GENUS FORMULAE FOR FAMILIES OF MODULAR CURVES

ASIMINA S. HAMAKIOTES AND JUN BO LAU

Abstract. For each open subgroup $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, there is a modular curve X_H, defined as a quotient of the full modular curve $X(N)$, where N is the level of H. The genus formula of a modular curve is well known for $X_0(N)$, $X_1(N)$, $X(N)$, $X_{\mathrm{sp}}(N)$, $X^*_{\mathrm{sp}}(N)$, $X_{\mathrm{ns}}(N)$, $X^*_{\mathrm{ns}}(N)$, and $X_{S_4}(p)$ for p prime. We explicitly work out the invariants of the genus formulas for $X^+_{\mathrm{sp}}(N)$, $X^+_{\mathrm{ns}}(N)$, and $X_{\mathrm{arith},1}(M, MN)$. In Table 1, we provide the invariants of the genus formulas for all of the modular curves listed.

1. Introduction

Let E be an elliptic curve defined over a number field K, with algebraic closure $\overline{K}$. For an integer $N \geq 2$, let $E[N]$ be the N-torsion subgroup of $E(\overline{K})$. Note that $E[N]$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. The absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $E[N]$ via the natural action on the coordinates of the points in $E[N]$, which induces the following Galois representation after fixing a basis of $E[N]$:

$$\rho_{E,N} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

We can obtain an adelic Galois representation by taking inverse limits $\rho_E : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$. It is known that for a non-CM elliptic curve E/K, the image of ρ_E is open and therefore of finite index [Ser72]. One could study these compatible subgroups explicitly by considering projection maps $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For a subgroup $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the K-rational points of the modular curves $X_H(N)$ parametrize elliptic curves E/K such that $\mathrm{im}\,\rho_{E,N}(\mathrm{Gal}(\overline{K}/K)) \subseteq H$. Classifying rational points on modular curves has been a subject of study for many years, e.g., Serre's Uniformity Problem [Ser72], Mazur's "Program B" [Maz77]. Faltings Theorem states that for a smooth curve C with genus $g \geq 2$, there are finitely many rational points on C. The genus of a curve C provides information on the arithmetic of the rational points on C and suggests methods to use to compute rational points.

In the classification of possible 2-adic and ℓ-adic images of Galois representations attached to elliptic curves over $\mathbb{Q}$, Rouse, Sutherland, and Zureick-Brown developed computational tools to determine the genus of modular curves [RZB15, RSZB22]. More precisely, given an integer $N > 1$ and a subgroup type $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, one could compute the generators of H, the index of the subgroup, number of elliptic points of order 2 and 3, and the number of cusps.

In this paper, we determine elementary genus formulas of modular curves associated to subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that they admit a model over $\mathbb{Q}$, without group-theoretic inputs. The list

Lau was supported partly by the Simons Foundation grant #550023 for the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation, and in part by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT - No. 101020788), by the Research Council KU Leuven grant C14/24/099 and by CyberSecurity Research Flanders with reference number VR20192203.

includes various families of interest which can be found on [LMF24] and contains the list from [Ser72]. Below is a summary of the families of modular curves for which the genus formula is known, with references where one can find the genus formulas.

(1) Let $N \geq 1$ be an integer. For the families $X_0(N), X_1(N)$, and $X(N)$, one can find the genus formulas worked out in [DS05, Shi71].
(2) Let p be a prime and $r \geq 1$ an integer. In [DLM22, Table 3.1] and references therein, one can find the invariants of the genus formulas for $X_{\mathrm{sp}}(p^r)$, $X^*_{\mathrm{sp}}(p^r)$, $X_{\mathrm{ns}}(p^r)$, and $X^*_{\mathrm{ns}}(p^r)$. Since the genus formula invariants are multiplicative, one can determine the invariants of the genus formula for composite levels N [DLM22, Equation 3.14].
(3) Let p be a prime such that $p \equiv \pm 3 \bmod 8$. Ligozat determined the genus formula of $X_{S_4}(p)$ [Lig77]. Also, see [Ser72, SD73].

We prove elementary genus formulas for $X^+_{\mathrm{sp}}(N), X^+_{\mathrm{ns}}(N), X_{\mathrm{arith},1}(M, MN)$ and $X_{\mathrm{arith},\pm 1}(M, MN)$. The results of this paper are summarized in Table 1, where we list the invariants of the genus formulas of the modular curves discussed above. In addition, the results of this work are published on the L-functions and Modular Forms Database (LMFDB) in the "Modular curves over $\mathbb{Q}$" section [LMF24]. There are pages for each family of modular curves in the database, where the invariants of the genus formula for that family are displayed.

1.1. **Structure of the paper.** In Section 2, we review background relating to modular curves and the genus formula of a modular curve, as well as background on Cartan subgroups. For composite levels N, we determine the genus formulas of $X^+_{\mathrm{sp}}(N)$ in Section 3; $X^+_{\mathrm{ns}}(N)$ in Section 4; and lastly, $X_{\mathrm{arith},1}(M, MN)$ and $X_{\mathrm{arith},\pm 1}(M, MN)$ in Section 5.

Acknowledgements. The authors would like to thank Jennifer Balakrishnan, Harris Daniels, Jeremy Rouse, Andrew Sutherland, John Voight, and David Zywina for help with references. They would like to thank Pietro Mercuri for sharing his work on split Cartan subgroups. They would also like to thank the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation for funding the Modular Curves 3 Workshop hosted by MIT, where this work began.

2. Background

Let N be a positive integer. There is a functor sending a $\mathbb{Z}[1/N]$-algebra R to the set of (isomorphism classes of) pairs (E, ϕ) where E is an elliptic curve over R and $\phi : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ is an isomorphism of R-group schemes. If $N \geq 3$, then the functor is representable by a smooth affine $\mathbb{Z}[1/N]$-scheme, denoted by $Y(N)$. If $N < 3$, we take the coarse moduli space to get a scheme. We denote by $X(N)$ the compactification of $Y(N)$ and call this the full modular curve of level N.

Every matrix $\gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is an automorphism of $(\mathbb{Z}/N\mathbb{Z})^2_R$, with γ acting on (E, ϕ) by sending it to $(E, \phi \circ \gamma)$. For a subgroup $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we denote by X_H the quotient $X(N)/H$. As a coarse moduli space, $Y_H := Y(N)/H$ parametrizes elliptic curves with H-structure. More precisely, the equivalence class of elliptic curves with H-structure is given by (E, ϕ) where E is an elliptic curve over a $\mathbb{Z}[1/N]$-scheme R and $\phi : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ is an isomorphism of R-group schemes and $(E, \phi) \sim_H (E', \phi')$ if and only if $(\phi')^{-1} \circ \iota|_{E[N]} \circ \phi = h$ for some $h \in H$ and $\iota : E \xrightarrow{\sim} E'$.

On the other end, it is well known that for a subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ with finite index, one could define a complex structure on $\mathbb{H}^*/\Gamma$, where $\mathbb{H}^*$ is the union of the upper half plane, $\mathbb{Q}$ and ∞. In particular, X_H defined above can be realized as a Riemann surface $\mathbb{H}^*/\Gamma_H$, where $\Gamma_H \leq \mathrm{SL}_2(\mathbb{Z})$ is defined as the lift of $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Before stating the genus formula of a modular curve, we will define elliptic points and cusps of a congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$. For each point $\tau \in \mathbb{H}^*$, let Γ_τ be the subgroup of Γ that fixes τ, i.e., $\Gamma_\tau = \{\gamma \in \Gamma : \gamma(\tau) = \tau\}$. A point $\tau \in \mathbb{H}^*$ is an *elliptic point* of Γ if Γ_τ is nontrivial as a group of transformations, i.e., if $\{\pm I\}\Gamma_\tau \supset \{\pm I\}$. The *cusps* of Γ are the Γ-equivalence classes of $\mathbb{Q} \cup \{\infty\}$.

The following invariants have a contribution to the genus formula of a modular curve X_H:

- The PSL_2-*index* of X_H, denoted $i(\Gamma_H)$, is the index of $\overline{H} \coloneqq H \cap \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ in $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$.
- The *number of elliptic points of order* 2 on X_H, denoted $\varepsilon_2(\Gamma_H)$, is the number of right cosets of Γ_H in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ fixed by the right action of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.
- The *number of elliptic points of order* 3 on X_H, denoted $\varepsilon_3(\Gamma_H)$, is the number of right cosets of Γ_H in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ fixed by the right action of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$.
- The *number of cusps* on X_H, denoted $\varepsilon_\infty(\Gamma_H)$, is the number of orbits of the right coset space $\Gamma_H \backslash \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ under the right action of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

That the number of elliptic points and cusps are equal to the number of cosets mentioned above is discussed in [DS05, Sections 2.3, 2.4]. It follows from the Riemann-Hurwitz formula that the genus of the modular curve X_H is given by:

$$g(\Gamma_H) = 1 + \frac{i(\Gamma_H)}{12} - \frac{\varepsilon_2(\Gamma_H)}{4} - \frac{\varepsilon_3(\Gamma_H)}{3} - \frac{\varepsilon_\infty(\Gamma_H)}{2}.$$

Common notation used in various genus formulas is: $\varphi(N)$ which is the usual Euler totient function, $\omega(N)$ which is the number of primes dividing N, and $\left(\frac{\cdot}{\cdot}\right)$ which is the usual Legendre symbol.

Remark 2.1. Let $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. An index 2 or *quadratic refinement* of H is a subgroup $H' \leq H$ such that $H = \pm H'$. The modular curves X_H and $X_{H'}$ are isomorphic as curves, but the moduli problem is refined from H to H'. Naturally, the genus of X_H and $X_{H'}$ are equal. The genus formulas for $X_{\pm 1}(N)$, $X_{\mathrm{arith},\pm 1}(M, MN)$, and their quadratic refinements are included in Table 1.

2.1. **Cartan Subgroups.** Let R be a commutative ring. Given a free rank 2 etalé R-algebra A, for $a \in A^\times$, the multiplication-by-a map defines an injective homomorphism $A^\times \hookrightarrow \mathrm{GL}_2(R)$. The image of this homomorphism is called a *Cartan subgroup* of $\mathrm{GL}_2(R)$. There is a canonical involution of A which gives another element of $\mathrm{GL}_2(R)$. The group generated by the image of $A^\times$ and the involution is called the *extended Cartan subgroup*. When $R = \mathbb{Z}/p^e\mathbb{Z}$, where p^e is some prime power, A has two possibilities: $A = R \times R$ (*split* Cartan) or $A = \mathcal{O}/p^e\mathcal{O}$ (*nonsplit* Cartan), where $\mathcal{O}$ is either a degree 2 unramified extension of $\mathbb{Z}/p\mathbb{Z}$ or a quadratic order where p is inert. In general, for $R = \mathbb{Z}/N\mathbb{Z}$, the extended Cartan subgroup is called the *normalizer of Cartan subgroup* and it is denoted by either $C_{\mathrm{sp}}^+(N)$ or $C_{\mathrm{ns}}^+(N)$, depending on whether A is split or nonsplit, respectively, at each prime dividing N. The Cartan subgroup has index 2 in the extended Cartan subgroup. In this paper, the normalizer of the Cartan subgroup will mean the extended Cartan subgroup.

Remark 2.2. For $R = \mathbb{Z}/N\mathbb{Z}$, it is possible to have a mix of split and nonsplit primes dividing N (see [DLM22, Theorem 3.8]). While the methods presented in this paper can handle the Cartan subgroups, the analysis for normalizers of Cartan subgroups is beyond the scope of this paper.

Remark 2.3. In the literature, sometimes the normalizer of the Cartan subgroup is defined as the group generated by the Cartan subgroup along with *an involution for each prime dividing* N, denoted by C_{sp}^* or C_{ns}^*, depending on whether A is split or nonsplit, respectively, at each prime dividing N. In contrast with the above, the Cartan subgroup here has index $2^{\omega(N)}$ in the extended Cartan subgroup and is generated by the Cartan subgroup and involutions from each prime dividing

N. Geometrically, X_{sp}^* (resp. X_{ns}^*) is isomorphic to the fiber product of split (resp. nonsplit) Cartan curves from lower levels.

Example 2.4. Consider the modular curve associated to the normalizer of a split Cartan subgroup of level 21, namely $X_{\mathrm{sp}}^+(21)$. Following our notation, $X_{\mathrm{sp}}^+(21)$ correponds to the LMFDB label `21.336.17.d.1` with genus 17. In [Bar10], the curve with the same notation is defined as in Remark 2.3 and has LMFDB label `21.168.9.f.1` and genus 9.

3. Split Cartan and normalizer of the split Cartan

The split Cartan modular curve, denoted $X_{\mathrm{sp}}(N)$, is the modular curve X_H for the subgroup $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ given by the inverse image of a Cartan subgroup $\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$ that is split at every prime dividing N. As a moduli space its k-points parametrize triples (E, C, D), where E is an elliptic curve over k, and C and D are Gal_k-stable cyclic subgroups such that $E[N](\overline{k}) \simeq C \oplus D$.

The normalizer of the split Cartan, denoted $X_{\mathrm{sp}}^+(N)$, is the modular curve X_H for the subgroup $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ given by the inverse image of an extended Cartan subgroup $\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \cup \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right) \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that is split at every prime dividing N. As a moduli space it parametrizes pairs $(E, \{C, D\})$, where E is an elliptic curve over k, and $\{C, D\}$ is a Gal_k-stable pair of cyclic subgroups such that $E[N](\overline{k}) \simeq C \oplus D$. Note that neither C nor D need be Gal_k-stable and the split Cartan subgroup is an index 2 subgroup in the normalizer.

In this section, we describe the genus formulas for the normalizer of the split Cartan modular curve $X_{\mathrm{sp}}^+(N)$. We derive the invariants of their genus formulas for composite level N, using methods communicated by Pietro Mercuri for prime power levels p^r in [DMS19, Remark 4.3].

From the definition above, the orders of the split Cartan subgroup $C_{\mathrm{sp}}(N)$ and its normalizer $C_{\mathrm{sp}}^+(N)$ are $\varphi(N)^2$ and $2 \cdot \varphi(N)^2$, respectively. Therefore, the indices are given by

$$[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : C_{\mathrm{sp}}(N)] = N^2 \cdot \prod_{\substack{p \mid N, \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right),$$

$$[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : C_{\mathrm{sp}}^+(N)] = \frac{N^2}{2} \cdot \prod_{\substack{p \mid N, \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right).$$

Lemma 3.1. *For prime power levels $N = p^r$, a set of coset representatives $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/C_{\mathrm{sp}}(N)$ have the form:*

$$\alpha(u, v) = \begin{pmatrix} 1 + uv & u \\ v & 1 \end{pmatrix}, \ \beta(u, v) = \begin{pmatrix} u & -1 \\ 1 & pv \end{pmatrix},$$

where $u, v \in \mathbb{Z}/p^r\mathbb{Z}$. A set of coset representatives $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/C_{\mathrm{sp}}^+(N)$ are the same as the ones above under the following identifications:

$$\alpha(u, v) \sim \begin{cases} \alpha((1 + uv)v^{-1}, -v) & \text{if } v \text{ is invertible mod } p^r, \\ \beta(u, -\frac{v}{p}(1 + uv)^{-1}) & \text{if } v \text{ is not invertible mod } p^r. \end{cases}$$

Proof. One checks that the number of coset representatives is equal to $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : C_{\mathrm{sp}}(N)]$ and that $\alpha(u', v')^{-1}\alpha(u, v), \beta(u', v')^{-1}\beta(u, v), \alpha(u', v')^{-1}\beta(u, v) \in C_{\mathrm{sp}}(N)$ or $C_{\mathrm{sp}}(N)$ if and only if $u' \equiv u \pmod{N}$ and $v' \equiv v \pmod{N}$. □

Let $N = \prod_i p_i^{e_i}$ be the prime factorization of N. The Chinese Remainder Theorem implies that there is a bijection:

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/C_{\mathrm{sp}}(N) \to \prod_i \mathrm{GL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})/C_{\mathrm{sp}}(p_i^{e_i}).$$

It follows that the coset representatives on the left are lifts of tuples of α's and β's on the right. Let $\omega := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the involution of the split Cartan subgroup. Then the subgroup generated by ω acts on $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/C_{\mathrm{sp}}(N)$ by left multiplication, which induces a natural action of $\vec{\omega} := (\omega, \omega, \ldots, \omega)$ on $\prod_p \mathrm{GL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})/C_{\mathrm{sp}}(p_i^{e_i})$, giving the following bijection:

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/C_{\mathrm{sp}}^+(N) = \Big(\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/C_{\mathrm{sp}}(N)\Big)/\langle\omega\rangle \to \Big(\prod_i \mathrm{GL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})/C_{\mathrm{sp}}(p_i^{e_i})\Big)/\langle\vec{\omega}\rangle.$$

The identification in Lemma 3.1 extends to the above bijection, thereby identifying pairs of tuples consisting of α's and β's for each prime dividing the level.

With this setup, we can begin calculating the quantities $\varepsilon_2, \varepsilon_3$, and ε_∞ in the genus formula.

Proposition 3.2. *Let ε_∞ and ε_∞^+ denote the number of cusps in $X_{\mathrm{sp}}(N)$ and $X_{\mathrm{sp}}^+(N)$, respectively. Then we have that*

$$\varepsilon_\infty = N \cdot \prod_{\substack{p \mid N, \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right),$$
$$\varepsilon_\infty^+ = \varepsilon_\infty/2.$$

Proof. Note that $\mathrm{SL}_2(\mathbb{Z})_\infty = \langle\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\rangle$. Let $g \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_{\mathrm{sp}}(N)$ be such that $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in g^{-1}\Gamma_{\mathrm{sp}}(N)g$, where Γ_{sp} is the lift of $C_{\mathrm{sp}}(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Observe that $a \equiv 0 \pmod N$. By [Shi71, Prop 1.37], the ramification index for each cusp is N and since the map $X_{\mathrm{sp}}(N) \to X(1)$ has degree $N^2 \cdot \prod_p (1+1/p)$, we have $\varepsilon_\infty = N \cdot \prod_p (1 + 1/p)$. Furthermore, the morphism $X_{\mathrm{sp}}(N) \to X_{\mathrm{sp}}^+(N)$ is of degree 2 and unramified over the cusps. It follows that $\varepsilon_\infty^+ = \varepsilon_\infty/2$. For $N = 2$, one could work directly with the definition of ε_2^+ as the number of cosets in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ fixed by the right action of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and find that there are 2 cusps. □

Proposition 3.3. *Let ε_3 and ε_3^+ denote the number of elliptic points of order 3 in $X_{\mathrm{sp}}(N)$ and $X_{\mathrm{sp}}^+(N)$, respectively. Then,*

$$\varepsilon_3 = \begin{cases} 0 & \text{if } 2 \mid N \text{ or } 3 \mid N, \\ \prod_{p \mid N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{otherwise.} \end{cases}$$
$$\varepsilon_3^+ = \varepsilon_3/2.$$

Proof. Let $\rho = e^{2\pi i/3}$ be a third root of unity. Note that $\mathrm{SL}_2(\mathbb{Z})_\rho = \left\langle\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)\right\rangle$. By [Shi71, Prop 1.37], the elliptic points of order 3 on $X_{\mathrm{sp}}(N)$ are the points in the inverse image $f^{-1}(\rho)$, where $f : \mathbb{H}^*/\Gamma_{\mathrm{sp}}(N) \to \mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z})$, with ramification index 1. By the same proposition, there exists $g \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_{\mathrm{sp}}(N)$ such that $\mathrm{SL}_2(\mathbb{Z})_\rho \subseteq g^{-1}\Gamma_{\mathrm{sp}}(N)g$. Therefore, it is sufficient to find the number of coset representatives γ such that $\gamma^{-1}\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)\gamma \in C_{\mathrm{sp}}(N)$ and $C_{\mathrm{sp}}^+(N)$, respectively.

11 Jun 2025 03:46:29 PDT
250127-Hamakiotes Version 2 - Submitted to LuCaNT

We begin with prime power levels $N = p^r$. We have the following matrices:

$$\alpha(u,v)^{-1}\left(\begin{smallmatrix}0 & -1\\ 1 & -1\end{smallmatrix}\right)\alpha(u,v) = \begin{pmatrix} -u^2v + uv - u - v & -u^2 + u - 1 \\ u^2v^2 - uv^2 + 2uv + v^2 - v + 1 & u^2 - uv + u + v - 1 \end{pmatrix}, \tag{1}$$

$$\beta(u,v)^{-1}\left(\begin{smallmatrix}0 & -1\\ 1 & -1\end{smallmatrix}\right)\beta(u,v) = (1+puv)^{-1}\begin{pmatrix} u - pv - 1 & -p^2v^2 - pv - 1 \\ u^2 - u + 1 & -puv - u + pv \end{pmatrix}. \tag{2}$$

For Equation (1) to be an element of $C_{\mathrm{sp}}(N)$, we require that the following conditions hold:

$$-u^2 + u - 1 \equiv 0 \pmod{N}, \tag{3}$$

$$-v^2(-u^2 + u - 1) + 2uv + -v + 1 \equiv 0 \pmod{N}. \tag{4}$$

Equation (3) has two solutions if $p \equiv 1 \pmod 3$ and 0 otherwise. Equation (4) is determined by Equation (3). For a matrix from Equation (2) to be an element of $C_{\mathrm{sp}}(N)$, we require that:

$$-p^2v^2 - pv - 1 \equiv 0 \pmod{N}, \tag{5}$$

$$u^2 - u + 1 \equiv 0 \pmod{N}. \tag{6}$$

However, this does not yield any solution since p is not invertible modulo N in Equation (5).

Writing the level N as a product of primes, we have two solutions for each prime p dividing N satisfying $p \equiv 1 \pmod 3$ and this gives ε_3. By the same argument in calculating ε_∞^+, the morphism $X_{\mathrm{sp}}(N) \to X_{\mathrm{sp}}^+(N)$ is of degree 2 and unramified over the elliptic points of order 3 and therefore, we have $\varepsilon_3^+ = \varepsilon_3/2$. □

Proposition 3.4. *Let ε_2 and ε_2^+ denote the number of elliptic points of order 2 in $X_{\mathrm{sp}}(N)$ and $X_{\mathrm{sp}}^+(N)$, respectively. Then we have that*

$$\varepsilon_2 = \begin{cases} 0 & \text{if } 2 \mid N, \\ \prod_{p\mid N}\left(1 + \left(\frac{-1}{p}\right)\right) & \text{otherwise.} \end{cases}$$

$$\varepsilon_2^+ = \frac{\varepsilon_2}{2} + \left(\frac{N}{2}\cdot \prod_{\substack{p\mid N,\\ p\equiv 1 \bmod 4}}\left(1 - \frac{1}{p}\right)\cdot \prod_{\substack{p\mid N,\\ p\equiv 3 \bmod 4}}\left(1 + \frac{1}{p}\right)\right),$$

Proof. Note that $\mathrm{SL}_2(\mathbb{Z})_i = \left\langle \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)\right\rangle$. By [Shi71, Prop 1.37], the elliptic points of order 2 on $X_{\mathrm{sp}}(N)$ are the points in the inverse image $f^{-1}(i)$, where $f : \mathbb{H}^*/\Gamma_{\mathrm{sp}}(N) \to \mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z})$, with ramification index 1. By the same proposition, there exists $g \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_{\mathrm{sp}}(N)$ such that $\mathrm{SL}_2(\mathbb{Z})_i \subseteq g^{-1}\Gamma_{\mathrm{sp}}(N)g$. Therefore, it is sufficient to find the number of coset representatives γ such that $\gamma^{-1}\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)\gamma \in C_{\mathrm{sp}}(N)$ and $C_{\mathrm{sp}}^+(N)$, respectively.

We begin with prime power levels $N = p^r$. We have the following matrices:

$$\alpha(u,v)^{-1}\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)\alpha(u,v) = \begin{pmatrix} -u^2v - u - v & -u^2 - 1 \\ u^2v^2 + 2uv + v^2 + 1 & u^2v + u + v \end{pmatrix}, \tag{7}$$

$$\beta(u,v)^{-1}\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)\beta(u,v) = (1+puv)^{-1}\begin{pmatrix} u - pv & -p^2v^2 - 1 \\ u^2 + 1 & pv - u \end{pmatrix}. \tag{8}$$

For a matrix from Equation (7) to be an element of $C_{\mathrm{sp}}(N)$, we require that the following conditions hold:

$$-u^2 - 1 \equiv 0 \pmod{N}, \tag{9}$$

$$-v^2(-u^2-1) + 2uv + 1 \equiv 0 \pmod{N}. \tag{10}$$

Equation (9) has two solutions when $p \equiv 1 \pmod 4$ and 0 otherwise. Equation (10) is determined by Equation (9). For a matrix from Equation (8) to be an element of $C_{\mathrm{sp}}(N)$, we require that:

$$-p^2v^2 - 1 \equiv 0 \pmod{N}, \tag{11}$$

$$u^2 + 1 \equiv 0 \pmod{N}. \tag{12}$$

However, this does not yield any solution since p is not invertible modulo N in Equation (11). Writing the composite level N as a product of prime powers, we obtain ε_2.

For ε_2^+, we use a different argument, starting with the prime power level $N = p^r$. For matrices from Equations (7, 8) to be elements of $C_{\mathrm{sp}}^+(N)$, in addition to Equations (9, 10, 11, 12), we also require that:

$$u^2v + u + v \equiv 0 \pmod{N}, \tag{13}$$

$$u - pv \equiv 0 \pmod{N}. \tag{14}$$

In Equation (13), note that $v \equiv -u(u^2+1)^{-1} \pmod N$. We observe that u^2+1 is not invertible when $p \equiv 1 \pmod 4$ and is always invertible when $p \equiv 3 \pmod 4$. It follows that there are p^r solutions when $p \equiv 3 \pmod 4$ and $p^r - 2p^{r-1}$ solutions when $p \equiv 1 \pmod 4$. When $p = 2$, u^2+1 is not invertible modulo N half of the time, so there are $2^r/2 = 2^{r-1}$ solutions. In Equation (14), there are p^{r-1} solutions, with no restrictions on p.

The identification from Lemma (3.1) identifies the two solutions from Equations (9, 10), and each solution of Equations (13, 14) is paired via

$$\alpha(u, -u(u^2+1)^{-1}) \sim \begin{cases} \alpha(-u^{-1}, u(u^2+1)^{-1}) & \text{if } u \text{ is invertible,} \\ \beta(u, u/p) & \text{if } u \text{ is not invertible.} \end{cases}$$

This recovers the formula in [DLM22] for prime power levels $N = p^r$:

$$\varepsilon_2^+ = \begin{cases} 2^{r-1} & \text{if } p = 2, \\ 1 + (p^r - p^{r-1})/2 & \text{if } p \equiv 1 \pmod 4, \\ (p^r + p^{r-1})/2 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

In the discussion after Lemma 3.1, the involution ω acts on both $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/C_{\mathrm{sp}}(N)$ and $\prod_i \mathrm{GL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})/C_{\mathrm{sp}}(p_i^{e_i})$, thus identifying pairs of solutions in $\prod_i \mathrm{GL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})/C_{\mathrm{sp}}(p_i^{e_i})$. Dividing the above analysis into two parts, one coming from $C_{\mathrm{sp}}(N)$ and the other from $C_{\mathrm{sp}}^+(N)$, we obtain the formula for ε_2^+.

□

Using the multiplicative relations from [DLM22], one can produce formulas for ε_2^*, ε_3^*, and ε_∞^* of $X_{\mathrm{sp}}^*(N)$.

Corollary 3.5. *Let ε_2^*, ε_3^*, ε_∞^* denote the number of elliptic points of orders 2, 3, and cusps in $X_{\mathrm{sp}}^*(N)$, respectively. Then we have that*

$$\varepsilon_\infty^* = \begin{cases} \frac{N}{3\cdot 2^{\omega(N)-2}} \prod_{p|N}(1+1/p) & \text{if } 2||N, \\ \frac{N}{2^{\omega(N)}} \prod_{p|N}(1+1/p) & \text{otherwise,} \end{cases}$$

$$\varepsilon_3^* = \begin{cases} 1 & p \equiv 1 \pmod 3 \text{ for all } p \mid N, \\ 0 & \text{otherwise,} \end{cases}$$

$$\varepsilon_2^* = 2^{\nu_2(N)-1} \cdot \prod_{\substack{p|N, \\ p\equiv 1 \bmod 4}} \left(1 + \frac{p^{\nu_p(N)-1}(p-1)}{2}\right) \cdot \prod_{\substack{p|N, \\ p\equiv 3 \bmod 4}} \frac{p^{\nu_p(N)-1}(p+1)}{2}.$$

4. Non-split Cartan and normalizer of the non-split Cartan

The non-split Cartan subgroup can also be defined explicitly. Let $R = \mathbb{Z}[\alpha]$ be a quadratic order such that α satisfies an irreducible monic polynomial $X^2 - uX + v \in \mathbb{Z}[X]$. Suppose that the discriminant of R is coprime to N and that every prime dividing N is inert in R. Then $A = R/NR$ is free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. For $x \in A$, the multiplication-by-x map induces a map $A^\times \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and the image is a non-split Cartan subgroup, denoted $C_{\mathrm{ns}}(N)$.

For the normalizer of $C_{\mathrm{ns}}(N)$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, there is an induced ring automorphism of order 2 from R in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, denoted by S_N. Viewing $C_{\mathrm{ns}}(N)$ as $(\mathbb{Z}/N\mathbb{Z})[\alpha]^\times$, since α is a root of $X^2 - uX + v$, $S_N(\alpha)$ also satisfies this polynomial and is therefore equal to $u - \alpha$. This gives an action of S_N on $(\mathbb{Z}/N\mathbb{Z})[\alpha]$ in the expected manner

$$1 \mapsto 1 \pmod N,$$
$$\alpha \mapsto u - \alpha \pmod N.$$

The normalizer of the non-split Cartan subgroup, denoted $C_{\mathrm{ns}}^+(N)$, is defined as the group generated by the non-split Cartan subgroup and this involution $\langle C_{\mathrm{ns}}(N), S_N\rangle$.

We denote the modular curves associated to $C_{\mathrm{ns}}(N)$ and $C_{\mathrm{ns}}^+(N)$ by $X_{\mathrm{ns}}(N)$ and $X_{\mathrm{ns}}^+(N)$, respectively. There are natural finite morphisms ϕ_1 and ϕ_2 such that

$$X_{\mathrm{ns}}(N) \xrightarrow{\phi_1} X_{\mathrm{ns}}^+(N) \xrightarrow{\phi_2} X(1),$$

where $\deg(\phi_1) = 2$ and $\deg(\phi_2) = N \cdot \varphi(N)/2$. Note that $\deg(\phi_2) = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : C_{\mathrm{ns}}^+(N)]$.

Let $C_{\mathrm{ns}}'(N) := C_{\mathrm{ns}}(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and let $C_{\mathrm{ns}}^{+\prime}(N) := C_{\mathrm{ns}}^+(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, where $C_{\mathrm{ns}}'(N)$ and $C_{\mathrm{ns}}^{+\prime}(N)$ can be identified with the following groups:

$$C_{\mathrm{ns}}'(N) = \{M_y : y \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times, N(\alpha) = 1\},$$
$$C_{\mathrm{ns}}^{+\prime}(N) = \{M_y : y \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times, N(\alpha) = 1\} \cup \{M_y \circ S_N : y \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times, N(\alpha) = -1\},$$

where M_y is the multiplication-by-y map on $(\mathbb{Z}/N\mathbb{Z})[\alpha]$, $N(x) = x\bar{x}$ is the norm map, and $\overline{a + b\alpha} = a + b(u - \alpha)$. For every element $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ or $a \in (\mathbb{Z}/N\mathbb{Z})^\times/\pm 1$, choose $y_a \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times$ such

that $N(y_a) = a$. We define the sets $\mathcal{Y}(N)$ and $\mathcal{Y}_\pm(N)$ as follows:

$$\mathcal{Y}(N) = \{y_a \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times : N(y_a) = a, a \in (\mathbb{Z}/N\mathbb{Z})^\times\},$$
$$\mathcal{Y}_\pm(N) = \{y_a \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times : N(y_a) = a, a \in (\mathbb{Z}/N\mathbb{Z})^\times/\pm 1\}.$$

The following proposition provides a matrix representation for a set of coset representatives of Γ_{ns} and Γ_{ns}^+ in $\mathrm{SL}_2(\mathbb{Z})$.

Proposition 4.1 (Proposition 6.2 and 6.3, [Bar10])**.** *A set of coset representatives of $C'_{\mathrm{ns}}(N)$ (resp. $C_{\mathrm{ns}}^{+\prime}(N)$) in $SL_2(\mathbb{Z}/N\mathbb{Z})$ can be represented as linear maps that transform the basis $\{1, \alpha\}$ as*

$$1 \mapsto y^{-1},$$
$$\alpha \mapsto \bar{y}(\alpha + x),$$

where $x \in \mathbb{Z}/N\mathbb{Z}$ and $y \in \mathcal{Y}(N)$ (resp. $y \in \mathcal{Y}_\pm(N)$).

Proof. We have the following equality

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_{\mathrm{ns}}(N)] = [\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : C'_{\mathrm{ns}}(N)] = [\mathrm{GL}_2(\mathbb{Z}/NZ) : C_{\mathrm{ns}}(N)]$$

and a similar statement holds for $C_{\mathrm{ns}}^+(N)$. The number of cosets of $C_{\mathrm{ns}}(N)$ and $C_{\mathrm{ns}}^+(N)$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ are $N\varphi(N)$ and $N\varphi(N)/2$, respectively, and $|\mathcal{Y}(N)| = \varphi(N)$ and $|\mathcal{Y}_\pm(N)| = \varphi(N)/2$. It remains to show that, under the identification above, the linear maps represent different cosets.

Suppose we have two elements in the same coset of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/C'_{\mathrm{ns}}(N)$:

$$1 \mapsto y^{-1}, \qquad 1 \mapsto y'^{-1},$$
$$\alpha \mapsto \bar{y}(\alpha + x), \qquad \alpha \mapsto \overline{y'}(\alpha + x').$$

Then we have $N(y) = N(y')$ and since $y, y' \in \mathcal{Y}(N)$, it follows that $y = y'$, which implies $x = x'$.

In the case of $C_{\mathrm{ns}}^+(N)$, observe that the linear maps that transform the basis $\{1, \alpha\}$ have two possibilities:

$$1 \mapsto y \qquad 1 \mapsto \bar{y}$$
$$\alpha \mapsto y\alpha \qquad \alpha \mapsto \bar{y}\bar{\alpha}.$$

where $y \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times$ with $N(y) = 1$ and $N(y) = -1$, respectively. Suppose we have two elements in the same coset of $\mathrm{SL}_2(\mathbb{Z}/NZ)/C_{\mathrm{ns}}^+(N)$:

$$1 \mapsto y^{-1}, \qquad 1 \mapsto y'^{-1},$$
$$\alpha \mapsto \bar{y}(\alpha + x), \qquad \alpha \mapsto \overline{y'}(\alpha + x').$$

Then the same argument shows that we have $N(y) = N(y')$ and since $y, y' \in \mathcal{Y}_\pm(N)$, it follows that $y = y'$, which implies $x = x'$. □

With this setup, we can begin calculating the quantities $\varepsilon_2, \varepsilon_3$, and ε_∞ in the genus formula.

Proposition 4.2. *Let ε_∞ and ε_∞^+ denote the number of cusps in $X_{\mathrm{ns}}(N)$ and $X_{\mathrm{ns}}^+(N)$, respectively. Then we have that*

$$\varepsilon_\infty = \varphi(N),$$
$$\varepsilon_\infty^+ = \begin{cases} 1 & \text{if } N = 2, \\ \varphi(N)/2 & \text{otherwise.} \end{cases}$$

Proof. Note that $\mathrm{SL}_2(\mathbb{Z})_\infty = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$. Let $g \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_{\mathrm{ns}}(N)$ such that $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in g^{-1}\Gamma_{\mathrm{ns}}(N)g$, for some $a \in \mathbb{Z}$, which stabilizes ∞. The element $g\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)g^{-1} \in \Gamma_{\mathrm{ns}}(N)$ can be represented in two ways: one in the manner of Proposition 4.1, and the other as a multiplication-by-k matrix, with $k \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times$, giving the following system of equations:

$$y^{-1} \equiv y^{-1}k \pmod{N},$$
$$\bar{y}(\alpha + x) \equiv \bar{y}(\alpha + x)k \pmod{N},$$

where $x \in \mathbb{Z}/N\mathbb{Z}, y \in \mathcal{Y}(N), k \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times$, and $N(k) = 1$. It follows that $k = 1$ and therefore $a = 0 \pmod{N}$. By [Shi71, Prop 1.37], the ramification index for each cusp of $X_{\mathrm{ns}}(N)$ is N and since the degree of the morphism $X_{\mathrm{ns}}(N) \to X(1)$ is $N\varphi(N)$, we have $\varepsilon_\infty = \varphi(N)$.

The same argument for $X^+_{\mathrm{ns}}(N)$ shows that the ramification index for each cusp is N and since the degree of the morphism $X^+_{\mathrm{ns}}(N) \to X(1)$ is $N\varphi(N)/2$, we have $\varepsilon^+_\infty = \varphi(N)/2$. When $N = 2$, $\varepsilon^+_\infty = 1$. □

Proposition 4.3. *Let ε_3 and ε_3^+ denote the number of elliptic points of order 3 in $X_{\mathrm{ns}}(N)$ and $X^+_{\mathrm{ns}}(N)$, respectively. Then we have that*

$$\varepsilon_3 = \begin{cases} 2^{\omega(N)} & p \equiv 2 \pmod 3 \text{ for all } p \mid N, \\ 0 & \text{otherwise,} \end{cases}$$
$$\varepsilon_3^+ = \varepsilon_3/2.$$

Proof. Let $\rho = e^{2\pi i/3}$ be a third root of unity. Note that $\mathrm{SL}_2(\mathbb{Z})_\rho = \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \right\rangle$. By [Shi71, Prop 1.37], the elliptic points of order 3 on $X_{\mathrm{ns}}(N)$ are the points in the inverse image $f^{-1}(\rho)$, where $f : \mathbb{H}^*/\Gamma_{\mathrm{ns}}(N) \to \mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z})$, with ramification index 1. By the same proposition, there exists $g \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_{\mathrm{ns}}(N)$ such that $\mathrm{SL}_2(\mathbb{Z})_\rho \subseteq g^{-1}\Gamma_{\mathrm{ns}}(N)g$. Therefore, ε_3 is equal to the number of coset representatives g such that

$$g \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} g^{-1} = \gamma,$$

for some $\gamma \in \Gamma_{\mathrm{ns}}(N)$. By Proposition 4.1, we can represent γ as a multiplication-by-k matrix for some $k \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times$, and we obtain the following system of equations:

$$\bar{y}(\alpha + x) \equiv y^{-1}k \pmod{N}, \tag{15}$$
$$\bar{y}(\alpha + x) - y^{-1} \equiv \bar{y}(\alpha + x)k \pmod{N}, \tag{16}$$

where $x \in \mathbb{Z}/N\mathbb{Z}, y \in \mathcal{Y}(N), k \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times$, and $N(k) = 1$.

We compute the number of solutions to the above equations, following [Bar10, Lem 7.7]. Suppose that x, y, k satisfy the equations above. Equation (15) can be rearranged as

$$N(y)\alpha + N(y)x \equiv k \pmod{N}.$$

Since $N(y) \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $k \notin (\mathbb{Z}/N\mathbb{Z})^\times$, equation (15) can be substituted into equation (16) as follows,

$$y^{-1}k - y^{-1} \equiv y^{-1}k^2 \pmod{N},$$

which implies that

$$k^2 - k + 1 \equiv 0 \pmod{N}. \tag{17}$$

We can reduce equation (17) modulo the primes p dividing N. Hensel's lemma and the Chinese Remainder Theorem imply that there are two nontrivial solutions for each prime dividing N. Since $\{1, \alpha\}$ is a basis for $(\mathbb{Z}/N\mathbb{Z})[\alpha]$, there are two unique solutions $(x, y) \in \mathbb{Z}/p^r\mathbb{Z} \times \mathcal{Y}(p^r)$ for the equation

$$N(y)\alpha + N(y)x \equiv k \pmod{p^r},$$

for each prime $p \equiv 2 \pmod 3$ dividing N and $p^r || N$. If there is a prime $p \not\equiv 2 \pmod 3$, then there will be no solutions. This yields the formula for ε_3. Since the morphism $X_{\mathrm{ns}}(N) \to X_{\mathrm{ns}}^+(N)$ is of degree 2 and unramified over the elliptic points of order 3, we obtain $\varepsilon_3^+ = \varepsilon_3/2$. □

Proposition 4.4. *Let ε_2 and ε_2^+ denote the number of elliptic points of order 2 in $X_{\mathrm{ns}}(N)$ and $X_{\mathrm{ns}}^+(N)$, respectively. Then we have that*

$$\varepsilon_2 = \prod_{p|N} \left(1 - \left(\frac{-1}{p}\right)\right),$$

$$\varepsilon_2^+ = \sum_{p|N} \frac{1 - \left(\frac{-1}{p}\right)}{2} \; + \; \left(\frac{1}{2}N \cdot \prod_{p|N}\left(1 + \frac{1}{p}\right) - \#S\right),$$

where $S = \{a + b\alpha \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times/\pm 1 : N(a + b\alpha) = -1, gcd(b, N) > 1\}$.

Proof. Note that $\mathrm{SL}_2(\mathbb{Z})_i = \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle$ and the elliptic points of order 2 on $X_{\mathrm{ns}}(N)$ are the points in the inverse image $f^{-1}(i)$, where $f : \mathbb{H}^*/\Gamma_{\mathrm{ns}}(N) \to \mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z})$, with ramification index 1. Therefore, by [Shi71, Prop 1.37], ε_2 is equal to the number of coset representatives $g \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_{\mathrm{ns}}(N)$ such that the equality

$$g \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} g^{-1} = \gamma,$$

holds for some $\gamma \in \Gamma_{\mathrm{ns}}(N)$. Considering the above equality as linear maps using Proposition 4.1 we have the equations:

$$\bar{y}(\alpha + x) \equiv y^{-1}k \pmod{N}, \tag{18}$$

$$-y^{-1} \equiv \bar{y}(\alpha + x)k \pmod{N}, \tag{19}$$

where $x \in \mathbb{Z}/N\mathbb{Z}, y \in \mathcal{Y}(N), k \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times$, and $N(k) = 1$.

We compute the number of solutions to the above equations, following [Bar10, Lem 7.8]. Suppose that x, y, k satisfy the above equations. Equation (18) can be rearranged and also substituted into equation (19) to get the following:

$$N(y)\alpha + N(y)x \equiv k \pmod{N}, \tag{20}$$

$$-y^{-1} \equiv y^{-1}k^2 \pmod{N}. \tag{21}$$

Since $N(y) \in (\mathbb{Z}/N\mathbb{Z})^\times$, equation (20) implies that $k \notin \mathbb{Z}/N\mathbb{Z}$. From equation (21), we obtain

$$-1 \equiv k^2 \pmod{N}.$$

By the Chinese Remainder Theorem and Hensel's lemma, since k is not an element of $(\mathbb{Z}/N\mathbb{Z})^\times$ and hence of $(\mathbb{Z}/p\mathbb{Z})^\times$ for any prime p dividing N, we have $p \equiv 3 \pmod 4$ for all primes p dividing N, and there are two solutions for the system of equations. This proves the ε_2 part of the proposition.

Recall that,

$$C_{\mathrm{ns}}^{+\prime}(N) = \{M_y : y \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times, N(\alpha) = 1\} \cup \{M_y \circ S_N : y \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^\times, N(\alpha) = -1\}.$$

Therefore, for the normalizer of a non-split Cartan subgroup, the same argument as above gives rise to two systems of equations, corresponding to the norm $+1$ and -1 elements:

$$\begin{aligned} \bar{y}(\alpha+x) &\equiv y^{-1}k \pmod N, & \bar{y}(\alpha+x) &\equiv \bar{y}^{-1}k \pmod N, \\ -y^{-1} &\equiv \bar{y}(\alpha+x)k \pmod N, & -y^{-1} &\equiv y(\bar{\alpha}+x)k \pmod N \end{aligned}$$

where $x \in \mathbb{Z}/N\mathbb{Z}, y \in \mathcal{Y}_{\pm}(N), k \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^{\times}$, and $N(k) = +1$ and -1, respectively. Notice that the system of equations on the left are the same as the systems of equations in the ε_2 case. Since the covering map $X_{\mathrm{ns}}^{+}(N) \to X_{\mathrm{ns}}(N)$ is of degree 2 and is unramified over these points, the norm $+1$ elements contribute $\sum_{p|N} \frac{1-\left(\frac{-1}{p}\right)}{2}$ to ε_2^{+}.

For the norm -1 elements, since $N(k) = -1$, the equations above on the right hand side are conjugate. Therefore, we want to know the number of solutions $(x, y) \in \mathbb{Z}/N\mathbb{Z} \times \mathcal{Y}_{\pm}(N)$ for which there exists a $k \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^{\times}$ such that the following equation holds

$$\bar{y}(\alpha+x) \equiv \bar{y}^{-2}k \pmod N.$$

Taking norms and rearranging terms, we obtain

$$N(\alpha+x) \equiv -N(y)^{-2} \pmod N.$$

Since the norm map $N : \mathcal{Y}_{\pm}(N) \to (\mathbb{Z}/N\mathbb{Z})^{\times}/\pm 1$ is an isomorphism, we need to count the number of $x \in \mathbb{Z}/N\mathbb{Z}$ and $v \in (\mathbb{Z}/N\mathbb{Z})^{\times}/\pm 1$ such that the following equality holds

$$N(\alpha+x) \equiv -v^2 \pmod N.$$

Now, we write $h = \frac{\alpha+x}{v} \in (\mathbb{Z}/N\mathbb{Z})[\alpha]^{\times}/\pm 1$, with $N(h) \equiv -1 \pmod N$. The problem at hand is to find how many such h's exist. Note that the norm map

$$N : (\mathbb{Z}/N\mathbb{Z})[\alpha]^{\times}/\pm 1 \to (\mathbb{Z}/N\mathbb{Z})^{\times}$$

is surjective and its kernel has order

$$\left(\frac{1}{2}N^2 \cdot \prod_{p|N}\left(1-\frac{1}{p^2}\right)\right)/\varphi(N) = \frac{1}{2}\cdot\prod_{p|N} p^{r-1}(p+1).$$

Therefore, the number of elements in $(\mathbb{Z}/N\mathbb{Z})[\alpha]^{\times}/\pm 1$ of norm -1 is equal to $\frac{1}{2}\prod_{p|N} p^{r-1}(p+1)$. Note that this count also includes elements whose α-coefficient is not coprime to N. We exclude these elements in the next few paragraphs.

Let $\mathcal{P} \in \mathbb{P}(N) := \mathrm{PowerSet}(\{p : p \text{ prime}, p \mid N\})$ and define

$$\begin{aligned} \Theta_{\mathcal{P}} : (\mathbb{Z}/N\mathbb{Z})[\alpha]^{\times}/\pm 1 &\to (\mathbb{Z}/N\mathbb{Z})^{\times} \times \prod_{p\in\mathcal{P}} \frac{(\mathbb{Z}/p\mathbb{Z})[\alpha]^{\times}}{(\mathbb{Z}/p\mathbb{Z})^{\times}}, \\ a+b\alpha &\mapsto (N(a+b\alpha), (a_p+b_p\alpha)_p), \end{aligned}$$

where a_p, b_p are the representatives of a, b under the reduction modulo p and projection maps.

Then the image of $\Theta_{\mathcal{P}}$ is given by

$$\mathrm{Im}(\Theta_{\mathcal{P}}) = \{(b, (c_p)_p) : b \equiv N(c_p)v_p^2 \pmod p \text{ for some } v_p \in (\mathbb{Z}/p\mathbb{Z})^{\times}, \text{ for all } p \in \mathcal{P}\},$$

which has cardinality $\varphi(N)\prod_{p\in\mathcal{P}}\frac{p+1}{2}\cdot 2^{\delta}$, where $\delta=1$ when $2\in\mathcal{P}$ and $\delta=0$ otherwise. The cardinality of the kernel can be calculated as

$$\begin{aligned}\#\ker(\Theta_{\mathcal{P}}) &= \#C_{\mathrm{ns}}^{+}(N)/\#\operatorname{Im}(\Theta_{\mathcal{P}}),\\ &= \frac{1}{2}N^2\left(\prod_{p\mid N}\left(1-\frac{1}{p^2}\right)\right)/\left(\varphi(N)\prod_{p\in\mathcal{P}}\frac{p+1}{2}\cdot 2^{\delta}\right),\\ &= 2^{\#\mathcal{P}-1-\delta}N\cdot\prod_{p\mid N}\left(1+\frac{1}{p}\right)/\prod_{p\in\mathcal{P}}(p+1).\end{aligned}$$

We are interested in

$$\Theta_{\mathcal{P}}^{-1}(-1,(1,\dots,1))=\{a+b\alpha : N(a+b\alpha)=-1,\ \gcd(b,p)>1,\ \text{for all } p\in\mathcal{P}\}.$$

Note that this set has the same cardinality as the kernel, and if there exists $p\equiv 3 \pmod 4\in\mathcal{P}$, then the preimage will be empty since the congruence condition

$$-1\equiv 1\cdot v_p^2 \pmod p$$

does not have a solution when $p\equiv 3 \pmod 4$. To summarize,

$$\#\Theta_{\mathcal{P}}^{-1}(-1,(1,\dots,1))=\begin{cases}0 & \exists p\in\mathcal{P}, p\equiv 3 \pmod 4,\\ 2^{\#\mathcal{P}-1-\delta}N\cdot\prod_{p\mid N}\left(1+\frac{1}{p}\right)/\prod_{p\in\mathcal{P}}(p+1) & \text{otherwise.}\end{cases}$$

By an inclusion-exclusion argument, one could compute the cardinality of the set

$$S:=\{a+b\alpha : N(a+b\alpha)=-1,\ \gcd(b,N)>1\}.$$

Let $\mathbb{P}(N)_k:=\{\mathcal{P}\in\mathbb{P}(N):\#\mathcal{P}=k\}$. Then,

$$\#S=\sum_{k=1}^{\omega(N)}(-1)^{k+1}\left(\sum_{\mathcal{P}\in\mathbb{P}(N)_k}\#\Theta_{\mathcal{P}}^{-1}(-1,\underbrace{(1,\dots,1)}_{k})\right)$$

and we obtain

$$\varepsilon_2^{+}=\underbrace{\sum_{p\mid N}\frac{1-\left(\frac{-1}{p}\right)}{2}}_{\text{norm}=+1}+\underbrace{\frac{1}{2}N\cdot\prod_{p\mid N}\left(1+\frac{1}{p}\right)-\#S}_{\text{norm}=-1}.$$

□

Remark 4.5. Propositions 4.2, 4.3, and 4.4 recover the formulas from [Bar10] when $N=p^r$.

Since the index, number of elliptic points and cusps are multiplicative in the level, one can produce formulas for ε_2^*, ε_3^*, and ε_∞^* of $X_{\mathrm{ns}}^*(N)$ from prime power levels (see [DLM22]).

Corollary 4.6. *Let ε_2^*, ε_3^*, ε_∞^* denote the number of elliptic points of orders 2, 3, and cusps in $X_{\mathrm{ns}}^*(N)$, respectively. Then we have that*

$$\varepsilon_\infty^* = \begin{cases} \varphi(N)/2^{\omega(N)-1} & \text{if } 2||N, \\ \varphi(N)/2^{\omega(N)} & \text{otherwise,} \end{cases}$$

$$\varepsilon_3^* = \begin{cases} 1 & p \equiv 2 \pmod 3 \text{ for all } p \mid N, \\ 0 & \text{otherwise,} \end{cases}$$

$$\varepsilon_2^* = 2^{\nu_2(N)-1} \cdot \prod_{\substack{p|N, \\ p\equiv 1 \bmod 4}} \frac{p^{\nu_p(N)-1}(p-1)}{2} \cdot \prod_{\substack{p|N, \\ p\equiv 3 \bmod 4}} \left(1 + \frac{p^{\nu_p(N)-1}(p+1)}{2}\right).$$

Remark 4.7. One can consider a different proof of the genus formula that follows from the ideas of Chen and de Smit-Edixhoven (see [DLM22, Theorem 3.8] and the references therein). The genus of the modular curve is equal to the dimension of its Jacobian; there is an isogeny between the Jacobian of the Cartan modular curve and the Jacobian of the Borel modular curve. Since the Borel case is well-known, this yields another proof for the genus formulae of $X_{\mathrm{sp}}, X_{\mathrm{sp}}^*, X_{\mathrm{ns}}$, and X_{ns}^*.

5. Modular Covers

For $N \geq 1$ an integer, $X_{\mathrm{arith}}(N)$ is the modular curve X_H for $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ given by the inverse image of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right) \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. As a moduli space, X_{arith} parametrizes isomorphism classes of triples (E, ϕ, P), where E is a generalized elliptic curve, P is a point of exact order N, and $\phi\colon E \to E'$ is a cyclic N-isogeny such that $E[N]$ is generated by P and $\ker \phi$. Alternatively, it parametrizes isomorphism classes of pairs (E, ψ), where E is a generalized elliptic curve and $\psi\colon \mu_N \times \mathbb{Z}/N\mathbb{Z} \to E[N]$ is a symplectic isomorphism. $X_{\mathrm{arith}}(N)$ corresponds to the subgroup of matrices that intersects $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ trivially and is a connected component of $X(N)$. Therefore, the genus formula for $X_{\mathrm{arith}}(N)$ is the same as the genus formula for $X(N)$.

In this section, we are interested in modular curves parametrizing full arithmetic level M-arithmetic structure with a compatible torsion point of level MN. Let E be an elliptic curve defined over a number field K of degree d. It is known that the torsion subgroup $\#E_{\mathrm{tors}}(K)$ can be generated by two elements and is uniformly bounded in the degree of K [Mer96]. The modular curve $X_{\mathrm{arith},1}(M, MN)$ is defined by the inverse image of $\left(\begin{smallmatrix} 1 & M* \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{Z}/MN\mathbb{Z})$. As a moduli space it parametrizes triples (E, P, C), where E is an elliptic curve over k, $P \in E[MN](k)$ is a point of order MN, and $C \leq E[M](k)$ is a Gal_k-stable cyclic subgroup of order M such that $E[M] = \langle NP \rangle + C$. The modular curve $X_{\mathrm{arith},1}(M, MN)$ is one of the quadratic refinements of $X_{\mathrm{arith},\pm 1}(M, MN)$, which is defined by the inverse image of $\pm\left(\begin{smallmatrix} 1 & M* \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{Z}/MN\mathbb{Z})$, see Remark 2.1.

The index of $\{\left(\begin{smallmatrix} 1 & M* \\ 0 & * \end{smallmatrix}\right)\}$ in $\mathrm{GL}_2(\mathbb{Z}/MN\mathbb{Z})$ is $M^3N^2\prod_{p|MN}(1-\frac{1}{p^2})$ and since $-I \notin \{\left(\begin{smallmatrix} 1 & M* \\ 0 & * \end{smallmatrix}\right)\}$, the PSL_2-index of the corresponding subgroup is $\frac{1}{2}M^3N^2\prod_{p|MN}(1-\frac{1}{p^2})$. Note that $X_{\mathrm{arith},1}(M, MN) \to X_1(MN)$ is a covering map of degree M. In particular, when $M = 1$, the corresponding modular curve $X_{\mathrm{arith},1}(M, MN)$ is equal to $X_1(N)$, and when $N = 1$, the corresponding modular curve is equal to $X_{\mathrm{arith}}(M)$. The reader can verify that the genus formulae of $X_1(N)$ and $X_{\mathrm{arith}}(M)$ follow from $X_{\mathrm{arith},1}(M, MN)$ after Propositions 5.1, 5.2.

Proposition 5.1. *For $M, N > 1$, there are no elliptic points of orders 2 and 3 for $\Gamma_{\mathrm{arith},1}(M, MN)$.*

Proof. The elliptic points of orders 2 and 3 for $\mathrm{SL}_2(\mathbb{Z})$ are $\mathrm{SL}_2(\mathbb{Z})i$ and $\mathrm{SL}_2(\mathbb{Z})e^{2\pi i/3}$, respectively. Any elliptic points of order $h \in \{2,3\}$ of a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ must map to one of the above two points. Since $X_{\mathrm{arith},1}(M,MN) \to X_1(MN)$ is a covering map, and there are no elliptic points of order h for $\Gamma_1(MN)$ when $M,N>1$, there are no elliptic points of order h for $\Gamma_{\mathrm{arith},1}(M,MN)$. □

Proposition 5.2. *For $M,N>1$, let ε_∞ denote the number of cusps in $X_{\mathrm{arith},1}(M,MN)$. Then we have that:*

$$\varepsilon_\infty = \begin{cases} 1 & \text{if } M,N=1, \\ 2 & \text{if } M=1,\ N=2, \\ 3 & \text{if } M=1,\ N=4, \\ \frac{1}{2}\cdot \sum\limits_{d\mid MN} \varphi\left(\frac{MN}{d}\right)\varphi(d)\gcd\left(M,\frac{MN}{d}\right) & \text{otherwise.} \end{cases}$$

Proof. We follow a similar approach to that in [DS05, Section 3.8]. Let $s'=a'/c', s=a/c \in \mathbb{Q}\cup\infty$. The coset decomposition $\Gamma_{\mathrm{arith},1}(M,MN) = \bigcup_{j=0}^{N-1}\Gamma(MN)\left(\begin{smallmatrix}1 & Mj\\ 0 & 1\end{smallmatrix}\right)$ gives the second equivalence:

$$\begin{aligned} \Gamma_{\mathrm{arith},1}(M,MN)s' = \Gamma_{\mathrm{arith},1}(M,MN)s &\iff s' \in \Gamma_{\mathrm{arith},1}(M,MN)s, \\ &\iff s' \in \Gamma(MN)\left(\begin{smallmatrix}1 & Mj\\ 0 & 1\end{smallmatrix}\right) \text{ for some } j, \\ &\iff \left(\begin{smallmatrix}a'\\ c'\end{smallmatrix}\right) \equiv \pm\left(\begin{smallmatrix}a+Mcj\\ c\end{smallmatrix}\right) \pmod{MN} \text{ for some } j. \end{aligned}$$

This implies that the top row a is determined modulo $\gcd(Mc,MN)$ and since this is a cusp, we also have $\gcd(a,c,MN)=1$. Let $d := \gcd(c,MN)$, there are $\varphi(MN/d)$ elements c such that $0\le c\le MN-1$ and $\gcd(c,MN)=d$. The set

$$\{a : 0\le a\le \gcd(Mc,MN), \gcd(a,c,MN)=1\} = \{a : 0\le a\le \gcd(Md,MN), \gcd(a,d)=1\}$$

has size $\varphi(d)\gcd(M,MN/d)$. Summing over divisors of MN yields the result. □

References

[Bar10] Burcu Baran. Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. *Journal of Number Theory*, 130(12):2753–2772, 2010. 2.4, 4.1, 4, 4, 4.5

[DLM22] Valerio Dose, Guido Lido, and Pietro Mercuri. Automorphisms of Cartan modular curves of prime and composite level. *Algebra & Number Theory*, 16(6):1423–1461, 2022. 2, 2.2, 3, 4, 4.7

[DMS19] Valerio Dose, Pietro Mercuri, and Claudio Stirpe. Double covers of Cartan modular curves. *Journal of Number Theory*, 195:96–114, 2019. 3

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, pages 371–411. Springer New York, New York, NY, 2005. 1, 2, 5

[Lig77] Gérard Ligozat. Courbes modulaires de niveau 11. In Jean-Pierre Serre and Don Bernard Zagier, editors, *Modular Functions of one Variable V*, pages 149–237, Berlin, Heidelberg, 1977. Springer Berlin Heidelberg. 3

[LMF24] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2024. [Online; accessed 12 June 2024]. 1, 1

[Maz77] B. Mazur. Rational points on modular curves. In Jean-Pierre Serre and Don Bernard Zagier, editors, *Modular Functions of one Variable V*, pages 107–148, Berlin, Heidelberg, 1977. Springer Berlin Heidelberg. 1

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, 124(1):437–450, 1996. 5

[RSZB22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with john voight). *Forum of Mathematics, Sigma*, 10, 2022. 1

11 Jun 2025 03:46:29 PDT
250127-Hamakiotes Version 2 - Submitted to LuCaNT

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Research in Number Theory*, 1(1):12, 2015. 1

[SD73] H. P. F. Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms. In Willem Kuijk and Jean-Pierre Serre, editors, *Modular Functions of One Variable III*, pages 1–55, Berlin, Heidelberg, 1973. Springer Berlin Heidelberg. 3

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math*, 15:259–331, 1972. 1, 3

[Shi71] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971. 1, 3, 3, 3, 4, 4, 4

Department of Mathematics, University of Connecticut, Storrs, CT 06269, USA
Email address: asimina.hamakiotes@uconn.edu
URL: https://asiminah.github.io/

Department of Electrical Engineering, KU Leuven, Kasteelpark Arenberg 10/2452, 3001 Leuven (Heverlee), Belgium
Email address: junbo.lau@kuleuven.be
URL: https://junbolau.github.io/

11 Jun 2025 03:46:29 PDT
250127-Hamakiotes Version 2 - Submitted to LuCaNT

TABLE 1. Invariants of genus formula

X_H	i	ε_2
$X_0(N)$	$N \cdot \prod_{p\mid N}\left(1+\frac{1}{p}\right)$	0 if $N \equiv 0 \bmod 4$ $\prod_{p\mid N}\left(1+\left(\frac{-1}{p}\right)\right)$ otherwise
$X_1(N)$, $X_{\pm 1}(N)$	1 if $N=1$ 3 if $N=2$ $\frac{N^2}{2}\cdot\prod_{p\mid N}\left(1-\frac{1}{p^2}\right)$ otherwise	1 if $N=1,2$ 0 otherwise
$X(N)$, $X_{\mathrm{arith}}(N)$	6 if $N=2$ $\frac{N^3}{2}\cdot\prod_{p\mid N}\left(1-\frac{1}{p^2}\right)$ if $N>2$	1 if $N=1$ 0 if $N>1$
$X_{\mathrm{arith},1}(M,MN)$, $X_{\mathrm{arith},\pm 1}(M,MN)$	1 if $M,N=1$ 3 if $M=1,N=2$ 6 if $M=2,N=1$ $\frac{M^3N^2}{2}\cdot\prod_{p\mid MN}\left(1-\frac{1}{p^2}\right)$ otherwise	1 if $M,N=1$ 1 if $M=2,N=1$ 0 otherwise
$X_{\mathrm{sp}}(N)$	$N^2\cdot\prod_{p\mid N}\left(1+\frac{1}{p}\right)$	0 if $2 \mid N$, $\prod_{p\mid N}\left(1+\left(\frac{-1}{p}\right)\right)$ otherwise
$X^+_{\mathrm{sp}}(N)$	$\frac{N^2}{2}\cdot\prod_{p\mid N}\left(1+\frac{1}{p}\right)$	See Proposition 3.4
$X^*_{\mathrm{sp}}(N)$	$\frac{N^2}{2^{\omega(N)}}\cdot\prod_{p\mid N}\left(1+\frac{1}{p}\right)$	See Corollary 3.5
$X_{\mathrm{ns}}(N)$	$N\cdot\varphi(N)$	$\prod_{p\mid N}\left(1-\left(\frac{-1}{p}\right)\right)$
$X^+_{\mathrm{ns}}(N)$	$\frac{1}{2}\cdot N\cdot\varphi(N)$	See Proposition 4.4
$X^*_{\mathrm{ns}}(N)$	$\frac{N}{2^{\omega(N)}}\cdot\varphi(N)$	See Corollary 4.6
$X_{S_4}(p)$	$\frac{1}{24}\cdot p(p^2-1)$	$\frac{1}{4}\cdot\left(p-\left(\frac{-1}{p}\right)\right)$

Table 1 continued on the next page ...

Table 1 continued ...

X_H	ε_3	ε_∞
$X_0(N)$	0 if $N \equiv 0 \bmod 9$ $\prod_{p\mid N}\left(1+\left(\frac{-3}{p}\right)\right)$ otherwise	$\sum_{\substack{d\mid N,\\ d>0}} \varphi\left(\left(d, \frac{N}{d}\right)\right)$
$X_1(N)$, $X_{\pm 1}(N)$	1 if $N = 1, 3$ 0 otherwise	1 if $N = 1$ 2 if $N = 2$ 3 if $N = 4$ $\frac{1}{2}\cdot\sum_{d\mid N}\varphi(d)\varphi\left(\frac{N}{d}\right)$ otherwise
$X(N)$, $X_{\text{arith}}(N)$	1 if $N = 1$ 0 if $N > 1$	1 if $N = 1$ $\frac{i}{N}$ if $N > 1$
$X_{\text{arith},1}(M, MN)$, $X_{\text{arith},\pm 1}(M, MN)$	1 if $M = 1$ and $N = 1, 3$ 0 otherwise	See Proposition 5.2
$X_{\text{sp}}(N)$	0 if $2 \mid N$ or $3 \mid N$, $\prod_{p\mid N}\left(1+\left(\frac{-3}{p}\right)\right)$ otherwise	$N\cdot\prod_{p\mid N}\left(1+\frac{1}{p}\right)$
$X^+_{\text{sp}}(N)$	0 if $2 \mid N$ or $3 \mid N$, $\frac{1}{2}\cdot\prod_{p\mid N}\left(1+\left(\frac{-3}{p}\right)\right)$ otherwise	$\frac{N}{2}\cdot\prod_{p\mid N}\left(1+\frac{1}{p}\right)$
$X^*_{\text{sp}}(N)$	See Corollary 3.5	See Corollary 3.5
$X_{\text{ns}}(N)$	$2^{\omega(N)}$ if $p \equiv 2 \pmod 3$ for all $p \mid N$, 0 otherwise,	$\varphi(N)$
$X^+_{\text{ns}}(N)$	$2^{\omega(N)-1}$ if $p \equiv 2 \pmod 3$ for all $p \mid N$, 0 otherwise,	1 if $N = 2$, $\frac{1}{2}\cdot\varphi(N)$ otherwise
$X^*_{\text{ns}}(N)$	See Corollary 4.6	See Corollary 4.6
$X_{S_4}(p)$	$\frac{1}{3}\cdot\left(p-\left(\frac{-3}{p}\right)\right)$	$\frac{1}{24}\cdot(p^2-1)$