# Ribet's use of the congruence subgroup property.

Kevin Buzzard

February 7, 2012

Last modified 05/03/2004.

Ribet makes use of something related to, but perhaps even a little stronger than, the congruence subgroup property of $\mathrm{SL}_2(\mathbf{Z}[1/p])$, in his original level-raising paper (the ICM paper). Ribet's argument for level-raising is basically that it's trivial once you know that the map $J_1(N)^2 \to J_1(N,p)$ is injective, and this is essentially a theorem of Ihara. Ribet leaves this part of the proof to the last section of his ICM paper. In this last section, Ribet gives a direct proof, following Ihara, to save the reader the task of finding Ihara's paper. It is "well-known" that somewhere in this proof Ribet uses something related to the congruence subgroup property for $\mathrm{SL}_2(\mathbf{Z}[1/p])$. But where?

I think that I have found where. Let $N$ be a positive integer prime to $p$ and let $\Gamma$ denote the subgroup of $\mathrm{SL}_2(\mathbf{Z}[1/p])$ consisting of matrices congruent to 1 mod $N$. Just a few lines from the end of the paper, Ribet makes the throw-away statement "Because $\Gamma$ is generated by its parabolic elements,...". Call this statment $(R)$. Let $(N)$ be the statement that $\Gamma$ is the normal closure of the matrix $\left(\begin{smallmatrix}1&N\\0&1\end{smallmatrix}\right)$. Let $(C)$ be the statement that $\mathrm{SL}_2(\mathbf{Z}[1/p])$ has the congruence subgroup property. My understanding is the following:

(i) $(R)$ implies $(N)$ implies $(C)$, and all these implications are easy.

(ii) $(C)$ is hard to prove.

Hence $(R)$ is hard to prove. I don't know if $(C)$ implies $(R)$. Diamond and Taylor say that Ribet uses the congruence subgroup property. Does he actually use epsilon more?

---

A digression: "if $(R)$ were true for $\mathrm{SL}_2(\mathbf{Z})$" (i.e., if every $\Gamma(N)$ in $\mathrm{SL}_2(\mathbf{Z})$ were generated by its parabolic elements) then $\mathrm{SL}_2(\mathbf{Z})$ would have the congruence subgroup property, by the same argument. It doesn't though, so $(R)$ should be false for $\mathrm{SL}_2(\mathbf{Z})$. And indeed it is—it's true for $N \leq 5$, but for any $n \geq 6$ one can show that $\Gamma(n)$ is not generated by its parabolic elements. Here's the argument for $n = 6$ but the general argument is the same: Let $c_1$, $c_2$,...,$c_12$ be the 12 cusps for $\Gamma(6)$ and choose $\gamma_i$ such that $\gamma_i c_i = \infty$. Then for any $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, if $\gamma^{-1}\infty = c$ a cusp, then choose $\delta \in \Gamma(6)$ such that $\delta c = c_i$ and then $\gamma_i\delta\gamma^{-1}$ fixes $\infty$ so it's $\pm\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)$ in $\mathrm{PSL}_2(\mathbf{Z})$. Hence $\left(\begin{smallmatrix}1&-n\\0&1\end{smallmatrix}\right)\gamma_i\delta = \gamma$ and hence $\left(\begin{smallmatrix}1&t\\0&1\end{smallmatrix}\right)\gamma_i$ are representatives for the cosets of $\Gamma(6)$ in $\mathrm{PSL}_2(\mathbf{Z})$. Now any parabolic element in $\Gamma(6)$ is conjugate to an upper triangular matrix in $\mathrm{PSL}_2(\mathbf{Z})$ and hence is $\Gamma(6)$-conjugate to an element of the form $\gamma_i^{-1}\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)\gamma_i$ for some $i$.

Hence in the abelianisation of $\Gamma(6)$, the image of the subgroup generated by the parabolic elements can be generated by 12 elements, namely $\gamma_i^{-1}\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\gamma_i$. But $\Gamma(6)$ has index 12 in $\Gamma(2)$ in $\mathrm{PSL}_2(\mathbf{Z})$ and is hence free of rank 13, so its abelianisation can't be generated by 12 elements. In fact this shows that the subgroup generated by the parabolic elements has infinite index.

---

Here is the justification of (i).

**Lemma 1.** $(R)$ *implies* $(N)$.

*Proof.* The smallest normal subgroup of $\mathrm{SL}_2(\mathbf{Z}[1/p])$ containing $\left(\begin{smallmatrix}1&N\\0&1\end{smallmatrix}\right)$ clearly lives in $\Gamma(N)$, and can also be described as the group generated by all the $\mathrm{SL}_2(\mathbf{Z}[1/p])$-conjugates of $\left(\begin{smallmatrix}1&aN\\0&1\end{smallmatrix}\right)$, $a \in \mathbf{Z}$. If we assume $(R)$, then to prove $(N)$ it suffices to prove that any parabolic $\gamma \in \Gamma(N)$ is $\mathrm{SL}_2(\mathbf{Z}[1/p])$-conjugate to an upper triangular matrix. But $\gamma$ is parabolic, so let $c$ denote the cusp that it fixes; choose $\delta \in \mathrm{SL}_2(\mathbf{Z})$ sending $c$ to $\infty$; then conjugating $\gamma$ by $\delta$ gives an element of $\Gamma(N)$ fixing $\infty$ which is what we needed. If $N > 2$ then we are done, because then we can't have $-1$s on the diagonal. If $N = 2$ or $N = 1$ then we've done the case $N = 4$ and now it's easy. $\square$

**Lemma 2.** $(N)$ *implies* $(C)$.

*Proof.* (this is in Mennicke's article) If $\Gamma$ is a finite index subgroup of $\mathrm{SL}_2(\mathbf{Z}[1/p])$ then, intersecting $\Gamma$ with its conjugates, WLOG $\Gamma$ is normal. Now say $m$ is the smallest positive integer such that $\left(\begin{smallmatrix}1&m\\0&1\end{smallmatrix}\right) \in \Gamma$ (such $m$ exist, e.g. the index of $\Gamma$ in $\mathrm{SL}_2(\mathbf{Z}[1/p])$ will clearly do). If $p \mid m$ then $\left(\begin{smallmatrix}1&pm\\0&1\end{smallmatrix}\right) \in \Gamma$ and by normality of $\Gamma$, and conjugating by $\left(\begin{smallmatrix}p&0\\0&p^{-1}\end{smallmatrix}\right)$, we see that $\left(\begin{smallmatrix}1&m/p\\0&1\end{smallmatrix}\right) \in \Gamma$, contradiction. So $m$ is prime to $p$ and $\Gamma$ contains $\left(\begin{smallmatrix}1&m\\0&1\end{smallmatrix}\right)$ and hence it contains $\Gamma(m)$, which is what we had to prove. $\square$