No elements of order five in $\mathrm{SL}_2(\mathbb{Z})$

Jim Fowler

June 26, 2012

Here are various methods by which one can see there are no elements of order five in $\mathrm{SL}_2(\mathbb{Z})$.

Cayley–Hamilton theorem

If $A \in \mathrm{SL}_2(\mathbb{Z})$, then the characteristic polynomial for A is $\lambda^2 - (\operatorname{trace} A)\lambda + 1$ and the trace is an integer. By the Cayley–Hamilton theorem,

$$A^2 - n\,A + \mathrm{Id} = 0 \text{ where } n = \operatorname{trace} A.$$

And also $A^5 = \mathrm{Id}$. So

$$\begin{aligned} A^5 &= (A^2)^2 A \\ &= (nA - \mathrm{Id})^2\, A \\ &= n^2 A^3 - 2nA^2 + A \\ &= (n^4 - 3n^2 + 1)A + (2n - n^3)\,\mathrm{Id} = \mathrm{Id}\,. \end{aligned}$$

In order to ensure A is not a multiple of the identity, $n = \operatorname{trace} A \in \mathbb{Z}$ must satisfy

$$n^4 - 3n^2 + 1 = 0$$

but there are no integer solutions to that polynomial.

Finding a free kernel

The abelianization map $\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{Z}/12\mathbb{Z}$ has kernel a free group. So the orders of elements of $\mathrm{SL}_2(\mathbb{Z})$ divide 12.

Recognizing it is as an amalgamated product

The group $\mathrm{SL}_2(\mathbb{Z})$ is $\mathbb{Z}/6\mathbb{Z} \star_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/4\mathbb{Z}$. Serre's book *Trees* would help here.

Counting modulo powers of two

The special linear group over the field with two elements is

$$\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Note that there are six elements. By more careful counting, $|\,\mathrm{SL}_2(\mathbb{Z}/2^n\mathbb{Z})| = 3 \cdot 2^{3n-2}$, so there are no elements of order five in $\mathrm{SL}_2(\mathbb{Z}/2^n\mathbb{Z})$. If $M \in \mathrm{SL}_2(\mathbb{Z})$ had order five, then by choosing n so large that the image of M in $\mathrm{SL}_2(\mathbb{Z}/2^n\mathbb{Z})$ is nontrivial, we would have a contradiction.

Counting modulo primes

The group $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ has $(p-1)(p)(p+1)$ elements. There are infinitely many primes so that $p \not\equiv \pm 1 \pmod 5$. For any $M \in \mathrm{SL}_2(\mathbb{Z})$, one can choose p large enough so that $M \bmod p$ is nontrivial, and so that 5 does not divide $(p-1)(p)(p+1)$. Then M cannot have order five.