Polynomials defining Teichmüller curves and their factorizations mod p

Ronen E. Mukamel

August 18, 2017

Abstract

We investigate the arithmetic nature of Teichmüller curves in the spirit of the theory developed for classical modular curves. We focus on the Weierstrass curves for square discriminants introduced in [Mc1] which give arithmetic Teichmüller curves in genus two. For these curves, we introduce an analogue of the classical modular polynomials. These Weierstrass polynomials have integer coefficients and give defining equations for Weierstrass curves. We formulate, and provide evidence towards, several conjectures concerning the factorizations of Weierstrass polynomials in positive characteristic similar to the factorizations for modular polynomials discovered by Kronecker and Deuring.

Contents

1 Introduction

In this paper, we introduce the Weierstrass polynomials which give defining equations for certain arithmetic Teichmüller curves in genus two. The Weierstrass polynomials have integer coefficients, and allow us to investigate the arithmetic nature of Teichmüller curves in the spirit of the theory developed for classical modular curves.

Weierstrass polynomials. Let $\mathcal{M}_g$ denote the moduli space of genus g curves. Each integer $d \geq 3$ determines a *Weierstrass curve*

$$W(d) \subset \mathcal{M}_1 \times \mathcal{M}_1.$$

A pair of genus one curves (E_1, E_2) lies in $W(d)$ if there exists a genus two curve $Y \in \mathcal{M}_2$ and a primitive, degree d map

$$f\colon Y \to E_1$$

such that E_2 is the kernel of the map f induces on Jacobians, and f has a critical Weierstrass point. Primitive means that f does not factor through a map of lower degree.

Using the j-invariant $j\colon \mathcal{M}_1 \to \mathbb{C}$, we identify $\mathcal{M}_1 \times \mathcal{M}_1$ with $\mathbb{C}^2$ and realize $W(d)$ as a plane curve. The *Weierstrass polynomial* Ψ_d for degree d is the defining polynomial for $W(d)$.

Theorem 1.1. *There is a square-free polynomial $\Psi_d \in \mathbb{Z}[j_1, j_2]$, unique up to sign, whose zero locus is equal to $W(d)$ and whose coefficients are relatively prime.*

The irreducible components of $W(d)$ and irreducible factors of Ψ_d can be determined from [Mc1]. The number of components is one or two depending on the parity of d.

Theorem 1.2. *If $d > 3$ is even or $d = 3$, then Ψ_d is irreducible in $\mathbb{C}[j_1, j_2]$. If $d > 3$ is odd, Ψ_d has two factors $\Psi_{d,0}$ and $\Psi_{d,1}$ in $\mathbb{Z}[j_1, j_2]$ both of which are irreducible in $\mathbb{C}[j_1, j_2]$.*

The j-invariant is arithmetic in nature in the sense that it is compatible with automorphisms of $\mathbb{C}$ and reduction modulo p. The Weierstrass polynomials give a window to the Weierstrass curves in positive characteristic.

Modular polynomials. The Weierstrass curves and polynomials are analogues of the classical modular curves and the associated modular polynomials:

$$X_0(m) \subset \mathcal{M}_1 \times \mathcal{M}_1 \text{ and } \Phi_m \in \mathbb{Z}[j_1, j_2].$$

For $m \geq 1$, the curve $X_0(m)$ consists of pairs of genus one curves related by a degree m map with cyclic kernel, and Φ_m is the square-free polynomial with relatively prime coefficients whose zero locus is equal to $X_0(m)$.

The curve $X_0(m)$ and the polynomial Φ_m are both irreducible over $\mathbb{C}$.

Factorizations in positive characteristic. The modular polynomials Φ_m satisfy recursive congruence relations when reduced modulo primes p dividing m. Deuring [De] showed that, if $m = p^e n$ where p is a prime not dividing n, then the following congruence holds modulo p:

$$\Phi_m(j_1, j_2) \equiv \Phi_n(j_1^{p^e}, j_2) \cdot \Phi_n(j_1, j_2^{p^e}) \cdot \prod_{k=1}^{e-1} \Phi_n(j_1^{p^{e-k-1}}, j_2^{p^{k-1}})^{p-1}. \qquad (1.1)$$

Specializing to the case $m = p$, we obtain Kronecker's congruence relation

$$\Phi_p(j_1, j_2) \equiv (j_1^p - j_2)(j_1 - j_2^p) \bmod p.$$

These congruences were discovered in the 19^{th} century, and they hint at the rich and celebrated theory of integral models for modular curves developed in the 20^{th} century [DR, Ig, KM].

For small values of d, we find that Ψ_d exhibits surprising congruences with modular polynomials in resonance with the congruence relations of Kronecker and Deuring.

Theorem 1.3. *For $3 \leq d \leq 9$ and a prime $p \leq d$, the Weierstrass polynomial Ψ_d is divisible by the product of linear and modular polynomials listed in Table 1.*

The complicated factorizations of Weierstrass polynomials in positive characteristic are especially surprising since Ψ_d has at most two irreducible factors over $\mathbb{C}$. Note that the factors in Table 1 involving modular polynomials, like the terms appearing in Deuring's congruence relation, are of the form $\Phi_m(j_1^k, j_2^l)$ where k and l are powers of p.

For primes p not dividing m, it is known that Φ_m is irreducible over the finite field $\mathbb{F}_p$ with p elements, as well as over the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. As a complement to Theorem 1.3, we establish the following

Theorem 1.4. *For $3 \leq d \leq 9$ and a prime p with $d < p < 10^4$, each irreducible factor of Ψ_d is irreducible over $\mathbb{F}_p[j_1, j_2]$.*

Hilbert modular surfaces for square discriminants. The Weierstrass curve $W(d)$ is closely related to a curve W_D, introduced in [Mc1], in the Hilbert modular surface for discriminant $D = d^2$

$$X_{d^2} = \mathbb{H} \times \overline{\mathbb{H}} / \operatorname{SL}_2(\mathcal{O}_{d^2}).$$

d	$p=2$	$p=3$	$p=5$	$p=7$
3	$\Phi_1(j_1,j_2^2)$	j_2^3		
4	$j_2^7\,\Phi_1(j_1,j_2)^2$	$\Phi_1(j_1,j_2^3)^3$		
5	$\Phi_1(j_1,j_2)^2\,\Phi_1(j_1,j_2^4)^3\,\Phi_3(j_1,j_2^2)$	$\Phi_2(j_1,j_2^3)^3$	$j_2^{15}\,(j_2+2)^5$	
6	$j_2^{18}\,\Phi_1(j_1^2,j_2)^2\,\Phi_1(j_1,j_2^2)^8$	$j_2^{27}\,\Phi_1(j_1,j_2)^9$	$\Phi_1(j_1,j_2^5)^3$	
7	$\Phi_3(j_1,j_2)^2\,\Phi_3(j_1,j_2^2)$ $\Phi_3(j_1,j_2^4)^3\,\Phi_5(j_1,j_2^2)$	$\Phi_4(j_1,j_2^3)^3\,\Phi_1(j_1,j_2^3)^3$ $\Phi_2(j_1,j_2^3)^3$	$\Phi_2(j_1,j_2^5)^3$	$(j_2+1)^{42}\,(j_2+2)^{21}$
8	$j_2^{76}\,\Phi_1(j_1,j_2)^{16}\,\Phi_3(j_1,j_2)^4$	$\Phi_5(j_1,j_2^3)^3\,\Phi_1(j_1,j_2^3)^{18}$	$\Phi_3(j_1,j_2^5)^3$	$\Phi_1(j_1,j_2^7)^3$
9	$\Phi_1(j_1^2,j_2)^2\,\Phi_1(j_1,j_2^2)^{18}\,\Phi_1(j_1,j_2^8)^3$ $\Phi_5(j_1,j_2)^2\,\Phi_5(j_1,j_2^4)^3\,\Phi_7(j_1,j_2^2)$	$j_2^{135}\,\Phi_2(j_1,j_2)^{18}$	$\Phi_4(j_1,j_2^5)^3\,\Phi_1(j_1,j_2^5)^3$	$\Phi_2(j_1,j_2^7)^3$

Table 1: For each $3 \le d \le 9$ and prime $p \le d$, the listed product of linear and modular polynomials divides Ψ_d modulo p.

The surface X_D is isomorphic to the moduli space of principally polarized abelian surfaces with real multiplication by the quadratic ring $\mathcal{O}_D$ of discriminant D, and is birational to the moduli space of primitive, degree d covers from genus two to genus one with no restriction on the critical points. The curve W_D consists of points in X_D which correspond to covers with a critical Weierstrass point.

There is a map $X_D \to \mathcal{M}_1 \times \mathcal{M}_1$ sending a point corresponding to the cover $f\colon Y \to E$ to the pair (E, F) where F is the kernel of the map f induces on Jacobians. Under this map, W_D maps onto $W(d)$ and the curves $W(d)$ and W_D are related by the diagram

$$\begin{array}{ccccc} W_D & \hookrightarrow & X_D & \dashrightarrow & \mathcal{M}_2 \\ \downarrow & & \downarrow & & \\ W(d) & \hookrightarrow & \mathcal{M}_1 \times \mathcal{M}_1. & & \end{array}$$

The hooked arrows are inclusions, and the dashed arrow is the rational map sending a Jacobian with real multiplication to the corresponding genus two curve. The regular map $X_D \to \mathcal{M}_1 \times \mathcal{M}_1$ is a covering map and arises from the inclusion $\mathrm{SL}_2(\mathcal{O}_D) \subset \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$. We will show that W_D is birational onto its image in $\mathcal{M}_1 \times \mathcal{M}_1$.

Theorem 1.5. *The curve $W(d)$, defined by the equation $\Psi_d = 0$, is birational to W_{d^2}.*

To prove Theorems 1.3 and 1.4, we use the equations for Hilbert modular surfaces for square discriminants in [Ku] to explicitly compute Ψ_d.

Theorem 1.6. *For $3 \leq d \leq 9$, the Weierstrass polynomial Ψ_d is the polynomial listed in Table 2.*

Theorems 1.3 and 1.4 are obtained by direct computations using the polynomials in Table 2.

Relation to Teichmüller curves. The curves W_{d^2} are part of a larger family of Weierstrass curves W_D in Hilbert modular surfaces indexed by discriminants D for real quadratic orders. The curve W_D is important in Teichmüller theory because its irreducible components, of which there are one or two, are Teichmüller curves. That is, each irreducible component $W \subset W_D$ is uniformized by a lattice Veech group $\Gamma_W \leq \mathrm{SL}_2(\mathbb{R})$, and the algebraic immersion

$$W = \mathbb{H}/\Gamma_W \to \mathcal{M}_2$$

is a local isometry for the Teichmüller metric on $\mathcal{M}_2$.

In the case $D = d^2$, the Fuchsian groups which arise are finite index in $\mathrm{SL}_2(\mathbb{Z})$. The Veech groups uniformizing components of W_{d^2} play the role of the congruence groups $\Gamma_0(m) \leq \mathrm{SL}_2(\mathbb{Z})$ which uniformize modular curves.

When D is not a square, there is no obvious analogue of the map $X_{d^2} \to \mathcal{M}_1 \times \mathcal{M}_1$. It would be interesting to explore the arithmetic nature of these curves as well.

Degree of Ψ_d. For general $d \geq 3$, the bidegree of Ψ_d can be expressed simply in terms of the orbifold Euler characteristic $\chi(W_{d^2})$ of W_{d^2}.

Theorem 1.7. *For each $d \geq 3$, the bidegree of Ψ_d is given by*

$$\deg_{j_1}(\Psi_d) = 6|\chi(W_{d^2})| \text{ and } \deg_{j_2}(\Psi_d) = 2|\chi(W_{d^2})|.$$

A formula for $\chi(W_{d^2})$ appears in [EMS] (see also [Ba, LR]), allowing us to explicitly compute the bidegree of Ψ_d. A similar formula holds for the bidegree of each irreducible factor of Ψ_d (cf. Propposition 2.7).

For $m > 1$, the modular polynomial Φ_m is known to be symmetric in j_1 and j_2, i.e. $\Phi_m(j_1, j_2) = \Phi_m(j_2, j_1)$. Theorem 1.7 shows that Ψ_d is *not* symmetric.

Leading coefficients. The modular polynomial is known to be monic in both j_1 and j_2.

By analyzing the Weierstrass curve near infinity, we describe the leading coefficients of Ψ_d in each variable. For instance, we prove

Theorem 1.8. *For each $d \geq 3$, the leading j_2-coefficient of Ψ_d lies in $\mathbb{Z}$.*

In each of the cases we computed, the polynomial Ψ_d is actually monic in j_2 (cf. Table 2). It would be interesting to determine whether this is true for all d.

The leading j_1-coefficient of Ψ_d, by contrast, is typically a non-constant polynomial in $\mathbb{Z}[j_2]$. In fact, it is related to a polynomial in j_2 defined in terms of the one-cylinder cusps of W_{d^2} (cf. Proposition 2.4).

Conjectural factorization. In light of Theorems 1.3 and 1.4, we formulate several conjectures concerning the factorization of Weierstrass polynomials in positive characteristic.

Conjecture 1. *For primes $p < d$, the Weierstrass polynomial Ψ_d has a non-trivial common factor with a product of modular polynomials over $\mathbb{F}_p[j_1, j_2]$.*

Conjecture 2. *For primes p dividing d, the Weierstrass polynomial Ψ_d is divisible over $\mathbb{F}_p[j_1, j_2]$ by the p^{th} power of a linear polynomial in $\mathbb{F}_p[j_2]$.*

Conjecture 3. *For primes $p > d$, each irreducible factor of Ψ_d is irreducible over $\overline{\mathbb{F}}_p[j_1, j_2]$.*

Our theorems show that Conjectures 1 and 2 hold for $d \leq 9$, and Conjecture 3 holds for $d \leq 9$ and $p < 10^4$ when $\overline{\mathbb{F}}_p$ is replaced with $\mathbb{F}_p$.

Primes of good and bad reduction. The congruence relations of Kronecker and Deuring for modular polynomials are related to theorems about good and bad reduction for the modular curves $X_0(m)$. We expect similar results to hold for Weierstrass curves.

To formulate a precise statement, let $W \subset W_{d^2}$ be an irreducible component, $\Gamma_W \leq \mathrm{SL}_2(\mathbb{Z})$ the Veech group uniformizing W, and define, for $m \geq 1$,

$$W[m] = \mathbb{H}/\Gamma_W[m] \text{ where } \Gamma_W[m] = \ker(\Gamma_W \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})).$$

The points in $W[m]$ correspond to branched covers $f\colon Y \to E$ in W together with a marking of the full m-torsion of E. We similarly define $W_{d^2}[m]$. For $m > 1$, the group $\Gamma_W[m]$ contains no elliptic elements, and $W_{d^2}[m]$ is a smooth hyperbolic manifold and affine algebraic curve.

We set $\overline{W}_{d^2}[m]$ to be the smooth, projective curve birational to $W_{d^2}[m]$. The curve $\overline{W}_{d^2}[m]$ has a canonical algebraic model defined over the field $\mathbb{Q}[\zeta_m]$ where $\zeta_m = e^{2\pi i/m}$ coming from the moduli interpretation of its points.

For a prime $p \in \mathbb{Z}$, we say that $\overline{W}_{d^2}[m]$ has *good reduction* at p if there exists a projective curve over $\mathbb{Z}[\zeta_m]$ which is isomorphic to $\overline{W}_{d^2}[m]$ over $\mathbb{Q}[\zeta_m]$ and is smooth when reduced modulo every prime ideal in $\mathbb{Z}[\zeta_m]$ dividing p. Otherwise, we say that $\overline{W}_{d^2}[m]$ has *bad reduction* at p.

Conjecture 4. *Fix $m > 1$, $d \geq 3$, and a prime p not dividing m. If $p \leq d$, then $\overline{W}_{d^2}[m]$ has bad reduction p. Otherwise, $\overline{W}_{d^2}[m]$ has good reduction at p.*

An analogous statement is known to hold for modular curves, and lies at the heart of applications to the study representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It would be interesting to investigate the Galois representations arising from the cohomology of Weierstrass curves and Teichmüller curves more generally.

Outline. In Section 2 we discuss the relationship between $W_D \subset X_D$ and $W(d) \subset \mathcal{M}_1 \times \mathcal{M}_1$, and prove Theorems 1.1, 1.2, 1.5, 1.7 and 1.8. In Section 3, we explain how we use the equations in [Ku] to compute Ψ_d for $d \leq 9$, we prove Theorem 1.6, and we deduce Theorems 1.3 and 1.4. In the Appendix, we discuss the cusps of W_D and the behavior of the coordinate functions j_1, j_2 on $W(d)$ near infinity. The results in the Appendix are used in Section 2.

Computer files. The coefficients of the polynomials Ψ_d are very large, even for $d \leq 9$. It is unreasonable to include these polynomials in their entirety in this text. They can be accessed at

`http://math.rice.edu/~rm51/papers/wpolys.txt.gz`.

Acknowledgments. The author is grateful for helpful conversations with Curt McMullen, Sarah Koch, Alex Wright, Keerthi Madapusi Pera, John Voight, and Andrew Sutherland. The computations in this paper were performed in MAGMA [Mag]. The author is partially supported by National Science Foundation grant DMS-1708705.

Examples of Weierstrass polynomials

$$\Psi_3(j_1,j_2) = j_2^3 - 1296j_2^2 + 559872j_2 - (729j_1j_2 + 80621568)$$

$$\begin{aligned}\Psi_4(j_1,j_2) = j_2^9 &- 2\cdot 3^3(-1840+3j_1)j_2^8 + 3^3(154158336 - 250048j_1 + 243j_1^2)j_2^7\\ &- 2^5\cdot 3^1(-970047097344 + 603165992j_1 + 1218645j_1^2)j_2^6\\ &+ 2^8\cdot 3^3(165993941101824 + 27425238848j_1 + 120608619j_1^2)j_2^5\\ &- 2^8\cdot 3^2(-2960177618953248768 + 72262513013760j_1\\ &\qquad + 1300315270336j_1^2 + 729j_1^3)j_2^4\\ &+ 2^{14}\cdot 3^1(139656133843075058688 - 136049229047669760j_1\\ &\qquad + 1140164191204 84j_1^2 + 533871j_1^3)j_2^3\\ &- 2^{17}\cdot 3^3(19517832888381723377664 - 10277625115341083520j_1\\ &\qquad + 1415260745619344j_1^2 + 43441281j_1^3)j_2^2\\ &+ 2^{22}\cdot 3^2(22292897117875638192046 08 - 1326624212145450516480j_1\\ &\qquad + 43192230438475404j_1^2 + 10604499373j_1^3)j_2\\ &\qquad - 2^{24}(2^{17}\cdot 3^3\cdot 7^3 + 13^4j_1)^3\end{aligned}$$

$$\begin{aligned}\Psi_{5,0}(j_1,j_2) = j_2^{18} &+ 3^2(293j_1 - 198000)j_2^{17} - 3(19683j_1^3 - 43690536j_1^2\\ &+ 20557595500j_1 - 1041788250000)j_2^{16} + \cdots + 2^{60}5^{30}(j_1 - 16581375)^6\end{aligned}$$

$$\begin{aligned}\Psi_{5,1}(j_1,j_2) = j_2^9 &+ 3^4(3j_1 - 2128)j_2^8 + 2^4\cdot 3^1(40213j_1 + 212761620)j_2^7 + \ldots\\ &- (20511149j_1 + 10512288000)^3\end{aligned}$$

$$\Psi_6(j_1,j_2) = j_2^{36} - (1458j_1^2 - 2132208j_1 + 207665856)j_2^{35} + \ldots$$

$$\Psi_{7,0}(j_1,j_2) = j_2^{54} - 9(243j_1^3 - 548424j_1^2 + 268959980j_1 - 9899198880)j_2^{53} + \ldots$$

$$\Psi_{7,1}(j_1,j_2) = j_2^{36} + 9(243j_1^3 - 540360j_1^2 + 257007956j_1 - 8642256192)j_2^{35} + \ldots$$

$$\Psi_8(j_1,j_2) = j_2^{108} - 108(243j_1^3 - 536872j_1^2 + 251851400j_1 - 8107623648)j_2^{107} + \ldots$$

$$\begin{aligned}\Psi_{9,0}(j_1,j_2) = j_2^{108} &- 9(2187j_1^5 - 8158968j_1^4 + 10022408532j_1^3 - 4495723997525j_1^2\\ &+ 552680124631602j_1 - 4495116061000512)j_2^{107} + \ldots\end{aligned}$$

$$\begin{aligned}\Psi_{9,1}(j_1,j_2) = j_2^{81} + 9(&19683j_1^5 - 73010808j_1^4 + 88952462388j_1^3 - 39398534643069j_1^2\\ &+ 4738793514127794j_1 - 3689666638025 9328)j_2^{80} + \ldots\end{aligned}$$

Table 2: The Weierstrass polynomials Ψ_d for $3 \le d \le 9$. When $d > 3$ is odd, $\Psi_d = \Psi_{d,0}\cdot\Psi_{d,1}$. For a complete list of the coefficients of Ψ_d, see the the auxiliary computer files described in §1.

2 Weierstrass polynomials

In this section, we discuss the Weierstrass curve W_{d^2} as well as its map to $\mathcal{M}_1 \times \mathcal{M}_1$. We prove Theorems 1.1, 1.2, 1.5, 1.7 and 1.8.

Setup. Fix a degree $d \geq 3$, and set $D = d^2$. As in §1, the discriminant D determines a Hilbert modular surface X_D as well as a curve $W_D \subset X_D$. We also fix an irreducible component $W \subset W_D$.

Moduli interpretation. The space X_D is birational to the moduli space of primitive degree d maps from genus two to genus one. See [Mc2, §4], [Ka, §4]. Every map

$$f\colon Y \to E,$$

where $Y \in \mathcal{M}_2$, $E \in \mathcal{M}_1$, and f is primitive of degree d corresponds to a point in X_D. Two such maps $f_1\colon Y_1 \to E_1$ and $f_2\colon Y_2 \to E_2$ correspond to the same point in X_D if there are isomorphisms $Y_1 \to Y_2$ and $E_1 \to E_2$ intertwining f_1 and f_2.

A typical point in X_D corresponds to a map with two simple critical points P, P' interchanged by the hyperelliptic involution on Y. The curve $W_D \subset X_D$ consists of points corresponding to maps with a critical Weierstrass point.

Irreducible components of W_D. The irreducible components of W_D are determined in [Mc1]. When $d > 3$ is even or $d = 3$, W_D is irreducible and we have $W = W_D$.

When $d \geq 3$ is odd, W_D is the union of two curves

$$W_D = W_D^0 \cup W_D^1.$$

A point in W_D lies in W_D^ϵ if it corresponds to a cover $f\colon Y \to E$ where f has n Weierstrass points in its critical fiber and $\epsilon = (n-1)/2$. When $d > 3$ is odd, W_D^0 and W_D^1 are both non-empty and irreducible, and $W = W_D^0$ or W_D^1. When $d = 3$, $W_D = W_D^0$ is irreducible.

Maps to $\mathcal{M}_1$. There is an obvious map

$$\pi_1\colon W \to \mathcal{M}_1,$$

which sends the point corresponding to $f\colon Y \to E$ to the genus one curve E. The map π_1 presents W as an orbifold cover of $\mathcal{M}_1 \cong \mathbb{H}/\operatorname{SL}_2(\mathbb{Z})$. In particular, the degree of π_1 can be computed from the Euler characteristic of W:

$$\deg(\pi_1) = \frac{\chi(W)}{\chi(\mathcal{M}_1)} = 6|\chi(W)|. \tag{2.1}$$

A formula for $\chi(W)$ appears in [Ba] (see also [LR]), allowing us to explicitly compute $\deg(\pi_1)$.

There is a second, more mysterious, map $W \to \mathcal{M}_1$. The map f induces a map on Jacobians

$$f^{\mathrm{Jac}}\colon \mathrm{Jac}(Y) \to \mathrm{Jac}(E) \cong E. \tag{2.2}$$

The kernel of f^{Jac} is again a curve of genus one, and we define

$$\pi_2\colon W \to \mathcal{M}_1,\ \pi_2(f\colon Y \to E) = \ker(f^{\mathrm{Jac}}). \tag{2.3}$$

Let $\Omega(Y)$ be the space of holomorphic 1-forms on Y, and $V \subset \Omega(Y)^*$ the space of linear functions on $\Omega(Y)$ which vanish on $f^*(\Omega(E))$. The genus one curve $\pi_2(f)$ is uniformized by V and given by the following equation

$$F = \pi_2(f) = V/\ker(f_*). \tag{2.4}$$

Here, f_* is the map f induces on homology. The curve F is orthogonal to the image of E under the Rosati dual of f^{Jac}, and the pair (E, F) lies in $W(d)$.

The degree of π_2 is related to the degree of π_1 by the second Lyapunov exponent $\lambda_2 = 1/3$ for W:

$$\deg(\pi_2) = \lambda_2 \cdot \deg(\pi_1) = 2|\chi(W)|. \tag{2.5}$$

See [Ba, Cor. 12.3].

The j-invariant. The j-invariant gives a bijection $j\colon \mathcal{M}_1 \to \mathbb{C}$, identifying $\mathcal{M}_1$ with $\mathbb{C}$. The j-invariant is arithmetic in nature in the sense that it is equivariant with respect to automorphisms of $\mathbb{C}$ and compatible with reduction modulo p. Composing the maps π_i with j gives rise to a pair of rational functions

$$j_i\colon W \to \mathbb{C}, j_i = j \circ \pi_i. \tag{2.6}$$

We regard j_i as an element of the field $\mathbb{C}(W)$ of all rational functions on W. In fact, j_i lies in $\mathbb{C}[W]$, the subring of $\mathbb{C}(W)$ consisting functions which are holomorphic on W.

Combining the functions j_1 and j_2, we have an algebraic map

$$\phi\colon W \to \mathbb{C}^2_{(j_1,j_2)}.$$

From our definitions, it is immediate that $\phi(W) = W(d)$ when $W = W_D$ is irreducible.

When W_D is reducible, we define

$$\phi(W) = W^\epsilon(d) \text{ where } W = W_D^\epsilon.$$

The curve $W^\epsilon(d)$ is an irreducible component of $W(d)$, and we have that $W(d) = W^0(d) \cup W^1(d)$.

The Weierstrass polynomial. We now prove the following

Proposition 2.1. *There is a square-free polynomial $\Psi_W \in \mathbb{Z}[j_1, j_2]$, unique up to sign, whose zero locus is equal to $\phi(W)$ and whose coefficients are relatively prime. The polynomial Ψ_W is irreducible in $\mathbb{C}[j_1, j_2]$.*

Proof. By virtue of being a plane curve, $\phi(W)$ is defined by a single polynomial equation $\Psi_W = 0$ where $\Psi_W \in \mathbb{C}[j_1, j_2]$ is square-free. The polynomial Ψ_W is determined by $\phi(W)$ up to scale in $\mathbb{C}$.

Since the moduli problem associated to the points on W is defined over $\mathbb{Q}$, the curve W and its map to $\mathcal{M}_1 \times \mathcal{M}_1$ are defined over $\mathbb{Q}$. It follows that we can scale Ψ_W so its coefficient lie in $\mathbb{Q}$. Cf. [BM, Thm. 3.3].

By clearing denominators and dividing by common factors, we arrange that the coefficients of Ψ_W lie in $\mathbb{Z}$ and are relatively prime.

For the uniqueness statement, note that another square-free polynomial Ψ'_W whose zero locus is equal to $\phi(W)$ must be a scalar multiple of Ψ_W, i.e. $\Psi'_W = c \cdot \Psi_W$. If the coefficients of Ψ'_W are also integers, then c is also an integer. If the coefficients of Ψ'_W are relatively prime, then $c = \pm 1$.

Finally, the irreducibility of Ψ_W in $\mathbb{C}[j_1, j_2]$ follows from the irreducibility of $\phi(W)$, which is implied by the irreducibility of W. □

Cusps and poles. Now let $\overline{W}$ denote the smooth projective curve birational to W. The curve $\overline{W}$ is obtained by smoothing the orbifold points of W and adding in finitely many cusps $\partial\overline{W} = \overline{W} \setminus W$. The cusps of W are enumerated in [Mc1], and in the Appendix, we determine the polar order of j_i at each cusp $x \in \partial\overline{W}$, i.e.

$$v_i(x) = \mathrm{ord}(x, (j_i)_\infty),$$

where $(j_i)_\infty$ is the polar divisor of j_i on $\overline{W}$.

The poles of j_1 coincide with the cusps of $\overline{W}$, and $v_1(x) > 0$ for $x \in \partial\overline{W}$. Geometrically, this is implied by the fact that π_1 is a covering map, hence topologically proper. Algebraically, this implies that the ring $\mathbb{C}[W]$ is in the integral closure of $\mathbb{C}[j_1]$. To see this, fix $u \in \mathbb{C}(W)$ and consider the minimal polynomial for u over $\mathbb{C}(j_1)$,

$$m_u(x) = x^e + a_{e-1}(j_1)x^{e-1} + \cdots + a_0(j_1) \in \mathbb{C}(j_1)[x].$$

The value of a_k at $j_1 = t$ is, up to sign, the k^{th} symmetric function of $\{u(x) : x \in W_D, j_1(x) = t\}$. If u is holomorphic on W, then the poles of u are contained in the poles of j_1, and a_k lies in $\mathbb{C}[j_1]$.

Proposition 2.2. *The rational function $j_2 \in \mathbb{C}(W)$ is integral over $\mathbb{C}[j_1]$.*

Proof. The function j_2 is holomorphic on W, so the coefficients of the minimal polynomial over $\mathbb{C}(j_1)$ have finite values whenever j_1 is finite, and are polynomials in $\mathbb{C}[j_1]$. □

Corollary 2.3. *The leading j_2-coefficient of Ψ_W lies in $\mathbb{Z}$.*

Proof. Let $m(j_1, j_2) \in \mathbb{C}(j_1)[j_2]$ be the minimal polynomial for $j_2 \in \mathbb{C}(W)$ over $\mathbb{C}(j_1)$. The polynomial Ψ_W is obtained from m by clearing denominators. Since j_2 is integral over $\mathbb{C}[j_1]$, the monic polynomial m has coefficients in $\mathbb{C}[j_1]$. Hence, Ψ_W has leading j_2-coefficient which is a constant polynomial in $\mathbb{Z}[j_1]$. □

The cusps of W correspond to cylinder decompositions of genus two surfaces, and are classified according to the number (one or two) of cylinders. The function j_2 is holomorphic at the one-cylinder cusps, and has poles at the two-cylinder cusps (cf. Propositions A.4 and A.5). We define

$$c_W(t) = \prod_x (t - j_2(x)) \in \mathbb{C}[t], \tag{2.7}$$

where the product ranges over the one-cylinder cusps $x \in \partial\overline{W}$. Arguing as above, we find that the coefficients of the minimal polynomial for j_1 over $\mathbb{C}(j_2)$ have poles only at the zeros of $c_W(t)$ and we conclude

Proposition 2.4. *The function $j_1 \in \mathbb{C}(W)$ is in the integral over $\mathbb{C}[j_2, c_W(j_2)^{-1}]$.*

Birational model. We now show that W is birational onto its image in $\mathcal{M}_1 \times \mathcal{M}_1$.

Proposition 2.5. *The curve $\Psi_W = 0$ is birational to W.*

Proof. The curve $\Psi_W = 0$ defines the image of W in the (j_1, j_2)-plane under the map

$$\phi\colon W \to \mathbb{C}^2_{(j_1,j_2)}.$$

The map ϕ extends to a map $\overline{W} \to \mathbb{P}^1 \times \mathbb{P}^1$, and the branches of $\overline{W}$ passing through $(j_1, j_2) = (\infty, \infty)$ correspond to the two-cylinder cusps of W.

To check that W is birational to $\Psi_W = 0$, we show that one of the branches of $\overline{W}$ through (∞, ∞) is simple. This amounts to exhibiting a two-cylinder cusp x such that

$$\gcd(v_1(x), v_2(x)) = 1, \text{ and } (v_1(x'), v_2(x')) \neq (v_1(x), v_2(x)) \text{ for } x' \neq x.$$

The first condition ensures that ϕ is 1-to-1 near x, and the second ensures the image of ϕ near x is distinct from the other branches of $\overline{W}$. For d odd, a cusp with these properties is furnished by Proposition A.7. For d even, we use Proposition A.8. □

We record the following corollaries of Theorem 1.5.

Theorem 2.6. *The functions j_1 and j_2 generate $\mathbb{C}(W)$ over $\mathbb{C}$, i.e.*

$$\mathbb{C}(W) = \mathbb{C}(j_1, j_2).$$

Proof. The subfield $\mathbb{C}(j_1, j_2) \subset \mathbb{C}(W)$ corresponds to the function field of the image of $\phi(W)$. By Proposition 2.5, $\phi(W)$ (which is defined by $\Psi_W = 0$) is birational to W. Hence $\mathbb{C}(j_1, j_2) = \mathbb{C}(W)$. □

Proposition 2.7. *The bidegree of Ψ_W is given by*

$$\deg_{j_2}(\Psi_W) = 6|\chi(W)|, \text{ and } \deg_{j_1}(\Psi_W) = 2|\chi(W)|.$$

Proof. The degree $\deg_{j_1}(\Psi_W)$ is equal to the degree of the field extension $\mathbb{C}(j_1, j_2)/\mathbb{C}(j_2)$. By Theorem 2.6, we have $\mathbb{C}(W) = \mathbb{C}(j_1, j_2)$ and $[\mathbb{C}(j_1, j_2) : \mathbb{C}(j_2)] = \deg(\pi_2)$. The desired formula for $\deg_{j_1}(\Psi_W)$ follows from (2.5). A similar argument using (2.1) gives $\deg_{j_2}(\Psi_W)$. □

Now define

$$\Psi_{d,\epsilon} = \Psi_W \text{ where } W = W^{\epsilon}_{d^2}.$$

Corollary 2.8. *For $d > 3$ odd, the polynomials $\Psi_{d,0}$ and $\Psi_{d,1}$ distinct.*

Proof. By the formula for $\chi(W^{\epsilon}_D)$ in [Ba, Thm. 1.4], we see that

$$\frac{\chi(W^0_D)}{\chi(W^1_D)} = \frac{d-1}{d-3}. \tag{2.8}$$

By Theorem 2.7, the polynomials $\Psi_{d,0}$ and $\Psi_{d,1}$ are distinguished by their degrees. □

We are now ready to give proofs of most of the theorems stated in the introduction.

Proof of Theorem 1.1. First suppose $W = W_D$ is irreducible. In this case, we can take $\Psi_d = \Psi_W$ and Proposition 2.1 ensures Ψ_d has the desired properties.

Now suppose W_D is reducible. In this case, we set

$$\Psi_d = \Psi_{d,0} \cdot \Psi_{d,1}.$$

Since $\Psi_{d,\epsilon}$ is irreducible over $\mathbb{C}$ by Proposition 2.1, and $\Psi_{d,0} \neq \Psi_{d,1}$ by Corollary 2.8, the polynomial Ψ_d is square free. Also, Ψ_d has integer coefficients which are relatively prime, and its zero locus is equal to $W(d)$ by Proposition 2.1.

The uniqueness statement follows from an argument similar to the one for Ψ_W in the proof of Proposition 2.1. □

Proof of Theorem 1.2. For $d > 3$ even or $d = 3$, we have that $\Psi_d = \Psi_W$ where $W = W_D$. This polynomial is irreducible by Proposition 2.1.

For $d > 3$ odd, we have that $\Psi_d = \Psi_{d,0} \cdot \Psi_{d,1}$ as in the proof of Theorem 1.1. The polynomials $\Psi_{d,\epsilon}$ have integer coefficients and are irreducible over $\mathbb{C}$ by Proposition 2.1. □

Proof of Theorem 1.5. For irreducible W_D, the curve $W(d)$ is birational to W_{d^2} by Proposition 2.5.

For reducible W_D, Proposition 2.5 ensures that W_D^ϵ is birational to its image $W^\epsilon(d)$ in $\mathcal{M}_1 \times \mathcal{M}_1$. Proposition 2.8 guarantees that $W^0(d)$ is distinct from $W^1(d)$, hence W_D is also birational to $W(d)$. □

Proof of Theorem 1.7. The formula for the bidegree of Ψ_d follows immediately from Proposition 2.7 and Corollary 2.8. □

Proof of Theorem 1.8. When W_D is irreducible, $\Psi_d = \Psi_W$. When W_D is reducible, Ψ_d is the least common multiple of $\Psi_{d,0}$ and $\Psi_{d,1}$. In either case, Corollary 2.3 immediately implies that the leading j_2-coefficient of Ψ_d is a constant polynomial. □

3 Computing Weierstrass polynomials

In this section, we explain how to compute Ψ_d using the equations for Hilbert modular surfaces in [Ku]. We also prove Theorems 1.6 and deduce Theorems 1.3 and 1.4.

Equations for Hilbert modular surfaces. We start with the equations for Hilbert modular surfaces for square discriminants computed in [Ku] using the method in [EK]. The paper [EK] describes a method for computing explicit, birational algebraic models for Hilbert modular surfaces. This method is implemented in [Ku] for square discriminants to give algebraic models for X_{d^2} along with its universal curve $Y \to X_{d^2}$ for $2 \leq d \leq 11$. The result is an explicit equation

$$Y : y^2 = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,\ a_i \in \mathbb{C}(X_{d^2}).$$

Equations for elliptic curves $E \to X_{d^2}$ and $F \to X_{d^2}$ along with primitive, algebraic maps $Y \to E$, $Y \to F$ of degree d are also computed.

Equations for Weierstrass curves. The equation for Y is normalized (using the algorithm in [KM]) so that the 1-forms dx/y and xdx/y are pulled back from the holomorphic 1-forms on F, E. In particular, the critical points of $Y \to E$ are the points with zero x-coordinate. The locus where $Y \to E$

has a critical Weierstrass point, i.e. W_{d^2}, is defined by the equation $a_0 = 0$. This equation gives an algebraic model for $W_{d^2} \subset X_{d^2}$.

The field of algebraic functions on an irreducible component $W \subset W_{d^2}$ is presented as an algebraic extension $\mathbb{C}(t,s)$ of the field $\mathbb{C}(t)$ of rational functions. In fact, since the equations furnished by [Ku] are defined over $\mathbb{Q}$, we can work in a finite extension $\mathbb{Q}(s,t)$ over $\mathbb{Q}(t)$ where exact arithmetic is possible. The equations for $E, F \to X_{d^2}$ allow us to compute $j_1 = j(E)$ and $j_2 = j(F)$ as explicit elements in $\mathbb{Q}(t,s)$.

Computing Ψ_W. To compute Ψ_W, we compute polynomials $u_{k,l}(s,t) \in \mathbb{C}[s,t]$ and $v(t) \in \mathbb{C}[t]$ which satisfy

$$j_1^k j_2^l = \frac{u_{k,l}(s,t)}{v(t)},$$

for each $k \leq \deg_{j_1}(\Psi_W)$ and $l \leq \deg_{j_2}(\Psi_W)$ (cf. Proposition 2.7). We then determine the linear relation among $j_1^k j_2^l$ by computing the kernel of the matrix whose entries are the coefficients of $u_{k,l}$. Scaling appropriately, we find an explicit formula for Ψ_W.

Note that the computation of $j_1^k j_2^l$ requires only arithmetic in a finite extension of the field $\mathbb{Q}(t)$, which can be done using exact integer calculations.

Remark. In most of the examples we computed, each component of W_{d^2} is of genus 0 and we can work exclusively over $\mathbb{Q}(t)$ after parametrizing W. To compute Ψ_8 and $\Psi_{9,0}$, associated to the curve W_{64} of genus one and the curve $W_{81,0}$ of genus two, we work in a degree two extension of $\mathbb{Q}(t)$. To speed up the computation, where possible we replace j_i with the associated Weber function, i.e. a solution to

$$j_i = \frac{(f_i^{24} - 16)^3}{f_i^{24}}.$$

We compute the polynomial relation satisfied by the f_1 and f_2 as above, and then use resultants to compute Ψ_d. This simplification is typical in the computation of the classical modular polynomials, see e.g. [Su].

Factors of Ψ_d. When $d > 3$ is odd, the two irreducible factors can be distinguished by their degrees (cf. proof of Corollary 2.8). We use this fact to determine the invariant ϵ attached to each irreducible component of Ψ_d.

Proof of Theorem 1.6. The polynomials listed in Table 2 were computed using the method outlined above. This method involves only exact arithmetic over number fields, and is guaranteed to yield the Weierstrass polynomial. □

Proof of Theorems 1.3 and 1.4. We verified the congruences of Table 1 and the irreducibility of Ψ_d in $\mathbb{F}_p[j_1, j_2]$ for $d < p < 10^4$ using the polynomials in Table 2 and direct computation. □

Hyperelliptic models for Weierstrass curves. The examples we computed include a complete list of Weierstrass polynomials associated to components of W_{d^2} of genus zero, cf. [Mu]. The components of positive genus included in our list are W_{64} and W_{81}^0 of genus 1 and 2 respectively. Since algebraic models for these curves have not appeared in the literature, we record defining equations for these curves here.

Theorem 3.1. *The Weierstrass curve W_{64} is birational to the elliptic curve*

$$y^2 = x^3 - 63x + 162.$$

Theorem 3.2. *The Weierstrass curve W_{81}^0 is birational to the hyperelliptic curve*

$$y^2 = 25x^6 - 60x^5 + 186x^4 - 260x^3 + 429x^2 - 240x + 64.$$

A Cusps

The smooth, projective curve $\overline{W}_{d^2}$ birational to W_{d^2} is obtained by smoothing out the orbifold points of W_{d^2} and adding finitely many cusps. The cusps of W_{d^2} are enumerated and sorted by component in [Mc1]. Since j_i is holomorphic on W_{d^2}, the polar divisor of j_i is supported at the cusps. In this appendix, we compute the order of pole of j_1 and j_2 at each cusp $x \in \overline{W}_{d^2}$, i.e.

$$v_1(x) = \mathrm{ord}(x, (j_1)_\infty) \text{ and } v_2(x) = \mathrm{ord}(x, (j_2)_\infty) \tag{A.1}$$

where $(j_i)_\infty$ is the polar divisor of j_i.‘

Setup. Fix a cusp $x \in \overline{W}_{d^2}$ and a map

$$f\colon Y \to E$$

with critical Weierstrass point corresponding to a point near x in W_{d^2}. We also choose a small loop γ about x beginning and ending at the point corresponding to f. As usual, we set $F = \ker(f^{\mathrm{Jac}})$.

Monodromy. The loop γ determines mapping classes T^Y, T^E, and T^F on Y, E, and $F = \pi_2(f)$. From the Veech dichotomy, we know that each of the transformations T^Y and T^E is a product of Dehn twists about a collection

of disjoint simple closed curves. The transformation T^F is either trivial, unipotent, or elliptic.

The induced transformation $T^E_*\colon H_1(E,\mathbb{Z}) \to H_1(E,\mathbb{Z})$ is unipotent stabilizing a primitive vector $w \in H_1(E,\mathbb{Z})$, and we define

$$m(T^E) = [U : \langle T^E_* \rangle]$$

where U is the entire stabilizer of w in $\mathrm{SL}(H_1(E,\mathbb{Z}))$. The quantity $m(T^E)$ measures the winding number of $(\pi_1)_*(\gamma)$ about the cusp of the modular curve $\mathcal{M}_1$, and is equal to the order of pole of j_1 at x. We similarly define $m(T^F)$ and conclude

$$v_1(x) = m(T^E) \text{ and } v_2(x) = m(T^F).$$

When T^F is trivial or elliptic, we define $m(T^F) = 0$ so the formula above continues to hold.

Homology. Now consider the map $f_*\colon H_1(Y,\mathbb{Z}) \to H_1(E,\mathbb{Z})$ that f induces on homology. We now identify $H_1(E,\mathbb{Z})$ and $H_1(F,\mathbb{Z})$ with explicit subspaces of $H_1(Y,\mathbb{Z})$ so that we can compute $m(T^E)$ and $m(T^F)$. We define

$$K_2 = \ker(f_*), \text{ and } K_1 = K_2^{\perp},$$

where the orthogonal complement is taken with respect to the symplectic intersection form on $H_1(Y,\mathbb{Z})$.

Proposition A.1. *The homology group $H_1(F,\mathbb{Z})$ is equal to $K_2 = \ker(f_*)$.*

Proof. This follows from the formula (2.4) for $F = \pi_2(f)$. □

Proposition A.2. *There is an integer e so that the map*

$$f_*\colon K_1 \to H_1(E,\mathbb{Z})$$

is an isomorphism onto the e-divisible in $H_1(E,\mathbb{Z})$.

In particular, the map

$$g\colon K_1 \to H_1(E,\mathbb{Z}),\ g(v) = (1/e)f_*(v)$$

is a natural isomorphism.

Proof. We use the theory of gluing for lattices, cf. [Mc3, §2]. The intersection form on $H_1(Y,\mathbb{Z})$ restricted to $K_i \cong \mathbb{Z}^2$ is e_i times the unimodular form.

The extension $H_1(Y,\mathbb{Z}) \supset K_1 \oplus K_2$ is primitive in the sense that $H_1(Y,\mathbb{Z})/K_i$ is torsion free. Hence, $H_1(Y,\mathbb{Z})$ corresponds to a gluing isomorphism $\phi\colon H_1 \to H_2$ where H_i is a subgroup of the glue group $G(K_i) = (1/e_iK_i)/K_i$. Since

$H_1(Y,\mathbb{Z})$ is unimodular and $K_1 \oplus K_2$ has index $(e_1e_2)^2$ in its dual, $|H_1| = |H_2| = e_1e_2$. From $|G(K_i)| = e_i^2$ we conclude that $e = e_1 = e_2$, and $H_i = G(K_i)$.

The lattice $H_1(Y,\mathbb{Z}) \subset (K_1 \oplus K_2) \otimes \mathbb{Q}$ is generated by $K_1 \oplus K_2$ together with representatives of the graph of ϕ in $(1/e)(K_1 \oplus K_2)$. Since f is primitive, f_* is onto, and

$$H_1(E,\mathbb{Z}) \cong H_1(Y,\mathbb{Z})/K_2 \cong (1/e)K_1.$$

So the map f_* restricted to K_1 is a bijection onto the e-divisible vectors in $H_1(E,\mathbb{Z})$. □

Proposition A.3. *The restriction of the symplectic intersection form to K_i is $d = \deg(f)$ times the unimodular symplectic form.*

Proof. We continue with the notation in the proof of Proposition A.2. Our goal is to prove $e = e_i = d$.

The lattice $H_1(Y,\mathbb{Z})$ is generated by K_1 and K_2 together with vectors representing the graph of the gluing homomorphism ϕ. The map ϕ negates the fractional form on $G(K_i)$, so we can choose positive bases a_i, b_i for K_i (i.e. $\langle a_i, b_i\rangle = e$) so that

$$\phi(a_1/e + K_1) = a_2/e + K_2, \text{ and } \phi(b_1/e + K_1) = -b_2/e + K_2.$$

A direct computation then shows that

$$A_1 = a_1, B_1 = 1/e(b_1 - b_2), A_2 = 1/e(a_1 + a_2), B_2 = b_2.$$

forms a standard symplectic basis for $H_1(Y,\mathbb{Z})$.

Note that $f_*(A_1) = ef_*(A_2)$ and $f_*(B_2) = 0$. Since f_* is onto, $H_1(E,\mathbb{Z})$ is generated by $f_*(A_2)$ and $f_*(B_1)$, hence $\langle f_*(A_2), f_*(B_1)\rangle_E = 1$. To see that $d = e$, we compute

$$d = \deg(f) = \langle f_*(A_1), f_*(B_1)\rangle_E + \langle f_*(A_2), f_*(B_2)\rangle_E = e.$$

□

Square-tiled surfaces. The cusps of W_{d^2} are enumerated in [Mc1] via square-tiled surfaces.

A square tiled surface is a surface built out of a finite collection of polygons $P_1, \ldots, P_n \subset \mathbb{C}$ with vertices in $\mathbb{Z}[i]$. The polygons are glued together along their edges by translations of the form $z \to z + c$ with $c \in \mathbb{Z}[i]$, and the result is a compact Riemann surface Y with a map $Y \to E = \mathbb{C}/\mathbb{Z}[i]$. If we deform the lattice $\mathbb{Z}[i]$ uniformizing E to $\Lambda_t = \mathbb{Z} + t\mathbb{Z}$ with $t \in \mathbb{H}$, and simultaneously deform the polygons P_i, we obtain a family of covers $f_t \colon Y_t \to E_t = \mathbb{C}/\Lambda_t$.

As t ranges in $\mathbb{H}$, the associated surfaces Y_t sweep out a Teichmüller curve C in $\mathcal{M}_g$. If $Y = Y_i$ is genus two, and $f = f_i$ is primitive of degree d with a critical Weierstrass point, we obtain a component of the Weierstrass curve W_{d^2}. In the limit as the imaginary part of t tends to ∞, we arrive at a cusp of C.

In [Mc1] an explicit collection of square-tiled surfaces is given which is in bijection with the cusps of W_{d^2}. The cusps are broadly classified according to the number of horizontal cylinders (one or two) on the associated square-tiled surface.

One-cylinder cusps. We start with the one-cylinder cusps. These are in bijection with the one-cylinder prototypes, i.e. cyclically order triples of integers $\langle a, b, c\rangle$ satisfying

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

In Figure 1, we depict a square-tiled surface obtained from a $(d \times 1)$-rectangle and associated to the prototype $\langle a, b, c\rangle$. The resulting branched cover $f\colon Y \to E = \mathbb{C}/\mathbb{Z}[i]$ is primitive of degree d with a critical Weierstrass point. In particular, we have $f \in W_{d^2}$ and an associated cusp of W_{d^2}.

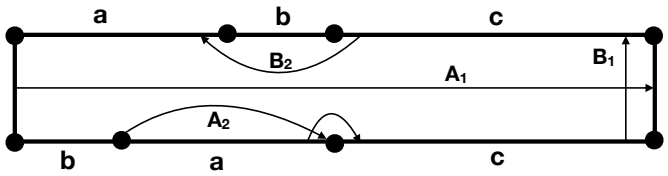

Figure 1: The one-cylinder prototype $\langle a, b, c\rangle$ determines a square-tiled surface and a cusp of W_{d^2}.

Proposition A.4. *Suppose $d > 3$ and $x \in \overline{W}_{d^2}$ is a one-cylinder cusp. The orders of the poles of j_i at x are*

$$v_1(x) = d \text{ and } v_2(x) = 0.$$

In particular, the function j_2 is holomorphic at x.

Proof. Let $\langle a, b, c\rangle$ be the associated one-cylinder prototype for x, $f_i\colon Y_i \to E_i = \mathbb{C}/\mathbb{Z}[i]$ the corresponding square-tiled surface as in Figure 1, and f_t for $t \in \mathbb{H}$ the associated point in W_{d^2} obtained by deforming f_i. Fixing some large $y > 0$, the collection

$$\gamma = \{f_t : t \in iy + [0, d]\} \subset W_{d^2}$$

is a small loop about about x. The transformation T^Y is a Dehn twist about A_1.

To compute $v_2 = m(T^F)$, we identify $H_1(F, \mathbb{Z})$ with the kernel of $f_*\colon H_1(Y, \mathbb{Z}) \to H_1(E, \mathbb{Z})$, and T^F_* with the restriction of T^Y_* to $\ker(f_*)$. The kernel of f_* is generated (rationally) by the vectors

$$w = bA_2 + aB_2 \text{ and } u = dA_2 - aA_1,$$

both of which are fixed by T^Y_*. Hence, T^F_* acts by the identity on $H_1(F, \mathbb{Z})$, $m(T^F) = 0$, and j_2 is holomorphic at x.

We compute $v_1 = m(T^E)$ by identifying $H_1(E, \mathbb{Z})$ with the orthogonal complement of $\ker(f_*)$ in $H_1(Y, \mathbb{Z})$. This space is generated by

$$w = A_1 \text{ and } u = dB_1 - bA_2 - aB_2,$$

and we see that $m(T^E) = d$ since $T^E_*(w) - w = du$. □

Remark. The function j_1 has a simple pole, rather than a pole of order 3, at the unique one-cylinder cusp $x \in \overline{W}_9$ corresponding to the prototype $\langle 1, 1, 1\rangle$. For this cusp, a small loop about x is represented by f_t as t ranges in the horizontal line $yi + [0, 1]$, rather than in $yi + [0, 3]$, reflecting the $\mathbb{Z}/3\mathbb{Z}$-symmetry of the prototype. The transformation T^F is elliptic of order 3.

Two-cylinder cusps. We now turn to the two-cylinder cusps of W_{d^2}. These are in bijection with splitting prototypes, i.e. quadruples of non-negative integers (a, b, c, e) satisfying

$$\begin{array}{lll} d^2 = e^2 + 4bc, & 0 \le a < \gcd(b, c), & e + c < b, \\ 0 < b, & 0 < c, \text{ and} & \gcd(a, b, c, e) = 1. \end{array} \tag{A.3}$$

The quantities

$$\lambda = \frac{d + e}{2} \text{ and } \lambda' = \frac{d - e}{2}$$

will play an important role.

In Figure 2, we depict a square-tiled surface Y built out of a square with side length λ and a parallelogram with sides of complex length b and $a + ic$. Note that map $Y \to E = \mathbb{C}/\mathbb{Z}[i]$ is not, in general, primitive. It factors through a unique primitive map of degree d with a critical Weierstrass point, and determines a cusp of W_{d^2} as above.

The mapping class T^Y is given by the formula

$$T^Y = D_1^{b'} \circ D_2^{c'} \text{ where } b' = b/\gcd(b, c), c' = c/\gcd(b, c), \tag{A.4}$$

and D_i is a Dehn twist about the curve A_i.

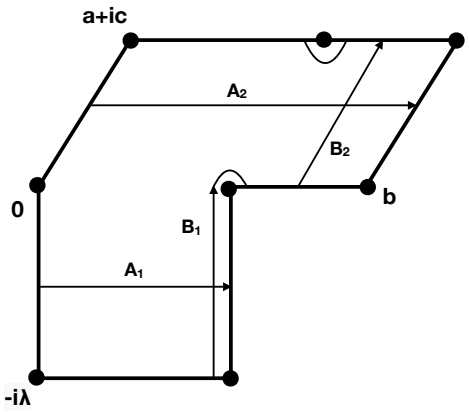

Figure 2: The two-cylinder prototype (a, b, c, e) determines a cusp of W_{d^2}.

Proposition A.5. *The cusp $x \in \overline{W}_{d^2}$ corresponding to the two-cylinder splitting prototype (a, b, c, e) has*

$$v_1(x) = \frac{\gcd(b, \lambda')\gcd(c, \lambda)}{\gcd(b, c)},\ v_2(x) = \frac{\gcd(b, \lambda)\gcd(c, \lambda')}{\gcd(b, c)}, \tag{A.5}$$

where $\lambda = (d + e)/2$ and $\lambda' = (d - e)/2$.

Proof. We proceed as in the proof of Proposition A.4. For $f\colon Y \to E$ and $F = \pi_2(f) = \ker(f^{\mathrm{Jac}})$ near x, the monodromy around a small loop about x determines mapping classes T^Y, T^E, and T^F on Y, E, and F respectively.

We start by computing $v_2 = m(T^F)$. The transformation T^F_* on $H_1(F, \mathbb{Z}) = \ker(f_*)$ stabilizes the primitive vector

$$w = (bA_1 - \lambda A_2)/\gcd(b, \lambda).$$

By Proposition A.3, the polarization on $\ker(f_*)$ is d times the principal polarization. The group $H_1(F, \mathbb{Z})$ is generated by w and a vector u where $\langle w, u\rangle = d$ and $f_*(u) = 0$. These conditions determine u up to adding a rational multiple of w, we have

$$u = (a\gcd(b, \lambda)/b)A_2 - \gcd(b, \lambda)B_2 + (c\gcd(b, \lambda)/\lambda)B_1 + tw$$

for some $t \in \mathbb{Q}$. Using (A.4), we compute that $(T^F_*(u) - u) = v_2 w$ where v_2 is given by the formula (A.5).

A similar analysis on $H_1(E, \mathbb{Z})$, which we identify with the orthogonal complement of $\ker(f_*)$, yields the formula above for v_1. □

Proposition A.6. *For $x \in \overline{W}_{d^2}$ the cusp corresponding to the two cylinder prototype (a, b, c, e), we have that*

$$v_1(x)v_2(x) \leq \frac{d^2 - e^2}{4}.$$

Equality holds if and only if $\gcd(b, c)$ *divides* $\gcd(\lambda, \lambda')$.

Note that the right hand side of the inequality above satisfies

$$bc = \frac{d^2 - e^2}{4} = \lambda\lambda'. \tag{A.6}$$

Proof. We will show that $m = v_1(x)v_2(x)$ divides $bc = (d^2 - e^2)/4$. For a prime p and integer n, let $v_p(n)$ denote the largest exponent e such that p^e divides n. From (A.5) we have

$$\begin{aligned} v_p(m) = \min(v_p(b), v_p(\lambda)) + \min(v_p(c), v_p(\lambda'))+ \\ \min(v_p(c), v_p(\lambda)) + \min(v_p(b), v_p(\lambda')) - 2\min(v_p(b), v_p(c)). \end{aligned} \tag{A.7}$$

Note that this equation is symmetric in (b, c) and in (λ, λ'), so we may assume $v_p(b) \leq v_p(c)$ and $v_p(\lambda) \leq v_p(\lambda')$. The equality $bc = \lambda\lambda'$ implies

$$v_p(b) + v_p(c) = v_p(\lambda) + v_p(\lambda').$$

If $v_p(b) \leq v_p(\lambda)$, we have $v_p(\lambda') \leq v_p(c)$ and

$$v_p(m) = v_p(\lambda') + v_p(\lambda) = v_p(bc).$$

If $v_p(b) > v_p(\lambda)$, we have $v_p(\lambda') > v_p(c)$ and

$$v_p(m) = 2v_p(\lambda) + v_p(c) - v_p(b) < v_p(\lambda) + v_p(\lambda') = v_p(bc).$$

We conclude that $v_p(m) \leq v_p(bc)$ for each prime p, and m divides $bc = (d^2 - e^2)/4$.

We have equality $m = bc$ if and only if $v_p(m) = v_p(bc)$ for all primes p. In the argument above, this occurs exactly when all the primes are of the first type. The condition that $m = bc$ is

$$\min(v_p(b), v_p(c)) \leq \min(v_p(\lambda), v_p(\lambda')) \text{ for all } p,$$

i.e. $\gcd(b, c)$ divides $\gcd(\lambda, \lambda')$. □

Proposition A.7. *Suppose $d \geq 3$ is odd. There is a unique two-cylinder cusp $x \in \overline{W}^0_{d^2}$ with*

$$v_1(x) = (d + 1)/2, v_2(x) = (d - 1)/2.$$

If $d > 3$, there is a unique two-cylinder cusp $x \in \overline{W}^1_{d^2}$ with

$$v_1(x) = (d - 1)/2, v_2(x) = (d + 1)/2.$$

Proof. Suppose (a, b, c, e) corresponds to a cusp with $v_1 = (d+1)/2$ and $v_2 = (d-1)/2$. Since $v_1 v_2 = (d^2-1)/4 \leq (d^2-e^2)/4$, we must have $e = 1$ or -1. From $\lambda - \lambda' = e$, we have that $\gcd(\lambda, \lambda') = 1$ and, by Proposition A.6, the equality $v_1 v_2 = (d^2 - e^2)/4$ implies that $\gcd(b, c) = 1$.

Assume $e = 1$. From (A.5) and $v_1 = \lambda$, we have $\gcd(b, \lambda') = 1$. From $v_2 = \lambda'$, we have $\gcd(b, \lambda) = 1$. Since b divides $bc = \lambda\lambda'$, $b = 1$, $c = (d^2-1)/4$, which is impossible since $e + c < b$. If $e = -1$, we similarly conclude that $c = 1$, $b = (d^2-1)/4$. The conditions on v_1, v_2 determine a unique prototype $(0, (d^2-1)/4, 1, -1)$. This is a valid prototype with invariant $\epsilon = 0$ (cf. [Mc1, Thm. 5.3]).

A similar argument shows that, if $v_1 = (d-1)/2$, $v_2 = (d+1)/2$, the prototype is $(0, (d^2-1)/4, 1, 1)$, which is a valid prototype provided $d > 3$. This prototype has invariant $\epsilon = 1$. □

Proposition A.8. *If $d \equiv 0 \bmod 4$, there is a unique two-cylinder cusp $x \in \overline{W}_{d^2}$ with*

$$v_1(x) = (d^2-4)/4, v_2(x) = 1.$$

If $d \equiv 2 \bmod 4$, there is a unique two-cylinder cusp $x \in \overline{W}_{d^2}$ with

$$v_1(x) = (d^2-16)/4, v_2(x) = 1.$$

Proof. Suppose $d \equiv 0 \bmod 4$. First note that the prototype $(a, b, c, e) = (0, (d+2)/2, (d-2)/2, -2)$ is a valid prototype, and corresponds to a cusp with $v_1 = (d^2-4)/4$ and $v_2 = 1$. Conversely, suppose $v_1 = (d^2-4)/4$ and $v_2 = 1$ for a cusp with prototype (a, b, c, e). Since $v_1 v_2 = (d^2-4)/4$ divides $(d^2 - e^2)/4$ (proof of Proposition A.6), we have that $e = 2$ or -2. Also, $\gcd(b, c) = \gcd(\lambda, \lambda') = 1$ since λ is odd and $\lambda - \lambda' = e = \pm 2$. From the formula for v_1, we see that

$$bc = \gcd(b, \lambda') \gcd(c, \lambda) = \lambda\lambda'$$

which holds only if $b = \lambda'$ and $c = \lambda$. We conclude that the prototype is $(0, (d+2)/2, (d-2)/2, -2)$ or $(0, (d-2)/2, (d+2)/2, 2)$, but the latter is not a valid prototype since it violates $e + c < b$.

Now suppose $d \equiv 2 \bmod 4$, where a similar argument yields the desired result. The prototype $(a, b, c, e) = (0, (d+4)/2, (d-4)/2, -4)$ is a valid prototype, and corresponds to a cusp with $v_1 = (d^2-16)/4$, $v_2 = 1$. Conversely, suppose $v_1 = (d^2-16)/4$ and $v_2 = 1$ for a cusp with prototype (a, b, c, e). Since $v_1 v_2 = (d^2-16)/4$ divides $(d^2 - e^2)/4$, we have that $e = 4$ or -4. Also, $\gcd(b, c) = \gcd(\lambda, \lambda') = 1$ since λ is odd and $\lambda - \lambda' = e = \pm 4$. From the formula for v_1, we see that $\gcd(b, \lambda') = \lambda'$ and $\gcd(c, \lambda) = \lambda$. From $bc = \lambda\lambda'$, we have $b = \lambda'$ and $c = \lambda$. We conclude that the prototype is either $(0, (d+4)/4, (d-4)/4, -4)$ or $(0, (d-4)/4, (d+4)/4, 4)$, and the latter violates $e + c < b$. □

References

[Ba] M. Bainbridge. Euler characteristics of Teichmüller curves in genus two. *Geom. Topol.* **11**(2007), 1887–2073, arXiv:math/0611409.

[Mag] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24**(1997), 235–265. Computational algebra and number theory (London, 1993).

[BM] I. Bouw and M. Möller. Differential equations associated with nonarithmetic Fuchsian groups. *J. Lond. Math. Soc.* **81**(2010), 65–90, arXiv:0710.5277.

[DR] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Uuniv. Antwerp, Antwerp, 1972)*, volume 349 of *Lecture Notes in Math.*, pages 143–316. Springer, Berlin, 1973.

[De] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abh. Math. Semin. Univ. Hansischen* **14**(1941), 197–272.

[EK] N. Elkies and A. Kumar. K3 surfaces and equations for Hilbert modular surfaces. *Algebra Number Theory* **8**(2014), 2297–2411, arXiv:1209.3527.

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

[Ig] J.-I. Igusa. Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.* **81**(1959), 561–577.

[Ka] E. Kani. Elliptic curves on Abelian surfaces. *Manuscripta Math.* **84**(1994), 199–223.

[KM] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[Ku] A. Kumar. Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields. *Res. Math. Sci.* **2**(2015), arXiv:1412.2849.

[KM] A. Kumar and R. E. Mukamel. Algebraic models and arithmetic geometry of Teichmüller curves in genus two. *Int. Math. Res. Not.* (2016), arXiv:1406.7057.

[LR] S. Lelièvre and E. Royer. Orbitwise countings in $\mathcal{H}(2)$ and quasimodular forms. *Int. Math. Res. Not.* (2006), arXiv:math/0509205.

[Mc1] C. T. McMullen. Teichmüller curves in genus two: Discriminant and spin. *Math. Ann.* **333**(2005), 87–130.

[Mc2] C. T. McMullen. Dynamics of $\mathrm{SL}_2(\mathbb{R})$ over moduli space in genus two. *Ann. of Math. (2)* **165**(2007), 397–456.

[Mc3] C. T. McMullen. K3 surfaces, entropy and glue. *J. Reine Agnew. Math.* **658**(2011), 1–25.

[Mu] R. E. Mukamel. Orbifold points on Teichmüller curves and Jacobians with complex multiplication. *Geom. Topol.* **18**(2014), arXiv:1606.04967.

[Su] Andrew V. Sutherland. On the evaluation of modular polynomials. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 531–555. Math. Sci. Publ., Berkeley, CA, 2013.