(*December 8, 2005*)

Surjectivity of $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/p)$

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/˜garrett/

In the discussion of the action of $SL_2(\mathbb{Z}_p)$ or $GL_2(\mathbb{Z}_p)$ on the p-power projective limit of modular curves, one begins with the *surjectivity* of the natural map

$$SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/p)$$

It is important to understand the simplicity of this and related results.

Claim: Let R be a principal ideal domain. Let M be a maximal ideal. Then the natural map

$$SL_2(R) \longrightarrow SL_2(R/M) \quad \text{is surjective}$$

Proof: Let q be the quotient map $R \longrightarrow R/M$. First, given u, v not both 0 in R/M, we will find *relatively prime* c, d in $SL_2(R)$ such that $q(c) = u$ and $q(d) = v$.

Consider the case that $v \neq 0$ in R/M. Since $q : R \longrightarrow R/M$ is surjective, there is $0 \neq d \in R$ such that $q(d) = v$. Consider the conditions on $c \in R$

$$\begin{cases} c &= u \bmod M \\ \\ c &= 1 \bmod Rd \end{cases}$$

As $d \notin M$, by the maximality of M there are $x \in R$ and $m \in M$ such that $xd + m = 1$. Let $c = xdu + m$. From $xd + m = 1$ we have $xd = 1 \bmod m$ and $m = 1 \bmod d$, so this expression for c does satisfy the system of congruences. In particular, $q(c) = u$, and since $c = 1 \bmod d$ it must be that $\gcd(c, d) = 1$.

For $v = 0$ in R/M, necessarily $u \neq 0$, and we reverse the roles of c, d in the previous paragraph.

Thus, we have relatively prime c, d in R whose images mod M are u, v. In a PID, given s, t there are a, b such that $\gcd(s, t) = as - bt$. Here, the coprimality of c, d implies that there are a, b in R such that $ad - bc = 1$. That is, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(R)$, and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} * & * \\ u & v \end{bmatrix} \mod M$$

Thus, given $\begin{bmatrix} r & s \\ u & v \end{bmatrix}$ in $SL_2(R/M)$, we have

$$\begin{bmatrix} r & s \\ u & v \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} 1 & w \\ 0 & 1 \end{bmatrix} \mod M \quad (\text{where } w = sa - br \bmod M)$$

since the right-hand side is in $SL_2(R/M)$. Let $t \in R$ be such that $q(t) = w$. Then

$$\begin{bmatrix} r & s \\ u & v \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} 1 & -t \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod M$$

So

$$\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \mod M$$

This gives the surjectivity. ///
