ON CONJUGACY CLASSES IN THE TEICHMÜLLER MODULAR GROUP

Jane Gilman

Let S be a compact Riemann surface of genus g with n punctures, and let M(g, n) be the Teichmüller modular group of S. Let $\lambda(p, g, n)$ denote the number of conjugacy classes of elements of prime order p in M(g, n). The purpose of this paper is to obtain an explicit formula for $\lambda(p, g, n)$ when $g \geq 2$. (W. J. Harvey has considered this problem [1]. He obtained a generating function for $\lambda(p, g, 0)$ in [1], but he has recently pointed out that his function actually gives the number of conjugacy classes of subgroups of M(g, 0) of order p and not $\lambda(p, g, 0)$.)

Let $|M^x_{T,p}|$ be the number of distinct (p - 1)-tuples of nonnegative integers $(n_1, \cdots, n_{p-1})$ with

$$\sum_{i=1}^{p-1} n_i = T \quad \text{and} \quad \sum_{i=1}^{p-1} i n_i \equiv x \pmod{p},$$

where T is a fixed integer. In Section 1 we obtain a set of invariants for each conjugacy class; these invariants make it clear that to compute $\lambda(p, g, n)$ we need to know $|M^x_{T,p}|$. In Section 2 we compute $|M^x_{T,p}|$, and in Section 3 we compute $\lambda(p, g, n)$.

1. INVARIANTS FOR A CONJUGACY CLASS

Let S and S' be compact surfaces of genus g with n punctures, so that $S = \bar{S} - Q$ and $S' = \bar{S}' - Q'$, where Q and Q' are sets of n points on the compact surfaces $\bar{S}$ and $\bar{S}'$. Let h and h' be homeomorphisms of S and S', respectively, whose pth powers are homotopic to the identity.

Definition. The pairs (S, h) and (S', h') are *topologically equivalent* if there is a homeomorphism f of S onto S' with $fhf^{-1} \simeq h'$, where $\simeq$ denotes homotopy (see [3]). This is clearly an equivalence relation.

LEMMA 1. (i) *The number of conjugacy classes of elements of order* p *in* M(g, n) *is equal to the number of topological equivalence classes of pairs* (S, h), *where* S *is of genus* g *with* n *punctures and* $h^p \simeq$ identity.

(ii) *For each pair* (S, h) *there is an equivalent pair* (S', h') *in which* h' *is conformal.*

Proof. Fix a surface S. Given any pair (S', h'), let f be a homeomorphism of S' onto S. Then (S', h') is topologically equivalent to $(S, fh'f^{-1})$. Thus, to count topological equivalence classes we need only consider pairs where the surface is fixed. But (S, h) is equivalent to (S, h') if and only if h and h' are conjugate in M(g, n).

Received December 4, 1974.

Michigan Math. J. 23 (1976).

The second statement (ii) is an immediate consequence of the fact that every element of finite order in $M(g, n)$ has a fixed point in the Teichmüller Space of S.

To count the number of conjugacy classes, we therefore need only look at topological equivalence classes in which the homeomorphism is conformal. We want to describe a set of invariants for these classes:

Let h be a conformal automorphism of S of prime order p. With S, $\bar{S}$, and Q as before, we see that h extends in a natural way to $\bar{S}$. We call the extension h, also, and we let tr h be the trace of the action of h on the first homology group of $\bar{S}$. Let $T = 2 - \text{tr } h$. C.-H. Sah has shown [4] that h has precisely T fixed points on $\bar{S}$. Let $Q = \{q_1, \cdots, q_n\}$; let $P = \{p_1, \cdots, p_T\}$ be the fixed points of h; let $P \cap Q = \{p_1, \cdots, p_{n_0}\}$; let $Q - (P \cap Q) = \{q_1, \cdots, q_{n-n_0}\}$; and finally, let $S_0 = (\bar{S} - (P \cup Q))/\langle h \rangle$ be of genus g_0. The homeomorphism h permutes in orbits of length p the points of Q that it does not fix. Thus p divides $n - n_0$. Let $s_0 = (n - n_0)/p$.

Let F_0 be the fundamental group of S_0, and let F be the defining subgroup of the covering $\pi: \bar{S} - (P \cup Q) \to S_0$. The group F_0 has the presentation

$$(*) \quad \begin{gathered} \langle x_1, \cdots, x_{s_0+n_0}, y_1, \cdots, y_{T-n_0}, a_1, \cdots, a_{g_0}, b_1, \cdots, b_{g_0}: \\ x_1 \cdots x_{s_0+n_0} y_1 \cdots y_{T-n_0} \prod_{i=1}^{g_0} [a_i, b_i] = 1 \rangle . \end{gathered}$$

We let $X = \{x_1, \cdots, x_{s_0+n_0}\}$ and $Y = \{y_1, \cdots, y_{T-n_0}\}$. Since F is a normal subgroup of F_0, F is the kernel of a homomorphism ϕ of F_0 onto Z_p, the integers modulo p. The homomorphism must satisfy

(1) $\phi(x_i) = 0$ for $i = 1, \cdots, s_0$,

(2) $\phi(x_i) \neq 0$ for each i greater than s_0,

(3) $\phi(y_i) \neq 0$ for each i.

Let $\ker \phi$ be the kernel of ϕ.

Our aim is to identify h with a unique homomorphism of F_0 onto Z_p. Clearly, h determines F.

LEMMA 2. *Let* ϕ *and* ψ *be homomorphisms of* F_0 *onto* Z_p. *Then* $\ker \phi = \ker \psi$ *if and only if there is an integer* r *with* $0 < r < p$ *and* $\phi = r\psi$.

Proof. Clearly, $\ker \phi = \ker r\psi$ for each nonzero integer r. Conversely, assume $\ker \psi = \ker \phi$. Let $k = \psi(x)$ for some fixed x in F with $\phi(x) = 1$. For every y in F_0, $\phi(yx^{-\phi(y)}) = 0$. Thus $\psi(yx^{-\phi(y)}) = 0$. Therefore $\psi(y) = \phi(y)\psi(x)$ or $\psi(y) = k\phi(y)$.

We can identify a given homomorphism ϕ of F_0 onto Z_p with a unique homeomorphism h_ϕ and surface S_ϕ as follows:

Let $\tilde{S}$ be the covering of S_0 with defining subgroup $F = \ker \phi$, where ϕ satisfies (1), (2), and (3) above. Recall that $\tilde{S}$ is the set of equivalence classes of pairs (p, α), where p is a point on S_0 and α is a curve on S_0 from a fixed base point q_0 to p. The pair (p, α) is equivalent to the pair (q, β) if $p = q$ and $\alpha\beta^{-1}$ is in F.

Let $[(p, \alpha)]$ denote the equivalence class of (p, α). The homomorphism ϕ induces a homeomorphism $\tilde{h}_\phi$ of $\tilde{S}$ defined by $\tilde{h}_\phi[(p, \alpha)] = [(p, \alpha + x)]$, where x is any element of F_0 for which $\phi(x) = 1$. The group of cover transformations is generated by $\tilde{h}_\phi$ and is isomorphic to Z_p.

Since ϕ satisfies (1), (2), and (3), there exist a compact surface $\bar{S}$ and sets Q and P of (respectively) n and T points on $\bar{S}$ such that $P \cap Q$ contains n_0 points and $\tilde{S} = \bar{S} - (P \cup Q)$. The homeomorphism $\tilde{h}_\phi$ of $\tilde{S}$ is actually conformal, and it extends to a conformal homeomorphism $\bar{h}_\phi$ of $\bar{S}$ with $\bar{h}_\phi(Q) = Q$. By construction, $\bar{h}_\phi$ has T fixed points. We denote the restriction of $\bar{h}_\phi$ to $\bar{S} - Q$ by h_ϕ, and we let $S_\phi = \bar{S} - Q$.

LEMMA 3. *Let* (S, h) *be a pair consisting of a compact surface* S *of genus* g *with* n *punctures and a conformal homeomorphism* h *of* S *of order* p. *Then there is a unique homomorphism* ϕ *of* F_0 *onto* Z_p *such that* $h = h_\phi$ *and* $S = S_\phi$.

Proof. Using the same notation as before, we have a covering

$$\pi: \bar{S} - (P \cup Q) \to S_0.$$

We let F be the defining subgroup of this covering, and we assume that $F = \ker \phi$, where ϕ is a homomorphism of F_0 onto Z_p. By Lemma 2, $F = \ker r\phi$ for all integers r between 0 and p, but F is not the kernel of any other homeomorphism. $\bar{S} - (P \cup Q) = \tilde{S}$ and $S = S_\phi = S_{r\phi}$ for all relevant integers r. The $(p - 1)$ covering transformations $h_\phi, h_{2\phi}, \cdots, h_{(p-1)\phi}$ are all distinct. Exactly one of them, h_ϕ say, must be the restriction of h to $\bar{S} - (P \cup Q)$, since this restriction is a covering transformation and there are only $(p - 1)$ covering transformations that are not the identity. Since h and h_ϕ agree on $\tilde{S}$, they must also agree on $S_\phi = S$.

Remark. Let r and t be integers between 0 and p. Assume $rt \equiv 1 \pmod p$. Then $h_{r\phi} = (h_\phi)^t$.

In what follows, ϕ will always be a homomorphism of F_0 onto Z_p, and F_0 will have presentation (*).

Notation. Denoting by $|E|$ the cardinality of the set E, we associate with ϕ the two sets of integers

$$N(\phi) = (n_1, \cdots, n_{p-1}), \qquad \text{where } n_i = |\phi^{-1}(i) \cap X|,$$

$$S(\phi) = (s_0, \cdots, s_{p-1}), \qquad \text{where } s_i = |\phi^{-1}(i) \cap Y|.$$

Remark. Since ϕ must preserve the defining relation of F_0, we see that

$$\sum_{i=1}^{p-1} i(s_i + n_i) \equiv 0 \pmod p. \tag{4}$$

Notation. Let (S, h) be any pair satisfying the hypotheses of Lemma 3. We associate with h the two sets of integers

$$N(h) = N(\phi) \quad \text{and} \quad S(h) = S(\phi),$$

where ϕ is the homomorphism of Lemma 3 with $h = h_\phi$.

Remark. $N(h)$ and $S(h)$ depend upon ϕ. If

$$N(h) = (n_1, \cdots, n_{p-1}) \quad \text{and} \quad N(h^r) = (n_1', \cdots, n_{p-1}'),$$

then $n_x' = n_i$, where $x \equiv ri \pmod p$. The similar statement holds for $S(h)$ and $S(h^r)$.

Next we fix one pair (S, h) with T and s_0 also fixed. There are a finite number of homomorphisms ϕ of F_0 onto Z_p with $|\phi^{-1}(0) \cap X| = s_0$. This is true because from each finitely generated group there are only a finite number of homomorphisms to a finite group. Let $\phi_1, \cdots, \phi_r$ be a complete list of all such homomorphisms, and let $\{(S_i, h_i)\}$ $(i = 1, \cdots, r)$ be the corresponding surfaces and conformal automorphisms. (Here $h_i = h_{\phi_i}$ and $S_i = S_{\phi_i}$). Taking a subset, and renumbering if necessary, we may assume that all of these pairs are distinct and none are topologically equivalent. Note: If ϕ_i appears in the list, so does $r\phi_i$, for each r $(0 < r \leq p - 1)$. Let $F_i = \ker \phi_i$.

For each pair (S', h'), the symbols $\overline{S}'$, P', and Q' have the obvious meaning.

LEMMA 4. *Let* S' *be a compact surface of genus* g *with* n *punctures. Let* h' *be a conformal automorphism of* S' *of order* p. *Assume* $2 - \operatorname{tr} h' = T$ *and* $|P' \cap Q'| = n_0$. *Then* (S', h') *is topologically equivalent to* (S_i, h_i) *for some* i.

Proof. We let F' be the defining subgroup of the covering

$$\pi': (\overline{S}' - (P' \cup Q'))/\langle h' \rangle \to S_0'.$$

Let τ be any homeomorphism of $\overline{S}'/\langle h' \rangle$ onto $\overline{S}/\langle h \rangle$. We may assume that $\tau(\pi'(P')) = \pi(P)$ and that $\tau(\pi'(Q')) = \pi(Q)$. Thus τ maps S_0' onto S_0 and induces an isomorphism τ_* of F_0' onto F_0. Assume $h' = h_\psi$. Then $\psi \circ \tau_*^{-1}$ is a homomorphism of F_0 onto Z_p, with

$$|(\psi \circ \tau_*^{-1})^{-1}(0) \cap X| = s_0 = \frac{n - n_0}{p}.$$

Thus $\psi \circ \tau_*^{-1} = \phi_i$ for some i. We can easily see that τ must lift to a homeomorphism $\tilde{\tau}$ of $\overline{S}' - (Q' \cup P')$ onto $S_i = \overline{S}_i - (P_i \cup Q_i)$, with $\tilde{\tau} h' \tilde{\tau}^{-1} \simeq h_i$. The relations $\tau(\pi'(Q')) = \pi(Q)$ and $\tau(\pi'(P')) = \pi(P)$ imply that $\tilde{\tau}$ extends to a map of S' onto S_i, with $\tilde{\tau} h' \tilde{\tau}^{-1} \simeq h_i$.

COROLLARY 1. *The number of conjugacy classes of elements* h *in* $M(g, n)$ *of order* p *with* $\operatorname{tr} h$ *and* s_0 *fixed is equal to the number of distinct pairs* (S_i, h_i) *that are not topologically equivalent.*

LEMMA 5. (i) *If* $T > 0$, *then* (S_i, h_i) *is topologically equivalent to* (S_ϕ, h_ϕ), *where* ϕ *is a homomorphism of* F_0 *onto* Z_p *that sends all hyperbolic generators to* 0.

(ii) *If* $T = 0$, *all coverings of* S_0 *are topologically equivalent.*

Proof. Let ϕ and ψ be homomorphisms of F_0 onto Z_p. If σ is an automorphism of F_0 with $\phi = \psi \circ \sigma$, then (S_ϕ, h_ϕ) is topologically equivalent to (S_ψ, h_ψ). This follows from basic covering theory, which shows that the homeomorphism of S_0 that induces σ will lift to a homeomorphism of S_ϕ onto S_ψ conjugating h_ϕ into h_ψ.

The proof of Theorem 14 of [1] shows that corresponding to each homomorphism ϕ of F_0 onto Z_p there is an automorphism σ of F_0 with the property that $\phi \circ \sigma$ and ϕ agree on the nonhyperbolic generators and $\phi \circ \sigma$ sends all hyperbolic generators to 0 except b_1. If $T \neq 0$, using the notation of Theorem 14 of [1], we replace σ by $\sigma \circ \mathscr{A}_4^t$, where t is the integer satisfying $t\phi(y_{T-n_0}) \equiv -\phi(b_1) \pmod{p}$.

If $T = 0$, let $\phi \circ \sigma(b_1) = r$. Let x satisfy $rx + 1 \equiv 0 \pmod{p}$. Let $\psi(b_1) = 1$, and let ψ agree with $\phi \circ \sigma$ on all other generators of F_0. Let τ_x, σ_r, and δ be automorphisms of F_0 that fix all generators except a_1 and b_1. Let $\tau_x(a_1) = a_1$ and $\tau_x(b_1) = b_1 a_1^x$. Let $\sigma_r(a_1) = a_1 b_1^r$ and $\sigma_r(b_1) = b_1$. Let $\delta(a_1) = a_1 b_1 a_1^{-1}$ and $\delta(b_1) = a_1^{-1}$. Then $\psi \circ \delta \circ \sigma_r \circ \tau_x = \phi \circ \sigma$.

THEOREM 1. *The conjugacy class of an element* h *in* M(g, n) *of prime order* p *is completely determined by* S(h) *and* N(h).

Proof. Let $\{(S_i, h_i)\}$ $(i = 1, \cdots, r)$ be as in the paragraphs preceding Lemma 4. It suffices to show that (S_i, h_i) is topologically equivalent to (S_j, h_j) if and only if $N(h_i) = N(h_j)$, $S(h_i) = S(h_j)$, and $\operatorname{tr} h_i = \operatorname{tr} h_j$. But by construction, all of these coverings have $\operatorname{tr} h_i = 2 - T$, and two conformal maps can only be conjugate if they have the same number of fixed points.

By Lemma 5, if $T \neq 0$, we may assume ϕ_i $(i = 1, \cdots, r)$ sends all hyperbolic generators to 0. If $T = 0$, the theorem is just Lemma 5 (ii).

Assume (S_i, h_i) and (S_j, h_j) are topologically equivalent, and let $\tau\colon S_i \to S_j$, with $\tau h_i \tau^{-1} \simeq h_j$. Since h_i and h_j are conformal, we may assume, replacing τ by the minimal quasiconformal map in its homotopy class, that $\tau h_i \tau^{-1} = h_j$, so that τ induces an homeomorphism $\tilde{\tau}$ of S_0 and thus induces an automorphism τ_* of F_0 with $\tau_*(F_i) = F_j$. If $\psi = \phi_j \circ \tau_*$, one can verify that $F_i = \ker \psi$. By Lemma 2, $\phi_j \circ \tau_* = k\phi_i$ for some integer k. We want to show $k = 1$. Let x and y be elements of F_0 with $\phi_i(x) = 1$ and $\phi_j(y) = 1$. We compute

$$\tau h_i[(p, \alpha)] = \tau[(p, \alpha + x)] = [(\tilde{\tau}(p), \tau_*(\alpha) + \tau_*(x))],$$

$$h_j \tau[(p, \alpha)] = h_j[(\tilde{\tau}(p), \tau_*(\alpha))] = [(\tilde{\tau}(p), \tau_*(\alpha) + y)],$$

where p is any point on S_0 and α any curve from q_0, the base point, to p. Since $h_j \tau[(p, \alpha)] = \tau h_i[(p, \alpha)]$, $\tau_*(x) - y$ is in the kernel of ϕ_j. Since $\phi_j(y) = 1$, $\phi_j \circ \tau_*(x) = 1$. But $\phi_j \circ \tau_*(x) = k\phi_i(x) = 1$. Thus $k = 1$ and $\phi_j \circ \tau_* = \phi_i$. Since $\tau(Q_i) = Q_j$, we see that $\tau(P_i) = P_j$. Thus τ_* maps the curves in X onto conjugates of curves in X and does the same to curves in Y. Since Z_p is an abelian group, it follows that

$$|\phi_j^{-1}(t) \cap X| = |(\phi_j \circ \tau_*)^{-1}(t) \cap X| \quad \text{for } t = 0, \cdots, p-1,$$

$$|\phi_j^{-1}(t) \cap Y| = |(\phi_j \circ \tau_*)^{-1}(t) \cap Y| \quad \text{for } t = 1, \cdots, p-1.$$

Thus $N(h_i) = N(h_j)$ and $S(h_i) = S(h_j)$.

Conversely, assume ϕ_j and ϕ_i are two mappings such that

$$|\phi_i^{-1}(t) \cap X| = |\phi_j^{-1}(t) \cap X| \quad \text{for } t = 0, \cdots, p-1$$

and $|\phi_i^{-1}(t) \cap Y| = |\phi_j^{-1}(t) \cap Y|$ for $t = 1, \cdots, p-1$. Corresponding to each permutation σ of the set $\{1, \cdots, s_0 + n_0\}$, there is an automorphism of F_0 that maps x_i onto a conjugate of $x_{\sigma(i)}$ and fixes the elements of Y and the hyperbolic generators. This is clear when we look at the automorphisms of F_0 generated by the permutations

$\{\sigma_{i,i+1}\}$ $(i = 1, \cdots, s_0 + n_0 - 1)$, where $\sigma_{i,i+1}(x_i) = x_i x_{i+1} x_i^{-1}$, $\sigma_{i,i+1}(x_{i+1}) = x_i$, and $\sigma_{i,i+1}(a) = a$ for all other generators a of F_0.

Similarly, every permutation of the elements of Y can be obtained, up to conjugation, by an automorphism of F_0. Since these are type-preserving automorphisms, they are induced by homeomorphisms of S_0 [2]. Since they do not interchange elements of the subgroups generated by X and Y, they extend to homeomorphisms of $\overline{S}/\langle h \rangle$ and fix $\pi(Q)$ and $\pi(P - Q)$.

For each integer t with $0 \leq t \leq p - 1$ and for each k with $\phi_i(x_k) = t$, we can find a k' with $\phi_j(x_{k'}) = t$, and thus we can define a permutation σ of $\{1, \cdots, n_0 + s_0\}$ such that $\phi_i(x_k) = \phi_j(x_{\sigma(k)})$ for $k = 1, \cdots, n_0 + s_0$. Similarly, we can find a permutation ν of $\{1, \cdots, T - n_0\}$ such that $\phi_i(y_m) = \phi_j(y_{\nu(m)})$. We let τ_* be the automorphism of F_0 that maps x_k onto a conjugate of $x_{\sigma(k)}$ for $k = 1, \cdots, n_0 + s_0$ and y_m onto a conjugate of $y_{\nu(m)}$ for $m = 1, \cdots, T - n_0$. Let τ denote the homeomorphism of S_0 inducing τ_*. Then τ gives the desired homeomorphism $\tilde{\tau}$ of S_i onto S_j, with $\tilde{\tau} h_i \tilde{\tau}^{-1} \simeq h_j$.

Remark. J. Nielsen [3, p. 53] has found a set of invariants that describe a topological equivalence class. They are, of course, equivalent to ours. We can see this by applying the Reidemeister-Schreier rewriting process to the subgroup F of F_0. This involves calculations almost as long as the proof of Theorem 1. In this case we prefer our set of invariants, because by giving condition (4) they make it clear how to count $\lambda(p, g, n)$.

2. THE COMBINATORIAL PROBLEM

Notation. Let $M_{T,p}$ be the set of all $(p - 1)$-tuples of nonnegative integers $(n_1, \cdots, n_{p-1})$ for which $\sum_{i=1}^{p-1} n_i = T$. Let $M_{T,p}^x$ be the set of all elements of $M_{T,p}$ for which $\sum_{i=1}^{p-1} in_i \equiv x \pmod p$ whenever $x = 0, \cdots, p - 1$.

Let $N_{T,p}$ be the set of all p-tuples of nonnegative integers $(n_0, \cdots, n_{p-1})$ with $\sum_{i=0}^{p-1} n_i = T$. Let $N_{T,p}^x$ be the set of all elements of $N_{T,p}$ for which $\sum_{i=0}^{p-1} in_i \equiv x \pmod p$ whenever $x = 0, \cdots, p - 1$.

It is clear that to compute $\lambda(p, g, n)$ we need to be able to compute $|M_{T,p}^x|$ for all T and x.

THEOREM 2. *Let* p *be a prime number, and let* T *and* x *be integers. Then*

$$|M_{T,p}^x| = \begin{cases} 0 & \text{if } x \neq 0 \text{ and } T = 0 \text{ or if } T < 0, \\ 1 & \text{if } x = 0 \text{ and } T = 0, \\ \dfrac{p-1}{pT}\dbinom{p+T-2}{T-1} + H(p, T, x) & \text{otherwise;} \end{cases}$$

here

$$H(p, T, x) = \begin{cases} 0 & \textit{if } T \not\equiv 0 \pmod p \textit{ and } T \not\equiv 1 \pmod p, \\ -\frac{1}{p} & \textit{if } T \equiv 0 \pmod p \textit{ and } x \not\equiv 0 \pmod p, \\ -\frac{1}{p}+1 & \textit{if } T \equiv 0 \pmod p \textit{ and } x \equiv 0 \pmod p, \\ \frac{1}{p} & \textit{if } T \equiv 1 \pmod p \textit{ and } x \not\equiv 0 \pmod p, \\ \frac{1}{p}-1 & \textit{if } T \equiv 1 \pmod p \textit{ and } x \equiv 0 \pmod p. \end{cases}$$

Proof. We want to compute $|M^x_{T,p}|$ for arbitrary x. We can identify $N^x_{T,p}$ with $\bigcup_{y=0}^{T} M^x_{T-y,p}$ by identifying $(n_0, \cdots, n_{p-1})$ in $N^x_{T,p}$ with $(n_1, \cdots, n_{p-1})$ in $M^x_{T-n_0,p}$. We identify $N^x_{T-1,p}$ with

$$\bigcup_{z=0}^{T-1} M^x_{T-1-z,p} = \bigcup_{y=1}^{T} M^x_{T-y,p}.$$

Thus $|M^x_{T,p}| = |N^x_{T,p}| - |N^x_{T-1,p}|$. Therefore, to compute $|M^x_{T,p}|$, we need to compute $|N^x_{T,p}|$ for all x and T.

We shall show that

$$|N^x_{T,p}| = \begin{cases} \frac{1}{p}\binom{p+T-1}{T} & \text{if } T \not\equiv 0 \pmod p, \\ \frac{1}{p}\binom{p+T-1}{T} - \frac{1}{p} & \text{if } T \equiv 0 \pmod p \text{ and } x \not\equiv 0 \pmod p, \\ \frac{1}{p}\binom{p+T-1}{T} - \frac{1}{p} + 1 & \text{if } T \equiv 0 \pmod p \text{ and } x \equiv 0 \pmod p. \end{cases}$$

The theorem follows from this.

Assume first that $T \not\equiv 0 \pmod p$. We shall show that $|N^x_{T,p}| = |N^y_{T,p}|$ for all x and y. For any integers a and b, we let $f_{a,b}$ be the mapping of Z_p to Z_p given by sending i into the remainder when $ai + b$ is divided by p. Assume that $a \not\equiv 0 \pmod p$, so that a^{-1} makes sense. Let F map $N_{T,p}$ to itself according to the formula

$$F(n_0, \cdots, n_{p-1}) = (n_{f(0)}, \cdots, n_{f(p-1)}).$$

It is easy to verify that F maps $N_{T,p}$ to itself and that F in fact maps $N^x_{T,p}$ to $N^{a^{-1}(x-bT)}_{T,p}$

If $T \not\equiv 0 \pmod p$, then for each x we can find a and b such that $a^{-1}(x - bT) \equiv 0 \pmod p$. Therefore F is a one-to-one map of $N^x_{T,p}$ onto $N^0_{T,p}$. Thus $|N^x_{T,p}| = |N^0_{T,p}|$ for all p, T, and x if $T \not\equiv 0 \pmod p$.

Clearly, $|N_{T,p}| = \binom{p+T-1}{T}$, since the latter is the number of ways one can choose T objects from p objects, allowing repetitions. Thus

$$|N^x_{T,p}| = \frac{1}{p}\binom{p+T-1}{T}$$

when $T \not\equiv 0 \pmod p$.

Assume next that $T \equiv 0 \pmod p$. If $x \not\equiv 0 \pmod p$, then we can find integers a and b such that $a^{-1}(x - bT) \equiv a^{-1}x \equiv 1 \pmod p$. Thus $|N^x_{T,p}| = |N^y_{T,p}|$ if $x \neq 0$ and $y \neq 0$. We want to compute $|N^0_{T,p}|$. If $T = 0$, clearly $|N^0_{T,p}| = 1$.

If $T > 0$, let S^x_i be the set of all p-tuples $(n_0, \cdots, n_{p-1})$ in $N^x_{T,p}$ with $n_i \neq 0$. Then $N^x_{T,p} = S^x_0 \cup \cdots \cup S^x_{p-1}$, but this is not a disjoint union. Note that $|S^x_i| = |N^{x-i}_{T-1,p}|$ and $|S^x_{i_1} \cap \cdots \cap S^x_{i_r}| = |N^{x-(i_1+\cdots+i_r)}_{T-r,p}|$ if the i_k are distinct. Thus

$$|N^x_{T,p}| = \sum_{j=1}^{p} \sum (-1)^{(j+1)} |S^x_{i_1} \cap \cdots \cap S^x_{i_j}|$$

$$= \sum_{j=1}^{p-1} \sum (-1)^{(j+1)} \cdot |N^{x-(i_1+\cdots+i_j)}_{T-j,p}| + |S^x_0 \cap \cdots \cap S^x_{p-1}|,$$

where the inner sums extend over all j-tuples $(i_1, \cdots, i_j)$ with

$$0 \le i_1 < \cdots < i_j \le p-1.$$

If $j \neq p$, then $T - j \not\equiv 0 \pmod p$. Thus in the sum on the right-hand side of the equation all terms except the last are independent of x. The last term is equal to $|N^{x-p}_{T-p,p}|$. Thus we can write $|N^x_{T,p}| = y + |N^x_{0,p}|$, by repeated application of this procedure, and y is independent of x. Since $|N^0_{0,p}| = 1$ and $|N^x_{0,p}| = 0$ for $x \neq 0$, it follows that if $x \neq 0$, then $|N^x_{T,p}| = y$ and $|N^0_{T,p}| = y + 1$. Since

$$|N_{T,p}| = \binom{p+T-1}{T} = (p-1)y + y + 1,$$

we see that

$$|N^x_{T,p}| = \frac{1}{p}\binom{p+T-1}{T} - \frac{1}{p} \quad \text{and} \quad |N^0_{T,p}| = \frac{1}{p}\binom{p+T-1}{T} - \frac{1}{p} + 1.$$

3. THE FORMULA FOR $\lambda(p, g, n)$

Definition. Let $\mu(p, g, n, T)$ be the number of conjugacy classes of elements h in $M(g, n)$ of order p with $2 - \operatorname{tr} h = T$.

We shall first compute $\mu(p, g, n, T)$, and from it, $\lambda(p, g, n)$.

THEOREM 3. *Let* p, g, *and* n *be integers* (p *a prime and* $g \geq 2$). *If* $p \neq 2$, *let* k_0 *be an integer with* $0 \leq k_0 \leq p-1$ *and* $k_0 \equiv 2 - 2g \pmod p$, *and let*

$$r = \left[\frac{2g - (k_0 - 2)(p - 1)}{p(p - 1)} \right],$$

where [ ] *denotes the greatest-integer function. If* $p = 2$, *we let* $k_0 = 0$ *when* $g \equiv 1 \pmod 2$ *and* $k_0 = 2$ *when* $g \equiv 0 \pmod 2$. *Let* $\tilde{n}_0$ *be the remainder when* n *is divided by* p, *and let* b *be the minimum of* $[(T - \tilde{n}_0)/p]$ *and* $(n - \tilde{n}_0)/p$ *when it is positive, and zero otherwise.*

$$\mu(p, g, n, T) = \sum_{s=0}^{b} \sum_{x=0}^{p-1} |M^x_{\tilde{n}_0 + sp, p}| \cdot |M^{p-x}_{T-(\tilde{n}_0+sp),p}|$$

when $p \neq 2$, $T \equiv k_0 \pmod p$, *and* $0 \leq T \leq k_0 + rp$.

$$\mu(2, g, n, T) = b + 1$$

when $p = 2$, $\frac{T}{2} \equiv \frac{k_0}{2} \pmod 2$, *and* $0 \leq T \leq 2g + 2$.

In all other cases, $\mu(p, g, n, T) = 0$. *The value of* $|M^x_{Y,p}|$ *is given in Theorem* 2.

Proof. Assume first that $p \neq 2$. Let S, $\bar{S}$, Q, h, P and other notation be defined as in Section 1. Recall that g_0 is the genus of the factor surfaces S_0 and $\bar{S}/\langle h \rangle$, and that g is the genus of S. The Riemann-Hurwitz formula implies that $g = pg_0 + (p - 1)(T - 2)/2$.

If S has an automorphism h of order p, then g_0 must be an integer. Thus $g - (p - 1)(T - 2)/2$ is divisible by p, and this implies that $T \equiv 2 - 2g \pmod p$. An automorphism of order p on S can have $k_0 + tp$ fixed points, where

$$0 \leq t \leq \left[\frac{2g - (k_0 - 2)(p - 1)}{p(p - 1)} \right].$$

The latter inequality follows from the requirement that g_0 be nonnegative. Thus $\mu(p, g, n, T) = 0$ if $T \not\equiv 2 - 2g \pmod p$ or $T \geq k_0 + (r + 1)p$.

Since $n - n_0$ must be divisible by p, the possible values for n_0 are $\tilde{n}_0, \tilde{n}_0 + p, \cdots, \tilde{n}_0 + bp$, where b is the minimum of $[(T - \tilde{n}_0)/p]$ and $(n - \tilde{n}_0)/p$. This follows from the fact that $\tilde{n}_0 + bp \leq n$ and $\tilde{n}_0 + bp \leq T$. Thus if $T < \tilde{n}_0$, $\mu(p, g, n, T) = 0$.

Fix T and n_0, and suppose $n - n_0$ is divisible by p. Assume $T = k_0 + mp$, where $0 \leq m \leq r$ and $n_0 \leq T$ and $n_0 \leq n$ with $n_0 \equiv \tilde{n}_0 \pmod p$. We want to show that for these numbers and for each (p - 1)-tuple $(n_1, \cdots, n_{p-1})$ and each p-tuple $(s_0, \cdots, s_{p-1})$, where $s_0 = (n - n_0)/p$ and

$$\sum_{i=0}^{p-1} s_i = n, \quad \sum_{i=1}^{p-1} (n_i + s_i) = T, \quad \sum_{i=1}^{p-1} i(n_i + s_i) \equiv 0 \pmod p,$$

we can construct a surface S of genus g with n punctures, and a homeomorphism h with $2 - \mathrm{tr}\, h = T$, $N(h) = (n_1, \cdots, n_{p-1})$, and $S(h) = (s_0, \cdots, s_{p-1})$.

The Riemann-Hurwitz formula shows that $2g - 2 + T = p(2g_0 - 2 + T)$. Thus, if $g \geq 2$, then $2g_0 - 2 + T > 0$, so that $2g_0 - 2 + T + s_0 > 0$. This means that we can construct a Fuchsian group F_0 with the presentation (*) given in Section 1. Let ϕ be the homomorphism of F_0 onto Z_p, with

$$\phi(x_1) = \cdots = \phi(x_{s_0}) = 0,$$

$$\phi(x_{s_0+1}) = \cdots = \phi(x_{s_0+s_1}) = 1,$$

$$\cdots,$$

$$\phi(x_{s_0+n_0-s_{p-1}}) = \cdots = \phi(x_{s_0+n_0}) = p - 1,$$

$$\phi(y_1) = \cdots = \phi(y_{n_1}) = 1,$$

$$\cdots,$$

$$\phi(y_{T-n_0-n_{p-1}}) = \cdots = \phi(y_{T-n_0}) = p - 1.$$

In Section 1 we saw that corresponding to ϕ we obtain a surface S of genus g with n punctures and a homeomorphism h_ϕ of S with tr h_ϕ, $N(h_\phi)$, and $S(h_\phi)$ as desired.

Thus, given any $(s_0, \cdots, s_{p-1})$ and $(n_1, \cdots, n_{p-1})$ as above, for a fixed T and $n_0 = n - ps_0$, we can construct a covering. Because each set of $2p - 1$ integers determines a distinct conjugacy class, we need only count the ways we can choose these sets of integers where $s_0 = (n - n_0)/p$.

We can let $(n_1, \cdots, n_{p-1})$ be any $(p - 1)$-tuple with $\sum_{i=1}^{p-1} n_i = T - n_0$. Assume that $\sum_{i=1}^{p-1} in_i \equiv y \pmod p$. Then $(s_1, \cdots, s_{p-1})$ can be any $(p - 1)$-tuple, as long as $\sum_{i=1}^{p-1} s_i = n_0$ and $\sum_{i=1}^{p-1} is_i \equiv p - y \pmod p$. For each possible y there are therefore $|M^y_{n_0,p}| \cdot |M^{p-y}_{T-n_0,p}|$ possible choices for $(s_1, \cdots, s_{p-1})$ and $(n_1, \cdots, n_{p-1})$. Thus, for a fixed n_0, we get $\sum_{y=0}^{p-1} |M^y_{n_0,p}| \cdot |M^{p-y}_{T-n_0,p}|$ conjugacy classes. But n_0 can be $\tilde{n}_0 + tp$, where $0 \leq t \leq b$. This gives the formula for $\mu(p, g, n, T)$.

The proof for the case $p = 2$ is the same, except for the analysis of the possible values of T. In this case the Riemann-Hurwitz formula shows that T can be $k_0, k_0 + 4, \cdots, 2g + 2$, where $k_0 = 0$ if $g \equiv 1 \pmod 2$ and $k_0 = 2$ if $g \equiv 0 \pmod 2$.

COROLLARY 2. *Let* p, g, *and* n *be integers* (p *a prime and* $g \geq 2$). *If* $p \neq 2$, *let* k_0 *be an integer with* $0 \leq k_0 \leq p - 1$ *and* $k_0 \equiv 2 - 2g \pmod p$, *and let* $r = \left[\dfrac{2g - (k_0 - 2)(p - 1)}{p(p - 1)}\right]$, *where* [ ] *denotes the greatest-integer function. If* $p = 2$, *let* $k_0 = 0$ *when* $g \equiv 1 \pmod 2$ *and* $k_0 = 2$ *when* $g \equiv 0 \pmod 2$, *and let* $r = (2g + 2 - k_0)/4$. *Let* $\tilde{n}_0$ *be the remainder of* n *when divided by* p, *and let* b_y *be the minimum of* $[(k_0 + yp - \tilde{n}_0)/p]$ *and* $(n - \tilde{n}_0)/p$.

If $p \neq 2$, *then*

$$\lambda(p, g, n) = \sum_{y=0}^{r} \sum_{s=0}^{b_y} \sum_{x=0}^{p-1} |M^x_{\tilde{n}_0+sp,p}| \cdot |M^{p-x}_{k_0+yp-(\tilde{n}_0+sp),p}| .$$

The value of $|M^x_{T,p}|$ *is given in Theorem* 2.

If $p = 2$, *let* b_y *be the minimum of* $[(k_0 + 4y - \tilde{n}_0)/2]$ *and* $(n - \tilde{n}_0)/2$ *when both numbers are positive, and zero otherwise; then*

$$\lambda(2, g, n) = \sum_{y=0}^{r} (b_y + 1).$$

Proof. $\lambda(p, g, n) = \sum \mu(p, g, n, T)$, the sum being taken over all possible values of T.

REFERENCES

1. W. J. Harvey, *On branch loci in Teichmüller space.* Trans. Amer. Math. Soc. 153 (1971), 387-399.

2. C. Maclachlan and W. J. Harvey, *On mapping-class groups and Teichmüller spaces.* Proc. London Math. Soc. (3) 30 (1975), 496-512.

3. J. Nielsen, *Die Struktur periodischer Transformationen von Flächen.* Danske Vid. Selsk. Mat.-Fys. Medd. 15, No. 1 (1937), 1-77.

4. Chih-han Sah, *Groups related to compact Riemann surfaces.* Acta Math. 123 (1969), 13-42.

Rutgers University
Newark, New Jersey 07102