Genera of Congruence Subgroups of $\mathrm{SL}_2(\mathbb{Z})$

Cooper Young

October 23rd, 2021

Abstract

Given an arbitrary finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, one can easily compute its genus. The reverse question is less straightforward; given an arbitrary genus, what can we say about the non-congruence and congruence subgroups that have that genus? In this paper, we investigate the possible genera (or possibly, the lack of genera) that congruence subgroups can attain.

Preliminaries and motivation

In this paper, we are interested in finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$, the special linear group consisting of 2-by-2 integer matrices with determinant 1. Recall that the principal congruence subgroup of level N is defined as

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

and a finite index subgroup $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup of level N if there exists some integer $N \geq 1$ such that $\Gamma(N) \leq \Gamma$. Otherwise, we call Γ a non-congruence subgroup.

Subgroups of $\mathrm{SL}_2(\mathbb{Z})$ act on the upper half plane $\mathfrak{H}$ by the linear fractional transformation $\gamma\tau \mapsto \frac{a\tau+b}{c\tau+d}$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Furthermore, we can extend this to the cusps to get an action on the extended upper-half plane $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \infty$. Let $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ be a finite index subgroup, then we define a fundamental domain D_Γ for Γ to be a hyperbolic polygon in $\mathfrak{H}^*$ such that for every $\tau \in \mathfrak{H}^*$, the interior of D_Γ contains exactly one point from the Γ-orbit of τ. We can then give $\Gamma\backslash\mathfrak{H}$ a complex structure to obtain a noncompact Riemann surface which we will denote as $Y(\Gamma)$. We can compactify this space by adding finitely many points corresponding to the cusps of Γ. This space, defined by $\Gamma\backslash\mathfrak{H}^*$, is denoted as $X(\Gamma)$ and when Γ is a congruence subgroup, we call it a modular curve. For any finite index subgroup $\Gamma < \mathrm{SL}_2(\mathbb{Z})$, we define the genus of Γ to be the genus of the space $X(\Gamma)$, and we denote it as $g(\Gamma)$.

Rademacher sparked interest in the math community when he conjectured that there are only finitely many genus 0 congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. This inspired work by Knopp and Newman [5], McQuillen [8], and Dennin [2], each of whom made progress on Rademacher's conjecture and its natural generalization to arbitrary genus. Finally, Thompson proved that there are only finitely many congruence subgroups of $\mathrm{PSL}_2(\mathbb{R})$ for any fixed genus g [10].

Thompson's result should come as a fairly surprising fact. Here's one reason why; the existence of non-congruence subgroups is itself a surprising phenomenon that occurs in SL_2, and Thompson's theorem proves that there are *a lot* more non-congruence subgroups than there are congruence subgroups. Let me elaborate on this a bit more. For $n \geq 3$, any finite index subgroup of $\mathrm{SL}_n(\mathbb{Z})$ must be a congruence subgroup, where the principal congruence subgroups of SL_n are defined in the same way as in SL_2, reducing each entry modulo N. We say that SL_n for $n \geq 3$ has the" congruence subgroup property," while SL_2 does not (this points to a larger, very open question as to which arithmetic groups have the congruence subgroup property). However, using techniques from Kulkarni's paper [6], one can explicitly construct infinitely many finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ with any arbitrary genus. This implies that for any fixed genus g, there are finitely many congruence subgroups with that genus but infinitely many non-congruence subgroups!

This leads me to my main question:

Question 1: Do congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ attain every genus?

The response to most mathematical questions is typically, why should we care? Well for one thing, if congruence subgroups miss a set of integers with positive density (or even if it misses any non-empty set), that's another example of how much SL_2 fails the congruence subgroup property.

If you aren't totally satisfied with that motivation, here's a little more; take any non-singular algebraic curve defined by coefficients that are algebraic numbers, we know this represents a compact Riemann surface, and Belyi's theorem (1979) proves that we can identify this surface as $\Gamma\backslash\mathfrak{H}^*$ where Γ is a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$. First off, Belyi's theorem is awesome and quite general (the only conditions imposed on our algebraic curve is that it's non-singular and the coefficients it's defined by are algebraic numbers!), and the fact that $\mathrm{SL}_2(\mathbb{Z})$ fails the congruence subgroup property means that not all of these algebraic curves are modular curves. In fact, if Question 1 is answered negatively, then there are some genera where none of the algebraic curves (that satisfy the conditions above) with that genus are modular curves.

So, hopefully your interest is a bit piqued, and we can get into some approaches.

Counting Genera

For a while, I was trying to prove that the answer to Question 1 is 'yes!' because otherwise the consequence in regards to Belyi's theorem would be pretty surprising to me. However, after unsuccessfully trying to explicitly construct congruence subgroups of arbitrary genus, I gave up for a while. A year and a half later, my interest in the problem reignited and I figured, why not try to prove the answer to Question 1 is 'no!'

There are known formulas for computing the genus of various congruence subgroups, such as for $\Gamma(N)$, $\Gamma_0(N)$, and $\Gamma_1(N)$. The genus increase with N at different rates for these classes of subgroups, and it increases the slowest for $\Gamma_0(N)$. One might wonder if subgroups of the form $\Gamma_0(N)$ attain every genus, but it can be checked using Sage that this is not true; the first few genera that are never attained by elements of $\Gamma_0(N)$ are $150, 180, 210, 286, 304, 312, 336$. In fact, it was proved in [1] that the set $\{g(\Gamma_0(N))\}_{N\in\mathbb{Z}}$ is a density zero subset of the integers. So maybe 'no' to question 1 isn't unfounded—and it would be very interesting if congruence subgroups as a whole only attained a density zero subset.

To begin, let's start with a proposition.

Proposition 1: Given finite index subgroups $\Gamma(N) < \Gamma_1, \Gamma_2 < \mathrm{SL}_2(\mathbb{Z})$
i) If $\Gamma_1 < \Gamma_2$, then $g(\Gamma_1) > g(\Gamma_2)$

ii) If Γ_1 and Γ_2 are conjugate (in $\mathrm{SL}_2(\mathbb{Z})$), then $g(\Gamma_1) = g(\Gamma_2)$.

<u>Proof:</u> i) Given $\Gamma_1 < \Gamma_2$, there is a natural projection of the corresponding modular curves $f : X(\Gamma_1) \to X(\Gamma_2)$, which is a nonconstant holomorphic map. It can be shown that the degree of this map is

$$\deg(f) = \begin{cases} [\Gamma_2 : \Gamma_1]/2 & \text{if } -I \in \Gamma_2 \text{ and } -I \notin \Gamma_1 \\ [\Gamma_2 : \Gamma_1] & \text{otherwise} \end{cases}$$

see [3] for more details. From the Riemann-Hurwitz theorem, we get

$$2g(\Gamma_1) - 2 = \deg(f)\big(2g(\Gamma_2) - 2\big) + \sum_{x \in X(\Gamma_1)} (e_x - 1)$$

where e_x is the ramification index at x. Since $\deg(f) > 1$ and $\sum_{x \in X(\Gamma_1)} (e_x - 1) \geq 0$, we get our result.

ii) Let

$$T = \pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \qquad S = \pm\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \qquad R = TS = \pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$$

McQuillan proved [9] that we can express the genus of Γ_1 in terms of N, and the number of distinct cyclic subgroups of Γ_1 generated by conjugates (in $\mathrm{SL}_2(\mathbb{Z})$) of T, R, and S^d (where d ranges through the divisors of N). The formula is a bit long, so I won't write it out here, but notice that the values it is a function of don't change when to we pass to a conjugate subgroup Γ_2 of the same level, so we get $g(\Gamma_1) = g(\Gamma_2)$.

□

As a consequence of this, we can show that Question 1 reduces to a problem of group theory and counting.

Corollary 1: $\big($# of distinct genera attained by congruence subgroups of level $N\,\big) \leq$ $\big($# of conjugacy classes of subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\,\big)$

<u>Proof:</u> From the third isomorphism theorem, we know that that congruence subgroups Γ of level N are in one-to-one correspondence with subgroups $G < \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, where $\Gamma/\Gamma(N) \cong G$. It is a brief exercise in group theory to show that two level N congruence subgroups Γ_1 and Γ_2 are conjugate if and only if their corresponding subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ are conjugate. Now using Proposition 1, we can conclude our claim.

□

At this point, we can turn our attention to counting the conjugacy classes of subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Each conjugacy class is in correspondence with a genus that congruence subgroups attain. But just counting them isn't enough—as we range through N, there are enough conjugacy classes of subgroups to account for every integer. We need to use extra information provided by the Riemann-Hurwitz theorem to see how the genera of level N congruence subgroups are spread out.

Since we can split up $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_i \mathrm{SL}_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z})$ using the Chinese Remainder theorem (where $N = p_1^{n_1} p_2^{n_2} \dots$ is the prime factorization), it makes sense to start with these building blocks. This leads to a simpler question

Question 2: Do congruence subgroups of prime level attain every genus?

The benefit of looking at Question 2 is that we know the subgroup structure of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. Indeed, Dickson's book [7] classifies the subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ (King wrote a summary of this result [4], though his classification is just sightly different from the book). Note that subgroups of $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ are in correspondence with congruence subgroups of level N which contain $-I$, and just as Thompson did, we may want to consider these types of subgroups.

Here is some of the useful information we can get out of this:

Proposition 2: i) In $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$, there are $\leq 2p$ conjugacy classes of subgroups.

ii) Depending on the prime $p > 2$, every maximal subgroup of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is conjugate to a group among the following list:

- Upper triangular matrices ($\Gamma_0(p)/\Gamma(N)$)
- A dihedral group of order $p-1$ or $p+1$
- S_4, A_4, or A_5

iii) For $p > 11$, the smallest genus attained by a congruence subgroup of level p is $g\big(\Gamma_0(p)\big)$.

Proof: i) and ii) follow directly from parsing through the summary in Dickson's book (page 285). For iii), we employ the genus equation

$$g(\Gamma) = \frac{\mu}{12} - \frac{e_2}{4} - \frac{e_3}{3} - \frac{t}{2} + 1$$

where $\mu = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$, t is the number of cusps for Γ, and e_i is the number of order-i elliptic points. Using the structure theorem in Dickson's book, we get that $\Gamma_0(p)$ is the subgroup with lowest order. It's also known that for $\Gamma_0(p)$ has $e_2, e_3 \in \{0, 1, 2\}$ and $t = 2$, so using the equation above, we see that we can't find a smaller genus.

$\square$

Now we have the following set up; as we range through p, the conjugacy classes of subgroups of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ give us $\leq 2p$ genera, the smallest of which is $g(\Gamma_0(p))$. By itself, the set $\{g(\Gamma_0(p))\}_p$ forms a density zero subset of the integers (recall [1]), and if $\Gamma_1 < \Gamma_2$ then

$$g(\Gamma_1) \geq [\Gamma_2 : \Gamma_1]\big(g(\Gamma_2) - 1\big) + 1$$

(from the proof of Proposition 1). The next step is: from this, what can we say about $S := \{g \mid g = g(\Gamma) \text{ where } \Gamma \text{ is a level } p\text{-congruence subgroup}\}$?

References

[1] Csirik, Janos, et al. *On the Genera of* $X_0(N)$. Preprint, 2000.

[2] Dennin Jr., Joseph B. *The genus of subfields of* $K(n)$. Proc. Amer. Math. Soc. 51 (1975), 282288.

[3] Diamond, Fred and Jerry Shurman. *A First Course in Modular Forms*. Springer, New York, 2005.

[4] King, Oliver. *The subgroup structure of finite classical groups in terms of geometric configurations*. Expository paper, 2015.

[5] Knopp, Marvin, and Morris Newman. *Congruence Subgroups of Positive Genus in the Modular Group*. Illinois Journal of Math 9, 577-583, (1965).

[6] Kulkarni, Ravi S. *An Arithmetic-Geometric Method in the Study of the Subgroups of the Modular Group*. American Journal of Mathematics, Vol. 113, No. 6. (Dec., 1991), pp. 1053-1133.

[7] L.E. Dickson, Linear groups, with an Exposition of the Galois Field Theory, Teubner, Leipzig, 1901.

[8] McQuillan, Donald. *Some results on the linear fractional group*. Illinois Journal of Mathematics, Volume 10, Issue 1, 1966.

[9] McQuillan, Donald. *On the genus of fields of elliptic modular functions*. Illinois Journal of Mathematics Volume 10, Issue 3, 1966.

[10] Thompson, John. *A Finiteness Theorem for Subgroups of* $\mathrm{PSL}_2(\mathbb{R})$ *Which are Commensurable with* $\mathrm{PSL}_2(\mathbb{Z})$. Proceedings of Symposia in Pure Mathematics, 37, pp. 533-555, 1980.