ON THE YAGITA INVARIANT OF MAPPING CLASS GROUPS

H. H. Glover, G. Mislin and Y. Xia

March 1993

Abstract. Let Γ denote a group of finite virtual cohomological dimension and p a prime. If the cohomology ring $H^*(\Gamma;\mathbb{F}_p)$ has Krull dimension one, the p-period of Γ is defined; it measures the periodicity of $H^*(\Gamma;\mathbb{F}_p)$ in degrees above the virtual cohomological dimension of Γ. The Yagita invariant $p(\Gamma)$ of Γ is a natural generalization of the p-period to groups with $H^*(\Gamma;\mathbb{F}_p)$ of Krull dimension larger than one. We compute the Yagita invariant $p(\Gamma_g)$ for the mapping class group Γ_g with respect to an arbitrary odd regular prime p.

Introduction

The mapping class group Γ_g is defined to be the group of path components of the group of orientation preserving diffeomorphisms of an oriented closed surface S_g of genus g. In this paper, we study for a given prime p the Yagita invariant $p(\Gamma_g)$, which is defined as follows (see [Y] for the case of finite groups and [T] for more general groups).

Let Γ be a group of finite virtual cohomological dimension and $\pi \subset \Gamma$ any subgroup of prime order p. It is well known that the image $\mathrm{Im}(H^k(\Gamma;\mathbb{Z}) \to H^k(\pi;\mathbb{Z}))$ of the restriction map in cohomology is non-zero for some degree $k > 0$. Because the natural map $H^*(\pi;\mathbb{Z}) \to H^*(\pi;\mathbb{F}_p)$ maps onto $\mathbb{F}_p[u] \subset H^*(\pi;\mathbb{F}_p)$ with u a generator in $H^2(\pi;\mathbb{F}_p)$, there exists a maximum value $m = m(\pi)$ such that

$$\mathrm{Im}((H^*(\Gamma;\mathbb{Z}) \longrightarrow H^*(\pi;\mathbb{F}_p)) \subset \mathbb{F}_p[u^m] \subset H^*(\pi;\mathbb{F}_p)\,.$$

It is easy to see (cf. Lemma 1.1) that the possible values $m(\pi)$ are bounded by a number depending on Γ only. The Yagita invariant $p(\Gamma)$ of Γ with respect to the prime p is then defined to be the least common multiple of values $2m(\pi)$, where π ranges over all subgroups of order p of Γ. We use the convention that $p(\Gamma) = 1$ if Γ is p-torsion free. The invariant $p(\Gamma)$ agrees with the p-period of a p-periodic group (i.e., a group with p-periodic Farrell cohomology groups, see [X1] and [X2] for a discussion of that concept) and, as it is the case for the p-period, the Yagita invariant $p(\Gamma)$ divides $2(p-1)p^k$, for some $k \geq 0$ (see Section 1).

The interest in $p(\Gamma)$ stems from the fact that it provides a lower bound for the dimension of a complex, which admits a certain type of action of Γ (see [Y] for the case of finite groups). For instance, one checks easily that if Γ acts properly discontinuously on $\mathbb{R}^n \times (S^m)^k$ and trivially on $H^*(\mathbb{R}^n \times (S^m)^k;\mathbb{Z})$, in a way that the stabilizer of any point $x \in \mathbb{R}^n \times (S^m)^k$ is a p-torsion free group, then $m+1$ is a

Typeset by $\mathcal{AMS}$-TEX

multiple of the Yagita invariant $p(\Gamma)$. We will discuss a variation of this in Section 4.

The mapping class group Γ_g is never 2-periodic for $g > 1$. For an odd prime p and p-periodic Γ_g we completely determined the p-period in [GMX]. We recall that for an odd prime p and genus $g \not\equiv 1 \mod p$, Γ_g is always p-periodic; thus we will only need to be concerned with the case $g \equiv 1 \mod p$ in the sequel. We have a complete result in case p is an odd regular prime, and partial results for general primes (recall that a prime p is called *regular* if p does not divide the class number of the cyclotomic field $\mathbb{Q}(\exp(2\pi\sqrt{-1}/p))$; the smallest irregular prime is 37). It is convenient for what follows to employ the following terminology.

Definition. *Let p be a prime. We say that an integer g satisfies the (p)-condition if and only if g is of the form $lp^\alpha + 1$ with l prime to p, $\alpha > 0$, and $2l = p(2h - 2) + k(p-1)$ for some integers $h > 0$, $k \geq 0$ with $k \neq 1$.*

Our main result is the following.

Theorem 1. *Let p be an odd regular prime and assume that $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$. Then the Yagita invariant $p(\Gamma_g)$ is determined as follows.*

(i) *If g does not satisfy the (p)-condition, then $p(\Gamma_g)$ equals $2(p-1)p^{\alpha-1}$.*
(ii) *If g satisfies the (p)-condition, then $p(\Gamma_g)$ equals $2(p-1)p^\alpha$.*

For the case of a general odd prime, we have the following partial results, which underline the role of the (p)-condition.

Theorem 2. *Let p be an odd prime and $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$. Then the following holds.*

(i) *$p(\Gamma_g)$ has the form $2(p-1)p^\alpha$ or $2(p-1)p^{\alpha-1}$.*
(ii) *If g satisfies the (p)-condition, then $p(\Gamma_g) = 2(p-1)p^\alpha$.*
(iii) *If $1 < 2l < p - 1$ then $p(\Gamma_g) = 2(p-1)p^{\alpha-1}$.*

Remark 1. For a fixed prime p and $\alpha > 0$ there are obviously only finitely many genera g of the form $lp^\alpha+1$ with l prime to p which do not satisfy the (p)-condition. Thus, we can think of (ii) in Theorem 2 as the generic case.

Remark 2. If the Krull dimension of $H^*(\Gamma_g; \mathbb{F}_p)$ equals one so that Γ_g is p-periodic, and if we assume g of the form $lp^\alpha + 1$ with l prime to p and $\alpha > 0$, then the (p)-condition does not hold for g. This can be seen by comparing the (p)-condition with the formula for the Krull dimension for Γ_g as stated in ([B]). Moreover, α is then necessarily equal to 1 (otherwise the Krull dimension is larger than 1 by [B]), and we recover the formula $p(\Gamma_g) = 2(p-1)$ of [GMX] for that case. The finite set of values l prime to p for which $g = lp+1$ gives rise to a p-periodic Γ_g was determined in an explicit way in [X3], where it is proved that Γ_{lp+1} with l prime to p is p-periodic if and only if $l+1$ is prime to p and the interval $[(2l+3)/p, (2l+2)/(p-1)]$ does not contain an integer. The reader can then easily check that the smallest genus g for which there is an odd prime such that the Yagita invariant is not given either by [GMX], Theorem 1 or Theorem 2 is $g = 1296 = 35 \cdot 37 + 1$.

Remark 3. From Lemma 2.2 it will become obvious that the (p)-condition has a geometric interpretation as follows. If p denotes a prime and $g = lp^\alpha + 1$ with l

prime to p and $\alpha > 0$ then g satisfies the p-condition if and only if Γ_g contains a cyclic subgroup C of order $p^{\alpha+1}$ such that C lifts to an action on S_g with all stabilizers of order $\leq p$; note also that the C action on S_g cannot be free, since $g-1 = lp^\alpha$ is not divisible by $p^{\alpha+1}$.

The remainder of this paper is organized as follows. In Section 1 we provide some basic facts about the Yagita invariant and establish rather crude lower and upper bounds. In Section 2 we recall the definition of the fixed point data of an element of finite order in the mapping class group Γ_g and develop a technique of *moves*, which requires the prime in question to be regular. The *moves* are used in Section 3 to study representations of subgroups of order p of Γ_g on the space of holomorphic differentials of a Riemann surface of genus g. As a result, we will obtain precise lower bounds for Γ_g. Using the action of Γ_g on a suitable submanifold of the Teichmüller space of surfaces of genus g we establish in Section 4 an upper bound for Γ_g and use it to determine sharp upper bounds in Section 5, completing the proofs of the Theorems 1 and 2.

We would like to thank R. Swan for providing the proof of Proposition 2.3.

Section 1 : Some basic facts concerning the Yagita invariant

Our first lemma provides an upper bound for the Yagita invariant $p(\Gamma)$.

Lemma 1.1. *Let p be a prime and Γ a group of finite virtual cohomological dimension, which has p-torsion. Let G denote a finite factor group of Γ such that the kernel of the projection $\Gamma \to G$ is p-torsion free. Then the Yagita invariant $p(\Gamma)$ divides $2(p-1)p^{k-1}$, where p^k denotes the largest power of p which divides the order of G.*

Proof. We consider the regular representation $\rho : G \to Gl_{|G|}(\mathbb{C})$ of the finite group G. If we restrict ρ to a subgroup π of order p in G, then $\rho|\pi$ is of the form $sp^{k-1}\sigma$, where s is prime to p and σ denotes the regular representation of π. Since the total Chern class $c(\sigma)$ in $H^*(\pi;\mathbb{Z})$ has the form $1 + c_{p-1}(\sigma)$ with $c_{p-1}(\sigma) \neq 0$, we see that $c_{(p-1)p^{k-1}}(\rho)$ restricts to $sc_{p-1}(\sigma)^{p^{k-1}}$, which is non-trivial in the integral cohomology of π. Therefore, the Yagita invariant of the factor group G must divide $2(p-1)p^{k-1}$. But every subgroup of order p in Γ_g injects into G via the projection, and therefore viewing ρ as a representation $\tilde{\rho}$ of Γ, its Chern class $c_{(p-1)p^{k-1}}(\tilde{\rho})$ will restrict non-trivially to any subgroup of order p in Γ, showing that $p(\Gamma)$ divides $2(p-1)p^{k-1}$ too.

It is often possible to improve on the power of p in the upper bound of $p(\Gamma)$ as follows.

Lemma 1.2. *Let p be a prime, Γ a group of finite virtual cohomological dimension, and assume that $\rho : \Gamma \to Gl_d(\mathbb{C})$ is a representation of degree d such that ρ does not have any element of order p in the kernel.*

(i) *If $d < p^m$ then $p(\Gamma)$ divides $2(p-1)p^{m-1}$.*
(ii) *If $\rho(\Gamma) \subset Gl_d(\mathbb{Q})$ and $d < (p-1)p^m$ then $p(\Gamma)$ divides $2(p-1)p^{m-1}$.*

Proof. We know already that $p(\Gamma)$ divides $2(p-1)p^n$ for some n. If we were not able to choose $n = m-1$, then there would exist a subgroup $\pi \subset \Gamma$ such that the restriction map $H^*(\Gamma;\mathbb{Z}) \to H^*(\pi;\mathbb{Z})$ is zero for $0 < * < 2p^m$. But, assuming $d < p^m$, one would infer for the total Chern class $c(\rho|\pi)$ equals 1. This is a contradiction, since ρ is faithful when restricted to π . In case $\rho(\Gamma) \subset Gl_d(\mathbb{Q})$, all non-zero Chern classes of $\rho|\pi$ lie in degrees of the form $2(p-1)p^l$, see ([EM]), and thus it suffices to assume $d < (p-1)p^m$ to conclude that some Chern class of $\rho|\pi$ is non-zero in the range $0 < * < 2p^m$.

Applying this to the case of the mapping class group Γ_g we obtain the following upper bound for the Yagita invariant.

Lemma 1.3. *Let p be an arbitrary prime and $0 < 2g < (p-1)p^m$. Then $p(\Gamma_g)$ divides $2(p-1)p^{m-1}$.*

Proof. We consider the natural action of Γ_g on $H_1(S_g;\mathbb{Q})$ which defines a representation $\rho : \Gamma_g \to Gl_{2g}(\mathbb{Q})$ with torsion-free kernel. The result then follows from (ii) of Lemma 1.2.

It is plain from the definition that the Yagita invariant for a subgroup of Γ divides $p(\Gamma)$. We can therefore find lower bounds for $p(\Gamma)$ by looking at suitable subgroups of Γ. This leads to the following useful lemma.

Lemma 1.4. *Let π be a cyclic subgroup of p-power order of Γ, with p an odd prime. If we denote by $C(\pi)$ (respectively $N(\pi)$) the centralizer (respectively normalizer) of π in Γ then $p(\Gamma_g)$ is a multiple of $2[N(\pi) : C(\pi)]$.*

Proof. Let W be the cyclic group $N(\pi)/C(\pi)$. The image of the restriction map in cohomology $H^*(\Gamma;\mathbb{Z}) \to H^*(\pi;\mathbb{Z})$ maps into the subring of W-invariant elements, which is of the form $\mathbb{Z}[x^m]/(p^k x^m)$, where $x \in H^2(\pi;\mathbb{Z})$ denotes a generator, $m = |W|$ the order of W, and p^k the order of π. The result then follows readily.

As an application of Lemma 1.4, we deduce the lower bound (i) of Theorem 2 of the introduction.

Lemma 1.5. *Let p be an odd prime and assume that g is of the form $lp^\alpha + 1$ with l prime to p and $\alpha > 0$. Then $p(\Gamma_g)$ equals $2(p-1)p^\beta$ for some $\beta \geq \alpha - 1$.*

Proof. We know from Lemma 1.1 that $p(\Gamma_g)$ divides $2(p-1)p^n$ for some $n \geq 0$. If $g = lp^\alpha + 1$ with l prime to p, the surface S_g is a p^α-fold regular (unbranched) covering space of S_h where $h = l + 1$, with cyclic covering transformation group generated by a map $f : S_g \to S_g$. Since f acts freely, it is conjugate in $\mathrm{Diffeo}^+(S_g)$ to f^j for any j prime to p ([N], see also Lemma 2.1 below). The subgroup $\Delta \subset \Gamma_g$ generated by the image of f in Γ_g has order p^α and $N(\Delta)/C(\Delta)$ is isomorphic to the full automorphism group of $\Delta \cong \mathbb{Z}/p^\alpha$ which has order $(p-1)p^{\alpha-1}$ (see also Lemma 2.1 below). Therefore, using Lemma 1.1 and Lemma 1.4, the result follows.

Comparing the lower and upper bounds for the Yagita invariant of the mapping class group, we obtain part (iii) of Theorem 2 of the Introduction.

Corollary 1.6. *Let p be an odd prime and $g = lp^\alpha + 1$ with $1 < 2l < p - 1$ and $\alpha > 0$. Then the Yagita invariant $p(\Gamma_g)$ equals $2(p-1)p^{\alpha-1}$.*

Proof. Since $2g = 2lp^\alpha + 2 \leq (p-2)p^\alpha + 2 < (p-1)p^\alpha$ we infer from Lemma 1.3 that $p(\Gamma_g)$ divides $2(p-1)p^{\alpha-1}$. On the other hand Lemma 1.5 shows that $p(\Gamma_g)$ is a multiple of $2(p-1)p^{\alpha-1}$.

Section 2 : Fixed point data and moves

A basic invariant of an orientation preserving diffeomorphism f of S_g of period $n > 1$ is its fixed point data. It is defined as follows. Since f preserves orientation, the singular set of f is necessarily discrete in S_g. Let $\{x_i\}$ be a set of representatives of the singular orbits of f and write α_i for the order of $stab_f(x_i)$, the stabilizer of f at $x_i \in S_g$. Then f^{n/α_i} generates $stab_f(x_i)$ and, with respect to a fixed Riemannian structure, the differential of f^{n/α_i} acts faithfully by rotation on the tangent space at x_i. Let β_i be an integer such that $f^{\beta_i n/\alpha_i}$ acts by rotation through $2\pi/\alpha_i$. The number β_i is well defined modulo α_i, and β_i is prime to α_i. The fixed point data of f, denoted $\delta(f)$, is then the collection

$$\delta(f) =< g, n \mid \beta_1/\alpha_1, \ldots, \beta_q/\alpha_q >$$

where g is the genus of the surface S_g, n the order of f, and q the number of singular orbits of the f-action; the numbers $\beta_1/\alpha_1, \ldots, \beta_q/\alpha_q$ are unique up to order, if we consider them as elements in $\mathbb{Q}/\mathbb{Z}$.

A classical theorem of Nielsen [N] states that two diffeomorphisms of finite order are conjugate in $\mathrm{Diffeo}^+(S_g)$ if and only if they have the same fixed point data. Symonds [Sy] proved that the fixed point data of a diffeomorphism of finite order depends only upon its isotopy class, and thus is well defined for an element of finite order of the mapping class group Γ_g; we will thus write $\delta(x)$ for the fixed point data of an element of finite order $x \in \Gamma_g$. He also shows that the Nielsen Theorem is still true for the mapping class group Γ_g, that is, two elements of finite order in Γ_g are conjugate if and only if they have the same fixed point data. As an immediate consequence, one can deduce the following.

Lemma 2.1. *Suppose that $f \in \mathit{Diffeo}^+(S_g)$ has finite order n and acts freely on S_g. Denote by x the image of f in Γ_g. Then the index $[N(x) : C(x)]$ of the centralizer of x in its normalizer equals $\phi(n)$, ϕ the Euler function.*

Proof. Indeed, all the generators of the cyclic group $< x >$ generated by x have the same fixed point data $\delta =< g, n| >$ and are therefore conjugate in Γ_g. Thus $N(x)$ maps onto the automorphism group of $< x >$, with kernel $C(x)$, and the result follows.

The well-known techniques on realizing fixed point data lead to the following result, of which we sketch the proof for the convenience of the reader.

Lemma 2.2. *Let p be a prime and $\beta_1, \ldots, \beta_q$ integers prime to p. Then the collection*

$$< g, p^t \mid \beta_1/p^{t_1}, \ldots, \beta_q/p^{t_q} >$$

can be realized as the fixed point data of an element of order p^t in Γ_g if and only if the following three conditions are satisfied.

- (i) $\sum \beta_i/p^{t_i}$ *is an integer .*
- (ii) *The Riemann-Hurwitz formula $2g-2 = p^t(2h-2) + p^t \sum (1 - 1/p^{t_i})$ holds for some $h \geq 0$.*
- (iii) *If $h = 0$ in* (ii), *then $t = max(t_1, \ldots, t_q)$.*

Proof. Suppose the given collection is the fixed point data of some $x \in \Gamma_g$, represented by the diffeomorphism f of S_g of order p^t. Then there is a branched covering $S_g \to S_h$ with set of branch points $\{y_1, \dots, y_q\} \subset S_h$ and group $\mathbb{Z}/p^t$, giving rise to a regular covering

$$S_g \setminus \pi^{-1}\{y_1, \dots, y_q\} \to S_h \setminus \{y_1, \dots, y_q\},$$

which induces a short exact sequence

$$\pi_1(S_g \setminus \pi^{-1}\{y_1, \dots, y_q\}) \longrightarrow \pi_1(S_h \setminus \{y_1, \dots, y_q\}) \xrightarrow{\partial} < f > \cong \mathbb{Z}/p^t .$$

Note that

$$\pi_1(S_h \setminus \{y_1, \dots, y_q\}) = < a_1, b_1, \dots, a_h, b_h, x_1, \dots, x_q \mid \prod_{i=1}^{h} [a_i, b_i] x_1 \dots x_q = 1 >$$

and $\partial(x_i) = f^{\beta_i p^{t-t_i}}$ for $1 \le i \le q$. Therefore (i) is true since the map ∂ preserves the relation $\prod_{i=1}^h [a_i, b_i] x_1 \dots x_q = 1$. By calculating the Euler characteristics of $S_g \setminus \pi^{-1}\{y_1, \dots, y_q\}$ and $S_h \setminus \{y_1, \dots, y_q\}$ one gets (ii), and (iii) follows from the surjectivity of the map ∂. Conversely, given (i), (ii) and (iii) we begin by constructing a surjective homomorphism

$$\partial : \pi_1(S_h \setminus \{y_1, \dots, y_q\}) \longrightarrow \mathbb{Z}/p^t$$

such that $\partial(x_i)$ is a suitable element of order p^{t_i} for $1 \le i \le q$. This can be done, if $h > 0$, by putting $\partial(a_1) = \partial(b_1) = 1$, $\partial(a_i) = \partial(b_i) = 0$ for $2 \le i \le h$, and $\partial(x_j) = \beta_j p^{t-t_j}$ for $1 \le j \le q$. In case $h = 0$, we still put $\partial(x_j) = \beta_j p^{t-t_j}$ for $1 \le j \le q$. The condition (iii) then guarantees that the map ∂ is surjective. The kernel of ∂ defines a p^t-sheeted regular covering $S_g \setminus \{z_1, \dots, z_r\} \longrightarrow S_h \setminus \{y_1, \dots, y_q\}$, giving rise to a branched covering $S_g \to S_h$, with covering transformation group generated by a diffeomorphism with the desired fixed point data.

Note that given an element $x \in \Gamma_g$ of order p^t, one can determine the fixed point data $\delta(x^k)$ from $\delta(x) = < g, p^t | \beta_1/p^{t_1}, \dots \beta_1/p^{t_q} >$ as follows. When k is prime to p then

$$\delta(x^k) = < g, p^t \mid l\beta_1/p^{t_1}, \dots, l\beta_q/p^{t_q} >$$

where l is a multiplicative inverse of $k \mod p^t$. When k is a multiple of p, say $k = mp^s$, with m prime to p, the subgroup generated by k in $\mathbb{Z}/p^t$ is naturally isomorphic to $\mathbb{Z}/p^{t-s}$ by mapping $k = mp^s$ to m in $\mathbb{Z}/p^{t-s}$. If we write n for a multiplicative inverse of $m \mod p^{t-s}$ then

$$\delta(x^{mp^s}) = < g, p^{t-s} \mid A_{1,1}, \dots, A_{1,m_1}, \dots, A_{q,1}, \dots, A_{q,m_q} >, \qquad 1 \le i \le q, 1 \le j \le m_i ,$$

where the $A_{i,j}$ correspond to β_i in $\delta(x)$, $m_i = p^{\min(s,t-t_i)}$, and $A_{i,j} = n\beta_i/p^{\min(t-s,t_i)}$ for $1 \le j \le m_i$.

For example, if

$$\delta(x) = < 183, 81 \mid 11/81, 14/81, 1/27, 1/9, 1/3 >$$

then

$$\delta(x^{41}) =< 183, 81 \,|\, 22/81, 28/81, 2/27, 2/9, 2/3 >$$

$$\delta(x^3) =< 183, 27 \,|\, 11/27, 14/27, 1/27, 1/27, 1/27, 1/9, 1/9, 1/9, 1/3, 1/3, 1/3 >$$

$$\delta(x^9) =< 183, 9 \,|\, 2/9, 5/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/3, 1/3, 1/3, 1/3, 1/3, 1/3, 1/3, 1/3, 1/3 >$$

and so on.

The following proposition, which will be used repeatedly later on, was suggested to us by an explicit computation with the help of a computer program. The actual proof as presented below was communicated to us by R. Swan ([Sw]). For an integer n and a fixed prime number p we will use the notation $\tilde{n}$ to denote the unique integer satisfying $0 \le \tilde{n} < p$ and $n \equiv \tilde{n} \mod p$. We will also write $< r >$ for the fractional part of a number $r \in \mathbb{Q}$, so that $r = [r] + < r >$, with $[r]$ the integral part of r. Note that for any $n \in \mathbb{Z}$ one has $\tilde{n} = p < n/p >= n - p[n/p]$.

Proposition 2.3. *Let p be an odd prime and consider the integral $(p-1)/2 \times (p-1)/2$ matrix $A = (a_{ij})$ whose (i,j) entry a_{ij} is defined to be p if $i = 1$, and $\widetilde{ij}$ if $2 \le i \le (p-1)/2$. Then the matrix A is non-singular. Moreover, the entries of the matrix pA^{-1} are rational numbers which have, in reduced form, no p in the denominators if and only if p is a regular prime.*

Proof [Sw]. For $p \le 5$ the claim is easily checked directly. If $p > 5$ we proceed as follows. By subtracting each column of A from the next one we get a matrix B which, after subtracting the second column of B from the first one, takes the form

$$C = \begin{pmatrix} p & 0 & 0 & \dots & 0 \\ 0 & 2 & 2 & \dots & 2 \\ 0 & 3 & & & \\ \vdots & \vdots & & a_{i,j} - a_{i,j-1} & \\ 0 & (p-1)/2 & & & \end{pmatrix}.$$

Now $a_{i,j} - a_{i,j-1} = ij - p[ij/p] - i(j-1) + p[i(j-1)/p] = i - pe_{i,j}$, where

$$e_{i,j} = [ij/p] - [i(j-1)/p], \qquad 3 \le i,j \le (p-1)/2$$

are the entries of a $(p-5)/2 \times (p-5)/2$ matrix E. Subtracting the second column of C from the rest reduces C to

$$D = \begin{pmatrix} p & 0 & 0 & \dots & 0 \\ 0 & 2 & 0 & \dots & 0 \\ 0 & 3 & & & \\ \vdots & \vdots & & -pE & \\ 0 & (p-1)/2 & & & \end{pmatrix}$$

with

$$D^{-1} = \begin{pmatrix} p^{-1} & 0 & 0 & \dots & 0 \\ 0 & 2^{-1} & 0 & \dots & 0 \\ 0 & f_{3,2} & & & \\ 0 & f_{4,2} & & & \\ \vdots & \vdots & & -\frac{1}{p}E^{-1} & \\ 0 & f_{(p-1)/2,2} & & & \end{pmatrix}.$$

The last $(p-5)/2$ entries of the second column of D^{-1} are given by

$$\begin{pmatrix} f_{3,2} \\ f_{4,2} \\ \vdots \\ f_{(p-1)/2,2} \end{pmatrix} = -\frac{1}{2p} E^{-1} \begin{pmatrix} 3 \\ 4 \\ \vdots \\ (p-1)/2 \end{pmatrix}$$

and pD^{-1} has no p in the denominators if and only if $\det E$ is prime to p. By [CO], $\det E = \pm h_1$, where h_1 is the first factor of the class number of $\mathbb{Q}(\exp 2\pi\sqrt{-1}/p)$. But Kummer showed p is regular if and only if p does not divide h_1.

The following lemma is immediate and we state it without proof.

Lemma 2.4. *Suppose we are given a prime p and an integral linear system*

$$\text{(L)} \qquad Ax = b$$

such that

(i) *$A \in M_n(\mathbb{Z})$ has non-zero determinant,*
(ii) *$b \equiv 0 \mod p^2$,*
(iii) *pA^{-1} in reduced form has the property that the matrix entries have no p in their denominators.*

If x denotes an integral solution of (L), then $x \equiv 0 \mod p$.

As a consequence we will prove the following proposition, which plays a crucial role in the sequel.

Proposition 2.5. *Let p be a regular prime and suppose we are given an integer $n > 0$ divisible by p and n integers β_i with $0 < \beta_i < p$, where $1 \le i \le n$. Write α_j for the number of β_i's which equal j for $1 \le j < p$. If the fractional parts $< j\beta_i/p >$ satisfy*

$$\text{(1)} \qquad \sum_i < j\beta_i/p > \equiv 0 \mod p, \qquad 1 \le j < p$$

then $\alpha_j \equiv \alpha_{p-j} \mod p$ for all j.

Proof. The case $p = 2$ is trivial, so we will assume $p \ge 3$. One can then rewrite each sum in (1) in terms of the α_i's as follows:

$$e_1 = \sum_i < \beta_i/p > = \sum_i \alpha_i < i/p > \equiv 0 \mod p$$

$$e_2 = \sum_i < 2\beta_i/p > = \sum_i \alpha_i < 2i/p > \equiv 0 \mod p$$

$$\cdots\cdots\cdots\cdots$$

$$e_{p-1} = \sum_i < (p-1)\beta_i/p > = \sum_i \alpha_i < (p-1)i/p > \equiv 0 \mod p.$$

For $(p+1)/2 \leq i \leq p-1$ we have $2 < i/p > - < 2i/p >= 1$, and the first two equations yield

$$\sum_{i=(p+1)/2}^{p-1} \alpha_i = 2e_1 - e_2\,.$$

Noting that $\sum_{i=1}^{p-1} \alpha_i = n = kp$, we obtain an equation which we consider as the first equation of a linear system (L) of the type $Ax = b$ considered in Lemma 2.4, with the transpose of x the vector

$$(x_1, \ldots, x_{(p-1)/2}) = (\alpha_1 - \alpha_{p-1}, \ldots, \alpha_{(p-1)/2} - \alpha_{(p+1)/2})$$

namely the equation

$$px_1 + px_2 + \cdots + px_{(p-1)/2} = p(n - 4e_1 + 2e_2)\,.$$

Observe that the right hand side is $0 \mod p^2$. By using the fact that $< (p-j)i/p >= 1- < ji/p >$, we obtain $(p-3)/2$ additional equations for our system (L), which take the form

$$p < 2/p > x_1 + p < 4/p > x_2 \cdots + p < (p-1)/p > x_{(p-1)/2} = p(e_2 - \sum_{i=(p+1)/2}^{p-1} \alpha_i)$$

$$p < 3/p > x_1 + p < 6/p > x_2 + \cdots + p < 3(p-1)/2p > x_{(p-1)/2} = p(e_3 - \sum_{i=(p+1)/2}^{p-1} \alpha_i)$$

$$\cdots\cdots\cdots$$

$$p < (p-1)/2p > x_1 + \cdots + p < (p-1)^2/4p > x_{(p-1)/2} = p(e_{(p-1)/2} - \sum_{i=(p+1)/2}^{p-1} \alpha_i)$$

It is easy to see that the right hand sides of all equations are $0 \mod p^2$ since by assumption all e_i's are $0 \mod p$ and, as we have seen, $\sum_{i=(p+1)/2}^{p-1} \alpha_i \equiv 0 \mod p$. Observing that for any integer k one has $k \equiv p < k/p > \mod p$, we see that the matrix A of the linear system (L) is precisely the matrix A of Proposition 2.3. Thus, by applying Lemma 2.4, we infer that $\alpha_j - \alpha_{p-j} \equiv 0 \mod p$ for $1 \leq j \leq p-1$, completing the proof.

The following theorem can be viewed as a purely algebraic version of our "moves" concerning fixed point data as considered in the next section.

Theorem 2.6. *Suppose p is an odd regular prime and $n > 0$ an integer which is divisible by p. Suppose the system of $p-1$ equations*

$$\sum_{i=1}^{n} < jx_i/p > \equiv 0 \mod p, \qquad 1 \leq j \leq p-1$$

has an integral solution $x = (x_1, \ldots, x_n)$ with $0 < x_i < p$ for all i. Then it also has an integral solution $z = (z_1, \ldots, z_n)$ with $0 < z_i < p$ for all i such that *for any given integer j the number of z_i's which equal j is divisible by p, and $\sum_i < jx_i/p >= \sum_i < jz_i/p >$ for all j.*

Proof. Let $x = (x_1, \ldots, x_n)$ be a solution as above, and denote by $\alpha_j(x)$ the number of x_i's which are equal to j, where $0 < j < p$. Then we can rewrite our system of equations as

$$\sum_{i=1}^{p-1} \alpha_i(x) < ji/p > \equiv 0 \mod p\,, \qquad 1 \le j \le p-1$$

so that for all j one has $\alpha_j(x) \equiv \alpha_{p-j}(x) \mod p$ by Proposition 2.5. We can now alter the solution $x = (x_1, \ldots, x_n)$ to $y = (y_1, \ldots, y_n)$ by applying a *move of type* (s, t), where $1 \le s, t \le p-1$ and $s \ne t$, by which we mean the following :

(i) replace $\alpha_s(x)$ by $\alpha_s(y) = \alpha_s(x) + 1$
(ii) replace $\alpha_{p-s}(x)$ by $\alpha_{p-s}(y) = \alpha_{p-s}(x) + 1$
(iii) replace $\alpha_t(x)$ by $\alpha_t(y) = \alpha_t(x) - 1$
(iv) replace $\alpha_{p-t}(x)$ by $\alpha_{p-t}(y) = \alpha_{p-t}(x) - 1$.

Note that for such a move to be possible we need to have a t such that $\alpha_t(x) > 0$. If we alter x accordingly into y, we obtain a new system of equations satisfying

$$\sum_{i=1}^{p-1} \alpha_i(y) < ij/p >= \sum_{i=1}^{p-1} \alpha_i(x) < ij/p >$$

for $0 < j < p$, because $< ij/p > + < (p-i)j/p >= 1$. Suppose now that not all $\alpha_i(x)$'s are already divisible by p. Then, using Proposition 2.5 and writing n as kp, we have

$$n = kp = \sum_{i=1}^{p-1} \alpha_i(x) \equiv 2 \sum_{i=1}^{(p-1)/2} \alpha_i(x) \equiv 0 \mod p,$$

and we conclude that there must exist a pair (s, t) with $1 \le s, t \le (p-1)/2$ and $s \ne t$ such that $\alpha_s(x)$ and $\alpha_t(x)$ are both not divisible by p. Performing a move of type (s, t) will provide a new solution y. If $\alpha_s(y)$ and $\alpha_t(y)$ are both still not divisible by p, we repeat the move of type (s, t), and eventually α_s or α_t will be a multiple of p. By continuing in this manner, we will end up with the required solution z.

Section 3 : Chern classes of representations on holomorphic differentials

The action of Γ_g on the symplectic space $H_1(S_g; \mathbb{R})$ with its intersection pairing gives rise to a representation $\rho : \Gamma_g \to Sp(2g, \mathbb{R})$, which we call the *canonical* representation of Γ_g in the sequel. Recall that

$$H^*(BSp(2g, \mathbb{R}); \mathbb{Z}) \cong \mathbb{Z}[d_1, \ldots, d_g]$$

where the d_i's are such that they restrict to the universal Chern classes of a maximal compact subgroup $U(g) \subset Sp(2g, \mathbb{R})$. The images of the d_i's under the induced map

$$\rho^* : H^*(BSp(2g, \mathbb{R}); \mathbb{Z}) \longrightarrow H^*(\Gamma_g; \mathbb{Z})$$

gives rise to *symplectic* characteristic classes

$$d_i(\rho) := \rho^*(d_i) \in H^{2i}(\Gamma_g;\mathbb{Z}), \qquad 0 \le i \le g\,.$$

We are going to study the behavior of the restriction of these symplectic characteristic classes to cyclic subgroups Δ of order p^n in Γ_g. Note that $\rho|\Delta$ factors, up to conjugation, through $U(g) \subset Sp(2g,\mathbb{R})$ and we can view the classes $d_i(\rho|\Delta)$ as the Chern classes $c_i(\bar\rho)$ of a representation $\bar\rho : \Delta \to U(g)$. This representation can be thought of in the following way. One chooses a lift of a generator of Δ to an element of order p^n in $\mathrm{Diffeo}^+(S_g)$ and chooses a complex structure on S_g compatible with the orientation of S_g such that f acts by a holomorphic automorphism. Then f acts on the associated space of holomorphic differentials, which is a complex vector space of complex dimension g. This action defines a representation of Δ, whose dual is equivalent to the representation $\bar\rho : \Delta \to U(g)$ introduced above. We will sometimes, by abuse of language, refer to $\bar\rho$ as the representation of Δ on holomorphic differentials of S_g.

We will make use of the following basic property of Chern classes of representations.

Lemma 3.1. *Let $\rho : \mathbb{Z}/p^n \to U(g)$ be a representation of $\mathbb{Z}/p^n$, p a fixed prime. Assume that ρ can be decomposed as $\oplus_{i=0}^{p^n-1} n_i\omega^i$ where ω denotes a faithful one dimensional representation and where $n_i = n_j$ for all (i,j) which satisfy $0 < i,j < p^n$ and $i \equiv j \not\equiv 0 \mod p$. Then the following are equivalent.*

(i) *The Chern classes $c_i(\rho) \in H^{2i}(\mathbb{Z}/p^n;\mathbb{Z})$ are all $0 \mod p$ for $1 \le i \le p^n-1$,*
(ii) *$n_i \equiv 0 \mod p$ for $0 < i < p$.*

Proof. We first prove that (i) implies (ii). It is convenient for this proof to assume that ρ satisfies in addition $n_0 = n_p = \cdots = n_{p^n-p}$; this will not change the $\mod p$ Chern classes of ρ. Consider the ring homomorphism

$$\phi : H^*(\mathbb{Z}/p^n;\mathbb{Z}) \to (\mathbb{Z}/p^n)[x]$$

given by mapping $c_1(\omega) \in H^2(\mathbb{Z}/p^n;\mathbb{Z})$ to x. Let $f(x) \in (\mathbb{Z}/p^n)[x]$ be defined by $\prod_{i=0}^{p^n-1}(1+ix)^{n_i}$ and $F(x) \in (\mathbb{Z}/p)[x]$ by $\prod_{i=0}^{p-1}(1+ix)^{n_i}$. Notice that $\phi(c(\rho)) = f(x)$. We then have $f(x) \equiv \prod_{k=0}^{p-1}(1+kx)^{n_k p^{n-1}} \equiv \prod_{k=0}^{p-1}(1+kx^{p^{n-1}})^{n_k} \mod p$, thus $f(x) \equiv F(x^{p^{n-1}}) \mod p$. Now, the assumption that $c_i(\rho) \equiv 0 \mod(p)$ for $1 \le i \le p^n-1$ implies that $f(x) \equiv 1 + pg(x) \mod x^{p^n}$, and therefore, $F(x) \equiv 1 \mod x^p$. So, by Lemma 4.1 of [GMX], we conclude that $n_k \equiv 0 \mod p$ for all k satisfying $1 \le k \le p-1$. It remains to check that (ii) implies (i). If (ii) holds, we can write ρ in the form $pk\sigma + \tau$, where σ denotes the reduced regular representation of $\mathbb{Z}/p^n$, and τ a representation which factors through $\mathbb{Z}/p^{n-1}$ so that $c(\tau) \equiv 1 \mod p$. Since $c(\sigma) = 1 + c_{(p-1)p^{n-1}}(\sigma)$ we see that

$$c(\rho) = c(\sigma)^{pk} \cdot c(\tau) \equiv (1 + c_{(p-1)p^{n-1}}(\sigma)^p)^k \mod p\,,$$

so that $c_i(\rho) \equiv 0 \mod p$ for $0 < i < (p-1)p^n$.

Our theorem on algebraic moves leads to the following result, obtained by a geometric version of "moves" of fixed point data. It will provide a proof of case (i) of Theorem 2 of the introduction (see Corollary 3.3), and it will also provide us with an improved lower bound for Γ_g, needed for the proof of case (ii) of Theorem 2.

Proposition 3.2. *Let p denote an odd regular prime and ρ the canonical representation of Γ_g in $Sp(2g,\mathbb{R})$. Assume $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$, and suppose g does not satisfy the (p)-condition. Then for every subgroup $\pi \subset \Gamma_g$ of order p, at least one characteristic class $d_i(\rho|\pi) \in H^{2i}(\pi;\mathbb{Z})$ is non-zero in the range $1 \le i \le p^\alpha - 1$.*

Proof. Suppose there is a subgroup π of order p in Γ_g such that $d_i(\rho|\pi) = 0$ for $1 \le i \le p^\alpha - 1$. We will show that this leads to a cyclic subgroup of Γ_g of order $p^{\alpha+1}$, which acts on S_g with stabilizers of order $\le p$. The Riemann-Hurwitz equation associated with this action yields then an equation contradicting the assumtion concerning the (p)-condition. The construction of such a subgroup is by induction on its order. First, we begin by modifying π slightly, not changing the Chern classes, using our technique of "moves" as follows. Let $\bar{\rho} : \pi \to U(g)$ be the representation of π on the space of holomorphic differentials on S_g (with respect to a suitable complex structure) and write $\bar{\rho}$ as $\oplus_{i=0}^{p-1} n_i \omega^i$, ω a faithful irreducible one dimensional representation of π. Thus we have $d_i(\rho|\pi) = c_i(\bar{\rho}) = 0$ for $1 \le i \le p-1$. Applying Lemma 3.1, we infer $n_i \equiv 0 \mod p$ for $1 \le i \le p-1$. Let $x \in \pi$ be a generator and denote by $< g, p \,|\, \beta_1/p, \ldots, \beta_n/p >$ the fixed point data of x, normalized such that $0 < \beta_i < p$. As we discussed in Proposition (4.3) of [GMX], see also [FK], one has then

$$n_j = h - 1 + n - \sum_{i=1}^{n} < j\beta_i/p > , \qquad 0 < j < p, \tag{2}$$

where h denotes the genus of S_g/π. Note that the Riemann-Hurwitz equation $2g - 2 = p(2h-2) + n(p-1)$ shows that $n \equiv 0 \mod p$ and, as argued in [GMX], by considering $n_j - n_{p-j} = 2\sum_i < j\beta_i/p > + n$ it follows, because for $0 < j < p$ each n_j is divisible by p, that

$$\sum_{i=1}^{n} < j\beta_i/p > \equiv 0 \mod p, \qquad 0 < j < p.$$

Equation (2) then implies that $h - 1 \equiv 0 \mod p$, which in particular shows that the orbit genus h is greater than 0. By applying Theorem 2.6 and Lemma 2.2, there are n integers γ_i with $0 < \gamma_i < p$, forming the fixed point data $< g, p|\gamma_1/p, \ldots, \gamma_n/p >$ of a generator of a subgroup $\tilde{\pi}$ of order p in Γ_g, which gives rise to a representation $\tilde{\pi} \to U(g)$ with multiplicities n_i of the one dimensional components still given by (2), but such that the number of γ_i's equal to a fixed j is always divisible by p. By reordering the γ's, we may assume that $\gamma_s \le \gamma_t$ for $s < t$, and we can then consider

$$\delta = < g, p^2 | \gamma_1/p, \gamma_{p+1}/p, \ldots, \gamma_{(k-1)p+1}/p > \tag{3}$$

where $n = kp$. Note that

$$\sum_{i=0}^{k-1} \gamma_{ip+1}/p = \sum_{i=1}^{n} \beta_i/p^2 \in \mathbb{Z}.$$

Also, with $h-1=p(s-1)$ and $n=pk$, we get

$$2g-2=p(2h-2)+n(p-1)=p^2(2s-2)+kp(p-1) \tag{4}$$

so that δ is the fixed point data of an element of order p^2 in Γ_g by Lemma 2.2. Furthermore, $s>0$ since $h>0$, and $k\neq 1$, because $\sum_{i=0}^{k-1}\gamma_{ip+1}/p$ is an integer. Thus, if $\alpha=1$ equation (4) implies that g satisfies the (p)-condition, a contradiction, and we are done. If $\alpha\geq 2$, we repeat our construction in the following manner. Let $\pi(2)$ denote the subgroup of Γ_g generated by an element whose fixed point data is given by equation (3). By construction, the associated representation $\rho(2):\pi(2)\rightarrow U(g)$ on holomorphic differentials (with, perhaps, a different complex structure on S_g), is such that again $c_i(\rho(2))\equiv 0 \mod p$ for $0<i<p^\alpha$. Decomposing $\rho(2)$ as $\oplus_{i=0}^{p^2-1}n_i\omega^i$, with ω faithful one dimensional, yields equations of the form

$$n_j=h(2)-1+k(2)-\sum_{i=1}^{k(2)}<j\beta_i(2)/p>\equiv 0 \mod p\,, \qquad 1<j<p\,, \tag{5}$$

with $h(2)$ the genus of $S_g/\pi(2)$, $\beta_i(2)=\gamma_{(i-1)p+1}$, and $k(2)=k$ as before. Also (see [FK])), one has $n_j=n_{j+p}$ if $0<j<j+p<p^2$ and j prime to p, so that by Lemma 3.1 $n_i\equiv 0 \mod p$ for $0<i<p$. The Riemann-Hurwitz equation for the $\pi(2)$ action is $2g-2=p^2(2h(2)-2)+k(2)p(p-1)$ and, as $\alpha\geq 2$, $k(2)\equiv 0 \mod p$; in particular, $k(2)\neq 1$. Again, by considering $n_j-n_{p-j}=2\sum_{i=1}^{k(2)}<j\beta_i(2)/p> +k(2)\equiv 0 \mod p$, we see that

$$\sum_{i=1}^{k(2)}<j\beta_i(2)/p>\equiv 0 \mod p\,, \qquad 0<j<p\,,$$

and thus $h(2)\equiv 1 \mod p$ from equation (5). This permits us to find $k(2)/p=k(3)$ integers $\delta_1,\ldots,\delta_{k(3)}\,, 1<\delta_i<p$, so that

$$\sum_{i=1}^{k(3)}\delta_i/p=\sum_{i=1}^{k(2)}\beta_i(2)/p^2\in\mathbb{Z}$$

as well as

$$2g-2=p^3(2s(2)-2)+k(3)p^2(p-1) \tag{6}$$

As $h(2)\neq 0$ we have $s(2)>0$, and $k(3)\neq 1$ because $\sum_{i=1}^{k(3)}\delta_i/p\in\mathbb{Z}$. If $\alpha=2$, equation (6) shows that g must satisfy the (p)-condition, a contradiction. If $\alpha>2$ we continue our construction. If g does not satisfies the (p)-condition, we will eventually arrive at a contradiction, finishing the proof. But we also note that if g satisfies the (p)-condition, we end up with a cyclic subgroup $\pi(\alpha+1)\subset\Gamma_g$ of order $p^{\alpha+1}$, which is generated by an element with fixed point data

$$<g,p^{\alpha+1}|\epsilon_1/p,\ldots,\epsilon_w/p>$$

and associated Riemann-Hurwitz equation of the form

$$2g-2=p^{\alpha+1}(2s(\alpha)-2)+k(\alpha+1)p^\alpha(p-1)$$

with the property that on $p^\alpha\pi(\alpha+1)$, the subgroup of order p of $\pi(\alpha+1)$, the characteristic classes $d_i(\rho|p^\alpha\pi(\alpha+1))$ agree with those associated with the original group π; in particular, they vanish in the range $0<i<p^\alpha$.

As an application, we can now prove part (i) of Theorem 1.

Corollary 3.3. *Let p be an odd regular prime and assume $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$. If g does not satisfy the (p)-condition then $p(\Gamma_g) = 2(p-1)p^{\alpha-1}$.*

Proof. We know from Lemma 1.5 that $p(\Gamma_g)$ has the form $2(p-1)p^\beta$ for some $\beta \geq \alpha - 1$. By Proposition 3.2. we can find for every subgroup $\pi \subset \Gamma_g$ of order p a non-zero element $d_i \in H^{2i}(\pi; \mathbb{Z})$ for some $i > 0$ of the form mp^γ with m prime to p and $\gamma < \alpha$, which lies in the image of the restriction map $H^*(\Gamma_g; \mathbb{Z}) \to H^*(\pi; \mathbb{Z})$. Thus the largest power of p dividing $p(\Gamma_g)$ must be less than α and the result follows.

This proof of Proposition 3.2 reveals, as a by-product, the following.

Corollary 3.4. *Let p be an odd regular prime and $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$. If Γ_g contains a subgroup π order p with $d_i(\rho|\pi) = 0$ for $0 < i < p^\alpha$ and if g satisfies the (p)-condition, then Γ_g contains a cyclic subgroup of order $p^{\alpha+1}$ with associated action on S_g having stabilizers of order $\leq p$.*

The converse of that Corollary is also true, by a simple construction; it does not need any regularity condition on the prime involved.

Corollary 3.5. *Let p be an arbitrary odd prime and assume $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$. If g satisfies the (p)-condition then Γ_g contains a cyclic subgroup $\pi(\alpha+1)$ of order $p^{\alpha+1}$ generated by an element with fixed point data of the form*

$$< g, p^{\alpha+1} | \beta_1/p, \ldots, \beta_k/p > .$$

Moreover, the subgroup $\pi = p^\alpha \pi(\alpha + 1)$ of order p satisfies $d_i(\rho|\pi) = 0$ for $0 < i < p^\alpha$.

Proof. If g satisfies the (p)-condition, we have integers $h > 0$ and $k \geq 0$ with $k \neq 1$ satisfying $2g - 2 = p^{\alpha+1}(2h-2) + p^\alpha k(p-1)$. Therefore, by Lemma 2.2, S_g admits a diffeomorphism of order $p^{\alpha+1}$ with exactly k singular orbits, and fixed point data

$$< g, p^{\alpha+1} | \beta_1/p, \ldots, \beta_k/p >$$

where the β_i's satisfy $0 < \beta_i < p$ and are chosen in such a way that $\sum_i \beta_i/p$ is an integer; this is possible since $k \neq 1$. If $\pi(\alpha+1)$ denotes the corresponding subgroup in Γ_g then its action on holomorphic 1-forms will be given by a representation of the form

$$\oplus_{i=0}^{p^{\alpha+1}-1} n_i \omega^i ,$$

with ω one dimensional and faithful, such that $n_i = n_{i+p}$ for any i prime to p such that $0 < i < i+p < p^{\alpha+1}$; this follows easily from the general formula concerning the n_i's, as presented for instance in [FK], by noting that the only nontrivial stabilizer occurring for the action on S_g is of order p. We can now apply Lemma 3.1 to the classes $d_i(\rho|\pi(\alpha+1))$ and infer that $d_i(\rho|\pi) = 0$ for $0 < i < p^\alpha$.

This Corollary leads to the following lower bound for $p(\Gamma_g)$, which will be used in the proof of (ii) of Theorems 1 and 2, presented in Section 5.

Corollary 3.6. *Let p be an odd prime and suppose $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$. If g satisfies the (p)-condition then $p(\Gamma_g)$ is a multiple of $2(p-1)p^\alpha$.*

Proof. By Corollary 3.5 we can find a cyclic subgroup $\pi(\alpha+1)$ in Γ_g of order $p^{\alpha+1}$ given by an element x with fixed point data

$$\delta(x) = < g, p^{\alpha+1} | \beta_1/p, \ldots, \beta_k/p >$$

for some β_i with $0 < \beta_i < p$. From our discussion on fixed point data we see that $\delta(x^j) = \delta(x)$ if $j \equiv 1 \mod p$. But this implies that p^α divides $[N(x) : C(x)]$. Applying Lemma 1.4 we see that $p(\Gamma_g)$ is a multiple of p^α and, using Lemma 1.5, it follows that $p(\Gamma_g)$ is actually a multiple of $2(p-1)p^\alpha$.

Section 4 : The action on Teichmüller space

Let S_g be a closed oriented surface of genus $g > 1$. It is classical that the Teichmüller space T_g of S_g is homeomorphic to $\mathbb{R}^{6g-6}$, and T_g admits a complex structure such that Γ_g acts on T_g properly discontinuously by holomorphic automorphisms. For a fixed subgroup $\pi \subset \Gamma_g$ of order p, let $\{\pi_i\}_{i \in J}$ be the set of all order p subgroups which are conjugate to π in Γ_g. This is a countable set (in general infinite) so that we may assume $0 \in J \subset \mathbb{N}$ with $\pi_0 = \pi$. The fixed point sets $F_i = (T_g)^{\pi_i} \subset T_g$ are closed submanifolds homeomorphic to $\mathbb{R}^{6h-6+2n}$ where h denotes the genus of the surface S_g/π and n the number of fixed points of the π-action on S_g, see Proposition 2.1 of [GMX] (strictly speaking, it is not π which acts on S_g, but some lift of π to $\mathrm{Diffeo}^+(S_g)$). We may choose a triangulation of T_g, by triangulating the algebraic variety T_g/Γ_g, such that Γ_g acts simplicially. Thus each F_i is a subcomplex of T_g. We now choose a subset $I \subset J$ containing 0 such that for $i, j \in I$ with $i \neq j$ one has $F_i \neq F_j$. Put $X_i = T_g \setminus F_i$ and $X_\infty = \bigcap X_i = X_0 \cap X_{>0}$, where $X_{>0} = \bigcap_{i>0} X_i$. Note that $F = \bigcup F_i$ is closed in T_g, since it is a subcomplex, and X_∞ is therefore a (connected) open submanifold of T_g, on which Γ_g acts, with stabilizers not containing any subgroup conjugate to π. One checks easily using the Riemann-Hurwitz equation that the only case for which $F = T_g$ (and thus X_∞ an empty space) is the case of π being generated by the hyperelliptic involution, acting on a genus 2 surface; in our applications we are only interested in actions of groups of odd order and thus X_∞ will not be empty. We will keep the notation introduced here through the entire section.

Lemma 4.1. *Let $\pi \subset \Gamma_g$ be a subgoup of prime order p and $F = \bigcup F_i \subset T_g$ the subspace of points fixed by some conjugate of π. In case $g = 2$ assume that π is not generated by the hyperelliptic involution. Denote by h be the genus of S_g/π and n the number of fixed points of the π-action on S_g. Then the singular cohomology with compact supports of F satisfies*

$$H^{6h-6+2n}_{cpt}(F; \mathbb{Z}) \cong \oplus_{i \in I} \mathbb{Z},$$

and $H^k_{cpt}(F; \mathbb{Z}) = 0$ for $k > 6h - 6 + 2n$.

Proof. Consider the natural map $\theta : \coprod F_i \to F$. Since the action of Γ_g on T_g is proper, no $f \in F$ lies in infinitely many F_i's, and therefore the map θ is proper and induces a map in cohomology with compact supports. Let $\mathrm{Sing}(F) \subset F$ be the subcomplex of points which lie in more than one F_i. Since for $i \neq j$ in I the complex submanifold $F_i \cap F_j$ is empty or has at least (real) codimension 2 in F_i, Sing(F) is empty, or is a subcomplex of F of codimension at least 2, and it follows that θ is a H^*_{cpt}-isomorphism for $* \geq 6h - 6 + 2n = \dim(F)$. Since each F_i is homeomorphic to $\mathbb{R}^{6h-6+2n}$ the result follows.

Lemma 4.2. *Let $F \subset T_g$ be as in Lemma 4.1 and put $X_\infty = T_g \setminus F$. Then X_∞ is a connected manifold of dimension $6g - 6$ with singular cohomology satisfying*

$$H^{6(g-h)-2n-1}(X_\infty; \mathbb{Z}) \cong \prod_{i \in I} \mathbb{Z},$$

and $H^k(X_\infty; \mathbb{Z}) = 0$ for $0 < k < 6(g-h) - 2n - 1$. Furthermore, the natural map $\nu : X_\infty \to X_0 \times X_{>0}$ induces an isomorphism

$$H^k(X_0 \times X_{>0}; \mathbb{Z}) \to H^k(X_\infty; \mathbb{Z})$$

for $0 < k \leq 6(g-h) - 2n - 1$.

Proof. Since F is closed in T_g we get by Alexander Duality

$$H_k(X_\infty; \mathbb{Z}) \cong H_{cpt}^{(6g-6)-k}(T_g, F; \mathbb{Z})$$

and, since $T_g \cong \mathbb{R}^{6g-6}$ and using Lemma 4.1, $H_{cpt}^{6g-6-k}(T_g, F; \mathbb{Z}) = 0$ for $0 < k < 6(g-h) - 2n - 1$. Moreover, for $k = 6(g-h) - 2n - 1$ we have

$$H_{6(g-h)-2n-1}(X_\infty; \mathbb{Z}) \cong H_{cpt}^{6h-6+2n+1}(T_g, F; \mathbb{Z}) \cong H_{cpt}^{6h-6+2n}(F; \mathbb{Z}) \cong \oplus_{i \in I} \mathbb{Z}.$$

Noting that by the universal coefficient theorem

$$H^k(X_\infty; \mathbb{Z}) \cong \mathrm{Hom}(H_k(X_\infty; \mathbb{Z}))$$

for $0 \leq k \leq 6(g-h) - 2n - 1$, the result on the cohomology of X_∞ follows. For the map $\nu : X_\infty \to X_0 \times X_{>0}$ one observes that the same type of argument applied to X_0 and $X_{>0}$ shows that they are homologically $6(g-h) - 2n - 2$ connected too, and satisfy

$$H_{6(g-h)-2n-1}(X_0; \mathbb{Z}) \cong \mathbb{Z}, \text{and} \quad H_{6(g-h)-2n-1}(X_{>0}; \mathbb{Z}) \cong \oplus_{i>0} \mathbb{Z}.$$

Using the Künneth Formula and the universal coefficient theorem the isomorphism result follows readily.

Proposition 4.3. *Let $g > 1$ and p an odd prime. Let π be a subgroup of order p, with associated Riemann-Hurwitz formula $2g - 2 = p(2h - 2) + n(p - 1)$. Then there exists a cohomology element $e \in H^{6(g-h)-2n}(\Gamma_g; \mathbb{Z})$ whose restriction to $H^{6(g-h)-2n}(\pi; \mathbb{Z})$ is non-trivial.*

Proof. Since p is odd, $6(g-h) - 2n > 0$ (it is the codimension of F_0 in T_g) so that, in the notation used above, $X_\infty = T_g \setminus F$ is non-empty. We first study the Serre spectral sequences with $\mathbb{Z}$-coefficients, associated with the fibrations

$$\text{(A)} \qquad X_\infty \to E\Gamma_g \times_{\Gamma_g} X_\infty \to B\Gamma_g$$

and

(B) $$X_\infty \to E\pi \times_\pi X_\infty \to B\pi\,.$$

Let us put $\omega = 6(g-h) - 2n - 1$. Then, in the obvious notation, one has

$$E_2^{\omega,0}(A) \cong H^\omega(X_\infty;\mathbb{Z})^{\Gamma_g} =< a >\cong \mathbb{Z}\,,$$

since Γ_g acts on $H^\omega(X_\infty;\mathbb{Z}) \cong \prod_{i\in I}\mathbb{Z}$ by permuting the factors transitively (the action is induced by the action on the set I). Because $H^k(X_\infty;\mathbb{Z}) = 0$ for $0 < k < \omega$, one has

$$E_2^{\omega,0}(A) = E_\omega^{\omega,0}(A) \xrightarrow{d_\omega^A} E_\omega^{0,\omega+1}(A) = H^{\omega+1}(\Gamma_g;\mathbb{Z})\,.$$

We will show that $d_\omega^A(a) \in H^{\omega+1}(\Gamma_g;\mathbb{Z})$ restricts non-trivially to $H^{\omega+1}(\pi;\mathbb{Z})$. For this it suffices to show that the element a considered as an element in $E_\omega^{\omega,0}(B) = H^\omega(X_\infty;\mathbb{Z})^\pi$ satisfies $d_\omega^B(a) \neq 0$ in $H^{\omega+1}(\pi;\mathbb{Z})$. We will analyze $d_\omega^B(a)$ using the π-map $X_\infty \to X_0 \times X_{>0}$ considered in Lemma 4.2. and the spectral sequences associated with

(C) $$X_0 \times X_{>0} \to E\pi \times_\pi (X_0 \times X_{>0}) \to B\pi$$

(D) $$X_0 \to E\pi \times_\pi X_0 \to B\pi$$

and

(E) $$X_{>0} \to E\pi \times_\pi X_{>0} \to B\pi\,.$$

Since the π-action on X_0 is free, $E\pi \times_\pi X_0$ is homotopy equivalent to X_0/π, a finite dimensional complex, so that all of

$$E_2^{\omega,0}(D) = H^\omega(X_0;\mathbb{Z})^\pi = H^\omega(X_0;\mathbb{Z})$$

is mapped isomorphically by d_ω^D onto $E_\omega^{0,\omega+1}(D) \cong H^{\omega+1}(\pi;\mathbb{Z})$; otherwise, as $H^*(X_0;\mathbb{Z}) \cong H^*(S^\omega;\mathbb{Z})$, one would get a contradiction to the finite dimensionality of X_0/π. The fibration (E) has a section, because the π-action on $X_{>0}$ has a fixed point; this follows from the fact that $F_0 \cap (\cup_{i>0}F_i)$ is either empty or a subcomplex of F_0 codimension ≤ 2, and F_0 is non-empty. Consequently, all elements in $E_2^{0,\omega+1}(E) = E_\omega^{0,\omega+1}(E) = H^{\omega+1}(\pi;\mathbb{Z})$ are permanent d^E-cycles. But this implies that $d_\omega^E : E_\omega^{\omega,0}(E) \to E_\omega^{0,\omega+1}(E)$ is the zero map. The π-map $\nu : X_\infty \to X_0 \times X_{>0}$ induces a map of spectral sequences $E_*^{*,*}(C) \Rightarrow E_*^{*,*}(B)$. As $\nu^* : H^*(X_0 \times X_{>0};\mathbb{Z}) \to H^*(X_\infty;\mathbb{Z})$ is an isomorphism for $0 < * \leq \omega$, and also $H^\omega(X_0 \times X_{>0};\mathbb{Z}) \cong H^\omega(X_0;\mathbb{Z}) \times H^\omega(X_{>0};\mathbb{Z})$, we see that for $x = (x_0, x_{>0}) \in H^\omega(X_0 \times X_{>0};\mathbb{Z})^\pi$ one has

$$d_\omega^C(x) = d_\omega^B(\nu^*(x)) = d_\omega^D(x_0) \in H^{\omega+1}(\pi;\mathbb{Z})\,.$$

Thus, if we decompose the generator

$$a \in H^\omega(X_\infty;\mathbb{Z})^{\Gamma_g} \subset H^\omega(X_0;\mathbb{Z}) \times H^\omega(X_{>0};\mathbb{Z})^\pi$$

as $a = (a_0, a_{>0})$, we have

$$\mathrm{res}_\pi^{\Gamma_g}(d_\omega^A(a)) = d_\omega^D(a_0) \in H^{\omega+1}(\pi;\mathbb{Z}),$$

and we need only show that $a_0 \in H^\omega(X_0;\mathbb{Z})$ is non-zero, to ensure that $d_\omega^D(a_0) \neq 0$. For this we view a as a Γ_g invariant function on $H_\omega(X_\infty;\mathbb{Z}) = H_\omega(X_0;\mathbb{Z}) \oplus H_\omega(X_{>0};\mathbb{Z})$ But every Γ_g-invariant function on $H_\omega(X_\infty;\mathbb{Z})$, which is constant on $H_\omega(X_0;\mathbb{Z}) \cong \mathbb{Z}$, must be trivial, because $H_\omega(X_\infty;\mathbb{Z})$ is isomorphic to $\oplus_{i\in I}\mathbb{Z}$, with Γ_g acting by permuting transitively the summands of $\oplus_{i\in I}\mathbb{Z}$. It follows that $a_0 \neq 0$ and we are done.

Corollary 4.4. *Let p be an odd prime and $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$. If π denotes a subgroup of order p of Γ_g such that the Riemann-Hurwitz equation of π has the form*

$$2g - 2 = p(2h-2) + n(p-1)$$

with $h - 1 = p^\alpha(s-1)$ and $n = (kp+i)p^\alpha$ where $0 < i < p$, then $2l$ has necessarily the form $mp - i$, and the restriction map

$$H^{[(3m+k)p-3(m+k)-2i]p^\alpha}(\Gamma_g;\mathbb{Z}) \to H^{[(3m+k)p-3(m+k)-2i]p^\alpha}(\pi;\mathbb{Z})$$

is non-trivial.

Proof. Since $2g - 2 = 2lp^\alpha$, the Riemann-Hurwitz equation shows that $2l \equiv -i \mod p$ so that we can write $2l$ in the form $mp - i$ for a unique $m > 0$. Thus $2g - 2 = (mp - i)p^\alpha$ and $2h - 2 = [m - k(p-1) - i]p^\alpha$ so that

$$6(g-h) - 2n = [(3m+k)p - 3(m+k) - 2i]p^\alpha .$$

Our claim then follows from Proposition 4.3.

Section 5 : The sharp upper bounds for Γ_g

We have already established that if $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$, then, $p(\Gamma_g) = 2(p-1)p^\beta$ for some $\beta \geq \alpha - 1$, see Lemma 1.5. To show that necessarily $\beta \leq \alpha$, we need only verify that for every subgroup $\pi \subset \Gamma_g$ there exists a number $j(\pi)$ prime to p such that the restriction map

$$H^{2j(\pi)p^\alpha}(\Gamma_g;\mathbb{Z}) \to H^{2j(\pi)p^\alpha}(\pi;\mathbb{Z}) \tag{7}$$

is non-trivial. This will be established in the next theorem, which proves (i) of Theorem 2 of the introduction.

Theorem 5.1. *Let p be an odd prime and $g = lp^\alpha + 1$ with l prime to p and $\alpha > 0$. Then the Yagita invariant Γ_g equals $2(p-1)p^\alpha$ or $2(p-1)p^{\alpha-1}$.*

Proof. As explained above, we need to study restriction maps of the type (7). Let π be a subgroup of Γ_g of order p and consider the associated Riemann-Hurwitz equation

$$2g - 2 = p(2h-2) + n(p-1),$$

where $n \geq 0$ denotes the number of fixed points of the π action on S_g. Write $\theta : \Gamma_g \to \mathrm{GL}_{2g}(\mathbb{C})$ for the representation given by the action of Γ_g on $H_1(S_g;\mathbb{C})$. Note that θ factors through $\mathrm{Gl}_{2g}(\mathbb{Q})$ so that $\theta|\pi = a\tau + b\sigma$, with τ the trivial one-dimensional representation and σ the reduced regular one of π. Thus

$$\dim_{\mathbb{C}} H_1(S_g;\mathbb{C}) = 2g = a + (p-1)b = 2lp^\alpha + 2$$

and, for a generator ϕ of the π-action on $H_1(S_g;\mathbb{C})$,

$$\mathrm{trace}(\phi : H_1(S_g;\mathbb{C}) \to H_1(S_g;\mathbb{C})) = a - b = 2 - n\,.$$

Thus $pb = 2g - a + b = 2g - 2 + n = 2lp^\alpha + n$ so that the following possibilities arise.

(a) $n \not\equiv 0 \mod p^\alpha$. Then $b = b_0 p^\gamma$ with $\gamma < \alpha - 1$ and b_0 prime to p. But then the Chern class $c_{(p-1)p^\gamma}(\theta|\pi) = b_0 c_{p-1}(\sigma)^{p^\gamma}$ is non-zero, providing a $j(\pi)$ for which the restriction map (7) is non-zero.

(b) $n = (kp+i)p^\alpha$ with $0 \leq i < p$. Since then $pb = 2lp^\alpha + n = (2l+kp+i)p^\alpha$, we see that in case $2l + i \not\equiv 0 \mod p$, b is not zero $\mod p^\alpha$, so that the same argument as before shows that $c_{(p-1)p^{\alpha-1}}(\theta)$ has a non-trivial restriction under the map (7). It remains to consider the case where $2l + i = mp$. This yields $pb = (m+k)p^{\alpha+1}$ and we find again two sub-cases. Firstly, if $m+k$ is prime to p, then we conclude again that the restriction map (7) is non-zero, with $j(\pi) = p-1$. Secondly, if $m + k \equiv 0 \mod p$, we observe that in the notation above $2h = a = 2g - (p-1)b$, which implies that $2h - 2$ is divisible by p^α. Also, we cannot have $i = 0$ in that case, because otherwise $2g - 2$ were divisible by $p^{\alpha+1}$. Thus $0 < i < p$ and we are precisely in the situation of Corollary 4.4, which shows that the restriction map (7) is non-trivial if one chooses

$$2j(\pi) = [(3m+k)p - 3(m+k) - 2i]\,,$$

and $j(\pi) \not\equiv 0 \mod p$ since we assume that $m + k$ is divisible by p.

This completes the proof of the theorem.

As a corollary, we obtain part (ii) of Theorem 2, by combining Theorem 5.1 with Corollary 3.6. Of course, this also implies (ii) of Theorem 1, and therefore we have completed all proofs of the theorems stated in the introduction.

References

[B] S.A. Broughton, *The equisymmetric stratification of the moduli space and the Krull dimension of mapping class groups*, Topology and its Applications **37** (1990), 101–113.

[CO] L.Carlitz and F.R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc. **6** (1955), 265–269.

[EM] B. Eckmann and G. Mislin, *Chern classes of group representations over a number field*, Math. Ann. **271** (1985), 349–358.

[FK] H. Farkas and I. Kra, *Riemann Surfaces*, Graduate Texts in Math., vol. 71, Springer Verlag, 1982.

[GMX] H.H. Glover, G. Mislin and Y. Xia, *On the Farrell Cohomology of Mapping Class Groups*, Invent. Math. **109** (1992), 535–545.

[N] J. Nielsen, *Die Struktur periodischer Transformationen von Flächen*, Danske Vid. Selsk. Mat.-Fys. Medd. **15** (1937), 1–77.

[Sw] R. Swan, private communication.

[Sy] P. Symonds, *The cohomology representation of an action of C_p on a surface*, Trans. Amer. Math. Soc. **306** (1988), 389–400.

[T] C.B. Thomas, *Free actions by p-groups on products of spheres and Yagita's invariants $po(G)$*, Lecture Notes in Math. **1375** (1989), 326–338.

[X1] Y. Xia, *Farrell-Tate cohomology of the mapping class group*, Ph.D. Thesis, Ohio State University (1990).

[X2] Y. Xia, *The p-period of an infinite group*, Publications Matemàtiques **36** (1992), 241–250.

[X3] Y. Xia, *The p-periodicity of the mapping class group and the estimate of its p-period*, Proc. Amer. Math. Soc **116** (1992), 1161–1169.

[Y] N. Yagita, *On the dimension of spheres whose product admits a free action by a non-abelian group*, Quart. J. Math. Oxford **36** (1985), 117–127.

H.H. Glover, Ohio State University, Columbus, Ohio
E-mail address: glover@math.ohio-state.edu

G. Mislin, ETH Zürich, Switzerland; and Ohio State University, Columbus, Ohio
E-mail address: mislin@math.ethz.ch and mislin@math.ohio-state.edu

Y. Xia, Northwestern University, Evanston, Illinois
E-mail address: xia@math.nwu.edu