ON THE GENERA OF MODULAR CURVES

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Bachelor of Arts

in

Mathematics

by

Calvin George

Advisor

John Voight

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 2024

Abstract

Alan Reid first posed the question, "for every genus g, is there a torsion-free congruence subgroup Γ such that the modular curve $X(\Gamma)$ has genus g?" In an attempt to answer this question, we define two new families of congruence subgroups: intermediate congruence subgroups, and intersection type congruence subgroups. We devise methods to calculate the degree and number of elliptic points and cusps of these congruence subgroups, as well as for the arbitrary intersections of congruence subgroups of coprime level. By investigating the properties of these congruence subgroups, we prove a limited result in the affirmative for $g < 500$.

Preface

I wonder if everyone remembers their first proof. For me, it was in Winter 2021, day one of linear algebra. I sat, staring at the first homework assignment which read "prove that zero is unique in a vector space." I remember distinctly that it took me three hours.

This thesis is the culmination of my study of Mathematics thus far, which I believe truly began with that first proof. I hope that the reader, whether it be a student, professor, or some passerby who happened upon this paper while browsing the Dartmouth library, may find in this document the joy that the last four years of Mathematics has brought me.

As I sit here, writing some of the last words I will ever write as an undergraduate, I am filled with gratitude. There are far too many people to thank in one humble preface, but there are a couple names I would be remiss not to mention.

Thank you to Mike Wong, who, despite being restricted by the grim curriculum of multivariable calculus, still managed to show me the beauty of pure mathematics in every lecture.

Thank you to Professor Auel. When I was feeling unsure of myself after a particularly rough term of complex analysis, Professor Auel's abstract algebra course reignited my love of pure mathematics and especially group theory, which you will surely find much of in this paper.

Thank you to Professor Voight. Your intellect terrifies me and your compassion inspires me. Words cannot describe how grateful I am to have been able to study with you the last couple years. I wish you nothing but the best as you move to Sydney.

Thank you to Paul Shin. I doubt I would have managed these last couple years without your help. You truly embody what it means to be a Mathematician– and a good friend.

Thank you to Ash. Your support means the world to me, and I am the luckiest person in the world to know that you are by my side.

Contents

Chapter 1

Introduction

Section 1.1

Why modular curves?

An elliptic curve over a field F with $\mathrm{char}(F) = 0$ is defined by an equation $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{C}$ such that $4a^3 + 27b^2 \neq 0$. The set of points $E(F) := \{(x, y) \in F^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$ has the structure of an abelian group with identity given by the point at infinity, distinguishing them among curves. Elliptic curves over finite fields are the basis for multiple cryptosystems, and even present potential pathways to quantum-secure cryptography. Also of particular interest are complex elliptic curves. Via the elliptic Weierstrass function, every elliptic curve over $\mathbb{C}$ is isomorphic to a complex torus $\mathbb{C}/\Lambda_\tau$ where $\Lambda = \tau\mathbb{Z} \oplus \mathbb{Z}$ for some $\tau \in \mathbb{C}$ with $\mathrm{Im}(\tau) > 0$. Furthermore, two complex tori Λ_τ and $\Lambda_{\tau'}$ are group isomorphic if and only if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\binom{\tau}{1} = \gamma\binom{\tau'}{1}$. We can extend this type of action to the upper-half plane, $\mathcal{H} := \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$, by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau \mapsto \frac{a\tau+b}{c\tau+d}$. The quotient by this group action $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ parameterizes isomorphism classes of complex tori, and therefore complex elliptic curves. The set of isomorphism classes of elliptic curves is called a **moduli space**.

Since $E(\mathbb{C})$ is an abelian group, we are led to study its torsion subgroups, $E[N](\mathbb{C}) := \{P \in E(\mathbb{C}) : NP = 0\}$. In particular, we may be interested in parameterizing equivalence classes of elliptic curves equipped with a point of order N. Just like in the general case, there is a similar quotient $Y_1(N) := \Gamma_1(N)\backslash\mathcal{H}$ that parameterizes the moduli space of equivalence classes of elliptic curves with an N-torsion point, where $\Gamma_1(N) := \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N\right\}$. In general, moduli spaces of elliptic curves equipped with extra torsion data are parameterized by **modular curves**, $\Gamma\backslash\mathcal{H}$ where $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup**, meaning a subgroup that contains $\Gamma(N) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv I \pmod N\}$ for some N.

$\mathrm{SL}_2(\mathbb{Z})$ also acts in a similar manner on $\mathbb{Q} \cup \{\infty\}$. The equivalence classes $\Gamma\backslash(\mathbb{Q} \cup \{\infty\})$ are called **cusps**. Denote $X(\Gamma) := \Gamma\backslash(\mathcal{H} \cup \mathbb{Q} \cup \{\infty\})$. Adding in the cusps gives $X(\Gamma)$ the structure of a compact Riemann surface. One may ask what genera may arise from modular curves as topological surfaces. To simplify the scope of this question, we restrict to the case when $\Gamma/\{\pm I\} \leq \mathrm{PSL}_2(\mathbb{Z})$ acts freely on $\mathcal{H}$, i.e. no $\tau \in \mathcal{H}$ has nontrivial stabilizer in $\Gamma/\{\pm I\}$.

Question 1.1.1 (Alan Reid)**.** *For all $g \in \mathbb{N}$, is there a compactified modular curve of genus g given by $X(\Gamma)$ where Γ acts freely on $\mathcal{H}$?*

In this thesis, we endeavor to understand this question and and answer a limited version of this question in the affirmative.

Section 1.2

Summary of results

Let $\mathbb{N} \in \mathbb{Z}_{\geq 0}$ and let $C \leq (\mathbb{Z}/N\mathbb{Z})^\times$ be a subgroup. We define an **intermediate congruence subgroup**

$$\Gamma_C(N) := \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} a & * \\ 0 & d \end{pmatrix}, a \in C\right\}$$

Note that $\Gamma_1(N) = \Gamma_C(N)$ when $C = \{1\}$. Define the other extreme $\Gamma_0(N) := \Gamma_C(N)$ with $C = (\mathbb{Z}/N\mathbb{Z})^\times$. The name "intermediate" follows from the fact that $\Gamma_1(N) \leq \Gamma_C(N) \leq$

$\Gamma_0(N)$. Write $X_1(N) := X(\Gamma_1(N))$ and $X_0(N) := X(\Gamma_0(N))$. For the principal congruence subgroups, write $X(\Gamma(N)) = X(N)$. We prove the following:

Theorem 1.2.1. *There is no modular curve of genus 138 of the form $X(\Gamma(N_1) \cap \Gamma_C(N_2))$ where $\Gamma(N_1) \cap \Gamma_C(N_2)$ acts freely on $\mathcal{H}$ and $N_1, N_2 \in \mathbb{Z}_{\geq 0}$ satisfy $\gcd(N_1, N_2) = 1$,*

In particular, by taking N_1 or N_2 to be 1, it follows that there is no such modular curve of the form $X(N)$ or $X(\Gamma_C(N))$. In fact, we will show that 138 is the smallest genus not achieved by an intermediate congruence subgroup. Thus, while intermediate congruence subgroups appear to achieve many different genera, they are not sufficient to conclusively answer Alan Reid's question.

We also define a new type of congruence subgroup. We say $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is of **intersection type** if there exists prime powers $p_i^{e_i}$ with each p_i distinct such that $\Gamma = \bigcap_{i=1}^{n} \Gamma_i$ where each $\Gamma_i \geq \Gamma(p_i^{e_i})$. By looking at both intermediate and intersection-type congruence subgroups, we are able to prove the following:

Theorem 1.2.2. *There is a modular curve $X(\Gamma)$ for every genus $0 \leq g < 500$, with the congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ acting freely on $\mathcal{H}$.*

We prove the above theorem by exhibiting a specific witness for each genera among both intermediate and intersection type congruence subgroups.

Section 1.3

Navigating this document

In chapter 2, we present background information and key theorems necessary to the study of modular curves. We define the modular group $\mathrm{SL}_2(\mathbb{Z})$ and its congruence subgroups along with their actions on the upper half-plane. We then provide an outline of the proof that the compactified modular curve $X(\Gamma)$ is indeed a compact Riemann surface, as well as the

genus formula based on the degree, elliptic points ($\tau \in \mathcal{H}$ with nontrivial stabilizer in Γ), and cusps of $X(\Gamma)$.

In Chapter 3 we start with a proof due to Csirik, Wetherell, and Zieve [3] of a lower bound on the genus of $X(\Gamma_0(N))$ in terms of N. Since $X(\Gamma_C(N))$ projects onto $X(\Gamma_0(N))$, Riemann-Hurwitz guarantees that our lower bound holds also for the genus of $X(\Gamma_C(N))$ for all $C \leq (\mathbb{Z}/N\mathbb{Z})^\times$. We will then foray into the intersections of congruence subgroups of relatively prime level, showing that the degree and number of elliptic points and cusps of intersections are multiplicative in the components.

In Chapter 4, we dive into formulas necessary to calculate the genus of intermediate congruence subgroups. We then use these formulas along with some SageMath [5] and Magma [1] code to prove theorems 1.2.1 and 1.2.2

In Chapter 5, we analyze the frequencies of genera achieved by intermediate congruence subgroups and pose questions for future work.

Appendix A includes data tables that provide witnesses for torsion-free congruence subgroups of genus up to 500, and Appendix B contains the relevant code used throughout this project.

Chapter 2

Background

Section 2.1

The modular group and its action

Any discussion on modular curves must begin with the **upper half-plane**. Let $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Key to this discussion is the aptly named **modular group**:

$$\mathrm{SL}_2(\mathbb{Z}) := \{A \in M_2(\mathbb{Z}) | \det(A) = 1\}$$

Within $\mathrm{SL}_2(\mathbb{Z})$ are the **principal congruence subgroups**:

$$\Gamma(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) | \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\right\}$$

Any subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** if it contains $\Gamma(N)$ for any $N \in \mathbb{Z}_{>0}$. The smallest such N is called the **level** of Γ. These subgroups arise naturally as groups whose quotients of the upper half-plane parameterize equivalence classes of complex elliptic curves with extra torsion data.

$\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ in the following manner:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

Of course, any subgroup of $\mathrm{SL}_2(\mathbb{Z})$ has an identical induced action.

We define a **modular curve** to be $Y(\Gamma) = \Gamma\backslash\mathcal{H}$, i.e. the quotient of $\mathcal{H}$ by the orbits of the action of Γ. The primary objects of our concern are **compactified modular curves** $X(\Gamma) = \Gamma\backslash(\mathcal{H} \cup \mathbb{Q} \cup \{\infty\})$ (henceforth referred to as just "modular curves"), where $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{Q}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{x}{y} = \begin{cases} \frac{ax+by}{cx+dy} & \frac{x}{y} \neq \frac{-d}{c} \\ \infty & \frac{x}{y} = \frac{-d}{c} \end{cases}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \begin{cases} \frac{a}{c} & c \neq 0 \\ \infty & c = 0 \end{cases}$$

The cosets of $\Gamma\backslash(\mathbb{Q} \cup \{\infty\})$ are called the **cusps** of $X(\Gamma)$.

Section 2.2

$X(\Gamma)$ as a compact Riemann surface

Theorem 2.2.1. *If $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup, then $X(\Gamma)$ is a compact Riemann surface.*

This is a highly nontrivial theorem that Diamond and Sherman devote an entire chapter to proving [4, Ch. 2]. An outline of the proof is sketched here:

Endow $\mathcal{H}$ with the Euclidean topology. Give $Y(\Gamma)$ the quotient topology under the surjection $\pi : \mathcal{H} \to Y(\Gamma)$ by $\tau \mapsto \Gamma\tau$. Since π is continuous ($\mathrm{SL}_2(\mathbb{Z})$, and by extension Γ, acting on $\mathcal{H}$ is a topological group action), $Y(\Gamma)$ is connected. Second countability also

follows from second countability of $\mathcal{H}$.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}, \tag{2.2.2}$$

revealing that the action of $\mathrm{SL}_2(\mathbb{Z})$ endows the upper half-plane with a geometry concentrated near the real axis. In particular, for any $a \in \mathbb{R}_{>}0$ and a compact set $C \subset \mathcal{H}$, there are only finitely many $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sup\{\mathrm{Im}(\tau) : \tau \in \gamma(C)\} \geq a$. We then conclude that the action of $\mathrm{SL}_2(\mathbb{Z})$ $\mathcal{H}$ is **acts properly** (sometimes confusingly called "properly discontinuous") meaning for $\tau_1, \tau_2 \in \mathcal{H}$, there exist neighborhoods U_1 and U_2 of τ_1 and τ_2 respectively such that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma(U_1) \cap U_2 \neq \emptyset \Rightarrow \gamma\tau_1 = \tau_2$. $Y(\Gamma)$ is Hausdorff follows from this property.

To prove that $Y(\Gamma)$ can be given the structure of a Riemann surface, we need to add charts. At points $\pi(\tau) \in Y(\Gamma)$ with $\tau \in \mathcal{H}$ such that $\mathrm{Stab}_\Gamma(\tau) = \Gamma \cap \{\pm I\}$ (this stabilizer is sometimes called the **isotropy subgroup** of τ in Γ), the property of $\mathrm{SL}_2(\mathbb{Z})$ acting properly guarantees a neighborhood U with no Γ-equivalent points, and thus a local inverse $\pi(U) \to U$ is a fine chart.

We run into some issues with **elliptic points**– i.e, $\tau \in \mathcal{H}$ such that there exists $\gamma \in \Gamma \backslash \{\pm I\}$ such that $\gamma\tau = \tau$. In this case we need to be a bit more creative with our maps. The key is that stabilizers under the action of congruence subgroups are finite and cyclic. It is not difficult to show that any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ that fixes some $\tau \in \mathcal{H}$ has characteristic polynomial $x^2 + 1$ or $x^2 \pm x + 1$ and thus has order 1,2,3,4, or 6. A dip into module theory confirms that these are exactly the conjugates of

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and their inverses. Indeed, $\mathrm{SL}_2(\mathbb{Z})$ has two elliptic points, namely $\mathrm{SL}_2(\mathbb{Z})i$ and $\mathrm{SL}_2(\mathbb{Z})e^{2\pi i/3}$ who have stabilizers

$$\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \text{ and } \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle$$

respectively. In fact, any $\mathrm{SL}_2(\mathbb{Z})$ equivalent point to i and $e^{2\pi i/3}$ in $\mathcal{H}$ has stabilizer conjugate to the stabilizer of i or $e^{2\pi i/3}$, and thus the stabilizer group of any $\tau \in \mathcal{H}$ is finite cyclic. Since congruence subgroups have finite index in $\mathrm{SL}_2(\mathbb{Z})$, it follows that there are finitely many elliptic points for any Γ, and their stabilizers in Γ are subgroups of the stabilizers in $\mathrm{SL}_2(\mathbb{Z})$, and therefore also finite and cyclic.

With this in hand, we are ready to put charts around elliptic points. Since $\mathrm{SL}_2(\mathbb{Z})$ acts properly, we are guaranteed a neighborhood U of τ with the property that if $\gamma(U) \cap U \neq \emptyset$, then $\gamma \in \mathrm{Stab}_\Gamma(\tau)$ and U contains at most one elliptic point. If we take δ_τ to be the map defined by

$$\delta_\tau := \begin{pmatrix} 1 & -\tau \\ 1 & -\overline{\tau} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$$

then by the usual action, this map takes τ to 0 and $\overline{\tau}$ to ∞. Note that

$$S := \mathrm{Stab}_{\delta_\tau\{\pm I\}\Gamma\delta_\tau^{-1}}(0)/\{\pm I\} = \delta_\tau \,\mathrm{Stab}_\Gamma(\tau)\delta_\tau^{-1}$$

and thus S is finite cyclic. Since S fixes 0 and ∞, any matrix in S must be of the form $z \mapsto az$. Additionally, since S is finite cyclic, all matrices in S act as rotations of angle $2\pi/h_\tau^n$ for some $n \in \mathbb{Z}_{>0}$ and $h_\tau := |\{\pm I\}\,\mathrm{Stab}_\Gamma(\tau)/\{\pm I\}|$ (the **period** of τ). By the properties of our neighborhood U of τ, if $\pi(\tau_1) = \pi(\tau_2)$ for some $\tau_1, \tau_2 \in H$, then $\tau \in \mathrm{Stab}_\Gamma(\tau)$, and thus $\delta_\tau(\tau_1) \in S\delta_\tau(\tau_2)$. This means that δ_τ makes Γ-equivalent points separated by fixed angles, and by taking the composition of the map δ_τ and the h_τth power map $z \mapsto z^{h_\tau}$. This composition induces a homeomorphism of $\pi(U)$ to an open disk $V \subseteq \mathbb{C}$. Thus, after checking the transition maps between charts, we conclude that $Y(\Gamma)$ is a Riemann surface.

To compactify $Y(\Gamma)$, add in the cusps. To give $\mathcal{H}^* := \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ an appropriate topology, we use the standard topology on $\mathcal{H}$, along with the sets generated by $\alpha(\mathcal{N}_M \cup \{\infty\})$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, where $\mathcal{N}_M = \{\tau \in \mathcal{H} : \mathrm{Im}(\tau) > M\}$, for all $M \in \mathbb{R}_{>0}$. Giving $X(\Gamma)$ the quotient topology, it's not too difficult to check that $X(\Gamma)$ is indeed Hausdorff, connected, and compact.

For a point $\Gamma\tau$ and Γs in $X(\Gamma)$, with $\tau \in \mathcal{H}$, $s = \alpha(\infty) \in \mathbb{Q} \cup \{\infty\}$, let U be a neighborhood of τ with compact closure K. Then by (2.2.2), there exists $M \in \mathbb{R}_{>0}$ such that $\mathrm{Im}(\gamma(\tau')) < M$ for all $\gamma \in \Gamma$, $\tau' \in K$. Thus, the two sets $\pi(U)$ and $\pi(\alpha(\mathcal{N}_M \cup \{\infty\}))$ contain $\pi(\tau)$ and $\pi(\alpha(\infty))$ respectively, and are disjoint.

For two cusps Γs_1 and Γs_2, where $s_1 = \alpha_1(\infty)$ and $s_2 = \alpha_2(\infty)$ the sets $\pi(\alpha_1(\mathcal{N}_2 \cup \{\infty\}))$ and $\pi(\alpha_2(\mathcal{N}_2 \cup \{\infty\}))$ work to satisfy the Hausdorff condition.

Connectedness is easy, since if $\mathcal{H}^* = U_1 \sqcup U_2$ (i.e., the union of disjoint open sets), without loss of generality, we can assume $\mathcal{H} \subseteq U_1$ since $\mathcal{H}$ is connected, and thus $U_2 \subseteq \mathbb{Q} \cup \{\infty\}$, contradicting the assumption that U_2 was open.

Finally, compactness follows from the fact that the fundamental domain for $Y(1)$ is $D := \{\tau \in \mathcal{H} : -1/2 \leq \mathrm{Re}(\tau) \leq 1/2, |\tau| \geq 1\}$, and taken with a point at infinity, $D^* = D \cup \{\infty\}$ is compact. For a congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, Γ has finite index in $\mathrm{SL}_2(\mathbb{Z})$, so $\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_j \Gamma\gamma_j$ for some finite set of representatives $\gamma_j \in \mathrm{SL}_2(\mathbb{Z})$. Since D is a fundamental domain and $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{Q} \cup \{\infty\}$, it follows that $\mathcal{H}^* = \bigcup_j \Gamma(\gamma_j) D^*$. Therefore, $X(\Gamma) = \bigcup_j \pi(\gamma_j D^*)$, i.e. the finite union of compact sets (since continuous maps preserve compactness). Thus, $X(\Gamma)$ is compact.

The last thing we need to do to conclude $X(\Gamma)$ is a compact Riemann surface is add charts for the cusps. Let $\delta \in \mathrm{SL}_2(\mathbb{Z})$ take $s \in \mathbb{Q} \cup \{\infty\}$ to ∞. Then since $\mathrm{SL}_2(\mathbb{Z})$ acts continuously on $\mathcal{H}^*$, $\delta^{-1}(\mathcal{N}_2 \cup \{\infty\})$ is an open neighborhood containing U. We can then "wrap" ($\mathcal{N}_2 \cup \{\infty\}$ into a disk with the map $z \mapsto e^{2\pi i z/h_s}$ where h_s is the **width** of s, given

by

$$h_s := [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) : \mathrm{Stab}_{\delta\{\pm I\}\Gamma\delta^{-1}}(\infty)],$$

an analogous concept to the "period" of an elliptic point. As with elliptic points, the composition of δ and the wrapping map induce a homeomorphism from $\pi(U) \to V$ an open subset of $\mathbb{C}$, where $U := \delta^{-1}(\mathcal{N}_2 \cup \{\infty\})$.

Section 2.3

The genus of $X(\Gamma)$

Since $X(\Gamma)$ is a compact Riemann surface, its topological structure is determined by its genus (up to homeomorphism). Before we begin our talk of the genus of $X(\Gamma)$, we assume some theorems from complex analysis [4, p. 65].

Theorem 2.3.1. *Let $f : X \to Y$ be a nonconstant holomorphic map between compact Riemann surfaces. Then the following are equivalent:*

(a) *f is surjective*

(b) *for all $y \in Y$, $f^{-1}(y)$ is discrete in X, and therefore finite since X is compact.*

(c) *There is a well-defined degree d such that $|f^{-1}(y)| = d$ for all but finitely many $y \in Y$.*

(d) *For all $y \in Y$ such that $|f^{-1}(y)| \neq d$, $\sum_{x \in f^{-1}(y)} e_x = d$ where e_x is the ramification degree, i.e. f acts as an e_x-to-1 map locally around x.*

In our case, if f is the holomorphic map from $X(\Gamma)$ to $X(1)$ given by $\Gamma\tau \mapsto \mathrm{SL}_2(\mathbb{Z})\tau$ and $d = [\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma]$. We also assume the following:

Theorem 2.3.2 (Riemann-Hurwitz)**.** *Let $f : X \to Y$ be a nonconstant holomorphic map of*

degree d. If g_X and g_Y is the genus of X and Y respectively, then

$$2g_X - 2 = d(2g_Y - 2) + \sum_{x \in X}(e_x - 1)$$

Note that f induces a local map $f' : \mathbb{C} \to \mathbb{C}$ between the image of charts of $X(\Gamma)$ and $X(1)$. For $\tau \in \mathcal{H}$, letting h_Γ, h_1 be the **period** τ in Γ and $\mathrm{SL}_2(\mathbb{Z})$ respectively, this must take $\delta(\tau)^{h_1}$ to $\delta(\tau)^{h_\Gamma}$, and thus f' is the map $q \mapsto q^{h_1/h_\Gamma}$ implying h_1/h_Γ is integral. Since all $\tau \in \mathcal{H}$ have period 1,2 or 3, this implies the ramification degree is

$$\begin{aligned} e_{\Gamma\tau} &= [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\tau) : \{\pm I\}\,\mathrm{Stab}_\Gamma(\tau)] \\ &= \begin{cases} h_1 & \text{if } \tau \text{ is an elliptic point for } \mathrm{SL}_2(\mathbb{Z}) \text{ but not for } \Gamma \\ 1 & \text{otherwise} \end{cases} \end{aligned}$$

Let ϵ_h be the number of order h elliptic points for Γ (i.e. $h = 2, 3$). Let $z_2 = \mathrm{SL}_2(\mathbb{Z})i$ and $z_3 = \mathrm{SL}_2(\mathbb{Z})e^{2\pi i/3}$. Using our ramification degree formula, we see that for $h = 2, 3$,

$$d = \sum_{x \in f^{-1}(z_h)} e_x = h(|f^{-1}(z_h)| - \epsilon_h) + \epsilon_h$$

or similarly,

$$\sum_{x \in f^{-1}(z_h)} (e_x - 1) = (h-1)(|f^{-1}(z_h)| - \epsilon_h)$$

Combining the two, we see that

$$\sum_{x \in f^{-1}(z_h)} (e_x - 1) = \frac{h}{h-1}(d - \epsilon_h) \tag{2.3.3}$$

Finally, if ϵ_∞ is the number of cusps of $X(\Gamma)$, we get

$$\sum_{x \in f^{-1}(\mathrm{SL}_2(\mathbb{Z})\infty)} (e_x - 1) = d - \epsilon_\infty \tag{2.3.4}$$

Since $e_x - 1 = 0$ for all points that aren't elliptic or cusps, specializing Theorem 2.3.2 to $X = X(\Gamma)$ and $Y = X(1)$ (genus 0), we get

$$g = 1 - d + \frac{1}{2}\Big(\sum_{x \in f^{-1}(z_2)} (e_x - 1) \ + \sum_{x \in f^{-1}(z_3)} (e_x - 1) \ + \sum_{x \in f^{-1}(\mathrm{SL}_2(\mathbb{Z})\infty)} (e_x - 1)\Big) \tag{2.3.5}$$

Combining this with equations (2.3.3) and (2.3.4), we simplify (2.3.5) to the subject of this document [4, Thm 3.1.1]:

Theorem 2.3.6. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of degree d. Let ϵ_h be the number of order h elliptic points, and let ϵ_∞ be the number of cusps. Then if the g is the genus of $X(\Gamma)$,*

$$g = 1 + \frac{d}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}$$

Naturally, we might wonder what possible genera can arise from this above equation? The rest of this document examines this very question in specifically the torsion-free case (no elliptic points).

Chapter 3

Intersections of congruence subgroups and lower bounds on genera

Let $N \in \mathbb{Z}_{\geq 1}$ and $C \leq (\mathbb{Z}/N\mathbb{Z})^\times$. Then there is a natural congruence subgroup

$$\Gamma_C(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \pmod{N}, a \in C \right\}$$

The restriction on the determinant mandates that $d \equiv a^{-1} \pmod{N}$ and thus $d \in C$ as well. When $C = (\mathbb{Z}/N\mathbb{Z})^\times$, $\Gamma_C(N) = \Gamma_0(N)$, and when C is the trivial group $\Gamma_C(N) = \Gamma_1(N)$. Denote the modular curve $X(\Gamma_C(N))$ as $X_C(N)$.

Section 3.1

A lower bound on the genus of $X_0(N)$

Let $g_0(N)$ be the genus of $X_0(N)$. Since $C \leq (\mathbb{Z}/N\mathbb{Z})^\times$, $\Gamma_C(N) \leq \Gamma_0(N)$ and thus there is a natural (surjective) projection $\pi : X_C(N) \to X_0(N)$, and thus by Theorem 2.3.2, the $g_0(N)$ is less than or equal to the genus of $X(\Gamma_C(N))$ for all $C \leq (\mathbb{Z}/N\mathbb{Z})^\times$. Thus, a lower bound on $g_0(N)$ also functions as a lower bound on the genus of $X_C(N)$. An unpublished paper

from Csirik, Wetherell, and Zieve [3] proves a lower bound on $g_0(N)$. We recreate the proof here, filling in details left to the reader. Also note that this proof is for all $\Gamma_0(N)$ congruence subgroups, regardless of whether they are torsion free or not.

Theorem 3.1.1. *Let $g_0(N)$ be the genus of $X_0(N)$. Then*

$$g_0(N) \geq (N - 5\sqrt{N} - 8)/12.$$

To prove the theorem, we first show a couple lemmas.

Lemma 3.1.2. *If $N = \prod_p p^{r_p}$, then $\epsilon_\infty = \prod_p \theta(p, r_p)$ where $\theta(p, 2r) = p^r + p^{r-1}$ and $\theta(p, 2r+1) = 2p^r$*

Proof. To prove this, we must step briefly into the world of arithmetic functions. An arithmetic function $f : \mathbb{N} \to \mathbb{R}$ is **multiplicative** if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$. It follows that if f is multiplicative and if $N = p_1^{r_1} \cdots p_n^{r_n}$ (for distinct primes p_i), then $f(N) = \prod_{i=1}^n f(p_i^{r_i})$.

Diamond and Shurman prove that for a modular curve of the form $X_0(N)$, the number of cusps is

$$\delta(N) := \epsilon_\infty = \sum_{d|N} \phi(\gcd(d, N/d))$$

where ϕ is Euler's totient function [4, p. 103]. We can check directly for prime powers that if $N = p^r$,

$$\sum_{d|N} \phi(\gcd(d, N/d)) = \theta(p, r)$$

Thus, if δ is multiplicative, Lemma 3.1.2 follows. We now proceed to show that δ is multiplicative.

Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Consider

$$\delta(mn) = \sum_{d|mn} \phi(\gcd(d, mn/d))$$

Since $\gcd(m, n) = 1$, if $d|mn$, then we can write $d = d_1 d_2$ where $d_1 = \gcd(d, m)$ and $d_2 = \gcd(d, n)$. Thus,

$$\delta(mn) = \sum_{d_1|m} \sum_{d_2|n} \phi(\gcd(d_1 d_2, mn/d_1 d_2))$$

I claim that $x := \gcd(d_1 d_2, mn/d_1 d_2) = \gcd(d_1, m/d_1)\gcd(d_2, n/d_2) =: y$. Let p^r be a prime power dividing x. Then $p^r | d_1 d_2$ and $p^r | mn/d_1 d_2$. However, since $\gcd(m, n) = 1$, that means either p^r divides d_1 and m/d_1, or p^r divides d_2 and n/d_2. Thus, $p^r | y$. Now suppose $p^r \mid y$. Then by the same logic, $p^r \mid x$. Since integers are uniquely determined by their decomposition into prime powers, it must be that $x = y$.

Therefore, since ϕ is multiplicative,

$$\begin{aligned}
\delta(mn) &= \sum_{d|mn} \phi(\gcd(d, mn/d)) \\
&= \sum_{d_1|m} \sum_{d_2|n} \phi(\gcd(d_1 d_2, mn/d_1 d_2)) \\
&= \sum_{d_1|m} \sum_{d_2|n} \phi(\gcd(d_1, m/d_1)(\gcd(d_2, n/d_2))) \\
&= \sum_{d_1|m} \sum_{d_2|n} \phi(\gcd(d_1, m/d_1))\phi((\gcd(d_2, n/d_2))) \\
&= \sum_{d_1|m} \phi(\gcd(d_1, m/d_1)) \sum_{d_2|n} \phi(\gcd(d_2, n/d_2)) \\
&= \delta(m)\delta(n)
\end{aligned}$$

Thus, δ is multiplicative and the proof is done. □

Lemma 3.1.3. *If N has exactly two distinct prime divisors p and q, then $N/p + N/q > 2\sqrt{N}$.*

Proof. We will prove this in the minimal case that $N = pq$ (with no multiplicity), and it follows in all other cases. If $N = pq$, then $N/p + N/q = p + q$. Thus, it suffices to show that $p + q > 2\sqrt{pq}$ or equivalently, $(p + q)^2 > 4pq$.

Without loss of generality, let $p = q + n$ with $n \in \mathbb{Z}^+$. Then

$$(p+q)^2 = p^2 + q^2 + 2pq = p^2 + (p-n)^2 + 2pq = 2p^2 - 2pn + n^2 + 2pq$$
$$= 2p(p-n) + n^2 + 2pq = 4pq + n^2 > 4pq$$

□

Let $\psi(N) := N \prod_{p|N}(1 + 1/p)$ be the Dedekind psi function.

Lemma 3.1.4. *In all cases,* $\epsilon_\infty \leq \psi(N)/\sqrt{N}$

Proof. Let $N = \prod_p p_p^r$ for distinct primes p. Then

$$\psi(N)/\sqrt{N} = \prod_{p|N}(p^{r_p/2} + p^{(r_p/2)-1})$$

We compare $\epsilon_\infty = \prod_{p|N} \theta(p, r_p)$ to $\psi(N)/\sqrt{N}$ term by term to construct our inequality.

Suppose for a given prime p that $r_p = 2x$ for some $x \in \mathbb{N}$.

$$\theta(p, r_p) = p^x + p^{x-1} \leq p^{r_p/2} + p^{(r_p/2)-1}$$

(in fact, they are equal). Now suppose $r_p = 2x+1$. Note that for all primes p, $p^{1/2}+p^{-1/2} > 2$. Thus,

$$p^{r_p/2} + p^{(r_p/2)-1} = p^x(p^{1/2} + p^{-1/2}) > 2p^x = \theta(p, r_p)$$

Thus, $\epsilon_\infty \leq \psi(N)/\sqrt{N}$. □

Lemma 3.1.5. *if N has 3+ prime divisors, then* $\psi(N) - N > 3N^{2/3}$

Proof. We first show that this holds in the case where $N = sqr$ for distinct primes s, q, r.

$$\psi(N) - N = 1 + s + q + r + sq + sr + qr$$

By the geometric-arithmetic mean inequality,

$$\frac{sq + sr + qr}{3} \geq (sq \cdot sr \cdot qr)^{1/3} = N^{2/3}$$

Thus,

$$\psi(N) - N > 3N^{2/3}.$$

Now let $M = Nm = sqrm$ for some $m \in \mathbb{Z}_{\geq 2}$. Then

$$\psi(M) - M = M\prod_{p|M}(1 + 1/p) - M = m\Big(N\prod_{p|M}(1 + 1/p) - N\Big) \geq m\Big(N\prod_{p|N}(1 + 1/p) - N\Big)$$
$$> m(3N^{2/3}) > 3M^{2/3}$$

Thus, the statement holds. □

Lemma 3.1.6. $\epsilon_2, \epsilon_3 \leq \epsilon_\infty$.

Proof. This one is quite easy. Diamond and Sherman prove that $\epsilon_2, \epsilon_3 \leq 2^k$ if N has k distinct prime divisors [4, p. 96], nut from Lemma 3.1.2 it is clear that $\epsilon_\infty \geq 2^k$. □

With this toolbox of Lemmas, we are finally ready to prove the lower bound on $g_0(N)$.

Proof. The proof proceeds in 3 cases. Note that Diamond and Shurman give explicit formulas for the degree, cusps, and elliptic points of $X_0(N)$ [4, p. 107], and thus it is trivial with a computer to check that our bound holds for $N \leq 2000$. Thus, we may assume $N > 2000$ in the following proof.

Case 1: N has one distinct prime divisor

Let $N = p^n$. First, we suppose $n = 2r$. Since the degree of $X_0(N)$ is given by $\psi(N)$ [3, p. 2], by Theorem 2.3.6

$$g_0(p^n) = 1 + \frac{\psi(N)}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{p^r + p^{r-1}}{2}$$

Since $\epsilon_2, \epsilon_3 \leq 2$,

$$g_0(N) \geq \frac{1}{12}(p^n + p^{n-1} - 6(p^r + p^{r-1}) - 2)$$

If $n = 2$, then we get (sometimes with equality):

$$g_0(p^2) \geq \frac{1}{12}(p^2 - 5p - 8)$$

We can also check directly in the case where $n = 4$, and since $p^n > 2000$ by assumption, $p \geq 7$.

$$12g_0(p^4) \geq p^4 + p^3 - 6(p^2 + p) - 2 \geq p^4 + 7p^2 - 12p^2 - 2 \geq p^4 - 5p^2 - 8$$

If $n = 6$, then $p \geq 5$:

$$12g_0(p^6) \geq p^6 + p^5 - 12p^3 - 2 \geq p^6 + 25p^3 - 12p^3 - 2 \geq p^6 - 5p^3 - 8$$

Thus, we can assume $n \geq 8$, and then

$$12g_0(p^n) \geq p^n + p^{n-1} - 12p^r - 2 \geq p^n + 8p^r - 12p^r - 2 \geq p^n - 5p^r - 8$$

Now suppose $n = 2r + 1$. The case of $n = 1$ is trivial ($g_0(N) \geq \frac{p-13}{12}$), so we assume

$n \geq 3$. First suppose $p \geq 5$. Then

$$12g_0(p) \geq p^n + p^{n-1} - 12p^r - 2 = p^n + p^{n/2}(p^{(n/2)-1} - \frac{12}{p^{1/2}}) - 2 \geq p^n - 5p^{n/2} - 8$$

Now suppose $p = 2$ or $p = 3$. Then since $N > 2000$, we know $n \geq 7$, and thus

$$12g_0(p) \geq p^n + p^{n-1} - 9p^{n/2} - 2 \geq p^n + 5p^{n/2} - 9p^{n/2} - 2 \geq p^n - 5p^{n/2} - 8$$

We have therefore exhausted all cases when $N = p^n$.

Case 2: N has 2 distinct prime divisors

Let $N = p^n q^m$. Then

$$d - N = \psi(N) - N = N(1 + 1/p)(1 + 1/q) - N = N/p + N/q + N/pq > N/p + N/q$$

thus by Lemma 3.1.3,

$$d > N + 2\sqrt{N}$$

Similar to case 1, $\epsilon_2, \epsilon_3 \leq 4$, so by Theorem 2.3.6 and Lemma 3.1.4

$$g_0(N) \geq 1 + \frac{d}{12} - 4/4 - 4/3 - \frac{d}{2\sqrt{N}}$$

and thus

$$\begin{aligned} 12g_0(N) &\geq d(1-\frac{6}{\sqrt{N}})-16 \\ &> (N+2\sqrt{N})(1-\frac{6}{\sqrt{N}})-16 \\ &= N+2\sqrt{N}-6\sqrt{N}-12-16 \\ &= N-5\sqrt{N}+\sqrt{N}-28 \\ &> N-5\sqrt{N}-8 \end{aligned} \tag{3.1.7}$$

Note that the last inequality holds since $N > 2000$, $\sqrt{N} > 44$.

Case 3: N has at least 3 distinct prime divisors

Using Lemma 3.1.6, we can write

$$g_0(N) \geq 1 + \frac{d}{12} - (\frac{1}{2}+\frac{1}{3}+\frac{1}{4})\epsilon_\infty$$

Then, invoking lemmas 3.1.4 and 3.1.5, we get

$$\begin{aligned} 12g_0(N) &\geq 12 + d - 13d/\sqrt{N} \\ &= (N-5\sqrt{N}-8)+(d-N)(1-\frac{13}{\sqrt{N}})-8\sqrt{N}+20 \\ &> (N-5\sqrt{N}-8)+3N^{4/6}-8N^{3/6}-39N^{1/6}+20 \end{aligned} \tag{3.1.8}$$

But the largest real root of $3x^4 - 8x^3 - 39x + 20 < 2000^{1/6}$, and therefore for all $N > 2000$, $3N^{4/6} - 8N^{3/6} - 39N^{1/6} + 20 > 0$, completing the proof. □

Section 3.2

Intersections of congruence subgroups of relatively prime level

This section is devoted to proving Theorem 3.2.1. For the rest of the chapter, let $\Gamma_i \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of level N_i, and since $-I$ acts trivially on $\mathcal{H}$ assume without loss of generality that $-I \in \Gamma_i$. Let $d_i = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_i]$ (the degree of $X(\Gamma_i)$), and let c_i be the number of cusps of $X(\Gamma_i)$. Finally, let ϵ_2^i and ϵ_3^i be the number of elliptic points of order 2,3 respectively of $X(\Gamma_i)$.

Theorem 3.2.1. *Suppose* $\gcd(N_1, N_2) = 1$. *Then the following statements hold.*

(a) *The degree of* $X(\Gamma_1 \cap \Gamma_2)$ *is* $d_1 d_2$

(b) *The number of cusps of* $X(\Gamma_1 \cap \Gamma_2)$ *is* $c_1 c_2$

(c) *The number of order 2 elliptic points of* $X(\Gamma_1 \cap \Gamma_2)$ *is* $\epsilon_2^1 \epsilon_2^2$

(d) *The number of order 3 elliptic points of* $X(\Gamma_1 \cap \Gamma_2)$ *is* $\epsilon_3^1 \epsilon_3^2$.

In other words, d, c, ϵ_2, and ϵ_3 are multiplicative in Γ_i.

As we are primarily concerned with smooth modular curves (no elliptic points), (c) and (d) are not especially relevant, but are very much in the spirit of the rest of theorem, and will be helpful for speeding up calculations in Chapter 4.

Theorem 2.3.6 yields the immediate result

Corollary 3.2.2. *Let* $\Gamma_1, \Gamma_2 \leq \mathrm{SL}_2(\mathbb{Z})$ *be congruence subgroups with* $\gcd(N_1, N_2) = 1$ *and at least one of* Γ_1, Γ_2 *torsion-free. Then the genus of* $\Gamma_1 \cap \Gamma_2$ *is*

$$g = 1 + \frac{d_1 d_2}{12} - \frac{c_1 c_2}{2} \tag{3.2.3}$$

Proof. Without loss of generality, let Γ_1 be torsion-free. Since $\Gamma_1 \cap \Gamma_2 \leq \Gamma_1$, $\Gamma_1 \cap \Gamma_2$ is also torsion-free. Thus, $X(\Gamma_1 \cap \Gamma_2)$ has no elliptic points, and using Theorem 3.2.1 the genus formula reduces to (3.2.3). □

Before we dive into the proof of Theorem 3.2.1, we first prove some helpful lemmas.

Lemma 3.2.4. *If* $\gcd(N_1, N_2) = 1$*, then* $\mathrm{SL}_2(\mathbb{Z}/N_1N_2\mathbb{Z}) \simeq \mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N_2\mathbb{Z})$

Proof. The Sunzi Theorem (CRT) guarantees a ring isomorphism $\phi : M_2(\mathbb{Z}/N_1N_2\mathbb{Z}) \xrightarrow{\sim} M_2(\mathbb{Z}/N_1\mathbb{Z}) \times M_2(\mathbb{Z}/N_2\mathbb{Z})$. In particular, this isomorphism preserves multiplicative structure. For $A \in M_2(\mathbb{Z}/N_1N_2\mathbb{Z})$, $\det(A) \equiv 1 \pmod{N_1N_2} \iff \det(A) \equiv 1 \pmod{N_1}$ and $\det(A) \equiv 1 \pmod{N_2}$. Thus, the restriction of ϕ to $\mathrm{SL}_2(\mathbb{Z}/N_1N_2\mathbb{Z})$ is an isomorphism of groups. □

Lemma 3.2.5. *For all positive integers* N*, the map* $\pi_N : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ *given by component-wise reduction modulo* N *is a surjection.*

Proof. Given a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, lift to a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$. Note that $ad - bc \equiv 1 \pmod{N}$, i.e. $ad - bc - kN = 1$ for some $k \in \mathbb{Z}$, and by the Bézout identity, $\gcd(c, d, N) = 1$. Since both c and d cannot be 0, first suppose $c \neq 0$. Let $g = \gcd(c, d)$. By the CRT, there exists $t \in \mathbb{Z}$ such that for primes p *midc*, $t \equiv 1 \pmod{p}$ when $p \mid g$, and $t \equiv 0 \pmod{p}$ when $p \nmid g$ but $p \mid c$. We claim that $\gcd(c, d + tN) = 1$.

Let p be a prime such that $p \mid c$ but $p \nmid d$. Then $p \mid t$ so p cannot divide $(d + tN)$. Now let $p \mid c$ and $p \mid d$. Since $\gcd(c, d, N) = 1$, it must be that $p \nmid N$. Then $t \equiv 1 \pmod{p}$, and $d + tN \equiv 0 + N \pmod{p} \not\equiv 0 \pmod{p}$. Thus, c and $d + tN$ share no nontrivial divisors. If $c = 0$, then $d \neq 0$ and an identical argument shows there exists $s \in \mathbb{Z}$ such that $\gcd(c + sN, d) = 1$. Hence, we can always lift c, d to a coprime pair c', d' that maintain the property $c', d' \equiv c, d \pmod{N}$.

Since $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, it follows that $ad' - bc' = 1 + kN$ for some $k \in \mathbb{Z}$. Since $\gcd(c', d') = 1$, it follows from the Bézout identity that there exist $x, y \in \mathbb{Z}$ such that

$xd' - yc' = 1$. Let $a' = a - xkN$, $b' = b - ykN$. Then

$$a'd' - b'c' = (a - xkN)d' - (b - ykN)c' = ad' - bc' - kN(xd' - yc') = 1 + kN - kN(1) = 1$$

Therefore, γ lifts to $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. □

Lemma 3.2.6. *Let* $C_N := \{\Gamma \leq \mathrm{SL}_2(\mathbb{Z}) : \Gamma(N) \leq \Gamma\}$ *and let* $H_N := \{H \leq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\}$. *The map* $\Phi : C_N \to H_N$ *given by* $\Gamma \mapsto \pi_N(\Gamma)$ *is a bijection.*

Proof. We exhibit an inverse given by $\Phi^{-1}(H) = \pi_N^{-1}(H)$. Note that since π_N is surjective by the previous lemma, the preimage of H under π_N maps surjectively onto H, and thus

$$\Phi\Phi^{-1}(H) = \pi_N(\pi_N^{-1}(H)) = H$$

Thus, ϕ^{-1} is a right inverse.

Let $\Gamma \in C_N$. Let $\Gamma' = \Phi^{-1}\Phi(\Gamma) = \pi_N^{-1}(\pi_N(\Gamma))$. Both map surjectively onto $\pi(\Gamma)$ with kernel $\Gamma(N)$, so by the first isomorphism theorem

$$\Gamma(N)\backslash\Gamma \simeq \pi_N(\Gamma) \simeq \Gamma(N)\backslash\Gamma'$$

Since $\Gamma \leq \Gamma'$, by the fourth isomorphism theorem we obtain $\Gamma(N)\backslash\Gamma \leq \Gamma(N)\backslash\Gamma'$, but they are isomorphic and finite so they must be equal. Thus, Φ is a bijection. □

Lemma 3.2.7. $H \cong H_1 \times H_2$

Proof. By Lemma 3.2.4, $\mathrm{SL}_2(\mathbb{Z}/N_1N_2\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N_2\mathbb{Z})$ and thus there is some $H' \leq \mathrm{SL}_2(\mathbb{Z}/N_1N_2\mathbb{Z})$ that is isomorphic to $H_1 \times H_2$. Specifically, for $A \in H'$, there is a unique $A_1 \times A_2 \in H_1 \times H_2$ such that $A \equiv A_i \pmod{N_i}$ and vis versa.

Well $\gamma \in \Gamma_1 \cap \Gamma_2 \iff \pi_{N_i}(\gamma) \in H_i (i = 1, 2) \iff \pi_{N_1N_2}(\gamma) \in H' \iff \gamma \in \pi_{N_1N_2}^{-1}(H')$

Thus, $\Gamma_1 \cap \Gamma_2 = \pi_{N_1N_2}^{-1}(H')$ and by Lemma 3.2.6 $H = H'$. □

The following lemma due to Diamond and Shurman shows that it suffices to think of cusps $\Gamma s \in \Gamma\backslash\mathbb{Q} \cup \{\infty\}$ as pairs $\pm\binom{a}{c} \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Lemma 3.2.8. *[4, Lemma 3.8.2, p.99] Let* $\binom{a}{c}, \binom{a'}{c'} \in \mathbb{Z}^2$ *such that* $\gcd(a,c) = \gcd(a',c') = 1$. *Then*

$$\binom{a}{c} = \gamma\binom{a'}{c'} \text{ for some } \gamma \in \Gamma(N) \iff \binom{a}{c} \equiv \pm\binom{a'}{c'} \pmod{N}$$

Furthermore, a pair $\binom{a}{c} \in (\mathbb{Z}/N\mathbb{Z})^2$ lifts to a pair $(a,c) \in \mathbb{Z}^2$ with $\gcd(a,c) = 1$ if and only if $\binom{a}{c}$ has additive order N in $(\mathbb{Z}/N\mathbb{Z})^2$ [4, Lemma 3.8.4], giving the following bijection

$$\Psi : \Gamma(N)\backslash(\mathbb{Q} \cup \{\infty\}) \to \left\{\binom{a}{c} \in (\mathbb{Z}/N\mathbb{Z})^2 : \binom{a}{c} \text{ has additive order } = N\right\}/\{\pm I\}.$$

For a congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of level N, define the group action of $H := \pi_N(\Gamma)$ on $\Gamma(N)\backslash(\mathbb{Q} \cup \{\infty\})$ by

$$\gamma\Gamma(N)x \mapsto \Psi^{-1}(\gamma\Psi(\Gamma(N)x))$$

Define the **projective line over** $\mathbb{Q}$ to be $\mathbb{P}^1(\mathbb{Q}) := \mathbb{Q} \cup \{\infty\}$.

Lemma 3.2.9. *Let* $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ *be a congruence subgroup of level* N. *Then the set of cusps of* $X(\Gamma)$ *is in bijection with the set of orbits of* H *acting on* $\Gamma(N)\backslash\mathbb{P}^1(\mathbb{Q})$ *where* $H = \pi_N(\Gamma) \leq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Proof. We construct a bijection $\rho : \Gamma\backslash\mathbb{P}^1(\mathbb{Q}) \to H\backslash(\Gamma(N)\backslash\mathbb{P}^1(\mathbb{Q}))$ defined by

$$\Gamma x \mapsto H\Gamma(N)x = \{h\Gamma(N)x : h \in H\}.$$

Since this is defined on representatives, we first must show that it is well defined. Let $\Gamma x = \Gamma x'$. We must show that $H\Gamma(N)x = H\Gamma(N)x'$. Since these are orbits, it suffices to show they have nonempty intersection. Thus, all we need to show is that $\Gamma(N)x = h\Gamma(N)x'$

for some $h \in H$. That is, if $\Psi(\Gamma(N)x) = \binom{a}{c}$ and $\Psi(\Gamma(N)x') = \binom{a'}{c'}$, then we must find h such that $\binom{a}{c} = h\binom{a'}{c'}$.

Well since $\Gamma x = \Gamma x'$, there exists $\gamma \in \Gamma$ such that $x = \gamma x'$. Reducing mod N, we get the relation that $\binom{a}{c} = \pi_N(\gamma)\binom{a'}{c'}$, and since $\pi_N(\gamma) \in H$, it must be that $H\binom{a}{c} = H\binom{a'}{c'}$ showing that ρ is well defined. Define ρ^{-1} by $H\Gamma(N)x \mapsto \Gamma x$. This is similarly well defined. If $H\Gamma(N)x = H\Gamma(N)x'$, then letting $x = a/c$ and $x' = a'/c'$ (with $\gcd(a, c) = \gcd(a', c') = 1$), there exists some $h \in H$ such that $\binom{\overline{a}}{\overline{c}} \equiv h\binom{\overline{a'}}{\overline{c'}}$, where $x \equiv \overline{x} \in \mathbb{Z}/N\mathbb{Z}$ for $x = a, b, a', c'$. By Lemma 3.2.8, $\binom{a}{c} = \alpha\gamma\binom{a'}{c'}$ where $\alpha \in \Gamma(N)$ and γ is a lift of h to Γ. Since $\alpha\gamma \in \Gamma$, $\binom{a}{c} = \gamma'\binom{a'}{c'}$ for some $\gamma' \in \Gamma$, and since the action of Γ on $\mathbb{Z}^2$ is identical to the action of Γ on $\mathbb{Q} \cup \{\infty\}$, it must be that $\Gamma x = \Gamma x'$.

Hence, ρ has a well defined inverse and is a bijection.

□

If we define $\Delta(N_1) = \Gamma(N_i)\backslash\mathbb{P}^1(\mathbb{Q})$, Lemma 3.2.9 reduces statement (b) of Theorem 3.2.1 to showing there is a bijection

$$H\backslash\Delta(N_1N_2) \to H_1\backslash\Delta(N_1) \times H_2\backslash\Delta(N_2)$$

where from here on $H := \pi_{N_1N_2}(\Gamma_1 \cap \Gamma_2)$.

Lemma 3.2.10. *If* $\gcd(N_1, N_2) = 1$*, then there is a bijection*

$$\Delta(N_1N_2) \to \Delta(N_1) \times \Delta(N_2)$$

Proof. Recall from Lemma 3.2.8 that there is a bijection

$$\Delta(N) \to A_N := \left\{ \begin{pmatrix} a \\ c \end{pmatrix} \in (\mathbb{Z}/N\mathbb{Z})^2 : \begin{pmatrix} a \\ c \end{pmatrix} \text{ has additive order} N \right\}$$

. Thus, it suffices to show that the equivalent sets $A_{N_1N_2}$ and $A_{N_1} \times A_{N_2}$ are in bijection. Clearly the map must be $\Phi\left(\binom{a}{c}\right) = \left(\binom{a}{c} \pmod{N_1}, \binom{a}{c} \pmod{N_2}\right)$. The well-definition of this map is partially satisfied by the CRT, so all we need to show is that Φ and Φ^{-1} preserves maximal additive order.

Let $\binom{a}{c} \in A_{N_1N_2}$. Let $\binom{a}{c}$ have order $k_1 \pmod{N_1}$ and $k_2 \pmod{N_2}$. Naturally, $k_i \mid N_i$ (implying $\gcd(k_1, k_2) = 1$). However, $k_1k_2\binom{a}{c} \equiv 0 \pmod{N_1N_2}$ so $N_1N_2 \mid k_1k_2 \mid N_1N_2$ implying $k_1k_2 = N_1N_2$. Thus, $\Phi(\binom{a}{c})$ has order $\operatorname{lcm}(k_1, k_2) = k_1k_2 = N_1N_2$, i.e. the maximal additive order in $A_{N_1} \times A_{N_2}$.

Now let $(\binom{a^*}{c^*}, \binom{a'}{c'}) \in A_{N_1} \times A_{N_2}$. By the CRT, there is a unique $\binom{a}{c} \in (\mathbb{Z}/N_1N_2\mathbb{Z})^2$ satisfying the respective modulo requirements mod N_1 and N_2 respectively. We must show that $\binom{a}{c}$ has additive order N_1N_2. Let $\mid \binom{a}{c} \mid = k \leq N_1N_2$. Then $k\binom{a^*}{c^*} \equiv 0 \pmod{N_1}$ and similarly with N_2. Then $N_1, N_2 \mid k$, but $0 < k \leq N_1N_2$ so by the CRT, $k = N_1N_2$.

Thus, Φ is well-defined with well-defined inverse, and is therefore a bijection. □

Armed with these lemmas, we are ready to prove statements (a), (b), and (c) of Theorem 3.2.1.

Proof. Let d be the degree of $\Gamma_1 \cap \Gamma_2$. Then the following holds:

$$
\begin{aligned}
d &= [\mathrm{SL}(\mathbb{Z}) : (\Gamma_1 \cap \Gamma_2)] \\
&= [\mathrm{SL}_2(\mathbb{Z}/N_1N_2\mathbb{Z}) : H] && \text{4th Isomorphism Theorem} \\
&= [\mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N_2\mathbb{Z}) : H_1 \times H_2] && \text{Lemmas 3.2.4 and 3.2.7} \\
&= [\mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) : H_1][\mathrm{SL}_2(\mathbb{Z}/N_2\mathbb{Z}) : H_2] \\
&= [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1][\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2] && \text{4th Isomorphism Theorem} \\
&= d_1d_2
\end{aligned}
$$

And thus statement (a) is proven.

For statement (b), by Lemma 3.2.9, it is sufficient to show the sets $H\backslash\Delta(N_1N_2)$ and $H_1\backslash\Delta(N_1) \times H_2\backslash\Delta(N_2)$ are in bijection. Once again, we consider $\Delta(N)$ as $A_N = \{\binom{a}{c} \in (\mathbb{Z}/N\mathbb{Z}) : \binom{a}{c}$ has additive order $= N\}$.

Define $\Psi : H\backslash A_{N_1N_2} \to H_1\backslash A_1 \times H_2\backslash A_2$ by

$$\Psi\Big(H\begin{pmatrix}a\\c\end{pmatrix}\Big) = (H_1 \times H_2)\Phi\Big(\begin{pmatrix}a\\c\end{pmatrix}\Big) = \Big(H_1\begin{pmatrix}a_1\\c_1\end{pmatrix}, H_2\begin{pmatrix}a_2\\c_2\end{pmatrix}\Big)$$

Where $a, c \equiv a_i, c_i \pmod{N_i}$. Now we must show this map is well defined.

$$\begin{aligned}
&H\begin{pmatrix}a\\c\end{pmatrix} = H\begin{pmatrix}a'\\c'\end{pmatrix}\\
\iff &\exists h \in H : \begin{pmatrix}a\\c\end{pmatrix} \equiv h\begin{pmatrix}a'\\c'\end{pmatrix} \pmod{N_1N_2}\\
\iff &\begin{pmatrix}a\\c\end{pmatrix} \equiv h\begin{pmatrix}a'\\c'\end{pmatrix} \pmod{N_i} && (i = 1, 2)\\
\iff &H_i\begin{pmatrix}a\\c\end{pmatrix} = H_i\begin{pmatrix}a'\\c'\end{pmatrix} && (i = 1, 2)\\
\iff &(H_1 \times H_2)\Phi\Big(\begin{pmatrix}a\\c\end{pmatrix}\Big) = (H_1 \times H_2)\Phi\Big(\begin{pmatrix}a'\\c'\end{pmatrix}\Big)
\end{aligned}$$

Following the logic backwards we also see that Ψ^{-1} is similarly well defined, and thus we get our desired bijection, proving (b).

For a general congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, since all congruence subgroups are of finite index, there exists representative $\{\gamma_j\}_{j=1}^n$ such that $\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=1}^n \Gamma\gamma_j$. Since the single order 2 elliptic point of $X(1)$ is $\mathrm{SL}_2(\mathbb{Z})i$, the possible order 2 elliptic points of $X(\Gamma)$ are $\{\Gamma\gamma_j i\}$. Of course, $\Gamma\gamma_j i$ is only an elliptic point of $X(\Gamma)$ if and only if γ_j has nontrivial stabilizer in Γ. That is, if $S := \begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}$ (the matrix that generates $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(i)$), $\Gamma\gamma_j i$ is elliptic in $X(1) \iff \gamma_j S\gamma_j^{-1} \in \Gamma \iff \gamma_j S \in \Gamma\gamma_j$. In fact, S induces a permutation $\sigma \in S_n$ on the set $\{\gamma_j\}_{j=1}^n$ given by $\sigma(\gamma_j) = \gamma_{j'}$ where $\gamma_j S \in \Gamma\gamma_{j'}$, and thus the number of order 2 elliptic points of $X(\Gamma)$ is given by the number of fixed points of σ.

Furthermore, letting $H := \pi_N(\Gamma)$ (where Γ is of level N), by the fourth isomorphism theorem, $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \bigsqcup_{j=1}^{n} H\overline{\gamma_j}$ where $\overline{\gamma_j} = \pi_N(\gamma_j)$. We conclude that $\overline{S} := \pi_N(S)$ induces an identical permutation on the set $\{\overline{\gamma_j}\}_{j=1}^{n}$, since if $\gamma_j S \in \Gamma\gamma_{j'}s$, then

$$\overline{\gamma_j}\overline{S} = \pi_n(\gamma_j S) \in \pi_N(\Gamma\gamma_{j'}) = H\overline{\gamma_{j'}}$$

Thus, it suffices to count fixed points of the identical permutation induced by $\overline{S}$ on $\{\overline{\gamma_j}\}_{j=1}^{n}$.

We now specialize $\Gamma = \Gamma_1 \cap \Gamma_2$ Let $S_1 := \pi_{N_1}(S)$ and $S_2 := \pi_{N_2}(S)$. Label the decompositions

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=1}^{n_1} \Gamma_1\alpha_i = \bigsqcup_{k=1}^{n_2} \Gamma_2\beta_k$$

with representatives $\alpha_i, \beta_k \in \mathrm{SL}_2(\mathbb{Z})$. Then again by the fourth isomorphism theorem,

$$\mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N_2\mathbb{Z}) = \bigsqcup_{i=1}^{n_1}\bigsqcup_{k=1}^{n_2} H_1 \times H_2(\overline{\alpha_i}, \overline{\beta_k})$$

where $\overline{\alpha_i} := \pi_{N_1}(\alpha_i)$ and $\overline{\beta_k} := \pi_{N_2}(\beta_k)$. Like in the general case, S_1 and S_2 induce permutations on $\{\overline{\alpha_i}\}_{i=1}^{n_1}$ and $\{\overline{\beta_k}\}_{k=1}^{n_2}$ respectively, and thus (S_1, S_2) induces a permutation on $\{(\overline{\alpha_i}, \overline{\beta_k})\}$ for $1 \le i \le n_1$ and $1 \le k \le n_2$. Let $F : H \xrightarrow{\sim} H_1 \times H_2$ be the isomorphism guaranteed from Lemma 3.2.7. Note that F is a restriction of the isomorphism $\mathrm{SL}_2(\mathbb{Z}/N_1N_2\mathbb{Z}) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N_2\mathbb{Z})$, and thus

$$\mathrm{SL}_2(\mathbb{Z}/N_1N_2\mathbb{Z}) = \bigsqcup_{i=1}^{n_1}\bigsqcup_{k=1}^{n_2} HF((\overline{\alpha_i}, \overline{\beta_k}))$$

Suppose for some fixed i, k, that $(\overline{\alpha_i}, \overline{\beta_k})(S_1, S_2) \in H_1 \times H_2(\overline{\alpha_{i'}}, \overline{\beta_{k'}})$. Then

$$F((\overline{\alpha_i}, \overline{\beta_k}))\overline{S} = F((\overline{\alpha_i}, \overline{\beta_k})(S_1, S_2)) \in F(H_1 \times H_2(\overline{\alpha_{i'}}, \overline{\beta_{k'}})) = HF((\overline{\alpha_{i'}}, \overline{\beta_{k'}}))$$

Therefore, the number of fixed points of the permutation induced by $\overline{S}$ acting on the coset representatives $F((\overline{\alpha_i}, \overline{\beta_k}))$ for $1 \leq i \leq n_1$ and $1 \leq k \leq n_2$ is the same as the number of fixed points of the permutation induced by (S_1, S_2) acting on $\{((\overline{\alpha_i}, \overline{\beta_k})\}$ for $1 \leq i \leq n_1$ and $1 \leq k \leq n_2$, which is in turn equal to the product of the number of fixed points of S_1 permuting $\{\overline{\alpha_i}\}_{i=1}^{n_1}$ and the number of fixed points of S_2 permuting $\{\overline{\beta_k}\}_{k=1}^{n_2}$. Therefore, the number of elliptic points of order 2 is indeed multiplicative in Γ_i. An identical proof for order 3 elliptic points works, examining possible candidates $\{\Gamma\gamma_j e^{2\pi i/3}\}_{j=1}^{n}$, replacing S with $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

We can finally conclude that when the levels of two congruence subgroups are relatively prime, the degree, number of cusps, and number of elliptic points of order 2 and 3 of their intersection are multiplicative.

□

Chapter 4

Results and calculations

Section 4.1

The Degree of $\Gamma_C(N)$

Recall that if $C \leq (\mathbb{Z}/N\mathbb{Z})^\times$, then

$$\Gamma_C(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \pmod{N}, a \in C \right\}$$

is a congruence subgroup of level N. We are interested in calculating the genera of $X(\Gamma_C(N))$ and various intersections. Key to calculating the genus is the degree, i.e. the projective index of $\Gamma_C(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Since all congruence subgroups are of finite index,

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_C(N)] = \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)]}{[\Gamma_C(N) : \Gamma_1(N)]} \tag{4.1.1}$$

By the fourth isomorphism theorem,

$$[\Gamma_C(N) : \Gamma_1(N)] = [\Gamma(N)\backslash\Gamma_C(N) : \Gamma(N)\backslash\Gamma_1(N)] = [\pi_N(\Gamma_C(N)) : \pi_N(\Gamma_C(N)]$$

Since $\pi_N(\Gamma_C(N)) = \left\{ \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} : a \in C \right\}$ maps surjectively onto C with kernel $\Gamma_1(N)$ by $\begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \mapsto a$, we get by the first isomorphism theorem:

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_C(N)] = \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)]}{\mid C \mid} \tag{4.1.2}$$

We can calculate $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)]$ via a similar trick. Again by the finite indices of congruence subgroups,

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]}{[\Gamma_1(N) : \Gamma(N)]}$$

But $\Gamma(N)$ is the kernel of the surjective map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, as well as the kernel of $\Gamma_1(N) \to (\mathbb{Z}/N\mathbb{Z})$ given by $\begin{pmatrix} 1+AN & b+BN \\ CN & 1+DN \end{pmatrix} \mapsto b$. Thus,

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = \frac{\mid \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \mid}{N} = N^2 \prod_{p \mid N} (1 - \frac{1}{p^2})$$

Thus,

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_C(N)] = \frac{N^2 \prod_{p \mid N} (1 - \frac{1}{p^2})}{\mid C \mid} \tag{4.1.3}$$

Without loss of generality, we can assume $-I \in \Gamma_C(N)$, and thus the degree is precisely the index.

Section 4.2

Elliptic points of $\Gamma_C(N)$

We are also interested in finding the elliptic points, i.e. $\Gamma\tau \in X(\Gamma)$ such that there exists $\gamma \in \mathrm{Stab}_\Gamma(\tau)$ with $\gamma \notin \{\pm I\}$. Since we are primarily interested in torsion-free congruence subgroups, it suffices to derive a method merely to test whether a modular curve has elliptic points or not.

The following theorem will be necessary for this discussion. Given that our focus is on torsion-free congruence subgroups, detailed proofs have been omitted, but a fair treatment cab be found in [4, p.54-55]

Theorem 4.2.1. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. Then:*

- *$X(\Gamma)$ has an elliptic point of order 2 $\iff$ $\exists \gamma \in \Gamma$ such that $\gamma^4 = I$ $\iff$ $\exists \gamma \in \Gamma$ such that $\gamma = \alpha \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \alpha^{-1}$.*
- *$X(\Gamma)$ has an elliptic point of order 3 $\iff$ $\exists \gamma \in \Gamma$ such that $\gamma^3 = I$ $\iff$ $\exists \gamma \in \Gamma$ such that $\gamma = \alpha \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \alpha^{-1}$.*

Thus, the existence of elliptic points in $X(\Gamma)$ is determined by the conjugates of the two matrices given above in Γ. Furthermore, since the characteristic polynomial of $\gamma \in \Gamma_C(N)$ reduces to $(x-\alpha)(x-\alpha^{-1}) = x^2 - (\alpha+\alpha^{-1})x + 1 \pmod N$ for some $\alpha \in \mathbb{C} \leq (\mathbb{Z}/N\mathbb{Z})^\times$, we get the following theorem

Corollary 4.2.2. *Let $\Gamma_C(N)$ be an intermediate congruence subgroup of level N. Then $X(\Gamma_C(N)$ has*

(a) *no period 3 elliptic points $\iff$ no $\alpha \in C$ satisfies $\alpha^2 + 1 \equiv 0 \pmod N$*

(b) *no period 3 elliptic points $\iff$ no $\alpha \in C$ satisfies $\alpha^2 + \alpha + 1 \equiv 0 \pmod N$*

Proof. For the reverse direction, note that $\alpha^2 \equiv -1 \pmod N$ implies $\alpha + \alpha^{-1} \equiv 0 \pmod N$. If no such α exists, then no $\gamma \in \Gamma_C(N)$ could have characteristic polynomial $x^2+1 \pmod N$, and thus cannot be equal to x^2+1 directly.

For the forward direction, we show the contrapositive. Suppose there exists $\alpha \in C$ such that $\alpha^2 \equiv -1 \pmod N$. This is equivalent to α having multiplicative order 4. By [4, Prop 3.7.1] elliptic points of order 2 in $\Gamma_0(N)$ are in bijection with ideals J of $\mathbb{Z}[i]$ such that $\mathbb{Z}[i]/J \simeq \mathbb{Z}/N\mathbb{Z}$, or in other words, surjective homomorphisms from $\mathbb{Z}[i]$ onto $\mathbb{Z}/N\mathbb{Z}$. Since

ring homomorphisms are determined by the image of the generators, we only need to specify where i goes. However, ring homomorphisms preserve order, so i must map to an order 4 element. In fact, the number of such surjective homomorphisms is exactly the number of order 4 elements in $(\mathbb{Z}/N\mathbb{Z})^\times$, since $\mathbb{Z}[i]$ clearly surjects to $\mathbb{Z}/N\mathbb{Z}$, so the only thing that we need to check for a homomorphism is that the relation on $i^2 = -1$ is satisfied, which is equivalent to the the image of i having order 4. Thus, for each element a of order 4 in $(\mathbb{Z}/N\mathbb{Z})^\times$, the subset $\left\{ \begin{pmatrix} a & * \\ 0 & a^{-1} \end{pmatrix} \right\} \subset \pi_N(\Gamma_0(N))$ guarantees a lift to a $\gamma \in \Gamma_0(N)$ with order 4. Thus, since $\Gamma_C(N) \leq \Gamma_0(N)$, if there exists $\alpha \in C$ of order 4, similarly there is a lift in $\Gamma_C(N)$ to a matrix of order 4, and thus $\Gamma_C(N)$ has an elliptic point of period 2, proving (a).

The proof for (b) is nearly identical, once we see that $\alpha^2 + \alpha + 1 \equiv 0$ implies $\alpha^3 \equiv 1$, and therefore α has order 3. (The one caveat is that since $-I \in \Gamma_0(N)$ for all N, we actually count elements of order 6, which is implied by $\alpha^2 - \alpha + 1 \equiv 0$. However, for each such α, α^2 has order 3, thus it suffices to check for order 3 elements). □

Section 4.3

Cusps of $\Gamma_C(N)$

To understand what the cusps of $\Gamma_C(N)$ are, it is helpful to first understand the cusps of $\Gamma_1(N)$. Like before, the cusps of a congruence subgroup can be viewed as pairs $\binom{x}{y} \in (\mathbb{Z}/N\mathbb{Z})^2$ with $\mathrm{SL}_2(\mathbb{Z})$ acting by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

mimicking the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{Q} \cup \{\infty\}$. This follows from the fact that every congruence subgroup contains $\Gamma(N)$ for some N, and Lemma 3.2.7.

In the case of $\Gamma_1(N)$, some of these pairs are identified.

Lemma 4.3.1. *Let $s = a/c, = a'/c' \in \mathbb{Q} \cup \{\infty\}$ with $\gcd(a, c) = \gcd(a', c') = 1$. Then*

$$\Gamma_1(N)s = \Gamma_1(N)s' \iff \begin{pmatrix} a \\ c \end{pmatrix} \equiv \pm \begin{pmatrix} a + jc \\ c \end{pmatrix} \pmod{N}$$

for some $j \in \mathbb{Z}$.

Proof. See [4, Prop 3.8.3]. □

Thus, given a lower entry c, the upper entry is determined modulo c. In fact, factoring in the condition that $\gcd(a, c, N) = 1$, we see that a is determined modulo $d := \gcd(c, N)$.

Lemma 4.3.2. *The map $f : \{c \in \mathbb{Z}/N\mathbb{Z} : \gcd(c, N) = d\} \to (\mathbb{Z}/(N/d)\mathbb{Z})^\times$ given by $c \mapsto c/d$ is a bijection.*

Proof. First we note that if $\gcd(c, N) = d$, then $\gcd(c/d, N/d) = 1$ so the map is well-defined. Suppose $c/d \equiv c'/d \pmod{N/d}$. Then there exists an integer j such that

$$c/d = c'/d + jN/d$$

or equivalently

$$c = c' + jN \iff c \equiv c' \pmod{N}$$

thus f is injective. Furthermore, given $\alpha \in (\mathbb{Z}/(N/d)\mathbb{Z})^\times$, we can lift α to $d\alpha \in \mathbb{Z}/N\mathbb{Z}$. Letting $x = \gcd(d\alpha, N)$, we see that $d \mid x$, so $(x/d) \mid \alpha$ and $(x/d) \mid (N/d)$, implying $x/d = 1 \Rightarrow x = d$. Thus, f surjects as well and is a bijection. □

It follows from Lemma 4.3.2 that the number of $c \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(c, N) = d$ is equal to $\phi(N/d)$ where ϕ is Euler's totient. For each such c, there are $\phi(d)$ unique a modulo c satisfying $\gcd(a, d) = 1$. Thus, there are $\sum_{d|N} \phi(d)\phi(N/d)$ viable representatives.

Of course, we cannot forget that cusps are pairs $\pm\binom{a}{c}$, thus if N is odd, each cusp is repeated twice, and we divide the sum above by 2 to get the total number of cusps. If N

is even, then each cusp $\binom{a}{c}$ with $c < N/2$ is matched with $-\binom{a}{c}$ (where $-c > N/2$). For $c = N/2$, for all $N > 4$, $\phi(N/2)$ is even, and thus $\binom{a}{c}$ is matched with $\binom{-a}{c}$.

Theorem 4.3.3. *For all $N \neq 1, 2, 4$, $\epsilon_\infty(\Gamma_1(N)) = \frac{1}{2}\sum_{d|N} \phi(d)\phi(N/d)$*

Proof. As described above, the cusps are given by

$$\Gamma_1(N)\backslash\mathbb{Q} \cup \{\infty\} \leftrightarrow \Big(\bigcup_{d|N} \bigcup_{\gcd(c,N)=d} \bigcup_{a\in(\mathbb{Z}/d\mathbb{Z})^\times} \binom{a}{c}\Big)/\{\pm 1\}.$$

□

We are nearly ready to talk about the cusps of $\Gamma_C(N)$. We first need to understand how $\Gamma_C(N)$ acts on $\mathbb{Q} \cup \{\infty\}$.

Note that for a given matrix $\gamma = \begin{pmatrix} x + aN & y + bN \\ cN & x^{-1} + dN \end{pmatrix} \in \Gamma_C(N)$ with $x, x^{-1} \in C \leq (\mathbb{Z}/N\mathbb{Z})^\times$, the matrix $\gamma' = \begin{pmatrix} 1 & -yx^{-1} \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$ has the property that $\gamma'\gamma \equiv \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \pmod N$. Thus, each coset of $\Gamma_1(N)\backslash\Gamma_C(N)$ has a representative that is a diagonal matrix modulo N. Furthermore, $\Gamma_1(N)$ fixes the upper left and lower right coordinates modulo N, so each such diagonal matrix represents a unique coset. To summarize,

$$\Gamma_C(N) = \bigcup_{x\in C} \Gamma_1(N)\gamma_x$$

where $\gamma_x \equiv \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \pmod N$. Thus, for a given $s \in \mathbb{Q} \cup \{\infty\}$,

$$\Gamma_C(N)s = \bigcup_{x\in C} \Gamma_1(N)\gamma_x s$$

Thus, to understand the cusps of $\Gamma_C(N)$, it suffices to know how $\Gamma_1(N)\gamma_x$ acts on s, or equivalently, how γ_x acts on $\Gamma_1(N)s$. We first note that $xa \equiv x'a \pmod d \iff x \equiv x' \pmod d$. Thus, for a given cusp of $\Gamma_1(N)$ represented by $\binom{a}{c} \in (\mathbb{Z}/N\mathbb{Z})^2$ with $\gcd(c, N) = d$,

the size of the orbit is given by the number of unique $x \in \pi_d(C)/\{\pm 1\}$ where $\pi_d : (\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$ is given by reduction modulo d. From this, we conclude that for each $d \mid N$, the size of the orbit of a cusp with bottom coordinate c such that $\gcd(c, N) = d$ is $|\pi_d(C)|\delta$ where $\delta = 1/2$ if $-1 \in \pi_d(C)$ and 1 if not. Assuming without loss of generality $-1 \in C$, and therefore in $\pi_d(C)$ for all $d \mid N$. Then we can finally conclude for $\Gamma_C(N)$, that

$$\epsilon_\infty = \sum_{d|N} \frac{\phi(d)\phi(N/d)}{|\pi_d(C)|} \tag{4.3.4}$$

Section 4.4

Genera of intermediate modular curves and their intersections

Csirik, Wetherall, and Zieve showed that the genera achieved by modular curves of the form $X_0(N)$ make up a density 0 subset of the integers [3, p.1]. Now that we know how to calculate the degree, cusps, and existence of elliptic points for intermediate congruence subgroups, we might feel inclined to show something similar. Some quick calculations appear to show a very different story. In fact, the first genus not achieved by a torsion-free intermediate congruence subgroup is 138. We show the slightly stronger result:

Theorem 4.4.1. *There is no smooth genus 138 modular curve of the form* $\Gamma(N_1) \cap \Gamma_C(N_2)$ *with* $\gcd(N_1, N_2) = 1$.

Proof. Using the theorems we have established so far, this is something we can exhaustively check using SageMath. First, we bound the level of congruence subgroups we must check. Using Theorem 3.1.1, we find that $\Gamma_0(N)$ (and by Riemann-Hurwitz, $\Gamma_C(N)$) has genus greater than 138 for $N \geq 1881$. Thus, we only have to check intermediate congruence subgroups up $N = 1880$. Furthermore, we can bound the genus of $\Gamma(N)$ (very crudely, using

the formula for the degree and cusps of $\Gamma(N)$ in [4, p.107]). When $N \geq 6$,

$$g(\Gamma(N)) = 1 + \frac{1}{2}N^2 \prod_{p|N}(1 - \frac{1}{p^2})(\frac{N}{12} - \frac{1}{2}) \geq 1 + \frac{1}{2}N(\frac{N}{12} - \frac{1}{2}) = \frac{N^2}{24} - \frac{N}{4} + 1 \qquad (4.4.2)$$

We compute directly that $g(\Gamma(N)) = 0$ for $1 \leq N \leq 5$. Hence, we only have to check $\Gamma(N)$ up to $N = 43$.

We can use code B.1 and B.2 in appendix B to generate the necessary data. Code B.3 generates the data for intermediate congruence subgroups up to level $N = 1880$. Then finally, using Corollary 3.2.2, Code B.4 calculates all possible genera of intersections:

Since 138 does not appear in the output of code B.4 ran with principal data up to level 44 and intermediate data up to level 1880, there can be no such modular curve. □

By applying the above method to all genera up to 500, we see that intermediate congruent subgroups achieve $\sim 96\%$ of genera up to 500, missing only 22 integers.

Section 4.5

Congruence subgroups of intersection type

Lemma 3.2.6 gives a bijection between congruence subgroups containing $\Gamma(N)$ and subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for a given N. Furthermore, the fourth isomorphism theorem, Lemma 3.2.8, and the proof of statement (c) of Theorem 3.2.1 show that the data for calculating the degree and number of cusps and elliptic points is all determined by the subgroup H. Since H is finite, in theory all of these values can be calculated by established group theory. However, even calculating the subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ can quickly become computationally infeasible, especially for composite N.

Luckily, for prime and relatively small prime power N, such computations are doable. Thus, by utilizing Theorem 3.2.1, we can quickly calculate large amounts of genera. This

motivates the following definition.

Definition 4.5.1. A congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of level N is of **intersection type** if $\pi_N(\Gamma) \simeq \prod_{i=1}^n H_i$ where each $H_i \leq \mathrm{SL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$ for distinct primes p_i.

We might wonder how to calculate the elliptic points and cusps of a general congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$. In the case of elliptic points, the proof of statement (c) of Theorem 3.2.1 already tells us. To recap, Letting $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, the matrix that generates $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(i)$, S induces a permutation σ on the set of coset representatives $\{\gamma_j\}_{j=1}^n$ where $\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{j=1}^n \Gamma\gamma_j$. The permutation is defined by $\sigma(\gamma_j) = \gamma_{j'}$ where $\gamma_j S \in \Gamma\gamma_{j'}$, The number of order 2 elliptic points is given by the number of fixed points of σ. Similarly, letting $A := \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, the generator of $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(e^{2\pi i/3})$, A induces a similar permutation whose fixed points again give us the number of order 3 elliptic points.

In the case of cusps, we are interested in the set of pre-images of ∞ under the map $X(\Gamma) \to X(1)$, given by $\{\Gamma\gamma_j\infty\}_{j=1}^r$. Of course, some of these may not be distinct. Thus, we must check when $\Gamma\gamma_a\infty = \Gamma\gamma_b\infty$, which is true if and only if there exists $\alpha \in \Gamma$ such that $\alpha\gamma_a\infty = \gamma_b\infty \iff \gamma_b^{-1}\alpha\gamma_a\infty = \infty$. Letting $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (the matrix that generates $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$), $\gamma_b^{-1}\alpha\gamma_a\infty = \infty$ is true if and only if

$$\gamma_b^{-1}\alpha\gamma_a \in \langle T \rangle$$

which in turn is true if and only if, $\Gamma\gamma_a = \Gamma\gamma_b T^n$ for some $n \in \mathbb{N}$. Thus, by counting the orbits of $\langle T \rangle$ acting on $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$ we can count the number of elliptic points.

The Magma code B.5 in the appendix utilizes the above ideas to calculate the genus of a general congruence subgroup of prime-power level, although it works in general for any congruence subgroup. We restrict to prime-power level primarily due to computational concerns. $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ has many more subgroups for highly composite N, and even trying to calculate the subgroups of $\mathrm{SL}_2(\mathbb{Z}/128\mathbb{Z})$ can take nearly an hour on the average laptop.

However, we can calculate the degree, elliptic points, and cusps for all congruence subgroups of prime power level less than 100 in roughly 30 minutes.

Theorem 4.5.2. *There is a smooth modular curve for every genus* $0 \leq g < 500$.

Proof. We use our established methods for intermediate congruence subgroups to knock off most of the genera, and then we can search through intersection type for the rest. See Appendix A for a list of smooth modular curves with genus up to 500. □

Chapter 5

Future work

Alan Reid's question is still very much open. The results in this paper may suggest that there is a smooth modular curve of every genus, but the answer is still far from conclusive. Future work may hope to answer the some of following questions.

Csirik, Wetherall, and Zieve prove in there paper that the density $S(x)/x$ where $S(x)$ is the number of genera achieved by modular curves of the form $X_0(N)$ (any, not just torsion-free) up to x approaches 0 as x tends to infinity. Given that there are vastly more intermediate congruence subgroups that Γ_0 congruence subgroups, there is no guarantee that intermediate congruence subgroups only make up a 0% density of possible genera, especially considering they make up a whopping $\sim 95\%$ of genera up to 500.

A frequency analysis of what genera up to 500 are hit by intermediate congruence subgroups may give us some insight. We can also look at specifically even and odd frequencies. It's clear immediately that, like $X_0(N)$, odd genera are hit with much higher frequency on average than even genera. This leads us to make the following conjecture:

Conjecture 5.0.1. *The set of even genera achieved by modular curves of the form $X(\Gamma_C(N))$ where $\Gamma_C(N)$ is a torsion-free intermediate congruence subgroup make up a density 0 subset of the even integers*

Figure 5.1: Frequency of genera up to 500 achieved by intermediate congruence subgroups

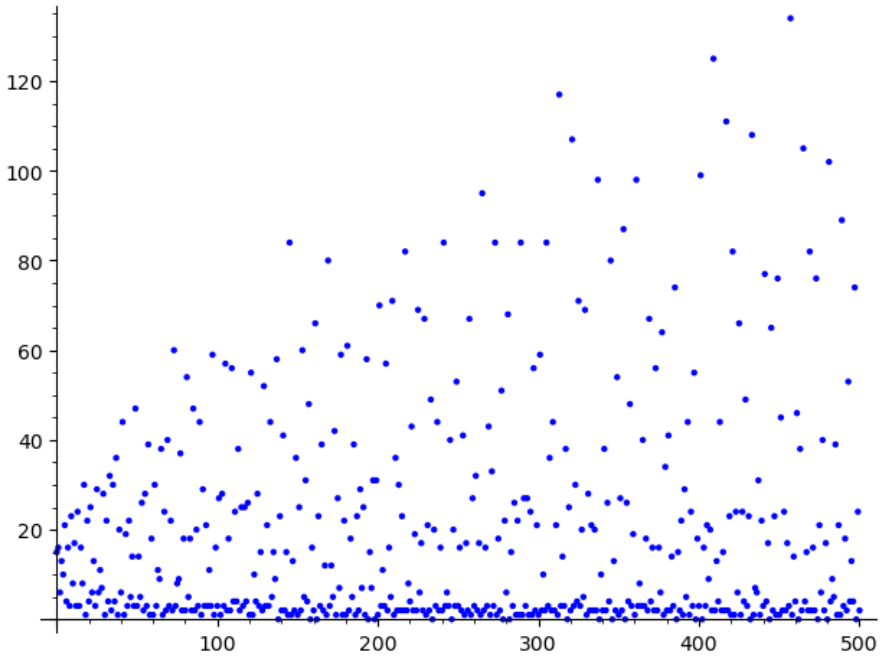


Figure 5.2: Frequency of odd genera up to 500 achieved by intermediate congruence subgroups

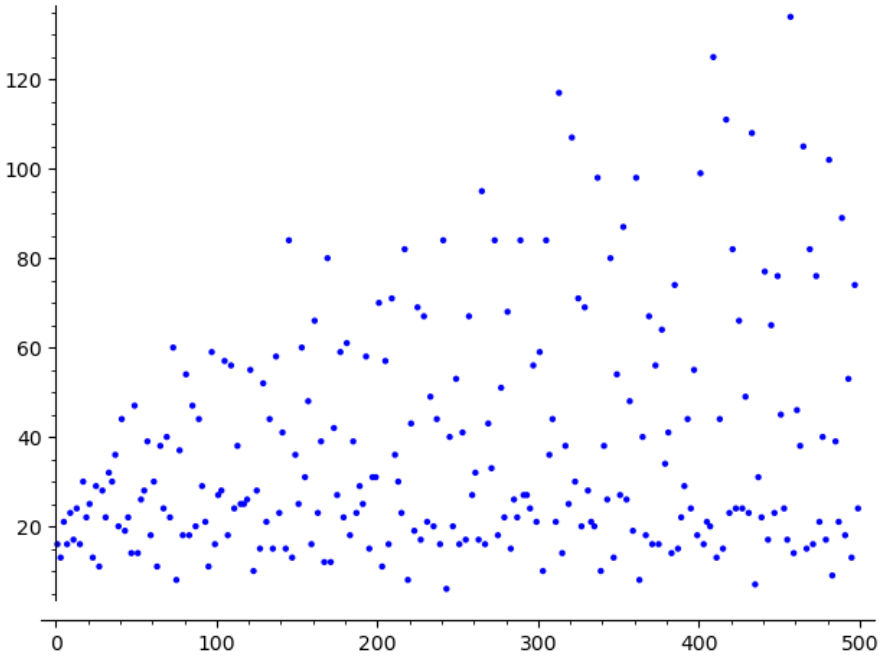
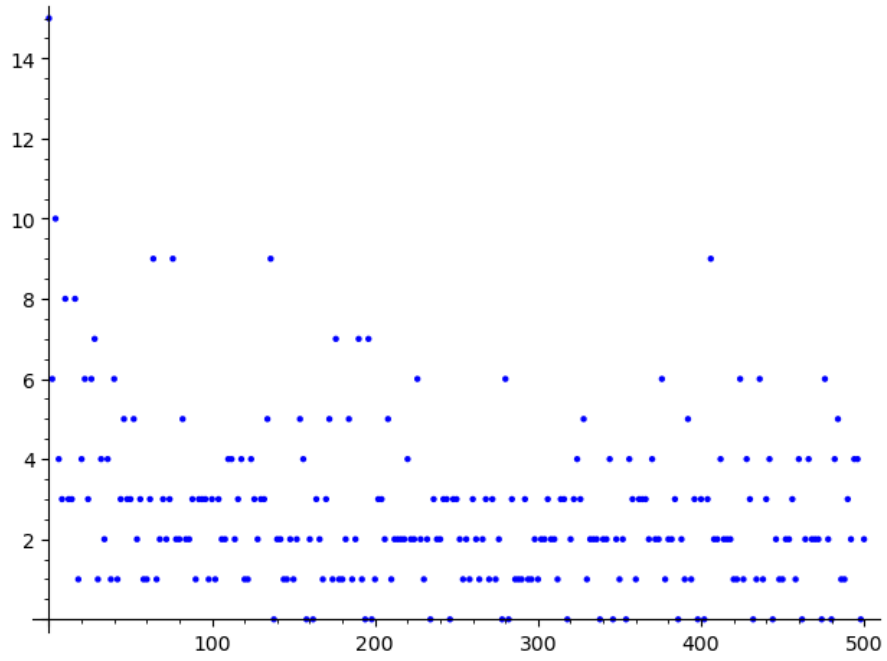


Figure 5.3: Frequency of even genera up to 500 achieved by intermediate congruence subgroups



It is difficult to say what density of the odd integers that intermediate congruence subgroups achieve, although given that the frequency with which odd genera are hit does not unanimously increase with the genera, it may be that at least some odd genera are missed.

We can ask the same questions about congruence subgroups of intersection type, although it is much more difficult to exhaustively check. While we can still bound the genus by the level of a general congruence subgroup due to a proof from Cox and Parry [2], to check frequency of genera hit up to 100 would require checking all congruence subgroups of prime power level up to ~ 1800, a task that is likely computationally infeasible for the average computer.

If intermediate and intersection-type subgroups are indeed insufficient for achieving all genera, we may also look at other families of congruence subgroups. Asher Auel and Eran

Assaf suggested looking at congruence subgroups of the form

$$\Gamma_{C,B}(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod{N}, a \in C \leq (\mathbb{Z}/N\mathbb{Z})^\times, b \in B \leq \mathbb{Z}/N\mathbb{Z} \right\}$$

where to make this a closed subgroup we mandate that $CB = B$. If we could quickly calculate the degree, elliptic points, and cusps of these congruence subgroups, perhaps it would expand the family of intermediate congruence subgroups enough to hit all genera, or at least all odd genera.

However, at the end of the day, we may have to look for something deeper than investigating families of congruence subgroups. It may be that no easily describable family, or set of families, encompasses all genera. If this is the case, then it may take a more creative approach to definitively answer Alan Reid's question. Even if it were not true, since all genera are achieved up to 500, it could very likely be infeasible to computationally prove that a certain genus is not hit.

Appendix A

Data tables

Table A.1: Genera up to 500 achieved by a modular curve of the form $X(\Gamma_C(N))$ where $\Gamma_C(N)$ is torsion-free. Each $\Gamma_C(N)$ presented is of the smallest level where such a subgroup occurs.
Missing genera: [138, 158, 162, 194, 198, 234, 246, 278, 282, 318, 338, 346, 354, 386, 398, 402, 432, 444, 462, 474, 480, 498]

0	$\Gamma_0(4)$	1	$\Gamma_0(11)$	2	$\Gamma_C(13)-[12]$	3	$\Gamma_C(20)-[19]$
4	$\Gamma_C(26)-[17]$	5	$\Gamma_C(17)-[16]$	6	$\Gamma_C(22)-[21]$	7	$\Gamma_C(19)-[18]$
8	$\Gamma_C(44)-[35]$	9	$\Gamma_C(30)-[29]$	10	$\Gamma_C(26)-[25]$	11	$\Gamma_C(33)-[10,23]$
12	$\Gamma_C(23)-[22]$	13	$\Gamma_C(27)-[26]$	14	$\Gamma_0(118)$	15	$\Gamma_C(60)-[7,11]$
16	$\Gamma_C(44)-[21,23]$	17	$\Gamma_C(32)-[31]$	18	$\Gamma_C(79)-[27]$	19	$\Gamma_C(48)-[41,47]$
20	$\Gamma_C(92)-[51]$	21	$\Gamma_C(33)-[32]$	22	$\Gamma_C(29)-[28]$	23	$\Gamma_C(84)-[19,29]$
24	$\Gamma_C(103)-[22]$	25	$\Gamma_C(35)-[34]$	26	$\Gamma_C(31)-[30]$	27	$\Gamma_C(89)-[11]$
28	$\Gamma_C(38)-[37]$	29	$\Gamma_C(60)-[19,41]$	30	$\Gamma_0(359)$	31	$\Gamma_C(56)-[13,55]$
32	$\Gamma_C(197)-[4]$	33	$\Gamma_C(39)-[38]$	34	$\Gamma_0(278)$	35	$\Gamma_C(80)-[13,79]$
36	$\Gamma_C(44)-[43]$	37	$\Gamma_C(48)-[47]$	38	$\Gamma_0(316)$	39	$\Gamma_C(90)-[37,71]$
40	$\Gamma_C(37)-[36]$	41	$\Gamma_C(45)-[44]$	42	$\Gamma_0(503)$	43	$\Gamma_C(57)-[20,37]$
44	$\Gamma_C(188)-[19]$	45	$\Gamma_C(46)-[45]$	46	$\Gamma_C(74)-[11]$	47	$\Gamma_C(153)-[35,37]$
48	$\Gamma_C(50)-[49]$	49	$\Gamma_C(63)-[8,55]$	50	$\Gamma_C(169)-[64]$	51	$\Gamma_C(41)-[40]$
52	$\Gamma_C(54)-[53]$	53	$\Gamma_C(93)-[23]$	54	$\Gamma_C(223)-[27]$	55	$\Gamma_C(52)-[51]$
56	$\Gamma_C(236)-[179]$	57	$\Gamma_C(43)-[42]$	58	$\Gamma_C(172)-[87,113]$	59	$\Gamma_C(217)-[33,216]$
60	$\Gamma_0(719)$	61	$\Gamma_C(56)-[55]$	62	$\Gamma_0(502)$	63	$\Gamma_C(201)-[68,109]$
64	$\Gamma_C(76)-[37,39]$	65	$\Gamma_C(51)-[50]$	66	$\Gamma_C(124)-[37,63]$	67	$\Gamma_C(69)-[22,47]$
68	$\Gamma_C(284)-[7]$	69	$\Gamma_C(49)-[48]$	70	$\Gamma_C(47)-[46]$	71	$\Gamma_C(110)-[23,109]$
72	$\Gamma_C(298)-[153]$	73	$\Gamma_C(75)-[26,49]$	74	$\Gamma_C(157)-[82]$	75	$\Gamma_C(233)-[81]$
76	$\Gamma_C(101)-[14]$	77	$\Gamma_C(90)-[19,71]$	78	$\Gamma_C(58)-[57]$	79	$\Gamma_C(98)-[19]$
80	$\Gamma_C(332)-[251]$	81	$\Gamma_C(55)-[54]$	82	$\Gamma_C(122)-[3]$	83	$\Gamma_C(176)-[23,79]$
84	$\Gamma_C(346)-[177]$	85	$\Gamma_C(57)-[56]$	86	$\Gamma_0(694)$	87	$\Gamma_C(175)-[68,174]$
88	$\Gamma_C(127)-[63]$	89	$\Gamma_C(91)-[12]$	90	$\Gamma_C(367)-[192]$	91	$\Gamma_C(62)-[61]$
92	$\Gamma_C(53)-[52]$	93	$\Gamma_C(64)-[63]$	94	$\Gamma_C(268)-[109,135]$	95	$\Gamma_C(485)-[389,393]$

96	$\Gamma_C(394) - [201]$	97	$\Gamma_C(63) - [62]$	98	$\Gamma_0(796)$	99	$\Gamma_C(208) - [59, 183]$
100	$\Gamma_C(92) - [45, 47]$	101	$\Gamma_C(112) - [31]$	102	$\Gamma_0(1223)$	103	$\Gamma_C(117) - [53, 73]$
104	$\Gamma_C(428) - [323]$	105	$\Gamma_C(68) - [67]$	106	$\Gamma_C(121) - [94]$	107	$\Gamma_C(333) - [130, 260]$
108	$\Gamma_C(439) - [298]$	109	$\Gamma_C(100) - [49, 51]$	110	$\Gamma_C(229) - [169]$	111	$\Gamma_C(115) - [47, 114]$
112	$\Gamma_C(316) - [41, 159]$	113	$\Gamma_C(85) - [16, 69]$	114	$\Gamma_C(463) - [27]$	115	$\Gamma_C(140) - [57, 111]$
116	$\Gamma_C(701) - [4]$	117	$\Gamma_C(59) - [58]$	118	$\Gamma_C(108) - [53, 55]$	119	$\Gamma_C(369) - [206, 253]$
120	$\Gamma_0(1439)$	121	$\Gamma_C(65) - [64]$	122	$\Gamma_0(982)$	123	$\Gamma_C(150) - [7, 101]$
124	$\Gamma_C(508) - [3]$	125	$\Gamma_C(201) - [8]$	126	$\Gamma_C(61) - [60]$	127	$\Gamma_C(203) - [75, 202]$
128	$\Gamma_C(524) - [395]$	129	$\Gamma_C(120) - [61, 119]$	130	$\Gamma_0(1046)$	131	$\Gamma_C(93) - [32, 61]$
132	$\Gamma_C(538) - [273]$	133	$\Gamma_C(69) - [68]$	134	$\Gamma_C(172) - [37, 87]$	135	$\Gamma_C(417) - [140, 226]$
136	$\Gamma_C(74) - [73]$	137	$\Gamma_C(80) - [79]$	139	$\Gamma_C(156) - [31, 131]$	140	$\Gamma_0(1126)$
141	$\Gamma_C(99) - [10, 89]$	142	$\Gamma_C(199) - [11]$	143	$\Gamma_C(444) - [19, 371]$	144	$\Gamma_C(586) - [297]$
145	$\Gamma_C(75) - [74]$	146	$\Gamma_0(1174)$	147	$\Gamma_C(304) - [39, 143]$	148	$\Gamma_C(412) - [89, 207]$
149	$\Gamma_C(164) - [23]$	150	$\Gamma_C(607) - [27]$	151	$\Gamma_C(112) - [41, 111]$	152	$\Gamma_0(1228)$
153	$\Gamma_C(90) - [89]$	154	$\Gamma_C(218) - [113]$	155	$\Gamma_C(67) - [66]$	156	$\Gamma_C(262) - [163]$
157	$\Gamma_C(168) - [13, 41, 127]$	159	$\Gamma_C(492) - [7, 83]$	160	$\Gamma_C(652) - [491]$	161	$\Gamma_C(119) - [33]$
163	$\Gamma_C(189) - [8, 188]$	164	$\Gamma_C(668) - [67]$	165	$\Gamma_C(176) - [79]$	166	$\Gamma_C(134) - [97]$
167	$\Gamma_C(196) - [99, 117]$	168	$\Gamma_C(1013) - [9]$	169	$\Gamma_C(116) - [57, 59]$	170	$\Gamma_C(349) - [60]$
171	$\Gamma_C(82) - [81]$	172	$\Gamma_C(162) - [53]$	173	$\Gamma_C(175) - [26, 99]$	174	$\Gamma_0(2087)$
175	$\Gamma_C(217) - [85, 125]$	176	$\Gamma_C(71) - [70]$	177	$\Gamma_C(180) - [71, 127]$	178	$\Gamma_0(1436)$
179	$\Gamma_C(368) - [143, 231]$	180	$\Gamma_C(727) - [125]$	181	$\Gamma_C(77) - [76]$	182	$\Gamma_C(373) - [64]$
183	$\Gamma_C(145) - [88, 144]$	184	$\Gamma_C(508) - [255, 281]$	185	$\Gamma_C(153) - [35, 55]$	186	$\Gamma_C(751) - [27]$
187	$\Gamma_C(73) - [72]$	188	$\Gamma_C(764) - [19]$	189	$\Gamma_C(485) - [357, 389]$	190	$\Gamma_C(81) - [80]$
191	$\Gamma_C(132) - [43, 89]$	192	$\Gamma_C(778) - [393]$	193	$\Gamma_C(96) - [95]$	195	$\Gamma_C(404) - [307]$
196	$\Gamma_C(124) - [61, 63]$	197	$\Gamma_C(208) - [95, 183]$	199	$\Gamma_C(146) - [9]$	200	$\Gamma_0(2399)$
201	$\Gamma_C(154) - [87]$	202	$\Gamma_C(556) - [279, 365]$	203	$\Gamma_C(617) - [81]$	204	$\Gamma_C(823) - [27]$
205	$\Gamma_C(117) - [53, 64]$	206	$\Gamma_C(421) - [64]$	207	$\Gamma_C(633) - [212, 343]$	208	$\Gamma_C(566) - [21]$
209	$\Gamma_C(144) - [73, 143]$	210	$\Gamma_C(92) - [91]$	211	$\Gamma_C(155) - [32, 154]$	212	$\Gamma_C(1277) - [4]$
213	$\Gamma_C(226) - [7]$	214	$\Gamma_0(1718)$	215	$\Gamma_C(657) - [151, 512]$	216	$\Gamma_C(1301) - [4]$
217	$\Gamma_C(140) - [69, 71]$	218	$\Gamma_C(197) - [6]$	219	$\Gamma_C(669) - [190, 224]$	220	$\Gamma_C(604) - [65, 303]$
221	$\Gamma_C(115) - [24, 91]$	222	$\Gamma_C(79) - [78]$	223	$\Gamma_C(307) - [34]$	224	$\Gamma_C(908) - [683]$
225	$\Gamma_C(85) - [84]$	226	$\Gamma_C(314) - [239]$	227	$\Gamma_C(464) - [147, 407]$	228	$\Gamma_C(922) - [465]$
229	$\Gamma_C(140) - [29, 111]$	230	$\Gamma_0(1852)$	231	$\Gamma_C(94) - [93]$	232	$\Gamma_C(284) - [85, 143]$
233	$\Gamma_C(144) - [89, 143]$	235	$\Gamma_C(98) - [97]$	236	$\Gamma_C(202) - [65]$	237	$\Gamma_C(369) - [118, 206]$
238	$\Gamma_C(652) - [265, 327]$	239	$\Gamma_C(355) - [238, 354]$	240	$\Gamma_C(967) - [125]$	241	$\Gamma_C(119) - [50, 69]$
242	$\Gamma_0(1942)$	243	$\Gamma_C(253) - [24, 252]$	244	$\Gamma_C(662) - [27]$	245	$\Gamma_C(150) - [49, 101]$
247	$\Gamma_C(83) - [82]$	248	$\Gamma_C(1004) - [759]$	249	$\Gamma_C(204) - [35, 55]$	250	$\Gamma_C(108) - [107]$
251	$\Gamma_C(211) - [63]$	252	$\Gamma_C(1018) - [513]$	253	$\Gamma_C(203) - [59, 202]$	254	$\Gamma_0(2038)$
255	$\Gamma_C(481) - [123, 443]$	256	$\Gamma_C(181) - [56]$	257	$\Gamma_C(187) - [50]$	258	$\Gamma_C(1039) - [27]$
259	$\Gamma_C(175) - [43, 174]$	260	$\Gamma_C(1052) - [531]$	261	$\Gamma_C(93) - [92]$	262	$\Gamma_C(362) - [99]$
263	$\Gamma_C(801) - [179, 181]$	264	$\Gamma_0(3167)$	265	$\Gamma_C(91) - [90]$	266	$\Gamma_0(3191)$
267	$\Gamma_C(129) - [44, 85]$	268	$\Gamma_C(1082) - [545]$	269	$\Gamma_C(417) - [8]$	270	$\Gamma_C(1087) - [27]$
271	$\Gamma_C(209) - [12, 153]$	272	$\Gamma_C(1637) - [4]$	273	$\Gamma_C(275) - [6, 199]$	274	$\Gamma_C(172) - [7]$
275	$\Gamma_C(562) - [81]$	276	$\Gamma_C(250) - [99]$	277	$\Gamma_C(156) - [53, 103]$	279	$\Gamma_C(849) - [284, 304]$
280	$\Gamma_C(758) - [237]$	281	$\Gamma_C(99) - [98]$	283	$\Gamma_C(485) - [28, 389]$	284	$\Gamma_C(1709) - [9]$
285	$\Gamma_C(444) - [115, 149]$	286	$\Gamma_C(191) - [7]$	287	$\Gamma_C(89) - [88]$	288	$\Gamma_C(1733) - [4]$
289	$\Gamma_C(95) - [94]$	290	$\Gamma_0(2326)$	291	$\Gamma_C(217) - [94, 216]$	292	$\Gamma_C(796) - [399, 425]$
293	$\Gamma_C(304) - [143]$	294	$\Gamma_0(3527)$	295	$\Gamma_C(208) - [21, 207]$	296	$\Gamma_0(2374)$
297	$\Gamma_C(260) - [209, 231]$	298	$\Gamma_C(412) - [295]$	299	$\Gamma_C(909) - [253, 809]$	300	$\Gamma_C(106) - [105]$

301	$\Gamma_C(112) - [111]$	302	$\Gamma_0(2428)$	303	$\Gamma_C(313) - [255]$	304	$\Gamma_C(1226) - [617]$
305	$\Gamma_C(205) - [64]$	306	$\Gamma_C(502) - [301]$	307	$\Gamma_C(133) - [20, 113]$	308	$\Gamma_C(1244) - [183]$
309	$\Gamma_C(161) - [45]$	310	$\Gamma_C(844) - [423, 641]$	311	$\Gamma_C(220) - [131, 133]$	312	$\Gamma_C(1877) - [4]$
313	$\Gamma_C(168) - [13, 167]$	314	$\Gamma_0(2518)$	315	$\Gamma_C(953) - [81]$	316	$\Gamma_C(524) - [217, 263]$
317	$\Gamma_C(492) - [83, 295]$	319	$\Gamma_C(333) - [260, 304]$	320	$\Gamma_0(2566)$	321	$\Gamma_C(160) - [49, 159]$
322	$\Gamma_0(2582)$	323	$\Gamma_C(141) - [46, 95]$	324	$\Gamma_C(239) - [38]$	325	$\Gamma_C(189) - [62]$
326	$\Gamma_C(661) - [31]$	327	$\Gamma_C(666) - [187, 593]$	328	$\Gamma_C(892) - [413, 447]$	329	$\Gamma_C(240) - [13, 239]$
330	$\Gamma_C(1327) - [27]$	331	$\Gamma_C(234) - [53, 73]$	332	$\Gamma_C(242) - [215]$	333	$\Gamma_C(147) - [50, 97]$
334	$\Gamma_C(458) - [169]$	335	$\Gamma_C(1017) - [566, 568]$	336	$\Gamma_C(284) - [39]$	337	$\Gamma_C(126) - [125]$
339	$\Gamma_C(688) - [87, 175]$	340	$\Gamma_0(2732)$	341	$\Gamma_C(355) - [51, 214]$	342	$\Gamma_C(268) - [97, 135]$
343	$\Gamma_C(196) - [19]$	344	$\Gamma_C(1388) - [1043]$	345	$\Gamma_C(97) - [96]$	347	$\Gamma_C(1049) - [81]$
348	$\Gamma_C(1399) - [419]$	349	$\Gamma_C(217) - [27]$	350	$\Gamma_C(709) - [64]$	351	$\Gamma_C(116) - [115]$
352	$\Gamma_C(326) - [23]$	353	$\Gamma_C(180) - [19, 161]$	355	$\Gamma_C(372) - [125, 151]$	356	$\Gamma_C(1436) - [7]$
357	$\Gamma_C(368) - [143]$	358	$\Gamma_C(422) - [61]$	359	$\Gamma_C(1267) - [363, 907]$	360	$\Gamma_C(1447) - [27]$
361	$\Gamma_C(143) - [12, 131]$	362	$\Gamma_C(733) - [335]$	363	$\Gamma_C(738) - [253, 575]$	364	$\Gamma_C(1466) - [769]$
365	$\Gamma_C(145) - [59, 86]$	366	$\Gamma_C(604) - [149, 303]$	367	$\Gamma_C(381) - [128, 190]$	368	$\Gamma_C(2213) - [4]$
369	$\Gamma_C(153) - [35, 118]$	370	$\Gamma_C(508) - [27]$	371	$\Gamma_C(752) - [207, 471]$	372	$\Gamma_C(2237) - [4]$
373	$\Gamma_C(189) - [143]$	374	$\Gamma_0(2998)$	375	$\Gamma_C(391) - [139, 390]$	376	$\Gamma_C(101) - [100]$
377	$\Gamma_C(485) - [43, 389]$	378	$\Gamma_C(118) - [117]$	379	$\Gamma_C(203) - [99, 146]$	380	$\Gamma_C(1532) - [771]$
381	$\Gamma_C(132) - [131]$	382	$\Gamma_0(3062)$	383	$\Gamma_C(1164) - [199, 971]$	384	$\Gamma_C(1543) - [125]$
385	$\Gamma_C(111) - [110]$	387	$\Gamma_C(775) - [172, 774]$	388	$\Gamma_C(1046) - [327]$	389	$\Gamma_C(593) - [38]$
390	$\Gamma_0(4679)$	391	$\Gamma_C(287) - [83, 120]$	392	$\Gamma_C(103) - [102]$	393	$\Gamma_C(208) - [95]$
394	$\Gamma_0(3158)$	395	$\Gamma_C(225) - [26, 82]$	396	$\Gamma_C(1594) - [801]$	397	$\Gamma_C(377) - [196, 233]$
399	$\Gamma_C(409) - [259]$	400	$\Gamma_C(172) - [85, 87]$	401	$\Gamma_C(165) - [56, 109]$	403	$\Gamma_C(476) - [71, 307]$
404	$\Gamma_C(262) - [73]$	405	$\Gamma_C(721) - [192]$	406	$\Gamma_C(122) - [121]$	407	$\Gamma_C(478) - [403]$
408	$\Gamma_C(1642) - [825]$	409	$\Gamma_C(117) - [116]$	410	$\Gamma_0(3292)$	411	$\Gamma_C(176) - [153, 175]$
412	$\Gamma_C(1658) - [833]$	413	$\Gamma_C(633) - [8]$	414	$\Gamma_C(1663) - [27]$	415	$\Gamma_C(405) - [53, 404]$
416	$\Gamma_C(1676) - [1259]$	417	$\Gamma_C(159) - [52, 107]$	418	$\Gamma_C(1132) - [21, 567]$	419	$\Gamma_C(437) - [116, 436]$
420	$\Gamma_0(5039)$	421	$\Gamma_C(155) - [61, 94]$	422	$\Gamma_C(853) - [40]$	423	$\Gamma_C(425) - [57, 324]$
424	$\Gamma_C(1142) - [27]$	425	$\Gamma_C(107) - [106]$	426	$\Gamma_C(1031) - [673]$	427	$\Gamma_C(270) - [161, 163]$
428	$\Gamma_C(508) - [255, 313]$	429	$\Gamma_C(657) - [25, 512]$	430	$\Gamma_0(3446)$	431	$\Gamma_C(308) - [43, 45]$
433	$\Gamma_C(128) - [127]$	434	$\Gamma_C(877) - [64]$	435	$\Gamma_C(430) - [37, 429]$	436	$\Gamma_C(362) - [119]$
437	$\Gamma_C(669) - [413]$	438	$\Gamma_C(1759) - [216]$	439	$\Gamma_C(304) - [31, 39]$	440	$\Gamma_C(1772) - [1331]$
441	$\Gamma_C(115) - [114]$	442	$\Gamma_C(109) - [108]$	443	$\Gamma_C(371) - [136, 370]$	445	$\Gamma_C(260) - [51, 53]$
446	$\Gamma_0(3574)$	447	$\Gamma_C(457) - [168]$	448	$\Gamma_C(2693) - [4]$	449	$\Gamma_C(224) - [31]$
450	$\Gamma_0(5399)$	451	$\Gamma_C(281) - [116]$	452	$\Gamma_0(3622)$	453	$\Gamma_C(363) - [94, 122]$
454	$\Gamma_C(1228) - [125, 615]$	455	$\Gamma_C(1603) - [54, 1602]$	456	$\Gamma_C(1831) - [27]$	457	$\Gamma_C(140) - [139]$
458	$\Gamma_0(3676)$	459	$\Gamma_C(1389) - [343, 464]$	460	$\Gamma_C(218) - [155]$	461	$\Gamma_C(198) - [89, 109]$
463	$\Gamma_C(161) - [22, 139]$	464	$\Gamma_C(1868) - [1403]$	465	$\Gamma_C(144) - [143]$	466	$\Gamma_C(631) - [122]$
467	$\Gamma_C(944) - [119, 207]$	468	$\Gamma_C(1879) - [216]$	469	$\Gamma_C(171) - [37, 134]$	470	$\Gamma_C(284) - [227]$
471	$\Gamma_C(533) - [150, 532]$	472	$\Gamma_C(2837) - [4]$	473	$\Gamma_C(369) - [64, 206]$	475	$\Gamma_C(572) - [135, 571]$
476	$\Gamma_C(625) - [224]$	477	$\Gamma_C(113) - [112]$	478	$\Gamma_C(652) - [171]$	479	$\Gamma_C(1687) - [381, 1686]$
481	$\Gamma_C(119) - [118]$	482	$\Gamma_C(316) - [159, 261]$	483	$\Gamma_C(976) - [307, 855]$	484	$\Gamma_C(188) - [93, 95]$
485	$\Gamma_C(253) - [68]$	486	$\Gamma_C(1951) - [27]$	487	$\Gamma_C(380) - [77, 189, 191]$	488	$\Gamma_C(1964) - [1475]$
489	$\Gamma_C(150) - [149]$	490	$\Gamma_C(1324) - [613, 663]$	491	$\Gamma_C(505) - [297, 504]$	492	$\Gamma_C(2957) - [4]$
493	$\Gamma_C(301) - [27]$	494	$\Gamma_C(997) - [3]$	495	$\Gamma_C(395) - [182, 394]$	496	$\Gamma_C(134) - [133]$
497	$\Gamma_C(204) - [67, 137]$	499	$\Gamma_C(196) - [97, 99]$				

Table A.2: Genera up to 500 not achieved in table 5.1 achieved by intersection type. Each entry in the right column is a list of congruence subgroups that intersect to form a smooth modular curve of a given genus, described by a prime power level and the matrices that generate $C_p \leq \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$. If there is a single prime power congruence subgroup with level < 100, it is given. If not, then a congruence subgroup with smallest component level (with all levels capped at 100) is given.

138	$7\ \begin{pmatrix}0&3\\2&0\end{pmatrix}\begin{pmatrix}2&2\\1&5\end{pmatrix}\begin{pmatrix}6&0\\0&6\end{pmatrix}\begin{pmatrix}4&1\\4&3\end{pmatrix}$ $79\ \begin{pmatrix}67&56\\71&57\end{pmatrix}\begin{pmatrix}35&37\\43&50\end{pmatrix}\begin{pmatrix}32&16\\25&15\end{pmatrix}\begin{pmatrix}78&0\\0&78\end{pmatrix}$
158	$8\ \begin{pmatrix}7&0\\0&7\end{pmatrix}\begin{pmatrix}3&3\\2&5\end{pmatrix}\begin{pmatrix}5&4\\0&5\end{pmatrix}\begin{pmatrix}5&0\\4&5\end{pmatrix}$ $79\ \begin{pmatrix}67&56\\71&57\end{pmatrix}\begin{pmatrix}35&37\\43&50\end{pmatrix}\begin{pmatrix}32&16\\25&15\end{pmatrix}\begin{pmatrix}78&0\\0&78\end{pmatrix}$
162	$29\ \begin{pmatrix}28&3\\11&24\end{pmatrix}\begin{pmatrix}28&0\\0&28\end{pmatrix}$
194	$8\ \begin{pmatrix}7&0\\0&7\end{pmatrix}\begin{pmatrix}2&3\\3&5\end{pmatrix}\begin{pmatrix}5&4\\0&5\end{pmatrix}\begin{pmatrix}5&0\\4&5\end{pmatrix}$ $49\ \begin{pmatrix}48&0\\0&48\end{pmatrix}\begin{pmatrix}46&36\\46&3\end{pmatrix}\begin{pmatrix}29&35\\42&22\end{pmatrix}\begin{pmatrix}0&3\\16&0\end{pmatrix}\begin{pmatrix}8&14\\7&43\end{pmatrix}\begin{pmatrix}47&5\\48&2\end{pmatrix}$
198	$9\ \begin{pmatrix}1&6\\0&1\end{pmatrix}\begin{pmatrix}4&0\\3&7\end{pmatrix}\begin{pmatrix}8&6\\0&8\end{pmatrix}$ $25\ \begin{pmatrix}4&10\\0&19\end{pmatrix}\begin{pmatrix}1&2\\24&24\end{pmatrix}\begin{pmatrix}16&15\\5&11\end{pmatrix}\begin{pmatrix}1&10\\5&1\end{pmatrix}\begin{pmatrix}2&24\\0&13\end{pmatrix}$
234	$16\ \begin{pmatrix}1&0\\8&1\end{pmatrix}\begin{pmatrix}7&7\\10&1\end{pmatrix}\begin{pmatrix}5&4\\8&13\end{pmatrix}\begin{pmatrix}9&0\\12&9\end{pmatrix}\begin{pmatrix}7&8\\0&7\end{pmatrix}\begin{pmatrix}9&8\\0&9\end{pmatrix}$ $59\ \begin{pmatrix}58&0\\0&58\end{pmatrix}\begin{pmatrix}34&44\\19&9\end{pmatrix}\begin{pmatrix}57&56\\3&4\end{pmatrix}$
246	$5\ \begin{pmatrix}4&0\\0&4\end{pmatrix}$ $11\ \begin{pmatrix}6&10\\10&4\end{pmatrix}\begin{pmatrix}10&0\\0&10\end{pmatrix}\begin{pmatrix}0&1\\10&0\end{pmatrix}\begin{pmatrix}7&4\\4&4\end{pmatrix}$
278	$2\ \begin{pmatrix}1&0\\0&1\end{pmatrix}$ $7\ \begin{pmatrix}3&4\\1&4\end{pmatrix}\begin{pmatrix}0&4\\5&6\end{pmatrix}\begin{pmatrix}3&1\\4&4\end{pmatrix}\begin{pmatrix}2&1\\2&5\end{pmatrix}\begin{pmatrix}6&0\\0&6\end{pmatrix}$ $79\ \begin{pmatrix}67&56\\71&57\end{pmatrix}\begin{pmatrix}35&37\\43&50\end{pmatrix}\begin{pmatrix}32&16\\25&15\end{pmatrix}\begin{pmatrix}78&0\\0&78\end{pmatrix}$
282	$2\ \begin{pmatrix}1&1\\0&1\end{pmatrix}$ $3\ \begin{pmatrix}2&2\\2&1\end{pmatrix}\begin{pmatrix}0&1\\2&0\end{pmatrix}\begin{pmatrix}2&0\\0&2\end{pmatrix}$ $5\ \begin{pmatrix}2&1\\0&3\end{pmatrix}\begin{pmatrix}1&1\\4&0\end{pmatrix}\begin{pmatrix}4&0\\0&4\end{pmatrix}\begin{pmatrix}4&2\\4&1\end{pmatrix}$ $37\ \begin{pmatrix}34&17\\21&4\end{pmatrix}\begin{pmatrix}3&26\\34&36\end{pmatrix}\begin{pmatrix}36&0\\0&36\end{pmatrix}\begin{pmatrix}25&7\\13&17\end{pmatrix}$

318	$5 \quad \begin{pmatrix}2&1\\0&3\end{pmatrix} \begin{pmatrix}4&0\\0&4\end{pmatrix} \begin{pmatrix}4&2\\4&1\end{pmatrix}$ $8 \quad \begin{pmatrix}7&0\\0&7\end{pmatrix} \begin{pmatrix}3&3\\2&5\end{pmatrix} \begin{pmatrix}5&4\\0&5\end{pmatrix} \begin{pmatrix}0&7\\1&7\end{pmatrix} \begin{pmatrix}5&0\\4&5\end{pmatrix}$ $31 \quad \begin{pmatrix}30&14\\11&0\end{pmatrix} \begin{pmatrix}30&0\\0&30\end{pmatrix} \begin{pmatrix}5&1\\15&28\end{pmatrix} \begin{pmatrix}9&20\\29&6\end{pmatrix}$
338	$2 \quad \begin{pmatrix}1&1\\0&1\end{pmatrix}$ $11 \quad \begin{pmatrix}10&4\\5&1\end{pmatrix} \begin{pmatrix}10&0\\0&10\end{pmatrix} \begin{pmatrix}1&9\\7&9\end{pmatrix}$ $61 \quad \begin{pmatrix}1&0\\44&1\end{pmatrix} \begin{pmatrix}60&0\\0&60\end{pmatrix} \begin{pmatrix}9&0\\22&34\end{pmatrix} \begin{pmatrix}14&0\\47&48\end{pmatrix}$
346	$2 \quad \begin{pmatrix}1&1\\0&1\end{pmatrix}$ $3 \quad \begin{pmatrix}1&1\\0&1\end{pmatrix} \begin{pmatrix}2&0\\0&2\end{pmatrix}$ $25 \quad \begin{pmatrix}24&0\\0&24\end{pmatrix} \begin{pmatrix}1&7\\14&24\end{pmatrix} \begin{pmatrix}11&20\\0&16\end{pmatrix} \begin{pmatrix}2&24\\0&13\end{pmatrix}$
354	$5 \quad \begin{pmatrix}2&1\\0&3\end{pmatrix} \begin{pmatrix}1&1\\4&0\end{pmatrix} \begin{pmatrix}4&0\\0&4\end{pmatrix} \begin{pmatrix}4&2\\4&1\end{pmatrix}$ $9 \quad \begin{pmatrix}8&6\\3&8\end{pmatrix} \begin{pmatrix}2&5\\8&7\end{pmatrix} \begin{pmatrix}3&1\\8&0\end{pmatrix} \begin{pmatrix}1&3\\6&1\end{pmatrix} \begin{pmatrix}4&0\\3&7\end{pmatrix}$ $16 \quad \begin{pmatrix}15&8\\0&15\end{pmatrix} \begin{pmatrix}1&12\\0&1\end{pmatrix} \begin{pmatrix}1&0\\8&1\end{pmatrix} \begin{pmatrix}1&0\\12&1\end{pmatrix} \begin{pmatrix}1&8\\0&1\end{pmatrix}$
386	$2 \quad \begin{pmatrix}1&0\\0&1\end{pmatrix}$ $3 \quad \begin{pmatrix}1&1\\0&1\end{pmatrix} \begin{pmatrix}2&0\\0&2\end{pmatrix}$ $29 \quad \begin{pmatrix}11&27\\12&19\end{pmatrix} \begin{pmatrix}28&0\\0&28\end{pmatrix} \begin{pmatrix}22&14\\13&7\end{pmatrix}$
398	$4 \quad \begin{pmatrix}3&0\\0&3\end{pmatrix} \begin{pmatrix}3&3\\2&1\end{pmatrix}$ $5 \quad \begin{pmatrix}2&1\\0&3\end{pmatrix} \begin{pmatrix}1&1\\4&0\end{pmatrix} \begin{pmatrix}4&0\\0&4\end{pmatrix} \begin{pmatrix}4&2\\4&1\end{pmatrix}$ $79 \quad \begin{pmatrix}67&56\\71&57\end{pmatrix} \begin{pmatrix}35&37\\43&50\end{pmatrix} \begin{pmatrix}32&16\\25&15\end{pmatrix} \begin{pmatrix}78&0\\0&78\end{pmatrix}$
402	$2 \quad \begin{pmatrix}1&1\\0&1\end{pmatrix}$ $3 \quad \begin{pmatrix}2&2\\2&1\end{pmatrix} \begin{pmatrix}0&1\\2&0\end{pmatrix} \begin{pmatrix}2&0\\0&2\end{pmatrix}$ $5 \quad \begin{pmatrix}2&1\\0&3\end{pmatrix} \begin{pmatrix}1&1\\4&0\end{pmatrix} \begin{pmatrix}4&0\\0&4\end{pmatrix} \begin{pmatrix}4&2\\4&1\end{pmatrix}$ $53 \quad \begin{pmatrix}52&0\\0&52\end{pmatrix} \begin{pmatrix}33&11\\7&12\end{pmatrix} \begin{pmatrix}16&41\\32&39\end{pmatrix}$
432	$8 \quad \begin{pmatrix}7&0\\0&7\end{pmatrix} \begin{pmatrix}3&3\\2&5\end{pmatrix} \begin{pmatrix}5&4\\0&5\end{pmatrix} \begin{pmatrix}0&7\\1&7\end{pmatrix} \begin{pmatrix}5&0\\4&5\end{pmatrix}$ $9 \quad \begin{pmatrix}8&6\\3&8\end{pmatrix} \begin{pmatrix}2&5\\8&7\end{pmatrix} \begin{pmatrix}3&1\\8&0\end{pmatrix} \begin{pmatrix}1&3\\6&1\end{pmatrix} \begin{pmatrix}4&0\\3&7\end{pmatrix}$ $71 \quad \begin{pmatrix}23&26\\36&50\end{pmatrix} \begin{pmatrix}70&0\\0&70\end{pmatrix} \begin{pmatrix}57&10\\33&22\end{pmatrix} \begin{pmatrix}53&6\\34&32\end{pmatrix}$

444	2	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$
	25	$\begin{pmatrix} 4 & 10 \\ 0 & 19 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 \\ 24 & 24 \end{pmatrix}$ $\begin{pmatrix} 16 & 15 \\ 5 & 11 \end{pmatrix}$ $\begin{pmatrix} 1 & 10 \\ 5 & 1 \end{pmatrix}$ $\begin{pmatrix} 2 & 24 \\ 0 & 13 \end{pmatrix}$
	27	$\begin{pmatrix} 10 & 15 \\ 18 & 19 \end{pmatrix}$ $\begin{pmatrix} 22 & 24 \\ 18 & 16 \end{pmatrix}$ $\begin{pmatrix} 7 & 25 \\ 15 & 19 \end{pmatrix}$ $\begin{pmatrix} 1 & 18 \\ 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 17 & 6 \\ 18 & 8 \end{pmatrix}$ $\begin{pmatrix} 10 & 9 \\ 0 & 19 \end{pmatrix}$
462	5	$\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 1 \\ 4 & 0 \end{pmatrix}$ $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$ $\begin{pmatrix} 4 & 2 \\ 4 & 1 \end{pmatrix}$
	2	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
	3	$\begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$ $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$
	61	$\begin{pmatrix} 1 & 0 \\ 44 & 1 \end{pmatrix}$ $\begin{pmatrix} 60 & 0 \\ 0 & 60 \end{pmatrix}$ $\begin{pmatrix} 9 & 0 \\ 22 & 34 \end{pmatrix}$ $\begin{pmatrix} 14 & 0 \\ 47 & 48 \end{pmatrix}$
474	2	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
	3	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$
	23	$\begin{pmatrix} 7 & 22 \\ 4 & 16 \end{pmatrix}$ $\begin{pmatrix} 15 & 3 \\ 4 & 7 \end{pmatrix}$ $\begin{pmatrix} 22 & 0 \\ 0 & 22 \end{pmatrix}$ $\begin{pmatrix} 4 & 12 \\ 12 & 19 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 \\ 22 & 0 \end{pmatrix}$
480	5	$\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 1 \\ 4 & 0 \end{pmatrix}$ $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$ $\begin{pmatrix} 4 & 2 \\ 4 & 1 \end{pmatrix}$
	16	$\begin{pmatrix} 13 & 8 \\ 4 & 5 \end{pmatrix}$ $\begin{pmatrix} 9 & 0 \\ 8 & 9 \end{pmatrix}$ $\begin{pmatrix} 11 & 3 \\ 10 & 13 \end{pmatrix}$ $\begin{pmatrix} 5 & 4 \\ 8 & 13 \end{pmatrix}$ $\begin{pmatrix} 7 & 8 \\ 0 & 7 \end{pmatrix}$ $\begin{pmatrix} 8 & 15 \\ 9 & 7 \end{pmatrix}$ $\begin{pmatrix} 9 & 8 \\ 0 & 9 \end{pmatrix}$
	71	$\begin{pmatrix} 23 & 26 \\ 36 & 50 \end{pmatrix}$ $\begin{pmatrix} 70 & 0 \\ 0 & 70 \end{pmatrix}$ $\begin{pmatrix} 57 & 10 \\ 33 & 22 \end{pmatrix}$ $\begin{pmatrix} 53 & 6 \\ 34 & 32 \end{pmatrix}$
498	2	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
	5	$\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 1 \\ 4 & 0 \end{pmatrix}$ $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$ $\begin{pmatrix} 4 & 2 \\ 4 & 1 \end{pmatrix}$
	29	$\begin{pmatrix} 11 & 27 \\ 12 & 19 \end{pmatrix}$ $\begin{pmatrix} 28 & 0 \\ 0 & 28 \end{pmatrix}$ $\begin{pmatrix} 22 & 14 \\ 13 & 7 \end{pmatrix}$

Appendix B

SageMath and Magma code

Section B.1

Intermediate congruence subgroups

B.1 (SageMath): Data for Principal Congruence Subgroups

```
def principal_list(N):
    prin = [(2, 6, 3, 0)];
    for n in range(3,N):
        new = Gamma(n);
        d = dn(n)
        prin.append((n, d, d/n, 1 +  d*(1/12 - 1/(2*n)) ))
    return prin
```

dn is the degree of $X(N)$ for $N > 2$ and is given by the following:

B.2 (SageMath): The degree of a Principal Congruence Subgroup

```
def dn(N):
```

```
    primes = list(factor(N));
    prod = 1;
    for pair in primes:
        p = pair[0];
        prod = prod * (1-1/(p^2))
    final = (1/2)*N^3 * prod
    return final
```

B.3 (SageMath): Data for intermediate congruence subgroups

Note that the methods *.ncusps*() and *.index*() use precisely the formulas derived in chapter 4 sections 1-3.

```
def intermediate_list(n):
    inter = [];
    for N in range(2,n):
        subgroups = Gamma0(N).gamma_h_subgroups();
        for s in subgroups:
            # -I acts trivially, assume WLOG -I in s.
            if s.is_even():
                C = s._list_of_elements_in_H();
                e_2 = False;
                e_3 = False;
                for c in C:
                    if (c^2 + 1) % N == 0:
                        e_2 = True;
                    elif (c^2 + c + 1) % N == 0:
                        e_3 = True;
```

```
                e = not (e_2 or e_3);
                d = s.index();
                c = s.ncusps();
                # Return 0 if there are elliptic points
                if e:
                    g = 1 + d/12 - c/2;
                else:
                    g = 0;
                inter.append([N,g,d,c,e])
    return inter
```

B.4 (SageMath): Intersections of principal and intermediate congruence subgroups

```
def intersect_pc(princ, inter):
    final_genera = [];

    # Adding the principal cong subgroup genus data
    for princ_data in princ:
        if princ_data[1] not in final_genera and princ_data[1] < 500:
            final_genera.append(princ_data[1]);

    # Adding intermediate subgroup genus data (if torsion free)
    for inter_data in inter:
        if inter_data[4] and inter_data[1] not in final_genera
        and inter_data[1] < 500:
            final_genera.append(inter_data[1]);
```

```
# Now to do the intersections:
for princ_data in princ:
    lev1 = princ_data[0];
    d1 = princ_data[2];
    c1 = princ_data[3];

    # loop over intermediate data:
    for inter_data in inter:
        lev2 = inter_data[0];
        if gcd(lev1,lev2) == 1:
            d2 = inter_data[2];
            c2 = inter_data[3]
            genus = 1 + d1*d2/12 - c1*c2/2;
            if genus not in final_genera and genus < 500:
                final_genera.append(genus);

final_genera.sort()
return final_genera
```

Section B.2

Intersection type congruence subgroups

B.5 (Magma) Gathering data for congruence subgroups of prime power level (developed by John Voight)

```
GenList := [* *];
for N in [2..100] do
  if IsPrimePower(N) then
    G := SL(2,Integers(N));
    nG := #G;
    m1 := G![-1,0,0,-1];
    for Hdat in Subgroups(G) do
      H := Hdat`subgroup;
      if not m1 in H or H eq G then continue; end if;

      ind := Index(G,H);

      GHT := CosetTable(G,H);
      pi := CosetTableToRepresentation(G,GHT);
      S := Matrix([[0,-1],[1,0]]);
      T := Matrix([[1,1],[0,1]]);
      ST := S*T;
      phiScyc := CycleStructure(pi(G!S));
      if phiScyc[#phiScyc][1] eq 1 then
        nu_2 := phiScyc[#phiScyc][2];
      else
        nu_2 := 0;
      end if;
      phiSTcyc := CycleStructure(pi(G!ST));
      if phiSTcyc[#phiSTcyc][1] eq 1 then
        nu_3 := phiSTcyc[#phiSTcyc][2];
```

```
      else
        nu_3 := 0;
      end if;
      eoo := #CycleDecomposition(pi(G!T));

      g := 1 + (ind/12) - (nu_2/4) - (nu_3/3) - (eoo/2);
      g := Integers()!g;
      Append(~GenList, [*[N, g, ind, nu_2, nu_3, eoo],Generators(H)*]);
    end for;
  end if;
end for;
GenList;
```

Bibliography

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[2] David A. Cox and Walter R. Parry., *Genera of congruence subgroups in q-quaternion algebras.*, Journal für die reine und angewandte Mathematik **351** (1984), 66–112.

[3] János A. Csirik, Joseph L. Wetherell, and Michael E. Zieve, *On the genera of x_0(n)*, 2000.

[4] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Springer, New York, New York, 2005.

[5] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version x.y.z)*, YYYY, `https://www.sagemath.org`.