–326.

[KS] R. Kenyon and J. Smillie. Billiards on rational-angled triangles. *Comment. Math. Helv.* **75**(2000), 65–108.

[Kn] A. W. Knapp. *Elliptic Curves.* Princeton University Press, 1992.

[KZ] M. Kontsevich and A. Zorich. Connected components of the moduli spaces of Abelian differentials with prescribed singularities. *Invent. math.* **153**(2003), 631–678.

[Lang] S. Lang. *Elliptic Functions.* Springer-Verlag, 1987.

[La] E. Lanneau. Hyperelliptic components of the moduli spaces of quadratic differentials with prescribed singularities. *Comment. Math. Helv.* **79**(2004), 471–501.

[Mc1] C. McMullen. Billiards and Teichmüller curves on Hilbert modular surfaces. *J. Amer. Math. Soc.* **16**(2003), 857–885.

[Mc2] C. McMullen. Teichmüller geodesics of infinite complexity. *Acta Math.* **191**(2003), 191–223.

[Mc3] C. McMullen. Teichmüller curves in genus two: Torsion divisors and ratios of sines. *Invent. math.* **165**(2006), 651–672.

[Mc4] C. McMullen. Dynamics of $\mathrm{SL}_2(\mathbf{R})$ over moduli space in genus two. *Annals of Math.* **165**(2007), 397–456.

[Pu] J.-C. Puchta. On triangular billiards. *Comment. Math. Helv.* **76**(2001), 501–505.

[Ru] B. Runge. Endomorphism rings of abelian surfaces and projective models of their moduli spaces. *Tôhoku Math. J.* **51**(1999), 283–303.

[Ser] J. P. Serre. *A Course in Arithmetic.* Springer-Verlag, 1973.

[St] H. Stevens. On Jacobsthal's $g(n)$-function. *Math. Ann.* **226**(1977), 95–97.

[V1] W. Veech. Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards. *Invent. math.* **97**(1989), 553–583.

[V2] W. Veech. The billiard in a regular polygon. *Geom. Funct. Anal.* **2**(1992), 341–379.

[Vo] Ya. B. Vorobets. Plane structures and billiards in rational polygons: the Veech alternative. *Russian Math. Surveys* **51**(1996), 779–817.

[Wa] C. C. Ward. Calculation of Fuchsian groups associated to billiards in a rational triangle. *Ergod. Th. & Dynam. Sys.* **18**(1998), 1019–1042.

Mathematics Department
Harvard University
1 Oxford St
Cambridge, MA 02138-2901