ISRAEL JOURNAL OF MATHEMATICS **126** (2001), 1–16

HOW OFTEN IS $84(g-1)$ ACHIEVED?

BY

MICHAEL LARSEN*

Department of Mathematics, Indiana University
Bloomington, IN 47405, USA
e-mail: larsen@math.indiana.edu

ABSTRACT

For any finitely generated group Γ, the asymptotics of the set of orders of finite quotient groups of Γ are determined by the minimum dimension of a complex linear group containing an infinite quotient of Γ. We give a proof and an application to the asymptotic behavior of the set of integers g for which the Hurwitz bound is sharp.

0. Introduction

It is a well-known theorem of Hurwitz [5] that a Riemann surface of genus $g \geq 2$ has at most $84(g-1)$ automorphisms. It has been shown [8] that this bound is attained for infinitely many values of g and [1] that it fails to be attained infinitely often. In this paper we look at the question of how often it is achieved. We prove that good values of g are about as common as perfect cubes.

More precisely, let H denote the set of integers $g \geq 2$ such that there exists at least one compact Riemann surface of genus g with automorphism group of order $84(g-1)$. We prove the following:

THEOREM 0.1: *The series $\sum_{g\in H} g^{-s}$ converges absolutely for $\Re(s) > 1/3$ and has a singularity at $s = 1/3$.*

If X is a Riemann surface of genus $g \geq 2$ and Δ is the automorphism group of X, then X can be regarded as a branched covering of X/Δ. From this point

* Partially supported by NSF Grant DMS-97-27553.
Received July 2, 2000

of view, it is not difficult to see that if $|\Delta| = 84(g-1)$, the covering is branched over three points and Δ is generated by inertia group generators x, y, and z of orders 2, 3, and 7 respectively, such that $xyz = 1$. Conversely, any finite group Δ generated by such a triple can be realized as the automorphism group of a Riemann surface of genus $g = |\Delta|/84 + 1$. Thus, the problem reduces to group theory.

We formulate the following general question: Let Γ be a finitely generated group. Let H_Γ denote the set of isomorphism classes of finite homomorphic images of Γ and $O(\cdot)$ the set of cardinalities of elements of a set of finite sets. Thus $O(H_\Gamma)$ is the set of integers n such that Γ has at least one normal subgroup of index n. Let

$$Z_\Gamma(s) = \sum_{n \in O(H_\Gamma)} n^{-s}. \tag{0.1.1}$$

This is not the only reasonable notion of zeta-function attached to a group (see [3]), but it is well adapted to our purposes. We want a formula for the abscissa of convergence of $Z_\Gamma(s)$. Of course if the profinite completion of Γ is finite, then $Z_\Gamma(s)$ is entire, so this case is trivial.

Definition 0.2: The **quotient dimension** q_Γ is the minimal dimension of any linear algebraic group G, not necessarily connected, such that $G(\mathbb{C})$ contains an infinite quotient group of Γ. If no such G exists, we say $q_\Gamma = \infty$.

We can now state the main theorem of the paper:

THEOREM 0.3: *If Γ is a finitely generated group with infinite profinite completion, then the abscissa of convergence of $Z_\Gamma(s)$ is $1/q_\Gamma$ and Z_Γ is singular at $1/q_\Gamma$.*

This theorem reflects the theme, familiar from the classification of finite simple groups, that finite groups can in some sense be approximated by linear algebraic groups. It not only implies Theorem 0.1, but it gives a fairly detailed overall picture of the frequency of g for which there exists a curve X of genus g with $|\operatorname{Aut}(X)|/(g-1)$ belonging to a given interval.

The proof of Theorem 0.3 depends on two inequalities. One of them can be proved without invoking the classification theorem, but the other seems to depend on classification in a fundamental way. The reader might find it interesting to compare the results and methods of this paper with [7], where the strong approximation theorem is also used to deduce results on finite index subgroups.

ACKNOWLEDGEMENT: I would like to thank Alex Lubotzky for his careful reading of this paper and his patient explanation of his own work in the same direction. I would also like to acknowledge the many helpful suggestions offered by Richard Pink.

1. Quotients of a finitely generated group

Before embarking on the proof of Theorem 0.3, we look a little more closely at Definition 0.2. Let G be a linear algebraic group over $\mathbb{C}$ of minimal dimension among those whose complex points contain an infinite quotient group of Γ. If N is a normal subgroup of G of positive dimension, then the image Γ' of Γ in the quotient $(G/N)(\mathbb{C})$ must be finite. The pre-image of Γ' in G contains Γ and must therefore have the same dimension as G. Consequently, $\dim N = \dim G$. This motivates the following definition:

Definition 1.1: We say a linear algebraic group G is **pseudo-simple** when every normal linear subgroup N of G is either finite or of finite index in G.

LEMMA 1.2: *If G is pseudo-simple, the identity component G° is either semisimple, multiplicative, or commutative and unipotent.*

Proof: Let R and U denote the radical and unipotent radical of G° respectively and U^{der} the derived group of U. As these subgroups are characteristic, they are normal in G, so the filtration $\{0\} \subset U^{\mathrm{der}} \subset U \subset R \subset G^\circ$ has one non-trivial step. A perfect unipotent group is trivial, so $U^{\mathrm{der}} = U$ implies $U = \{0\}$. ∎

We say that G is of **non-abelian**, **toral**, or **vector** type according to which of the three possibilities in Lemma 1.2 occurs.

PROPOSITION 1.3: *If G is a pseudo-simple linear algebraic group of toral type such that $G(\mathbb{C})$ contains an infinite homomorphic image of Γ, then there exists a pseudo-simple group G' of vector type with $\dim G' \leq \dim G$ such that $G'(\mathbb{C})$ also contains an infinite quotient of Γ.*

Proof: Without loss of generality we may assume that Γ is an infinite subgroup of $G(\mathbb{C})$. Let $\Delta = G/G^\circ$, and $\Lambda = \Gamma \cap G^\circ(\mathbb{C})$. As Λ is of finite index in Γ, it is finitely generated, and of course it is commutative. Its torsion is therefore bounded, and dividing G and Γ by μ_m^n and $\mu_m^n \cap \Gamma$ respectively, where μ_m^n denotes the n-th cartesian power of the group of m-th roots of unity, we can reduce to the case that Λ is free abelian. Now, as Λ has a Δ-equivariant embedding in $G^\circ(\mathbb{C}) = \mathbb{C}^n/X_*(G^\circ)$, where $X_*(G^\circ)$ is the group of cocharacters of G°, it has an extension by $X_*(G^\circ)$ with a Δ-equivariant embedding in $\mathbb{C}^n$. In particular, $\Lambda \otimes \mathbb{C}$ maps to a Δ-representation space V of dimension at most n, and $V \rtimes \Delta$ contains an infinite quotient of Γ. ∎

The easier direction of Theorem 0.3 depends on the fact that we can reduce a homomorphic image of Γ in $G(\mathbb{C})$ (mod p) for suitable p in order to obtain a collection of finite quotients of Γ sufficient to make Z_Γ diverge. The following lemma gives a technical formulation of this idea in a general geometric context. In applications, the scheme X below will parametrize homomorphisms from Γ to a suitable group scheme.

LEMMA 1.4: *Let X be a scheme of finite type over* $\operatorname{Spec}\mathbb{Z}$. *The following conditions are equivalent.*

(1) *$X(\mathbb{C})$ is non-empty.*
(2) *$X(\overline{\mathbb{F}}_p)$ is non-empty for infinitely many primes p.*
(3) $\sum_{\{p|X(\overline{\mathbb{F}}_p)\neq\emptyset\}} 1/p = \infty$.

Proof: It is trivial that (3) implies (2). Chevalley's constructibility theorem gives (2) implies (1). To deduce (3) from (1), we observe that every non-empty variety over $\mathbb{Q}$ has a point over $\overline{\mathbb{Q}}$ and therefore over some number field. Applying this theorem to the generic fiber of X, we obtain a K-point of $X\otimes\mathbb{Q}$ and therefore a $\mathcal{O}_K[1/n]$-point of X for some positive integer n. For each maximal ideal $\mathfrak{m}$ of $\mathcal{O}_K[1/n]$ with quotient field $\mathbb{F}$, $X(\mathbb{F}) \neq \emptyset$. As the Dedekind zeta-function of K diverges at $s = 1$,

$$\sum_{\mathfrak{m}\in\operatorname{Spec}\mathcal{O}_K[1/n]} \|\mathfrak{m}\|^{-1} = \infty. \tag{1.4.1}$$

On the other hand, since each rational prime p has at most $[K : \mathbb{Q}]$ prime ideals lying over it, and

$$\sum_{p\text{ prime}} \sum_{k=2}^{\infty} p^{-k} \le \sum_{m=2}^{\infty}\sum_{k=2}^{\infty} m^{-k} = 1,$$

the contribution to (1.4.1) by prime ideals $\mathfrak{m}$ with $\|\mathfrak{m}\|$ not prime is finite. The lemma follows. ∎

We can now prove one direction of Theorem 0.3.

THEOREM 1.5: *If G is a pseudo-simple group of dimension n over $\mathbb{C}$ such that $G(\mathbb{C})$ contains an infinite quotient of Γ, then the series $Z_\Gamma(1/n)$ diverges.*

Proof: Let ϕ denote the homomorphism from Γ to $G(\mathbb{C})$, which we regard as a subgroup of $\mathrm{GL}_N(\mathbb{C})$ for some N. Let A denote the subring of $\mathbb{C}$ generated over

$\mathbb{Z}$ by the entries of the elements of $\phi(\Gamma)$. As Γ is finitely generated, the same is true of A. Without loss of generality, we may assume that $\phi(\Gamma)$ is Zariski-dense in G. Let Γ° denote the subgroup of Γ mapping into $G^\circ(\mathbb{C})$. As G/G° is finite, Γ° is a finite index subgroup of Γ and therefore finitely generated.

We consider the non-abelian case first. Let $\mathcal{G}$ denote the Zariski-closure of $\phi(\Gamma^\circ)$ in GL_N over A. As semisimplicity is an open property of a group scheme (see, for example, [9] p. 297), by replacing A by some localization $A[1/b]$, we may assume that $\mathcal{G}$ is a semisimple group scheme over A and that $\mathcal{G}_{\mathbb{C}} = G^\circ$. Replacing A by a finite étale cover, we may assume that $\mathcal{G}$ is split. The quotient of $\mathcal{G}$ by its (finite) center is a split adjoint semisimple group scheme over A and therefore the product of split adjoint simple group schemes $\mathcal{H}_i$. In fact, the $\mathcal{H}_i$ must be isomorphic to one another, but we do not need this.

Let $\psi_i\colon \Gamma^\circ \to \mathcal{H}_i(A)$ be the composition homomorphism. By construction, the image is Zariski-dense in the generic fiber of $\mathcal{H}_i$. By [6] Th. 12.3, there exists a scheme T of finite type over A and a subgroup scheme $\mathcal{K}_i$ of the pullback $\mathcal{H}_{i\,T} = \mathcal{H}_i \times_A T$ with the following properties: First, every fiber of $\mathcal{K}_i$ is a proper subgroup of the corresponding fiber of $\mathcal{H}_{i\,T}$; and second, if s is a geometric point of $\operatorname{Spec} A$ and Δ a finite subgroup of $\mathcal{H}_{i\,s}$ which is not contained in any $\mathcal{K}_{i\,t}$, for t lying over s, then Δ satisfies

$$(\mathcal{H}_{i\,s}^F)^{\mathrm{der}} \subset \Delta \subset \mathcal{H}_{i\,s}^F$$

for some Frobenius map F on $\mathcal{H}_{i\,s}$. The set of s such that the specialization of $\psi_i(\Gamma^\circ)$ to $\mathcal{H}_{i\,s}$ lies in some $\mathcal{K}_{i\,t}$ is constructible and nowhere dense, since Γ° is finitely generated. Therefore, localizing A once again, we may assume without loss of generality that this set is empty for all i. Note that A is still finitely generated over $\mathbb{Z}$.

If $\mathbb{F}_p$ is a quotient of A, then the image of $\psi_i(\Gamma^\circ)$ in $\mathcal{H}_i(\mathbb{F}_p)$ contains $\mathcal{H}_i(\mathbb{F}_p)^{\mathrm{der}}$ as a normal subgroup. Thus, $\psi_i(\Gamma^\circ)$ has a quotient of order $\le (p+1)^{\dim \mathcal{H}_i}$ which contains $\mathcal{H}_i(\mathbb{F}_p)^{\mathrm{der}}$ as a normal subgroup, which means that $\phi(\Gamma^\circ)$ has a quotient of order $\le (p+1)^n$ which contains each $\mathcal{H}_i(\mathbb{F}_p)^{\mathrm{der}}$ as a subquotient. Finally, $\phi(\Gamma)$ and therefore Γ itself has a quotient of order $\le |\Gamma/\Gamma^\circ|(p+1)^n$ which has each $\mathcal{H}_i(\mathbb{F}_p)^{\mathrm{der}}$ as a subquotient. The other Jordan–Hölder constituents of this quotient are cyclic groups of prime order or subquotients of Γ/Γ°. For $p \gg 0$, therefore, these quotients are pairwise distinct, and by Lemma 1.4, they are enough to guarantee the divergence of $Z_\Gamma(1/n)$.

Weisfeiler's work on strong approximation [9] gives an alternative, somewhat easier, argument for the nonabelian case. Unfortunately, it makes use of the classification of finite simple groups.

For the vector case, we observe that Γ must be an extension of the component group $\Delta = G/G^\circ$ by a free abelian group Λ. Given two short exact sequences $0 \to A_i \to B_i \to C_i \to 0$ where A_i are abelian and fixed homomorphisms $\alpha\colon A_1 \to A_2$ and $\gamma\colon C_1 \to C_2$, there exists a homomorphism $\beta\colon B_1 \to B_2$ making the diagram commute if and only if α and γ are compatible with the actions of C_i on A_i and the cohomology classes $H^2(C_i, A_i)$. Since we have a map from Γ to $G(\mathbb{C})$, there is an n-dimensional quotient of the Δ-representation $\Lambda \otimes \mathbb{C}$. This Δ-equivariant quotient map can be defined over a number field K and therefore over $\mathcal{O}_K[1/m]$ for some positive integer m. If $\mathfrak{m}$ is a prime ideal of $\mathcal{O}_K[1/m]$ with residue field $\mathbb{F}_p$, then there exists an n-dimensional $\mathbb{F}_p$-representation of Δ which is a quotient of $\lambda \otimes \mathcal{O}[1/m]$. If $p > |\Delta|$, the image of any cohomology class in $H^2(\Delta, \Lambda)$ in $H^2(\Delta, \mathbb{F}_p^n)$ is zero, so there exists a map from Γ to the semi-direct product $\mathbb{F}_p^n \rtimes \Delta$ which induces the identity on Δ. If $p \gg 0$, it is onto, and the homomorphic images of Γ thus obtained are clearly pairwise non-isomorphic. We conclude, as in the non-abelian case, using Lemma 1.4.

The toral case reduces to the vector case by Proposition 1.3. ∎

The converse is more difficult, since here we must start with a collection of finite homomorphic images and eventually produce an infinite image in a complex linear group. The crucial point is that, according to the classification theorem, "most" finite simple groups are of Lie type and can therefore be regarded as (mod p) reductions of simple Lie groups. To make this precise, we have the following theorem:

PROPOSITION 1.6: *There exists a set Ξ of finite simple groups such that*

$$\sum_{G\in\Xi} |G|^{-s}$$

converges for $\Re(s) > 0$ and every non-abelian finite simple group not in Ξ is of Lie type.

Proof: By the classification theorem [4], every finite simple group is cyclic, alternating, of Lie type, of Suzuki or Ree type, or sporadic, and there are only finitely many sporadic groups. Note that in what follows, the Suzuki and Ree groups will not be considered to be of Lie type. Let Ξ consist of the alternating, Suzuki–Ree, and sporadic groups. The series

$$\sum_{n=5}^{\infty} (n!/2)^{-s}$$

is obviously entire as are the series

$$\sum_{f=1}^{\infty}(2^{4f+2}(2^{f4+2}+1)(2^{2f+1}-1))^{-s}$$

for Suzuki groups and

$$\sum_{f=1}^{\infty}(3^{6f+3}(3^{6f+3}+1)(3^{2f+1}-1))^{-s},$$
$$\sum_{f=1}^{\infty}(2^{24f+12}(2^{12f+6}+1)(2^{8f+4}-1)(2^{6f+3}+1)(2^{2f+1}-1))^{-s}$$

for Ree groups. ∎

It should be noted that Proposition 1.2 is a priori a good deal weaker than the full classification theorem. It allows for the possibility that there are infinitely many sporadic groups, provided that the order of the nth such group grows at a more than polynomial rate in n. This weaker version of classification is all that we use in this paper, and it would be interesting to know whether it is easier to prove than the full statement.

It should also be noted that Ξ can be augmented to contain additional groups which are in any respect troublesome, as long as the order of the nth such group grows faster than any polynomial in n. In what follows, we will find it convenient to assume that every finite group of Lie type is of the form $H(\mathbb{F}_q)^{\mathrm{der}}$, where H is an adjoint simple algebraic group over the finite field $\mathbb{F}_q$. We also find it convenient to assume that all automorphisms of such a group are obtained by composing a field automorphism, a diagonal automorphism, and a graph automorphism in a unique way. By [2], we can guarantee these statements for $G \notin \Xi$ without sacrificing Proposition 1.6.

Proposition 1.6 allows us to show that the abscissa of convergence of $Z_\Gamma(s)$ is not affected by quotient groups of Γ which contain normal subgroups of the form Δ^k, $\Delta \in \Xi$. At the same time, we also want to exclude quotient groups with non-trivial center.

Let Σ be a family of finite groups, and N and d positive integers. Let $O_{N,d,\Xi}(\Sigma)$ denote the set of expressions of the form $m|\Delta|$, where $\Delta \in \Sigma$ and m is a product of terms m_i, where each m_i is of one of the following kinds:

(1) a prime $\leq N$;
(2) a prime dividing $|\Delta|$;
(3) a prime power p^a where $a \geq d$;

(4) the order of an element of Ξ;

(5) an expression of the form $|H(\mathbb{F}_{p^b})^{\mathrm{der}}|^a$, where H is a simple algebraic group and $ab \dim H \geq d$.

PROPOSITION 1.7: *Given positive integers N and d and a real $\sigma > 1/d$, if*

$$\sum_{n\in O_{N,d,\Xi}(H_\Gamma)} n^{-\sigma}$$

diverges, then $Z_\Gamma(s)$ diverges for $\Re(s) < \sigma$.

Proof: We define the **saturation** of a set A of positive integers with respect to another set B as the set

$$A[B] := \Big\{a\prod_i b_i \mid a \in A,\, b_i \in B\Big\}.$$

Thus for real s,

$$\sum_{n\in A[B]} n^{-s} \leq \prod_{b\in B}(1-b^{-s})^{-1}\sum_{n\in A} n^{-s}. \tag{1.7.1}$$

If $\sum_{b\in B} b^{-s}$ converges, then $\sum_{n\in A} n^{-s}$ converges if and only if $\sum_{n\in A[B]} n^{-s}$ converges. This shows that saturating with respect to primes $\leq N$ or with respect to orders of elements of Ξ has no effect on convergence for $\Re(s) > 0$. Groups of Lie type can be divided into the classical types (A_n, ${}^2A_n$, B_n, C_n, D_n, and ${}^2D_n$), and a finite number of exceptional types (${}^3D_4$, E_6, ${}^2E_6$, E_7, E_8, F_4, and G_2). By [2] the order of a group associated to a type of dimension e and a prime power q is greater than

$$\frac{q^e}{e}\cdot\prod_{n=1}^{\infty}(1-q^{-n}) \geq \frac{q^e}{4e}.$$

If we fix a type of dimension d_0, the sum of $|H(\mathbb{F}_{p^b})^{\mathrm{der}}|^{-as}$ over all a and b with $abd_0 \geq d$ and p prime is at most

$$\sum_p\sum_a\sum_b \frac{p^{-abd_0s}}{(4d_0)^{-as}}.$$

This converges as long as $s > 1/d$. Therefore the contribution of any single type in (5) above can be neglected. For the classical cases, we use the fact that the order of a group of Lie type is greater than the order of its p-Sylow subgroup, which is at least p^{br}, where $q = p^b$ and r is the rank. For r_0 sufficiently large,

$$\sum_p\sum_{a=1}^{\infty}\sum_{b=1}^{\infty}\sum_{r=r_0}^{\infty}(p^{abr})^{-s}$$

converges.

To deal with primes of type (2), we observe that for fixed σ and $\epsilon > 0$, for all $p \gg 0$,

$$(1-p^{-\sigma})^{-1} < 2 < p^{\epsilon}.$$

By (1.7.1), there exists a constant M independent of $n = p_1^{a_1} \cdots p_k^{a_k}$ such that

$$\sum_{m\in\{n\}[\{p_1,\dots,p_k\}]} m^{-\sigma} < Mn^{\epsilon-\sigma}.$$

It follows that $Z_\Gamma(\sigma-\epsilon)$ diverges. ∎

If the abscissa of convergence of $Z_\Gamma(s)$ is greater than $1/d$, it coincides with the abscissa of convergence of any series of the form

$$\sum_{n\in O(H'_\Gamma)} n^{-s}$$

where $O_{N,d,\Xi}(H_\Gamma) = O_{N,d,\Xi}(H'_\Gamma)$. In particular, we set H'_Γ to be the set of finite quotients Δ of Γ satisfying the following conditions:

(1) the order of every non-trivial normal subgroup of Δ has a prime factor $> N$;

(2) if Ω is a commutative normal subgroup of Δ, $|\Omega|$ is relatively prime to $|\Delta/\Omega|$;

(3) a non-trivial normal elementary p-subgroup of Δ has rank $< d$;

(4) Δ has no normal subgroup which is the power of an element of Ξ;

(5) Δ has no normal subgroups of the form $\left(H(\mathbb{F}_{p^b})^{\mathrm{der}}\right)^a$, where $ab \dim H \geq d$.

To choose N, we note that the abelianization $\Gamma/[\Gamma,\Gamma]$ is a finitely generated abelian group. If it is a torsion group, we choose N larger than any prime dividing its order. If it has a non-trivial free part, then $q_\Gamma = 1$ and $Z_\Gamma(s)$ is the Riemann ζ-function, so Theorem 0.3 is obvious. We may therefore assume from now on that the abelianization of Γ is torsion.

LEMMA 1.8: *Every element in H'_Γ has trivial center.*

Proof: Let Ω_p denote the p-torsion subgroup of the center of an element $\Delta \in H'_\Gamma$. By (2), $|\Delta/\Omega_p|$ is relatively prime to p, so the cohomology class in $H^2(\Delta/\Omega_p, \Omega_p)$ determining the central extension is trivial. It follows that Ω_p is a homomorphic image of Δ and therefore of Γ. If Ω_p is non-trivial, then $p < N$, but this is impossible by (1). ∎

We can now prove the following theorem:

THEOREM 1.9: *If Γ is a finitely generated group, n is a positive integer, and the abscissa of convergence of Z_Γ is greater than $1/n$, then $q_\Gamma < n$.*

Proof: The crucial property of the set H_Γ is that it is closed under the process of taking quotients. For any such set $\mathcal{S}$ of isomorphism classes of finite groups, we construct a group scheme over $\mathbb{Z}$ such that infinitely many elements of $\mathcal{S}$ appear as subgroups of different fibers. For $\mathcal{S} = H_\Gamma$, this allows us to apply Lemma 1.4 to obtain a Zariski dense homomorphism from Γ to the complex points of the group scheme.

We set $d = n$ and construct H'_Γ as above. Let Δ be an element of H'_Γ, and let Ω^a be a characteristically simple normal subgroup of Δ. We consider two cases: Ω non-abelian and $\Omega = \mathbb{Z}/p\mathbb{Z}$.

If Ω is non-abelian, setting $\Omega' = \Delta/Z_\Delta(\Omega^a)$, we obtain a homomorphic image of Γ satisfying

$$\Omega^a \subset \Omega' \subset \mathrm{Aut}(\Omega^a) = \Omega^a \rtimes \mathrm{Out}(\Omega^a).$$

As $\Omega \not\in \Xi$, we may assume without loss of generality that Ω is of the form $H(\mathbb{F}_{p^b})^{\mathrm{der}}$, where $ab \dim H < n$ and every outer automorphism of Ω is the product of a field automorphism, a diagonal automorphism, and a graph automorphism in a unique way. In other words, setting G to be the Weil restriction of scalars of H^a from $\mathbb{F}_{p^b}$ to $\mathbb{F}_p$, $\Omega^a \subset G(\mathbb{F}_p)$, and Ω' can be realized as a subgroup of $G(\overline{\mathbb{F}}_p) \rtimes \mathrm{Out}(\Phi)$, where Φ is the root system of G. Moreover, p can be chosen to be as large as we wish simply by increasing the size of N.

If $\mathcal{G}$ denotes the semidirect product of the adjoint Chevalley group scheme with root system Φ by $\mathrm{Out}(\Phi)$, there are infinitely many geometric fibers of $\mathcal{G}$ admitting homomorphisms from Γ, and the orders of the images go to infinity. The scheme $Y := \mathrm{Hom}(\Gamma, \mathcal{G})$ is a closed subscheme of $\mathcal{G}^g$ if Γ has g generators, so it is of finite type over $\mathrm{Spec}\,\mathbb{Z}$. It is therefore a finite union of irreducible components Y_i. For each generic point of a component Y_i, we have a representation of Γ. If the image of this representation is finite of order N_i, then the representation corresponding to any point in Y_i has image of order $\leq N_i$. We choose N to be larger than any N_i. Any homomorphic image Ω' with $p > N$ must correspond to a point of Y which does not lie in any such component. Let X be the open subscheme of Y consisting of the union of all components whose generic points correspond to a homomorphism of infinite image. Applying Lemma 1.4 to this scheme, we conclude that $X(\mathbb{C})$ is non-empty.

There remains the case $\Omega = \mathbb{Z}/p\mathbb{Z}$. We again set $\Omega' = \Delta/Z_\Delta(\Omega^a)$. Clearly Ω' is a homomorphic image of Γ and a subgroup of $\mathrm{GL}_a(\mathbb{F}_p)$. Moreover, by conditions

(2) and (3) for H'_Γ, Ω' has order prime to p and $a < n$. By a standard lifting argument, we can realize Ω' as a subgroup of $\mathrm{GL}_a(\mathbb{Z}_p) \subset \mathrm{GL}_a(\mathbb{Q}_p)$. By Jordan's theorem, Ω' is an extension of a group of order $\leq J(a)$ by an abelian group Ω'_{ab} with $\leq a$ generators. We now distinguish two cases: either Ω'_{ab} is bounded for all choices of Ω, as p goes to ∞, or $|\Omega'_{\mathrm{ab}}|$ grows without bound. In the first case, we observe that $\ker(\Gamma \to \Omega')$ contains Ω^a as a central subgroup. By property (2), Ω^a splits as a direct factor. The complementary factor is uniquely determined and therefore normal in Γ; the quotient is an extension of Ω' by Ω^a. Thus, in the first case as in the second, Γ has a homomorphic image which is an extension of a group of bounded order by an abelian group whose order can be taken arbitrarily large but which can be generated by $\leq a$ elements. The theorem now follows from the following lemma:

LEMMA 1.10: *Let Δ denote a fixed finite group. Suppose that for some integer a there exists an arbitrarily large finite group which is a homomorphic image of Γ and also an extension of Δ by an abelian group with a generators and order prime to $|\Delta|$. Then there exists an extension of Δ by $\mathbb{C}^a$ which admits a homomorphic image of Γ of infinite order.*

Proof: As Γ is finitely generated, there are finitely many homomorphisms $\pi: \Gamma \to \Delta$. Every homomorphic image of Γ which is an extension of Δ determines one such homomorphism, and we fix π such that $\ker \pi$ contains normal subgroups Γ_i of arbitrarily large finite index for which $\ker \pi/\Gamma_i$ is abelian with a generators and order prime to $|\Delta|$. Let Λ denote the abelianization of $\ker \pi$. Thus, Λ is a finitely generated abelian group. By hypothesis, Λ has Δ-invariant normal subgroups $\bar{\Gamma}_i$ of arbitrarily large finite index for which the quotients have a generators and order prime to $|\Delta|$. The same is automatically true for the free $\mathbb{Z}$-module $\Lambda/\Lambda_{\mathrm{tor}}$, and working locally, we see the same is true if we restrict attention to subgroups of prime-power index. Fix one prime p not dividing $|\Delta|$ for which such a subgroup exists. As $(\Lambda/\Lambda_{\mathrm{tor}}) \otimes \mathbb{F}_p$ has an $\mathbb{F}_p[\Delta]$-invariant subspace of dimension $\leq a$,

$$(\Lambda/\Lambda_{\mathrm{tor}}) \otimes \mathbb{C} = \Lambda \otimes \mathbb{C}$$

has a $\mathbb{C}[\Delta]$-invariant subspace V of the same dimension, so $V \rtimes \Delta$ contains a homomorphic image of Γ of infinite order. ∎

This concludes the proof of Theorem 1.9 and therefore, given Theorem 1.5, the proof of Theorem 0.3.

2. The geography of $(g, |\operatorname{Aut}(X)|)$

Let X be a Riemann surface of genus $g \geq 2$, Δ its automorphism group, $Y = X/\Delta$ the quotient Riemann surface, and π the quotient map. Suppose π is ramified at points $y_1, \ldots, y_n$ of Y with ramification indices $e_1, \ldots, e_n$; we choose the numbering so that $2 \leq e_1 \leq e_2 \leq \cdots \leq e_n$. Then the degree of the ramification divisor is

$$S|\Delta|,\ S = \sum_{i=1}^{n}(1 - e_i^{-1}).$$

Thus, if h is the genus of Y,

$$2g - 2 = (2h - 2 + S)|\Delta|.$$

We are only interested in the range $|\Delta| > 4(g-1)$, so we may assume $h = 0$. This is because if $h = 1$, the condition $g > 1$ implies $S > 0$, which implies $S \geq 1/2$. Thus, we may assume Y is a sphere.

Let $Y' := Y \smallsetminus \{y_1, \ldots, y_n\}$ and $X' := \pi^{-1}(Y')$. Thus X' is a regular covering space of Y', and the group of deck transformations is Δ. Fixing a base point $y \in Y'$, we obtain a surjective homomorphism p from $\pi_1(Y', y)$ to Δ by the usual method of lifting loops in Y' to paths in X'. We choose loops γ_i around y_i such that $\gamma_1 \cdots \gamma_n = 1$. By definition of ramification index, $\gamma_i^{e_i}$ lifts to a loop in X'. Thus p factors through the group $\Gamma_{e_1,\ldots,e_n}$ defined as follows:

Definition 2.1: We write $\Gamma_{e_1,\ldots,e_k}$ for the group with presentation

$$\langle x_1, x_2, \ldots, x_k | x_1^{e_1}, x_2^{e_2}, \ldots, x_k^{e_k}, x_1 x_2 \cdots x_k \rangle.$$

Conversely, a surjective homomorphism from $\Gamma_{e_1,\ldots,e_n}$ to a finite group Δ determines a regular covering space X' of Y' with group Δ and satisfying the property that each $\gamma_i^{e_i}$ lifts to a loop in X'. Lifting the structure of complex algebraic curve from Y' to X', we see that the latter is an open complex algebraic curve and therefore has a canonical compactification X. As X is canonical, Δ acts with quotient Y, and the ramification indices at y_i divide e_i. If the homomorphism does not factor through any $\Gamma_{d_1,\ldots,d_n}$, where $d_i \mid e_i$ and $\prod d_i < \prod e_i$, the ramification indices are exactly e_i.

PROPOSITION 2.2: *If a, b, c are positive integers, then $\Gamma_{a,b,c}$ has quotient dimension ≤ 3.*

Proof: It is clear that $\Gamma_{a,b,c}$ is the group of orientation-preserving isometries of a sphere, a Euclidean plane, or a hyperbolic plane generated by reflections through the sides of a triangle with angles π/a, π/b, and π/c. It is therefore contained in $\mathrm{SO}_3 \subset \mathrm{SO}_3(\mathbb{C})$, a wallpaper group, or $\mathrm{PSL}_2(\mathbb{R}) \subset \mathrm{PGL}_2(\mathbb{C})$. Thus the quotient dimension is no more than 3. ∎

PROPOSITION 2.3: *If a, b, c are positive integers such that*

$$11/12 < 1/a + 1/b + 1/c < 1,$$

then $\Gamma_{a,b,c}$ has quotient dimension ≥ 2.

Proof: If the quotient dimension is 1, by Proposition 1.3, we may assume that $\Gamma := \Gamma_{a,b,c}$ has an infinite quotient Zariski-dense in $G(\mathbb{C})$, an extension of a finite group by $\mathbb{C}$. As $G/Z_G(G^\circ)$ acts faithfully on $\mathbb{C}$, it is finite cyclic. Let d be its order. Thus Γ maps onto $\mathbb{Z}/d\mathbb{Z}$. This is possible only if every prime power factor of d divides at least two of a, b, and c. As $1/a + 1/b + 1/c \in (11/12, 1)$, the only possibilities are $(2,3,c)$, $7 \leq c \leq 11$ and $(2,4,5)$. In each case at least one of the exponents is relatively prime to both of the others. Without loss of generality we may assume that a is relatively prime to b and c and therefore that d divides the greatest common divisor of b and c. The kernel of the homomorphism $\Gamma \to \mathbb{Z}/d\mathbb{Z}$ is generated by conjugates of x, y^d, and z^d. Indeed,

$$y^k z^k = \prod_{i=1}^{k} y^{k-i} x^{-1} y^{i-k},$$

so both yz and $(zy)^{-1} = y^{bc-1} z^{bc-1}$ are such products. The image of the kernel in $G(\mathbb{C})$ lies in a central extension of $\ker(G/G^\circ \to \mathbb{Z}/d\mathbb{Z})$ by $\mathbb{C}$, which is necessarily trivial. Thus, we can project and obtain a homomorphism from the kernel to $\mathbb{C}$ with infinite image, generated by elements of finite order. The contradiction proves the proposition. ∎

PROPOSITION 2.4: *The groups $\Gamma_{2,3,7}$, $\Gamma_{2,3,8}$, and $\Gamma_{2,3,12}$ have quotient dimensions 3, 2, and 1 respectively.*

Proof: If the quotient dimension of $\Gamma := \Gamma_{2,3,7}$ is 2, there exists a 2-dimensional pseudo-simple group G of vector type such that $G(\mathbb{C})$ contains a quotient of Γ of vector type.

The quotient group $G/Z_G(G^\circ)$ is therefore a homomorphic image of Γ, and it acts faithfully on $\mathbb{C}^2$. It has no non-trivial commutative homomorphic image, since commuting elements x, y, z satisfying

$$x^2 = y^3 = z^7 = xyz = 1 \qquad (2.4.1)$$

must satisfy $x = y = z = 1$. By the classification of finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$, every finite subgroup of $\mathrm{GL}_2(\mathbb{C})$ which is not solvable maps onto the alternating group A_5. However, (2.4.1) has only trivial solutions in A_5 since $z^7 = 1$ implies $z = 1$. It follows that G is a central extension of $\pi_0(G)$ by G°. As $G^\circ = \mathbb{C}^2$, such an extension is trivial, so G° as a quotient of G admits a non-trivial homomorphism from Γ, which is absurd.

For $\Gamma := \Gamma_{2,3,8}$, we note first the homomorphism onto $\mathrm{GL}_2(\mathbb{F}_3)$:

$$x \mapsto A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad y \mapsto B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad z \mapsto C = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let ρ: $\mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathbb{C})$ denote a non-trivial representation. For any $v \in \mathbb{C}^2$, we can map Γ to $\mathbb{C}^2 \rtimes \mathrm{GL}_2(\mathbb{F}_3)$ sending x to $(0, A)$, y to $(-\rho(B)v, B)$, and z to (v, C). The image of z^4 is $((1 + \rho(C) + \rho(C^2) + \rho(C^3))v, -1)$. The commutator of $(w, -1)$ with the image of x is a non-trivial translation as long as w is not in the -1-eigenspace of the image of x. As $1 + \rho(C) + \rho(C^2) + \rho(C^3)$ is invertible, this can be guaranteed by a judicious choice of v.

For $\Gamma := \Gamma_{2,3,12}$ we can map to $\mathbb{C} \rtimes \mathbb{Z}/6\mathbb{Z}$ as follows:

$$x \mapsto (0,3),\ y \mapsto (1,2),\ z \mapsto (-e^{\frac{2\pi i}{3}}, 1).$$

As

$$z^3 \mapsto (-e^{\frac{2\pi i}{3}}(1 + e^{\frac{\pi i}{3}} + e^{\frac{2\pi i}{3}}), 1)$$

the commutator of x and z^3 is of infinite order in $\mathbb{C}$. ∎

Remark: $\Gamma = \Gamma_{2,3,7}$ has an additional homomorphism to a 3-dimensional pseudo-simple group. This is obtained in the following way. Let N be the normal subgroup of Γ of index 168, corresponding to the Klein quartic. The quotient Γ/N^{der} is an extension of $\mathrm{PSL}_2(7)$ by $\mathbb{Z}^6$ which gives rise to a Zariski-dense map from Γ to $\mathbb{C}^6 \rtimes \mathrm{PSL}_2(7)$. The latter has a pseudo-simple quotient of dimension 3. Aside from PGL_2, this is the only 3-dimensional complex group containing a Zariski-dense quotient of $\Gamma_{2,3,7}$.

THEOREM 2.5: *Let*

$$f(x) = \begin{cases} 1 & \text{if } x \le 24, \\ 1/2 & \text{if } 24 < x \le 48, \\ 1/3 & \text{if } 48 < x \le 84, \\ -\infty & \text{if } x > 84. \end{cases}$$

If $H_x = \{g \in \mathbb{N} \mid$ *There exists a Riemann surface* X *with* $\mathrm{Aut}(X) \ge x(g-1)\}$, *then*

$$\sum_{g \in H_x} g^{-s}$$

converges for $\Re(s) > f(x)$ and diverges at $s = f(x)$ assuming $x \leq 84$. In particular, for all $\epsilon > 0$, for all sufficiently large N,

$$N^{f(x)-\epsilon} \leq |\{1,2,\ldots,N\} \cap H_x| < N^{f(x)+\epsilon}.$$

Proof: The case $x > 84$ is immediate from the theorem of Hurwitz. For $x \in (48, 84]$, H_x is the set H in the introduction. It consists of finite quotients of $\Gamma_{2,3,7}$, so the corresponding ζ-function has abscissa of convergence $\Re(s) = 1/3$ and diverges at $1/3$. For $x \in (24, 48]$, H_x is a finite union of orders of finite quotients of certain $\Gamma_{a,b,c}$ all of which have quotient dimension ≥ 2 and at least one of which has quotient dimension 2. Moreover, each of these groups has the property that every sufficiently large quotient fails to be a quotient of a smaller $\Gamma_{a',b',c'}$ where $a' \mid a$, $b' \mid b$, and $c' \mid c$. For $x \leq 24$, the set in question includes all homomorphic images of $\Gamma := \Gamma_{2,3,12}$. This group has infinite quotient $\Gamma_{2,3,6}$, so we must exercise some care in showing that the set of homomorphic images of Γ which do not factor through $\Gamma_{2,3,6}$ is enough to give divergence at $s = 1$. If $\phi\colon \Gamma \to \Delta$ is any surjective homomorphism, we can map Γ to $\Delta \times S_{12}$ by

$$x \mapsto (\phi(x), (3\,4)(6\,7)(9\,10)),\ y \mapsto (\phi(y), (1\,2\,3)(4\,5\,6)(7\,8\,9)(10\,11\,12)),$$
$$z \mapsto (\phi(z), (1\,3\,6\,9\,12\,11\,10\,8\,7\,5\,4\,2)).$$

This gives a collection of homomorphisms which do not factor through $\Gamma_{2,3,6}$, and they are enough to give divergence at $s = 1$ since $Z_\Gamma(s)$ diverges at $s = 1$. ∎

Theorem 0.1 is a special case of this result. We remark that the fact that $f(24) = 1$ does not mean that H_{24} has positive density. On the other hand, by [1], H_8 contains all $g \geq 2$.

References

[1] R. D. M. Accola, *On the number of automorphisms of a closed Riemann surface,* Transactions of the American Mathematical Society **131** (1968), 398–408.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[3] M. du Sautoy and D. Segal, *Zeta functions of groups,* in *New Horizons in Pro-p Groups* (M. du Augoty, D. Segal and A. Shalev, eds.), Birkhauser, Boston, to appear.

[4] D. Gorenstein, *Classifying the finite simple groups,* Bulletin of the American Mathematical Society **14** (1986), 1–98.

[5] A. Hurwitz, *Über algebraische Gebilde mit eindeutigen Transformationen in sich*, Mathematische Annalen **41** (1893), 403–442.

[6] M. Larsen and R. Pink, *Finite subgroups of algebraic groups*, Journal of the American Mathematical Society, to appear.

[7] A. Lubotzky, *On finite index subgroups of linear groups*, The Bulletin of the London Mathematical Society **19** (1987), 235–328.

[8] A. M. Macbeath, *On a theorem of Hurwitz*, Proceedings of the Glasgow Mathematical Association **5** (1961), 90–96.

[9] B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups*, Annals of Mathematics **120** (1984), 271–315.