EXERCISE 1
NUMBER THEORY SEMINAR 2014/15
PROF. ZEÉV RUDNICK
DUE DATE: NOVEMBER 6, 2014

For a commutative ring R, Let

$$\mathrm{SL}(2,R) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in R,\ \det(A) := ad - bc = 1\}$$

be the special linear group of 2×2 matrices over R, and

$$\mathrm{O}(2,R) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : A^T A = I\}$$

be the orthogonal group of 2×2 matrices (where A^T is the transpose matrix and I is the identity matrix).

1. For p prime, compute the numbers $\#\mathrm{O}(2,\mathbb{Z}/p\mathbb{Z})$ and $\#\mathrm{SL}(2,\mathbb{Z}/p\mathbb{Z})$.

2. Show that the reduction map

$$\mathrm{O}(2,\mathbb{Z}) \to \mathrm{O}(2,\mathbb{Z}/N\mathbb{Z}), \quad A \mapsto A \mod N$$

is <u>not</u> surjective for $N \gg 1$.

3. Show that the reduction map

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z}), \quad A \mapsto A \mod N$$

is surjective for all $N > 1$.