---

37 #1485
Mennicke, J.
On Ihara's modular group.
Invent. Math. **4** 1967 202–228
20.75

Consider the ring $Z^{(p)}=\{x/p^t|t,x\in Z\}$ and the group $G=\mathrm{SL}(2,Z^{(p)})$, where Z is the ring of rational integers and p is a fixed prime number. The author proves the following theorems. Theorem 1: For each $m\not\equiv 0\ (\mathrm{mod}\,p)$, let $N_m=\{X\in G|X\equiv 1\ (\mathrm{mod}\,m)\}$ be the full congruence subgroup of G modulo m, and let Q_m be the normal closure of the element $\begin{pmatrix}1&0\\m&1\end{pmatrix}$. Then $N_m=Q_m$. As an immediate consequence of this, he obtains the corollary. The group G has the congruence subgroup property; i.e., every subgroup of G with finite index contains N_m for some m. He also proves Theorem 2: The normal subgroups of G of infinite indices are contained in the center $\{\pm 1\}$ of G.

As is well-known today, the congruence subgroup property had been established for various groups, e.g., for $\mathrm{SL}(n,Z)$ $(n\ge 3)$, $\mathrm{Sp}(2n,Z)$ $(n\ge 2)$, by the author; H. Bass, M. Lazard and J. P. Serre; H. Matsumoto; H. Bass, J. Milnor and J. P. Serre, etc. But as for $\mathrm{SL}(2)$ over arithmetic rings R, this is not true if $R=Z$ (well-known) or if R is the ring of integers of totally imaginary number fields (T. Kubota); and the above corollary is the first affirmative result for $\mathrm{SL}(2)$. (This was a conjecture made by the reviewer in connection with some problems on algebraic curves modulo p.) From the author's note: "After a preliminary version of this paper (which contained a proof of $N_m=Q_m$ for $p=2$) had been circulated, Serre found that one can obtain, by combining methods of C. Moore and R. Steinberg, and the author, strikingly general results on the congruence subgroup property for $\mathrm{SL}(2)$ over arithmetic rings R." J. P. Serre's result will appear in a forthcoming paper ("Le problème des groupes de congruence pour SL_2"). It covers the case $R=Z^{(p)}$ and hence the author's corollary; however, the author's theorem $N_m=Q_m$ is sharper than Serre's for $R=Z^{(p)}$.

The proof depends more on arithmetic properties of the ring $Z^{(p)}$ than on the linear algebraic structure of $\mathrm{SL}(2)$, and one can find considerable number theoretic elegance in the proofs. To prove Theorem 1, the author first proves that if $p^2-1|m|(p^2-1)^t$ for some t, then N_m/Q_m lies in the center of G/Q_m. The method is arithmetic (uses the Dirichlet theorem on the primes in arithmetical progressions). Then he deduces $N_m=Q_m$ for such m by making use of the triviality of the Schur multiplier of $G/N_m=\mathrm{SL}(2,Z/mZ)$ (a fact essentially known, but an independent proof is given in the text). Finally, he generalizes this relation to the case of the general modulus m. Theorem 2 is an easy consequence of Theorem 1 (not of its corollary).

Reviewed by *Y. Ihara*