

# Elliptic elements in congruence groups

David Leaman

August 10, 2009

## Abstract

During the course of my investigation, the question was raised: do principal congruence subgroups  $m\hat{\Gamma}$  of the modular group  ${}_1\hat{\Gamma}$  ever contain elliptic elements? If so, when? It turns out the answer is "only in the whole modular group."

**Theorem 1.** The group  $m\hat{\Gamma}$  contains elliptic elements if and only if  $m\hat{\Gamma} = {}_1\hat{\Gamma}$ .

*Proof.* In three parts.

1. It is easy to see that  ${}_1\hat{\Gamma}$  contains elliptic elements. For instance, the matrix  $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$  is elliptic, with fixed points  $\pm i$ .
2. Assume that  $m > 1$ . Let:

$$P = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \alpha m + 1 & \beta m \\ \gamma m & \delta m + 1 \end{bmatrix} \in m\hat{\Gamma} \quad ; \quad \alpha, \beta, \gamma, \delta \in \mathbb{Z}$$

The characteristic polynomial of  $P$  is  $cz^2 + (d - a)z - b$ . Thus, using the fact that  $ad - bc = 1$ , the discriminant is:

$$\begin{aligned} & (d - a)^2 + 4cb \\ &= (a + d)^2 - 4 \end{aligned}$$

To show that  $P$  is elliptic, we aim to establish that its fixed points are two distinct complex conjugate points, ie, that its discriminant is negative. For this to be true it is necessary and sufficient for the trace  $(a + d)$  of  $P$  to be between -2 and 2. Since all variables here are integers, we make use of the stronger statement:

$$(\alpha + \delta)m \in \{-3, -2, -1\}$$

This implies that  $m|1, m|2$  or  $m|3$ . The only possibilities are that  $m \in \{2, 3\}$  and  $\alpha + \delta = -1$ .

3. Now we suppose that  $m \in \{2, 3\}$ , and return to:

$$\begin{aligned} ad - bc &= 1 \\ (\alpha m + 1)((-\alpha - 1)m + 1) - \beta\gamma m^2 &= 1 \\ (-\alpha^2 - \alpha - \beta\gamma)m^2 - m &= 0 \\ (-\alpha^2 - \alpha - \beta\gamma)m &= 1 \end{aligned}$$

This implies that  $m|1$ , a contradiction.

Therefore, the only principal congruence subgroup that contains elliptic elements is the modular group itself. ■