RESEARCH BLOG 3/10/03

In blog 2/27/03 Train Tracks on train tracks, I mentioned Lee Mosher had said that the number of conjugacy classes of elements in $\mathrm{SL}(2,\mathbb{Z})$ with the same trace is the class number of the field $\mathbb{Q}$ adjoin the eigenvalue with that trace. It turns out that the formula is a class number, but not just of the field. I'll describe this in some greater generality.

Suppose that we have a matrix $A \in \mathrm{SL}(n,\mathbb{Z})$, such that its characteristic polynomial $p_A(x)$ is irreducible. Let λ be an eigenvalue of A. Consider the field $\mathbb{Q}(\lambda)$, and let $\mathcal{O} \subset \mathbb{Q}(\lambda)$ be the ring of integers, then $\lambda \in \mathcal{O}$ is a unit, since $\det(A) = 1$. Then $\mathbb{Z}[\lambda] \subset \mathcal{O}$ is an *order*, that is a subring with 1 of $\mathcal{O}$ of rank n. If we take $\{1, \lambda, ..., \lambda^{n-1}\}$ as a basis for $\mathbb{Q}(\lambda)$, identifying it with $\mathbb{Q}^n$, then multiplication by λ acts as an element $R_\lambda \in \mathrm{SL}(n,\mathbb{Z}) \subset \mathrm{GL}(n,\mathbb{Q})$, and this is the usual rational canonical form for matrices in $\mathrm{GL}(n,\mathbb{Q})$ with eigenvalue λ and eigenvector $\Lambda = [1, \lambda, ..., \lambda^{n-1}]^T$ (therefore, it has eigenvalues $\lambda = \lambda_1, \lambda_2, ..., \lambda_n$, where $p_A(x) = \prod(x - \lambda_i)$). Then there exists $V \in \mathrm{GL}(n,\mathbb{Q})$ such that $R_\lambda = V^{-1}AV$, the well-known fact that any matrix is conjugate to rational canonical form. In this case, $\mathrm{span}_{\mathbb{Z}} V\Lambda$ forms a $\mathbb{Z}[\lambda]$ submodule of $\mathcal{O}$, such that the action in the basis formed by the rows of $V\Lambda$ is given by A, since $AV\Lambda = VR_\lambda\Lambda = \lambda V\Lambda$.

For any order $R \subset \mathcal{O}$, one may consider the R-ideal classes I_R, which consist of R-submodules of $\mathbb{Q}(\lambda)$ of $\mathbb{Z}$-rank n (that is, as additive subgroups of $\mathbb{Q}(\lambda)$, they are isomorphic to $\mathbb{Z}^n$), up to scalar multiplication in $\mathbb{Q}(\lambda)^\times$. That is, the subset $P_R = \{qR \mid q \in \mathbb{Q}(\lambda)^\times\}$ form the principle R-ideals. I_R is closed under multiplication with unit R, and P_R forms a subgroup, so we may form the quotient $I_R/P_R = C(R)$ to obtain a monoid, with unit R. The $\mathcal{O}$-ideal classes $C(\mathcal{O})$ clearly map injectively to $C(R)$. We also have a map $C(R) \to C(\mathcal{O})$, given by $I \to \mathcal{O}I$. This is clearly not injective if $R \neq \mathcal{O}$, since $\mathcal{O}R = \mathcal{O}^2 = \mathcal{O}$, but since $[\mathcal{O} : R] < \infty$, the map is clearly finite-to-one. Since $C(\mathcal{O})$ is finite, this implies $C(R)$ is finite, for all orders $R \subset \mathcal{O}$. Then $|C(R)|$ is the *R-class number.*

Theorem 0.1. *The number of conjugacy classes in* $\mathrm{SL}(n, \mathbb{Z})$ *with eigenvalue* λ *is* $|C(\mathbb{Z}[\lambda])|$.

If we let $I \subset R$ be the largest $\mathcal{O}$-ideal contained in R, then I is called the *conductor* of R. Jeremy Teitelbaum tells me that $|C(R)|$ may be computed from the knowledge of I, and the index of $\mathbb{Z}[\lambda]^\times \subset \mathcal{O}^\times$, the group of units.

To prove the theorem, we have seen how to associate a $\mathbb{Z}[\lambda]$-ideal class to $A \in \mathrm{SL}(n, \mathbb{Z})$, given by $\mathrm{span} V\Lambda$. It is easy to see that this map is onto, since given a $\mathbb{Z}[\lambda]$-ideal I, choosing a $\mathbb{Z}$-basis for I to identify it with $\mathbb{Z}^n$ (such that the basis has the same orientation as $\{1, \lambda, ..., \lambda^{n-1}\}$ as a basis for $\mathbb{Q}(\lambda)$), we see that multiplication of I by λ is an element of $\mathrm{SL}(n, \mathbb{Z})$ in this basis, and is only well defined up to conjugacy depending on our choice of (oriented) basis of I. I claim that this is the inverse of our previous map. If we have two $\mathbb{Z}[\lambda]$-ideal classes I and J, with associated matrices A and B, respectively, then suppose A and B are conjugate in $\mathrm{SL}(n, \mathbb{Z})$. Then there is $C \in \mathrm{SL}(n, \mathbb{Z})$, $CA = BC$. But we have $AV = VR_\lambda$, and there is $W \in \mathrm{GL}(n, \mathbb{Q})$ such that $BW = WR_\lambda$. Thus, $CVR_\lambda(CV)^{-1} = WR_\lambda W^{-1}$, so $W^{-1}CV$ commutes with R_λ, and therefore has the same eigenspaces as R_λ. Thus, $W^{-1}CV[1, \lambda_i, ..., \lambda_i^{n-1}]^T = \mu_i[1, \lambda_i, ..., \lambda_i^{n-1}]^T$. But $W^{-1}CV \in \mathrm{GL}(n, \mathbb{Q})$, so from the first coordinate, we see that $\mu_i = p(\lambda_i)$, for some $p(x) \in \mathbb{Q}[x]$ which is independent of i (the coefficients of $p(x)$ the first row of $W^{-1}CV$), in other words $W^{-1}CV = p(R_\lambda)$. Thus, we have the relation $J = p(\lambda)I$, so these $\mathbb{Z}[\lambda]$-ideals are in the same class.

(added 3/17/03 I think that this correspondence of conjugacy classes with class numbers should be well-known to people who study lattices, but I haven't done a literature search to find references. David Fisher points out that the arguments should generalize to lattices in arithmetic groups in general - thanks Dave).

Hopefully, at some later date I'll give some examples of this construction for $\mathrm{SL}(2, \mathbb{Z})$. Since there is an explicit algorithm for solving the conjugacy problem in $\mathrm{SL}(2, \mathbb{Z})$, it would be nice to see how the combinatorics of this solution relates to the algebraic solution given here.