

THE HURWITZ PROBLEM FOR ABELIAN DIFFERENTIALS

JULIEN BOULANGER, RODOLFO GUTIÉRREZ-ROMO, AND ERWAN LANNEAU

ABSTRACT. Fix $g \geq 2$. Let $t(g)$ be the maximal order of the translation group among all genus- g abelian differentials. By work of Schlage-Puchta and Weitze-Schmithüsen, $t(g) \leq 4(g-1)$. They also classify the g attaining this bound. We assume g is outside this class.

We first prove that either $t(g) = (2(m+1)/m)(g-1)$ for some $m \in \mathbb{N} \setminus \{0\}$, when regular genus- g origamis exist, or $t(g) = 2(g-1)$, when they do not exist.

In the former case, only some values of $m > 1$ are realizable; $m = 5$ is the smallest. The resulting set of genera, those satisfying $t(g) = (12/5)(g-1)$, contains infinitely long arithmetic progressions. The same holds for any odd prime m congruent to 2 modulo 3.

In the latter case, “many” strata of the form $\mathcal{H}(g-1, g-1)$, $\mathcal{H}(2k^q)$ or $\mathcal{H}(k^{2q})$, where $k \geq 1$ is an integer and q is prime, contain no regular origamis; we derive a complete classification. As an application, we exhibit infinite families of genera g for which $t(g) = 2(g-1)$: $g = p+1$ for prime $p \geq 5$; $g = p^2+1$ for prime, but not Sophie Germain prime, p ; and $g = pq+1$, for distinct primes $p, q \geq 5$.

1. INTRODUCTION

In 1892, Hurwitz [Hur92] obtained a celebrated upper bound of $84(g-1)$ on the maximal number of automorphisms a genus- g compact Riemann surface may possess. Several decades later, between 1968 and 1969, Accola [Acc68] and Maclachlan [Mac69b] independently obtained a lower bound of $8(g+1)$. Both bounds are known to be sharp in the sense that they are attained for infinitely many g .

A finer question is: what is the maximal number of automorphisms of genus- g compact Riemann surfaces? The answer is known for small g , and for several infinite families of genera, although it is not known in full generality [Kil70; BJ05; BG21; MZ24].

A related question is counting automorphisms with additional restrictions. This subject has been extensively studied and several versions have been considered, such as counting automorphisms of specific families of compact Riemann surfaces (e.g. p -gonal surfaces [CI10; BCI13], pseudo-real surfaces [BCC20], or others [IRR21]), or those with a prescribed group structure (e.g. cyclic or abelian automorphism groups [Wim95; Har66; Mac65; HMQ24] or with a specific number of elements [Kul91; CR21; IRR21]).

This article focuses on the automorphisms of a compact Riemann surface that also preserve a given holomorphic 1-form, that is, an *abelian differential*.

Date: October 2025.

2020 Mathematics Subject Classification. 30F30, 14H37, 32G15, 20D60.

Key words and phrases. Riemann surface, abelian differential, translation group, automorphism group, origami.

A Riemann surface X endowed with a nonzero abelian differential ω is called a *translation surface* [AM24; DHV24]. For this reason, we use the term *translation group* of (X, ω) for the subgroup of $\text{Aut}(X)$ that preserves ω , that is,

$$\text{Trans}(X, \omega) = \{f \in \text{Aut}(X) \mid f^*\omega = \omega\}.$$

By slightly abusing notation, we often omit the differential ω and refer to the pair (X, ω) simply as X and to its translation group as $\text{Trans}(X)$. We will always assume X to be compact.

More precisely, our aim is to study the quantity

$$\mathfrak{t}(g) = \sup \left\{ |\text{Trans}(X, \omega)| \mid \begin{array}{l} X \text{ is a genus-}g \text{ compact Riemann surface} \\ \text{and } \omega \text{ is a nonzero abelian differential on } X \end{array} \right\}.$$

The investigation on this quantity was initiated in 2017 by Schlage-Puchta and Weitze-Schmithüsen [SW17]. They first show that $\mathfrak{t}(g) \leq 4(g-1)$ for every $g \geq 2$. In addition, they prove that the pairs (X, ω) attaining this bound are essentially regular covers, branched over a single point, of pairs (Y, η) for some Y of genus 1. Such pairs (X, ω) are sometimes referred to as *regular origamis*. More precisely, they prove, using the Riemann–Hurwitz formula, that the upper bound $4(g-1)$ is attained if and only if (X, ω) is a regular origami and the abelian differential ω has exactly $2g-2$ zeros of order one. Finally, they completely characterize the $g \geq 2$ such that $\mathfrak{t}(g) = 4(g-1)$ as those with $g-1$ divisible by 2 or 3.

Our goal is to generalize these results. By refining their application of the Riemann–Hurwitz formula, we show:

Theorem A (Theorem 3.1). *Let $g \geq 2$. The number $\mathfrak{t}(g)$ is always of the form*

$$\mathfrak{t}(g) = \mathfrak{c}(g)(g-1).$$

where the “slope” $\mathfrak{c}(g)$ is either 2, or has the form $2(m+1)/m$ for some integer $m = \mathfrak{m}(g) \geq 1$ such that $m \mid 2(g-1)$, $3 \nmid m$, and $4 \nmid m$.

Finally, the case $\mathfrak{c}(g) = 2$ arises if and only if no genus- g regular origamis exist.

In particular, the number $\mathfrak{c}(g)$ belongs to the set

$$\left\{ 2 < \dots < \frac{36}{17} < \frac{15}{7} < \frac{28}{13} < \frac{24}{11} < \frac{11}{5} < \frac{16}{7} < \frac{12}{5} < 3 < 4 \right\}.$$

We will see that some of these numbers, such as 3 and $16/7$, do not actually occur.

Notation. In the case where $\mathfrak{c}(g) = 2$, we will say that $\mathfrak{m}(g) = \infty$. This notation is justified by the fact that $\lim_{m \rightarrow \infty} 2(m+1)/m = \inf_{m \geq 1} 2(m+1)/m = 2$.

Moreover, for (possibly infinite) $m \geq 1$, we define the set $\mathbf{G}(m)$ of genera $g \geq 2$ for which $\mathfrak{m}(g) = m$, that is,

$$\mathbf{G}(m) = \{g \geq 2 \mid \mathfrak{m}(g) = m\} = \begin{cases} \left\{ g \geq 2 \mid \mathfrak{t}(g) = \frac{2(m+1)}{m}(g-1) \right\} & \text{if } m < \infty \\ \{g \geq 2 \mid \mathfrak{t}(g) = 2(g-1)\} & \text{if } m = \infty. \end{cases}$$

Observe that $\mathbf{G}(1)$ is completely characterized by the work of Schlage-Puchta and Weitze-Schmithüsen. Moreover, Theorem A implies that $\mathbf{G}(m)$ is empty when $3 \mid m$ or $4 \mid m$. Our aim is to study the sets $\mathbf{G}(m)$ for m outside of these cases.

We start by determining that $\mathbf{G}(m)$ is empty for some particular values of m .

Theorem B (Theorems 4.1 and 4.3). *The sets $\mathbf{G}(2)$ and $\mathbf{G}(2^\alpha - 1)$ are empty for each $\alpha \geq 2$.*

As a consequence, the smallest integer m , outside of the case $m = 1$ [SW17], such that $G(m)$ is nonempty, satisfies $m \geq 5$. We prove that $G(5)$ is infinitely large; the proof also works for other prime m :

Theorem C (Theorem 5.1). *If m is an odd prime and is congruent to 2 modulo 3, then $G(m)$ contains explicit infinitely long arithmetic progressions. In particular, $G(5)$ contains all $g \geq 2$ of the form*

$$g = \frac{5kp(p-1)(p+1)}{24} + 1$$

where p is prime, $p \bmod 72$ is 11, 13, 59, or 61, and $k \equiv \pm 1 \pmod 6$.

To prove Theorem C, we construct regular origamis with a translation group of the form $\mathrm{PSL}(2, p) \times \mathbb{Z}/k\mathbb{Z}$ and show that they achieve the maximal number of translations in genus g .

Remark 1.1. *Numerical experiments suggest that the density of $G(5)$ is well-defined and at least 0.001957.*

Recall now that a *Sophie Germain prime* is a prime p such that $2p + 1$ is also prime. Our next result shows that the set $G(\infty)$ is also infinitely large:

Theorem D (Theorem 6.1). *We have that $g \in G(\infty)$ for each g of any of the following forms:*

- $g = p + 1$, where $p \geq 5$ is prime;
- $g = p^2 + 1$, where p is prime, but is not a Sophie Germain prime;
- $g = pq + 1$, where $p, q \geq 5$ are distinct primes.

In particular, Theorem D shows that, for infinitely many $g \geq 2$, no genus- g regular origamis exist.

Remark 1.2. *A follow-up question is if regular origamis exist in genus $g = pqr + 1$ when $p, q, r \geq 5$ are distinct primes. We know that both cases can arise: they exist if $g = 456 = 5 \cdot 7 \cdot 13 + 1$ (from Theorem C with $m = 5$, $p = 13$, and $k = 1$), and do not exist if $g = 386 = 5 \cdot 7 \cdot 11 + 1$ (from computer experiments).*

The previous theorem suggests focusing on the case of Sophie Germain primes, allowing us to show the following:

Theorem E (Theorem 6.1 and Corollary 6.6). *If $p \geq 5$ is a Sophie Germain prime, then $p^2 + 1 \in G(2p)$. Moreover, $\ell p^2 + 1 \notin G(\infty)$ for every integer $\ell \geq 1$.*

If p is a Sophie Germain prime, the first part of the statement shows, in particular, that the set $G(2p)$ is nonempty. The second part is equivalent to the existence of regular origamis of genus $g = \ell p^2 + 1$.

Remark 1.3. *Whenever p is a Sophie Germain prime, Theorem E shows, in particular, that regular origamis exist in genus $g = p^\alpha + 1$ for every $\alpha \geq 2$.*

Assume now that p is prime, but not a Sophie Germain prime. Theorem D shows that regular origamis do not exist in genus $g = p^2 + 1$. It is natural to ask if they exist in genus $g = p^\alpha + 1$ for $\alpha > 2$. We know that they do not exist, for example, if $p = 7$ and $\alpha = 3$, that is, when $g = 344 = 7^3 + 1$ (from computer experiments).

The proofs of Theorems D and E are based on analyzing the existence of regular origamis whose associated abelian differentials have zeros of specific types, that is,

belonging to particular *strata*. We focus on the cases $g = p + 1$ and $g = pq + 1$ primarily because, in these situations, the Euler characteristic $2 - 2g$ admits a simple prime factorization, and the problem reduces to finding groups with a cyclic subgroup of prime or twice-prime index.

Let us point out that the full automorphism group (and some of its subgroups) of a Riemann surface of genus $g = p + 1$ and $g = p^2 + 1$ has been considered before in the literature [BJ05; IJR21; CR21]. While the group-theoretic setting differs, the simple factorization of the Euler characteristic similarly facilitates the analysis.

Remark 1.4. *As a consequence of Theorems A to E, an updated list of the possible slopes $c(g)$ such that $\mathfrak{t}(g) = c(g)(g - 1)$ is:*

$$\left\{ 2 < \cdots < \frac{52}{25} < \frac{48}{23} < \frac{23}{11} < \frac{40}{19} < \frac{36}{17} < \frac{15}{7} < \frac{28}{13} < \frac{24}{11} < \frac{11}{5} < \frac{12}{5} < 4 \right\}.$$

We do not know if the slopes $28/13$, $15/7$, $40/19$, or $52/25$ are realizable.

1.1. Context and motivations. This article lies at the intersection between the study of automorphism groups of compact Riemann surfaces and the study of abelian differentials. Whereas the study and classification of the automorphism groups of compact Riemann surfaces is a classical problem that has attracted considerable interest since the late nineteenth century, the case of abelian differentials has cemented its relevance only during the last decades, especially in relation to the study of moduli spaces [AM24; DHV24].

The subgroup $\text{Trans}(X, \omega)$ of $\text{Aut}(X)$ associated with an abelian differential ω has been studied in several recent works [SW17; Hid21; FT23]. As in the general case, every finite group can be achieved as the translation group of a pair (X, ω) [Hid21]. However, when the genus g of X or the orders of the zeros of ω are prescribed, this group had not, to the best of our knowledge, been investigated outside two cases: the “upper bound” case $\mathfrak{t}(g) = 4(g - 1)$ [SW17], and the case where it is a p -group [FT23].

Geometric interpretation. This work was originally motivated by the connection between abelian differentials and flat geometry. As previously mentioned, a Riemann surface X with a nonzero abelian differential ω is also called a *translation surface*. Translation surfaces admit other equivalent definitions, which also provide equivalent definitions of the translation group. A more combinatorial definition is a collection of polygons on the plane with side identifications by translations up to scissors congruences. Equivalently, it is a genus- g topological surface S endowed with a *translation atlas*, that is, an atlas whose transition functions are translations, except at finitely many points called singularities. This atlas allows us to define the total area of X . Since we assume X to be compact, this area is finite.

Using the translation atlas, we may also define the group of *affine homeomorphisms* $\text{Aff}(X, \omega)$ of a translation surface as the subgroup of $\text{Homeo}^+(S)$ with constant derivative in the atlas. This group is well-defined since any matrix remains constant when conjugated by a translation. By taking the derivative of an affine homeomorphism, we obtain the *derivative map* $D: \text{Aff}(X, \omega) \rightarrow \text{SL}(2, \mathbb{R})$. The image of this map is known as the *Veech group* $\text{SL}(X, \omega)$ of (X, ω) and records all possible matrices that can be lifted to affine homeomorphisms. The kernel of this map is exactly the translation group $\text{Trans}(X, \omega)$.

Regular origamis. One of the simplest examples of a translation surface is the unit square torus $\mathbb{T} = \mathbb{R}^2/\mathbb{Z}^2$, equipped with the 1-form dz . By considering covers of $\mathbb{T}$ branched over a single point (given by the points of integer coordinates), we obtain an *origami* or *square-tiled surface*. The differential also lifts to the covering surface.

A particular case of origamis of special interest is *regular origamis* (also known as *normal origamis*): those for which the cover to the unit torus is normal. Regular origamis can also be defined in terms of their translation group. Indeed, given a finite group G generated by two elements x and y , we can define a regular origami by labeling unit squares with the elements of G , and declaring that rightward gluings are given by multiplication by x , and upward gluings, by y . Then, the translation group of the resulting origami is isomorphic to G .

It turns out regular origamis constitute the translation surfaces with the largest translation group. Namely, a translation surface is a regular origami if and only if its translation group has more than $2(g-1)$ elements (see Lemma 3.2). Furthermore, if (X, ω) is a regular origami, the order $\text{Trans}(X, \omega)$ only depends on the order m of the zeros of ω . Indeed, it equals $(2(m+1)/m)(g-1)$. This number can be computed from the generators $x, y \in G$ as $m = \text{ord}([x, y]) - 1$. See Section 3.3.

Strata of abelian differentials. In geometric terms, the zeros of the abelian differential ω correspond to the singularities of the translation surface (X, ω) . In fact, the (moduli) space of translation surfaces is partitioned into *strata* prescribing the orders of the zeros of ω .

Notation. As standard in the theory, we will denote the set of genus- g translation surfaces whose abelian differential has s_i zeros of order k_i , for $i \in \{1, \dots, \ell\}$, by $\mathcal{H}_g(k_1^{s_1}, \dots, k_\ell^{s_\ell})$. As such, a superscript in this notation will always mean a multiplicity (and never an exponent). We refer to such a set as a stratum.

The Riemann–Roch Theorem relates the singularity data and the genus:

$$(1.5) \quad 2g - 2 = \sum_{i=1}^{\ell} s_i k_i.$$

Hence, we often omit the subscript g .

The work of Schlage-Puchta and Weitze-Schmithüsen [SW17] focuses on regular origami in the stratum $\mathcal{H}(1^{2g-2})$. To obtain the first part of Theorem B, and Theorems D and E, we study the existence of regular origamis in several other strata. We obtain:

Theorem F. *Let $k, \ell \geq 1$ be integers. Then:*

- $\mathcal{H}(k^\ell)$, for even k, ℓ , contains regular origamis (Section 3.3.2 Example (2));
- $\mathcal{H}(2^\ell)$, for odd ℓ , contains regular origamis if and only if ℓ is divisible by 9 (Theorem 4.2);
- $\mathcal{H}(k^2)$, for odd k , contains no regular origamis (Lemma 6.3);
- $\mathcal{H}(k^4)$ contains regular origamis (Section 3.3.2 Example (1));
- $\mathcal{H}(k^6)$, when $k \equiv 1 \pmod{4}$, contains regular origamis if and only if every prime factor of $(k+1)/2$ is congruent to 1 modulo 3 (Theorem 6.8); and
- $\mathcal{H}(k^6)$, when $k \equiv 3 \pmod{4}$, contains regular origamis if and only if every prime factor of $(k+1)/4$ is congruent to 1 modulo 3 (Theorem 6.8);

Furthermore, if q is an odd prime, then:

- $\mathcal{H}(k^{2q})$, for odd k and $q > 3$, contains no regular origamis (Theorem 6.8);
and
- $\mathcal{H}(2k^q)$ contains regular origamis if and only if every prime factor of $2k+1$ is congruent to 1 modulo q (Theorem 6.4).

Remark 1.6. From Equation (1.5), translation surfaces in $\mathcal{H}(k^\ell)$ have genus g satisfying $2g - 2 = k\ell$. In particular, k and ℓ cannot both be odd.

In the case of $\ell = 2$, we have $\mathcal{H}(k^2) = \mathcal{H}(g-1, g-1)$ for genus $g = k+1$. The previous theorem states that this stratum contains regular origamis if and only if g is odd. Similarly, surfaces in $\mathcal{H}(2^\ell)$ have genus $g = \ell+1$. Thus, this stratum contains regular origamis if and only if $g-1$ is divisible by 2 or 9.

This result is somewhat complementary to the work of Flake and Thevis [FT23], which investigates the strata in which a regular origamis whose translation group is a p -group may occur. Together with the classification of $\mathbf{G}(1)$ [SW17], their work shows that $1 < \mathfrak{m}(g) \leq p^\alpha - 1$ for every g of the form $g = p^\beta(p^\alpha - 1)/2 + 1$, where $p > 3$ is prime, $\alpha \geq 1$ and $\beta \geq \alpha + 1$. In contrast, Theorem F does not make assumptions about the form of the group, but only deals with specific strata.

It is known that a regular origami constructed from a group G and two generators x, y belongs to the stratum $\mathcal{H}(k^\ell)$ if and only if the cyclic subgroup $H = \langle [x, y] \rangle$ has order $k+1$ and index ℓ in G [SW17; FT23] (see Section 3.3). As a consequence, Theorem F reduces to a classification problem for groups of order $(k+1)\ell$ generated by two elements whose commutator has order $k+1$. In the case where $k+1$ and ℓ have simple prime factorizations, we are able to provide a full classification.

Furthermore, we can further classify the translation groups of regular origamis in the strata $\mathcal{H}(k^6)$ when k is odd, and $\mathcal{H}(2k^q)$. Indeed, the former case only admits groups of the form $(\mathbb{Z}/\lambda\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$, or $(\mathbb{Z}/\lambda\mathbb{Z} \times \mathbb{Q}_8) \rtimes \mathbb{Z}/3\mathbb{Z}$; the latter case only admits groups of the form $\mathbb{Z}/(2k+1)\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$. See Theorems 6.4 and 6.8 for more details.

Acknowledgments. The first author was supported by Centro de Modelamiento Matemático (CMM) BASAL fund FB210005 for center of excellence from ANID-Chile.

The second author is grateful to Ferrán Valdez for introducing them to the original article by Schlage-Puchta and Weitze-Schmithüsen, to Gabriela Weitze-Schmithüsen for interesting discussions, and is supported by Centro de Modelamiento Matemático (CMM) BASAL fund FB210005 for center of excellence from ANID-Chile, and the FONDECYT Regular N°1221934 and N°1250798 grants from ANID-Chile.

The third author has been partially supported by the LabEx PERSYVAL-Lab (ANR-11-LABX-0025-01) funded by the French program Investissement d’avenir and by the CNRS. The third author would like to thank the Center for Mathematical Modeling (CMM) at Universidad de Chile for excellent working conditions.

We are also grateful to Milagros Izquierdo and Sebastián Reyes-Carocca for pointing us to interesting references on automorphism groups of Riemann surfaces, and to David Grimm for the beautiful argument in the proof of Lemma 5.4.

2. BACKGROUND AND PRELIMINARIES

In this section, we will first provide the necessary context in group theory. We will also state and prove a series of simple lemmas that will be useful later.

2.1. Basic facts about groups. Throughout the article, we will mainly deal with finite groups. Given a finite group G , its *order* is its number of elements, which will be denoted by $|G|$. If $H \leq G$ is a subgroup of G , its *index* is the number of cosets of H inside G , equals $|G|/|H|$, and is denoted by $(G : H)$ (other common notations include $[G : H]$ and $|G : H|$).

We start with some well-known facts about subgroups.

Lemma 2.1. *Let G be a finite group and let $H, K \leq G$ be subgroups of G . We have that*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Consider the group $H \times K$ acting on the set HK via $(h, k)x = h x k^{-1}$. The action is transitive and the stabilizer of $1 \in HK$ is isomorphic to $H \cap K$. Hence, by the orbit-stabilizer theorem, we get

$$|HK| \cdot |H \cap K| = |H \times K| = |H||K|.$$

Solving for $|HK|$ yields the desired result. $\square$

Lemma 2.2. *Let G be a group and let $H \leq G$ be an index-two subgroup. Then, H is normal in G .*

Lemma 2.3. *Let G be a group and let $H \leq G$ be an index-two subgroup. If $x, y \in G \setminus H$, then $xy \in H$. In particular, $x^2 \in H$ for every $x \in G$.*

Proof. The group H is normal by the previous lemma. Thus, if $x, y \in G \setminus H$, we have that x and y project to the only nontrivial element of $G/H \simeq \mathbb{Z}/2\mathbb{Z}$. Hence, $xyH = H$, so $xy \in H$.

Finally, if $x \in G \setminus H$, we get that $x^2 \in H$. If $x \in H$, we also have $x^2 \in H$. $\square$

We recall that a subgroup $H \leq G$ is *characteristic* if it is preserved (setwise) by every automorphism of G , and continue with a simple fact stating that a subgroup of a cyclic group is cyclic and uniquely determined by its order:

Theorem 2.4. *Let G be a finite cyclic group. We have that every subgroup of G is cyclic. Moreover, there exists a unique such subgroup of order k for every divisor k of $|G|$. In particular, every subgroup of G is characteristic.*

Lemma 2.5. *Let G be a group, and assume that H is a normal subgroup of G . If K is a characteristic subgroup of H , then K is normal in G .*

Proof. Consider the action $\varphi: G \rightarrow \text{Aut}(H)$ given by conjugation. This morphism is well-defined since H is normal in G . Since K is characteristic in H , we deduce that $\varphi(g)$ stabilizes K for every $g \in G$. Thus, $K \triangleleft G$. $\square$

If $g, h \in G$, we denote their *commutator* by $[g, h] = ghg^{-1}h^{-1}$. Recall that the *commutator subgroup* of G (also known as the *derived subgroup* of G) is the group generated by its commutators. We denote it by G' or $[G, G]$. The commutator subgroup is characteristic, and G/H is abelian whenever $G' \leq H \triangleleft G$ (particularly when $H = G'$).

Now, it is possible to iterate the derivation process and consider the *derived series* associated with G :

$$G^{(0)} = G, \quad G^{(1)} = [G^{(0)}, G^{(0)}], \quad G^{(2)} = [G^{(1)}, G^{(1)}], \quad \dots$$

A group is called *solvable* if its derived series eventually reaches the trivial group. The celebrated results of Burnside and Feit–Thompson give criteria on the order of a group for it to be solvable:

Theorem 2.6 (Burnside’s theorem [Bur04; Isa08, Theorem 7.8]). *If p, q are prime and α, β are nonnegative integers, then every group of order $p^\alpha q^\beta$ is solvable.*

Theorem 2.7 (Feit–Thompson [FT62; FT63]). *Any finite group of odd order is solvable.*

Roughly speaking, solvable groups are those that can be split into abelian blocks. Examples of nonsolvable groups include (nontrivial) *perfect groups*: groups G with $G' = G$. These results show that perfect groups can only exist for some orders.

Recall that the *center* of G , denoted $\mathbf{Z}(G)$, is the subgroup of those elements of G commuting with every other element of G . We include two facts about the center of a perfect group for later use:

Lemma 2.8. *Assume that H is a cyclic normal subgroup of a finite group G . Then, $H \leq \mathbf{Z}(G')$. In particular, if G is perfect, then $H \leq \mathbf{Z}(G)$.*

Proof. Since H is normal, the action by G on H by conjugation is well-defined, and induces a homomorphism $G \rightarrow \text{Aut}(H)$. Since H is cyclic, the group $\text{Aut}(H)$ is abelian and, thus, this homomorphism factors through the abelianization G/G' . In other words, H is contained in its kernel, namely $H \leq \mathbf{Z}(G')$. $\square$

Lemma 2.9 (Grün’s Lemma [Ros94, p. 61]). *If G is a perfect group, then $G/\mathbf{Z}(G)$ has a trivial center.*

2.2. Semidirect products and their commutator subgroup. Recall that a *semidirect product* between groups N and H via a homomorphism $\varphi: H \rightarrow \text{Aut}(N)$ is the group G of with underlying set $N \times H$ and the operation

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2).$$

We denote it by $G = N \rtimes_\varphi H$. We will sometimes omit the map φ .

We will encounter commutator subgroups of semidirect products. The following lemma follows directly from the definitions:

Lemma 2.10. *The commutator subgroup of a semidirect product $G = N \rtimes H$ is a subgroup of $N \rtimes H'$, where H' is the commutator subgroup of H .*

A particular case is a semidirect product of cyclic groups. If k, ℓ are integers and $d^\ell \equiv 1 \pmod k$, we can define $\varphi_d: \mathbb{Z}/\ell\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/k\mathbb{Z})$ by declaring that $\varphi_d(1)$ maps 1 to d , and extending by cyclicity. We denote $\mathbb{Z}/k\mathbb{Z} \rtimes_{\varphi_d} \mathbb{Z}/\ell\mathbb{Z}$ simply as $\mathbb{Z}/k\mathbb{Z} \rtimes_d \mathbb{Z}/\ell\mathbb{Z}$. More explicitly:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 + d^{b_1} a_2, b_1 + b_2).$$

Lemma 2.11. *In the context above, $\mathbb{Z}/k\mathbb{Z} \rtimes_d \mathbb{Z}/\ell\mathbb{Z}$ has a presentation:*

$$\langle x, y \mid x^k = y^\ell = 1 \text{ and } [y, x] = x^{d-1} \rangle.$$

Proof. Take $x = (1, 0)$ and $y = (0, 1)$. $\square$

Semidirect products of cyclic groups fall under the more general class of *metacyclic groups*. These are defined as extensions of cyclic groups by cyclic groups, meaning that they obey a short exact sequence

$$1 \rightarrow \mathbb{Z}/k\mathbb{Z} \rightarrow G \rightarrow \mathbb{Z}/\ell\mathbb{Z} \rightarrow 1,$$

and have a presentation

$$G = \langle x, y \mid x^k = 1, y^\ell = x^r \text{ and } [y, x] = x^{d-1} \rangle,$$

where, as before, $d^\ell = 1 \pmod k$ and, moreover, $k \mid r(d-1)$ and $r \mid k$. In this context, a metacyclic group is a semidirect product of cyclic groups if and only if $r = k$. Every element of a metacyclic group admits a normal form: it can be written uniquely as $y^\alpha x^\beta$ for $0 \leq \alpha < \ell$ and $0 \leq \beta < k$. Indeed, the group $K = \langle x \rangle$ is normal, cyclic of order k , and G/K has order ℓ . Indeed, the cosets $y^\alpha(G/K)$ are distinct for distinct α .

The following lemma is well-known:

Lemma 2.12. *Using the presentation above, the commutator subgroup of a metacyclic group G is $G' = \langle x^{d-1} \rangle$. In the particular case of $G = \mathbb{Z}/k\mathbb{Z} \rtimes_d \mathbb{Z}/\ell\mathbb{Z}$, we have $G' \simeq \mathbb{Z}/t\mathbb{Z} \leq \mathbb{Z}/k\mathbb{Z}$, where $t = k/\gcd(d-1, k)$.*

Proof. Let $H = \langle x^{d-1} \rangle$. Since $x^{d-1} = [y, x]$, we have $H \leq G'$. We will show that $G' \leq H$.

We start by showing that, if $\alpha, \beta \in \mathbb{Z}$, then:

$$y^\alpha x^\beta y^{-\alpha} = x^{\beta d^\alpha}.$$

First, from the relation $[y, x] = x^{d-1}$ we get $xyx^{-1} = x^d$, so

$$y^\alpha x y^{-\alpha} = y^{\alpha-1} x^d y^{-\alpha+1} = (y^{\alpha-1} x y^{-\alpha+1})^d.$$

Inductively,

$$y^\alpha x y^{-\alpha} = x^{d^\alpha}$$

and, therefore,

$$y^\alpha x^\beta y^{-\alpha} = (y^\alpha x y^{-\alpha})^\beta = x^{\beta d^\alpha}.$$

Now, we have that

$$[y^\alpha, x^\beta] = (y^\alpha x^\beta y^{-\alpha}) x^{-\beta} = x^{\beta d^\alpha} x^{-\beta} = x^{\beta(d^\alpha-1)} = (x^{d^\alpha-1})^\beta.$$

Moreover,

$$x^{d^\alpha-1} = (x^{d-1})^{1+d+d^2+\dots+d^{\alpha-1}} \in H,$$

so $[y^\alpha, x^\beta] \in H$.

Finally, if $\alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathbb{Z}$, we have:

$$\begin{aligned} [y^{\alpha_1} x^{\beta_1}, y^{\alpha_2} x^{\beta_2}] &= y^{\alpha_1} x^{\beta_1} y^{\alpha_2} x^{\beta_2} x^{-\beta_1} y^{-\alpha_1} x^{-\beta_2} y^{-\alpha_2} \\ &= (y^{\alpha_1} x^{\beta_1} y^{-\alpha_1}) (y^{\alpha_1+\alpha_2} x^{\beta_2-\beta_1} y^{-(\alpha_1+\alpha_2)}) (y^{\alpha_2} x^{-\beta_2} y^{-\alpha_2}) \\ &= x^{\beta_1 d^{\alpha_1}} x^{(\beta_2-\beta_1)d^{\alpha_1+\alpha_2}} x^{-\beta_2 d^{\alpha_2}} \\ &= x^{-(\beta_1 d^{\alpha_1})(d^{\alpha_2}-1)} x^{(\beta_2 d^{\alpha_2})(d^{\alpha_1}-1)} \\ &= (x^{d-1})^{(-\beta_1 d^{\alpha_1})(1+d+\dots+d^{\alpha_2-1})+(\beta_2 d^{\alpha_2})(1+d+\dots+d^{\alpha_1-1})} \in H. \end{aligned}$$

In the particular case where $G = \mathbb{Z}/k\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$, we get that $G' = \langle (d-1, 0) \rangle$. The order of $(d-1, 0)$ is exactly $t = k/\gcd(d-1, k)$, so $G' \simeq \mathbb{Z}/t\mathbb{Z}$. $\square$

A fundamental tool in the theory of finite groups is the following result of Schur and Zassenhaus, which in some cases exhibits a group as a semidirect product.

Theorem 2.13 (Schur–Zassenhaus [Isa08, Section 3B]). *Let G be a finite group. Let $H \triangleleft G$ be a normal subgroup of G whose order is coprime to its index in G . Then, G can be written as a semidirect product $G \simeq H \rtimes G/H$.*

In view of this result, it is natural to look for normal subgroups of prime order or normal subgroups whose index is a maximal power of a prime. This is the content of the next subsection.

2.3. Basic facts about p -groups. Given a prime p , a finite group G is a p -group if its order is p^α for some $\alpha \in \mathbb{N}$. We will use several facts about p -groups.

Lemma 2.14 ([Isa08, Corollary 1.24]). *If G is a p -group of order p^α , then G contains a normal subgroup of order p^β for each $0 \leq \beta \leq \alpha$.*

This allows us to prove:

Corollary 2.15. *If G is a p -group of order at least p^2 , then $(G : G') \geq p^2$.*

Proof. Assume that the order of G is p^α for $\alpha \geq 2$. By Lemma 2.14, there exists a normal subgroup H of G of order $p^{\alpha-2}$. In particular $(G : H) = p^2$. The group G/H has order p^2 , so it is abelian. Since G' is the smallest normal subgroup of G such that G/G' is abelian, we get $G' \leq H$. Consequently, $(G : G') \geq (G : H) = p^2$. $\square$

The study of p -groups is central to understanding the structure of finite groups. A cornerstone result is Sylow's theorems. They state that every finite group has subgroups with a maximal prime-power order and derive some of their properties. Given a finite group G and a prime number p , write $|G| = p^\alpha k$ for k coprime to p . Then, a subgroup of G of order p^α is called a *Sylow p -subgroup* of G . We have:

Theorem 2.16. [Isa08, Theorems 1.7, 1.12, 1.17] *Let G be a finite group and p be a prime number. Then,*

- *there exists at least one Sylow p -subgroup of G ;*
- *all such groups are conjugate; and*
- *the number n_p of these groups satisfies $n_p \equiv 1 \pmod{p}$.*

In fact, Hall generalized this result to collections of prime numbers in the case where G is solvable. More precisely, given a collection π of prime numbers dividing $|G|$, a π -Hall subgroup of G is a subgroup H whose order is a multiple of every prime in π and whose index is coprime to every prime in π . Hall [Hal28] showed that every solvable group contains a π -Hall subgroup, namely:

Theorem 2.17. [Isa08, Theorem 3.13] *Suppose G is a finite solvable group and let π be a collection of primes dividing $|G|$. Then:*

- *there exists a π -Hall subgroup of G ; and*
- *all such groups are conjugate.*

Furthermore, the number of Hall subgroups is of the form

$$1 + \sum_{p \in \pi} a_p p$$

for some integers $a_p \geq 0$ [SW17, Lemma 15].

As previously mentioned, understanding the Sylow or Hall subgroups of a group provides deeper insight into its structure. Many of the groups we consider will contain, for any prime p dividing its order, a cyclic subgroup of index p inside any of their Sylow p -subgroups. The p -groups containing a cyclic subgroup of index p were classified by Burnside. Here we will state this result for $p = 2$.

Theorem 2.18 ([Bro94, p. IV.4; CD14, Proposition 10.1; Rob96, §5.3.4]). *The only finite 2-groups containing a cyclic subgroup of index two are:*

- (1) $\mathbb{Z}/2^\alpha\mathbb{Z}$ for $\alpha \geq 1$;
- (2) $\mathbb{Z}/2^{\alpha-1}\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for $\alpha \geq 2$;
- (3) $M_{2^\alpha} = \mathbb{Z}/2^{\alpha-1}\mathbb{Z} \rtimes_d \mathbb{Z}/2\mathbb{Z}$, where $d = 2^{\alpha-2} + 1$, for $\alpha \geq 3$.
- (4) The dihedral group $D_{2^\alpha} = \mathbb{Z}/2^{\alpha-1}\mathbb{Z} \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$, for $\alpha \geq 3$;
- (5) $SD_{2^\alpha} = \mathbb{Z}/2^{\alpha-1}\mathbb{Z} \rtimes_d \mathbb{Z}/2\mathbb{Z}$, where $d = 2^{\alpha-2} - 1$, for $\alpha \geq 4$; and
- (6) The dicyclic group Dic_{2^α} , for $\alpha \geq 3$.

The dicyclic group Dic_{2^α} is not a semidirect product of cyclic groups, but it is a metacyclic group. Concretely, it has a presentation:

$$Dic_{2^\alpha} = \langle x, y \mid x^{2^{\alpha-1}} = 1, y^2 = x^{2^{\alpha-2}} \text{ and } [y, x] = x^{-2} \rangle.$$

In particular, its commutator subgroup is isomorphic to $\mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

We now provide useful results about the groups in Theorem 2.18:

Proposition 2.19. *Assume that G is a finite 2-group containing a cyclic subgroup of index two. Then, $\text{Aut}(G)$ is a 2-group unless*

- $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, for which $\text{Aut}(G) \simeq S_3$ has 6 elements; or
- $G = Dic_8 = Q_8$, for which $\text{Aut}(G) \simeq S_4$ has 24 elements.

Proof. We check each case in Theorem 2.18:

- The order of $\text{Aut}(\mathbb{Z}/2^\alpha\mathbb{Z})$ is $\varphi(2^\alpha) = 2^{\alpha-1}$ [Rob96, §1.5.5].
- The order of $\text{Aut}(\mathbb{Z}/2^{\alpha-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ is 2^α except for $\alpha = 2$, for which it is 6 [Sha15].
- The order of $\text{Aut}(D_{2^\alpha}) \simeq \text{Aut}(Dic_{2^\alpha})$ is $2^{2\alpha-1}$, except for $\alpha = 3$ for which we have $\text{Aut}(Q_8) \simeq S_4$ [Wal86; Rob96, Exercise 5.3.4].
- The order of $\text{Aut}(SD_{2^\alpha})$ is $\varphi(2^{\alpha-1}) \cdot 2^{\alpha-2} = 2^{2\alpha-4}$ [Mar24, §2.3.2].
- The order of $\text{Aut}(M_{2^\alpha})$ is 2^α [Sha15]. □

This specificity for the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and Q_8 also imply:

Proposition 2.20. *Assume that G is a finite 2-group containing a cyclic subgroup of index two. Then, G contains a characteristic subgroup of index two, unless $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G \simeq Q_8$.*

Remark 2.21. *The groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and Q_8 both contain three (cyclic) subgroups of index two, which are permuted by the automorphisms of order 3. In particular, none of these subgroups is characteristic.*

Proof of Proposition 2.20. We first use that the number of subgroups of index two of a finite group is given by $n = (G : G^2) - 1$ [Nga12]. By hypothesis, we know that $n > 0$. In particular, since G is a 2-group and $(G : G^2)$ divides $|G|$, we deduce that n is odd.

Now, $\text{Aut}(G)$ acts on the set of subgroups of index two. By hypothesis and Proposition 2.19, we know that $\text{Aut}(G)$ is a 2-group, so the size of each orbit of this

action is a power of two by the orbit-stabilizer theorem. As the sum of all these sizes is n , which is odd, we deduce that there exists an orbit $\{H\}$ of size one. In other words, the group $H \leq G$ is characteristic. $\square$

We end this section with a discussion on the existence of *normal p' -Hall subgroups*.

2.4. Frobenius p -complement theorem. From the Schur–Zassenhaus theorem, a group G can be split into a semidirect product if one finds a *normal* Hall subgroup. In the specific case where π is the collection of primes dividing G , except for the prime p , we write $\pi = p'$. A normal p' -Hall subgroup is called a *normal p -complement*.

As usual, we will denote by $\mathbf{N}_G(X) = \{g \in G \mid gXg^{-1} = X\}$ the *normalizer* of the subgroup X in G and by $\mathbf{C}_G(X) = \{g \in G \mid gx = xg \text{ for every } x \in X\}$ the *centralizer* of X in G . We now state the Frobenius p -complement theorem, which provides the existence of a normal p -complement under certain conditions.

Theorem 2.22 (Frobenius p -complement theorem [Isa08, Theorem 5.26]). *Let p be a prime number, and let G be a finite group. The following are equivalent:*

- (1) *G has a normal p -complement; and*
- (2) *for every p -subgroup $X \leq G$, the group $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is a p -group.*

Remark 2.23. *The original theorem contains a third equivalent statement, but we will not use it.*

Remark 2.24. *Recall, for later use, that the action of $\mathbf{N}_G(X)$ on X by conjugation induces a monomorphism $\mathbf{N}_G(X)/\mathbf{C}_G(X) \hookrightarrow \text{Aut}(X)$.*

We continue with several facts about normal p -complements.

Lemma 2.25. *Let p be a prime number. Let G be a finite group admitting a normal p -complement N . If $p^2 \nmid (G : G')$, then $G \simeq N \rtimes \mathbb{Z}/p\mathbb{Z}$.*

Proof. By the Schur–Zassenhaus theorem (Theorem 2.13), we have

$$G \simeq N \rtimes L,$$

where L is a Sylow p -subgroup of G . If $|L| \geq p^2$, by Lemma 2.10 and Corollary 2.15 we deduce that $p^2 \mid (G : N \rtimes L')$, so $p^2 \mid (G : G')$. This contradicts the hypothesis.

Therefore, $L \simeq \mathbb{Z}/p\mathbb{Z}$ and

$$G \simeq N \rtimes \mathbb{Z}/p\mathbb{Z}. \quad \square$$

Corollary 2.26. *Let p be a prime number. Let G be a finite group containing a cyclic normal subgroup H of index p . If $H \leq G'$, then $G \simeq \mathbb{Z}/\ell\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, where $\ell = |H|$. Moreover, $p \nmid \ell$.*

Proof. Write $|H| = kp^\alpha$ with $p \nmid k$ and $\alpha \geq 0$. Since H is cyclic, we have that:

$$H \simeq \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z}.$$

Moreover, $\mathbb{Z}/k\mathbb{Z} \leq H$ is characteristic in H by Theorem 2.4 and, since H is normal in G , we deduce that $\mathbb{Z}/k\mathbb{Z}$ is normal in G by Lemma 2.5. Thus, $\mathbb{Z}/k\mathbb{Z}$ is a normal p' -Hall subgroup of G . Since $H \leq G'$, we have $p = (G : H) \geq (G : G')$, so Lemma 2.25 shows that

$$G \simeq \mathbb{Z}/k\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}.$$

We deduce that $\alpha = 0$. Taking $\ell = k$, we obtain the desired conclusion. $\square$

We will also use the following result:

Lemma 2.27. *Let G be a finite group containing a cyclic 2-subgroup H such that $(G : H)$ is even, but not divisible by 4. Then, every nontrivial 2-subgroup X of G contains a cyclic subgroup of index two.*

Proof. We first show that this is the case when X is a Sylow 2-subgroup. We know that H is contained in some Sylow 2-subgroup L . Moreover, $(L : H) = 2$ since $(G : H)$ is even, but not divisible by 4. Finally, since X and L are conjugate, X also contains a cyclic subgroup of index two.

Now, assume that X is any 2-subgroup of G and let L be a Sylow 2-subgroup containing X . We know that there exists a cyclic subgroup $K \leq L$ of index two. Moreover, K is normal by Lemma 2.2.

We consider two cases. If $X \leq K$, we have that X itself is cyclic, and in particular it has a cyclic subgroup of index 2 by Theorem 2.4

If there exists $t \in X \setminus K$, then $L = \langle K, t \rangle$ since $(L : K) = 2$ is prime. By the second isomorphism theorem, XK is a group. Moreover, XK contains both t and K , so $XK = L$. The same theorem shows that

$$2 = (L : K) = (XK : K) = (X : X \cap K),$$

so $X \cap K$ has index two inside X , and it is cyclic as a subgroup of (the cyclic group) K by Theorem 2.4. $\square$

3. BASIC FACTS ABOUT REGULAR ORIGAMIS AND $\mathfrak{t}(g)$

In this section we prove Theorem A, which is stated more precisely below.

Theorem 3.1. *Let $g \geq 2$. If genus- g regular origamis exist, then there exists an integer $m \geq 1$ such that $m \mid 2(g-1)$, $3 \nmid m$, $4 \nmid m$ and*

$$\mathfrak{t}(g) = \frac{2(m+1)}{m}(g-1).$$

In this case, every translation surface realizing $\mathfrak{t}(g)$ translations is a regular origami up to the action of $\mathrm{GL}^+(2, \mathbb{R})$, and belongs to the stratum $\mathcal{H}(m^{2(g-1)/m})$.

Otherwise, if no genus- g regular origamis exist, then $\mathfrak{t}(g) = 2(g-1)$. In this case, every translation surface attaining $\mathfrak{t}(g)$ translations is a normal cover of a torus with two marked points, each with ramification index $g-1$, and belongs to the principal stratum $\mathcal{H}(1^{2g-2})$.

Theorem 3.1 is essentially an extension of an argument by Schlage-Puchta and Weitze-Schmithüsen [SW17, Lemma 4].

Notation. *When the number m in the previous theorem exists, we will denote $\mathfrak{m}(g) = m$. Otherwise, we set $\mathfrak{m}(g) = \infty$.*

We first state a few useful lemmas.

3.1. Riemann–Hurwitz formula. Schlage-Puchta and Weitze-Schmithüsen used the classical Riemann–Hurwitz formula to show that $\mathfrak{t}(g) \leq 4(g-1)$ for every $g \geq 2$ [SW17, Lemma 4]. The following is a refinement of their argument:

Lemma 3.2. *Let X be a translation surface of genus $g \geq 2$ with s singularities. We have the following facts:*

- (1) If X belongs to the $\mathrm{GL}^+(2, \mathbb{R})$ -orbit of a regular origami, then there exists $m \geq 1$ such that $X \in \mathcal{H}(m^s)$ and

$$|\mathrm{Trans}(X)| = \frac{2(m+1)}{m}(g-1).$$

- (2) If X belongs to the $\mathrm{GL}^+(2, \mathbb{R})$ -orbit of a nonregular origami, then

$$|\mathrm{Trans}(X)| \leq 2(g-1),$$

with equality if and only if $s = 2g - 2$ and, moreover, X is a regular cover of a torus ramified at exactly two distinct points.

- (3) If X does not belong to the $\mathrm{GL}^+(2, \mathbb{R})$ -orbit of an origami, then

$$|\mathrm{Trans}(X)| \leq \frac{4}{3}(g-1).$$

Proof. Let $G = \mathrm{Trans}(X)$. Consider the quotient translation surface $Y = X/G$ with genus $h \geq 1$. The covering $p: X \rightarrow Y$ is regular, and its degree d coincides with $|G|$. Moreover, p is ramified at $k \geq 1$ points $P_1, \dots, P_k \in Y$. Each P_i has a number $s_i \geq 1$ of preimages by p . Since the covering is regular, all preimages of P_i share the same ramification index $e_i \geq 2$. We have $d = s_i e_i$ for every $1 \leq i \leq k$. In particular, observe that X is in the $\mathrm{GL}^+(2, \mathbb{R})$ -orbit of an origami if and only if Y is a torus, that is, if and only if $h = 1$. Moreover, such origami is regular if and only if the covering is also ramified at a single point, that is, $k = 1$.

With this data, the Riemann–Hurwitz formula gives

$$\begin{aligned} 2g - 2 &= d(2h - 2) + \sum_{i=1}^k s_i(e_i - 1) \\ &= d(2h - 2 + k) - \sum_{i=1}^k s_i. \end{aligned}$$

Since $h \geq 1$ and $k \geq 1$, we have $2h - 2 + k \geq 1$. Thus,

$$d = \frac{2g - 2 + \sum_{i=1}^k s_i}{2h - 2 + k}.$$

Furthermore, we have

$$2g - 2 \geq s \geq \sum_{i=1}^k s_i,$$

with equality in the right hand side inequality if and only if all the singularities of Y are ramification points.

We distinguish the three cases in the statement.

- (1) If $h = 1$ and $k = 1$, the translation surface Y has no singularities. Hence, $s = s_1$ and

$$d = 2g - 2 + s.$$

Furthermore, every singularity of X shares the same order

$$m = \frac{2g - 2}{s}$$

so X belongs to the stratum $\mathcal{H}(m^s)$. With this notation,

$$d = 2g - 2 + \frac{2g - 2}{m} = \frac{2(m+1)}{m}(g-1).$$

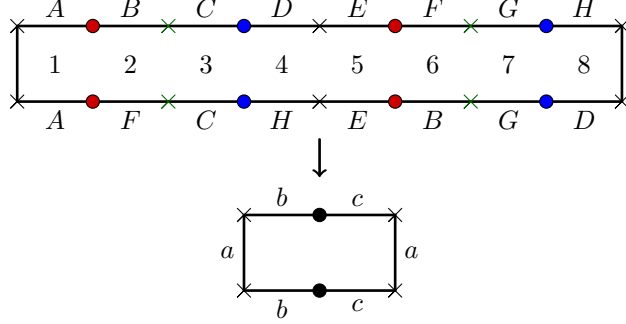


FIGURE 3.1. An origami in the stratum $\mathcal{H}_3(1^4)$ constructed as a regular cover over a torus with two marked points and possessing translation group $\mathbb{Z}/4\mathbb{Z}$.

- (2) If $h = 1$, but $k \geq 2$, we obtain:

$$d \leq \frac{2g-2+s}{k} \leq 2(g-1),$$

with equality if and only if $k = 2$ and $s = 2g - 2$.

- (3) Finally, if $h \geq 2$, we have

$$d \leq \frac{2g-2+s}{2+k} \leq \frac{2g-2+s}{3} \leq \frac{4}{3}(g-1).$$

□

We now show that, for every genus $g \geq 2$, there exists a translation surface achieving the bound in the second case of Lemma 3.2.

Lemma 3.3. *Let $g \geq 2$. There exists a genus- g translation surface with exactly $2(g-1)$ translations.*

Proof. We exhibit a genus- g origami X on $d = 4g - 4$ squares with translation group $\mathbb{Z}/(2g-2)\mathbb{Z}$. Following Matheus' lecture notes [Mat22, Definition 5], define X by the following permutations:

$$\begin{aligned} \sigma_h(i) &= i + 1 \bmod d \\ \sigma_v(i) &= \begin{cases} 2g-2+i \bmod 4g-4 & \text{if } i \text{ is even} \\ i & \text{if } i \text{ is odd.} \end{cases} \end{aligned}$$

This one-cylinder origami belongs to the stratum $\mathcal{H}(1^{2g-2})$ and its translation group is exactly $\mathbb{Z}/(2g-2)\mathbb{Z}$. Indeed, first observe that the covering $X \rightarrow \mathbb{T}$ is not regular, so the number of translations is at most $2(g-1)$ by Lemma 3.2. Moreover, for each $k \in \{0, 2, 4, \dots, 4g-6\}$, the map sending the square labeled i to the square labeled $i+k \bmod 4g-4$ defines a translation. Finally, these translations commute. □

3.2. Proof of Theorem 3.1. We now have all the ingredients for the proof.

Proof of Theorem 3.1. Assume first that genus- g regular origamis exist. By examining the three cases in Lemma 3.2, we deduce that regular origamis possess strictly

more translations than nonregular origamis and nonorigamis. Hence, there exists $m \geq 1$ such that

$$(3.4) \quad \mathfrak{t}(g) = \frac{2(m+1)}{m}(g-1),$$

where m is the order of the singularities of a translation surface X attaining $\mathfrak{t}(g)$ translations. This surface must lie in the $\mathrm{GL}^+(2, \mathbb{R})$ -orbit of a regular origami in the stratum $\mathcal{H}(m^s)$, where $s = (2g-2)/m$. In particular, $m \mid 2(g-1)$.

If $3 \mid m$, we deduce that $3 \mid (g-1)$, so there exists a genus- g origami with translation group of order $4(g-1)$ [SW17, Theorem 1]. This contradicts Equation (3.4). Similarly, if $4 \mid m$, we deduce that $2 \mid (g-1)$ and arrive at a similar contradiction.

If no genus- g origami is regular, we combine the last two cases in Lemma 3.2 to obtain that $\mathfrak{t}(g) \leq 2(g-1)$. By Lemma 3.3, there exists a genus- g origami with this number of translations, and such a surface must lie in the $\mathrm{GL}^+(2, \mathbb{R})$ -orbit of an origami covering a torus and ramified at exactly two distinct points. $\square$

3.3. Building regular origamis. Given a finite group G and elements $x, y \in G$ such that $G = \langle x, y \rangle$, we can build a regular origami whose squares are labeled by the elements of G , and whose horizontal and vertical permutations are given by (left) multiplication by G . If H is the cyclic group generated by $[x, y]$, the resulting regular origami belongs to the stratum $\mathcal{H}(m^s)$, where $m = |H| - 1$ and $s = (G : H)$. Since $sm = 2g - 2$, we get

$$|G| = |H| \cdot (G : H) = (m+1)s = 2g - 2 + \frac{2g-2}{m} = \frac{2(m+1)}{m}(g-1).$$

Equivalently, a regular origami exists in the stratum $\mathcal{H}(m^s)$ if and only if there exists a group G of order $(2(m+1)/m)(g-1)$, together with two generators $x, y \in G$ such that $H = \langle [x, y] \rangle$ has order $m+1$ and index s [FT23, Remark 2.9].

3.3.1. Direct products. A useful tool to build a regular origami inside a stratum of a prescribed form is to use a direct product between a known translation group G and a cyclic group $\mathbb{Z}/k\mathbb{Z}$. Concretely, we generalize some ideas of Schlage-Puchta and Weitz-Schmithüsen [SW17, Proposition 11] to include the case where $|G|$ and k are possibly not coprime.

Lemma 3.5. *Let G be a group generated by two elements $x, y \in G$ of orders α and β . Let k be coprime with $\gcd(\alpha, \beta)$. Consider the group $H = G \times \mathbb{Z}/k\mathbb{Z}$. Then, there exist elements $a, b \in H$ such that $H = \langle a, b \rangle$ and $\mathrm{ord}([a, b]) = \mathrm{ord}([x, y])$.*

Furthermore, when k is coprime to α , one can choose $a = (x, 1)$ and $b = (y, 0)$.

Finally, if the regular origami induced by the group G and the generators $x, y \in G$ lies in the stratum $\mathcal{H}(m^s)$, then the new regular origami induced by the group H and the generators $a, b \in H$ lies in the stratum $\mathcal{H}(m^{ks})$.

Proof. Since k is coprime with $\gcd(\alpha, \beta)$, we can write $k = ts$ where:

- t and s are coprime;
- t is coprime with α ; and
- s is coprime with β .

Now, since t and s are coprime, there is an isomorphism

$$H = G \times \mathbb{Z}/k\mathbb{Z} \simeq G \times \mathbb{Z}/t\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}.$$

Take the elements $a = (x, 1, 0)$ and $b = (y, 0, 1)$ of H . Since $\mathbb{Z}/k\mathbb{Z}$ is abelian, we have $[a, b] = ([x, y], 0, 0)$ and, therefore, $\mathrm{ord}([a, b]) = \mathrm{ord}([x, y])$.

Furthermore, since t is coprime with α , there exists u such that $u\alpha \equiv -1 \pmod{t}$, and we have that

$$a^{u\alpha+1} = (x^{u\alpha+1}, u\alpha + 1, 0) = (x, 0, 0),$$

so $(x, 0, 0) \in \langle a, b \rangle$. Moreover, if $e \in G$ denotes the identity element of G , we have

$$(e, 1, 0) = (x^{\alpha-1}, 0, 0)(x, 1, 0) \in \langle a, b \rangle.$$

Analogously, we obtain that $(y, 0, 0) \in \langle a, b \rangle$ and $(e, 0, 1) \in \langle a, b \rangle$. Therefore, we deduce that $H \supseteq G \times \{1\} \times \{1\}$, $H \supseteq \{e\} \times \mathbb{Z}/t\mathbb{Z} \times \{1\}$, and $H \supseteq \{e\} \times \{1\} \times \mathbb{Z}/s\mathbb{Z}$, so $H = \langle a, b \rangle$.

Finally, the orders of $[x, y]$ in G and $[a, b]$ in H match, and the index of $\langle [a, b] \rangle$ inside H is ks , so the discussion at the beginning of Section 3.3 shows that the regular origami induced by H and the generators $a, b \in H$ lies in the stratum $\mathcal{H}(m^{ks})$. $\square$

3.3.2. Examples of regular origamis. We now provide a few examples of regular origamis that lie in specific strata, for later use.

(1) For any integer $k \geq 1$, the stratum $\mathcal{H}(k^4)$ contains regular origamis. Indeed, consider the group $D_{4(k+1)} \simeq \mathbb{Z}/2(k+1)\mathbb{Z} \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$, together with the generators $x = (1, 0)$ and $y = (0, 1)$. We have $[x, y] = [y, x]^{-1} = x^2$; it has order $k+1$ and generates a group of index 4. Thus, the induced regular origami lies in $\mathcal{H}(k^4)$.

(2) For any even integers $k, \ell \geq 2$, the stratum $\mathcal{H}(k^\ell)$ contains regular origamis. Indeed, first consider the group $D_{2(k+1)} = \mathbb{Z}/(k+1)\mathbb{Z} \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$, together with the generators $x = (1, 0)$ and $y = (0, 1)$. We have $[x, y] = [y, x]^{-1} = x^2$; it has order $k+1$ (since k is even) and generates a group of index 2. Thus, the induced regular origami lies in $\mathcal{H}(k^2)$.

Now, observe that $\gcd(\text{ord}(x), \text{ord}(y)) = \gcd(k+1, 2) = 1$. Take $\lambda = \ell/2$ and apply Lemma 3.5 using the groups $D_{2(k+1)}$ and $\mathbb{Z}/\lambda\mathbb{Z}$, together with the generators $x, y \in D_{2(k+1)}$. The resulting regular origami lies in the stratum $\mathcal{H}(k^\ell)$.

(3) For any $g \geq 2$ with $9 \mid (g-1)$, the stratum $\mathcal{H}(2^{g-1})$ contains regular origamis. Indeed, first consider the group $M_{3^{\alpha+1}} = \mathbb{Z}/3^\alpha\mathbb{Z} \rtimes_{3^{\alpha-1}+1} \mathbb{Z}/3\mathbb{Z}$, together with the generators $x = (1, 0)$ and $y = (0, 1)$. We have $[x, y] = [y, x]^{-1} = x^{3^{\alpha-1}}$; it has order 3 and generates a group of index 9. Thus, the induced regular origami lies in the stratum $\mathcal{H}(2^s)$, for $s = 3^\alpha$.

Now, observe that $\gcd(\text{ord}(x), \text{ord}(y)) = \gcd(3^\alpha, 3) = 3$. Write $g-1 = 3^\alpha\lambda$, for $\alpha \geq 2$ and λ not divisible by 3. We use Lemma 3.5 with the groups M_{3^α} and $\mathbb{Z}/\lambda\mathbb{Z}$, together with the generators $x, y \in M_{3^\alpha}$. The resulting regular origami lies in the stratum $\mathcal{H}(2^{g-1})$.

In fact, it is possible to completely characterize the strata where regular origamis with a translation group isomorphic to a semidirect product of two cyclic groups. See Proposition B.2.

4. THE SETS $G(2)$ AND $G(2^\alpha - 1)$ FOR $\alpha \geq 1$ ARE EMPTY

Now that we have proven Theorem A, we study the set

$$G(m) = \left\{ g \geq 2 \mid t(g) = \frac{2(m+1)}{m}(g-1) \right\}$$

In this section, we study some particular values of m , namely $m = 2$ and m of the form $2^\alpha - 1$ for $\alpha \geq 1$. Using elementary group-theoretic methods, we show that $\mathbf{G}(m)$ is empty for such values of m , proving Theorem B.

4.1. The set $\mathbf{G}(2)$. We start with the case of $m = 2$. This result will be crucial in later sections to compute certain values of $\mathbf{m}(g)$.

Theorem 4.1. *The set $\mathbf{G}(2)$ is empty, that is, $\mathbf{t}(g) \neq 3(g-1)$ for every $g \geq 2$.*

In fact, we completely classify the set of genera such that the stratum $\mathcal{H}(2^{g-1})$ contains regular origamis.

Theorem 4.2. *There exist regular origamis in $\mathcal{H}(2^{g-1})$ if and only if $g-1$ is even or $9 \mid (g-1)$.*

Since all the genera in the statement of Theorem 4.2 belong to $\mathbf{G}(1)$, this shows that regular origamis in $\mathcal{H}(2^{g-1})$ never achieve $\mathbf{t}(g)$, proving Theorem 4.1.

Proof of Theorem 4.2. From the discussion of Section 3.3, the statement is equivalent to the existence of a group G of order $n = 3(g-1)$ generated by two elements whose commutator has order 3. If $g-1$ is even or if $9 \mid (g-1)$, we already know that a regular origami exists in $\mathcal{H}(2^{g-1})$. More precisely, if $g-1$ is even, this is covered in Example (2); if $9 \mid (g-1)$, this is covered in Example (3). We will therefore assume that $g-1$ is odd and that $9 \nmid (g-1)$.

Observe that $2 \nmid n$. Thus, by the Feit–Thompson theorem (Theorem 2.7), G is solvable. As a consequence, since $3 \mid n$, we know from Theorem 2.17 that there exists a $3'$ -Hall subgroup U of G .

From $9 \nmid (g-1)$, we obtain that $27 \nmid n$, and therefore that $(G : U) \mid 9$. Let $\ell = n/(G : U) = |U|$. By construction, $3 \nmid \ell$. We will show that U is normal.

First, the number of conjugates of U is $k = (G : \mathbf{N}_G(U))$. But,

$$(G : U) = (G : \mathbf{N}_G(U))(\mathbf{N}_G(U) : U),$$

and, therefore, $k = (G : \mathbf{N}_G(U))$ must be either 1, 3 or 9.

Using the action of U on the set $\Omega = \{gUg^{-1} \mid g \in G\}$, Schlage-Puchta and Weitze-Schmithüsen show [SW17, Lemma 15] that there exist integers $a_p \geq 0$ for each prime divisor p of ℓ such that:

$$k = 1 + \sum_{p \mid \ell} a_p p.$$

Now, since ℓ is not divisible by $p = 2$ or $p = 3$, these factors do not appear in the sum. Hence, k cannot be 3 or 9. Thus, $k = 1$, and U is normal.

As a consequence, the quotient G/U is a group of order either 3 or 9, hence it is abelian. Thus, the commutator subgroup of G is a subgroup of U , and any commutator has an order dividing $\ell = |U|$. As $3 \nmid \ell$, the order of any commutator is not 3. $\square$

4.2. The set $\mathbf{G}(2^\alpha - 1)$. We now turn our attention to $m = 2^\alpha - 1$.

We will prove the following:

Theorem 4.3. *The set $\mathbf{G}(2^\alpha - 1)$ is empty for each $\alpha \geq 2$.*

We again work in the group theoretic setting. We will show a stronger version of this:

Theorem 4.4. *Let $g \geq 2$ be an integer with $g \notin \mathbf{G}(1)$. Let $\alpha \geq 2$ be an integer. Then, a group G of order*

$$n = \frac{2^{\alpha+1}}{2^\alpha - 1}(g - 1),$$

together with two generators $x, y \in G$ such that $[x, y]$ has order 2^α , does not exist.

Remark 4.5. *In geometric terms, this means the stratum $\mathcal{H}((2^\alpha - 1)^\ell)$ contains no regular origamis if $g = \ell(2^\alpha - 1)/2 + 1 \notin \mathbf{G}(1)$, that is, if $\ell \equiv 2 \pmod{4}$ and $3 \nmid \ell(2^\alpha - 1)$. Nevertheless, such origamis do exist if $g \in \mathbf{G}(1)$ [FT23, Theorem A].*

The crux of the proof is the following lemma:

Lemma 4.6. *In the context of Theorem 4.4, G contains a normal $2'$ -Hall subgroup.*

Proof. This is an application of Frobenius p -complement theorem (Theorem 2.22) together with Lemma 2.27. Indeed, given a 2-subgroup $X \leq G$, we will show that $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is a 2-group.

Let $q > 3$ be prime. Since $H = \langle [x, y] \rangle$ is a cyclic 2-subgroup of G of index

$$(G : H) = \frac{2}{2^\alpha - 1}(g - 1)$$

and $g - 1$ is odd as $g \notin \mathbf{G}(1)$, Lemma 2.27 shows that X contains an index-two cyclic subgroup and, in particular, that it is isomorphic to one of the groups in Theorem 2.18. By Proposition 2.19, q does not divide $|\mathrm{Aut}(X)|$. In particular, from Remark 2.24 q does not divide $|\mathbf{N}_G(X)/\mathbf{C}_G(X)|$ either.

On the other hand, we have that 3 does not divide $|G|$, so it does not divide $|\mathbf{N}_G(X)|$. Thus, the only prime factor of $|\mathbf{N}_G(X)/\mathbf{C}_G(X)|$ is 2, so this group is a 2-group. We conclude using the Frobenius p -complement theorem. $\square$

We can now finish the proof of Theorem 4.4:

Proof of Theorem 4.4. Let N be a normal $2'$ -Hall subgroup of G , which exists by Lemma 4.6.

Let $H = \langle [x, y] \rangle$. Since $2^2 \nmid (G : H)$, we have that $2^2 \nmid (G : G')$. Thus, Lemma 2.25 shows that

$$G \simeq N \rtimes \mathbb{Z}/2\mathbb{Z},$$

with $|N|$ odd. Hence, 2^α does not divide $|G|$, so no commutator has order 2^α . $\square$

5. REGULAR ORIGAMIS WITH TRANSLATION GROUP $\mathrm{PSL}(2, p)$

In this section, we prove a more precise version of Theorem C, namely:

Theorem 5.1. *Let $m \geq 5$ be prime and assume that $3 \mid (m + 1)$. There exist infinitely many prime numbers p such that, for every $k \geq 1$ not divisible by any prime number $q < m$, we have*

$$\frac{kmp(p-1)(p+1)}{4(m+1)} + 1 \in \mathbf{G}(m).$$

In particular, $\mathbf{G}(m)$ contains infinitely long arithmetic progressions.

For this, we will construct regular origamis with translation group of the form $\mathrm{PSL}(2, p) \times \mathbb{Z}/k\mathbb{Z}$ for suitable prime p , integer k , and appropriate pairs of generators (A, B) , and we will show that they have the largest automorphism group for their genus. The main technical device for this section is producing generators A, B of $\mathrm{SL}(2, p)$ such that $[A, B]$ has a desired order d and such that B has order two:

Proposition 5.2. *Let $p > 13$ be a prime number. Then, for any integer $d \geq 6$ satisfying $p \equiv \pm 1 \pmod{d}$, there exists $A \in \mathrm{SL}(2, p)$ such that A and $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ generate $\mathrm{SL}(2, p)$, and $[A, B]$ has order d in $\mathrm{SL}(2, p)$.*

Proposition 5.2 is very similar to the work of McCullough and Wanderley [MW11, Theorem 2.2]: they show that any element can be realized as the commutator of a generating pair (A, B) , except for $-\mathrm{Id}$ and those of trace 2. In fact, their result is sufficient to prove a slightly weaker version of Theorem 5.1, where we additionally assume that k is coprime with the order of $\mathrm{PSL}(2, p)$ (that is, k is coprime with p , $p - 1$, and $p + 1$). This additional assumption makes k depend not only on m , but also on p . To rule out the dependence on p , we will additionally need to control $\gcd(\mathrm{ord}(A), \mathrm{ord}(B))$ in order to apply Lemma 3.5, and therefore we include a complete (and different) proof.

Before proving this Proposition 5.2, we need a result about generating pairs of $\mathrm{SL}(2, p)$ and two lemmas. Our first lemma shows that order- d elements exist in $\mathrm{SL}(2, p)$ for suitable d . This result is well-known and it is actually more general [GS87, Theorem 2.4]. Nevertheless, we include a short proof for the sake of completeness.

Lemma 5.3. *Let p be an odd prime number. Let $d \geq 3$ be such that $p \equiv \pm 1 \pmod{d}$. Then, there exists an order- d element $M \in \mathrm{SL}(2, p)$. Moreover, $\mathrm{tr}(M) \neq \pm 2$.*

Proof. We will construct M explicitly. We consider two cases:

- If $p \equiv 1 \pmod{d}$, we choose $\lambda \in \mathbb{F}_p^\times$ of multiplicative order d . This is possible since $\mathbb{F}_p^\times$ is cyclic of order $p - 1$. The element $M = \mathrm{diag}(\lambda, \lambda^{-1}) \in \mathrm{SL}(2, p)$ has order d .
- If $p \equiv -1 \pmod{d}$, we choose $\lambda \in \mathbb{F}_{p^2}^\times \setminus \mathbb{F}_p^\times$ of multiplicative order d . This is possible since $\mathbb{F}_{p^2}^\times$ is cyclic of order $(p - 1)(p + 1)$. Since λ is sent to λ^{-1} by the unique nontrivial element of the Galois group $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$, the element $t = \lambda + \lambda^{-1}$ belongs to $\mathbb{F}_p$. Moreover, $\lambda \neq \lambda^{-1}$ since, otherwise, $\lambda \in \mathbb{F}_p$.

Now, λ and λ^{-1} are the roots of the quadratic polynomial $x^2 - tx + 1$. Take $M = \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}(2, p)$. This matrix has characteristic polynomial $x^2 - tx + 1$, so it is conjugate to $\mathrm{diag}(\lambda, \lambda^{-1})$. Thus, it has order d , as required. $\square$

In both cases, $\mathrm{tr}(M) \neq \pm 2$ since, otherwise, $\lambda = \pm 1$, which does not have order d .

We continue with a folklore lemma in elementary number theory:

Lemma 5.4. *Let $p \geq 17$ be prime and let $a \in \mathbb{F}_p^\times$. Then, a can be written as the sum of two nonzero squares in at least two different ways. That is, there exist $s_1, t_1, s_2, t_2 \in \mathbb{F}_p^\times$ such that $a = s_1^2 + t_1^2 = s_2^2 + t_2^2$, and $\{s_1^2, t_1^2\} \cap \{s_2^2, t_2^2\} = \emptyset$.*

Proof. Fix $a \in \mathbb{F}_p^\times$. Consider $Q: \mathbb{F}_p^2 \rightarrow \mathbb{F}_p$ given by $Q(x, y) = x^2 + y^2$ and define $R = \{x^2 \mid x \in \mathbb{F}_p\}$. We have that $|R| = (p + 1)/2$, so $R \cap (a - R) \neq \emptyset$. We get $x^2 = a - y^2$ for some $x, y \in \mathbb{F}_p$, so $Q(x, y) = a$.

Now, the group $\mathrm{SO}(Q)$ has order at least $p - 1 \geq 16$ [Tay92, p. 141]. Define $S = \mathrm{SO}(Q) \cdot (x, y)$. Since the stabilizer of (x, y) is trivial, we obtain that $|S| \geq 16$.

Finally, S contains at most two elements of the form $(\pm r, 0)$ and at most two elements of the form $(0, \pm r)$, so at least twelve of its elements belong to $(\mathbb{F}_p^\times)^2$. If (s_1, t_1) is such an element, S contains at most four elements of the form $(\pm s_1, \pm t_1)$

and at most four elements of the form $(\pm t_1, \pm s_1)$, so there exist $(s_2, t_2) \in S$ not of these forms. We obtain that $a = s_1^2 + t_1^2 = s_2^2 + t_2^2$ and $\{s_1^2, t_1^2\} \cap \{s_2^2, t_2^2\} = \emptyset$. $\square$

Our final ingredient to prove Theorem 5.1 is the following number-theoretic fact:

Lemma 5.5. *Let m be prime with $3 \mid (m+1)$. Then, there exist infinitely many prime numbers p with $p \equiv \pm 1 \pmod{2(m+1)}$ such that*

$$z = \frac{(p-1)(p+1)}{4(m+1)}$$

is an integer and is not divisible by any prime number $q < m$.

Proof. We will use the Chinese remainder theorem to show that this holds if p belongs to certain residue classes. Then, infinitely many such prime numbers will exist due to Dirichlet's theorem.

Observe that z is an integer if $p \equiv \pm 1 \pmod{2(m+1)}$. Indeed, this means that $2(m+1)$ divides either $p-1$ or $p+1$, and the other factor of $(p-1)(p+1)$ is even.

Let 2^α , with $\alpha \geq 1$, be the largest power of 2 that divides $m+1$. Observe that the largest power of 2 that divides $4(m+1)$ is $2^{\alpha+2}$. For z to be an odd integer, we need the largest power of 2 that divides $(p-1)(p+1)$ also to be $2^{\alpha+2}$. This is equivalent to

$$p \equiv a \pmod{2^{\alpha+2}},$$

where $a \not\equiv \pm 1 \pmod{2^{\alpha+2}}$, and $a \equiv \pm 1 \pmod{2^{\alpha+1}}$. Indeed, this equation imposes that the largest power of 2 that divides $p-1$ or $p+1$ is $2^{\alpha+1}$, and the other factor in $(p-1)(p+1)$ is always even (and cannot be divisible by 4). Consequently, we take $a = 2^{\alpha+1} \pm 1$.

Now, let Π be the set of primes q with $3 \leq q < m$. If $q \in \Pi$, consider the largest power q^{β_q} that divides $m+1$ (possibly, $\beta_q = 0$). For z to be an integer, we need $p \equiv \pm 1 \pmod{q^{\beta_q}}$.

Furthermore, observe that $q \nmid z$ is equivalent to $p \not\equiv \pm 1 \pmod{q^{\beta_q+1}}$. This is equivalent to

$$p \equiv b_q \pmod{q^{\beta_q+1}},$$

where $b_q \not\equiv \pm 1 \pmod{q^{\beta_q+1}}$, and $b_q \equiv \pm 1 \pmod{q^{\beta_q}}$. Hence, we take $b_q = \ell_q q^{\beta_q} \pm 1$, where $0 < \ell_q < q$ if $\beta_q > 0$, and $1 < \ell_q < q-1$ otherwise. The previous argument works for $q = 3$ since $\beta_q \geq 1$ as $3 \mid (m+1)$ by hypothesis (this is necessary since every prime $p \geq 5$ satisfies $(p-1)(p+1) \equiv 0 \pmod{3}$, so we need $\beta_q + 1 > 1$).

Combining this information, p must satisfy the system of congruences:

$$\begin{aligned} p &\equiv \pm 1 \pmod{2(m+1)} \\ p &\equiv 2^{\alpha+1} \pm 1 \pmod{2^{\alpha+2}} \\ p &\equiv \ell_q q^{\beta_q} \pm 1 \pmod{q^{\beta_q+1}} \text{ for every } q \in \Pi, \end{aligned}$$

Then, the (generalized) Chinese remainder theorem shows that the system admits a solution if and only if the equations are pairwise compatible modulo the corresponding greatest common divisors. We have:

$$\begin{aligned} \gcd(2(m+1), 2^{\alpha+2}) &= 2^{\alpha+1} \\ \gcd(2(m+1), q^{\beta_q+1}) &= q^{\beta_q} \\ \gcd(2^{\alpha+2}, q^{\beta_q+1}) &= 1. \end{aligned}$$

Thus, the compatibility is automatic as long as the choice of signs is consistent (that is, all signs are “+1”, or all signs are “−1”), independently of the ℓ_q .

Finally, observe that

$$\text{lcm}(\{2(m+1), 2^{\alpha+2}\} \cup \{q^{\beta_q+1} \mid q \in \Pi\}) = 4(m+1)Q,$$

where Q is the product of all $q \in \Pi$. Hence, the Chinese remainder theorem also shows that there exists t such that p is a solution if $p \equiv t \pmod{4(m+1)Q}$. Since p is coprime with $4(m+1)Q$ by construction, so is t .

We conclude by Dirichlet’s theorem: infinitely many primes belong to this residue class t modulo $4(m+1)Q$. $\square$

Remark 5.6. *When m is a Sophie Germain prime, the smallest prime number p as in the previous lemma is $p = 2m + 1$. This choice yields $z = m$.*

To show that two matrices A and B generate $\text{SL}(2, p)$, we will use the results of McCullough and Wanderley [MW13], building on the results of Macbeath [Mac69a].

Theorem 5.7 ([MW13, Section 11]). *Let $p \geq 13$ be a prime number. Two elements $A, B \in \text{SL}(2, p)$ are generators if and only if:*

- (1) *at least two of the numbers $\text{tr}(A)$, $\text{tr}(B)$ and $\text{tr}(AB)$ are nonzero;*
- (2) *$\text{tr}([A, B]) \neq 2$; and*
- (3) *$\langle A, B \rangle$ is not isomorphic to A_4 , S_4 or A_5 .*

The conditions they find are, in fact, more general since they deal with any finite field. Nevertheless, Theorem 5.7 is enough for our purposes, as we only work with fields of odd-prime order.

Finally, McCullough and Wanderley provide a full classification of conjugacy classes in $\text{SL}(2, p)$ [MW11, Proposition 2.3]. We recall part of it: $A, B \in \text{SL}(2, p)$ with $\text{tr}(A), \text{tr}(B) \neq \pm 2$ are conjugate if and only if $\text{tr}(A) = \text{tr}(B)$.

We can now prove the proposition:

Proof of Proposition 5.2. We take $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, p)$, where $a, b, c, d \in \mathbb{F}_p$ will be chosen appropriately.

Let $M \in \text{SL}(2, p)$ be an element of order d , which exists by Lemma 5.3. Take $x = \text{tr}(M)$; we have $x \neq \pm 2$. On the one hand, we will ensure that $\text{tr}([A, B]) = x$. This implies A has order d by the classification of conjugacy classes above.

On the other hand, by Theorem 5.7, we need to verify conditions (1), (2), and (3) to obtain $\text{SL}(2, p) = \langle A, B \rangle$. In fact, it will be enough to focus on condition (1). Indeed, condition (2) follows automatically from $\text{tr}([A, B]) = x$. Moreover, condition (3) is automatic from the fact that $d \geq 6$, since the only possible orders of commutators in A_4 , S_4 , and S_5 are 1, 2, 3, and 5.

Observe that

$$\begin{aligned} \text{tr}(A) &= a + d \\ \text{tr}(AB) &= b - c \\ \text{tr}([A, B]) &= a^2 + b^2 + c^2 + d^2. \end{aligned}$$

Consider the equation

$$(5.8) \quad x^2 - 4 = (2s)^2 + t^2,$$

with variables s and t . Since $x \neq \pm 2$, we have $x^2 - 4 \neq 0$. By Lemma 5.4, there exist two pairs of solutions $(s_1, t_1), (s_2, t_2) \in (\mathbb{F}_p^\times)^2$ of Equation (5.8) such that

$\{s_1^2, t_1^2\} \cap \{s_2^2, t_2^2\} = \emptyset$. If $t_1 \neq \pm x$, we define $(s, t) = (s_1, t_1)$. Otherwise, we have $t_2 \neq \pm x$ since $t_1^2 \neq t_2^2$, and we take $(s, t) = (s_2, t_2)$.

Now, take $u = (x + t)/2$, which is nonzero by our choice of t . A straightforward computation shows that

$$(5.9) \quad ux - (u^2 + 1) = s^2.$$

Using Lemma 5.4 again, we continue by taking $(a_1, c_1), (a_2, c_2) \in (\mathbb{F}_p^\times)^2$ such that $u = a_1^2 + c_1^2 = a_2^2 + c_2^2$ and $\{a_1^2, c_1^2\} \cap \{a_2^2, c_2^2\} = \emptyset$.

Now, for $i \in \{1, 2\}$, we define:

$$b_i^\pm = \frac{-c_i \pm a_i s}{a_i^2 + c_i^2}, \quad d_i^\pm = \frac{1 + b_i^\pm c_i}{a_i}.$$

The choice of $d_i^\pm$ directly implies $a_i d_i^\pm - b_i^\pm c_i = 1$. Moreover,

$$\begin{aligned} a_i^2 + (b_i^\pm)^2 + c_i^2 + (d_i^\pm)^2 &= \frac{(a_i^2 + c_i^2)^2 + 1 + s^2}{a_i^2 + c_i^2} \\ &= \frac{u^2 + 1 + ux - (u^2 + 1)}{u} \\ &= x, \end{aligned}$$

where we used that $a_i^2 + c_i^2 = u$ and Equation (5.9).

We will show that, for some choice of $i \in \{1, 2\}$ and $\varepsilon \in \{+, -\}$, we have $a_i + d_i^\varepsilon \neq 0$ and $b_i^\varepsilon - c_i \neq 0$, so we can take $a = a_i$, $b = b_i^\varepsilon$, $c = c_i$, and $d = d_i^\varepsilon$ to finish the proof.

Observe that

$$\begin{aligned} a_i + d_i^\pm &= \frac{a_i(u + 1) \pm c_i s}{u} \\ b_i^\pm - c_i &= \frac{-c_i(u + 1) \pm a_i s}{u}. \end{aligned}$$

If one of these quantities vanishes, we can solve for s to obtain

$$\begin{aligned} a_i + d_i^\pm = 0 &\implies s = \mp \frac{a_i}{c_i}(u + 1) \\ b_i^\pm - c_i = 0 &\implies s = \pm \frac{c_i}{a_i}(u + 1). \end{aligned}$$

In particular, if any of these numbers vanish, then $u \neq -1$ since $s \neq 0$. Furthermore, we deduce that $a_i + d_i^\varepsilon = 0$ for both choices of $\varepsilon \in \{+, -\}$ implies $s = 0$, which is impossible. Similarly, $b_i^\varepsilon - c_i = 0$ for both choices of $\varepsilon \in \{+, -\}$ is impossible.

Thus, if one of the numbers $a_i + d_i^\varepsilon$ or $b_i^\varepsilon - c_i$ vanishes for both choices of $\varepsilon \in \{+, -\}$, we only have two possible cases: either both $a_i + d_i^+$ and $b_i^- - c_i$ vanish, or both $a_i + d_i^-$ and $b_i^+ - c_i = 0$ do. In both cases, solving for s as above and canceling $u + 1$ out yields $a_i/c_i = c_i/a_i$, so $c_i^2 = a_i^2$.

Finally, we see that $u = a_i^2 + c_i^2$ is written as a sum of two *equal* squares. This can only happen for a single choice of $i \in \{1, 2\}$ since $\{a_1^2, c_1^2\} \cap \{a_2^2, c_2^2\} = \emptyset$. Thus, if j is such that $\{i, j\} = \{1, 2\}$, we deduce that $a_j + d_j^\varepsilon \neq 0$ and $b_j^\varepsilon - c_j \neq 0$ for at least one of the choices of $\varepsilon \in \{+, -\}$, completing the argument. $\square$

Remark 5.10. *The only reason why we need $d \geq 6$ in the previous proof is to rule out the groups A_4 , S_4 , and A_5 , that is, to establish condition (3) in Theorem 5.7. This condition is actually not necessary, since $\langle A, B \rangle$ is one of these groups only in*

very particular situations. Since we only need the result for $d \geq 6$, we refrain from stating this more general version and refer the reader to the work of McCullough [McC] for more details.

We now have all the tools to prove the main result of this section.

Proof of Theorem 5.1. Let p be as in Lemma 5.5, and let k be as in the statement. We take $G = \mathrm{PSL}(2, p)$. We define the group $H = G \times \mathbb{Z}/k\mathbb{Z}$, together with two generators $a, b \in H$ with $\mathrm{ord}([a, b]) = m + 1$. Such generators exist. Indeed, by Proposition 5.2, since $p \equiv \pm 1 \pmod{2(m+1)}$ there exist two generators $x, y \in \mathrm{SL}(2, p)$ whose commutator $[x, y]$ has order $2(m+1)$ in $\mathrm{SL}(2, p)$, or $m+1$ in G . Moreover, in Proposition 5.2, we can take the order of y to be two. Thus k is coprime with $\mathrm{gcd}(\mathrm{ord}(x), \mathrm{ord}(y))$, and Lemma 3.5 applies.

Let n be the order of H , that is,

$$n = \frac{kp(p-1)(p+1)}{2}.$$

Now, consider the regular origami induced by H , a , and b , and let g be its genus. We have that

$$\frac{kp(p-1)(p+1)}{2} = n = \frac{2(m+1)}{m}(g-1),$$

so

$$g-1 = \frac{mkp(p-1)(p+1)}{4(m+1)}.$$

As a consequence, observe that our assumptions on p and k guarantee that $g-1$ is not divisible by any prime number $q < m$. In particular $2 \nmid (g-1)$ and $3 \nmid (g-1)$, so $g \notin \mathbf{G}(1)$. Thus, $m(g) \in \{5, \dots, m\}$ (recall that $\mathbf{G}(2)$ is empty by Theorem 4.1, and $m(g) \neq 3, 4$ by Theorem 3.1). Further, if $5 \leq d < m$, we see that $d \nmid 2(g-1)$ and therefore $g \notin \mathbf{G}(d)$. Hence, $g \in \mathbf{G}(m)$. $\square$

Remark 5.11. In the particular case of $m = 5$, the previous proof shows that every prime number $p > 13$ satisfying that $p \bmod 72$ is 11, 13, 59, or 61 allows us to produce an infinitely long arithmetic progression inside $\mathbf{G}(5)$, where the condition $p > 13$ is only needed because of the use of Lemma 5.4. Nevertheless, the values $p = 11$ and $p = 13$ also work, although the general proof fails.

To see this, we can exhibit explicit matrices that generate the groups $\mathrm{PSL}(2, 11)$ and $\mathrm{PSL}(2, 13)$, one of which has order 2, and with a commutator of order 6.

For example, the following choices work for $\mathrm{PSL}(2, 11)$:

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Similarly, these matrices do the trick for $\mathrm{PSL}(2, 13)$:

$$A = \begin{pmatrix} 2 & 4 \\ 0 & 7 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Primes smaller than 17 only arise in the case of $m = 5$, so it is not necessary to consider them in other cases.

Finally, in the case of $m = 11$, the condition that $7 \nmid z$ is not needed in Lemma 5.5, since we know that $\mathbf{G}(7)$ is empty (Theorem 4.3). This case is somewhat simplified to requiring only that $2 \nmid z$, $3 \nmid z$, and $5 \nmid z$. We obtain that any prime p such that $p \bmod 720$ is 23, 167, 263, 313, 407, 457, 553, 697 induces an infinitely long arithmetic progression inside $\mathbf{G}(11)$.

6. INFINITE FAMILIES OF GENERA IN $G(\infty)$

In this section, we prove Theorems D to F by producing infinite families of genera $g \geq 2$ with no genus- g regular origamis and studying the special case of Sophie Germain primes (i.e. a prime p such that $2p + 1$ is also prime):

Theorem 6.1. *Let $g \geq 6$ be of the form:*

- (1) $g = p + 1$, where $p \geq 5$ is prime;
- (2) $g = p^2 + 1$, where p is prime, but it is not a Sophie Germain prime;
- (3) $g = pq + 1$, where $p, q \geq 5$ are distinct primes.

Then there exist no genus- g regular origamis.

On the other hand, if $p \geq 5$ is a Sophie Germain prime there exist regular origamis of genus $p^2 + 1$. Such origamis belong to the stratum $\mathcal{H}(2p^p)$ and have translation group $\mathbb{Z}/(2p + 1)\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. In particular, $p^2 + 1 \in G(2p)$.

Remark 6.2. *Combining the last part of Theorem 6.1 with Lemma 3.5, we obtain that for any Sophie Germain prime $p \geq 5$ and any integer $\ell \geq 1$, it is possible to construct a regular origami of genus $g = \ell p^2 + 1$ with translation group $(\mathbb{Z}/(2p + 1)\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \times \mathbb{Z}/\ell\mathbb{Z}$. In particular $\ell p^2 + 1 \notin G(\infty)$.*

This proof will be done in several steps. The crux of the proof is showing that regular origamis in the strata $\mathcal{H}(g - 1, g - 1)$, $\mathcal{H}(2p^q)$, and $\mathcal{H}(p^{2q})$, for p, q prime, can only exist in very particular situations. These cases will be done in Section 6.1, Section 6.2, and Section 6.3, respectively. Recall from Section 3.3 that if $m \mid (2g - 2)$, the existence of a regular origami in $\mathcal{H}(m^s)$, for $s = (2g - 2)/m$, is equivalent to the existence of a group G of order

$$n = |G| = \frac{2(m + 1)}{m}(g - 1)$$

that is generated by two elements, $x, y \in G$, such that $[x, y]$ has order $m + 1$. To rule out the existence of regular origami in such strata, we will use several group-theoretic tools.

Finally, we will combine these results to complete the proof of Theorem 6.1 in Section 6.4.

6.1. The stratum $\mathcal{H}(g - 1, g - 1)$. We will show that $\mathcal{H}(g - 1, g - 1)$ can only contain regular origamis if g is odd:

Lemma 6.3. *Let $g \geq 2$. If the stratum $\mathcal{H}(g - 1, g - 1)$ contains regular origamis if and only if g is odd.*

Proof. Assume that regular origamis exist in the stratum $\mathcal{H}(g - 1, g - 1)$. From the group-theoretic viewpoint, this means assuming the existence of a group G of order $2g$, generated by two elements $x, y \in G$ whose commutator has order g . We will show that g is odd.

Consider the cyclic subgroup $H = \langle [x, y] \rangle \leq G'$ of G . Since $|H| = g$, we see that H has index two in G . Hence, H is normal by Lemma 2.2.

We now apply Corollary 2.26 with $p = 2$ to deduce that

$$G \simeq \mathbb{Z}/g\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z},$$

with $2 \nmid g$, so g is odd.

The converse follows directly from the first example of Section 3.3.2 □

6.2. The stratum $\mathcal{H}(2k^q)$. If q is an odd prime and k is an integer, regular origamis in the stratum $\mathcal{H}(2k^q)$ can only exist under very special conditions:

Theorem 6.4. *Let $k \geq 1$ be an integer and let q be an odd prime. There exist regular origamis in the stratum $\mathcal{H}(2k^q)$ if and only if there exists $d \in \{2, 3, \dots, 2k\}$ such that*

- $d^q \equiv 1 \pmod{2k+1}$;
- $d-1$ is coprime with $2k+1$.

In this case, the translation group of such a regular origami is isomorphic to the semidirect product $\mathbb{Z}/(2k+1)\mathbb{Z} \rtimes_d \mathbb{Z}/q\mathbb{Z}$.

Furthermore, the existence of such d is equivalent to all prime factors of $2k+1$ being congruent to 1 modulo q .

Remark 6.5. *The case $\mathcal{H}(k^2)$ reduces to the case $\mathcal{H}(g-1, g-1)$, which has been dealt with in Lemma 6.3. Moreover, since q is odd, $\mathcal{H}(u^q)$ is empty if u is odd, so we assume $u = 2k$.*

Proof of Theorem 6.4. As before, we consider a group G of order $n = (2k+1)q$, together with two generators x, y such that $[x, y]$ has order $2k+1$.

First, observe that $H = \langle [x, y] \rangle \leq G'$ is a cyclic subgroup of G of prime index q . We deduce that either $G' = H$ or $G = G'$. The latter case cannot occur. Indeed, it would mean that G is nonsolvable, but, since $|G|$ is odd, the Feit–Thompson theorem (Theorem 2.7) implies that G is solvable.

We deduce that $G' = H$. In particular, since the commutator subgroup is always normal, we get that H is normal in G .

Now, we use Corollary 2.26 to obtain that:

$$G \simeq \mathbb{Z}/(2k+1) \rtimes_d \mathbb{Z}/q\mathbb{Z}$$

for some $d \in \{1, \dots, 2k\}$. We know that such a semidirect product exists if and only if $d^q \equiv 1 \pmod{2k+1}$. Moreover, its commutator subgroup is $\mathbb{Z}/(2k+1)\mathbb{Z}$ (see Lemma 2.12): this is possible if and only if $d-1$ is coprime with $2k+1$. In this case, the generators $x = (1, 0)$ and $(y, 0)$ satisfy $[x, y] = (1-d, 0)$, which has order $2k+1$. This proves the first part of the statement.

Finally, the existence of $d \in \{2, \dots, 2k\}$ meeting the requirements is equivalent to all prime factors of $2k+1$ being congruent to 1 modulo q by Proposition B.1. $\square$

Using Lemma 3.5, this construction can be bootstrapped to other strata:

Corollary 6.6. *Let $k \geq 1$ be an integer and let q be an odd prime such that every prime factor of $2k+1$ is congruent to 1 modulo q . Then, there exist regular origamis in the stratum $\mathcal{H}(2k^{\ell q})$. In particular, $g = \ell k q + 1 \notin \mathbf{G}(\infty)$.*

Proof. The previous proposition shows the existence of a regular origami in the stratum $\mathcal{H}(2k^q)$ with translation group $\mathbb{Z}/(2k+1)\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$.

Now, the hypothesis implies $\gcd(2k+1, q) = 1$. Thus, Lemma 3.5 directly shows that regular origamis with translation group $(\mathbb{Z}/(2k+1)\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}) \times \mathbb{Z}/\ell\mathbb{Z}$ exist in the stratum $\mathcal{H}(2k^{\ell q})$. $\square$

An immediate consequence of this proposition is that, if $\mathcal{H}(2k^q)$ contains regular origamis, then $2k+1 \equiv 1 \pmod{q}$ and, hence, $q \mid 2k$. In particular, since $q \neq 2$, we must have $q \mid k$. If $k = p$ is a prime number, we get:

Corollary 6.7. *If p, q are odd primes, there exist regular origamis in the stratum $\mathcal{H}(2p^q)$ if and only if $p = q$ and $2p + 1$ is prime.*

Proof. Taking $\ell = 1$ in the previous corollary shows existence.

Now, assume a regular origami exists in $\mathcal{H}(2p^q)$. By Theorem 6.4 and the discussion above, we get that $q \mid p$ and, since p is prime, that $p = q$. Now, Theorem 6.4 also shows that every prime factor r of $2p + 1$ is congruent to 1 modulo p . This can only happen if $r = 2p + 1$ and $2p + 1$ is itself prime: otherwise we get $r < p$, so r is not congruent to 1 modulo p . $\square$

6.3. The stratum $\mathcal{H}(k^{2q})$. We will now study regular origamis in the stratum $\mathcal{H}(k^{2q})$, where q is an odd prime, and k is odd. Our goal is to show:

Theorem 6.8. *Let k be an odd integer and q be an odd prime. Then, regular origamis exist in the stratum $\mathcal{H}(k^{2q})$ if and only if $q = 3$ and either:*

- $k \equiv 1 \pmod{4}$ and every prime factor of $(k+1)/2$ is congruent to 1 modulo 3; or
- $k \equiv 3 \pmod{4}$ and every prime factor of $(k+1)/4$ is congruent to 1 modulo 3.

Moreover, any regular origami belonging to such strata has a translation group isomorphic to either $(\mathbb{Z}/((k+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$ (in the former case) or $(\mathbb{Z}/((k+1)/4)\mathbb{Z} \times \mathbb{Q}_8) \rtimes \mathbb{Z}/3\mathbb{Z}$ (in the latter case).

Remark 6.9. *When either $q = 2$ or k is even, we already know that there exist regular origamis in $\mathcal{H}(k^{2q})$, constructed via semidirect products, see Section 3.3.2.*

An equivalent formulation of Theorem 6.8 is the following:

Theorem 6.10. *Let k be an odd integer and let q be an odd prime. Then, a group G of order $n = 2(k+1)q$, together with two generators $x, y \in G$ such that $[x, y]$ has order $k+1$, exists if and only if $q = 3$ and either:*

- $k \equiv 1 \pmod{4}$ and every prime factor of $(k+1)/2$ is congruent to 1 modulo 3; or
- $k \equiv 3 \pmod{4}$ and every prime factor of $(k+1)/4$ is congruent to 1 modulo 3.

Moreover, G is isomorphic to either $(\mathbb{Z}/((k+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$ (in the former case) or $(\mathbb{Z}/((k+1)/4)\mathbb{Z} \times \mathbb{Q}_8) \rtimes \mathbb{Z}/3\mathbb{Z}$ (in the latter case).

As before, we will use the notation $H = \langle [x, y] \rangle$. We start by showing that $H \neq G'$, by contradiction.

Lemma 6.11. *In the context of Theorem 6.10, we have $H < G'$.*

Proof. Assume by contradiction that $H = G'$. Observe that G/G' is abelian and has order $2q$, so it is isomorphic to $\mathbb{Z}/2q\mathbb{Z}$. Thus, G is a metacyclic group with presentation:

$$\langle a, b \mid a^{k+1} = 1, b^{2q} = a^j, [b, a] = a^{d-1} \rangle,$$

where $d^{2q} \equiv 1 \pmod{k+1}$ and $(k+1) \mid j(d-1)$. The first condition implies that d is coprime with $k+1$. Since $k+1$ is even, we get that r is odd. As a consequence, $d-1$ is even and the commutator subgroup of G , which is generated by a^{d-1} , is strictly contained in H . This is a contradiction. $\square$

Since $(G : H) = 2q$, we deduce that $(G : G')$ divides $2q$, but does not equal $2q$, so this quantity is either 1, 2 or q . We will analyze each of these cases separately, obtaining that the only admissible case is $(G : G') = q$. Unlike the case of $\mathcal{H}(2k^q)$, the subgroup H is *never* normal in G (see Lemma 6.26). Thus, we need to resort to more intricate devices.

6.3.1. *G is perfect.* We start by assuming that G is perfect, that is, $G' = G$ and we will derive a contradiction.

Throughout this section, we will not assume that k is odd, so we will prove a more general statement than needed for Theorem 6.10. That is, our goal is to show:

Proposition 6.12. *Let q be an odd prime. Then, a perfect group G , together with two generators $x, y \in G$, such that $H = \langle [x, y] \rangle$ has index $2q$, does not exist.*

Remark 6.13. *Since there exist 2-generated perfect groups, there exist regular origamis in some strata whose translation group is perfect. A notable example is the case of $\mathrm{PSL}(2, p)$, treated in Section 5.*

We will assume the existence of such a group G . In the spirit of Theorem 6.10, we write $|G| = 2(k+1)q$. Observe that this quantity has at least *three* distinct prime factors: 2 , q , and at least one more prime p . Indeed, if this were not the case, G would be solvable by Burnside's theorem (Theorem 2.6). This is impossible as nontrivial perfect groups are nonsolvable. In particular, we have $p \mid (k+1)$. We will use this fact several times throughout the proof of Proposition 6.12. In fact, we can also show that the order of $\mathbf{Z}(G)$ is not a multiple of p . More precisely:

Lemma 6.14. *In the context of Theorem 6.10, we have that $|\mathbf{Z}(G)|$ divides $2q$.*

The proof of this lemma relies on the following result:

Theorem 6.15 ([Isa08, Corollary 5.9]). *Suppose that G is a finite group and that $(G : \mathbf{Z}(G)) = \ell$. Then, the ℓ -th power of every commutator is the identity.*

Proof of Lemma 6.14. Let $\ell = (G : \mathbf{Z}(G))$. By Theorem 6.15, the ℓ -th power of $[x, y]$ is trivial. Since the order of $[x, y]$ is $k+1$, ℓ must be a multiple of $k+1$, say $\ell = t(k+1)$. Hence,

$$|\mathbf{Z}(G)| = \frac{|G|}{(G : \mathbf{Z}(G))} = \frac{2q}{t}. \quad \square$$

In fact, we will show that up to taking the quotient by $\mathbf{Z}(G)$, we can assume $\mathbf{Z}(G) = 1$. This is a consequence of:

Lemma 6.16. *In the context of Proposition 6.12, we have $\mathbf{Z}(G) \leq H$.*

Indeed, if we assume this Lemma to be true, then the group $G/\mathbf{Z}(G)$:

- is generated by $x\mathbf{Z}(G)$ and $y\mathbf{Z}(G)$;
- is perfect, as it is a quotient of a perfect group;
- is centerless, from Grün's Lemma (Lemma 2.9); and
- admits a cyclic subgroup $\langle [x\mathbf{Z}(G), y\mathbf{Z}(G)] \rangle = H/\mathbf{Z}(G)$ of index $2q$.

Thus, if a group G as in Proposition 6.12 exists, then a centerless group $G/\mathbf{Z}(G)$ as in Proposition 6.12 also exists. Hence, we can assume that G is centerless.

Before proving Lemma 6.16, we need two preliminary results.

Theorem 6.17 ([Isa08, Theorem 5.18]). *Let P be an abelian Sylow p -subgroup of a finite group G . Then,*

$$G' \cap P \cap \mathbf{Z}(\mathbf{N}_G(P)) = \{1\}.$$

Lemma 6.18. *In the context of Proposition 6.12, fix a prime number p different from 2 and q dividing $k+1$. Then, there exists a unique Sylow p -subgroup of G contained in H . Moreover, we have $\mathbf{N}_G(P) = \mathbf{N}_G(H)$, and*

$$(G : \mathbf{N}_G(H)) = q \quad \text{and} \quad (\mathbf{N}_G(H) : H) = 2.$$

In particular, $q \equiv 1 \pmod{p}$, so $q > 3$.

Proof. Let p be a prime number p different from 2 and q dividing $k+1$. There exists a Sylow p -subgroup P of H , which is unique as H is cyclic. Since $(G : H) = 2q$ and p are coprime, P is also a Sylow p -subgroup of G . Furthermore, since $P \leq H$ and H is abelian, every element of H normalizes P , so we have $H \leq \mathbf{N}_G(P) \leq G$. We will show that $(\mathbf{N}_G(P) : H) = 2$ and that $\mathbf{N}_G(H) = \mathbf{N}_G(P)$. We start by showing that both inclusions are strict.

If $\mathbf{N}_G(P) = G$, then P is normal in G . By Lemma 2.8, we have $P \leq \mathbf{Z}(G)$. This is impossible since p does not divide $|\mathbf{Z}(G)|$, as $|\mathbf{Z}(G)|$ divides $2q$ by Lemma 6.14.

If $\mathbf{N}_G(P) = H$, we have $\mathbf{Z}(\mathbf{N}_G(P)) = \mathbf{Z}(H) = H$ since H is abelian. Moreover, we have $G' \cap P \cap \mathbf{Z}(\mathbf{N}_G(P)) = P$ since G is perfect. This contradicts Theorem 6.17.

We deduce that $\mathbf{N}_G(P)$ is an index- q subgroup of G containing H . Indeed, the number of Sylow p -subgroups of G is exactly $(G : \mathbf{N}_G(P))$, and this number is congruent to 1 modulo p from Theorem 2.16. Since $(G : H) = 2q$ and $H < \mathbf{N}_G(P)$, we obtain that $(G : \mathbf{N}_G(P))$ is either 2 or q . Since $2 \not\equiv 1 \pmod{p}$, the only possibility is that $(G : \mathbf{N}_G(P)) = q$ and that $q \equiv 1 \pmod{p}$. Hence, $(\mathbf{N}_G(P) : H) = 2$ and $q > p > 2$, so $q > 3$.

Finally, we show that $\mathbf{N}_G(H) = \mathbf{N}_G(P)$. Indeed, since $(\mathbf{N}_G(P) : H) = 2$, we have that $H \triangleleft \mathbf{N}_G(P)$ by Lemma 2.2. Thus, $\mathbf{N}_G(P) \leq \mathbf{N}_G(H)$. Conversely, we have $\mathbf{N}_G(H) \leq \mathbf{N}_G(P)$ since $P \leq H$ is a characteristic subgroup of H and, therefore, conjugation by an element $g \in \mathbf{N}_G(H)$, which induces an automorphism of H , also normalizes P . This proves that $\mathbf{N}_G(H) = \mathbf{N}_G(P)$. $\square$

We can now prove Lemma 6.16.

Proof of Lemma 6.16. Let p be a prime number different from 2 and 3, and let P be a Sylow p -subgroup of G contained in H . We have $\mathbf{Z}(G) \leq \mathbf{C}_G(P) \leq \mathbf{N}_G(P)$.

Now, assume by contradiction that $\mathbf{Z}(G) \not\leq H$ and take $t \in \mathbf{Z}(G) \setminus H$. Since $t \in \mathbf{N}_G(P)$ and $(\mathbf{N}_G(P) : H) = 2$ by Lemma 6.18, we have $\mathbf{N}_G(P) = \langle H, t \rangle$. Moreover, $t \in \mathbf{C}_G(P)$ and also $H \leq \mathbf{C}_G(P)$ since $P \leq H$ and H is abelian, so we deduce that

$$\mathbf{N}_G(P) = \langle H, t \rangle \leq \mathbf{C}_G(P) \leq \mathbf{N}_G(P).$$

Hence, $P \leq \mathbf{Z}(\mathbf{C}_G(P)) = \mathbf{Z}(\mathbf{N}_G(P))$, which again contradicts Theorem 6.17. We conclude that $\mathbf{Z}(G) \leq H$. $\square$

As previously discussed, we may now assume that $\mathbf{Z}(G) = 1$. We will investigate the number of elements of order q to prove that $q \leq 3$, which will contradict $q > 3$ from Lemma 6.18. We first show:

Lemma 6.19. *In the context of Proposition 6.12, and assuming that G is centerless, we have $H \cap tHt^{-1} = \{1\}$ for any $t \in G \setminus \mathbf{N}_G(H)$.*

Proof. We first prove that $K = H \cap tHt^{-1}$ is normal by showing that $\mathbf{N}_G(K) = G$. Since $(G : \mathbf{N}_G(H)) = q$ is prime, we have $G = \langle \mathbf{N}_G(H), t \rangle$, so it is enough to establish that $\mathbf{N}_G(H) \leq \mathbf{N}_G(K)$ and that $t \in \mathbf{N}_G(K)$.

Let $s \in \mathbf{N}_G(H)$. We have that $K \leq H$ and that $sKs^{-1} \leq sHs^{-1} = H$. Since sKs^{-1} and K are subgroups of the same order of the cyclic subgroup H , we deduce that $sKs^{-1} = K$ by Theorem 2.4. Hence, $s \in \mathbf{N}_G(K)$.

Now, $K \leq tHt^{-1}$ and $tKt^{-1} \leq tHt^{-1}$. Again, tKt^{-1} and K are subgroups of the same order of the cyclic subgroup tHt^{-1} , so $tKt^{-1} = K$ by Theorem 2.4. We get that $t \in \mathbf{N}_G(K)$.

Finally, we have that $tHt^{-1} \cap H$ is a cyclic normal subgroup of G , and therefore it is central in G by Lemma 2.8. Since $\mathbf{Z}(G) = 1$, we get that $tHt^{-1} \cap H$ is trivial. $\square$

The following is a somewhat direct consequence of Lemma 6.19.

Lemma 6.20. *In the context of Proposition 6.12, and assuming that G is centerless, define $H_2 = \{h \in H \mid h^2 = 1\}$, let $t \in G \setminus \mathbf{N}_G(H)$, and take $0 \leq \beta < \alpha$ with $t^{\alpha-\beta} \notin \mathbf{N}_G(H)$. Then,*

$$t^\alpha(\mathbf{N}_G(H) \setminus H_2)t^{-\alpha} \cap t^\beta(\mathbf{N}_G(H) \setminus H_2)t^{-\beta}$$

contains at most a single element.

Proof. Recall that $(\mathbf{N}_G(H) : H) = 2$ from Lemma 6.18.

Let $u = t^{\alpha-\beta}$ and $K = \mathbf{N}_G(H) \cap u\mathbf{N}_G(H)u^{-1}$. If $s \in K$, we have $s^2 = 1$. Indeed, $s^2 \in H$ by Lemma 2.3. Similarly, $s^2 \in uHu^{-1}$. Hence, $s^2 = 1$ by Lemma 6.19.

Next, we will show that the set

$$S = (\mathbf{N}_G(H) \setminus H) \cap u(\mathbf{N}_G(H) \setminus H)u^{-1} \subseteq K$$

has at most a single element. If $s, s' \in S$, we have that $ss' \in H \cap uHu^{-1}$ by Lemma 2.3, so $ss' = 1$ by Lemma 6.19. Hence, $s' = s^{-1} = s$. We get that $|S| \leq 1$.

Now, let

$$T = (\mathbf{N}_G(H) \setminus H_2) \cap u(\mathbf{N}_G(H) \setminus H_2)u^{-1} \subseteq K.$$

We will show that $T \subseteq S$, so T also has at most a single element. Let $s \in T$.

By definition, $s \notin H_2$, so $s \notin H$ as every element of K has order at most 2. Similarly, $s \notin uH_2u^{-1}$, so $s \notin uHu^{-1}$. We deduce that $s \in S$.

Finally, we have that

$$t^\alpha(\mathbf{N}_G(H) \setminus H_2)t^{-\alpha} \cap t^\beta(\mathbf{N}_G(H) \setminus H_2)t^{-\beta} = t^\beta T t^{-\beta},$$

so the latter set also has at most a single element. $\square$

Lemma 6.19 also allows us to estimate the number of elements of order q in G .

Lemma 6.21. *In the context of Proposition 6.12, and assuming that G is centerless, we have that q^2 does not divide $|G|$. Moreover, the number of Sylow q -subgroups of G is at least $q + 1$, and each of them is isomorphic to $\mathbb{Z}/q\mathbb{Z}$. In particular, the number of order- q elements of G is at least $q^2 - 1$.*

Proof. Let $t \in G \setminus \mathbf{N}_G(H)$. Since $tHt^{-1} \cap H = \{1\}$ by Lemma 6.19 the cardinality of the set $(tHt^{-1})H$ is $|H|^2$. Indeed, by Lemma 2.1:

$$\frac{|H||tHt^{-1}|}{|H \cap tHt^{-1}|} = |H|^2.$$

Hence, $|H|^2 \leq |G|$. Dividing by $|H|$ yields

$$k + 1 = |H| \leq (G : H) = 2q.$$

Since $|G| = 2(k+1)q$, we obtain that q^2 does not divide $|G|$. Indeed, we know that $k+1$ has a prime factor p different from 2 and q , and

$$\frac{k+1}{p} \leq \frac{2q}{p} < q.$$

Therefore, any Sylow q -subgroup Q of G must be isomorphic to $\mathbb{Z}/q\mathbb{Z}$.

Now, the number of Sylow q -subgroups is congruent to 1 modulo q . However, this number cannot be 1: this would mean that Q is normal and, hence, central by Lemma 2.8. This is impossible as $\mathbf{Z}(G) = 1$. In particular, the number of Sylow q -subgroups of G is at least $q + 1$.

Finally, since every nontrivial element of $\mathbb{Z}/q\mathbb{Z}$ is generating, the intersection of two distinct Sylow q -subgroups is trivial. Thus, the number of order- q elements of G is at least $(q + 1)(q - 1) = q^2 - 1$. $\square$

We can now finish the proof of Proposition 6.12.

Proof of Proposition 6.12. First, recall that we can assume that G is centerless. Fix an order- q element $t \in G$.

We have $t \notin \mathbf{N}_G(H)$ since $q \nmid 2(k + 1) = |\mathbf{N}_G(H)|$ as $q^2 \nmid 2(k + 1)q = |G|$ by Lemma 6.21. Similarly, $t^\alpha \notin \mathbf{N}_G(H)$ for every $1 \leq \alpha \leq q - 1$, as the order of this element is also q .

Consider the set $S = \bigcup_{\alpha=0}^{q-1} t^\alpha \mathbf{N}_G(H) t^{-\alpha}$. We claim that

$$|S| \geq 1 + |G| - \frac{q(q + 3)}{2}.$$

Indeed, set $H_2 = \{h \in H \mid h^2 = 1\}$. From Theorem 2.4, we have $|H_2| \leq 2$. Now, we estimate the elements of S by excising H_2 from $\mathbf{N}_G(H)$ and using Lemma 6.20:

$$\begin{aligned} |S| &\geq 1 + \sum_{\alpha=0}^{q-1} \left(|t^\alpha (\mathbf{N}_G(H) \setminus H_2) t^{-\alpha}| \right. \\ &\quad \left. - \sum_{\beta=0}^{\alpha-1} |t^\alpha (\mathbf{N}_G(H) \setminus H_2) t^{-\alpha} \cap t^\beta (\mathbf{N}_G(H) \setminus H_2) t^{-\beta}| \right) \\ &\geq 1 + \sum_{\alpha=0}^{q-1} (|\mathbf{N}_G(H)| - 2 - \alpha) = 1 + q|\mathbf{N}_G(H)| - \frac{q(q + 3)}{2} = 1 + |G| - \frac{q(q + 3)}{2}, \end{aligned}$$

where the “1” corresponds to counting the trivial element, and where we used that $(G : \mathbf{N}_G(H)) = q$ from Lemma 6.18.

Finally, Lemma 6.21 shows that G contains at least $q^2 - 1$ elements of order q . Since no element of S has order q (using that q does not divide $|\mathbf{N}_G(H)|$), we get:

$$(q^2 - 1) + \left(1 + |G| - \frac{q(q + 3)}{2} \right) \leq |G|.$$

Hence,

$$q^2 \leq \frac{q(q + 3)}{2}.$$

This inequality holds if and only if $0 \leq q \leq 3$, which contradicts that $q > 3$ from Lemma 6.18. $\square$

6.3.2. G' has index two. We now assume that G' has index two inside G , and we will again derive a contradiction. That is, our goal is to show:

Lemma 6.22. *Let k be an odd integer and let q be an odd prime. Then, a group G of order $n = 2(k + 1)q$ with $(G : G') = 2$, together with two generators $x, y \in G$ such that $[x, y]$ has order $k + 1$, does not exist.*

We start by showing that such a group must admit a normal $2'$ -Hall subgroup:

Lemma 6.23. *In the context of Lemma 6.22, G contains a normal $2'$ -Hall subgroup.*

Proof. We will use the Frobenius p -complement theorem (Theorem 2.22), that is, we need to show that, for every 2-subgroup $X \leq G$, we have that $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is also a 2-group.

Recall that $H = \langle [x, y] \rangle$ and write $k + 1 = 2^\alpha \ell$, with ℓ odd. By Theorem 2.4, H admits a cyclic subgroup $L \leq H$ of order 2^α .

Observe that $(G : L) = 2\ell q$ is even, but not divisible by 4. Thus, Lemma 2.27 shows that X admits a cyclic subgroup of index two. Hence, X is isomorphic to one of the groups in Theorem 2.18.

Recall that $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ injects into $\text{Aut}(X)$ (Remark 2.24). By Proposition 2.19, we have that $\text{Aut}(X)$ is 2-group, except when $X \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and when $X \simeq Q_8$. Thus, we only need to focus on these two cases.

Assume then that $X \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $X \simeq Q_8$. Since X is not cyclic, it is not contained in G' . Indeed, L is cyclic and is a Sylow 2-subgroup of G' , so every 2-subgroup of G' is cyclic by Sylow's theorems (Theorem 2.16) and Theorem 2.4. Then, $(G : G') = 2$ implies that $G = XG'$. Defining $K = X \cap G'$ and using that $G' \triangleleft G$, the second isomorphism theorem shows that

$$(X : K) = (XG' : G') = (G : G') = 2.$$

Since every index-two subgroup of X is cyclic, we also obtain that K is cyclic.

Let $s \in K$ be a generator of K . Let $t \in X \setminus K = X \setminus G'$. Since $(X : K) = 2$ is prime, we have that $X = \langle K, t \rangle$, so $X = \langle s, t \rangle$.

Now, let $\varphi \in \mathbf{N}_G(X)/\mathbf{C}_G(X)$ seen a subgroup of $\text{Aut}(X)$. We claim that φ preserves K and $X \setminus K$. To see this, observe that φ acts on X by conjugation by an element of G , so there exists an inner automorphism $\bar{\varphi} \in \text{Inn}(G)$ such that $\bar{\varphi}|_X = \varphi$. Since G' is normal in G , $\bar{\varphi}$ preserves G' , so φ preserves K . The second equality follows from the first, as φ is bijective.

Finally, we check the two particular cases:

Case 1: When $X \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the group $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ has at most 2 elements. Indeed, $\varphi(s) = s$ and $\varphi(t) \in \{t, ts\}$.

Case 2: When $X \simeq Q_8$, the order of $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ divides 8. Indeed, s has order 4, so $\varphi(s) \in \{s, s^3\}$. Moreover, $\varphi(t) \in Q_8 \setminus \langle s \rangle = \{t, st, s^2t, s^3t\}$. We get $\mathbf{N}_G(X)/\mathbf{C}_G(X) \leq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

From Theorem 2.22, we conclude that G has a normal 2-complement. $\square$

We can now finish the proof of Lemma 6.22:

Proof of Lemma 6.22. By Lemma 6.23, G contains a normal $2'$ -Hall subgroup N . Since $2^2 \nmid 2 = (G : G')$, Lemma 2.25 shows that

$$G \simeq N \rtimes \mathbb{Z}/2\mathbb{Z},$$

where $|N|$ is odd. In particular, $|G|$ is not divisible by 4, which contradicts that $|G| = 2(k+1)q$ for odd k . $\square$

6.3.3. G' has index q . We finally focus on the case where G' has index q inside G . We will show that regular origamis can exist in the stratum $\mathcal{H}(k^{2q})$ under very special conditions:

Proposition 6.24. *Let k be an odd integer and let q be an odd prime. Then, a group G of order $n = 2(k+1)q$ with $(G : G') = q$, together with two generators $x, y \in G$ such that $[x, y]$ has order $k+1$, exists if and only if $q = 3$ and either:*

- $k \equiv 1 \pmod{4}$ and every prime factor of $(k+1)/2$ is congruent to 1 modulo 3; or
- $k \equiv 3 \pmod{4}$ and every prime factor of $(k+1)/4$ is congruent to 1 modulo 3.

Moreover, G is isomorphic to either $(\mathbb{Z}/((k+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$ (in the former case) or $(\mathbb{Z}/((k+1)/4)\mathbb{Z} \times Q_8) \rtimes \mathbb{Z}/3\mathbb{Z}$ (in the latter case).

Remark 6.25. *Any regular origami in $\mathcal{H}(k^{2q})$, for odd k and odd prime q , has genus g satisfying $g-1 = qk = 3k$, so $3 \mid (g-1)$. Since the genera covered by the statement of Theorem 6.1 never satisfy this property, the existence of such origamis is not an obstruction for this theorem.*

We start by remarking that $(G' : H) = 2$, so H is normal in G' by Lemma 2.2. We will use this fact several times. Nevertheless, H is not normal in G :

Lemma 6.26. *Let G be a group as in Lemma 6.27. Then, $H = \langle [x, y] \rangle$ is not normal in G .*

Proof. Assume that H is normal. Consider the short exact sequence

$$1 \rightarrow G' \rightarrow G \rightarrow \mathbb{Z}/q\mathbb{Z} \rightarrow 1.$$

Since $(G' : H) = 2$, the quotient by H yields the short exact sequence:

$$1 \rightarrow \mathbb{Z}/2\mathbb{Z} \simeq G'/H \rightarrow G/H \rightarrow \mathbb{Z}/q\mathbb{Z} \rightarrow 1.$$

We deduce that G/H is a metacyclic group with presentation:

$$G/H = \langle a, b \mid a^2 = 1, b^q = a^\varepsilon \text{ and } [b, a] = a^{d-1} \rangle,$$

where $d^q \equiv 1 \pmod{2}$ and $2 \mid \varepsilon(d-1)$. In particular, d is odd, so $d-1$ is even and the group is abelian. Hence, $(G/H)'$ is trivial. We deduce that $G'/H \simeq (G/H)'$ is trivial, which is a contradiction. $\square$

Now, we can greatly restrict the structure of G' :

Lemma 6.27. *In the context of Proposition 6.24, we have $G' \simeq \mathbb{Z}/\lambda\mathbb{Z} \times L$, where either $L \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $L \simeq Q_8$ and λ is odd. Furthermore, L is normal in G .*

Proof. Write $k+1 = |H| = 2^\alpha \lambda$ (where $\alpha \geq 1$ since k is odd by assumption). Let K be the unique subgroup of H of order λ . Notice that K is normal in G' , since it is a characteristic subgroup of H , which has index two in G' . As a consequence, and again using that $(G : H) = 2$, we obtain that K is a normal 2'-Hall subgroup of G' . In particular, the Schur–Zassenhaus theorem (Theorem 2.13) shows that:

$$G' \simeq \mathbb{Z}/\lambda\mathbb{Z} \rtimes L,$$

where L is a 2-group of order $2^{\alpha+1}$. In fact, a normal Hall subgroup is characteristic [Rot95, Exercise 5.31], so K is characteristic in G' and normal in G . In particular, we can use Lemma 2.8 to conclude that $K \leq \mathbf{Z}(G')$. This implies that the semidirect product is actually a direct product. Moreover, the 2-group L contains a cyclic

subgroup of index two, so it is one of the groups of Theorem 2.18. Furthermore, since λ and $|L|$ are coprime, we have

$$\text{Aut}(G') \simeq \text{Aut}(\mathbb{Z}/\lambda\mathbb{Z} \times L) \simeq \text{Aut}(\mathbb{Z}/\lambda\mathbb{Z}) \times \text{Aut}(L),$$

so, in particular, L is characteristic in G' and, hence, normal in G by Lemma 2.5.

Assume now by contradiction that L is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Q}_8$. Using Proposition 2.20, it contains a characteristic subgroup U of index two. Since L is normal in G , we deduce that U is normal in G by Lemma 2.5. Thus, the group G/U lies in the short exact sequence:

$$1 \rightarrow G'/U \rightarrow G/U \rightarrow G/G' \rightarrow 1$$

Since $G'/U \simeq (\mathbb{Z}/\lambda\mathbb{Z} \times L)/U \simeq \mathbb{Z}/\lambda\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\lambda\mathbb{Z}$ and $G/G' \simeq \mathbb{Z}/q\mathbb{Z}$ is cyclic, we have:

$$1 \rightarrow \mathbb{Z}/2\lambda\mathbb{Z} \rightarrow G/U \rightarrow \mathbb{Z}/q\mathbb{Z} \rightarrow 1.$$

Therefore, G/U is a metacyclic group with presentation:

$$\langle x, y \mid x^{2\lambda} = 1, y^q = x^r \text{ and } [y, x] = x^{d-1} \rangle,$$

where $d^q = 1 \pmod{2\lambda}$. In particular, d is odd. Consequently, $d-1$ is even and $2 \mid \gcd(d-1, 2\lambda)$. In particular, from Lemma 2.12, we deduce that $(G/U)'$ is strictly contained in $G'/U \simeq \mathbb{Z}/2\lambda\mathbb{Z}$. This is a contradiction since $(G/U)' \simeq G'/U$. $\square$

According to Lemma 6.27, we only have to distinguish two cases for G' . When $G' \simeq \mathbb{Z}/\lambda\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we have that $|G| = 2(k+1)q = (4\lambda) \cdot q$, so $\lambda = (k+1)/2$. This number is an odd integer, so we get that $k \equiv 1 \pmod{4}$. Similarly, when $G' \simeq \mathbb{Z}/\lambda\mathbb{Z} \times \mathbb{Q}_8$, we have that $|G| = 2(k+1)q = (8\lambda) \cdot q$, so $\lambda = (k+1)/4$. This number is an odd integer, so we get $k \equiv 3 \pmod{8}$ (and, in particular, $k \equiv 3 \pmod{4}$).

We will now show the desired conditions on q and λ , and group structure for G :

Lemma 6.28. *Let G be a group as in Proposition 6.24. Then, $q = 3$ and every prime factor of λ is congruent to 1 modulo 3. Furthermore, $G \simeq (\mathbb{Z}/\lambda\mathbb{Z} \times L) \rtimes \mathbb{Z}/3\mathbb{Z}$, where $L \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $L \simeq \mathbb{Q}_8$.*

Proof. Write $G' = \mathbb{Z}/\lambda\mathbb{Z} \times L$, with $L \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $L \simeq \mathbb{Q}_8$, as per Lemma 6.27.

We start by proving that $q = 3$. On the one hand, observe that, since H is not normal in G by Lemma 6.26, we have $\mathbf{N}_G(H) < G$. Moreover, since $(G' : H) = 2$, H is normal in G' by Lemma 2.2, and $G' \leq \mathbf{N}_G(H)$. We deduce $G' \leq \mathbf{N}_G(H) < G$. Since $(G : G') = q$ is prime, we get that $\mathbf{N}_G(H) = G'$. Thus,

$$(G : \mathbf{N}_G(H)) = (G : G') = q,$$

so the number of conjugacy classes of H inside G is exactly q .

On the other hand, the number of cyclic subgroups of index two inside L is exactly three: either $\langle(1,0)\rangle$, $\langle(0,1)\rangle$, and $\langle(1,1)\rangle$ if $L \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; or $\langle\mathbf{i}\rangle$, $\langle\mathbf{j}\rangle$, and $\langle\mathbf{k}\rangle$ if $L \simeq \mathbb{Q}_8$. This also holds inside $G' \simeq \mathbb{Z}/\lambda\mathbb{Z} \times L$, since λ is odd. Therefore, the number of conjugacy classes of H inside G' is at most 3. We deduce that $q \leq 3$, so $q = 3$ as it is an odd prime.

Now, L is normal in G by Lemma 6.27. The quotient $K = G/L$ is part of the short exact sequence:

$$1 \rightarrow \mathbb{Z}/\lambda\mathbb{Z} \rightarrow K \rightarrow \mathbb{Z}/3\mathbb{Z} \rightarrow 1,$$

so K is a metacyclic group with presentation

$$K = \langle a, b \mid a^\lambda = 1, b^3 = a^i \text{ and } [b, a] = a^{d-1} \rangle,$$

where $d^3 \equiv 1 \pmod{\lambda}$ and $\lambda \mid i(d-1)$. Since $H = \langle [x, y] \rangle$ contains $\mathbb{Z}/\lambda\mathbb{Z}$, we deduce that $[xL, yL] \in K'$ generates the group $\mathbb{Z}/\lambda\mathbb{Z} \leq K$. Moreover, we have $K' = \langle a^{d-1} \rangle$ by Lemma 2.12, so we deduce that $\gcd(d-1, \lambda) = 1$. This gives the desired conditions on λ by Proposition B.1.

Finally, since G' has order 2λ or 4λ , with $\lambda \equiv 1 \pmod{3}$, and $(G : G') = q = 3$, the Schur–Zassenhaus theorem (Theorem 2.13) implies that

$$G \simeq G' \rtimes \mathbb{Z}/3\mathbb{Z} \simeq (\mathbb{Z}/\lambda\mathbb{Z} \times L) \rtimes \mathbb{Z}/3\mathbb{Z},$$

as desired. $\square$

To complete the proof of Proposition 6.24, we exhibit groups, together with two generators, satisfying the required properties:

Proof of Proposition 6.24. Let $k \geq 1$ be odd and assume that it satisfies the hypothesis of Proposition 6.24. Concretely, we define $\lambda = (k+1)/2$ if $k \equiv 1 \pmod{4}$ and $\lambda = (k+1)/4$ if $k \equiv 3 \pmod{4}$, and assume that every prime factor of λ is congruent to 1 modulo 3 (in particular, λ is odd).

We will exhibit a group G of order $n = 6(k+1)$, together with two generators $x, y \in G$, such that $[x, y]$ has order $k+1$. Since the assumed conditions on λ are necessary by Lemma 6.28, this is enough to finish the proof.

We know that there exists $r \in \mathbb{Z}/\lambda\mathbb{Z}$ such that $r^3 = 1$ and such that $r-1$ has order λ by Proposition B.1.

Now, Lemma 6.28 suggests considering two cases:

Case 1: Let $G = (\mathbb{Z}/\lambda\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_{\varphi \times \theta} \mathbb{Z}/3\mathbb{Z}$, where $\varphi: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/\lambda\mathbb{Z})$ and $\theta: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ are explicitly given by the relations $\varphi(1)(1) = r$, and $\theta(1)(u, v) = (u+v, u)$. Since both $\varphi(1)$ and $\theta(1)$ have order 3, the semidirect product construction giving G is well-defined.

Consider the elements $x = ((1, 1, 0), 0)$ and $y = ((0, 0, 1), 1)$. We will show that $G = \langle x, y \rangle$ and that $[x, y]$ has order $k+1 = 2\lambda$.

We compute the commutator:

$$\begin{aligned} [x, y] &= ((1, 1, 0), 0) \cdot ((0, 0, 1), 1) \cdot ((1, 1, 0), 0)^{-1} \cdot ((0, 0, 1), 1)^{-1} \\ &= ((1, 1, 0), 0) \cdot ((0, 0, 1), 1) \cdot ((-1, 1, 0), 0) \cdot ((0, 1, 1), -1) \\ &= ((1, 1, 1), 1) \cdot ((-1, 1, 0), 0) \cdot ((0, 1, 1), -1) \\ &= ((1-r, 0, 0), 1) \cdot ((0, 1, 1), -1) \\ &= ((1-r, 0, 1), 0). \end{aligned}$$

Since $1-r$ has order λ in $\mathbb{Z}/\lambda\mathbb{Z}$ and $(0, 1)$ has order 2 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which are coprime, we obtain that

$$\text{ord}([x, y]) = \text{ord}(1-r) \text{ord}(1) = 2\lambda = k+1.$$

Moreover, since $(1, 0)$ and $(0, 1)$ generate $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and λ and 4 are coprime, Lemma 3.5 shows that $x' = (1, 1, 0)$ and $y' = (0, 0, 1)$ generate $\mathbb{Z}/\lambda\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now, observe that $y^2 x^\lambda y = (y', 0)$. Indeed,

$$\begin{aligned} y^2 x^\lambda y &= ((0, 0, 1), 1) \cdot ((0, 0, 1), 1) \cdot (\lambda(1, 1, 0), 0) \cdot ((0, 0, 1), 1) \\ &= ((0, 1, 1), 2) \cdot ((0, 1, 0), 0) \cdot ((0, 0, 1), 1) \\ &= ((0, 1, 0), 2) \cdot ((0, 0, 1), 1) \\ &= ((0, 0, 1), 0) = (y', 0). \end{aligned}$$

In particular, $\langle x, y \rangle$ contains $(\mathbb{Z}/\mathbb{Z}\lambda \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \{0\}$. Furthermore, it contains the two elements y and y^2 , which belong respectively to $(\mathbb{Z}/\mathbb{Z}\lambda \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \{1\}$ and to $(\mathbb{Z}/\mathbb{Z}\lambda \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \{2\}$. Therefore $G = \langle x, y \rangle$.

Case 2: Let $G = (\mathbb{Z}/\lambda\mathbb{Z} \times \mathbb{Q}_8) \rtimes_{\varphi \times \theta} \mathbb{Z}/3\mathbb{Z}$, where $\varphi: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/\lambda\mathbb{Z})$ and $\theta: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Q}_8)$ are explicitly given by the relations $\varphi(1)(1) = r$, and

$$\theta(1)(-1) = -1, \quad \theta(1)(\mathbf{i}) = -\mathbf{j}, \quad \theta(1)(\mathbf{j}) = \mathbf{k}, \quad \theta(1)(\mathbf{k}) = -\mathbf{i}.$$

Since both $\varphi(1)$ and $\theta(1)$ have order 3, the semidirect product construction giving G is well-defined.

Consider the elements $x = ((1, \mathbf{i}), 0)$ and $y = ((0, \mathbf{k}), 1)$. We will show that $G = \langle x, y \rangle$ and that $[x, y]$ has order $k + 1 = 4\lambda$.

We compute the commutator:

$$\begin{aligned} [x, y] &= ((1, \mathbf{i}), 0) \cdot ((0, \mathbf{k}), 1) \cdot ((1, \mathbf{i}), 0)^{-1} \cdot ((0, \mathbf{k}), 1)^{-1} \\ &= ((1, \mathbf{i}), 0) \cdot ((0, \mathbf{k}), 1) \cdot ((-1, -\mathbf{i}), 0) \cdot ((0, -\mathbf{j}), -1) \\ &= ((1, -\mathbf{j}), 1) \cdot ((-1, -\mathbf{i}), 0) \cdot ((0, -\mathbf{j}), -1) \\ &= ((1 - r, 1), 1) \cdot ((0, -\mathbf{j}), -1) \\ &= ((1 - r, -\mathbf{k}), 0). \end{aligned}$$

Since $1 - r$ has order λ in $\mathbb{Z}/\lambda\mathbb{Z}$ and $-\mathbf{k}$ has order 4 in $\mathbb{Q}_8$, which are coprime, we obtain that

$$\text{ord}([x, y]) = \text{ord}(1 - r) \text{ord}(-\mathbf{k}) = 4\lambda = k + 1.$$

Moreover, since $\mathbf{i}$ and $\mathbf{k}$ generate $\mathbb{Q}_8$, and λ and 8 are coprime, Lemma 3.5 shows that $x' = (1, \mathbf{i})$ and $y' = (0, \mathbf{k})$ generate $\mathbb{Z}/\lambda\mathbb{Z} \times \mathbb{Q}_8$.

Now, choose $\varepsilon \in \{1, 3\}$ so that $\lambda \equiv \varepsilon \pmod{4}$. We have that $y^2 x^{\varepsilon\lambda} y = (y', 0)$. Indeed,

$$\begin{aligned} y^2 x^{\varepsilon\lambda} y &= ((0, \mathbf{k}), 1) \cdot ((0, \mathbf{k}), 1) \cdot ((1, \mathbf{i})^{\varepsilon\lambda}, 0) \cdot ((0, \mathbf{k}), 1) \\ &= ((0 + \varphi(1)(0), \mathbf{k} \cdot \theta(1)(\mathbf{k})), 2) \cdot ((0, \mathbf{i}), 0) \cdot ((0, \mathbf{k}), 1) \\ &= ((0, -\mathbf{j}), 2) \cdot ((0, \mathbf{i}), 0) \cdot ((0, \mathbf{k}), 1) \\ &= ((0, -\mathbf{j} \cdot \theta(2)(\mathbf{i})), 2) \cdot ((0, \mathbf{k}), 1) \\ &= ((0, \mathbf{i}), 2) \cdot ((0, \mathbf{k}), 1) \\ &= ((0, \mathbf{i} \cdot \theta(2)(\mathbf{k})), 3) \\ &= ((0, \mathbf{k}), 0) = (y', 0). \end{aligned}$$

In particular, $\langle x, y \rangle$ contains $(\mathbb{Z}/\mathbb{Z}\lambda \times \mathbb{Q}_8) \times \{0\}$. Furthermore, it contains the two elements y and y^2 , which belong respectively to $(\mathbb{Z}/\mathbb{Z}\lambda \times \mathbb{Q}_8) \times \{1\}$ and to $(\mathbb{Z}/\mathbb{Z}\lambda \times \mathbb{Q}_8) \times \{2\}$. Therefore $G = \langle x, y \rangle$. □

6.4. Proof of Theorem 6.1. Assume g is either of the form $g = p+1$ or $g = pq+1$, where $p, q > 3$ are prime numbers. Recall from Section 3.3 that a genus- g regular origami can only belong to a stratum of the form $\mathcal{H}(m^s)$, where $m \mid (2g-2)$ and $s = (2g-2)/m$. Furthermore:

- since $g-1$ is not divisible by 2 or 3, $g \notin \mathbf{G}(1)$ by the work of Schlage-Puchta and Weitze-Schmithüsen [SW17, Theorem 1.1], and we can rule out the case $m = 1$;
- since $g-1$ is not divisible by 2 or 9, we can rule out the case $m = 2$ by Theorem 4.2;
- it is well-known that every origami in a minimal stratum $\mathcal{H}(2g-2)$ has a trivial automorphism group [MMY15, Proposition 2.4]. In particular, no regular origamis exist in the stratum $\mathcal{H}(2g-2)$ and we can rule out the case $m = 2g-2$.

Now, if $g = p+1$, the only remaining divisor of $2g-2 = 2p$ is $m = p = g-1$, and this case is also ruled out by Lemma 6.3 since p is odd by assumption. This shows that there are no regular origamis in case (1).

If $g = pq+1$, we can rule out $m = pq = g-1$ for the same reason. Therefore, we only need to consider the additional divisors $p, q, 2p$, and $2q$.

The cases $m = p$ and $m = q$ correspond to the symmetric cases $\mathcal{H}(p^{2q})$ and $\mathcal{H}(q^{2p})$. Since $p, q > 3$, this case is treated in Theorem 6.8, showing that no regular origamis exist.

The cases $m = 2p$ and $m = 2q$ correspond to $\mathcal{H}(2p^q)$ or $\mathcal{H}(2q^p)$. We know that such strata contain regular origamis by Corollary 6.7 if and only if $p = q$ is a Sophie Germain prime. This shows that:

- there are no regular origamis if either (2), or (3) holds;
- if $g = p^2 + 1$ and $p \geq 5$ is a Sophie Germain prime, every genus- g regular origami belongs to $\mathcal{H}(2p^p)$ and has translation group $\mathbb{Z}/(2p+1)\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. Therefore, $p^2 + 1 \in \mathbf{G}(2p)$.

APPENDIX A. EXPLICIT COMPUTATIONS AND SUMMARIES

The following table shows regular origamis apparently realizing a maximal translation group for each g such that $t(g) \leq 2000$. We also include the values of $m(g)$, and of $c(g) = t(g)/(g-1) = 2(m(g)+1)/m(g)$. The examples were found using randomized computer experiments, so some values of $t(g)$ could actually be larger, and some regular origamis could be missing.

For all unlisted values of g , we have $t(g) = 4(g-1)$ if $g-1$ is even or divisible by 3. Otherwise, if no genus- g regular origami exists, then $t(g) = 2(g-1)$ (but, since some regular origamis could be missing from this list, we cannot ensure that this is the case if g is unlisted and $g-1$ is both odd and not divisible by 3). We include a translation group with a short description that realizes the maximal number of translations for each genus, although this choice is, in general, not unique.

g	$t(g)$	$m(g)$	$c(g)$	Stratum	Translation group
26	55	10	11/5	$\mathcal{H}(10^5)$	$\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}$
122	253	22	23/11	$\mathcal{H}(22^{11})$	$\mathbb{Z}/23\mathbb{Z} \rtimes \mathbb{Z}/11\mathbb{Z}$
126	275	10	11/5	$\mathcal{H}(10^{25})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z}$
176	385	10	11/5	$\mathcal{H}(10^{35})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/7\mathbb{Z}$
246	497	70	71/35	$\mathcal{H}(70^7)$	$\mathbb{Z}/71\mathbb{Z} \rtimes \mathbb{Z}/7\mathbb{Z}$
276	660	5	12/5	$\mathcal{H}(5^{110})$	$\text{PSL}(2, 11)$
326	715	10	11/5	$\mathcal{H}(10^{65})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/13\mathbb{Z}$
426	935	10	11/5	$\mathcal{H}(10^{85})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/17\mathbb{Z}$
456	1092	5	12/5	$\mathcal{H}(5^{182})$	$\text{PSL}(2, 13)$
476	1045	10	11/5	$\mathcal{H}(10^{95})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/19\mathbb{Z}$
530	1081	46	47/23	$\mathcal{H}(46^{23})$	$\mathbb{Z}/47\mathbb{Z} \rtimes \mathbb{Z}/23\mathbb{Z}$
576	1265	10	11/5	$\mathcal{H}(10^{115})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/23\mathbb{Z}$
606	1331	10	11/5	$\mathcal{H}(10^{121})$	$\mathbb{Z}/121\mathbb{Z} \rtimes \mathbb{Z}/11\mathbb{Z}$
626	1375	10	11/5	$\mathcal{H}(10^{125})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/25\mathbb{Z}$
726	1595	10	11/5	$\mathcal{H}(10^{145})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/29\mathbb{Z}$
776	1705	10	11/5	$\mathcal{H}(10^{155})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/31\mathbb{Z}$
834	1673	238	239/119	$\mathcal{H}(238^7)$	$\mathbb{Z}/239\mathbb{Z} \rtimes \mathbb{Z}/7\mathbb{Z}$
842	1711	58	59/29	$\mathcal{H}(58^{29})$	$\mathbb{Z}/59\mathbb{Z} \rtimes \mathbb{Z}/29\mathbb{Z}$
846	1703	130	131/65	$\mathcal{H}(130^{13})$	$\mathbb{Z}/131\mathbb{Z} \rtimes \mathbb{Z}/13\mathbb{Z}$
848	1771	22	23/11	$\mathcal{H}(22^{77})$	$(\mathbb{Z}/23\mathbb{Z} \rtimes \mathbb{Z}/11\mathbb{Z}) \times \mathbb{Z}/7\mathbb{Z}$
876	1925	10	11/5	$\mathcal{H}(10^{175})$	$(\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/35\mathbb{Z}$

TABLE 1. Value of $t(g)$ for small g .

For each prime $2 < m \leq 300$ with $m \equiv 2 \pmod{3}$, the following table shows the smallest prime p satisfying the conditions in Lemma 5.5. Namely, we have that $p \equiv \pm 1 \pmod{2(m+1)}$ and that $(p-1)(p+1)/(4(m+1))$ is an integer not divisible by any prime number $q < m$. Hence, the regular origami with translation group $G = \text{PSL}(2, p)$ produces a genus- g surface with $g \in \mathcal{G}(m)$. We also include $n = |G|$.

m	p	g	n
5	11	276	660
11	23	2784	6072
17	37	11952	25308
23	47	24864	51888
29	59	49620	102660
41	83	139524	285852
47	5087	32224176332	65819594208
53	107	300564	612468
59	7079	87208034462	177372273480
71	13967	671699860608	1362320844048
83	167	1150464	2328648
89	179	1417860	2867580
101	23053	3032798528504	6125652473412
107	24407	3601166766512	7269645061368
113	227	2898564	5848428
131	263	4513344	9095592
137	277	5274912	10626828
149	44699	22178309490152	44654314409700
167	56113	43907394117050	88340625289392
173	347	10385364	20890788
179	359	11502720	23133960
191	383	13972224	28090752
197	397	15563592	31285188
227	457	23756232	47721768
233	467	25352964	50923548
239	479	27360960	54950880
251	503	31689504	63631512
257	200723	2013932191752920	4043537007566172
263	138863	666885785842058	1338842946481392
269	541	39438360	79169940
281	563	44455044	89226492
293	587	50393364	101130708

TABLE 2. Choice of p so $g \in \mathcal{G}(m)$.

The following table summarizes our current knowledge about the sets $G(m)$ for $m \in \{1, \dots, 25\}$. As previously stated, $G(1)$ was completely classified by Schlage-Puchta and Weitze-Schmithüßen [SW17]. Additionally, such sets are empty since $3 \mid m$ or $4 \mid m$ (Theorem 3.1). Moreover, if $m \in \{5, 11, 17, 23\}$, then m is prime and satisfies $m \equiv 2 \pmod{3}$, so $G(m)$ is large (Theorem 5.1). Furthermore, when $m \in \{10, 22\}$, then $m = 2p$ for p a Sophie Germain prime, so $G(m)$ is nonempty (Theorem 6.1). Finally, we do not know if $G(m)$ is empty or not for the remaining values of m .

m	$G(m)$
1	$\{g \geq 2 \mid g - 1 \not\equiv \pm 1 \pmod{6}\}$
2	Empty
3	Empty
4	Empty
5	Contains infinitely long arithmetic progressions
6	Empty
7	Empty
8	Empty
9	Empty
10	Nonempty
11	Contains infinitely long arithmetic progressions
12	Empty
13	?
14	?
15	Empty
16	Empty
17	Contains infinitely long arithmetic progressions
18	Empty
19	?
20	Empty
21	Empty
22	Nonempty
23	Contains infinitely long arithmetic progressions
24	Empty
25	?

TABLE 3. Summary of $G(m)$.

APPENDIX B. COMMUTATOR SUBGROUP OF $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z}$

In this section, we prove:

Proposition B.1. *Let $u \geq 1$ be an integer and q be a prime number. Then, the following are equivalent:*

- (1) *There exists $d \in \{2, \dots, u-1\}$ such that the commutator subgroup of the semidirect product $\mathbb{Z}/u\mathbb{Z} \rtimes_d \mathbb{Z}/q\mathbb{Z}$ is isomorphic to $\mathbb{Z}/u\mathbb{Z}$;*
- (2) *There exists $d \in \{2, \dots, u-1\}$ with $d^q \equiv 1 \pmod{u}$ and $\gcd(d-1, u) = 1$;*
- (3) *Every prime factor of u is congruent to 1 modulo q .*

It is clear from the last property that u must be odd for it to hold. Indeed, if $q = 2$, the property states that every prime factor of u is odd. If $q > 2$, the property implies that 2 is not a prime factor of u .

Moreover, the first two properties are equivalent by Lemma 2.12. We will show that the last two are equivalent. In fact, we will show a slightly more general result which is useful for our purposes: we are interested in the case where a semidirect product realizes the translation group of a regular origami in a given stratum.

We have:

Proposition B.2. *Let $u, \ell \geq 1$ be integers. Assume u is odd. Then, the following are equivalent:*

- (1) *There exist integers $m, n \geq 1$ and $d \in \{2, \dots, m-1\}$ such that the regular origami induced by the group $\mathbb{Z}/m\mathbb{Z} \rtimes_d \mathbb{Z}/n\mathbb{Z}$ and the generators $x = (1, 0)$ and $y = (0, 1)$ belongs to the stratum $\mathcal{H}((u-1)^\ell)$;*
- (2) *There exist integers m, n and $d \in \{2, \dots, n-1\}$ such that:*
 - $mn = u\ell$,
 - $d^n \equiv 1 \pmod{m}$,
 - $\gcd(d-1, m) = m/u$;
- (3) *For every prime power p^α dividing u , we have either*
 - $p^{\alpha+1} \mid \ell$, or
 - $p \equiv 1 \pmod{q}$ for some prime divisor q of ℓ .

Remark B.3. *If u is even, the number d in the first property exists if and only if ℓ is a multiple of 4. In that case, one can choose $\mathbb{Z}/2u\mathbb{Z} \rtimes_{-1} \mathbb{Z}/(\ell/2)\mathbb{Z}$.*

Proposition B.1 is obtained from Proposition B.2 by taking $m = u$ and $\ell = n = q$. We first state the following structure result for cyclic p -groups:

Proposition B.4. *Let $p \neq 2$ be prime and let $\alpha \geq 1$ be an integer. Then, the group $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is cyclic of order $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$. Furthermore, for any $1 \leq \gamma \leq \alpha-1$, the set*

$$H_\gamma = \{x \in \mathbb{Z}/p^\alpha\mathbb{Z} \mid x \equiv 1 \pmod{p^\gamma}\}$$

is the (unique) subgroup of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ of order $p^{\alpha-\gamma}$, and is generated by $(1+p^\gamma)$.

Proof. The facts that $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is cyclic and that H_1 is generated by $1+p$ are well-known [Rot95, Theorem 6.7]. The proof readily extends to the general case. $\square$

We can now prove Proposition B.2:

Proof of Proposition B.2. For any fixed finite group G , recall that the stratum $\mathcal{H}((u-1)^\ell)$ contains a regular origami with translation group G if and only if

there exist generators $x, y \in G$ such that $H = \langle [x, y] \rangle$ has order u and index ℓ . In the case where $G = \mathbb{Z}/m\mathbb{Z} \rtimes_d \mathbb{Z}/n\mathbb{Z}$, this is equivalent to the conditions:

- (i) $nm = |G| = u\ell$ (so a subgroup can have order u and index ℓ);
- (ii) $d^n \equiv 1 \pmod{m}$ (for the semidirect product to be well-defined); and
- (iii) $\gcd(d-1, m) = m/u$ (to have $G' \simeq \mathbb{Z}/u\mathbb{Z}$).

Therefore, properties (1) and (2) are indeed equivalent. We will show that properties (2) and (3) are equivalent.

(2) $\implies$ (3). Assume the existence of such m, n and d , and write $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$ for the prime factorization of m and n , respectively.

By condition (iii), u is a divisor of m , so its prime factors are among the $p_1, \dots, p_r$. Take $i \in \{1, \dots, r\}$ such that $p_i \mid u$. Observe that $p_i \neq 2$, since u is assumed to be odd. In particular, $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ is cyclic.

From condition (ii), we deduce that $d^n \equiv 1 \pmod{p_i^{\alpha_i}}$. In particular, n is a multiple of the order $\text{ord}(d)$ of d in the group $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$. We also deduce that the prime factorization of $\text{ord}(d)$ can be written in terms of the $q_1, \dots, q_s$.

Let $\gamma_i \in \mathbb{N}$ be the multiplicity of p_i in the prime decomposition of $d-1$. We apply Proposition B.4 to the group $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ and define the groups $H_1, \dots, H_{\alpha_i-1}$ of respective orders $p_i^{\alpha_i-1}, \dots, p_i$.

We consider two disjoint cases:

Case 1: If $\gamma_i = 0$, then $d \not\equiv 1 \pmod{p_i}$. This means that $d \notin H_1$. Thus, d is not contained in any of the H_δ , for $\delta \in \{1, \dots, \alpha_i-1\}$, so $\text{ord}(d)$ is not a power of p_i . Since $\text{ord}(d)$ divides $|\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}| = (p_i-1)p_i^{\alpha_i-1}$, we deduce that $\text{ord}(d) = (p_i-1)p_i^\delta$ for some $\delta \in \{0, \dots, \alpha_i-1\}$. In particular, $(p_i-1) \mid \text{ord}(d)$. Hence, the prime factorization of p_i-1 can be written in terms of the primes $q_1, \dots, q_s$.

Let $j \in \{1, \dots, s\}$ such that $q_j \mid (p_i-1)$. We obtain that $p_i \equiv 1 \pmod{q_j}$. By condition (i), $\ell = (m/u)n$ and, by condition (iii), m/u is an integer. Thus, $q_j \mid \ell$.

Case 2: If $\gamma_i > 0$, then $\gamma_i < \alpha_i$. Indeed, p_i divides u by assumption, and we have $u = m/\gcd(m, d-1)$ by condition (iii). We obtain that the multiplicity of p_i in the prime factorization of u is $\alpha_i - \gamma_i$.

We have that $d \equiv 1 \pmod{p_i^{\gamma_i}}$, so $d \in H_{\gamma_i}$. We must have $\text{ord}(d) = p_i^{\alpha_i - \gamma_i}$. Indeed, if $\text{ord}(d) = p_i^{\alpha_i - \delta}$ for $\delta > \gamma_i$, then $d \in H_\delta$, so $d \equiv 1 \pmod{p_i^\delta}$ and $p_i^\delta \mid (d-1)$. This contradicts the definition of γ_i .

Since $\text{ord}(d)$ divides n , we deduce that $p_i^{\alpha_i - \gamma_i} \mid n$. Finally, by condition (iii), we have that $\ell = mn/u$, so the multiplicity of p_i in the prime factorization of ℓ is at least $\alpha_i + (\alpha_i - \gamma_i) - (\alpha_i - \gamma_i) = \alpha_i > \alpha_i - \gamma_i$.

(3) $\implies$ (2). We now assume that u and ℓ satisfy property (3), and we construct m, n and d satisfying conditions (i), (ii) and (iii).

We start by using property (3) to write the prime factorization of u in a “split form” as $u = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$, where the primes $p_1, \dots, p_r$ are congruent to 1 modulo some prime factor of ℓ , and $q_j^{\beta_j+1} \mid \ell$ for each $j \in \{1, \dots, s\}$. Since u is odd, none of these prime numbers is 2.

Moreover, we may write the prime factorization of ℓ as $\ell = q_1^{\gamma_1} \cdots q_t^{\gamma_t}$ for some $t \geq s$ and exponents $\gamma_j > \beta_j$ for each $j \in \{1, \dots, s\}$. If $i \in \{1, \dots, r\}$, we choose $j_i \in \{1, \dots, t\}$ such that $p_i \equiv 1 \pmod{q_{j_i}}$.

We define:

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\gamma_1} \cdots q_s^{\gamma_s}$$

$$n = q_1^{\beta_1} \cdots q_s^{\beta_s} q_{s+1}^{\gamma_{s+1}} \cdots q_t^{\gamma_t}$$

We have $mn = u\ell$, so condition (i) is satisfied.

Now, we have $\varphi(p_i^{\alpha_i}) = (p_i - 1)p_i^{\alpha_i - 1}$, so $q_{j_i} \mid \varphi(p_i^{\alpha_i})$ for each $i \in \{1, \dots, r\}$. In particular, since the group $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ is cyclic (as $p_i \neq 2$), Theorem 2.4 ensures the existence of an order- q_{j_i} element d_i . By Proposition B.4, we have $d_i \not\equiv 1 \pmod{p_i}$ (since, otherwise, $\text{ord}(d_i) \mid p_i^{\alpha_i - 1}$).

By the Chinese remainder theorem, there exists a unique $d \in (\mathbb{Z}/m\mathbb{Z})^\times$ with:

- for every $i \in \{1, \dots, r\}$, $d \equiv d_i \pmod{p_i^{\alpha_i}}$;
- for every $j \in \{1, \dots, s\}$, $d \equiv 1 + q_j^{\gamma_j - \beta_j} \pmod{q_j^{\gamma_j}}$.

Observe that $d^{q_{j_i}} \equiv 1 \pmod{p_i^{\alpha_i}}$ for every $i \in \{1, \dots, r\}$ by our choice of d_i . Moreover, from Proposition B.4, the order of $1 + q_j^{\gamma_j - \beta_j} \in (\mathbb{Z}/q_j^{\gamma_j}\mathbb{Z})^\times$ divides $q_j^{\beta_j}$.

Therefore, $d^{q_j^{\beta_j}} \equiv 1 \pmod{q_j^{\gamma_j}}$. We get $d^n \equiv 1 \pmod{m}$, yielding condition (ii).

Furthermore, using the notation of Proposition B.4, we have $d_i \notin H_\delta$ for every $i \in \{1, \dots, r\}$ and $\delta \in \{1, \dots, \alpha_i - 1\}$, since, otherwise, its order q_{i_j} would divide a power of p_i . This yields:

$$\gcd(d - 1, m) = q_1^{\gamma_1 - \beta_1} \cdots q_s^{\gamma_s - \beta_s} = \frac{p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\gamma_1} \cdots q_s^{\gamma_s}}{p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}} = \frac{m}{u}.$$

We obtain that condition (iii) holds, completing the proof. $\square$

REFERENCES

- [Acc68] R. D. M. Accola. “On the number of automorphisms of a closed Riemann surface”. In: *Trans. Amer. Math. Soc.* 131 (1968), pp. 398–408. DOI: 10.2307/1994955.
- [AM24] J. S. Athreya and H. Masur. “Translation surfaces”. Vol. 242. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2024, pp. xi+179. DOI: 10.1090/gsm/242.
- [BCC20] E. Bujalance, F. J. Cirre, and M. D. E. Conder. “Bounds on the orders of groups of automorphisms of a pseudo-real surface of given genus”. In: *J. Lond. Math. Soc. (2)* 101.2 (2020), pp. 877–906. DOI: 10.1112/jlms.12296.
- [BCI13] G. Bartolini, A. F. Costa, and M. Izquierdo. “On automorphisms groups of cyclic p -gonal Riemann surfaces”. In: *J. Symbolic Comput.* 57 (2013), pp. 61–69. DOI: 10.1016/j.jsc.2013.05.005.
- [BG21] C. Bagiński and G. Gromadzki. “On the orders of largest groups of automorphisms of compact Riemann surfaces”. In: *J. Pure Appl. Algebra* 225.12 (2021), Paper No. 106758, 14. DOI: 10.1016/j.jpaa.2021.106758.
- [BJ05] M. Belolipetsky and G. A. Jones. “Automorphism groups of Riemann surfaces of genus $p + 1$, where p is prime”. In: *Glasg. Math. J.* 47.2 (2005), pp. 379–393. DOI: 10.1017/S0017089505002612.
- [Bro94] K. S. Brown. “Cohomology of groups”. Vol. 87. Graduate Texts in Mathematics. Corrected reprint of the 1982 original. Springer-Verlag, New York, 1994, pp. x+306. ISBN: 0-387-90688-6.
- [Bur04] W. Burnside. “On Groups of Order $p^\alpha q^\beta$ ”. In: *Proc. London Math. Soc. (2)* 1 (1904), pp. 388–392. DOI: 10.1112/plms/s2-1.1.388.

- [CD14] K. Cziszter and M. Domokos. “The Noether number for the groups with a cyclic subgroup of index two”. In: *J. Algebra* 399 (2014), pp. 546–560. DOI: 10.1016/j.jalgebra.2013.09.044.
- [CI10] A. F. Costa and M. Izquierdo. “Maximal order of automorphisms of trigonal Riemann surfaces”. In: *J. Algebra* 323.1 (2010), pp. 27–31. DOI: 10.1016/j.jalgebra.2009.09.041.
- [CR21] A. Carocca and S. Reyes-Carocca. “Riemann surfaces of genus $1 + q^2$ with $3q^2$ automorphisms”. In: *J. Algebra* 588 (2021), pp. 440–470. DOI: 10.1016/j.jalgebra.2021.09.001.
- [DHV24] V. Delecroix, P. Hubert, and F. Valdez. “Infinite Translation Surfaces in the Wild”. 2024. arXiv: 2403.05424 [math.GT].
- [FT23] J. Flake and A. Thevis. “Strata of p -origamis”. In: *Math. Nachr.* 296.3 (2023), pp. 1087–1116. DOI: 10.1002/mana.202100290.
- [FT62] W. Feit and J. G. Thompson. “A solvability criterion for finite groups and some consequences”. In: *Proc. Nat. Acad. Sci. U.S.A.* 48 (1962), pp. 968–970. DOI: 10.1073/pnas.48.6.968.
- [FT63] W. Feit and J. G. Thompson. “Solvability of groups of odd order”. In: *Pacific J. Math.* 13 (1963), pp. 775–1029.
- [GS87] H. Glover and D. Sjerve. “The genus of $\mathrm{PSL}_2(q)$ ”. In: *J. Reine Angew. Math.* 380 (1987), pp. 59–86. DOI: 10.1515/crll.1987.380.59.
- [Hal28] P. Hall. “A Note on Soluble Groups”. In: *J. London Math. Soc.* 3.2 (1928), pp. 98–105. DOI: 10.1112/jlms/s1-3.2.98.
- [Har66] W. J. Harvey. “Cyclic groups of automorphisms of a compact Riemann surface”. In: *Quart. J. Math. Oxford Ser. (2)* 17 (1966), pp. 86–97. DOI: 10.1093/qmath/17.1.86.
- [Hid21] R. A. Hidalgo. “Automorphism groups of origami curves”. In: *Arch. Math. (Basel)* 116.4 (2021), pp. 385–390. DOI: 10.1007/s00013-020-01559-9.
- [HMQ24] R. A. Hidalgo, Y. L. Marín Montilla, and S. Quispe. “Quasi-abelian group as automorphism group of Riemann surfaces”. In: *Manuscripta Math.* 175.1-2 (2024), pp. 591–616. DOI: 10.1007/s00229-024-01552-4.
- [Hur92] A. Hurwitz. “Über algebraische Gebilde mit eindeutigen Transformationen in sich”. In: *Math. Ann.* 41.3 (1892), pp. 403–442. DOI: 10.1007/BF01443420.
- [IJR21] M. Izquierdo, G. A. Jones, and S. Reyes-Carocca. “Groups of automorphisms of Riemann surfaces and maps of genus $p + 1$ where p is prime”. In: *Ann. Fenn. Math.* 46.2 (2021), pp. 839–867. DOI: 10.5186/aasfm.2021.4649.
- [IRR21] M. Izquierdo, S. Reyes-Carocca, and A. M. Rojas. “On families of Riemann surfaces with automorphisms”. In: *J. Pure Appl. Algebra* 225.10 (2021), Paper No. 106704, 21. DOI: 10.1016/j.jpaa.2021.106704.
- [Isa08] I. M. Isaacs. “Finite group theory”. Vol. 92. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2008, pp. xii+350. ISBN: 978-0-8218-4344-4. DOI: 10.1090/gsm/092.
- [Kil70] W. T. Kiley. “Automorphism groups on compact Riemann surfaces”. In: *Trans. Amer. Math. Soc.* 150 (1970), pp. 557–563. DOI: 10.2307/1995537.
- [Kul91] R. S. Kulkarni. “Infinite families of surface symmetries”. In: *Israel J. Math.* 76.3 (1991), pp. 337–343. DOI: 10.1007/BF02773869.
- [Mac65] C. Maclachlan. “Abelian groups of automorphisms of compact Riemann surfaces”. In: *Proc. London Math. Soc. (3)* 15 (1965), pp. 699–712. DOI: 10.1112/plms/s3-15.1.699.
- [Mac69a] A. M. Macbeath. “Generators of the linear fractional groups”. In: *Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967)*. Amer. Math. Soc., Providence, RI, 1969, pp. 14–32.

- [Mac69b] C. Maclachlan. “A bound for the number of automorphisms of a compact Riemann surface”. In: *J. London Math. Soc.* 44 (1969), pp. 265–272. DOI: 10.1112/jlms/s1-44.1.265.
- [Mar24] Y. L. Marín Montilla. “Generalized quasi-dihedral and quasi-abelian groups actions on Riemann/Klein surfaces”. PhD thesis. Universidad de La Frontera, Temuco, Chile, 2024.
- [Mat22] C. Matheus. “Three lectures on square-tiled surfaces”. In: *Teichmüller theory and dynamics*. Ed. by P. Dehornoy and E. Lanneau. Vol. 58. Panoramas et Synthèses [Panoramas and Syntheses]. Papers based on lectures given at the 27th summer school on Teichmüller dynamics, mapping class groups and applications held at the Institut Fourier of Grenoble, June 11–22, 2018. Société Mathématique de France, Paris, 2022, pp. 77–99. ISBN: 978-2-85629-966-1.
- [McC] D. McCullough. “Exceptional subgroups of $SL(2, F)$ ”. Unpublished manuscript. See <http://www2.math.ou.edu/~dmccullough/research/pdf/s/exceptional.pdf>.
- [MMY15] C. Matheus, M. Möller, and J.-C. Yoccoz. “A criterion for the simplicity of the Lyapunov spectrum of square-tiled surfaces”. In: *Invent. Math.* 202.1 (2015), pp. 333–425. DOI: 10.1007/s00222-014-0565-5.
- [MW11] D. McCullough and M. Wanderley. “Writing elements of $PSL(2, q)$ as commutators”. In: *Comm. Algebra* 39.4 (2011), pp. 1234–1241. DOI: 10.1080/00927871003645383.
- [MW13] D. McCullough and M. Wanderley. “Nielsen equivalence of generating pairs of $SL(2, q)$ ”. In: *Glasg. Math. J.* 55.3 (2013), pp. 481–509. DOI: 10.1017/S0017089512000675.
- [MZ24] C. L. May and J. Zimmerman. “Maximal order group actions on Riemann surfaces of genus $1 + 3p$ ”. In: *Rocky Mountain J. Math.* 54.2 (2024), pp. 495–508. DOI: 10.1216/rmj.2024.54.495.
- [Nga12] J. B. Nganou. “How rare are subgroups of index 2?” In: *Math. Mag.* 85.3 (2012), pp. 215–220. DOI: 10.4169/math.mag.85.3.215.
- [Rob96] D. J. S. Robinson. “A course in the theory of groups”. Second. Vol. 80. Graduate Texts in Mathematics. Springer-Verlag, New York, 1996, pp. xviii+499. ISBN: 0-387-94461-3. DOI: 10.1007/978-1-4419-8594-1.
- [Ros94] J. S. Rose. “A course on group theory”. Reprint of the 1978 original [Dover, New York; MR0498810 (58 #16847)]. Dover Publications, Inc., New York, 1994, pp. x+310. ISBN: 0-486-68194-7.
- [Rot95] J. J. Rotman. “An introduction to the theory of groups”. Fourth. Vol. 148. Graduate Texts in Mathematics. Springer-Verlag, New York, 1995, pp. xvi+513. ISBN: 0-387-94285-8. DOI: 10.1007/978-1-4612-4176-8.
- [Sha15] M. Shabani-Attar. “On equality of order of a finite p -group and order of its automorphism group”. In: *Bull. Malays. Math. Sci. Soc.* 38.2 (2015), pp. 461–466. DOI: 10.1007/s40840-014-0030-z.
- [SW17] J.-C. Schlage-Puchta and G. Weitze-Schmithüsen. “Finite translation surfaces with maximal number of translations”. In: *Israel J. Math.* 217.1 (2017), pp. 1–15. DOI: 10.1007/s11856-017-1436-8.
- [Tay92] D. E. Taylor. “The geometry of the classical groups”. Vol. 9. Sigma Series in Pure Mathematics. Heldermann Verlag, Berlin, 1992, pp. xii+229. ISBN: 3-88538-009-9.
- [Wal86] G. L. Walls. “Automorphism groups”. In: *Amer. Math. Monthly* 93.6 (1986), pp. 459–462. DOI: 10.2307/2323470.
- [Wim95] A. Wiman. “Über die hyperelliptischen Curven und diejenigen vom Geschlechte $p = 3$, welche eindeutige Transformationen in sich zulassen”. In: *Bih. Kongl. Svenska Vetensk.-Akad. Handl.* 21.1 (1895), pp. 3–23.

(Julien Boulanger) CENTRO DE MODELAMIENTO MATEMÁTICO (CNRS IRL2807), UNIVERSIDAD DE CHILE, SANTIAGO, CHILE

Email address: `jboulanger@cmm.uchile.cl`

URL: `https://julien-boulanger.github.io/webpage/`

(Rodolfo Gutiérrez-Romo) DEPARTAMENTO DE INGENIERÍA MATEMÁTICA, FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS, UNIVERSIDAD DE CHILE & CENTRO DE MODELAMIENTO MATEMÁTICO (CNRS IRL2807), UNIVERSIDAD DE CHILE, SANTIAGO, CHILE

Email address: `g-r@rodol.fo`

URL: `http://rodol.fo`

(Erwan Lanneau) UMR CNRS 5582, UNIV. GRENOBLE ALPES, CNRS, INSTITUT FOURIER, F-38000 GRENOBLE, FRANCE

Email address: `erwan.lanneau@univ-grenoble-alpes.fr`

URL: `https://www-fourier.ujf-grenoble.fr/~lanneau`