Noncongruence subgroups in H(2)

Pascal Hubert, Samuel Lelièvre

NONCONGRUENCE SUBGROUPS IN $\mathcal{H}(2)$

PASCAL HUBERT AND SAMUEL LELIÈVRE

Abstract. We study the congruence problem for subgroups of the modular group that appear as Veech groups of square-tiled surfaces in the minimal stratum of abelian differentials of genus two.

Keywords: congruence problem, Veech group, square-tiled surfaces

Contents

1. Introduction

Let ω be a holomorphic 1-form on a compact Riemann surface X. If there exists a branched covering $f : X \to \mathbf{T}^2 = \mathbf{R}^2/\mathbf{Z}^2$, ramified only over the origin of $\mathbf{T}^2$, such that $f^*(dz) = \omega$, the flat surface $(X, |\omega|)$ is tiled by squares whose vertices project to the origin of the torus, and (X, ω) is called a **square-tiled (translation) surface**.

In each genus g, square-tiled surfaces are the integer points of the moduli space $\mathcal{H}_g = \Omega\mathcal{M}_g$ of holomorphic 1-forms on Riemann surfaces of genus g. This space is stratified by the combinatorial type of zeros, and each stratum is a complex orbifold endowed with an action of $\mathrm{SL}(2, \mathbf{R})$. Orbits for this action are called Teichmüller discs.

The main problem in dynamics in Teichmüller spaces is to understand this $\mathrm{SL}(2, \mathbf{R})$-action, and to obtain Ratner-like classification results for its orbit closures and its invariant closed submanifolds.

Date: 29 May 2004.

The first step is to determine as many invariant closed submanifolds as possible. The simplest of them are closed orbits. These are the orbits of translation surfaces with finite-covolume stabilisers, called Veech surfaces because of Veech's pioneering work [Ve]. These Teichmüller discs project to geodesically embedded curves, called Teichmüller curves, in the moduli space $\mathcal{M}_g$ of complex curves of genus g. These curves are uniformised by the stabiliser of the corresponding $\mathrm{SL}(2,\mathbf{R})$-orbit.

Square-tiled surfaces are Veech surfaces. They already appeared in Thurston's work on the classification of surface diffeomorphisms, see [FLP, exposé 13]. Nevertheless up to recently their Teichmüller discs have been little discussed, due to the difficulty of proving precise statements about them. The only classical result is Gutkin and Judge's theorem [GuJu] which states that the corresponding stabilisers are arithmetic (commensurable to $\mathrm{SL}(2,\mathbf{Z})$). Very recently the Teichmüller discs of square-tiled surfaces were studied into more detail, see [HL], [Mc4], [Mö], [Schmi].

A square-tiled surface (X,ω) is called **primitive** if the lattice of relative periods of ω is $\mathbf{Z}^2$ (in other words the covering $(X,\omega)\to(\mathbf{T}^2,dz)$ does not factor through a bigger torus). In this case, the stabiliser, denoted by $\mathrm{SL}(X,\omega)$, is a (finite-index) subgroup of $\mathrm{SL}(2,\mathbf{Z})$.

In order to give the most accurate description of Teichmüller discs of square-tiled surfaces, we investigate these subgroups. In the theory of subgroups of $\mathrm{SL}(2,\mathbf{Z})$, a natural and important question is the congruence problem. This question is the central object of this paper: we give a negative answer in the stratum $\mathcal{H}(2)=\Omega\mathcal{M}_2(2)$ of 1-forms on genus 2 surfaces having one double zero.

Recent results about square-tiled surfaces in $\mathcal{H}(2)$. The discrete orbit $\mathrm{SL}(2,\mathbf{Z})\cdot(X,\omega)$ of a primitive square-tiled surface (X,ω) consists of all the primitive square-tiled surfaces in its Teichmüller disc $\mathrm{SL}(2,\mathbf{R})\cdot(X,\omega)$; indeed, $\mathrm{SL}(2,\mathbf{Z})$ acts on primitive square-tiled surfaces, preserving the number of squares. Understanding the Teichmüller discs or the discrete orbits of primitive square-tiled surfaces is therefore equivalent. We will use the following result about the discrete orbits of primitive square-tiled surfaces in $\mathcal{H}(2)$.

Theorem A. *Primitive n-square-tiled surfaces in the stratum $\mathcal{H}(2)$ form: one orbit A_3 if $n=3$; two orbits A_n and B_n if n is odd $\geqslant 5$; one orbit C_n if n is even.*

This was shown for prime n in [HL], and conjectured for arbitrary n; the conjecture was proved in full generality in [Mc4].

Let Γ_{A_n}, Γ_{B_n} and Γ_{C_n} denote the stabilisers of these orbits.

Remark. The indices of the groups Γ_{A_n}, Γ_{B_n}, Γ_{C_n} in $\mathrm{SL}(2,\mathbf{Z})$ are the cardinalities a_n, b_n, c_n of the discrete orbits A_n, B_n, C_n.

Eskin–Masur–Schmoll [EsMaSc] give a formula for the number of primitive n-square-tiled surfaces in $\mathcal{H}(2)$:

Theorem B. *The number of primitive n-square-tiled surfaces in $\mathcal{H}(2)$ is $\frac{3}{8}(n-2)n^2\prod_{p|n}(1-\frac{1}{p^2})$.*

Remark. Throughout this paper, the letter p always denotes prime numbers; in particular, $\prod_{p|n}$ is the product over prime divisors of n.

This formula gives c_n (and a_3) when there is one orbit and $a_n + b_n$ when there are two. We conjectured in [HL]:

Conjecture 1. *For odd $n \geqslant 5$, a_n and b_n are given by:*
$$a_n = \tfrac{3}{16}(n-1)n^2\prod_{p|n}(1-\tfrac{1}{p^2}), \quad b_n = \tfrac{3}{16}(n-3)n^2\prod_{p|n}(1-\tfrac{1}{p^2}).$$

Statement of results. In this paper, we show:

Theorem 1. *For all even $n \geqslant 4$, Γ_{C_n} is a noncongruence subgroup. For all odd $n \geqslant 5$ satisfying Conjecture 1, Γ_{A_n} and Γ_{B_n} are noncongruence subgroups.*

Remark. Conjecture 1 is proved up to $n = 10000$ by an explicit combinatorial computer calculation.

Corollary 1.1. *Under Conjecture 1, the only primitive square-tiled surfaces in $\mathcal{H}(2)$ whose stabiliser is a congruence subgroup are those tiled with 3 squares.*

Corollary 1.2. *Under Conjecture 1, of all the Teichmüller curves embedded in $\mathcal{M}_2$ that come from orbits in $\mathcal{H}(2)$, only one is uniformised by a congruence subgroup of $\mathrm{SL}(2,\mathbf{Z})$.*

Remark. For $n = 3$, Γ_{A_3} is the level 2 congruence subgroup Θ generated by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$, named after its link to the Jacobi Theta function.

Link with the Hurwitz problem. An essential ingredient in our proof of Theorem 1 is the knowledge of the indices in $\mathrm{SL}(2,\mathbf{Z})$ of Γ_{A_n}, Γ_{B_n} and Γ_{C_n} (given by Theorem B and Conjecture 1).

Since these indices are the cardinalities of the discrete orbits A_n, B_n and C_n, finding these numbers is a variant of Hurwitz's problem, which consists in counting the number of branched covers of a fixed combinatorial type (number and multiplicity of ramification points) and fixed degree of a Riemann surface S. A very detailed survey of this subject can be found in the introduction of Zvonkine's thesis [Zv].

When S is the torus $\mathbf{T}^2 = \mathbf{R}^2/\mathbf{Z}^2$ (or more generally an elliptic curve), it can be endowed with the 1-form dz. Hurwitz's problem amounts to counting the number of coverings (with fixed combinatorial type) $f : (X, \omega) \to (\mathbf{T}^2, dz)$ where $\omega = f^*(dz)$. For a fixed combinatorial type c, denote by $h_{n,c}$ the number of such coverings, weighted by the inverse of their number of automorphisms.

We have the following fundamental theorem:

Theorem C. *For any combinatorial type, the generating series* $F_c(z) = \sum_{h=1}^{\infty} h_{n,c}\, q^n$, *where* $q = e^{2i\pi z}$, *is a quasi-modular form of maximal weight* $6g - 6$.

This theorem was first proved in the case of simple ramifications by Dijkgraaf [Di] and Kaneko–Zagier [KaZa]; the general proof relies on results of Bloch–Okounkov [BlOk], see [EsOk].

The quasi-modular form is explicitated by Kani [Ka] and by Eskin–Masur–Schmoll [EsMaSc] in particular cases. Some generalisations are proved by Eskin–Okounkov–Pandharipande [EsOkPa].

Note also that the asymptotics of the countings of square-tiled surfaces of bounded area serve to compute the volumes of strata (see [Zo], [EsOk]).

Acknowledgements. We thank Gabriela Schmithüsen for the inspiration and useful discussions, and Giovanni Forni for encouraging this research.

2. Background

2.1. **Square-tiled surfaces, action of** $\mathrm{SL}(2, \mathbf{Z})$**, cusps.** We recall here some tools used in [HL], to which we refer for more detail.

The modular group $\Gamma(1) = \mathrm{SL}(2, \mathbf{Z})$ acts on primitive square-tiled surfaces, preserving the number of squares tiles. Indeed, the property of having $\mathbf{Z}^2$ as lattice of relative periods is $\mathrm{SL}(2, \mathbf{Z})$-invariant.

Given a primitive square-tiled surface (X, ω), its stabiliser $\mathrm{SL}(X, \omega)$ is a finite-index subgroup of $\mathrm{SL}(2, \mathbf{Z})$, therefore the curve $\mathrm{SL}(X, \omega)\backslash\mathbf{H}$ is a branched cover of the modular curve $\mathrm{SL}(2, \mathbf{Z})\backslash\mathbf{H}$, and the degree of the cover is the index of $\mathrm{SL}(X, \omega)$ in $\mathrm{SL}(2, \mathbf{Z})$.

The modular group is generated by any two matrices among $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Denote by $\mathcal{U}$ the subgroup generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Cusps. The cusps of $\mathrm{SL}(X, \omega)\backslash\mathbf{H}$ are classified combinatorially by the following lemma.

Lemma 2.1 (Zorich)**.** *Let* (X, ω) *be a primitive square-tiled surface. There is a* 1-1 *correspondence between the set of cusps of* $\mathrm{SL}(X, \omega)\backslash\mathbf{H}$ *and the* $\mathcal{U}$*-orbits of* $\mathrm{SL}(2, \mathbf{Z})\cdot(X, \omega)$.

Any square-tiled surface decomposes into horizontal cylinders, which are also square-tiled, and bounded by unions of saddle connections of integer lengths. This provides a way to give coordinates for square-tiled surfaces in each stratum (see below for the stratum $\mathcal{H}(2)$).

The action of the generators $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ of $\mathrm{SL}(2,\mathbf{Z})$ is easily seen in these coordinates: $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ exchanges the horizontal and vertical directions; $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ only changes the twists.

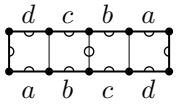
The width of a cusp is given by the cardinality of the corresponding $\mathcal{U}$-orbit. If the horizontal cusp has width ℓ, the primitive parabolic in the horizontal direction is $\left(\begin{smallmatrix}1&\ell\\0&1\end{smallmatrix}\right)$. Considering how the cylinders behave under the action of $\mathcal{U}$, we get the following lemma.

Lemma 2.2. *If a primitive square-tiled surface decomposes into horizontal cylinders c_i of height h_i and width w_i, then its (horizontal) cusp width equals the least common multiple of the $\frac{w_i}{h_i \wedge w_i}$, possibly divided by some factor.*

Notation. Here, and in the sequel, $a \wedge b$ denotes the greatest common divisor of two integers a and b.

The following example illustrates the case of division by a factor.

This surface is in $\mathcal{H}(1,1)$ and has a nontrivial translation by the vector $(2,0)$; though it is made of one cylinder of height 1 and width 4, its cusp width is only 2.



In the stratum $\mathcal{H}(2)$ on which we will focus from now on, this situation does not occur.

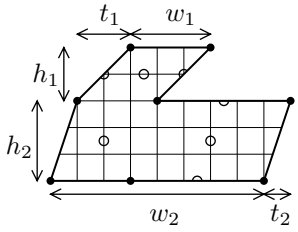
2.2. **Square-tiled surfaces in $\mathcal{H}(2)$.** The stratum $\mathcal{H}(2)$ has recently received much attention ([EsMaSc], [Ca], [Mc1, Mc3, Mc4], [HL]).

Square-tiled surfaces in $\mathcal{H}(2)$ are of two types [Zo], the one-cylinder ones and the two-cylinder ones. The corresponding coordinates are: for one-cylinder surfaces, one height, three lengths of saddle connections and one twist parameter; for two-cylinder surfaces, one height, width and twist for each cylinder.

Theorem A says that for each odd $n \geqslant 5$, primitive n-square-tiled surfaces are in two orbits A_n and B_n. These orbits are distinguished by a simple invariant, the number of integer Weierstrass points (i.e. Weierstrass points located at vertices of the square tiles). A surface is in A_n if it has one integer Weierstrass point, in B_n if it has three.

The coordinates for square-tiled surfaces in $\mathcal{H}(2)$ were used in [Zo], in [EsMaSc] and in [HL] where the position of Weierstrass points was also discussed and the invariant introduced. This invariant was independently expressed in terms of divisors by Kani [Ka]. McMullen [Mc4] expressed it as the parity of a spin structure.

Notation. Denote by $S(h_1, h_2, w_1, w_2, t_1, t_2)$ the two-cylinder surface with cylinders c_i of height h_i, width w_i and twist t_i, with $w_1 < w_2$.



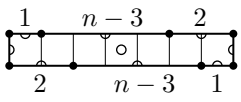
The figure shows a fundamental polygon for $S(2, 3, 3, 8, 2, 1)$; the surface is obtained from this polygon by identifying pairs of parallel sides of same lengths. We indicate the double zero by black dots and the other Weierstrass points by circles. The same conventions hold for all pictures in this paper.

Let us give some examples of square-tiled surfaces in $\mathcal{H}(2)$.

First, some one-cylinder surfaces of particular interest.

Lemma 2.3. *For each $n \geqslant 4$, there is a primitive n-square-tiled surface which is one-cylinder both horizontally and vertically.*

The one-cylinder surface with saddle connections of lengths 1, $n-3$, 2 on the top and 2, $n-3$, 1 on the bottom has this property.



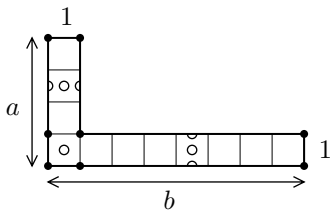
Corollary 2.4. *The stabiliser of this surface contains $\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ n & 1\end{smallmatrix}\right)$.*

Indeed, one-cylinder cusps have width n.

Remark. When n is odd, the surface described above is in orbit B_n.

Some two-cylinder surfaces also deserve special attention.

Notation. For a and $b \geqslant 2$, denote by $\mathrm{L}(a, b)$ the surface $S(a-1, 1, 1, b, 0, 0)$. This surface is a primitive square-tiled surface tiled by $n = a+b-1$ squares. This surface has cusp width b and vertically a.



When n is odd, this surface is in A_n if a and b are even, in B_n if a and b are odd.

2.3. **Congruence subgroups; level of a subgroup.** The material in this section is classical, and can be found in [Ra].

For any integer $m > 1$, consider the natural projection $\mathrm{SL}(2, \mathbf{Z}) \to \mathrm{SL}(2, \mathbf{Z}/m\mathbf{Z})$. This projection is a group homomorphism. Its kernel is called the **principal congruence subgroup of level** m, and denoted by $\Gamma(m)$. It consists in all matrices congruent to $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ modulo m. This is consistent with the notation $\Gamma(1)$ for $\mathrm{SL}(2, \mathbf{Z})$.

Lemma 2.5. *For any m, $[\Gamma(1) : \Gamma(m)] = m^3 \prod_{p|m}(1 - \frac{1}{p^2})$.*

Corollary 2.6. *If $m \wedge m' = 1$, then $[\Gamma(m) : \Gamma(mm')] = [\Gamma(1) : \Gamma(m')]$.*

Any group Γ containing some $\Gamma(m)$ is called a **congruence subgroup**, and its **level** is defined to be the least m such that $\Gamma(m) \subset \Gamma$ (i.e. the level of the largest principal congruence subgroup it contains).

Remark. A principal congruence subgroup is a normal subgroup of $\Gamma(1)$. Hence being a congruence subgroup is invariant by conjugation in $\mathrm{SL}(2, \mathbf{Z})$; the level is also invariant.

There is a more general notion of level, due to Wohlfahrt [Wo]. The **level** of a finite-index subgroup of $\mathrm{SL}(2, \mathbf{Z})$ is the least common multiple of its cusp widths. Wohlfahrt proved that for congruence subgroups, it coincides with the previous definition, and that:

Lemma 2.7 (Wohlfahrt [Wo])**.** *A finite-index subgroup of level ℓ is a congruence subgroup if and only if it contains the principal congruence subgroup of level ℓ.*

2.4. **Quasi-modular forms.** As said in the introduction, the generating function for the weighted countings of surfaces tiled by n squares is a quasi-modular form.

The numbers $h_{n,c}$ of surfaces tiled by n squares in a given stratum, and the numbers $h^{\mathrm{P}}_{n,c}$ of primitive ones, are related by

$$h_{n,c} = \textstyle\sum_{d|n} \sigma(n/d) h^{\mathrm{P}}_{d,c},$$

where $\sigma(k) = \sum_{d|k} d$ is the sum of divisors of k. This is because the number of tori tiled by n squares is $\sigma(n)$.

In addition, we note that in $\mathcal{H}(2)$, the coverings have no automorphisms, hence the weighted and unweighted countings are the same.

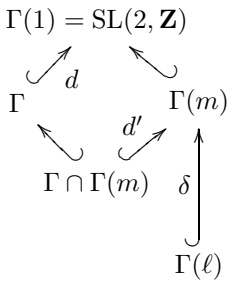
Conjecture 2. *In $\mathcal{H}(2)$, the countings for odd n according to the invariant are generated by a quasi-modular form.*

Theorem B is mentioned in [EsMaSc] as a consequence of the quasi-modularity. Likewise, Conjecture 1 would follow from Conjecture 2.

3. Strategy for the proof of Theorem 1

We build on the proof by Schmithüsen [Schmi] that the stabiliser of a 4-square-tiled surface in $\mathcal{H}(2)$ is a noncongruence subgroup, based on an idea of Stefan Kühnlein.

3.1. **Sufficient conditions for noncongruence.** Let Γ be a subgroup of $\Gamma(1)$ of finite index d and level ℓ. For any divisor m of ℓ, consider the finite-index inclusions represented on the figure.



Two remarks. First, if Γ projects surjectively to $\mathrm{SL}(2,\mathbf{Z}/m\mathbf{Z})$, one can conclude by observing the two exact sequences below that $d' = d$, where $d' = [\Gamma(m) : \Gamma \cap \Gamma(m)]$ and $d = [\Gamma(1) : \Gamma]$.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma(m) & \longrightarrow & \Gamma(1) & \longrightarrow & \mathrm{SL}(2,\mathbf{Z}/m\mathbf{Z}) & \longrightarrow & 1 \\ \| & & \uparrow{\scriptstyle d'} & & \uparrow{\scriptstyle d} & & \| & & \| \\ 1 & \longrightarrow & \Gamma \cap \Gamma(m) & \longrightarrow & \Gamma & \longrightarrow & \mathrm{SL}(2,\mathbf{Z}/m\mathbf{Z}) & \longrightarrow & 1 \end{array}$$

Second, if Γ is a congruence subgroup, and hence by Lemma 2.7 contains $\Gamma(\ell)$, then $\Gamma(\ell)$ is contained in $\Gamma\cap\Gamma(m)$ and the indices satisfy $[\Gamma(m) : \Gamma(\ell)] = [\Gamma(m) : \Gamma\cap\Gamma(m)]\cdot[\Gamma\cap\Gamma(m) : \Gamma(\ell)]$, which implies $d' \mid \delta$.

Combining these two remarks, we get the following sufficient condition for noncongruence, which was used by Schmithüsen [Schmi].

Proposition 3.1 (Kühnlein)**.** *If Γ is a subgroup of $\Gamma(1)$ of finite index d and level ℓ and there exists a divisor m of ℓ for which*
- *Γ projects surjectively to $\mathrm{SL}(2,\mathbf{Z}/m\mathbf{Z})$, and*
- *the index $\delta = [\Gamma(m) : \Gamma(\ell)]$ is not a multiple of d,*

then Γ is not a congruence subgroup.

Remark. Suppose Γ contains two matrices $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ k' & 1 \end{smallmatrix}\right)$. If m is an integer relatively prime to both k and k', then k and k' are invertible modulo m so some powers of $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ k' & 1 \end{smallmatrix}\right)$ project to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ in $\mathrm{SL}(2,\mathbf{Z}/m\mathbf{Z})$, hence the projection $\Gamma \to \mathrm{SL}(2,\mathbf{Z}/m\mathbf{Z})$ is surjective.

This extra remark yields the following sufficient condition for non-congruence.

Proposition 3.2. *If a subgroup $\Gamma \subset \Gamma(1)$ of finite index d contains two matrices $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ k' & 1 \end{smallmatrix}\right)$ and if its level ℓ has a divisor m relatively prime to both k and k', such that the index $\delta = [\Gamma(m) : \Gamma(\ell)]$ is not a multiple of d, then Γ is not a congruence subgroup.*

3.2. **Strategy.** Consider an orbit A_n, B_n or C_n, with n as in Theorem 1. Its stabiliser Γ_{A_n}, Γ_{B_n} or Γ_{C_n} is defined only up to conjugation in $\mathrm{SL}(2,\mathbf{Z})$; the representatives of the conjugacy class are the stabilisers of the (square-tiled) surfaces in the orbit. The index and level are preserved by conjugation in $\mathrm{SL}(2,\mathbf{Z})$.

Choice. Let S be a (square-tiled) surface in an orbit A_n, B_n or C_n, and Γ be its stabiliser.

Notation. Denote by d the index of Γ and by ℓ its level. Consider the prime factor decompositions $n = \prod p^\nu$ and $\ell = \prod p^\lambda$, where ν and λ can denote a different integer for each prime p.

Choice. Choose some $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ k' & 1 \end{smallmatrix}\right)$ in Γ, for instance k and k' could be taken to be the horizontal and vertical cusp widths of S.

Notation. Following [Mc4], if a and b are two integers, denote by $a//b$ the greatest divisor of a that is prime to b. If $a = \prod p^\alpha$ is the prime factor decomposition of a, we have $a//b = \prod_{p\nmid b} p^\alpha = a/\prod_{p|b} p^\alpha$.

Choice. Choose $m = \ell//kk' = \ell/\prod_{p|kk'} p^\lambda$.

Notation. Denote by δ the index of $\Gamma(\ell)$ in $\Gamma(m)$.

By construction m is a divisor of ℓ, relatively prime to both k and k'. In view of applying Proposition 3.2, there remains only to check that d does not divide δ. Since m is also relatively prime to ℓ/m, by Corollary 2.6, $\delta = (\ell/m)^3 \prod_{p|\ell/m}(1-\frac{1}{p^2})$.

Remark. If a is an integer and $a = \prod p^\alpha$ is its prime factor decomposition, one can rewrite $a^r \prod_{p|a}(1-\frac{1}{p^2})$ as $\prod_{p|a} p^{r\alpha-2}(p^2-1)$. Hence
- $\delta = \prod_{p|kk'} p^{3\lambda-2}(p^2-1)$, and
- $d = f(n)\prod_{p|n} p^{2\nu-2}(p^2-1)$, where $f(n)$ is one of $\frac{3}{16}(n-1)$, $\frac{3}{16}(n-3)$, $\frac{3}{8}(n-2)$, according to whether orbit A_n, B_n or C_n is under consideration.

In order to complete the proof, there merely remains to describe how to apply our strategy.

For this we need the levels of Γ_{A_n}, Γ_{B_n} and Γ_{C_n}; we give them in § 4.

The last three sections then describe, in each orbit, good choices of a surface S, values of k and k', and, keeping the notations (d, ℓ, ν, λ, m, δ) introduced here (and consistent with those in § 3.1), show that d does not divide δ.

4. The level of Γ_{A_n}, Γ_{B_n} and Γ_{C_n}

As said above, the stabiliser of an $\mathrm{SL}(2,\mathbf{Z})$-orbit of square-tiled surfaces is defined up to conjugacy in $\mathrm{SL}(2,\mathbf{Z})$, but its level is well-defined.

Proposition 4.1. *The groups Γ_{A_n}, Γ_{B_n} and Γ_{C_n} have levels:*

$$\operatorname{lev}\Gamma_{A_n} = d_n, \quad \operatorname{lev}\Gamma_{B_n} = d_n/4, \quad \operatorname{lev}\Gamma_{C_n} = d_n,$$

where $d_n = \operatorname{lcm}(1,2,3,\dots,n)$.

Remark. The prime factor decomposition of d_n is $\prod_{p\leqslant n} p^\tau$ where the exponents τ are the integers such that $p^\tau \leqslant n < p^{\tau+1}$.

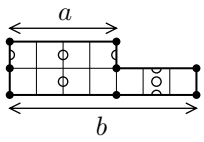
The remainder of this section is devoted to proving the proposition.

First recall that the level of $\Gamma \subset \mathrm{SL}(2,\mathbf{Z})$ is defined as the least common multiple of the amplitudes of the cusps of Γ. When Γ is the stabiliser of a primitive square-tiled surface S, its cusp widths are equivalently the horizontal cusp widths of the surfaces in the $\mathrm{SL}(2,\mathbf{Z})$-orbit of S.

Recall also Lemma 2.2. If S is tiled by n squares, the widths of its cylinders are at most n, so the level of Γ divides $\operatorname{lcm}(1,2,3,\dots,n)$.

Orbit C_n (for even n) contains one-cylinder surfaces, which have cusp width n, and, for all a and b such that $a+b=n+1$ and $2 \leqslant a,b \leqslant n-1$, two-cylinder surfaces $\mathrm{L}(a,b)$, which have cusp width b. Hence, the level of Γ_{C_n} is a multiple of, and therefore equals, $\operatorname{lcm}(1,2,3,\dots,n)$.

Orbit A_n (for odd n) contains one-cylinder surfaces, which have cusp width n, and, for all a and b such that $a+b=n$ and $1 \leqslant a < b \leqslant n-1$, two-cylinder surfaces with two cylinders of height 1 and widths a and b, which have cusp width $\operatorname{lcm}(a,b)$. Hence, the level of Γ_{A_n} is a multiple of, and therefore equals, $\operatorname{lcm}(1,2,3,\dots,n)$.



Orbit B_n (for odd n) contains one-cylinder surfaces, which have cusp width n, and, for all odd a and b such that $a+b=n+1$ and $2 \leqslant a,b \leqslant n-1$, two-cylinder surfaces $\mathrm{L}(a,b)$, which have cusp width b. Hence, the level of Γ_{B_n} is a multiple of $\operatorname{lcm}(1,3,5,\dots,n)$.

Since $\operatorname{lcm}(1,2,3,\dots,n)$ is a power of 2 times $\operatorname{lcm}(1,3,5,\dots,n)$, there remains only to determine the power of 2 in the level of Γ_{B_n}, i.e. the maximal power of 2 that can arise as a divisor of $\frac{w}{h\wedge w}$ for the height h and the width w of a cylinder of a surface of B_n.

Let τ be the integer such that $2^\tau < n < 2^{\tau+1}$.

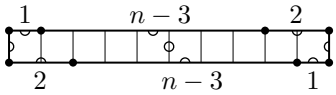
There is at least one two-cylinder surface $S(h_1,2,w_1,2^{\tau-1},t_1,t_2)$ with odd t_2 in B_n; such a surface satisfies $\frac{w_2}{h_2\wedge w_2} = 2^{\tau-2}$.

Suppose a surface S in B_n has even cusp width $k = 2^t\cdot q$ with q odd. Then S has two cylinders, and by the discussion in [HL, § 5.1], one cylinder has even width w and even height h, while the other

has odd height h' and odd width w'. Since $k = \mathrm{lcm}(\frac{w}{w\wedge h}, \frac{w'}{w'\wedge h'})$ and $\frac{w'}{w'\wedge h'}$ is odd, 2^t divides $\frac{w}{h\wedge w}$. But $h \geqslant 2$ and since $n = hw + h'w'$, $w < n/h \leqslant n/2 < 2^\tau$, so $\frac{w}{h\wedge w} \leqslant w/2 < 2^{\tau-1}$. Therefore $t \leqslant \tau - 2$.

5. Noncongruence of Γ_{C_n} for even $n \geqslant 4$

5.1. **Case when $n-2$ is not a power of 2.** We take S to be the one-cylinder surface with saddle connections of lengths 1, $n-3$, 2 on the top and 2, $n-3$, 1 on the bottom.



As a one-cylinder surface it has cusp width $k = n$ and since its vertical direction is also one-cylinder, its vertical cusp width k' is also n, so Γ contains $\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ n & 1\end{smallmatrix}\right)$.

Recall that Γ has index $d = \frac{3}{8}(n-2)\prod_{p|n} p^{2\nu-2}(p^2-1)$.

Choosing $m = \ell//n = \ell/\prod_{p|n} p^\lambda$ leads to $\delta = \prod_{p|n} p^{3\lambda-2}(p^2-1)$.

So d divides δ if and only if $3(n-2)$ divides $2^3\cdot\prod_{p|n} p^{3\lambda-2\nu}$.

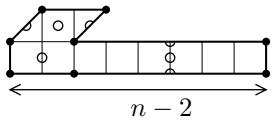
Since $n \wedge (n-2) = 2$, the assumption that $n-2$ is not a power of 2 implies it has some (odd) prime factors that do not divide n.

Hence d does not divide δ, so Γ cannot be a congruence subgroup.

5.2. **Case when $n-2$ is a power of 2.** The case $n = 4$ is known from [Schmi]. It can also be treated as above, since the index of Γ_{C_4} is $d = 9$ and, taking S and m as above, $\delta = 2^4\cdot 3$.

From now on assume $n > 4$.

We take $S = S(1, 1, 1, n-2, 1, 0)$.



Note that this requires that $n - 2 > 2$, which is why the case $n = 4$ was dealt with separately.

This surface has horizontal cusp width $n-2$ and vertical cusp width 4, so the stabiliser Γ contains $\left(\begin{smallmatrix}1 & n-2\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 4 & 1\end{smallmatrix}\right)$.

Recall that Γ has index $d = \frac{3}{8}(n-2)\prod_{p|n} p^{2\nu-2}(p^2-1)$.

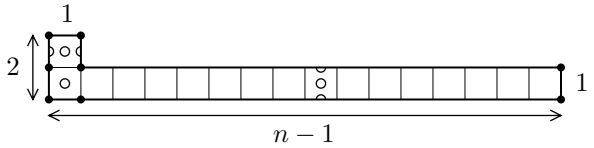
Choosing $m = \ell//2 = \ell/2^\lambda$ leads to $\delta = 2^{3\lambda-2}(2^2-1) = 2^{3\lambda-2}\cdot 3$.

Since n is even, it has $p = 2$ as a prime factor, which gives 3 as p^2-1, so 3^2 divides d.

Hence d does not divide δ, so Γ cannot be a congruence subgroup.

6. Noncongruence of Γ_{A_n} for odd $n \geqslant 5$

6.1. **Case when $n-1$ is a power of 2.** Take $S = \mathrm{L}(2, n-1)$.



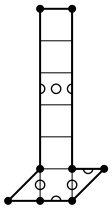
Its cusp width is $n-1$ $(= 2^\lambda)$ and its vertical cusp width is 2, so its stabiliser Γ contains $\left(\begin{smallmatrix} 1 & n-1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$.

Here $d = \frac{3}{16}(n-1)\prod_{p|n} p^{2\nu-2}(p^2-1)$.

The choice of $m = \ell//2 = \ell/2^\lambda$ leads to $\delta = 2^{3\lambda-2}\cdot 3$.

If n is a power of 3, then 3^3 divides d; otherwise n has some (odd) prime factor $p \neq 3$, for which $p^2-1 = (p-1)(p+1)$ is a multiple of 3, so that 3^2 divides d. Therefore d does not divide δ and Γ is not a congruence subgroup.

6.2. **Case when $n-1$ is not a power of 2.** Here we take the surface $S = S(n-2, 1, 1, 2, 0, 1)$. This surface is $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\cdot \mathrm{L}(n-1, 2)$.



The cusp width of S is 2, and S has one vertical cylinder, hence vertical cusp width n. So Γ contains $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$.

Here $d = \frac{3}{16}(n-1)\prod_{p|n} p^{2\nu-2}(p^2-1)$.

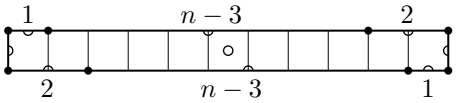
The choice of $m = \ell//2n = \ell/(2^\lambda \prod_{p|n} p^\lambda)$ leads to $\delta = 2^{3\lambda-2}\cdot 3\cdot \prod_{p|n} p^{3\lambda-2}(p^2-1)$.

It follows that d divides δ if and only if $(n-1)$ divides $2^{3\lambda+2}\cdot \prod_{p|n} p^{3\lambda-2\nu}$.

Since n is not some 2^k+1, $n-1$ has odd prime factors; these do not divide n, so d does not divide δ and Γ is not a congruence subgroup.

7. Noncongruence of Γ_{B_n} for odd $n \geqslant 5$

7.1. **A proof for most cases.** Consider the one-cylinder surface S having saddle connections of lengths 1, $n-3$, 2 on the top and 2, $n-3$, 1 on the bottom.



The stabiliser of this surface contains $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$.

Here $d = \frac{3}{16}(n-3)\prod_{p|n} p^{2\nu-2}(p^2-1)$.

The choice of $m = \ell//n$ leads to $\delta = \prod_{p|n} p^{3\lambda-2}(p^2-1)$.

Thus d divides δ if and only if $3(n-3)$ divides $16\prod_{p|n} p^{3\lambda-2\nu}$.

Call an odd $n \geqslant 5$ "bad" if $3(n-3)$ divides $16\prod_{p|n} p^{3\lambda-2\nu}$.

As we are about to see, this is very rare, so that for "most" odd $n \geqslant 5$, d does not divide δ.

7.2. **The bad case.** If n is such that $3(n-3)$ divides $16\prod_{p|n} p^{3\lambda-2\nu}$,
- $n-3$ is not a multiple of 2^5;
- n is a multiple of 3 (and hence $(n-3)\wedge n = 3$);
- all odd prime factors of $n-3$ divide n.

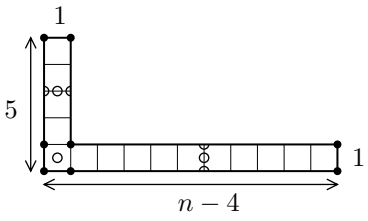
Combining these three remarks, we see the bad case is when $n-3$ is of the form $2^r\cdot 3^s$ with $1 \leqslant r \leqslant 4$ and $1 \leqslant s$.

Thus the bad case consists of the four sequences $n_{r,s} = 2^r\cdot 3^s + 3$ for $r = 1$ to 4 and $s \geqslant 1$, which have exponential growth, hence zero density.

In particular, the discussion in § 7.1 proves the noncongruence of Γ_{B_n} when n is out of these four sequences.

7.3. **First bad cases.** Here we examine the first element of each of the four sequences, i.e. $n \in \{9, 15, 27, 51\}$. We include the second element of the first sequence, i.e. $n = 21$.

Take $S = \mathrm{L}(5, n-4)$. Its horizontal cusp width is $n-4$ and its vertical cusp width is 5, so its stabiliser Γ contains $\left(\begin{smallmatrix} 1 & n-4 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 5 & 1 \end{smallmatrix}\right)$.



Here $d = \frac{3}{16}(n-3)n^2\prod_{p|n}(1-\frac{1}{p^2})$.

Choosing $m = \ell//5(n-4)$ leads to $\delta = \prod_{p|5(n-4)} p^{3\lambda-2}(p^2-1)$.

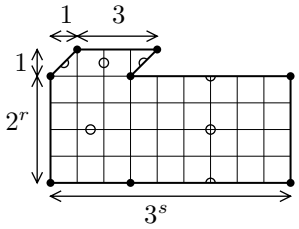
The values of d and δ for $n \in \{9, 15, 21, 27, 51\}$ are:

n	9	15	21	27	51
d	3^4	$2^4\cdot 3^3$	$2^4\cdot 3^4$	$2^2\cdot 3^6$	$2^8\cdot 3^4$
δ	$2^3\cdot 3\cdot 5$	$2^6\cdot 3^2\cdot 5^2\cdot 11$	$2^8\cdot 3^3\cdot 5\cdot 17$	$2^7\cdot 3^2\cdot 5^4\cdot 11\cdot 23$	$2^8\cdot 3^2\cdot 5^4\cdot 23\cdot 47$

In each case, we see by observing the power of 3 in d and δ that d does not divide δ.

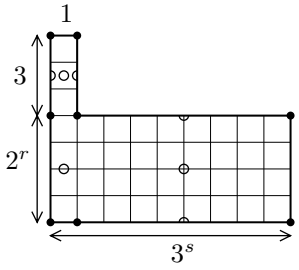
7.4. **Remaining bad cases.** Here we will consider two surfaces S_1 and S_2 in orbit B_n, and for each S_i find some k_i and k_i' such that $\left(\begin{smallmatrix} 1 & k_i \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ k_i' & 1 \end{smallmatrix}\right)$ are in the stabiliser Γ_i of S_i ($i \in \{1, 2\}$). The groups Γ_1 and Γ_2, being conjugate, have the same index d in $\Gamma(1)$ and the same level ℓ. Using $m_i = \ell//k_ik_i'$ will yield a δ_i for each $i \in \{1, 2\}$ and we will show that d cannot divide both δ_1 and δ_2, implying that Γ_{B_n} is not a congruence subgroup.

Take $S_1 = S(1, 2^r, 3, 3^s, 1, 0)$.



Its stabiliser contains $\left(\begin{smallmatrix} 1 & k_1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ k_1' & 1 \end{smallmatrix}\right)$, with $k_1 = 3^s$ and $k_1' = 2^r \cdot (2^r \cdot 3 + 3)$. Note that here k_1' is not the exact vertical cusp width of S_1, but a multiple of it. For $r = 1, 2, 3, 4$, the value of k_1' is respectively $2 \cdot 3^2$, $2^2 \cdot 3 \cdot 5$, $2^3 \cdot 3^3$, $2^4 \cdot 3 \cdot 17$.

Take $S_2 = S(3, 2^r, 1, 3^s, 0, 0)$.



Its stabiliser contains $\left(\begin{smallmatrix} 1 & k_2 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ k_2' & 1 \end{smallmatrix}\right)$, with $k_2 = 3^s$ and $k_2' = 2^r \cdot (2^r + 3)$; again k_2' is not the exact vertical cusp width, but a multiple of it. It equals $2 \cdot 5$, $2^2 \cdot 7$, $2^3 \cdot 11$, $2^4 \cdot 19$, respectively for $r = 1, 2, 3, 4$.

Recall that $n = 2^r \cdot 3^s + 3$, with $s \geqslant 2$.

Here, $d = \frac{3}{16}(n-3)n^2 \prod_{p|n}(1 - \frac{1}{p^2})$. Since 3^2 divides $(n-3)$, it does not divide n. Hence we can rewrite $d = 2^{r-1} \cdot 3^{s+1+2\nu-2} \prod_{p|\frac{n}{3}} p^{2\nu-2}(p^2-1)$.

The choice of $m_i = \ell // k_i k_i'$ leads to $\delta_i = \prod_{p|k_i k_i'} p^{3\lambda-2}(p^2-1)$.

Given the values of $p^2 - 1$ for $p \in \{2, 3, 5, 7, 11, 17, 19\}$ (cf. table),

p	2	3	5	7	11	17	19
p^2-1	3	2^3	$2^3 \cdot 3$	$2^4 \cdot 3$	$2^3 \cdot 3 \cdot 5$	$2^5 \cdot 3^2$	$2^3 \cdot 3^2 \cdot 5$

the prime factors of δ_1 and δ_2 for each $r \in \{1, 2, 3, 4\}$ are:

r	1	2	3	4
δ_1	$2, 3$	$2, 3, 5$	$2, 3$	$2, 3, 17$
δ_2	$2, 3, 5$	$2, 3, 7$	$2, 3, 5, 11$	$2, 3, 5, 19$

If d divides δ_1 and δ_2, we deduce that $\prod_{p|\frac{n}{3}} p^{2\nu-2}(p^2-1)$ can have only 2 and 3 as prime factors. If this is the case, then n has no square factor, and, by Lemma 7.1 (postponed to the end of the section), its prime factors are in $\{3, 5, 7, 17\}$. The integers of the form $3 \cdot 5^a \cdot 7^b \cdot 17^c$ with $a, b, c \in \{0, 1\}$ are 3, 15, 21, 51, 105, 255, 357, 885. The only bad ones are 15, 21, and 51, and these were dealt with in § 7.3.

To complete the proof of Theorem 1, there remains only to prove:

Lemma 7.1. *If p is prime and $p^2 - 1$ has no other prime factors than 2 and 3, then $p \in \{2, 3, 5, 7, 17\}$.*

This follows from the fact that 8 and 9 are the only two consecutive nontrivial powers, a famous long-standing conjecture that was recently proved by Mihăilescu [Mi].

Theorem D (Catalan's Conjecture)**.** *The equation*

$$x^u - y^v = 1,\ x > 0,\ y > 0,\ u > 1,\ v > 1$$

has no other integer solution than $x^u = 3^2,\ y^v = 2^3$.

Proof of the lemma. By Catalan's Conjecture, consecutive powers of 2 and 3 are: (1, 2); (2, 3); (3, 4); (8, 9). Suppose $(p-1)(p+1)$ has no other prime factors than 2 and 3. If p is odd, then exactly one of $p-1$, $p+1$ is a multiple of 4, and the other one is $2{\cdot}3^\alpha$. If $\frac{p-1}{2} = 3^\alpha$, then either $\alpha = 0$, and $p = 3$, or $\alpha = 1$, and $p = 7$. If $\frac{p+1}{2} = 3^\alpha$, then either $\alpha = 1$, and $p = 5$, or $\alpha = 2$, and $p = 17$. □

References

[BlOk] S. Bloch, A. Okounkov. The character of the infinite wedge representation. *Adv. Math.* **149**:1 (2000) 1–60.

[Ca] K. Calta. Veech surfaces and complete periodicity in genus 2. *Preprint.* `arXiv:math.DS/0205163`

[Di] R. Dijkgraaf. Mirror symmetry and elliptic curves. *The moduli space of curves (Texel Island, 1994)*, 149–163, Progr. Math. 129, Birkhäuser Boston, Boston, MA, 1995.

[EsMaSc] A. Eskin, H. Masur, M. Schmoll. Billiards in rectangles with barriers. *Duke Math. J.* **118**:3 (2003) 427–463.

[EsOk] A. Eskin, A. Okounkov. Asymptotics of numbers of branched coverings of a torus and volumes of moduli spaces of holomorphic differentials. *Invent. Math.* **145**:1 (2001) 59–103.

[EsOkPa] A. Eskin, A. Okounkov, R. Pandharipande. The theta characteristic of a branched covering. *Preprint* (2003). `arXiv:math.AG/0312186`

[FLP] A. Fathi, F. Laudenbach, V. Poenaru et al. *Travaux de Thurston sur les surfaces. Astérisque*, **66-67**, Soc. Math. France, 1979, 1991.

[GuJu] E. Gutkin, C. Judge. Affine mappings of translation surfaces: geometry and arithmetic. *Duke Math. J.* **103**:2 (2000) 191–213.

[Ka] E. Kani. The number of genus 2 covers of an elliptic curve. *Preprint* (2003).

[KaZa] M. Kaneko, D. Zagier. A generalized Jacobi theta function and quasimodular forms. *The moduli space of curves (Texel Island, 1994)*, 165–172, Progr. Math. 129, Birkhäuser Boston, Boston, MA, 1995.

[HL] P. Hubert, S. Lelièvre. Prime arithmetic Teichmüller discs in $\mathcal{H}(2)$. To appear in *Isr. J. of Math.*

[Mc1] C. T. McMullen. Billiards and Teichmüller curves on Hilbert modular surfaces. *J. Amer. Math. Soc.* **16**:4 (2003) 857–885.

[Mc2] C. T. McMullen. Teichmüller geodesics of infinite complexity. *Acta Math.* **191**:2 (2003) 191–223.

[Mc3] C. T. McMullen. Dynamics of $\mathrm{SL}_2\,\mathbf{R}$ over moduli space in genus two. *Preprint* (2003).

[Mc4] C. T. McMullen. Teichmüller curves in genus two: discriminant and spin. *Preprint* (2004).

[Mi] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *Preprint* (2002).

[Mö] M. Möller. Teichmüller curves, Galois actions and $\widehat{GT}$-relations. *Preprint* (2003). arXiv:math.AG/0311308

[Ra] R. A. Rankin. *Modular forms and functions.* Cambridge University Press, Cambridge-New York-Melbourne, 1977.

[Schmi] G. Schmithüsen. An algorithm for finding the Veech group of an origami. To appear in *Experiment. Math.*

[Ve] W. A. Veech. Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards. *Invent. Math.* **97**:3 (1989) 553-583.

[Wo] K. Wohlfahrt. An extension of F. Klein's level concept. *Illinois J. Math.* **8** (1964) 529-535.

[Zo] A. Zorich. Square tiled surfaces and Teichmüller volumes of the moduli spaces of abelian differentials. *Rigidity in dynamics and geometry (Cambridge, 2000)*, 459–471, Springer, Berlin, 2002.

[Zv] D. Zvonkine. *Énumération des revêtements ramifiés des surfaces de Riemann.* Thèse de doctorat, Université Paris-Sud, Orsay, 2003.

IML, UMR CNRS 6206, Université de la Méditerranée, Campus de Luminy, case 907, 13288 Marseille cedex 9, France
E-mail address: hubert@iml.univ-mrs.fr

Irmar, UMR CNRS 6625, Université de Rennes 1, Campus Beaulieu, 35042 Rennes cedex, France;
I3M, UMR CNRS 5149, Université Montpellier 2, case 51, Place Eugène Bataillon, 34095 Montpellier cedex 5, France;
IML, UMR CNRS 6206, Université de la Méditerranée, Campus de Luminy, case 907, 13288 Marseille cedex 9, France.
E-mail address: samuel.lelievre@polytechnique.org
URL: http://carva.org/samuel.lelievre/